Monitor Alarms and Events

This chapter contains the following topics:

What Are Alarms and Events?

An *event* is a distinct incident that occurs at a specific point in time, such as a port status change, or a device becoming unreachable. Events can indicate an errors, failures, or exceptional conditions in the network. Events can also indicate the *clearing* of those errors, failures, or conditions.

An *alarm* is a Prime Infrastructure response to one or more related events. Only certain events generate alarms. Alarms have a state (cleared or not cleared) and a severity (Critical, Major, Minor, and so forth). An alarm inherits the severity of its most recent event. Alarms remain open until a clearing event is generated (or if the alarm is manually cleared).

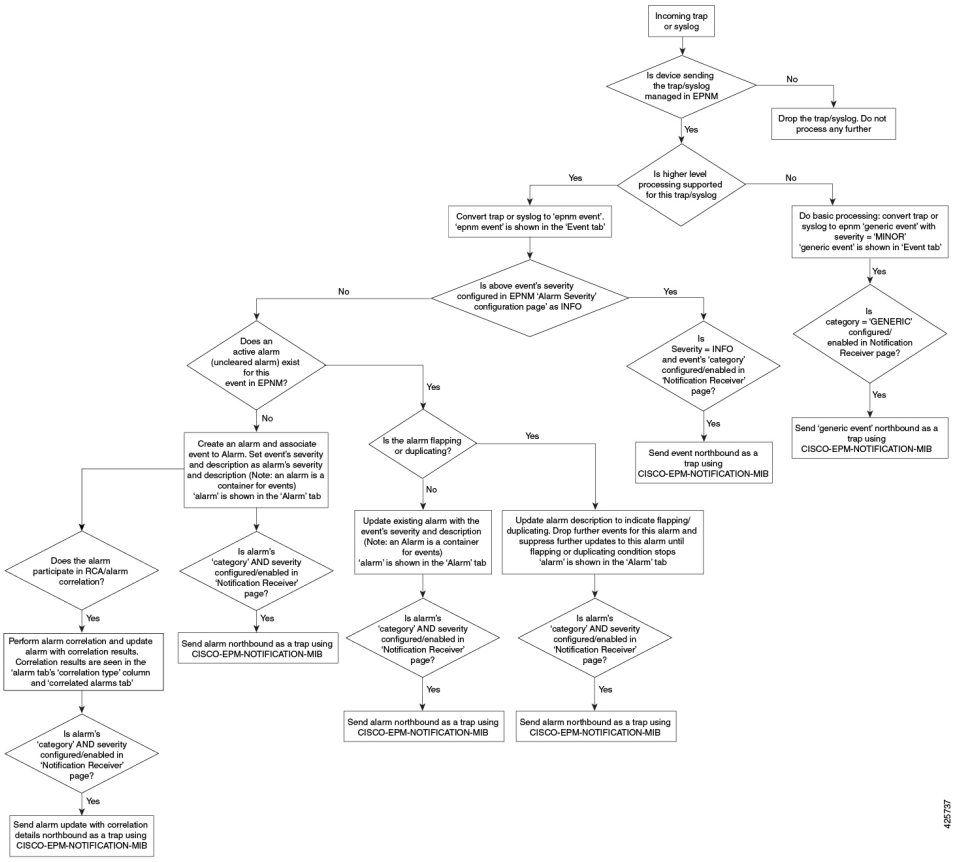
Related Topics

How are Alarms and Events Created and Updated?, on page 2
Acknowledge and Clear Alarms, on page 10
Interpret Event and Alarm Badges and Colors, on page 8

How are Alarms and Events Created and Updated?

The Prime Infrastructure processes SNMP traps, syslogs, and TL1 messages from both IPv4 and IPv6 devices. It maintains an event catalog that determines how it should respond to these events. The flowchart below represents the manner in which these alarms and events are processed:

Figure 1: Alarm processing flowchart



Prime Infrastructure performs the following general steps when it processes an event:

1. If the trap or syslog is not supported by Prime Infrastructure, event is not created. If it is supported then the trap or syslog is considered for higher level processing and Prime Infrastructure creates a processed event with a severity and potentially an alarm.
2. Identifies the device and device component that is causing the event (localizes the event).
3. Checks whether the supported event triggers inventory collection.

   Some events have specific rules that instruct Prime Infrastructure what information it should collect.

4. Checks whether the event severity is INFO or CLEARED.
   - If it is INFO or CLEARED, Prime Infrastructure saves the event and displays it in the GUI.
   - If it is any other severity, Prime Infrastructure evaluates whether a new alarm should be opened (next step).
5. Checks whether an alarm already exists or a new alarm should be created.
   - If an alarm does exist, Prime Infrastructure associates the event to the existing alarm. The alarm severity is changed to match the severity of the new event, and the alarm time stamp is updated. If it is a clearing event (for example, a link up event), the alarm will be cleared.

Note In some cases, a device may not generate a clearing alarm. The administrator should set the alarm auto-clearing interval.

   - If an alarm does not exist, Prime Infrastructure creates a new alarm and assigns it the same severity as the event.

Link Up/Down Flapping

Flapping is a flood of consecutive transitions from link down to link up (or visa versa) for the same interface on a device. It can occur when a fault causes repeated event notifications (for example, a cable with a loosely fitting connector). Prime Infrastructure will mark an alarm as flapping if there are five occurrences of link up/down transitions within 60 seconds. The five occurrences could be of a sequence such as, Interface Down, Interface Up, Interface Down, Interface Up, Interface Down, and so on.

