Monitor Alarms and Events

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. Event have associated severities (which you can adjust as described in Change Event Severity Levels).

An *alarm* is a Cisco EPN Manager 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).

- How are Alarms and Events Created and Updated?
- Acknowledge and Clear Alarms
- Interpret Event and Alarm Badges and Colors

LIMITED ORDERABILITY RELEASE

How are Alarms and Events Created and Updated?

Cisco EPN Manager processes syslogs, traps, and TL1 messages from both IPv4 and IPv6 devices. It maintains an event catalog that determines when an event is created and whether to create an associated alarm for an event. Cisco EPN Manager creates events by:

- Receiving notification events from devices, such as syslogs, traps, and TL1 messages
- Discovering changes during regular polling or inventory collection using the settings specified in the system (see Find Devices With Inventory Collection Problems)

Cisco EPN Manager performs the following general steps when it processes an event:

1. Checks the event catalog to see if it contains a matching event (by examining the new event for predefined patterns).
   - If it cannot match the event to the catalog, the event is considered a *generic* event. Generic events are displayed events in the GUI and can be forwarded in notifications. (Generic event handling can be disabled; see Disable and Enable Generic Trap and Syslog Handling.)
   - If it can match the event to the catalog, the event is considered supported and Cisco EPN Manager creates an event and severity. Events are broadly considered flagging or informational. Flagging events indicate a fault; informational events are clearing and generic events.
2. Identifies the device and device component that is causing the event (localizes the event).
3. Checks whether the supported event is an expedited event.

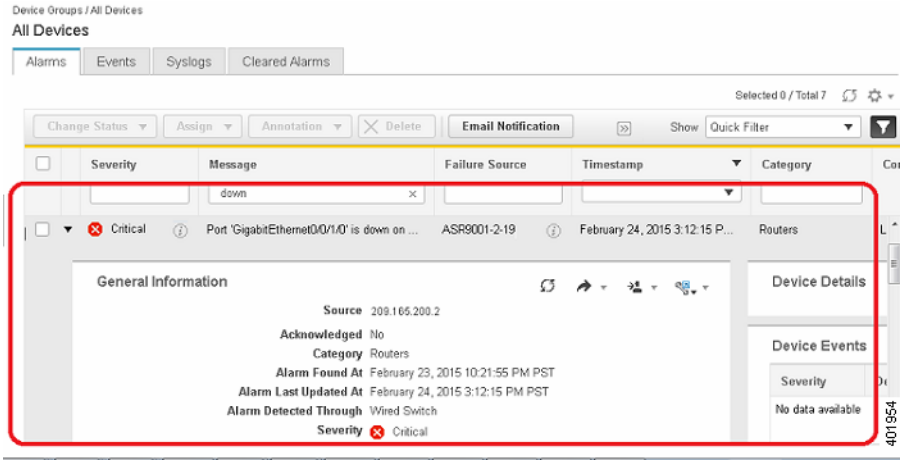
   Expedited events are handled differently from normal events. Expedited events have specific rules that instruct Cisco EPN Manager to wait for possible related incoming events before collecting more information. The waiting period is called the expedited event hold-off timer (which must be a minimum of 1 minutes). These rules instruct Cisco EPN Manager whether to perform an inventory collection only on specific parts of the network element, or on the whole NE.
4. Checks whether the supported event is a duplicate. If an event is a duplicate of an existing event, it is listed in the Events tab and saved in the database, but a new alarm is not created.
5. Checks the alarm catalog to determine whether an alarm is associated with the event type.
   - If it is, Cisco EPN Manager evaluates whether a new alarm should be opened (next step).
   - If not, it saves the event and displays it in the GUI.
6. Checks whether an alarm already exists.
   - If an alarm does exist, Cisco EPN Manager correlates the event to the existing alarm. A correlated event is an event that is caused by (correlated to) another event (the correlating event). 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. You should manually clear those alarms because by default, Cisco EPN Manager never deletes alarms that are not cleared. (See Alarm, Event, and Syslog Purging).

   - If an alarm does not exist, Cisco EPN Manager creates a new alarm and assigns it the severity of the new event.

