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 receiver. 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 8
- SNMP trap format. See Forward Alarms and Events as SNMP Trap Notifications, on page 8

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

Alerts and events are sent as SNMPv2.

User Roles and Access Permissions for Configuring Alarm Notification Settings

This table describes the user roles and access permissions for configuring notification destination and creating customized notification policies.

Note Ensure that you enable the following Task Permissions for any user roles to view, create, and edit notification destination and notification policy:

- Notification Policies Read-Write Access under Alerts and Events
- Virtual Domains List

For more information, see View and Change the Tasks a User Can Perform.

User Role	Access Permission
Root user with root domain	View, create, delete and edit notification destination and notification policy.
Root user with non-root domain	View notification destination and notification policy.
Admin user with root domain	View, create, delete and edit notification destination and notification policy.
Super user with root domain	View, create, delete and edit notification destination and alarm notification policy.
System monitoring user with root domain	View notification destination and notification policy.
Config manager with root domain	View notification destination and notification policy.
Admin user with non-root domain	View notification destination and notification policy created under their respective virtual domain.
Super user with non-root domain	View notification destination and notification policy created under their respective virtual domain.
System monitoring user with non-root domain	View notification destination and notification policy created under their respective virtual domain.

User Role	Access Permission
Config manager with non-root domain	View notification destination and notification policy created under their respective virtual domain.

Points to Remember While Adding a New Notification Policy

The following table lists few points you must remember when adding a new notification policy.

Category selected under Notification Policy Page	Points to Remember
Email	• Each virtual domain must have a unique Contact Name and email address (email recipient). • Email recipients can be added, modified, and deleted only from the ROOT-DOMAIN. • Same email address can be associated with multiple virtual domains. • Cisco EPN Manager does not use the Telephone Number, Cell Number, and Postal Address details for sending alarm notifications.
Trap Receiver	• Contact Name is unique for each trap receiver. • Trap receivers can be added, modified, and deleted only from the ROOT-DOMAIN. Trap receivers are applicable only in ROOT-DOMAIN. • Only North Bound trap receivers can receive alarms/events forwarded from the Notification Policy engine. • Guest-Access trap receivers will receive only alarms related to guest clients.

Category selected under Notification Policy Page	Points to Remember
Notification Policy	• Each notification policy consists of following criteria: alarm categories, alarm severities, alarm types, device groups, notification destinations, and time range.
	• Each notification policy is associated with a unique virtual domain.
	• While selecting the required conditions, you can drill down the tree view drop-down list and select the individual categories (for example, Switches and Routers) and the severity (for example, Major). You can further select the specific Alarm types (for example, link down).
	• Alarms that match the criteria in a policy are forwarded to the respective notification destinations.
	• If an alarm is matched against multiple policies in the same virtual domains and these policies have the same destinations, only one notification is sent to each destination.
	• If the virtual domain associated with a notification policy is deleted, no alarm will match this policy. Though, this notification policy will be listed in the main Notification Policy page, you cannot modify or view the details of this notification policy. However, you can delete this policy.
	• If one or more device groups specified in a policy is deleted, no alarm will match this policy. Though, this notification policy will be listed in the main Notification Policy page, you cannot modify or view the details of this notification policy. However, you can delete this policy.
	• Alarms that are suppressed due to an existing alarm policy will not be forwarded to the notification destinations.
	• If a notification policy that includes both system and non-system category alarms in the rule criteria, you must select the device group(s) for the non-system category alarms.
	• The alarms generated in the specified duration alone are sent to the notification destination. For example, if you specify the duration as 8:00 to 17:00, the alarms will be notified from 8.00 a.m. to 5.00 p.m.

Configure Alarms Notification Destination

You can configure the email notification and Northbound trap receiver settings to notify the alarms generated by Cisco EPN Manager.

Step 1 Choose **Administration** > **Settings** > **System Settings** > **Mail and Notification** > **Notification Destination**.

Step 2 Click the **Add** icon to create a new notification destination.

