CHAPTER 9

Managing Network Alarms and Events

Prime Performance Manager allows you to view alarms and events that occur in your network. The following topics provide information about displaying network alarms and events:

Displaying Active Alarms and Event History

You can view active network alarms and historical events and manage them in multiple ways. Each alarm and event includes parameters to help you understand the alarm, its cause, and its history. Alarms and events are displayed from the Prime Performance Manager Performance menu:

- From the Network menu, choose **Alarms/Events > Active Alarms** to display all network alarms organized by occurrence date and time.
- From the Network menu, choose **Alarms/Events > Event History** to display historical events organized by occurrence date and time.
- Move cursor over **Alarm Browser** at the bottom of the Prime Performance Manager window to display all network alarms organized by occurrence date and time in a popup window.
- Move cursor over **Alarm Summary** at the bottom of the Prime Performance Manager window to display the number of alarms organized by device in a popup window.

Note The popup Alarm Browser and Alarm Summary can be turned off. For information, see Changing User Preferences, page 3-7.

- Display a device and choose **Active Alarms** to display alarms for that device.

Table 9-1 shows the alarm and event parameters. Not all parameters are displayed by default. To display them, see Adding and Removing Properties from Property Views, page 3-13.

Table 9-1 Active Alarms and Event History

Column	Description
Internal ID[1]	Internal ID of the alarm or event. The internal ID is a unique ID that Prime Performance Manager assigns for its own internal use. This ID can also be used when the Cisco Technical Assistance Center must debug problems.
Ack	Indicates whether the alarm or event is acknowledged.
Name	The alarm or event name.
Alarm Nature[1]	The alarm nature, which is determined when the alarm is created. Valid values: • ADAC—Automatically detected and automatically cleared • ADMC—Automatically detected and manually cleared • Undefined—Undefined
Alarm Type[1]	The alarm type. Alarm types include: • Communications • Processing Error • Environmental • QOS • Equipment • Undefined
Probable Cause[1]	The alarm or event probable cause.
Element Name[1]	The network element name associated with the event.
Category[1]	The event category. Categories include: • Network—Events pertaining to managed elements. • System—Events pertaining to Prime Performance Manager. • TCA—Threshold crossing alarm.
Severity	The alarm or event severity. Severities include: Critical, Major, Minor, Warning, Normal, Indeterminate, Informational **Note** You cannot change the severity of an event.
Original Severity[1]	The original severity of the event.
Count	The number of events in the event sequence for an alarm.
Note[1]	Indicates whether a note is associated with the event.
Create Time (*gateway time zone*)[2]	The time when this event was received in the gateway time zone. This column is displayed by default in the Event History window and the Events tab.
Create Time (Device Time Zone)[13]	The time when the event was created in the device time zone.
Change Time (*gateway time zone*)[2]	The time when this event was last updated in the gateway time zone.
Change Time (Device Time Zone)[2]	The time when the event was last updated in the device time zone.

Table 9-1 Active Alarms and Event History (continued)

Column	Description
Ack By[1]	The user who last acknowledged the alarm or event, or, user-based access is not implemented, the device name that last acknowledged the event. If not acknowledged, this field is blank.
Ack Time (*gateway time zone*)[2]	The time when the event was acknowledged in the gateway time zone.
Ack Time (Device Time Zone)[1]	The time when the event was acknowledged in the device time zone.
Device	Name of the device associated with the alarm or event. If no device is associated, None is displayed.
Device type[1]	The device type.
Clear By[1]	The user who cleared the event. If cleared automatically, the device name or IP address that cleared the alarm.
Clear Time (*gateway time zone*)[12]	The time when the event was cleared in the gateway time zone.
Clear Time (*device time zone*)[13]	The time when the event was cleared in the device time zone.
Message	Message associated with the alarm or event.

1. Not displayed by default. To display hidden properties, see Adding and Removing Properties from Property Views, page 3-13.
2. Format: mm-dd-yy hh:mm (XXX), where XXX is the gateway server time zone.
3. Format: mm-dd-yy hh:mm GMT-hh:mm.

Managing Alarms and Events

Prime Performance Manager provides many functions to filter and change the alarms and events display. Most functions are performed from the Network Active Alarms tab (Network > Alarms/Events > Active Alarms) or the Network Event History tab (Network > Alarms/Events > Event History). Actions that you can perform are described in the following topics:

Displaying an Alarm Summary

You can display a snap shot of your network health including the devices with the highest number of alarms, the device types with the highest alarm counts, alarm severity percentages, and alarm counts by device. These charts are displayed in one window so you get a quick overview of your network health at any given time.

To view the alarm summary, from the Network menu, choose **Alarms/Events**, then click **Alarms Overview**.

The following alarm charts are displayed:

- Top 10 Devices by Alarm Count—Displays the top 10 devices in the network with the highest alarm counts, starting with the highest alarm count.
- Top 10 Device Types by Alarm Count—Displays the top 10 device types in the network with the highest alarm counts, starting with the highest alarm count.
- Percentage of Alarm Severities—Displays the percentages of active alarms on the network, starting with the highest percentage.
- Number of Devices by Highest Severity—Presents a chart of devices and the device highest severity alarm.

