Cisco Crosswork Situation Manager 7.0.x Operator Guide

Powered by Moogsoft AIOps 7.0.1

Last Updated: November 29, 2018

Getting Started

Cisco Crosswork Situation Manager collects raw data, called events, from your monitoring systems. It applies machine learning to deduplicate events into alerts and to group similar alerts into Situations so you can focus on resolving critical issues.

The following video introduces the Operator workflow and incident management process:

For more information about events, alerts, and Situations, watch the following video:

Launch Cisco Crosswork Situation Manager

Before You Begin

This guide assumes that an administrator has already set up your Cisco Crosswork Situation Manager system and that it integrates with monitor tools that provide event data about the systems you support.

Your Cisco Crosswork Situation Manager administrator should provide you following so that you can log in to Cisco Crosswork Situation Manager:

- Your username
- Your password
- The Cisco Crosswork Situation Manager server name

If you do not have any of these things then contact your Cisco Crosswork Situation Manager administrator.

If you are a Cisco Crosswork Situation Manager administrator and want information about system setup and configuration, see the Administrator Guide.

Log in to Cisco Crosswork Situation Manager

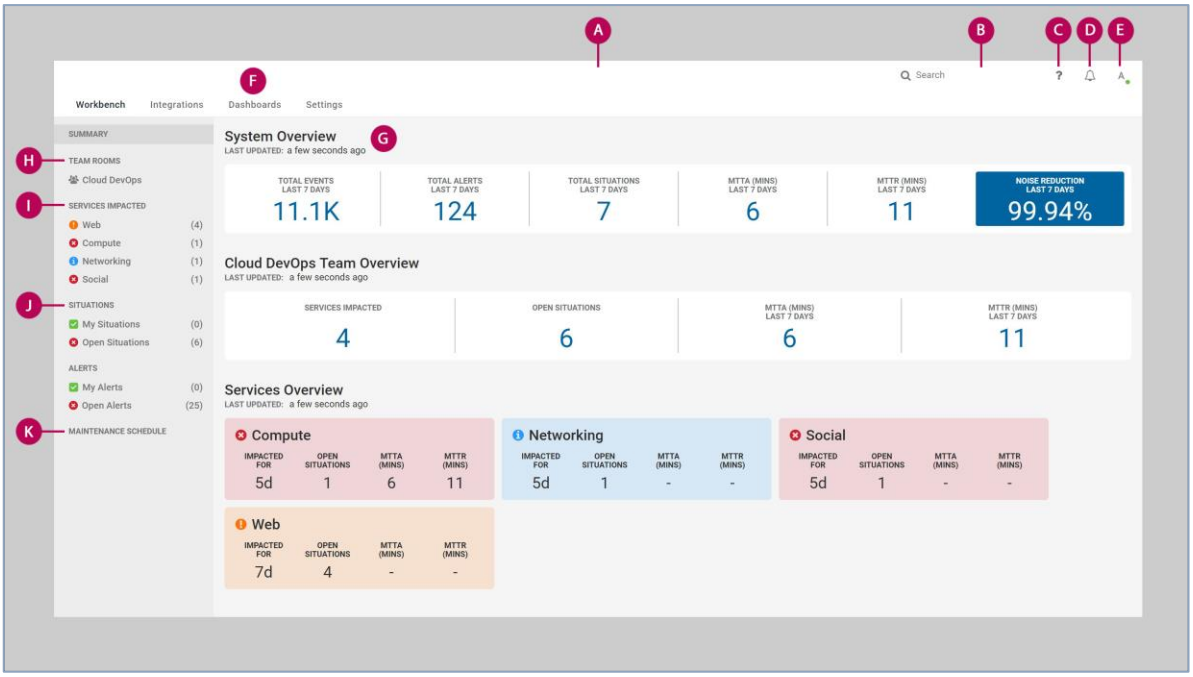
When you're ready you can access your Cisco Crosswork Situation Manager system at the link provided by your administrator using one of the following browsers:

- Apple Safari, latest version
- Google Chrome, latest version
- Microsoft Edge, latest version
- Microsoft Internet Explorer, version 11
- Mozilla Firefox, latest version

Navigate the Cisco Crosswork Situation Manager UI

The Cisco Crosswork Situation Manager UI is split into several key components including the top bar, workbench summary and side menu.

The sections below give a brief overview and description of these components. Click any of the links on this page for more information.



A. Workbench - The Workbench is the default landing page and working area where you will spend most of your time.

B. Search Bar - Allows you to perform a contextual search for a specific alert or Situation or both alerts and Situations.

C. Help & Support - Provides links for help, tutorials and support information such as your version number, database schema and upgrade history.

D. Notifications - Displays notifications about invitations and assignments. See Notifications.

E. User Menu - The User Menu is where you can perform a number of user-related actions such as changing personal details and customizing Cisco Crosswork Situation Manager.

Note: If you forget your password, please contact administrator to reset it.

F. Dashboards - Dashboards are screens comprising of a series of widgets which offer overviews and statistics for different aspects of Cisco Crosswork Situation Manager.

G. Workbench Summary - Displays an overview of statistics for your system, for your teams and for your Services.

H. Team Rooms - Links to the Team Room(s) for your team(s).

I. Services Impacted - Displays all Services monitored by your team which are impacted by Situations.

Note: The Services Impacted in the side menu will update every minute. The Situations and alerts counts will update in real time.

J. Situation and Alert Views - Displays Situations and alerts which are assigned to you under My Situations and My Alerts, as well all unresolved Situations and Alert under Open Situations and Open Alerts.

K. Maintenance Schedule - Schedules maintenance windows if you want to reduce noise so do not want new Situations being created.

Summary Overviews

The System Overview offers a high-level overview of the key statistics for your Cisco Crosswork Situation Manager system such as the noise reduction and the number of Events, Alerts or Situations over the past week. These statistics are automatically updated every five minutes. It also displays the mean time to acknowledge (MTTA) in minutes and the mean time to resolve (MTTR) over the past week.

The Team Rooms displays an overview for your team and includes statistics about the number of impacted Services, situations assigned to the team, the MTTA and MTTR in minutes. These statistics are automatically updated every five minutes.

The Services Overview displays the latest impacted Services and the number of hours or days the Services have been affected. The color of each Service panel indicates the highest severity of the Situations impacting it.

Note: The 'Impacted For' and 'Open Situations' statistics will update every minute. The 'MTTA' and 'MTTR' will automatically update every hour.

Search Bar

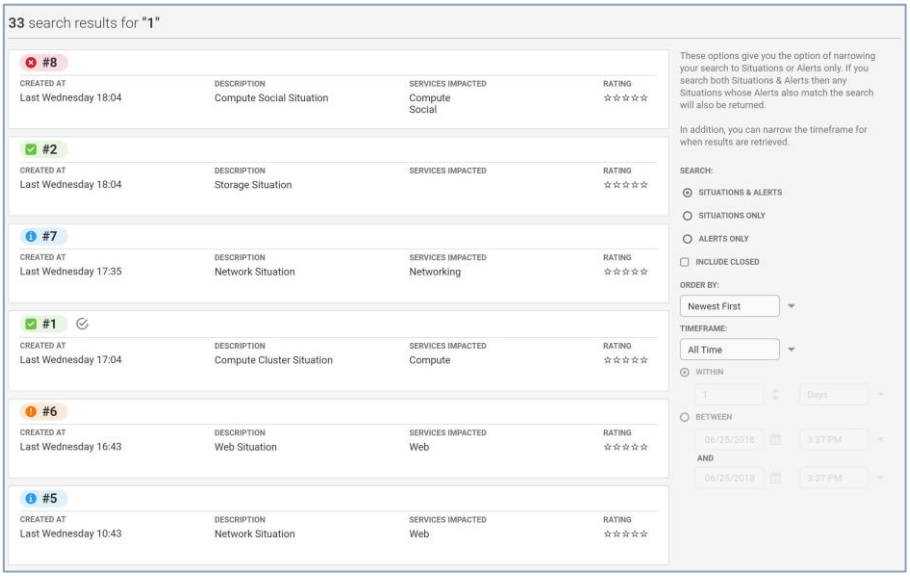
You can use the Search bar in the top bar to quickly find Alerts or Situations you are interested in.

Once a search has been made, you can narrow down the search results to pinpoint exactly what you are looking for.

Enter any alphanumeric text into the Search bar, such a Situation ID number or a Service name, and then hit Enter to continue.

The search results should appear in new screen, showing all successful results relating to both Situations and Alerts by default.

Note: The search results will appear in the order in which they occurred (oldest to most recent in descending order)



You can narrow the search results using the field options on the right side of the screen:

Field	Options	Description

Search	Situations & Alerts Situations Only Alerts Only	Select whether the search results display Situations and Alerts, Situations Only or Alerts Only
Timeframe	All Time Created Last Updated	Select whether the results are for all time, from a created date range or last updated date range
Within	X Minutes X Days X Weeks X Years	Select the number of minutes, days, weeks or years
Between	Date range and time	Select two dates and times of the date range

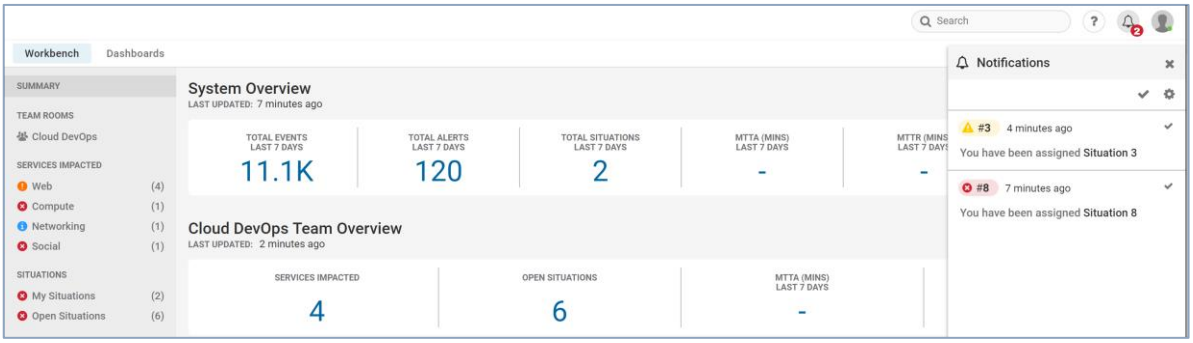
Note: Results generated from the search bar are static.

For example, a search for Situations created within the last hour will show a static list of Situations created within one hour of when the search was carried out. As time progresses, this information becomes out of date. Therefore, to show Situations created within one hour of the present time, carry out the search again to get new results.

Cisco Crosswork Situation Manager Notifications

Notifications keep you informed of your invitations, assignments and any critical Situations in Cisco Crosswork Situation Manager.

You can subscribe to receive Situation notifications about invitations, assignments, critical Situations assigned to your team.



To analyze a Situation in the Situation Room, click the Situation number in the notification.

Mark Notifications as Read or Unread

To mark all notifications as read, click Notifications and then the check icon at the top of the drop-down menu.

To mark one notification as read, click the check icon next to the notification.

A read notification will appear grayed out. Click the check icon again to mark a read notification as unread again.

Configure your Notifications

To configure your notifications, click the Notifications icon on the top bar and then click the Settings cog icon.

You will only receive notifications about invitations and assignments by default. To change the default settings, uncheck 'Use System Defaults' and check one or more of the other 'Type' options from: 'Invitations', 'Assignments' or 'Critical Situations Assigned to My Team'. Click Done to continue.

Note: You must select at least one notification type from the group.

Push Notifications

The settings for push notifications differ depending on which browser you are using for Cisco Crosswork Situation Manager and which browser you are using when the notification is sent:

Instructions for turning push notifications on or off and examples of notifications for different browsers are shown below:

Google Chrome

Push notifications from websites or apps are enabled for Chrome by default. To enable or disable notifications for Windows and Mac, open Chrome and go to Settings > + Show advanced settings.
Under 'Privacy' click Content Settings... and under 'Notifications' choose whether to allow or block notifications.

Apple Safari

Notifications from websites and apps are blocked for Safari by default. To enable notifications, got to Safari > Preferences (⌘,). Click Notifications and then Allow for Cisco Crosswork Situation Manager.

Mozilla Firefox

Mozilla Firefox will ask your permission to allow a notification from a website by default.
To enable or disable Firefox push notifications go to the top left corner of your browser, click the menu icon and open Preferences. Under 'Privacy & Security' > 'Permissions' allow Cisco Crosswork Situation Manager to notify you.

Microsoft Edge

Microsoft Edge will ask your permission to allow a notification from a website by default.
To enable notifications from Cisco Crosswork Situation Manager, go to Advanced Settings > Manage Notifications and set notifications to On for Cisco Crosswork Situation Manager.

Cisco Crosswork Situation Manager for Mobile

Cisco Crosswork Situation Manager for Mobile enables ITOps and DevOps teams to resolve potential incidents at any time and from anywhere using a mobile device. You can send and receive SMS notifications when you assign Situations to colleagues or invite them to Situation Rooms.

System Requirements

The mobile version of Cisco Crosswork Situation Manager is supported by the following browsers and mobile platforms:

Browsers

Browser	Version	iOS	Android

Chrome	Latest	Recommended	Recommended
Safari	Latest	Recommended	N/A

Platforms

The recommended platforms for Cisco Crosswork Situation Manager for mobile are: iPhone SE, iPhone 6, iPhone 7 and iPhone 7 Plus (iOS 10 or higher).

Android phones using OS 6 are also supported. Our browser and platform recommendations are defined as follows:

Recommended - Tested and recommended by Cisco for the optimal solution experience
Supported - Smoke tested and supported by Cisco

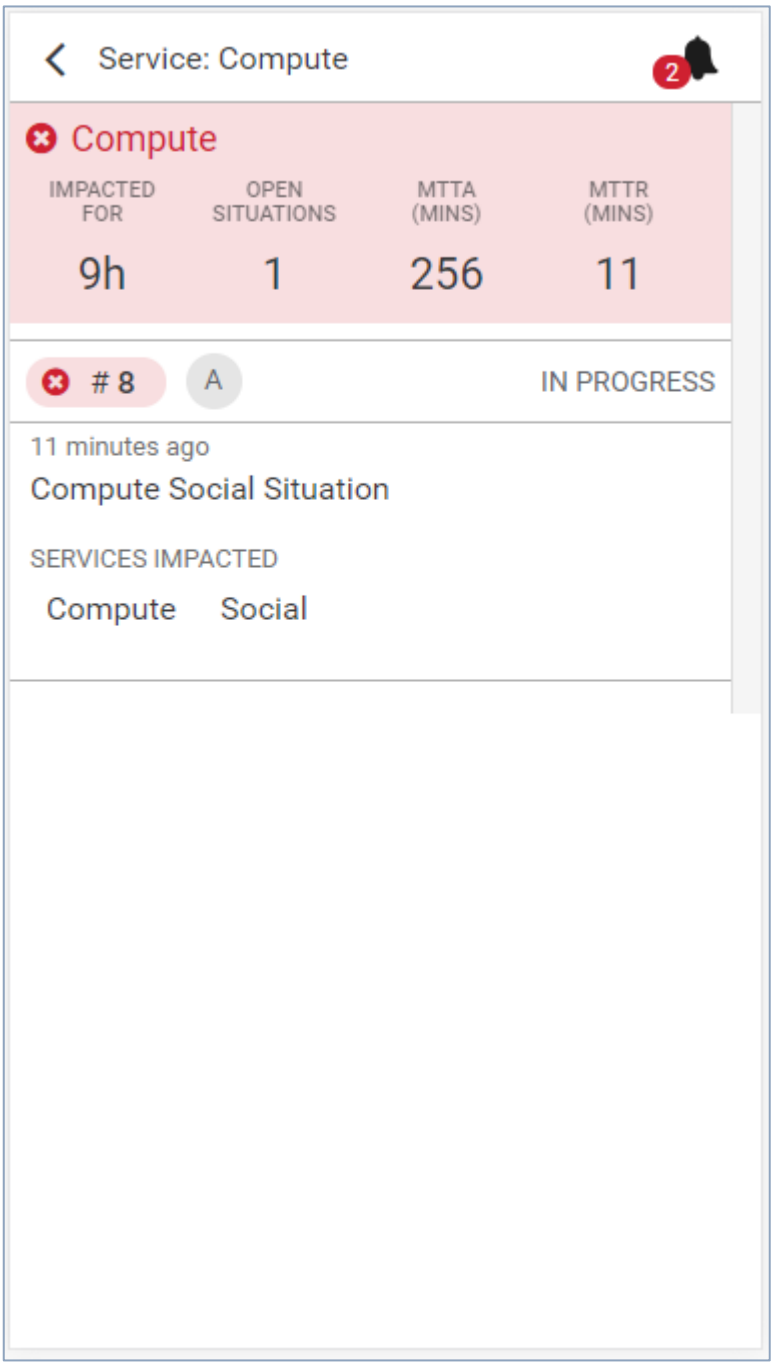
Using Cisco Crosswork Situation Manager for Mobile

The differences between the mobile version and the standard desktop version of Cisco Crosswork Situation Manager are outlined in the sections below:

Navigate on Summary Screens

The Dashboard is divided into two summary screens in mobile, with separate Team Summary and Service Summary screens.

- Tap the Team Summary and Service Summary buttons at the top of the screen to navigate between the screens.
- Swipe up and down on the Service Summary screen to scroll through Services further down on the list.
- Tap any service to view the Situations which are impacting it. The screenshot below shows a single Service view:



Access the Navigation Menu

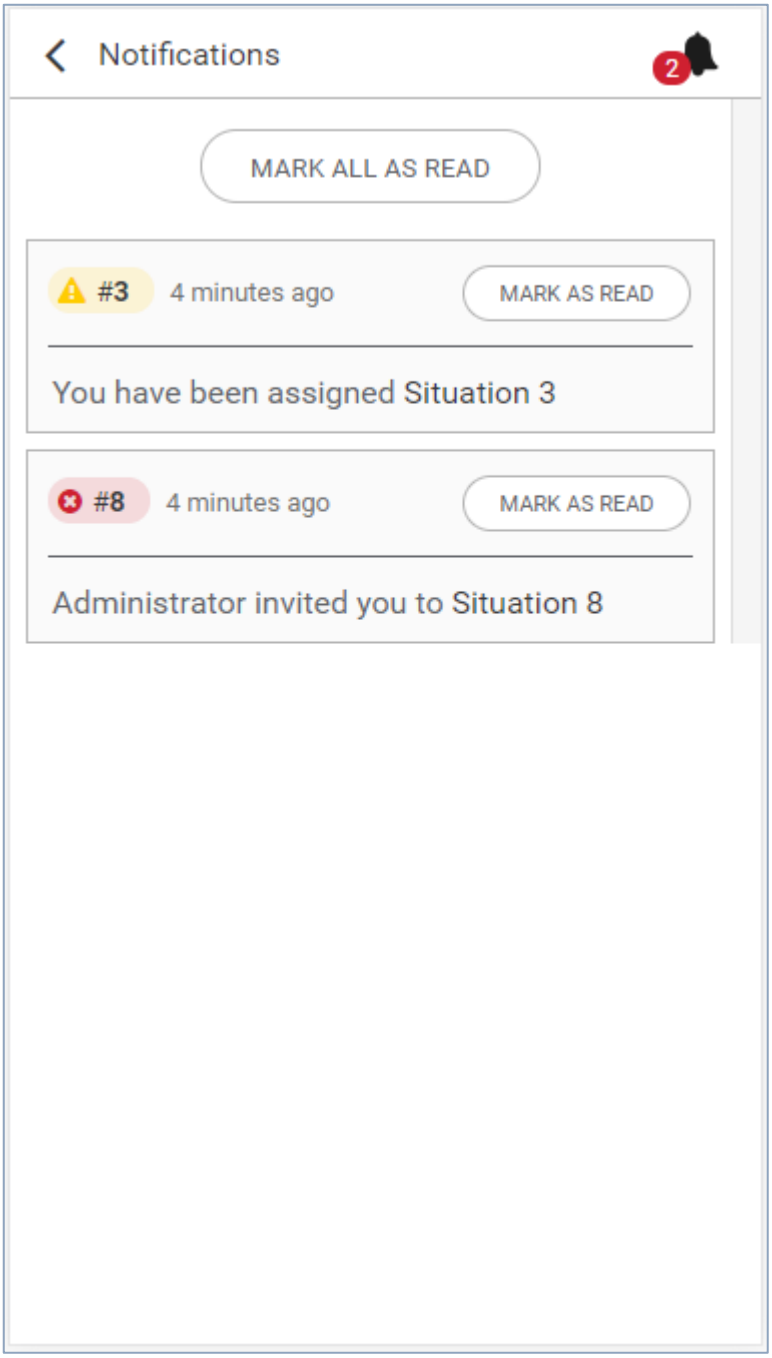
Swipe right from any location to open the navigation menu. The navigation menu has links to the Summary home screen, Settings, My Situations, Open Situations and your Team Rooms.

Tap the bell icon to access Notifications.

Notifications

The Notifications is much the same as the tab in the desktop version but you cannot edit the settings.

Tap Mark As Read to mark a notification as read. Notifications marked as read will appear grayed out.

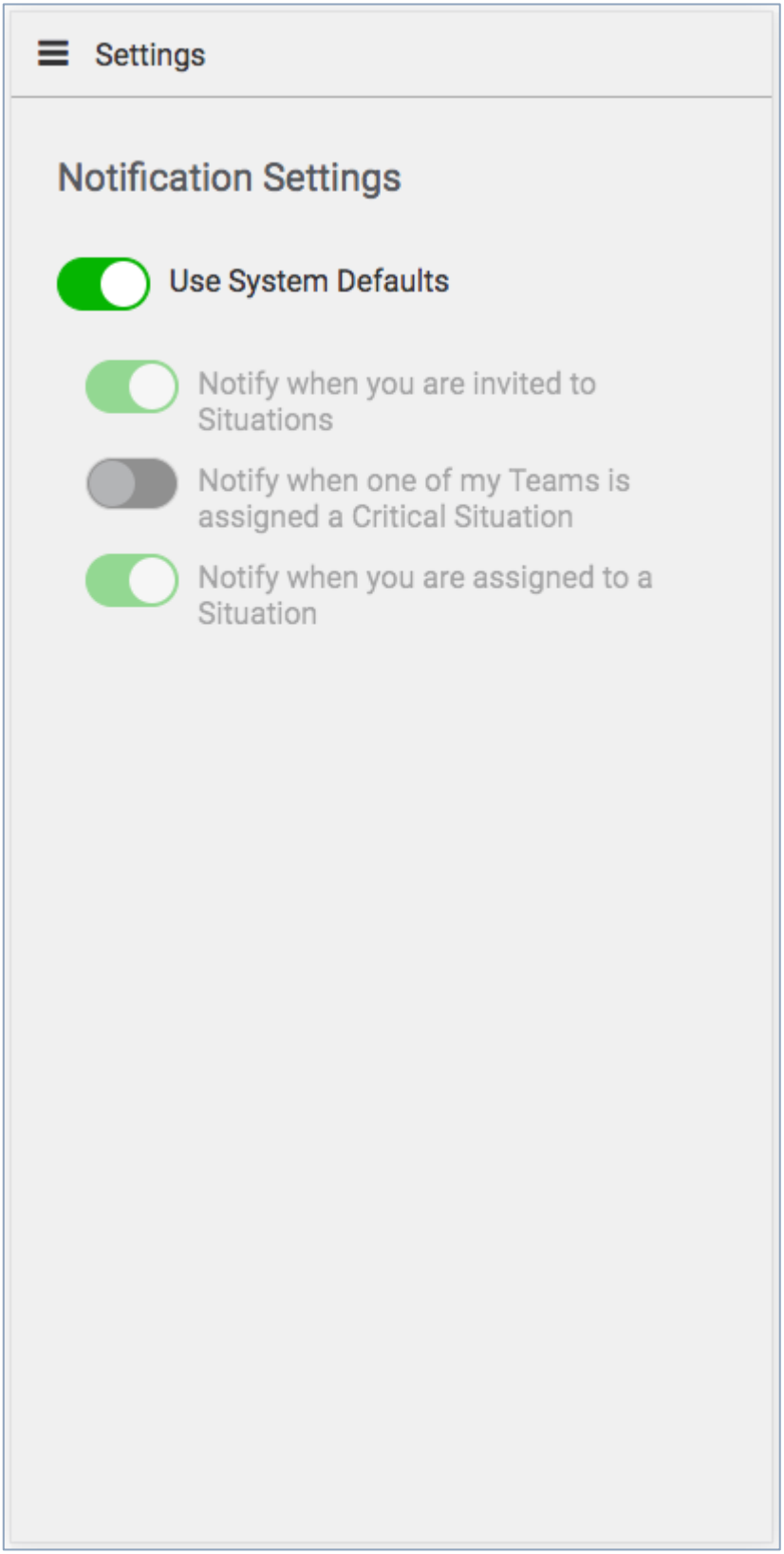


You can configure your notifications and determine which actions you receive notifications about under mobile Settings.

Alternatively go to the desktop version, click Notifications and click the menu icon to open Notification Settings in the desktop version.

Settings

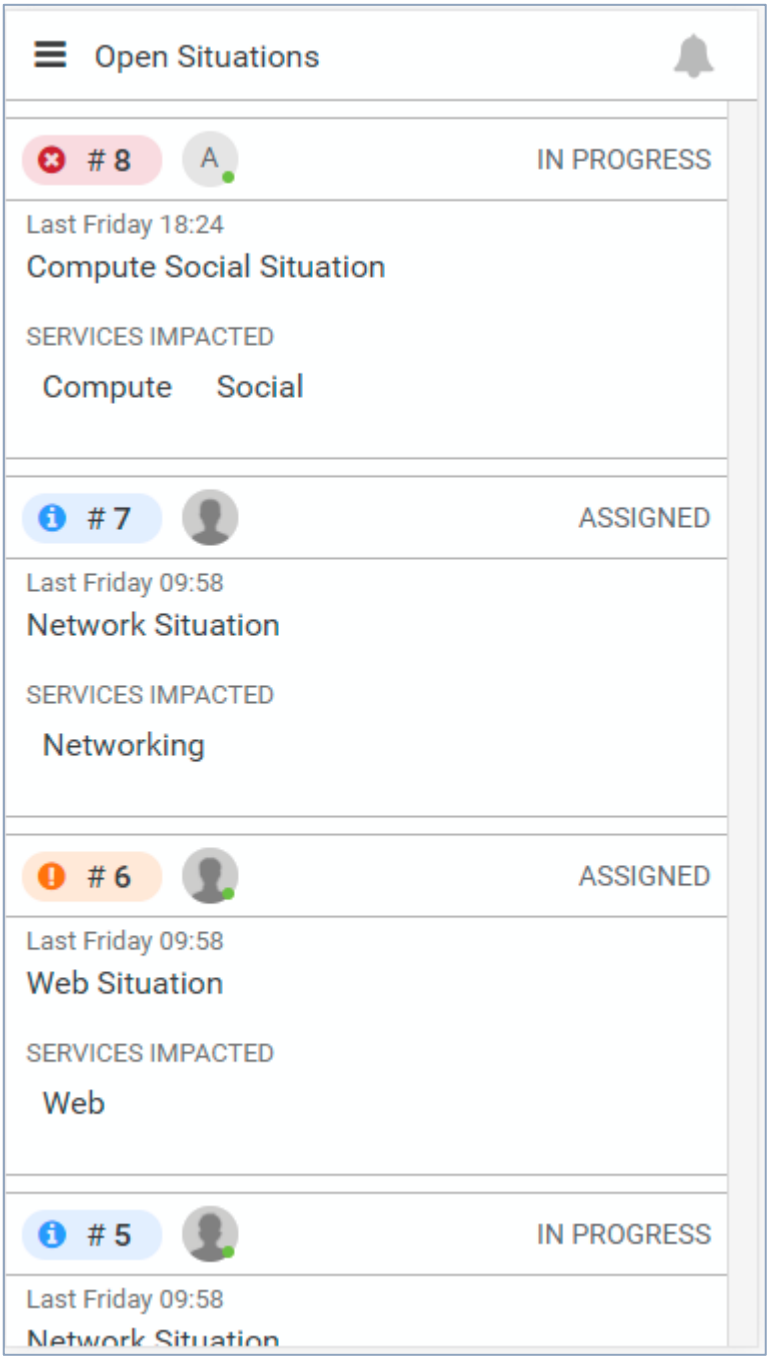
You can choose whether to use the system defaults or configure notifications in mobile Settings.


