



Monitoring System Activity

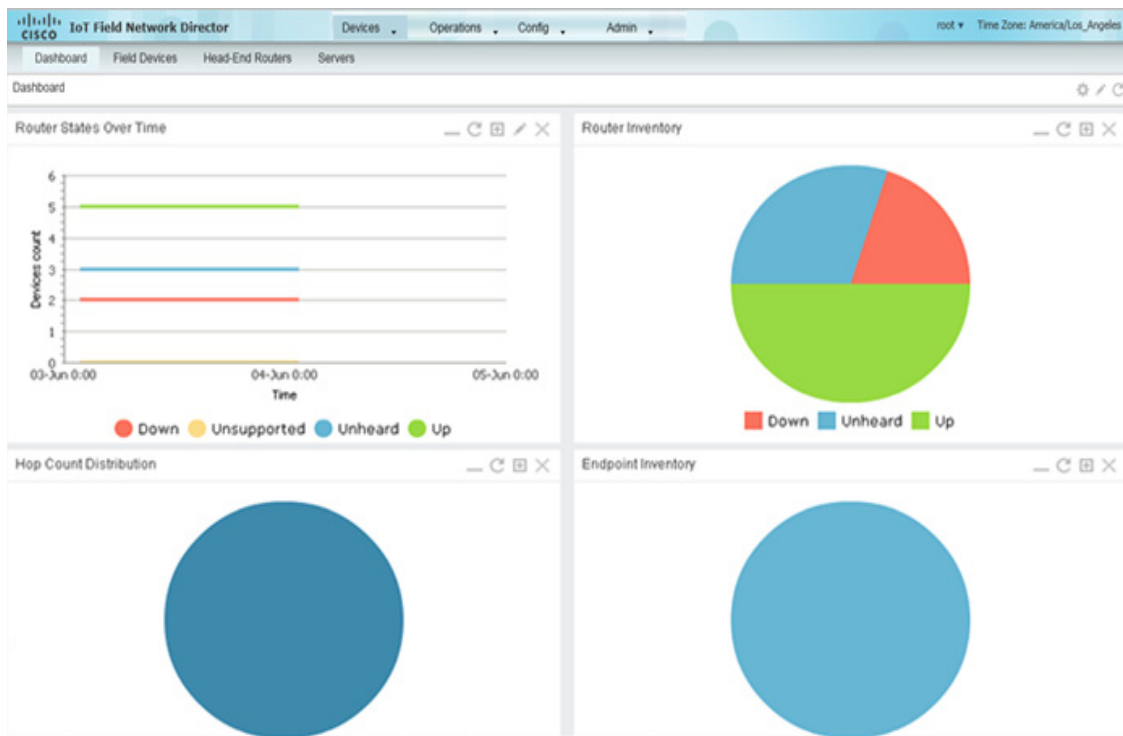
This section describes how to monitor IoT FND system activity, including the following topics:

- [Using the Dashboard](#)
- [Monitoring Events](#)
- [Monitoring Issues](#)
- [Viewing Device Charts](#)

Using the Dashboard

The IoT FND Dashboard ([Figure 1](#)) displays *dashlets* to provide a visual overview of important network metrics.

Figure 1 IoT FND Dashboard



This section describes the following Dashboard features:

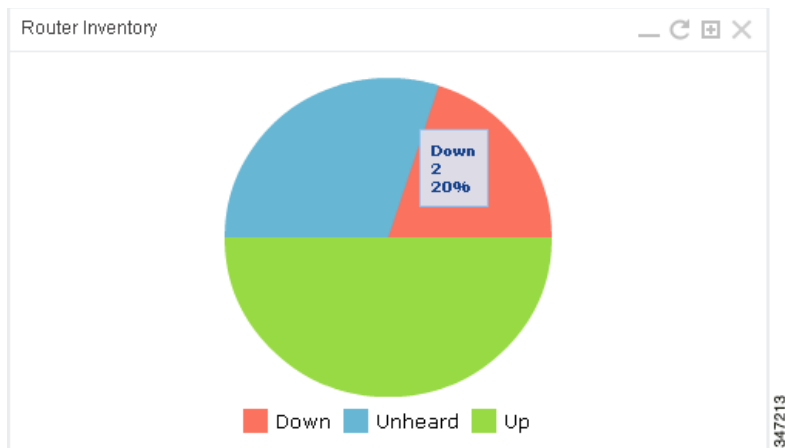
- [Types of Dashlets](#)
- [Repositioning Dashlets](#)
- [Setting the Dashlet Refresh Interval](#)

- [Adding Dashlets](#)
- [Removing Dashlets](#)
- [Exporting Dashlet Data](#)

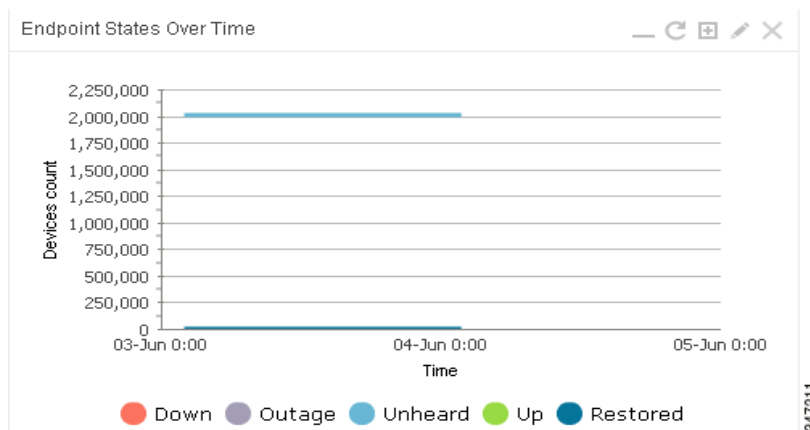
Types of Dashlets

The Dashboard displays two types of dashlets:

- Pie-chart dashlets display a ratio of device properties as a pie chart.



- Line-graph dashlets display graphs that show device counts over time.



Tip: Graphs set to intervals longer than one day may not display the data at the last datapoint exactly as shown in the matching field on the Device Info page. This is because data aggregation is occurring less frequently than polling to update the fields on the Device Info page. Set these graphs to the 6h or 1d intervals to update the data more frequently. Use intervals longer than one day to view data trends.

Dashboard Dashlets

The IoT FND Dashboard dashlets are described below.

Dashlet	Description
Router Inventory	This FAR status counts pie chart displays the status distribution and absolute count of FARs.
Router States Over Time	This line graph shows a count of the FARs and their states for the configured time interval.
Endpoint Inventory	This endpoint status displays the proportion (and count) of endpoints. For example, the count of devices with an Unheard status relative to the other states: Up, Down, and Outage.
Endpoint States Over Time	This line graph shows a count of endpoints and their states for the configured time interval.
Endpoint Config Group Template Mismatch Over Time	This line graph shows the number of endpoints across all configuration groups and particular configuration groups that are out of sync for the configured time interval.
Endpoint Firmware Group Membership Mismatch Over Time	This line graph shows the number of endpoints across all firmware groups and particular firmware groups that are out of sync for the configured time interval.
Config Group Template Mismatch	This pie chart shows the number of devices with matched and mismatched configuration group templates (applicable only to ME configuration groups).
Firmware Group Membership Mismatch	This pie chart shows the number of devices with mismatched firmware groups (applicable only to endpoint firmware groups).
Hop Count Distribution	This pie chart shows the hop count distribution for mesh devices.
Service Providers with Maximum Down Routers for Cellular 1	This dashlet displays the aggregated maximum Down Routers for device types CGR1000, C800 and IR800 for single modem routers.
Service Providers with Maximum Down Routers for Cellular 2	This dashlet will display the aggregated maximum Down Routers for device types CGR1000, C800 and IR800 for dual modem routers.
Service Providers with Maximum Routers	This dashlet shows the service provider names, their associated cell IDs (if available), their associated total router count, and the count of down routers. This dashlet also displays the bandwidth usage and a sparkline showing the down routers over time.

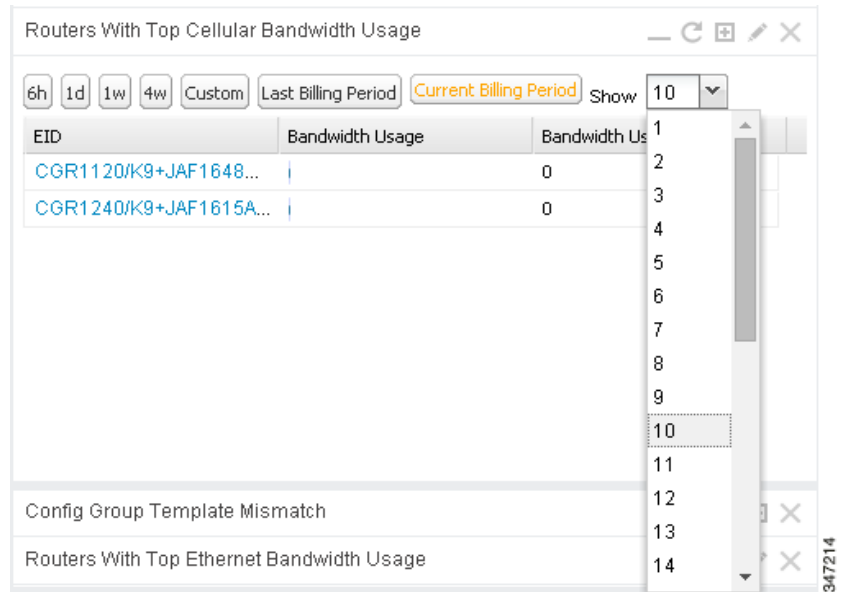
Tip: Click the triangle in any column heading, select Columns in the context menu, and check the Down Routers Over Time check box to hide this column.

Dashlet

Routers With Top Cellular Bandwidth Usage

Description

This bandwidth chart displays the top n routers using the maximum cellular bandwidth, where n is the number of top routers to display. It also identifies each cellular interface. Click the Filter button and select the number of routers to display from the **Show** drop-down list.



- Click the **Last Billing Period** button to display the bandwidth usage information for the top n routers that used the maximum bandwidth during last billing period.
- Click the **Current Billing Period** button to display the bandwidth usage information for the current billing period.

The start days are defined on the Billing Period Settings tab (**Admin > System Management > Server Settings**).

Routers With Top Ethernet Bandwidth Usage

This dashlet is similar to the Routers With Top Cellular Bandwidth Usage dashlet, except that it displays the top n routers with the maximum Ethernet bandwidth usage.

Routers With Least Cellular RSSI

This dashlet displays a chart of routers with the lowest RSSI values at the last poll, which indicates the quality of the signal strength and identifies each cellular interface. Use this chart to gauge the cellular channel conditions for FARs.

