FORTINET

User Guide

FortiSOAR 7.3.0

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

November, 2022
FortiSOAR 7.3.0 User Guide
00-400-000000-20210106

TABLE OF CONTENTS

Change Log

Date	Change Description
2022-11-04	Initial release of 7.3.0

Overview

FortiSOAR is a centralized hub for all of your security operations. Our platform provides customizable mechanisms for prevention, detection, and response that work across tools in your environment. The integrations here are intended to provide a demonstration of how FortiSOAR can enable your security operations from end-to-end.

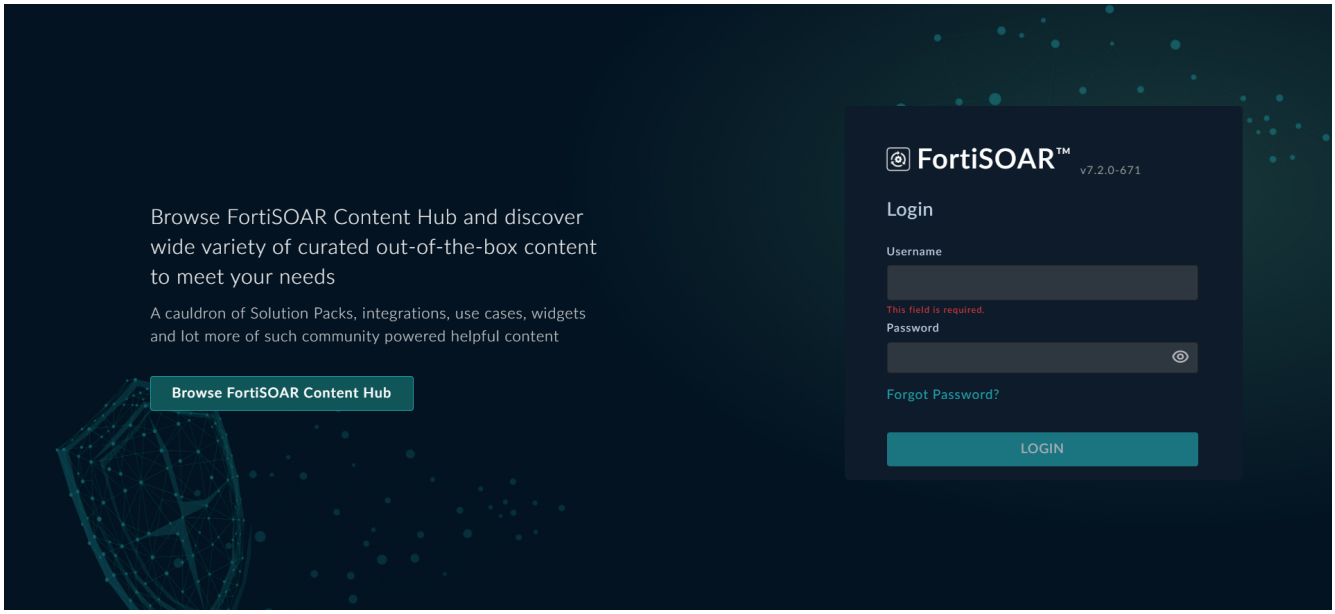
Use the user guide to understand how to use FortiSOAR, including using modules such as Alerts and Incidents, importing data, searching within FortiSOAR, and creating your own custom dashboards and templates.

Logging on to FortiSOAR

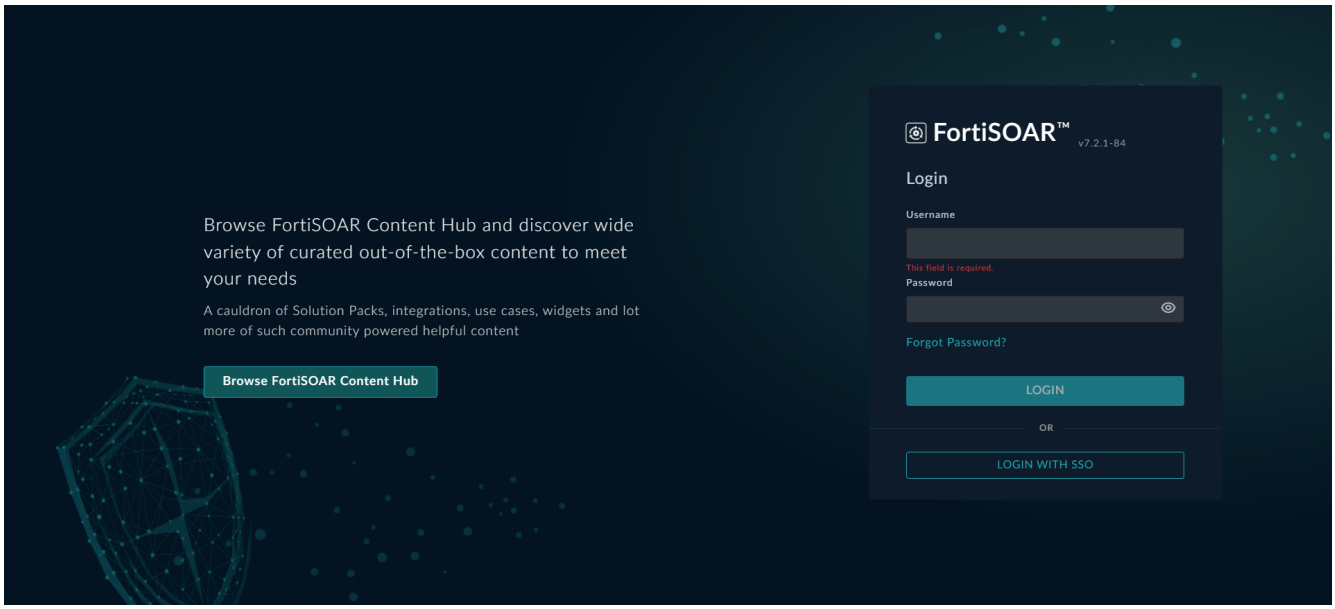
Your administrator will provide you access and credentials to log on to the FortiSOAR application.

You must change the password when you first log on to FortiSOAR, irrespective of the complexity of the password assigned to you, by clicking the **User Profile** icon ( ) and then selecting the **Change Password** option.

Upon accessing the FortiSOAR login screen, enter your login credentials.



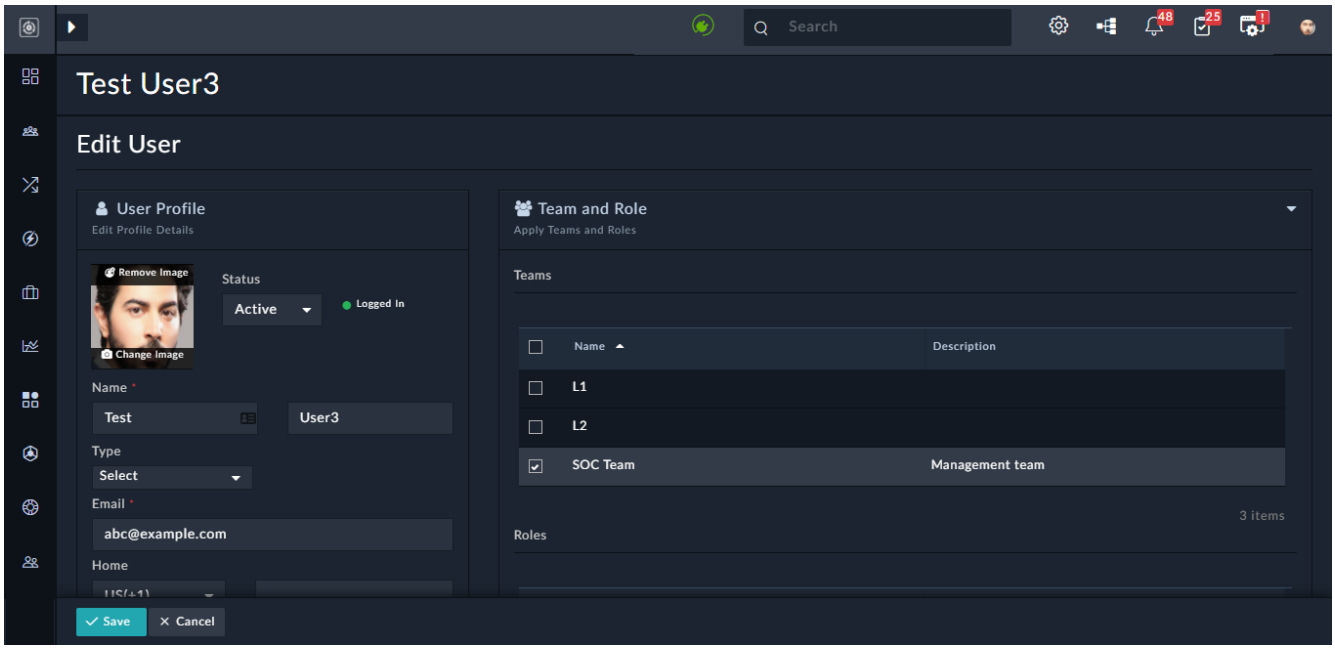
If your organization uses SSO and your administrator has completed the configuration of SSO for FortiSOAR, you can use Single Sign On (SSO) to log on to FortiSOAR. Log on to FortiSOAR using SSO by clicking the **Login with SSO** button that is present on the FortiSOAR login page.



Once you click the **Login with SSO** button, you are redirected to a third-party identity login page, where you must enter your credentials and get yourself authenticated. Once you successfully log on to FortiSOAR, your user profile automatically gets created. Your user profile is created based on the default values, such as your default team and role, configured by your administrator. You can update your profile by editing your user profile.

User Profile

All users of the system have a profile. Once you log on to FortiSOAR, you can access your own profile and can update your information. To access your profile, click the **User Profile** icon ( ) on the top-right bar in FortiSOAR.

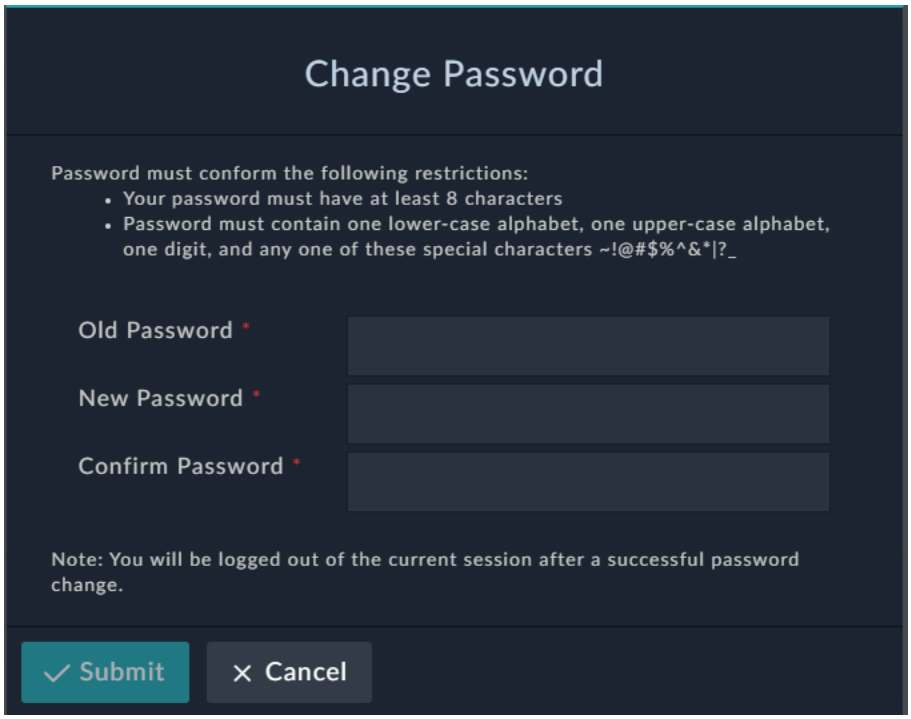


You can view your name, email, username, password, phone numbers, teams and roles to which you are assigned. You can also view your own audit logs, which display a chronological list of all the actions that you have performed across all the modules of FortiSOAR.

The **Username** field is **mandatory** and **case sensitive** and it cannot be changed once it is set.

You can upload your profile picture by clicking **Change Image**, which opens the `Upload a Profile Picture` dialog, where you can drag-and-drop the profile image file, or click the **Import** icon and browse to the image file to import the profile image file to FortiSOAR, and then click **Save Profile Image** to add the profile image. Once the profile image is added, the same can be removed at anytime by clicking the **Remove Image** button that appears on the profile image.

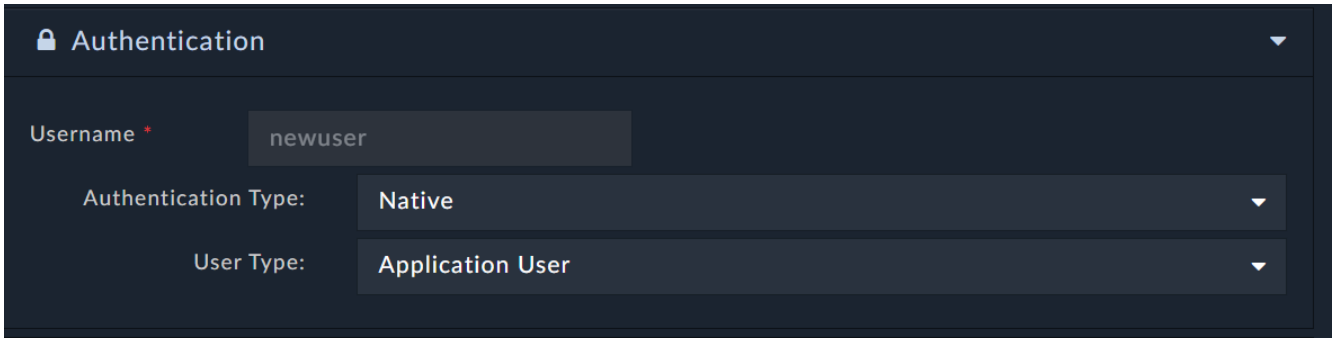
You must change your password when you first log on to FortiSOAR. You can also change your password at any time by clicking the **User Profile** icon and selecting the **Change Password** option. Clicking the **Change Password** option opens the `Change Password` dialog in which you enter your old password in the **Old Password** field, new password in the **New Password** field and re-enter the new password in the **Confirm Password** Field. New passwords that are set must contain at least 8 characters, one lower-case alphabet, one upper-case alphabet, one digit, and any one of the following special characters `~ ! @ # $ % ^ & * | ? _`
Click **Submit** to change your password.



If you face issues with user preferences such as, applying filters on the grid or column formatting within a grid, click the **More Options** icon ( ) and click on the **Reset Columns To Default** option.

Authentication

You can view your user type and username in the **Authentication** section. **Do not change these options**



2-Factor

The **2-Factor** authentication menu displays the current user preference for the 2-factor method. Currently, FortiSOAR supports only TeleSign for 2-Factor authentication. **Do not change this option.**

Notifications

Notification preferences determine how FortiSOAR notifications get consumed by users. **Do not change this option.**

Theme Settings

You can update your FortiSOAR theme using the **Theme Settings** menu on the `Edit User` page. There are currently three theme options, **Dark**, **Light**, and **Space**, with **Space** being the default. Click **Preview Theme** to see the Theme as it would look and save the profile to apply the theme.

History

Use the `History` menu to view your authentication history and your ten most recent authentication attempts and their outcome.

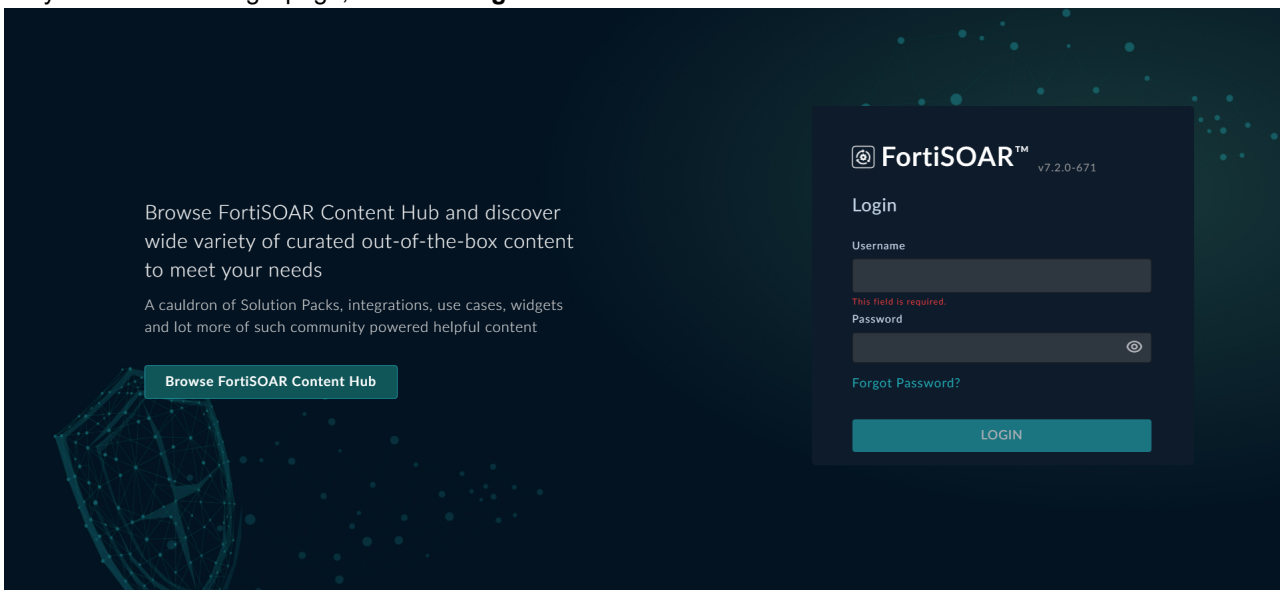
Audit Logs

Use the `User Specific Audit Logs` panel to view a chronological list of all the actions that you have performed across all the modules of FortiSOAR. The audit log also displays users' login success or failures and logout events. The login event includes all three supported login types, which are DB Login, LDAP Login, and SSO Login.

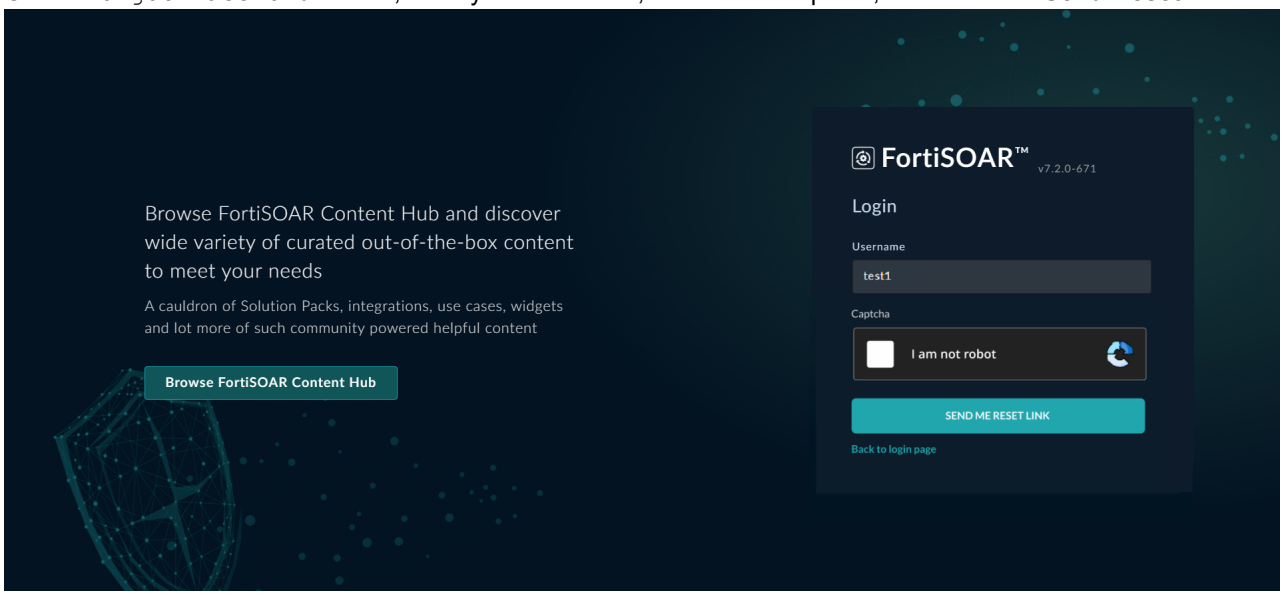
Regenerating your password

In case you forget your FortiSOAR password, use the following procedure to reset or regenerate your password:

1. On your FortiSOAR login page, click the **Forgot Password** link.



2. On the `Forgot Password` screen, enter your username, validate the captcha, and then click **Send Reset Link**.



Once you click **Send Reset Link**, an email is sent to the email address associated with the specified username.

Feature Tour

Working in FortiSOAR

The FortiSOAR interface is based around a common navigation bar on the left side of the application, a global search bar, and filtering within modules. All navigation is built on top of the authorization you are provided according to your RBAC permissions.

For instance, if you have Read privileges to the Incidents module, you will be able to view all Incidents that are within your Ownership Sphere.

