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?

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.

Choose **Operate > Alarms & Events**, then click **Events** to access the Events Browser page.

Event Creation

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

Prime Infrastructure discovers events in the following ways:

- By receiving notification events and analyzing them; for example, syslog and traps.
- By automatically polling devices and discovering changes; for example, device unreachable.
- By receiving events when a significant change occurs on the Prime Infrastructure server; for example, rebooting the server.
- By receiving events when the status of an alarm is changed; for example when the user acknowledges or clears an alarm.

Incoming event notifications (traps and syslogs) are identified by matching the event data to predefined patterns. A trap or syslog is considered supported by Prime Infrastructure if it has matching patterns and can be properly identified. If the event data does not match predefined patterns, the event is considered unsupported, and it is dropped.

Faults are discovered by Prime Infrastructure through polling, traps, or syslog messages. Prime Infrastructure maintains the context of all faults and ensures that duplicate events or alarms are not maintained in the Prime Infrastructure database.

The following table provides examples of when Prime Infrastructure creates an event.

Time	Event	Prime Infrastructure Behavior
10:00AM PDT December 1, 2011	Device A becomes unreachable.	Creates a new unreachable event on device A.
10:30AM PDT December 1, 2011	Device A continues to be unreachable.	No change in the event status.
10:45AM PDT December 1, 2011	Device A becomes reachable.	Creates a new reachable event on device A.
11:00AM PDT December 1, 2011	Device A stays reachable.	No change in the event status.
12:00AM PDT December 1, 2011	Device A becomes unreachable.	Creates a new unreachable event on device A.

Recurring Alarms and Events

To reduce the amount of unnecessary alarms and events, Prime Infrastructure detects underlying causes for events and modifies when it issues alarms and events when devices have any of the following problems:

- Repeated restart—When a device repeatedly restarts and is continuously cycling (because, for example, there is a problem with the device or its software), Prime Infrastructure generates a *Repeated Restart* event if the same device sends a cold start or warm start trap a repeatedly within a short time period.
- Flapping—Prime Infrastructure detects when several link up and link down traps are received for the same interface within a short time period and creates a *Flapping* event.
- Module or Link Fault—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.

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.

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. For example, for an active interface error alarm, if multiple interface error events occur on the same interface, are all associated with the same alarm.

Alarm Status

Table 11-1 provides alarm status descriptions.

Table 11-1 Alarm Status Descriptions

Alarm Status	Description
New	When an event triggers a new alarm or a new event is associated with an existing alarm.

Table 11-1 Alarm Status Descriptions

Alarm Status	Description
Acknowledged	When you acknowledge an alarm, the status changes from New to Acknowledged.
Cleared	A cleared alarm can involve any of the following: • 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. • 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. • If a fault continues to exist in the network, a new event and alarm are created subsequently, based on event notification (traps/syslogs).

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 Informational severity.

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

Where to Find Alarms

Table 11-2 lists where you can find alarms.

Table 11-2 Where to Find Alarms

Location in GUI	Description
Operate > Alarms & Events	Displays a new page listing all alarms with details such as severity, status, source, and time stamp. You can change the status of alarms, and assign, annotate, delete, and specify email notifications from this page.
Hover your mouse cursor on **Alarm Summary**	Displays a table listing the critical, major, and minor alarms currently detected by Prime Infrastructure.
Alarm Browser	Opens a window that displays the same information as in the **Operate > Alarms & Events** but does not take you to a new page.
From device 360° view	Click the **Alarms** tab to view alarms on the device and their status and category, or click the **Alarm Browser** icon to launch the Alarm Browser.
Operate > Monitoring Dashboard > Incidents	Displays dashlets that contain alarm summary information, top sites with the most alarms, top alarm types, top events, and top interfaces with issues.

Where to Find Syslogs

Prime Infrastructure logs all emergency, alert, and critical messages generated by all devices that are managed by Prime Infrastructure.

Prime Infrastructure also logs all SNMP messages and syslogs it receives. To view syslogs, choose **Operate > Alarms & Events**, then click the **Syslogs** tab.

Syslog Pre-defined Filters

Prime Infrastructure uses the following syslog filters:

- Severity 0 and 1
- Severity 2
- Environmental Monitor
- Memory Allocation Failure
- Catalyst Integrated Security Features
- Cisco IOS Firewall Denial of Service

Defining Alarm Thresholds

Use monitoring templates to define thresholds. When the thresholds that you specify are reached, Prime Infrastructure issues an alarm.

Step 1 Choose **Design > Configuration > Monitor Configuration**.

Step 2 Expand the Features menu on the left and choose **Threshold**.

Step 3 Complete the basic template fields. For descriptions of the template parameters, see the *Cisco Prime Infrastructure 2.0 Reference Guide*.

Step 4 Under the Feature Category, choose one of the following metrics:

- Device Health—Change threshold values for CPU utilization, memory pool utilization, and environment temperature.
- Interface Health—Change threshold values for the number of outbound packets that are discarded.

Step 5 Under Metric Parameters, choose the threshold setting that you want to change, then click **Edit Threshold Setting**.

Note If you configure multiple threshold settings or parameters, Prime Infrastructure raises an alarm when *any* of the thresholds are reached.

Step 6 Enter a new value, choose the alarm severity to assign when the threshold is met or exceeded, and click **Done**.

Step 7 Click **Save as New Template**.

Step 8 You can now deploy the template (see Deploying Monitor Configuration Templates, page 8-17).

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 **Operate > Alarms & Events**.

Step 2 Select an alarm, then choose **Change Status > Acknowledge** or **Clear**.

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 device 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 > System Settings > Alarms and Events** page and disable the **Hide Acknowledged Alarms** preference.

Note 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. Use the **Administration > User 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 > 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:

Step 1 Choose **Administration > System Settings**.

Step 2 From the left sidebar menu, choose **Alarms and Events**.

Step 3 Change the alarm or event settings, then click **Save**.

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:

Step 1 Choose **Administration > System Settings**.

Step 2 From the left sidebar menu, choose **Severity Configuration**.

Step 3 Check the check box of the alarm condition whose severity level you want to change.

Step 4 From the Configure Security Level drop-down list, choose a severity level, then click **Go**.

Step 5 Click **OK** to confirm the changes.

Getting Help for Alarms

If you receive an alarm in **Operate > Alarms & Events** for which you cannot find a resolution in the Cisco Support Community (click on an alarm, then choose **Troubleshoot > Support Forum**.), you can use Prime Infrastructure to open a support request (click on an alarm, then choose **Troubleshoot > Support Case**). See "Troubleshooting Prime Infrastructure" in the *Cisco Prime Infrastructure 2.0 Administrator Guide* for more information.