Filtering Alarms and Events

You can filter alarms and events to show only alarms and events with particular interest, for example, you might want to display only critical alarms, or display only alarms and events for a particular device. These settings are applied to all alarms or events displayed in the current view.

To filter alarms or events:

Step 1 From the Network menu, choose **Alarms/Events**, then click **Active Alarms** or **Event History**.

Step 2 In the Active Alarms or Event History tab, click the **Modify event filter** tool.

In the Alarm and Event Filter dialog box, set the categories, severities, and other filter options that you want to use to filter the alarms and events.

- Categories options specify the alarm or event categories you want displayed:
  - System—Prime Performance Manager alarms and events.
  - Network—Managed element alarms and events.
  - TCA—Threshold crossing alerts.

  All categories are checked by default.
- Severities options specify the alarm and event severities you want displayed:
  - Informational
  - Normal
  - Indeterminate
  - Warning
  - Critical
  - Minor

  - Major

- Other options, listed in Table 9-2, further define the alarms and events you want filtered.

Table 9-2 Alarm and Event Filter Dialog Box Other Pane

Field	Description
Acknowledged	Indicates whether only acknowledged alarms/events appear in the Active Alarms or Event History window. This check box is checked by default.
Unacknowledged	Indicates whether only unacknowledged alarms/events appear in the Active Alarms or Event History window. This check box is checked by default.
Time Before	Indicates whether only alarms/events that Prime Performance Manager logs before a specified date and time, appear in the Active Alarms or Event History window. This check box is unchecked by default.
Time Before	Specifies the date and time prior to which alarms/events that Prime Performance Manager logs appear in the Active Alarms or Event History window. This field is dimmed unless the Time Before check box is checked.
Time After	Check box indicating whether only alarms/events that Prime Performance Manager logs after a specified date and time, appear in the Active Alarms or Event History window. This check box is unchecked by default.
Time After	Specifies the date and time after which alarms/events that Prime Performance Manager logs appear in the Active Alarms or Event History window. This field is dimmed unless the Time After check box is checked.
Name or Message Matches	Indicates whether only alarms/events that contain the specified message text appear in the Active Alarms or Event History window. This check box is unchecked by default. The Name or Message Matches field value is retained after a message filter is set.
Match Case	Indicates whether only alarms/events that match the case of the text in the Name or Message Matches field should appear in the Active Alarms or Event History window. This field is dimmed unless Name or Message Matches is selected. Match Case default is not selected by default if Name or Message Matches is selected. Match Case is disabled if Match Regex is selected. The Active Alarms or Event History table is filtered properly, based on the text entered in the Name or Message Matches text box (case sensitive), if Match Case is selected. The Match Case selection is retained after a message filter is set.

Table 9-2 Alarm and Event Filter Dialog Box Other Pane (continued)

Field	Description
Match Regex	Indicates whether only alarms/events that match the regular expression of the text in the Name or Message Matches field should appear in the Active Alarms or Event History window. This field is dimmed unless the Name or Message Matches check box is checked. Match Regex is unchecked by default, if the Name or Message Matches check box is checked. Match Regex is disabled if the Match Case check box is checked. The Active Alarms or Event History table is filtered properly, based on the regular expression entered in the Name or Message Matches text box (case-sensitive), if the Match Regex check box is selected. The check box Match Regex is selected after a message filter is checked. **Note** If invalid regex is provided, then Active Alarms or Event History table does not contain any rows.
Acknowledged By	Filters alarms or events by the individual who acknowledged the alarm. The username text you enter must match the Prime Performance Manager username or, if Prime Performance Manager is integrated with Prime Central, the Prime Central username.
Cleared By	Filters alarms or events by the individual who cleared the alarm. The username text you enter must match the Prime Performance Manager username or, if Prime Performance Manager is integrated with Prime Central, the Prime Central username.
Device Type	Filters alarms or events by device type. Check **Device Type**, then choose a network device from the drop-down list.
Suppress for unmanaged devices	Suppresses alarms/events for any objects that have been set to the unmanaged state. To suppress alarms/events for unmanaged objects, check the check box. To retain alarms/events for unmanaged objects, uncheck the check box. **Note** If you are viewing alarms/events for a specific object in the navigation tree of Prime Performance Manager main window, this button is not available.

Step 3 When finished, click **OK**.

Prime Performance Manager filters the alarms and events by the filter options you entered. To turn off the filter, click **Remove Filter**. Alternatively, to apply the filter, click **Apply Filter**. (The tool name alternates depending on whether the filter is applied.)

Displaying Alarm and Event Properties

Not all alarm or event properties are displayed in the Active Alarms or Event History windows. While you can choose to display the properties not displayed by default in the Active Alarms and Event History window, you can quickly view all parameters for individual alarms and events.

To view the properties for an individual alarm or event:

Step 1 From the Network menu, choose **Alarms/Events**.

Step 2 Do one of the following:

- In Active Alarms window, check the alarm whose properties you want to view or,
- Click **Event History** and check the event whose properties you want to view.

Step 3 From the Active Alarms or Event History window toolbar, click **Properties**.

The Prime Performance Manager Alarm and Event Properties window Properties tab displays the all properties listed in Table 9-1.

