Monitoring Alarms

An alarm is a Cisco Prime Infrastructure response to one or more related events. If an event is considered of high enough severity (critical, major, minor, or warning), Prime Infrastructure raises an alarm until the condition no longer occurs.

- What Is an Event?
- What Is an Alarm?
- Defining Alarm Thresholds
- Where to Find Alarms
- Display Options
- Changing Alarm Status
- Changing Alarm and Event Options
- Configuring Alarm Severity Levels
- Customizing Alarms and Events For Traps
- Getting Help for Alarms
- Where to Find Syslogs

What Is an Event?

An event is an occurrence or detection of some condition in or around the network. An event is a distinct incident that occurs at a specific point in time. Examples of events include:

- Port status change
- Device reset
- Device becomes unreachable by the management station

An event can also result from:

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

One or more events may generate an abnormal state or alarm. The alarm can be cleared, but the event remains. You can view the list of events using the Event Browser.
What Is an Alarm?

An alarm is a Prime Infrastructure response to one or more related events. If an event is considered of high enough severity (critical, major, minor, or warning), Prime Infrastructure raises an alarm until the resulting condition no longer occurs.

Recurring Alarms and Events

To reduce the amount of unnecessary alarms and events, Prime Infrastructure detects the underlying causes of an event, and then modifies when it issues alarms and events if the devices have any of the problems. For example, for module or link faults, if a module is down, Prime Infrastructure creates one Module Down alarm only, and associates all of the interfaces’ link down events to the Module Down alarm. When the module state is restored, Prime Infrastructure clears the module alarm and all interface messages are associated to the cleared alarm.

When several link-up and link-down traps are received for the same interface, within a short time period, then Prime Infrastructure detects those traps and creates a Flapping event.
One or more events can result in a single alarm being raised. An alarm is created in the following sequence:

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

An alarm is associated with two types of events:

- **Active Events**: Events that have not been cleared. An alarm remains in this state until the fault is resolved in a network.
- **Historical Events**: Events that have been cleared. An event state changes to a historical event when the fault is resolved in a network.

A cleared alarm represents the end of an alarm’s lifecycle. A cleared alarm can be revived if the same fault recurs within a preset period of time. The default is 5 minutes.

**Event and Alarm Association**

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

When a notification is received:

1. Prime Infrastructure compares an incoming notification against the event and alarm catalog.
2. Prime Infrastructure decides whether to raise an event.
3. If an event is raised, Prime Infrastructure decides if the event triggers a new alarm or if it is associated with an existing alarm.

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

**Alarm Status**

Table 11-1 provides alarm status descriptions.

<table>
<thead>
<tr>
<th>Alarm Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not acknowledged</td>
<td>When an event triggers a new alarm or a new event is associated with an existing alarm.</td>
</tr>
<tr>
<td>Acknowledged</td>
<td>When you acknowledge an alarm, the status changes from Not acknowledged to Acknowledged.</td>
</tr>
<tr>
<td>Cleared</td>
<td>A cleared alarm can involve any of the following:</td>
</tr>
<tr>
<td></td>
<td>• Auto-clear from the device—The fault is resolved on the device and an event is triggered for the device. For example, a device-reachable event clears a device-unreachable event. This, in turn, clears the device-unreachable alarm.</td>
</tr>
<tr>
<td></td>
<td>• Manual-clear from Prime Infrastructure users—You can manually clear an active alarm without resolving the fault in the network. A clearing event is triggered and the alarm is cleared.</td>
</tr>
<tr>
<td></td>
<td>• If a fault continues to exist in the network, a new event and alarm are created subsequently, based on event notification (traps/syslogs).</td>
</tr>
</tbody>
</table>
Event and Alarm Severity

Each event has an assigned severity. Events fall broadly into the following severity categories, each with an associated color in Prime Infrastructure:

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

For example, a Link Down event might be assigned Critical severity, while its corresponding Link Up event will be Cleared severity.

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

Defining Alarm Thresholds

Use monitoring templates to define thresholds. When the thresholds that you specify are reached, Prime Infrastructure issues an alarm. See Creating Monitoring Policies and Thresholds for information about defining thresholds.

