Cisco Prime Collaboration 9.0 Fault Management Guide

September 3, 2013

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-27262-01

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco Prime Collaboration 9.0 Fault Management Guide

CONTENTS

Preface v

Fault Management Overview 1-1

Event 1-1

Alarms 1-2

Event Creation 1-2

Alarm Creation 1-3

Event and Alarm Association 1-3

Event and Alarm Correlation 1-4

Event Aggregation 1-4

Event Masking 1-5

Alarm Status 1-5

Event Severity 1-5

Event and Alarm Database 1-6

Alarm Notifications 1-6

Customizing Alarms and Events 2-1

Configuring Thresholds 2-1

Configuring TelePresence Endpoint Thresholds-Global 2-1

Configuring TelePresence Endpoint Threshold—Device Level 2-2

Enabling Automatic Troubleshooting for TelePresence Endpoints 2-2

Configuring Infrastructure Device Thresholds 2-3

Customizing Infrastructure Device Threshold Settings 2-3

Overview of Device Pool Thresholds 2-4

Editing Device Pool Thresholds 2-4

Restoring Default Device Pool Thresholds 2-5

Generating an RTMT Thresholds Report 2-5

Synchronizing RTMT Thresholds 2-6

Overview of Call Quality Thresholds and Threshold Groups 2-6

Configuring Global Thresholds 2-8

Restoring Global Thresholds to Default Values 2-8

Oveview of CDR Threshold Groups 2-8

Adding a CDR Threshold Group 2-9

Editing a CDR Threshold Group 2-9

Updating CDR Threshold Group Priority 2-9
Deleting a CDR Threshold Group 2-10
Overview of Sensor Threshold Groups 2-10
Adding a Sensor Group 2-10
Editing a Sensor Group 2-11
Updating Sensor Group Priority 2-11
Deleting a Sensor Group 2-11
Threshold Parameter Values 2-12
Overview of Event Flooding Control 2-16
Event Flooding Rules 2-16
Event Flood Logs 2-16
Adding Dynamic Syslogs 2-17
Customizing Events—Global 2-17
Customizing Events—Device Level 2-18
Alarm Correlation Rules 2-19
Modifying Alarm Correlation Rules 2-20
Activating Events in Prime Collaboration 2-20
Configuring Alarm and Event Notification 3-1
Prime Collaboration Notifications Triggers 3-1
Notification Groups 3-2
Notification Criteria 3-3
Types of Notifications 3-3
Notifications Limited to Specific Alarms 3-4
Adding an Alarm Set 3-5
Adding and Device Notification Groups 3-6
Monitoring Alarms and Events 4-1
Alarm Summary 4-1
Alarms 4-2
Events 4-3

Preface

This guide is one of multiple short guides for Cisco Prime Collaboration 9.0 that are used in sequence to install, set up, and administer Prime Collaboration.

After managing the devices in the Prime Collaboration Assurance server, the Prime Collaboration Assurance application raises events and alarms to alert you on the network issues. See this guide to perform the following tasks to easily monitor and resolve the issues in your network:

- Define the threshold parameters to monitor the faults.
- Define the notification services to receive e-mail alerts on alarms.
- Customize the events that you want to monitor in your network.
- Manage the fault and rectify the issues using other Cisco Prime applications, Cisco Network Analysis Module and Cisco Prime LAN Management Solution.

This guide is one of multiple short guides for Cisco Prime Collaboration 9.0. To perform other Prime Collaboration tasks, such as user management, device management, voice provisioning, network monitoring, and fault management, see *Cisco Prime Collaboration 9.0 Documentation Overview* for a list of all available documents.

New and Changed Information

The following table describes information that has been added or changed since the initial release of this guide.

Date	Revision	Location
November 7, 2012	Initial version.	—
September 3, 2013	Added information on polling settings for each parameter type.	Customizing Infrastructure Device Threshold Settings
	Added information on how to activate events in Prime Collaboration.	Activating Events in Prime Collaboration

Audience

This guide is targeted at the voice and video engineers who are responsible for the configuration and maintenance of infrastructure based real-time collaboration services such as video (TelePresence) and telephony (VOIP) including the endpoints, management servers, and service specific network devices.

The Prime Collaboration application is deployed on the virtual server. The engineer must be familiar with the virtual server configuration and UNIX commands using CLI.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

CHAPTER 1

Fault Management Overview

Cisco Prime Collaboration ensures near-real time quick and accurate fault detection. After identifying the event, Prime Collaboration groups related events, creates alarms, and performs fault analysis to determine the root cause of the fault in a network.

Prime Collaboration allows you to monitor the events that are of importance to you. You can customize the event severity and enable management applications to receive notifications from Prime Collaboration, based on the severity. Prime Collaboration monitor events from the endpoints and service infrastructure devices.

This chapter explains the concepts that are key to the Prime Collaboration fault management framework.

Event

An event is a distinct incident that occurs at a specific point in time.

An event is a:

- Possible symptom of a fault that is an error, failure, or exceptional condition in the network. For example, when a device becomes unreachable, an Unreachable event is triggered.
- Possible symptom of a fault clearing. For example, when a device state changes from unreachable to reachable, an event is triggered.

Examples of events include:

- Port status change.
- Node reset
- Node becoming reachable for the management station.
- Connectivity loss between routing protocol processes on peer routers.

Events are derived from incoming traps and notifications, detected status changes (by polling), and user actions.

It is important to understand that an event, once it occurs, does not change its status even when the conditions that triggered the event are no longer present.

Alarms

The life cycle of a fault scenario is called an alarm.

An alarm:

- Is a Prime Collaboration response to events it receives.
- Is a sequence of events, each representing a specific occurrence in the alarm life cycle (see below example). In a sequence of events, the event with the highest severity determines the severity of the alarm.
- Represents a series of correlated events that describe a fault occurring in the network.
- Describes the complete event life cycle, from the time that the alarm is raised (when the fault is first detected) until it is cleared and acknowledged.

In a sequence of events, the event with the highest severity determines the severity of the alarm.

Prime Collaboration constructs alarms from a sequence of correlated events. A complete event sequence for an alarm includes a minimum of two events:

- Alarm active (for example, an interface down event raises an alarm).
- Alarm clear (for example, an interface up event clears the alarm).

The lifecycle of an alarm can include any number of correlated events that are triggered by changes in severity, updates to services, and so on.

When a new related event occurs, Prime Collaboration correlates it to the alarm and updates the alarm severity and message text based on the new event. If you manually clear the alarm, the alarm severity changes to cleared.

