Case Management Overview

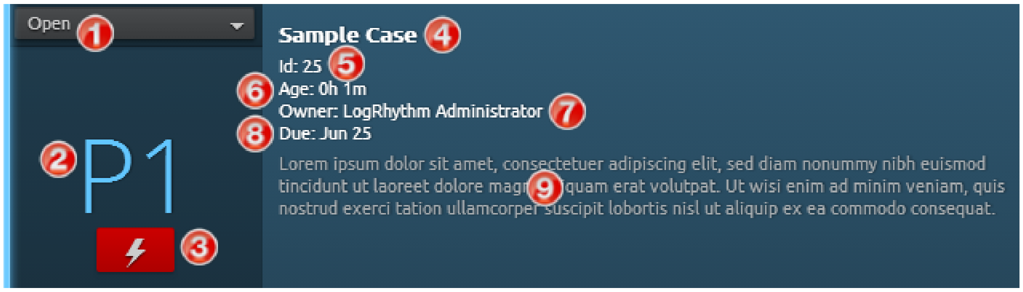
The Case Management feature is a collaborative forensic tool for creating cases to track and document suspicious logs and alarms that are believed to be related to the same threat. The ability to create and own cases, as well as to collaborate on cases that are created and owned by others, extends to all Web Console users.

From the Cases panels on the Dashboards, Alarms, and Analyze pages, you can conveniently open new cases and build upon existing ones whenever you encounter logs, alarms, or files that can be used as evidence. The Cases page provides an expanded layout and customizable widgets for you to further view and manage the cases you are working on.

Case Cards

The most basic element of a case is its case card, which you can view from both the Cases page and the Cases panels. In addition to displaying basic details about the case, case cards contain the controls for opening and closing cases and managing their incident statuses.

The elements of a case card are diagrammed in the following image and identified in the subsequent table.



Sample Case

Id: 25

Age: 0h 1m

Owner: LogRhythm Administrator

Due: Jun 25

Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat.

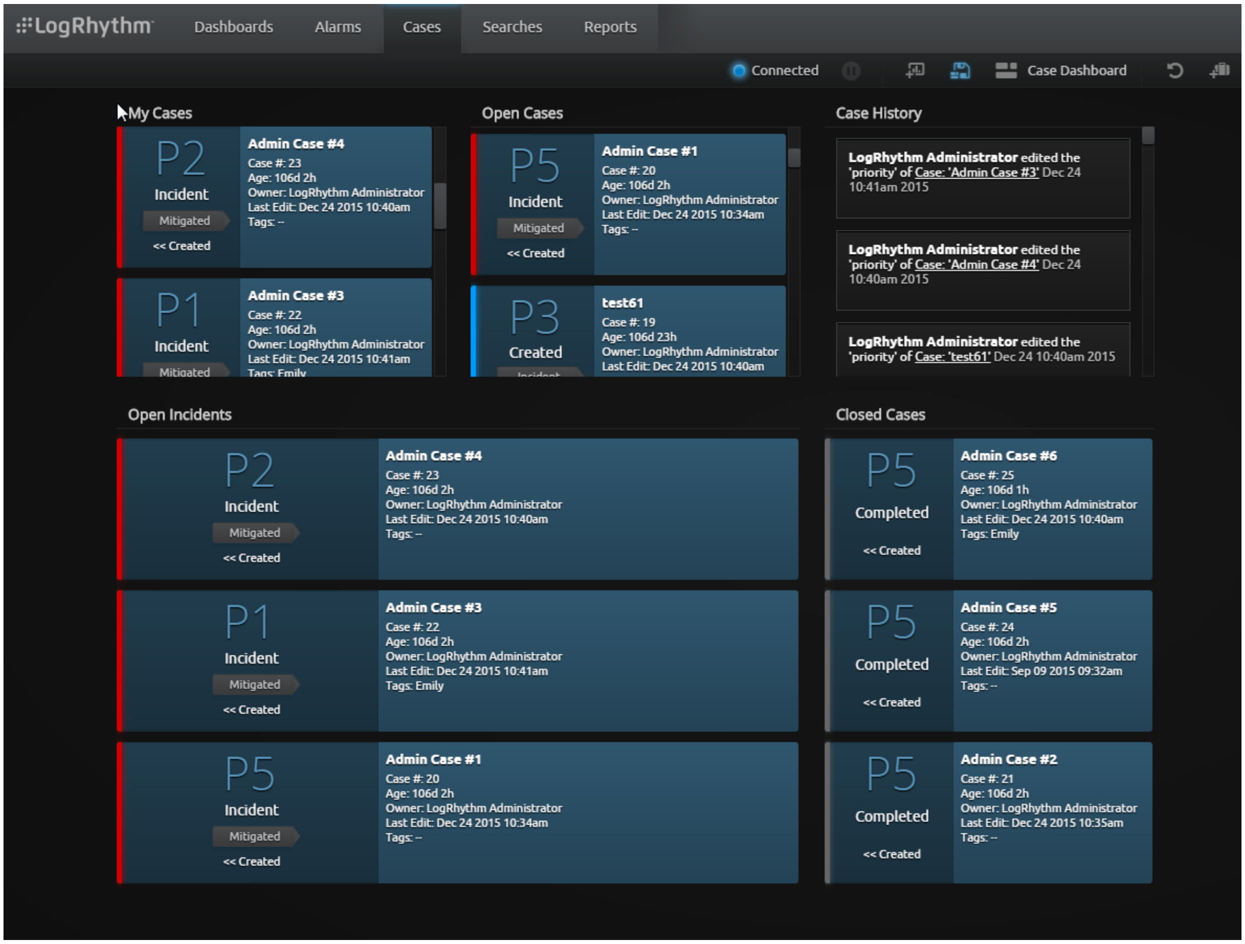
1	Case Open/Close drop-down	6	Case age
2	Priority level	7	Owner
3	Incident status	8	Due date
4	Case name	9	Case summary
5	Case ID*		