Where to Find Alarms

Table 11-2 lists where you can find alarms.

<table>
<thead>
<tr>
<th>Location in GUI</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor &gt; Monitoring Tools &gt; Alarms &amp; Events</td>
<td>Displays a new page listing all alarms with details such as severity, status, failure source, time stamp, owner, category, and condition. You can change the status of alarms and assign, annotate, delete, specify email notifications from this page and use the troubleshoot functionality to devices from Prime Infrastructure. If you enable Alarm Badging, Prime Infrastructure displays severity icons next to the device groups. See Displaying Alarm Icons.</td>
</tr>
<tr>
<td>Toolbar on top right of the Prime Infrastructure window</td>
<td>The red box on the top right of the Prime Infrastructure window displays the total number of critical alarms currently detected by Prime Infrastructure. You can click on the box to open the Alarm Summary. See Customizing the Alarm Summary.</td>
</tr>
<tr>
<td>From device 360° view</td>
<td>On the Alarms tab, when you hover the mouse over the Failure Source field, the crosshair icon appears. Click the icon to see the 360° view of the device. Or, on the Alarm browser, when you hover the mouse over the Failure Source field, the crosshair icon appears. Click the icon to see the 360° view of the device.</td>
</tr>
<tr>
<td>Dashboard &gt; Overview &gt; Incidents</td>
<td>Displays dashlets that contain alarm summary information, top n sites with the most alarms, top n alarm types, device reachability status, syslog watch, and syslog summary.</td>
</tr>
<tr>
<td>Dashboard &gt; Network Summary &gt; Incidents</td>
<td>Displays dashlets that contain Alarms, Top N Alarm Types, Syslog Summary and Top N Event Types.</td>
</tr>
<tr>
<td>Dashboard &gt; Data Center &gt; Compute</td>
<td>Displays Compute Resources Summary dashlet which shows alarms associated with each Compute Resource.</td>
</tr>
</tbody>
</table>
Display Options

The following sections explain the various ways you can modify how alarms, events, and syslogs are displayed:

- Viewing Options for Alarms, Events, and Syslogs
- Displaying Alarm Icons
- Changing Alarm Display Behavior

Viewing Options for Alarms, Events, and Syslogs

When you choose Monitor > Monitoring Tools > Alarms & Events, then click any of the tabs at the top of the page (Alarms, Events, or Syslogs), you can click on either of the following viewing modes:

- **Show Latest 4000 Alarms**—Prime Infrastructure displays the most recent alarms, events, or syslogs (depending on which tab you clicked), based on the timestamp when it was last modified. The Most Recent cache supports till 4000 alarms that can be displayed in the Show Latest 4000 Alarms. If a newer alarm, event, or syslog occurs, Prime Infrastructure removes an older item from the list and adds the most recent one.

- **Show All**—Prime Infrastructure retrieves all alarms, events, or syslogs from the database and displays them.

You can use filters on either view.

By default, Prime Infrastructure deletes alarms older than 30 days and deletes events older than 7 days. Prime Infrastructure stores up to a maximum of 8,000,000 events. There is no limit on the number of alarms that Prime Infrastructure stores. You can change the number of days that events are stored by choosing Administration > Settings > System Settings > Alarms and Events.

Table 11-2 Where to Find Alarms (continued)

<table>
<thead>
<tr>
<th>Location in GUI</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory &gt; Device Management &gt; Compute Devices &gt; Compute Resources &gt; Clusters &gt; Cluster Detail Page</td>
<td>Displays Severity, Status, Timestamp and Description of the Alarms in the Alarms area.</td>
</tr>
<tr>
<td>Inventory &gt; Device Management &gt; Compute Devices &gt; Compute Resources &gt; Host &gt; Host Details Page</td>
<td>Displays Severity, Status, Timestamp and Description of the Alarms in the Alarms area.</td>
</tr>
<tr>
<td>Inventory &gt; Device Management &gt; Compute Devices &gt; Compute Resources &gt; Virtual Machines &gt; Virtual Machine Details Page</td>
<td>Displays Severity, Status, Timestamp and Description of the Alarms in the Alarms area.</td>
</tr>
</tbody>
</table>
Prime Infrastructure displays a maximum of 200,000 rows of events, alarms, and syslogs for any particular active filter. If there are more than 200,000 rows of data on the Alarms, Events, or Syslog page, the global toolbar displays 200000 of N where N is the total number of rows in the table. If you hover your cursor over 200000 of N, a message appears saying that “Only the first 200,000 rows are displayed. Use the table filter controls to display a smaller result set.” To see all records, use the time and date filters to view all records day-by-day.