You can view the events that form an alarm in the Alarms and Events browser.

Event Creation

Prime Collaboration maintains an event catalog and decides how and when an event has to be created and whether to associate an event with an alarm. Multiple events can be associated to the same alarm.

Prime Collaboration discovers events in the following ways:

- By receiving notification events and analyzing them; for example, syslog and traps.
- By automatically polling devices and discovering changes; for example, device unreachable.
- By receiving events when the status of the alarm is changed; for example, when the user clears an alarm.

Prime Collaboration allows you to disable monitoring of events that may not be of importance to you. The events that are disabled will not be listed in the Alarms and Events browser. Also, Prime Collaboration will not trigger an alarm.

Incoming event notifications received as syslogs or traps are identified by matching the event data to predefined patterns. An event is considered supported by Prime Collaboration if it has matching patterns and can be properly identified. If the event data does not match with predefined patterns, the event is considered as unsupported and it is dropped.

The following table illustrates the Prime Collaboration behavior while it deals with event creation:

Time	Event	Prime Collaboration Behavior
10:00AM PDT June 7, 2012	Device A becomes unreachable	Creates a new Unreachable event on device A.
10:30AM PDT June 7, 2012	Device A continues to be in the unreachable state.	No change in the event status.
10:45AM PDT June 7, 2012	Device A becomes reachable.	Creates a new Reachable event on device A.
11:00AM PDT June 7, 2012	Device A stays reachable	No change in the event status.
12:00AM PDT June 7, 2012	Device A becomes unreachable.	Creates a new Unreachable event on device A.

Alarm Creation

An alarm represents the life cycle of a fault in a network. Multiple events can be associated with a single alarm.

An alarm is created in the following sequence:

1. A notification is triggered when a fault occurs in the network.
2. An event is created, based on the notification.
3. An alarm is created after checking if there is no active alarm corresponding to this event.

An alarm is associated with two types of events:

- Active events: Events that have not been cleared. An alarm remains in this state until the fault is resolved in a network.
- Historical events: Events that have been cleared. An event changes its state to an historical event when the fault is cleared. See Alarm Status, page 1-5 to know how an alarm is cleared.

The alarm life cycle ends after an alarm is cleared. A cleared alarm can be revived if the same fault recurs within a preset period of time.

For Prime Collaboration, the preset period is 60 minutes.

Event and Alarm Association

Prime Collaboration maintains a catalog of events and alarms. The catalog contains the list of events managed by Prime Collaboration, and the relationship among the events and alarms. Events of different types can be associated to the same alarm type.

When a notification is received:

1. Prime Collaboration compares an incoming notification against the event and alarm catalog.
2. Prime Collaboration decides whether an event has to be raised.
3. If an event is raised, Prime Collaboration decides whether the event should trigger a new alarm or associate it to an existing alarm.

A new event is associated with an existing alarm, if the new event triggered is of the same type and occurs on the same source.

An active interface error alarm is an example. All interface error events that occur on the same interface, are associated to the same alarm.

If any event is cleared, its severity changes to informational.

Note Some events have default severity as informational. For these events, alarms will not be created. If you want Prime Collaboration to create alarms for these events, you must change the severity of these events.

Event and Alarm Correlation

Event correlation is the process of relating one event to other events.

Prime Collaboration distinguishes two event relationship types:

- An event sequence. Events that have the same type and the same source are considered part of an event sequence, or an alarm. An alarm represents the complete lifecycle of a fault.
- An event sequence hierarchy (alarms), representing causality.

Prime Collaboration associates a new event to an existing alarm if the existing alarm has the same event type and source as the new event.

Prime Collaboration raises an alarm, if the number of related events received (by fault management system) from the device element exceeds a specified threshold in a specified unit of time, based on predefined correlation rules. See Alarm Correlation Rules.

Example use cases:

- Call Manager location goes out-of-resource for more than 5 times over the last one hour.
- CPU usage of a device is over 80% for last15 minutes.

You can modify these rules and configure the number of event occurrences to set the trigger. This can vary from two to 100. You can also set the time interval. You can modify these rules at **Administration > Alarm & Event Configuration > Rules Settings**. See Modifying Alarm Correlation Rules for details.

If an administrator does not specify a time interval, maximum time period, or a count for a specific alarm, the default values for the time interval, maximum time period, and count is attached on an alarm, device type, or device class basis.

Event Aggregation

If the number of same event received from a set of elements exceeds a specified threshold, Prime Collaboration creates an alarm,.

Example use cases:

- Number of unregistered phones on a device pool / Unified CM location is more than 5%.
- Number of service quality issues experienced on a device pool / Unified CM location is more than 5%
- All the call quality events raised against a single poor-quality call are grouped.

Event Masking

Prime Collaboration automatically masks the hierarchy of events when the top-level component is the cause for the issue, and raises an alarm against the top level component while masking all the downstream events.

Example use cases:

- When a Call Manager goes down, Prime Collaboration masks all its component (such as powersupply, interface, fan) events.
- When a switch card goes down, Prime Collaboration masks all the contained port level events.

Alarm Status

The following are the supported statuses for an alarm:

Table 1-1 Alarm Status

Status	Description
Not Acknowledged	When an event triggers a new alarm or an event is associated with an existing alarm.
Acknowledged	When you acknowledge an alarm, the status changes from Not Acknowledged to Acknowledged
Cleared	• System-clear from the device—The fault is resolved on the device and an event is triggered for the same. For example, a device-reachable event clears the device-unreachable alarm. • Alarms are also triggered during the session because of packet loss, jitter, and latency. These alarms are auto-cleared after the session ends. • Manual-clear from Prime Collaboration users: You can manually clear an active alarm without resolving the fault in the network. A clearing event is triggered and this event clears the alarm. • If the fault continues to exist in the network, a new event and alarm are created subsequently based on the polling. • Auto-clear from the Prime Collaboration server—Prime Collaboration clears all session-related alarms, when the session ends. If there are no updates to an active alarm for 24 hours, Prime Collaboration automatically clears the alarm. **Note** Certain alarms might get cleared automatically before 24 hours. See *Supported Alarms for Prime Collaboration* and *Supported Events for Prime Collaboration*.

Event Severity

Each event has an assigned severity, and can be identified by its color in Prime Collaboration.

Events fall broadly into the following severity categories:

- Flagging—Indicates a fault: Critical (red), Major (orange), Minor (yellow), or Warning (sky blue).
- Informational—Info (blue). Some of the Informational events clear the flagging events.