Related Topics

- Adding Notes to Alarms or Events, page 9-7
- Displaying Alarm or Event Details, page 9-8
- Displaying Alarm Events, page 9-8
- Displaying Daily Alarm and Event Archives, page 9-9

Adding Notes to Alarms or Events

Prime Performance Manager allows you to add notes to alarms and events, for example, you might want to add information about an alarm for others to know or as reminders, for example, the alarm or event's associated object, what triggered the alarm or event, how often it has occurred, and so on.

To add a note to an alarm or event:

Step 1 From the Network menu, choose **Alarms/Events**.

Step 2 Do one of the following:

- In Active Alarms window, click the alarm to which you want to add a note or,
- Click **Event History** and click the event to which you want to add a note.

Step 3 From the Active Alarms or Event History window toolbar, click **Edit Notes**.

The Prime Performance Manager Alarm and Event Properties window Notes tab is displayed. Any previously added notes are displayed. The date and time the notes were last updated is displayed in the Last Updated field. (If no notes have been added, the Last Updated field displays Not Set.)

Step 4 To add a new note, type the text in the note page, then click **Save Note** on the Notes toolbar.

Related Topics

- Displaying Alarm and Event Properties, page 9-6
- Displaying Alarm or Event Details, page 9-8
- Displaying Alarm Events, page 9-8
- Displaying Daily Alarm and Event Archives, page 9-9

Displaying Alarm or Event Details

Prime Performance Manager includes additional details for some alarms and events that are not included in the alarm or event message text or properties. For example, the SchedulerQueueSize alarm might display the following message:

```
Unit: unitname - The PPM scheduler queue size is over threshold which indicates a possible
performance problem.
```

The Alarm and Event Properties window Details tab might display additional details, such as:

```
QSize    110
QMax    155
QMin    0
QThreshold    100
QAvg    105
isAlarm    True
UnitEventId    468002
```

To display alarm or event details:

Step 1 From the Network menu, choose **Alarms/Events**.

Step 2 Do one of the following:

- In Active Alarms window, check the alarm whose details you want to view or,
- Click **Event History** and check the event whose details you want to view.

Step 3 From the Active Alarms or Event History window toolbar, click **Event Properties**, then click the **Details** tab.

Additional alarm or event details, if present, will be displayed.

Related Topics

- Displaying Alarm and Event Properties, page 9-6
- Adding Notes to Alarms or Events, page 9-7
- Displaying Alarm Events, page 9-8
- Displaying Daily Alarm and Event Archives, page 9-9

Displaying Alarm Events

To assist you in analyzing any individual alarm, you can view the events that comprise it. The events can be displayed chronologically, or sorted by other criteria such as device, severity, or message text. The collection of events provide a more detailed profile of any give alarm.

To display alarm events:

Step 1 From the Network menu, choose **Alarms/Events**.

Step 2 In Active Alarms window, check the alarm whose events you want to view.

Step 3 From the Active Alarms window toolbar, click **Events for Alarm**.

The alarm events are displayed.

Step 4 From the Events for Alarm tab you can perform any event function described in Table 9-1 on page 9-2.

Related Topics

- Displaying Alarm and Event Properties, page 9-6
- Adding Notes to Alarms or Events, page 9-7
- Displaying Alarm or Event Details, page 9-8
- Displaying Daily Alarm and Event Archives, page 9-9

Displaying Daily Alarm and Event Archives

Prime Performance Manager archives alarms and events every night. The archive process gathers all the events and alarms for that day and places them in a file-based archive. The daily archives can be stored back as far as several months, if needed. Eventually, you can move the daily archives out of your database and into compressed-file-based archives for long term storage.

To display the daily archive:

Step 1 From the Network menu, choose **Alarms/Events**.

Step 2 From the Active Alarms window, click **Daily Archives**.

The message archive is displayed. The daily archive is named Status+Alarms.*archivedate*.

Step 3 To display the archive, click the archive link.

Step 4 In the archive you can do any of the following to change the archive display:

- Limit the number of events displayed per page by clicking **10/Page** (10 events per page), **20/Page**, **50/Page**, **100/Page**, **200/Page**, **300/Page**, **400/Page**, or **500/Page**. In addition, you can:
  - Click **Max/Page** to display all archive events on one page.
  - Click **DefPrefs** to return to the default archive display.
  - Click **Reload** to reload the archive.
- Display only alarms and events with a particular severity level by clicking **Critical**, **Major**, **Minor**, **Warning**, **Informational**, **Admin**, **Error**, **Normal**, **Indeterminate**, **AlarmsOnly**, **AllEvents**.

Related Topics

- Displaying Alarm and Event Properties, page 9-6
- Adding Notes to Alarms or Events, page 9-7
- Displaying Alarm or Event Details, page 9-8
- Displaying Alarm Events, page 9-8

Displaying Device Details for an Alarm

Step 1 From the Network menu, choose **Alarms/Events**.

Step 2 In the Active Alarms window, click the alarm whose details you want to view.

Step 3 From the Active Alarms window toolbar, click **Properties**.

Step 4 In the Alarm and Event Properties window, click **Device Details**.