Displaying Alarm Icons

To have Prime Infrastructure display alarm severity icons next to the device groups on the Monitor > Monitoring Tools > Alarms & Events page, you need to enable Alarm Badging. This feature is disabled by default because it could impact performance if Prime Infrastructure is monitoring more than 2,000 devices with more than 10,000 active alarms. If you notice performance degradation issues, we suggest you disable this feature.

Step 1  Click your login name at the top-right of the screen and choose My Preferences.
Step 2  Click the checkbox next to Enable Alarm Badging on Alarms & Events page.
Step 3  Click Save.

Changing Alarm Display Behavior

Prime Infrastructure provides user preference settings that let you control whether:

- Automatically refreshes the Alarms and Events page.
- Prime Infrastructure displays prompts and warning messages when you acknowledge an alarm or clear all alarms of a condition.
- Cleared alarm conditions are always set to the “Information” severity level.

Step 1  Click the Settings icon and choose My Preferences.
Step 2  If you want Alarms/Events/Syslog page to automatically refresh at a periodic interval, select the Automatically refresh Alarms & Events page.
Step 3  If you do not want the warning message to appear whenever you acknowledge an alarm, select the Disable Alarm Acknowledge Warning Message check box. Note that the warning message displays as a reminder that a recurrence of the problem does not generate another alarm unless this functionality is disabled.
Step 4  If you do not want to be prompted to confirm each time you clear an alarm condition, select the Disable confirmation prompt for “Clear all of this condition” check box. Note that the warning displays as a reminder that you are clearing all occurrences of the specified condition.
Step 5  If you do not want to be prompted to confirm the severity change each time you clear an alarm condition, select the Disable “Set severity to Information?” prompt for “Clear all of this condition” check box.
Step 6  Click Save.
Customizing the Alarm Summary

Prime Infrastructure provides user settings that control the information shown in the Alarm Summary box (shown in the top right of the Toolbar at the top on the Prime Infrastructure window) and in the Alarm Summary pop-up page displayed when you click on the Alarm Summary box. These include:

- How often the alarm count is refreshed in the Alarm Summary box and page.
- Which category of alarm to track as the default alarm category shown in the Alarm Summary box.
- Which categories of alarms to include in the Alarm Summary page, and in the total displayed in the Alarm Summary box.

**Step 1**
Click the **Settings** icon and choose **My Preferences**.
You can also access the User Preferences page by clicking the arrow next to your login name in the Global Toolbar at the top right.

**Step 2**
To change the Alarm Summary refresh frequency: In the **Refresh Alarm count in the Alarm Summary every** drop down list, choose a refresh frequency (every 1 minute, 2 minutes, or 5 minutes).

**Step 3**
To select the alarm categories to display in the Alarm Summary box and pop-up page:

a. Click **Edit Alarm Categories**. The Select Alarm Categories pop-up displays.

b. In the **Default Category to display** drop-down, choose the default category whose total alarm count you want to display in the Alarm Summary box. For example: Choose “AP Rogue” to have the Alarm Summary box display the count for AP Rogue alarms only. Choose “Alarm Summary” to have the box display a count of all alarms in all selected categories and subcategories.

c. In the pick list under the **Show** drop-down, choose the checkbox next to each category or sub-category of alarm that you want to include in the Alarm Summary popup page.

**If Default Category to display** is set to “Alarm Summary”, the alarm totals shown will be the total of all critical alarms for all the categories and sub-categories you select in the pick list. If any other category or sub-category is selected as the Default Category, the box displays totals only for that category.

d. When you are finished, click **OK**. Your selected alarm category and subcategories are listed on the User Preferences page.

