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
- What is an Alarm Policy?
- Getting Help for Alarms
- Viewing 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.
Choose **Monitor > Monitoring Tools > 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.

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.

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Prime Infrastructure Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>10:00AM PDT December 1, 2014</td>
<td>Device A becomes unreachable.</td>
<td>Creates a new unreachable event on device A.</td>
</tr>
<tr>
<td>10:30AM PDT December 1, 2014</td>
<td>Device A continues to be unreachable.</td>
<td>No change in the event status.</td>
</tr>
<tr>
<td>10:45AM PDT December 1, 2014</td>
<td>Device A becomes reachable.</td>
<td>Creates a new reachable event on device A.</td>
</tr>
<tr>
<td>11:00AM PDT December 1, 2014</td>
<td>Device A stays reachable.</td>
<td>No change in the event status.</td>
</tr>
<tr>
<td>12:00AM PDT December 1, 2014</td>
<td>Device A becomes unreachable.</td>
<td>Creates a new unreachable event on device A.</td>
</tr>
</tbody>
</table>

**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.

**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.

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 12-1 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 12-2 lists where you can find alarms.

<table>
<thead>
<tr>
<th>Location in GUI</th>
<th>Description</th>
</tr>
</thead>
</table>
| Monitor > Monitoring Tools > Alarms & Events                                   | Displays a new page listing all alarms with details such as severity, status, failure source, timestamp, Device Timestamp, 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. |
| Toolbar on top right of the Prime Infrastructure window                        | 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. |
| From device 360° view                                                         | 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. |
| Dashboard > Overview > Incidents                                              | 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. |
| Dashboard > Network Summary > Incidents                                       | Displays dashlets that contain Alarms, Top N Alarm Types, Syslog Summary and Top N Event Types.                                                                                                |
| Dashboard > Data Center > Compute                                             | Displays Compute Resources Summary dashlet which shows alarms associated with each Compute Resource.                                                                                                      |
| Inventory > Device Management > Compute Devices > Compute Resources > Clusters> Cluster Detail Page | Displays Severity, Status, Timestamp and Description of the Alarms in the Alarms area.                                                                                                                    |
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
- Alarm Counts in Latest Alarms and All Alarms
- Displaying Alarm Icons
- Changing Alarm Display Behavior
- Modifying Alarm Failure Source Pattern

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.

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 $200000 \times N$ 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.

### Alarm Counts in Latest Alarms and All Alarms

The number of alarms displayed in the All Alarms view can be different from the number of alarms in the Latest 4000 Alarms view on the Monitor > Alarms and Events page.

The Latest 4000 Alarms view shows the most recently created and/or modified alarms of all severities and from all virtual domains. Depending on your user privileges and the display settings you configured, you might see fewer than 4000 alarms in this view, even if there are more than 4000 alarms, for the following reasons:

- The Latest 4000 Alarms includes cleared alarms, which are hidden unless you disable the Hide Cleared Alarms option (Administration > Settings > System Settings > Alarms and Events). Some of the latest 4000 alarms are cleared alarms, which are not displayed.
- The latest 4000 alarms might include alarms from virtual domains that are not visible to you.

You might also temporarily see more alarms in the Latest 4000 Alarms view than in the All Alarms view for the following reasons:

- When a cleared alarm becomes active, and Hide Cleared Alarms is enabled, the alarm might appear in the Latest 4000 Alarms view before it appears in the All Alarms view. This is because the alarm is still cleared (and therefore hidden) in the All Alarms view. The two views should synchronize within two minutes.
- When an alarm is created for the first time, it might appear in the Latest 4000 Alarms view before it appears in the All Alarms view. The alarm will be visible in the All Alarms view after it has been written to the database. The two views should synchronize within two minutes.
- When data pruning is running, Prime Infrastructure might remove alarms from the database (and the All Alarms view) before it updates the Latest 4000 Alarms view. This means that pruned alarms might remain visible in the Latest 4000 Alarms view for a short time. When pruning is complete, Prime Infrastructure corrects the discrepancy.
- When an alarm is updated, even if its severity has not changed, it appears in the Latest 4000 Alarms view before it appears in the All Alarms view.

### 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**
Click **Alarms & Events** tab.

**Step 3**
If you want **Alarms/Events/Syslog** page to automatically refresh at a periodic interval, select the **Automatically refresh Alarms & Events** page.