In a sequence of events, the event with the highest severity determines the severity of the alarm.

Prime Collaboration allows you to customize the settings and severity of an event. The events that are of importance to you can be given higher severity. See Customizing Alarms and Events to know how to customize the event settings and severity.

The event settings and severity predefined in the Prime Collaboration application is used if you have not customized the event settings and severity.

Event and Alarm Database

All events and alarms, including active and cleared, are persisted in the Prime Collaboration database.

The relationships between the events are retained. The Alarm and Event Browser lets you review the content of the database. The purge interval for this data is four weeks.

Note Events are stored in the form of the Prime Collaboration event object. The original notification structure of incoming event notifications (trap or syslog) is not maintained.

Alarm Notifications

Prime Collaboration allows you to subscribe to receive notifications for alarms. Prime Collaboration sends notifications based on user-configured alarm sets and notification criteria.

See Configuring Alarm and Event Notificationfor details about how to configure for notifications.

CHAPTER 2

Customizing Alarms and Events

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

Configuring Thresholds

You can configure the devices to generate events when certain parameters cross pre-defined thresholds. These settings are to be done at **Administration > Alarm & Event Configuration > Threshold Settings**.

You can view and configure thresholds for:

- TelePresence Endpoint
- Infrastructure Device
- Device Pool
- RTMT Synchronization
- Global Call Quality
- Sensor Call Quality
- CDR Call Quality

Prime Collaboration does not need to install the RTMT plug-in to poll the device data (for example, memory usage) through RTMT. Prime Collaboration uses the default settings for these events. If you want to configure the threshold settings for specific events, you must install the RTMT plug-in.

Configuring TelePresence Endpoint Thresholds-Global

You can set up Prime Collaboration to have events generated when the threshold value exceeds the configured limit for Rx packet loss, jitter, or latency.

To configure thresholds for TelePresence endpoints:

Note The changes you make here applies to all TelePresence devices. See Configuring TelePresence Endpoint Threshold—Device Level for information about how to modify thresholds at a device-level for video endpoints.

Step 1 Choose **Administration > Alarm & Event Configuration**.

Step 2 From the Threshold Settings drop down list, choose TelePresence Endpoints.

Step 3 Check the check box corresponding to Average Period Jitter, Average Period Latency, or Rx Packet Loss, then click the row to enable editing.

Step 4 Modify the values for Minor, Major, and Critical thresholds, then click **Save**.

Configuring TelePresence Endpoint Threshold—Device Level

You can configure the thresholds for TelePresence endpoints at a device level, if you do not want to have the thresholds to be applied at a global level.

To do this:

Step 1 Choose **Operate > Device Work Center**.

Step 2 From the Device Groups pane, choose the video end point for which you need to modify the threshold.

Step 3 Click **Threshold Settings**.

Step 4 Check the check box corresponding to Average Period Jitter, Average Period Latency, or Rx Packet Loss, then click the row to enable editing.

Step 5 Modify the values for Minor, Major, and Critical thresholds, then click **Save**.

Enabling Automatic Troubleshooting for TelePresence Endpoints

You can enable automatic troubleshooting of a session when the threshold value exceeds the limit, for packet loss, jitter, and/or latency.

To enable automatic troubleshooting:

Step 1 Choose **Administration > Alarm & Event Configuration**.

Step 2 From the Threshold Settings drop down list, choose TelePresence Endpoints.

Step 3 Check the check box corresponding to Average Period Jitter, Average Period Latency, or Rx Packet Loss, then click the row to enable editing.

Step 4 From the drop down list under Automatic Troubleshooting, and choose from Minor, Major, or Critical, then click **Save**.

To disable, choose Disable from the drop down list.

Configuring Infrastructure Device Thresholds

You can set up Prime Collaboration to generate alarms when devices cross the threshold you configure. When you configure thresholds, the values get associated with groups, not with individual devices, device pools, ports, or interfaces.

To configure thresholds for a selected device group:

Step 1 Choose **Administration > Alarm & Event Configuration**.

Step 2 Choose Infrastructure Device.

Step 3 Choose a device group for which you can set thresholds.

Generally, this is a device group that does not contain subgroups.

Step 4 Click the Edit button and enter the appropriate information in the Managing Thresholds: Edit dialog box.

Step 5 Click **Save**.

Step 6 Repeat Step 4 and Step 5 until you are done editing thresholds for the selected group.

⚠ **Caution** Your changes will be lost if you select another threshold category or parameter type *before* you click Save.

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

Step 7 Click **Save**, then click **Apply**.

Step 8 In the confirmation message box, click **Yes**.

Customizing Infrastructure Device Threshold Settings

You can selectively disable threshold settings, moving them from an active settings list to an inactive settings list. Prime Collaboration does not monitor threshold parameters for threshold settings that are on an inactive settings list.

To customize infrastructure device threshold:

Step 1 Choose **Administration > Alarm & Event Configuration**.

Step 2 Choose Infrastructure Device from the Threshold Settings drop down list.

Step 3 Choose a device group for which you can set thresholds.

Generally, this is a device group that does not contain subgroups.

Step 4 Click the **Customize Settings** button.

Step 5 To update the Active Settings list for a particular parameter type:

a. Scroll to the parameter type and update the inactive and active settings lists.

b. Scroll to the bottom of the window and click **Save**.

To reset all parameter types with Prime Collaboration default settings:

a. Click **Revert to Default Settings**.

b. Click **Yes**.

c. Click **Cancel** to close the Managing Thresholds: Edit dialog box.

Note The settings are stored in the database, but not yet applied to the IP fabric.

Step 6 Click **Save**, then click **Apply**.

Overview of Device Pool Thresholds

A device pool is a logical group of devices. Device pools provide 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. You can view and edit device pool thresholds using Prime Collaboration.

Within Prime Collaboration, device pools are displayed onlyafter 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.

The device pool threshold settings in Prime Collaboration 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, Prime Collaboration 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.

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

Editing Device Pool Thresholds

You can view and edit device pool thresholds using Prime Collaboration.

To view or configure device pool thresholds:

Step 1 Select **Administration > Alarm & Event Configuration**.

Step 2 Select Device Pool from the Threshold Settings drop down list.

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

Step 3 Click 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/Service Quality Thresholds dialog box edit the threshold% and click **Update**.

To revert any settings back to the default settings, check a check box and click **Revert to Default Settings**.