Step 3 To configure Email Destination, do the following:

a) From the **Select Contact Type** drop-down list, choose **Email**.

b) Enter the **Contact Name** in the text box.

c) Enter a valid email ID in the **Email To** text box.
The email is sent to the email ID entered in the **Email To** field.

d) Enter the **Contact Full Name**.

e) Choose the virtual domain from the **Virtual Domain** drop-down list.

f) Enter the **Telephone Number**, **Mobile Number**, and **Postal Address**.

g) Click **Save**.

Step 4 To configure a Northbound trap receiver using IP Address, do the following:

a) From the **Select Contact Type**, choose **Northbound Trap Receiver**.

b) Select the **IP Address** radio button and enter the **IP Address** and **Server Name**.

c) Choose the required **Receiver Type** and **Notification Type**.

d) Enter the **Port Number**, and choose the **SNMP Version**.

e) If you choose the **SNMP Version** as **v2c**, enter the **Community** settings as required.

f) If you choose the **SNMP Version** as **v3**, enter the **Username**, **Mode**, **Auth.Type**, **Auth.Password**, **Confirm Auth.Password**, **Privacy Type**, **Privacy Password** and **Confirm Privacy Password**.

g) Click **Save**.

Step 5 To configure a Northbound trap receiver using DNS, do the following:

a) From the **Select Contact Type**, choose **Northbound Trap Receiver**.

b) Select the **DNS** radio button and enter the **DNS Name**.

c) Choose the required **Receiver Type** and **Notification Type**.

d) Enter the **Port Number**, and choose the **SNMP Version**.

e) If you choose the **SNMP Version** as **v2c**, enter the **Community** settings as required.

f) If you choose the **SNMP Version** as **v3**, enter the **Username**, **Mode**, **Auth.Type**, **Auth.Password**, **Confirm Auth.Password**, **Privacy Type**, **Privacy Password** and **Confirm Privacy Password**.

g) Click **Save**.

Note • If you choose the **Receiver Type** as **Guest Access**, Cisco EPN Manager will not forward the alarms to the Northbound trap receiver using the notification policy. The Guest Access receiver receives only guest-client related events. The notification policy uses only Northbound trap receivers. Make sure that you use the same Engine ID and same auth and priv passwords when configuring the external SNMPv3 trap receiver.

• While updating the Notification Destination Trap Receiver, the operational status shows the previous Trap Receiver status until the status is updated by the next polling.

• You can also navigate to Notification Policies page by choosing **Monitor > Monitoring Tools > Alarm Notification Policies**.

• If recipient email id is configured in multiple Notification policies, alarm will be forwarded only once to the email id, when condition matches.

• You will not be allowed to delete Notification Destinations which are associated with Notification Policies.

• Alarms forwarded to NBI will not have fields such as "correlationType", "serviceImpacting" and any "UDF" upon alarm creation. These fields are sent only on the next alarm update.

Customize Alarm Notification Policies

You can add a new alarm notification policy or edit an existing alarm notification policy to send notifications on specific alarms of interest that are generated on particular device groups, to specific recipients: either email recipients or northbound trap receivers or both.

Step 1 Choose **Administration > Settings > System Settings > Alarms and Events> Alarm Notification Policies**. To add a new alarm notification policy, do the following:

a) Click the **Add** icon and choose the required virtual domain in the **Select a Virtual Domain** pop-up window.

Cisco EPN Manager matches the alarms that are received from devices from a virtual domain against the notification policies for the same virtual domain. The system category alarms generated by Cisco EPN Manager can be matched against all the alarm notification policies.

Note For a non-root domain, the alarms from a device will be forwarded only if the device or device group(s) containing the device was added or selected under **Network Devices** tab in virtual domain page.

b) Click **OK**.
The **Notification Policies** wizard appears.

c) Choose the severity, category, and event condition for which the notifications must be triggered. By default all the severity types, categories, and conditions are selected.

d) Click **Next** and choose the device groups for which you want the alarm notifications to be triggered.

The alarm notifications are triggered only for the device groups that you select.

For instance, if you select the **User Defined** device group type, then the alarm notification is triggered for all the configured user defined device groups. Similarly, if you select both the **User Defined** and **Locations** device group types, then the alarm notifications are triggered for all the configured user defined and location device groups.

Select the desired device group type to abstain from receiving insignificant alarm notifications from other device groups.

