Monitor Alarms and Events

This section explains the following:

Monitor Alarms and Events

This chapter explains about monitoring the alarms and events.

Alarms and Alarm Summary

You can view Alarms and Alarm Summary pages through **Monitor** > **Alarms & Events**.

The Alarms tab displays the following information for each alarm in the Alarm browser:

Severity

Indicates the severity of the alarm which can be, critical, major, minor, warning. The collapsible icon for an alarm displays the General Info of the alarm, Messages, Annotation, Recommended Actions for an alarm.

To view events associated with an alarm, rest the mouse over the alarm severity, and click the quick view icon. The **Events for Alarm** page is displayed, containing the following details:

- Description - Alarm description.
- Status - Device that triggered the alarm.
- Time - Date and time when the alarm occurred.

This summary windows lists only the five latest events. To see the complete list, see **Event History**.

In the **Events for Alarm**, you can click:

- The **See Event History link**to display the events associated with the selected alarm.
- The **Monitor Endpoint** or **Monitor Conference**link to launch the Endpoints Monitoring or **Conference Monitoring** page. This link is displayed only for conference and endpoint alarms.

Clipboard icon/Is Annotated

Indicates the alarm has user notations.

Status

Indicates the status of the alarm.

It shows the alarm clearing status details.

Alarm Name

Name of the generated alarm. Rest the mouse over the alarm name and the Quickview icon that is displayed, to view details of the alarm selected.

Customer

If you have installed Cisco Prime Collaboration Assurance in MSP mode, the customer that the device belongs to, is displayed for both Alarms and Alarm Summary.

Device Name

Displays the name of the device that triggered the alarm.

Device IP

Displays the IP address of the device. You can launch the endpoint or the infrastructure device log in page using the link.

You cannot launch the endpoint or the infrastructure device log in page using this link, if you have deployed Cisco Prime Collaboration Assurance in MSP mode.

Component Name

Device name, or the name of component such as a device pool, an interface.

Last Updated

Displays the date and time when the alarm occurred.

Device Type

Displays the type of the device.

Owner

Displays the name of the person to whom this alarm is assigned. (If a name was entered.)

Description

Displays a short description about the alarm.

Category

Displays the category of alarm. For example: conference, endpoint, service infrastructure.

Endpoint Name

Indicates the name assigned to the endpoint for ease of identification. By default, the **Endpoints Name** column is hidden. To see all the columns, click the Settings option on the top right corner.

Model

Displays the device model, such as ciscoEX90, ciscoCTS500, ciscoC20, and so on.

Private IP address

If you have installed Cisco Prime Collaboration Assurance in MSP mode, private IP address of the device is displayed. By default, the **Private IP Address** column is hidden. To see all the columns, click the Settings option on the top right corner.

Overall, the alarm browser allows you to:

- View events associated with an alarm—Rest the mouse over the icon next to alarm status for the popup window to appear displaying all the events for the alarms.
- Clear or acknowledge an alarm.
- Assign the alarm—Check the desired check box, click **Assign to me** from the assign drop-down list.
- Add Annotation - Check the desired check box, click the **Annotate** drop-down list to add notes.
- Delete Alarm - Check the desired check box, click **Delete**.
- Set up Email Notification - Check the desired check box, click **Email Notification**. Enter the recipient addresses, comments, and subject, then click **Submit**. For a list of supported alarms and events, see Supported Alarms and Events for Cisco Prime Collaboration.

Alarm Summary

Alarm Summary provides a summary of the alarms for each device.

The following factor distinguishes Alarm Summary from Alarms: When you select a device, the alarms and events that correspond to the selections appear in the Alarms and Events for *device* pane at the bottom of the page. You can export the alarms as a CSV or PDF file. To export the alarms, select the desired alarms, and click the export icon on the top right of the Alarm Summary pane.

The Alarm Summary displays the following information:

Severity

Alarm severity icon. Indicates the severity of the alarm.

Last 15 Minutes

Indicates that this device is one of the most recent in the table (within the last 15 minutes). Devices are sorted based on the time of the most recent event status changes.

Device Name

Device name or IP address.

Device IP

Device IP. Click on the quick view icon to launch the Device 360° View.

Type

Device type.

Severity Columns

- Critical - Total number of critical alarms.
- Major - Total number of major alarms
- Minor - Total number of minor alarms
- Warning - Total number of warning alarms.

Last Update Time

Time and date of alarm update (indicates activity, such as an alarm recurrence, alarm acknowledgment, the addition of a note, and so forth). Alarms are grouped by severity, and within severities, alarms with the latest change are listed first.

Endpoint Name

Indicates the name assigned to the endpoint for ease of identification. By default, the **Endpoints Name** column is hidden. To see all the columns, click the Settings option on the top right corner.

Private IP address

If you have installed Cisco Prime Collaboration Assurance in MSP mode, private IP address of the device is displayed. By default, the **Private IP Address** column is hidden. To see all the columns, click the Settings option on the top right corner.

Events

The Events tab displays the following information:

ID

Event unique identification number.

Severity

Event severities include: Critical, Major, Minor, Warning, and Informational. Click the title to sort the events list by severity (ascending or descending order). If any event is cleared, its severity changes to informational.

