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 Alarms and Events

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 one of the following:

- From the Network menu, choose **Alarms/Events > Alarms** to display all network alarms organized by occurrence date and time. The alarms are organized by the time they are last changed.
- From the Network menu, choose **Alarms/Events > Events** to display historical events organized by occurrence date and time. The events are organized by the time they occurred.
- 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 Customizing the GUI and Information Display, page 3-8.

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

Table 10-1 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 3-20.

Table 10-1 Alarms and Events

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.
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.
Condition	The alarm or event condition.
TCA Name[1]	For threshold crossing alerts (TCA), the TCA name. The name is assigned by the user who created the threshold.
TCA Metric	For TCAs, the TCA metric, for example, if the threshold is a percentage, the percent at which the threshold was crossed.
TCA Type	For TCAs, the TCA type.
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.

Table 10-1 Alarms and Events (continued)

Column	Description
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 Events 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.
Tenant	The tenant affected by, or connected to, the alarm.
Owner	The user assigned to the alarm, if user-access is enabled. To assign users to alarms, see Assigning Users to Alarms or Events, page 10-8.
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.
Clear By[1]	The user who cleared the event. If cleared automatically, the device name or IP address that cleared the alarm.
Clear Time	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 3-20.
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 Alarms tab (Network menu > Alarms/Events > Alarms) or the Network Events tab (Network menu > Alarms/Events > Events). Actions that you can perform are described in the following topics:

Responding to Alarms and Events

You can respond to alarms or events in the Alarms or Events window, for example, acknowledge, clear, or delete an alarm or an event. You can also add notes to alarms and change the alarm severity. You can also acknowledge and clear alarms from the device level.

Note If Prime Performance Manager is integrates with Prime Central, alarm responses and other actions are not available. All alarm responses must be performed in Prime Central.

To respond to alarms or events from the Alarms or Events window:

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

Step 2 In the Alarms or Events tab, select the alarm or event, then choose any of the following responses on Alarms or Events toolbar:

- Ack (Acknowledge)—Acknowledges the alarm or event.
- Unack (Unacknowledge)—Unacknowledges the alarm or event.
- Clear—Clears the alarm or event.
- Annotate—Allows you to add notes to the alarm. (see Adding Notes to Alarms or Events, page 10-9)
- Assign—Assign this alarm to another user through e-mail. (Only visible when user access is enabled.)
- Delete—Deletes the alarm.
- Clear/Delete—Clears and deletes the alarm.
- Properties—Displays the alarm properties. See Displaying Alarm and Event Properties, page 10-7.
- Time Diff—Compares the time difference between two alarms. To compare alarms, click the first alarm, press **Ctrl** and choose the second, then click **Time Diff**.
- Events—Displays events associated with the alarm. See Displaying Alarm and Event Properties, page 10-7.
- Report—For alarms based on threshold crossing alerts (TCAs), displays the report containing the threshold on which the TCA was created.
- Change severity—Changes the alarm severity.

In addition, you can ping or start a trace route for any device with an alarm by selecting an alarm clicking the **Ping** or **Traceroute** tools on the alarm totals bar above the Network Alarms toolbar.

To acknowledge or clear alarms by device:

Step 1 From the Network menu, choose **Devices**, then click **Alarms by Device**.

Step 2 Select the device whose alarms you want to acknowledge or clear, then from the Actions menu choose:

- Acknowledge Alarm—Acknowledges the alarm or event for the selected device.
- Clear Alarms—Clears the alarm or event for the selected device.

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 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 **Alarms** or **Events**.

Step 2 In the Alarms or Events tab, click the **Modify 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
  - Warning
  - Critical
  - Minor
  - Major

- Other options, listed in Table 10-2, further define the alarms and events you want filtered.

