Set Threshold Rules

This section explains the following:

Set Threshold Rules

This section explains how to customize alarms and events to suit your business needs.

Threshold Rules

You can configure the devices to generate events when certain parameters cross predefined thresholds.

For Cisco Prime Collaboration Release 11.5 and later

You can perform the settings at **Alarm & Report Administration** > **Event Customization** > **Threshold Rules**.

The threshold rules page contains two tabs—Basic and Advanced. The Basic tab lists the inline events in Cisco Prime Collaboration Assurance that you can raise or suppress.

The Advanced tab lists all the available events and also allows you to create custom events. To create custom events: click **Add Event**; select a cluster or device from the drop-down; enter the required details; and click **Save**.

For Cisco Prime Collaboration Release 11.1 and later

For each of the events listed in both these tabs, you can add or edit custom threshold by expanding the event and clicking **Custom Rule**. In the Basic tab, you can only create threshold based on the device type selected whereas in the Advanced tab, you can also set threshold rules, such as scheduling alerts, setting frequency, severity, and so on, for the thresholds that you create. You can add, edit, or delete the custom threshold rules at the device level or device type level. For the changes to apply for all devices, check the Apply for All Devices check box.

In both Basic and Advanced tabs, you can add additional information about events in **Notes for Email** and the note should not exceed 1000 characters. You can also edit or delete the note in **Notes for Email** using **Edit** or **Delete** link. When you edit the note, keep minimum of one character in the **Notes for Email**. This additional information is sent as an email notification.

We do not recommend you to add special characters like dollar ($), vertical bar (|), and tilde (~) in **Notes for Email**.

On clicking the **Custom Rule** in the Advanced tab, the Add Alert Settings page is displayed. Select the **Device Type**, **Cluster**, and click **Next**. In the Add Threshold Rules tab, enter the required details and click **Save**.

Apart from adding events and thresholds, you can also perform the actions mentioned in the table below:

Actions	Basic	Advanced
Change Severity	Yes Check the box against Name—To select all the events; or check the boxes of the events of your choice and click **Change Severity**.	Yes Check the box against Name—To select all the events; or check the boxes of the events of your choice and click **Change Severity**. You can also change the severity of custom threshold using the Custom Rule option and that of custom event using the Edit Threshold option.
Raise or Suppress events	Yes Check the box against Name—To select all the events; or check the boxes of the events of your choice and click **Raise** or **Suppress**.	Yes Check the box against Name—To select all the events; or check the boxes of the events of your choice and click **Raise** or **Suppress**.
Raise or Suppress thresholds	Yes Expand the event, select threshold, and select **Raise**, or **Suppress** from the drop-down.	Yes Expand the event, select threshold, and select **Raise**, **Suppress**, or **Conditional** from the drop-down.

Edit, Reset, and Delete existing thresholds	No You can edit or reset the threshold settings, but cannot delete. To edit or reset the threshold, expand the event, edit the threshold settings, and click **Save Changes**.	Yes To edit or reset the threshold, expand the event, edit the threshold settings, and click **Save Changes**. You can delete only the custom thresholds. To delete a threshold, expand the event, select the threshold, and click **Delete**.
Edit or Delete Events	No	Yes Expand the event, edit the settings, and click **Save**. You can delete only the custom events. To delete an event, select the check box and click **Delete**.
Clone for events	No	Yes Click **Clone**, fill in the details, and click **Save**. **Note** You can use the clone option only for CVP and Unified CCE devices. This option is disabled for events of the other device types such as Communication Manager, Media Sense, IM and Presence, Finesse, and so on.

Configure TelePresence Endpoint Threshold—Device Level

For Cisco Prime Collaboration Release 11.5 and earlier

Perform the following procedure to configure the thresholds for Cisco TelePresence endpoints at a device level, if you do not want the thresholds to be applied at a global level.