* Case ID numbers are based on the order that cases were created.

Cases Page

The Cases page provides a full-page layout with customizable widgets for exploring and managing cases and case trends. For quick access to different types of cases and information, you can create and save multiple dashboard layout configurations for the Cases page.

The following screen shot shows the predefined "Case Dashboard" view.



My Cases

P2 Incident Mitigated << Created
Admin Case #4
Case #: 23
Age: 106d 2h
Owner: LogRhythm Administrator
Last Edit: Dec 24 2015 10:40am
Tags: --

P1 Incident Mitigated
Admin Case #3
Case #: 22
Age: 106d 2h
Owner: LogRhythm Administrator
Last Edit: Dec 24 2015 10:41am
Tags: Emily

Open Cases

P5 Incident Mitigated << Created
Admin Case #1
Case #: 20
Age: 106d 2h
Owner: LogRhythm Administrator
Last Edit: Dec 24 2015 10:34am
Tags: --

P3 Created Incident
test61
Case #: 19
Age: 106d 23h
Owner: LogRhythm Administrator
Last Edit: Dec 24 2015 10:40am

Case History

LogRhythm Administrator edited the 'priority' of Case: 'Admin Case #3' Dec 24 10:41am 2015

LogRhythm Administrator edited the 'priority' of Case: 'Admin Case #4' Dec 24 10:40am 2015

LogRhythm Administrator edited the 'priority' of Case: 'test61' Dec 24 10:40am 2015

Open Incidents

P2 Incident Mitigated << Created
Admin Case #4
Case #: 23
Age: 106d 2h
Owner: LogRhythm Administrator
Last Edit: Dec 24 2015 10:40am
Tags: --

P1 Incident Mitigated << Created
Admin Case #3
Case #: 22
Age: 106d 2h
Owner: LogRhythm Administrator
Last Edit: Dec 24 2015 10:41am
Tags: Emily

P5 Incident Mitigated << Created
Admin Case #1
Case #: 20
Age: 106d 2h
Owner: LogRhythm Administrator
Last Edit: Dec 24 2015 10:34am
Tags: --

Closed Cases

P5 Completed << Created
Admin Case #6
Case #: 25
Age: 106d 1h
Owner: LogRhythm Administrator
Last Edit: Dec 24 2015 10:40am
Tags: Emily

P5 Completed << Created
Admin Case #5
Case #: 24
Age: 106d 2h
Owner: LogRhythm Administrator
Last Edit: Sep 09 2015 09:32am
Tags: --

P5 Completed << Created
Admin Case #2
Case #: 21
Age: 106d 2h
Owner: LogRhythm Administrator
Last Edit: Dec 24 2015 10:35am
Tags: --

Note: In addition to the Cases List and Case History widgets, Global Administrators and Global Analysts have access to "Case Trend by Status" and "Case Trend by Priority" widgets, which can be used on both the Cases and Dashboards pages. These widgets are not available to restricted users.

For more information on Case Trend widgets, see "Case Trend Widgets" on page 115 and "Configuring Case Trend Widget Settings" on page 120.

Case Owners vs. Collaborators

Case Owners:

Case owners have full administrative control over their cases. In addition to being able to add, edit, and remove their own evidence and notes, case owners can edit and remove evidence and notes added by case collaborators. Case owners are also the only users who can perform the following case-related tasks:

- Closing and reopening cases
- Escalating/deescalating case incident statuses
- Editing case names, priorities, due dates, and summaries
- Assigning and removing case collaborators
- Transferring case ownership to another user

Cases cannot have more than one owner at a time. When a case is created, it is owned by the user who created it until ownership is assigned to another user. When owners transfer ownership to other users, their case privileges are immediately reduced to that of a case collaborator. A former owner will remain a collaborator unless and until the new owner removes him or her from the case. The only way a former owner can regain ownership privileges is if the new owner transfers case ownership back to him or her.