**Step 4**
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 5**
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 6**
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 7**
Click **Save**.

**Related Topics**
- Customizing the Alarm Summary
- Customizing Alarms and Events For Traps

Modifying Alarm Failure Source Pattern

- Select the category you need to customize and click **Edit**.
- Select the failure source pattern from the options available and click **OK**.
- Select the category for which you want to customize the separator and click **Edit Separator**. Select one of the options available, then click **OK**.

The alarms generated for the selected category will have the customized pattern that you set. For example, if you select the Clients category, and then edit the separator to be #, when any supported client alarm is generated, when you select **Monitor > Monitoring Tools > Alarms and Events**, the Failure Source column for that alarm will be **MACaddress#Name**.

**Note**
- Failure Source is not supported for Custom traps and Custom syslog translation.
- Failure Source is not supported for Syslog generated events.
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:

- **Step 1** Choose Administration > Settings > 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, follow these steps:

- **Step 1** Choose Administration > Settings > System Settings > Alarms and Events > Alarm Severity and Auto Clear.
- **Step 2** Choose Severity Configuration.
- **Step 3** Select the check box of the alarm condition whose severity level that you want to change.
- **Step 4** From the Configure Severity Level drop-down list, choose a severity level.
- **Step 5** Click OK to confirm the changes.

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.
What is an Alarm Policy?

An Alarm Policy is a filtering method that allows you to control the alarms on network conditions, thereby reducing noise in the system.

If you choose to suppress alarms for a group that contains a port or device, the alarm types you specified are suppressed for that port or device even if that port or device is also in another group for which alarms are marked as active.

Prime Infrastructure supports the following Alarm Policies:

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
What is an Alarm Policy?

- **Interface Alarm Policy**—Allows you to activate or suppress the interface alarms on interface-related events, device groups, and port groups.
- **Controller Alarm Policy**—Allows you to activate or suppress the alarms on controller-related events for the selected device groups.
- **Access Points Alarm Policy**—Allows you to activate or suppress the AP alarms on AP-related events, device groups, and alarm thresholds.
- **Layer2 Switch**—Allows you to activate and suppress alarms on Layer 2 switch-related events for the selected device groups.
- **Wired Infrastructure**—Allows you to activate and suppress alarms on Wired Infrastructure-related events for the selected device groups.

**Note**
The new alarm policies will not be applicable for the alarms already generated by Prime Infrastructure. You must delete or clear the existing alarms for the alarm policy to be effective in Prime Infrastructure.

**Related Topics**
- Customizing Interface Alarm Policy
- Customizing Controller Alarm Policy
- Customizing Access Point Alarm Policy
- Customizing Layer2 Switch Alarm Policy
- Customizing Wired Infrastructure Alarm Policy
- Viewing the Alarm Policy Summary
- Restoring Default Settings

## Customizing Interface Alarm Policy

You can activate or suppress the types of events, device groups and port groups on which you want the alarms to be generated or ignored.

To edit the Interface Alarm Policy, follow these steps:

**Step 1** Choose **Monitor > Monitoring Tools > Alarm Policies**.

**Step 2** Check the **Interface** check box and then click **Edit**.

The **Edit Interface Alarm Policy** page displays the default list of events that you want to modify.

**Step 3** Click the **Activated** or **Suppressed** toggle button to activate or suppress the alarm for the required event.

To perform a bulk edit, select the required **Events** check boxes and select **Activate** or **Suppress** from the **Activate** drop-down list.

**Step 4** Set the required severity for an alarm from the **Severity** drop-down list.

To perform a bulk edit, select the required **Events** check boxes and select a severity from the **Change Severity** drop-down list.

**Step 5** In the **Auto Clear Duration** field, enter the value in hours for the alarm to clear automatically for an event.

To perform a bulk edit, select the required **Events** check boxes and edit the **Alarm Auto Clear** field.
Alternatively, you can choose Administration > Settings > System Settings > Alarms and Events > Alarm Severity and Auto Clear to set the severity and auto clear duration for an alarm.

**Step 6**
Click **Save and Activate**, or click **Next** to continue with the **Device Groups** page.

**Step 7**
Click the **All devices are selected** or **No devices are selected** toggle button to activate or suppress the events selected in **Step 3** for the particular device groups. **Some devices are selected** is displayed only when a few devices in a device group are selected.