Procedure

Step 1 Choose **Assurance Administration** > **Event Customization** > **Threshold Rules**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Alarm & Report Administration** > **Event Customization** > **Threshold Rules**.

Step 2 In the **Basic** tab, expand the Jitter, Packet loss or Latency event and modify the values for Minor, Major, and Critical Thresholds.

You also have the option to Raise or Suppress the event.

Step 3 Click **Save Changes**.

You can also apply the changes to all the devices of a device type or for selected devices of a device type. To do this, click **Custom Rule** and select the Device Type. To apply for all the devices, select All Devices of this Type. To apply the changes for selected devices, click Select Devices, select the devices of your choice and click **Save**.

To search for a device, select **Quick Filter** from the **Show** drop-down list and type the Host Name or IP Address of that device.

Configure TelePresence Endpoint Thresholds—Global

For Cisco Prime Collaboration Release 11.1 and earlier

You can set up Cisco Prime Collaboration Assurance when the threshold value exceeds the configured limit for Rx packet loss, jitter, or latency for all TelePresence devices.

To configure thresholds for TelePresence endpoints:

Procedure

Step 1 Choose **Assurance Administration** > **Conference Path Threshold Settings**.

Step 2 Modify the values for Rx Packet Loss, Average Period Jitter or DSCP and click **Save**.

You can also modify the Polling Interval for the thresholds. If you want to reset the values to default, click **Reset to Default**.

When the TelePresence threshold value exceeds the defined value, you can enable to start automatic troubleshooting. Go to **Assurance Administration** > **Event Customization** > **Threshold Rules**; in the Basic tab, expand the Jitter, Packet loss or Latency event and choose Minor, Major, or Critical from the Automatic Troubleshooting drop-down list. To disable, choose Disabled from the drop-down list.

What to do next

For information on how to configure Cisco TelePresence endpoints at a device level, see the "Configure TelePresence Endpoint Threshold—Device Level" section in the Cisco Prime Collaboration Assurance Guide-Advanced, 11.x.

Configure Thresholds for Conference Troubleshooting

For Cisco Prime Collaboration Release 11.6 and later

You can configure thresholds in Cisco Prime Collaboration Assurance to display the metric violation in the path, or to start automatic troubleshooting when the threshold value exceeds the configured limit for Rx packet loss, jitter, or latency for all TelePresence devices.

To configure thresholds for TelePresence endpoints:

Procedure

Step 1 Choose **Alarm & Report Administration** > **Conference Path Threshold Settings**.
The **Conference Path Threshold Settings** page is displayed.

Step 2 Modify the values for Memory Utilization and Rx Packet Loss if you want to change the color of the bubbles in path statistics.

You can also modify the values for CPU Utilization, Average Period Jitter, and DSCP for any metric violation in the path. A blue badge information icon is displayed in the Path View and Quick View if the threshold value exceeds the configured limit for Rx Packet Loss, Average Period Jitter, or DSCP for all devices.

Step 3 (Optional) Modify the values for Flows Statistics Polling Interval if you want to modify the polling interval.

Step 4 Click **Save**.

If you want to reset the values to default, click **Reset to Default**.

Enable Automatic Troubleshooting for TelePresence Endpoints

For Cisco Prime Collaboration Release 11.6 and later

Perform the following procedure to enable automatic troubleshooting of a conference when the threshold value exceeds the defined value for packet loss, jitter, and/or latency.

Procedure

Step 1 Choose **Alarm & Report Administration** > **Event Customization** > **Threshold Rules**.

Step 2 In the **Basic** tab, expand the Jitter, Packet loss, or Latency event and choose **Minor**, **Major**, or **Critical** from the **Automatic Troubleshooting** drop-down list.

To disable, choose **Disabled** from the drop-down list.

Overview of Device Pool Thresholds

A device pool is a logical group of devices. It provides a convenient way to define a set of common characteristics that can be assigned to devices, for example, the region in which the devices are located.