Navigation

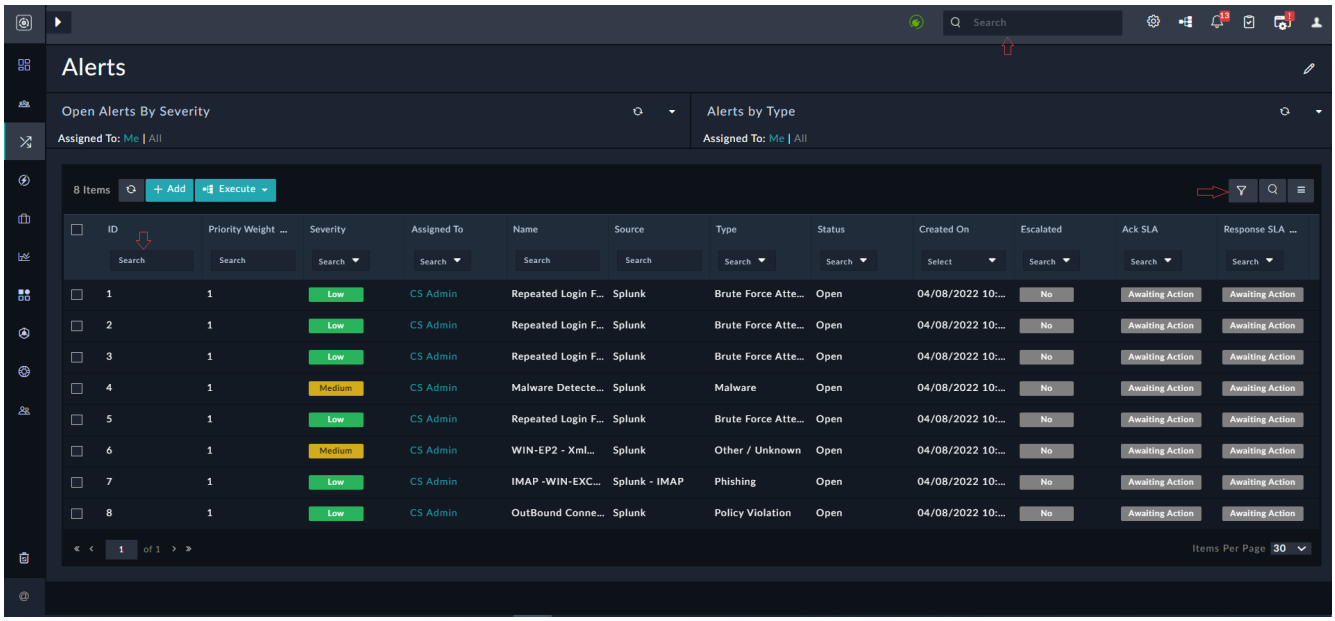
The navigation bar provides quick access to the Components and Modules you are authorized to view.

At the highest level, the navigation bar provides Components, which open when you click on the component to reveal a module menu with all accessible modules. For example, when you click on the Incident Response, its module menu reveals the Alerts, Incidents, Tasks, Indicators, War Rooms modules. Module links go to the Module's record listing pages.

Searching

There are three methods of searching within FortiSOAR.

Search Method	Description
Global Search	The Global Search bar at the top of the screen allows you to search for one or more keywords across all records within the system
Table Filter	The Table Filter method allows you to search the name field quickly, such as Incidents, within the context of an individual data column on the table
Column Filter	The Column Filter method within tables allows you to search specific records from a module, such as Incidents, within the context of an individual data column on the table



Global Search

The Global Search mechanism leverages an Elastic Search database to achieve rapid, efficient searches across the entirety of the record system. All the record data is stored in Elastic Search, including from file attachments, and made searchable.

The Global Search mechanism respects authorization from users to return search results, meaning users without Read permissions on a Module would not see results returned from that module even if they were found during the search.

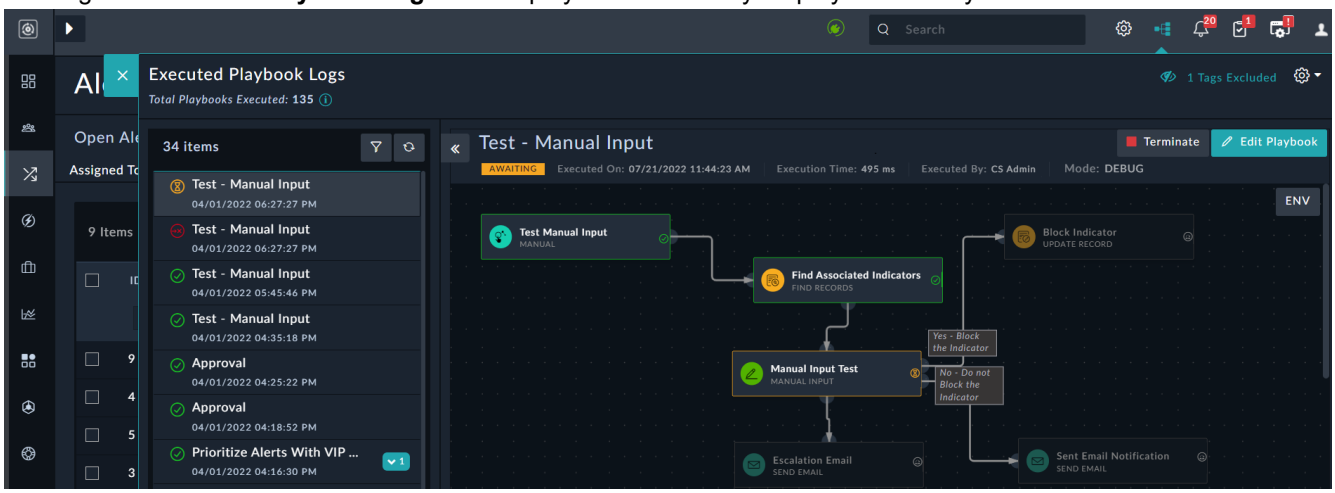
Global Search result findings may be exported in the results table to CSV and then stored for future reference if desired.

Viewing Settings and Executed Playbook Logs

The **Settings** and the **Executed Playbook Logs** icons appear on the top-right corner of your FortiSOAR screen.

Clicking the **Settings** icon displays the various administrative settings used to configure and customize FortiSOAR. Your administrator would already have configured these options, therefore you should not edit these options.

Clicking the **Executed Playbook Logs** icon displays the results of your playbooks that you have executed.

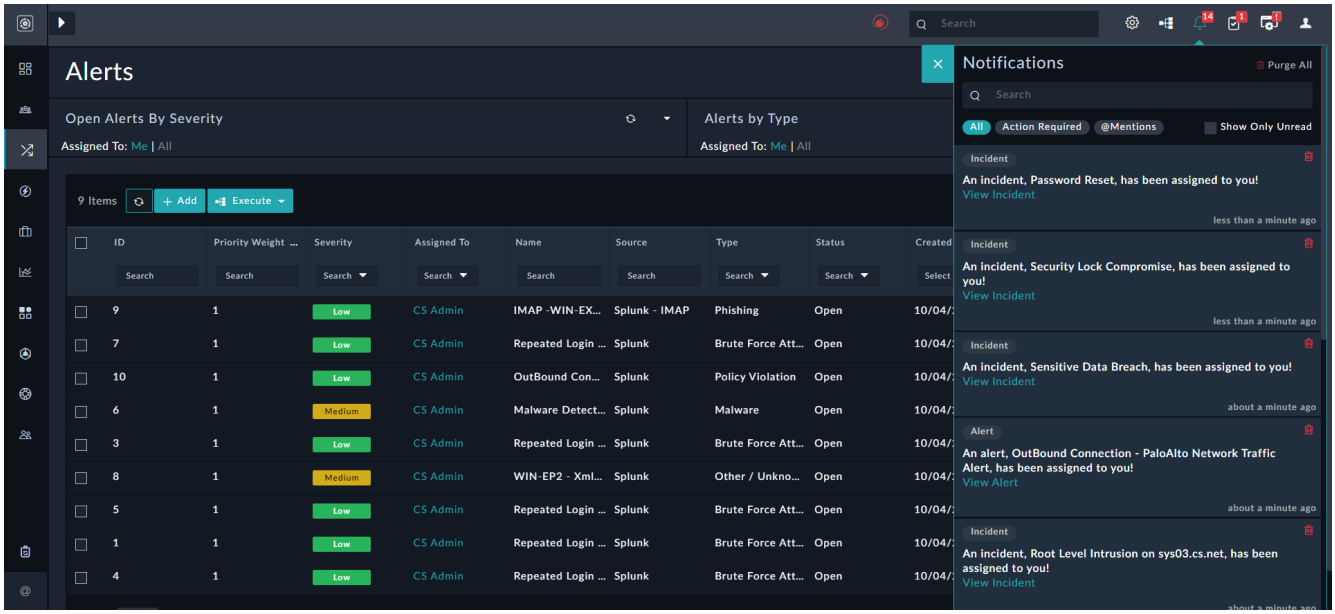


You can also use the executed playbook logs to debug your playbooks. For more information on all the **Executed Playbook Logs**, see the *Debugging and Optimizing Playbooks chapter* in the "Playbooks Guide."

Viewing Notifications and Pending Tasks

The **Notifications** and the **Pending Tasks** icons appear on the top-right corner of your FortiSOAR screen.

The **Notifications** icon contains a number in red color that mentions the number of unread notifications. Notifications include informative information, such as failure of workflows, assignment of user on created and updated alerts, incidents, tasks, etc., and actions that are pending for some user action. Clicking the **Notifications** icon displays the 'Notifications Panel':



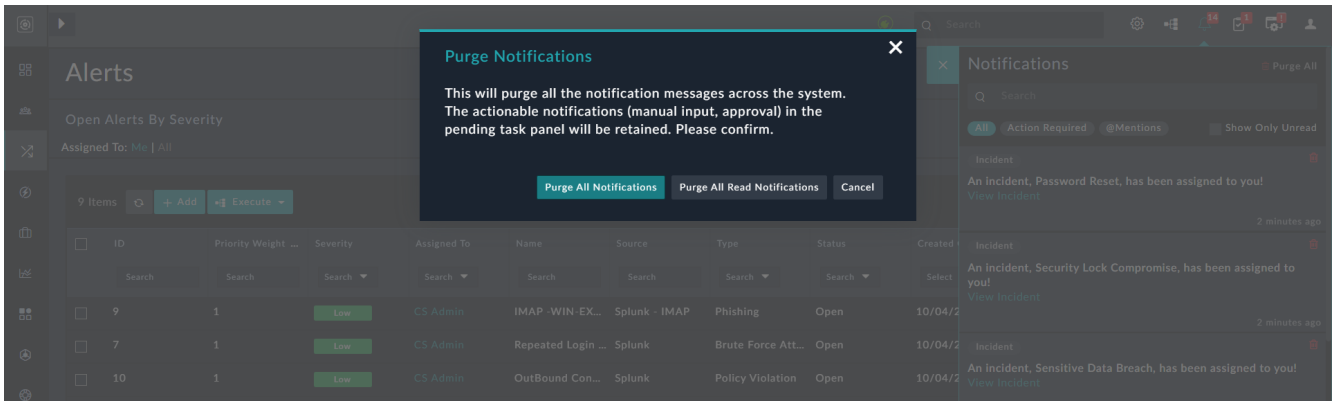
In the Notification Panel, you can use the **Search** box to search for a particular notification, or filter notifications as follows:

- Click **All** to display all the notifications.
- Click **Action Required** to display only those notifications such as approvals, that are pending for some user action.

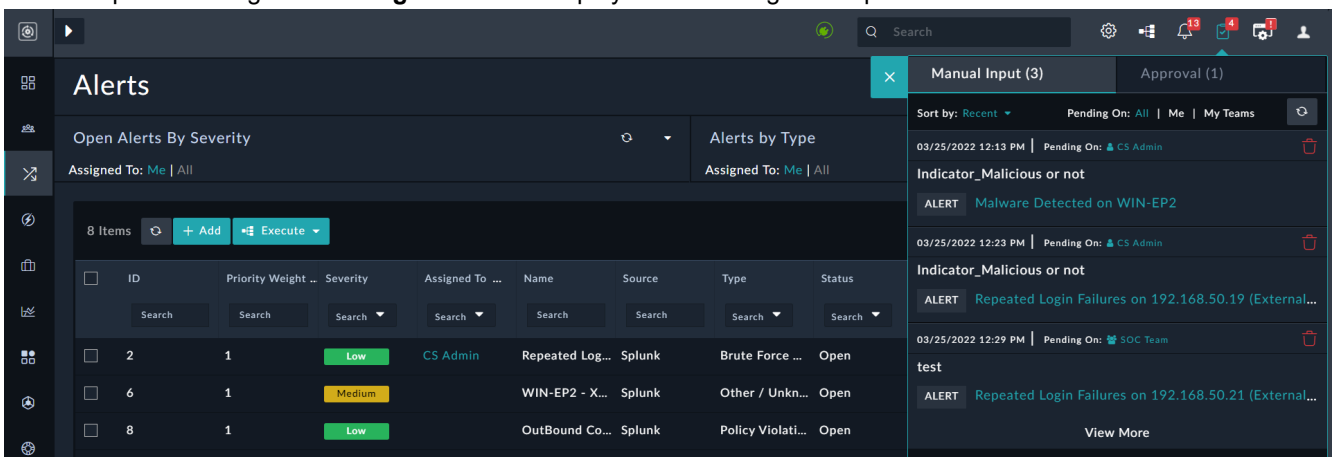
- Click **@Mentions** to display a list of comments in which you have been tagged.
- Select **Show only Unread** to display only those notifications that have not been read. Notifications get read once you click on them opening their corresponding records.

You can also delete notifications from the Notifications Panel or Pending Tasks panel, once you have read them by clicking the **Delete** icon. However, you can delete only those notifications that are assigned to you and not those that are assigned to a team, or any other user, or system (global) notifications such as workflow failures.

Users with a minimum of `Update` permissions on the `Security` Module can also click the **Purge All** icon to display the `Purge Notifications` dialog. Click **Purge All Notifications** to delete all notifications or click **Purge All Read Notifications** to delete all read notifications:



The **Pending Tasks** icon contains a number in red color that mentions the number of pending tasks, both approvals and manual inputs. Clicking the **Pending Tasks** icon displays the 'Pending Tasks' panel:



For more information on the pending tasks panel, manual inputs, and approvals, see the *Triggers and Steps* chapter in the "Playbooks Guide."

Adding Records

Add records to a module using the **Add** button present on top of the grid that lists module records based on RBAC permissions.

Editing

Record editing within the record detail view can be accomplished via Inline editing, which allows for quick changes to fields and requires confirmation for all updates.

Additionally, in the detail view of every record is an Edit button on the top right in the breadcrumb bar. This gives you access to a bulk editing interface for all fields that are allowed within the authorization model of your user.

Modules & Models

One of the primary features of FortiSOAR is the ability to provide a clean interface with customized data models optimized for tracking day-to-day security data, such as Alerts.

FortiSOAR unifies the data streams to provide a centralized management interface for tracking. This means Incidents may spend their entire lifecycle rolled up inside of FortiSOAR and working across other related data being tracked, such as Tasks or Assets.

By providing a single place to view and organize security data, much of the overhead and manual effort of going to disparate security tools is significantly reduced. Users are enabled to focus on analyzing the data, not collecting the data.

Models within FortiSOAR are easily customizable according to the needs of an organization via API.

Many modules may be accessed through relationships but might not be directly displayed in the interface navigation. Please see the detailed list of modules provided for more description.

Modules provide access to individual data models within the FortiSOAR database, such as Incidents.

All Module fields are editable and can be customized or extended as needed via API. Models are based on a standard JSON schema.

We recommend you do not delete the core module fields that are included in your instance without consulting FortiSOAR Support. Deletion of core module fields may result in upgrade issues at a future date.

Not all modules will be exposed in the navigation. Some of them are only accessible within the context of other modules. You can modify the default navigation if you desire to add new modules at any time.

From release 7.2.0 onwards, the Incident Response modules have been removed from the FortiSOAR platform and moved to the SOAR Framework Solution Pack (SP). The SOAR Framework SP is the **Foundational** Solution Pack that creates the framework, including modules, dashboard, roles, widgets, etc., required for effective day-to-day operations of any SOC. As the Incident Response modules, i.e., Alerts, Incidents, Indicators, and War Rooms are not part of the FortiSOAR platform, it becomes essential for users to install the SOAR Framework SP to optimally use and experience FortiSOAR's incident response. For detailed information about the SOAR Framework SP, see the SOAR Framework SP documentation.
From release 7.2.0 onwards, the SOAR Framework Solution Pack is installed by default with the fresh installations of FortiSOAR.

A brief about the incident response modules follows:

- **Alerts**: Alerts generally represent records that contain a notice of suspicious activity typically triggered in a SIEM.
- **Incidents**: Incidents generally represent records of an actual breach of security.
- **Indicators**: Indicators generally represent records that contain simple identifiable information regarding a threat such as an IP or URL.
- **Tasks**: Tasks represent a discrete action taken by either an individual or automated response. Tasks might link to outside systems, such as ticketing systems, to track specific actions beyond that of your SOC team.
- **War Rooms**: War Rooms in FortiSOAR is a collaborative space that enables SOC teams to mitigate a critical cyber threat scenario or campaign.

NOTE: Playbooks and Reporting do not have any associated Module definition.

Linking

Individual records are easily linked in the FortiSOAR interface to provide context and make it simple to track relationships. Linking may be contextual or operational.

Operational Links

For instance, an Incident may have multiple Tasks automatically generated based on the type of Incident. These Tasks stay linked to the Incident throughout the lifecycle and allow for an easy operational overview of where an Incident is beyond tracking just the Incident phase.

Contextual Links

In contextual situations, linking provides the ability to relate data records together and increase velocity during Preparation and Analysis activities.

For instance, Alerts link to Artifacts which then may be automatically linked to Assets. Artifacts within an Alert from your SIEM tool may contain information that helps identify and link Asset records making it simple for an Analyst to understand the potential scope of an Alert. FortiSOAR can find identifiable Asset information and then use that to search one or more Asset resources, such as a CMDB, local DNS, or DHCP records.

Linking is accomplished within the record detail view.

Automation

FortiSOAR provides a powerful Workflow Engine where machine-to-machine (M2M) automation, policy enforcement, data enrichment, and notifications, are all available within a simple drag-and-drop interface.

Security Playbooks may be digitized and automated via Workflows. A standard library of Playbooks may be added at the time of installation to provide a quick level of defaults that may then be customized to match the specific use cases of your environment.

Access Control

FortiSOAR utilizes a robust security model with Role Based Access Control (RBAC) as well as team ownership.

RBAC provides Create, Read, Update, and Delete (CRUD), permissions on individual models within the platform. Roles are created by granting CRUD privileges on models within the available models' list.

Teams provide for row-level ownership of records. Teams have an explicit hierarchy model to allow for complex relationships. The Teams you are a member of and their relationships combined define an Ownership Sphere. An Ownership Sphere is the full set of records on which you can exercise your permissions.

Live UI - Web Sockets

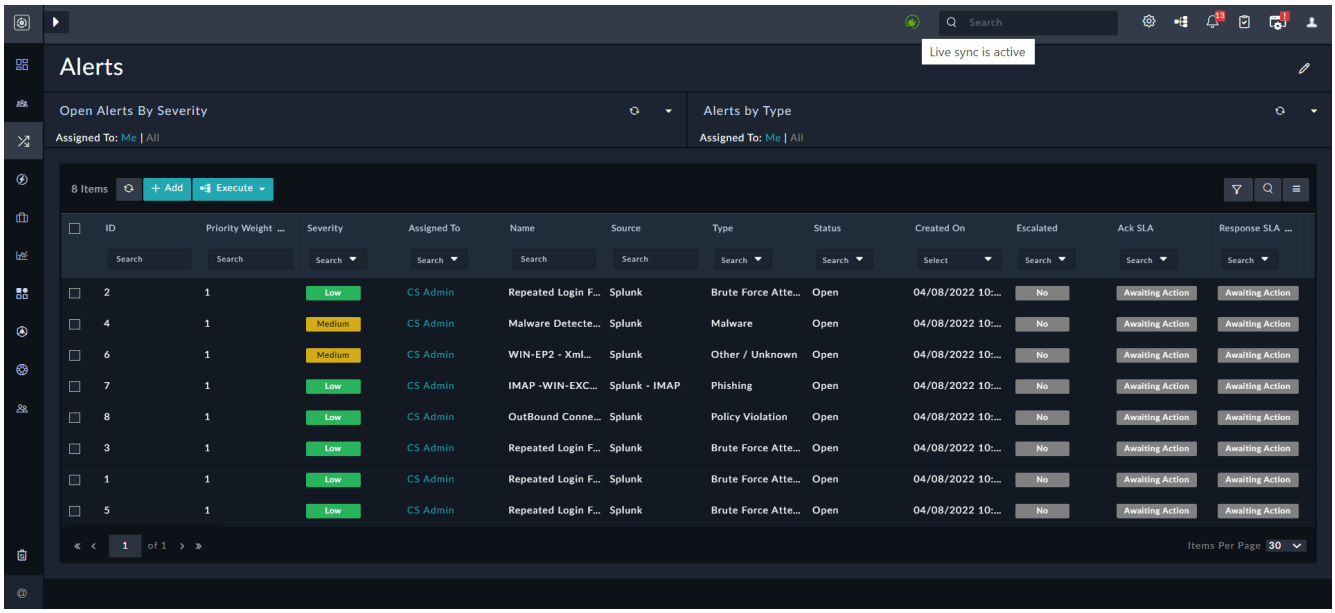
Live UI provides users with many benefits, such as immediate refreshing of records in case of an update by users or workflow (playbook or API), without the users having to refresh the views to see the updates manually.

When a user or workflow (playbook or API) updates any record that is being displayed in the following UI components:

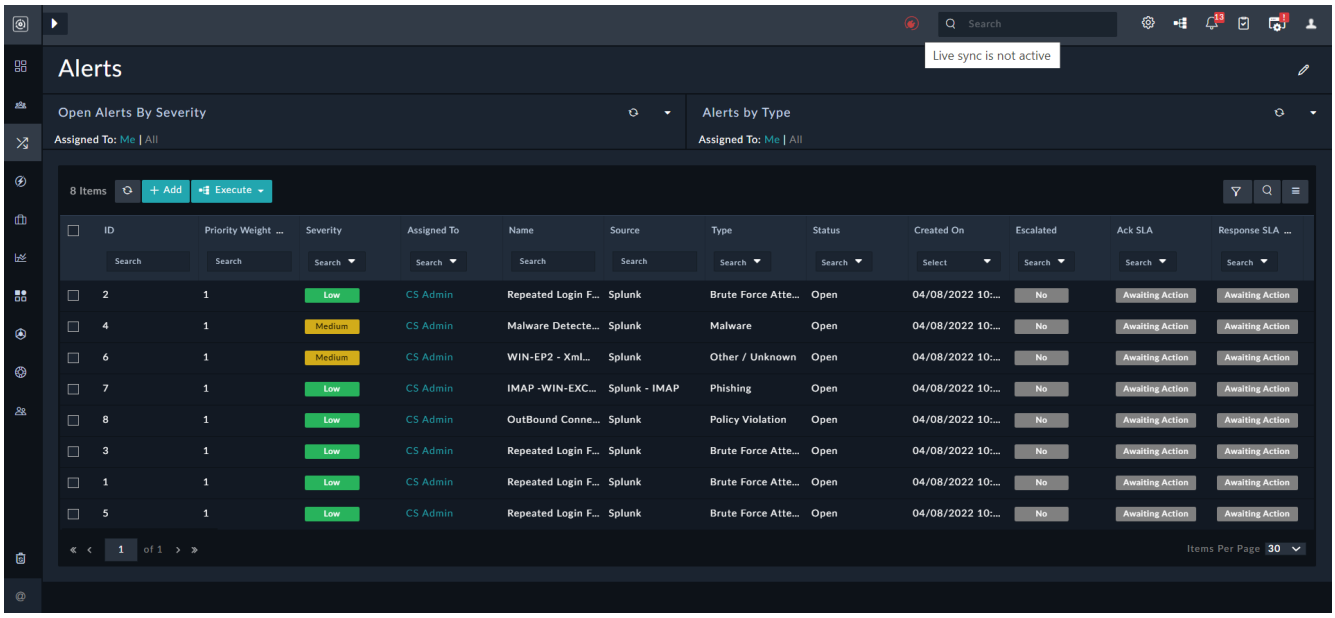
- Grid and Relationship grid (view panel)
- Details View Panel
- Collaboration Panel: Comments or Attachments
- Approvals in notification panel

Then these changes are immediately reflected to other users who are active on that FortiSOAR instance.