The following device details are displayed.

- Naming Information
- Status Information
- Polling Information
- Descriptive Information
- Uptime Information
- IP Addresses for SNMP

For information about the properties displayed, see Table 8-10 on page 8-18.

Step 5 From the Device Details tab, you can perform the following device actions.

- Poll Device—Polls the devices selected in the device list.
- Edit Properties—Allows you to edit the device display name and default web port. See Editing a Device Name, Web Port, and Time Zone, page 8-13.
- Edit Report Policy—Allows you to change the report policy assigned to the device. See Editing the Report Policy Assigned to a Device, page 8-15
- Edit Polling Policy—Allows you to change the polling policy assigned to the device. See Creating and Editing Device Polling Groups, page 8-22 and Editing the Polling Group Assigned to a Device, page 8-15.
- Edit SNMP IP Addresses—Allows you to edit a device SNMP IP addresses. See Editing the Device SNMP IP Addresses, page 8-16.
- Relocate Device—Allows you to relocate a device from one unit to another. See Relocating Devices to Units, page 8-16.
- Disable/Enable Sending Alarms—Disables or enables sending alarms from the selected device. The menu item displayed is based on the current device state.
- Manage/Unmanage Device—Changes managed devices to unmanaged, and unmanaged devices to managed. The menu item displayed is based on the current device state.
- Delete—Deletes the selected device(s).
- Ping—Pings the device to check connectity.
- Trace—Invokes traceroute to map the network route to the device.
- Launch—Launches the device home page.

Related Topics

- Displaying Alarm and Event Properties, page 9-6
- Adding Notes to Alarms or Events, page 9-7
- Displaying Alarm or Event Details, page 9-8
- Displaying Daily Alarm and Event Archives, page 9-9

Displaying Alarms by Device From the Alarms Window

You can display alarms by device from the Prime Performance Manager Alarms window or the Devices window. To display alarms by device from the Alarms window, choose **Alarms/Events** from the Network menu, then click **Alarms by Device**. For a description of alarms by device parameters, see Table 8-3 on page 8-5.

Displaying Alarms by Device Type From the Alarms Window

You can display alarms by device type from the Prime Performance Manager Alarms window or the Devices window. To display alarms by device from the Alarms window, choose **Alarms/Events** from the Network menu, then click **Alarms by Device**. For a description of alarms by device parameters, see Table 8-3 on page 8-5.

Configuring Upstream Alarm Hosts and Tuning Event and Alarm Parameters

The following topics tell you how to add upstream OSS hosts for Prime Performance Manager alarm SNMP traps. They also tell you how to tune Prime Performance Manager alarms and events:

Adding Upstream OSS Hosts

Prime Performance Manager allows you to send alarms and events to OSS hosts. To add an OSS host for Prime Performance Manager SNMP traps:

Step 1 Log into the Prime Performance Manager GUI as a System Administrator user.

Step 2 From the Administration menu, choose **Alarms/Events Editor**.

Step 3 On the Alarms/Events Editor toolbar, click the **Add a New Host** tool.

Step 4 In the Add Upstream OSS Host dialog box, enter the host parameters:

- Host—Enter the hostname or IP address
- Port—Enter the port Prime Performance Manager should use to connect to the host.
- Community—Enter the SNMP community string.
- SNMP Version—Enter the SNMP version, either Version 1 or 2c.

Note Prime Performance Manager supports SNMP v3 for device SNMP credentials. However, only SNMP v1 and 2c are supports for upstream OSS hosts.

- Trap Type—Enter the SNMP trap type:
  - CISCO-PRIME—The Cisco Prime trap type. See CISCO-PRIME Notification Attributes, page 9-16
  - CISCO-SYSLOG—The Cisco Syslog trap type.
  - CISCO-EPM-2—The Cisco EPM 2 trap type. See CISCO-EPM-2 Trap Notification Attributes, page 13-6

Step 5 Click **OK**.

Step 6 On the Alarms/Events Editor toolbar, click **Save Configuration**.

The new host is added to the Upstream OSS Hosts table.

Editing Upstream OSS Hosts

After you add an OSS host, you can edit the SNMP community, version, and trap type at a later point. You can filter alarms and events based upon alarm category or severity, device type, days of the week and hours within the day.

To edit OSS host SNMP details and/or filter events sent to the host:

Step 1 Log into the Prime Performance Manager GUI as a System Administrator user.

Step 2 From the Administration menu, choose **Alarms/Events Editor**.

Step 3 In the Upstream OSS Host table, select the host entry you want to edit, then modify the following as needed. For field descriptions, see Adding Upstream OSS Hosts, page 9-11.

- Host
- Port

Note Host and Port are not editable. If you need to change the host or host port, delete the host entry by clicking the Delete tool, then complete Adding Upstream OSS Hosts, page 9-11.

- Community
- SNMP Version
- Trap Type:
  - CISCO-PRIME
  - CISCO-SYSLOG
  - CISCO-EPM-2

Step 4 On the Alarms/Events Editor toolbar, click **Save Configuration**.

Step 5 To filter the alarms and events sent to OSS hosts, complete the "Configuring Alarms Sent to OSS Hosts" procedure on page 9-13.

