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 EPN REST API, click at the at the top right of the Cisco EPN Manager window, then choose **EPN REST API**.

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.

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
- SNMP trap format. See Configure SNMP Trap Notifications and Notification Receivers

LIMITED ORDERABILITY RELEASE

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 > Alarms and Events** and make your changes in the Alarm Email Options area.

For information on configuring an e-mail notification, see Configure E-Mail Notifications for Alarms and Events.

Forward Alarms and Events in SNMP Trap Format

You can configure Cisco EPN Manager can forward alarms and events that match your criteria to configured notification receivers in EPM-NOTIFICATION-MIB format as an SNMPv2 trap. Alarms of any severity can be forwarded but only events with INFO severity can be forwarded. Before a notification is sent, Cisco EPN Manager pings the receiver to ensure it can be reached. If it does not respond, the receiver is deleted from the system. For more information, see Configure SNMP Trap Notifications and Notification Receivers.

Configure SNMP Trap Notifications and Notification Receivers

Once you have enabled trap notifications and customized their severities and thresholds, you must configure one or more Notification Receivers to receive the traps.

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

Step 1 As a user with admin privileges, choose **Administration > Settings > System Settings > Notification Receivers**.

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

Step 3 Provide information about the new notification receiver.

Note Do not change the port number.

- 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.

Step 4 Configure the notification filter to control what information is forwarded.

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.

- Under Category, check all alarm types to be forwarded.
- 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 Default Behavior for Alarms and Events

By default, when an alarm is acknowledged or cleared, it is removed from the alarm summary display. The alarm summary display is the page shown when you choose **Monitor > Alarms and Events** and click the Alarms tab. If desired, you can further adjust the following settings.

The following global settings can be configured by choosing **Administration > Settings > System Settings > Alarms and Events**.

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

These global settings are controlled from the User Preference page (**Administration > User Preferences**). Cisco EPN Manager web GUI users can override these settings by adjusting their own user preferences, which they can do by clicking at the top right of the Cisco EPN Manager window.

User Preference Setting	Description
Refresh Map/Alarms page on new alarm	Refreshes the alarms list when a new alarm is generated (enabled by default).
Refresh Alarm count in the Alarm Summary every ___ minutes/seconds	Sets the refresh interval for the alarm count in the Alarm Summary (1 minutes by default) (seeCustomize the Alarm Summary).
Select alarms for Alarm Summary Toolbar	Controls what is displayed in the Alarm Summary (seeCustomize the Alarm Summary).

User Preference Setting	Description
When clearing all alarms of a condition, always set the condition's severity to Information	When user selects and alarm and chooses **Change Status > Clear all of this condition**, changes the severity of all like alarms to Informational (disabled by default).
Disable Alarm Acknowledge Warning Message	**Note** This setting is only configurable if **Hide Acknowledged Alarms** is also enabled; that setting is disabled by default (see the previous table). Disables the following message from displaying when user selects an alarm and chooses **Change Status > Acknowledge**: Warning: This alarm will not be generated, if the original event recurs again, within next 7 days, as it is acknowledged now. Clearing the alarm instead of acknowledging will cause the alarm to be generated if the event recurs again. Proceed with alarm acknowledgment? (Disabled by default)
Disable confirmation prompt for “clear all of this condition”	Disables the following message from displaying when user selects an alarm and chooses **Change Status > Clear all of this condition**: Are you sure you want to clear all alarms of this condition? (Disabled by default)
Disable “Set severity to information” prompt for “clear all of this condition”	Disables the following message which is displayed when user selects an alarm and chooses **Change Status > Clear all of this condition**: Do you want to set the severity for the selected alarm's condition to Information? WARNING: This is a system-wide change that will prevent creation of future alarms of this condition. You can undo this change on the Severity Configuration page under System Settings. (Disabled by default) **Note** You can reset the severity to its original value using the procedure in Configure Global Default Behavior for Alarms and Events.

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 > Logging** and download the log files.

Step 3 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

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).

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

Configure Technical Support Request Settings

You can customize the settings for creating a support case with Cisco Technical Support.

Step 1 Choose **Administration > System Settings > Support Request Settings**.

Step 2 Select the type of interaction you prefer:

- Enable interactions directly from the server—Specify this option to create the support case directly from the Cisco EPN Manager server. E-Mails to the support provider are sent from the e-mail address associated with the Cisco EPN Manager server or the e-mail address you specify.
- Interactions via client system only—Specify this option to download the information required for your support case to a client machine. You must then e-mail the downloaded support case details and information to the support provider.

Step 3 Select your technical support provider:

- Click **Cisco** to open a support case with Cisco Technical Support, then enter your Cisco.com credentials. Click **Test Connectivity** to check the connectivity to the following servers:
  - Cisco EPN Manager mail server
  - Cisco support server
  - Forum server
- Click **Third-party Support Provider** to create a service request with a third-party support provider. You will need to enter the provider's e-mail address, the subject line, and the website URL.

Open a Cisco Support Case

If you have a direct Internet connection on the Cisco EPN Manager server and a Cisco.com user name and password, you can open a support case from the GUI. Cisco EPN Manager automatically populates the case form with information it can retrieve from the 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.

Step 1 Choose one of the following:

- **Monitor > Alarms & Events**, click an alarm, then choose **Troubleshoot > Support Case**.
- From the device ° 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 again populates the form with data it retrieves from the device. It a 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:

- **Monitor > Alarms & Events**, click an alarm, then choose **Troubleshoot > Support Forum**.
- From the device ° 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.