Repositioning Dashlets

The Dashboard is configurable to display charts in your preferred arrangement. To configure the Dashboard:

- Click and drag the title bar of a chart to the desired position.
- Click the close box to remove the chart from the page.
- Click the interval button to do the following:
 - Define an interval for line-graph chart displays.
 - Define a custom interval for line-graph chart displays.
 - Select the number of devices to chart for line-graph chart displays.
 - Select a series to refine data in line-graph chart displays.
 - Filter line-graph chart displays by group.
- Click the Settings button in the title bar to set the refresh interval for all charts and add dashlets back to the Dashboard.



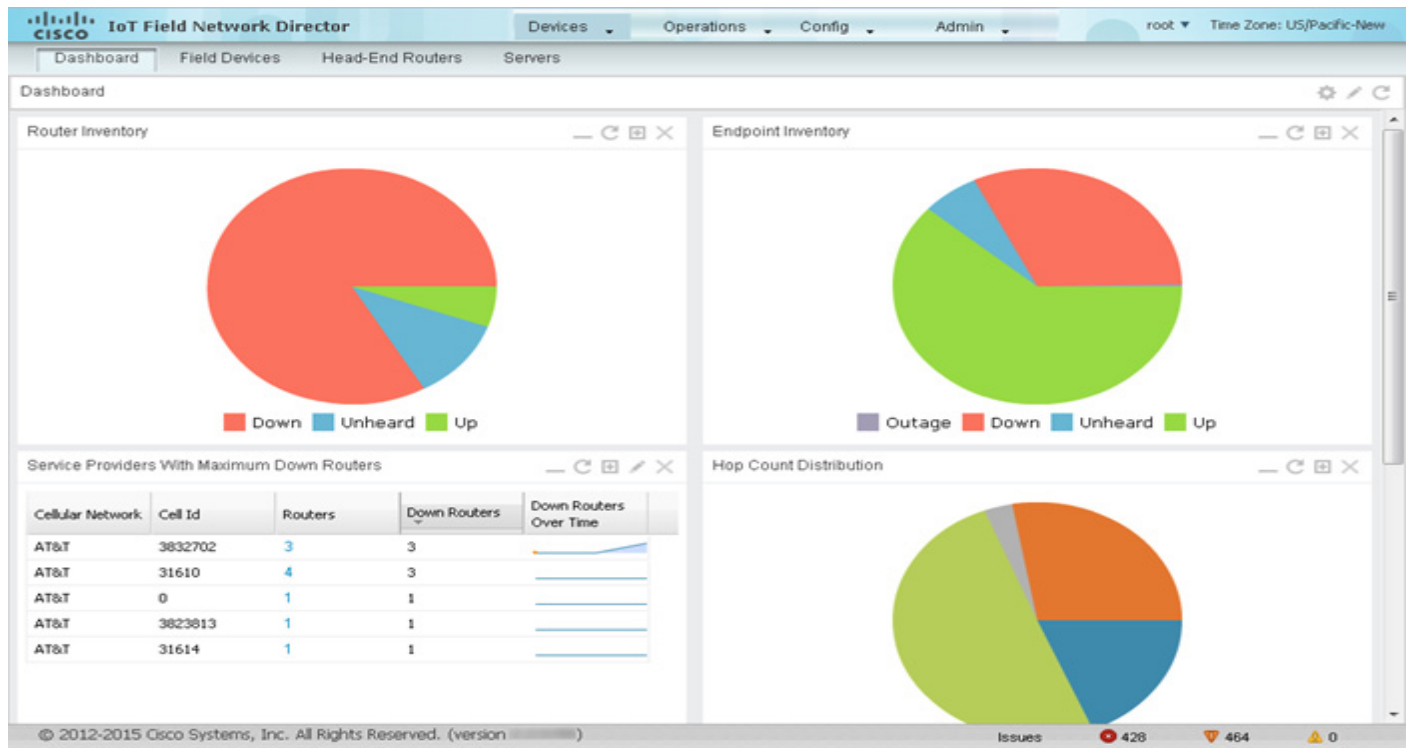

To better view dashlets in the bottom of the Dashboard, collapse a dashlet to just its title bar by clicking the dashlet show/hide button (). In [Figure 2](#) the Config Group Template Mismatch dashlet is expanded in the Dashboard with several other dashlets collapsed above it. To refresh the Dashboard, click the **Refresh** button (). To refresh a dashlet, click its **Refresh** button.

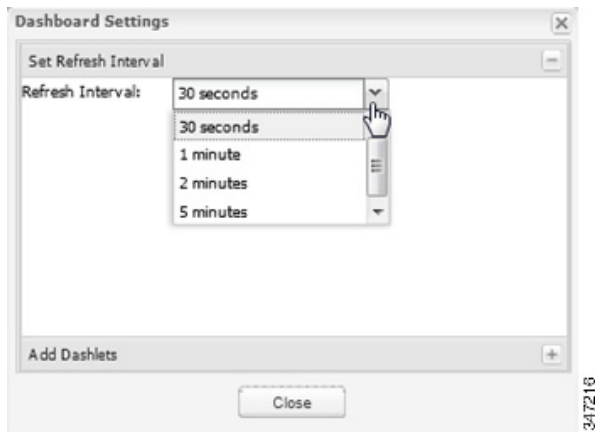
Figure 2 Dashboard with Collapsed Dashlets



Setting the Dashlet Refresh Interval

To set the refresh interval for dashlets:

1. Choose **Devices > Dashboard**.
2. Click the **Settings** button ().
3. Click **Set Refresh Interval**.




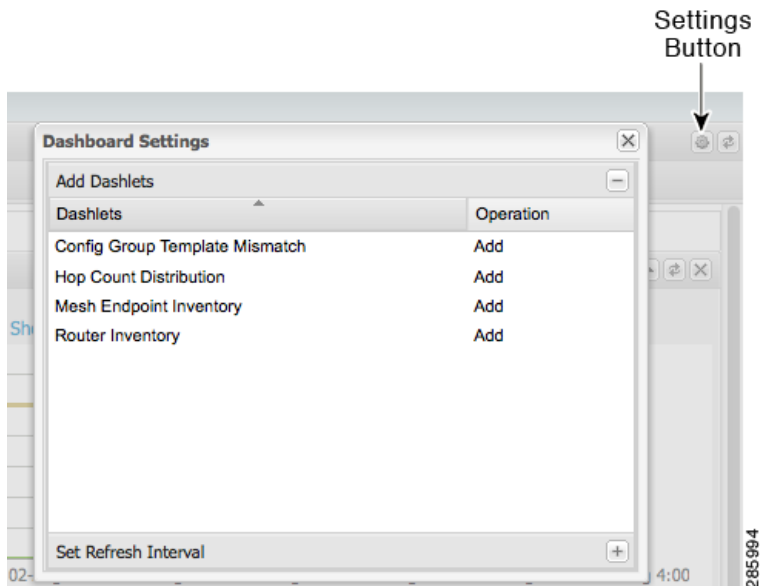
Note: On line-graph dashlets, open the filter bar and click an interval button to display metrics for that time period.

4. From the drop-down menu, choose a refresh interval.
5. Close the Dashboard Settings dialog box when finished.

Adding Dashlets

To add dashlets to the Dashboard:

1. Choose **Devices > Dashboard**.
2. Click the **Settings** button ().



3. Click **Add Dashlets**.

Note: No dashlets display in this dialog box if all are displaying on the Dashboard.

4. Click the dashlet to add to the Dashboard.

5. Close the Dashboard Settings dialog box when finished.

Removing Dashlets

To delete dashlets from the Dashboard:


1. Choose **Devices > Dashboard**.

2. Click the dashlet **Close** button.

Using Pie Charts to Get More Information

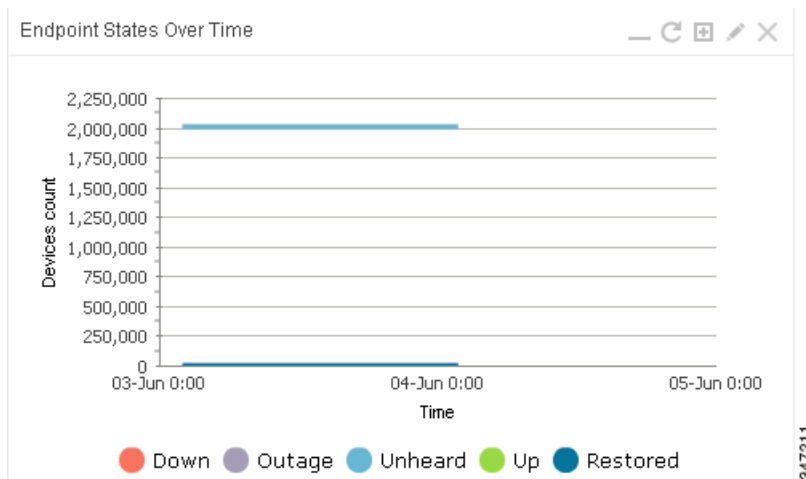
Mouse over any segment of a pie chart to display a callout with information on that segment. Click any segment in the Router Inventory and Mesh Endpoint Inventory pie charts to display the devices in List View.

Setting Dashlet Time Properties

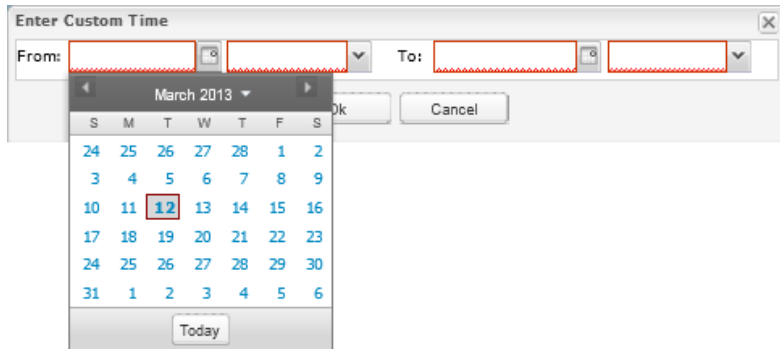
To specify the time interval for data collection for line-graph dashlets, click the interval icon () in the title bar to display the **6h**, **1d**, **1w**, **4w**, or **Custom** buttons. The **6h** button sets the data-collection time interval to the last six hours. The **1d** button sets the time interval to the last 24 hours.

To specify a custom time interval for a line-graph dashlet:

1. Click **Custom**.




2. In the **From** fields, specify the beginning date and time.



347210

3. In the **To** fields, specify the end date and time.
4. Click **OK**.

Collapsing Dashlets

Click the show/hide icon () at the top-right of the dashlet to collapse it to its title bar.

