Revised: August 28, 2024

Monitoring SD-Routing Alarms and Events

Information about Alarms and Events on SD-Routing Devices

SD-Routing Devices record, and store various events generated by control components and routers whenever a state or condition changes in the network. When an event is generated, the device reports it by sending a notification to the Cisco SD-WAN Manager. The SD-WAN manager processes them and runs a correlation algorithm using the correlating engine or alarms engine to determine whether an event indicates a problem, evaluates its severity, and determines if it warrants creating an alarm. While not all events escalate to alarms, every alarm originates from an event.

The SD-WAN Manager then sends a Remote Procedure Call (RPC) to retrieve these alarms once generated and the device replays those notifications to the Manager once the control connection is up. The system subsequently filters these notifications, correlates related events, and consolidates them by severity levels. These alarms not only assist in monitoring and troubleshooting the network but can also be used for further root cause analysis of the underlying issues.

Limitations for Alarms and Events on SD-Routing Devices

SD-Routing Devices can maintain a circular buffer for storing 256 alarms only.

Types of Alarms and Events

Cisco SD-WAN Manager groups the alarms and events based on its severity:

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

View and Manage Alarms on Cisco SD-WAN Manager

Use the alarms screen to display detailed information about alarms generated by control components and routers in the network. Navigate to **Monitor** > **Logs** > **Alarms** to open the Alarm window which displays alarms in graphical and tabular format along with the heatmap view of the alarm.

When you click the **Bell** icon located at the top-right corner of the title bar, the Notifications pane appears. To filter or group alarms by Object, Severity, Type, and time (24 or 72 hours), click the **Gear** icon in this pane. By default, alarms are displayed for the last 24 hours.

View Alarm Details

To view alarm details such as alarm name, severity, and alarm description follow the below steps.

Customize Alarms Table

To view the probable cause of the alarm, impacted entities, and other details in the table displayed on the screen, click the **Gear** icon and select the preferred columns to display. The specifics of the available columns are listed below.

Parameters	Description
Impacted entities	Impacted entities specify the host used for network communication and identification within the IP address space of the local network.
Impacted entities details	Impacted entity details specifies the network component on the host with the IP address and the interface.
Severity	The severity indicates the seriousness of the alarm. There are four types of severity: critical, major, medium, minor.
Object	Alarms are grouped based on either the device or site for which the alarm is generated.
Alarm Type	Indicates that the alarms are categorized according to their type.
Message	Specifies the description of the alarm.
Related Events	Displays events, related to an alarm, that occurs around the time the alarm is generated.
Date and Time	Displays the Date and Time when the alarm was generated.
Cleared Date and Time	Displays the Date and Time when the alarm was cleared.
Action	Displays an ellipsis, which, when clicked, opens a menu providing you with detailed information about the alarm.

Set Alarm Time Range

Click on the **24 Hours** icon at the top-left of the screen to select the Time Range and customize the range by selecting the preferred start day, time and end date, time. By default, alarms and events are displayed for the last 24 hours.

Setup Advanced Alarm Filters

You can use the following steps to filter alarms and view details of a specific/multiple alarms

Step 1 Click **Advanced Filter** and select **Site** or **Device** for which you want to view alarms and choose the following fields.

Field	Description
Object List	Choose either **Site ID** or **Device** for which you want to view alarms. You can choose more than one site or device.
Severity	Select the preferred alarm **severity** levels from the drop-down list. You can specify multiple severity levels.
Alarm Type	Select the preferred **alarm type** that is supported on SD-Routing Devices. You can either select All or specify multiple alarm types.

Step 2 Click **Apply Filters** to view alarms that match the filter criteria.

Export Alarm Details

Step 1 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. (Here mm, dd, and yyyy refer to the month, day, and year the file was downloaded).

Step 2 Open the downloaded file to view alarm details.

Configure Email Notifications for Alarms

You can configure Cisco SD-WAN Manager to enable, send, edit and delete email notifications.

Enable Email Notifications

Configure SMTP and email recipient parameters to enable email notifications for alarms. Follow these steps to complete the configuration.

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.

Step 2 In **Alarm Notifications**, choose **Enabled**.

Step 3 Check the **Email Settings** check box.

Step 4 Choose the security level for sending the email notifications. The security level can be **None**, **SSL**, or **TLS**.