If you choose only system category alarms in the previous step, a message "Device Groups are not applicable when only 'System' based alarms are selected" is displayed under the **Device Group** tab. However, if you choose a non-system category alarm, you must select at least one device group.

e) Click **Next** and choose the required destination in the **Notification Destination** page.
If you choose root-domain in Step 1-a, all the Email and Northbound trap receiver destinations created in Cisco EPN Manager will be listed in the **Notification Destination** page. If you choose, non-root domain, the Email destinations created under that particular domain will be listed in the **Notification Destination** page. See Configure Alarms Notification Destination, on page 5 .

f) Alternately, choose the **Email** or **Northbound Trap Receiver** option from the Add icon drop-down list and complete the required fields.

g) Choose the notification destination and click **Change Duration**.

h) Choose the **From** and **To** timings in the **Set Duration** pop-up window and click **OK**.
The alarms generated in the specified duration alone are sent to the notification destination.

i) Click **Next** and enter the **Name** and **Description** for the alarm notification policy in the **Summary** page.

j) Click **Save**.

Note   "Interface" is a reserved word and hence don't use it as the name for Alarm Notification Policy.

Step 2   To edit an alarm notification policy, do the following:

a) Choose the policy and click the **Edit** icon.
The **Notification Policies** wizard appears.

b) Choose the **Conditions**, **Device Groups**, and **Destination** as explained in Step 1.

c) Click **Save**.

Convert Old Email and Trap Notification Data to New Alarm Notification Policy

The email and trap notification data created in previous Cisco EPN Manager releases is converted in to new alarm notification policies while upgrading or migrating Cisco EPN Manager from previous release to the latest version.

The migrated alarm notification policies can be viewed in the Alarms and Events Notification Policies pages.

The following Alarm categories are supported in Cisco EPN Manager Release 4.0:

- Change Audit
- Generic
- System
- Application Performance
- Compute Servers
- Nexus VPC switch
- Switches and Routers
- AP
- Adhoc Rogue
- Clients

- Context Aware Notifications

- Controller

- Coverage Hole

- Mesh Links

- Mobility Service

- Performance

- RRM

- Rogue AP

- SE Detected Interferers

- Security

- Third Party AP

- Third Party Controller

The following Alarm categories are not supported in Cisco EPN Manager Release 4.0:

- Autonomous AP

- Cisco UCS Series

- Routers

- Switches and Hubs

- Wireless Controller

To edit the migrated alarm notification polices, see Customize Alarm Notification Policies, on page 6.

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.

See Configure Alarms Notification Destination, on page 5 for more information.

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.

Specify Alarm Clean Up, Display and Email Options

The **Administration > Settings > System Settings > Alarms and Events** page enables you to specify when and how to clean up, display and email alarms.

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

Step 2   Modify the **Alarm and Event Cleanup Options**:

- Delete cleared non-security alarms after—Enter the number of days after which non-security alarms are deleted. Non-security alarms include all alarms that do not fall under the Security, Rogue AP, or Adhoc Rogue categories.

- Delete cleared security alarms after—Enter the number of days after which Security, Rogue AP, and Adhoc Rogue alarms are deleted.

- Delete all (active & cleared) alarms after—Enter the number of days after which active and cleared alarms are deleted.

- Delete all events after—Enter the number of days after which all the events are deleted.

The maximum is 8000000 events or the number of days specified, whichever is lower.

Step 3   Modify the **Syslog Cleanup Options**:

- Delete all Syslogs after—Enter the number of days after which all aged syslogs are to be deleted.

- Max Number of Syslog to Keep—Enter the number of Syslogs that needs to be maintained in the database.

Step 4   Modify the **Alarm Display Options** as needed:

- Hide acknowledged alarms—When the check box is selected, Acknowledged alarms do not appear in the Alarm page. This option is enabled by default. Emails are not generated for acknowledged alarms, regardless of severity change.

- Hide assigned alarms—When the check box is selected, assigned alarms do not appear in the Alarm page.

- Hide cleared alarms—When the check box is selected, cleared alarms do not appear in the Alarm page. This option is enabled by default.

- Show only Active Alarms in Alarms tab - When the check box is selected, only Active Alarms appear in the Alarms list under Alarms tab.

- Add device name to alarm messages—Select the check box to add the name of the device to alarm messages.