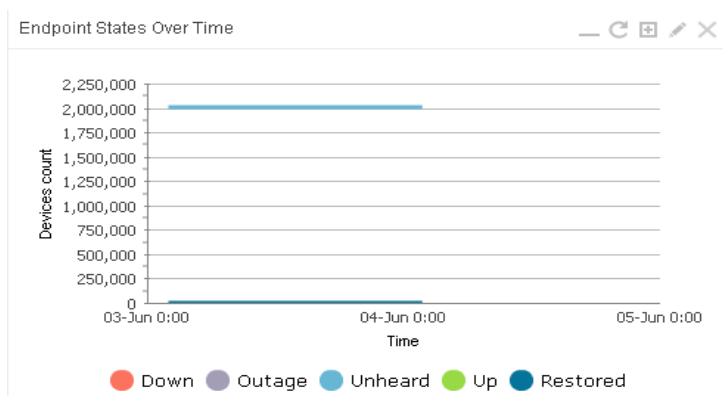
Using the Series Selector

You use the Series Selector to refine line-graphs to display by device status. The device options are:

- Routers: Down, Outage, Unheard, Unheard, and Up
- Mesh Endpoint Config Group: Config Out of Sync and Config In Sync
- Mesh Endpoint Firmware Group: Membership Out of Sync and Membership In Sync
- Mesh Endpoint States: Down, Outage, Unheard, and Up

To use the Series Selector:

1. Click **Series Selector**.



347211

2. In the **Series Selector** dialog box, check the check boxes for the data series to show in the graph.



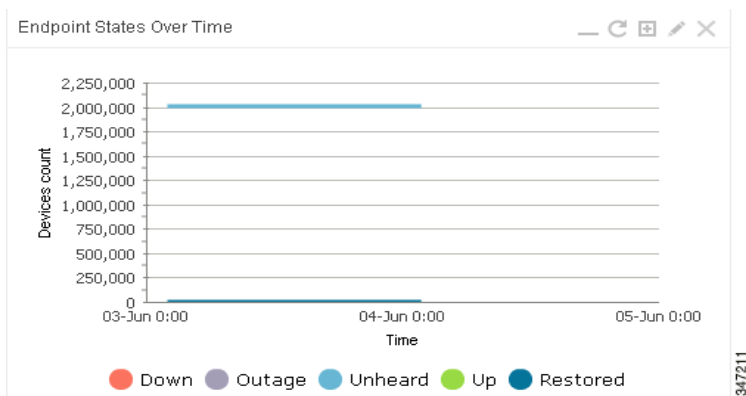
3. Click **Close**.

Using Filters

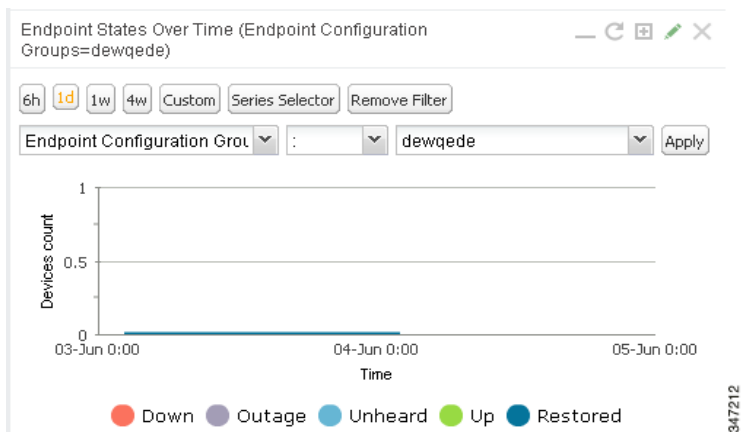
You use filters to refine the displayed line-graph data by groups. Applied filters display after the dashlet title.

To use the filters:

1. Click **Add Filter** in the line-graph dashlet pane.



2. From the first drop-down menu, choose a group type.



3. From the third drop-down menu, choose a group.

4. Click **Apply**.


The pencil icon is green and the filter displays next to the dashlet name to indicate that a filter is applied.

Note: Click the **Remove Filter** button to remove the filter and close the filter options.

Exporting Dashlet Data

You can export dashlet data to a CSV file.

To export dashlet data:

1. On the desired dashlet, click the export button ().

A browser download session begins.

2. Navigate to your default download directory to view the export file.

The filename begins with the word “export-” and includes the dashlet name (for example, export-Node_State_Over_Time_chart-1392746225010.csv).

Monitoring Events

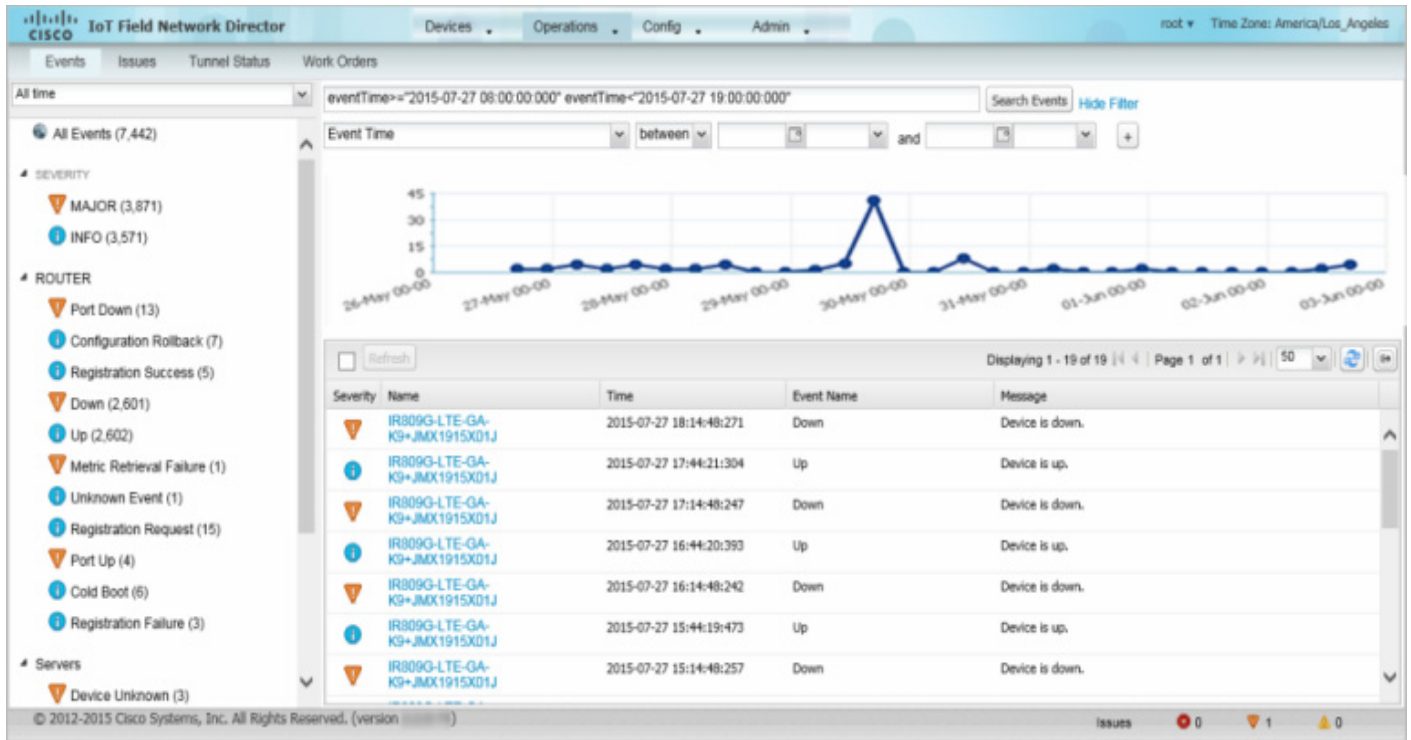
This section provides an overview of events and how to search and sort events, including the following topics:

- [Viewing Events](#)
- [Filtering by Severity Level](#)
- [Advanced Event Search](#)
- [Sorting Events](#)
- [Searching By Event Name](#)
- [Searching by Labels](#)

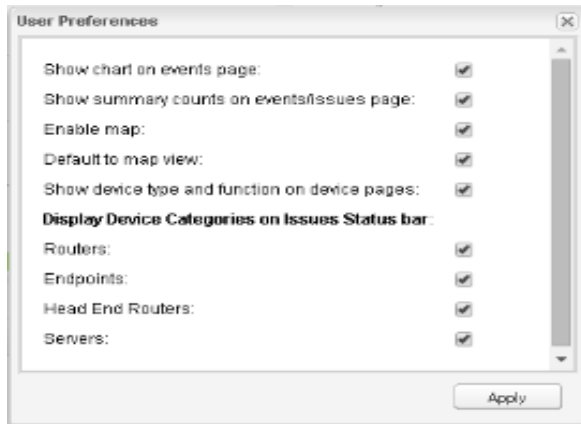
Viewing Events

As shown in [Figure 3](#), the Events page (**Operations > Events**) lists all events for those devices that IoT FND tracks. All events are stored in the CG-NMS database server.

Figure 3 Events Page



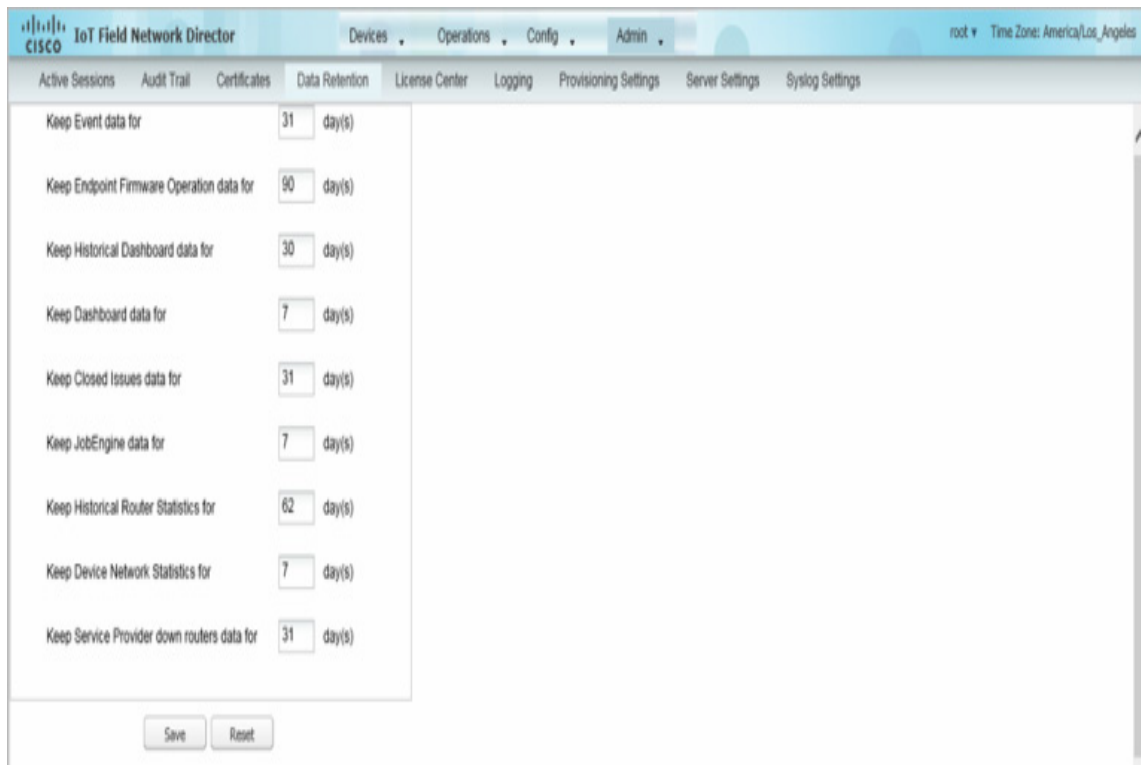
By default, the Events page displays the Events chart, which is a visual view of events in a time line. However, depending on the number of devices the CG-NMS server manages, this page can sometimes time out, especially when the system is fully loaded. In that case, open the Preferences window by choosing **username > Preferences** (top right), clearing the check boxes for showing chart and summary counts on the Events page, and clicking Apply.