To perform a bulk edit, select the required device group check boxes and select **Activate** or **Suppress** from the **Activate** drop-down list.

If you choose to suppress alarms for a group that contains a port or device, the alarm types you specified are suppressed for that port or device even if that port or device is also in another group for which alarms are marked as **active**.

**Step 8**
Click **Save and Activate**, or click **Next** to continue with the **Ports Group** page.

**Step 9**
Click the **All port types are selected** or **No port types are selected** toggle button to activate or suppress the selected events. Network events on the ports belonging to the unselected groups will be suppressed. **Some port types are selected** is displayed only when a few ports in a port group are selected.

To perform a bulk edit, select the required port group check boxes and select **Activate** or **Suppress** from the **Activate** drop-down list.

**Step 10**
Click **Save and Activate**.

---

**Related Topics**
- What is an Alarm Policy?
- Customizing Controller Alarm Policy
- Customizing Access Point Alarm Policy
- Customizing Layer2 Switch Alarm Policy
- Customizing Wired Infrastructure Alarm Policy
- Viewing the Alarm Policy Summary
- Restoring Default Settings

---

**Customizing Controller Alarm Policy**

You can activate or suppress the types of events and device groups for which you want the alarms to be generated or ignored. If you choose to suppress alarms for a group that contains a port or device, the alarm types you specified are suppressed for that port or device even if that port or device is also in another group for which alarms are marked as **active**.

To edit the Controller Alarm Policy, follow these steps:

**Step 1**
Choose **Monitor > Monitoring Tools > Alarm Policies**.

**Step 2**
Check the **Controller** check box and then click **Edit**.

The **Edit Controller Alarm Policy** page displays the default list of events that you want to modify.

**Step 3**
Click the **Activated** or **Suppressed** toggle button to activate or suppress the alarm for the required event.
To perform a bulk edit, select the required **Events** check boxes and select **Activate** or **Suppress** from the **Activate** drop-down list.

**Step 4**

Set the required severity for an alarm from the **Severity** drop-down list.

To perform a bulk edit, select the required **Events** check boxes and select a severity from the **Change Severity** drop-down list.

**Step 5**

In the **Auto Clear Duration** field, enter the value in hours for the alarm to clear automatically for an event.

To perform a bulk edit, select the required **Events** check boxes and edit the **Alarm Auto Clear** field.

Alternatively, you can choose **Administration > Settings > System Settings > Alarms and Events > Alarm Severity and Auto Clear** to set the severity and auto clear duration for an alarm.

**Step 6**

Click **Save and Activate**, or click **Next** to continue with the **Device Groups** page.

**Step 7**

Click the **All devices are selected** or **No devices are selected** toggle button to activate or suppress the events selected in **Step 3** for the particular device groups. **Some devices are selected** is displayed only when a few devices in a device group are selected.

To perform a bulk edit, select the required device group check boxes and select **Activate** or **Suppress** from the **Activate** drop-down list.

If you choose to suppress alarms for a group that contains a port or device, the alarm types you specified are suppressed for that port or device even if that port or device is also in another group for which alarms are marked as **active**.

**Step 8**

Click **Save and Activate**.

---

**Related Topics**

- What is an Alarm Policy?
- Customizing Interface Alarm Policy
- Customizing Access Point Alarm Policy
- Customizing Layer2 Switch Alarm Policy
- Customizing Wired Infrastructure Alarm Policy
- Viewing the Alarm Policy Summary
- Restoring Default Settings

---

**Customizing Access Point Alarm Policy**

You can activate or suppress the types of events and device groups for which you want the alarms to be generated or ignored. Also, you can set the threshold value to control the alarms.

If you choose to suppress alarms for a group that contains a port or device, the alarm types you specified are suppressed for that port or device even if that port or device is also in another group for which alarms are marked as **active**.

To edit the Access Point Alarm Policy, follow these steps:

**Step 1**

Choose **Monitor > Monitoring Tools > Alarm Policies**.

**Step 2**

Check the **Access Point** policy name, then click the **Edit Policy** link.
The Edit Access Point Alarm Policy page displays the default list of events that you want to modify.

**Step 3**
Click the Activated or Suppressed toggle button to activate or suppress the alarm for the required event.

To perform a bulk edit, select the required Events check boxes and select Activate or Suppress from the Activate drop-down list.