Settings
Notification Settings
Use System Defaults
Notify when you are invited to Situations
Notify when one of my Teams is assigned a Critical Situation
Notify when you are assigned to a Situation

Touch any of the toggle switches to enable or disable the settings. The toggle switch turns green if the setting is enabled and gray for any setting that is disabled.

Situation Screens

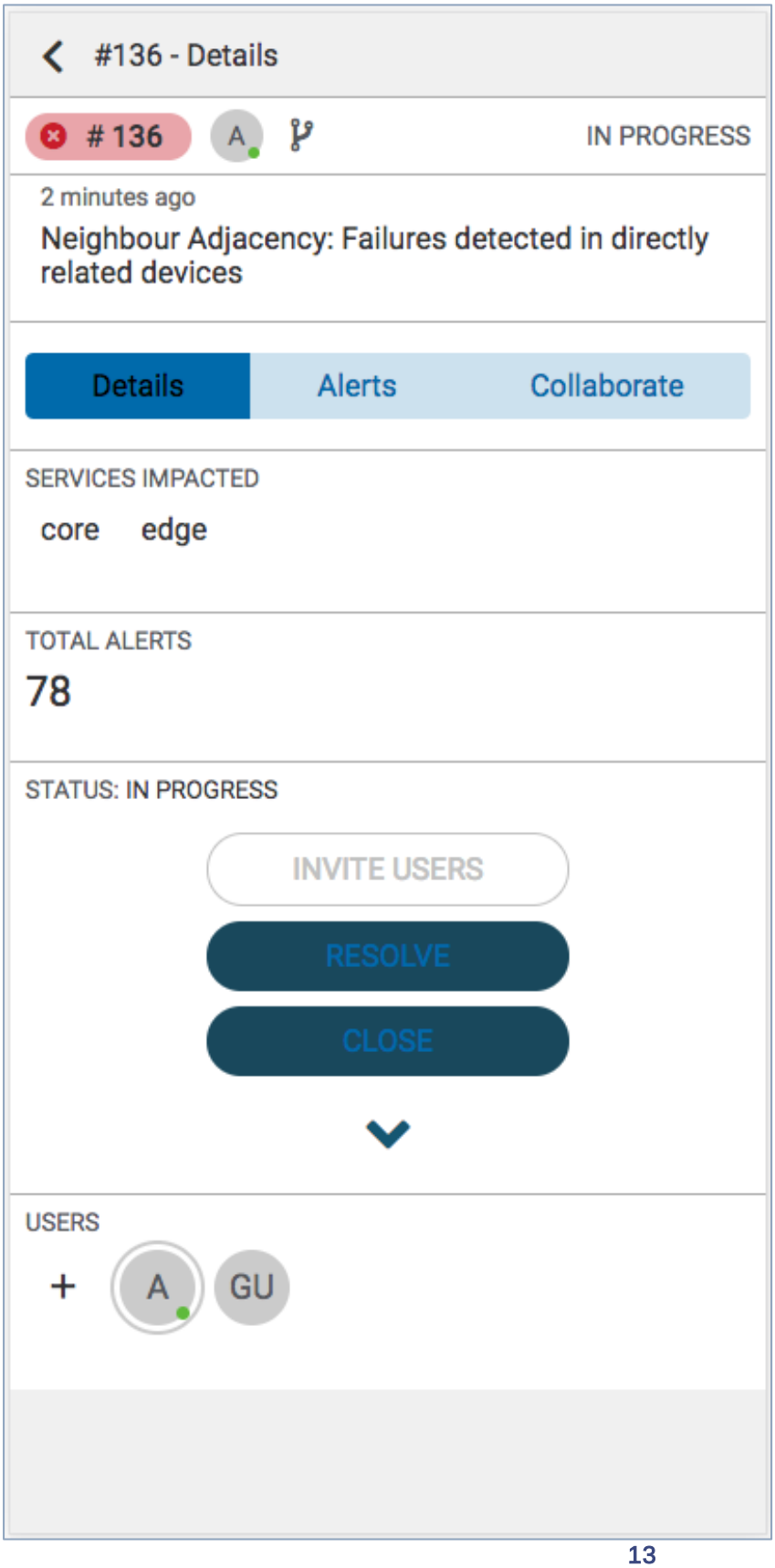
The Situations screens behave in the same way as the desktop version of Cisco Crosswork Situation Manager, displaying all open Situations and all assigned Situations:



Tap a Situation number to open the Situation Room, this is very similar to the desktop version.

Situation Room

The Situation Room screen is split into three tabs: Details, Alerts and Collaborate.


#136 - Details
136
A
IN PROGRESS
2 minutes ago
Neighbour Adjacency: Failures detected in directly related devices
Details
Alerts
Collaborate
SERVICES IMPACTED
core
edge
TOTAL ALERTS
78
STATUS: IN PROGRESS
INVITE USERS
RESOLVE
CLOSE
USERS
+
A
GU

The Details tab displays the current status of the Situation, any Services that are impacted, the total number of Alerts within the Situation and any Users who are in the Situation Room.

Swipe up and down to scroll through the tabs.

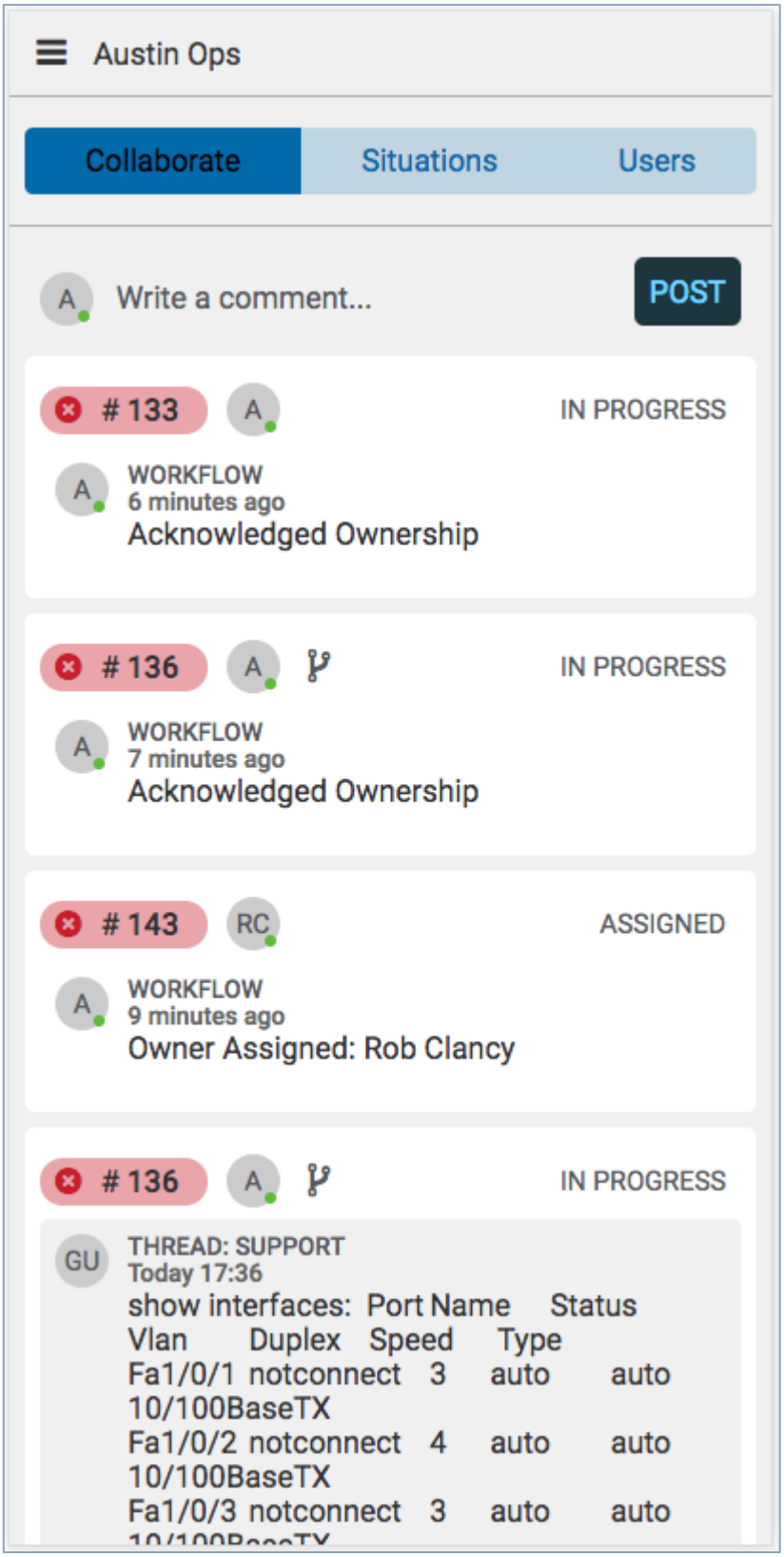
You can message other users using the Collaborate tab. Click Write a comment... and type to write a message.

Alerts associated with the Situation will appear in the Alerts tab. Each Alert will be listed along with the time it was created, the host name and a description.

Team Room

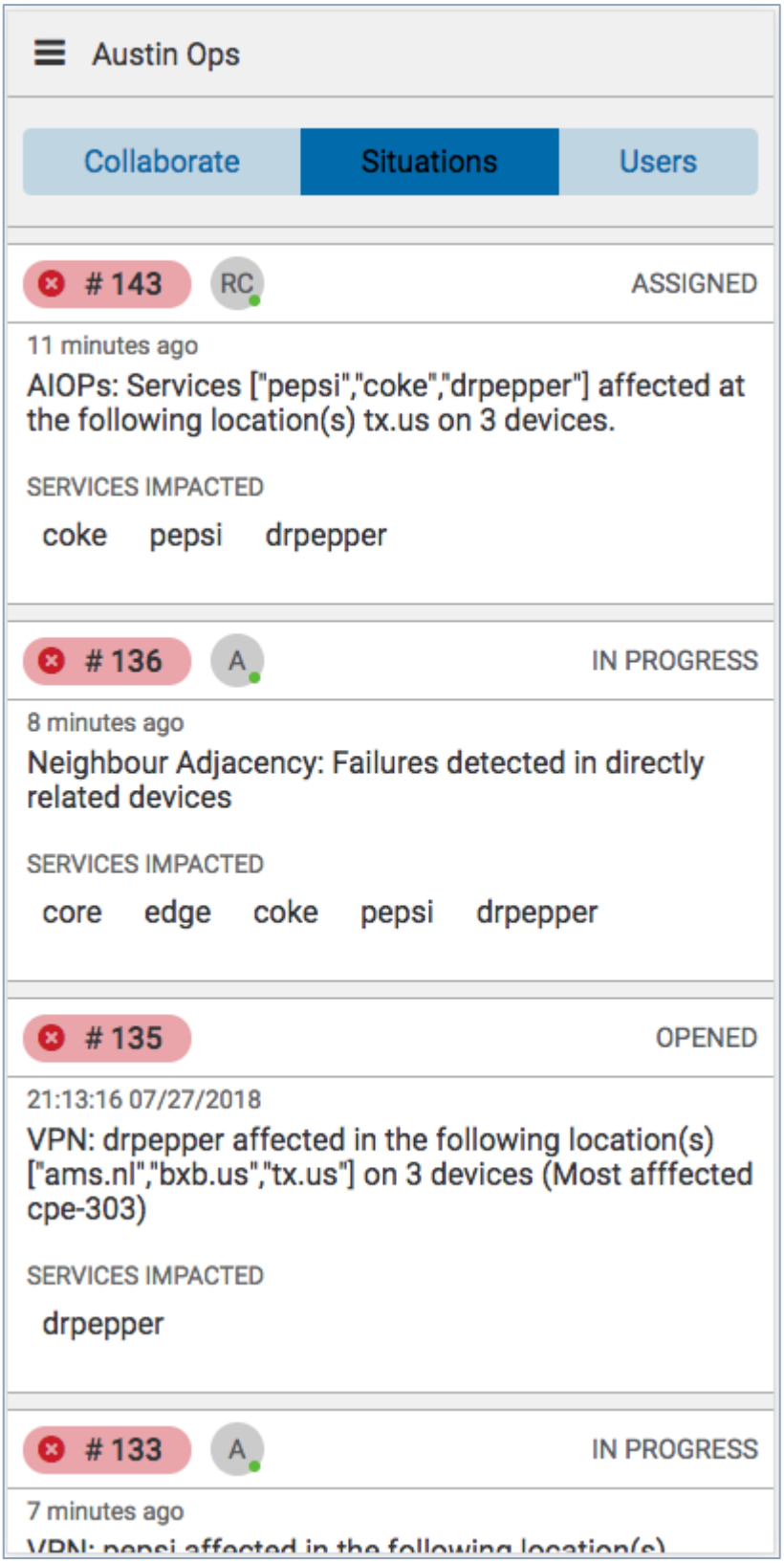
Collaborate

The Collaborate tab displays the all of the latest activity by users who belong to the team.


Austin Ops
Collaborate
Situations
Users
A
Write a comment...
POST
133
A
IN PROGRESS
A
WORKFLOW
6 minutes ago
Acknowledged Ownership
136
A
IN PROGRESS
A
WORKFLOW
7 minutes ago
Acknowledged Ownership
143
RC
ASSIGNED
A
WORKFLOW
9 minutes ago
Owner Assigned: Rob Clancy
136
A
IN PROGRESS
GU
THREAD: SUPPORT
Today 17:36
show interfaces: Port Name Status
Vlan Duplex Speed Type
Fa1/0/1 notconnect 3 auto auto
10/100BaseTX
Fa1/0/2 notconnect 4 auto auto
10/100BaseTX
Fa1/0/3 notconnect 3 auto auto

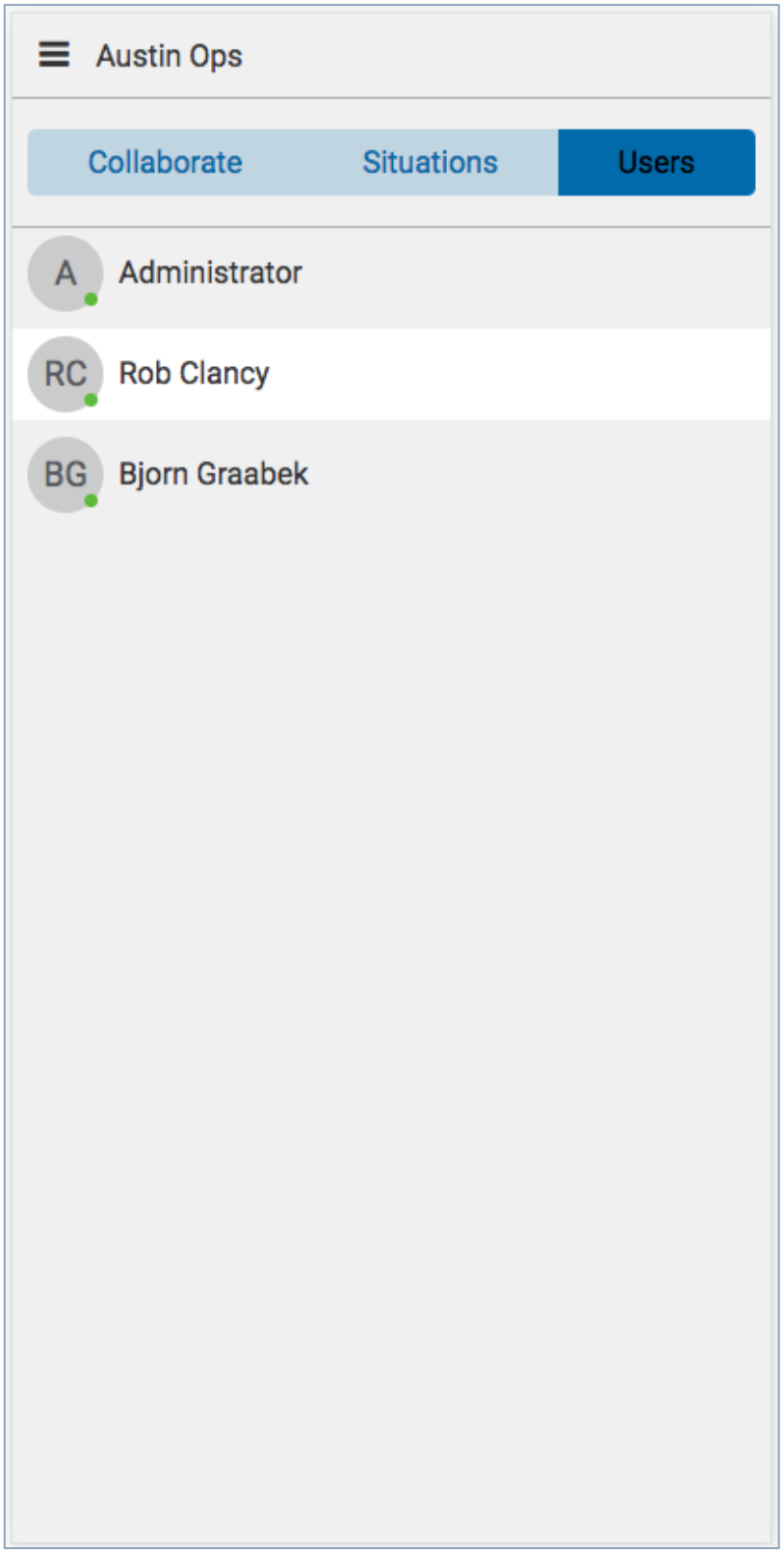
Situations

The Situations tab displays all Situations which are impacting Services being monitored by the team.


Austin Ops
Collaborate
Situations
Users
143
RC
ASSIGNED
11 minutes ago
AIOPs: Services ["pepsi","coke","drpepper"] affected at the following location(s) tx.us on 3 devices.
SERVICES IMPACTED
coke pepsi drpepper
136
A
IN PROGRESS
8 minutes ago
Neighbour Adjacency: Failures detected in directly related devices
SERVICES IMPACTED
core edge coke pepsi drpepper
135
OPENED
21:13:16 07/27/2018
VPN: drpepper affected in the following location(s) ["ams.nl","bxb.us","tx.us"] on 3 devices (Most afffected cpe-303)
SERVICES IMPACTED
drpepper
133
A
IN PROGRESS
7 minutes ago

Users

The Users tab displays all users who are members of the team. In the example below, this will display all members of the Cloud DevOps team.

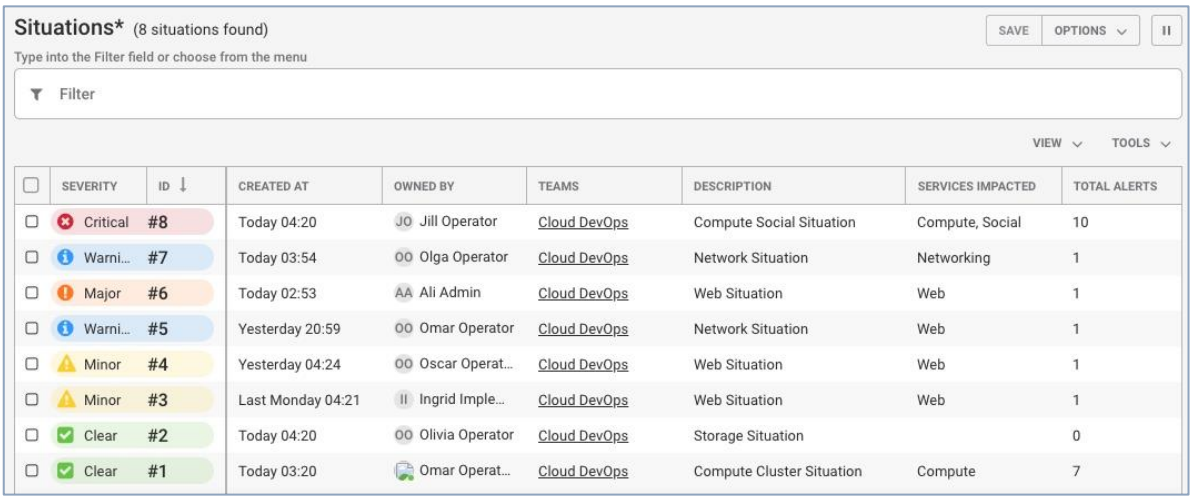

Austin Ops
Collaborate
Situations
Users
A
Administrator
RC
Rob Clancy
BG
Bjorn Graabek

Situations

Situations Overview

Cisco Crosswork Situation Manager uses machine-learning algorithms called Sigalisers to cluster alerts together based on the similarity of their timestamps, language and/or topology.

These can be viewed in filterable lists in the Side Menu, the Search bar and by looking at which Situations are impacting Services.



My Situations/ Open Situations Views

Note: You may receive Notifications about Situations assignments if notifications are enabled for assignments.

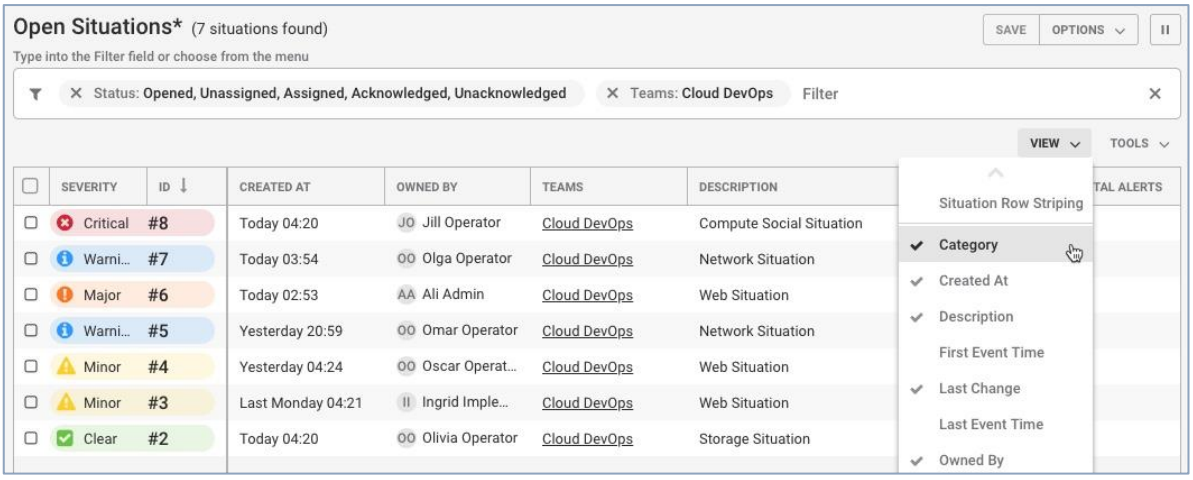
The Open Situations View displays all open Situations that are currently unresolved.

You can find out more about each Situation and open its Situation Room by clicking the colored pill containing the Situation ID. For more information see Work with Situations.

Situation View Menu

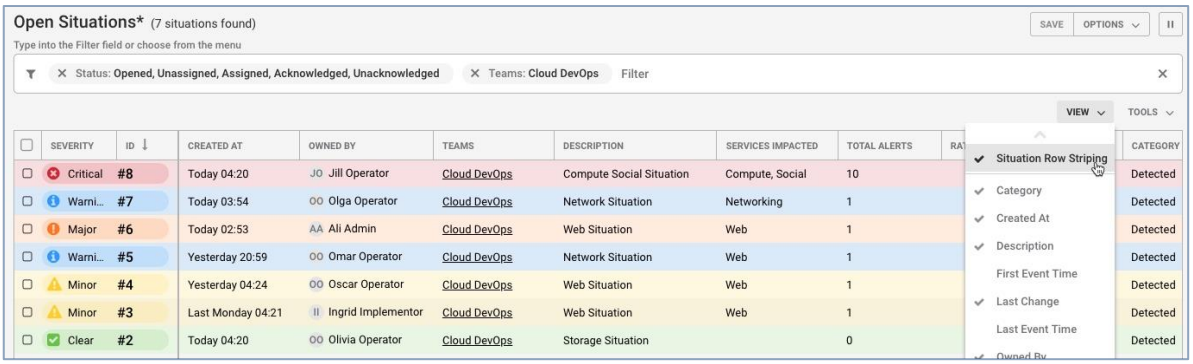
You can use the View menu to configure which columns are shown in My Situations, Open Situations, or a filtered Situation view.

Click View in the top right corner of the screen and select the different options in the drop-down menu to enable them.



