Configure Notifications

This section explains the following:

Configure Notifications

Cisco Prime Collaboration Assurance 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 Assurance 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 Assurance 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 Assurance 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 • Cleared - The event is no longer active.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 • Cleared - The alarm is no longer active.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.
Notification type	The type of notification to send: SNMP trap, e-mail, or syslog.

Item	Description
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 Assurance 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 Assurance 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 Notifications Limited to Specific Alarms device-based events displayed by Notifications.

Types of Notifications

Cisco Prime Collaboration Assurance 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 Assurance 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 Assurance 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 Assurance. **Note** Cisco Prime Collaboration Assurance supports SNMP version 1 (SNMPv1) and SNMPv2 traps for polling and receiving. Cisco Prime Collaboration Assurance forwards traps as SNMPv2 traps. However, trap processing with SNMPv3 is not supported in Cisco Prime Collaboration Assurance. See SNMP Trap Notifications for details on mapping between the MIB OIDs to the relevant value that is assigned by Cisco Prime Collaboration Assurance for alarms and events.
E-Mail Notifications	Cisco Prime Collaboration Assurance 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. **Note** If you have installed Cisco Prime Collaboration Assurance in Enterprise mode, you will get an email notification with the subject line in the following format:
[PC-ALERT-CLUSTERNAME] DEVICE IP : EVENTNAME : SEVERITY. For example: *[PC-ALERT-#CPCM-Ent-Cluster#]50.0.50.230:Gatekeeper Registration Failure:CRITICAL* If the Cluster name or Device IP is not available, it can be left empty.	
	In a NAT environment, the Private IP Address of the device is also displayed. If you have installed Cisco Prime Collaboration Assurance in MSP mode, you can see the customer to which the device belongs to.

Type	Description
Syslog Notifications	Cisco Prime Collaboration Assurance generates syslog messages for alarms that can be forwarded to syslog daemons on remote systems. In a NAT environment, the Private IP Address of the device is also displayed. If you have installed Cisco Prime Collaboration Assurance in MSP mode, you can see the customer to which the device belongs to. See Syslog Notifications for sample syslog messages and description.

SNMP Trap Notifications

When an alarm or an event is received in the Cisco Prime Collaboration Assurance server, it is converted to the trap format defined in the CISCO-EPM-NOTIFICATION-MIB. Other MIB objects are not supported. All the trap receivers receive the same traps in same trap format.

The CISCO-EPM-NOTIFICATION-MIB can be downloaded from Cisco.com.

The table below describes the mapping between the MIB OIDs to the relevant value that is assigned by Cisco Prime Collaboration Assurance for alarms.

Table 5: CISCO-EPM-NOTIFICATION-MIB Summary for Alarms

Trap Field Name	OID	Type	Prime Collaboration Alarm	Content as in Trap Forwarder (EPM MIB)
cenAlarmIndex	1.3.6.1.4.1.9.9.311.1.1.2.1.1	Unsigned32	-	MIB index
cenAlarmVersion	1.3.6.1.4.1.9.9.311.1.1.2.1.2	SnmpAdmin String	-	The version of this MIB. The version string will be of the form *major version* . *minor version* . **Note** Always set to 9.0
cenAlarmTimestamp	1.3.6.1.4.1.9.9.311.1.1.2.1.3	Timestamp	Timestamp	The time when the alarm was triggered.
cenAlarmUpdated Timestamp	1.3.6.1.4.1.9.9.311.1.1.2.1.4	Timestamp	lastmodified timestamp	The last time when the alarm was modified.
cenAlarmInstanceID	1.3.6.1.4.1.9.9.311.1.1.2.1.5	SnmpAdmin String	ID	The unique alarm ID generated by Cisco Prime Collaboration Assurance.