If your FortiSOAR instance is connected to the web sockets server then a green connection icon is displayed at the top-middle of the FortiSOAR UI as shown in the following image:



If your FortiSOAR instance cannot connect to the web sockets server, due to connectivity or any other issues, then a red connection icon and a message such as "Live Sync is not active...." is displayed at the top-middle of the FortiSOAR UI as shown in the following image:



In such a case FortiSOAR also displays a message to the users asking users to use manual refresh to update the views.

Searches and Filters

Search in FortiSOAR is based upon an included Elasticsearch database.

FortiSOAR provides you search at the following levels:

- **Global Search**: Searches for the keywords you have specified across all records in FortiSOAR.
- **List Search**: Searches for the keywords you have specified in all records in a specific module.

Filters: You can filter records belonging to a module and also save filters for future use.

You cannot search or filter encrypted fields.

Global Search

Keyword Search

Global Search searches the titles, descriptions, or tags across all records in FortiSOAR. You can also search for the name of the file and any other details that are associated with the file attachment. The file names should be descriptive to ensure that the file can be found through keyword searches related to the file content.

From version 7.0.2 onwards, you can perform an 'Exact Text Search' so that the search does not split up text with spaces, @, etc and the search results contain the complete text.

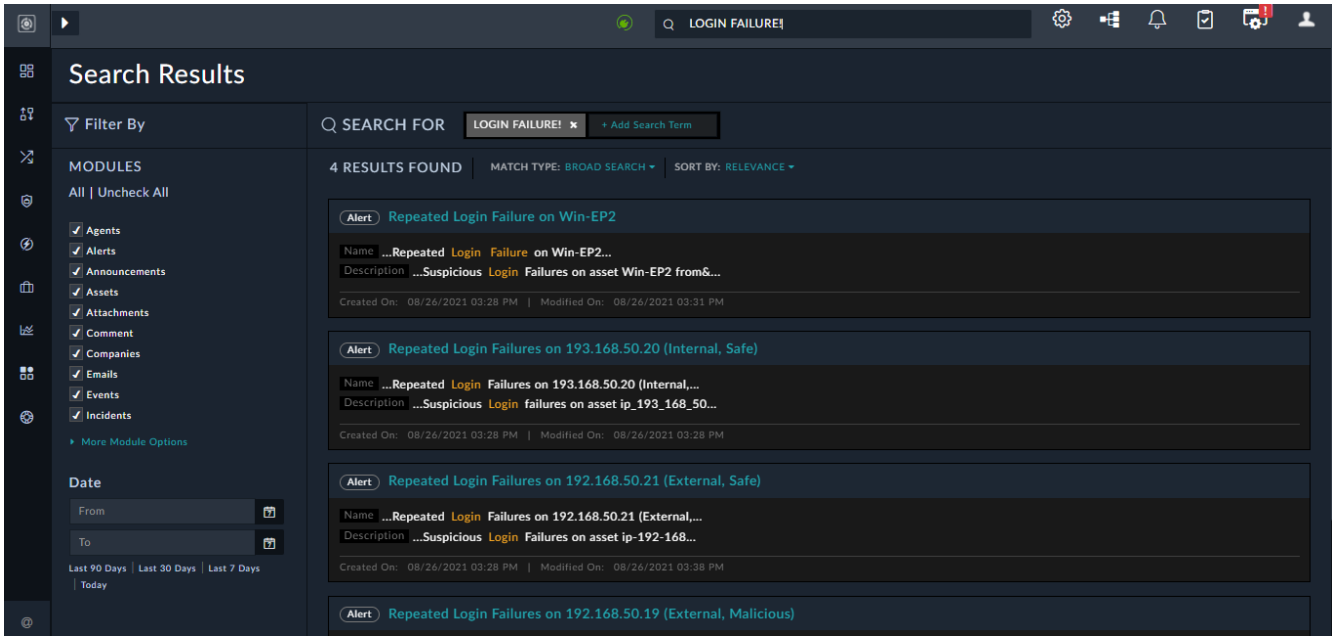
The **Search** bar at the top of the FortiSOAR interface allows for fast access to the Global Search feature. Entering any keyword in the **Search** bar and hitting `Enter` begins the search for the keyword.

Using **Global Search**, you can search for playbooks, templates, etc., based on tags, name, and description. You can add special characters and spaces in tags; however, the following special characters are not supported in tags: `'`, `,` , `"`, `#`, `?`, and `/`. For example, if you have added `sample` as a tag to the playbook and you type `sample` in Global Search, the search results will contain the playbook with the `sample` tag. Also, note that records that are in the recycle bin will not be visible in the Global Search results. For more information on the recycle bin, see the *Recycle Bin* chapter in the "Administration Guide."

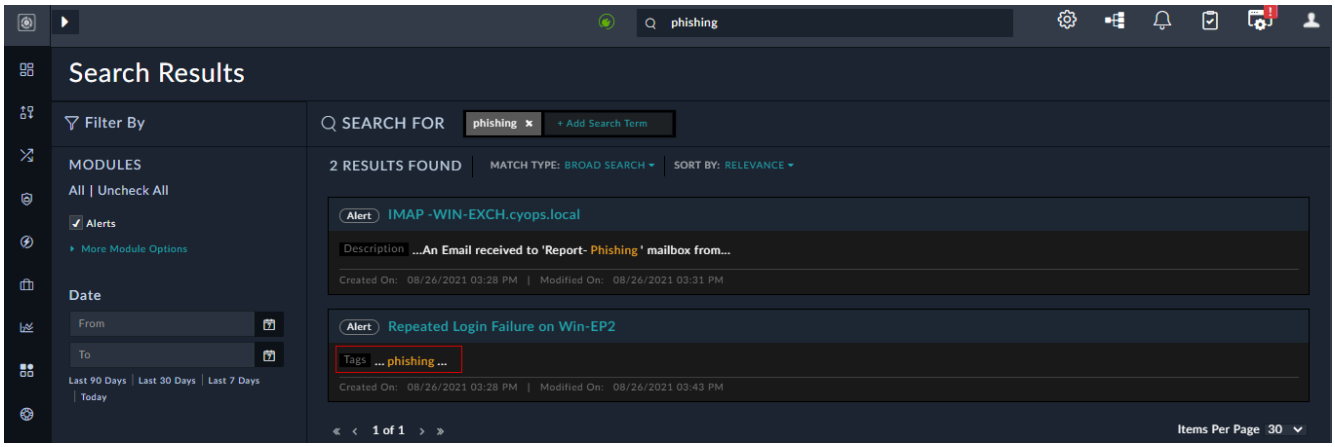
If you want to search for tags in custom modules based on Tags, then you must ensure that you assign a minimum of Read permission to the custom module in a role(s) that has permissions on the Appliances module. This is required since custom modules require to be given permission in the playbook appliance for the record to get indexed and be searchable.

Term Matching

The Global Search function accessible from the **Search** bar uses the full-text match query function within Elasticsearch. This passes the search string through the standard analyzer, stripping any extra characters to the root term. For instance, the term `login failure` would be searched the same way as the term `"Login Failure!"`, for text fields such as description or name as shown in the following image:



In the case of tags, search results will be displayed only in case of an exact match, without case sensitivity, for example, if you have added `phishing` as a tag and you search for `phish`, there will be no search results. However, if you search for `Phishing`, you will get a search result:



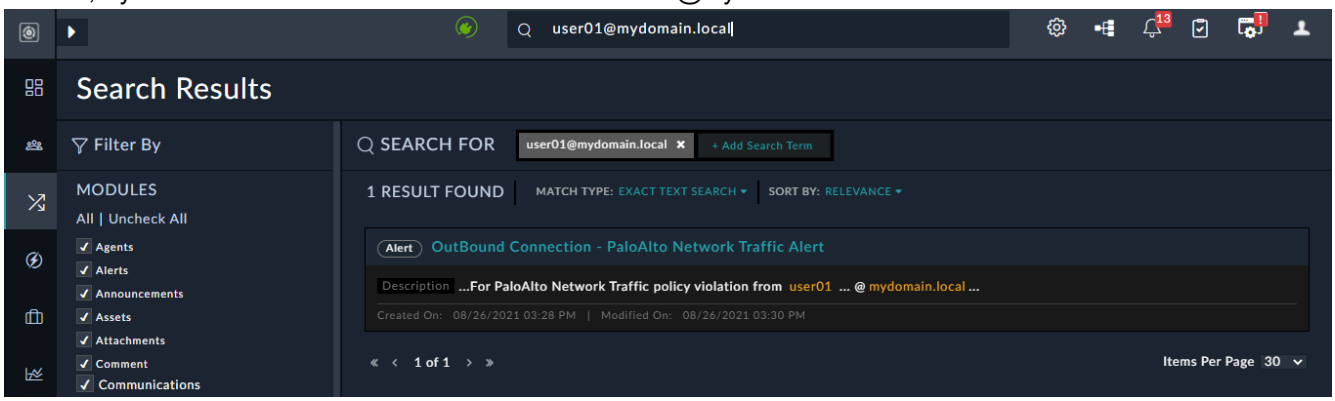
You can search for multiple terms using the search function by adding a term in the **Add Search Term** field. If multiple terms are entered, they are searched using the `AND` operation. FortiSOAR displays the results only when the results contain all the terms that you have entered.

Global Search also works for stop words such as dots, @, etc. For example, if you are searching for the text google.com, then the results are displayed for both `com` and `google`. If however, you want to search for the complete 'google.com' text, you can select the match type as **Exact Text Search**.

Search Results

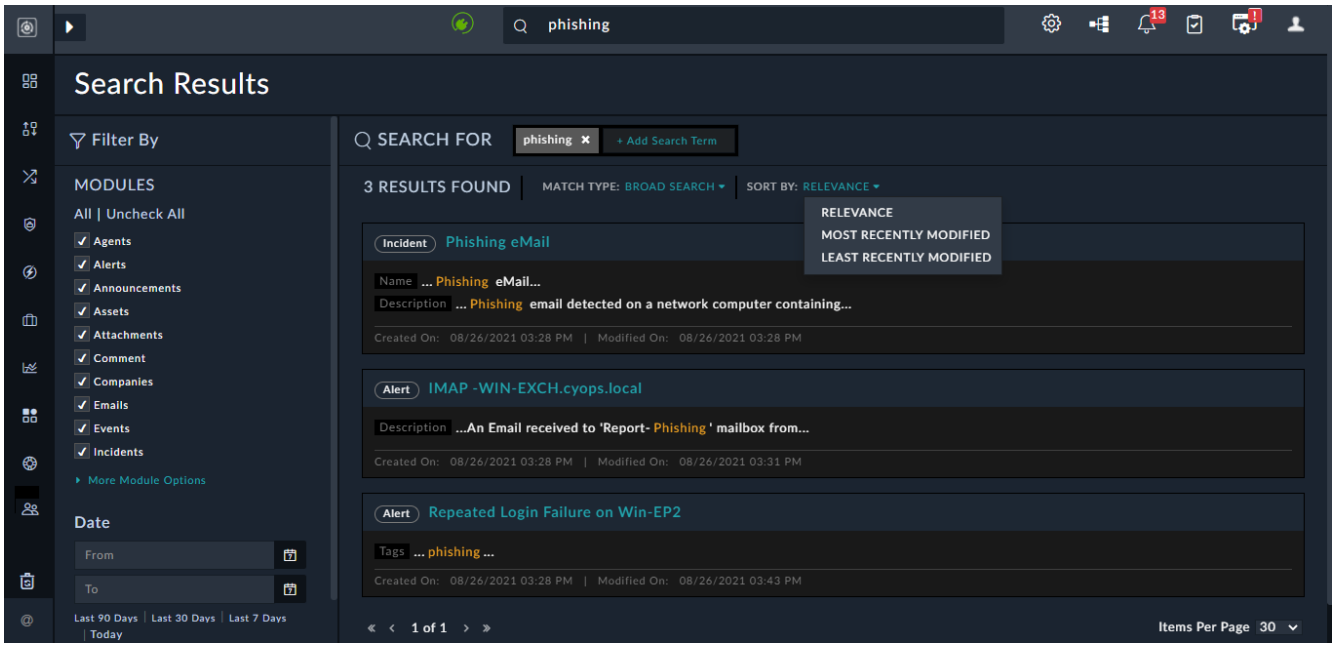
Search results are returned as a listing with a summary of the record metadata that provides information such as, the record name, the record type (the model of the record, such as an Incident), the created date and the last modified date of the record, and a contextual preview of the search term or terms position within the resulting record text.

You can set the Match Type as 'Broad Search' or 'Exact Text Search'. An exact text search does not split up text with spaces, @, etc and the search results contain the complete text. For example, set the match type as **Exact Text Search**, if you want to search for records that contain 'user01@mydomain.local'.



However, if you want to search records of that contain any mention of 'user01', then you can set the match type as **Broad Search**.

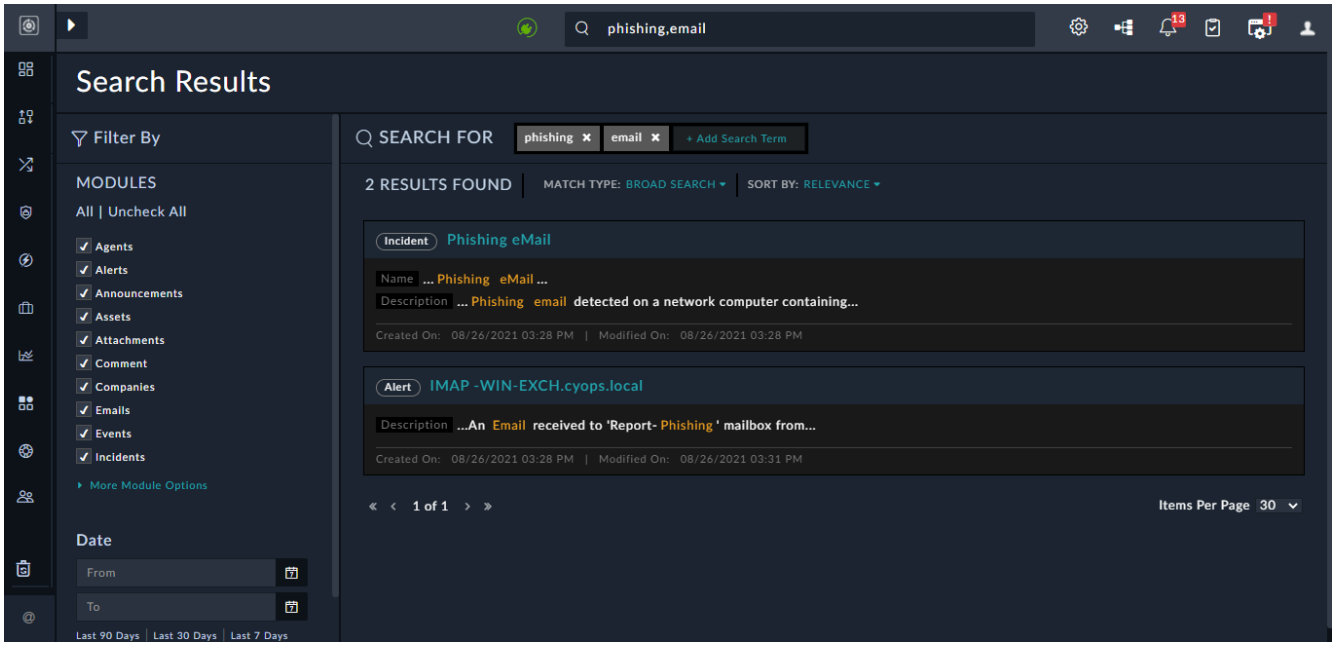
You can sort the search result by **Relevance**, which is based on the number of instances of the keyword within the record body. You can also sort the results by when the record was modified, the **Most Recently Modified** record or the **Least Recently Modified** record. Clicking on a search result displays the record details.



Filter By Pane

Use the **Filter By** pane to perform additional filtering of the results returned after a Global Search has been performed. When using the Filter bar, the term being searched on is applied directly to the already returned search results. This *does not* repeat the full-text match query from the Global Search function. This feature enables you to filter out a larger batch of returned results without repeating the search of the entire database.

For example, as shown in the previous image we had searched for the keyword `phishing` using Global Search, and the search result had returned 3 results. Now we can perform additional filtering on the search results by adding an additional keyword, `email`. The search records are filtered using the `AND` operator, and then the search result displays 2 search results as shown in the following image:



The contextual preview of the term context from the original Global Search function is not updated with applied filters. The preview remains the same, but the records returned in the table are filtered according to the `AND` combination of terms as displayed above in the table.

Filtering Results

You can perform additional filtering in the `Filter By` pane on the search results based on the `Module` and `Date` of the records. All modules are filterable. The date search uses the `Created On date` field to filter the records based on the period you have specified. You can either specify the From and To dates, or select relative dates, such as Last 90 Days, Last 7 days, Today, etc. These additional filters refine the returned search results to the applied scope.

Authorization

Global Search respects authorization permissions based on the context of the user who is performing the search. This means that records not owned by the user's teams, any child or sibling teams, or not within the user's role permissions scope, are not displayed within the results.

Searching Record Contents

All records, such as Incidents, Alerts, and Assets, are included in the Elasticsearch database in addition to Attachments. The record contents do not store field labels, Picklist values, or model information. This is so that the search results do not contain results based on the field label values or terms in the model information, which would lead to meaningless results. For instance, if you perform a Global Search for the keyword **Source**, the Global Search will not return any result even though in an Alert record, the term `Source`, represents a field label in the record. Similarly, `Brute Force Attempt` might be set as a picklist value of the `Type` field in an Alert record, but the Global Search will not return any matches for `Brute Force Attempt` even if records existed with that picklist value. However, you could search for the same using tags, if you have added tags to the record. For example, if you have added a tag BruteForceAttempt or BFA in the record, then you can search for that record using `BFA`.

FortiSOAR essentially searches the record content, i.e., text saved into the field values, such as the Name, or Description and also searches for tag values.

List Search

Keyword Search

List Search searches for data or keywords across a module in FortiSOAR. The search also includes file attachments if they are part of any record within that module.

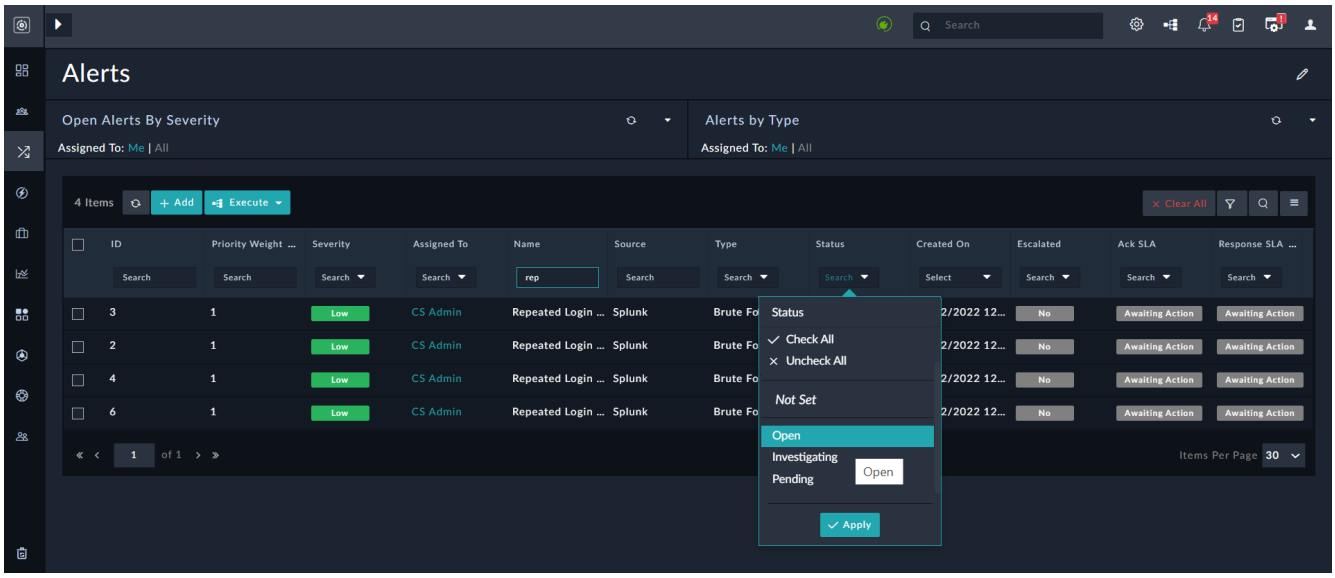
For list search, use the **Search** bar at the top of the record list in a particular module in FortiSOAR. Type any keyword in the **Search** bar and hit `Enter` to begin the search for the keyword.

Term Matching, Authorization, etc., in 'List Search' works the same way as in 'Global Search.'

Filter Search

Searches for keywords in the search criteria row underneath the column header in the list (grid) view of a module. You can either specify the keyword or select an option from the picklist or lookup fields.