View Options

You can edit any Situation view to display each Situation row in the color of the severity using the 'Situation Row Striping' option:



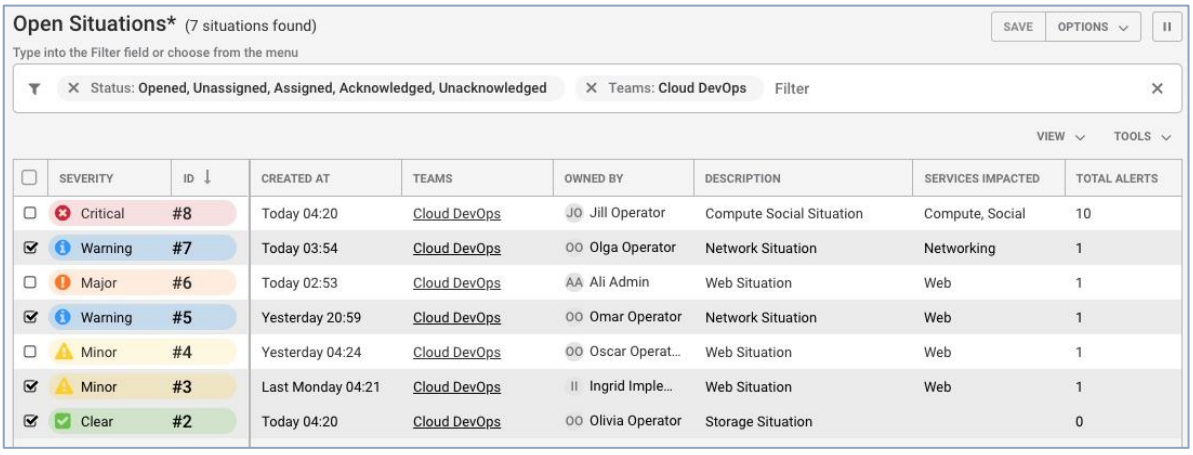
You can configure which Situation columns are displayed by clicking to select them in the View menu. Available columns include:

Column	Description
Category	Indicates the type and state of the Situation. Categories include: Closed, Created, Detected, Priority, Spam and Superseded.
Created At	Time and date when the Situation was created.
Description	Text description of the Situation.
First Event	Time and date when the first Event was recorded.
Last Change	Time that the Alert was last updated in the Cisco Crosswork Situation Manager UI.
Last Event	Time and date when the last Event was recorded.
Owned By	Situation owner's username.
Participants	Number of Users participating in the Situation Rooms.

Process Impacted	All processes associated with the Situation that have been impacted.
Queue	Queue number the Situation belongs to.
Rating	Rating given to the Situation.
Scope	Scope of the different source groups affected by the Situation (End-User, All, Network, Applications, Database, Storage, Desktop, Cloud, Other).
Scope Trend	Indicates whether the scope is increasing or decreasing/staying the same.
Service Impacted	All services associated with the Situation that have been impacted.
Sev Trend	Indicates if the severity is becoming more or less severe.
Status	The Situation's current status: Opened, Closed, Resolved, Assigned, Acknowledged etc.
Story	Story ID number that matches the Situation ID number at the top of the Merge tree.
Teams	Teams that the Situation are associated with.
Total Alerts	Total number of Alerts associated with the Situation.
User Comments	Number of user comments about the Situation.

Select a Situation

You can click the checkboxes in the far left column to select each Situation individually:



To select multiple Situations at once, hold down Shift and then click the checkboxes of the Situations you want to select. If you select one Situation using this method and then click another Situation further down the list, all Situations between the two will also be selected.

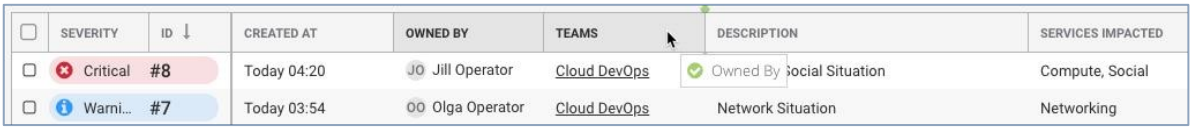
Another method is to left-click and drag down to highlight the Situations you want to select and then right-click to select them and open the Tools Menu (also known as the Right-Click menu).

Click the Select All checkbox in the top left corner to select all Situations. If the checkbox is grayed out, scroll down to load all Situations and activate it.

Move View Columns

You can change the width of each column by hovering your mouse cursor over the column order and clicking and dragging it to increase or decrease the width.

To change the order of the columns, click the column title cell of the column you want to move and drag it to a new location in the top row. Two green arrows will indicate if the move is valid:

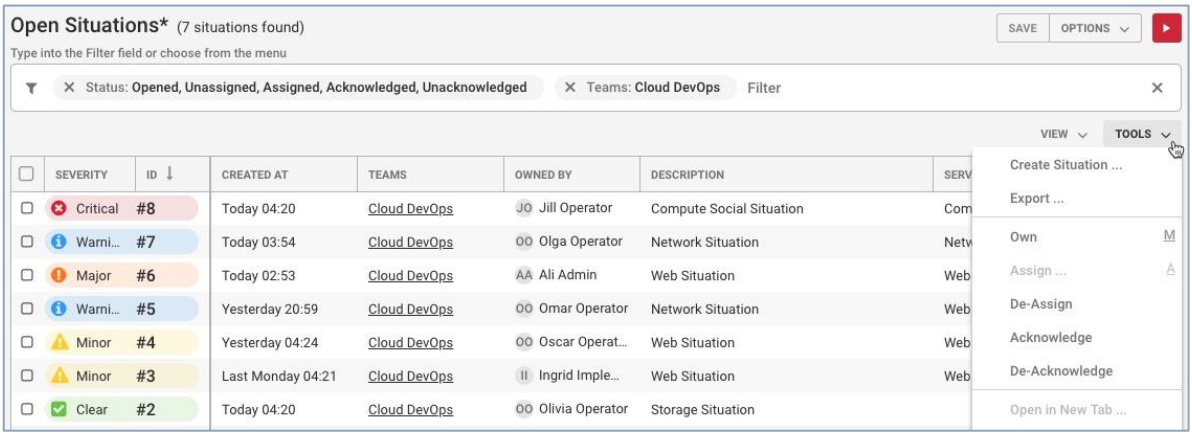


You can also configure the order in which the Situations are shown by clicking the column title cell to rearrange them in ascending or descending alphabetical or numerical order.

For example, click the 'Severity' column to arrange the Situations in ascending or descending order of severity.

Situation Tools Menu

Use the Tools menu or right-click menu to perform any other action on one or more selected Situations.



This can be accessed by clicking Tools or by right-clicking on the Situation list.

Select a Situation or multiple Situations by clicking in the checkboxes in the far left column, or use the Select All checkbox. Then click Tools and select one of the following actions:

Action	Options	Description
Create a Situation	-	Opens a new pop-up window. From here you can create a new Situation
Export	Filename: String Format: CSV (Comma Separated Values) JSON (JavaScript Object Notation) Export:	Export a row, multiple selected rows or all rows in CSV or JSON format

	All Rows Selected Rows	
Own	-	Makes you the owner of the selected Situation or Situations
Assign	-	Enables you to assign the Situation to a User if you have the correct rights
De-Assign	-	This de-assigns the Situation from its current owner
De-Acknowledge	-	This de-acknowledges the Situation so it is no longer in progress
Show Details	-	This opens Situation Details
Tools	-	This links to any configured Server Tools
Add to Merge...	-	This adds the selected Situation in a new 'Merge Situations' panel. See Merge Situations
Resolve...	-	Opens a new pop-up window. From here you can add a Situation Rating and journal entry prior to resolving the Situation*
Close...	-	Opens a new pop-up window. From here you can add a Situation Rating and journal entry prior to closing the Situation*
Reopen...	-	This reopens a resolved or closed Situation

Note: See Resolve Situations for more information.

Situation Severity

There are six default industry-standard severity levels, which are shown and described below:

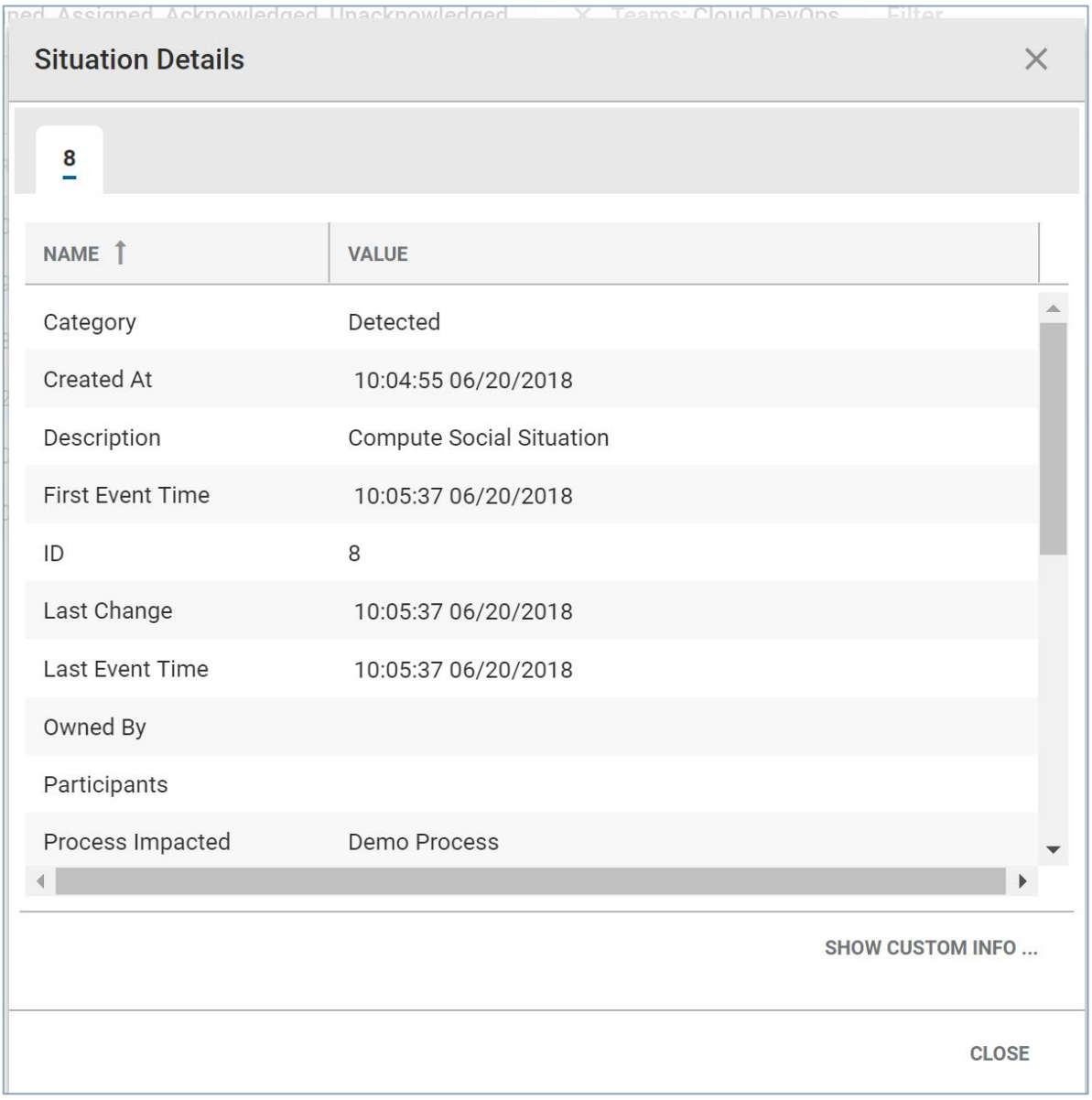
- Clear - indicates that one or more Events have been reported but then subsequently cleared either manually or automatically
- Indeterminate - indicates the severity level could not be determined
- Warning - indicates that a number of potential or imminent service affecting faults have been detected
- Minor - indicates there is a non-service affecting fault but action could be required to prevent it becoming a more serious issue
- Major - indicates a service affecting fault has developed and corrective action is urgently required
- Critical - indicates that a serious service affecting fault has occurred and corrective action is required immediately

The color severity of the My Situations and Open Situations icons on the Side Menu indicates the highest severity level of the Alerts within each list.

A Situation's severity will be determined by its Alert with the highest severity level. If this Alert is cleared then the Situation will adopt the severity level of the Alert with the next highest severity.

Situation Details

The Situations Details window allows you to explore the forensic details of a Situation.



The individual column names and their descriptions are listed in the table below:

Name	Description
Category	The category of the Situation. These include:

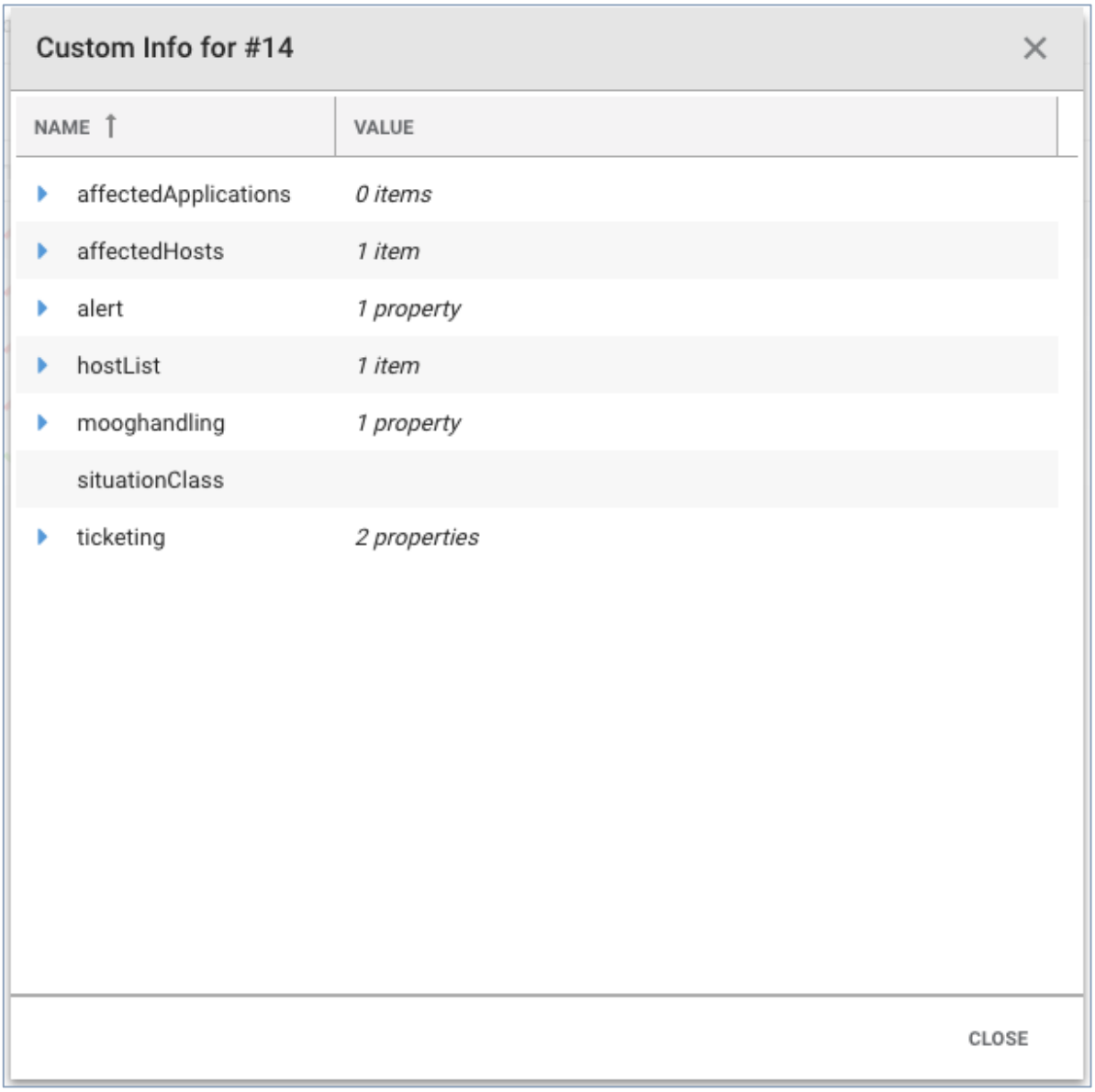
	Closed - Situations that are closed Created - Situations created by a User Detected - Situations generated by an algorithm/Sigaliser Priority - An automatically created Situation with Alerts that match a user-defined template Superseded - Situations that have been merged with another Situation
Created At	The time the Situation was created (the number of seconds, minutes, hours, days ago)
Description	The text description of the Situation
First Event Time	The time of the first Event (the number of seconds, minutes, hours, days ago)
ID	The Situation ID
Last Change	The time of the last change that was made to the Situation
Last Event	The time that the last Event was recorded (the number of seconds, minutes, hours, days ago)
Owned By	The username of the User who owns the Situation
Participants	The number of participants in the Situation. A User becomes a participant after commenting in the Situation Rooms
Process Impacted	The number of processes the Situation is impacting
Scope	The scope of the different source groups that are affected by the Alert or Situation (End-User, All, Network, Applications, Database, Storage, Desktop, Cloud, Other)
Scope Trend	Whether the scope is increasing or decreasing/staying the same. This is indicated by an up or down arrow
Severity	The severity of the Situation
Status	The status of the Situation
Story	The story is the Situation ID at the top of the merge tree
Teams	The teams that are impacted by the Situation
Total Alerts	The total number of Alerts associated with the Situation
User Comments	The number of User comments in the Situation Room

You can copy out the Situation Details by clicking and dragging across the text to highlight it. You can use Ctrl+C (⌘+c on Mac) to copy the text. This can be pasted in an external editor or tool as required.

Custom Info

Custom Info is where you can view custom fields for the Situation.

This will appear in a page tree format. Click the blue-drop down arrows to view the properties beneath each branch.

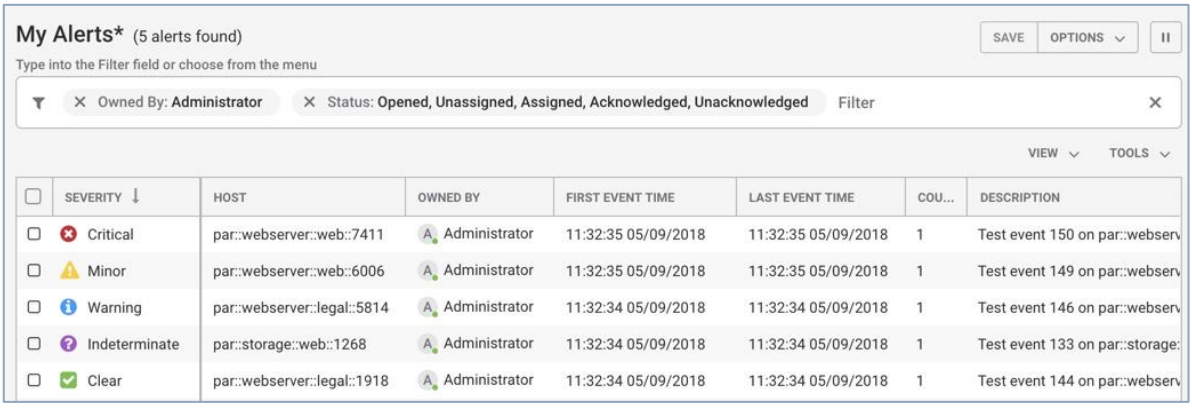


Note: Administrators can add Custom Info to alerts during system configuration. Otherwise you can add Custom Info using the Situation Client Tool using a JSON snippet under the 'Merge Custom Info' field

Alerts Overview

Alerts represent new instances of events or de-duplicated events that have been created by Cisco Crosswork Situation Manager.

You can be view these in filterable and sortable lists, via the Side Menu links, from the Search bar or by looking within Situation Rooms.



The highest severity alert within a Situation determines the severity of a Situation. Alerts follow the same severity levels as Situations.

My Alerts/Open Alerts Views

The My Alerts View displays all of the alerts that have been assigned to you.

The Open Alerts view displays all open Alerts created in Cisco Crosswork Situation Manager and are yet to be resolved.

Alert View Menu

You can select the different columns displayed in the View screens using the View menu.

For more information on the different options see the Configure an Alert View section below.

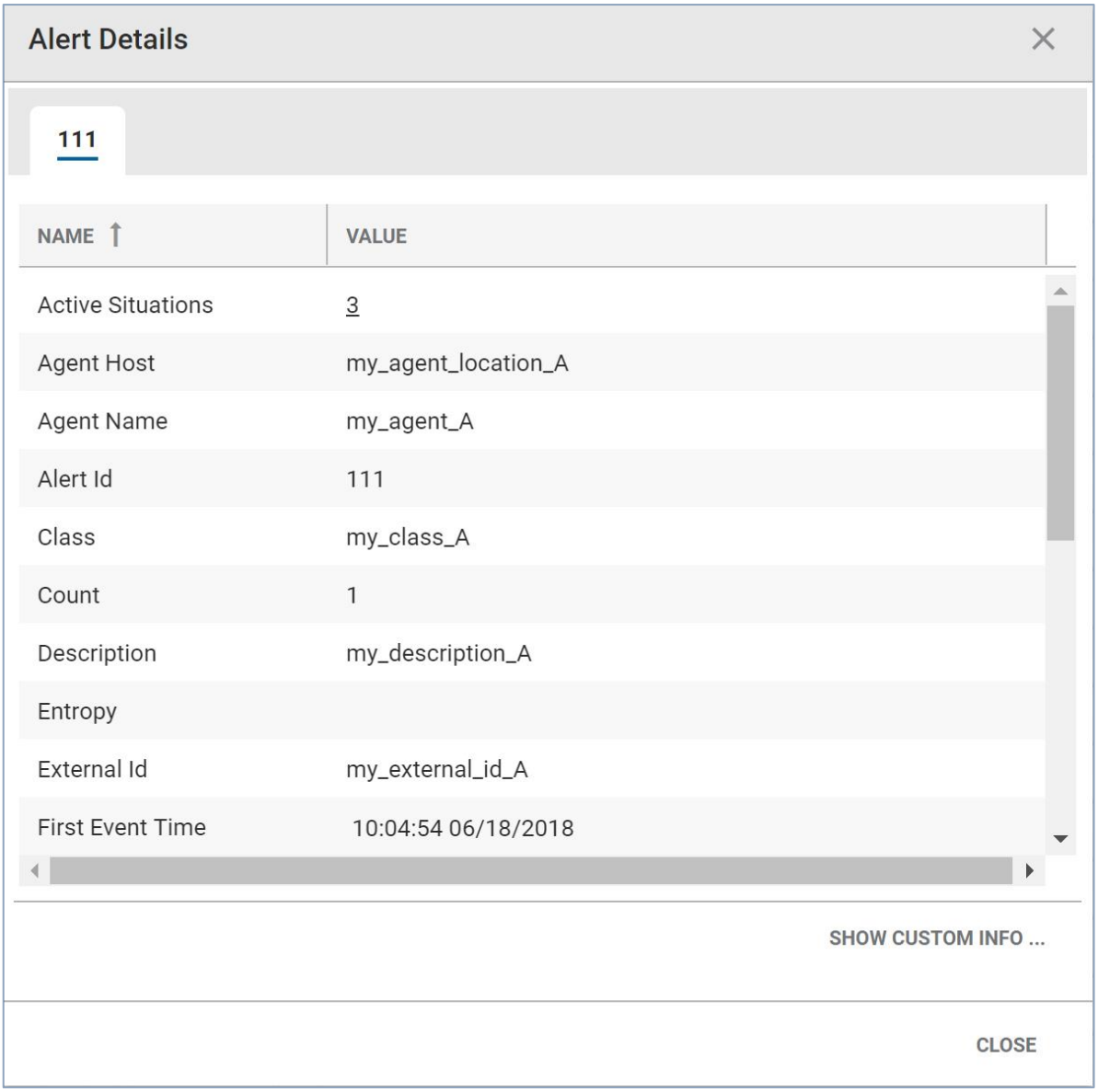
Alert Tools Menu

All other actions you can perform on an alert or group of alerts can be done using the Tools menu or Right-Click menu.

This can be accessed by clicking Tools or by right-clicking on the alert list. For more information see the Alert Tools Menu section.

Alert Details

You can explore the forensic details of an alert in Alert Details:



The individual column names and their descriptions are listed in the table below:

Name	Description
Active Situations	All active Situations to which this Alert is linked
Agent Host	The IP address or co-ordinates of the geographic location where the Events were detected
Agent Name	The name of the monitor that detected the Events. Frequently a sub-category of Manager
Alert Id	This is the numeric identifier given to the Alert
Class	The subcategory of the Agent
Count	The number of events in the Alert.

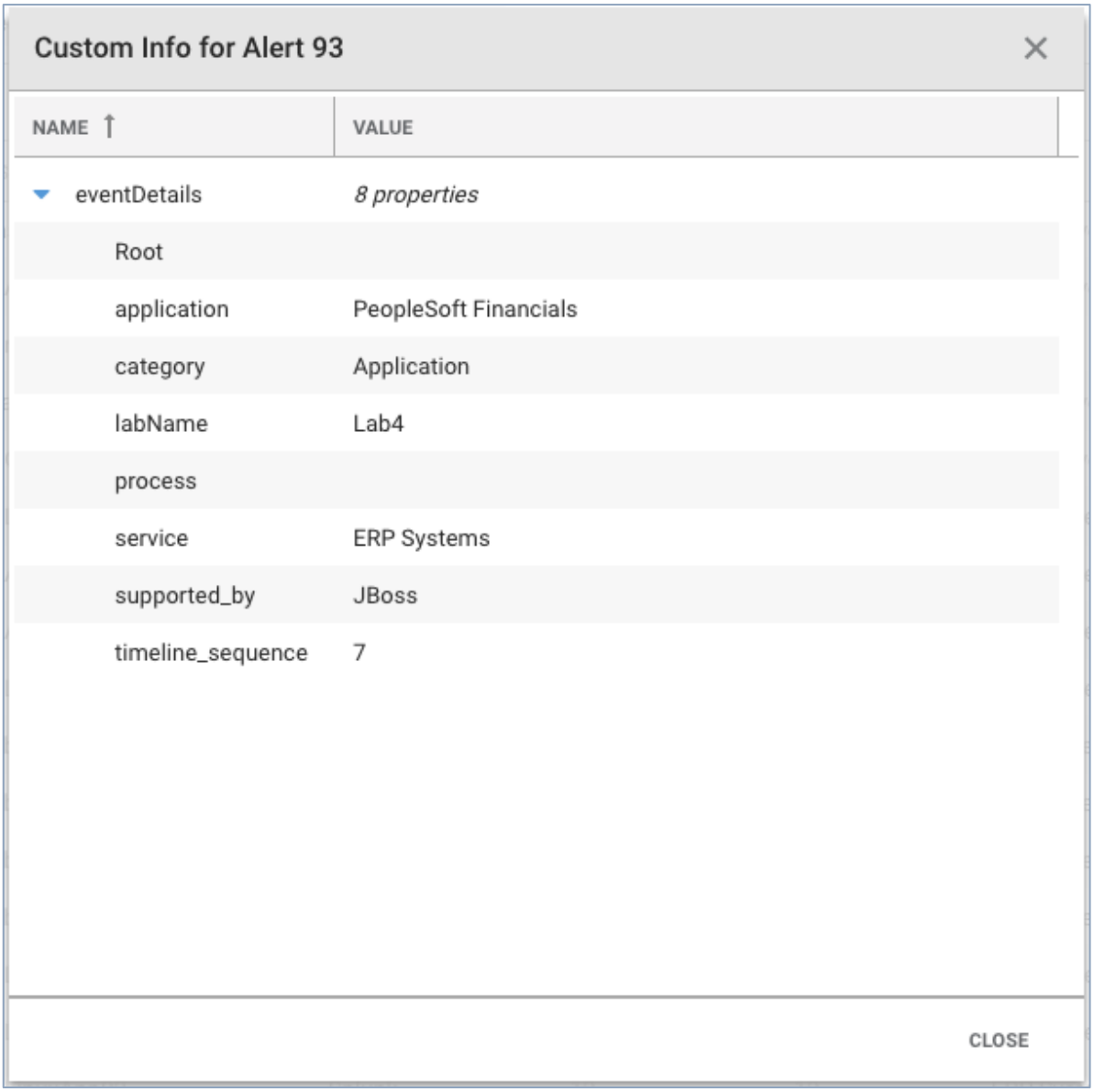
Description	A text summary or description of the Alert
Entropy	The entropy value (between 0 and 1)
External Id	The external ID given by another management system to reference the Alert
First Event Time	The time of the first Event that was recorded by Cisco Crosswork Situation Manager
Host	The source where the Alert originated
Internal Last Event Time	The internal time recorded within the last Event itself
Last Change	The time of the last change to the Alert
Last Event Time	The time of the last Event that was recorded by Cisco Crosswork Situation Manager
Manager	The system sending the Alert
Owned By	The username of the User who owns the Alert
Severity	The severity of the Alert
Significance	The significance of the Alert
Situations	The Situations that the Alert is associated with
Source Id	The unique number of the source being managed
Status	The status of the Alert
Type	The Alert type. E.g DBFail, HTTPDDown, LinkDown etc.