To reset all parameter types with Prime Collaboration default settings:

a. Check the check box for All Device Pools/CMEs and click **Revert to Default Settings**.

b. Click **Yes**.

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

Step 6 Click **Save**, then click **Apply**

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 Configuring Alarm and Event Notification.

Restoring Default Device Pool Thresholds

Use this procedure to reset the values of parameters in all active threshold settings in all threshold categories for a selected group. For information on active threshold settings, see Customizing Infrastructure Device Threshold Settings.

To see default threshold values before you apply them, view the Thresholds report.

To restore default thresholds:

Step 1 Choose **Administration > Alarm & Event Configuration**.

Step 2 Choose Device Pool from the Threshold Settings drop down list.

Step 3 Click the **Revert to Default Settings** button.

Step 4 Click **Yes**.

The settings are stored in the database, but not yet applied to the IP fabric.

Generating an RTMT Thresholds Report

You can view real-time monitoring threshold (RTMT) parameters for Unified CM devices. You can export the RTMT thresholds report as a PDF or CSV file.

To view RTMT thresholds:

Step 1 Choose **Administration > Alarm & Event Configuration**.

Step 2 Choose RTMT Synchronization from the Threshold Settings drop down list.

Step 3 Choose a voice cluster for which you can view thresholds.

Step 4 Click the **View** button.

The thresholds report window opens and displays the following information for all clusters or Unified Communications Manager devices. The information is updated each hour.

Step 5 When you are done viewing the threshold report, close the window.

Synchronizing RTMT Thresholds

You can synchronize real-time monitoring tool (RTMT) threshold parameters for clusters and Unified CM devices. You may want to do this when you do not want to wait for the next scheduled polling.

To synchronize RTMT thresholds:

Step 1 Choose **Administration > Alarm & Event Configuration**.

Step 2 Choose RTMT Synchronization from the Threshold Settings drop down list.

Step 3 Click the **Synchronize thresholds with RTMT now** icon in the RTMT Threshold: Select Voice Cluster window to update the information in *all* clusters.

Synchronizing the thresholds with RTMT may take a few minutes to complete. There is no option to synchronize individual voice clusters.

Overview of Call Quality Thresholds and Threshold Groups

Prime Collaboration uses thresholds to determine when a MOS value—reported from a sensor or included in CDRs from a Unified Communications Manager cluster—has fallen to an unacceptable level. When MOS falls below a threshold, Prime Collaboration sends a QoVMOSViolation trap to up to four trap receivers.

Prime Collaboration supplies global thresholds and provides default values for them. Prime Collaboration can use global thresholds to compare against MOS values reported from sensors or clusters. Since the MOS threshold values might vary depending upon the codec being used in a call, global thresholds include separate values for commonly used codecs such as these:

- AAC
- G711Alaw 56k
- G711Alaw 64k
- G711Ulaw 56k
- G711Ulaw 64k
- G722 48k
- G722 56k
- G722 64k
- G722.1 24k

- G722.1 32k
- G723.1
- G726 16K
- G726 24K
- G726 32K
- G728
- G729
- G729AnnexA
- G729AnnexAwAnnexB
- G729AnnexB
- GSM
- GSM Enhanced Full Rate
- GSM Full Rate
- GSM Half Rate
- iSAC

  Note The iSAC codec applies to CVTQ data only.

- NonStandard

Note For more information about codecs, see Understanding Codecs: Complexity, Hardware Support, MOS, and Negotiation at this URL: http://www.cisco.com/en/US/tech/tk1077/technologies_tech_note09186a00800b6710.shtml

You can update the global threshold default values to reflect MOS values below the average MOS seen in your system. By monitoring Prime Collaboration reports, you can determine average MOS values and then adjust global thresholds accordingly. You can also easily restore global thresholds to the default values that Prime Collaboration supplies.

If you would like to use different threshold values for particular sensors, clusters, or groups of endpoints reported on by either sensors or clusters, you can override global thresholds by adding these threshold groups:

- CDR Groups—A CDR group includes one or more clusters, two sets of endpoints, and one or more threshold values for commonly used codecs.
- Sensor Groups—A sensor group includes one or more sensors, two sets of endpoints, and one or more threshold values for commonly used codecs.

You can create up to ten CDR groups and up to ten sensor groups. CDR groups are prioritized from highest (one) to lowest (ten), as are sensor groups. In cases where an endpoint is included in more than one CDR group or more than one sensor group, Prime Collaboration compares MOS for the endpoint against the highest priority group that it belongs to.

For more information, see the following topics:

- Configuring Global Thresholds, page 2-8
- Oveview of CDR Threshold Groups, page 2-8

- Overview of Sensor Threshold Groups, page 2-10

Configuring Global Thresholds

Prime Collaboration compares MOS reported from sensors and clusters against global thresholds when no CDR group or sensor group setting is applicable. You cannot delete or clear global thresholds. You can update them and you can restore them to default values. You can override global thresholds by creating user-defined threshold groups; for more information, see Oveview of CDR Threshold Groups, page 2-8 and Overview of Sensor Threshold Groups, page 2-10.

Note Grading is based on the global threshold settings only.

To configure global thresholds:

Step 1 Choose **Administration > Alarm & Event Configuration**.

Step 2 Choose Global Call Quality Settings from the Threshold Settings drop down list.

Step 3 Enter a new current value for any codec in the table and click **Apply**.

Restoring Global Thresholds to Default Values

You can restore global threshold values to the suggested default values that are displayed on the Global Thresholds page.

To do this:

Step 1 Choose **Administration > Alarm & Event Configuration**.

Step 2 Choose Global Call Quality Settings from the Threshold Settings drop down list.

Step 3 Click **Revert to Suggested Defaults**.

Oveview of CDR Threshold Groups

A CDR group includes one or more Unified Communications Manager clusters, two sets of endpoints, and threshold values for one or more commonly used codecs. You can define up to ten CDR Threshold groups; Prime Collaboration prioritizes the CDR threshold groups from 1 (highest priority) to ten (lowest priority), initially reflecting the order in which you create the groups. (You can reprioritize them.) If an endpoint belongs to more than one CDR threshold group, Prime Collaboration uses the thresholds for the highest priority CDR threshold group.

To configure threshold groups, choose **Administration > Thresholds > CDR Call Quality Settings**. The CDR Call Quality Settings page displays up to ten user-defined CDR threshold groups.