Changes in these options affect the Alarm page only. Quick searches for alarms for any entity will display all alarms for that entity, regardless of alarm state.

Step 5   Modify the alarm Failure Source Pattern:

- Select the category you need to customize and click **Edit**.

- Select the failure source pattern from the options available and click **OK**.

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

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

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

Step 6   Modify the Alarm Email Options:

- Add Cisco EPN Manager address to email notifications—Select the check box to add the Cisco EPN Manager address to email notifications.

- Include alarm severity in the email subject line—Select the check box to include alarm severity in the email subject line. This option is enabled by default.

- Include alarm Category in the email subject line—Select the check box to include alarm category in the email subject line. This option is enabled by default.

- Include prior alarm severity in the email subject line—Select the check box to include prior alarm severity in the email subject line.

- Include custom text in the email subject line—Select the check box to add custom text in the email subject line. You can also replace the email subject line with custom text by selecting the Replace the email subject line with custom text check box.

- Include custom text in body of email—Select the check box to add custom text in the body of email.

- Include alarm condition in body of email—Select the check box to include alarm condition in the body of email.

- Include alarm application category data in body of email—Select the check box to include alarm category in the body of email.

- Add link to Alarm detail page in body of email—Select the check box to add a link to the Alarm detail page in the body of email.

- Enable Secure Message Mode—Select the check box to enable a secure message mode. If you select the Mask IP Address and Mask Controller Name check boxes, the alarm emails are sent in secure mode where all the IP addresses and controller names are masked.

- Email Send Interval—Specify the time interval in which the email has to be sent.

Note   Cisco EPN Manager sends alarm notification email for the first instance of an alarm and the subsequent notification is sent only if the alarm severity is changed.

Step 7   Modify the **Alarm Other Settings**:

- Controller License Count Threshold - Enter a threshold percentage. An alarm is triggered if the number of access points connected to a controller reaches the specified rate of the licenses available on the controller. For example, if a controller is configured with 100 access point licenses and 80% threshold, an alarm will be triggered when the number of access points connected to a controller exceeds 80.

- Enable AP count threshold alarm - Select the check box to enable the AP count for threshold alarms.

- Controller Access Point Count Threshold - Enter a threshold percentage. An alarm is triggered if the number of access points connected to a controller reaches the specified rate of the maximum number of access points supported by the controller. For example, if a controller supports a maximum of 6000 access points and threshold is configured as 80%, an alarm will be triggered when the number of access points connected to the controller exceeds 4800.

- Suppress Interface Optical SFP TCAs in Admin Down State - Selecting this check box will prevent optical SFP TCAs to be raised for interfaces in Admin Down state.

- Enable Service Impact Analysis - Selecting this check box will enable the service impact analysis.

- Enable creation of subtrees from a correlation tree when root cause of the tree clears - When the root cause of a correlation tree clears, subtrees of this correlation tree are created, where each subtree has an uncleared root cause, Selecting this check box enabled the feature.

- Enable alarms from interface status polling - If this check box is raised, LinkDown alarms will be raised and cleared by polling the interface status of Ethernet and Bundle Interfaces.

- Enable alarm generation based on EPNM inventory collection - EPNM uses inventory status of entities to raise and clear certain alarms. This mechanism acts as a backup for syslogs and traps which may be lost or missing (due to device not generating them, lost in network and other reasons).

- Enable User Defined Field - This setting is disabled by default. You can enable the setting by selecting the checkbox. Alarms that are localized to equipment are considered as Hardware Alarms. If this setting is enabled, PRODUCT_NAME and PRODUCT_ID are conditionally populated for Hardware Alarms in the Alarms list under the **Alarms** tab. This setting does not affect existing alarms and does not apply retrospectively on previously raised alarms.

Step 8   For **Alarm Manager Settings**, see Configure Alarm Manager in Cisco IOS XR Devices, on page 12.

Step 9   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 8

- 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	Do not display cleared alarms in the Alarms list or in search results For example, if there are 3900 cleared alarms out of 4000 alarms, enabling this setting will display 100 uncleared alarms in the Alarms list under **Alarms** > **Showing Active Alarms**. **Note** Cleared alarms remain viewable under the **Cleared Alarms** tab.	No
Show only Active Alarms in Alarms tab	Diplay only Active Alarms in the Alarms list under **Alarms** tab. For example, if there are 3900 cleared alarms out of 4000 alarms, enabling this setting will display the latest 4000 uncleared alarms in the Alarms list under **Alarms** > **Showing Active Alarms**. **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.