Step 5 In the **SMTP Server** field, enter the name or the IP address of the SMTP server to receive the email notifications.

Step 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.

Step 7 In the **From address** field, enter the email address to include as the sender in email notifications.

Step 8 In the **Reply to address** field, enter the email address to include in the Reply-To field of the email. This address can be a no-reply address, such as noreply@cisco.com.

Step 9 Check the **Use SMTP Authentication** check box to enable SMTP authentication to the SMTP server.

Step 10 Enter the username and password to use for SMTP authentication. The default user email suffix is appended to the username. Note, the password that you type is hidden.

Step 11 Click **Save**

Send Email Notifications

To send email notifications, click **Add Alarm Notification** or click the **bell icon** at the top-right corner of the title bar and follow the below steps.

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. For more details, see *Enable Email Notifications*.

Step 1 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.

Step 2 In the **Object Type** field, select **Site or Device** for which you want to view alarms.

Step 3 In the **Object List** field, choose either **Site ID** or **Device** for which you want to view alarms. You can choose more than one site or device

Step 4 In the **Severity** field, choose one or more alarm severity levels from the drop-down list.

Step 5 In the **Type** field, choose one or more alarms.

Step 6 In the **Delivery Method** field, enter the following:

a) Check the **Email** check box and fill out the Email recipients. You can add up to 5 recipients. 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 when an alarm notification event occurs and choose a channel for Webhook. The available channels are Cisco Webex, Slack and Custom.

- In the **WebHook URL** field, enter the URL of the webhook server.
- Enter the **Username** and **Password** to authenticate the webhook server.
- In the **WebHook Threshold** field, enter the threshold value. 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.

Step 7 Click **Add Notification**.

Edit Email Notifications

To edit email notifications, navigate to**Monitor** > **Logs** > **Alarms**. Click **Alarm Notifications** to view a list of configured notifications. Select the **Edit** icon next to the preferred notification and click **Update** when done.

Delete Email Notifications

To delete email notifications, navigate to **Monitor** > **Logs** > **Alarms**. Click **Alarm Notifications** to view a list of configured notifications. Choose the **Trash Bin** icon next to the preferred notification and Click **OK** in the dialog box to confirm.

View and Manage Events on Cisco SD-WAN Manager

Use the events screen to display detailed information about events generated by SD-Routing Devices. Navigate to **Monitor** > **Logs** > **Events**to open the Event window which displays events in graphical and tabular format along with the heatmap view of the alarm.

View Event Details

To view event details such as event time, severity, and hostname follow the below steps.

Customize Events Table

To view the component, hostname and other details in the table displayed on the screen, click the **Gear** icon and select the preferred columns to display. The specifics of the available columns are listed below.

Parameters	Description
Message	Specifies the description of the alarm.
Event Time	Displays the time of the event.
Hostname	Specifies the name of the host.
System IP	Displays the system IP of the devices.
Name	Specifies the event name.
Severity	Indicates the seriousness of the event. There are three types of event severity: critical, major, minor.
Component	Specifies the components that caused the event.
Details	Displays the event details.
Action	Displays an ellipsis, which, when clicked, opens a menu providing you with detailed information about the alarm.

Set Event Time Range

Click on the **24 Hours** icon at the top-left of the screen to select the Time Range and customize the range by selecting the preferred start day, time and end date, time. By default, events are displayed for the last 24 hours.

Setup Advanced Event Filters

You can use the following steps to filter Events and view details of a specific/multiple events.

Step 1 Click **Advanced Filter** and select **Site or Device** for which you want to view events and choose the following fields.

Field	Description
Object List	Choose either **Site ID** or **Device** for which you want to view events. You can choose more than one site or device.
Severity	Select the preferred event severity levels from the drop-down list. You can specify multiple severity levels.
Event Type	Select the preferred event type that is supported on SD-Routing Devices. You can either select All or specify multiple event types.

Step 2 Click **Apply Filters** to view events that match the filter criteria.

Export Event Details

Step 1 Click **Export** to export data for all events to a file in CSV format. 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 alarms-mm-dd-yyyy.csv. (Here mm, dd, and yyyy refer to the month, day, and year the file was downloaded).

Step 2 Open the downloaded file to view event details.