**Step 4**
Set the required severity for an alarm from the Severity drop-down list.

To perform a bulk edit, select the required Events check boxes and select a severity from the Change Severity drop-down list.

**Step 5**
In the Auto Clear Duration field, enter the value in hours for the alarm to clear automatically for an event.

To perform a bulk edit, select the required Events check boxes and edit the Alarm Auto Clear field.

Alternatively, you can choose Administration > Settings > System Settings > Alarms and Events > Alarm Severity and Auto Clear to set the severity and auto clear duration for an alarm.

**Step 6**
Click Save and Activate, or click Next to continue with the Device Groups page.

**Step 7**
Click the All devices are selected or No devices are selected toggle button to activate or suppress the events selected in Step 3 for the particular device groups. Some devices are selected is displayed only when a few devices in a device group are selected.

To perform a bulk edit, select the required device group check boxes and select Activate or Suppress from the Activate drop-down list.

**Step 8**
Click Save and Activate, or click Next to continue with the Alarm Threshold page.

**Step 9**
Enter the threshold value in percentage in the AP Down Group Impact % field of the required device group to set the threshold so that alarm will be generated only when the specified percentage of APs are dissociated in the selected groups.

**Step 10**
Enter the time in minutes in the AP Down Sustain Time (Minutes) field of the required device group to set the maximum duration after which the alarm can be generated for an AP that goes down or not reachable.

**Note**
If you specify both AP Down Group Impact % and AP Down Sustain Time (Minutes) for a device group, then an alarm will be generated only when the specified percentage of APs dissociated from the controller are down for the specified duration. See Understanding Access Point Alarm Policy Thresholds.

**Step 11**
Click Save and Activate.

**Related Topics**
- Understanding Access Point Alarm Policy Thresholds
- What is an Alarm Policy?
- Customizing Interface Alarm Policy
- Customizing Controller Alarm Policy
- Customizing Layer2 Switch Alarm Policy
- Customizing Wired Infrastructure Alarm Policy
- Viewing the Alarm Policy Summary
- Restoring Default Settings
Understanding Access Point Alarm Policy Thresholds

Specifying an AP Down Group Impact percentage and/or an AP Down Sustain Time duration for a device group modifies when alarms are created as described below:

- If you select an AP Down Group Impact percentage for a device group, any AP dissociated alarms for APs in the group are suppressed.
  
  When the percentage of down APs in the group exceeds the threshold percentage, Prime Infrastructure generates an ImpactedGroup alarm. When the percentage of down APs falls below the threshold, the ImpactedGroup alarm is cleared.

- If you specify an AP Down Sustain Time duration only for a device group, when an AP dissociated alarm event occurs for an AP within the group, Prime Infrastructure creates an alarm only if the AP dissociated alarm does not clear before the sustain time has elapsed.

- If you specify both an AP Down Group Impact percentage and an AP Down Sustain Time duration:
  
  - If an AP dissociated alarm event occurs for an AP within the group, Prime Infrastructure does not generate an alarm.
  
  - If the AP dissociated alarm event does not clear before the specified time has elapsed, the group is considered as a down AP.
  
  - If the percentage of APs in the group that have AP dissociated alarms that have not cleared before the configured time exceeds the threshold percentage, Prime Infrastructure generates an ImpactedGroup alarm.
  
  - If a clearing event for one of the AP dissociated alarms occurs for one of the APs that are considered down by the Group, the ImpactedGroup alarm is cleared.

The following example explains the policy behavior when you specify an AP Down Group Impact percentage and an AP Down Sustain Time duration for a device group.

Floor1 has 3 APs—AP A, AP B, and AP C and the Alarm Thresholds have the following values:

- AP Down Group Impact %: 50%
- AP Down Sustain Time (Minutes): 5 minutes

1. AP A sends AP_DISASSOCIATED.
2. After 3 minutes, AP B sends AP_DISASSOCIATED.
3. After 5 minutes, ‘AP A’ AP_DISASSOCIATED expires.
4. After 8 minutes, ‘AP B’ AP_DISASSOCIATED expires.

Prime Infrastructure generates an Impacted Group alarm because the 50% AP Down Group Impact threshold has been crossed.

Customizing Layer2 Switch Alarm Policy

You can activate or suppress the types of events and device groups on which you want the alarms to be generated or ignored.