The alarm marked as flapping is either cleared or marked back as a link down when there is no occurrence of any link up/down transition for 60 seconds. The alarm will be updated based on the last non-flapping event received (up or down). This helps control the flow of events and constant updating of the alarm state and the associated notifications (display, emails, northbound traps).

Find and View Alarms

To view alarms, choose **Monitor > Monitoring Tools > Alarms and Events**. The alarms are classified into four categories and displayed in separate tabs in the Alarms table as given below:

- Network Health—Shows the controller, switches, and router category alarms.
- Rogue AP—Shows the Rogue AP and Adhoc Rogue category alarms.
- Security—Shows the security category alarms.
- System—Shows the system category alarms.

The count next to each tab name indicates the total number of alarms in that specific alarm category.

Show Active Alarms—You can search for specific alarms and also create and save customized (preset) filters as described in the procedure that follows the table - By default, the Alarms and Events page shows the latest 4000 active alarms excluding the cleared alarms. The active alarms are automatically refreshed based on the settings chosen in **My Preferences** page. For more details, see Set Up Your Alarm and Event Display Preferences, on page 6. You can temporarily disable the automatic refreshing of alarms by clicking the Pause Auto-Refresh button.

Show Alarm History—Click **Show Alarm History** in the **Alarms and Events** page to view up to 20,000 alarms. If you want to view the cleared alarms, see Cleared , on page 10. The alarms are not refreshed automatically in the Show Alarm History mode. But, you can manually refresh the alarms by clicking the Refresh icon in the Alarms and Events table.

The following table describes the alarm viewing options available in the show drop-down filter list.

To find these alarms:	Choose Monitor > Monitoring Tools > Alarms and Events and:
Alarms generated by specific device	For active alarms, click the "I" icon next to the device name to open the Device 360 view, then click the **Alarms** tab. For cleared alarms, refer to the Alarms and Events table. For certain devices, you can also use the Chassis View to check device alarms.
Alarms assigned to you	Click the **Show** drop-down filter list and choose **Alarms assigned to me**. You can also use this filter for cleared and correlated alarms.
Unassigned alarms	Click the **Show** drop-down filter list and choose **Unassigned** Alarms. You can also use this filter for cleared and correlated alarms.
Latest alarms according to the Prime Infrastructure timestamp	For active alarms: • Alarms in the last 30 minutes—Click the Show drop-down filter and choose the last 5, 15, or 30 minutes **(PI timestamp)**. • Alarms in the last 24 hours—Click the Show drop-down filter and choose the last 1, 8, or 24 hours **(PI timestamp)**. • Alarms in the last 7 days—Click the Show drop-down filter and choose the last 7 days **(PI timestamp)**.
Latest Alarms according to the device timestamp	Follow the same instructions as in the previous row, but choose the filters with the suffix **(Device timestamp)**
All alarms generated by a device group, series, or type	Choose a group from the navigation pane on the left. You can also use this filter for cleared and correlated alarms.
Alarms using customized filters	Create and save the advanced filter (see the procedure that follows this table).

Suppress an Existing Alarm

You can suppress an existing alarm for a specific duration or permanently by creating an alarm policy.

To suppress an Alarm:

Step 1 Choose **Monitor** > **Monitoring Tools** > **Alarms and Events**.

Step 2 Choose the Alarm that you want to suppress.

Step 3 Click the **Create Alarm Policy** drop-down list and choose **Suppress**.

Note The **Create Alarm Policy** drop-down list will be enabled only if you have selected any alarm.

Step 4 In the **Create New Alarm Policy** dialog, choose any one of the suppress options as required:

- Suppress Permanently.
- Display if the condition persists for this duration (minutes); and select the time duration using the time slider.

Step 5 Click **Summary** to view the details of the policy. If you wish to change the settings, navigate to the previous page and do the necessary changes.

Step 6 Click **Finish**. A new policy is created.

Note You can view, edit, delete, and re-order this policy from **Monitor** > **Monitoring Tools** > **Alarm Policies** page.

Note Policies created in Alarms and Events page do not impact existing alarms. They are applicable only for future alarms.

Related Topics

Delete Alarm Policy, on page 23
Edit an Existing Alarm Policy, on page 23
What is an Alarm Policy?, on page 19

Change Severity of an Existing Alarm

You can change the severity of an existing alarm by creating an alarm policy.

To change the severity:

Step 1 Choose **Monitor** > **Monitoring Tools** > **Alarms and Events**.

Step 2 Choose the Alarm that you want to change the severity.

Step 3 Click the **Create Alarm Policy** drop-down list and choose **Change Severity....**. The event types of the selected alarm will be displayed in the **Create New Alarm Policy** dialog.

Note The **Create Alarm Policy** drop-down list will be enabled only if you have selected any alarm.

Step 4 Click on a row in the table to select a new severity for an event type.

Step 5 Click the **Severity** drop-down list of the selected event type and change the severity.

Step 6 Click **Save**.

Note The policy cannot be saved until a severity other than the default is chosen.

Step 7 Click **Summary** to view the details. The name and description are automatically generated for this policy and will apply to alarms from any source.

Step 8 Click **Finish**.

Note You can view, edit, delete, and re-order this policy from **Monitor** > **Monitoring Tools** > **Alarm Policies** page.

