Configure Notification

Configure Notifications

Cisco Prime Collaboration displays event and alarm information in response to events that occur in the IP Telephony and TelePresence environment and the IP fabric.

You can view events and alarms on Cisco Prime Collaboration dashboards, such as the alarms and events browser. In addition, you can configure notifications to forward information about events to SNMP trap collectors on other hosts, syslog collectors, and users.

Notifications monitor events on device roles, not on device components. For a list of supported events and alarms, see Supported Alarms and Events for Prime Collaboration.

For each alarm, Cisco Prime Collaboration compares the alarms, devices, severity, and state against the configured notification groups and sends a notification when there is a match. Matches can be determined by user-configured alarm sets and notification criteria. The procedure for configuring notification criteria is described in Add a Device Notification Group.

The following table lists values for severity and explains how the state of an alarm changes over time.

Note You can change the event severity sent in notifications from the Cisco Prime Collaboration default value to a user-defined value.

This table describes the alarm and event severity and status.

Table 1: Alarm and Event Severity and Status

Events	Alarms
Severity	
• Critical. • Major • Minor • Warning. • Informational—If any event is cleared, its severity changes to informational. Some events, by default, have severity as Informational.	• Critical • Major • Minor • Warning • Cleared
Status	
• Active—The event is live. • Cleared—The event is no longer active.	• Acknowledged—A user has manually acknowledged the alarm. A user can acknowledge only active events. • Cleared—The alarm is no longer active. • Active—The alarm is live. • User Cleared

Notification Groups

A notification group is a user-defined set of rules for generating and sending notifications.

The following table describes the contents of a notification group.

Table 2: Notification Groups

Item	Description
Notification criterion	A named set of reasons to generate a notification.

Item	Description
Notification type	The type of notification to send: SNMP trap, e-mail, or syslog.
Notification recipients	Hostnames and ports for systems that listen for SNMP traps, syslog messages, or e-mail addresses.
Daily subscription activity period	The hours during which Cisco Prime Collaboration should use this subscription while monitoring the events for which to send notifications.

Notification Criteria

Notification criteria define what you want to monitor for the purpose of sending notifications. A notification criterion is a user-defined, named set of devices or phones, and events of a particular severity and status. You must specify notification criteria to configure a notification group.

Cisco Prime Collaboration supports device-based notification criterion. The following table describes the device-based notification criterion.

Table 3: Notification Criterion

Item	Description
Devices	The devices, device groups, or clusters that you want to monitor.
Alarm sets	(Optional). One or more groups of alarms that you want to monitor. See Notifications Limited to Specific Alarms.
Alarm severity and status	One or more alarm severity levels and status.

You can also customize the names and severity of the device-based events displayed by Notifications.

Types of Notifications

Cisco Prime Collaboration provides three types of notification: SNMP trap, e-mail, and syslog. When you configure a notification group, you specify one or more types of notification to send and you must also specify recipients for each type of notification.

The following table describes the types of notification.

Table 4: Notification Types

Type	Description
SNMP Trap Notifications	Cisco Prime Collaboration generate traps for alarms and events and sends notifications to the trap receiver. These traps are based on events and alarms that are generated by the Cisco Prime Collaboration server. CISCO-EPM-NOTIFICATION-MIB defines the trap message format. Using SNMP trap notification is different from forwarding raw traps to another server before they have been processed by Cisco Prime Collaboration. **Note** Cisco Prime Collaboration supports SNMP version 1 (SNMPv1) and SNMPv2 traps for polling and receiving. Cisco Prime Collaboration forwards traps as SNMPv2 traps. However, trap processing with SNMPv3 is not supported in Cisco Prime Collaboration.
E-Mail Notifications	Cisco Prime Collaboration generates e-mail messages containing information about the alarms. When you create an e-mail subscription, you can choose whether to include the subject line only or the complete e-mail message.
Syslog Notifications	Cisco Prime Collaboration generates syslog messages for alarms that can be forwarded to syslog daemons on remote systems.

Configure SMTP Server

You can configure the SMTP server to send and receive e-mail notifications for alarms by specifying the SMTP server name and the sender AAA E-mail address. The value in the **Sender AAA E-mail Address** field helps you to identify the server you receive the e-mail from, in case of many servers.

Notifications Limited to Specific Alarms

In some cases, you might want to send notifications for only a subset of the alarms that Cisco Prime Collaboration monitors. You can set the alarm that are of interest to you when you define the notification criterion:

- Specify an alarm set for a device-based notification criterion. You can create as many alarm sets as you would like.

You can use alarm sets to:

- Limit the number of alarm that Cisco Prime Collaboration notification monitors. When you do not use alarm sets, Cisco Prime Collaboration notification monitors all alarms to determine whether to send a notification.

- Aggregate the notifications that you want to send to different destinations. For example, you can create separate alarm sets for each of the following purposes:
  - Limit the amount of e-mail notification sent to specific individuals or departments to only those for certain alarms.
  - Write all occurrences of particular alarm to syslog.
  - Send SNMP traps when certain alarms occur.

When you create device-based notification criteria, you must include an alarm set as one of the criteria. The default alarm set, All, includes all alarms.

Add an Alarm Set

You can create alarm sets for which you can set up notifications.

To add and edit an Alarm set:

Step 1 Choose .

Step 2 Click **Custom Notification** and enter the details.