cenAlarmStatus	1.3.6.1.4.1.9.9.311.1.1.2.1.6	Integer32	lastcleartime	Indicates whether the alarm is active (1) or cleared (2)
cenAlarmStatus Definition	1.3.6.1.4.1.9.9.311.1.1.2.1.7	SnmpAdmin String	lastcleartime	A short description of the status of the alarm: • 1-Active • 2-Cleared
cenAlarmType	1.3.6.1.4.1.9.9.311.1.1.2.1.8	Integer	-	The alarm type is direct (2).
cenAlarmCategory	1.3.6.1.4.1.9.9.311.1.1.2.1.9	Integer32	category	The alarm categories. It is represented as an integer value.
cenAlarmCategory Definition	1.3.6.1.4.1.9.9.311.1.1.2.1.10	SnmpAdmin String	category	This is a string representation of AlarmCategory (number,description): • 3,Endpoint-Hardware alarms (peripheral errors) in all endpoints. • 4,Network Devices-Hardware alarms (interface errors) in all network devices. • 5,Service Infrastructure-Alarms in call and conference control (Cisco Unified CM and VCS), management (TMS), multipoint switches (CTMS), and multipoint control units (TPS, MCU). • 6,Conference-Endpoints alarms (that are part of the conference) and network alarms (jitter, latency, or drop).
cenAlarmServer AddressType	1.3.6.1.4.1.9.9.311.1.1.2.1.11	InetAddress Type	-	The type of Internet address at which the server that is generating this trap, is reachable. This value is set to 1 for IPv4 management.
cenAlarmServer Address	1.3.6.1.4.1.9.9.311.1.1.2.1.12	InetAddress	-	Cisco Prime Collaboration Assurance IP address.

cenAlarmManaged ObjectClass	1.3.6.1.4.1.9.9.311.1.1.2.1.13	SnmpAdmin String	Source	Entity type of the source, such as Cisco VCS and so on.
cenAlarmManaged ObjectAddressType	1.3.6.1.4.1.9.9.311.1.1.2.1.14	InetAddress Type	Source	The type of Internet address at which the managed device is reachable. This value is set to 1 for IPv4 management.
cenAlarmManaged ObjectAddress	1.3.6.1.4.1.9.9.311.1.1.2.1.15	InetAddress	Source	IP Address of the managed object.
cenAlarmDescription	1.3.6.1.4.1.9.9.311.1.1.2.1.16	OctetString	Description	A detailed description of the alarm.
cenAlarmSeverity	1.3.6.1.4.1.9.9.311.1.1.2.1.17	Integer32	Severity	Indicates the severity of the alarm using an integer value. The valid integers are 0 - 7.
cenAlarmSeverity Definition	1.3.6.1.4.1.9.9.311.1.1.2.1.18	OctetString	Severity	Alarm severity string representation (number,description): • 0,critical • 1,major • 2,minor • 3,warning • 4,info • 5,normal • 6,unknown • 7,cleared
cenAlarmTriageValue	1.3.6.1.4.1.9.9.311.1.1.2.1.19	Integer32	-	Not used.
cenEventIDList	1.3.6.1.4.1.9.9.311.1.1.2.1.20	OctetString	-	List of event IDs that led to this alarm.
cenUserMessage1	1.3.6.1.4.1.9.9.311.1.1.2.1.21	SnmpAdmin String	isacknowledged	Indicates whether the alarm is acknowledged or unacknowledged.