Adding a CDR Threshold Group

When you add a CDR threshold group, it is assigned the lowest priority among existing CDR threshold groups. To adjust its priority, see Updating CDR Threshold Group Priority, page 2-9.

Note You can add up to ten CDR threshold groups.

Step 1 Choose **Administration > Thresholds > CDR Call Quality Settings**.

Step 2 Click **Add**.

Step 3 Do the following to enter data for each of the fields:

a. Click ⌄

b. Enter the appropriate information.

c. Click OK.

Step 4 After you finish entering the data, click **OK**.

The CDR Threshold Group displays the newest CDR threshold group last in the list (in the lowest priority position).

Editing a CDR Threshold Group

Note To change CDR threshold group priority, see Updating CDR Threshold Group Priority, page 2-9.

Step 1 Choose **Administration > Thresholds > CDR Call Quality Settings**.

Step 2 Choose a group and click **Edit**.

Step 3 Do the following to enter data for each of the fields:

a. Click ⌄

b. Enter the appropriate information.

Step 4 Click OK.

Updating CDR Threshold Group Priority

If the directory number or IP address for an endpoint is included in more than one CDR group, Prime Collaboration applies the thresholds for the highest priority CDR threshold group.

Step 1 Choose **Administration > Thresholds > CDR Call Quality Settings**. The CDR Threshold Group page appears, displaying up to 10 user-defined CDR threshold groups.

Step 2 Enter any unique numbers—up to two digits—in the Priority column.

Step 3 Click **Update Priority**. Prime Collaboration reorders the CDR threshold groups and displays them in priority order.

Deleting a CDR Threshold Group

Step 1 Choose **Administration > Thresholds > CDR Call Quality Settings**. The CDR Threshold Group page appears, displaying up to 10 user-defined CDR threshold groups.

Step 2 Check the check boxes for the CDR threshold groups that you want to delete.

Step 3 Click **Delete**.

Step 4 Click **Yes**. Prime Collaboration displays any remaining CDR threshold groups in priority order.

Overview of Sensor Threshold Groups

A sensor group includes one or more sensors, two sets of endpoints, and threshold values for one or more commonly used codecs. You can define up to ten sensor threshold groups; Prime Collaboration prioritizes the sensor threshold groups from one (highest priority) to ten (lowest priority), initially reflecting the order in which you create the groups. You can reprioritize them.

If an endpoint belongs to more than one sensor threshold group, Prime Collaboration uses the thresholds for the highest priority sensor threshold group.

Adding a Sensor Group

When you add a sensor group, it is assigned the lowest priority among existing sensor groups. To adjust its priority, see Updating Sensor Group Priority, page 2-11.

Note You can add up to 10 sensor groups.

Step 1 Choose **Administration > Alarm & Event Configuration**.

Step 2 Choose Sensor Call Quality Settings from the Threshold Settings drop down list.

Step 3 Click **Add**.

Step 4 Do the following to enter data for each of the fields:

a. Click ⌄

b. Enter the appropriate information.

c. Click OK.

Step 5 After you finish entering the data, click **OK**.

The Sensor Threshold Group page appears, displaying the new sensor group threshold group last in the list (in the lowest priority position).

Editing a Sensor Group

You can edit the details for a sensor threshold group you created.

Note To change sensor group priority, see Updating Sensor Group Priority, page 2-11.

To edit the details:

Step 1 Choose **Administration > Alarm & Event Configuration**.

Step 2 Choose Sensor Call Quality Settings from the Threshold Settings drop down list.

Step 3 Choose a group and click the **Edit** link for a sensor group.

Step 4 Do the following to enter data for each of the fields:

a. Click ⌄

b. Enter the appropriate information.

c. Click **OK**.

Updating Sensor Group Priority

If a sensor is included in more than one sensor group, Prime Collaboration applies the thresholds for the highest priority sensor threshold group.

Step 1 Choose **Administration > Alarm & Event Configuration**.

Step 2 Choose Sensor Call Quality Settings from the Threshold Settings drop down list.

The Sensor Threshold Group page appears, displaying up to 10 user-defined sensor groups.

Step 3 Enter any unique numbers—up to two digits—in the Priority column.

Step 4 Click **Update Priority**. Prime Collaboration reorders the sensor groups and displays them in priority order.

Deleting a Sensor Group

You can delete a sensor threshold group.

To delete a sensor threshold group:

Step 1 Choose **Administration > Alarm & Event Configuration**.

Step 2 Choose Sensor Call Quality Settings from the Threshold Settings drop down list.

The Sensor Threshold Group page appears, displaying up to 10 user-defined sensor groups.

Step 3 Check the check boxes for the sensor groups that you want to delete.

Step 4 Click **Delete**. A confirmation dialog box is displayed.

Step 5 Click **Yes**. Prime Collaboration displays any remaining sensor groups in priority order.

Threshold Parameter Values

Table 2-1 lists the threshold categories, the threshold parameters in each category, and the minimum and maximum values for the threshold parameters.

Table 2-1 Minimum and Maximum Threshold Parameter Values

Threshold Category	Threshold Parameter (with unit of measure)	Min	Max	Parameter Type
Backup Interface Support Settings	Maximum Up Time (seconds)	0	86400	Data Settings
Cisco Communication Manager Express Utilization	Registered IP Phones Threshold (%)	1	100	Voice Utilization Settings
	Registered Key IP Phones Threshold (%)			
Cisco Communication Manager Port Utilization	FXS Port Utilization Threshold (%)	1	100	Voice Utilization Settings
	FXO Port Utilization Threshold (%)			
	BRI Channel Utilization Threshold (%)			Voice Utilization Settings
	T1 PRI Channel Utilization Threshold (%)			
	E1 PRI Channel Utilization Threshold (%)			
	T1 CAS Channel Utilization Threshold (%)			
	MOH Multicast Resources Active Threshold (%)			
	MOH Unicast Resources Active Threshold (%)			
	MTP Resources Active Threshold (%)			
	Transcoder Resources Active Threshold (%)			
	Hardware Conference Resources Active Threshold (%)			
	Software Conference Resources Active Threshold (%)			
	Conference Streams Active Threshold (%)			
	MOH Streams Active Threshold (%)			
	MTP Streams Active Threshold (%)			
	Location Bandwidth Available Threshold (%)			

Table 2-1 Minimum and Maximum Threshold Parameter Values (continued)