Note Policies created in Alarms and Events page do not impact existing alarms. They are applicable only for future alarms.

Related Topics

Delete Alarm Policy, on page 23
Edit an Existing Alarm Policy, on page 23
What is an Alarm Policy?, on page 19

Set Alarm and Event Management Preferences

Note Advanced users can also use the Prime Infrastructure Representational State Transfer (REST) API to access device fault information. For information on the API, click ⚙ at the top right of the Prime Infrastructure window and choose **Help** > **REST API**.

Set Up Your Alarm and Event Display Preferences

Note The list of 4000 alarms and events also includes cleared alarms which are not displayed. Click **Show All** to see all the open alarms.

You can customize the following alarm and event display by clicking ⚙ at the top right of the Prime Infrastructure window and choosing **My Preferences**. After you make your changes, click **Save** to apply your new settings. Other settings, such as whether acknowledged, cleared, and assigned alarms are displayed, are controlled globally by the administrator.

User Preference Setting	Description
Automatically refresh Alarms & Events page	Enables or disables automatically refreshing of the active alarms and events data in the Alarms and Events page. If enabled, the page is refreshed according to the setting in **Refresh Alarm count in the Alarm Summary**.
Refresh Alarm count in the Alarm Summary every ___ minutes/seconds	Sets the refresh interval for the alarm count in the Alarm Summary (1 minute by default) (see Customize the Alarm Summary, on page 8).

User Preference Setting	Description
Enable Alarm Badging on Alarms & Events page	When user enables Alarm Badging, alarm severity icons are displayed next to the device groups on the **Monitor** > **Monitoring Tools** > **Alarms & Events** page.
Disable Alarm Acknowledge Warning Message	**Note** This setting is only configurable if **Hide Acknowledged Alarms** is also enabled; that setting is disabled by default (see the previous table). Disables the following message from displaying when user selects an alarm and chooses **Change Status** > **Acknowledge**: **Warning: This alarm will not be generated, if the original event recurs again, within next 7 days, as it is acknowledged now. Clearing the alarm instead of acknowledging will cause the alarm to be generated if the event recurs again. Proceed with alarm acknowledgment?**
Disable confirmation prompt for "Clear all of this condition"	Disables the following message from displaying when user selects an alarm and chooses **Change Status** > **Clear all of this condition**: **Are you sure you want to clear all alarms of this condition?** (Disabled by default)
Disable "Set severity to information" prompt for "Clear all of this condition"	Disables the following message which is displayed when user selects an alarm and chooses **Change Status** > **Clear all of this condition**: **Do you want to set the severity for the selected alarm's condition to Information?** **WARNING: This is a system-wide change that will prevent creation of future alarms of this condition. You can undo this change on the Severity Configuration page under System Settings.** (Disabled by default) **Note** Users with sufficient privileges can reset the severity to its original value.
Select alarm categories for Alarm Summary Toolbar	Controls what is displayed in the Alarm Summary (see Customize the Alarm Summary, on page 8).
When clearing all alarms of a condition, always set the condition's severity to Information	When user selects and alarm and chooses **Change Status** > **Clear all of this condition**. (Disabled by default)
Enable New Critical Alarm Count Notifications	Enables the notification pop-up that displays the count of critical alarms.The count gets updated once the alarm interval is refreshed depending on the interval set in **Refresh Alarm count in the Alarm Summary** (see Customize the Alarm Summary, on page 8). Only the outstanding critical alarms are displayed.

Customize the Alarm Summary

You can specify what alarm categories are displayed:

- In the Prime InfrastructureCisco Prime Infrastructure title bar alarm count (bell). This gives you a quick visual count of alarms you are interested in.
- In the Alarm Summary pop-up window that is launched when you click the alarm count. The pop-up window gives you a quick look at alarm counts with their severity, as shown in the following figure.

To customize this information:

Step 1 Click **Edit** at the top left of the Alarm Summary pop-up window. This opens your My Preferences page. You can also open this page by clicking at the top right of web GUI window and choosing **My Preferences**.

Step 2 Click the **Alarms & Events** tab.

Step 3 To change the Alarm Summary refresh interval, select a number from the **Refresh Alarms & Events page and Alarm count in the Alarm Summary every** drop-down list.

Step 4 To specify what is included in the Alarm Summary, Go to the **Alarm Categories** area. Select **Alarm Summary** from the **Default category to display**drop-down list. Enable or disable the required Alarm Category by selecting or deselecting the corresponding checkbox.

Step 5 Click **Save** to confirm the changes made in the My Preferences window.

Interpret Event and Alarm Badges and Colors

When there is a problem in the network, Prime Infrastructure flags the problem by displaying an alarm or event icon with the element that is experiencing the problem. Alarm Severity Icons, on page 8 lists the icons and their colors.

Alarm Severity Icons

The table below lists the alarm colors and their respective severity levels for the icons displayed in various parts of the web GUI.

Severity Icon	Description	Color
	Critical alarm	Red
	Major alarm	Orange
	Minor alarm	Yellow
	Warning alarm	Light Blue
	Alarm cleared; normal, OK	Green

Severity Icon	Description	Color
	Informational alarm	Medium Blue
	Indeterminate alarm	Dark Blue

Get Troubleshooting and Detailed Alarm Information

View an Alarm's Details

To get more details about an alarm, expand it. You can do this from the Alarms list (by choosing **Monitor** > **Monitoring Tools** > **Alarms and Events**, or by clicking **Details** in the Alarm Summary pop-up).