Configure Alarm Manager in Cisco IOS XR Devices

As part of reliable alarming, Cisco EPN Manager polls the Alarm Manager in Cisco IOS XR devices for any outstanding alarms or events.

Note   Alarm Manager support is limited to Cisco IOS XR devices NCS 10xx, NCS 40xx and NCS 55xx only.

Follow this procedure to enable or disable the Alarm Manager from Cisco EPN Manager GUI.

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

Step 2   Under **Alarm Manager Settings**, select the device type to enable or disable the Alarm Manager as required.

Note By default, Alarm Manager is enabled for all the device types listed under the **Alarm Manager Settings** area.

Step 3 Click **Save** to apply your changes.

Step 4 Click **Save** at the bottom of the Alarms and Events window.

If the Alarm Manager is enabled, Cisco EPN manager polls the device every 5 minutes. You cannot change this polling interval. All alarms raised by Alarm Manger are displayed in the list under **Alarms** tab in **Monitor** > **Monitoring Tools** > **Alarms and Events** page. You cannot modify the Severity or Clear or Delete the alarms raised by Alarm Manager in this list. The source of the alarm is displayed as "Synthetic_Event" for alarms raised by the Alarm Manager,

If the Alarm Manger is disabled, all the alarms previously raised by Alarm Manager are cleared. Cisco EPN Manager will no longer poll the device but continues to receive alarms directly from the device. All PKT-INFRA-FM alarms will be listed under the **Events** tab in **Monitor** > **Monitoring Tools** > **Alarms and Events** page.

Configure Alarm Resync in Cisco IOS XE Devices

The alarm resync feature, based on the "show facility" command is part of reliable alarming for Cisco IOS XE devices. This feature is supported from software version 16.6.6vS and 16.9.1 in Cisco NCS 42xx devices. You can enable or disable alarm resync by modifying the `/conf/fault/ncs42xx/resources/NCS42xxAlarmManager.properties` file.

When the alarm resync is enabled, the alarms received from the device are displayed under Alarms tab in **Monitor** > **Monitoring Tools** > **Alarms and Events** page. You cannot modify the Severity or Clear or Delete these alarms through Cisco EPN Manager.

Note The alarm resync feature is supported only for DSX, SONET and select system alarms. Refer to Cisco Evolved Programmable Network Manager Supported Syslogs for more information.

The following procedure lists the steps to enable or disable the alarm manager in Cisco NCS 42xx devices.

Step 1 Open a CLI session with the Cisco EPN Manager server. See Connect via CLI for more information.

Step 2 Open the `/conf/fault/ncs42xx/resources/NCS42xxAlarmManager.properties` file.

Step 3 Modify `shfacilityenabled`, `resyncperiodmillis`, and `pollerperiodmillis` as required.

- `shfacilityenabled` - flag to enable or disable Alarm Manager. Setting this flag to true will enable the alarm resync. By default, this value is set to true. System restart is not required when you change this value.

- `resyncperiodmillis` - polling interval to poll the device. You can modify this value as desired. Default value is 600000 milliseconds or 10 minutes. System restart is required for this change to take effect.

- `pollerperiodmillis` - poller which updates the device list to poll for alarm manager. You can modify the value as desired. Default value is 3600000 milliseconds or 1 hour. System restart is required for this change to take effect.

Configure Alarm Profiling in Cisco IOS XE Devices

Cisco EPN Manager supports alarm profiling for Cisco IOS XE devices. Set `alarmprofileEnabled` to `true` for Cisco EPN Manager to reflect the alarm profiling changes. To do this:

Step 1   Open a CLI session with the Cisco EPN Manager server. See Connect via CLI for more information.

Step 2   Open the `/conf/fault/ncs42xx/resources/NCS42xxVersion.properties` file.

Step 3   Set `alarmprofileEnabled` to `true` and save your changes. By default, the `alarmprofileEnabled` is enabled.