To limit the amount of event data displayed on this page, use the Filter drop-down menu (at the top of the left pane). For example, you can show the events for the last 24 hours relative to the last 30 days, or events for a specific day within the last seven days.

To enable automatic refresh of event data to refresh every 14 seconds, check the check box next to the **Refresh** button. To immediately refresh event data click the **Refresh** button or the refresh icon.

Note: The amount of event data displayed on the Events page is limited by the data retention setting for events (**Admin > System Management > Data Retention**).



All Events Pane Filters

Use the preset filters in the All Events pane to only view those event types.

Device Events

In the left pane, IoT FND tracks events for the following devices:

- Routers
- Endpoints
- Head-end Devices
- CG Mesh Devices
- NMS Servers
- Database Servers


Event Severity Level

In the left pane, select an event severity level to filter the list view to devices with that severity level:

- Critical
- Major
- Minor
- Info

Each event type has a preset severity level. For example, a Router Down event is a Major severity level event.

Preset Events By Device

IoT FND has a preset list of events it reports for each device it tracks. A list of those events is summarized under each device in the left pane on the Events page. For example, in the left pane click the show/hide icon () next to Routers to expand the list of all events for routers.

Filtering by Severity Level

To filter by severity level:

1. Choose **Operations > Events**.
2. Click the **SEVERITY** show/hide arrow.

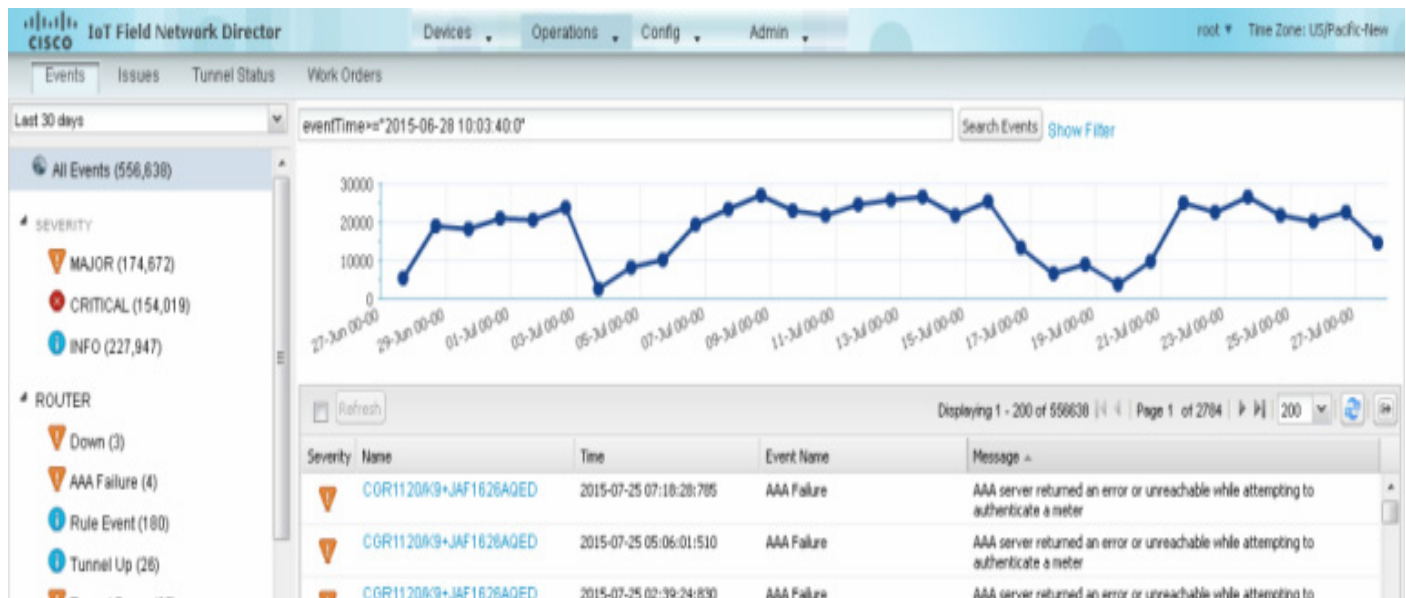
Note: Only severity levels that have occurred display.
3. Click a severity level (**CRITICAL**, **MAJOR**, **MINOR**, OR **INFO**).

All events of that severity level display in the Events pane.

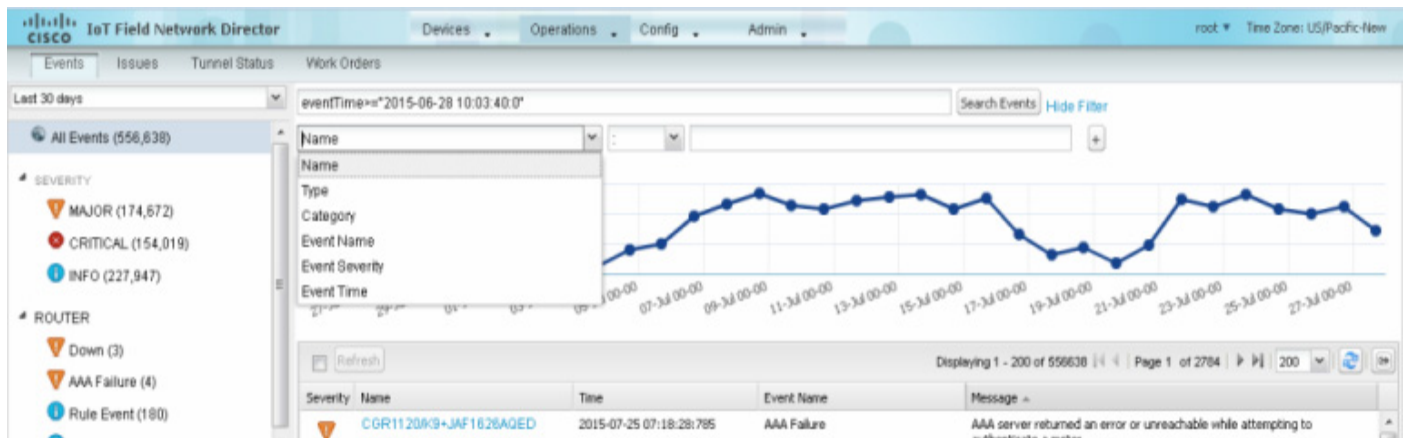
Advanced Event Search

To use the filter to search for events:

1. Choose **Operations > Events**.
2. Under All Events (left pane), select an event category to narrow down your search.
3. Click the **Show Filter** link at the top of the main pane.



4. Use the filter drop-down menus and fields to specify your search criteria.



5. Click the plus button (**+**) to add the search strings to the Search field.

Repeat the process of adding search strings to the Search field as needed.

6. Click **Search Events** or press Enter.

The search results display in the Events pane.

You can also add search strings manually, as shown in the following examples:

- To filter events by Name (EID), enter the following string in the Search Events field, as shown in [Figure 3](#):

name: *router eid string*.

Search Events by Name Filter



Note: Note the use of the asterisk (*) wild card with this filter.

- To filter by event time period, enter the following string in the Search Events field, as shown in [Figure 4](#):

eventTimeoperator "YYYY-MM-DD HH:MM:SS:SSS"

Supported operators are: <, >, >=, <=, :

Note: Do not enter a space between **eventTime** and the operator.

Figure 4 Search Events by Time Filter Example



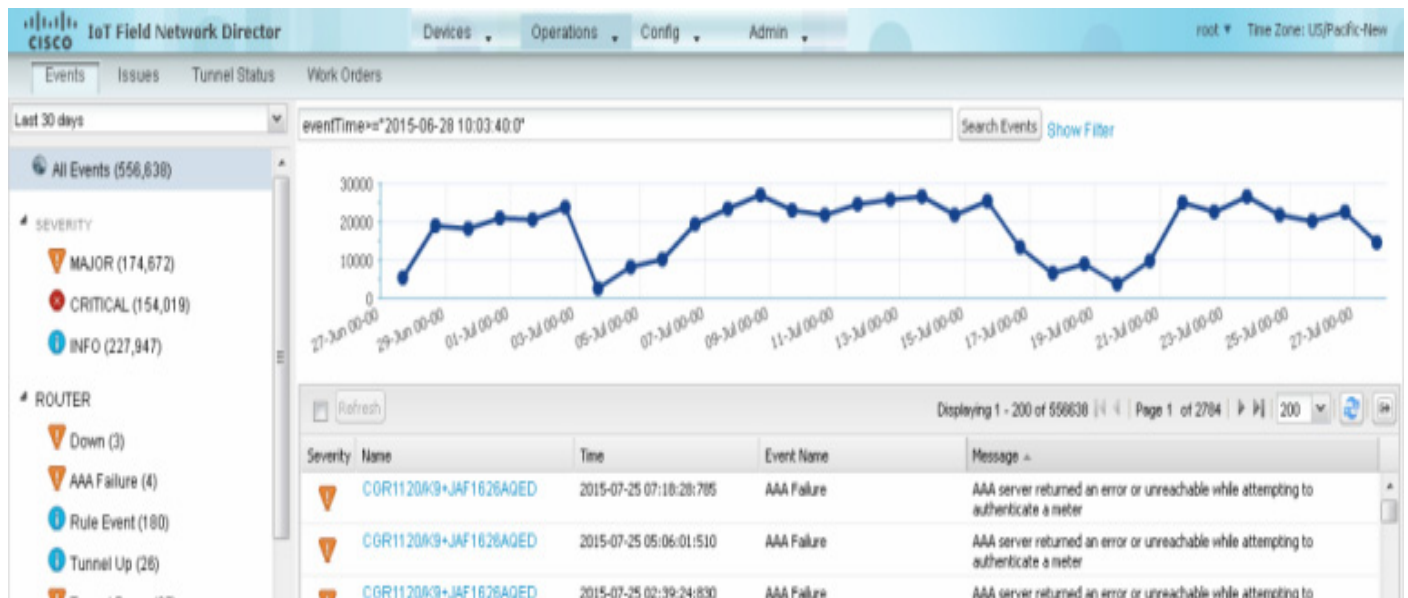
Sorting Events

To sort events in ascending or descending order, mouse over any column and select the appropriate option from the heading drop-down menu.