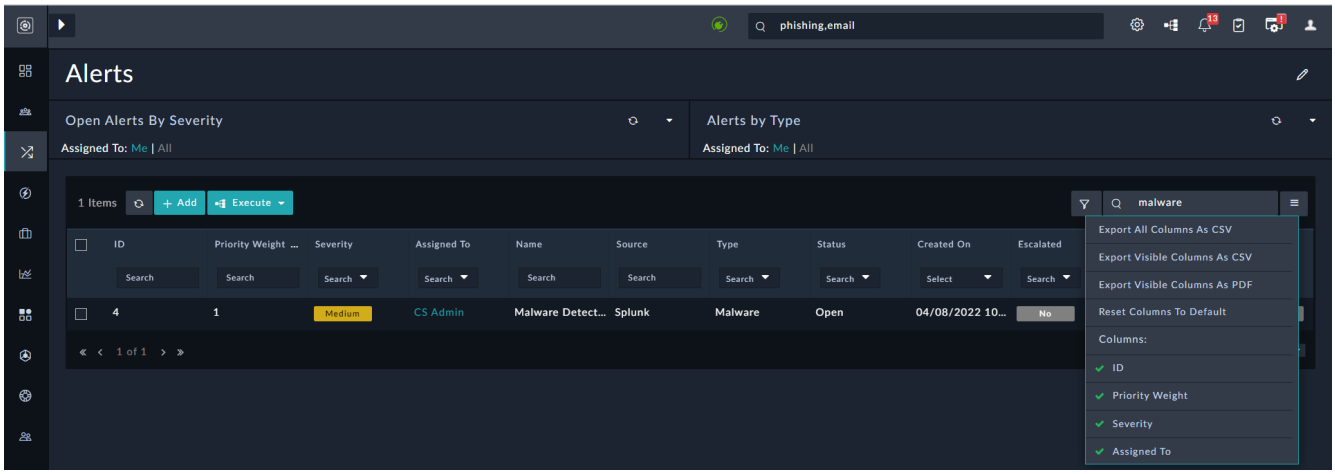
For example, to search for alerts that have 'repeated' in their name and whose status is set as 'Open', enter `rep` in the name search criteria row underneath the column header and select **Open** from the 'Status' picklist:



From release 7.2.1 onwards, a new option **Not Set** is added so that you can filter data (picklist or lookup fields) that has empty (not set) values in a grid. For example, to search for alerts whose 'Status' or 'Type' is not set.

Search Results

Search results are returned in a tabular format as shown in the following image:



The above image displays the results of a search performed in the `Alerts` module, with the keywords **malware**. The search results are displayed in a tabular form, and you can use the **Menu** button to specify the visible columns in the table by selecting or deselecting the columns from the **Columns** list. You can also choose to export the table results to a `.csv` or a `.pdf` file. You can download the search result and store the results for future reference, potentially even as an attachment within FortiSOAR to a particular record.

FortiSOAR Search Errors

FortiSOAR might display an `Internal Server Error` or any of the following errors when you are performing a search operation in FortiSOAR:

- `Search indexing is in progress. Partial results are returned.`
- `Search indexing has stopped. You must manually rerun indexing (see product documentation for instructions) or raise support ticket for the same.`
- `We are sorry, but the server encountered an error while handling your search request. Please contact your administrator for assistance.`

For troubleshooting any errors with FortiSOAR Search, please contact your administrator.

Filtering Records

You can filter records on the listing view by typing the filter term, tag, or selecting the option on which you want to filter records based on the column headers. You can also specify complex conditional filters on the records in the module listing page using the 'Advanced Filter'.

Users can quickly and easily switch between saved filters since filters are directly exposed on the grid, making it easy for you to select and apply available saved filters without having to open the filter editing mode. In the filter editing mode, you can easily view and modify the filter definitions of a saved filter, without having to save that particular filter (you can save the modified filter if you want). You can also easily clear all or a particular filter applied on the grid.

To filter records, you can use two types of filters:

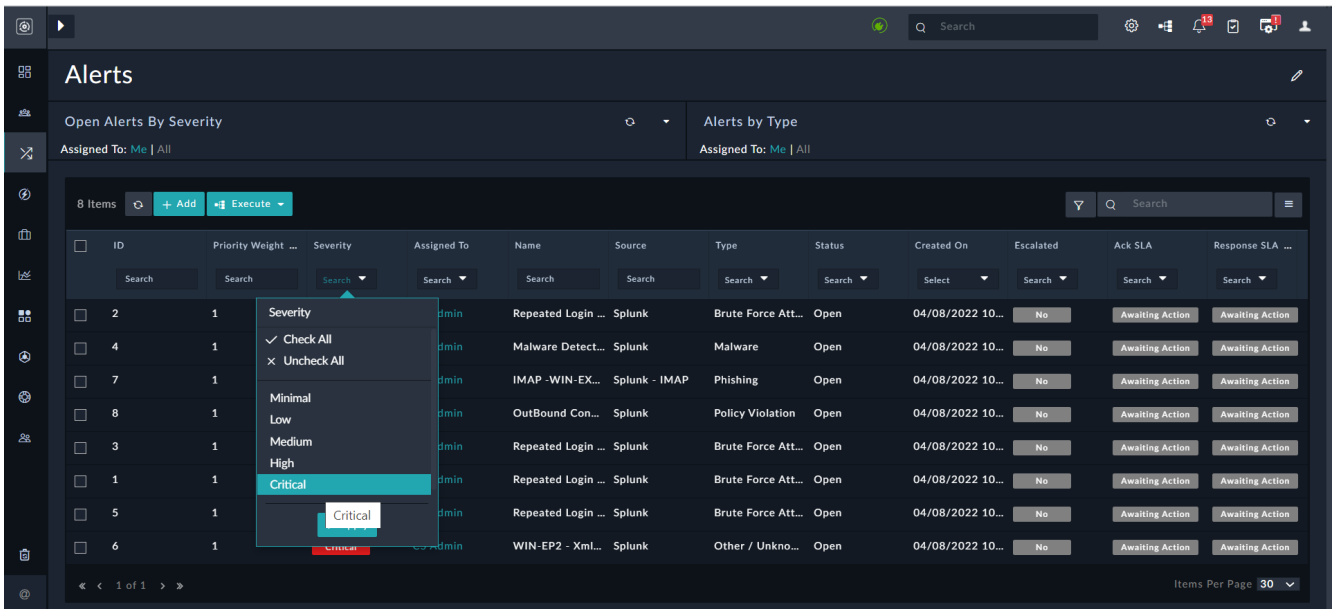
- Simple Filters: Used for filtering of records using a combination of columns.
- Advanced Filters: Used for complex sorting and filtering of records.

Simple Filters

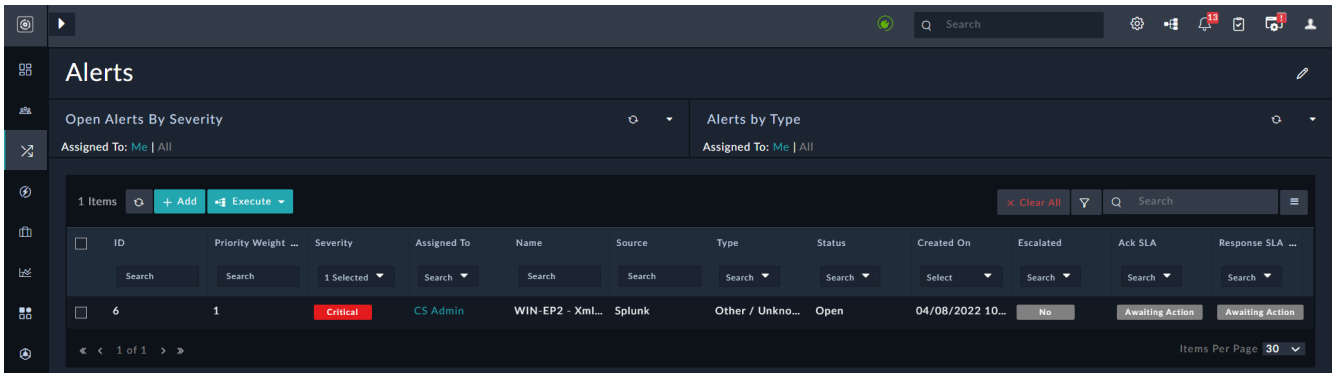
You can use simple filters on the module records grid to filter records based on a combination of columns.

The following example explains how to filter alert records based on Severity, i.e., it only displays records whose Severity is set to Critical. In this example, you are setting a filter criterion from the UI, i.e., selecting a column (field) based on which you are filtering records.

Open the **Incidents Response** > **Alerts**. From the `Severity` column select **Critical** and click **Apply**.

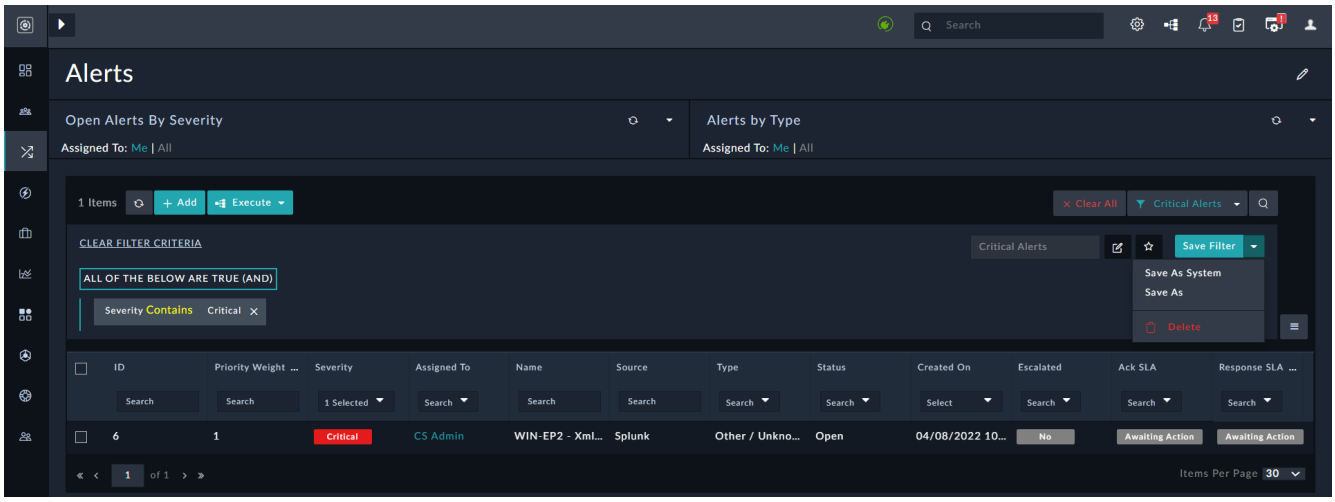


Once you click **Critical** as shown in the above image and click **Apply**, a filter is set on the `Severity` column, and the value of the filter is set to **Critical**. Therefore, based on the set filter criterion, only records whose `Severity is Critical` are displayed in the list of records as shown in the following image:



To clear all the filters applied on the grid, click **Clear All**.

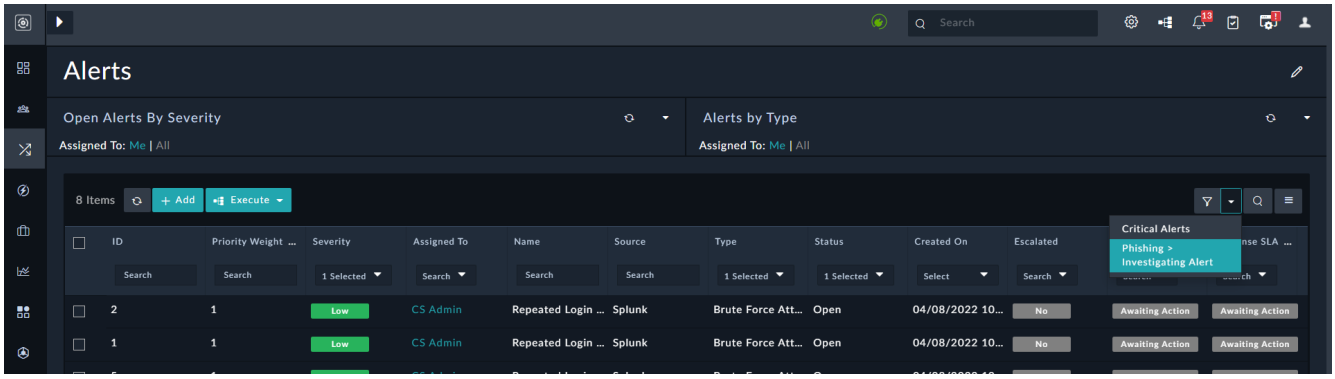
To edit a filter, click the **Filter** icon to see the filter criteria. You can save the filter for future use by clicking the **Save Filter** button. When you click the **Save Filter** button, the `Save New Filter` dialog is displayed. In this dialog, type the name of the filter in the **Name** field and click **Save**. For example, type the filter name as **Critical Alerts** and click **Save**. If you are an administrator, then you can also save a filter as a *System Filter* by clicking **Save Filter** > **Save As System**. System Filters are displayed to all users of the system:



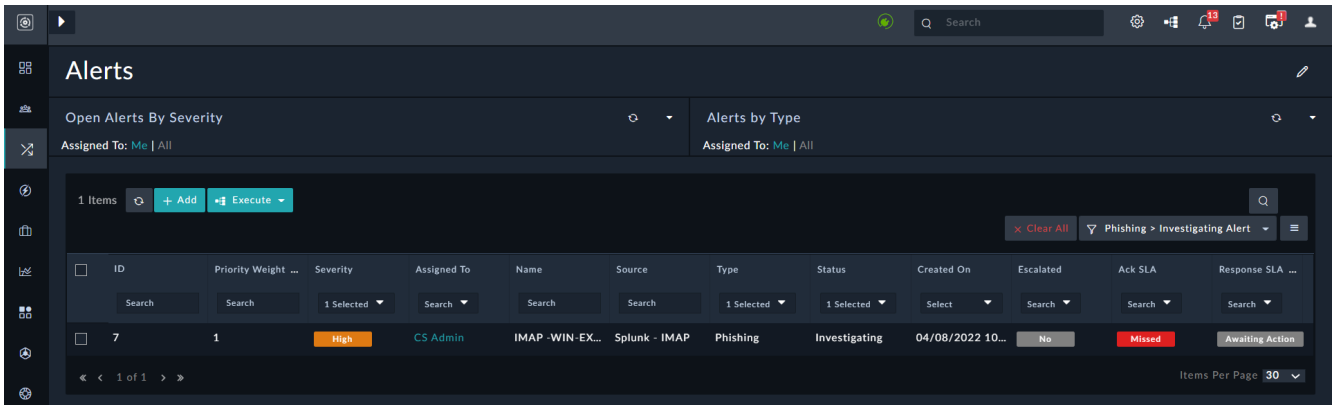
In the filter editing mode, you can perform the following operations:

- Save a filter (user-specific or system).
- Edit the name of an existing filter by clicking the **Edit Name** icon
- Mark an existing filter as a default filter by clicking the **Set Default Filter** (**star**) icon.
- Delete an existing filter by clicking the **Save Filter** drop-down list and selecting the **Delete** option.
- To remove a particular filter criterion that has been applied to the grid, click the **Clear Filter Criteria** link.

Click the **Filters** icon to view a list of all existing filters that have been defined for the grid or record, as shown in the following image:



Using this filtering option, you can filter records using only the **AND** condition; for example, you can filter records whose **Type is Phishing** AND **Status is Investigating**. When you apply this filter, in our example, only one record is displayed, as shown in the following image:



You cannot use the **OR** condition to filter records using this method.

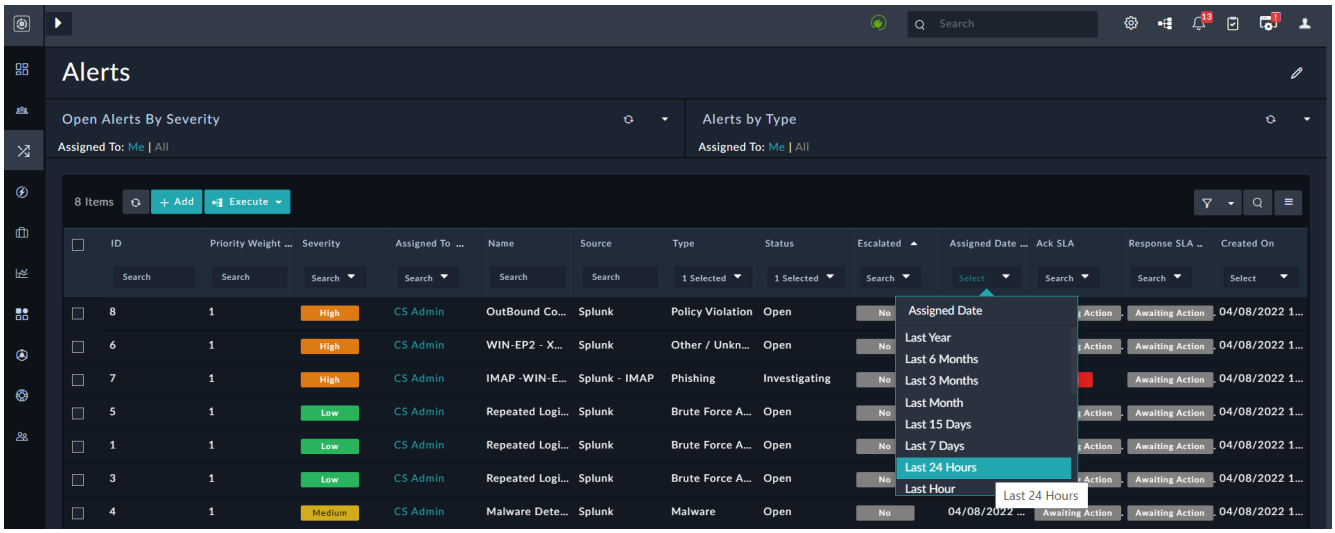
You can also filter records displayed in the module's grid while defining the grid (using the 'Grid' widget) in the listing view using the **Nested Filters** component. The **Nested Filters** component allows you to filter group conditions at varying levels and use **AND** and **OR** logical operators. See the Dashboards, Templates, and Widgets chapter for information on the Grid widget and the Nested Filters component.

The filter condition defined on the listing view will override the filter condition defined in the grid widget.

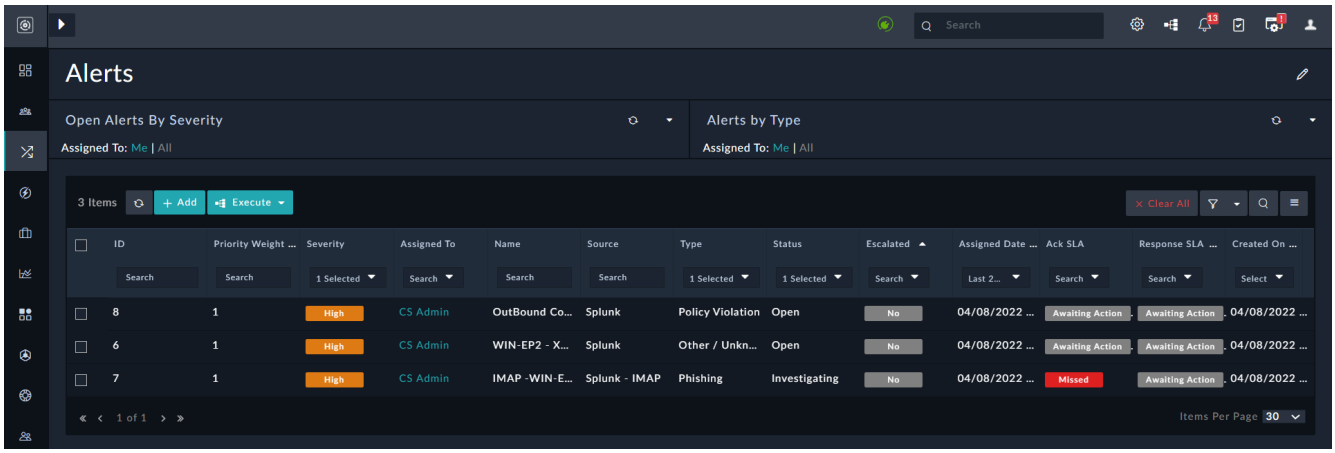
The filter operator for date fields includes many pre-defined options such as Last Year, Last 7 days, Next 24 hours, etc., making it easier for you to filter records for a relative time range of your choice. You can also now specify static custom date ranges for filters. For information on what defines a time range in a filter, see the **Nested Filters** section in the Dashboards, Templates, and Widgets chapter.