Configuring Alarms Sent to OSS Hosts

You can configure the alarms and events that you want sent to OSS hosts based upon alarm category or severity, device type, days of the week and hours within the day.

To edit OSS host SNMP details and/or filter events sent to the host:

Step 1 Log into the Prime Performance Manager GUI as a System Administrator user.

Step 2 From the Administration menu, choose **Alarms/Events Editor**.

Step 3 In the Upstream OSS Hosts list, click the OSS host whose alarms you want to configure and click the **Set Filter** tool.

Step 4 In the OSS Filter dialog box, uncheck the alarm and event categories and severities that you do not want to send to the OSS host. (By default, all categories and severities are enabled.)

- Categories—System, Network, and TCA.
- Severities—Critical, Major, Minor, Warning, Informational, Indeterminate, Normal.
- Device Types—Include all the device types that have been added to Prime Performance Manager.
- Applicable—Specifies the days of the week and time of day when you want alarms sent to the OSS host.

Step 5 If you want an automation script executed when alarms and events are sent to the host, enter the path/script name in the Run Script field. The script can reside anywhere on your file system as long as you specify the full path, and the root user has the appropriate file and directory permissions to execute the script.

Step 6 Click **OK**.

Step 7 On the Alarms/Events Editor toolbar, click **Save Configuration**.

Configuring Alarms Sent to E-mail Addresses

You can configure alarms and events to be sent to e-mail addresses based upon alarm category or severity, device type, days of the week and hours within the day. You can configure multiple e-mail groups and define

To configure e-mail addresses:

Step 1 Log into the Prime Performance Manager GUI as a System Administrator user.

Step 2 From the Administration menu, choose **Alarms/Events Editor**.

Step 3 If a mail server is not configured, that is, the Mail Server field under Properties is blank, complete the following steps:

a. Under Properties, enter the mail server in the Mail Server field.

b. On the Alarms/Events Editor toolbar, click **Save Configuration**.

Note By default, Prime Performance Manager uses SMTP port 25. Should you need to change it to a different port, use the ppm smtpport command. See ppm smtpport, page B-75.

Step 4 On the Alarms/Events Editor toolbar, click **Add email address**.

Step 5 Enter the address(es) in the Add Email Address dialog box. If you are adding multiple addresses, use a semicolon to separate them.

Step 6 Click **OK**. The address(es) are added to the first row of the Email Addresses group at the bottom

Step 7 To configure the alarms and events you want sent to the addresses, in the address row click the **Set Filter** tool.

Step 8 In the Email Filter dialog box, uncheck the alarm and event categories and severities that you do not want to send to the OSS host. (By default, all categories and severities are enabled.)

- Categories—System, Network, and TCA.
- Severities—Critical, Major, Minor, Warning, Informational, Indeterminate, Normal.
- Device Types—Include all the device types that have been added to Prime Performance Manager.
- Applicable—Specifies the days of the week and time of day when you want alarms sent to the OSS host.

Step 9 Click **OK**.

Step 10 On the Alarms/Events Editor toolbar, click **Save Configuration**.

Step 11 You can perform the following actions at any future point:

- Repeat Steps 4 through 10 to add another address row. This allows you to send different alarms and events to different e-mail addresses.
- Add a new address or delete an existing from an address row.
- Click **Resend events and/or alarms** to send the alarms and events to the addresses in an address row.
- Click **Delete this entry** to delete the address row.

Forwarding Traps Directly to Hosts

In certain circumstances, you might want to forward SNMP traps directly to other alarm-processing servers without any Prime Performance Manager interaction. To forward SNMP traps to other hosts and bypass Prime Performance Manager alarm processing:

- Add the host information to TrapForwarder.properties, then,
- Use ppm traprelay command to enable trap forwarding.

By default, TrapForwarder.properties resides in /opt/CSCOppm-gw/properties. Enter host information using the format:

```
SERVERxx=dest-address[,portno]
```

where:

- •xx—Is the user-defined server number.
- •dest-address—Is the hostname, or the IP address in IPv4 or IPv6 format.
- •portno—Is the optional port number. The default port number is 162.

For example:

```
SERVER01=64.102.86.104
SERVER02=64.102.86.104,162
SERVER03=2011::2:c671:feff:feb0:e1ee
SERVER04=2011::2:c671:feff:feb0:e1ee,162
```

After you make changes to TrapForwarder.properties file:

- Restart the gateway using the ppm restart command (see ppm restart, page B-56).
- Enable trap forwarding using the ppm traprelay command (see ppm traprelay, page B-76).

Tuning Event and Alarm Parameters

To modify Prime Performance Manager event and alarm parameters:

Step 1 Log into the Prime Performance Manager GUI as a System Administrator user.

Step 2 From the Administration menu, choose **Alarms/Events Editor**.