You can copy the Alert Details by clicking and dragging across the text to highlight it. You can use Ctrl+C (⌘+c on Mac) to copy the text. This can be pasted in an external editor or tool as required.

Custom Info

You can view custom fields for the Alert in the Custom Info tab.

This appears in a page tree format. Click the blue-drop down arrows to view the properties beneath each branch.



Note: Custom Info fields can be added by Admins during system configuration. They can also be added with a Situation Client Tool using a JSON snippet under the 'Merge Custom Info' field

Configure an Alert View

Use the View menu to customize which field columns are displayed in My Alerts/ Open Alerts or an Alert filter view.

Click View in the top right corner of the screen to view and select the different options in the drop-down menu.

View Options

The top option, 'Alert Row Striping', will change the filter display and each Alert row will appear as colored stripes. This is shown in the screenshot below:

The Alert columns that can be added and removed are listed in the table below:

Column	Description
Active Situations	Any active Situations the Alerts are linked to
Agent Host	The IP address or co-ordinates of the geographic location where the Events were detected
Agent Name	The name of the monitor that detected the Events. Frequently a sub-category of Manager
Alert Id	The numeric Alert Id
Class	The subcategory of the Agent
Count	The number of times this Alert has been counted
Description	A text summary or description of the Alert
Entropy	The entropy value (between 0 and 1). See Entropy
External Id	The external ID given by another management system to reference the Alert
First Event Time	The time when the Alert's first Event was recorded
Host	The source where the Alert originated
Internal Last Even Time	The last time and date there was an internal change to the Alert
Last Change	The last time and date there was a change to the Alert
Last Event Time	The time when the Alert's last Event was recorded
Manager	The system sending the Alert
Owned By	The User that owns the Alert
Significance	The Significance of an Alert (Collateral, Related, Impacting or Causal). See Significance
Situations	All of the Situations that the Alert is linked to
Source Id	The unique name of the source being managed

Status	The Alert status (Unassigned, Assigned, Acknowledged)
Type	The Alert type. E.g DBFail, HTTPDDown, LinkDown etc.

Move View Columns

You can change the width of each column by hovering your mouse cursor over the column order and clicking and dragging it to increase or decrease the width.

To change the order of the columns, click the column title cell of the column you want to move and drag it to a new location in the top row. Two green arrows will indicate if the move is valid.

You can also configure the order in which the Alerts are shown by clicking the column title cell to rearrange them in ascending or descending alphabetical or numerical order.

For example, click the 'Severity' column to arrange the Alerts in ascending or descending order of severity.

Alert Tools Menu

All other actions that can be performed to an Alert or group of Alerts can be done using the Tools menu or Right-Click menu.

This can be accessed by clicking Tools or by right-clicking on the Alert list.

Select an alert or multiple alerts by clicking in the checkboxes in the far left column.

Next click Tools to perform one of the following actions available in the Tools menu:

Action	Options	Description
Export	Filename: String Format: CSV (Comma Separated Values) JSON (JavaScript Object Notation) Export: All Rows Selected Rows	Export a row, multiple selected rows or all rows in CSV or JSON format
Own	-	Makes you the owner of an Alert or Alerts
Assign	-	Assigns an Alert or Alerts to a user, subject to permissions
De-Assign	-	Deassigns an Alert or Alerts from a user
Acknowledge	-	Acknowledge an Alert and assume responsibility for it
De-Acknowledge	-	De-acknowledge an Alert to indicate you are no longer responsible for it
Set Severity	Critical Major Minor Warning	Enables you to change the severity of an Alert or Alerts

	Indeterminate Clear	
Set Significance	Causal Impacting Related Collateral	Sets the relative significance of an Alert, initially calculated based on its entropy (a measure of the rarity or uniqueness of this alert) with 'Causal' being the most unique, and 'Collateral' being the least. See Significance
Show Details	-	Opens the Alert Details pop-up window with more information about the Alert
Show Timeline	-	Displays the timeline view for the Alert showing you the time extent of the alert, from when it first began to its last change
Tools	Server Tools... SSH to Host	Lists the client-side Alert tools that can be run Connect to the host using Secure Shell (SSH)
Add to Situation...	-	Opens a new pop-up window. From here you can add the Alert(s) to a Situation. See Adding Alerts to Situations
Remove from Situation...	-	Opens a new pop-up window. From here you can remove the Alert(s) from a Situation
Move to Situation...	-	Opens a new pop-up window. From here you can move the Alert(s) to a Situation
Resolve...	-	Resolves an Alert and prompts you to submit an entry to the Journal thread of all Situations the Alert is a member of
Close...	-	Closes an Alert. Once an Alert has been changed to a closed state it cannot be revived

Add Alerts to Situations

A single or multiple alerts can be added to a Situation if a User thinks they are related or it makes sense to do so.

To do this from the alert filter view such as My Alerts or Open Alerts, follow the numbered steps below:

1. Select the alert or alerts you want to add to a Situation by clicking the checkbox(es) in the far left column.
2. Right-click on the alerts or click Tools to open the Tools menu and then click Add to Situation...
3. Use the Filter to find the relevant Situations and select the Situation or Situations to add the Alert(s) to. Click Done to continue.

Alert Workflow

Alerts can be assigned to different Cisco Crosswork Situation Manager users, owned by Administrators and added to Situations.

The standard method of working with Alerts is to have an Administrator who assigns Alerts to the Users within a team. An alternative is to have a single Administrator who owns Situations and deals with all of their associated Alerts.

The sections below outline the standard workflow that can be applied to both of these methods.

Assigned Alerts

Once an Alert has been assigned to you, you will either receive a Notification or it will appear in your My Alerts filter.

After identifying which alerts have the highest priority, typically the alert with the highest severity, the next step is to Acknowledge them to let others know that you are aware of it. A standard way of working would be to work through all of the days 'Critical' alerts and resolve those first before working on the days 'Major' and then 'Warning' alerts to prevent them becoming 'Critical' alerts.

To do this, right click in the alert's row or tag it using the checkbox in the far left column and then click Tools > Acknowledge.

Timeline

To access an alert's timeline, right click on it and select Show Timeline.

The timeline shows a graphical view of an alert and a breakdown of the events that were de-duplicated to create the alert. It also displays the severity of each event and the times at which they occurred.

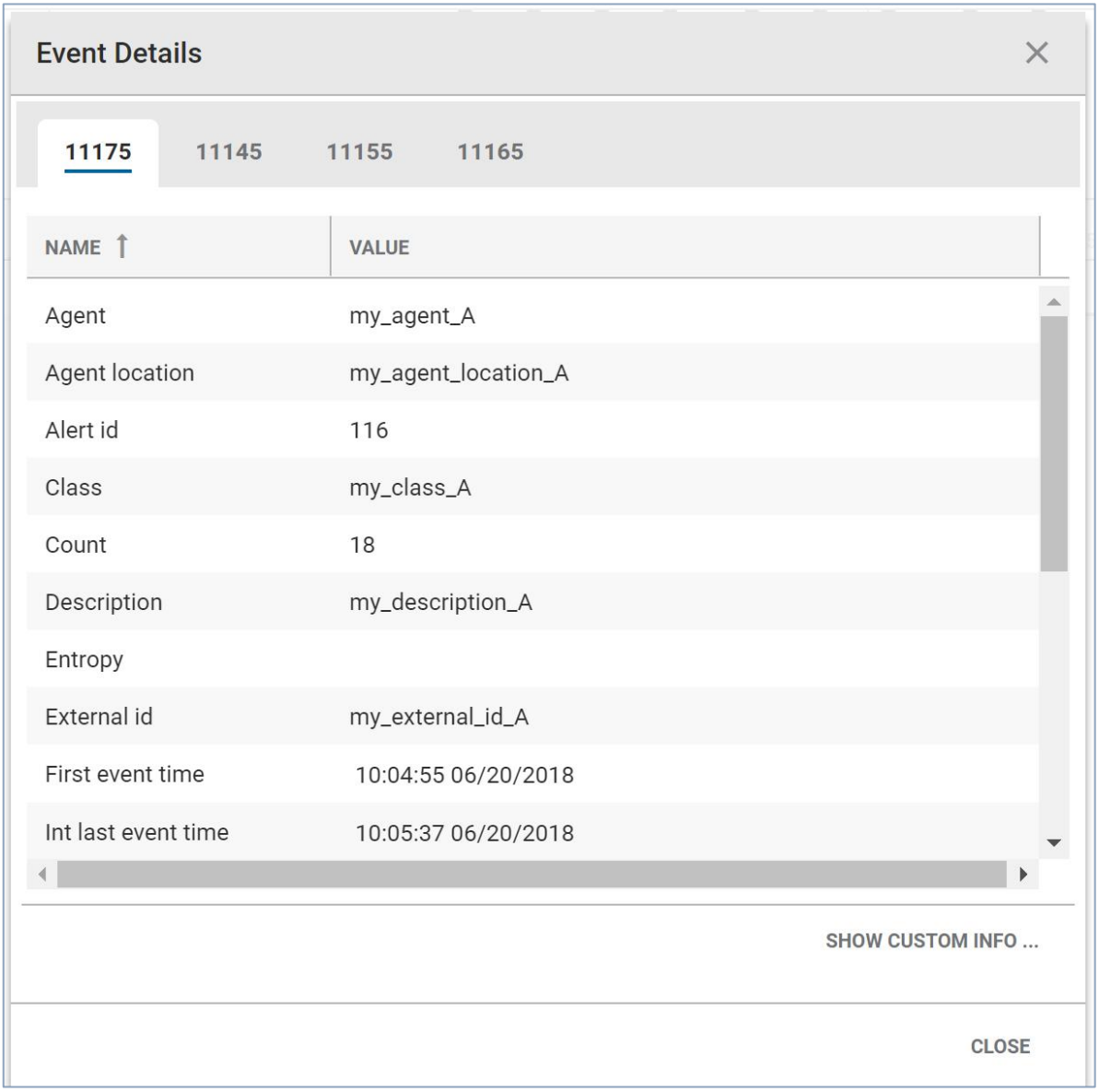
Click the Zoom In or Zoom Out options to focus in on a particular time period or group of events. Alternatively use the blue sliders to focus in on an area of interest.

The severity of each event is indicated by the color of the line (e.g. the Events in the screenshot above are a mixture of indeterminate and critical Events).

Note: The alert's severity is defined by the severity of the latest event rather than the event with the highest severity

Click any of the colored lines for more information on any event in the timeline. This will open the Event Details window:

The Events Details window allows you to explore the forensic details of an event or events.



The individual column names and their descriptions are listed below:

Name	Description
Agent	The name of the monitor that detected the events. Frequently a sub-category of Manager
Agent Location	The IP address or co-ordinates of the geographic location where the events were detected
Alert Id	This is the numeric identifier given to the alert
Class	The subcategory of the Agent
Count	The number of times this alert has been counted
Description	A text summary or description of the alert

Entropy	The entropy value (between 0 and 1)
Event Id	The ID given to the event
Event Time	The time of the event
Event Type	The type of event
First Event Time	The time of the first event that was recorded by Cisco Crosswork Situation Manager
Internal Last Event Time	The time that the last event was recorded by Moogdb
Last Event Time	The time of the last event that was recorded by the Agent. This may be set by the LAM or the Alert Builder. The default is when the LAM first registered the event.
Last State Change	The time of the last event state change
Manager	The system sending the event
Owner	The username of the user who owns the alert and its events
Severity	The severity of the event
Significance	The significance of the alert
Source	The name of the source machine.
Source Id	The unique identifier for the source machine.
State	The state of the event
Type	The alert type. E.g DBFail, HTTPDDown, LinkDown etc.

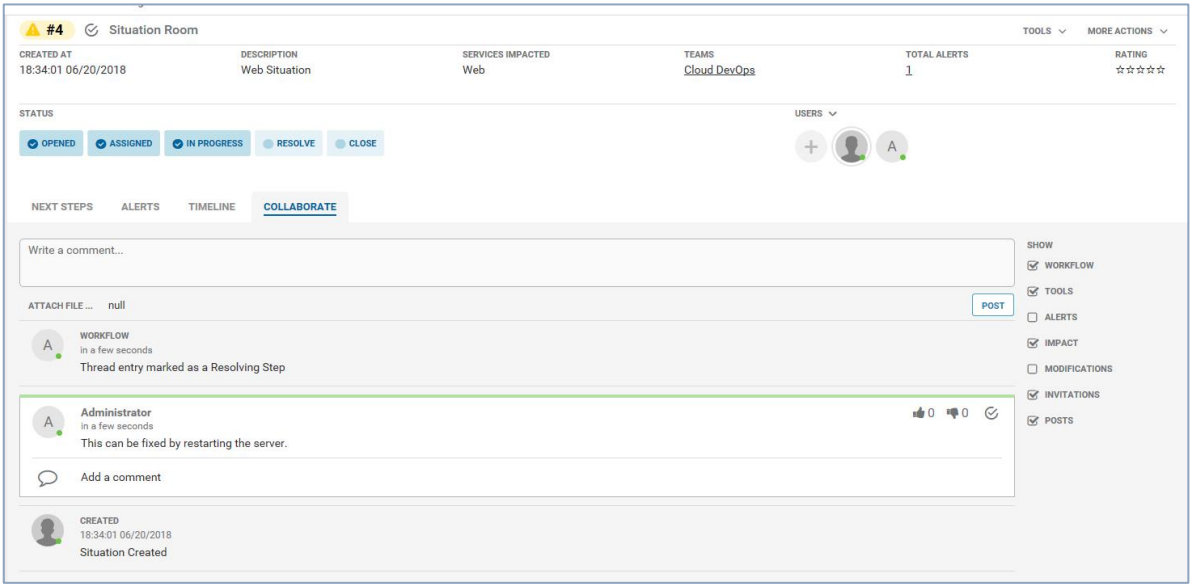
Collaborate

Go to Collaborate in the Situation Room and share comments or ideas with your colleagues to find a resolution.

Ultimately, the aim is to resolve high severity alerts before you resolve the Situation. If anyone proposes a solution, this can be tested using Tools or going back to the My Alerts view and clicking on the Host column to SSH into it.

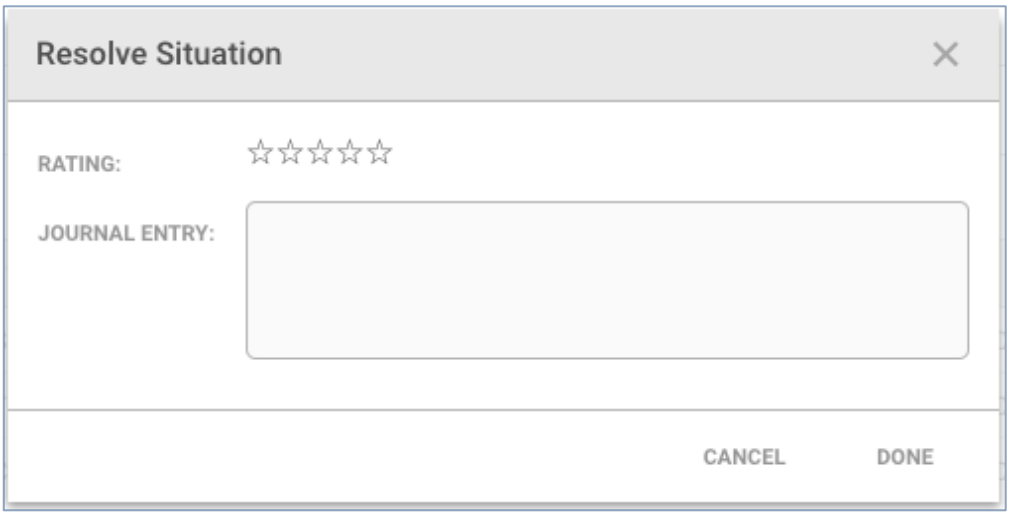
Resolving Steps

If you or another user finds a solution that fixes the problem, then the comment should be marked as the Resolving Step. To do this, click the check icon next to the post in Comments or under Collaborate:



The comment which has been marked as the Resolving Step will be highlighted with a green line. Now a resolution has been found, this Situation can be resolved.

To do this click on the Resolve button under Status in the Situation Room. The 'Resolve Situation' pop-up window will appear:



Add a star rating to indicate the relevance and quality of information given in the Situation along with a journal entry comment. Click Done to continue.

Assign and Acknowledge Situations

After Cisco Crosswork Situation Manager creates and opens a Situation, the next steps are:

1. A user goes to the Situation Room and assigns the Situation.
2. The assigned user acknowledges the Situation.

Assign to a User

To assign to a user, go to the Situation Room, click ASSIGN, and choose the relevant user.

Team Assignment

The Team Room shows all Situations assigned to that team. Cisco Crosswork Situation Manager assigns each situation to teams automatically based on the current Service Filters and Situation Filters defined for each team. Note the following:

- If a team has no Service or Situation filters defined, Cisco Crosswork Situation Manager assigns all open situations to that team.
- If a team has both Service and Situation filters defined, Cisco Crosswork Situation Manager assigns a situation only if the team has both a matching Service Filter and a matching Situation Filter.
- You can manually override the default team assignments for a specific Situation: Go to the Situation Room and click TEAMS.
- If you override the team assignment for a situation, automatic team assignment is permanently disabled for that situation.
- If you unassign a situation from your team, based upon your role, you might be unable to access the Situation afterwards.

Acknowledge an Assigned Situation

You should receive a Notification when you are assigned to a Situation. You need to acknowledge the assignment before you investigate and resolve it. Go to the Situation Room and click ACKNOWLEDGE.

Change a Situation Assignment

Go to the Situation Room and click MORE ACTIONS. You can

- Own – Re-assign to your self and acknowledge
- De-Assign – Set status to Open
- De-Acknowledge – Available only if the Situation is assigned to you and you have acknowledged the current assignment.

For information about other actions, see Take Additional Actions.

Work with Situations

After Cisco Crosswork Situation Manager creates Situations from the alerts ingested from your monitoring systems, you can use various tools to resolve them. When you resolve the Situation, you can provide feedback to help with the resolution of similar Situations that arise.

This topic guides you through the various steps in the workflow to resolve Situations.

How to resolve Situations

The following workflow represents the typical steps to resolve a Situation. You may not need to execute every step for every Situation. As you become more experienced with Cisco Crosswork Situation Manager you may develop your own workflow to suit your requirements.

1. Check for Impacted Services in the Services Overview.

   In the Cisco Crosswork Situation Manager workbench, the Services Overview section indicates which of your Services are impacted by Situations.

2. Click on the Team Room name in the Side Menu to open your Team Room.

   The Team room is a good place to collaborate with the colleagues in your Team to find a resolution to your Situations. Click the Team Room name in the Side Menu. The Team Room displays all recent activity such as Situations being assigned, new comments that have been posted and any Resolving Steps that have been created. You can also see which members of your Team are currently logged into Cisco Crosswork Situation Manager on the right side of the screen.

3. Click the Task Board tab to view Situations in a Kanban-style board

   You can see which Situations have been assigned to you in the "Assigned" column.

4. Click Acknowledge on any Situation that has been assigned to you.

   This changes the status to "In Progress" and alerts your team to the fact that you are working on a situation.

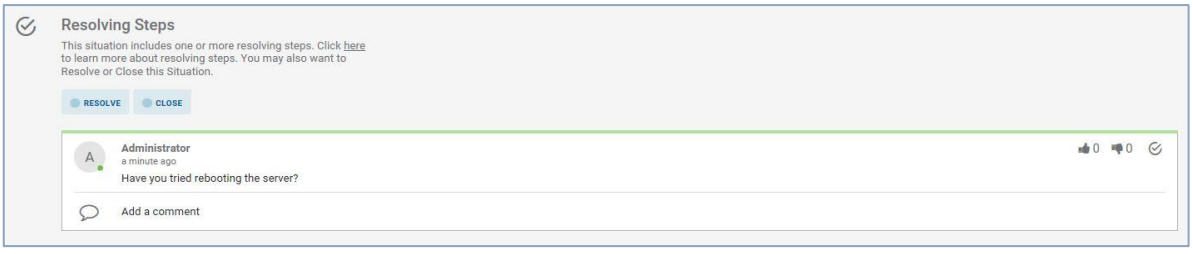
5. Click on your assigned Situation

   The Situation Room opens to display key information about the Situation including:

   - The Situation status
   - The number of Alerts
   - Impacted services
   - Next steps to resolve the Situation.

Resolve Situations

A Resolving Step is the comment, suggestion or action in the Collaborate section of a Situation Room or Team Room that has been marked as the solution to a Situation.

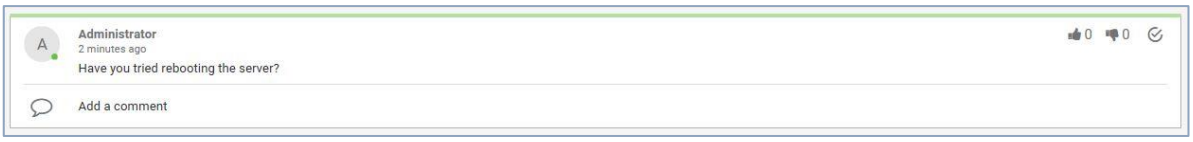


If a Situation has a Resolving Step, it is indicated by a check icon next to the Situation ID, as shown in the screenshot below:

Mark a Resolving Step

If you find a comment or suggestion has helped to resolve the root cause of the Situation then you should mark it as a Resolving Step.

To do this, click the gray check icon in the top right corner of the comment:



When a comment has been marked as a Resolving Step, a green line will appear along the top of the comment to highlight it.

It will also be pinned under the Next Steps in the Situation Room.

Note: Multiples comments can be marked as the Resolving Steps. It doesn't have to be a singular comment or action.

Other users can subsequently approve or disapprove of the Resolving Step using the upvote and downvote icons. The number next to each icon will indicate the number of votes it has had.

Unmark a Resolving Step

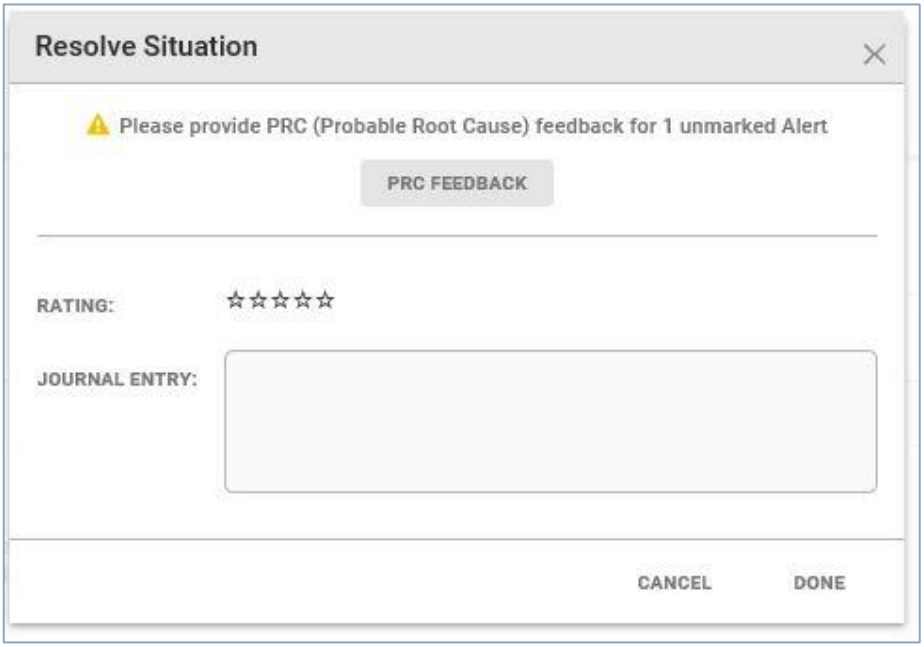
A comment that has been made a Resolving Step can be unmarked at any point.

To do this, click the check icon on the comment under Next Steps or Collaborate. This action will appear on the Collaborate wall in the Team Room.

Resolve a Situation

A Situation can be resolved once a Resolving Step has been found.

To do this, click Resolve under Status in the Situation Room or change its status on the Team Room Task Board. The 'Resolve Situation' pop-up window then appears:



If Cisco Crosswork Situation Manager warns you that you have unmarked PRC Alerts, click the Mark Alerts button to return to the Alerts list and mark the appropriate Alerts.

Click the stars to give it a star rating out of five to indicate the relevance and quality of information given in the Situation along with a journal entry comment*.

Note: It is important to reflect an accurate rating, particularly if you are using the Feedback Sigaliser which takes information such as Situation ratings into account.

When you have entered your rating and journal entry, click Done to continue.

Rate a Situation

You can rate the relevance and quality of the information given in a Situation each time you resolve one by giving it a star rating between 1 and 5.

Each Situation rating is always followed by a journal entry or comment, where you can provide any additional information.

Ratings can be given directly from the Situation Room or when resolving or closing a Situation from any Situation filter or from the Task Board.

Note: It is important to reflect an accurate rating, particularly if you are using the Feedback Sigaliser which takes information such as Situation ratings into account.

E.g. The default rating threshold for Feedback Sigaliser is 3 so it will learn from any Situations with a rating of 3 stars or more.