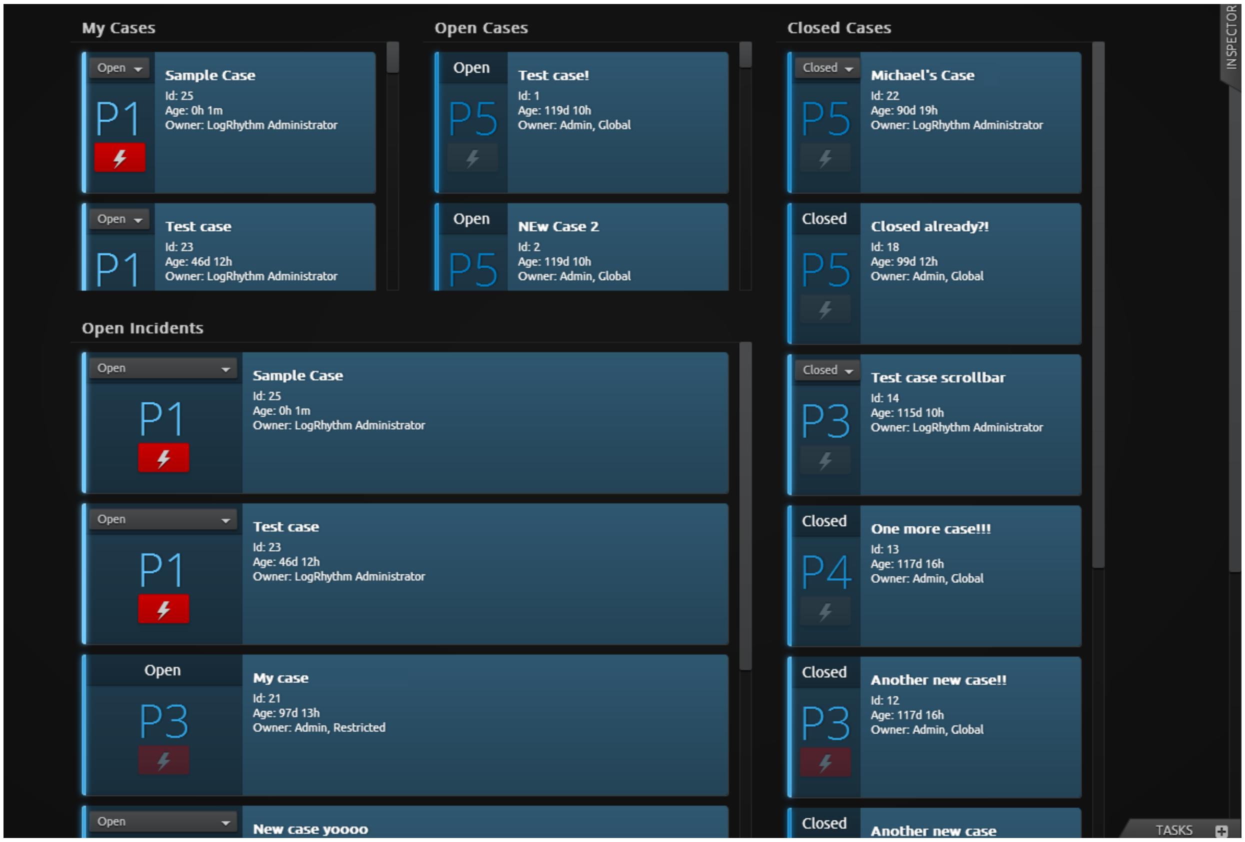
Collaborators:

A case collaborator is either A) a user who has been assigned to help work on a case by the case's owner or B) a former case owner who has not been removed from the case by the new owner. Collaborators can view all the evidence and notes that have been attached to a case and add to them as needed. Collaborators can edit or remove any notes or evidence that they add to a case, but they cannot edit or remove contributions made by other users.

Only case owners can add or remove collaborators. Collaborators can neither add nor remove themselves from cases.

Case List Widgets

Case List widgets allow you to view, sort, and manage cases. They are available for use only on Cases page layouts. The following screen shot shows a Cases page layout that uses only Case List widgets, illustrating some of the different ways they can be configured.



My Cases

Open
P1
Sample Case
Id: 25
Age: 0h 1m
Owner: LogRhythm Administrator

Open
P1
Test case
Id: 23
Age: 46d 12h
Owner: LogRhythm Administrator

Open Cases

Open
P5
Test case!
Id: 1
Age: 119d 10h
Owner: Admin, Global

Open
P5
NEw Case 2
Id: 2
Age: 119d 10h
Owner: Admin, Global

Closed Cases

Closed
P5
Michael's Case
Id: 22
Age: 90d 19h
Owner: LogRhythm Administrator

Closed
P5
Closed already?!
Id: 18
Age: 99d 12h
Owner: Admin, Global

Closed
P3
Test case scrollbar
Id: 14
Age: 115d 10h
Owner: LogRhythm Administrator

Closed
P4
One more case!!!
Id: 13
Age: 117d 16h
Owner: Admin, Global

Closed
P3
Another new case!!
Id: 12
Age: 117d 16h
Owner: Admin, Global

Closed
Another new case

Open Incidents

Open
P1
Sample Case
Id: 25
Age: 0h 1m
Owner: LogRhythm Administrator

Open
P1
Test case
Id: 23
Age: 46d 12h
Owner: LogRhythm Administrator

Open
P3
My case
Id: 21
Age: 97d 13h
Owner: Admin, Restricted

Open
New case yoooo

Configuring Case List Widget Settings

You can reconfigure Case Lists widgets by filtering and/or resorting the cases that they display. You can also change their titles to give them more meaning.