      Note   If `alarmprofileEnabled` is set to false, Cisco EPN Manager does not reflect the alarm profiling changes.

Change Alarm 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 **Alarm Condition** column, or search for the Alarm Condition you want by entering all or part of the event text in the **Alarm Condition** search field just below the column heading.

Step 3   Select the events and set their new severity.

      a.   Check the event's check box.

      b.   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**.

   Note   The **Alarm Auto Clear** button is enabled only for the events that do not have an auto-clear event configured.

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

When Cisco EPN Manager receives a configuration change event from a device, it waits for a certain time interval 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**).

The following events are processed by Cisco EPN Manager within the default time interval of 10 minutes:

Type	Supported Events
Link	`LINK-3-UPDOWN`
Card Protection	`CARD_PROTECTION-4-PROTECTION` `CARD_PROTECTION-4-ACTIVE`
VLAN	`PORT_SECURITY-6-VLAN_REMOVED` `PORT_SECURITY-6-VLAN_FULL`

Type	Supported Events

ICCP SM	`L2-L2VPN_ICCP_SM-4-REMOTE_CORE_ISOLATION`
	`L2-L2VPN_ICCP_SM-4-REMOTE_CORE_ISOLATION_CLEAR`
	`L2-L2VPN_ICCP_SM-3-CONFIG_LOCAL_ERROR`
	`L2-L2VPN_ICCP_SM-3-CONFIG_REMOTE_ERROR`
	`L2-L2VPN_ICCP_SM-4-LOCAL_CORE_ISOLATION`
	`L2-L2VPN_ICCP_SM-4-LOCAL_CORE_ISOLATION_CLEAR`
	`L2-L2VPN_ICCP_SM-4-PEER_REACHABILITY_FAILURE`
	`L2-L2VPN_ICCP_SM-4-PEER_REACHABILITY_CLEAR`
	`L2-L2VPN_ICCP_SM-4-REMOTE_ACCESS_MAIN_PORT_FAILURE`
	`L2-L2VPN_ICCP_SM-4-REMOTE_ACCESS_MAIN_PORT_FAILURE_CLEAR`
	`INFRA-ICCP-5-ISOLATION`
	`INFRA-ICCP-5-ISOLATION_CLR`
	`INFRA-ICCP-5-NEIGHBOR_STATE_UP`
	`INFRA-ICCP-5-NEIGHBOR_STATE_DOWN`
	`INFRA-ICCP-6-BACKBONE_INTERFACE_STATE_UP`
	`INFRA-ICCP-6-BACKBONE_INTERFACE_STATE_DOWN`
	`L2-BM-6-ACTIVE_CLEAR`
	`L2-BM-6-ACTIVE_PROBLEM`
	`L2-L2VPN_ICCP_SM-3-CONFIG_INVALID_NODEID`
	`L2-L2VPN_ICCP_SM-3-CONFIG_INVALID_NODEID_CLEAR`

Satellite	`PKT_INFRA-ICPE_GCO-5-SATELLITE_STATUS_PROBLEM` `PKT_INFRA-ICPE_GCO-5-SATELLITE_STATUS_CLEAR`

Cluster	`PLATFORM-REDDRV-7-ROLE_CHANGE`
	`PLATFORM-CE_SWITCH-6-UPDN`
	`PLATFORM-CLUSTER_CLM-6-UPDN`
	`LINK_UP`
	`LINK_DOWN`

Celeborn cards	`UEA_SPA_MODE-6-UEA_SPA_MODE_CHG`
Configuration Commit syslogs	`MGBL-CONFIG-6-DB_COMMIT` `SYS-5-CONFIG_I`

However, in case of the following critical events, Cisco EPN Manager performs a full discovery of the device immediately when the event occurs:

```
SYS-5-RELOAD
SYS-5-RESTART
OIR-6-INSCARD
OIR-SP-6-INSCARD
SWT_CEFC_STATUS_CHANGE
cefcFRURemoved
cefcFRUInserted
```

Granular Inventory Event Flow Controllers

Granular inventory identifies the events generated and processes only the changes made in the devices. To avoid continuous syncing of devices due to event inflow, granular inventory uses Event Burst Flow Controller and Continuous Events Flow Controller.