Table 10-2 Alarm and Event Filter Dialog Box Other Pane

Field	Description
Acknowledged	Indicates whether only acknowledged alarms/events appear in the Alarms or Events window. This check box is checked by default.
Unacknowledged	Indicates whether only unacknowledged alarms/events appear in the Alarms or Events window. This check box is checked by default.
Time Before	(Checkbox and date entrance fields) Indicates whether only alarms/events that Prime Performance Manager logs before a specified date and time, appear in the Alarms or Events window. This check box is unchecked by default. This field is dimmed unless the **Time Before** checkbox is checked
Time After	(Checkbox and date entrance fields) Indicates whether only alarms/events that Prime Performance Manager logs after a specified date and time, appear in the Alarms or Events window. This check box is unchecked by default.This field is dimmed unless the **Time After** checkbox is checked.
Name or Message Matches	Indicates whether only alarms/events that contain the specified message text appear in the Alarms or Events 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 Alarms or Events 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 Alarms or Events 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 10-2 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 Alarms or Events 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 Alarms or Events 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 Alarms or Events 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.
Owner	Filters alarms or events by the alarm or event owner. After you check this option, choose a user from the list of Prime Performance Manager users that appear in the drop-down list. See Assigning Users to Alarms or Events, page 10-8 for more information.
Device Type	Filters alarms or events by device type. Check **Device Type**, then choose a network device or tenant 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 Alarms or Events windows. While you can choose to display the properties not displayed by default in the Alarms and Events 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 Alarms window, check the alarm whose properties you want to view or,
- Click **Events** and check the event whose properties you want to view.

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

The Prime Performance Manager Alarm and Event Properties window Properties tab displays the all properties listed in Table 10-1.

Related Topics

- Adding Notes to Alarms or Events, page 10-9
- Displaying Alarm or Event Details, page 10-9
- Displaying Alarm Events, page 10-10
- Displaying Daily Alarm and Event Archives, page 10-10

Assigning Users to Alarms or Events

Prime Performance Manager allows administrators to assign users to alarms and events when:

- Prime Performance Manager is not integrated with Prime Central. For information, see Integrating Prime Performance Manager with Prime Central, page 4-2.
- User access is enabled. For information, see Setting Up User Access and Security, page 6-1.
- The user you want to access is added to Prime Performance Manager. For information, see Adding New Users, page 6-15.

To assign a user to an alarm:

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

Step 2 In Alarms window, click the alarm that you want to assign.

Step 3 From the Alarms window toolbar, click **Assign**.

Step 4 In the Alarm Owner dialog box, choose the user you want to assign from the Owner list.

Step 5 Click **Send Email** if you want to send the user you assign an e-mail about the alarm or event assignment. (This option is only available if an email address was added to the user profile. For information, see Adding New Users, page 6-15.

Step 6 Click **OK**.

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

Step 3 From the Alarms or Events window toolbar, click **Annotate**.

The Details for Selected Alarm or Details for Selected Event 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 Type the note text, then click **Save Note** on the Notes toolbar.

Related Topics

- Displaying Alarm and Event Properties, page 10-7
- Displaying Alarm or Event Details, page 10-9
- Displaying Alarm Events, page 10-10
- Displaying Daily Alarm and Event Archives, page 10-10

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 Alarms window, check the alarm whose details you want to view or,
- Click **Events** and check the event whose details you want to view.

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

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

Related Topics

- Displaying Alarm and Event Properties, page 10-7
- Adding Notes to Alarms or Events, page 10-9
- Displaying Alarm Events, page 10-10
- Displaying Daily Alarm and Event Archives, page 10-10

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 Alarms window, check the alarm whose events you want to view.

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

The alarm events are displayed.

Step 4 From the Events for Alarm tab you can perform any event function described in Table 10-1 on page 10-2.

Related Topics

- Displaying Alarm and Event Properties, page 10-7
- Adding Notes to Alarms or Events, page 10-9
- Displaying Alarm or Event Details, page 10-9
- Displaying Daily Alarm and Event Archives, page 10-10

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 Alarms window, click the **Daily Archives** tab.

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 10-7
- Adding Notes to Alarms or Events, page 10-9
- Displaying Alarm or Event Details, page 10-9
- Displaying Alarm Events, page 10-10

Displaying Device Details for an Alarm

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

Step 2 Click the Alarms tab and select the alarm whose details you want to view.

Step 3 From the 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
- Device Performance
- Descriptive Information
- Uptime Information
- Device Performance
- Unique Device Identifier

For information about the properties displayed, see Table 9-11 on page 9-26.

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, Time Zone, and Location, page 9-16.