Case List filter options:

- **Status**: Display only opened or closed cases. The default setting ("Any") displays them both.
- **Is Incident?**: Display only Incidents or non-Incidents. The default setting ("Any") displays them both.
- **Owner**: Display only your own cases or the cases that are owned by a particular user. The default setting ("Any") displays all cases regardless of who owns them.

Case List sort order options:

- **Age (Asc)**: Sort by age in ascending order (newest to oldest – this is the default sort).
- **Age (Desc)**: Sort by age in descending order (oldest to newest).
- **Priority (Asc)**: Sort by priority numbers in ascending order (highest to lowest).

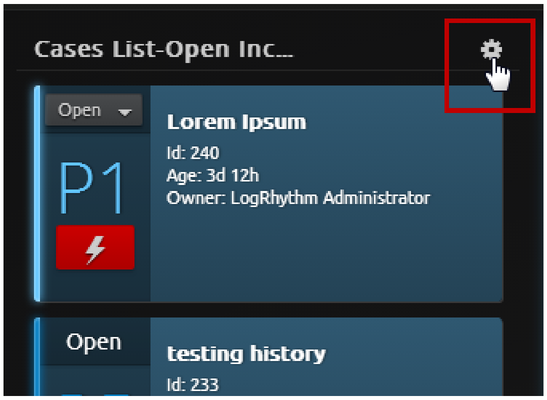
- **Priority (Desc)**: Sort by priority numbers in descending order (lowest to highest).
- **Status**: Sort by opened and closed status (open cases display on top).

To configure Case List widgets:

1. From the Cases page, hover your cursor over the Case List widget that you want to reconfigure.

   The Settings icon appears on the upper-right side of the widget.

2. Click the **Settings** icon.

   Cases List-Open Inc...

   Lorem Ipsum
   Id: 240
   Age: 3d 12h
   Owner: LogRhythm Administrator

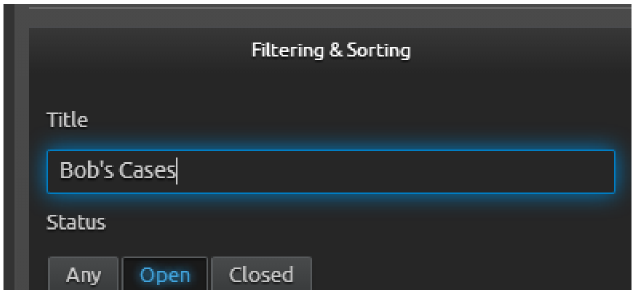
   testing history
   Id: 233

   A blue border appears around the widget and the Inspector panel opens on the right.

3. From the Inspector panel, do one or both of the following:

   - Enter a new title for the widget.

     a. Click in the **Title** text field at the top of the Inspector.

     Filtering & Sorting

     Title: Bob's Cases

     Status: Any [✓ Open] Closed

     b. Delete existing text as needed and enter a new title.

   - Use the toggle buttons and drop-down menus to modify filtering and sorting options (described at the beginning of the topic) as needed.

4. When you are finished with your changes, click the **Close** icon (☒) on the upper-left side of the panel to exit the Inspector.

The Save icon in the toolbar on the upper-right side of the page begins flashing blue, indicating that changes have been made to the layout (modifying a widget amounts to modifying a dashboard layout).

For instructions on saving your changes, see "Saving Dashboard Layout Changes" on page 43.