To edit the Layer2 Switch Alarm Policy, follow these steps:

**Step 1** Choose **Monitor > Monitoring Tools > Alarm Policies**.

**Step 2** Check the **Layer2 Switch** check box and then click **Edit**.

The **Edit Layer2 Switch Alarm Policy** page displays the default list of events that you want to modify.
Step 3  Click the **Activated** or **Suppressed** toggle button to activate or suppress the alarm for the required event. To perform a bulk edit, select the required **Events** check boxes and select **Activate** or **Suppress** from the **Activate** drop-down list.

Step 4  Set the required severity for an alarm from the **Severity** drop-down list. To perform a bulk edit, select the required **Events** check boxes and select a severity from the **Change Severity** drop-down list.

Step 5  In the **Auto Clear Duration** field, enter the value in hours for the alarm to clear automatically for an event. To perform a bulk edit, select the required **Events** check boxes and edit the **Alarm Auto Clear** field. Alternatively, you can choose **Administration > Settings > System Settings > Alarms and Events > Alarm Severity and Auto Clear** to set the severity and auto clear duration for an alarm.

Step 6  Click **Save and Activate**, or click **Next** to continue with the **Device Groups** page.

Step 7  Click the **All devices are selected** or **No devices are selected** toggle button to activate or suppress the events selected in Step 3 for the particular device groups. **Some devices are selected** is displayed only when a few devices in a device group are selected. To perform a bulk edit, select the required device group check boxes and select **Activate** or **Suppress** from the **Activate** drop-down list.

If you choose to suppress alarms for a group that contains a port or device, the alarm types you specified are suppressed for that port or device even if that port or device is also in another group for which alarms are marked as **active**.

Step 8  Click **Save and Activate**.

**Related Topics**
- What is an Alarm Policy?
- Customizing Interface Alarm Policy
- Customizing Controller Alarm Policy
- Customizing Access Point Alarm Policy
- Customizing Wired Infrastructure Alarm Policy
- Viewing the Alarm Policy Summary
- Restoring Default Settings

**Customizing Wired Infrastructure Alarm Policy**

You can activate or suppress the types of events and device groups on which you want the alarms to be generated or ignored.

To edit the Wired Infrastructure Alarm Policy, follow these steps:

**Step 1**  Choose **Monitor > Monitoring Tools > Alarm Policies**.

**Step 2**  Check the **Wired Infrastructure** check box and then click **Edit**.

The **Edit Wired Infrastructure Alarm Policy** page displays the default list of events that you want to modify.
What is an Alarm Policy?

Step 3  Click the Activated or Suppressed toggle button to activate or suppress the alarm for the required event.
        To perform a bulk edit, select the required Events check boxes and select Activate or Suppress from the Activate drop-down list.

Step 4  Set the required severity for an alarm from the Severity drop-down list.
        To perform a bulk edit, select the required Events check boxes and select a severity from the Change Severity drop-down list.

Step 5  In the Auto Clear Duration field, enter the value in hours for the alarm to clear automatically for an event.
        To perform a bulk edit, select the required Events check boxes and edit the Alarm Auto Clear field.
        Alternatively, you can choose Administration > Settings > System Settings > Alarms and Events > Alarm Severity and Auto Clear to set the severity and auto clear duration for an alarm.

Step 6  Click Save and Activate, or click Next to continue with the Device Groups page.

Step 7  Click the All devices are selected or No devices are selected toggle button to activate or suppress the events selected in Step 3 for the particular device groups. Some devices are selected is displayed only when a few devices in a device group are selected.
        To perform a bulk edit, select the required device group check boxes and select Activate or Suppress from the Activate drop-down list.
        If you choose to suppress alarms for a group that contains a port or device, the alarm types you specified are suppressed for that port or device even if that port or device is also in another group for which alarms are marked as active.

Step 8  Click Save and Activate.

Related Topics
  • What is an Alarm Policy?
  • Customizing Interface Alarm Policy
  • Customizing Controller Alarm Policy
  • Customizing Access Point Alarm Policy
  • Customizing Layer2 Switch Alarm Policy
  • Viewing the Alarm Policy Summary
  • Restoring Default Settings

Viewing the Alarm Policy Summary

To view the summary of the interface, controller and access point, Layer 2 switch, and wired infrastructure alarm policies, follow these steps:

Step 1  Choose Monitor > Monitoring Tools > Alarm Policies.

