Fault Management Administration Tasks

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 at the top right of the Cisco EPN Manager window, then choose **Help** > **API Help**.

Event Receiving, Forwarding, and Notifications

Cisco EPN Manager processes syslogs and SNMPv1, v2, and v3 traps that it receives from devices. The server automatically listens for these events on UDP port 162. You do not have to perform any event listening configuration on the server, but you do have to configure devices to forward traps and syslogs to Cisco EPN Manager on the appropriate port.

Notifications are forwarded in SNMPv2 or SNMPv3 format. They are also forwarded to email recipients when you setup corresponding Notification Policies. If you are adding a notification receiver with the notification type UDP, the receiver you add should be listening to UDP on the same port on which it is

configured. Only INFO level events are processed for the selected category and alarms are processed with critical, major, minor and warning levels.

Cisco EPN Manager can forward alarms and events that are generated by the processing of received syslogs, traps, and TL/1 alarms to northbound notification receivers. Alarms of any severity can be forwarded, but only events with INFO severity can be forwarded. Information can be forwarded in :

- E-Mail format. See Configure Default Settings for E-Mail Notifications, on page 3
- SNMP trap format. See Forward Alarms and Events as SNMP Trap Notifications, on page 4

You can also use the SNMP trap notification mechanism to forward SNMP traps that indicate server problems.

Alerts and events are sent as SNMPv2.

Forward Alarms and Events as Email Notifications (Administrator Procedure)

When you configure an e-mail notification, e-mail is sent to the configured receivers when an alarm matching the criteria is created or updated. By default, the subject line includes the alarm severity and category. These settings, along with the message mode, are controlled from the system settings page for alarms and events. For more information, see Configure Default Settings for E-Mail Notifications, on page 3.

If you want to forward generic (unsupported) events, make sure generic event handling is enabled. (To check the setting, see Disable and Enable Generic Trap and Syslog Handling, on page 8.)

You can also forward alarms and events as SNMP trap notifications. For more information, see Forward Alarms and Events as SNMP Trap Notifications, on page 4.

Users can also configure email notifications from the Alarms and Events page. Users are allowed to pick the event and severity, and specific a receiver's email address.

Before You Begin

If you have not configured the mail server, perform the instructions in Set Up the SMTP E-Mail Server. Otherwise notifications will not be sent.

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **Mail and Notification** > **Mail Server Configuration**.

Step 2 In the **Sender and Receivers** area, add the receivers. You can specify multiple recipients as a comma-separated list.

To forward alarms from specific categories to:	Do the following :

The same receivers	1 Enter the receiver(s) in the **To** field. Specify multiple receivers in a comma-separated list. 2 Click the **Configure email notification for individual alarm categories** hyperlink and specify the data for the notification: • Choose the alarms you want to include. **Note** If you are forwarding server internal SNMP traps, choose the **System** category. • To specify alarms of specific severities, click the alarm name hyperlink, then choose the severities. **Note** Do *not* enter any receiver e-mail addresses when you specific the alarm severities. 3 Click **Save** to save the alarm categories and their settings.
To different receivers	1 Do *not* enter any e-mail addresses in the **To** field. 2 Click the **Configure email notification for individual alarm categories** hyperlink. **Note** If you are forwarding server internal SNMP traps, choose the **System** category. 3 Select the alarms in which you are interested. You can specify the severities by clicking the alarm link and choosing **Critical**, **Major**, **Minor**, or **Warning**. **Note** If you are forwarding server internal SNMP traps, choose the **System** category. 4 Click **Save** to save the alarm categories and their settings.

Step 3 Click **Test**. to send a test email using the parameters you configured. The results of the test operation appear on the same page. The test feature checks connectivity to both primary and secondary mail servers by sending an email with a "Cisco EPN Manager test email" subject line.

Step 4 Click **Save** to save the new notifications.