For example, if you want to filter alerts that were assigned in the last 24 hours and whose severity is High, do the following:

Click **High** in the **Severity** column and then in the **Search** box in the **Assigned Date** column and select **Last 24 Hours**:

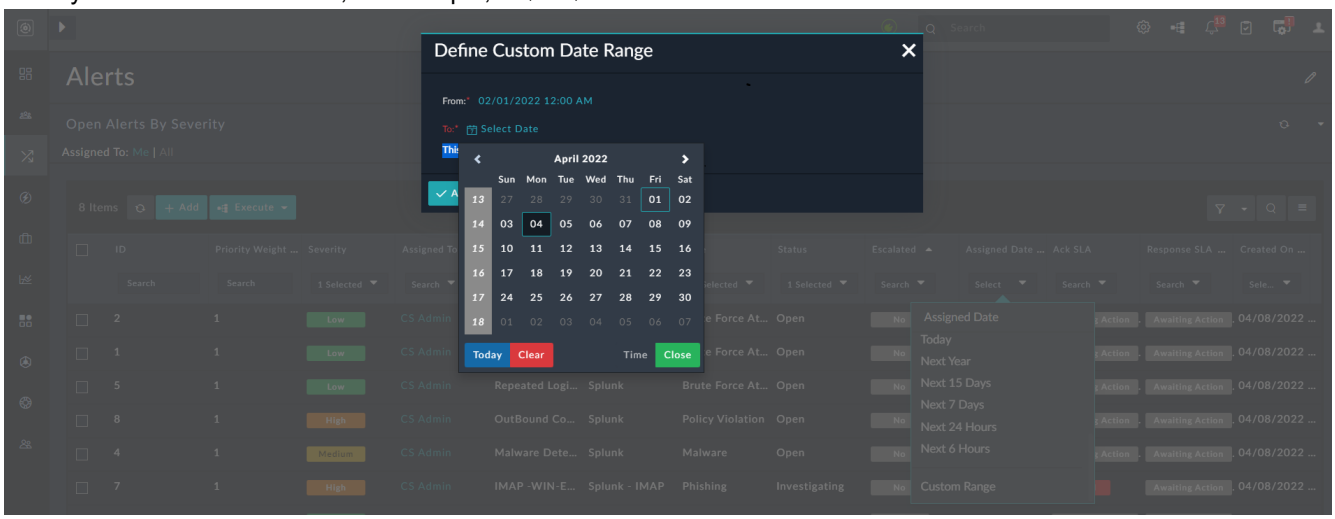


Filtered alerts are displayed as shown in the following image:



Select the **Custom** option to filter records according to custom static date ranges. For example, select **Custom**, and in the `Define Custom Date Range` dialog, from the **From** date field, select the date and time from the Calendar, from when you want to filter records, for example, `01/01/2022 02:00 PM`, and in the **To** field, select the date and time till

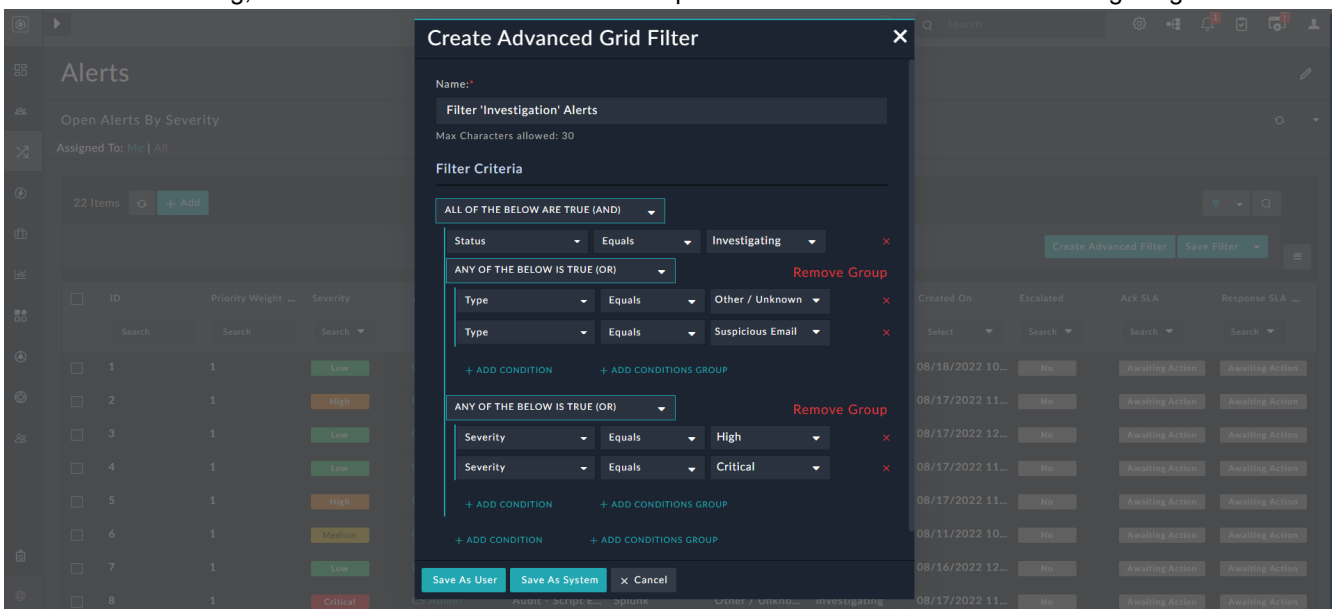
when you want to filter records, for example, `04/01/2022 09:00 AM`:



Advanced Filters

You can use the 'Advanced Filter' to apply conditional filters to the grid columns on the module listing page. You can achieve complex sorting and filtering of records as well as setting a default view per user using the advanced filter.

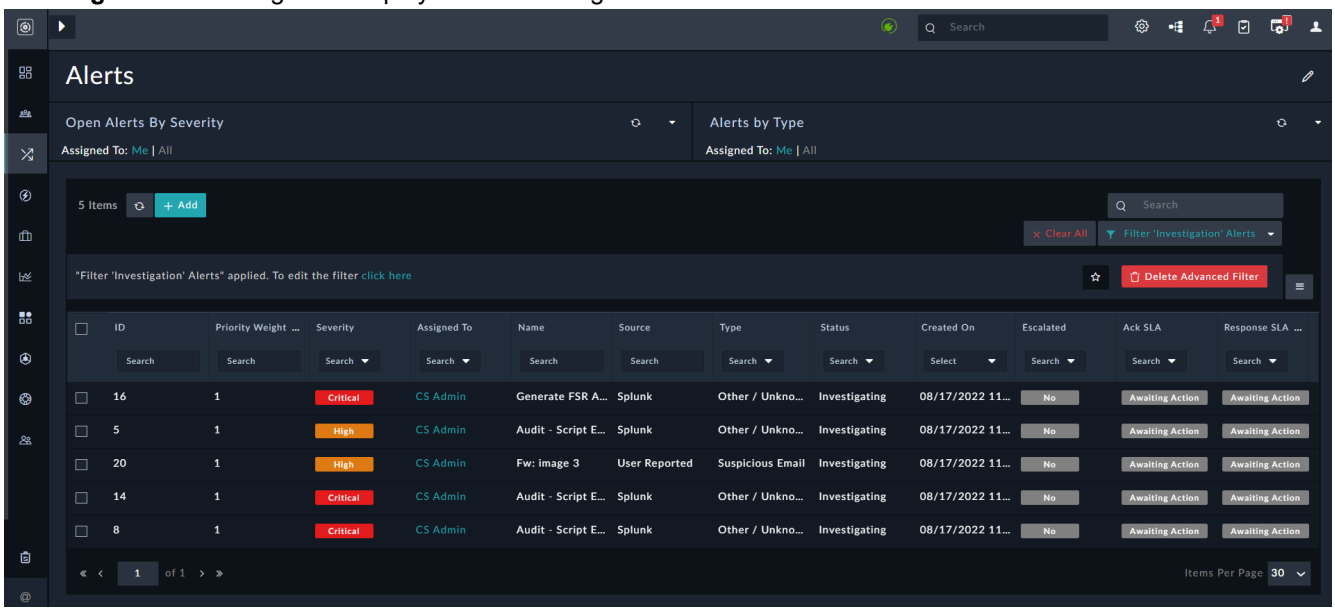
To create an advanced filter, navigate to the module's listing page, for example, the 'Alerts' page. Click the **Filter** icon to display the 'Create Advanced Filter' button. Click **Create Advanced Filter** button to display the `Created Advanced Grid Filter` dialog, in which you can define complex filter conditions. An example of complex conditions used to filter alert records on the grid view could be the filtering of 'High' or 'Critical' alert records whose type is either 'Other / Unknown' or 'Suspicious Email' and whose status is set to 'Investigating'. To create this filter in the `Created Advanced Grid Filter` dialog, enter a name for the filter and the complex conditions as shown in the following image:



You can save this filter as a 'User' filter, i.e., this filter will be visible only to that particular user by clicking **Save as User**. Or, if you are an administrator, then you can also save this filter as a 'System' filter, i.e., this filter will be visible to all users of the system by clicking **Save As System**. For our example, we have saved the filter as a 'User' filter. Once the

advanced filter is applied, the 'Alerts' page displays a filtered list of alerts in the grid. To clear all the filters applied on the grid, click **Clear All**.

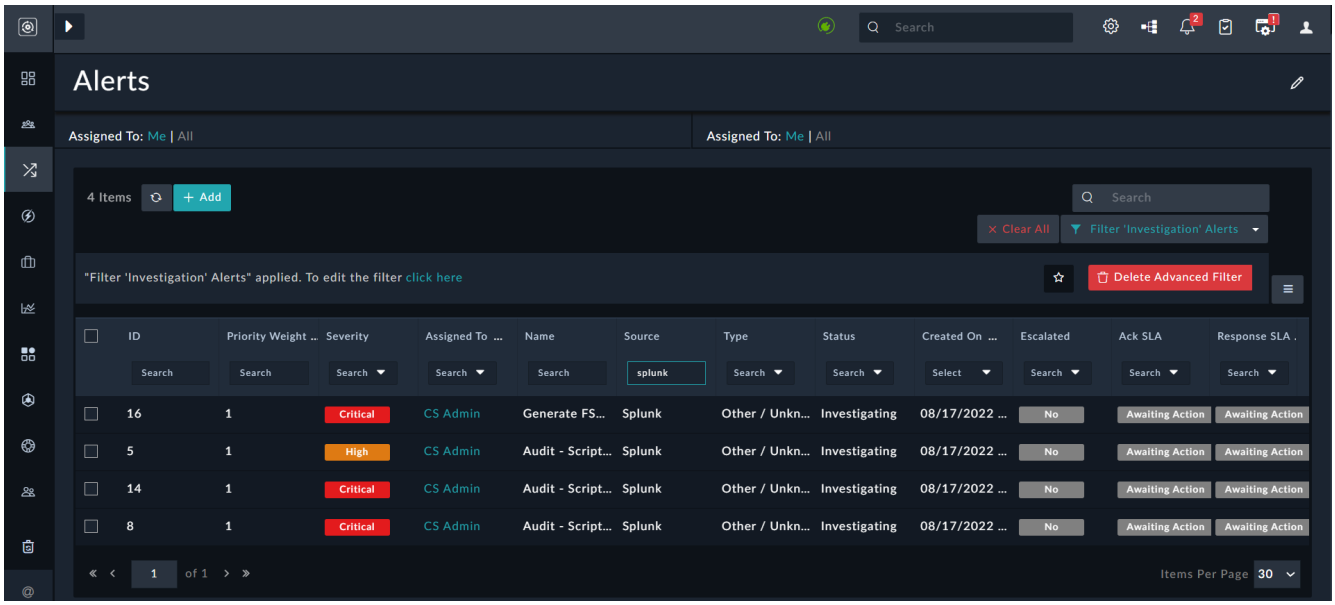
If you have refreshed the browser and want to reapply a created filter on the grid, click the '**Filter**' drop-down list and then select the filter that you want to apply, for example, the 'Filter 'Investigation' Alerts' filter. To edit this filter, click **Filter 'Investigation' Alerts** again to display the filter editing mode:



In the filter editing mode, you can perform the following operations:

- Edit the existing filter, including updating the name and/or conditions of the filter by clicking '**click here**' to open the `Update Advanced Grid Filter` dialog.
- Mark the existing filter as a default filter by clicking the **Set Default Filter** (star) icon.
- Delete the existing filter by clicking **Delete Advanced Filter**.

You can apply column filters on top of the selected advanced filters. For example, further filtering the records based on the 'Source column':



However, the column filters do not get appended to the advanced filter, i.e., the applied column filters are not reflected when you edit the advanced filter.

Dashboards, Templates, and Widgets

Overview

Dashboards

A Dashboard is default landing and home page after a user logs into FortiSOAR.

By default, FortiSOAR includes the **System Dashboard**, which is displayed on all users when they log into FortiSOAR for the first time. Only users who have a minimum of **Read** and **Update** permission on the `Dashboard` module and **Read** permission on the `Security` and `Application` modules can modify the System Dashboard.

Dashboards and reports have good performance since only the required content is loaded and lazy loading of the content is enabled.

Templates

The FortiSOAR interface is rendered using Templates, which can be modified as needed to suit your specific purposes better. Currently, Templates are system-wide, meaning everyone will see the same Template on every interface, e.g., your Incidents screen would be the same as all others. The system interface is composed of View Templates, which are JSON definitions of the interface structure composed of widgets.

Widgets

Widgets render information for the visual display inside View Template. Widget types vary such that specific widgets only correspond to certain view types. For example, the detail view has some exclusive widgets, such as Visual Correlation, Comments, Timeline, etc.

The `People`, `System Assigned Queues`, and `Approval` modules are not part of dashboard widgets since these are system modules and used for administration purposes.

Using Dashboards

Dashboards are the users' default home page. Users use the dashboard and at one glance see what are the critical tasks that they need to work on to be effective.

When an administrator modifies dashboards, those modifications apply to the system and users. Administrators assign dashboards to users based on their roles. If a non-admin user modifies the dashboard, then changes are applicable only to that user. However, both types of users can see the `Edit Dashboard` option.

For Users

You can go to your Dashboard (Home) page and use it to determine "What's important to me right now?" To effectively accomplish answering this question, you must scope your Home page to match up to your operational goals. For example, if you are a user who works on alerts, then you can customize your Dashboard to display alerts that are Critical and High. Using the dashboard, you can then immediately prioritize your work based on the critical and high alerts.

For Administrators

Administrators create dashboards that are applicable throughout the application and are assigned to users based on their roles. Presented here are some options of how administrators can leverage the Dashboard with a specific widget set and increase effectiveness across their organization.

Operation focus

For organizations where Task management is a key focus of using the FortiSOAR platform, tailor the Dashboard to display the user's work.

For example, you can create a dashboard that displays alerts that are Critical and High and then assign them to users who have a role of handling alerts. Users can prioritize their work looking at their Dashboard, which is displaying the Critical and High alerts.

Analytics focus

For organizations where analytics is a key focus of using the FortiSOAR platform, tailor the Dashboard to display trends.

For example, you can create a dashboard that displays the number and type of alerts that are created daily, weekly, or monthly and then assign them to users who have a role of an analyst. Analysts can view and analyze the dashboard and come up with solutions. If for example, the dashboard displays an increase in the number of instances of alerts of type Malware over the period of three months, analysts analyze the dashboard and come up with mitigation solutions.

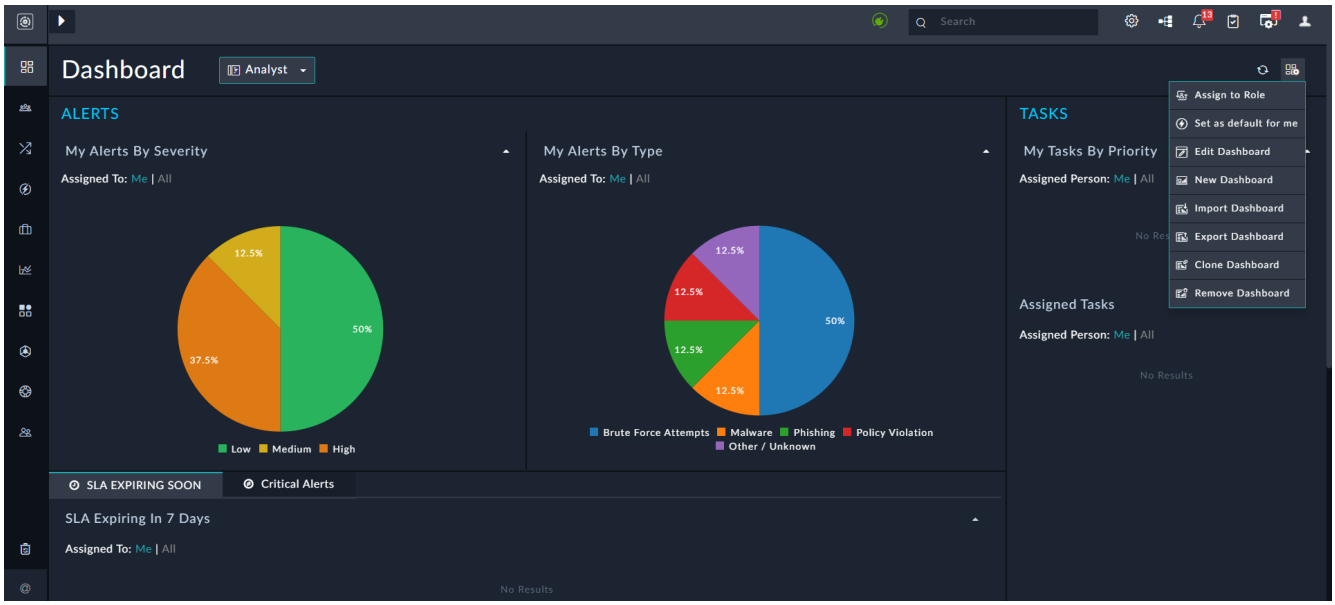
Strategic focus

For organizations where strategizing is a key focus of using the FortiSOAR platform, tailor the Dashboard to display key performance indicators.

For example, you can create a dashboard that displays the number of incidents in the open state, per region, and severity for six months and then assign them to users who have a role of an executive. Executives can then view and analyze the dashboard and come up with solutions on how to optimize operational efficiency. If for example, the dashboard displays a consistent increase in the number of open incidents over the period of six months, executives can analyze the dashboard, understand the cause of this trend, such as is it because of inefficiencies or need for automation, or both and come up with informed solutions.

Process of creating or editing dashboards

To add or edit an existing dashboard, click the **Actions** icon (), which appears at the top-right corner of a page, and click **New Dashboard** or **Edit Dashboard**.



Templates are JSON definitions of the interface structure composed of widgets. Widgets are configurable interface elements that are used to represent data, such as charts or lists visually.

If you have changed a dashboard that an administrator has assigned to you, then you will not be able to view the administrator changes to that dashboard. To view the administrator changes to the report, click **Actions** > **Reset to Original State**.

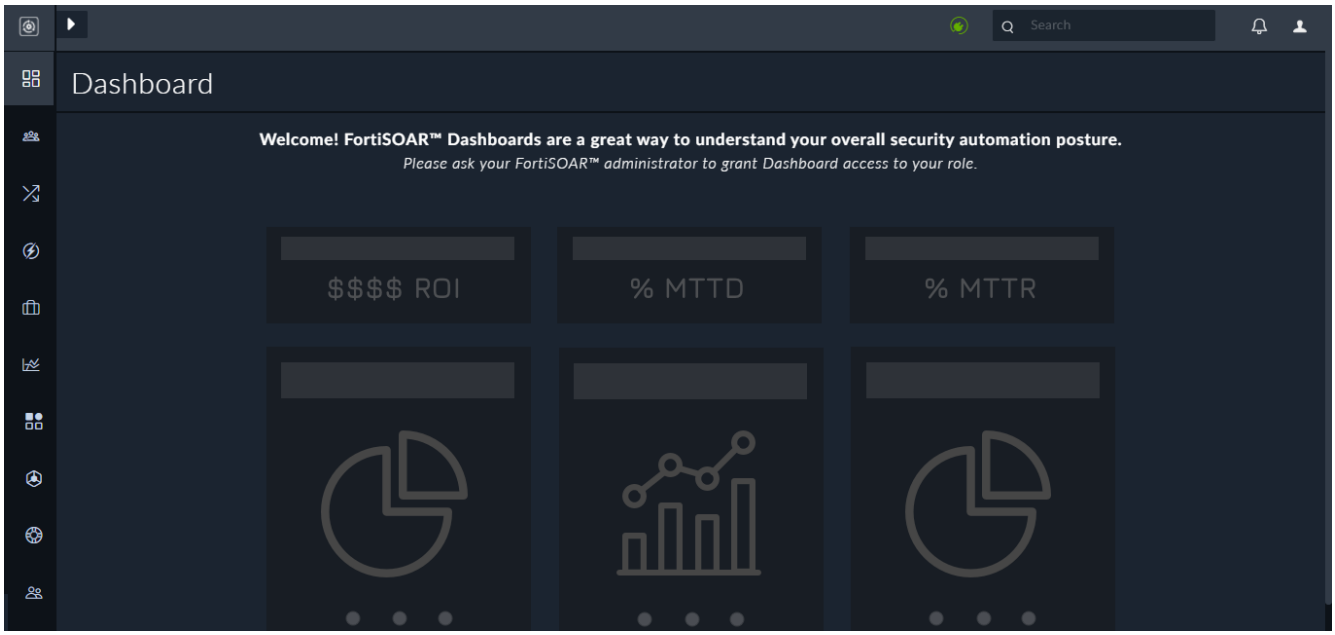
For information on using templates, see the Using Templates section and for information on widgets, see the Using Template Widgets section.

Permissions required for modifying dashboards

Only when an administrator, modifies dashboards, those modifications are applicable across the system and applicable to users, based on their roles.

To view dashboards, you must be assigned a role that has `Read` permissions on the `Application` and `Dashboard` modules, and the dashboard must be assigned to your role.

If you are assigned a role that *does not* have any permissions on the `Dashboard` module, your landing page will appear as shown in the following image:



To create and update dashboards, you must be assigned a role that has `Read`, `Create`, and `Update` permissions on the `Dashboard` module and `Read` permissions on the `Application` module. Additionally, if you also want to delete dashboards and configurations, you must be assigned a role that has `Read`, `Create`, `Update`, and `Delete` permissions on the `Dashboard` module and `Read` permissions on the `Application` module.

For users who should only be able to customize their own dashboards, and whose changes will not be visible to any other user, a role with, `Update` and `Create` permissions on the `Dashboard` module and `Read` permission on the `Application` module is sufficient. If such a user (a non-admin user) changes the dashboard, then a copy of the original dashboard is created and those changes are visible to only that particular user and not to other users.

For users who should be able to customize dashboards, and whose changes should be visible to all users who have access to that dashboard, a role that has `Read` and `Update` permissions on the `Dashboard` module and `Read` permissions on the `Application` and `Security` modules must be assigned. If you have these permissions, then the changes are made in the original dashboard and these changes are visible to all the users who have access to the dashboard.

In addition to the appropriate permissions as mentioned above, users also require to have appropriate rights on the module for which they want to create or edit dashboards. Since if users do not have `Module Read` permissions on the module that they want to consume in the dashboard, then they will not be able to view the details of that module in the dashboard. For example, if you have `Module Read` permissions on the **Alerts** module but not on the **Incidents** module, then you can update dashboards that consume Alerts as their data source. However, if you try to update a dashboard that consumes Incidents as the data source, FortiSOAR displays a message such as `You do not have necessary permissions for Incidents`.

Users: Working with dashboards

Administrators assign dashboards to you based on your roles, so that you can have access to multiple dashboards. You can customize your home page choosing a default dashboard from the dashboards assigned to you.

You can also add, edit, clone, import, export, and remove dashboards that are assigned to you.

You can create personalized dashboards based on your roles. Customizations that you make to your dashboards are visible and applicable only to you. Administrators must update the dashboard for the changes to apply to all users. Updates, including removal, and additions that administrators make to the dashboards apply to all users.