Within Cisco Prime Collaboration Assurance, device pools are displayed only after a cluster discovery is completed. If no device pools display in the thresholds window, schedule the inventory to run. By default, cluster device discovery is not scheduled.

Note If there are no devices attached to a device pool, Cisco Prime Collaboration Assurance does not display the device pool even after completing the cluster device discovery.

The device pool threshold settings in Cisco Prime Collaboration Assurance allow the user to configure the amount of aggregated events.

- If you raise the default or current percentage settings for any of the device pool thresholds, you decrease the amount of aggregated events you will receive.
- If you lower the default or current percentage settings for the device pool threshold, you will receive more aggregated events from this device pool.

If the number of impacted phones is equal to the threshold value, Cisco Prime Collaboration Assurance raises one service quality event.

For example, if the device pool contains 100 phones and 10 phones are impacted with a network problem, when the device pool threshold is set to 10% you will receive one aggregated event about this device pool.

After an aggregated event is raised, no other aggregated events will be sent until this event is cleared. To clear an aggregated event, all individual device or service quality events must be cleared first.

Note For the "ServiceQualityThresholdCrossed" event, Cisco Prime Collaboration Assurance rounds off the threshold value from decimal to whole number.

For Cisco Prime Collaboration Release 11.6

Note For both the "ServiceQualityThresholdCrossed" and "PhoneUnregThresholdExceeded" events, Cisco Prime Collaboration Assurance rounds off the threshold value from decimal to whole number.

If you have deployed Cisco Prime Collaboration Assurance in MSP mode, the device pools that are displayed belong to the customer(s) you have selected using the global Customer Selection field.

For Cisco Prime Collaboration Release 12.1 and later

Note For both the "ServiceQualityThresholdCrossed" and "EndpointUnregThresholdExceeded" events, Cisco Prime Collaboration Assurance rounds off the threshold value from decimal to whole number.

If you have deployed Cisco Prime Collaboration Assurance in MSP mode, the device pools that are displayed belong to the customer(s) you have selected using the global Customer Selection field.

Cisco Prime Collaboration Assurance considers these device pool threshold events as device events and not service level events.

Edit Device Pool Thresholds

Perform the following procedure to view and configure device pool thresholds by using Cisco Prime Collaboration Assurance.

Procedure

Step 1 Choose **Event Customization** > **Correlation Rules**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Alarm & Report Administration** > **Event Customization** > **Correlation Rules**.

Step 2 Select EndpointUnregThresholdExceeded or ServiceQualityThresholdCrossed event.

If no device pools appear in this window, schedule the cluster inventory to run.

Step 3 Check the check box next to the device pool you want to view or edit.

Step 4 Click **Edit**.

Step 5 To edit the current default thresholds:

a) Select a group, change the default threshold, and click **Edit**.

b) In the Phone Unregistration Threshold/Service Quality Threshold dialog box, edit the threshold and click **Save**.

To reset all parameter types with Cisco Prime Collaboration Assurance default settings:

c) Check the check box for All Device Pools/CMEs and click **Revert**.

d) Click **Save**.

Although the changes are saved in the database, they are not yet applied to the IP fabric.

To be notified automatically when you receive this type of aggregated event, you can set up a notification to have an email sent when this event is raised. For details on how to set up a notification email, see Configure Notifications section in Cisco Prime Collaboration Assurance Guide - Advanced.

Overview of Voice Call Grade Settings

The voice quality grading is performed based on Severely Conceal Seconds Ratio (SCSR) (%). It helps you to get better call quality measurement throughout the entire call duration than MOS based grading. It also supports various audio codecs especially wide-band codec. For more information on MOS to SCSR(%) change, see Cisco Prime Collaboration Assurance and Analytics: Grade VoIP Calls for Efficiency and Reliability White Paper.

The call is categorized as long call/short call based on duration of call. If the duration of the call is greater than or equal to 20 seconds then it is long call and the duration of the call is less than 20 seconds then it is short call.