General Information—When alarm was found and last updated, current and last severity, and how it was detected	**Device Details**—Managed device name, address, uptime, reachability status, collection status, and so forth
Messages—Trap, syslog, or TL1 message	**Device Events**—Recent device events from past hour (of any type, in chronological order)

Find Troubleshooting Information for an Active Alarm

Use this procedure to get an explanation for why an active alarm occurred, and the recommended response to the alarm.

Note Not all alarms have this information. Users with sufficient privileges can add or change the information that is displayed in the popup window.

Step 1 Choose **Monitor** > **Monitoring Tools** > **Alarms and Events**, then click the **Alarms** tab. (For interface alarms, you can also get this information from the Interface 360 view under the **Alarms** tab.)

Step 2 Locate the alarm, then click the "i" icon in the **Severity** column to open the popup window that provides the explanation and the recommended action that can be taken to troubleshoot the alarm.

If you take any actions, we recommend you document your actions. Choose the alarm, click **Annotation**.

Find Out Which Events Are Associated With An Alarm

To view the events that have been correlated to an alarm, from the Alarms table, click the “i” icon next to the Severity.

Acknowledge and Clear Alarms

An alarm can have a status of Not Acknowledged, Acknowledged, or Cleared.

Not Acknowledged

Not Acknowledged means the problem is not being worked on. It could indicate that a new fault condition in the network, or that a cleared fault condition that has recurred. Not Acknowledged alarms are not removed from the Alarms and Events tables until they are either acknowledged or cleared.

Acknowledged

Acknowledged means a fault condition has either been recognized and is being worked on, or it can be ignored. Moving an alarm to the acknowledged status is a manual operation and changes the alarm Status to Acknowledged. An acknowledged event is still considered to be open (that is, not cleared), so if any related events recur, the events are added to the alarm.

By default, acknowledged alarms are not removed from the Alarms list. This behavior depends on the **Hide Acknowledge Alarms** setting that is controlled by the Administrator.

Acknowledged alarms can be moved back to the Not Acknowledged status (for example, if you acknowledged the wrong alarm).

Cleared

Cleared means the fault condition no longer exists. If an alarm is cleared but an associated event recurs, Prime Infrastructure opens a new alarm.

By default, cleared alarms will not be shown in the Alarms and Events page. To view the cleared alarms in the Alarms History table in the Alarms and Events page:

Note When FRU alarms are generated, if inventory lacks location parameters then, generated alarms will not have location parameters. When the FRU alarms are cleared, the alarms may not have inventory location parameters.

- Choose **Administration** > **Settings** > **System settings**, then choose **Alarms and Events**.
- Under **Alarm Display Options**, uncheck the **Hide cleared Alarms** check box.

To change the status of an alarm:

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

Step 2 Select an alarm, then choose **Change Status** and the appropriate status (Acknowledge, Unacknowledge, Clear, Clear all of this Condition).

Note **Clear all of this Condition** triggers a clearing event for *all alarms* with the same condition as the alarm you selected. When you choose this status, Prime Infrastructure displays a dialog asking if you want to change the severity for the selected alarm condition to Information. This prevents Prime Infrastructure from issuing alarms for the specified condition. To later reset the condition's severity, choose **Administration > System Settings > Severity Configuration** and modify the severity.

Step 3 Click **Yes** to confirm that you want to clear all alarms of the specified condition.

Add Notes To an Alarm

The annotation feature allows you to add free-form text to the alarm, which is displayed in the Messages area of the alarm details. To add text to an alarm, choose the alarm in the Alarms and Events table, click **Annotation**, and enter your text. As with acknowledging, when you annotate an alarm, Prime Infrastructure adds your user name and the annotation time stamp to the Messages area of the alarm details.

Manage How Alarms are Triggered (Alarm Thresholds)

You can customize how often information is gathered (polling interval), the threshold value that indicates a problem, and whether Prime Infrastructure should generate an informational event or an alarm (of an severity) when a problem is detected. Not all policies have all of these settings; for example, a policy may only collect statistics, so it would not have any thresholds or alarms associated with it.

Step 1 Choose **Monitor > Monitoring Tools > Monitoring Policies > My Policies** and select the policy you want to edit.

Step 2 Locate the parameter you want to change. You can search for the parameter by entering a string in the **Parameter** text box.

Step 3 To adjust the polling interval, select the new interval from the **Polling Frequency** drop-down list. To disable polling, choose **No Polling**. Note that some polling frequencies are applied to groups of parameters. Changing the group interval will change the polling for all settings in the group. If a policy does not have any thresholds or events associated with it, Prime Infrastructure prompts you to save the changes.

Step 4 To change a threshold value, expand the parameter and choose a value from the parameter's drop-down list.

Step 5 To specify what Prime Infrastructure should do when the threshold is surpassed, choose an alarm value from the parameter's drop-down list. You can configure Prime Infrastructure to generate an alarm of a specified severity, generate an informational event, or do nothing (if no reaction is configured).

Step 6 Click:

- **Save and Activate** to save and activate the policy immediately on the selected devices.
- **Save and Close** to save the policy and activate it at a later time.

Note If an Access Point is detected as rogue by other APs but is managed in Prime Infrastructure, no alarms will be raised.