Searching By Event Name

To search by event name (for example, Battery Low):

1. Choose **Operations > Events**.
2. Click the device type to search for in the left pane.
3. Click the **Show Filter** link at the top of the right pane.



The filter fields display under the Search Events field.

4. Choose **Event Name** from the left drop-down menu.

The screenshot shows the Cisco IoT Field Network Director interface. The search field contains the text "eventTime=>2015-06-28 10:03:40.0". A dropdown menu is open over the search field, listing options: Name, Type, Category, Event Name, Event Severity, and Event Time. The main panel shows a line graph of event counts over time and a table of events below it.

Severity	Name	Time	Event Name	Message
MAJOR	CGR1120K9+JAF1626AQED	2015-07-25 07:18:28:785	AAA Failure	AAA server returned an error or unreachable while attempting to authenticate a user

5. Choose the event name from the options in the right drop-down menu.

The screenshot shows the Cisco IoT Field Network Director interface. The search field is empty. A dropdown menu is open over the search field, listing various event names such as AAA Failure, ACT2L Failure, Archive Log Mode Disabled, Archive Log Mode Enabled, Battery Backup Unit Configuration Failed, Battery Backup Unit Firmware Upgrade Failed, Battery Backup Unit Lock Out, Battery Backup Unit PowerOff, Battery Failure, Battery Low, Battery Normal, BBU Firmware Download Failed, BBU Firmware Download Passed, and BBU Firmware Mismatch Found. The main panel shows a line graph of event counts over time and a table of events below it.

Severity	Name	Time	Event Name	Message
MAJOR	CGR1120K9+JAF1636ANIK	2015-07-28 08:39:55	Battery Backup Unit Configuration Failed	
MAJOR	CGR1120K9+JAF1710ANJE	2015-07-28 07:54:45	BBU Firmware Download Failed	

6. Click the plus button (**+**) at the right to add the filter to the Search Events field.

The filter syntax appears in the Search Events field.


7. Click the **Search Events** button.

The search results display in the Events pane.

Searching by Labels

Allows you to search and filter events based on Label names tagged to Field Devices.

1. Choose **Operations > Events**.
2. Click **All Events** in the left pane.
3. Click the **Show Filter** link at the top of the right pane.
4. Choose **Label** from the left drop-down menu.
5. Click the **Show Filter** link at the top of the right pane.

6. Choose the event name from the options in the right drop-down menu or create your own.
7. Click the plus button () at the right to add the filter to the Search Events field.

The filter syntax appears in the Search Events field.


8. Click the **Search Events** button.

The search results display in the Events pane.

Exporting Events

You can export events to a CSV file to examine as a log of event severity, time, name and event description by device.

To export events:

1. Choose **Operations > Events**.
2. Click the desired severity level or device type in the left pane.
3. Click the **Export** button ().

A browser download session begins.

4. Navigate to your default download directory to access the CSV file.

Events Reported

Table 1 lists the events reported by IoT FND 3.1.x (and later). Details include the event severity (Critical, Major, Minor, Information) and the devices that report those events.

Table 1 Events Reported

Event	Devices	Severity
CRITICAL EVENTS		
Certificate Expired	AP800, CGR1000, C800, FND, IR800	Critical
DB FRA Space Critically Low	Database	Critical
DB Table Space Critically Low	Database	Critical
Invalid CSMP Signature	CGMESH, IR500	Critical
Outage	Cellular, CGMESH, IR500	Critical
RPL Tree Size Critical	CGR1000	Critical
SD Card Removal Alarm	CGR1000	Critical
MAJOR EVENTS		
AAA Failure	C800, CGR1000, IR800	Major
ACT2L Failure	C800, CGR1000, IR800	Major
Archive Log Mode Disabled	Database	Major
Battery Failure	CGR1000	Major
Battery Low	CGR1000, IR500	Major
BBU Configuration Failed	IR500	Major
BBU Firmware Download Failed	CGR1000	Major

Table 1 Events Reported

Event	Devices	Severity
BBU Firmware Mismatch Found	CGR1000	Major
BBU Firmware Upgrade Failed	IR500	Major
BBU Lock Out	IR500	Major
BBU Power Off	IR500	Major
Block Mesh Device Operation Failed	CGR1000	Major
Certificate Expiration	AP800, C800, CGR1000, FND, IR800	Major
DB FRA Space Very Low	Database	Major
Default Route Lost	CGMESH, IR500	Major
Device Unknown	FND	Major
Door Open	C800, CGR1000, IR800, LORA	Major
Dot1X Authentication Failure	CGR1000	Major
Dot1X Authentication Flood	C800, CGR1000, IR800	Major
Down	AP800, ASR, C800, Cellular, CGMESH, CGR1000, Database, FND, IR500, IR800, ISR3900, LORA	Major
Element Configuration Failed	C800, CGR1000, IR800	Major
High CPU Usage	LORA	Major
High Flash Usage	LORA	Major
High Temperature	LORA	Major
HSM Down	FND	Major
Interface Down	ASR, ISR3900	Major
Linecard Failure	C800, CGR1000, IR800	Major
Line Power Failure	C800, CGR1000, IR800	Major
Link Down	IR500	Major
Low Flash Space	C800, CGR1000, IR800	Major
Low Memory/Memory Low	C800, CGR1000, FND, IR800, LORA (Memory Low)	Major
Low Temperature	LORA	Major
Mesh Connectivity Lost/ Node Connectivity Lost	CGMESH, IR500	Major
Mesh Link Key Timeout/ Node Link Key Timeout	CGMESH, IR500	Major
Metric Retrieval Failure	ASR, C800, CGR1000, IR800, ISR3900	Major
Modem Temperature Cold Alarm	C800, CGR1000, IR800	Major
Modem Temperature Warm Alarm	C800, CGR1000, IR800	Major
Node Connectivity Lost	CGMESH, IR500	Major
Node Link Key Timeout	CGMESH, IR500	Major
Packet Forwarder Usage High	LORA	Major
Port Down	AP800, C800, CGR1000, IR800	Major
Port Failure	AP800, C800, CGR1000, IR800	Major
Refresh Router Mesh Key Failure	CGR1000	Major
RPL Tree Size Warning	CGR1000	Major

Table 1 Events Reported

Event	Devices	Severity
Software Crash	C800, CGR1000, IR800	Major
SSM Down	FND	Major
System Software Inconsistent	C800, CGR1000, IR800	Major
Temperature Major Alarm	C800, CGR1000, IR800	Major
Time Mismatch	CGMESH, IR500	Major
Tunnel Down	C800, CGR1000, IR800	Major
Tunnel Provisioning Failure	C800, CGR1000, IR800	Major
Unknown WPAN Change	CGMESH, IR500	Major
MINOR EVENTS		
DB FRA Space Low	Database	Minor
Dot1X Re-authentication	CGMESH, IR500	Minor
Temperature Minor Alarm	C800, CGR1000, IR800	Minor
Temperature Low Minor Alarm	C800, CGR1000, IR800	Minor
RPL Tree Reset	CGR1000	Minor
INFORMATION EVENTS		
Archive Log Mode Enabled	Database	Information
Battery Normal	CGR1000	Information
Battery Power	CGR1000	Information
BBU Firmware Download Passed	CGR1000	Information
Certificate Expiration Recovery	AP800, C800, CGR1000, FND, IR800	Information
Cold Boot	AP800, C800, CGMESH, CGR1000, IR500, IR800	Information
Configuration is Pushed	FND	Information
Configuration Rollback	AP800, C800, CGR1000, IR800	Information
DB FRA Space Normal	Database	Information
DB Table Space Normal	Database	Information
Device Added	Cellular, C800, CGMESH, CGR1000, IR500, IR800	Information
Device Location Changed	C800, CGR1000, IR800	Information
Device Removed	Cellular, C800, CGMESH, CGR1000, IR500, IR800	Information
Door Close	C800, CGR1000, IR800, LORA	Information
Dot11 Deauthenticate Send	C800, CGR1000, IR800	Information
Dot11 Disassociate Send	C800, CGR1000, IR800	Information
Dot11 Authentication Failed	C800, CGR1000, IR800	Information
Hardware Insertion	C800, CGR1000, IR800	Information
Hardware Removal	C800, CGR1000, IR800	Information
High CPU Usage Recovery	LORA	Information
High Flash Usage Recovery	LORA	Information
High Temperature Recovery	LORA	Information
HSM Up	FND	Information

Table 1 Events Reported

Event	Devices	Severity
Interface Up	ASR, ISR3900	Information
Line Power	C800, CGR1000, IR800	Information
Line Power Restored	C800, CGR1000, IR800	Information
Link Up	IR500	Information
Low Flash Space OK	C800, CGR1000, IR800	Information
Low Memory OK/Low Memory Recovery	C800, CGR1000, IR800, LORA (Low Memory Recovery)	Information
Manual Close	ASR, Cellular, C800, CGMESH, CGR1000, IR500, IR800, ISR3900	Information
Major RPL Tree Size Warning OK	CGR1000	Information
Manual NMS Address Change	CGMESH, IR500	Information
Manual Re-Registration	CGMESH, IR500	Information
Mesh Certificate Change/ Node Certificate Change	CGMESH, IR500	Information
Mesh Module Firmware Upgrade has been successful	CGR1000	Information
Migrated To Better PAN	CGMESH, IR500	Information
Modem Status Changed	LORA	Information
Modem Temperature Cold Alarm Recovery	C800, CGR1000, IR800	Information
Modem Temperature Warm Alarm Recovery	C800, CGR1000, IR800	Information
NMS Address Change	CGMESH, IR500	Information
NMS Returned Error	CGMESH, IR500	Information
Node Certificate Change	CGMESH, IR500	Information
Packet Forwarded High Usage Recovery	LORA	Information
Packet Forwarder Status	LORA	Information
Packet Forwarded High Usage Recovery	LORA	Information
Port Up	AP800, C800, CGR1000, IR800	Information
Power Source OK	C800, CGR1000, IR800	Information
Power Source Warning	C800, CGR1000, IR800	Information
Registered	ASR, ISR3900	Information
Registration Failure	AP800, Cellular, C800, CGR1000, IR800, LORA	Information
Registration Request	AP800, C800, CGR1000, IR800, LORA	Information
Registration Success	AP800, Cellular, C800, CGR1000, IR800, LORA	Information
Rejoined With New IP Address	CGMESH, IR500	Information
Restoration	Cellular, CGMESH, IR500	Information
Restoration Registration	CGMESH, IR500	Information
RPL Tree Size Critical OK	CGR1000	Information
Rule Event	ASR, C800, CGMESH, CGR1000, Database, FND, IR500, IR800, ISR3900	Information
SSM Up	FND	Information