Rate a Situation

When you resolve a Situation from either a filter or the Task Board, the 'Resolve Situation' pop-up window appears.

Click on the appropriate star rating depending on how relevant or accurate the Situation was. The Situation rating scores are:

Rating	Definition
-	Not yet rated
*	Bad
**	Poor
***	Adequate
****	Good
*****	Excellent

Next type in the 'Journal Entry' box to provide a comment about why the Situation was resolved or closed and a description of the resolution (if applicable). This can be as long as required.

When you have finished writing the entry, click Done to continue.

Check Impacted Services

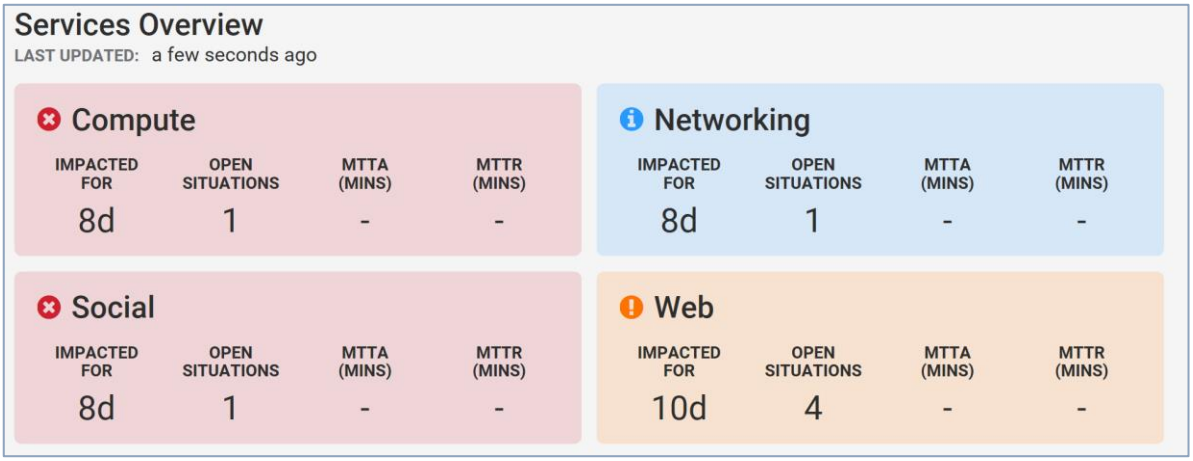
To prioritize which Situations to deal with first, check for impacted services with the highest severity. Typically you should deal with services impacted by critical Situations first.

You can check for impacted services in Cisco Crosswork Situation Manager in three different ways: in the Services Overview, by creating a filter, and in the Services Impacted menu.

Services Overview

The Services Overview section displays any Services which are assigned to your Team or which are impacted by Situations assigned to your Team.

Important: To assign Services to your Team, go to System Settings > Security > Teams and add the required Services to your Service Filter.



Each Service panel will also include the amount of time it has been impacted for, the number of open Situations which are impacting it, the MTTA and the MTTR in minutes.

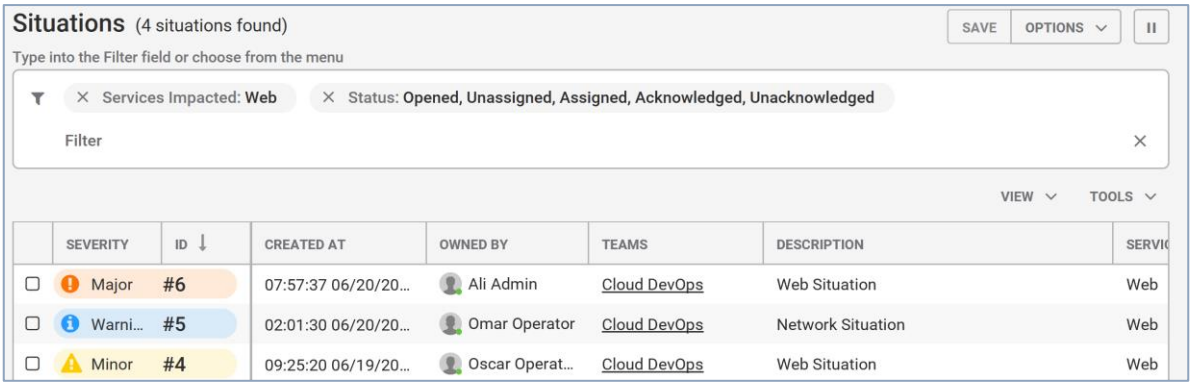
The color of the Service indicates the highest severity level of the Situations that are impacting it.

Note: This panel will automatically update every minute by default. Click the text alongside 'Last Updated' for the exact time the update took place.

Service Filter

Click any Service for more information about the impacting Situations.

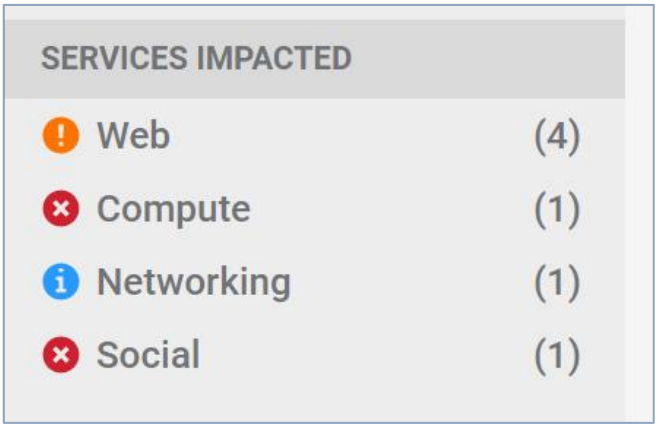
These Situations are displayed in a Situation filter, allowing you to identify those which you want to prioritize. E.g. Those with the highest severity or number of high severity Alerts etc.



You can see which other Services each Situation is impacting by referring to the 'Services Impacted' column.

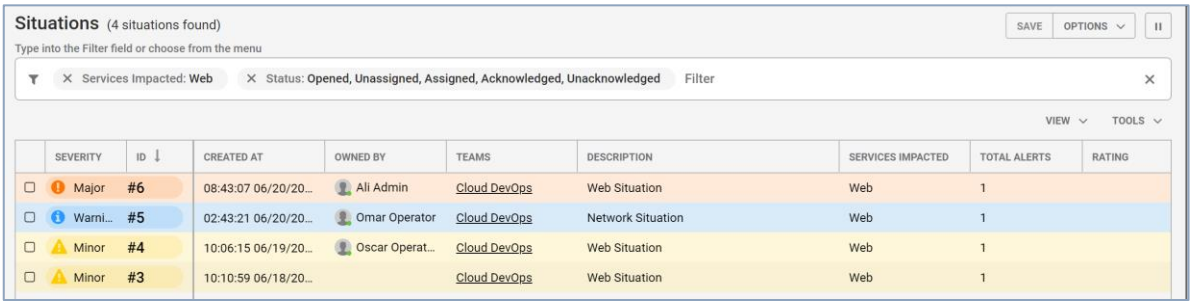
Services Impacted

A list of all Services that have been impacted will appear in the Side Menu on the left side of the Workbench.



Click any of the Service names to view the Situations that are impacting it. Alternatively click Services Impacted to view all Situations that are impacting your Services in a Situation Filter.

The Services Impacted link from the Side Menu will open all Situations which are impacting your system's services in a new Situation Filter:

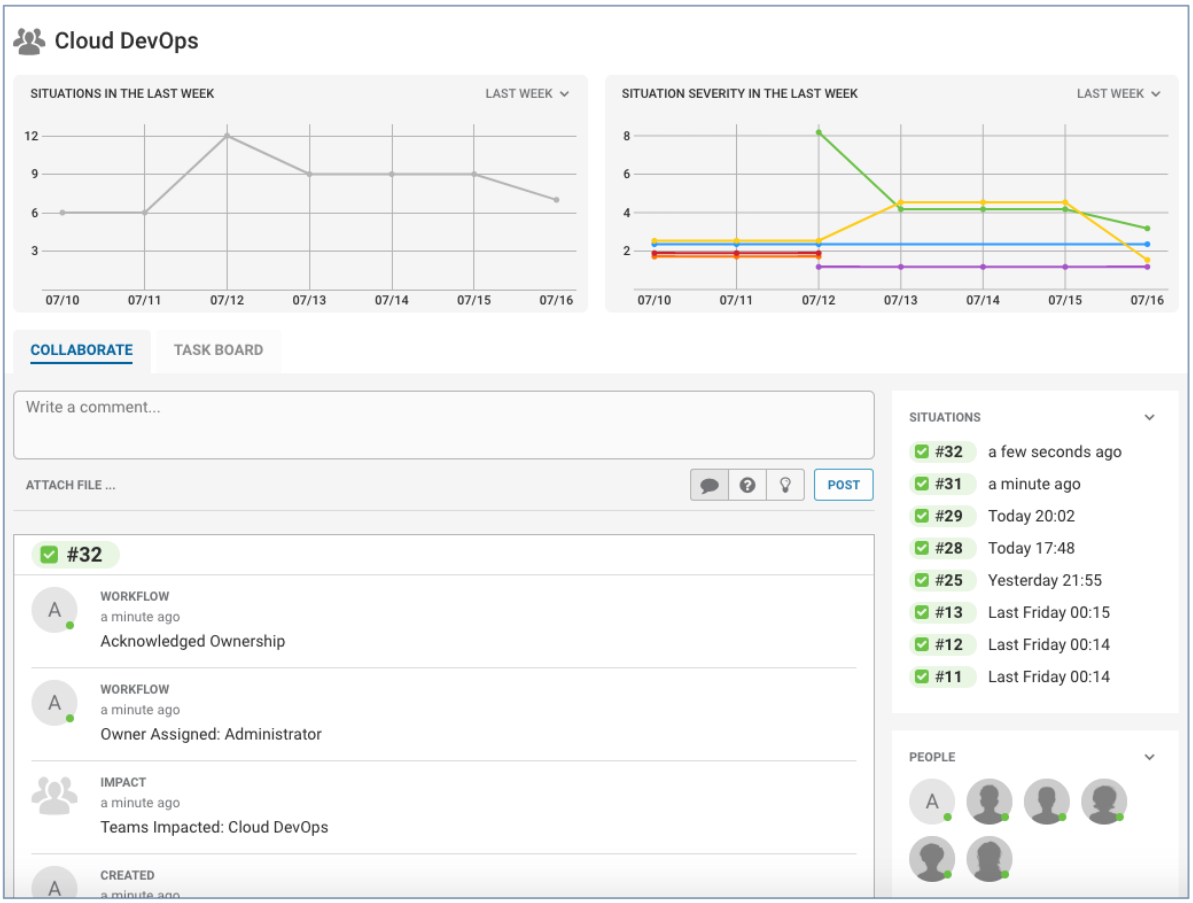


This screen offers a useful overview of the Situations which are affecting the most of your Services and can help you identify and prioritize which Situations to deal with first. It also allows you to see the Situations which impacting Services which are not associated with your team.

Work in a Team Room

The Team Room is the first place you should go for a general overview of the latest Situation activity in your team.

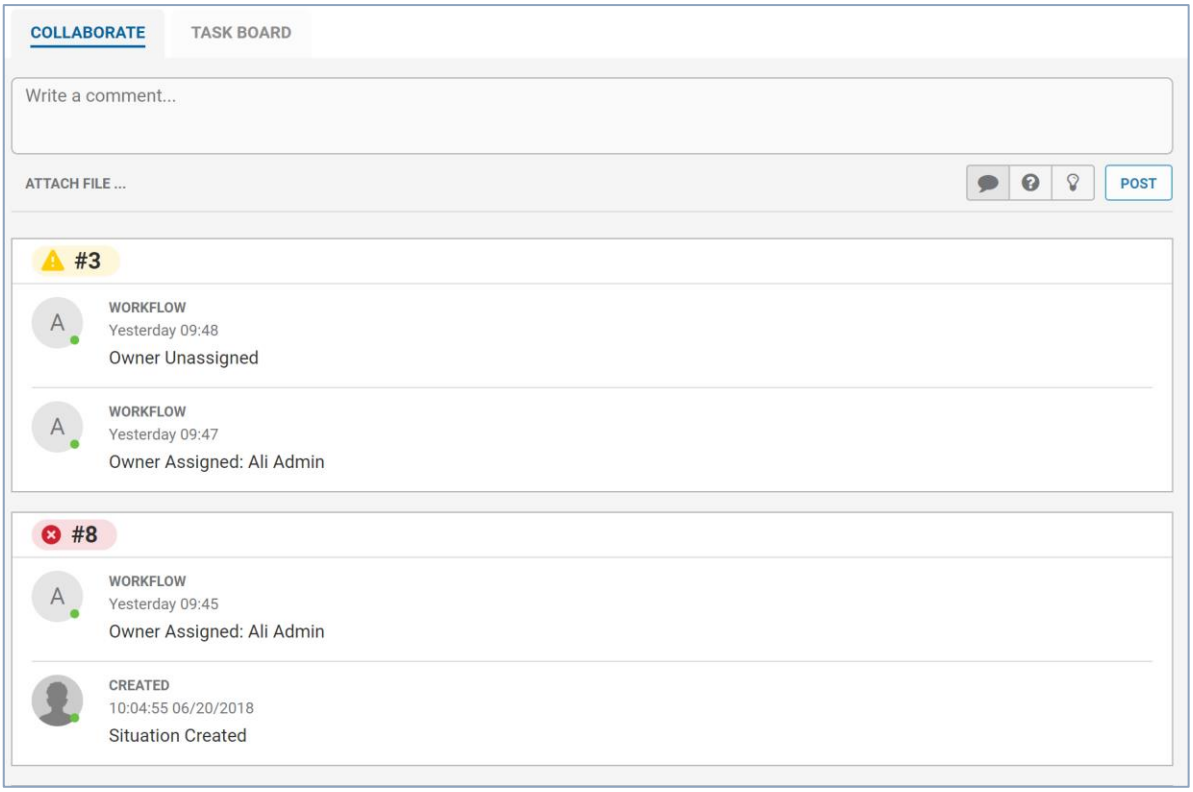
This is where you can discuss issues with team members and collaborate to find a resolution to alerts and Situations.



There are two key components to the Team Room screen: Collaborate and Task Board.

Collaborate

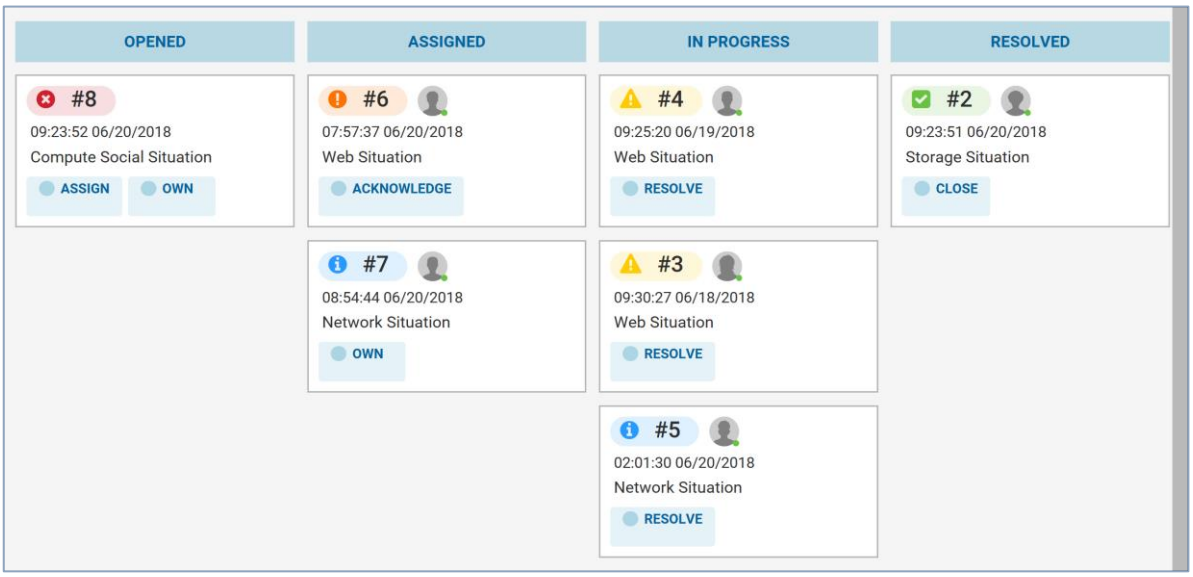
The Collaborate tab is where you can view the latest activity and communicate with members of your team to find resolutions to Situations.



You can post questions, ideas, general comments and attach files that will appear on the Collaborate news feed in chronological order.

Task Board

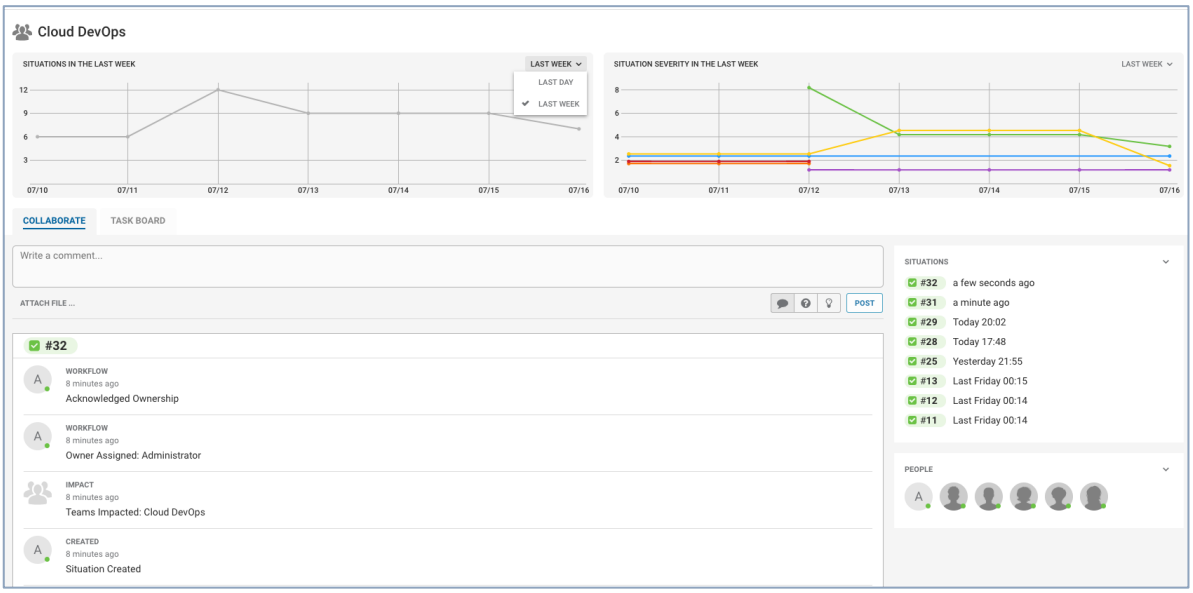
The Task Board is a Kanban-style board where you can see an overview of the team's Situations and their statuses.



This is a useful screen to see your assigned Situations and manage what work you have to do. It is also where Administrators can assign Situations to different users.

Team Insights

Team Insights shows Situation summary data and Situation Severity data from two time frames: the last week and the last day.



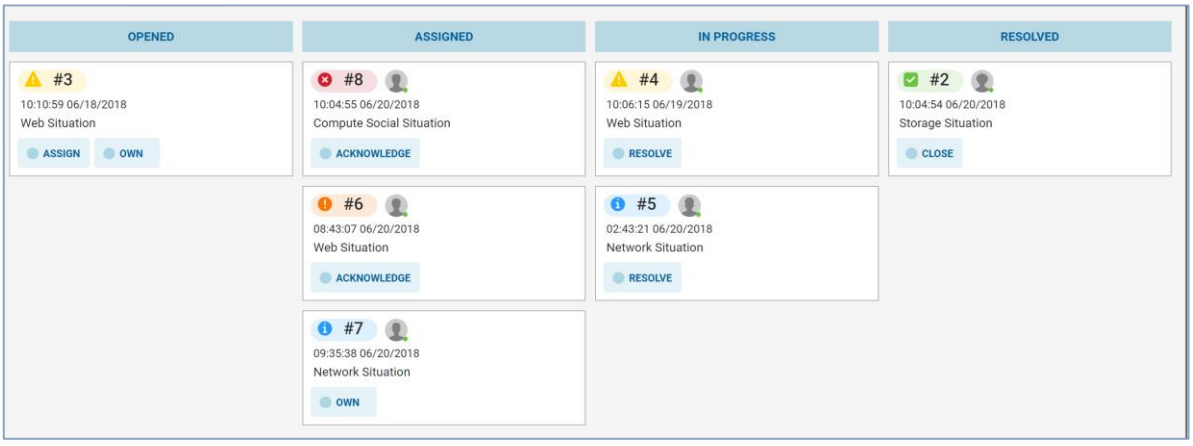
Use the drop-down to choose from the last week or the last day. The default is the last week.

Highlight a line in a graph with your mouse pointer. Dots denote data points.

Note: Cisco Crosswork Situation Manager collects data at a specific time in each 24 hour period and this may not reflect the highest number or severity of Situations during that period.

Monitor your Task Board

The Task Board is a Kanban-style board where you can see an overview of the Team's Situations, where they are in the workflow, how much work is in progress and in the queue.



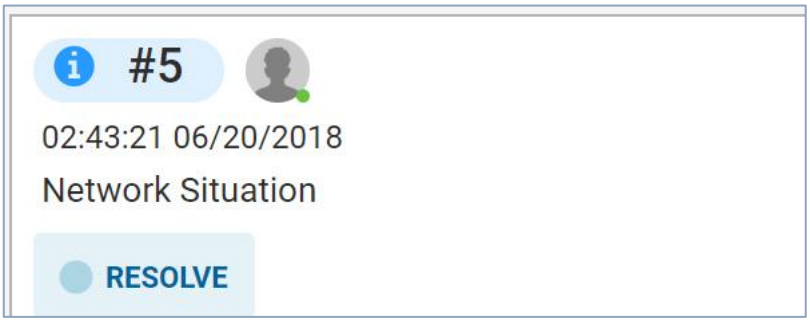
This is a useful screen to see what work you and your teammates have to do. It is also where Administrators can assign Situations to different Users.

Note: What is a Kanban Board?: A Kanban board is a visualization tool which can be used to see an overview of your workload and optimize the flow of your work.

Navigation

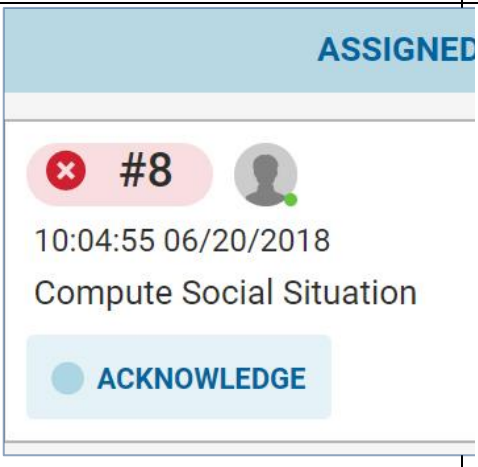
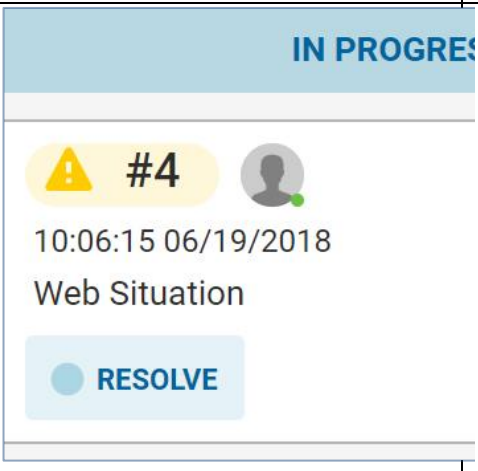
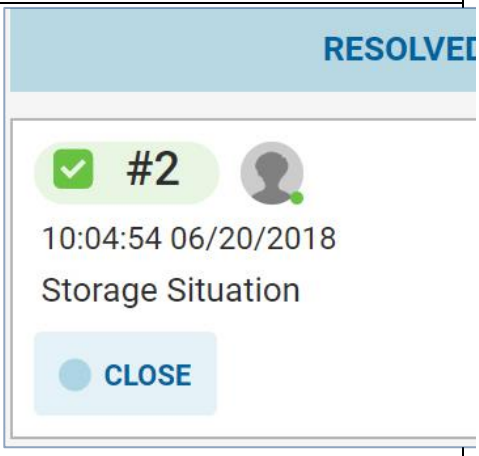
The Situations will appear in columns arranged in order of status: opened, assigned, in progress and resolved.

Each Situation will appear with a colored pill-shaped marker displaying the Situation ID number, the severity color, the user who is assigned to the Situation, the time the Situation was created, the description, and the action that can be performed:



Task Board Flow

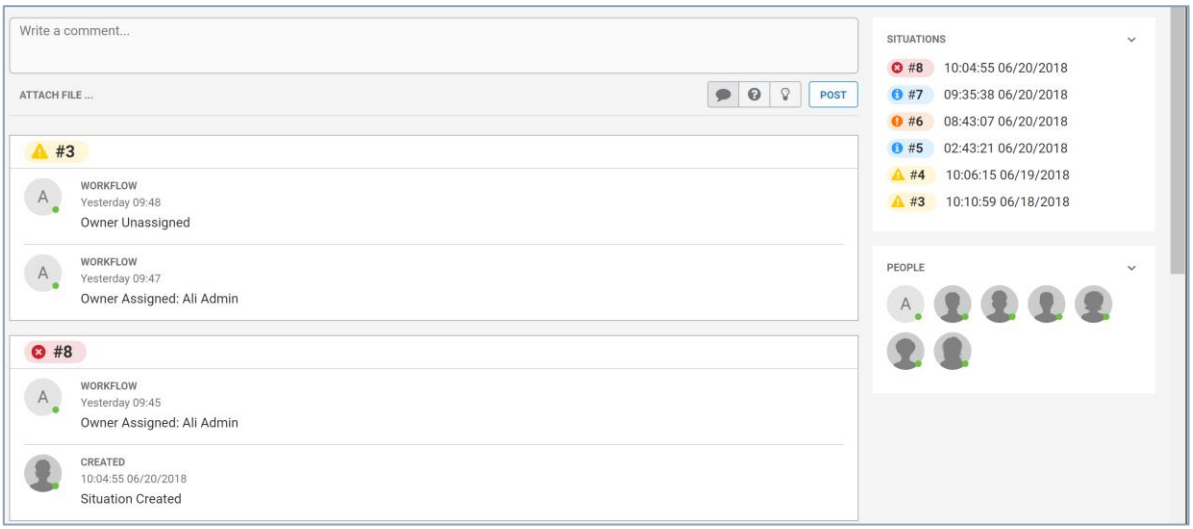
If you are a standard operator User, you can perform the following actions to Situations that have been assigned to you:

Assigned ->	In Progress ->	Resolved
		
Click Acknowledge to inform others you have seen the Situation and are investigating. This moves the Situation to In Progress.	Click Resolve when an initial resolution to the Situation or a Resolving Step has been found. This moves the Situation to Resolved.	Click Close if the resolution fixes the root cause and the moderator or end user is satisfied. This removes the Situation from the Task Board.