Note When you create an alarm set that has several alarms, you might need to use multiple search criteria. In such situations, you need to use the Advanced Filtering option to enter multiple search criteria using the + icon, with Match selection as Any. The Quick Filter option might not work as desired.

Step 3 Click **Add** and provide the necessary information

Step 4 Click **Save** to save your changes.

Add a Device Notification Group

Perform the following procedure to add and edit device notification groups.

Note You can use existing notification groups as templates for creating new notification groups.

Step 1 Choose , then select .

Step 2 Click **Add** to add a new criterion.

Step 3 In The New Device-Based Criterion wizard, add the information in the Define General Information page.

Step 4 Click **Next**.
The Select Devices/Device Groups pane is displayed.

If you check the check box for New devices that will be added to all the groups should automatically be a part of the group, the devices that are added to or deleted from Cisco Prime Collaboration, are also added to or deleted from the notification criterion. This happens when the notification criterion includes a device group that the devices belong to.

Uncheck to maintain a static list of devices for any device groups included in the notifications criterion.

Step 5 Click **Add**.

Step 6 In the Select Device/Device Groups window, expand device group folders and select check boxes for one or more devices, device groups, or clusters.
If you select a device group, the notification criterion will stay up-to-date when devices are added or deleted from Cisco Prime Collaboration *only* if you also select the Include updates to group membership check box. New devices that will be added to all the groups should automatically be a part of the group

Step 7 Click **Next**.

Step 8 In the Set up Destination pane, add the required information.

Step 9 Click **Next**.

Step 10 Review the information in the summary, then click **Save**.

General Information Field Descriptions

This table describes the fields in the General Information window.

Table 5: Add General Information

Graphical User Interface Element	Description
Criterion Name field	Enter a name for the notification criterion.
Customer Identification field	Enter any desired identifying information. If you leave this field empty, it remains blank in e-mail and syslog notifications. In SNMP trap notifications, it is displayed as follows: `Customer ID: -`
Customer Revision field	Enter any desired identifying information. If you leave this field blank, it remains blank in e-mail and syslog notifications. In SNMP trap notifications, it is displayed as follows: `Customer Revision: *`
Alarm Set Type list box	Choose one.
Alarm Severity check boxes	Check none, one, or more of the following: • Critical. • Major • Minor • Warning

Graphical User Interface Element	Description
Alarm Status check boxes	Check none, one, or more of the following: • Active. • Acknowledged. • Cleared. • User Cleared
OperationInterval	Click the Always radio button to schedules the notification group to always be active. Choose the hours of the day during which you want this notification group to be active: • From: HH:MM—Choose hour and minute that the subscription becomes active. • To: HH:MM—Choose the last hour and minute during which the subscription is active. By default, the values are from *00:00* to *00:00* and the subscription is active for 24 hours. Use this field, for example, to send e-mail notifications during one shift and not during another.

Set up Destinations Field Descriptions

This table describes the fields in the Set up Destinations page.

Table 6: Set Up Destination

Graphical User Interface Element	Description
Include Link to Notification Details check box	Check to include URLs in the notification from which users can directly open the relevant page in Cisco Prime Collaboration for more information. Uncheck to omit URLs from notifications.

Graphical User Interface Element	Description
Subscription Type radio buttons	Click one at a time to enter data for each subscription type that you want to include in this subscription: • Trap—Enter data in the Trap Subscription Type fields. • E-Mail—Enter data in the E-Mail Subscription Type fields. • Syslog—Enter data in the Syslog Subscription Type fields. Cisco Prime Collaboration does not save the data you enter until you click **Finish** on the Subscription: Summary page. To go to the Subscription: Summary page, click **Next**.
Trap Subscription Type fields	
IP Address/Fully Qualified Domain Name editable column	Enter an IP address or Fully Qualified Domain Name (FQDN) of the host.
Port editable column	Enter a port number on which the host can receive traps. A valid port value is a number from 0 to 65,535. You can enter the default port number value 162.
Comments editable column	(Optional) Enter a comment.
E-Mail Subscription Type fields	
SMTP Server field	Enter a fully qualified DNS name or IP address for a Simple Mail Transfer Protocol (SMTP) server. (The name of the default SMTP server might already be displayed.) To select from any nondefault SMTP servers in use by existing subscriptions, click the SMTP Servers button. For instructions on how to configure a default SMTP server, see Setting System-Wide Parameters Using System Preferences.
Sender Address field	Enter the e-mail address that notifications should be sent from. If the sender's e-mail service is hosted on the SMTP server specified, you need enter only the username. You do not need to enter the domain name.
Recipient Address(es) field	Enter one or more e-mail addresses that notifications should be sent to, separating multiple addresses with either a comma or a semicolon. If a recipient's e-mail service is hosted on the SMTP server specified, you need to enter only the username. You do not need to enter the domain name.
Send Recipient(s) Subject Only check box	Check to include only the subject in the e-mail message. Uncheck to send a fully detailed e-mail message (default).
Syslog Subscription Type fields	

Graphical User Interface Element	Description
IP Address/Fully Qualified Domain Name editable column	Enter an IP address or Fully Qualified Domain Name (FQDN) of the host.
Port editable column	Enter a port number on which the syslog daemon is listening. A valid port value is a number from 0 to 65,535. You can enter the default port number value 514. The syslog daemon on the remote system (hostname) must be configured to listen on a specified port.
Comments editable column	(Optional) Include comments.