Threshold Category	Threshold Parameter (with unit of measure)	Min	Max	Parameter Type
Cisco Unity Connection Utilization	Inbound Port Utilization Threshold (%) Outbound Port Utilization Threshold (%)	1	100	Voice Utilization Settings
Cisco Unity Express Threshold Settings	Total Time Used Threshold (%)	0	100	Voice Health Settings
Cisco Unity Express Utilization	Capacity Utilization Threshold (%) Session Utilization Threshold (%) Orphaned Mailboxes Threshold (%)	1	100	Voice Utilization Settings
Cisco Unity Services Settings	CPU Utilization Threshold (%)			Voice Health Settings
Cisco Unity Threshold Settings	Unity License Threshold (count) Unity Inbox License Threshold (count)			Voice Health Settings
	Hung Port Threshold (seconds)	1800	7200	
Cisco Unity Utilization	Inbound Port Utilization Threshold (%) Outbound Port Utilization Threshold (%)	1	100	Voice Utilization Settings
Cluster Utilization Settings	Route Group Utilization Threshold (%)	1	100	Voice Utilization Settings
Conferencing Utilization	Persitent Chat Rooms Utilization Threshold Text Conferencing Rooms Utilization Threshold	0 0	2000 20000	Voice Utilization Settings
Dial-On-Demand Interface Support Settings	Maximum Up Time (seconds)	0	86400	Data Settings

Table 2-1 Minimum and Maximum Threshold Parameter Values (continued)

Threshold Category	Threshold Parameter (with unit of measure)	Min	Max	Parameter Type
Disk Usage and Virtual Memory Settings	Drive Array Faults Threshold (%)	0	100	Voice Health Settings
	Free Hard Disk Threshold (%) Free Virtual Memory Threshold (%)			Data Settings/ Voice Health Settings
Environment - Temperature Sensor Settings	Relative Temperature Threshold (%)			Voice Health Settings
Environment Settings	Relative Temperature Threshold (%) Relative Voltage Threshold (%)			Data Settings
Gatekeeper Utilization	Total Bandwidth Utilization for Local Zone Threshold (%) Interzone Bandwidth Utilization for Local Zone Threshold (%)	1	100	Voice Utilization Settings
Generic Interface/Port Performance Settings	Broadcast Threshold (%) Collision Threshold (%) Discard Threshold (%) Error Threshold (%)	0	100	Data Settings
	Error Traffic Threshold (%)	0.00	100.00	
	Queue Drop Threshold (%) Utilization Threshold (%)	0	100	
H323 Gateway Port Utilization	FXS Port Utilization Threshold (%) FXO Port Utilization Threshold (%) EM Port Utilization Threshold (%) BRI Channel Utilization Threshold (%) T1 PRI Channel Utilization Threshold (%) E1 PRI Channel Utilization Threshold (%) T1 CAS Channel Utilization Threshold (%) E1 CAS Channel Utilization Threshold (%) DSP Utilization Threshold (%)	1	100	Voice Utilization Settings
Interface/Port Flapping Settings	Link Trap Threshold (count)	0	10	Data Settings
	Link Trap Window (sec)	30	3600	

Table 2-1 Minimum and Maximum Threshold Parameter Values (continued)

Threshold Category	Threshold Parameter (with unit of measure)	Min	Max	Parameter Type
MGCP Gateway Port Utilization	FXO Port Utilization Threshold (%) FXS Port Utilization Threshold (%) BRI Channel Utilization Threshold (%) T1 PRI Channel Utilization Threshold (%) E1 PRI Channel Utilization Threshold (%) T1 CAS Channel Utilization Threshold (%)	1	100	Voice Utilization Settings
MWI Threshold Settings	MWI On-Time Threshold (seconds)	5	240	Voice Health Settings
Personal Assistant Threshold Settings	CPA Login Failure (count) CPA Transfer Fail (count) CPA Voice Mail (count)	0	100	Voice Health Settings
Presence Utilization	Common Partition LowWaterMark Utilization Threshold	0	94	Voice Utilization Settings
	CPU Utilization Threshold	0	100	
	Common Partition HighWaterMark Utilization Threshold	0	100	
Processor and Memory Settings	Backplane Utilization Threshold (%) Free Memory Threshold (%) Memory Buffer Miss Threshold (%) Memory Buffer Utilization Threshold (%) Memory Fragmentation Threshold (%) Processor Utilization Threshold (%)	0	100	Data Settings
Processor and Memory Settings	Free Physical Memory Threshold (%) Processor Utilization Threshold (%)	0	100	Voice Health Settings
Reachability Settings	Restart Trap Threshold (count)	0	10	Data Settings
	Restart Trap Window (seconds)	30	3600	
SIP Proxy	Active Subscriptions Utilization Threshold	0	300000	Voice Utilization Settings
Voice Mail Gateway Utilization	Voice Mail Port Utilization Threshold (%) PBX Port Utilization Threshold (%)	0	100	Voice Utilization Settings

Overview of Event Flooding Control

When Prime Collaboration detects a flood of active events, it can reduce the number of active events processed by enabling event flood control. After event flooding stops, the events that were temporarily not monitored are again processed by Prime Collaboration.

To understand more about event flood control, see the following topics:

- Event Flooding Rules
- Event Flood Logs

Event Flooding Rules

Prime Collaboration detects event flooding using the following rules. If any of the following occurs, it is considered an event flood.

- For a specific device, the same event occurs X number of times in Y number of minutes. The X and Y values are preconfigured in the system and stored in the database. Each event name has its own values.

  For example, if an InsufficientFreeMemory event occurs for a device 2 times 16 minutes, then it is considered an event flood.
- For a specific device, different types of events occur X number of times in Y number of minutes. The X and Y values are preconfigured in the system and stored in the database. The global setting for all devices is 1,000 events in 4 minutes.

After an event flood is detected for a given event, the subsequent events are not monitored until the device rule indicates that the event flood has stopped. Flood control is performed only for active events. The other event states (Cleared, UserCleared, and Acknowledged) are not considered flooding.

When the event flood is detected in Prime Collaboration, events get dropped and are logged in to the CSCOpx\log\CUOM\EPM\FloodDroppedEvents.log file.