When resolving or closing a Situation, you can give it a Situation Rating and add a journal entry in the pop-up window as normal. Once a Situation is closed, it will not appear on the board.

Collaborate in a Team Room

The Collaborate tab is where you can view the latest activity and communicate with members of your team to find resolutions to Situations.



Users can post questions, ideas, general comments and attach files that will appear on the Collaborate news feed in chronological order.

Navigation

The Situations listed on the right side of the screen are all of the Situations which are impacting services included in the team's service filter. The 'People' panel beneath that lists all team members who are currently logged into Cisco Crosswork Situation Manager.

Note: A team's Service Filter can be configured by a User with Administrator rights or higher. This can be found under System Settings > Teams > General.

There are several ways to view a Situation from the Collaborate screen. One way is to click on the Situation ID in the Collaborate wall. Alternatively click the View button in the top corner of each panel:

Both of these options will open the Situation Room for the Situation.

Creating a Comment

You can comment in a Team Room by clicking 'Write a comment...' at the top of the screen and starting to type.

When you have finished, you can click one of the icons to indicate the type of comment you are posting. The speech bubble icon is for general comments, the question mark is for questions and the lightbulb is for ideas.

Next click Post to add the comment to the Collaborate wall. Alternatively use the Ctrl+↵ or ⌘+↵ keyboard shortcut.

You can make additional comments in a comment thread. To do this, click Add a comment, type your message and press Enter to submit.

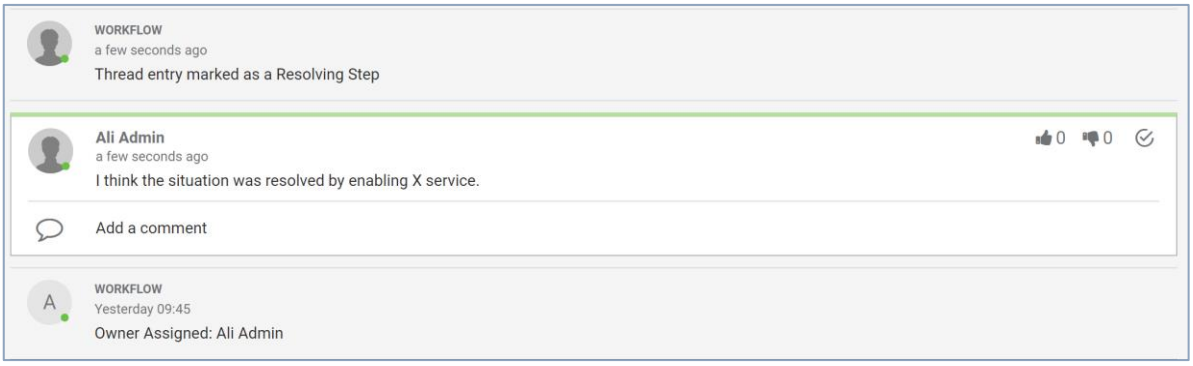
You can up vote or down vote comments using the buttons in the top right corner of the primary comment.

Note: You can only vote on Situation Room comment entries. You cannot vote on your own comments, only on comments made by other users

Marking a Resolving Step

You can mark any suggestion from another user, such as tools which were run to resolve a Situation, as a 'Resolving Step'.

To do this, click the Resolving Step icon in the top right corner of the comment. This will highlight the comment with a green line:



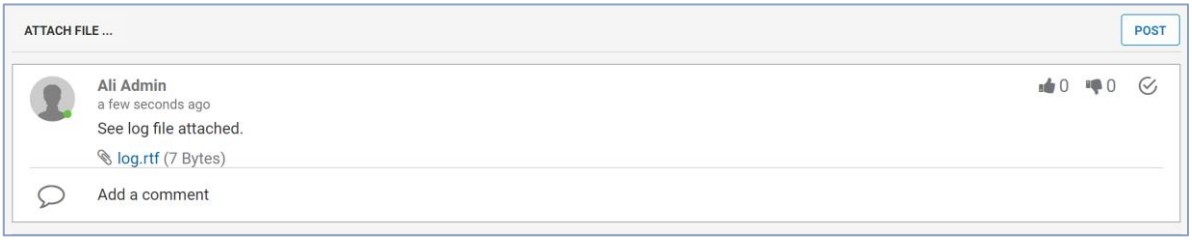
The Resolving Step icon will subsequently appear on any similar Situations. By default, similar Situations are deemed to be all those which share at least 50% of the same alerts.

Note: A comment can be deselected as a Resolving Step at any time by clicking on the check icon again.

Attaching a File

You can attach a file such as a screenshot, error message or log file to any Collaborate wall. To do this, click Attach File... and select the file from any location on your local machine.

Next create a comment as normal to accompany the attachment and then click Post.

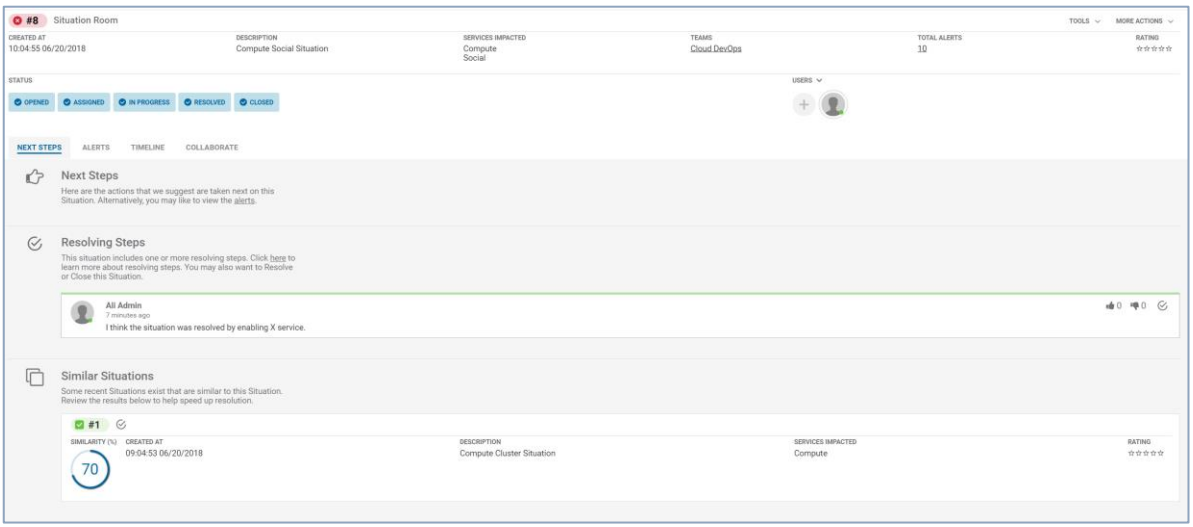


The attachment will appear in blue text alongside the file size in brackets.

Identify Next Steps

You can identify the recommended actions to take with a Situation under Next Steps. This tab is open by default when you first look at a Situation.

The next steps depend on the current status of the Situation and may include similar Situations with Resolving Steps or the alerts which are most likely to be the root cause of the Situation.

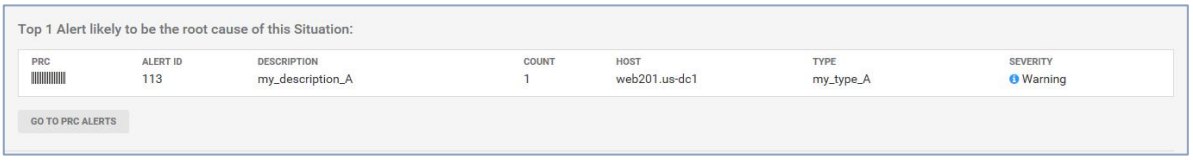


In the example above, the first required step is to Acknowledge the Situation. This can be done by clicking the Acknowledge button under 'Status' or Next Steps.

You can also see there is a similar situation with 70% similarity. If this had a Resolving Step, indicated by a check icon, you could click this to see what action was taken to resolve the similar Situation.

Probable Root Cause

If you have been training your Probable Root Cause model, you will see up to three alerts likely to be the root cause of the Situation. For more information about marking alerts for PRC and training your model see Check Situation Alerts.



Click Go To PRC Alerts to view these alerts in more detail.

Please note: There will be no PRC Alerts in this section if:

- You have not trained your model
- You do not have any Alerts with PRC equal to or greater than 50%.

Topology View and Important Nodes

If you enable Situation topology, you can see a visual representation of the connections within the Situation, based on topological data for the relevant nodes. You can put the Situation into context and gain a better understanding of its impact.

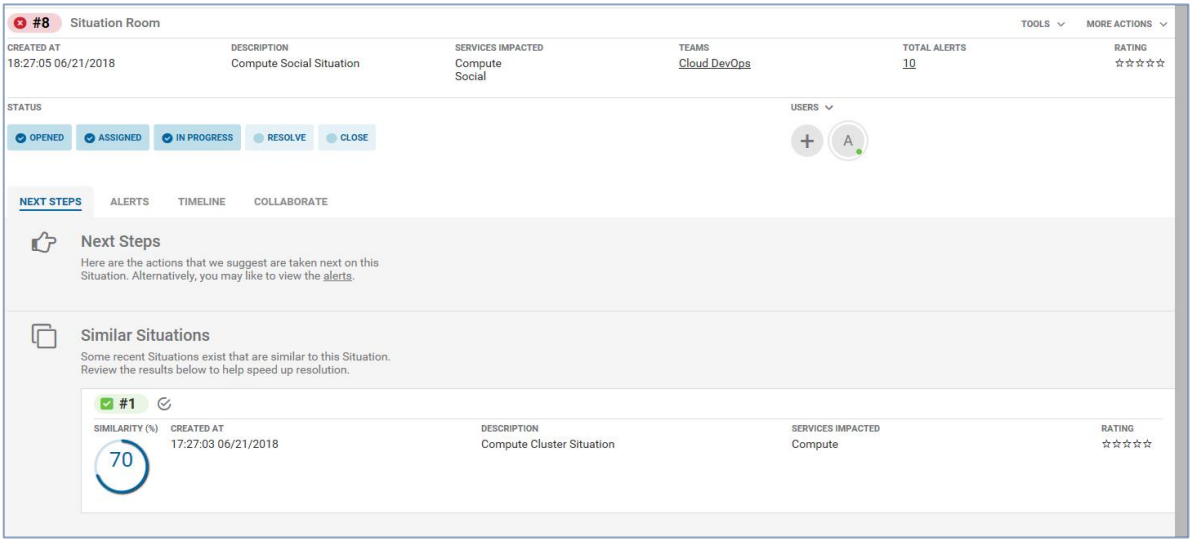
The most important nodes in the Situation topology are listed together with Vertex Entropy data if available. Click View in the Vertex Entropy column or Go to Topology View to display the Situation Topology tab. See View Situation Topology for more information.

Similar Situations

Cisco Crosswork Situation Manager identifies if two or more Situations are similar and groups them in a subsection of Next Steps called Similar Situations.

You can use Next Steps to identify trends and reduce the number of escalations. E.g. If a current Situation is similar to one that was previously resolved then the resolution information might be re-useable. Alternatively, if Situations recur at regular intervals, steps can be taken to prevent future occurrences.

Note: To generate similar Situations, Cisco Crosswork Situation Manager analyzes all Situations, calculates their similarity and highlights those with a similarity of 50% or above. This means at least half of the alerts will be shared between two similar Situations.



For each similar Situation, it will display the Situation ID, similarity (%), the created at time, a description, any impacted services and the Situation Rating.

Click the date beneath 'Created at' for an exact time and date that the Situation was created. Click 'Description', 'Impacted Services' and 'Rating' to make edits.

Note: Only users with the correct Role permissions can made edits to 'Description' and 'Impacted Services'

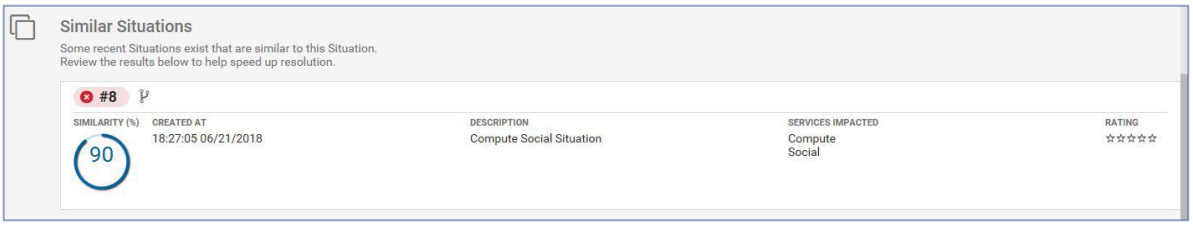
Alternatively, click the Situation ID or View to open the Situation Room for the Similar Situation.

Merged Similar Situations

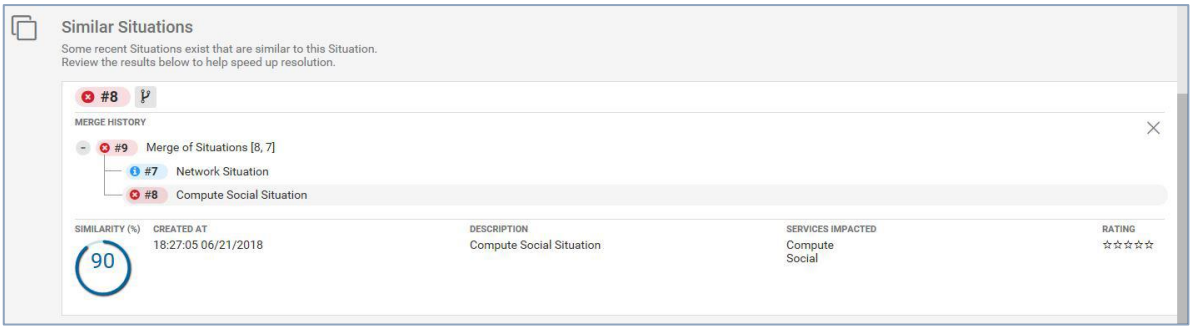
If a number of Situations share a high similarity and alerts then Cisco Crosswork Situation Manager will merge them together automatically to create a new Situation.

Note: By default Cisco Crosswork Situation Manager carries out an automatic merge when Situations share a 70% similarity

If a Situation has been merged automatically or manually there will be a merge icon alongside the Situation ID:



Click the icon to show or hide the merge history. In this example, Situation #8 had an 90% similarity so was merged into Situation #24.



For more information about merging Situations see Merge Situations.

Similar Situations with Resolving Steps

If a Similar Situation has a Resolving Step, this is indicated by the check icon:

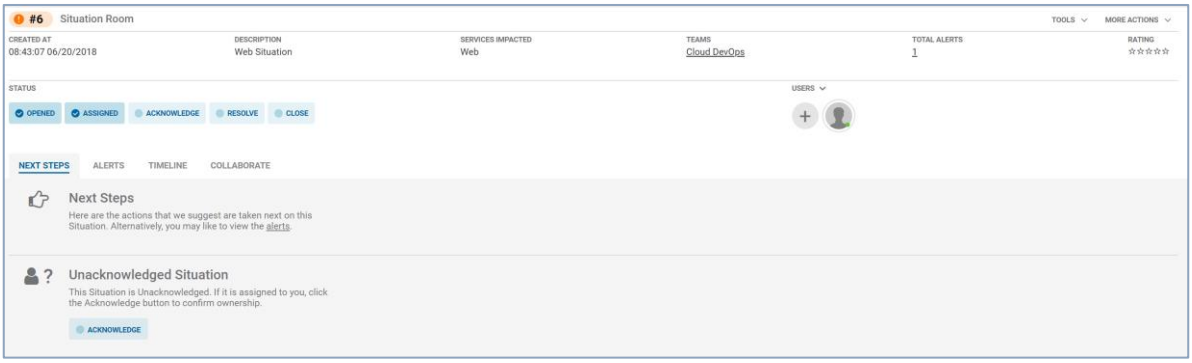
Click the check icon to reveal any Resolving Steps, which are comments that appeared in the Collaborate tab that led to or provided a resolution:

Click the Resolving Step icon at the top of the panel again to close it. Alternatively you can add a comment or a vote if it was helpful or not.

Situation Rooms

The Situation Room is the virtual meeting place for all users involved in finding the resolution to the Situation and its alerts.

This is where you will spend the most time when you are investigating the root cause of an incident.



At the top of the Situation Room you can see when it was created, any impacted services, the Alerts it contains and the rating it was given at resolution.

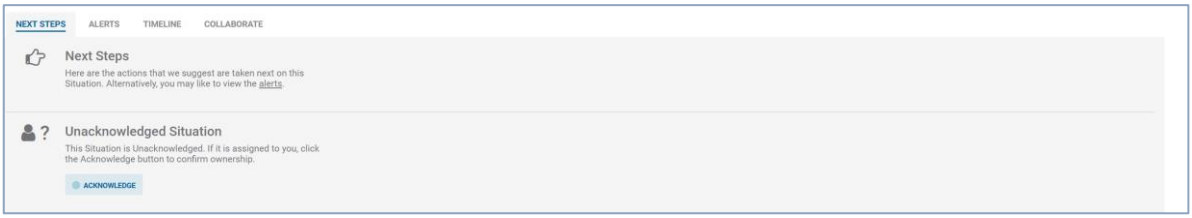
Situation Room Tabs

The Situation Room tabs at the bottom of the screen offer links to the Next Steps, Alerts, Timeline and Collaborate which can be followed in a logical order:

Note: Additional tabs linking to third-party tools can be added in the form of Situation Room plugins.

Next Steps

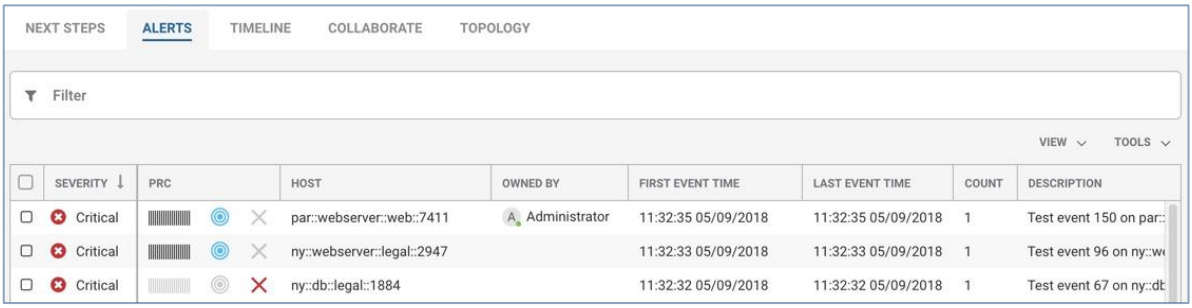
The Next Steps tab will offer you a suggested action step to take in relation to the Situation.



The suggestion will depend on the status, if it has similar Situations or if there are Resolving Steps.

Alerts

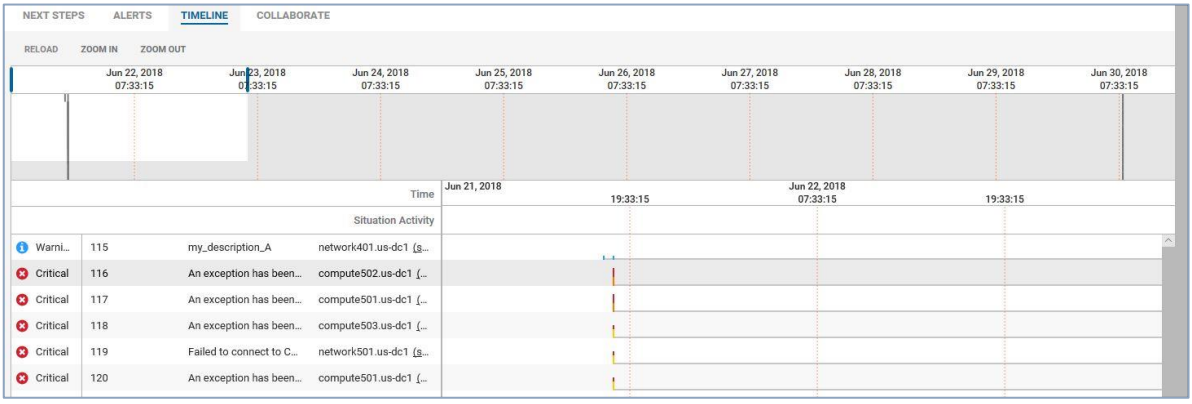
The Alerts tab is useful for looking at the Situation's individual associated alerts in more detail.



From here you can filter and identify the alerts of interest and then seek a resolution. To activate the Select All checkbox, scroll down to load all alerts.

Timeline

The Timeline offers a powerful graphical view displaying the progression of a Situation with a breakdown of its associated Alerts in the order they occurred.



Alongside the Alerts, you can also inspect the markers where activity took place. See Analyze the Situation Timeline.

Collaborate

The final step is to collaborate with other users by looking at the comments and talking to colleagues.

The ultimate goal is to find a way to resolve the Alerts and subsequently the Situation. See Collaborate on the Situation.

Invite Users to the Situation Room

You can invite team members who you think might be able to help resolve a Situation using the + invite button. You can only invite users who are members of your team by default.

Type the name of the user you want to invite, add a note if required and click Done. The invited user will receive the invitation as a notification.

You will only be able to invite others users to a Situation Room if you have been assigned to the Situation.

Note: You may only be able to invite members of your team to a Situation Room if your administrator has configured team access only.

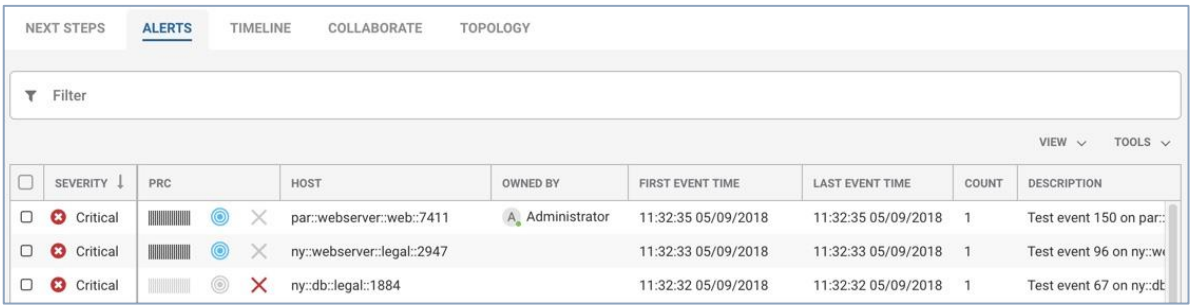
Other Situation Room Actions

There are a number of other actions that can be performed using the Tools and More Actions drop-down menus on the top bar of the Situation Room.

For more information about these menus and other actions that can be performed see Take Additional Actions.

Check Situation Alerts

You can look at the Situation's associated alerts from the Situation Room by clicking the alerts tab.



From here you can filter and identify the alerts of interest, typically those with the highest severity or that are impacting services, and then seek a resolution.

View Unique Alerts

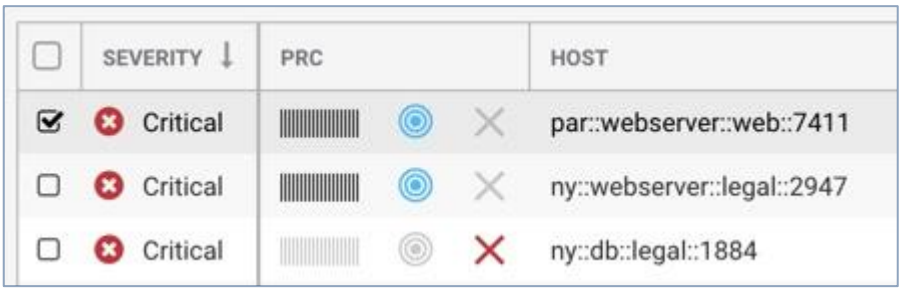
You can switch between viewing all alerts and all unique alerts using the View menu.

Click View and then either Show All Alerts or Show Unique Alerts to toggle between which group of alerts are displayed.

Mark Alerts for PRC

Follow the steps below to mark individual Alerts for PRC:

1. Click the circular PRC icon to mark an Alert as a Root Cause Alert.



2. When selected, the PRC icon turns blue.

   Cisco Crosswork Situation Manager will also report that PRC feedback is in progress.

3. If there are any alerts you know are not the root cause of the Situation, click the cross icon. This will turn red when selected.

4. Click the Save button. The % PRC will be indicated by the bars in the PRC column.

   Note: If you do not know the status of an alert do not label it. You do not have to label every alert: PRC is effective with consistent data

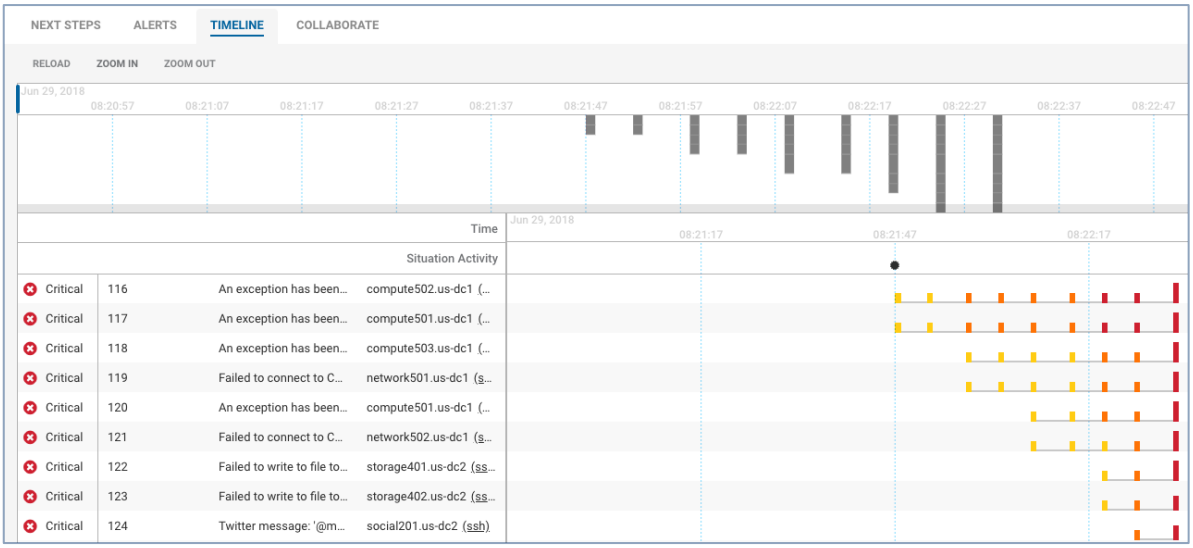
5. Open another Situation and look at the alerts. The PRC column will automatically populate with estimated PRC values based on the user feedback.