Configure Default Settings for E-Mail Notifications

If you have not configured the mail server, perform the instructions in Set Up the SMTP E-Mail Server. Otherwise notifications will not be sent.

You can configure certain default settings that are applied across all alarm and event e-mail notifications. These settings can be overwritten when users configure individual notifications and receivers.

By default, the email subject line will include the alarm severity and category. The following settings are also available but are disabled by default.

- Subject line—Include the prior alarm severity or add custom text. Alternatively you can replace all of the subject line with custom text.
- Body of the email—Include custom text, the alarm condition, and a link to the alarm detail page.
- Secure message mode—Enabling this mode masks the IP address and controller name.

To enable, disable, or adjust these settings, choose **Administration** > **Settings** > **System Settings**, then **Alarms and Events** > **Alarms and Events**. Make your changes in the **Alarm Email Options** area.

For information on configuring an e-mail notification, see Forward Alarms and Events as Email Notifications (Administrator Procedure), on page 2.

Forward Alarms and Events as SNMP Trap Notifications

Cisco EPN Manager can forward alarms and events in EPM-NOTIFICATION-MIB format as an SNMPv2c and SNPv3 trap notifications. You can specify:

- A specific alarm or event category, such as **System** for internal server SNMP traps.
- Alarms of a specific severity. Only INFO *events* are forwarded; you cannot specify other severities for events.

Before a notification is sent, Cisco EPN Manager pings the receiver to ensure it can be reached. If it does not respond, an alarm is generated to notify that the device is unreachable.

Note Cisco EPN Manager sends traps to notification receivers on port 162. Do not change this port number.

You can also forward alarms and events as email notifications. For more information, see Forward Alarms and Events as Email Notifications (Administrator Procedure), on page 2.

Step 1 As a user with Admin privileges, choose **Administration** > **Settings** > **System Settings**, then choose **Alarms and Events** > **Notification Receivers.**

Step 2 Select **Add Notification Receiver** from the **Select a command** drop-down list, then click **Go**.

Step 3 Configure the new notification receiver.

a) Provide the IP address and server name.

- **IP Address—**Enter the IPv4 or IPv6 address of the server on which the receiver will run.
- **Server Name—**Enter the host name of the server on which the receiver will run.

b) Click the **North Bound** radio button. The notification type defaults to UDP.

c) Enter the port number and SNMP version. The receiver that you configure should be listening to UDP on the same port that is configured.

Note Do not change the port number.

- For SNMPv2c, enter the community string.
- For SNMPv3, enter the username and password (the Engine ID is auto-populated), then select a mode from the Mode drop-down list (depending on the security level).

Step 4 Specify the category and (for alarms) severity of the alarms and events you want to forward.

Note Generic events will only be forwarded if generic event handling is enabled. To check the setting, see Disable and Enable Generic Trap and Syslog Handling, on page 8.

- Under **Category**, check all alarm types to be forwarded. If you are forwarding server internal SNMP traps, choose **System**.
- Under **Severity**, select the highest Severity Level that you set when you configured the trap notifications themselves.

Step 5 When you are finished, click **Save**.

Configure Global Display and Search Settings for Acknowledged, Cleared, and Assigned Alarms

The following table lists some display options for acknowledged, cleared, and assigned alarms. These settings *cannot* be adjusted by individual users (in their display preferences) because, for very large systems, a user could make a change that will impact system performance.

Other settings shown on the Alarms and Events page can be adjusted by users, but you can set the global defaults here. For information on those settings, see these topics:

- Configure Default Settings for E-Mail Notifications, on page 3
- Alarm, Event, and Syslog Purging

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **Alarms and Events** > **Alarms and Events**.