Status

The current status of the event.

Event Name

The name of the event. Rest your mouse over the quick view icon to view the event details. Click **Customize Event** to cross-launch to the **Event Customization** page, which displays the details of the selected event. Expand the event and click Custom Rule to edit the event details.

Customer

If you have installed Cisco Prime Collaboration Assurance in MSP mode, the customer that the device belongs to, is displayed in the Events pane.

Device Name

The name of the event. Rest your mouse over the event name to view the event details.

Device IP

Displays the IP address of the device. You can launch the endpoint or the infrastructure device using the link.

Component Name

Device name, or the name of component such as a device pool, an interface.

Last Updated

Displays the date and time when the event occurred.

Device Type

Displays the type of the device.

Category

Displays the alarm assigned category, such as conferences, endpoints, and so on.

Description

Description of the event.

Endpoint Name

Indicates the name assigned to the endpoint for ease of identification. By default, the **Endpoints Name** column is hidden. To see all the columns, click the Settings option on the top right corner.

Model

Displays the device model, such as cat4506, ciscoMCS7828I, and so on.

Private IP Address

If you have installed Cisco Prime Collaboration Assurance in MSP mode, the private IP Address of the device is displayed. By default, the **Private IP Address** column is hidden. To see all the columns, click the Settings option on the top right corner.

Note

- Click the refresh icon to view the latest list of events raised.
- If you have installed Cisco Prime Collaboration Assurance in MSP mode, you can see the customer to which the device belongs to.
- At any point, to see the Alarm Browser or Alarm Summary, click the links available at the bottom right.

View Call Events

Cisco Prime Collaboration Assurance displays the Cisco TelePresence Management Suite (TMS) informational events. It displays call connected or disconnected information for Cisco TelePresence System Profile MXP Series devices, Cisco TelePresence Integrator C Series codecs, and Cisco TelePresence Video Communication Server (VCS).

Call events can be displayed for only one supported device at a time.

To view call events:

Step 1 **For Cisco Prime Collaboration Release 11.5 and later**

Choose **Inventory** > **Inventory Management**

Step 2 Select a device, and Click **Call Events**.

Note Call events are displayed only for Cisco VCS, MXP, MCU devices, and codecs.

Step 3 The Call Events page displays the following details:

For MXP and Codecs:

- Start Time—The call start time
- Remote Site—The site to which the call was made.
- Call State
- Duration
- Call Direction—Whether an incoming or outgoing call.
- Call Protocol—H323/SIP
- Encryption Mode
- Cause
- Bandwidth
- Call ID

For VCS:

- Time
- Source Address
- Source Alias
- Destination
- Address
- Destination Alias
- Duration
- Call State
- Call
- Protocol
- Bandwidth
- Call Type

Notes for Alarms and Events

1. Alarms that are dependent on the polling interval, might have a situation where the alarm is raised and cleared before the next poll. Therefore, it is not being reported to Cisco Prime Collaboration Assurance.
2. **Behavior of SIPTrunk Out Of Service (OOS) Correlation Alarm :**

   SIP Trunk OOS : This correlation alarm is introduced to track and combine multiple SIPTrunk OOS Alarms and generate one single correlated Alarm at the Cluster level. Correlation happens in a span of 2 minutes time window.

   Following are the conditions for the correlation alarms to get cleared :

- SIPTrunk OOS Correlation alarm gets cleared when the associated individual SIPTrunk OOS alarms are cleared by processing InService Syslogs.
- There is a time base clear as well, where the correlation alarms are cleared automatically after 24 hours.

Using the conditions mentioned above, correlation alarm is cleared in any one of the following scenarios :

Scenario 1:

- SIPTrunk OOS alarms are raised in Cisco Prime Collaboration Assurance.
- Individual SIPTrunk OOS alarms are correlated and Corresponding SIPTrunk OOS correlation alarm is raised at the cluster level.
- SIPTrunk OOS gets cleared once the SIPTrunks are back and the SIPTrunk OOS also gets cleared with that.

Scenario 2:

- SIPTrunk OOS alarms are raised in Cisco Prime Collaboration Assurance.
- Individual SIPTrunk OOS alarms are correlated and Corresponding SIPTrunk OOS correlation alarm is raised at cluster level.
- SIPTrunk stays down for more than 24 hours.
- SIPTrunk OOS gets cleared after 24 hours based on 24 hours time based clear and the SIPTrunk OOS individual alarms will clear once the SIPTrunk is back Inservice and syslog is processed for that.

Scenario 3 :

- Individual SIPTrunk OOS alarms are raised and cleared rapidly within the 2 minutes correlation window.
- Correlation engine will still run and raise the SIPTrunk OOS correlation alarm and now as the associated individual alarm has already cleared, the SIPTrunk OOS will be left alone.
- Then the correlation alarm gets cleared automatically after 24 hours, based on 24 hours time based clear.

3. In a multi-node call manager cluster, if the same alert exists on more than one node at the same time, PCA displays one latest alert.
4. Polling frequency of RTMT alerts

   For Cisco Prime Collaboration Release 12.1 and later

   The default polling frequency of RTMT alerts for Small, Medium, and Large setups is 1 minute and the recommended polling frequency for Very Large setup is 2 minutes.