Which Events Are Supported?

See Cisco Prime Infrastructure Alarms, Events, and Supported SNMP Traps and Syslogs for information on the events that are supported by Cisco Prime Infrastructure.

View Events

To view alarms, choose **Monitor > Monitoring Tools > Alarms and Events**, and then click the **Events** tab.

Show Active Events—By default, the **Alarms and Events** page shows the latest 4000 active events including the cleared events. The active events are automatically refreshed based on the settings chosen in **My Preferences** page. For more details, see Set Up Your Alarm and Event Display Preferences, on page 6. You can temporarily disable the automatic refreshing of events by clicking the **Pause Auto-Refresh** button.

Show Event History—Click **Show Event History** in the **Alarms and Events** page to view up to 20,000 events. The events are not refreshed automatically in the **Show Event History** mode. But, you can manually refresh the events by clicking the Refresh icon in the Alarms and Events table.

The **Events** tab provides a variety of filters that you can use to find the information you are looking for. You can also create and save customized (preset) filters using the same procedure described in Find and View Alarms, on page 3. The following table lists some of the ways you can filter events.

Click the **Take Snapshot** tab to view the paged events. You can view up to 20,000 paged events. The tab name gets changed as **Snapshot of** *current date and time*. By defalut 50 events will be displayed per page. You can vary the**Page Size** from 50 to 200.

To find these events:	Select Monitor > Monitoring Tools > Alarms and Events, click the Events tab, and:
All events generated by a device group, series, type, location group, or user-defined group	Choose a group from the left sidebar menu
Events in last *x* minutes, hours, or days	Click the **Show** drop-down filter list and choose the appropriate filter
Non-informational events generated in the last hour	From the **Show** drop-down filter list, choose **Non-info events in last hour**

To find these events:	Select Monitor > Monitoring Tools > Alarms and Events, click the Events tab, and:
Events using customized filters	Create and save an advanced filter (see Find and View Alarms, on page 3)

View Syslog Policies

To view the Syslog policy, do the following:

Step 1 Choose **Monitor** > **Monitoring Tools** > **Syslog Policies**. All the syslog policies are listed in the Syslog Policies page.

Step 2 Click the Expand icon to view the policy details.

Related Topics

Create a New Syslog Policy, on page 13
Edit a Syslog Policy, on page 14
Change Syslog Policy Ranks, on page 15
Change Syslog Policy Ranks

Create a New Syslog Policy

To create a new Syslog policy, do the following:

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

Step 2 Click the **Add** icon. The **Create New Syslog Policy** window appears.

Step 3 In the **Policy Attributes** page, enter the unique Name, Description (optional), and choose the desired type of action that the policy will perform.

Step 4 Click **Next**.

Step 5 You will view the **Send Email** option or **Run Script** option based on the policy action chosen in the Policy Attributes window.

- **Send Email Option**
  - Click **Create New Email Recipient** and enter the Name and Email Address to create new recipient.
  - Alternatively, select a recipient and notification time range from the drop-down list.
  - Click the **Add** icon to specify multiple recipients. Send Email will notify one or more recipients by email when matching syslogs are received during corresponding certain times period.
- **Run Script Option**
  - Click the **Upload scripts** button to upload a new script from your system. You can upload scripts of any type and provide parameters pertaining to those scripts. Alternatively, you can select a script from the **Script file** drop-down list.

By default **Run Script** option is disabled. To enable **Run Script** option, go to **Administration > Settings > System Settings > Alarms and Events > Syslog Policies**. You must have Syslog Policies Settings access privilege to access the Syslog Policies system settings page.

Step 6 Click **Next**.

Step 7 In the **Device Groups** window, choose the Device Groups to which you want to apply the syslog policy. If you do not select any device groups the policy will be applied to all the devices.

Step 8 In the Syslog Fields window, configure the following filters for the syslog fields

- All Messages - The policy will activate for any syslog that meets its other conditions (such as device groups). The content of the syslog message will not affect whether the policy is activated or not.
- Message Types: - The policy will apply only for syslogs that match certain message types such as specific combinations of facility, severity, and mnemonic fields.
- Advanced Filters - To create more complex filters on the facility, severity, and mnemonic fields.
  - Choose a field (facility, severity, or mnemonic).
  - Chose a filter operation. Most filters will also require a value. The “Match” radio buttons above the list of filters determines whether all given conditions must be true, or if at least one must be true.

Step 9 Click **Summary** to view the details of the syslog policy. If you wish to change the settings, navigate to the respective window and do the necessary changes.

Step 10 Click **Finish**.

Edit a Syslog Policy

To edit a new Syslog policy, do the following:

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

Step 2 Choose the policy and then click the **Edit** icon. The **Edit Syslog policy** wizard appears.

Step 3 In the **Policy Attributes** window, check and modify the Description if required.

Note The policies name and action type cannot be changed after the policy is created.

Step 4 To make desired changes in the Edit Syslog Policy wizard follow the same as the steps in Create a New Syslog Policy Wizard.

Step 5 Click **Finish** to save the changes or click Cancel to discard.

Delete Syslog Policy

To delete a Syslog Policy, do the following :

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

Step 2 Choose the syslog policy which you want to delete and click the **Delete** icon.

Step 3 Click **yes** in the Delete Confirmation dialog box to delete, or **No** to cancel.

Change Syslog Policy Ranks

To change an existing syslog policy rank, do the following :

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

Step 2 Choose the syslog policy which you want to change the rank.