cenUserMessage2	1.3.6.1.4.1.9.9.311.1.1.2.1.22	SnmpAdmin String	previous Severity	Previous severity of the alarm. For example, assume that while the conference was in-progress, a major alarm was triggered. After the conference is complete, the conference alarm is automatically Cleared. The alarm severity displays Major because the previous alarm severity for this conference was Major.
cenUserMessage3	1.3.6.1.4.1.9.9.311.1.1.2.1.23	SnmpAdmin String	-	Not used.
cenAlarmMode	1.3.6.1.4.1.9.9.311.1.1.2.1.24	Integer	-	2-alert. Indicates this trap is either an alarm or event notification.
cenPartitionNumber	1.3.6.1.4.1.9.9.311.1.1.2.1.25	Unsigned32	-	Not used.
cenPartitionName	1.3.6.1.4.1.9.9.311.1.1.2.1.26	SnmpAdmin String	-	Not used.
cenCustomer Identification	1.3.6.1.4.1.9.9.311.1.1.2.1.27	SnmpAdmin String	ownerid	In the Enterprise mode, the Customer Identification details entered in the Cisco Prime Collaboration Assurance notification user interface is displayed. In the MSP mode, the customer name will be displayed.
cenCustomer Revision	1.3.6.1.4.1.9.9.311.1.1.2.1.28	SnmpAdmin String	-	Not used.
cenAlertID	1.3.6.1.4.1.9.9.311.1.1.2.1.29	SnmpAdmin String	id	The Unique alarm ID assigned by Cisco Prime Collaboration Assurance. See the Cisco Prime Collaboration Assurance Supported Alarms and Events table for the assigned alarm IDs.

The following table describes the mapping between the MIB OIDs to the relevant value that is assigned by Cisco Prime Collaboration Assurance for events.

Table 6: CISCO-EPM-NOTIFICATION-MIB Summary for Events

Trap Field Name	OID	Type	Prime Collaboration Event	Content as in Trap Forwarder (EPM MIB)
cenAlarmIndex	1.3.6.1.4.1.9.9.311.1.1.2.1.1	Unsigned32	-	MIB index
cenAlarmVersion	1.3.6.1.4.1.9.9.311.1.1.2.1.2	SnmpAdmin String	-	The version of this MIB. The version string will be of the form *major version* . *minor version* . **Note** Always set to 9.0
cenAlarmTimestamp	1.3.6.1.4.1.9.9.311.1.1.2.1.3	Timestamp	Timestamp	The time when the event was triggered.
cenAlarmUpdatedTimestamp	1.3.6.1.4.1.9.9.311.1.1.2.1.4	Timestamp	-	Not used.
cenAlarmInstanceID	1.3.6.1.4.1.9.9.311.1.1.2.1.5	SnmpAdmin String	ID	The unique event ID generated by Cisco Prime Collaboration Assurance.
cenAlarmStatus	1.3.6.1.4.1.9.9.311.1.1.2.1.6	Integer32	-	Not used.
cenAlarmStatus Definition	1.3.6.1.4.1.9.9.311.1.1.2.1.7	SnmpAdmin String	-	Not used.
cenAlarmType	1.3.6.1.4.1.9.9.311.1.1.2.1.8	Integer	-	The event type is direct (2).
cenAlarmCategory	1.3.6.1.4.1.9.9.311.1.1.2.1.9	Integer32	category	The event categories. It is represented as an integer value.

cenAlarmCategory Definition	1.3.6.1.4.1.9.9.311.1.1.2.1.10	SnmpAdmin String	category	This is a string representation of AlarmCategory (number,description): • 3,Endpoint-Hardware events (peripheral errors) in all endpoints. • 4,Network Devices-Hardware events (interface errors) in all network devices. • 5,Service Infrastructure-events in call and conference control (Cisco Unified CM and VCS), management (TMS), multipoint switches (CTMS), and multipoint control units (TPS, MCU). • 6,Conference-Endpoints events (that are part of the conference) and network events (jitter, latency, or drop).
cenAlarmServer AddressType	1.3.6.1.4.1.9.9.311.1.1.2.1.11	InetAddress Type	-	The type of Internet address at which the server that is generating this trap, is reachable. This value is set to 1 for IPv4 management.
cenAlarmServer Address	1.3.6.1.4.1.9.9.311.1.1.2.1.12	InetAddress	-	Prime Collaboration IP address.
cenAlarmManaged ObjectClass	1.3.6.1.4.1.9.9.311.1.1.2.1.13	SnmpAdmin String	Source	Entity type of the source, such as CTS, Cisco VCS, and so on.
cenAlarmManaged ObjectAddressType	1.3.6.1.4.1.9.9.311.1.1.2.1.14	InetAddress Type	Source	The type of Internet address at which the managed device is reachable. This value is set to 1 for IPv4 management.