You can update the threshold value for long call SCSR (%) and short call SCSR (%). The threshold settings for short call SCSR (%) and long call SCSR (%) are different. The following table details the available call grades:

Call Grade	Explanation
Poor	If the SCSR (%) value of call is greater than threshold value of long call SCSR (%) or short call SCSR (%) then call grade is Poor.
Acceptable	If the SCSR (%) value of call is greater than or equal to threshold value of long call SCSR (%) or short call SCSR (%) then call grade is acceptable.
Good	If the SCSR (%) value of call is less than threshold value of long call SCSR (%) or SCSR (%) then call grade is good.

To configure the threshold settings for long call SCSR (%) or short call SCSR (%), choose **Alarm & Report Administration** > **CDR Analysis Settings** > **Configure Voice Call Grade** and enter the threshold values in the appropriate fields. If you want to reset the threshold values to default settings, click **Reset to Default**.

Add Dynamic Syslogs

Cisco Prime Collaboration Assurance enables you to add unsupported syslogs. You must get the exact syslog details from the device before you use the syslog in Cisco Prime Collaboration Assurance; for example, you must enter the exact syslog name. The syslog name you enter is taken as the event name.

You can set the severity and the time by which the syslog must be cleared.

Note Dynamic Syslog supports all the devices except TP_CONDUCTOR and non-Cisco devices.

Note Syslog communication is supported through UDP.

We recommend that you do not add:

- Syslogs that are likely to create an excessive load on Cisco Prime Collaboration Assurance due to a possible flood of syslogs.
- More than 20 syslogs.

For Cisco Prime Collaboration Release 11.1 and later

You can add additional information about events or alarms in **Notes for Email** and the note should not exceed 1000 characters. You can also edit or delete the note in **Notes for Email** using **Edit** or **Delete** link. When you edit the note, keep minimum of one character in the **Notes for Email**. This additional information is sent as an email notification.

We do not recommend you to add special characters like dollar ($), vertical bar (|), tilde (~) in **Notes for Email**.

To add syslogs:

Procedure

Step 1 Choose **Assurance Administration** > **Event Customization** > **Syslog Rules**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Alarm & Report Administration** > **Event Customization** > **Syslog Rules**.

Step 2 Click **Add Event**.

The New Syslog Event window opens. Enter the following:

- Syslog Name
- Event Description
- Event Severity
- Event Clear Interval

Step 3 (Optional) Check the **Raise Event for Each Occurrence** check box.

Use this option judiciously. Cisco Prime Collaboration Assurance raises an event for each syslog. If syslogs are raised with unique details each time, this is a feasible option.

Step 4 Click **Save**.

You can:

- Use the **Edit** option to change the event name, severity, and check or uncheck the **Raise Event for Each Occurrence** check box.
- Customize the syslog name or event severity. To do this, go to the Event Customization page. See the Set Threshold Rules, on page 1 for details.

Example

Below is an example for unsupported syslog, which is raised when ITLRecovery certificate that has not been backed up in the cluster.

Enter the following values:

- Syslog Name - ITLRecoveryCertBackup
- Event Description - ITLRecoveryCertBackup Event
- Event Severity - Major
- Event Clear Interval -1 hour

Note Event Severity and Event Clear Interval values are configurable.

<187>9009: Jul 31 2017 16:05:38.777 IST :%UC_CERT-4-ITLRecoveryCertBackup: %[Message=][AppID=Cisco Certificate Monitor][ClusterID=ccm234][NodeID=cucm107886234]: This cluster has an ITLRecovery certificate that has not been backed up. Taking a manual backup of this certificate is recommended to avoid the need to manually delete the ITL file from every phone in the cluster after certain cluster reconfiguration operations

Correlation Rules

When an event is raised from connected devices, Cisco Prime Collaboration Assurance applies correlation rules. In the following table, for a device, when event A and event B (or a single event) occurs at a certain frequency within a specified time window, Cisco Prime Collaboration Assurance correlates these events and raises an alarm. The alarm is auto-cleared within 24 hours.