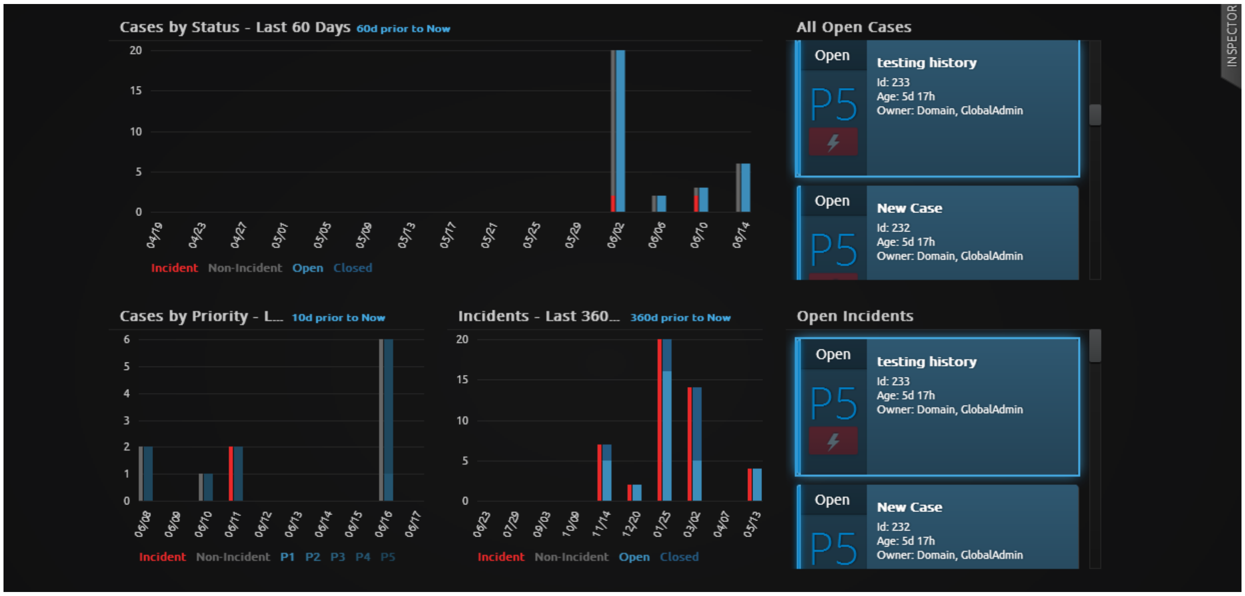
Case Trend Widgets

Note: Case Trend widgets are available only to Global Administrators and Global Analysts.

Case Trend widgets display bar charts that allow global users to monitor case status and priority trends as they relate to case creation dates. Case trending data provides an additional means for identifying threat patterns and making predictions. It can also be used to help gauge user activity levels on the Web Console.

Two types of Case Trend widgets are available: "Case Trend by Status" and "Case Trend by Priority." Both of these widgets can be applied on Dashboards and Cases page views. For more information on the charts displayed by Case Trend widgets, see "Reading Case Trend by Status Charts" below and "Reading Case Trend by Priority Charts" on page 119.

The following graphic shows the predefined "Case Management Dashboard" view (available only to Global Administrators and Analysts), which features three Case Trend and two Case List widgets.


Cases by Status - Last 60 Days 60d prior to Now
20
15
10
5
0
04/19
04/23
04/27
05/01
05/05
05/09
05/13
05/17
05/21
05/25
05/29
06/02
06/06
06/10
06/14
Incident Non-Incident Open Closed
Cases by Priority - L... 10d prior to Now
6
5
4
3
2
1
0
06/08
06/09
06/10
06/11
06/12
06/13
06/14
06/15
06/16
06/17
Incident Non-Incident P1 P2 P3 P4 P5
Incidents - Last 360... 360d prior to Now
20
15
10
5
0
06/23
07/29
09/03
10/09
11/14
12/20
01/25
03/02
04/07
05/13
Incident Non-Incident Open Closed
INSPECTOR

All Open Cases

Open
P5
testing history
Id: 233
Age: 5d 17h
Owner: Domain, GlobalAdmin

Open
P5
New Case
Id: 232
Age: 5d 17h
Owner: Domain, GlobalAdmin

Open Incidents

Open
P5
testing history
Id: 233
Age: 5d 17h
Owner: Domain, GlobalAdmin

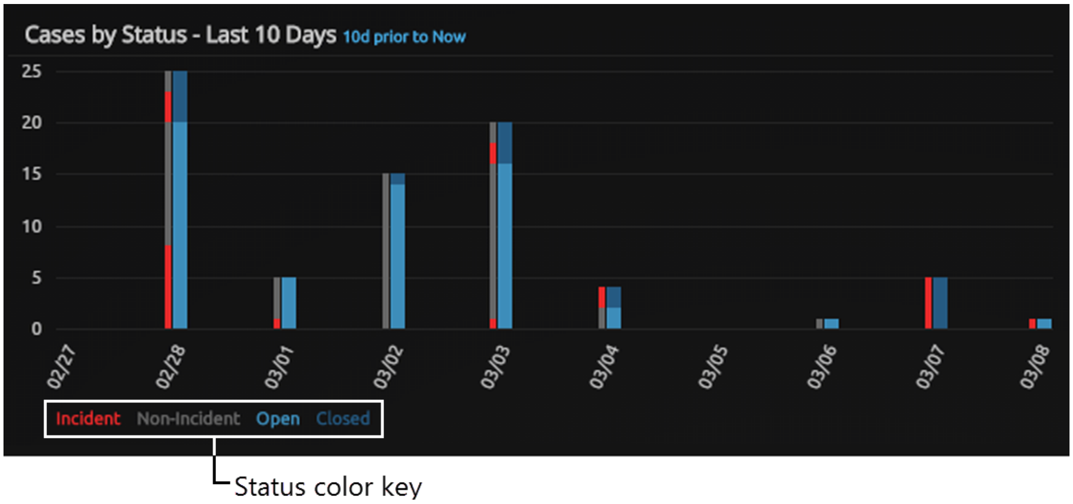
Open
P5
New Case
Id: 232
Age: 5d 17h
Owner: Domain, GlobalAdmin