Table 1 Events Reported

Event	Devices	Severity
Temperature Low Recovery	LORA	Information
Temperature Low Minor Alarm Recovery	C800, CGR1000, IR800	Information
Temperature Major Recovery	C800, CGR1000, IR800	Information
Temperature Low Major Alarm Recovery	C800, CGR1000, IR800	Information
Temperature Minor Recovery	C800, CGR1000, IR800	Information
Time Mismatch Resolved	CGMESH, IR500	Information
Tunnel Provisioning Request	C800, CGR1000, IR800	Information
Tunnel Provisioning Success	C800, CGR1000, IR800	Information
Tunnel Up	C800, CGR1000, IR800	Information
Unknown Event	AP800, ASR, C800, Cellular, CGMESH, CGR1000, Database, FND, IR500, IR800, ISR3900, LORA	Information
Unknown Registration Reason	CGMESH, IR500	Information
Unsupported	AP800, C800, CGR1000, IR800, LORA	Information
Up	AP800, ASR, C800, Cellular, CGMESH, CGR1000, Database, FND, IR500, IR800, ISR3900, LORA,	Information
Warm Start	IR500	Information
WPAN Watchdog Reload	CGR1000	Information

Monitoring Issues

This section provides an overview of issues and how to search for and close issues in IoT FND, including the following topics:

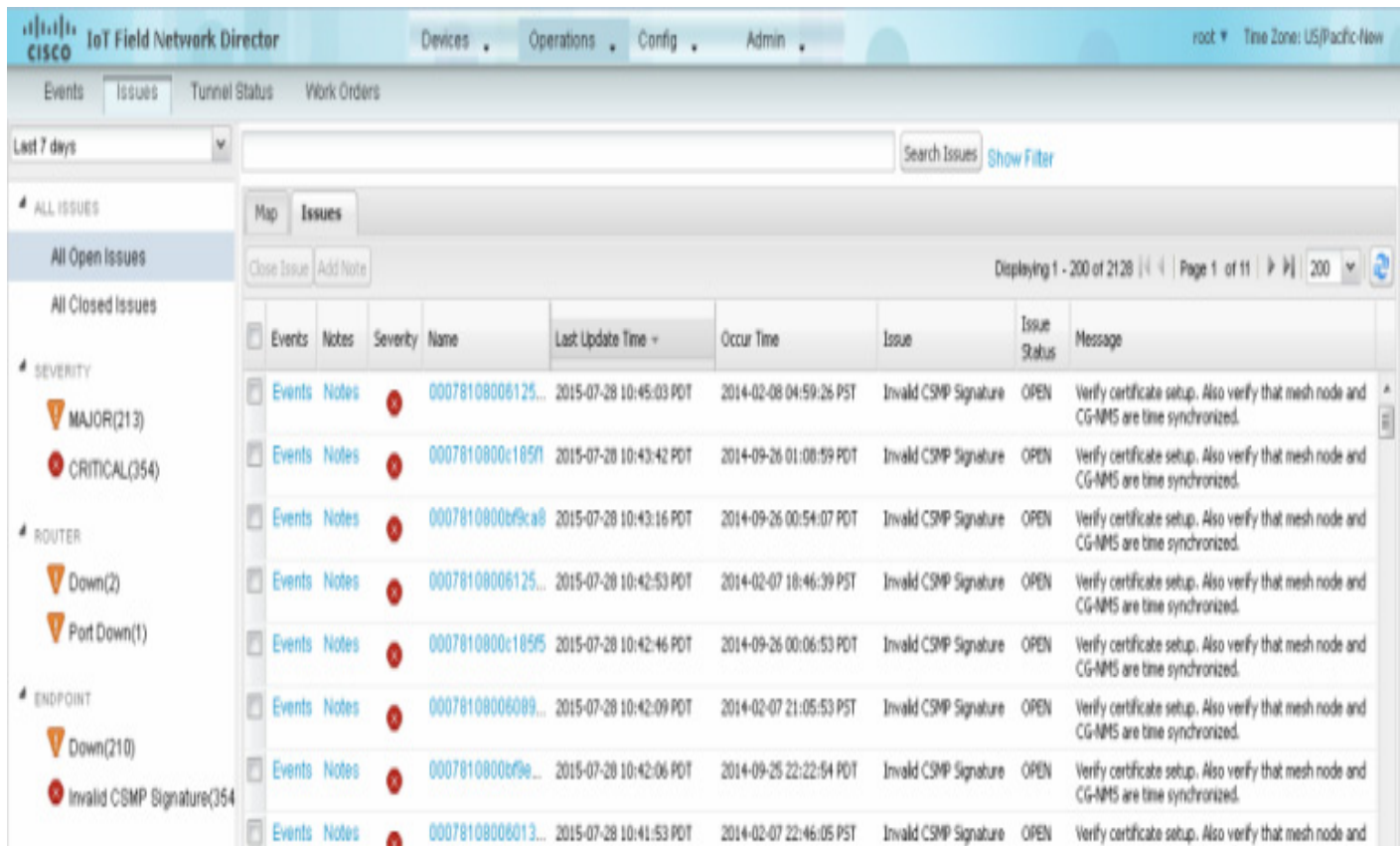
- [Viewing Issues](#)
- [Viewing Device Severity Status on the Issues Status Bar](#)
- [Adding Notes to Issues](#)
- [Searching Issues Using Predefined Filters](#)
- [Search Issues Using Custom Filters](#)
- [Closing an Issue](#)

Viewing Issues

IoT FND offers different ways to monitor issues:

- The **Operations > Issues** page ([Figure 5](#)) provides a snapshot of the health of the network by highlighting only major and critical events that are active within the network.
- The Issues Status bar ([Figure 6](#)) displays in the footer of the browser window and shows a count of all issues by severity for selected devices.

Figure 5 Issues Page



Events	Notes	Severity	Name	Last Update Time	Occur Time	Issue	Issue Status	Message
Events	Notes	CRITICAL	00078108006125...	2015-07-28 10:45:03 PDT	2014-02-08 04:59:26 PST	Invalid CSMP Signature	OPEN	Verify certificate setup. Also verify that mesh node and CG-AMS are time synchronized.
Events	Notes	CRITICAL	0007810800c185f1	2015-07-28 10:43:42 PDT	2014-09-26 01:08:59 PDT	Invalid CSMP Signature	OPEN	Verify certificate setup. Also verify that mesh node and CG-AMS are time synchronized.
Events	Notes	CRITICAL	0007810800b9ca8	2015-07-28 10:43:16 PDT	2014-09-26 00:54:07 PDT	Invalid CSMP Signature	OPEN	Verify certificate setup. Also verify that mesh node and CG-AMS are time synchronized.
Events	Notes	CRITICAL	00078108006125...	2015-07-28 10:42:53 PDT	2014-02-07 18:46:39 PST	Invalid CSMP Signature	OPEN	Verify certificate setup. Also verify that mesh node and CG-AMS are time synchronized.
Events	Notes	CRITICAL	0007810800c185f5	2015-07-28 10:42:46 PDT	2014-09-26 00:06:53 PDT	Invalid CSMP Signature	OPEN	Verify certificate setup. Also verify that mesh node and CG-AMS are time synchronized.
Events	Notes	CRITICAL	00078108006089...	2015-07-28 10:42:09 PDT	2014-02-07 21:05:53 PST	Invalid CSMP Signature	OPEN	Verify certificate setup. Also verify that mesh node and CG-AMS are time synchronized.
Events	Notes	CRITICAL	0007810800b9e...	2015-07-28 10:42:06 PDT	2014-09-25 22:22:54 PDT	Invalid CSMP Signature	OPEN	Verify certificate setup. Also verify that mesh node and CG-AMS are time synchronized.
Events	Notes	CRITICAL	00078108006013...	2015-07-28 10:41:53 PDT	2014-02-07 22:46:05 PST	Invalid CSMP Signature	OPEN	Verify certificate setup. Also verify that mesh node and

The Issues page provides an abbreviated subset of unresolved network events for quick review and resolution by the administrator. Issues remain open until either the associated event is resolved (and IoT FND generates a resolution event) or the administrator manually closes the event.

Only one issue is recorded when multiple entries for the same event are reported. Each issue has a counter associated with it. As an associated event is closed, the counter decrements by one. Every open or closed issue has an associated event.

Note: The amount of closed issues data that displays on the Issues page is limited by the **Keep Closed Issues for** data retention setting (**Admin > System Management > Data Retention**), which is based on the time the issue was closed. When the issue was closed displays as the Last Update Time for the issue.

Viewing Device Severity Status on the Issues Status Bar

A tally of issues listed by severity for the selected devices displays in the Issues status bar in the bottom-right of the browser window frame (Figure 6). You can set the device types for issues that display in the Issues status bar in User Preferences (see [Setting User Preferences](#)).

Figure 6 Issues Status Bar



Issues	0	30979	4285
--------	---	-------	------

Click the Issues status bar to view the Issues Summary pane (Figure 7), which displays issues listed by the selected device category. Click count links in the Issues Summary pane to view complete issue criteria filtered by severity on the **Operations > Issues** page.

Figure 7 Issues Summary Pane

Device Category	Critical	Major	Minor
router	0	6526	4285
her	0	0	0
server	0	0	0
endpoint	0	24453	0

Issues: 0 Critical, 30979 Major, 4285 Minor

Adding Notes to Issues

On the **Operations > Issues** page, you can maintain notes on issues for the device. Click the Notes link inline with the issue to access any notes entered in the issue or add a note on the Notes for Issues Name page. You can add and delete notes from issues on this page. Issues can have multiple notes. The Notes for Issues Name page displays the time the note was created, the name of the user who wrote the note, and the text of the note. You can also add a note when closing an issue. Notes are purged from the database with the issue.