See Probable Root Cause more information about how PRC can help you reduce MTTR.

Analyze the Situation Timeline

The timeline offers a powerful graphical view displaying the progression of a Situation with a breakdown of its associated alerts in the order they occurred alongside key activity markers.

Use the timeline to analyze the Situation, see how it developed and determine the hotspots where there are higher volumes of more severe alerts.



Note: Situation severity is determined by the highest severity of its alerts.

In the example above the Situation is critical because the 4th of six recorded alerts was critical, which was ultimately the highest severity.

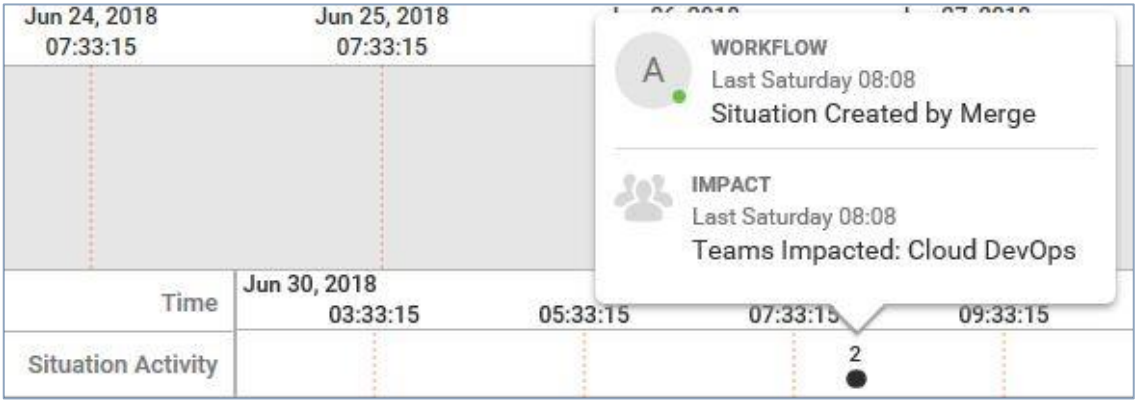
Timeline Navigation

There are several components to the timeline tab which allow you to zoom in on a specific time, view Situation activity and display when alerts occurred.

Situation Activity

The Situation Activity panel will show activity markers at times where different things happened following the creation of the Situation.

The number indicates how many Situations activities occurred. Click on any of the activity markers for more details of what happened at that time.

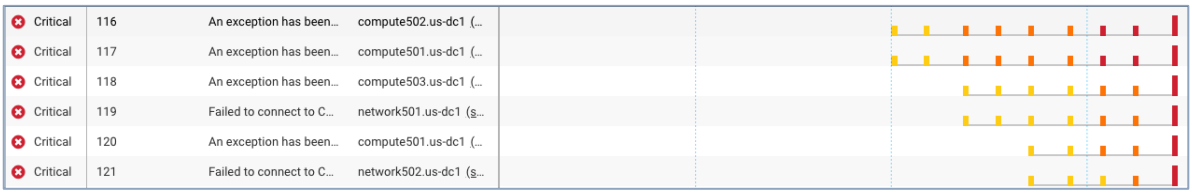


In this example above, the five activities were: the creation of the Situation itself, it impacted the Ops Team, the Situation custom info was changed, 15 further Alerts were added to the Situation and then it was assigned to a User.

The activity marker icons will differ depending on the type of activity that occurred.

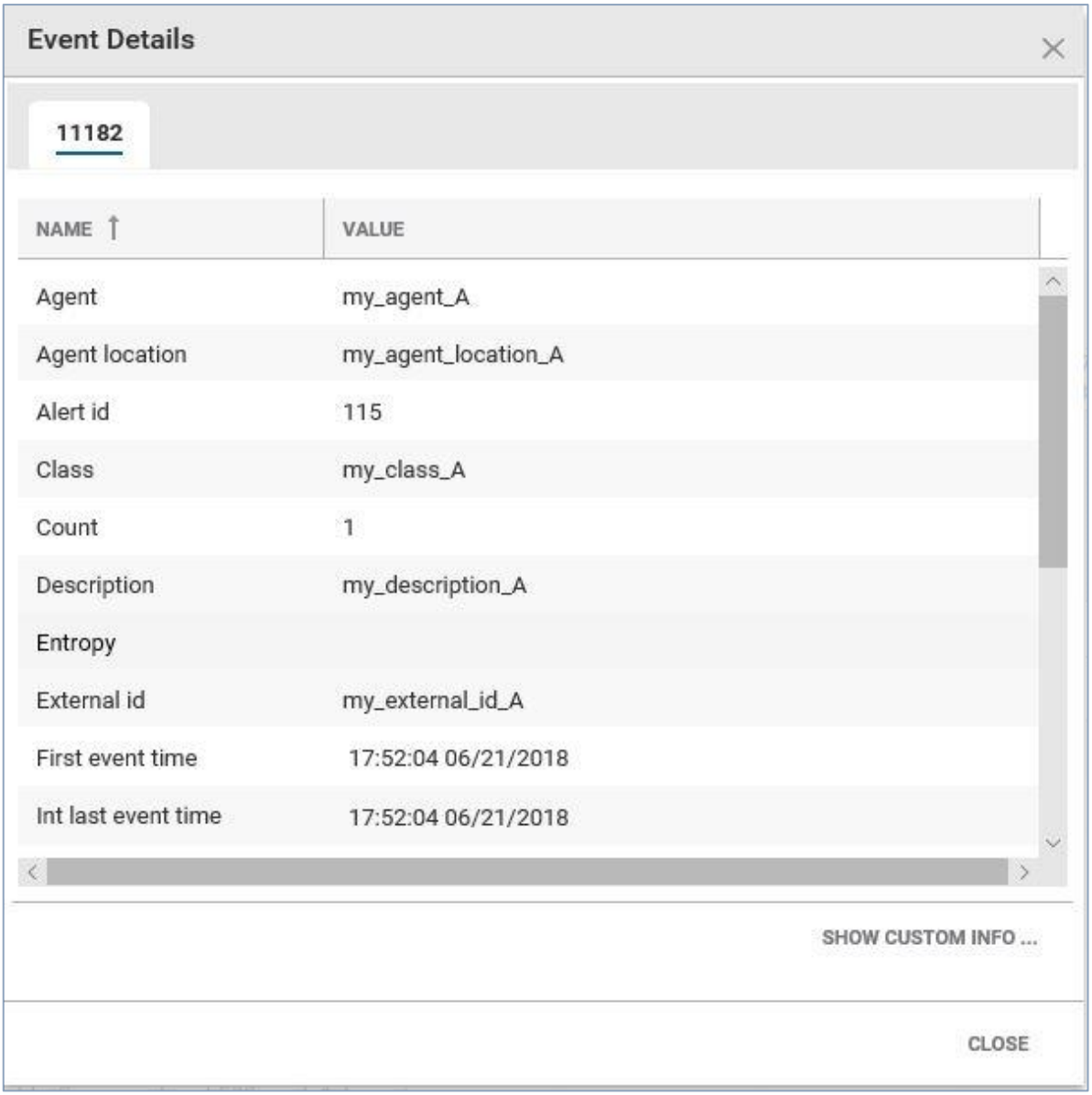
Alerts and Event Details

The alerts are displayed in graphical form on the bottom of the Timeline tab, with each alert represented by a rectangular block the color of its severity.



You can view the details of the events within each alert by clicking each block. This opens the Event Details window:

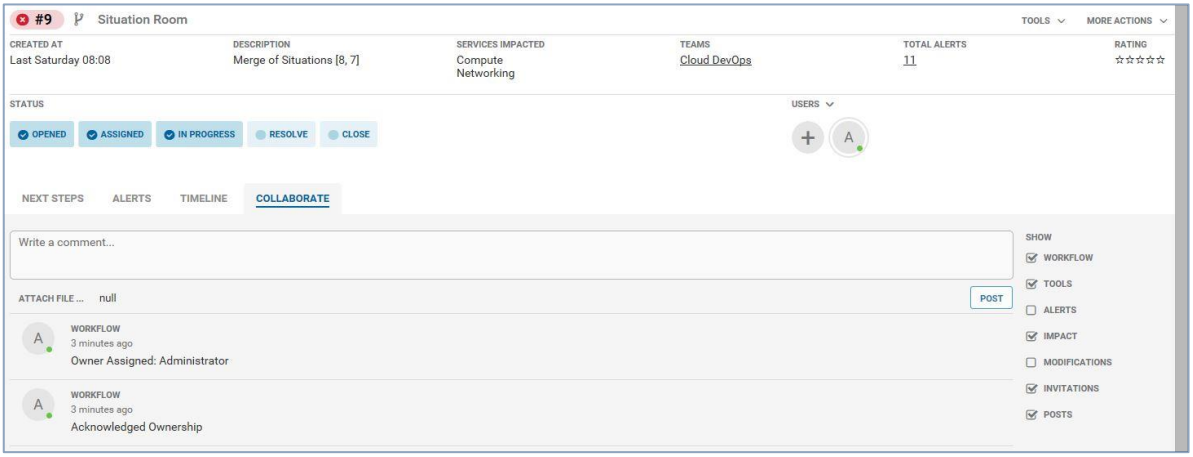
Note: You can open the Alert Details window by clicking the Alert ID.



In this example, alert 94 contains events 200 and 201 which were detected by a Network Monitor.

Collaborate on a Situation

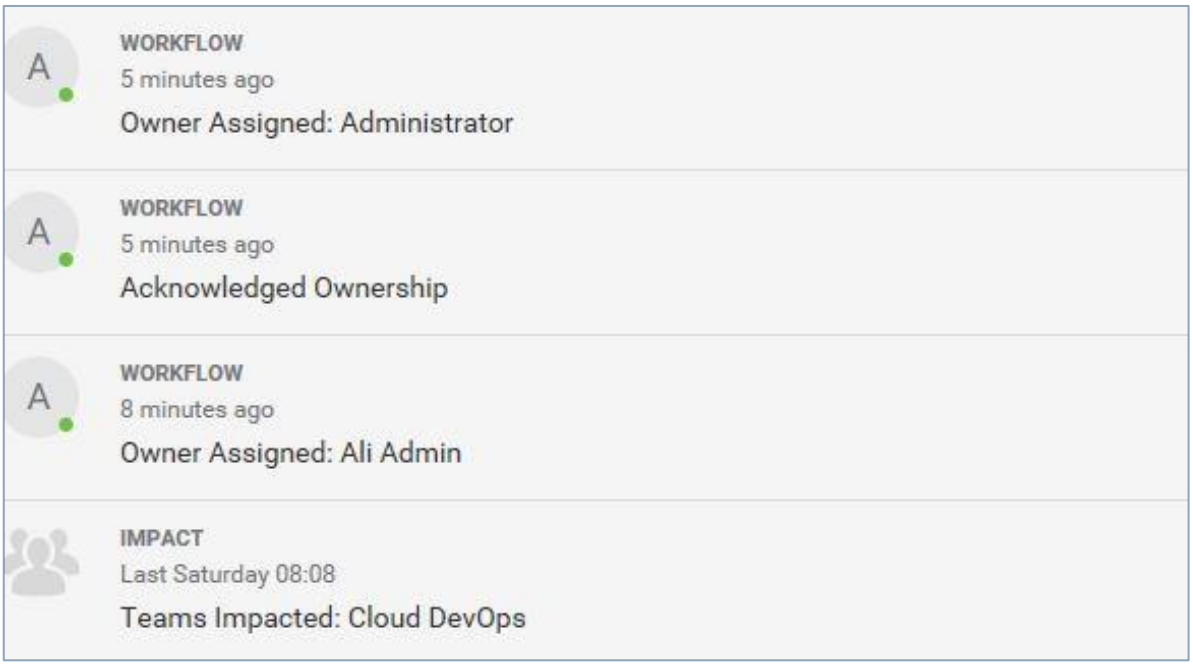
The Collaborate tab provides a chat environment where you can talk to your team members and resolve a Situation.



You can add comments, attach files, and view activity such as which teams are impacted and when the Situation was created or assigned to a user etc.

Navigation

To view all previous comments and Situation activity, scroll down to the bottom of the Collaborate view.



It works much like a social media news feed wall with the oldest comments and activity at the bottom and the latest at the top.

Custom Situation Room Tools

You can run a number of custom tools in the Situation Room that your admin has configured for you and your team.

These might include Client tools, URL tools and tools triggered by ChatOps commands.

Run a ChatOps Tool

As well as comments, you can also run ChatOps tools to try and find a resolution to the issue.

Generic Tools, Alert and Situation Server Tools, or Alert and Situation Client Tools can be run using the @moog or @bot command following by the configured ChatOps shortcut.

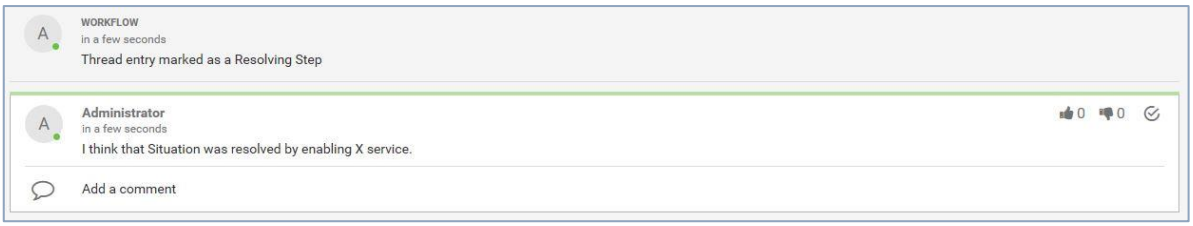
Note: An administrator must configure ChatOps and Tools See ChatOps.

If the ChatOps tool was successful in resolving the issue, it can be marked as a Resolving Step.

Mark a Resolving Step

If a user makes a suggestion that resolves the Situation or its alerts, then it can be marked as a 'Resolving Step'.

To do this, click the Resolving Step icon in the top right corner of the comment. This will highlight the comment with a green line:

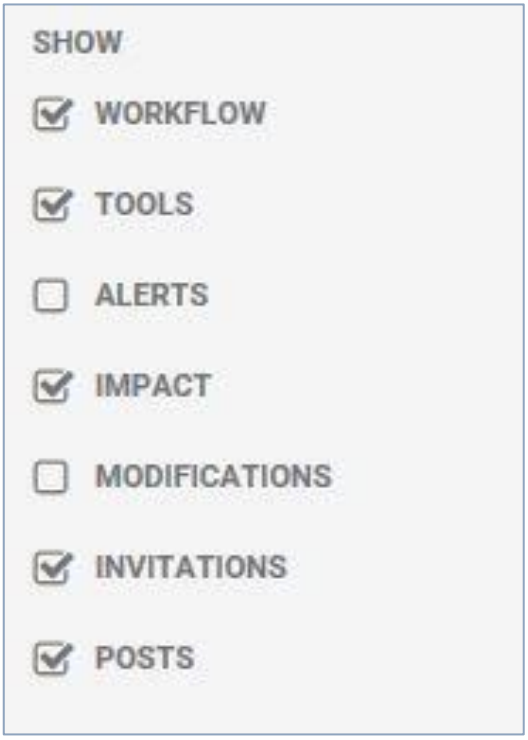


The Resolving Step icon will subsequently appear on any Similar Situations.

Note: Click the icon again to remove a Resolving Step.

Use the Show Filter

The Show filter can be used to filter which types of activity and comments appear in the Collaborate tab.



The different types can be added or excluded by checking or unchecking the boxes.

These types include: workflow, tools, alerts, impact, modifications, invitations and posts.

View Situation Topology

Issues affecting different systems in your network can frequently be related to the same Situation. Cisco Crosswork Situation Manager uses topological data to present a visual representation of connections between the hosts impacted by a Situation.

The topology is host-based. Cisco Crosswork Situation Manager identifies hosts using the "host" field from alerts. Each host in your system is a potential node in the topology.

When a Situation affects more than one node and Cisco Crosswork Situation Manager has topological data for those nodes, you can use the Situation Room Topology tab.

Before You Begin

Your administrator must follow these steps to enable the topology view in the Situation Room:

1. Run the topology builder utility to generate the topology data.
2. Optionally run the graph analyser utility if you want to generate Vertex Entropy data.

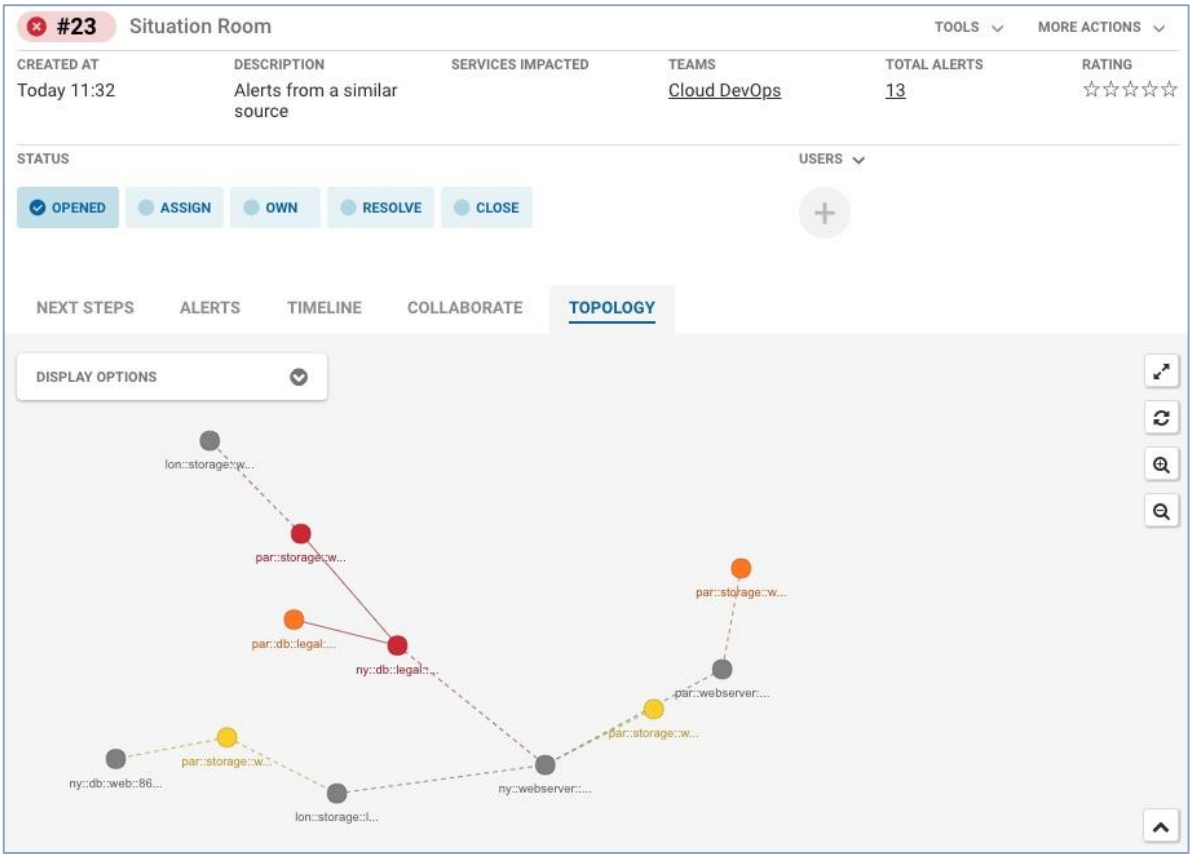
   Once the topology builder utility has been run, the Situation topology automatically renders based on the contents of the Situation.

Topology Navigation

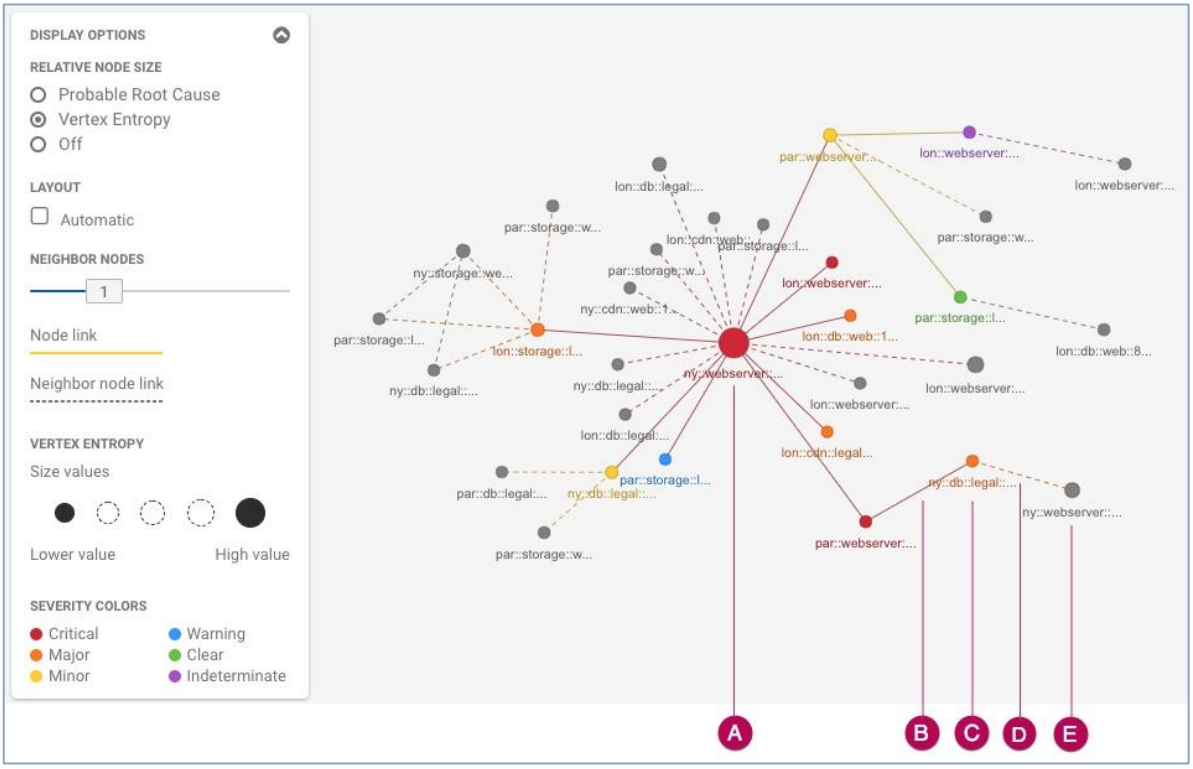
While in a Situation Room, click the Topology tab. You can toggle full screen view to hide the other elements on the screen and focus on the topology. Use the zoom buttons on the right side of the topology to zoom in and out. Node labels appear as you zoom in.

Click and drag the nodes to rearrange the topology view. Hover your mouse cursor over a node to display its name, description and service data. Open the Display Options window to access options for relative node size, neighbor node selection and a description of the severity colors.

For example, consider the following topology that indicates a potentially serious Situation that requires immediate investigation. Two nodes (red) are critical, another two nodes (orange) are major and they are connected to other nodes that are as yet unaffected.



The following example shows a Situation with many involved nodes, some of which are critical:



A. The node with the highest Vertex Entropy value is critical in this Situation.

B. A solid line indicates a link between affected nodes. The higher severity determines the color of the line.

C. Several other nodes are involved in the Situation with varying levels of severity.

D. A dotted gray line indicates a link between unaffected nodes.

E. Gray nodes are not involved in the Situation but appear on the topology depending on the Neighbor Nodes selection.

View Neighbor Nodes

The topology displays affected nodes and their immediate neighbors, even if the neighbors are not involved in the Situation. Neighbor nodes provide context about the nodes in the Situation, relative to their location in the topology. For example, if you increase the number of neighbor nodes you may see that two nodes in the Situation are connected to the same switch, that is not part of the Situation.

Open the Display Options window on the left side of the topology view and use the neighbor nodes slider to control the number of neighbor nodes on display. You can show:

- a maximum of 4 neighbors
- up to 150 uninvolved neighbor nodes in total

The maximum number of neighbor nodes on the slider corresponds to the total number of uninvolved nodes in the topology. For example, if a neighbor node level of 4 includes 151 uninvolved nodes, the slider maximum is automatically set to 3. There is no limit on the number of affected nodes you can display, however large topologies of 500+ affected nodes can take more than a minute to load.

View Alert Severity

The color of the node reflects the highest severity of its alerts. Open the Display Options window to see a description of the severity colors. Neighbor nodes that are not involved in the Situation are gray.

View Related Alerts

Click a colored node to display its related alerts in the alerts list beneath the topology. The selected node and its links are highlighted in the topology view and alerts affecting the selected node appear in the list.

The alerts are shown with the same layout as the Situation Room alert list.

Filter Alerts

You can add filters to refine the list of alerts using full or partial matching. Nodes matching the filter are highlighted in the topology. For example, the filter "Host: web" will display all alerts with host names that include the string "web".

View Vertex Entropy

If you want the topology to indicate Vertex Entropy, your administrator must run the graph analyser utility to generate the data.

Open the Tools window and select Vertex Entropy. The size of the node indicates Vertex Entropy. The larger the node, the higher the Vertex Entropy value.

View PRC

If you want the topology to indicate Probable Root Cause (PRC), ensure that PRC data exists for one or more alerts in the Situation.

Open the Display Options window and select Probable Root Cause. The size of the node indicates PRC. The larger the node, the higher the PRC value.

Refresh the Topology

Cisco Crosswork Situation Manager does not automatically update the topology when alert details change. Click the Refresh button on the right side of the topology view to update the topology.