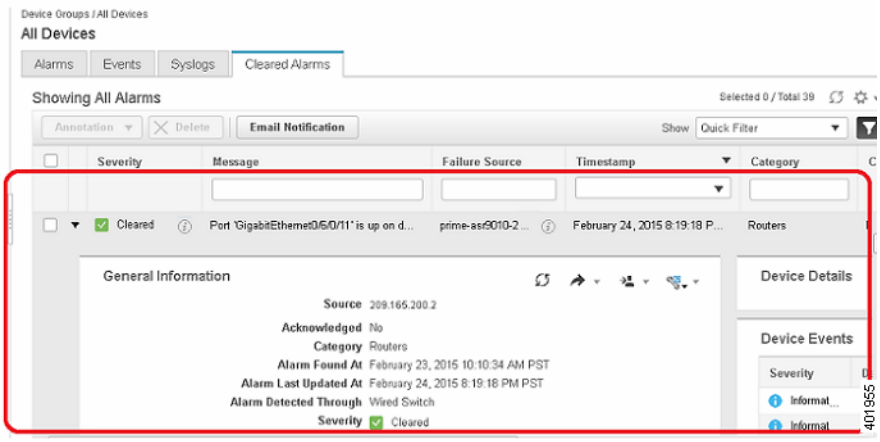
Example: Link Down Alarm

In this example, Cisco EPN Manager receives a Link Down trap that it receives from a device. Cisco EPN Manager generates a Link Down event and, because the port is operationally down, it also generates a Link Down alarm. (Cisco EPN Manager will not open an alarm when a port is simply issued a shutdown command.)



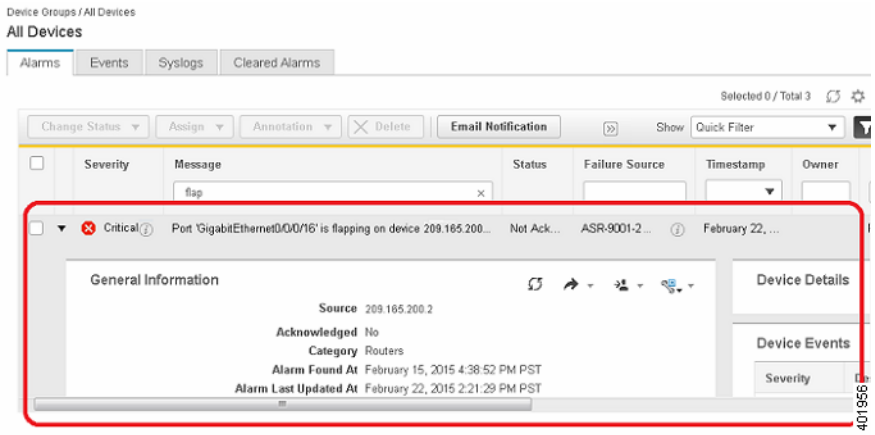
When Cisco EPN Manager receives a Link Up trap from the device, it generates a Link Up event and clears the alarm.

LIMITED ORDERABILITY RELEASE



Flapping Events

Flapping is a flood of consecutive event notifications related to the same alarm. It can occur when a fault causes repeated event notifications (for example, a cable with a loosely-fitting connector.) An event is identified as a flapping event if multiple events are of the same type, are associated with the same source, and recur in a short period of time. Cisco EPN Manager will generate an alarm for flapping events.



LIMITED ORDERABILITY RELEASE

Which Events Are Supported?

Refer to the following documents for information on the events that are supported by Cisco EPN Manager.

- *Cisco Evolved Programmable Network Manager Supported SNMP Traps*
- *Cisco Evolved Programmable Network Manager Supported Syslogs*
- *Cisco Evolved Programmable Network Manager Supported TL1 Messages*

For information about how unsupported events are handled, see View Events (Including Generic Events) and Syslogs.

Set Alarm and Event Management Preferences

- Set Up Your Alarm and Event Display Preferences
- Customize the Alarm Summary
- Check Settings for Email Notifications
- Check Current SNMP Trap Notifications and Receivers

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

Set Up Your Alarm and Event Display Preferences

Some alarm and event behavior is controlled by Administrators and cannot be customized by users. These behaviors include whether Cisco EPN Manager should remove alarms from the Alarms list when they are acknowledged, assigned, or cleared. By default only cleared alarms are removed, but they can still by viewed by choosing **Monitor > Alarms and Events** and clicking the Cleared Alarms tab. (See Configure Global Default Behavior for Alarms and Events.).