To add a note to an issue:

1. Click the **Notes** link inline with the desired issue or check the check box of the device and click **Add Note**.

Events	Notes	Severity	Name	Last Update Time	Occur Time	Issue	Issue Status	Message
<input type="checkbox"/>	Events	<input type="checkbox"/>	00078108006125...	2015-07-28 10:45:03 PDT	2014-02-08 04:59:26 PST	Invalid CSMP Signature	OPEN	Verify certificate setup. Also verify that mesh node and CG-NMS are time synchronized.
<input type="checkbox"/>	Events	<input type="checkbox"/>	0007810800c185f1	2015-07-28 10:43:42 PDT	2014-09-26 01:08:59 PDT	Invalid CSMP Signature	OPEN	Verify certificate setup. Also verify that mesh node and CG-NMS are time synchronized.
<input type="checkbox"/>	Events	<input type="checkbox"/>	00078108005f9ca8	2015-07-28 10:43:16 PDT	2014-09-26 00:54:07 PDT	Invalid CSMP Signature	OPEN	Verify certificate setup. Also verify that mesh node and CG-NMS are time synchronized.
<input type="checkbox"/>	Events	<input type="checkbox"/>	00078108006125...	2015-07-28 10:42:53 PDT	2014-02-07 18:46:39 PST	Invalid CSMP Signature	OPEN	Verify certificate setup. Also verify that mesh node and CG-NMS are time synchronized.
<input type="checkbox"/>	Events	<input type="checkbox"/>	0007810800c185f5	2015-07-28 10:42:46 PDT	2014-09-26 00:06:53 PDT	Invalid CSMP Signature	OPEN	Verify certificate setup. Also verify that mesh node and CG-NMS are time synchronized.
<input type="checkbox"/>	Events	<input type="checkbox"/>	00078108006089...	2015-07-28 10:42:09 PDT	2014-02-07 21:05:53 PST	Invalid CSMP Signature	OPEN	Verify certificate setup. Also verify that mesh node and CG-NMS are time synchronized.
<input checked="" type="checkbox"/>	Events	<input type="checkbox"/>	00078108006f9e...	2015-07-28 10:42:06 PDT	2014-09-25 22:22:54 PDT	Invalid CSMP Signature	OPEN	Verify certificate setup. Also verify that mesh node and CG-NMS are time synchronized.

The Notes for Issues Name pane displays. The issue in the following example has existing notes.

The screenshot shows the Cisco IoT Field Network Director interface. The top navigation bar includes 'Events', 'Issues', 'Tunnel Status', and 'Work Orders'. The 'Issues' tab is active, displaying a list of issues. A specific issue is selected, showing details such as 'Last Update Time', 'Occur Time', 'Name', 'EID', 'Status', and 'Severity'. The 'Add Note' button is circled in red. Below the issue details, there is a table with columns for 'Time', 'User Name', and 'Note'. The table contains one entry: '2015-07-28 10:54:42 PDT', 'root', and 'Check this on 7-29'. The 'Add Note' button is located above this table.

2. Click **Add Note**.

The Add Note dialog displays.

The screenshot shows the 'Add Note' dialog box. It has a title bar with 'Add Note' and a close button. The main area contains a label 'Note:' followed by a large text input field. Below the input field are two buttons: 'Add' and 'Cancel'. The dialog box is positioned over the main interface.

3. Insert your cursor in the **Note** field and type your note.

4. Click **Add** when finished.

The note text displays on the Notes for Issues Name pane in the Note column.

To add notes to issues with existing notes:

1. Click the **Notes** link inline with the issue or check the check box of the device and click **Add Note**.

The Notes for Issues Name pane displays.

2. To add a new note to the issue, click **Add Note**.

The Add Note dialog displays.


3. Insert your cursor in the **Note** field and type your note.

4. Click **Add** when finished.

To edit an existing note in an issue:

1. Click the **Notes** link inline with the issue.

The Notes for Issues Name pane displays.

2. To edit an existing note, click the pencil icon () at the right of the note that you want to edit.

Time	User Name	Note
2013-05-01 21:37:00 UTC	root	testnote
2013-05-01 21:37:04 UTC	root	testnote
2013-05-01 21:37:06 UTC	root	testnote

3. Edit the note, and click **Done** when finished.

To delete a note from an issue:

1. Click the **Notes** link inline with the issue.

The Notes for Issues Name pane displays.

2. To delete a note, click the red X icon (X) at the right of the note.

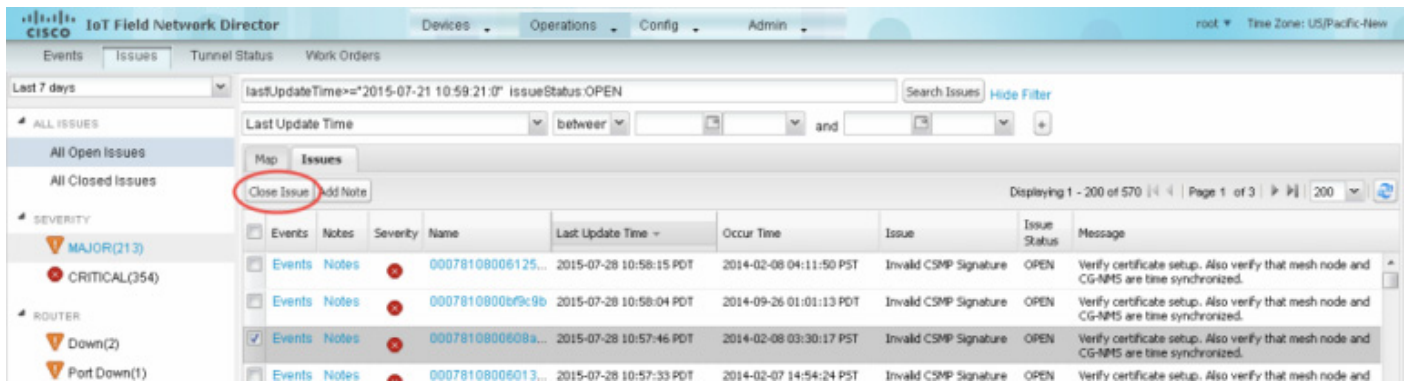
Time	User Name	Note
2013-05-01 21:37:00 UTC	root	testnote
2013-05-01 21:37:04 UTC	root	testnote
2013-05-01 21:37:06 UTC	root	testnote

3. Click **Yes** to confirm the deletion.

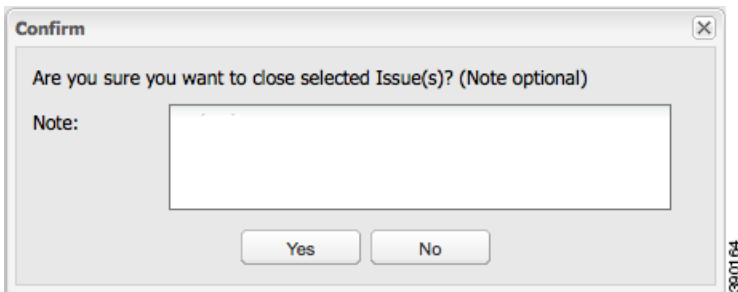
To add a note when closing an issue:

1. Check the check box of the issue to close.

2. Click **Close Issue**.



3. In the Confirm dialog box, insert your cursor in the Note field and type the note text.



4. To confirm that you want to close the issue and save the note, click **Yes**.

Searching Issues Using Predefined Filters

To search for open issues for a specific system or severity level:

1. Choose **Operations > Issues**.

To list only open issues, click **All Open Issues** (left pane).

Note: By default, IoT FND displays all issues that occurred within the specified data retention period (see [Configuring Data Retention](#)). To see Closed Issues associated with an event type or severity level, change **issueStatus:OPEN** to **issueStatus:CLOSED** in the Search Issues field, and then click **Search Issues**. To list all closed issues, in the left pane, click **All Closed Issues**.

2. Click a device category, event type, or severity level to filter the list.

The filter syntax appears in the Search Issues field, and the search results display in the main pane.

Search Issues Using Custom Filters

To search by creating custom filters:

1. Choose **Operations > Issues**.
2. Click **Show Filter**.
3. From the Filter drop-down menus, choose the appropriate options.

For example, to filter severity levels by EID:

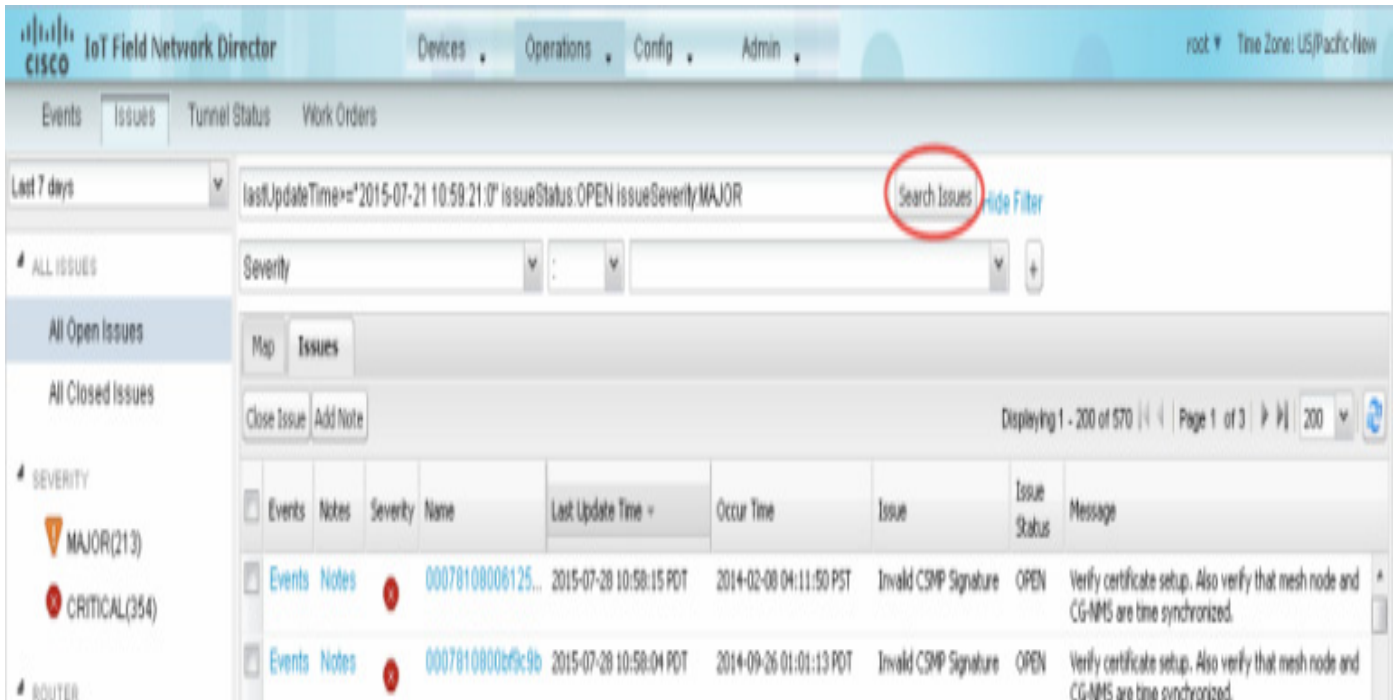
- In the left pane, select a severity level.
- From the first Filter drop-down menu, choose **EID**.
- In the third Filter field, enter the EID of the device to discover issues about.