Customizing your Home page

Administrators assign dashboards to you based on your roles, so that you can have access to multiple dashboards. When you log on to FortiSOAR to for the first time, by default your home page is set to the **System Dashboard**. You can customize your home page by selecting the default dashboard from the dashboards assigned to you, as follows:

1. Log on to FortiSOAR.
2. On the `Dashboard` bar, the dashboards assigned to you are listed as a drop-down in the top bar.
   View all the dashboards assigned to you.
3. Open the dashboard you want to set as your default by selecting the same from the drop-down list present in the `Dashboard` bar, and then clicking the **Actions** icon () and selecting **Set as default for me**.
   When you log on to FortiSOAR the next time, your home page is set as the selected dashboard.

Customizing your dashboards

To add or edit your dashboards:

1. Log on to FortiSOAR.
2. On the `Dashboard` bar, to add a new dashboard click the **Actions** icon and select the **New Dashboard** option. To edit an existing dashboard, click the **Actions** icon and select **Edit Dashboard**.
3. In the **Template Title** field, enter the template title.
4. Click **Add Row** and structure the row by defining the number and layout of columns from the options displayed in **Define a new structure**.
5. Click **Add Widget** and from the **Choose Widget** dialog box, select the appropriate widget.
   For information on widgets, see the Using Template Widgets section.
   The `Choose Widget` dialog includes the categorization of different types of widgets that you can use to build dashboards or reports. For example, the **Tabs** widget is categorized as a `Structure` widget, and the **Richtext Content** widget is categorized as a `Custom Content` widget.
6. In the `Edit <name of widget>` dialog, configure the widget properties, and click **Save**.
7. Click **Apply Changes**.
   To revert the changes, you have made to the template, click **Revert Changes**.

Using dashboards

To clone a dashboard:

1. Log on to FortiSOAR.
2. On the `Dashboard` bar, click the **Actions** icon and select **Clone Template**.
3. Update the template title.
   By default, the template title appears as **cloned: name of the original template**.
4. Update the template and widgets as required.
5. Click **Apply Changes**.

To import a dashboard template:

Use the Export and Import Dashboard Template feature to share dashboards across users. If you see a dashboard that a colleague has created that you feel would be useful to you as well, then instead of you having to recreate the dashboard, your colleague can export the dashboard, and you can import it and start using the same.

You can only import a valid JSON template. The template that you import is only applicable to your dashboard. Administrators must import, update, and assign dashboards for the changes to apply to all users.

1. Log on to FortiSOAR.
2. On the `Dashboard` bar, click the **Actions** icon and select **Import Dashboard**.
3. In the `Import Dashboard Template` dialog box, drag-and-drop the JSON template file, or click to browse to the JSON template file.
4. Click **Import**.
   If the file is in the appropriate JSON format, FortiSOAR displays `Template Imported successfully!`

To export a dashboard template:

Dashboard templates get exported in the JSON template.

1. Log on to FortiSOAR.
2. On the `Dashboard` bar, click the **Actions** icon and select **Export Template**.
   FortiSOAR downloads the template on your machine in the JSON format.

To remove a dashboard:

You can only remove dashboards that you have added. You cannot remove the System Dashboard or any dashboard that is created by the administrator.

1. Log on to FortiSOAR.
2. Open the dashboard you want to remove by selecting the same from the drop-down list present in the `Dashboard` bar, and then clicking the **Actions** icon and selecting **Remove Dashboard**.
3. On the **Confirm** dialog, select **OK**.

Administrators: Working with dashboards

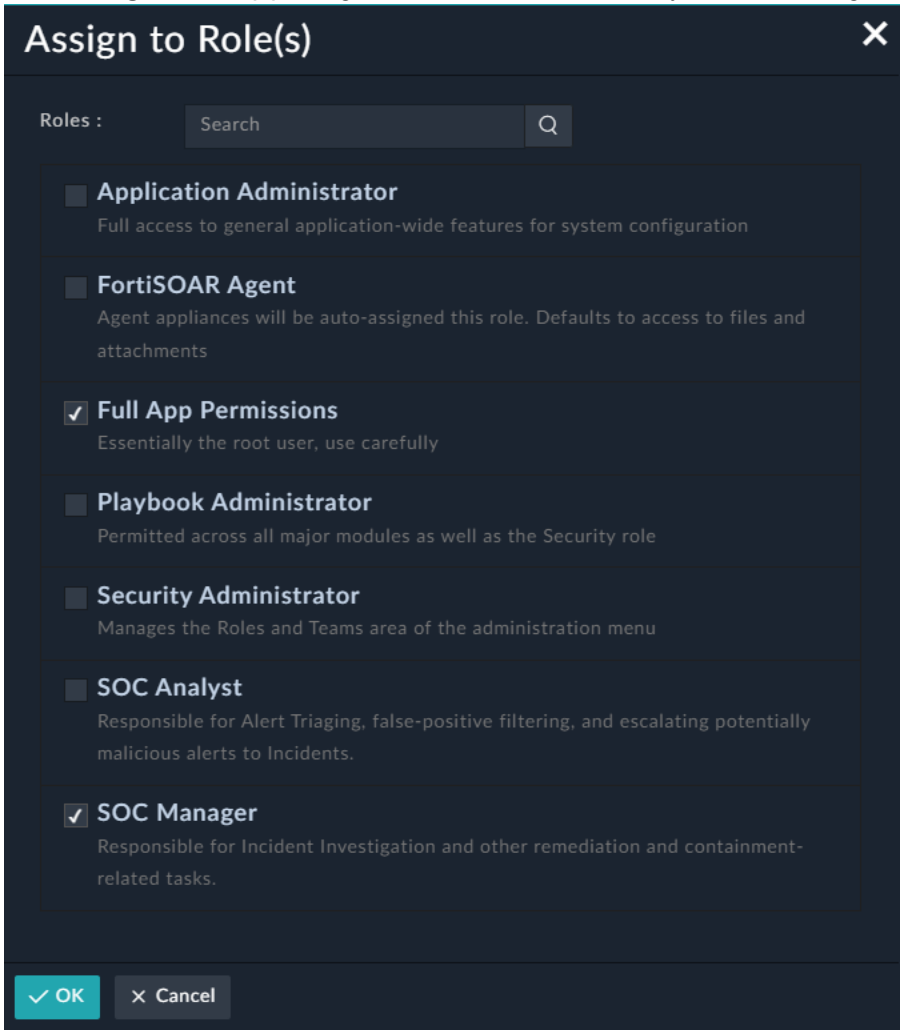
Administrators can perform all the tasks users can perform, which include customizing home pages and dashboards. Administrators also create and edit system-wide dashboards and assign dashboards to roles. To create system-wide dashboards, click the **Actions** icon and then select **New Dashboard** option, and then add the template name and widgets that you want in the dashboard. After you have completed creating a template, you must remember to assign the dashboard to the appropriate roles.

Updates, including removal, and additions that you make to dashboards apply to all users.

Assigning dashboards to roles

You must have a minimum of "Read" permission on the Security module, apart from other appropriate privileges to perform this task.

1. Log on to FortiSOAR.
2. On the `Dashboard` bar, select the dashboard that you want to assign to a role.
3. Click the **Actions** icon and select **Assign to Role** OR
   Click the **Actions** icon and select **Edit Dashboard** and then click the **Assign To Roles** or ***Number of Roles Assigned*** link.
   This displays the Assign to Role (s) dialog in which you can select the role(s) to whom you which to assign the dashboard.
4. In the **Assign to Role(s)** dialog box, select the role to which you want to assign the dashboard.



   You can also search for a role in the **Search** text box.
5. Click **OK**.
   Users having the role specified will be able to see the dashboard(s) associated with that role the next time they log on to FortiSOAR.

Input Variables in Dashboards and Reports

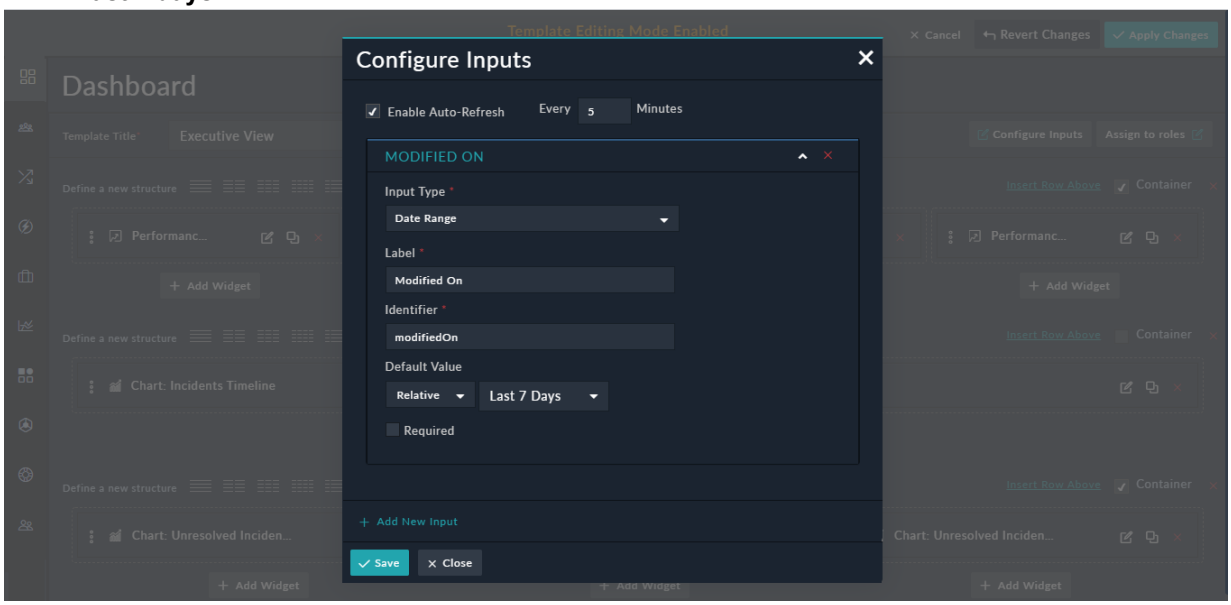
You can define variables that you want to use in widgets as filters to consume inputs and create a dashboard or a report dynamically. Using input variables, you can filter data in a dashboard or report to display a particular set of data without having to define the same criteria in each widget in the dashboard. Once you configure the variable as a filter in widgets, the dashboard is displayed according to the filter value you have specified. You can now specify inputs for dashboards or reports, based on which dashboard or reports are updated dynamically to display the dashboard or report according to the updated input values.

Defining Input Variables

This procedure demonstrates how to define an input variable for a dashboard or report to display only those records that were modified in the last 7 days.

1. Log on to FortiSOAR.
2. On the `Dashboard` bar, click the **Actions** icon and select **Edit Dashboard**.
3. On the `Template Editing Mode Enabled` page, click **Configure Inputs**.
4. In the `Configure Inputs` dialog, configure the input variable according to your requirements:
   a. (Optional) Select the **Enable Auto-Refresh** option to automatically refresh your dashboards or reports after the set time interval.
   By default, the time interval is set at 10 minutes. You can modify the time interval according to your requirements.
   b. Click **Add New Input**.
   c. From the **Input Type** drop-down list, select the type of field that is going to be applied as the input variable. You can choose from the following options: Text, Number, Date, Date Range, Picklist, or Lookup.
   For our example, select **Date Range**.
   d. In the **Label** field, type the name that describes this variable.
   For our example, type `Modified On`.
   The **Identifier** field gets automatically populated with the identifier based on the "Label" you have specified. In case of our example, the Identifier field is populated with the modifiedOn variable. The value that is present in the Identifier field is the key by which this variable will be identified.
   e. (Optional) In the `Default Value` section, choose the value based on which the dashboard will be displayed, by default. The date ranges are relative, i.e, relative to the current date. You can choose between a **Relative** date range or a **Custom** relative date range.
   If you choose **Relative**, then you get a list of pre-defined relative date ranges such as Last 24 Hours, Last 30 Mins, etc. If you choose **Custom**, then you can specify a custom date/time range, such as **Last 2 Hours**. For more information, see Support for Custom Time Ranges in Filters. For our example, select **Relative** and then

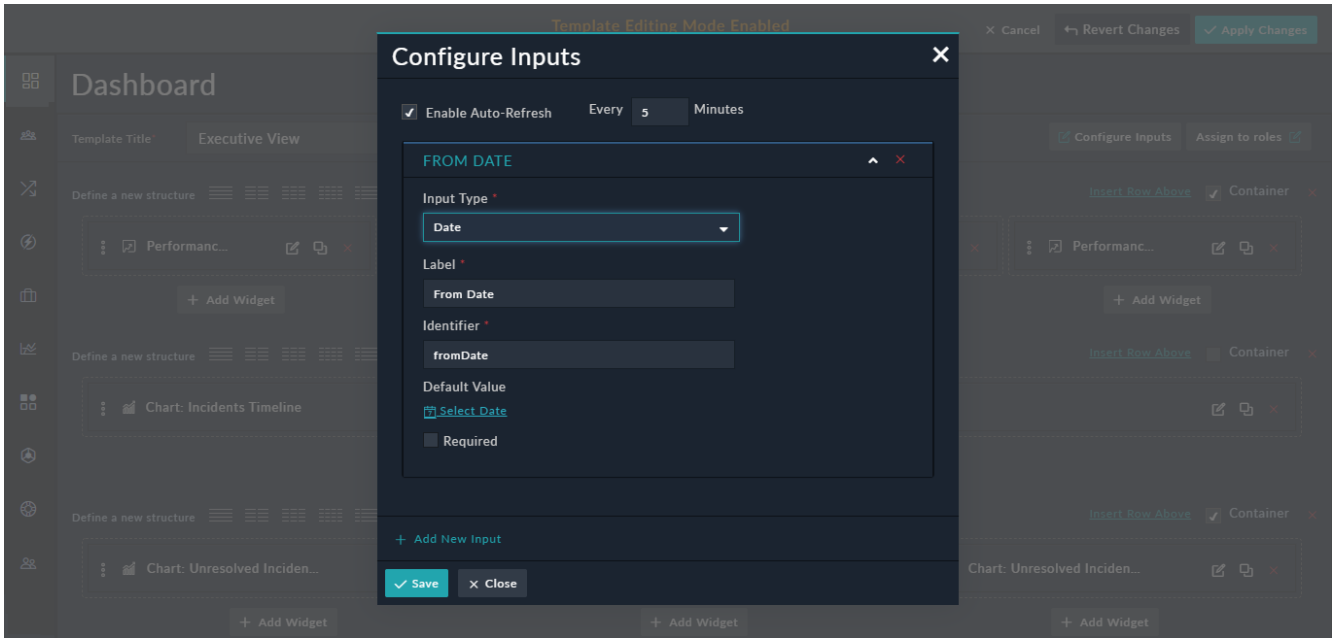
select **Last 7 days**.



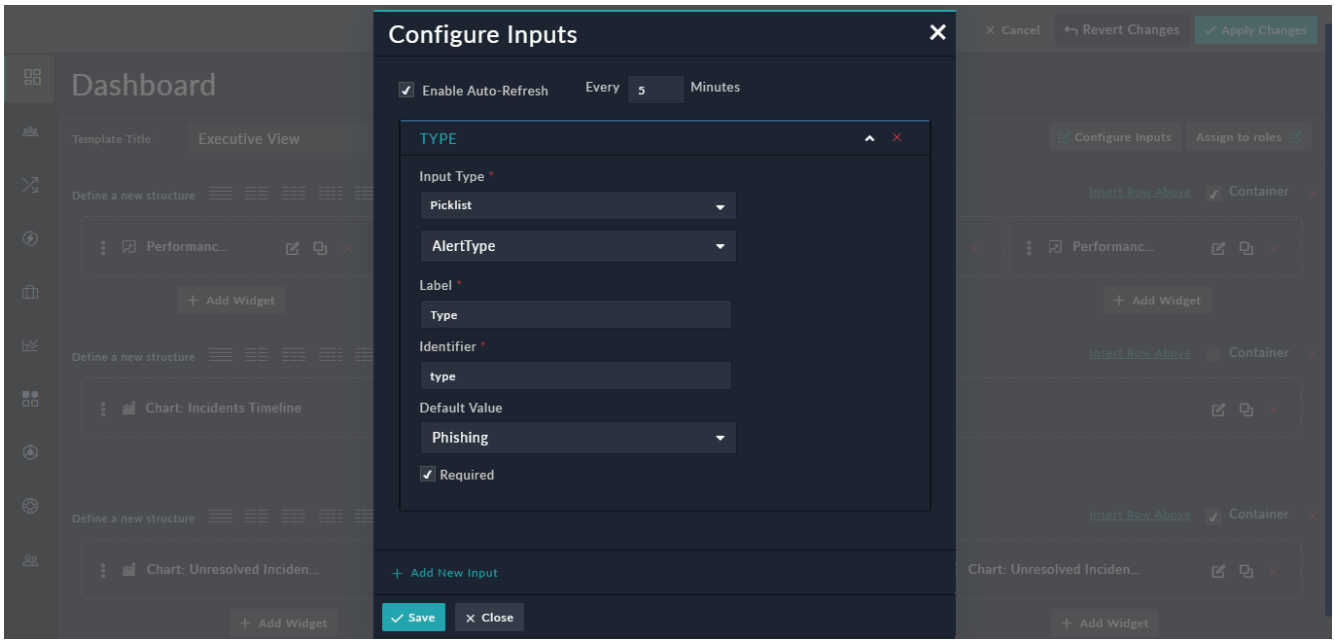
f. (Optional) To make the input field mandatory, click the **Required** checkbox. If you select the Required checkbox, then the report or dashboard will not be displayed unless the user provides the input.

5. (Optional) To define more input variables, click the **Add New Input** button.
6. Click **Save** to save the variable(s).

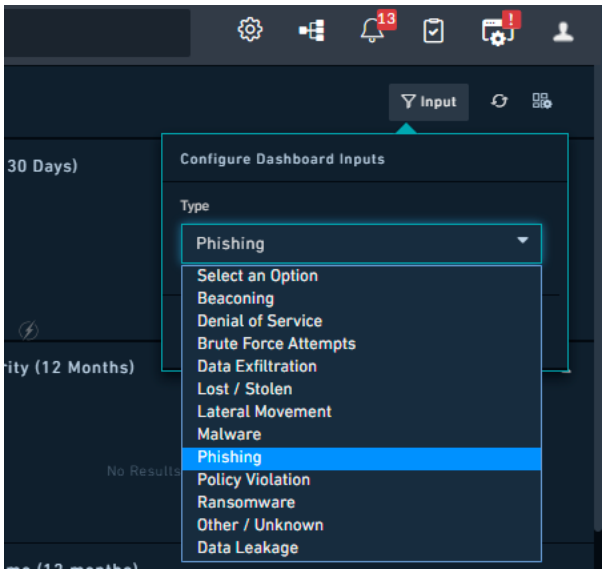
The **Date** input type enables you to ask a user for a date based on which they want to filter the dashboard or report, using the **Select Date** link in the `Default Value` section. An example of using the **Date** input type would be to define the From Date, i.e., the date from when the user wants to view the report:



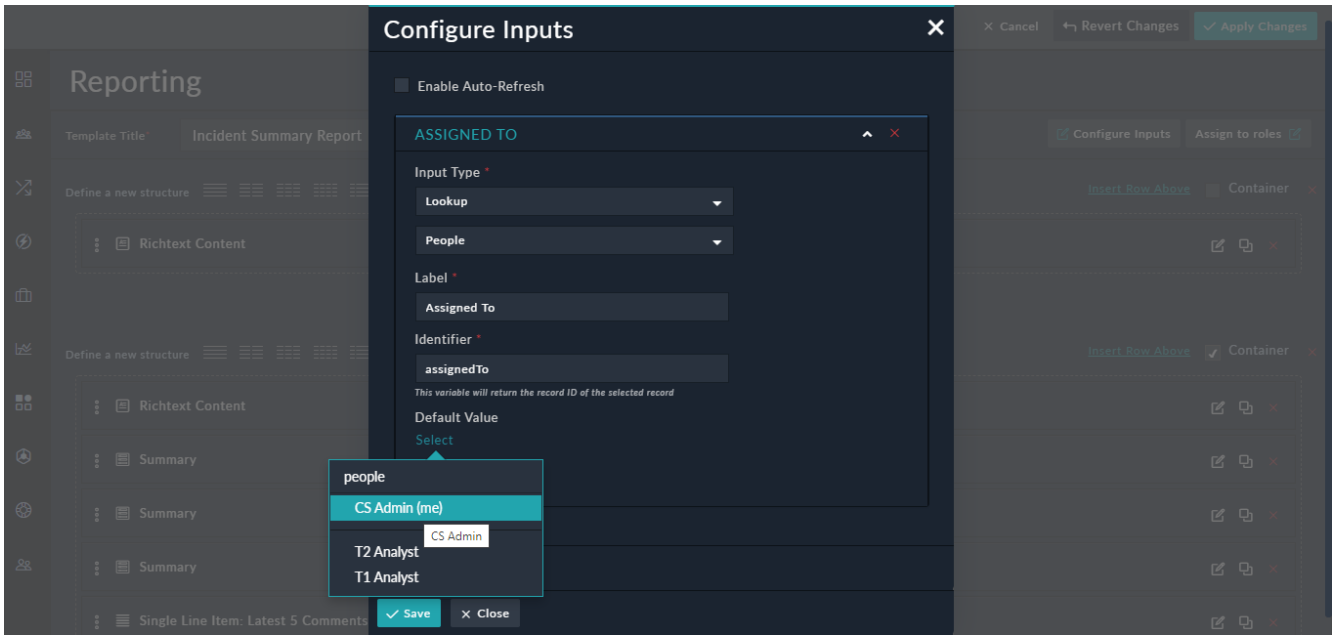
The **Picklist** input enables you to ask a user to select a value of an existing picklist based on which they can filter the dashboard or report. You can set a default value to filter the dashboard or report, for example, as shown in the following image, **Phishing** is selected in the **Default Value** field. This means that the report or dashboard, by default, will be filtered to display only those alerts that are of type *Phishing*.