Step 2 Under the Alarm Display Options area, enable or disable these settings, as desired:

Alarm Display Options	Description	Does setting also affect search results?
Hide acknowledged alarms	Do not display Acknowledged alarms in the Alarms list or include them in search results	Yes
Hide assigned alarms	Do not display assigned alarms in the Alarms list or in search results	Yes
Hide cleared alarms in alarm browser	Do not display cleared alarms in the Alarms list or in search results **Note** Cleared alarms remain viewable under the **Cleared Alarms** tab.	No
Add device name to alarm messages	Include device name in e-mail notifications	No

Step 3 To apply your changes, click **Save** at the bottom of the Alarms and Events window.

Change Event Severity Levels

Each alarm in Cisco EPN Manager has a severity. The alarm severity is determined by the most severe event associated to the alarm. You can adjust the severity for alarms by changing the severity for newly-generated events.

Note For alarms that are related to Cisco EPN Manager system administration, such as high availability, refer to Customize Server Internal SNMP Traps and Forward the Traps.

You can change the severity level for network- and device-level alarms in two ways:

- Threshold-crossing alarms generated by optical, Carrier Ethernet, device health, or interface health monitoring policies—Change the settings in the relevant monitoring policy. See Change Thresholds and Alarm Behavior for a Monitoring Policy .
- Specific alarms—Use the procedure in this section.

Step 1 Choose **Administration** > **System Settings**, then choose **Alarms and Events** > **Alarm Severity and Auto Clear**.

Step 2 Expand the categories available under the **Event Types** column, or search for the event type you want by entering all or part of the event text in the **Event Types** search field just below the column heading.

Step 3 Select the events and set their new severity.

1. Check the event's check box.
2. Choose a severity level from the **Severity** drop-down list or , then click **Save**.

Customize the Troubleshooting Text for an Alarm

You can associate troubleshooting and explanatory information with an alarm so that users with access to the Alarms and Events tables will be able to see it. Use this procedure to add or change the information that is displayed in the popup window.

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **Alarms and Events** > **Alarm Severity and Auto Clear**.

Step 2 Select and alarm, then click **Recommended Action**.

Step 3 Add or change the content in the **Explanation** and **Recommended Actions** fields, then click **Save**. To revert to the default text, click **Reset** and **Save**.

Change Alarm Auto-Clear Intervals

You can configure an alarm to auto-clear after a specific period of time. This is helpful in cases, for example, where there is no clearing event. Auto-clearing an alarm will not change the severity of the alarm's correlated events.

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **Alarms and Events** > **Alarm Severity and Auto Clear**.

Step 2 Expand the categories available under the **Event Types** column, or search for the event type you want by entering all or part of the event text in the **Event Types** search field just below the column heading.

Step 3 To change the auto-clear duration for an event or group of events:

- For a single event, check the event's check box, click in the **Auto Clear Duration** field, enter the new duration, then click **Save**.
- For multiple events, select the events, then click **Alarm Auto Clear**, enter the new duration in the dialog box, then click **OK**.

Step 4 Change the Auto Clear Interval by performing one of the following tasks:

- Click on the **Auto Clear Duration** field, enter the new interval, and click **Save**.
- Select the check box of the event type, click **Alarm Auto Clear**, enter the new interval, and click **OK**.

Change the Information Displayed in the Failure Source for Alarms

When an alarm is generated, it includes information about the source of the failure. Information is presented using a specific format. For example, performance failures use the format *MACAddress*:*SlotID*. Failure sources for other alarms may include the host name, IP address, or other properties. Adjust the properties and separators (a colon, dash, or number sign) that are displayed in the alarm's failure source using the following procedure.

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **Alarms and Events** > **Alarms and Events**.

Step 2 In the Failure Source Pattern area, select the alarm category you want to customize.

Step 3 Adjust the failure source format as follows:

- To customize the *properties* that are displayed, click **Edit**, select the properties, then click **OK**. If a property is greyed-out, you cannot remove it.
- To customize the *separators* that are displayed between the properties, click **Edit Separator**.

Step 4 To apply your changes, click **Save** at the bottom of the Alarms and Events settings window.