Step 3 Under properties, edit the following parameters:

- Maximum Events—Edit the maximum number of events that Prime Performance Manager should retain in the events database. The default is 50,000 events.
- Maximum Alarms—Edit the maximum number of alarms that Prime Performance Manager should retain in the alarms database. The default is 25,000 alarms.
- Maximum Database Size—Edit the maximum database size that Prime Performance Manager should allow the database to reach. The default is 200,000 table rows.
- Event Age—Edit the number of days Prime Performance Manager should retain events. The default is 7 days.
- Alarm Age—Edit the number of days Prime Performance Manager should retain alarms. The default is 14 days.
- Cleared Alarm Age—Edit the number of seconds Prime Performance Manager should retain cleared alarms. The default is 1440 minutes (24 hours).
- Archive Active Alarms—Indicate whether active alarms should be archived, True (default) or False.
- Send Events—Indicates whether traps are sent to the OSS upstream host for events, True or False (default).
- Send Alarms—Indicates whether traps are sent to the OSS upstream host for alarms, True (default) or False.
- Send Updates—Indicates whether traps are sent to the OSS upstream host for updates, True (default) or False.
- Send Deletes—Indicates whether traps are sent to the OSS upstream host for deletes, True (default) or False.

Note Send Events, Send Alarms, Send Updates, and Send Deletes control the traps sent to the OSS host. For example, if Send Updates is false, Prime Performance Manager only sends traps when the alarm is raised, and not when it is updated.

- OSS Trap Throttle—Slows down the rate that Prime Performance Manager sends traps to the OSS so that the OSS is not overwhelmed. The default is 0 milliseconds.
- Heartbeat Interval—Sets the rate at which Prime Performance Manager sends a heartbeat trap to the OSS to indicate that Prime Performance Manager is still running. The default is 0, which means no trap is sent.
- Node Display Name—Sets the device display name in the Prime Performance Manager Alarms and Events window:
  - DNS or User Defined—Uses the device DNS or user-defined name (default).
  - IP Address—Uses the device IP address.
  - System Name—Uses the device system name.
  - Sync Name—Uses the device sync name.
  - Business Tag—Uses the device business tag.
  - Business Tag - DNS Name—Uses the device DNS name business tag.
  - Business Tag - System Name—Uses the device system name business tag.
  - Business Tag - Sync Name—Uses the device sync name business tag.
- Database Maintenance Interval—Sets the interval, in minutes, when the events database is updated based on the properties entered here. The default is 15 minutes.
- Automation Timeout—Sets the amount of time to wait, in seconds, before an OSS host automation script times out because it cannot execute, for whatever reason. (See Editing Upstream OSS Hosts, page 9-12 for information about adding automation scripts.) The default is 300 seconds.
- Event Automation: Disable Override—Specifies the event script priority if event automation scripts are entered for the OSS host and for thresholds.
  - True (default)—The OSS automation script and threshold script are executed.
  - False—Scripts entered for thresholds are executed when the trap is sent northbound not the script entered in for the OSS host.
- Mail Server—Enter the e-mail server to be used for e-mail addresses entered for TCAs (see Creating Thresholds, page 10-1) and OSS traps.

Step 4 When finished, on the Alarms/Events Editor toolbar, click **Save Configuration**.

Prime Performance Manager SNMP Traps

The following sections describe the OSS host traps used by Prime Performance Manager.

CISCO-PRIME Notification Attributes

The CISCO-PRIME trap (CISCO-EPM-NOTIFICATION-MIB::ciscoEpmNotification) supports new, update, and delete events. Information was removed from it to correspond to the Cisco Prime Network trap.

Table 9-3 describes the CISCO-PRIME notification attributes.

Table 9-3 CISCO-PRIME Notification Attributes

Attribute Name	OID	Value
cenAlarmVersion	1.3.6.1.4.1.9.9.311.1.1.2.1.2	The version of this MIB. The version string format is: major version.minor version. **Note** Always set to 3.
cenAlarmTimestamp	1.3.6.1.4.1.9.9.311.1.1.2.1.3	Unused Varbind.
cenAlarmUpdatedTimestamp	1.3.6.1.4.1.9.9.311.1.1.2.1.4	Unused Varbind.
cenAlarmInstanceID	1.3.6.1.4.1.9.9.311.1.1.2.1.5	The unique alarm instance ID.
cenAlarmStatus (Integer32)	1.3.6.1.4.1.9.9.311.1.1.2.1.6	Possible values: • 0—New • 1—Update • 2—Delete
cenAlarmStatusDefinition	1.3.6.1.4.1.9.9.311.1.1.2.1.7	Alarm name (short description).
cenAlarmType	1.3.6.1.4.1.9.9.311.1.1.2.1.8	Alarm nature: • ADAC(1)—Auto detected; auto cleared • ADMC(2)—Auto detected; manually cleared
cenAlarmCategory	1.3.6.1.4.1.9.9.311.1.1.2.1.9	Integer corresponding to a user-defined event category.
cenAlarmCategoryDefinition	1.3.6.1.4.1.9.9.311.1.1.2.1.10	String representation of the event category. Default Categories: <0,System> <1,Network> <2,TCA>
cenAlarmServerAddressType	1.3.6.1.4.1.9.9.311.1.1.2.1.11	The Internet address type where the server generating this trap is reached. This value is set to 1 for IPv4 management, and 2 for IPv6 management.
cenAlarmServerAddress	1.3.6.1.4.1.9.9.311.1.1.2.1.12	Prime Performance Manager gateway IP address. Set the server address to any address (0.0.0.0) if it is a SNMP v1 trap with an IPv6 address.
cenAlarmManagedObjectClass	1.3.6.1.4.1.9.9.311.1.1.2.1.13	For service and TCA events, this is a string that identifies the source of the event. For example: Node=1.2.3.4 Node=1.2.3.4,ifDescr=Ethernet0/0 For PPM system events, this is an empty string ("").
cenAlarmManagedObjectAddressType	1.3.6.1.4.1.9.9.311.1.1.2.1.14	The Internet address type where the managed object is reachable. This value is set to 1 for IPV4 management, and 2 for IPv6 management.

