



Monitor Alarms and Events

- [What Are Alarms and Events?](#), on page 1
- [How are Alarms and Events Created and Updated?](#), on page 2
- [Which Events Are Supported?](#), on page 5
- [Set Alarm and Event Management Preferences](#), on page 5
- [Interpret Event and Alarm Badges and Colors](#), on page 9
- [Find and View Alarms](#), on page 9
- [View a Specific Alarm in the Topology Map](#), on page 11
- [View Root Cause and Correlated Alarms](#), on page 12
- [Get Troubleshooting and Detailed Alarm Information](#), on page 12
- [Acknowledge and Clear Alarms](#), on page 15
- [Add Notes To an Alarm](#), on page 16
- [Forward Alarms and Events as Email Notifications](#), on page 16
- [Manage How Alarms are Triggered \(Alarm Thresholds\)](#), on page 17
- [View Events \(Including Generic Events\)](#), on page 17
- [View Syslogs \(Historic\)](#), on page 18
- [Export Alarms or Events to a CSV or PDF File](#), on page 20
- [Get Support from Cisco](#), on page 20
- [Respond to Problems Within Cisco EPN Manager](#) , on page 20

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).

Related Topics

- [How are Alarms and Events Created and Updated?](#), on page 2
- [Acknowledge and Clear Alarms](#), on page 15
- [Interpret Event and Alarm Badges and Colors](#), on page 9

The Cisco EPN Manager 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:

```

graph TD
    Start([Incoming trap or syslog]) --> D1{Is device sending the trap/syslog managed in EPNM}
    D1 -- No --> Drop([Drop the trap/syslog. Do not process any further])
    D1 -- Yes --> D2{Is higher level processing supported for this trap/syslog}
    D2 -- No --> Basic[Do basic processing: convert trap or syslog to 'generic event' with severity = 'MINOR' 'generic event' is shown in 'Event tab']
    D2 -- Yes --> Convert[Convert trap or syslog to 'epnm event'. 'epnm event' is shown in the 'Event tab']
    Basic --> D3{Is category = 'GENERIC' configured/enabled in Notification Receiver page?}
    D3 -- Yes --> SendGeneric[Send 'generic event' northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    Convert --> D4{Is above event's severity configured in EPNM Alarm Severity configuration page as INFO}
    D4 -- No --> D5{Does an active alarm (uncleared alarm) exist for this event in EPNM?}
    D5 -- No --> Create[Create an alarm and associate event to Alarm. Set event's severity and description as alarm's severity and description (Note: an alarm is a container for events) 'alarm' is shown in the 'Alarm' tab]
    D5 -- Yes --> D6{Is the alarm flapping or duplicating?}
    Create --> D7{Does the alarm participate in PCA/Alarm correlation?}
    D7 -- Yes --> Correlate[Perform alarm correlation and update alarm with correlation results. Correlation results are seen in the 'alarm tab's 'correlation type' column and 'correlated alarms' tab']
    D7 -- No --> D8{Is alarm's 'category' AND severity configured/enabled in Notification Receiver page?}
    D8 -- Yes --> SendTrap[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D8 -- No --> D9{Is alarm's 'category' AND severity configured/enabled in Notification Receiver page?}
    D9 -- Yes --> SendTrap2[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D9 -- No --> SendUpdate[Send alarm update with correlation details northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D6 -- No --> UpdateDesc[Update existing alarm with the event's severity and description (Note: an Alarm is a container for events) 'alarm' is shown in the 'Alarm' tab]
    D6 -- Yes --> UpdateFlap[Update alarm description to indicate flapping/duplicating. Drop further events for this alarm until flapping or duplicating condition stops 'alarm' is shown in the 'Alarm' tab]
    UpdateDesc --> D10{Is alarm's 'category' AND severity configured/enabled in Notification Receiver page?}
    D10 -- Yes --> SendTrap3[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D10 -- No --> SendUpdate2[Send alarm update with correlation details northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    UpdateFlap --> D11{Is alarm's 'category' AND severity configured/enabled in Notification Receiver page?}
    D11 -- Yes --> SendTrap4[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D11 -- No --> SendUpdate3[Send alarm update with correlation details northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
  
```

1. Checks the event catalog to see if higher level processing is necessary (as opposed to just generic processing) for the incoming SNMP trap, syslog, or TL1 message (by examining the raw event for predefined patterns).