System Setting	Description
Hide acknowledged alarms	Do not display Acknowledged alarms in the Alarms list (disabled by default)
Hide assigned alarms	Do not display assigned alarms in the Alarms list (disabled by default)
Hide cleared alarms in alarms browser	Do not display cleared alarms in the Alarms list (enabled by default) **Note** These alarms remain viewable under the Cleared Alarms tab.
Add device name to alarm messages	Include device name in e-mail notifications (disabled by default)

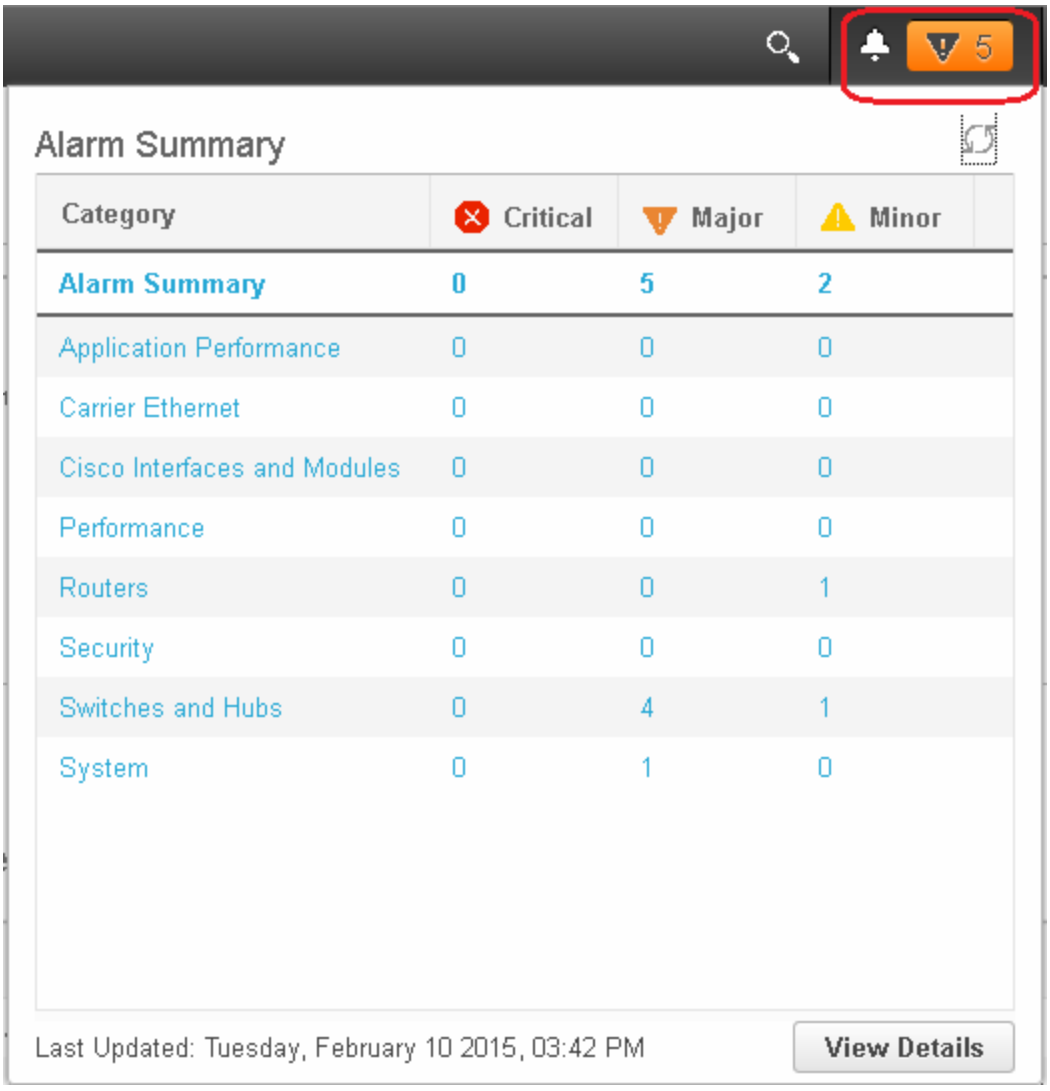
You are permitted to customize following settings by clicking at the top right of the Cisco EPN Manager window and choosing **User Preferences**. Although the defaults for these settings is controlled by the Administrator, you are allowed to override them.