- Edit Report Policy—Allows you to change the report policy assigned to the device. See Editing the Report Policy Assigned to a Device, page 9-20
- Edit Polling Group—Allows you to change the polling group assigned to the device. See Creating and Editing Device Polling Groups, page 9-35 and Editing the Polling Group Assigned to a Device, page 9-20.
- Edit Management IP Addresses—Allows you to edit a device management IP addresses. See Editing the Device Management IP Addresses, page 9-21.
- Change Interface Polling—Allows you to change interface polling. For information, seeRemoving Device Interfaces From Polling, page 9-22.
- Relocate Device—Allows you to relocate a device from one unit to another. See Relocating Devices to Units, page 9-22.
- Disable Alarms and TCAs—Disables sending alarms and TCAs from the selected device for the time period entered the date and time range dialog that is displayed.
- 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 connectivity.
- Trace—Invokes traceroute to map the network route to the device.

Note You can also ping or invoke a traceroute for a device from the Network Alarms window.

- Pause—Pauses the device polling.
- Refresh Interval—Changes the device refresh interval.

Related Topics

- Displaying Alarm and Event Properties, page 10-7
- Adding Notes to Alarms or Events, page 10-9
- Displaying Alarm or Event Details, page 10-9
- Displaying Daily Alarm and Event Archives, page 10-10

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 9-3 on page 9-6.

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 Type**. For a description of alarms by device parameters, see Table 9-3 on page 9-6.

Monitoring System Health

Prime Performance Manager predefined alarms help you monitor your system health. Alarms reflecting your system health are listed in Table 10-3.

Note System health is affected by many network factors. Use the predefined alarms as a starting point.

Table 10-3 System Health Alarms

Alarm	Severity
DiskUtilization	• Critical—Exceeds minimum disk space requirement. • Warning—Approaching minimum disk space requirement.
ServerStateChanged	• Major—The gateway or unit changed state.
BulkStatsInfo	• Informational—Bulk statistics file processing information messages include: – DeviceNotDiscovered – NoHeader – NoFooter – MissingFilenameParams
BulkStatsError	Bulk statistics file processing error conditions: • Major - MultiDeviceFailure—Multiple devices failed to receive bulk statistics files. • Major - NoFiles—A single device is not seeing any bulk statistics files. • Minor - MinorSkip—A single device did not receive one bulk statistics file. • Minor - MajorSkip—A single device did not receive multiple bulk statistics files
ServerConnectionStatus	• Critical—A gateway or unit lost connection to each other unexpectedly. • Warning—A gateway or unit lost connection to each other through an operator shutdown.
ServerClockStatus	• Major—The unit server clock is out of sync with the gateway.

Table 10-3 System Health Alarms (continued)

Alarm	Severity
InventorySyncStatus	• Major—Inventory sync with Prime Network, Prime Central, or Prime Network Services Controller failed.
AlarmSyncStatus	• Major—Alarm sync with an upstream OSS failed.
UnitFailOver	• Major—Unit failed over to redundant unit unexpectedly. • Minor—Unit failed over to redundant unit via operator command.
GatewayFailOver	• Major—The gateway failed over to the secondary gateway unexpectedly or dual primary gateways are detected. • Informational—The gateway failed over to secondary gateway through operator command.
CSVFileError	• Major—An error occurred writing an exported CSV file.
DBProcessorError	• Major—An error occurred writing data to the database.
SchedulerQueueSize	• Major—The scheduler queue size is over threshold, indicating a possible performance problem.
PollerTaskOutOfMemeory	• Major—A congested scheduler queue indicates too many tasks are scheduled and waiting to be run on the queue. A performance issue could be preventing the system from running all the scheduled tasks.
SyncMsgOutOfMemory	• Major—Out of memory while trying to sync messages between gateway and unit.

You can also create TCAs on underlying server or OS metrics. Common ones include:

- CPU Utilization
- Memory Utilization
- Disk Utilization
- Swap Utilization

For information about setting thresholds, see Creating and Managing Thresholds, page 11-1.

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:

- Prime Performance Manager SNMP Traps, page 10-21

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 OSS 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 supported for upstream OSS hosts.