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

**Related Topics**
- Changing Alarm Display Behavior
- Toolbar
Changing Alarm Status

You can remove an alarm from the list of alarms by changing its status to Acknowledged or Cleared. No e-mails will be generated for these alarms.

---

**Step 1**
Choose **Monitor > Monitoring Tools > Alarms & Events**. By default, the Alarms tab is selected.

**Step 2**
Select an alarm, then choose one of the following options under **Change Status**:

- **Acknowledge**—Removes the alarm from the Alarms list and prevents the alarm from being counted as an active alarm on the Alarm Summary page or any alarms list.
- **Unacknowledge**—Returns the alarm to its active alarm state on the Alarm Summary page and all alarms lists.
- **Clear**—Sets the alarm state to Cleared. Cleared alarms remain in the Prime Infrastructure database, but in the Clear state. You clear an alarm when the condition that caused it no longer exists.
- **Clear all of this Condition**—Sets the alarm state to Cleared for all alarms with the same Condition as the alarm you selected.

After you click **Yes** to confirm that you want to clear all alarms of the specified condition, a dialog appears asking if you want to change the severity for the selected alarm condition to Informational. This prevents Prime Infrastructure from issuing alarms for the specified condition. To later reset the condition’s severity, choose **Administration > Settings > System Settings > Alarms and Events > Alarm Severity and Auto Clear > Severity Configuration** and modify the severity.

---

**Related Topics**
- Configuring Alarm Severity Levels
- When to Acknowledge Alarms
- Including Acknowledged and Cleared Alarms in Searches

---

**When to Acknowledge Alarms**

You may want certain alarms to be removed from the Alarms list. For example, if you are continuously receiving an interference alarm from a certain device, you may want to stop that alarm from being counted as an active alarm on the Alarm Summary page or any alarms list. In this scenario, you can find the alarm for the device in the Alarms list, select an alarm and choose **Change Status > Acknowledge**.

If the device generates a new violation on the same interface, Prime Infrastructure does not create a new alarm, and the Alarm Summary page shows no new alarms. However, if the interference violation is created on another interface, a new alarm is created.

By default, acknowledged alarms are not displayed on either the Alarm Summary page or in any alarm list. Also, no emails are generated for acknowledged alarms. By default, acknowledged alarms are not included for any search criteria. To change this default, go to the **Administration > Settings > System Settings > Alarms and Events** page and disable the **Hide Acknowledged Alarms** preference.

When you acknowledge an alarm, a warning message appears as a reminder that a recurrence of the problem does not generate another alarm unless this functionality is disabled. Click the **Settings** icon and choose **My Preferences** page to disable this warning message.
You can also search for all previously acknowledged alarms to reveal the alarms that were acknowledged during the last seven days. Prime Infrastructure automatically deletes cleared alerts that are more than seven days old, so your results can show activity for only the last seven days. Until an existing alarm is deleted, a new alarm cannot be generated for any managed entity for which Prime Infrastructure has already generated an alarm.

Including Acknowledged and Cleared Alarms in Searches

By default, acknowledged and cleared alarms are not included for any search criteria. To change this default, choose Administration > Settings > System Settings > Alarms and Events and disable the Hide Acknowledged Alarms or Hide Cleared Alarms preference.

Cleared alarms remain in the Prime Infrastructure database, but in the Clear state. You clear an alarm when the condition that caused it no longer exists.

Changing Alarm and Event Options

You might want to change the schedule for deleting alarms, the alarm severities that are displayed, or alarm email options.

To change alarm and event options, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose Administration &gt; Settings &gt; System Settings.</td>
</tr>
<tr>
<td>2</td>
<td>From the left sidebar menu, choose Alarms and Events.</td>
</tr>
<tr>
<td>3</td>
<td>Change the alarm or event settings, then click Save.</td>
</tr>
</tbody>
</table>

Configuring Alarm Severity Levels

A newly generated alarm has a default severity level that you might want to change.