cenAlarmManaged ObjectAddress	1.3.6.1.4.1.9.9.311.1.1.2.1.15	InetAddress	Source	IP Address of the managed object.
cenAlarmDescription	1.3.6.1.4.1.9.9.311.1.1.2.1.16	OctetString	Description	A detailed description of the event.
cenAlarmSeverity	1.3.6.1.4.1.9.9.311.1.1.2.1.17	Integer32	Severity	Indicates the severity of the event using an integer value. The valid integers are 0 - 7.
cenAlarmSeverity Definition	1.3.6.1.4.1.9.9.311.1.1.2.1.18	OctetString	Severity	Alarm severity string representation (number, description): • 0,critical • 1,major • 2,minor • 3,warning • 4,info • 5,normal • 6,unknown • 7,cleared
cenAlarmTriageValue	1.3.6.1.4.1.9.9.311.1.1.2.1.19	Integer32	-	Not used.
cenEventIDList	1.3.6.1.4.1.9.9.311.1.1.2.1.20	OctetString	-	Not used.
cenUserMessage1	1.3.6.1.4.1.9.9.311.1.1.2.1.21	SnmpAdmin String	-	Not used.
cenUserMessage2	1.3.6.1.4.1.9.9.311.1.1.2.1.22	SnmpAdmin String	-	Not used.
cenUserMessage3	1.3.6.1.4.1.9.9.311.1.1.2.1.23	SnmpAdmin String	-	Not used.
cenAlarmMode	1.3.6.1.4.1.9.9.311.1.1.2.1.24	Integer	-	3-event. Indicates this trap is either an alarm or event notification.
cenPartitionNumber	1.3.6.1.4.1.9.9.311.1.1.2.1.25	Unsigned32	-	Not used.
cenPartitionName	1.3.6.1.4.1.9.9.311.1.1.2.1.26	SnmpAdmin String	-	Not used.
cenCustomer Identification	1.3.6.1.4.1.9.9.311.1.1.2.1.27	SnmpAdmin String	-	Not used.
cenCustomerRevision	1.3.6.1.4.1.9.9.311.1.1.2.1.28	SnmpAdmin String	-	Not used.
cenAlertID	1.3.6.1.4.1.9.9.311.1.1.2.1.29	SnmpAdmin String	-	Not used.

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 on the **E-mail Setup for Alarms & Events** page (**Alarm & Report Administration** > **E-mail Setup for Alarms & Events**). 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.

Syslog Notifications

Syslog messages have a limitation of 1,024 characters (including the heading). Any syslog-based event details may not contain the full information due to this syslog limitation. If the syslog message exceeds this limitation, it is truncated to 1,024 characters by the syslog sender.

The following is a sample syslog message generated by the Cisco Prime Collaboration Assurance server for an alarm.

```
Local7.Emerg     10.78.110.27       Feb 19 14:42:49 pcollab-44798 pcollab-44798:
%local7-0-ALARM: 14$Description=Device temperature or voltage is outside the normal operating
 range.
When an OutofRange event is generated, you will normally also see fan, power supply, or
temperature
events.::Status=1,active^Severity=critical^Acknowledged=no^AlarmURL=https://10.78.110.27/emsam/index.html
#pageId=com_cisco_ifm_web_page_alarms&queryParams=Id%3D84837&forceLoad=true^Device Work
Center=
https://10.78.110.27/emsam/index.html#pageId=com_cisco_emsam_page_inventory&deviceId=3681728
^CUSTOMER=customer2^CUSTREV=2,324^Default Alarm Name=OutofRange^Managed Object=150.50.3.2
^Managed Object Type=Router^MODE=2;Alarm ID=84837^Component=150.50.3.2/8<000><000>
```

This table describes the syslog notification parameters based on the above example:

Table 7: Syslog Notification Description

Parameter	Description
Local7.Emerg 10.78.110.27 Feb 19 14:42:49 pcollab-44798 pcollab-44798	IP address and hostname of the Cisco Prime Collaboration Assurance server where the syslog is generated
%local7-0-ALARM	• Syslog Facility data: %local7 • Severity: 0-Critical, 1-Major, 2-Minor, and 3-Warning • Type is Alarm
14	Calendar year
Description	Alarm description
Status=1,active	Status of alarm; where 1 is active and 2 is cleared
Severity	Severity of alarm
Acknowledged	Indicates whether alarm is acknowledged or not
AlarmURL	URL to launch the Alarm page
Inventory Management	URL to launch the Inventory Management page
CONFERENCEDIAGNOSTICS	URL to launch Conference Diagnostics page, if it is a conferencealarm
CUSTOMER	Customer ID defined while configuring the notification

Parameter	Description
CUSTREV	Customer revision defined while configuring the notification
Default Alarm Name	Alarm name
Managed Object	IP address or hostname of the device, where an alarm is raised
Managed Object Type	Device type, such as router, endpoint and so on
MODE	Indicates if the syslog message is an alarm (2)
Alarm ID	Unique ID for alarm
Component	Device component where the alarm is raised

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 Assurance 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 Assurance notification monitors. When you do not use alarm sets, Cisco Prime Collaboration Assurance 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 **Notification Setup**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Alarm & Report Administration** > **Notification Setup**

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.

Note When you add more alarms to an existing alarm set, do not use filter to search for alarms as filtering overwrites the original set of alarms.

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 **Notification Setup**, then select the **Custom Notification**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Alarm & Report Administration** > **Notification Setup**, then select the **Custom Notification**.

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

Step 3 In The New Device-Based Criterion wizard add the information on the Define General Information page:

Based on your mode of deployment, you can create domain-specific or customer-specific device notification groups. In the New Device-Based Criterion wizard, enter the required details and select a domain from the Associate to Domain drop-down list or a customer from the Customer drop-down list.

Note The Super administrator has access to all domains and can create notification groups for a domain or all the domains.

Step 4 Click **Next**.

The Select Devices/Device Groups pane is displayed.

If you check the check box for New devices that are 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 Assurance, 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, click **Include all Devices** or **Select Devices** radio button.

If you select the **Include all Devices** option, expand device group folders and select one or more devices, device groups, or clusters.

If you select the **Select Devices** option, expand device group folders and select check boxes for one or more devices, device groups, or clusters.

Note If you want to add cluster level email notification, you must select the cluster ID from the list of all the nodes in the cluster and cluster ID listed under **Infrastructure** > **UCM Clusters** device group folder.

If you select a device group, the notification criterion stays up-to-date when devices are added or deleted from Cisco Prime Collaboration Assurance *only* if you also select the Include updates to the group membership check box. New devices that are 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**.

After you save the device notification group, the details that you entered in the New Device-Based Criterion wizard is displayed on the Assurance Notification Criteria page. Customer column depicts the customer to which the notification group belongs.

General Information Field Descriptions

This table describes the fields in the General Information window.

Table 8: 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: *`

Graphical User Interface Element	Description
Alarm Set Type list box	Choose one.
Alarm Severity check boxes	Check none, one, or more of the following: • Critical. • Major • Minor • Warning
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 9: 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 Assurance 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 Assurance 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.

Graphical User Interface Element	Description
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). **For Cisco Prime Collaboration Release 11.1 and later** **Note** You will get an e-mail notification with the subject line in the following format :
[PC-ALERT-CLUSTERNAME] DEVICE IP : EVENTNAME : SEVERITY. For example: *[PC-ALERT-CPCM-Ent-Cluster]50.0.50.230:Gatekeeper Registration Failure:CRITICAL* *CLUSTERNAME* is included in the subject line for Unified Communications Manager and Cisco VCS only. For all other device types *CLUSTERNAME* is left empty. If the *DEVICE IP* or *CLUSTERNAME* is not available, it is left empty.	
Syslog 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 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.