- Trap Type—Enter the SNMP trap type:
  - CISCO-PRIME—The Cisco Prime trap type. See CISCO-PRIME Notification Attributes, page 10-21
  - CISCO-SYSLOG—The Cisco Syslog trap type.
  - CISCO-EPM-2—The Cisco EPM 2 trap type. See CISCO-EPM-2 Trap Notification Attributes, page 10-24

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 10-15.

- 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 10-15.

- 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 10-16.

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, Normal.
- Device Types—Include all the device types that have been added to Prime Performance Manager.
- Tenants—If tenants are created, they appear under Tenants and can be selected.
- Groups—If report groups are created, they appear under Groups and can be selected. For information, see Creating a Report Group, page 7-54. (If no groups are available, this item is not displayed.)
- Report Policies—If report policies are created, they appear under Report Policies and can be selected. For information, see Assigning Devices to Report Policies, page 7-34. (If no report policies are available, this item is not displayed.)
- 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 Send 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 **System Settings**.

Step 3 If a mail server is not entered in the SMTP Mail Server field, enter your mail server IP address or hostname now. The mail server must be configured before you can send alarms and event e-mails.

Step 4 From the Administration menu, choose **Alarms/Events Editor**.

Step 5 On the Alarms/Events Editor toolbar, click **Add Email Address**.

Step 6 In the From Email Address box, enter the email address that you want displayed to recipients. That is, while the email is generated by the gateway, the From Email Address is the one recipients will see and, should they respond to the email, the address to which responses are sent.

Step 7 In the Email To Addresses box, enter the address(es) to which you want the alarm email sent. To add multiple addresses, separate the addresses with semicolons and no spaces.

Step 8 Click **OK**. The address(es) are added to the first row of the Email Addresses group at the bottom

Step 9 To configure the alarms and events you want sent to the addresses, in the address row click the **Set Filter** tool.

Step 10 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, 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.
- Tenants—If tenants are created, they appear under Tenants and can be selected.
- Groups—If report groups are created, they appear under Groups and can be selected. For information, see Creating a Report Group, page 7-54. (If no groups are available, this item is not displayed.)

Step 11 Click **OK**.

Step 12 On the Alarms/Events Editor toolbar, click **Save Configuration**.

Step 13 You can perform the following actions at any future point:

- Repeat Steps 5 through 12 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-84).
- Enable trap forwarding using the ppm traprelay command (see ppm traprelay, page B-109).

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 Event Engine Parameters, edit the following:

- 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 Alarms—Indicate whether 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 10-15 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.

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

Creating an Advanced Message Queuing Protocol Connection

Advanced Message Queuing Protocol (AMQP) is added to Prime Performance Manager alarms and events.

To add an AMQP connection:

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

Step 2 On the Administration Alarms/Events Editor toolbar, click **Add AMQP Connection**.

Step 3 Enter the AMQP server and queue details:

- Description
- Host
- Port
- Virtual Host
- Exchange
- Exchange Type
- Queue
- Routing Key
- Username
- Password
- Message Type

For information about AMQP parameters, see the AMQP user documentation, which can be found at: http://www.amqp.org.

Step 4 Click **OK**.

A row representing the AMQP connection is added to the AMQP Connections table of the Alarms/Events Configuration window. Use the table to see the status of the connection, either Active or Down. You can edit the connection details, or delete the connection at any time.

If the AMQP connection message type is Alarm, a row representing the AMQP connection is also added to the Upstream OSS Hosts table of the Alarms/Events Configuration window. Use this table to filter and resend alarms.

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 10-4 describes the CISCO-PRIME notification attributes.

Table 10-4 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	1.3.6.1.4.1.9.9.311.1.1.2.1.6	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.

Table 10-4 CISCO-PRIME Notification Attributes (continued)

Attribute Name	OID	Value
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.
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 • 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.

Table 10-4 CISCO-PRIME Notification Attributes (continued)

Attribute Name	OID	Value
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. Contains additional key/value pairs described in cenEventIDList.
cenUserMessage2	1.3.6.1.4.1.9.9.311.1.1.2.1.22	User input message. Value is “PPM”.
cenUserMessage3	1.3.6.1.4.1.9.9.311.1.1.2.1.23	User input message. **Note** The custom event message text is found in this varbind.
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.