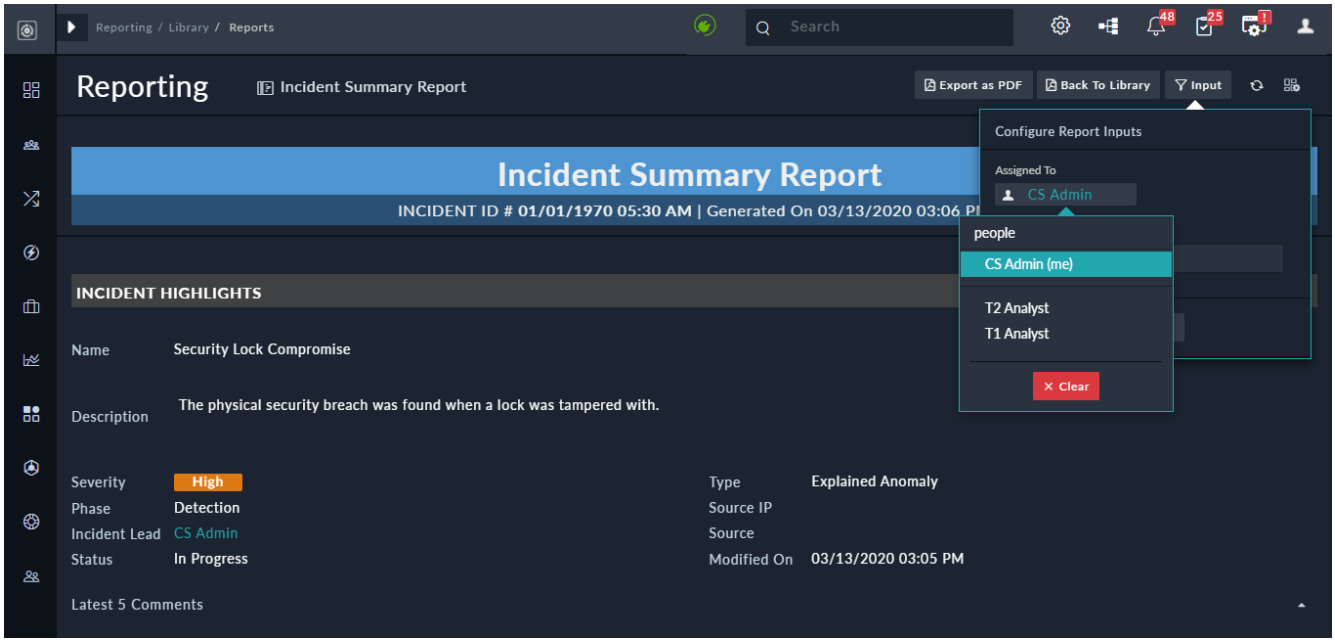
The defined input variables can be seen on the Dashboard by clicking the **Input** button. However, to use the input variables for filtering the Dashboard, you must also configure them in the appropriate widgets, as specified in the following Configuring Input Variables section. Users can click Input on the dashboard or report and choose any other alert type for which they want to see the dashboard or report:



You can also select the **Lookup** option as an input type. The **Lookup** input enables you to ask a user to select a value of an existing lookup based on which they can filter the dashboard or report. For example, filtering an "Incident Summary Report" based on the user to whom that incident was assigned. You can also set a default value to filter the dashboard or report, for example, as shown in the following image, **CS Admin** is selected in the **Default Value** field. This means that the report or dashboard, by default, will be filtered to display the summary of the incident that has been assigned to "CS Admin".



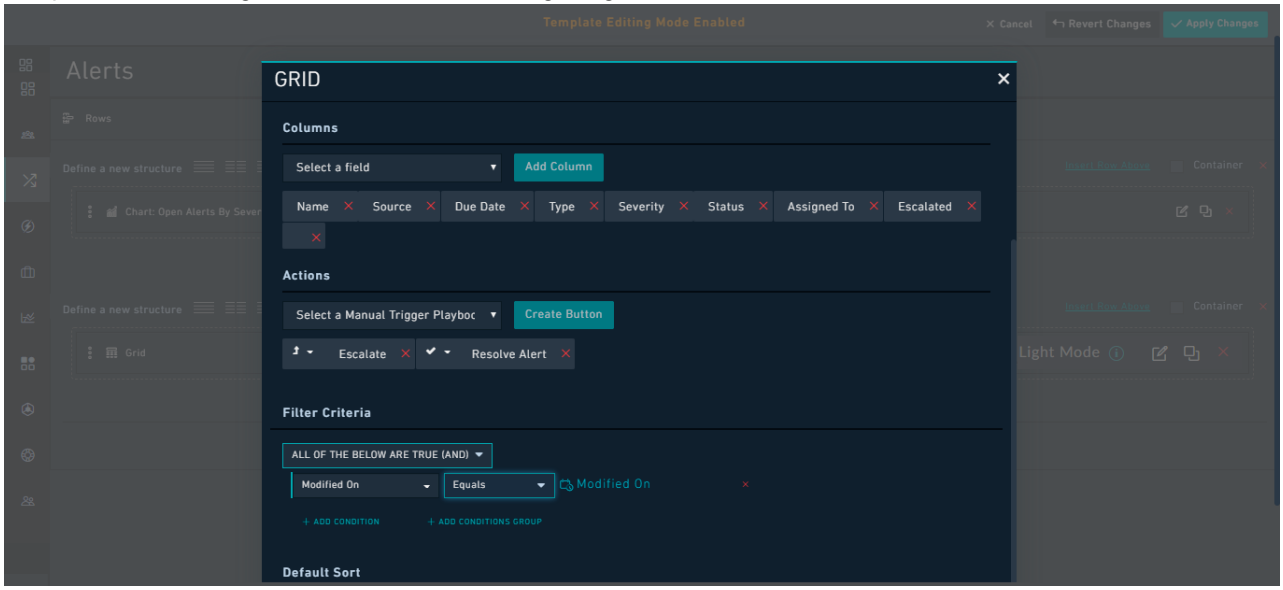
The defined input variables can be seen on the Report by clicking the **Input** button. However, to use the input variables for filtering the Dashboard, you must also configure them in the appropriate widgets, as specified in the following Configuring Input Variables section. Users can click **Input** on the dashboard or report and choose any user for who they want to see the dashboard or report:



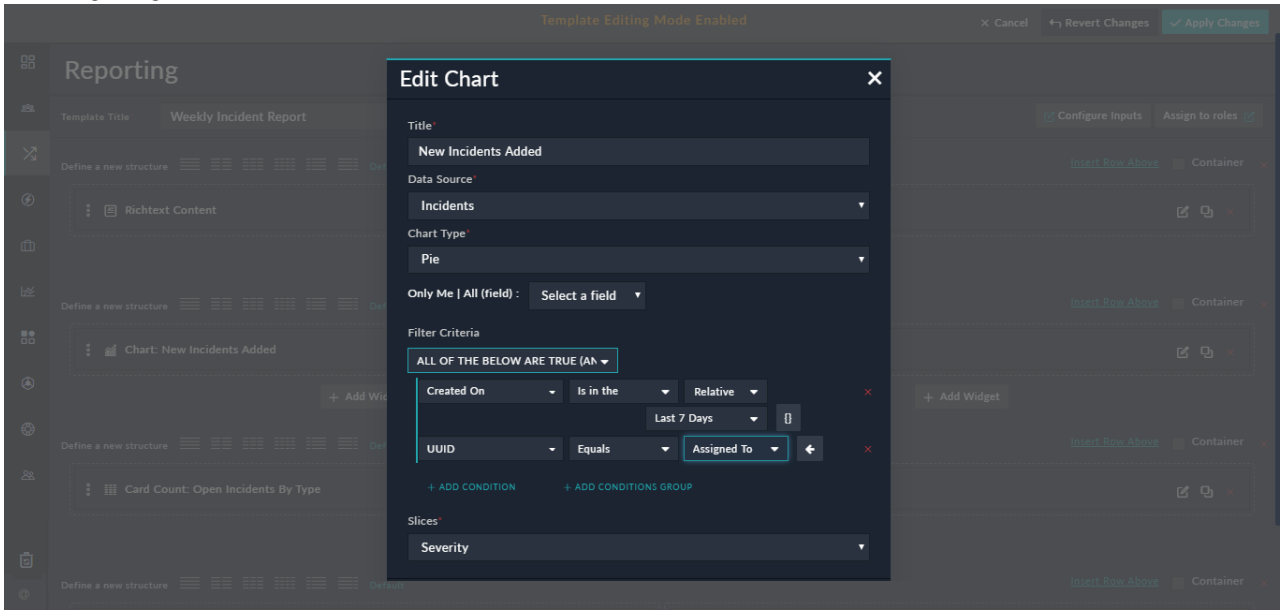
Configuring Input Variables

Once you complete defining the input variables, you must configure them in the widgets that require to consume the input variables that you have defined.

1. Log on to FortiSOAR.
2. On the `Dashboard` bar, click the **Actions** icon and select **Edit Dashboard**.
3. Open the widget that is required to consume this input variable.
   For example, in a **Grid** widget, that displays Alert records, you can add the **Modified On** filter in the Nested Filters component in the widget as shown in the following image:



Important: "Lookup" Fields must be bound using UUID. For example, in case of the "Incident Summary Report", where you want to see the summary of the incident which is assigned to a particular user, you would add the filter such as `UUID Equals Assigned To`. For example, in a Chart widget, that displays newly added Incident records, you can add the `Assigned To` filter in the Nested Filters component in the widget as shown in the following image:

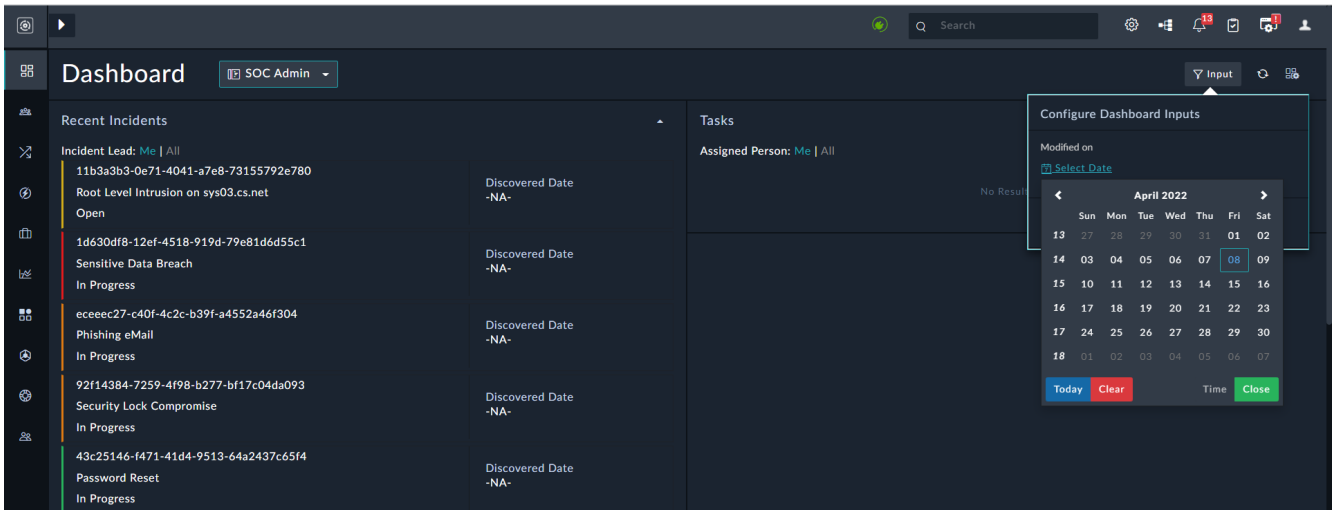


4. Click **Save**.

Using Input Variables

Once input variables are defined for a dashboard, then you can dynamically specify inputs to the dashboard, which will then display the dashboard according to the updated input values that the user has specified. Use the **Inputs** button on the `Dashboard` page to change the inputs to the dashboard and update the dashboard dynamically.

For example, if you want the Grid widget in our dashboard to display only those records that were modified in the last 15 days, instead of the last 7 days, then you click the **Input** button and in the `Configure Dashboard Inputs` dialog, in the **Modified By** field select **Last 15 days** and click **Apply**. This will dynamically update the Grid in the dashboard to include records that were modified in the last 15 days.

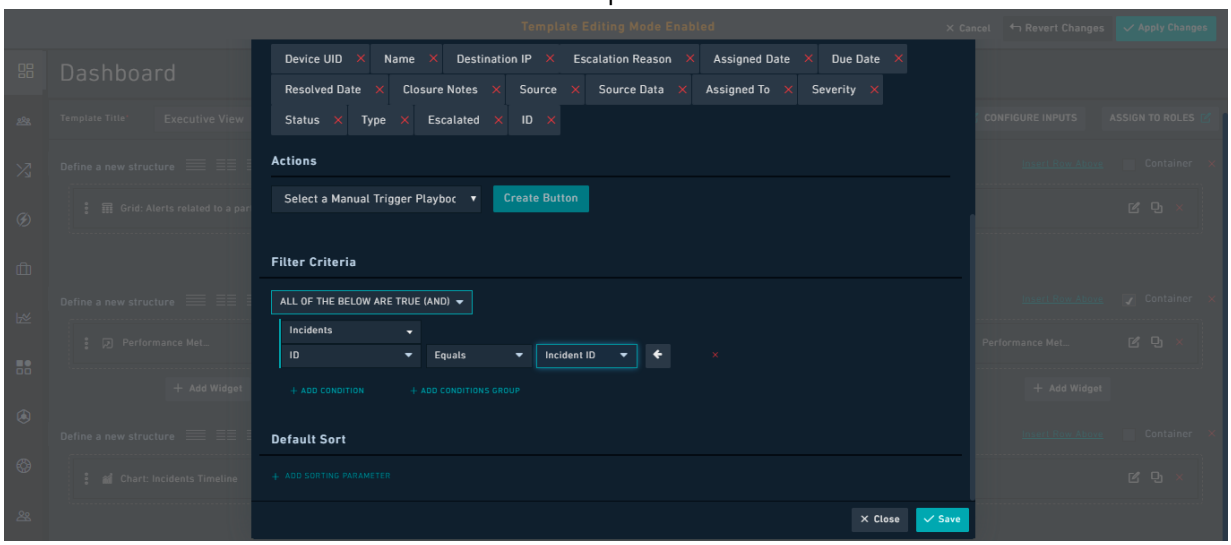


Related Records Filter in Widgets

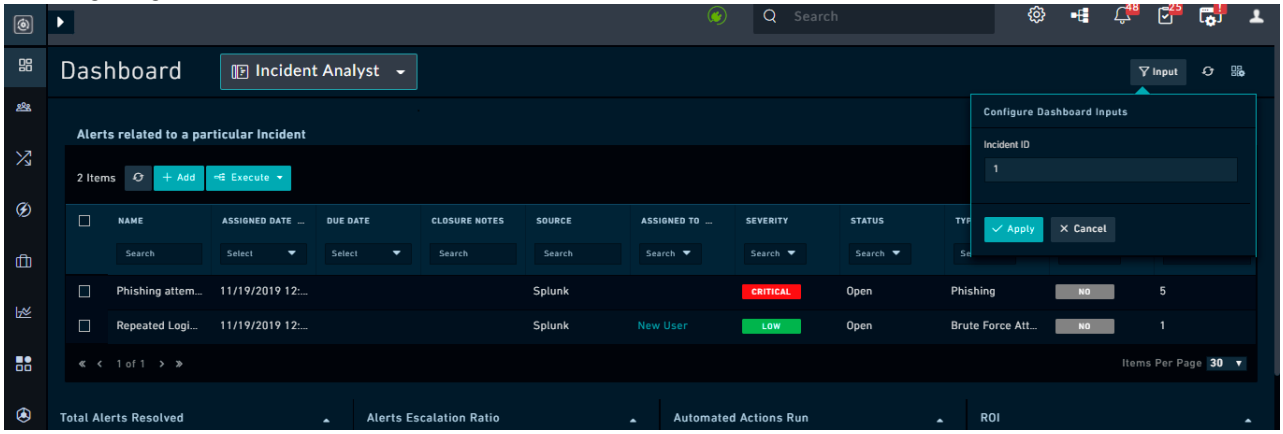
The Nested Filters component is enhanced to have the ability to display fields with many-to-many relationships. Earlier, only primitive types and one-to-many relationship fields were displayed in the Nested Filters component. For example, if you require to display alerts associated with a specified incident, which you will specify using the Filters option on the Reports or Dashboard page, to be displayed in a Grid, then do the following:

1. Add a `Grid` widget with the Data Source set as **Alerts** and select the columns to be displayed in the grid.
2. Create an Input Variable called `IncidentID` with the following properties:
   a. Input Type: Number
   b. Label: Incident ID
   c. Identifier: IncidentID
3. Configure the grid to display alerts associated with a specific Incident record as follows:
   a. In the `Filter Criteria` section, select the **Incidents** module (available under `Related Modules` section).

b. Add the criterion as `ID Equals Incident ID` as a filter and click **Save**.
This will retrieve all alerts that are associated with the specified Incident ID.



4. Click the **Input** button on the `Dashboard` page and in the `Configure Dashboard Inputs` dialog in the Incident ID field enter the Incident ID based on which you want to filter the grid, for example, `1`, and click **Apply**.
In the Grid, you will see all the alerts that are related to the Incident ID that you have specified, as shown in the following image:



Using Templates

Use the Template Editor to design the way you view FortiSOAR, such that you can change the location, visibility, and visualization method being used across the application. The system interface is composed of View Templates, which are JSON definitions of the interface structure composed of widgets. Widgets are configurable interface elements that are used to represent data, such as charts or lists visually. For information on widgets, see the Using Template Widgets section.

Editing Templates

Administrators should read the Permissions required for modifying dashboards section, as it explains what roles you must assign to users to edit dashboards.

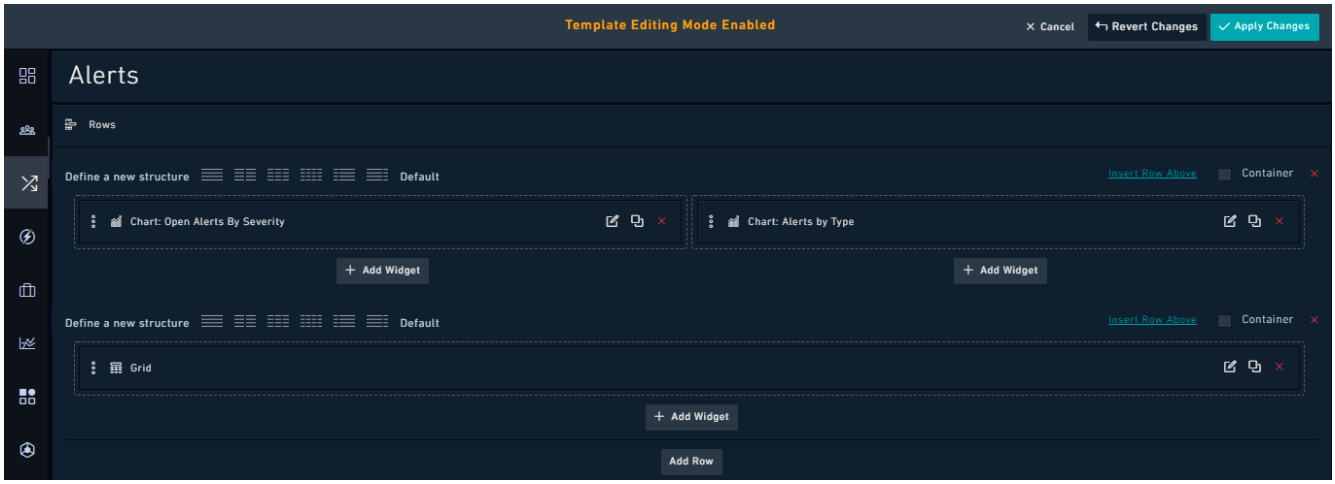
In FortiSOAR templates can be edited at three levels:

- Dashboard level: Determines the display of dashboards.
- Module Listing level: Determines the display of the modules in the "List" view.
- Module Detail level: Determines the display of the individual records within a module, i.e., determines how the record is displayed in the "Detail" view.

Template Editing Mode

If you have the appropriate permissions as specified in the Permissions required for modifying dashboards section, you can edit templates by clicking the **Actions** icon and selecting the `Edit Dashboard` option. Clicking `Edit Dashboard` opens the Template Editor so that you can modify the interface. Use the Template Editor on any Dashboard or Module screen.

You know that you have entered the Template Editing mode when `Template Editing Mode Enabled` is displayed on the top of the screen.



If you make a mistake during the Template Editing session, you can either `Cancel` to exit the mode and discard the changes or `Revert Changes` to stay in the Template Editing Mode but discard any changes since the last `Apply`.

Template Types

Dashboard

The Dashboard is the default home page for a user. Administrators can assign multiple dashboards to you, based on your role. By default, an administrator sets **System Dashboard** as your home page. You can customize your home page, as well as all the dashboards assigned to you. Refer to the Dashboards section for more information dashboards.

Customizations that you make to your dashboards are visible and applicable only for you. Administrators must update the dashboard for the changes to apply to all users.

Modules

The remaining Templates are stored on a per Module basis. There are three types of Templates per Module:

- List
- Detail
- Form

Widget types vary such that specific widgets only correspond to certain view types. Detail views have some exclusive widgets, such as Comments.

List Views

The List view is the first view that you see when you click on any Module in the main navigation, for example, Incidents. The List view, by default, has a grid widget that displays all the records matching the filter applied to the grid.

Filters are applied per user and can also be modified at a global level for any grid on a Module. Also, you cannot apply Filters to encrypted fields.

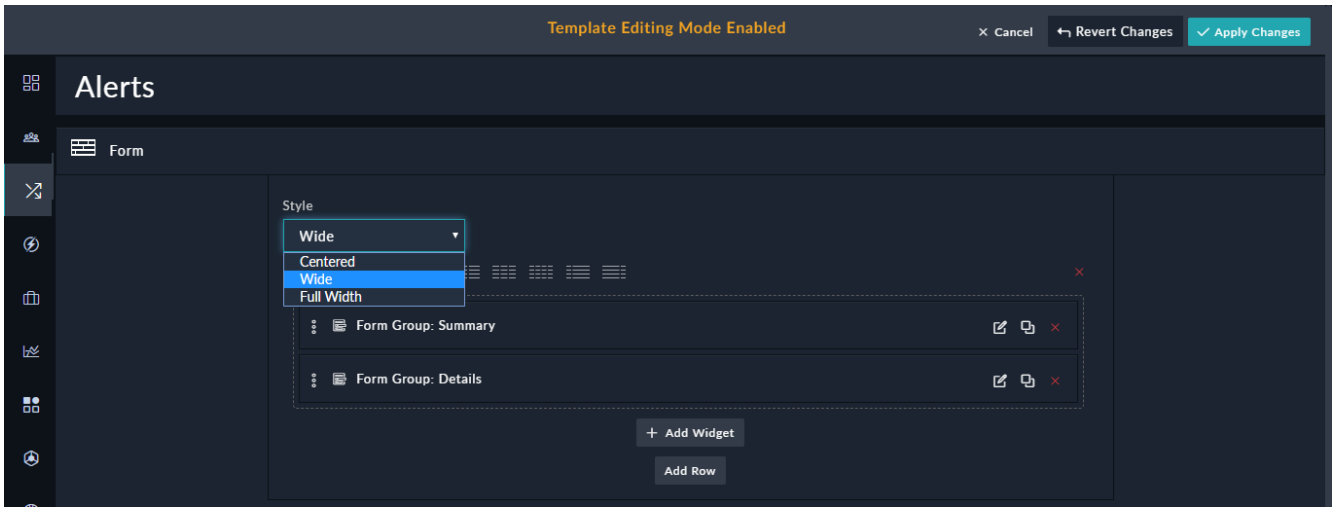
List views can have associated charts, lists, or other widgets contained on their pages. See the Using Template Widgets section for more information on configuring each widget.