Step 3 Click **Move Up** or **Move Down** button to increase or decrease the rank of the selected policy. Click Move Up or Move Down button to increase or decrease the rank of the selected policy. Or

Step 4 Click **Move To** button. You can enter the desired ranks in the drop-down box and click enter to save the changes.

View 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. Syslogs from devices that are not managed are not logged or displayed. Prime Infrastructure also logs all SNMP messages.

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

- Live syslog streaming—Latest 2,000 syslogs
- Historic syslogs—Maximum of 100,000 syslogs
- Snapshot—No limit

Step 1 To view syslogs, choose **Monitor** > **Monitoring Tools** > **Syslog Viewer**.

Use the filters to locate different syslogs. You can enter regular expressions in the fields; for example:

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

Step 2 To view live syslogs, click the **Live** tab. If the data is excessive, click the Pause icon. You can click the Resume arrow at any time.

Step 3 If you do not want to see duplicates of a syslog, click **Deduplicate**. Prime Infrastructure will aggregate the syslogs of that type into one line item and display the count in the **Count** field.

Step 4 To view older syslogs (syslogs that were received before you clicked the **Live** tab), click the **Historic** tab. Click the **Create Syslog Policy** button to create a new syslog policy.

Step 5 Click the **SnapShot** tab to view the static syslogs. The tab will have the current date and time as the tab name.

Note By default, syslogs are sorted in descending order of the timestamp.

Step 6 Enter the **Page Size** to select the number of syslogs to be displayed per page. Number of records per page ranges from 50 to 200.

Note The **Page** drop-down list displays the date and time range of the records for each page as tool tip. It will be easier for you to track the records.

Step 7 To export the Live/History/Snapshot syslogs to a CSV, click at the top right of the table/page on the particular syslog tab to open the **Export** dialog box.

Step 8 Click **Export**. The first 1000 records will be exported.

Export Alarms, Events or Syslogs to a CSV or PDF File

Use this procedure to save alarms, events or syslogs as a CSV or PDF file.

Step 1 Navigate to the data you want to export.

Alarms—Choose **Monitor** > **Monitoring Tools** > **Alarms and Events**, then click the **Alarms** tab.

Step 2 If you have a very large amount of data, apply a filter; otherwise the export process may take some time.

Step 3 Click at the top right of the table to open the **Export** dialog box.

Step 4 Choose CSV or PDF, click **OK**, and save the file.

Working with Alarms, Events and Syslog Reports

This section describes how to create, schedule and run a alarms, events and syslog reports.

Related Topics

Create a New Alarm Report, on page 16
Create a New Events Report, on page 17
Create a New Syslog Report, on page 18

Create a New Alarm Report

You can create an alarm report by performing the following steps.

Step 1 Navigate to **Report** > **Report Launch Pad** > **Fault** > **Alarm Reports**.

Step 2 Click the **New** button. The **New Alarm Reports** page appears.

Step 3 Select the **Create the report in the current virtual domain and each of its sub-domains** check box, if you wish to create alarm reports for both the main domain and sub-domains.

Step 4 Enter the title of the report in the **Report Title** text box.

Step 5 Select an option from the **Report By** list box.

Step 6 Click the **Edit** button adjacent to the **Report Criteria** field to modify the criterion.

Step 7 Select a severity level of the report from the **Severity** list box. The available options are cleared, critical, information, major, minor, and warning.

Step 8 Select any of the options from the **Alarm Category** list box.

Step 9 Select a **Reporting Period**. You can either select an option from the list box or specify the From and To period.

Step 10 Click the **Customize** button to customize the report.

Step 11 Select the **Enable** check box to allow scheduling.

Step 12 Select a format in which the report must be exported from the **Export Format** list box. The available formats are CSV and PDF.

Step 13 Enter the destination to which the report must be delivered. It can either be an email ID or an SFTP server name.

Step 14 Set the date and time by clicking the calendar icon in the **Start Date/Time** text box. It displays the current date and time, by default.

Step 15 Set a desired Recurrence period.

Step 16 Click the save icon adjacent to the **Report Run Result** label to launch the **Run History** page.

Step 17 Click the **Run** button to generate the report.

Step 18 Click the **Save** button to save the report.

Step 19 Click the **Run and Save** button to generate the report and save it for later use.

Step 20 Click the **Save and Export** button to save the report parameters and export it as a CSV or PDF file.

Step 21 Click the **Save and Email** button to save the report parameters and send it through email.

Step 22 Click the **Cancel** button to discard the changes.

Create a New Events Report

You can create an events report by performing the following steps.

Step 1 Navigate to **Report** > **Report Launch Pad** > **Fault** > **Events Reports**.

Step 2 Click the **New** button. The **New Events Reports** page appears.

Step 3 Select the **Create the report in the current virtual domain and each of its sub-domains** check box, if you wish to create events reports for both the main domain and sub-domains.

Step 4 Enter the title of the report in the **Report Title** text box.

Step 5 Select an option from the **Report By** list box.

Step 6 Click the **Edit** button adjacent to the **Report Criteria** field to modify the criterion.

Step 7 Select a severity level of the report from the **Severity** list box. The available options are cleared, critical, information, major, minor, and warning.

Step 8 Select any of the options from the **Event Category** list box.

Step 9 Select a **Reporting Period**. You can either select an option from the list box or specify the From and To period.