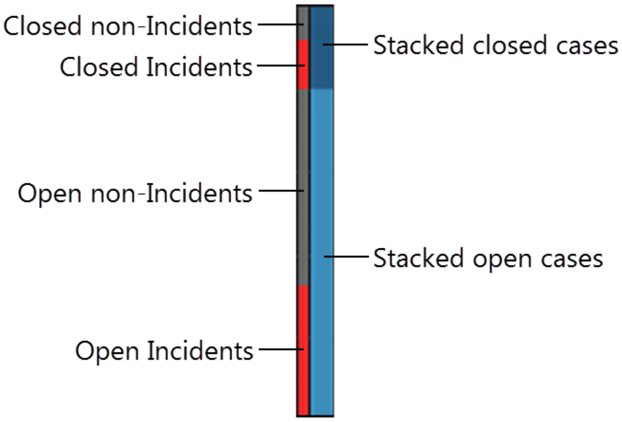
Reading Case Trend by Status Charts

Case statuses fall into four different categories: open Incidents, closed Incidents, open non-Incidents, and closed non-Incidents. Case Trend by Status charts provide visual representations of case statuses and activity in terms of A) the number of cases created at different points in time and B) the relationship between the time cases were created and their current status.

In Case Trend by Status charts, the horizontal axis plots the range of creation times while the vertical axis measures the total number of cases created. Color-coded stacked bars are used to break down the current statuses of the cases.

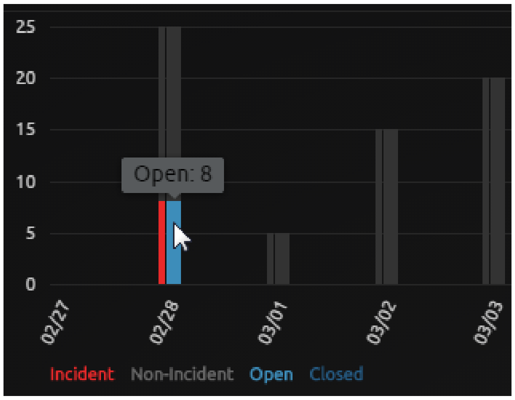
The following graphic shows an example of a Case Trend by Status chart with a 10-day time range. Note the status color key below the horizontal axis.



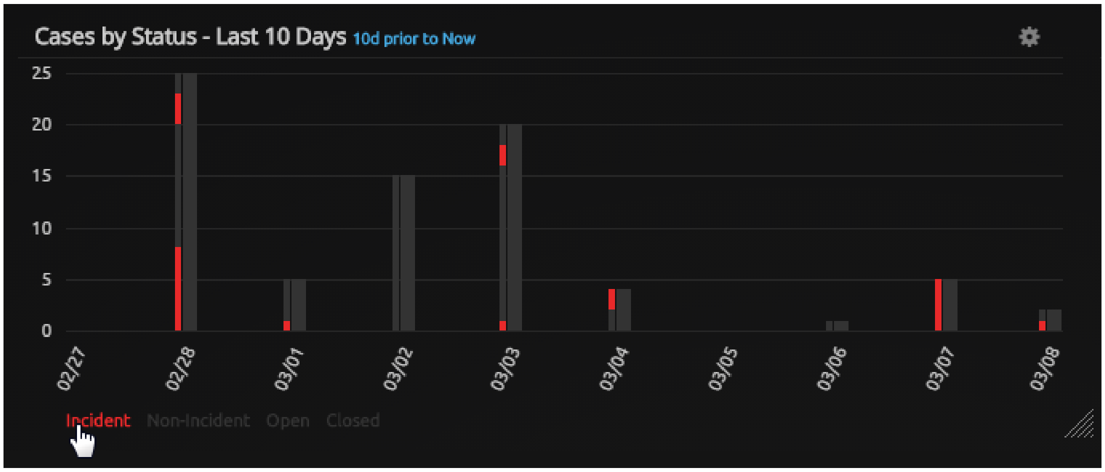


Case Trend by Status charts include interactive features that allow you to do the following:

- To view the count values within a stacked bar, hover your cursor over the different color segments to display them, as demonstrated in the following graphic with the number of open Incidents.

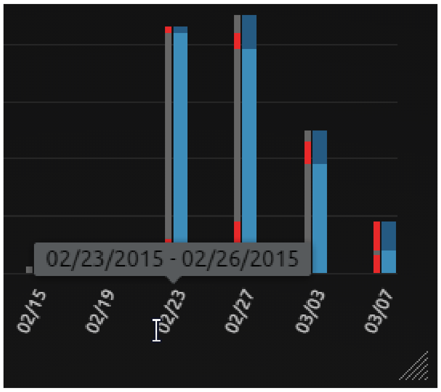


- To focus the chart on a single status, hover your cursor over a status in the chart key below the horizontal axis, as shown with the Incident status in the following graphic.