Change the Behavior of Expedited Events

By default, when Cisco EPN Manager receives a configuration change event from a device, it waits 10 minutes before starting inventory collection in case other related events are sent. This prevents multiple collection processes from running at the same time. This is called the *inventory collection hold off time* and is set to 10 minutes by default. This setting is controlled from the Inventory system settings page (**Administration > Settings > System Settings** > **Inventory**).

Expedited events are handled differently. Although they use the same hold off time mechanism, expedited events use the value set in a rules file rather than the value set in the web GUI. The rules file also instructs Cisco EPN Manager whether to perform an inventory collection only on specific parts of the network element, or on the whole NE.

Cisco EPN Manager has multiple rules file that are stored in /opt/CSCOlumos/conf/fault/correlationEngine. Expedited event settings are controlled by the files that end in the string **EventBasedInventoryRules.xml**.

You can make the following changes to expedited events by editing a rules file.

- Adjust the hold off timer for a specific event by changing the following setting in the rules file:
  `<property name="holdoffTime" value="mins">`

  mins indicates the number of minutes Cisco EPN Manager should wait before performing any other actions in response to the even. The value of *mins* must be set to a minimum of **1** (minute).

- Reconfigure an event to be normal, rather than expedited, by removing the event from the rules file.

You do not have to restart Cisco EPN Manager after editing the rules file. The change takes effect from when you save the rules file.

Customize Generic Events That Are Displayed in the Web GUI

You can customize the description and severity for generic events generated by SNMP traps and syslogs. Your customization will be displayed in the Events tab for SNMP trap events. If a MIB module is not loaded, you can load it manually and then customize the notifications provided in that MIB.

See Customize Generic Events Based on SNMP Traps, on page 9, for information on how to customize these generic events.

Disable and Enable Generic Trap and Syslog Handling

By default Cisco EPN Manager does not drop any received syslogs or traps. As mentioned in How are Alarms and Events Created and Updated?, Cisco EPN Manager maintains an event catalog that determines whether Cisco EPN Manager should create a new event for incoming syslogs or traps (and if it creates a new event, whether it should also create an alarm). If Cisco EPN Manager does not create an event, the trap or syslog is considered a *generic event* .

By default, Cisco EPN Manager does the following:

- Displays the generic events in the Events list.
- Forwards generic events in e-mail or SNMP trap notifications, after normalizing them using the CISCO-EPM-NOTIFICATION-MIB.

All of these events are assigned the INFO severity, regardless of the trap contents, and fall under the alarm category Generic.

Disable and Enable Generic Trap Processing

Use the genericTrap.sh command to manage generic syslogs.

To do the following:	Use this command:
Turn off generic trap processing	**/opt/CSCOlumos/bin/genericTrap.sh -l**
Turn on generic trap processing	**/opt/CSCOlumos/bin/genericTrap.sh -u**

Disable and Enable Generic Syslog Processing

Use the genericSyslog.sh command to manage generic syslogs.

To do the following:	Use this command:
Turn off generic syslog processing	**/opt/CSCOlumos/bin/genericSyslog.sh -l**
Turn on generic syslog processing	**/opt/CSCOlumos/bin/genericSyslog.sh -u**

Customize Generic Events Based on SNMP Traps

Cisco EPN Manager supports the customized representation of generic events in the GUI. Managed objects normally generate SNMP traps and notifications that contain an SNMP trap object identifier (SnmpTrapOID) and a variable bind object identifier (VarBindOIDs) in numerical format. Cisco EPN Manager translates the numeric SnmpTrapOIDs and VarBindOIDs into meaningful names using customized MIB modules, then displays the generic events in the web GUI (in the event tables, Device 360 view, and so forth). For more details on Generic Events see How are Alarms and Events Created and Updated?.

Using the SNMP MIB files that are packaged with Cisco EPN Manager , you can customize the defined MIBs for your deployment's technology requirement.