- 106-7927

3. Checks whether the supported event triggers inventory collection.

Some events have specific rules that instruct Cisco EPN Manager what information it should collect. For more information, see [How Is Inventory Collected?](#)

4. Checks whether the event severity is INFO or CLEARED.

- If it is INFO or CLEARED, Cisco EPN Manager saves the event and displays it in the GUI.
- If it is any other severity, Cisco EPN Manager 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, Cisco EPN Manager 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 as described in [Change Alarm Auto-Clear Intervals](#).

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

6. Checks whether the new or existing alarm can be correlated to any other alarms. (Note that here, alarms are being correlated with other alarms, not with events.) If they can be correlated, Cisco EPN Manager does the following:

- Identifies the causing alarm as the **root cause alarm**.
- Identifies the resulting alarm as a **symptom alarm**.

You can identify uncleared correlated alarms by checking the Correlated Alarms tab in the Alarms and Events table. For more information on these kinds of alarms, see [View Root Cause and Correlated Alarms, on page 12](#).

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.)

Device Groups
All Devices

Alarms Events Syslogs Cleared Alarms

Showing Latest 4000 Alarms [Show All](#) Selected 0 / To

Change Status Change State Assign Annotation Show Quick Filter

	Severity	Message	Status	Failure Source	Times
<input type="checkbox"/>	Critical	Port 'GigabitEthernet0/3/0/2'...	Not Ack...	prime-asr9010-3.cisco.com	Septen

General Information

Source 172.23.222.254

Acknowledged No

Category Routers

Alarm Found At September 14, 2015 7:52:14 PM PDT

Alarm Last Updated At September 14, 2015 9:26:12 PM PDT

Alarm Detected Through Wired Switch

Severity Critical

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

Device Groups
All Devices

Alarms Events Syslogs Cleared Alarms

Showing Latest 4000 Cleared Alarms [Show All](#) Selected 0 / Total

Annotation Delete Show Quick Filter

	Severity	Message	Status	Failure Source
<input type="checkbox"/>	Cleared	Port 'GigabitEthernet0/3/0/2' is up on device '172.23.222.254'.	Not Ack...	prime-asr9010-3...

General Information

Source 172.23.222.254

Acknowledged No

Category Routers

Alarm Found At September 14, 2015 7:52:14 PM PDT

Alarm Last Updated At September 15, 2015 3:32:48 PM PDT

Alarm Detected Through Wired Switch

Severity Cleared

Flapping Events and Flow Controllers

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. This alarm is generated when there are five occurrences of the same event within 300 seconds. The five occurrences could be of a sequence such as, Interface Down, Interface Up, Interface Down, Interface Up, Interface Down, and so on.

When an alarm is generated for a flapping event, the devices often go into a continuous synchronization state. This can prevent deployment of device configuration such as service provisioning, OAM, etc, on the device. However, in Cisco EPN Manager, when a monitored device raises a Flapping alarm, Cisco EPN Manager detects this alarm and stops further updates of the alarm until the flapping condition on the device is cleared.

The alarm detected as a Flapping Event is cleared based on an exit condition, which is that when there is no occurrence of the same event within the next 300 seconds, the alarm is cleared. This helps control the flow of events to avoid unnecessary triggering of device synchronization.