You can also enter the search string in the Search Issues field. For example:

```
issueSeverity:CRITICAL issueStatus:OPEN eid:CG-NMS-DB+localhost
```

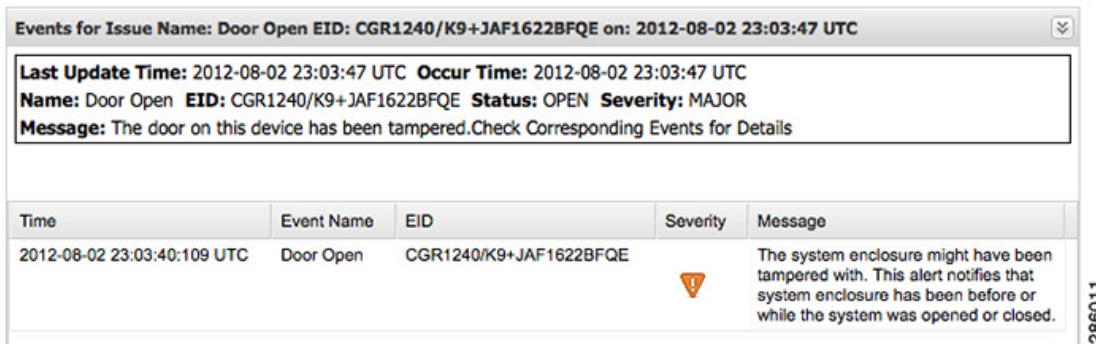
4. Click **Search Issues**.

The issues, if any, display in the Search Issues section (right pane).



5. Click the **Events** link to display events associated with an issue.

The Events for Issue Name pane displays all events for that device.



6. Click **Search Issues** or any link in the left pane to return to the Issues pane.

Closing an Issue

In most cases, when an event is resolved, the issue is closed automatically by the software. However, when the administrator has actively worked on resolving the issue, it might make sense to close the issue directly. When the issue is closed, IoT FND generates an event.

To close a resolved issue:

1. Choose **Operations > Issues**.
2. Locate the issue by following the steps in either the [Searching Issues Using Predefined Filters](#) or [Search Issues Using Custom Filters](#) section.
3. In the Search Issues section (right pane), check the check boxes of the issues to close.

4. Click **Close Issue**.

Note: You can also add a note to the issue at this time.

5. Click **Yes**.

Viewing Device Charts

- [Router Charts](#)
- [Mesh Endpoint Charts](#)

Router Charts

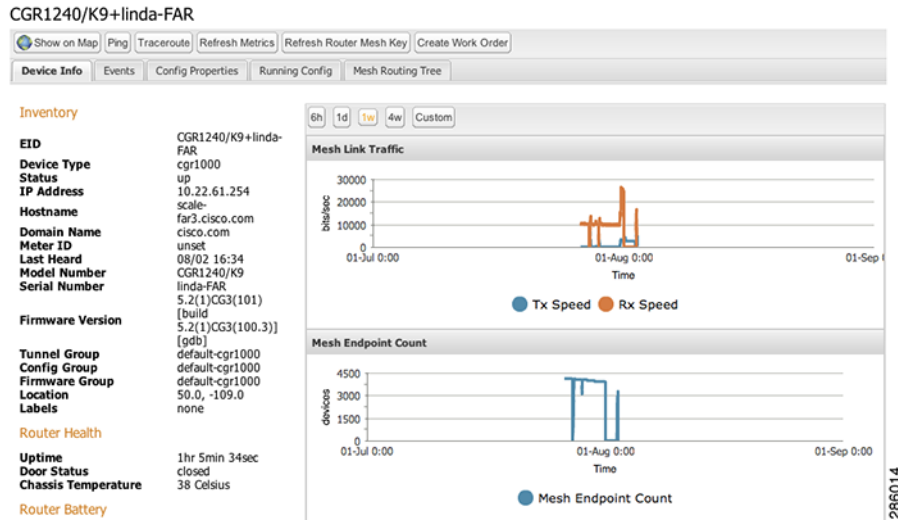
IoT FND provides these charts in the Device Info pane on the Device Details page for any FAR:

Table 2 Device Detail Charts

Chart	Description
Mesh Link Traffic	Shows the aggregated WPAN rate for a FAR over time.
Mesh Endpoint Count	Shows the number of MEs over time.
Cellular Link Metrics	Shows the metrics (transmit and receive speed), RSSI, Bandwidth Usage (current Billing Cycle) for all logical cellular GSM and CDMA interfaces.
Cellular Link Settings	Shows properties for cellular physical interfaces with dual and single modems.
Cellular Link Traffic	Shows the aggregated WPAN rate per protocol over time.
Cellular RSSI	Cellular RSSI.
WiMAX Link Traffic	Shows the receiving and sending rates of the WiMAX link traffic for the FAR over time.
WiMAX RSSI	Shows the receiving and sending rates of the WiMAX RSSI traffic for the FAR over time.
WPAN Traffic	(Master only) Shows Dual PHY WPAN traffic trends.
Ethernet Link Traffic	Shows the receiving and sending rates of the Ethernet traffic for the FAR over time.
Cellular Bandwidth Usage Over Time	Shows the bandwidth usage over time for the cellular interface.
Ethernet Bandwidth Usage Over Time	Shows the bandwidth usage over time for the Ethernet interface.

[Figure 8](#) shows the Mesh Link Traffic and Mesh Endpoint Count charts.

Figure 8 FAR Device Charts



Mesh Endpoint Charts

IoT FND provides the charts listed in [Table 3](#) in the Device Info pane on the Device Details page ([Figure 9](#)) for any ME.

Table 3 Device Detail Charts

Chart	Description
Mesh Link Traffic	Shows the aggregated WPAN rate for a FAR over time.
Mesh Path Cost and Hops	Shows the RPL path cost value between the element and the root of the routing tree over time (see Configuring RPL Tree Polling).
Mesh Link Cost	Shows the RPL cost value for the link between the element and its uplink neighbor over time.
Mesh RSSI	Shows the measured RSSI value of the primary mesh RF uplink (dBm) over time.

Figure 9 Mesh Endpoint Device Charts

<< Back

00173BAB003C3100

[Show on Map](#)
[Ping](#)
[Traceroute](#)
[Sync Config Membership](#)
[Sync Firmware Membership](#)
[Block Mesh Device](#)

[Device Info](#)
[Events](#)
[Config Properties](#)
[Mesh Routing Tree](#)

Inventory

EID 00173BAB003C3100
Device Type cgmesh
Status up
IP Address 2001:dead:beef:6108:217:3bab:3c:3100
Meter ID unset
Last Heard 2012-07-24 17:05
Model Number OWCN/3.1
Serial Number 00173BAB003C3100
Firmware Version 5.0.92
Config Group default-cgmesh
Firmware Group default-cgmesh
Location 49.4, -132.9
Labels none

Mesh Endpoint Health

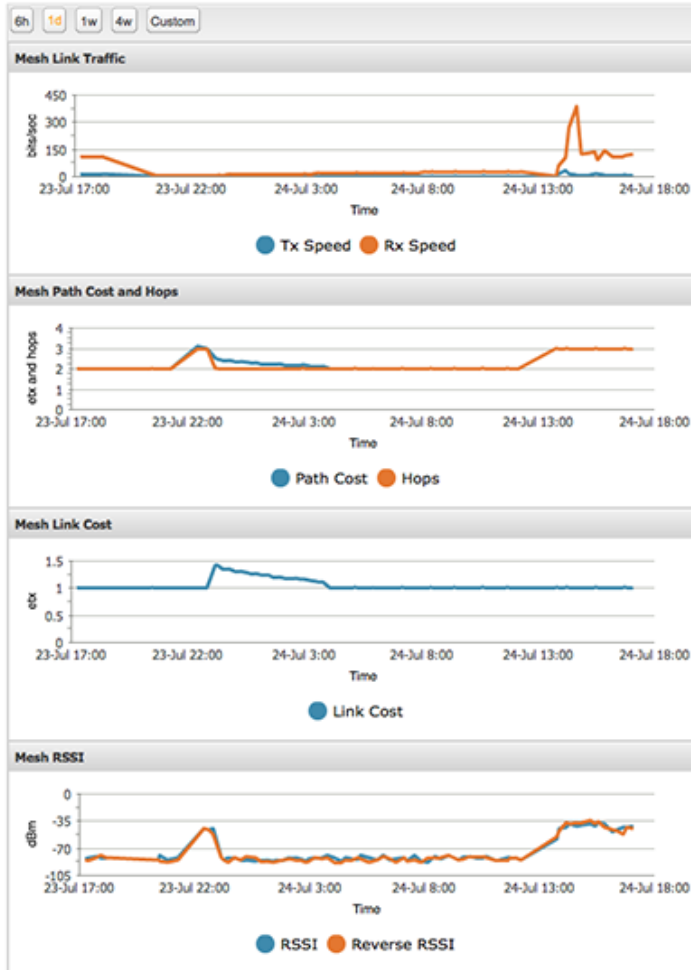
Uptime unknown

Mesh Link Settings

SSID unit
PANID 323
Transmit Power -34
Security Mode 1

Mesh Link Metrics

Mesh Link Transmit Speed 7.32 bits/sec
Mesh Link Receive Speed 121.63 bits/sec
Mesh Link Transmit Packet Drops 0 drops/sec
Mesh Route RPL Hops 3 hops
Mesh Route RPL Link Cost 1
Mesh Route RPL Path Cost 3
Mesh Route RSSI -42 dBm
Mesh Route Reverse RSSI -45 dBm



Network Interfaces

Interface	Admin Status	Oper. Status	IP Address	Physical Address	Tx Speed (bits/sec)	Tx Drops (bits/sec)	Rx Speed (bits/sec)
lo	up	up	0:0:0:0:0:0:1::64		0		0
lowpan	up	up	2001:dead:beef:6108:217:3bab:3c:3100/64 fe80:0:0:217:3bab:3c:3100/64	00173bab003c3100	6.8		139.55
ppp	up	up	fe80:0:0:0:0:0:1::64	00173bab003c3100	13.24		7.43

Network Routes

Destination	Next Hop IP Address	Next Hop Element ID	Interface	Hops	Path Cost	Link Cost	RSSI	Reverse RSSI
default	fe80:0:0:217:3bab:3c:3102	00173BAB003C3102	lowpan	3	3	1	-39	-43

Routing Path

Hops	IP Address	Element ID	Status	Last Heard
this element	2001:dead:beef:6108:217:3bab:3c:3100	00173BAB003C3100	up	2012-07-24 17:05
1 hop	2001:dead:beef:6108:217:3bab:3c:3102	00173BAB003C3102	up	2012-07-24 16:44
2 Hops	2001:dead:beef:6108:217:3bab:3c:3208	00173BAB003C3208	up	2012-07-24 16:53

286000