Step 10 Click the **Customize** button to customize the report.

Step 11 Select the **Enable** check box to allow scheduling.

Step 12 Select a format in which the report must be exported from the **Export Format** list box. The available formats are CSV and PDF.

Step 13 Enter the destination to which the report must be delivered. It can either be an email ID or an SFTP server name.

Step 14 Set the date and time by clicking the calendar icon in the **Start Date/Time** text box. It displays the current date and time, by default.

Step 15 Set a desired Recurrence period.

Step 16 Click the save icon adjacent to the **Report Run Result** label to launch the **Run History** page.

Step 17 Click the **Run** button to generate the report.

Step 18 Click the **Save** button to save the report.

Step 19 Click the **Run and Save** button to generate the report and save it for later use.

Step 20 Click the **Save and Export** button to save the report parameters and export it as a CSV or PDF file.

Step 21 Click the **Save and Email** button to save the report parameters and send it through email.

Step 22 Click the **Cancel** button to discard the changes.

Create a New Syslog Report

You can create a syslog report by performing the following steps.

Step 1 Navigate to **Report** > **Report Launch Pad** > **Fault** > **Syslog Reports**.

Step 2 Click the **New** button. The **New Syslog Reports** page appears.

Step 3 Select the **Create the report in the current virtual domain and each of its sub-domains** check box, if you wish to create syslog reports for both the main domain and sub-domains.

Step 4 Enter the title of the report in the **Report Title** text box.

Step 5 Select an option from the **Report By** list box.

Step 6 Click the **Edit** button adjacent to the **Report Criteria** field to modify the criterion.

Step 7 Select a severity level of the report from the **Severity** list box. The available options are Alert, Critical, Debug, Emergency, Error, Informational, Notice, and Warning.

Step 8 Select a **Reporting Period**. You can either select an option from the list box or specify the From and To period.

Step 9 Click the **Customize** button to customize the report.

Step 10 Select the **Enable** check box to allow scheduling.

Step 11 Select a format in which the report must be exported from the **Export Format** list box. The available formats are CSV and PDF.

Step 12 Enter the destination to which the report must be delivered. It can either be an email ID or an SFTP server name.

Step 13 Set the date and time by clicking the calendar icon in the **Start Date/Time** text box. It displays the current date and time, by default.

Step 14 Set a desired Recurrence period.

Step 15 Click the save icon adjacent to the **Report Run Result** label to launch the **Run History** page.

Step 16 Click the **Run** button to generate the report.

Step 17 Click the **Save** button to save the report.

Step 18 Click the **Run and Save** button to generate the report and save it for later use.

Step 19 Click the **Save and Export** button to save the report parameters and export it as a CSV or PDF file.

Step 20 Click the **Save and Email** button to save the report parameters and send it through email.

Step 21 Click the **Cancel** button to discard the changes.

Get Support from Cisco

If you receive an alarm in **Monitor > Monitoring Tools > Alarms and Events** for which you cannot find a resolution in the Cisco Support Community (click 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**).

Respond to Problems Within Prime Infrastructure

Prime Infrastructure generates internal SNMP traps to monitor its own functions—such as server CPU and disk utilization, fan and power supply failures, and high availability (HA) state changes.

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. Choose **Monitor > Monitoring Tools > Alarm Policies** to view the alarm policies. You can create, edit, delete, and rank the alarm policies. Alarm policy includes one or more conditions, and an action that is applied to any events/alarms that meet all the defined conditions.

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.

You can create alarm policies to perform the following actions:

- Suppress alarms—Does not generate alarms for the selected events. But, events will be created and saved normally.
- Suppress events and alarms—Does not create events and alarms.
- Change alarm severities—Overrides the system-wide default severity for the alarms/events that meet the conditions set in the policy.
- Create disassociation threshold alarm—Generates an alarm when a certain percentage of access points across one or more device groups are disassociated from their controllers.
- Configure AP Disassociated alarm suppression—Suppress the alarms with the condition “AP disassociated from controller” either permanently or temporarily.

Related Topics

Create a New Alarm Policy, on page 21
Types of Alarm Policies, on page 19
Edit an Existing Alarm Policy, on page 23
Alarm Policy Ranks, on page 21

Types of Alarm Policies

The table below shows the alarm policy types and the various alarm actions available for each alarm policy type.

Policy Type	Available Action Options
Access Point	• Suppress Alarms • Suppress Alarms and Events • Change Alarm Severities
AP Disassociation	• Create Disassociation Threshold Alarm • Configure Suppression for AP Disassociated Alarm
Controller	• Suppress Alarms • Suppress Alarms and Events • Change Alarm Severities
Interface	• Suppress Alarms • Suppress Alarms and Events • Change Alarm Severities
Layer 2 Switch	• Suppress Alarms • Suppress Alarms and Events • Change Alarm Severities
System	• Suppress Alarms • Suppress Alarms and Events • Change Alarm Severities
Unclassified	• Suppress Alarms • Suppress Alarms and Events • Change Alarm Severities
Wired Infrastructure	• Suppress Alarms • Suppress Alarms and Events • Change Alarm Severities

Note The **Unclassified** policy type displays all supported event types that are not associated with another policy type. The available conditions and actions for **Unclassified** policies are similar to other available policy types, such as **Controller**.