To configure an alarm’s severity level, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose Administration &gt; Settings &gt; System Settings &gt; Alarms and Events &gt; Alarm Severity and Auto Clear.</td>
</tr>
<tr>
<td>2</td>
<td>Choose Severity Configuration.</td>
</tr>
<tr>
<td>3</td>
<td>Select the check box of the alarm condition whose severity level that you want to change.</td>
</tr>
<tr>
<td>4</td>
<td>From the Configure Severity Level drop-down list, choose a severity level.</td>
</tr>
<tr>
<td>5</td>
<td>Click OK to confirm the changes.</td>
</tr>
</tbody>
</table>
Customizing Alarms and Events For Traps

You can enable Prime Infrastructure to recognize additional traps and to customize how Prime Infrastructure creates events and alarms for these traps. You can specify a trap notification name or syslog message identifier, and specify the event severity, category, and message to use when the specified trap is received. Prime Infrastructure creates an event with the settings you specify.

Step 1  Choose Monitor > Monitoring Tools > Alarms & Events.

Step 2  Click the Events tab.

Step 3  Click Custom Trap Event. The Custom Trap Events window opens displaying any previously created custom trap events.

Step 4  Click Add.

Step 5  Select a MIB from the menu, which includes all MIBs that are not fully supported, or click Upload New MIB to upload a MIB file.

If you upload a new MIB file, wait approximately 15 seconds, then click Refresh MIBs to have the newly added MIB added to the MIB drop-down list.

Step 6  Select a Notification Name from the list of unsupported notification names included in the selected MIB.

Step 7  In the Event Description field, enter the text you want displayed in the Description column for the events that are generated from traps with the selected notification name.

Step 8  Select a Default Severity level, then click OK.

Prime Infrastructure creates a new event type and alarm condition for the specified trap.

Related Topic
•  Modifying a Customized Trap Event

Modifying a Customized Trap Event

You can modify a previously created customized trap event.

Step 1  Choose Monitor > Monitoring Tools > Alarms & Events.

Step 2  Click the Events tab.

Step 3  Click Custom Trap Event. The Custom Trap Events window opens displaying any previously created custom trap events.

Step 4  Select the custom trap event you want to modify, then click Edit.

Step 5  Modify the necessary fields, then click OK.

Related Topic
•  Customizing Alarms and Events For Traps
Getting Help for Alarms

If you receive an alarm in Monitor > Monitoring Tools > Alarms & Events for which you cannot find a resolution in the Cisco Support Community (select an alarm, then choose Troubleshoot > Support Forum.), you can use Prime Infrastructure to open a support request (click an alarm, then choose Troubleshoot > Support Case). See “Troubleshooting Prime Infrastructure” in the Cisco Prime Infrastructure 3.0 Administrator Guide for more information.

Where to Find Syslogs

Prime Infrastructure logs all syslogs from severity 0 through 7 (emergency through debugging messages) generated by all devices that are managed by Prime Infrastructure. Prime Infrastructure also logs all SNMP messages.

Prime Infrastructure logs and displays syslogs from managed devices only. Syslogs from devices that are not managed by Prime Infrastructure are not logged or displayed.

To view syslogs, choose Monitor > Monitoring Tools > Alarms & Events, then click the Syslogs tab. You can use the predefined filters provided by Prime Infrastructure, or use the Quick or Advanced Filters to search on your own criteria.

Prime Infrastructure stores a maximum of 2,000,000 syslogs. You can view up to 50 syslogs per UI page, up to a maximum of 200,000 total syslogs.