User Preference Setting	Description
Refresh Map/Alarms page on new alarm	Refreshes the alarms list when a new alarm is generated (enabled by default).
Refresh Alarm count in the Alarm Summary every ___ minutes/seconds	Sets the refresh interval for the alarm count in the Alarm Summary (1 minutes by default) (seeCustomize the Alarm Summary).
Select alarms for Alarm Summary Toolbar	Controls what is displayed in the Alarm Summary (seeCustomize the Alarm Summary).
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**, changes the severity of all like alarms to Informational (disabled by default).
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? (Disabled by default)
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** You can reset the severity to its original value using the procedure in Configure Global Default Behavior for Alarms and Events.

Customize the Alarm Summary

You can specify what alarm categories are displayed:

- In the Cisco EPN Manager 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 Choose **Administration > User Preferences**.

Step 2 To change the Alarm Summary refresh interval, select a number from the **Refresh Alarm count in the Alarm Summary every** drop down list.

Step 3 To specify the alarm types you want to include in the Alarm Summary count *shown in the title bar*:

a. Click **Edit Alarm Categories**.

b. From the **Default Category to display** drop-down, choose the category you want to see in the title bar alarm count.

Step 4 To specify the alarm types you want to include in the Alarm Summary *pop-up window*:

a. Click **Edit Alarm Categories**.

b. Under the **Show** drop-down, check each alarm category or sub-category you want to see in the Alarm Summary pop-up window.

Step 5 Click **Save** to save your changes.

Check Settings for Email Notifications

Alarm and event information can be forwarded in e-mail notifications. Notifications can include alarms of any severity, and events with Informational severity. An e-mail is sent to the configured receivers when an alarm matching the criteria is created or updated. By default users with Administrator privileges can check the current notification receivers by choosing **Administration > Settings > System Settings > Mail Server Configuration**. For information on configuring new e-mail notifications, see Set Up the SMTP E-Mail Server.

All e-mail notifications include device IP addresses. The device name can also be included if the **Add device name to alarm messages** setting is enabled (it is disabled by default). That setting is also controlled by Administrators (**Administration > Settings > System Settings > Alarms and Events**).

Check Current SNMP Trap Notifications and Receivers

Alarms and events can be forwarded to notification receivers in EPM-NOTIFICATION-MIB format as SNMPv2 traps. Notifications can be customized to only forward events of a specific category and severity (for example, critical and major performance events). Users with Administrator privileges can check the current notification receivers by choosing **Administration > Settings > System Settings > Notification Receivers**. For information on configuring new notifications and receivers, see Configure E-Mail Notifications for Alarms and Events.

Interpret Event and Alarm Badges and Colors

When there is a problem in the network, Cisco EPN Manager flags the problem by displaying an alarm or event icon with the element that is experiencing the problem. The following table displays the event and alarm badges and their meaning.

Icon	Color	Severity
	Red	Critical
	Orange	Major

Icon	Color	Severity
	Yellow	Minor
	Light Blue	Warning
	Green	Cleared, Normal, or OK
	Medium Blue	Informational
	Dark Blue	Indeterminate

View and Filter Alarms

Note 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.

The following table explains the different ways to find the exact alarms you are looking for. You can also create and save customized (preset) filters as described in the procedure that follows the table below.