Table 9-3 CISCO-PRIME Notification Attributes (continued)

Attribute Name	OID	Value
cenAlarmManagedObjectAddress	1.3.6.1.4.1.9.9.311.1.1.2.1.15	IP Address of the managed object: • Node and TCA events - IP Address of the network element • System event-Cisco PPM gateway IP address.
cenAlarmDescription	1.3.6.1.4.1.9.9.311.1.1.2.1.16	Event message text.
cenAlarmSeverity	1.3.6.1.4.1.9.9.311.1.1.2.1.17	Indicates the severity of the alarm using an integer value.
cenAlarmSeverityDefinition	1.3.6.1.4.1.9.9.311.1.1.2.1.18	String representation of the alarm severity. Alarm severity values are: • 0—Normal • 1—Indeterminate • 2—Informational • 3—Warning • 4—Minor • 5—Major • 6—Critical A separate OID indicating a clear alarm is not provided. A clear alarm is indicated by this OID when the severity is 0 (Normal).
cenAlarmTriageValue (Integer32)	1.3.6.1.4.1.9.9.311.1.1.2.1.19	Unused varbind.
cenEventIDList (OCTET STRING)	1.3.6.1.4.1.9.9.311.1.1.2.1.20	Examples: Format: key=value; includes X.733 alarm type and probable cause. AlarmType=Communications ProbableCause=ThresholdCrossed NodeCreateTime=Alarm create time in device time zone NodeChangeTime=Alarm change time in device time zone NodeClearTime=Alarm clear time in device time zone NodeAckTime=Alarm acknowledgement time in device time zone VNEName=Prime Network VNE name, if applicable Other values can be set for different alarms and events.
cenUserMessage1	1.3.6.1.4.1.9.9.311.1.1.2.1.21	User input message.
cenUserMessage2	1.3.6.1.4.1.9.9.311.1.1.2.1.22	User input message. Value is “PPM”.

Table 9-3 CISCO-PRIME Notification Attributes (continued)

Attribute Name	OID	Value
cenUserMessage3	1.3.6.1.4.1.9.9.311.1.1.2.1.23	User input message.
cenAlarmMode	1.3.6.1.4.1.9.9.311.1.1.2.1.24	The possible values are: • 2—Alarm • 3—Event
cenPartitionNumber (Unsigned32)	1.3.6.1.4.1.9.9.311.1.1.2.1.25	Unused varbind.
cenPartitionName (SnmpAdminString)	1.3.6.1.4.1.9.9.311.1.1.2.1.26	Acknowledged by username/time.
cenCustomerIdentification (SnmpAdminString)	1.3.6.1.4.1.9.9.311.1.1.2.1.27	Cleared by username/time.
cenCustomerRevision (SnmpAdminString)	1.3.6.1.4.1.9.9.311.1.1.2.1.28	Create Time.
cenAlertID (SnmpAdminString)	1.3.6.1.4.1.9.9.311.1.1.2.1.29	Update Time.

CISCO-EPM-2 Trap Notification Attributes

The CISCO-EPM-2 trap (CISCO-EPM-NOTIFICATION-MIB::ciscoEpmNotificationAlarmRev2) supports new, update, and delete events. This is the second EPM trap version.

Table 9-4 describes the CISCO-EPM-2 notification attributes.

Table 9-4 CISCO-EPM-2 Notification Attributes

Attribute Name	OID	Value
cenAlarmVersion	1.3.6.1.4.1.9.9.311.1.1.2.1.2	EPM version number: EPM(1), EPM-2(2).
cenAlarmTimestamp	1.3.6.1.4.1.9.9.311.1.1.2.1.3	The time when the alarm was raised. The cenAlarmTimestamp value is contained in the SNMP TimeTicks Variable Binding type, which represents the time in hundredths of a second. The event creation time (long) value in Cisco Prime Network is divided by 10 and modulo by (2^32)-1 before it is packaged. For example: Cisco PPM Event Creation time = X cenAlarmTimestamp = (X / 10)%((2^32) - 1)
cenAlarmUpdatedTimestamp	1.3.6.1.4.1.9.9.311.1.1.2.1.4	Alarms persist over time and their fields can change values. The updated time indicates the last time a field changed and this alarm updated.
cenAlarmInstanceID	1.3.6.1.4.1.9.9.311.1.1.2.1.5	Unique event ID.
cenAlarmStatus	1.3.6.1.4.1.9.9.311.1.1.2.1.6	The alarm status: 0,New 1,Update 2,Delete