An example of an event that violates the event flood rule:

```
2012|11:36:18.437|ERROR|Flood|EventBinder|EventFloodController|checkFlood|null|Minute:2
0762286 Received 28 in last 16 minutes. To suppress
la-ccm-11.cisco.com^#!$la-ccm-11.cisco.comServerUnreachable
23 Jun
2012|11:36:18.437|ERROR|Flood|EventBinder|EPMPluginImpl|processEventFilteration|null|Fl
ood has occurred for device = la-ccm-11.cisco.com, component= la-ccm-11.cisco.com,
eventName= ServerUnreachable, state= Active
```

An example of a dropped event:

```
2012|12:16:03.984|ERROR|Event|EventBinder|EventBinder|processNormalizedEvent|null|
Event Dropped for component: 172.25.109.221 ; Reason :-> Exceeded limit for eventStatus
= Active
```

Event Flood Logs

When event flooding occurs, the following files in CSCOpx\log\cuom\EPM provide details about the events:

1. FloodDroppedEvents.log—When events violate the flood control rules an entry appears in this file.

2. EPMDroppedEvents.log—When the events are huge in number and exceed the product limits an entry appears in this file.
3. ClearedDroppedEvents.log—When the events are huge in number, exceed the product limits, and are Cleared events that cannot be processed, an entry appears in this file.

Adding Dynamic Syslogs

Prime Collaboration enables you to add unsupported syslogs. You must get the exact syslog details from the device before you use the syslog in Prime Collaboration; 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.

We recommend that you do not add:

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

To add syslogs:

Step 1 Choose **Administration > Alarm & Event Configuration > Event Customization**.

Step 2 Click **Add Event**.

The New 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.

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

Step 4 Click **Add**.

You can:

- Use the **Edit** option to change the Event Clear interval.
- Customize the syslog name or event severity. To do this, go to the Event Customization page. See Customizing Alarms and Events for details.

Customizing Events—Global

You can enable or disable events or change the event severity globally for all the devices you manage.

Note The customizations you make here are applicable to all the devices.

To do this:

Step 1 Choose **Administration > Alarm & Event Configuration > Event Customization**.

Step 2 Check the check box corresponding to the Event, then select the desired option from the toolbar.

Step 3 Click Save.

Note The customizations you make here are applicable to all the devices.

To restore default event state and severity, select the desired check box, and click **Reset to Defaults**.

Customizing Events—Device Level

You can customize the events at a device level if you do not want to modify the events for all the devices.

To customize events at a device level,

Step 1 Choose **Operate > Device Work Center**.

Step 2 Select a device from Device Groups pane.

Step 3 Click **Customize Events.**

Note Device level customization takes precedence over global settings.

Step 4 Check the check box corresponding to the Event, then choose the desired option from the toolbar.

Step 5 Click **Save**.

Alarm Correlation Rules

The following are the predefined correlation rules in Prime Collaboration:

Table 2-2 Prime Collaboration Correlation Rules

Correlation Rule	Events	Attributes Used	Correlated Alarm	Number of Occurrences	Time Window (Min)
Call Throttling Detected	• CPUPegging • Code Yellow	• eventName • deviceId	Call Throttling Detected	NA	30
Prolonged Low Memory Condition Detected	LowAvailableVirtualMemory	• eventName • deviceId • state	Prolonged Low Memory Condition Detected	NA	10
Interface Flapping Occurrences	OperationallyDown	• eventName • deviceId • Component • OperStatus	InterfaceFlapping	3	20
Too many CPU Spikes Detected	• CPUPegging • HighUtilization	• eventName • deviceId	TooManyCPUSpikes	3	20
Repeated Authentication Failure	Authentication Failed	• eventName • deviceId	Repeated Authentication Failure	3	20
Repeated Location Bandwidth Out Of Resource Occurrences	LocationBWOutOfResources	• eventName • deviceId • Component	Repeated Location Bandwidth Out of Resource	3	20
WAN Link Outage Detected	Unresponsive	• eventName • XGS_VD_OBJECT_GRAPH	Wan Link Outage Detected	NA	10
Too many phones dropped connectivity					
Too many phones experienced poor call quality					

Modifying Alarm Correlation Rules

To modify the correlations rules:

Step 1 Choose **Administration > Alarm & Event Configuration > Rules Settings**.

Step 2 Click **Edit** corresponding to the desired rule to change the settings. See Alarm Correlation Rules for details about each rule.

Step 3 To enable or disable a rule, choose Enable or Disable from the drop down list at the eye icon for each rule.

Step 4 Click **Save**.

Activating Events in Prime Collaboration

Most device events are displayed in the user interface after the device has been added to the Prime Collaboration database. However, several events are not displayed in Prime Collaboration out of the box. You must activate the following events to enable Prime Collaboration to display them:

- Hardware Failure
- Number Of Registered Gateways Increased
- Number Of Registered Gateways Decreased
- Number Of Registered MediaDevices Increased
- Number Of Registered MediaDevices Decreased

To activate these events:

Step 1 Open the /opt/CSCOpx/conf/seg/sysLogConfig.xml file.

Step 2 Delete the commented lines in this file that appear around the event information that you want to enable:

```
<!--****Please delete this line and restart SEGServer process to enable processing of this
syslog
***** Please delete this line and restart SEGServer process to enable processing of this
syslog -->
```

Step 3 Save the file and restart the SEGServer process.

CHAPTER 3

Configuring Alarm and Event Notification

Cisco Prime Collaboration (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 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 for Prime Collaboration* and *Supported Events for Prime Collaboration*.

Prime Collaboration Notifications Triggers

For each alarms, 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 Adding and Device Notification Groups.

Table 3-1 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 Prime Collaboration default value to a user-defined value. See Customizing Events—Global.

Table 3-1 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.

Table 3-2 describes the contents of a notification group.

Table 3-2 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.
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 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.

Prime Collaboration supports device-based notification criterion. Table 3-3 describes the device-based notification criterion.

Table 3-3 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

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.

Table 3-4 describes the types of notification.

Table 3-4 Notification Types

Type	Description
SNMP Trap Notifications	Prime Collaboration generates traps with information about the alarms that caused it. CISCO-EPM-NOTIFICATION-MIB defines the trap message format. The CISCO-EPM-NOTIFICATION-MIB can be downloaded from Cisco.com. Using SNMP trap notification is different from forwarding raw traps to another server before they have been processed by Prime Collaboration. **Note** Prime Collaboration supports SNMP version 1 (SNMPv1) and SNMPv2 traps for polling and receiving. Prime Collaboration forwards traps as SNMPv1 traps. However, trap processing with SNMPv3 is not supported in Prime Collaboration.
E-Mail Notifications	Prime Collaboration generates e-mail messages containing information about the alarms. CISCO-EPM-NOTIFICATION-MIB defines the message, which is included in the e-mail in text format. When you create an e-mail subscription, you can choose whether to include the subject line only or the complete e-mail message. See *Cisco Prime Collaboration 9.0 Provisioning Guide* for details. about configuring email notifications for provisioning events.
Syslog Notifications	Prime Collaboration generates syslog messages that can be forwarded to syslog daemons on remote systems. 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.