Device Groups
All Devices

Alarms Events Syslogs Cleared Alarms

Showing All Events [Show Latest 4000 Events](#) Selected 0 / Total 1

Troubleshoot Upload New Mibs Show Quick Filter

Description
flapping

☐ Port 'GigabitEthernet0/3/0/19' is flapping on device '10.126.165.17'.

General Information

Event Type	Link up
Event Source	10.126.165.17
Event Category	Routers
Change Last Detected	September 11, 2015 5:30:13 AM IST
Device IP Address	10.126.165.17
Severity	✖ Critical

406010

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 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 \(Including Generic Events\)](#), on page 17.

Set Alarm and Event Management Preferences

- [Set Up Your Alarm and Event Display Preferences](#), on page 6
- [Customize the Alarm Summary](#), on page 8




Note

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

Set Up Your Alarm and Event Display Preferences

In the Alarms and Events tables, Cisco EPN Manager displays the last 4000 alarms or events, by default. Cisco EPN Manager can only display what is available in the cache (which may be less than 4000). If you want to see more than 4000 alarms or events, click **Show All** above the table.

You can customize the following alarm and event display by clicking  at the top right of the Cisco EPN Manager 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. (see [Configure Global Display and Search Settings for Acknowledged, Cleared, and Assigned Alarms](#)).

User Preference Setting	Description
Automatically refresh Alarms & Events page	Enables or disables automatically refreshing of 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 minutes by default) (see Customize the Alarm Summary, on page 8).
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	<p>Note This setting is only configurable if Hide Acknowledged Alarms is also enabled; that setting is disabled by default (see the previous table).</p> <p>Disables the following message from displaying when user selects an alarm and chooses Change Status > Acknowledge:</p> <p>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?</p>
Disable confirmation prompt for “Clear all of this condition”	<p>Disables the following message from displaying when user selects an alarm and chooses Change Status > Clear all of this condition:</p> <p>Are you sure you want to clear all alarms of this condition?</p> <p>(Disabled by default)</p>

User Preference Setting	Description
Disable “Set severity to information” prompt for “Clear all of this condition”	<p>Disables the following message which is displayed when user selects an alarm and chooses Change Status > Clear all of this condition:</p> <p>Do you want to set the severity for the selected alarm's condition to Information?</p> <p>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.</p> <p>(Disabled by default)</p> <p>Note Users with sufficient privileges can reset the severity to its original value using the procedure in Configure Global Display and Search Settings for Acknowledged, Cleared, and Assigned Alarms.</p>
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 an 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.

View Critical Alarm Notifications

The count of the critical alarms in the network is displayed as a notification pop-up in every page. The count gets refreshed every 1 minute or some interval depending on the interval set in the **My Preferences** page.

Evolved Programmable Network Manager

Application Search

2 new critical alarm in Show Details Total 22

Managed Elements / Network Devices

Device Groups: All Devices

Reachability	Admin Status	Device Name	IP Address	DNS Name	Device Type	Last Inventory Collection
<input checked="" type="checkbox"/>	Managed	ASR9001-127.156.cisco	10.127.101.156	10.127.101.156	Cisco ASR 9001 Router	Completed
<input checked="" type="checkbox"/>	Managed	ASR903-101.110.cisco	10.127.101.110	10.127.101.110	Cisco ASR 903 Router	Completed
<input checked="" type="checkbox"/>	Managed	ASR903-101.112.cisco	10.127.101.112	10.127.101.112	Cisco ASR 903 Router	Partial Collection Failure
<input checked="" type="checkbox"/>	Managed	ASR920-101.114.cisco	10.127.101.114	10.127.101.114	Cisco ASR920 12 CZA Ro...	Completed

Click the **Show Details** hyperlink to view the list of critical alarms in the **Monitor > Monitoring Tools > Alarms and Events > Alarms** page.



Note Only the outstanding critical alarms are taken count and displayed.

The notification is not enabled by default and needs to be enabled from the **My Preferences** page. For details on how to enable the critical alarm count notification, see [Set Up Your Alarm and Event Display Preferences](#), on page 6.