The following table illustrates how ObjectIDs are decoded and displayed in the GUI.

Table 1: Example: ObjectID Representation

OIDs before Decoding	OIDs after Decoding
`snmpTrapOID = 1.3.6.1.4.1.9.10.120.0.1', Values: 1.3.6.1.4.1.9.10.119.1.1.2.1.11.7.1=1`	`mplsL3VpnVrfDown, values: mplsL3VpnVrfOperStatus.("vrf1").(1) = 1`

Follow the steps below to create customized generic events.

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

Step 2 Click the **Events** tab.

Step 3 Click **Custom Trap Events** and then click **Upload New Mibs**.

Step 4 In the **Upload Mib** window, click **Upload New MIB** to upload a MIB file.

Step 5 If you upload a new MIB file, wait until the file upload is complete, and then click **Refresh MIBs** to have the newly added MIB included in the **MIB** drop-down list.

Step 6 Click **OK**.

Note

Cisco EPN Manager creates a new event type and alarm condition for the specified trap.

Troubleshoot Fault Processing Errors

If your deployment is having fault processing problems, follow this procedure to check the fault logs.

Step 1 Log in to Cisco EPN Manager with a user ID that has Administrator privileges.

Step 2 Select **Administration** > **Settings** > **Logging**, then choose **General Logging Options**.

Step 3 In the **Download Log File** area, click **Download**.

Step 4 Compare the activity recorded in these log files with the activity you are seeing in your management application:

console.log

ncs-x-x.log

decap.core.java.log

xmp_correlation.log

decap.processor.log

What to Do Next

You can also get help from the Cisco support community. If you do need to open a support case, attach the suspect log files with your case. See Get Help from the Cisco Support Community and Technical Assistance Center (TAC), on page 11.

Get Help from the Cisco Support Community and Technical Assistance Center (TAC)

Open a Cisco Support Case

When you open a support case from the web GUI, Cisco EPN Manager automatically populates the case form with information it can retrieve from a device. This includes technical details about the device, configuration changes on the device, and all device events that occurred in the last 24 hours. You can also attach your own files to the case.

Before You Begin

You can open a support case from the web GUI if:

- Your administrator has configured Cisco EPN Manager to allow you to do so. See Set Up Defaults for Cisco Support Requests.
- The Cisco EPN Manager server has a direct connection to the internet, or a connection by way of a proxy server.
- You have a Cisco.com username and password.

Step 1 Choose one of the following:

- From **Monitor** > **Monitoring Tools** > **Alarms and Events**. Click a single alarm, then choose **Troubleshoot** > **Support Case**. If you do not see the **Troubleshoot** button, widen your browser window.
- From the Device 360 view. Hover your mouse cursor over a device IP address, then click the information icon. Choose **Support Request** from the **Actions** drop-down menu.

Step 2 Enter your Cisco.com username and password.

Step 3 Click **Create**. Cisco EPN Manager populates the form with data it retrieves from the device.

Step 4 (Optional) Enter a Tracking Number that corresponds to your own organization's trouble ticket system.

Step 5 Click **Next** and enter a description of the problem.
Cisco EPN Manager populates the form with data it retrieves from the device and automatically generates the necessary supporting documents.

If desired, upload files from your local machine.

Step 6 Click **Create Service Request**.

Join the Cisco Support Community

You can access and participate in discussion forums in the online Cisco Support Community. You will need a Cisco.com username and password.

Step 1 Choose one of the following:

- From **Monitor > Monitoring Tools > Monitoring Tools > Alarms and Events**. Click a single alarm, then choose **Troubleshoot > Support Forum**. If you do not see the **Troubleshoot** button, widen your browser window.
- From the Device 360 view. Hover your mouse cursor over a device IP address, then click the information icon. Choose **Support Community** from the **Actions** drop-down menu.

Step 2 In the Cisco Support Community Forum page, enter your search parameters to find what you need.