Notifications Limited to Specific Alarms

In some cases, you might want to send notifications for only a subset of the alarms that 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 Prime Collaboration notification monitors. When you do not use alarm sets, 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.

Adding 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 **Alarm & Event Configuration > Notification > Assurance Notification Criteria.**

Step 2 Click Alarm Set 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. Using the Quick Filter might not work as desired.

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

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

To delete an Alarm Set, select the check box and click **Delete**.

Adding and Device Notification Groups

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

To add and edit device notification groups:

Step 1 Choose **Alarm & Event Configuration > Notification**, then select Assurance Notification Criteria from the drop-down list.

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:

Table 3-5 Add General Information

GUI Element	Description/Action
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

Table 3-5 Add General Information (continued)

GUI Element	Description/Action
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.

Step 4 Click **Next**.

The Select Devices/Device Groups pane appears.

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 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 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 Prime Collaboration *only* if you also select the 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 following information:

Table 3-6 Set Up Destination

GUI Element	Description/Action
Include Link to Notification Details check box	Check to include URLs in the notification from which users can directly open the relevant page in Prime Collaboration for more information. Uncheck to omit URLs from notifications.
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, page 3-8. • E-Mail—Enter data in the E-Mail Subscription Type fields, page 3-8. • Syslog—Enter data in the Syslog Subscription Type fields, page 3-8. 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 the Setting System-Wide Parameters Using System Preferences, page 20-17.
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 Recepient(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	
IP Address/Fully Qualified Domain Name editable column	Enter an IP address or Fully Qualified Domain Name (FQDN) of the host.

Table 3-6 Set Up Destination (continued)

GUI Element	Description/Action
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.

Step 9 Click **Next**.

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

CHAPTER 4

Monitoring Alarms and Events

Choose **Operate > Alarms & Events** to access the Alarms & Events page appears. You can filter alarms and events based on groups, using the **Device Group** pane on the left of the page.

The page has the following tabs:

- Alarm Summary
- Alarms
- Events

Alarm Summary

Alarm Summary provides a summary of the alarms for each device. The following details are displayed:

Table 4-1 Alarm Summary Tab Contents

Field	Description
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. Place the mouse pointer on this link to see the Device Details window.
Device IP	Device IP.
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 Updated Time	Time and date of alarm update (indicates activity, such as an alarm recurrence, alarm acknowledgement, the addition of a note, and so forth). Alarms are grouped by severity, and within severities, alarms with the latest change are listed first.

The alarms and events that correspond to the selections appear in the Alarms and Events for *device* subpane.

Alarms

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

Table 4-2 Alarm Browser

Field	Description
Severity	Indicates the severity of the alarm which can be, critical, major, minor, warning, or cleared. To view the events are associated with the alarm, hover the mouse over an alarm severity and click the quick view icon that appears. The Events of Alarm window appears, displaying the following details about the events for the alarm you selected: • Description—Alarm description. • Source—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 of Alarm window, you can click on: • The **See Event History** link to display the events associated with the selected alarm. • The **Monitor Endpoint** or **Monitor Session** link to launch the Endpoints Monitoring or Sessions Monitoring page. This link appears only for session and endpoint alarms.
Clipboard icon/Is Annotated	Indicates the alarm has user notations.
Status	Indicates the status of 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.
Device Name	Displays the name of the device that triggered the alarm.
Component Name	Device name, or the name of component such as a device pool, an interface.
Category	Displays the category of alarm. For example: session, endpoint, service infrastructure.
Name	Name of the generated alarm.
Message	Displays messages about the alarm.
Timestamp	Displays the date and time when the alarm occurred.
Owner	Displays the name of the person to whom this alarm is assigned. (If a name was entered.)

From the alarm browser, you can:

- View events associated with an alarm—Hover over your mouse on the icon next to alarm status to get a pop up window that displays 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**.

Events

The Events tab provide opens the event browser. To get the latest information, click the Refresh icon.

Table 4-3 Event Browser

Field	Description
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	
Event Name	
Device Name	
Device IP	
Component Name	
Last Updated	
Category	Displays the alarm assigned category, such as sessions, endpoints, and so on.
Description	Description of the event.

The Event Browser displays the total number events, a Refresh icon, and the Settings icon to customize the Event browser columns.

At any point, to see the Alarm Browser or Alarm Summary, click the links available at the bottom right.

INDEX

A

adding
- alarm set 3-5
- device-based notification group 3-6
- threshold group
  - CDR 2-9
  - sensor 2-10

alarm
- browser 4-2
- summary 4-1

alarms
- severity 1-5
- status 1-5

C

CDR threshold group
- adding 2-9
- deleting 2-10

cluster device discovery, running for device pool thresholds 2-4

codec thresholds, setting
- for CDR groups 2-9
- global values 2-8

D

deleting
- alarm set 3-5
- threshold groups 2-10, 2-11

device-based notifications 3-6

E

editing
- threshold groups
  - CDR 2-9
  - sensor 2-10

e-mail
- notifications 3-4

event
- browser 4-2
- severity 1-5

event flooding
- rules 2-16
- understanding 2-16

events
- flooding, control 2-16

F

fault management
- alarm creation 1-3
- alarms 1-2
- event creation 1-2
- events 1-1

flooding, event control 2-16

G

global thresholds 2-8
- restoring default 2-8
- updating 2-8

M

modifying
- device-based notification group 3-6

N

notification group
- device-based
  - adding 3-6
  - modifying 3-6

notifications
- e-mails, sending as 3-4
- SNMP traps, sending as 3-4
- syslogs, sending as 3-4

P

polling
- and user-defined groups 2-3
- data settings 2-3

R

restoring
- default thresholds 2-5

RTMT thresholds
- synchronizing 2-6
- viewing 2-5

S

SNMP
- trap
  - notifications 3-4

synchronize, RTMT thresholds 2-6

syslog notifications 3-4

T

thresholds
- CDR
  - group 2-9
  - priority 2-9
- global 2-8
- sensor
  - priority 2-11
- synchronizing RTMT 2-6
- thresholds, managing
  - default values, restoring 2-5
- viewing RTMT 2-5

U

updating
- thresholds
  - CDR group 2-9
  - global 2-8
  - sensor group 2-11