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.

Category	Critical	Major	Minor
Alarm Summary	20	42	115
Application Performance	0	0	0
Autonomous AP	0	0	0
BGP	0	4	2
Carrier Ethernet	0	5	27
Cisco Interfaces and Modules	0	0	0
Cisco UCS Series	0	0	0
MPLS	0	0	0
MPLS-L3VPN	0	2	0
Optical Transport	17	21	77
OSPF	0	4	2
Performance	0	0	0
Routers	3	5	5
Security	0	0	0

Last Updated: Wednesday, September 16 2015, 11:43 AM [View Details](#)

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** Go to the **Alarms** area.
- Step 3** To change the Alarm Summary refresh interval, select a number from the **Refresh Alarm count in the Alarm Summary every** drop-down list.
- Step 4** To specify what is included in the Alarm Summary, next to **Select alarms for Alarm Summary Toolbar**, click **Edit Alarm Categories**. This opens the Select Alarm Categories dialog box.

To change:	Do the following:
Alarm count displayed in the web GUI title bar	From the Default Category to display drop-down list, choose the categories you want to include in the alarm count.
Alarm types listed in the Alarm Summary pop-up window	Under the Show drop-down, check each alarm category or sub-category you want to see listed in the Alarm Summary pop-up window. If you want to include most alarms, check the Alarm Category/Subcategory check box, then uncheck the alarms you do not want to include.







Step 5 Click **OK** in the Select Alarm Categories dialog box, then click **Save** in the My Preferences window.

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. [Alarm Severity Icons, on page 9](#) 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
	Informational alarm	Medium Blue
	Indeterminate alarm	Dark Blue

Find and View Alarms

To view alarms, go to **Monitor > Monitoring Tools > Alarms and Events**. From the displayed alarms table, you can search for specific alarms, as described in the table below. You can also create and save customized

(preset) filters as described in the procedure that follows the table. To get more information about an alarm, see [View an Alarm's Details](#), on page 13.

**Note**

By default, acknowledged and cleared alarms are not included for any search criteria. This behavior is controlled by the system administrator. See [Configure Global Display and Search Settings for Acknowledged, Cleared, and Assigned Alarms](#)

To find these alarms:	Choose Monitor > Monitoring Tools > Alarms and Events and:
Alarms generated by specific device	<p>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.</p> <p>For cleared alarms or correlated alarms, click the appropriate tab and enter the device name or component in the Location column. You can use wild cards.</p> <p>For certain devices, you can also use the Chassis View to check device alarms. See View Alarms in the Chassis View.</p>
Alarms generated by a specific circuit/VC	<ol style="list-style-type: none"> 1. Click the “i” icon next to the device name to open the Device 360 view, then click the Circuit/VC tab. 2. Click the “i” icon next to the Circuit/VC name to open the Circuit/VC 360 view, then click the Alarms tab. <p>See Check Circuits/VCS for Faults for information on other ways to get circuit/VC alarm information.</p>
All alarms in the network	Click the Show All link.
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 Cisco EPN Manager timestamp	<p>For active alarms:</p> <ul style="list-style-type: none"> • Alarms in the last 30 minutes—Click the Show drop-down filter and choose the last 5, 15, or 30 minutes (CEPNM timestamp). • Alarms in the last 24 hours—Click the Show drop-down filter and choose the last 1, 8, or 24 hours (CEPNM timestamp). • Alarms in the last 7 days—Click the Show drop-down filter and choose the last 7 days (CEPNM timestamp). <p>You can use these same filters for cleared and correlated alarms. The filters do not have the (CEPNM timestamp) suffix because filtering by device timestamps is not supported for cleared and correlated alarms. For more information on (CEPNM timestamp) and (Device timestamp), see Device Timestamp and CEPNM Timestamp, on page 11.</p>

To find these alarms:	Choose Monitor > Monitoring Tools > Alarms and Events and:
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) This filter is not supported when searching for cleared or correlated alarms.
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).