Depending on a chart's width (as defined by the number of dashboard columns that it spans) and the scope of its time range, data bars may represent a group of consecutive dates as opposed to the single dates listed along the horizontal axis. For instance, group dates are standard for one- and two-column charts with time ranges greater than 10 days.

- To determine the exact date span that each bar represents, hover your cursor over the dates along the horizontal axis to display the information, as demonstrated with the *02/23* date in the following graphic.

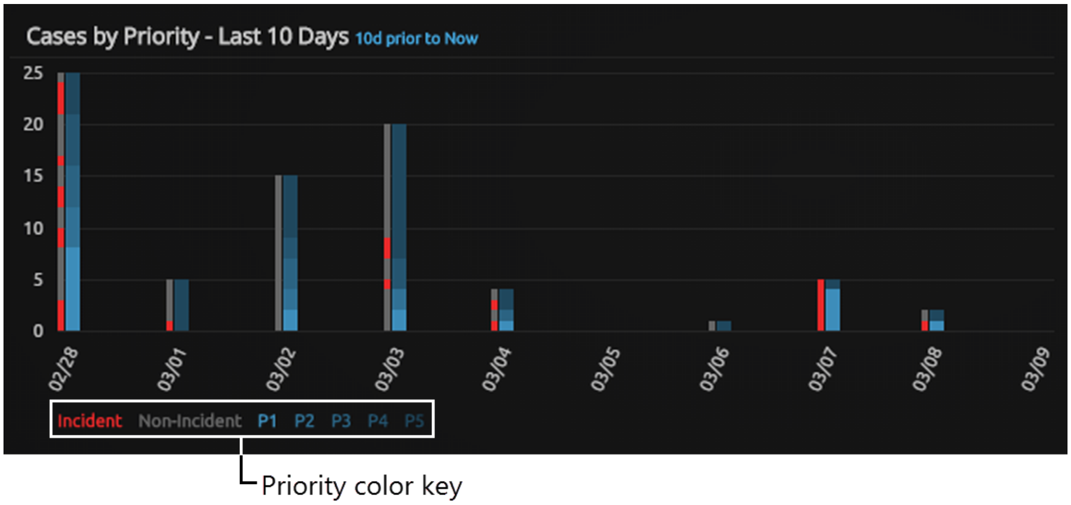


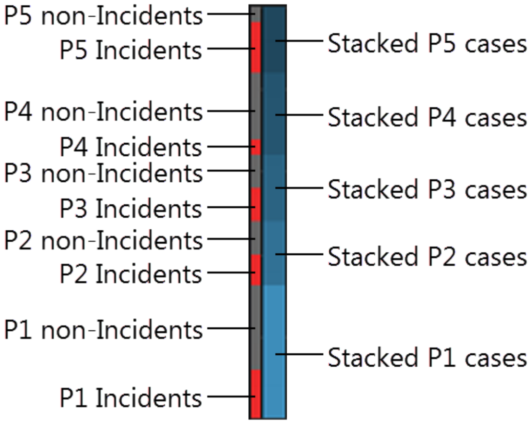
Reading Case Trend by Priority Charts

Case Trend by Priority charts display case distribution trends as they relate to case creation dates and their current priority levels. Priority levels range from P1 to P5, with P1 cases being the highest priorities and P5 the lowest. Case priority levels should also be considered in conjunction with whether or not they been flagged as Incidents.

In Case Trend by Priority charts, the horizontal axis plots the range of creation dates while the vertical axis measures the total number of cases created. Color-coded stacked bars are used to break down the current priority levels of both Incident and non-Incident cases.

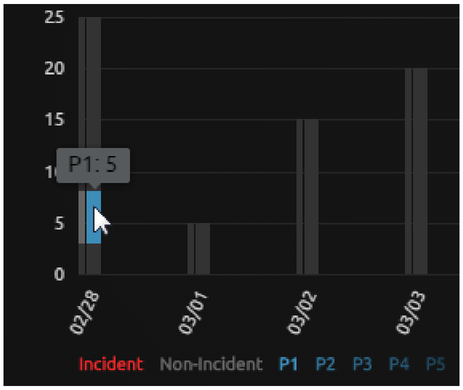
The following graphic shows an example of a Case Trend by Priority chart for cases created within the last 10 days. Note the priority color key below the horizontal axis.