For example, whenever a Utilization threshold value changes, Cisco Prime Collaboration Assurance generates a High Utilization event. If the High Utilization event occurs thrice within the 20 minute time interval, High Utilization Detected alarm is raised.

The following are the predefined correlation rules in Cisco Prime Collaboration Assurance:

If you have added the Cisco Prime Collaboration Contact Center Assurance license, certain correlation rules can be exclusively applied for Cisco Prime Collaboration Contact Center Assurance. For details, see the "Contact Center Correlation Rules" section in the Cisco Prime Collaboration Contact Center Assurance Guide.

Name of the Correlation Rule	Main Events Responsible for the Alarm to be Raised	Symptom Events that Occur Due to the Main Event	Name of the Correlated Alarm	The Correlated Alarm is Raised When ...	Window Time (in min) within which the Main Events and Symptom Events are Received	No of Occurrences
Call Throttling Detected	Code Yellow, CpuPegging	NA	CodeYellow	Both the main events occur.	20	1

Name of the Correlation Rule	Main Events Responsible for the Alarm to be Raised	Symptom Events that Occur Due to the Main Event	Name of the Correlated Alarm	The Correlated Alarm is Raised When ...	Window Time (in min) within which the Main Events and Symptom Events are Received	No of Occurrences
Interface Flapping	OperationallyDown, OperationallyDown cleared	NA	Interface Flapping	OperationallyDown is followed by OperationallyDown cleared event alternatively for more than three instances.	20	3
Repeated Location Bandwidth Out Of Resource	LocationBWOutOf Resources	NA	Repeated Location Bandwidth Out Of Resource	LocationBWs-OutOfResource is raised on Cisco Unified Communications Manager for three or more instances.	20	3
WAN Link Outage Detected	Unresponsive	NA	Wan Link Outage Detected	Unresponsive event is triggered.	10	NA
Note This rule cannot be edited or deleted from user interface.						
VM Down	VMDown	Unreachable	VMDown	VMDown trap is received from vCenter and Unreachable event for VM is received, based on ICMP polling.	5	NA

Name of the Correlation Rule	Main Events Responsible for the Alarm to be Raised	Symptom Events that Occur Due to the Main Event	Name of the Correlated Alarm	The Correlated Alarm is Raised When ...	Window Time (in min) within which the Main Events and Symptom Events are Received	No of Occurrences
ESX Host Down	HostConnection Failure	Unreachable, VMDown	ESXHost Down	HostConnection Failure trap is received from vCenter and Unreachable event for ESXHost is received, based on ICMP polling.	5	NA
Network Down	NetworkConnectivity Lost, LostNetwork Connectivity ToDVPorts	Unreachable	Network Down	One of the main event occurs and Unreachable event for ESXHost is received, based on ICMP polling.	5	NA
UCS Chassis Down	ChassisInOperable, ChassisIOCardInaccessible, ChassisThermal ThresholdNon Recoverable	Unreachable, VMDown, HostConnection Failure, Network ConnectivityLost	UCS Chassis Down	One of the main event occurs.	5	NA

Name of the Correlation Rule	Main Events Responsible for the Alarm to be Raised	Symptom Events that Occur Due to the Main Event	Name of the Correlated Alarm	The Correlated Alarm is Raised When ...	Window Time (in min) within which the Main Events and Symptom Events are Received	No of Occurrences
Endpoint Unreg Threshold Exceeded	Phone Unregistered Threshold Exceeded	NA	NA	Endpoint Unreg Threshold Exceeded	Phone Unregistered Threshold Exceeded	NA	NA
Service Quality Threshold Crossed	NA	NA	Service Quality Threshold Crossed	NA	NA	NA
Analog EndPoint LostContact	EndPointLostContact occurred ONLY from analog phone.	NA	AnalogEnd Point LostContact	Main event(s) occur.	5	Greater than or equal to 10
OtherEnd PointLost Contact	EndPoint LostContact occurred from any endpoint (other than analog phone).	NA	OtherEnd Point LostContact	Main event(s) occur.	NA	Greater than or equal to 1