Supported Syslog Formats for Event Based Inventory

The following are the supported Syslog formats. Prime Infrastructure will trigger the inventory collection if the device syslog matches any one of the following conditions:

- Message Type is any one of the following:
  - LINK-3-UPDOWN
  - PORT_SECURITY-6-VLAN_REMOVED
  - PORT_SECURITY-6-VLAN_FULL
  - G8032-STATE_IDLE
  - G8032-STATE_PENDING
  - G8032-STATE_PROTECTION
  - G8032-STATE_FORCED_SWITCH
  - G8032-STATE_MANUAL_SWITCH
  - L2-G8032-3-APS_CHANNEL_INACTIVE
  - L2-G8032-6-APS_CHANNEL_ACTIVE
  - L2-L2VPN_ICCP_SM-4-REMOTE_CORE_ISOLATION
  - L2-L2VPN_ICCP_SM-4-REMOTE_CORE_ISOLATION_CLEAR
  - L2-L2VPN_ICCP_SM-3-CONFIG_LOCAL_ERROR
  - L2-L2VPN_ICCP_SM-3-CONFIG_REMOTE_ERROR
  - L2-L2VPN_ICCP_SM-4-LOCAL_CORE_ISOLATION
L2-L2VPN_ICCP_SM-4-LOCAL_CORE_ISOLATION_CLEAR
L2-L2VPN_ICCP_SM-4-PEER_REACHABILITY_FAILURE
L2-L2VPN_ICCP_SM-4-PEER_REACHABILITY_CLEAR
L2-L2VPN_ICCP_SM-4-REMOTE_ACCESS_MAIN_PORT_FAILURE
L2-L2VPN_ICCP_SM-4-REMOTE_ACCESS_MAIN_PORT_FAILURE_CLEAR
INFRA-ICCP-5-ISOLATION
INFRA-ICCP-5-ISOLATION_CLR
INFRA-ICCP-5-NEIGHBOR_STATE_UP
INFRA-ICCP-5-NEIGHBOR_STATE_DOWN
INFRA-ICCP-6-BACKBONE_INTERFACE_STATE_UP
INFRA-ICCP-6-BACKBONE_INTERFACE_STATE_DOWN
L2-BM-6-ACTIVE_CLEAR
L2-BM-6-ACTIVE_PROBLEM
L2-L2VPN_ICCP_SM-3-CONFIG_INVALID_NODEID
L2-L2VPN_ICCP_SM-3-CONFIG_INVALID_NODEID_CLEAR
PKT_INFRA-ICPE_GCO-5-SATELLITE_STATUS_PROBLEM
PKT_INFRA-ICPE_GCO-5-SATELLITE_STATUS_CLEAR
PLATFORM-REDDRVR-7-ROLE_CHANGE
PLATFORM-CE_SWITCH-6-UPDN
PLATFORM-CLUSTER_CLM-6-UPDN
E_CFM-6-LCK
E_CFM-6-AIS
E_CFM-6-AIS_INT
E_CFM-6-LCK_INT
LINK_UP
LINK_DOWN
cefcPowerStatusChange
cefcFRURemoved
cefcFRUInserted
SYS-5-RELOAD
SYS-5-RESTART
OIR-6-INSCARD
OIR-SP-6-INSCARD
SWT_CEFC_STATUS_CHANGE
Customizing Alarms and Events For Syslogs

You can enable Prime Infrastructure to create events for particular syslogs. You can specify a syslog message identifier, and specify the event severity and message to use when the specified syslog is received. Prime Infrastructure creates an event with the settings you specify.

Step 1  Choose Monitor > Monitoring Tools > Alarms & Events.
Step 2  Click the Syslogs tab.
Step 3  If there is an existing syslog for which you want to create an event, select the syslog, then click Custom Syslog Events. To create a new event for which there is not an existing syslog, click Custom Syslog Events.
Step 4  Click Add. Complete the required fields. If you selected a syslog in Step 3, the Message Type and Event Message fields are prepopulated with the values of the syslog you selected.
Step 5  Select a Default Severity level, then click OK. The Default Severity field controls the severity of the event that is created from the syslog. The syslog itself is not modified in any way.

Modifying a Customized Syslog Event

You can modify a previously created customized syslog event.

Step 1  Choose Monitor > Monitoring Tools > Alarms & Events.
Step 2  Click the Syslogs tab.
Step 3  Click Custom Syslog Events. The Custom Syslog Events window opens displaying any previously created event mappings.
Step 4  Select the custom syslog event you want to modify, then click Edit.
Step 5  Modify the necessary fields, then click OK.

Related Topic
• Customizing Alarms and Events For Syslogs
Customizing Alarms and Events For Syslogs