Merge Situations

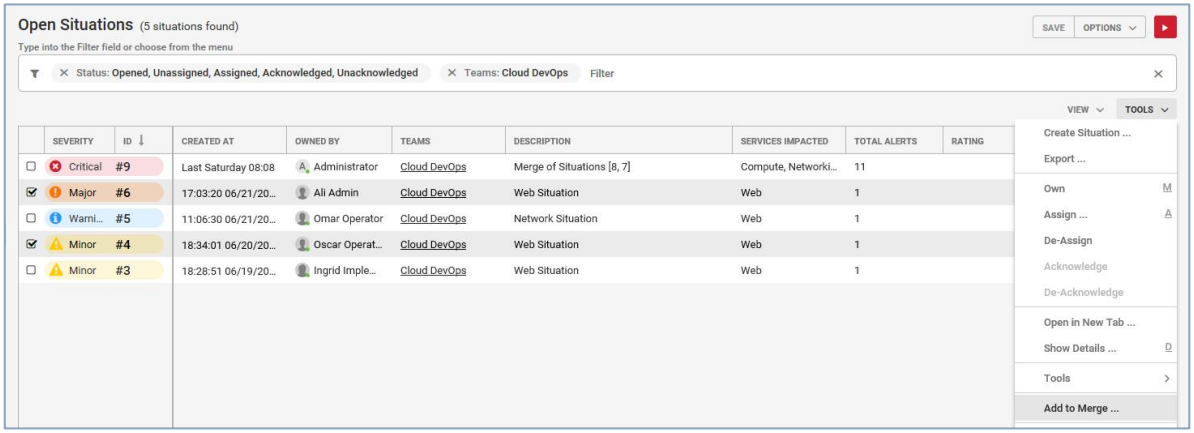
You might want to merge multiple Situations into one Situation if they share a significant number of alerts, or if you think they all share the same root cause.

Cisco Crosswork Situation Manager merges Situations automatically if they share 70% of the same alerts. You can also merge Situations manually from any of the Situation filter views and from a Situation Room.

Merge Two or More Situations

To merge Situations from a Situations view:

1. Select the Situations you want to merge: click the boxes in the far-left column.



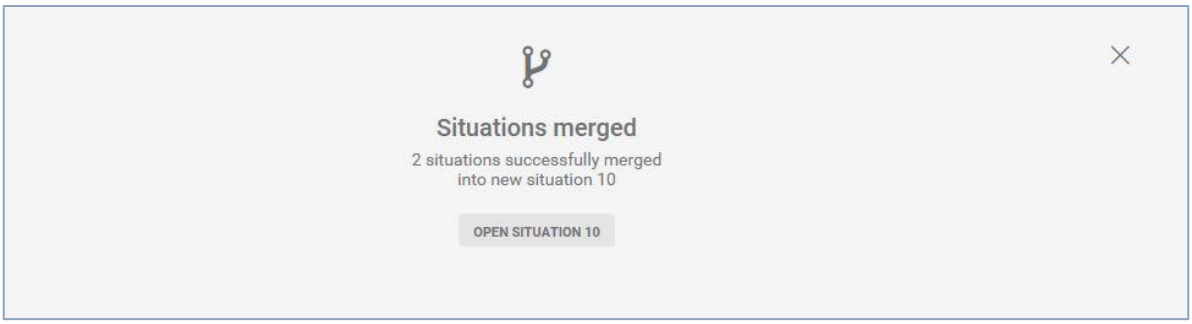
2. Click Tools or right-click on the Situations to open the Tools Menu.

3. Click Add to Merge... to open the Merge Situations panel displaying the selected Situations. This should appear at the top of the Situations view.

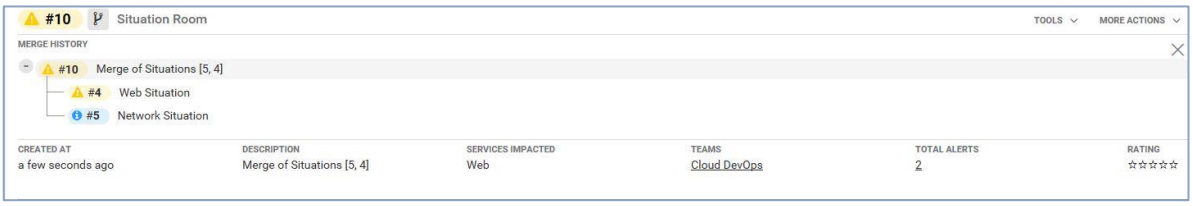
4. To add more Situations, repeat these steps. To remove Situations, click the 'X' icons.

5. To complete the merge, click Merge Situations. A message appears with a link to the new Situation.

   Note: By merging Situations, you are combining all of Situations' alerts so the severity of the new Situation will reflect the highest severity of those alerts.



Click Open Situation to open the Situation Room for the new Situation. From here you can click the merge icon to show the Situation's merge history and see the Situations which were merged to create it.



Take Additional Actions

You can use the menus and icons at the top of the Situation Room in Cisco Crosswork Situation Manager to perform additional actions on a Situation.

Tools

The Tools menu links to any Client Tools, General Server Tools and Situation Server Tools which have been set up by your administrator.

Client tools use Situation and Alert data to carry out actions through a specified URL. Generic, Alert and Situation Server Tools allow a user to execute a utility on a remote host.

More Actions

There are a number of actions under the More Actions menu:

Action (Hotkey)	Description
Show details...	This opens the Situation Details pop-up window
Own (M)	This makes you the owner of the Situation. This also automatically acknowledges the Situation*
Assign (A)	This allows you to assign the Situation to a user*
De-Assign	This de-assigns the Situation from a user
De-Acknowledge	This de-acknowledges the Situation
Add to Merge...	This adds the Situation to the merge panel (where multiple Situations can be merged). See Merge Situations.
Resolve...	This opens the Situation Rating dialog where you can resolve the Situation
Close...	This opens the Situation Rating dialog where you can close the Situation
Reopen...	This reopens the Situation if it has been resolved or closed

Note: Only users with the correct permissions can 'Own' or 'Assign' a Situation.

Situation Status

The Situation status shows the Situation's workflow journey. The highlighted item furthest to the right indicates the current status. For example, the status for the Situation below is "In Progress":

Clicking any of the subsequent statuses or actions in the row will allow you to change the Situation's status or perform an action.

When Cisco Crosswork Situation Manager creates a Situation, it is "Opened" by default. Then someone assigns it to a user who acknowledges' it. When the user begins work, they update the status to 'In Progress'. When they have solved the issue, they mark it as 'Resolved'. Subsequently, someone can close the issue. The following table provides full descriptions of all Situation statuses:

Status	Description
Opened	The Situation is open but not yet owned or assigned.
Assigned	The Situation is assigned to a user but not yet acknowledged.
In Progress	The Situation has been acknowledged and is being worked on.
Resolved	This is an internal status and means that the operator believes they have a resolution to the Situation.
Closed	The resolution has been confirmed by the person or system who reported the issue and they are satisfied with the resolution.
Dormant	The Situation has been merged into a newer Situation. The older Situation adopts the dormant status.

ChatOps

The ChatOps feature enables Cisco Crosswork Situation Manager users to run tools, such as executing utilities on remote hosts, from the Collaborate section of a Situation Room. This is useful when collaborating to resolve a Situation.

Tools run by ChatOps include Generic, Alert and Situation Server tools, as well as Alert and Situation tools.

Note: Your administrator will first need to configure both your tools and the ChatOps shortcuts in the System Settings.

Run a ChatOps Tool

To run ChatOps from Collaborate, you will need to start a new entry and type @moog or @bot and a drop-down menu of available tools will appear:

Scroll through the tools or start typing to find the required tool. Once you have found the one you want to run, hit Enter or Tab to continue.

If the tool ran successfully, a message will appear in green stating "Tool success" as shown in the screenshot below:

For certain tools, the diagnostic results appear as a comment under that entry that is visible to all collaborators and team members.

If the tool did not run successfully, either because it was not configured properly or there was an error, you can expect an error response.

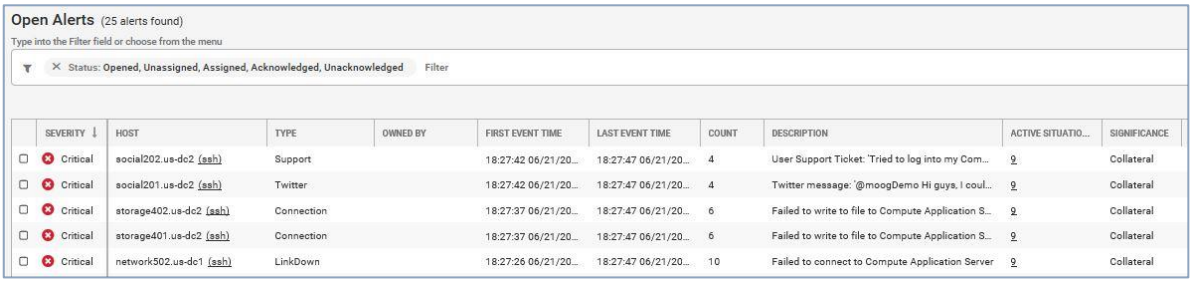
If the ChatOps tool was successful at resolving the root cause of the incident, it should be marked as a Resolving Step. See Resolve Situations.

Advanced Usage

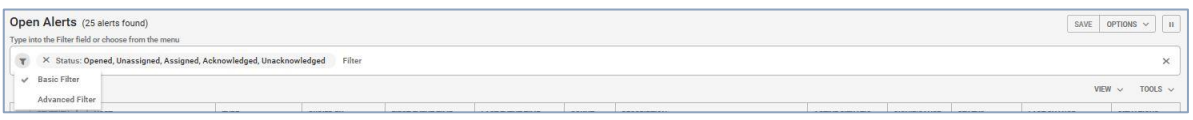
Filter Search Data

You can search for specific Alerts, Situations, and Impacted Services in Cisco Crosswork Situation Manager using filters.

The default filter views that can be accessed from the Workbench are Impacted Services, My Situations, Open Situations, My Alerts, and Open Alerts.



There are two types of the filter: Basic Filter and Advanced Filter. Click the funnel filter icon to open the drop-down menu and switch between the filter types.



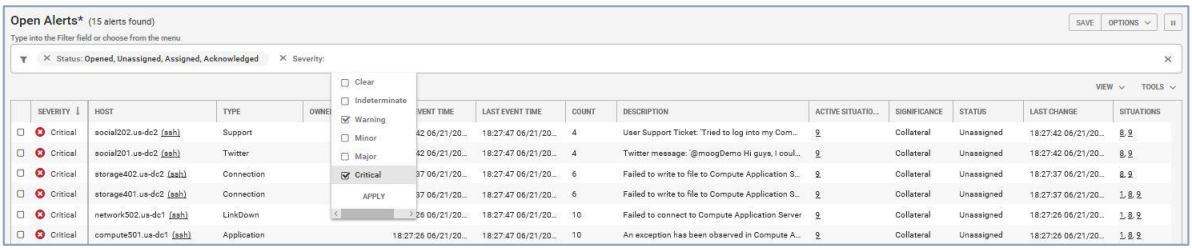
Note: We recommend you use the Basic Filter in most cases but if you want more flexibility or need to filter for something more complex then use the Advanced Filter.

Create a Basic Filter

To use the Basic Filter, click in the "Filter" bar. A drop-down menu then appears with available fields.

Select a field and any values as required; then click Apply or click away from the menu. Repeat this for as many fields as you want to add to your filter.

Alternatively, type the name of the fields you want to apply to the filter. Once you have entered one or more fields, click away from the menu to apply the filter.



Alert Column Parameters

You can use the columns and operators displayed in the tables below in your Basic Filter:

Column Display Name	Associated Operators
Active Situations	IN
Alert Id	> >= < <= != =
Agent Name	MATCHES
Agent Host	MATCHES
Class	MATCHES
Count	>> >= < <= != =
Description	MATCHES
Entropy	>> >= < <=

	!= =
External ID	MATCHES
First Event Time	>= AND <=
Host	MATCHES
Internal Last Event Time	>= AND <=
Last Change	>= AND <=
Last Event Time	>= AND <=
Manager	MATCHES
Owned By	IN
Severity	IN
Significance	IN
Situations	IN
Source ID	MATCHES
Status	IN
Type	MATCHES

Situation Column Parameters

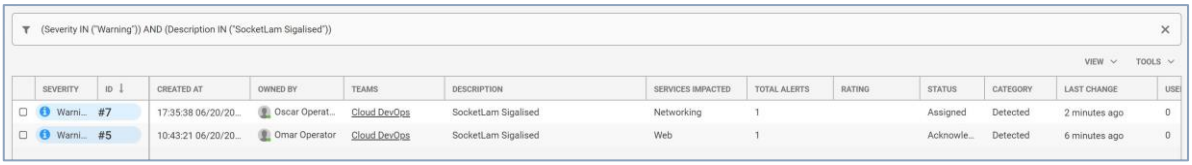
Column Display Name	Associated Operators
Category	MATCHES
Created At	>= AND <=
Description	MATCHES
First Event Time	>= AND <=
ID	> >= < <= != =
Last Change	>= AND <=
Last Event Time	>= AND <=

Owned By	IN
Participants	> >= < <= != =
Process Impacted	CONTAINS
Scope Trend	>0 <=0
Services Impacted	CONTAINS
Sev Trend	>0 <=0
Severity	IN
Status	IN
Story	>= < <= != =
Teams	IN
Total Alerts	>= < <= != =
User Comments	>= < <= !=

Create an Advanced Filter

The Advanced Filter is for complex queries and operates in a similar way to the Basic Filter but uses Cisco's filter query language which is based on SQL.

To show all Situations with 'Severity' as 'Warning' and 'Description' as 'SocketLam Sigalised', the correct syntax would be: (Internal Severity IN ("Warning")) AND (Description MATCHES "SocketLam Sigalised").

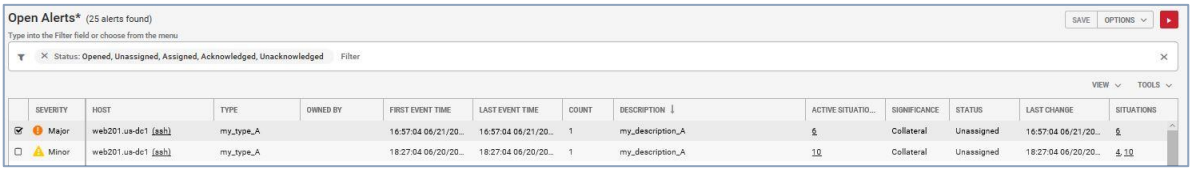


For more information on the query language syntax, see the tables of available operators and the examples below.

Pause Alerts and Situations

Click the Pause button to temporarily stop Alerts or Situations being added to the Alert or Situation view.

Note: When paused, Cisco Crosswork Situation Manager will not update the list with the latest data unless you apply a new filter which will trigger a one-time load of data.



After any edits have been made, the live feed of data can be reactivated again by clicking the Play button.

Advanced Filter Syntax

The Advanced Filter query syntax can be used to create more complex filters for Alerts and Situations.

This syntax uses column display name parameters alongside common query operators used in filters. The column parameters and their associated operators are listed in the sections below.

Note: The Advanced Filter query syntax uses the display column names (those shown in the UI) rather than the database column names.

Alert Column Parameters

Column Display Name	Associated Operators
Active Situations	IN CONTAINS = !=
Alert Id	> >= < <= != = IN
Agent Name	MATCHES = !=

Agent Host	MATCHES = !=
Class	MATCHES = !=
Count	> >= < <= != =
Description	MATCHES = !=
Entropy	> >= < <= != =
External ID	MATCHES = !=
First Event Time	> >= < <=
Host	MATCHES = !=
Internal Last Event Time	> >= < <=
Last Change	> >= < <=
Last Event Time	> >= < <=

Manager	MATCHES = !=
Owned By	IN = !=
Severity	IN = !=
Significance	IN = !=
Situations	IN CONTAINS = !=
Source ID	MATCHES = !=
Status	IN = !=
Type	MATCHES = !=

Situation Column Parameters

Column Display Name	Associated Operators
Category	MATCHES = !=
Created At	> >= < <=
Description	MATCHES = !=
First Event Time	> >= <

	<=
ID	>= < <= != = IN
Last Change	>= < <=
Last Event Time	>= < <=
Owned By	IN = !=
Participants	>= < <= != =
Process Impacted	IN CONTAINS = !=
Scope Trend	>0 <=0
Services Impacted	IN CONTAINS = !=
Sev Trend	>0 <=0
Severity	IN = !=
Status	IN =

	!=
Story	> >= < <= != =
Teams	IN CONTAINS = !=
Total Alerts	>> >= < <= != =
User Comments	>> >= < <= !=

The associated operators are described in the tables below.

Comparison Operators

Operator	Description	Example	Result
=	Equal to	Alert ID = 120	Alerts which have an Alert Id of 120
<>	Not equal to	Alert ID <> 120	Alerts which do not have an Alert Id of 120
>	Greater than	ID > 100	Situations where the Situation Id is greater than 100
<	Less than	ID < 100	Situations where the Situation Id is less than 100
>=	Greater than or equal to	ID >= 100	Situations where the Situation Id is greater than or equal to 100
<=	Less than or equal to	ID <= 100	Situations where the Situation Id is less than or equal to 10

Literal Operators

Operator	Description	Example	Result
' ' or " "	Single or double quotations indicate the start	description = "test"	Situations with 'test' as the

	and end of a string value		description
( )	List of items	teams = (1,2,3)	Situations that are assigned to teams 1, 2 and 3 (and only 1, 2 and 3)

Logical Operators

Operator	Description	Example	Result
AND	AND allows the existence of multiple conditions	ID < 100 AND queue=4	Situations where the Situation Id is less than 100 and the queue is 4 (both must be true)
OR	OR is used to combine multiple conditions	ID < 100 OR queue=4	Situations where either the Situation Id is less than 100 or the queue is 4
NOT	Reverses the meaning of the logical operator used. E.g. NOT IN, IS NOT NULL etc.	queue NOT IN (1,2,3)	Situations where the queue is not 1, 2 or 3

Other Operators

Operator	Description	Example	Result
IN	Compares a value to a list of specified values	queue IN (1,2,3)	Situations where the queue is 1, 2 or 3
IS NULL	Compares with a NULL value	queue IS NULL	Situations where there is no queue
MATCHES	Matches the regular expression	description MATCHES "test"	Situations where the description matches the regular expression "test"
ANY_MATCH	Any matches of the regular expression	teams ANY_MATCH "team[0-9]+"	Situations where one of the teams names match the regular expression team[0-9]+
ALL_MATCH	All matches of the regular expression	teams ALL_MATCH "team[0-9]+"	Situations where all of teams names match the regular expression team[0-9]+
CONTAINS	Contains the value	teams CONTAINS (1,2,3)	Situations where the teams contain 1, 2 and 3

Creating an Advanced Filter

When creating an Advanced Filter, it should contain at least one column name, an associated operator, and a value. As a general rule, the column name should always be to the left of the operator.

Important: If the column name or the value contains a space then it needs to be surrounded by single or double quotation marks (both " " and ' ' are accepted). This applies to columns such as External ID, Last Event Time, Last Change, Scope Trend etc. For example, 'External ID' MATCHES 01 or "External ID" MATCHES 01 are both valid.

It is also important to note that column names are case insensitive but the values are case sensitive. For example, 'severity' = 'Critical' is valid but 'severity' = 'critical' is not.

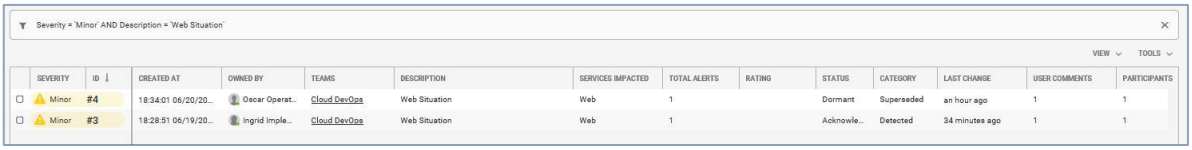
If the syntax is incorrect or invalid then the filter bar will flash, see screenshot below:

For reference please see the examples and screenshots displayed below:

Example 1

Severity = 'Minor' AND Description = 'Web Situation'

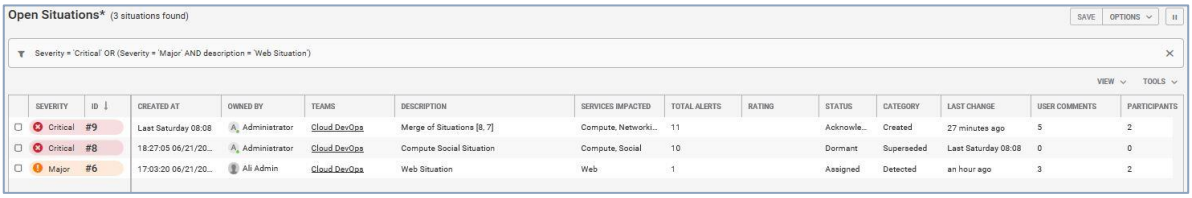
In this example, the filter shows all Alerts with 'Minor' severity and with the description 'Web Situation':



Example 2

Severity = 'Critical' OR (Severity = 'Major' AND description = 'SocketLam Sigalised')

In this example, the filter shows all Alerts with 'Critical' or 'Major' severity and with a type of 'SocketLam Sigalised':



Example 3

Type MATCHES 'Anomalyflag' AND Count = 1

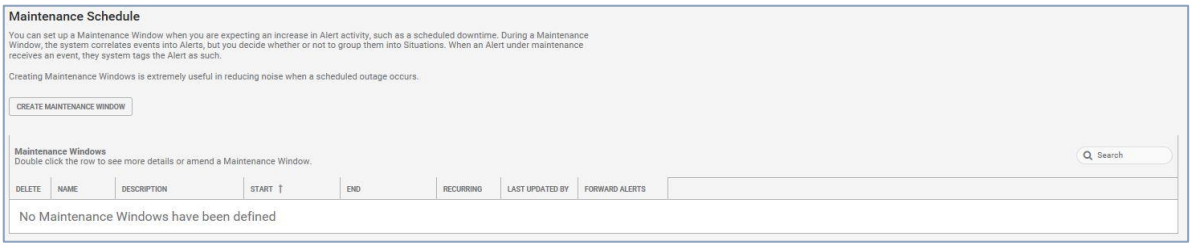
In this example, the filter shows all Alerts which match the 'Anomalyflag' type and have a count of 1:

Quick tip: If you want to create a filter where the owner is empty, enter 'Owned By' = 'Moog'

Schedule Maintenance Downtime

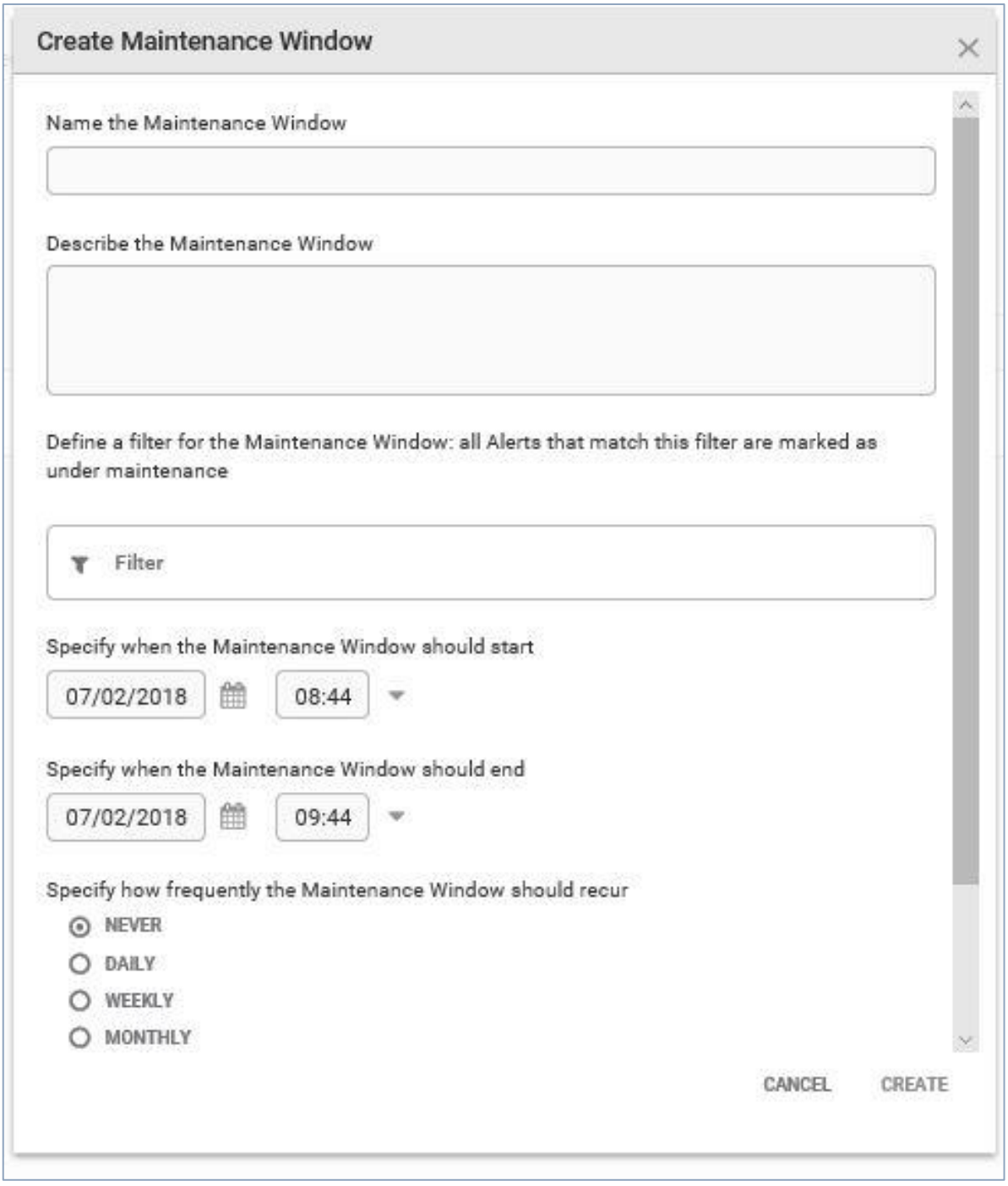
To reduce unnecessary noise, you can define Maintenance Windows for scheduled downtimes (such as during server or software upgrades).

During a maintenance window, Events will continue to be correlated into Alerts and labeled as 'in maintenance' but you can choose not to group them into Situations. If an Alert under a maintenance schedule receives an Event, it will be tagged as such.



Create a Maintenance Window

Click Create Maintenance Window to create a new window:



Field	Input	Description
Name the Maintenance Window	Mandatory String	A text name for the new Maintenance Window
Describe the Maintenance Window	Mandatory String	A description of the new Maintenance Window

Define a filter for the Maintenance Window	-	Defines a filter to target specific Alert or larger group of Alerts
Start date and time	Date/Time	Sets the start time and date of the new Maintenance Window
End date and time	Date/Time	Sets the end time and date of the new Maintenance Window
How frequently the Maintenance Window should recur	Never Daily Weekly Monthly	Selects whether the Maintenance Window will never recur or will recur on a daily, weekly or monthly basis
Allow Situation Membership for Alerts under Maintenance	Boolean	Allows Alerts created during a maintenance schedule to be included in Situations. By default, Alerts under maintenance are omitted from Situations.

Note: Historical, expired and manually deleted windows are not displayed here. It is possible to edit one of the displayed windows by double-clicking it if you are an administrator.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco Trademark

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Cisco Copyright