For a list of events that are monitored/not monitored for burst and continuous modes.

Event Burst Flow Controller

When the number of incoming events for any technology for a managed device is greater than the threshold (BurstThreshold for BurstHoldOffTimer), Cisco EPN Manager considers it as an event burst condition. In this scenario, the granular inventory sync for the events breaching the threshold is held for a certain time period (BurstHoldOffTimer) until the event burst condition is cleared. This condition check is repeated at regular intervals. After the specified number of retries (BurstCheckRetryCount), if the threshold is still breached, Cisco EPN Manager stops all the granular inventory processing for the device.

If the event burst condition is detected and cleared before 3 retries, then the Event Burst Flow Controller triggers feature sync for the corresponding technology. If the event burst condition is detected and continues after 3 retries, then the controller stops all the granular inventory processing, raises the DISABLE_GRANULAR_INVENTORY_EVENT event, and disables the granular inventory for the device.

Table 1: Event Burst Action Properties

Property Name	Description	Default Value
BurstThreshold	The number of events of a given type over a period of time, which is considered as the 'burst' of that event type.	100 (events)
BurstHoldOffTimer	The time period for which the inventory sync is withheld.	300000 ms (5 mins)
BurstCheckRetryCount	The permitted number of retries.	3 (times)

After the granular inventory is disabled, a system check is initiated to monitor the event burst condition for the specific device; this system check will identify if the event burst condition continues. If there is no event burst condition, then it clears DISABLE_GRANULAR_INVENTORY_EVENT, followed by a full sync of the device. The granular inventory processing for the device will resume for any new incoming events.

Note When you enable the granular inventory for the device manually (see Enable or Disable Granular Inventory, on page 19), the corresponding DISABLE_GRANULAR_INVENTORY_EVENT is cleared.

Continuous Events Flow Controller

When the number of incoming events for a managed device is greater than the threshold (contEventsThresholdCount for contEventsCheckPeriod), Cisco EPN Manager considers it as continous events condition. In this scenario, the granular inventory sync for the events breaching the threshold is held for a certain time period (contEventsDropPeriod) until the continous events condition is cleared.

If the continuous events condition is detected, then the Continuous Events Flow Controller stops all the granular inventory processing for the device and raises the INVENTORY_SYNC_SUPPRESSED alarm to indicate that the device is in continuous state. It continues to perform feature sync at regular intervals, for all the events identified, until the continuous events condition is cleared.

Table 2: Continuous Event Action Properties

Property Name	Description	Default value
contEventsThresholdCount	Maximum number of allowed events at a time in the queue.	50 (events)
contEventsCheckPeriod	The time interval in milli-seconds, to check for the incoming event count.	300000 ms (5 mins)
contEventsDropPeriod	Time interval in milli-seconds, to trigger feature sync at regular intervals in case of continuous events.	300000 ms (5 mins)

Enable or Disable Granular Inventory

You can enable or disable granular inventory at the global level from the System Settings page. Choose **Administration** > **Settings** > **System Settings** > **Inventory** > **Inventory**, and then check or uncheck the **Enable Granular Inventory** check box. By default, this setting is enabled.

Note   Disabling granular inventory will stop all the granular inventory processing for all the managed devices.

You can also enable or disable the granular inventory at the device level from the Network Devices page. To disable granular inventory for a device, select the required device in the Network Devices page, and then choose **Admin State** > **Disable Granular Inventory**. This will disable the granular inventory for the selected device only, and will not impact the granular inventory processing of any other devices in the system. To re-enable granular inventory for a device, select the required device in the Network Devices page, and then choose **Admin State** > **Enable Granular Inventory**. You can select one or more devices, and apply these actions. However, in case of multiple device selection, all the selected devices should be in either of the two states. If the selected devices are in mixed states, these options are not enabled.

Note   If the granular inventory is disabled at the global level, then it precedes the granular inventory settings at the device level. If the granular inventory is enabled at the global level, then it succeeds the granular inventory settings at the device level.

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 20, 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 CISCO-EPM-NOTIFICATION-MIB. For more information, refer to the CISCO-EPM-NOTIFICATION-MIB section in the guide.

All of these events are assigned the MINOR 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**

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 3: 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**.

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 21.

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 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 > 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 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.