Alarm Policy Ranks

Rank determines the priority or execution order of the alarm policy whenever two or more policies are applied to the same alarm or event. By default, the alarm policies will be ranked in the order they are created.

Points to be remembered while ranking the alarm policies:

1. A lower rank number indicates higher priority
2. A policy with highest rank is applied first, then next highest rank, and so on
3. A high-ranked policy may affect the behavior of a lower-ranked policy or may override the lower-ranked policy entirely.
    - Suppress Alarms will not be applied if a higher-rank alarm suppression policy has already been applied to the event.
    - Suppress Alarms and Events will not be applied if either:
        - A higher-rank suppression policy has already been applied to the event.
        - The event indicates an AP has been disassociated for a sustained period of time.
    - Change Alarm Severities will not be applied if a higher-rank severity change policy has already been applied to the event or alarm.
    - Create Disassociation Threshold Alarm—Does not count AP disassociated alarms that are suppressed by a higher-rank suppression policy. If the AP disassociated alarms are temporarily suppressed, they will be counted once their suppression time expires.
    - Configure AP Disassociated Alarm—Suppression will not be applied if a higher-ranked suppression policy has already been applied to the alarm.

To change the ranking of alarm policies, do the following:

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

All the alarm policies are listed in the order they are created.

Step 2 Choose the alarm policy which you want to change the order.

Step 3 Click the Move To icon and enter the ranking number in the **Row** field or click the Move up icon or Move down icon and change the ranking order.

View Alarm Policies

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

All the alarm polices are listed in the Alarm Policies page.

Step 2 Click the Expand icon to view the policy details.

Create a New Alarm Policy

To create a new Alarm Policy, do the following:

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

Step 2 Click the Add icon and choose the policy type from the **Select A Policy Type** window.

The **Create a New Alarm Policy** wizard appears.

Step 3 In the **Policy Attributes** page, enter the Name, Description (optional), and choose the type of action you want to perform.

The type of action displayed here is based on the chosen policy in the previous step. See, Types of Alarm Policies in Related Links.

Step 4 For Access Point, Controller, Interface, Layer 2 Switch, unclassified, System and Wired Infrastructure policy types, do the following:

a) Choose one of the following options under **Action Options** tab.

- Suppress Permanently
- Display if the condition persists for this duration (minutes); and select the time duration using the time slider.

Note This tab will be enabled only if you have choosen **Suppress Alarms** in step 3.

b) Choose the Device groups.

If you do not select any device the policy will apply to all devices.

c) (Only for Interface policies) Choose the Port groups.

If you do not select any port the policy will apply to all the port groups.

d) Choose the alarms/events that you want to suppress or the alarms/events that you want to change the severity based on the action chosen in the **Policy Attributes** page.

e) Click **Summary** to view the details of the policy. If you wish to change the settings, navigate to the respective page and do the necessary changes.

f) Click **Finish**.

Step 5 For AP Disassociation policy type, do the following:

Note The AP disassociation alarm policy will be applied only to the leaf nodes.

a) Choose one of the following options under **Action Options** tab.

Choose the following options if you have selected Configure Suppression for AP Disassociated Alarms in step 3:

- Suppress Permanently
- Display if the condition persists for this duration (minutes); and select the time duration using the time slider.

Choose the following options if you have selected Create Disassociation Threshold Alarm in step 3:

- Suppress Permanently
- Suppress after the configured disassociation threshold is reached
- Do not Suppress

b) Choose the Device groups.

This is a mandatory step, if you have chosen **Create Diassociation Threshold Alarm** action in the **Policy Attributes** page. If you do not select any device for **Configure Suppression for AP Disassociated Alarms** action, the policy will be applied to all the devices.

c) For **Create Diassociation Threshold Alarm** action, choose the desired dissociation threshold percentage.
d) For **Configure Suppression for AP Disassociated Alarms** action, click **Suppress Permanently** if you want to permanently suppress the alarm or click **Display if the condition persists for this duration** and select a suppression duration using the slider.
e) Click **Summary** to view the details of the policy. If you wish to change the settings, navigate to the respective page and do the necessary changes.
f) Click **Finish**.

Related Topics

Types of Alarm Policies, on page 19
Edit an Existing Alarm Policy, on page 23

Edit an Existing Alarm Policy

To edit the Alarm Policy, follow these steps:

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

Step 2 Choose the policy and then click the Edit icon.

The **Edit Alarm Policy** wizard appears.

Step 3 In the **Policy Attributes** page, check and modify the Description if required.

You cannot edit the policy name and action chosen while creating the policy.

Step 4 The remaining steps in the **Edit Alarm Policy** wizard are same as the steps in **Create a New Alarm Policy** wizard. See, Create a New Alarm Policy, on page 21.

Step 5 Click **Finish** to save the changes or click **Cancel** to discard.

Related Topics

What is an Alarm Policy?, on page 19
Create a New Alarm Policy, on page 21

Delete Alarm Policy

To delete the alarm policy, do the following;

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

Step 2 Choose the alarm policy which you want to delete and click the Delete icon.

Step 3 Click **yes** in the Delete Confirmation dialog box to delete, or **No** to cancel.

Alarms and Events Notification Policies

You can create policies for sending notifications on specific alarms of interest that are generated from particular device groups, to specific recipient groups.

For more information see the section *Event Receiving, Forwarding, and Notifications* in the chapter Fault Management Administration Tasks in the Cisco Prime Infrastructure Administrator Guide.