You can also filter the data to find specific alarms using a *quick filter* or an *advanced filter* from the **Show** drop-down list. For information about how to filter the data, see [Filter Data in the Detailed Tables](#).

Device Timestamp and CEPNM Timestamp

While **Device timestamp** is the information embedded inside the syslogs message, **CEPNM timestamp** is the time at which that message from the device is received at Cisco EPN Manager end.

The following configuration is recommended on the device:

service timestamps log datetime show-timezone msec year

Note that these are the default formats supported in case of a Device timestamp:

- yyyy MMM dd HH:mm:ss.SSS z
- yyyy MMM dd HH:mm:ss z
- MMM dd HH:mm:ss z
- yyyy MMM dd HH:mm:ss.SSS
- yyyy MMM dd HH:mm:ss
- MMM dd HH:mm:ss

Where **z** in the format implies a time zone.



Note Only 3 letter time zones are supported and time zones with hour/minute offsets are not supported.

View a Specific Alarm in the Topology Map

From the Alarms table, you can select a specific alarm and launch the topology map to see the alarm on the map.

Step 1 To display the Alarms table, choose **Monitor > Monitoring Tools > Alarms and Events**.

Step 2 In the Alarms tab, locate and select the required alarm.

Step 3 Choose **Troubleshoot > Network Topology**.

The view switches to the topology map and the device with the alarm is highlighted in the map.

View Root Cause and Correlated Alarms

The Cisco EPN Manager correlation process determines the causality for alarms and alarm sequences. Alarms that support the correlation process can be:

- A root cause alarm—An alarm that causes other alarms (the "correlating" alarm).
- A symptom alarm—An alarm that is the result of another alarm (the "correlated to" alarm).

Root cause and symptom alarms are displayed in a hierarchical manner to help you easily identify impacted network elements. The following is an example of an uncleared link down alarm that is the root cause for two other link down symptom alarms. To display an alarm tooltip in the hierarchy, hover your mouse over an alarm.

Contained Alarms for ASR903-101.110 : Port 'GigabitEthernet0/3/1' (Description: 'Connected to CE - 144 "') is down on device '10.255.101.110'.

Severity	Message	Failure Source	Timestamp	Category	Condition	Location
Critical	Port 'GigabitEthernet0/3/1' is down on device '10.255.101.110'	ASR903-101.110	8 June, 2016 12:25:47 P...	Routers	Link down	GigabitEthernet0/3/1
Major	mplsL3vpnVrfDown on Device: ASR903-101.110, vrf instance: CUST1	ASR903-101.110	8 June, 2016 12:25:45 P...	MPLS-L3VPN	mplsL3vpnVrfDown	CUST1
Warning	cvVrfDown on Device: ASR903-101.110, vrf instance: CUST1	ASR903-101.110	8 June, 2016 12:25:44 P...	MPLS-L3VPN	cvVrfDown	GigabitEthernet0/3/1

This view is especially helpful when alarm sequence has multiple hierarchies. All alarm sequences, regardless of the number of hierarchies, have only one root cause alarm.

Step 1 Choose **Monitor > Alarms and Events**.**Step 2** To view *uncleared* correlated alarms, click the **Correlated Alarms** tab.

You can also view uncleared correlated alarms in the main Alarms and Events table. The **Correlation Type** column will identify whether it is an uncleared root cause alarms or symptom alarm (with a hyperlink to more information).

Cleared correlated alarms are displayed in the **Cleared Alarms** tab. Like uncleared alarms, the **Correlation Type** column will identify it as a cleared root cause or symptom alarm.

Get Troubleshooting and Detailed Alarm Information

- [View an Alarm's Details, on page 13](#)

- [Find Troubleshooting Information for an Active Alarm](#), on page 13
- [Find Out Which Events Are Associated With An Alarm](#), on page 14
- [Find Out If An Alarm Impacts Other Services or Network Elements](#), on page 14

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). The circled areas are explained in the table that follows this figure.