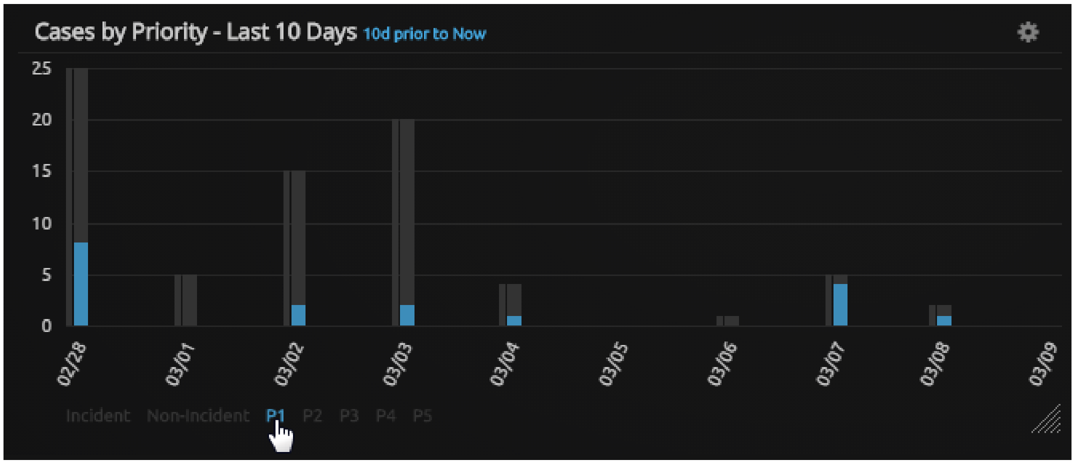


Case Trend by Priority charts include interactive features that allow you to do the following:

- To view the count values within a stacked bar, hover your cursor over the different color stacks to display the numbers, as demonstrated in the following graphic with the number of P1 non-Incidents.

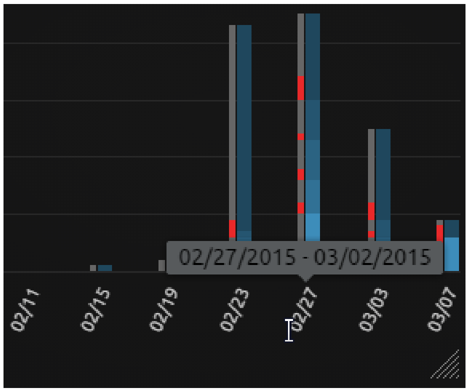


- To focus the chart on a single priority, hover your cursor over a priority in the chart key, as demonstrated in the following graphic with P1 Cases.



Depending on a chart's width (as defined by the number of dashboard columns that it spans) and the scope of its time range, data bars may represent a group of consecutive dates as opposed to the single dates listed along the horizontal axis. For instance, group dates are standard for one- and two-column charts with time ranges greater than 10 days.

- To determine the exact date span that each bar represents, hover your cursor over the dates along the horizontal axis to display the information, as demonstrated with the *02/27* date in the following graphic.



Configuring Case Trend Widget Settings

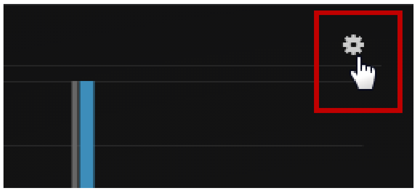
You can reconfigure Case Trend widgets by changing their time ranges and/or filtering the types of cases that they display. You can also change their titles to give them more meaning. The following instructions can be applied to both Case Trend by Status widgets *and* Case Trend by Priority widgets.

To configure Case Trend widgets:

1. Hover your cursor over the Case Trend widget that you want to modify.

   A Settings icon appears on the upper-right side of the widget.

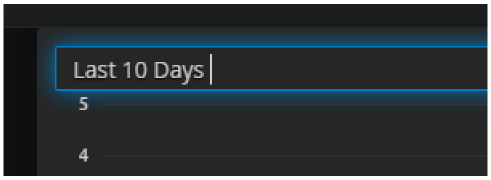
2. Click the **Settings** icon.



   A blue border appears around the widget and the Inspector panel opens on the right.

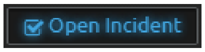
3. From the Inspector panel, do any of the following:

- Click in the **Title** text field at the top of the widget and enter a new title.

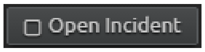

Last 10 Days

- In the **Show Stacks** field, click to select the check boxes for the status/priority bars that you want visible, and/or click to clear the check boxes for status/priority bars that you want hidden.

  Selected check boxes have glowing blue text:


☑ Open Incident

  Cleared check boxes have plain light-gray text:


□ Open Incident

- In the **Time Range** field, click the drop-down list and select a time range.
- In the **Prior To** field, click either **Now** or **Selected Date** for the time range.

  If you clicked "Selected Date," a calendar picker appears. Click to select a date in it. You can scroll through the months as needed by using the left (<) and right (>) angle brackets.

Note: Depending on a Trend Chart's width (as measured by the number of dashboard columns it occupies) and the number of days in its time range, data bars may represent a group of consecutive dates despite having only single dates listed on the horizontal axis. Refer to the following table for information on different Trend Chart widget configurations in terms of the number of bars they display and the number of days that each bar represents.

Time Range	Columns Wide	Number of Data Bars	Days Per Bar
10 days	1–4	10	10
30 days	1	10	3
30 days	2	15	2