Fault Management Administration Tasks

This section contains the following topics:

Event Receiving, Forwarding, and Notifications

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 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 with the notification type UDP, the 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.

can forward alarms and events that are generated by the processing of received syslogs, traps, and TL/1 alarms to northbound notification .

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 (under Reports)

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.
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 explains you some points you must remember while 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. • Prime Infrastructure 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 Prime Infrastructure.

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**, 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** > **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.

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**> **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 Prime Infrastructure 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 Prime Infrastructure 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 Prime Infrastructure 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**.

Note Notifications will not be sent to email recipient for North Bound trap receiver, if you change the severity of an alarm type from **Monitor** > **Monitoring Tools** > **Alarm Policies**.

Related Topics

Configure Alarms Notification Destination, on page 5

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

The email and trap notification data created in previous releases is converted in to new alarm notification policies while upgrading or migrating 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 Release 3.6:

- 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 Release 3.6:

- Autonomous AP
- Cisco UCS Series
- Routers
- Switches and Hubs
- Wireless Controller

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

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 active and cleared alarms after—Enter the number of days after which active and cleared alarms are deleted.
- Delete cleared security alarms after—Enter the number of days after which Security, Rogue AP, and Adhoc Rogue alarms are deleted.
- 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 all events after—Enter the number of days after which all the events are deleted.
- Max Number of Events to Keep—Enter the number of events that needs to be maintained in the database.

Cisco Prime Infrastructure deletes old alarms and events, as part of normal data cleanup tasks, and checks the storage size of the database alarm table once in every 2 hours, by default. When the alarm table exceeds the 300,000 limit, Prime Infrastructure deletes the oldest cleared alarms until the alarm table size is within the limit. If you want to keep cleared alarms for more than seven days, then you can specify a value more than seven days in the **Delete cleared non-security alarms after** text box, until the alarm table size reaches the limit.

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 Summary page. This option is enabled by default.
- 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 Prime Infrastructure address to email notifications—Select the check box to add the Prime Infrastructure 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 Prime Infrastructure 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.
- 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.

Step 8 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.

-
- 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	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 Severity Levels

Each alarm in 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 system administration, such as high availability, refer to Customize Server Internal SNMP Traps and Forward the Traps.

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

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

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 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 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, 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
```

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 14, for information on how to customize these generic events.

Disable and Enable Generic Trap and Syslog Handling

By default does not drop any received syslogs or traps. maintains an event catalog that determines whether 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 does not create an event, the trap or syslog is considered a *generic event* .

By default, does the following:

- Displays the generic events in the Events list.

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**

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

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. 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).

Using the SNMP MIB files that are packaged with , 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**.

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 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 16.

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, 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 to allow you to do so. .
- The 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**. 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.

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.