To find these alarms:	Use this navigation:
All alarms in the network	Select **Monitor > Alarms and Events**
All alarms generated by a device group, series, or type	Select **Monitor > Alarms and Events** and choose a group from the navigation pane on the left
Alarms generated by specific device	Click the Alarms tab in the Device
Alarms generated by a specific circuit	Click the Alarms tab in the Circuit
Alarms assigned to you	Click the Show drop-down filter list and choose **Alarms assigned to me**
Unassigned alarms	Click the Show drop-down filter list and choose **Unassigned Alarms**
Alarms in last 5, 15, 30 minutes; last hour; last 8 hours, last 24 hours, last 7 days	Click the Show drop-down filter list and choose the appropriate filter

To find these alarms:	Use this navigation:
Cleared alarms	Click the Show drop-down filter list and choose **Cleared Alarms**
Alarms using customized filters	Create and save and advanced filter (see the procedure that follows this table)

You can also filter the data to find specific alarms using a *quick filter* or an *advanced filter* from the **Show** drop-down list. The quick filter narrows the content that is displayed in a column according to the text you enter above the column. The advanced filter allows you to narrow down the data in a table by applying a filter using multiple operators such as Does not contain, Does not equal, Ends with, Is empty, and so on. You can also create a *customized* (preset) filter which, if saved, will be added to the Show drop-down menu.

To create and save a customized (preset) filter:

Step 1 Choose **Advanced Filter** from the Show drop-down list above the Alarms table.

Step 2 Enter the advanced filter criteria, then click **Go**.

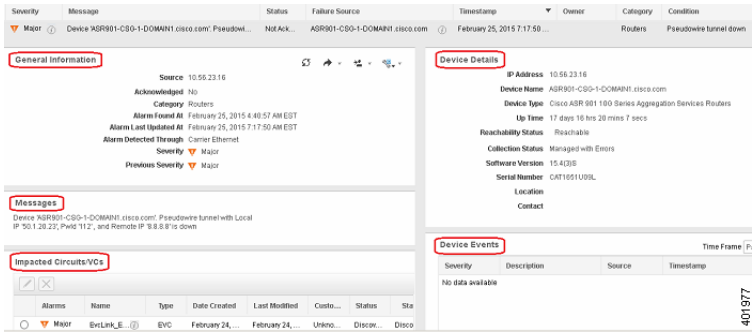
Step 3 Click the Save icon above the table, enter a name for your filter in the Save Preset Filter dialog box, and click **Save**.

To edit or remove a preset filter, choose **Manage Preset Filters** from the Show drop-down list.

Get More Information About An Alarm

View the Alarm Details

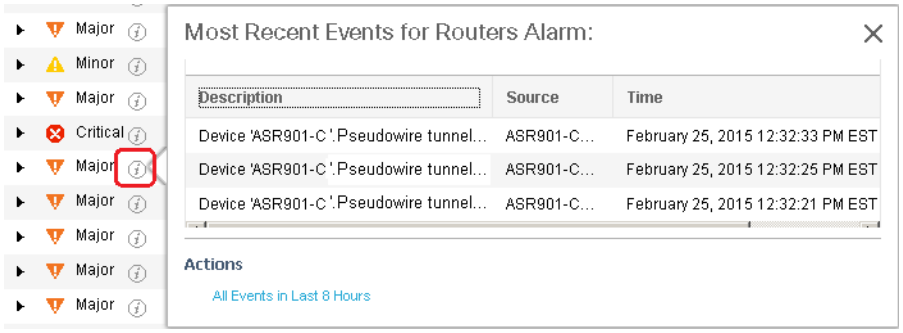
To get more details about an alarm, expand the alarm. You can do this from the Alarms list (by choosing **Monitor > Alarms and Events**, or by clicking Details in the Alarm Summary pop-up). The circled areas are explained in the table that follows this figure.



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)
Impacted Circuits/VCs—Carrier Ethernet or Optical circuits/VCs affected by alarm	

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.



Find Out If An Alarm Impacts Other Services or Network Elements

Note This information is displayed for optical devices only.

The Alarms table contains a Service Affecting column which tells you if an alarm affects other parts of the network:

- **SA** means it is a service-affecting alarm
- **NSA** means it is not a service-affecting alarm

To identify all alarms that can affect services, choose **Quick Filter** from the Show drop-down list and enter **SA** in the field above the Service Affecting column.

To find out which services are affected, expand the alarm and check the details in the Impacted Circuits/VCs area of the alarm details.

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, Cisco EPN Manager opens a new alarm. An alarm can be cleared by a user or by the Cisco EPN Manager system. Cleared alarms are removed from the Alarms list (but you can still view them under the Cleared Alarms tab).