The screenshot displays the 'View an Alarm's Details' interface. At the top, a table lists alarm details with columns: Severity, Message, Status, Failure Source, Timestamp, Owner, Category, and Condition. Below this, the details are organized into five main sections, each highlighted with a red circle:

- General Information:** Includes fields for Source (10.56.23.16), Acknowledged (No), Category (Routers), Alarm Found At (February 25, 2015 4:40:57 AM EST), Alarm Last Updated At (February 25, 2015 7:17:50 AM EST), Alarm Detected Through (Carrier Ethernet), Severity (Major), and Previous Severity (Major).
- Device Details:** Includes fields for IP Address (10.56.23.16), Device Name (ASR901-CSG-1-DOMAIN1.cisco.com), Device Type (Cisco ASR 901 10G Series Aggregation Services Routers), Up Time (17 days 16 hrs 20 mins 7 secs), Reachability Status (Reachable), Collection Status (Managed with Errors), Software Version (15.4(3)B), Serial Number (CAT1651U0SL), Location, and Contact.
- Messages:** Displays a message: 'Device ASR901-CSG-1-DOMAIN1.cisco.com: Pseudowire tunnel with Local IP '50.1.20.23', Pwld '112', and Remote IP '8.8.8.8' is down'.
- Impacted Circuits/VCs:** Shows a table with columns: Alarms, Name, Type, Date Created, Last Modified, Custo..., Status, and Sta. The table contains one entry: 'EvcLink_E...' with Type 'EVC'.
- Device Events:** Shows a table with columns: Severity, Description, Source, and Timestamp. It currently displays 'No data available'.

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 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.



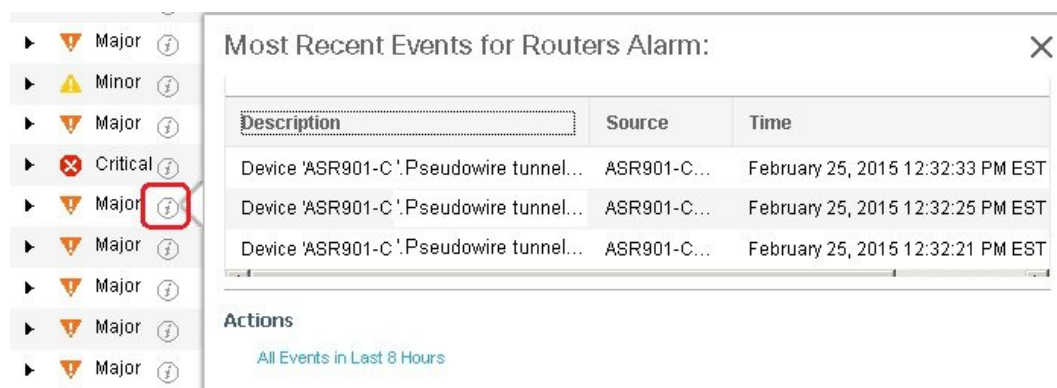
Note

Not all alarms have this information. Users with sufficient privileges can add or change the information that is displayed in the popup window. See [Customize the Troubleshooting Text for an Alarm](#).

- 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 **Condition** 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.



The screenshot shows a list of alarms on the left and a popup window titled "Most Recent Events for Routers Alarm:". The popup contains a table with three columns: Description, Source, and Time. Below the table is an "Actions" section with a link "All Events in Last 8 Hours".

Description	Source	Time
Device 'ASR901-C'.Pseudowire tunnel...	ASR901-C...	February 25, 2015 12:32:33 PM EST
Device 'ASR901-C'.Pseudowire tunnel...	ASR901-C...	February 25, 2015 12:32:25 PM EST
Device 'ASR901-C'.Pseudowire tunnel...	ASR901-C...	February 25, 2015 12:32:21 PM EST

Actions
[All Events in Last 8 Hours](#)

Find Out If An Alarm Impacts Other Services or Network Elements

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



Note Service-affecting information is displayed for optical devices only.