Table 9-4 CISCO-EPM-2 Notification Attributes (continued)

Attribute Name	OID	Value
cenAlarmStatusDefinition	1.3.6.1.4.1.9.9.311.1.1.2.1.7	The alarm status definition: 0,New 1,Update 2,Delete
cenAlarmType	1.3.6.1.4.1.9.9.311.1.1.2.1.8	AlarmNature (Undefined(0), ADAC(1), ADMC(2))
cenAlarmCategory	1.3.6.1.4.1.9.9.311.1.1.2.1.9	Integer corresponding to user-defined event category.
cenAlarmCategoryDefinition	1.3.6.1.4.1.9.9.311.1.1.2.1.10	String representation of event category. Default categories: <0,System> <1,Network> <2,TCA>
cenAlarmServerAddressType	1.3.6.1.4.1.9.9.311.1.1.2.1.11	The alarm server address type. This is set to 1 for IPV4 management and 2 for IPv6 management.
cenAlarmServerAddress	1.3.6.1.4.1.9.9.311.1.1.2.1.12	Prime Performance Manager gateway IP address. Set the server address to any address (0.0.0.0) if it is a SNMP v1 trap with an IPv6 address.
cenAlarmManagedObjectClass	1.3.6.1.4.1.9.9.311.1.1.2.1.13	For network and TCA alarms that pertain to a managed element, the value is Node. For alarms that pertain to Prime Performance Manager, the value is an empty string.
cenAlarmManagedObjectAddressType	1.3.6.1.4.1.9.9.311.1.1.2.1.14	The Internet address type where the managed object is reachable. This value is set to 1 for IPV4 management, and 2 for IPv6 management.
cenAlarmManagedObjectAddress	1.3.6.1.4.1.9.9.311.1.1.2.1.15	The IP address of the managed object. Values are either the IP address of the router or the IP address of the Prime Performance Manager server.
cenAlarmDescription	1.3.6.1.4.1.9.9.311.1.1.2.1.16	Event message text.
cenAlarmSeverity	1.3.6.1.4.1.9.9.311.1.1.2.1.17	Integer corresponding to user-defined event severity.

Table 9-4 CISCO-EPM-2 Notification Attributes (continued)

Attribute Name	OID	Value
cenAlarmSeverityDefinition	1.3.6.1.4.1.9.9.311.1.1.2.1.18	String representation of event severity. Severity values are: 0—Normal 1—Indeterminate 2—Informational 3—Warning 4—Minor 5—Major 6—Critical A separate OID indicating a clear alarm is not provided. A clear alarm is indicated by this OID when the severity is 0 (Normal).
cenAlarmTriageValue	1.3.6.1.4.1.9.9.311.1.1.2.1.19	Unused (Always 0).
cenEventIDList	1.3.6.1.4.1.9.9.311.1.1.2.1.20	List of key/value pairs to accommodate alarm attributes not included in other EPM notification varbinds. Includes timestamps in the managed device time zone. NodeCreateTime=2010-06-17,23:25:44.65,-2202 NodeChangeTime=2010-06-17,23:31:41.517,-2202 NodeClearTime=2010-06-17,23:31:41.516,-2202 NodeAckTime=2010-06-17,23:28:38.337,-2202 AlarmType=Communications; TCAValue=; TCAObject=; TCARelation=; TCAEvaluation=; TCAPeriod=;
cenUserMessage1	1.3.6.1.4.1.9.9.311.1.1.2.1.21	The event/alarm name.
cenUserMessage2	1.3.6.1.4.1.9.9.311.1.1.2.1.22	UNIX time when event occurred. See cenAlarmTimestamp. Example: 2030-04-14, 16:05:05.369,+0400
cenUserMessage3	1.3.6.1.4.1.9.9.311.1.1.2.1.23	UNIX time when event changed. See cenAlarmUpdatedTimestamp. Example: 2030-04-14, 16:05:05.369,+0400
cenAlarmMode	1.3.6.1.4.1.9.9.311.1.1.2.1.24	The alarm mode. Values are either Alarm(2) Event(3)
cenPartitionNumber	1.3.6.1.4.1.9.9.311.1.1.2.1.25	Number of times this event or alert has occurred.

Table 9-4 CISCO-EPM-2 Notification Attributes (continued)

Attribute Name	OID	Value
cenPartitionName	1.3.6.1.4.1.9.9.311.1.1.2.1.26	Correlation key
cenCustomerIdentification	1.3.6.1.4.1.9.9.311.1.1.2.1.27	Network element name
cenCustomerRevision	1.3.6.1.4.1.9.9.311.1.1.2.1.28	Format: AckUserName;Timestamp AckUserName is one of: • < *PPM Client Name* > - the Prime Performance Manager client name if user access is disabled • < *PPM username* > - the Prime Performance Manager username if user access is enabled
cenAlertID	1.3.6.1.4.1.9.9.311.1.1.2.1.29	Format: ClearUserName;Timestamp ClearUserName is one of: • < *PPM Client Name* > - manual clear: the Prime Performance Manager client name if user access is disabled • < *PPM username* > - manual clear: the Prime Performance Manager username if user access is enabled • < AutoClear > - auto clear: the string value "AutoClear"