The following shows the CISCO-PRIME trap when tenants are defined. The tenant information is provided in the cenUserMessage1 varbind. The tenant information is also visible as part of the device FQDN in the cenAlarmManagedObjectClass and cenAlarmDescription varbinds. This tenant information is only present when the tenant feature is enabled and the TCA is defined for the tenant.

```
[ Tue Sep 02 14:39:42 EDT 2014]  TrapPDU [version = 2C community = public enterpriseOid =
.1.3.6.1.4.1.9.9.311.0.2 enterpriseName = ciscoEpmNotificationRev1 agentIpAddr =
10.81.82.99 genericId = 6 specificId = 2 sysUpTime = 4 days 23:22:42
```

```
OID: cenAlarmVersion              VALUE: 3
OID: cenAlarmTimestamp            VALUE: 0:0:0
OID: cenAlarmUpdatedTimestamp     VALUE: 0:0:0
OID: cenAlarmInstanceId           VALUE: 94760001
OID: cenAlarmStatus               VALUE: 0
OID: cenAlarmStatusDefinition     VALUE: ThresholdCrossing
OID: cenAlarmType                 VALUE: 1
OID: cenAlarmCategory             VALUE: 2
OID: cenAlarmCategoryDefinition   VALUE: 2,TCA
OID: cenAlarmServerAddressType    VALUE: 1
OID: cenAlarmServerAddress        VALUE: 10.81.82.99
OID: cenAlarmManagedObjectClass   VALUE:
Tenant=153ffb475fa0405bb94fc52696aa32c9,Node=172.18.116.190,UUID=9ef4f7a3-965d-4b0d-99c2-8
75e00ad02ca,name=instance-00000037
OID: cenAlarmManagedObjectAddressType VALUE: 1
OID: cenAlarmManagedObjectAddress VALUE: 172.18.116.190
OID: cenAlarmDescription          VALUE: Threshold : 'CPU_UTIL_1' -
'Tenant=153ffb475fa0405bb94fc52696aa32c9,Node=172.18.116.190,UUID=9ef4f7a3-965d-4b0d-99c2-
875e00ad02ca,name=instance-00000037' crossed threshold for 'Nova VM CPU Utilization 5
Minute/CPU Utilization' - value '7' threshold '2'. Severity: Critical
OID: cenAlarmSeverity             VALUE: 6
OID: cenAlarmSeverityDefinition   VALUE: 6,Critical
OID: cenAlarmTriageValue          VALUE: 0
OID: cenEventIdList               VALUE:
AlarmType=Communications;ProbableCause=ThresholdCrossed;NodeCreateTime=2014-08-28,15:51:56
.891,-0400;NodeChangeTime=2014-08-28,15:51:56.891,-0400;NodeClearTime=;NodeAckTime=;VNENam
e=;
OID: cenUserMessage1              VALUE:
Owner=;TCAName=CPU_UTIL_1;Tenant=153ffb475fa0405bb94fc52696aa32c9;
OID: cenUserMessage2              VALUE: PPM
OID: cenUserMessage3              VALUE: Threshold : 'CPU_UTIL_1' -
'Tenant=153ffb475fa0405bb94fc52696aa32c9,Node=172.18.116.190,UUID=9ef4f7a3-965d-4b0d-99c2-
875e00ad02ca,name=instance-00000037' crossed threshold for 'Nova VM CPU Utilization 5
Minute/CPU Utilization' - value '7' threshold '2'. Severity: Critical
OID: cenAlarmMode                 VALUE: 2
OID: cenPartitionNumber           VALUE: 0
OID: cenPartitionName             VALUE:
OID: cenCustomerIdentification    VALUE:
OID: cenCustomerRevision          VALUE: 2014-08-28,15:51:56.891,-0400
OID: cenAlertID                   VALUE: 2014-08-28,15:51:56.891,-0400
```

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 10-5 describes the CISCO-EPM-2 notification attributes.

Table 10-5 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	1.3.6.1.4.1.9.9.311.1.1.2.1.6	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
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.

Table 10-5 CISCO-EPM-2 Notification Attributes (continued)

Attribute Name	OID	Value
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.
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=2010-06-17,23:31:41.617,-2202 NodeClearTime=2010-06-17,23:31:41.616,-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.

Table 10-5 CISCO-EPM-2 Notification Attributes (continued)

Attribute Name	OID	Value
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.
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"