- 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.

The Alarms table also contains a **Correlation Type** column which tells you if the alarm is causing other alarms (Root Cause Alarm), or if the alarm is a symptom of another alarm (Symptom Alarm). For more information, see [View Root Cause and Correlated Alarms, on page 12](#).

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 > 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, 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.
-

What are the Supported Alarm Clearing Mechanisms

At times you may face a situation where there are so many alarms that are available irrespective of their events being cleared. If you encounter any such problems, here are some of the solutions supported in Cisco EPN Manager .

- **Default clearing of alarms**—The fault is resolved on the device and an event is triggered for the same. For example, a device-reachable event clears the device-unreachable event. This in-turn, clears the device-unreachable alarm.
- **Auto-clearing of alarms**—In some cases, a device may not generate a clearing alarm. In such cases, Cisco EPN Manager waits for 24 hours (default interval) and then auto-clears the alarm. You need to have administrator privileges to change the auto-clear duration and to know how to set that interval, see [Change Alarm Auto-Clear Intervals](#) .
- **Clearing alarms based on inventory status of ports**—When a device is rebooted, a card is reloaded or a RSP failover happens, the inventory collection is triggered for that device. During this inventory synchronisation, Cisco EPN Manager clears several types of alarms located on some specific ports based on the operational status of that particular port of the device. For example, when Cisco EPN Manager receives a Link Down trap from a device, it generates a Link Down alarm on the specific port since it is operationally down. After a device reboot, if the operational status of the port changes to up, then the Link Down alarm is cleared automatically by Cisco EPN Manager .
- **Syncing device to clear alarms**—Here, the devices are synced so that Cisco EPN Manager gets the list of the outstanding active alarms and the events that does not exist are cleared. This is a different mechanism when compared to the event based alarm/event reporting (over traps/syslogs). Once the sync is over, the Alarms Table is refreshed to display only the outstanding active alarms.



Note

This feature is supported only for certain devices or for certain device functionalities. For example, this feature is supported for optical devices/optical part of devices (For example, NCS 4K, NCS 1K) and is not supported for packet devices (For example, ASR 9K, 9xx, 42xx, 4K).

- **Manual clearing of alarms**—In situations where the clearing event is missing, you can manually clear an alarm by choosing the particular alarm, and changing its status to Clear. For more information, see the **Cleared** section under [Acknowledge and Clear Alarms, on page 15](#).

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, Cisco EPN Manager adds your user name and the annotation time stamp to the Messages area of the alarm details.

Forward Alarms and Events as Email Notifications

You can configure Cisco EPN Manager to send email notifications for alarms and events. You can specify the severity for which you want to be notified, and the notification email destinations. The settings for the email subject line and body of the email are controlled globally by the administrator; you cannot adjust them.

-
- Step 1** Choose **Monitor > Monitoring Tools > Alarms and Events**.
- Step 2** Click **Email Notification**.
- Step 3** Configure the email notification contents.
- In the **Enable** column, select the check box for the alarm you want to include in the notification.
 - Click the alarm name hyperlink and do the following:
 - Select the severity levels for which you want a notification to be sent.
 - Enter the email addresses in the **To** field.
- Step 4** Click **Save**.
-

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 Cisco EPN Manager 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, Cisco EPN Manager 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 Cisco EPN Manager should do when the threshold is surpassed, choose an alarm value from the parameter's drop-down list. You can configure Cisco EPN Manager 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.
-

View Events (Including Generic Events)

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?](#), on page 2. 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](#)). If desired, you can customize the information displayed by generic events; see [Customize Generic Events That Are Displayed in the Web GUI](#). For information about supported events, see [Which Events Are Supported?](#), on page 5.