Note The last two rules listed in the table above are threshold rules. Alarms for these rules are raised when the "EndpointUnregThresholdExceeded" and "ServiceQualityThresholdCrossed" threshold values exceed the permitted limit.

In the Event Customization page, you can search and filter events using the search option available at the top of the page. However, for the events listed under Correlation Rules, the name-based search does not work as the names of the events are not unique and are same as events listed under the other tabs in the Event Customization page. To search for events under the Correlation Rules tab, use the name of the correlation rule.

For Cisco Prime Collaboration Release 11.1 and later

You can add additional information about events or alarms in **Notes for Email** and the note should not exceed 1000 characters. You can also edit or delete the note in **Notes for Email** using **Edit** or **Delete** link. When you edit the note, keep minimum of one character in the **Notes for Email**. This additional information is sent as email notification.

We do not recommend you to add special characters like dollar ($), vertical bar (|), and tilde (~) in **Notes for Email**.

For all the correlation rules in Cisco Prime Collaboration Assurance, the alarm suppression logic is applied, by default. When event A or event B occurs within a specified time window, the correlated alarm is triggered first along with corresponding events. The alarm for the individual event is raised only if the correlation is not met, and after the specified time window. For example, whenever a Unified CCE component like logger, PG, or router goes down, Cisco Prime Collaboration Assurance generates the correlated alarm and a set of events. The alarm for that event is raised only if the correlation does not happen and after the time interval of 10 minutes. To disable the alarm suppression, select the correlated rule, and click **Edit**. In the Edit Correlation Rule page, check the Disable Alarm Suppression check box and click **Save**.

Note Disabling alarm suppression logic for a correlation rule does not mean that the events part of that correlation rule cannot be raised. If an event is part of two or more correlation rules and the alarm suppression logic is applied to one of the rules, then the event can still be raised as the other rules take precedence.

Triggers for Alarms of VMware vCenter Server - Do not disable or modify the VMware vCenter Server (vCenter) triggers as this blocks generation of the vCenter alarms. For the list of these triggers, see the Setting Up Devices for Cisco Prime Collaboration Assurance 11.0 wiki page for Cisco Prime Collaboration Assurance 11.0 and Configure Devices for Prime Collaboration Assurance 11.5 for Cisco Prime Collaboration Assurance 11.5. To view the list of events and alarms for VMware vCenter Server, see Supported Alarms and Events for Cisco Prime Collaboration. For more information on VMware vCenter Server (vCenter), see the vSphere - ESX and VCenter Datacenter Administration Guide.

Create Custom Alerts

You can create custom alerts and also include the threshold and alert trigger parameters. See Custom Alert Parameters for details about the parameters.

To create custom alerts

Procedure

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

Choose **Alarm & Report Administration** > **Event Customization** > **Threshold Rules**.

You can also add events directly from a custom dashboard that you created.

Step 2 Click **Add Event**.

Step 3 In the New Performance Counter Event page:

a) Specify the cluster and the server.

b) Select the counter from the Available Counters drop-down list.

If you have installed Cisco Prime Collaboration Assurance in MSP mode, public IP address is displayed when you select the server and counter. However, you cannot create/add a custom event for such nodes if a specific performance counter/device is not added or managed in Cisco Prime Collaboration Assurance.

Also, in the Cluster drop-down list, only those products and clusters which belong to a specific customer (that is selected from the global filter drop-down) are displayed.

c) Add a description and the recommended action. This is optional.

d) Specify the threshold values, duration and frequency, and the schedule for monitoring.

e) Click **Save**.