You can also clear an alarm by choosing **Clear all of this Condition**, which will clear all alarms that are having the same problem. You may also be prompted to change all alarms with that condition to Informational severity. This means that if an associated event recurs, a new alarm will *not* be opened. You should use that setting with care.

To change the status of an alarm:

Step 1 Choose **Monitor > 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, Cisco EPN Manager displays a dialog asking if you want to change the severity for the selected alarm condition to Information. This prevents Cisco EPN Manager from issuing alarms for the specified condition. To later reset the condition's severity, choose **Administration > System Settings > Severity Configuration** and modify the severity. See Change Event Severity Levels for more information.

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, click the Annotate icon in the Messages area of the alarm details. As with acknowledging, when you annotate an alarm, Cisco EPN Manager adds your user name, and the annotation time stamp to the Messages area of the alarm details.

View Events (Including Generic Events) and Syslogs

The Events tab displays supported and generic (unsupported) events. Supported events are events that Cisco EPN Manager generates based on information about the network. It receives this network information either through syslogs and traps generated by devices, or through polling and inventory collection. This process is described in How are Alarms and Events Created and Updated? Generic events are events that Cisco EPN Manager does not recognize. Rather than drop the events, Cisco EPN Manager assigns the events a Minor severity (this severity is applied to all generic events; to change it, see Change Event Severity Levels). For information about supported events, see Which Events Are Supported?

The Syslogs tab displays syslogs of severity 0 through 7 (emergency through debugging messages) that are generated by devices that are managed by Cisco EPN Manager. Syslogs from unmanaged devices are displayed in the Events tab under the Generic category.

Generic event processing is disabled by default. Users with Administrator privileges can disable or re-enable it using the procedure in Disable and Enable Generic Trap and Syslog Handling.

The Events and Syslogs tabs provide 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 View and Filter Alarms. The following table lists some of the ways you can filter events.

To find these events:	Use this navigation:
All events in the network	Select **Monitor > Alarms and Events** and click the **Events** tab
All events generated by a device group, series, type, location group, or user-defined group	Select **Monitor > Alarms and Events**, choose a group from the navigation pane on the left, and click the **Events** tab
Events in last 5, 15, 30 minutes; last hour; last 8 hours, last 24 hours, last 7 days	Under the **Events** tab, click the Show drop-down filter list and choose the appropriate filter
Non-informational events generated in the last hour	Under the **Events** tab, click the Show drop-down filter list and choose **Non-info events in last hour**
Events using customized filters	Create and save and advanced filter (see the procedure in View and Filter Alarms)

The following table lists some of the ways you can filter syslogs:

To find these syslogs:	Use this navigation:
All syslogs in the network	Select **Monitor > Alarms and Events** and click the **Syslogs** tab
All syslogs generated by a device group, series, type, location group, or user-defined group	Select **Monitor > Alarms and Events**, choose a group from the navigation pane on the left, and click the **Syslogs** tab
Syslogs in last 5, 15, 30 minutes; last hour; last 8 hours, last 24 hours, last 7 days	Under the **Syslogs** tab, click the Show drop-down filter list and choose the appropriate filter
Severity 0-2 syslogs	Under the **Syslogs** tab, click the Show drop-down filter list and choose **Severity 0-2**
Environmental monitor syslogs, memory allocation syslogs, and others	Under the **Syslogs** tab, click the Show drop-down filter list and choose **Environmental Monitoring**, **Memory Allocation Failure**, and so forth
Syslogs using customized filters	Create and save and advanced filter (see the procedure in View and Filter Alarms)

Get Support from Cisco

If you receive an alarm in **Monitor > Alarms & Events** for which you cannot find a resolution in the Cisco Support Community (click an alarm, then choose **Troubleshoot > Support Forum**.), you can use Cisco EPN Manager to open a support request (click an alarm, then choose **Troubleshoot > Support Case**).

LIMITED ORDERABILITY RELEASE

Respond to Problems Within Cisco EPN Manager

Cisco EPN Manager 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. For information on these types of events, see Respond to Cisco EPN Manager Internal SNMP Traps.