Step 2  Click one of the options below to view the alarm policy summary and display a list of activated alarms on device groups:
  • Interface
  • Controller
Chapter 12 Monitoring Alarms

Getting Help for Alarms

• Access Point
• Layer2 Switch
• Wired Infrastructure

Related Topics
• What is an Alarm Policy?
• Customizing Interface Alarm Policy
• Customizing Controller Alarm Policy
• Customizing Access Point Alarm Policy
• Customizing Layer2 Switch Alarm Policy
• Customizing Wired Infrastructure Alarm Policy
• Restoring Default Settings

Restoring Default Settings

To reset the alarm policy to its default settings, follow these steps:

**Step 1** Choose Monitor > Monitoring Tools > Alarm Policies.

**Step 2** Select one of the alarm policy types, then click Reset to Default to restore the default settings.

The customized settings are cleared and all the alarms are activated on all devices, device groups and port groups.

Related Topics
• What is an Alarm Policy?
• Customizing Interface Alarm Policy
• Customizing Controller Alarm Policy
• Customizing Access Point Alarm Policy
• Customizing Layer2 Switch Alarm Policy
• Customizing Wired Infrastructure Alarm Policy
• Viewing the Alarm Policy Summary

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 3.1 Administrator Guide for more information.
Viewing 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 logs and displays syslogs from managed devices only. Syslogs from devices that are not managed by Prime Infrastructure are not logged or displayed.

In order for Prime Infrastructure to provide client troubleshooting, you must configure SNMP write credentials and Telnet credentials when adding or importing the devices.

Prime Infrastructure stores a maximum of 2,000,000 syslogs with the following display limits:

- Live syslog streaming displays the latest 2,000 syslogs.
- Historic syslogs displays a maximum of 200,000 total syslogs.
- Client Troubleshooting displays the latest 1,000 syslogs.
- Infrastructure Troubleshooting displays the latest 1,000 syslogs.

---

**Step 1**
To view syslogs, choose Monitor > Monitoring Tools > Syslog Viewer. The first time you access this page, an overlay screen explains the main features.

By default, live streaming of syslogs is displayed. As syslogs are generated, they appear in the window. It might take a few seconds for data to be generated. If syslogs were generated before you clicked the Live tab, they appear in the Historic tab.

**Step 2**
Click the Pause icon to pause the live streaming if the incoming data is too excessive. Click the Resume arrow to resume live streaming of syslogs.

**Step 3**
Click Deduplicate to enable or disable deduplication of syslogs. Deduplication aggregates all syslogs of the same type into one line item and displays the count of this syslog type in the Count field.

**Step 4**
To troubleshoot a client based on syslogs, select one of the following options from the Troubleshooting Type drop-down menu:

- **Client**—Enter a client MAC address, then click Troubleshoot to start a troubleshooting session and view the syslogs for the specified client.

- **Infrastructure**—Select a troubleshooting option, then click Troubleshoot.

**Step 5**
To open a TAC support case, click the Open Support Case icon. You need to enter your cisco.com login credentials to open a case.

**Step 6**
To export the syslogs in either CSV or PDF format, click the Export icon.

**Step 7**
Click the filter icon to view and change filter, such as location and devices. You can also enter text in the fields at the top of the table to filter the results; regular expression filtering is supported. For example, you can enter the following regular expression to filter the results:

```
^Auth, V|violation$,^Sec*V|violation$
```

**Step 8**
Click the yellow Filter icon in the Syslog Viewer page for Historic and Live tabs:

- Historic syslog page filter criteria has only location grouping. You can select either a separate group or all location with respect to the requirement. If a group is selected, then it shows syslogs from devices present in that group only.
Live page syslog viewer filter criteria has location grouping and device grouping. Device grouping supports only 10 devices at a time and by default, the first 10 devices are selected. In the location group, unassigned devices are selected by default. You can change the preferences with respect to your requirement.

**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-PER_REALACHABILITY_FAILURE
- L2-L2VPN_ICCP_SM-4-PER_REALACHABILITY_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
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 > Syslogs.

Step 2  Click the Historic 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 > Syslogs**.

Step 2  Click **Custom Syslog Events**. The Custom Syslog Events window opens displaying any previously created event mappings.

Step 3  Select the custom syslog event you want to modify, then click **Edit**.

Step 4  Modify the necessary fields, then click **OK**.

**Related Topic**
- Customizing Alarms and Events For Syslogs