Note The threshold rules that are created for any performance counter for a device, are saved in the database. This generates the alarms when the counter value violates any of the threshold conditions defined in the threshold rule. For information on the purge policies, see the Purge Policies chapter in Cisco Prime Collaboration Assurance Guide—Advanced.

Custom Alert Parameters

Table describes the parameters you can specify for the custom alert.

Setting	Description
Threshold	
	Check the check box and enter the value that applies. • Over—Check this check box to configure a maximum threshold that must be met before an alert notification is activated. In the Over value field, enter a value. For example, enter a value that equals the number of calls in progress. • Under—Check this check box to configure a minimum threshold that must be met before an alert notification is activated. In the Under value field, enter a value. For example, enter a value that equals the number of calls in progress. **Note** Use these check boxes in conjunction with the Frequency and Schedule configuration parameters.
Value	

Setting	Description
	Click the radio button that applies. • Absolute—Choose Absolute to display the data at its current status. These counter values are cumulative. • Delta—Choose Delta to display the difference between the current counter value and the previous counter value. • Delta Percentage—Choose Delta Percentage to display the counter performance changes in percentage.
Duration	
• Trigger alert only when value constantly... • Trigger immediately	• Trigger alert only when value constantly...—If you want the alert notification only when the value is constantly below or over threshold for a desired number of seconds, click this radio button and enter seconds after which you want the alert to be sent. • Trigger immediately—If you want the alert notification to be sent immediately, click this radio button.
Frequency	
• Trigger on every poll • Trigger <> events within <> minutes	Click the radio button that applies. • Trigger on every poll—If you want the alert notification to activate on every poll when the threshold is met, click this radio button. For example, if the calls in progress continue to go over or under the threshold, the system does not send another alert notification. When the threshold is normal (between 50 and 100 calls in progress), the system deactivates the alert notification; however, if the threshold goes over or under the threshold value again, the system reactivates alert notification. • Trigger <> events within <> minutes—If you want the alert notification to activate at certain intervals, click this radio button and enter the of alerts that you want sent and the number of minutes within which you want them sent.
Schedule	
• Trigger immediately (Non-stop monitoring • Schedule between <> to <>	Click the radio button that applies: • Trigger immediately (Non-stop monitoring)—If you want the alert to be triggered 24 hours a day, click this radio button. • Schedule between <> to <>—If you want the alert notification activated within a specific time frame, click the radio button and enter a start time and a stop time. If the check box is checked, enter the start and stop times of the daily task. For example, you can configure the counter to be checked every day from 9:00 am to 5:00 pm or from 9:00 pm to 9:00 am.

System

For Cisco Prime Collaboration Release 11.1 and later

and

For Cisco Prime Collaboration Release 11.5 and later

You can view all the predefined alarms and events of Cisco Prime Collaboration Assurance in **Alarm & Report Administration** > **Event Customization** > **System**.

System tab displays the following information:

- **Name**
- **Category**
- **Status**
- **Severity**
- **Default Severity**
- **For Cisco Prime Collaboration Release 11.1 and later**

  Custom Rules
- **For Cisco Prime Collaboration Release 11.5 and later**

  Exception Indicator
- **Notes for Email**

Note You can add additional information about events or alarms in **Notes for Email** and the note should not exceed 1000 characters. You can also edit or delete the note in **Notes for Email** using **Edit** or **Delete** link. When you edit the note, keep minimum of one character in the **Notes for Email**. This additional information is sent as email notification.

We do not recommend you to add special characters like dollar ($), vertical bar (|), and tilde (~) in **Notes for Email**.

You can perform the following actions:

Actions	Description
Change Severity	Check the box against Name—To select all the events; or check the boxes of the events of your choice and click **Change Severity**.
Raise or Suppress events	Check the box against Name—To select all the events; or check the boxes of the events of your choice and click **Raise** or **Suppress**.