Generic event processing is disabled by default. Users with Administrator privileges can disable or re-enable it.

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 9. The following table lists some of the ways you can filter events.

To find these events:	Select Monitor > Monitoring Tools > Alarms and Events , click the Events tab, and:
All events in the network	Click the Show All hyperlink
Latest 4,000 Events	Click the Show Latest 4000 Events hyperlink
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
Events using customized filters	Create and save an advanced filter (see Find and View Alarms , on page 9)

View Syslogs (Historic)



Cisco EPN Manager logs all syslogs from severity 0 through 7 (emergency through debugging messages) generated by all devices that are managed by Cisco EPN Manager. Syslogs from devices that are not managed are not logged or displayed. Cisco EPN Manager also logs all SNMP messages.

Cisco EPN Manager stores a maximum of 2,000,000 syslogs with the following display limits:

- Live syslog streaming—Latest 2,000 syslogs. For more information on live syslogs, see [View Live Syslogs](#), on page 19.
- Historic syslogs—Maximum of 200,000 syslogs.

Step 1 Choose **Monitor > Monitoring Tools > Alarms and Events**. Click the **Syslogs** tab.

You can also view the historic syslogs in the **Historic** tab in **Monitor > Monitoring Tools > Syslog Viewer**.


- Step 2** Click **Custom Syslog Events** to enable Cisco EPN Manager to create events for particular syslogs. You can specify a syslog message identifier, event severity and message to use when the specified syslog is received. Cisco EPN Manager creates an event with the settings you specify.
- Also, if there is an existing syslog for which you want to create an event, select the syslog, then click **Custom Syslog Events**.
- Step 3** Click **Add**. Complete the required fields. If you selected an existing syslog in Step 2, the Message Type and Event Message fields are pre-populated with the values of the syslog you selected.
- You can edit or delete the customized event that was created.
- Step 4** 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.
- Step 5** To export the 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 6** Click **Export**. The first 100000 records will be exported.
- Step 7** Click  to open a Support Case. See [Open a Cisco Support Case](#).

View Live Syslogs

Cisco EPN Manager displays the live streaming of syslogs in **Monitor > Monitoring Tools > Syslog Viewer**.



Note However, this view is not recommended as it has a limitation of only 10 devices. Instead, you can view syslogs (historic) in the **Syslogs** tab in **Monitor > Monitoring Tools > Alarms and Events**. See [View Syslogs \(Historic\)](#), on page 18.

- Step 1** Choose **Live** tab in the Syslog Viewer page.
- Step 2** Use the filters to locate different syslogs. You can enter regular expressions in the fields; for example: `^Auth,V|violation|$,^Sec*V|violation$`
- Step 3** If the data is excessive, click the Pause icon. You can click the Resume arrow at any time.
- Step 4** If you do not want to see duplicates of a syslog, click **De-duplicate**. Cisco EPN Manager will aggregate the syslogs of that type into one line item and display the count in the **Count** field.
- Step 5** To view older syslogs (syslogs that were received before you clicked the **Live** tab), click the **Historic** tab. See [View Syslogs \(Historic\)](#), on page 18.
- Step 6** To export the live 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 7** Click **Export**. The first 100000 records will be exported.



Step 8 Click  to open a Support Case. See [Open a Cisco Support Case](#).


Export Alarms or Events to a CSV or PDF File

Use this procedure to save alarms or events 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** or **Cleared Alarms** tab.
- Events—Choose **Monitor > Monitoring Tools > Alarms and Events**, then click the **Events** 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.

To export the events for a particular alarm, in the **Alarms** tab, hover the mouse over the "i" icon next to the particular alarm. In the pop-up window that opens, click  at the top right corner to perform the export operation.

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 Cisco EPN Manager to open a support request (click an alarm, then choose **Troubleshoot > Support Case**).

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 [Troubleshoot Server Internal SNMP Traps](#).