When you create a new Module, using the Application Editor, the default List view is applied, which is a single grid displaying all records for the Module.

Form Views

The Form view is the displayed interface for an individual record in a form view. This view is generally used when you want to add a record manually or if you want to edit a complete record.

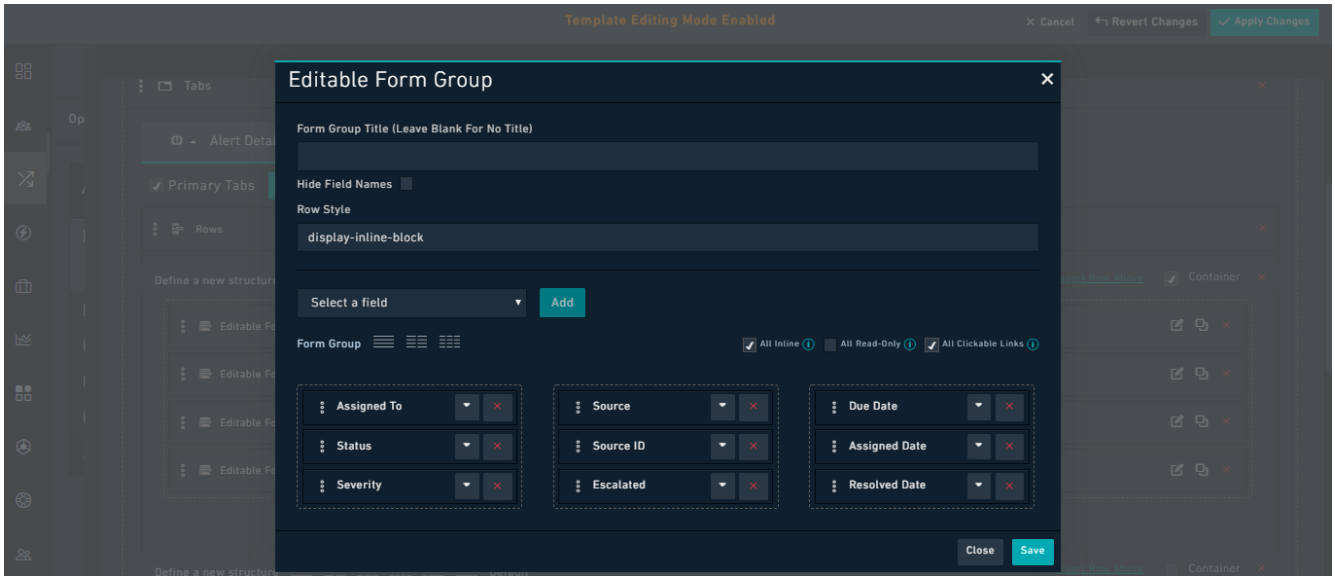
You can assign a style to "Forms" to make them wider or narrower as per your requirements as shown in the following image:



You can choose between the following styles:

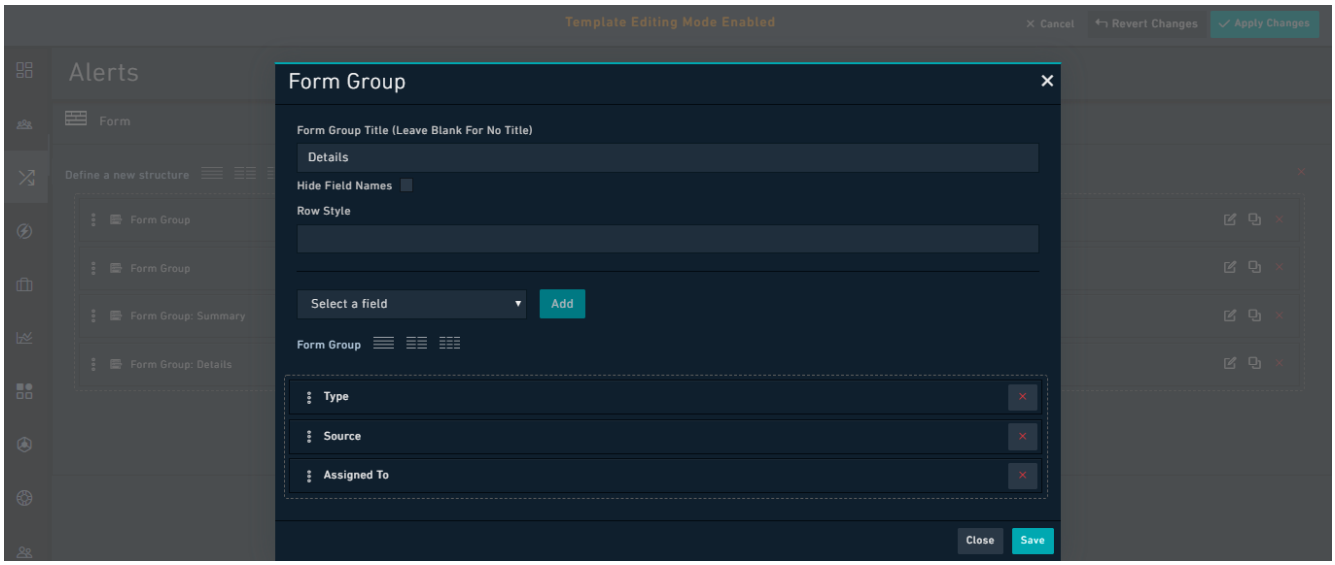
- **Centered**: Using "Centered" makes the add/edit record forms centered on the page. The fields, in this case, appear in a narrow-centered column.
- **Wide**: Using "Wide" increases the width of the fields within the add/edit record forms when compared to the width of the fields using the "Centered" style.
- **Full Width**: Using "Full Width" increases the width of the fields within the add/edit record forms to cover the complete page.

Editable Form Group widget: Forms display editable forms for an individual record, in its detail view, in a module. The form view defines what information users require to add while creating a record. You can modify the form view of each module independently of other modules.

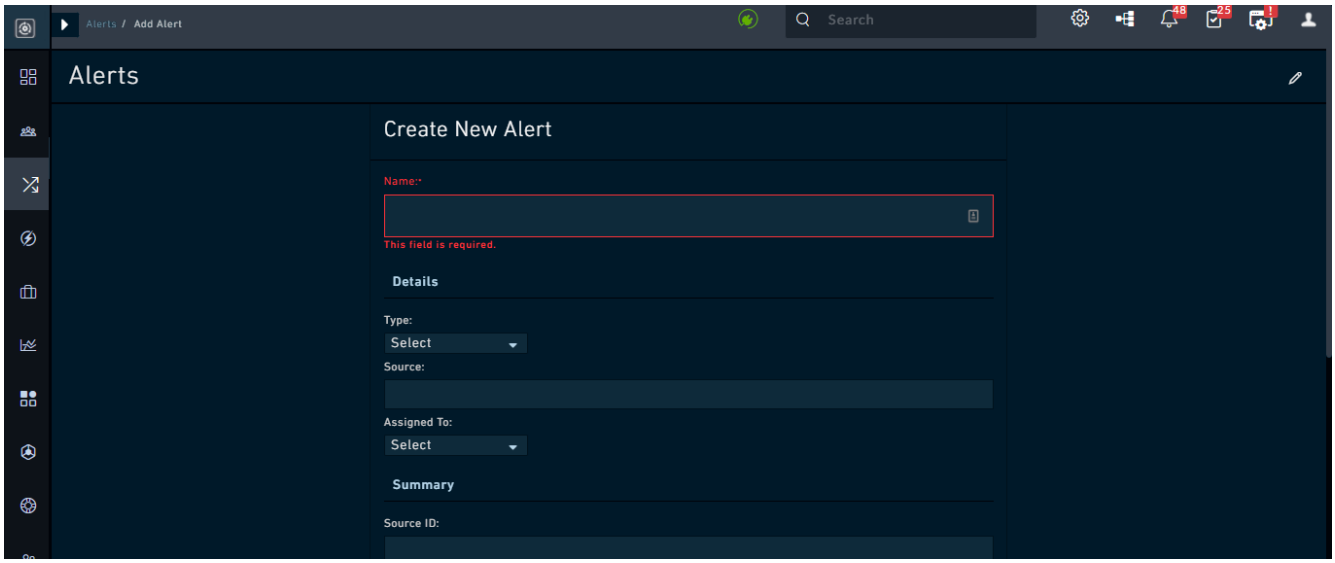


The following image illustrates how the Editable Form Group widget is displayed in the detail view of the Alerts module:

Form Group widget: Use this widget to insert a group of form fields as part of a form. You can use this widget to create a form that users can use to fill in the details for a record.



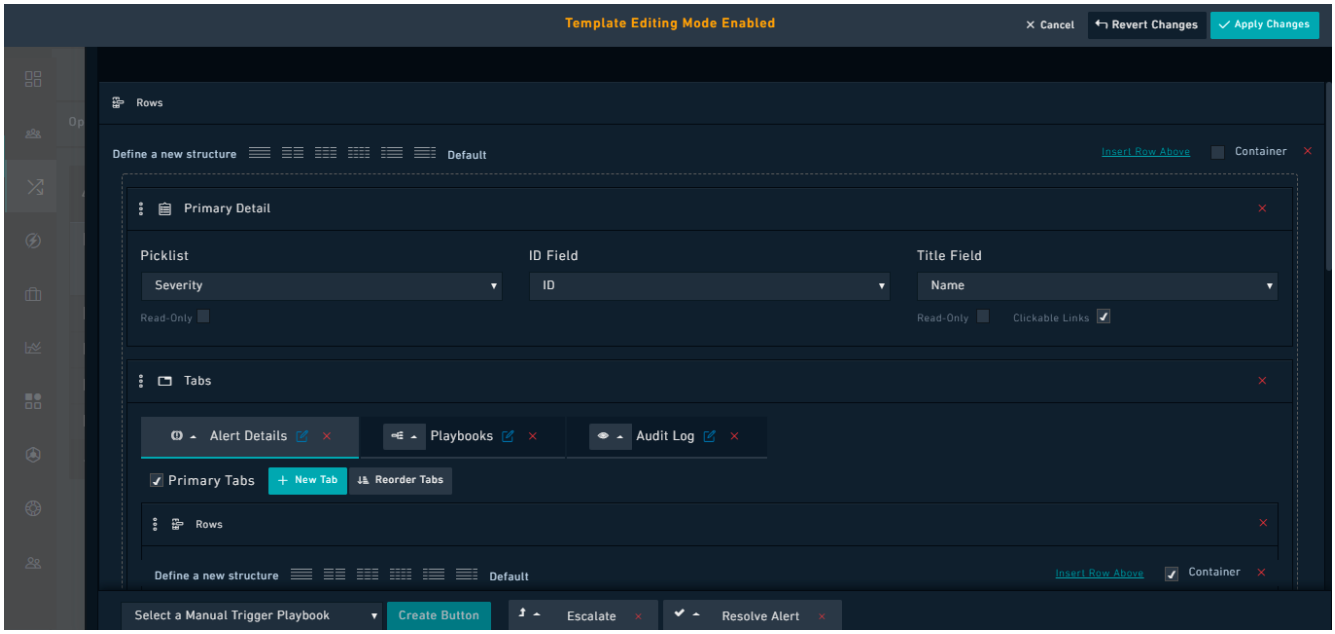
The following image illustrates how the Form Group widget is displayed in the Form view of the Alerts module:



Detail Views

The Detail view is the displayed interface for an individual record in a module. When you click an individual record, FortiSOAR displays the detail view of that record.

You can modify the detail view of each module independently of other modules.

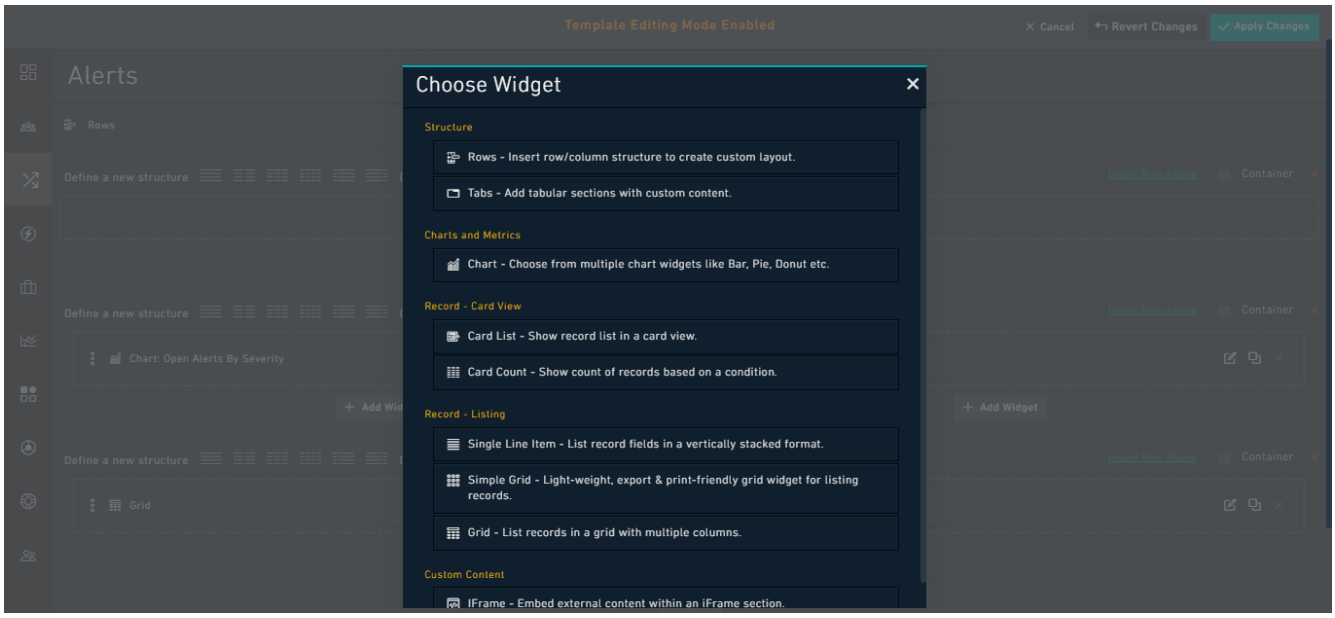


Using Template Widgets

Use widgets to render information for the visual display inside View Template. The View Template contains embedded configuration information about the widget and configures the widget location relative to the screen.

The `People`, `System Assigned Queues`, and `Approval` modules are not part of dashboard widgets since these are system modules and used for administration purposes.

Widgets have been categorized as per its usage, as shown in the following image:



For example, Rows and Tabs are categorized as structure widgets, and Single Line Item, Simple Grid, and Grids are listed as Record - Listing widgets.

Widget types vary such that specific widgets only correspond to certain view types.

Some widgets are common to all types of view such as:

- Rows
- Tabs
- Simple Grid
- Grid
- Richtext Content

Some widgets are common to more than one type of view such as, the following widgets are common to Dashboard and Grid views:

- Chart
- Card List
- Card Count
- Single Line Item
- iFrame

Some widgets are common to more than one type of view, such as, the following widgets are common to Dashboard and Detail views:

- Summary

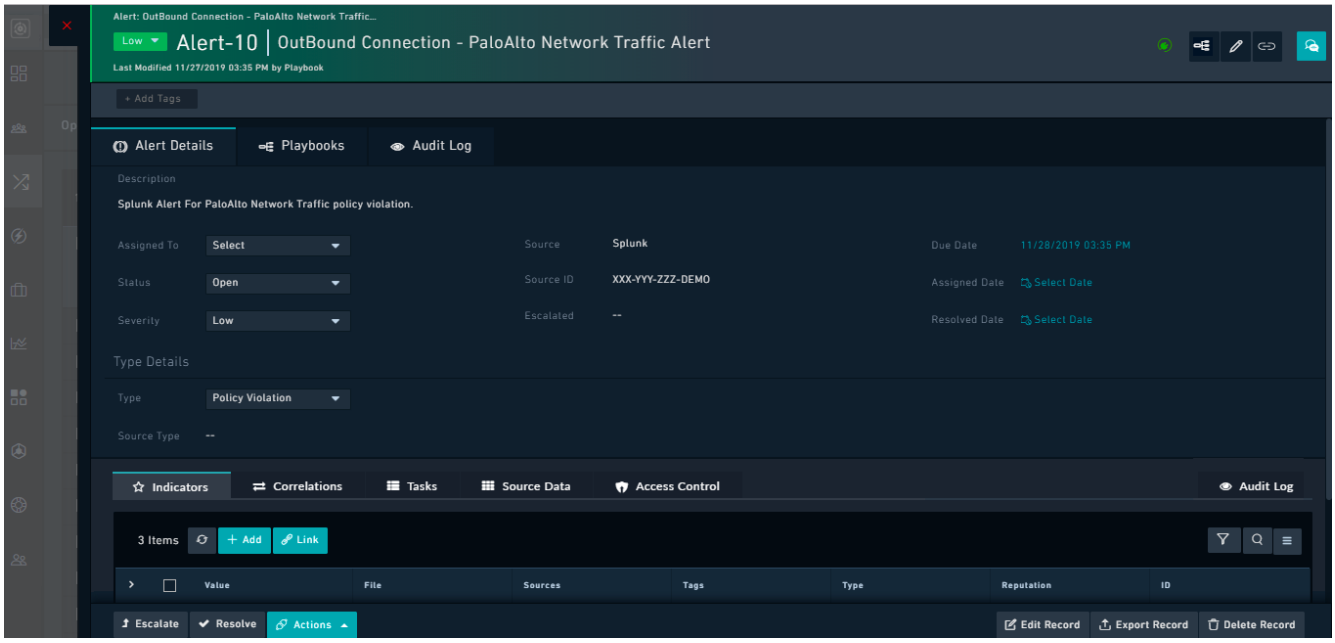
Dashboard views have some exclusive widgets, such as:

- Relationship count
- System Monitoring
- Connector Health
- Performance Metrics

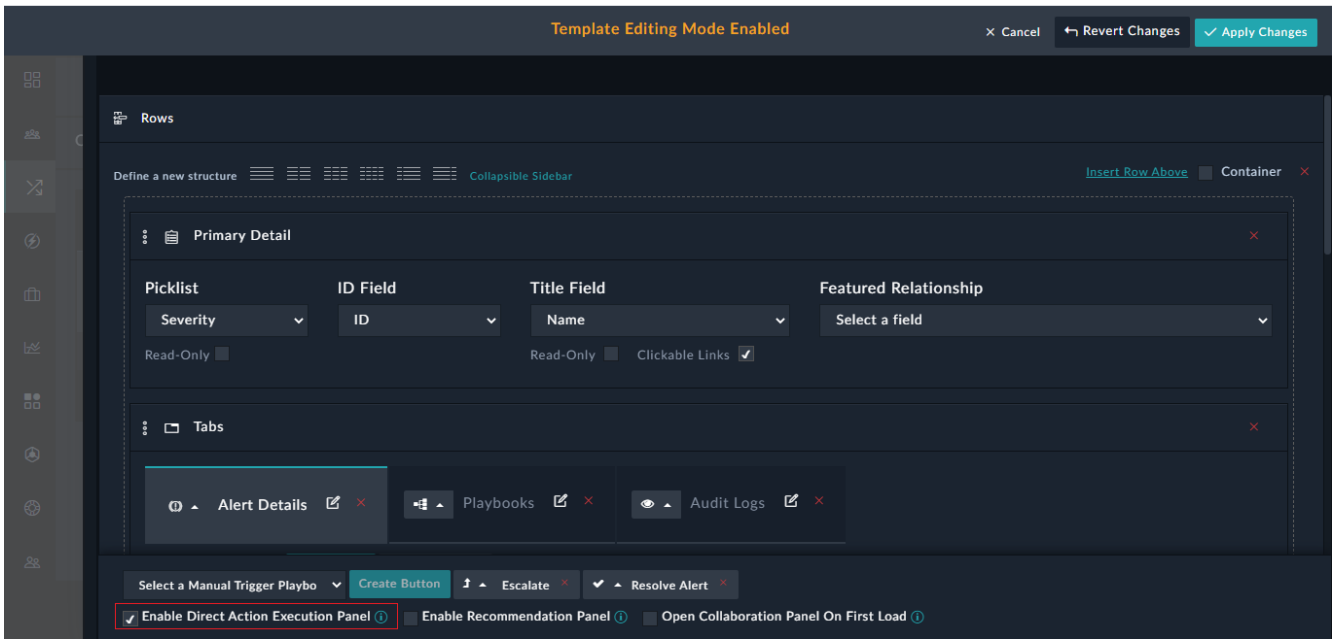
Detail views have some exclusive widgets, such as:

- Editable Form
- Editable Form Group
- Uncategorized fields
- Primary Detail
- Record Type
- Relationships
- Relationships Single Line Card
- Comments
- Visual Correlations
- File Upload
- Timeline
- Executed Playbooks

In the List and Detail views, you can create buttons for commonly used actions by selecting a manual trigger playbook from the **Select a Manual Trigger Playbook** list and click **Create Button**. For details on how to create buttons in the List view, see the Grid section. In a similar way, you can also add action buttons, such as, **Escalate** and **Resolve**, in the footer section of the detail view of a record as shown in the following image:



In the above image, you can also see the **Actions** button, using which users can directly execute connector actions on the record. You can stop the users from directly executing connector actions by clearing the **Enable Direct Action Execution Panel** checkbox (this is checked by default) in the detail view template:



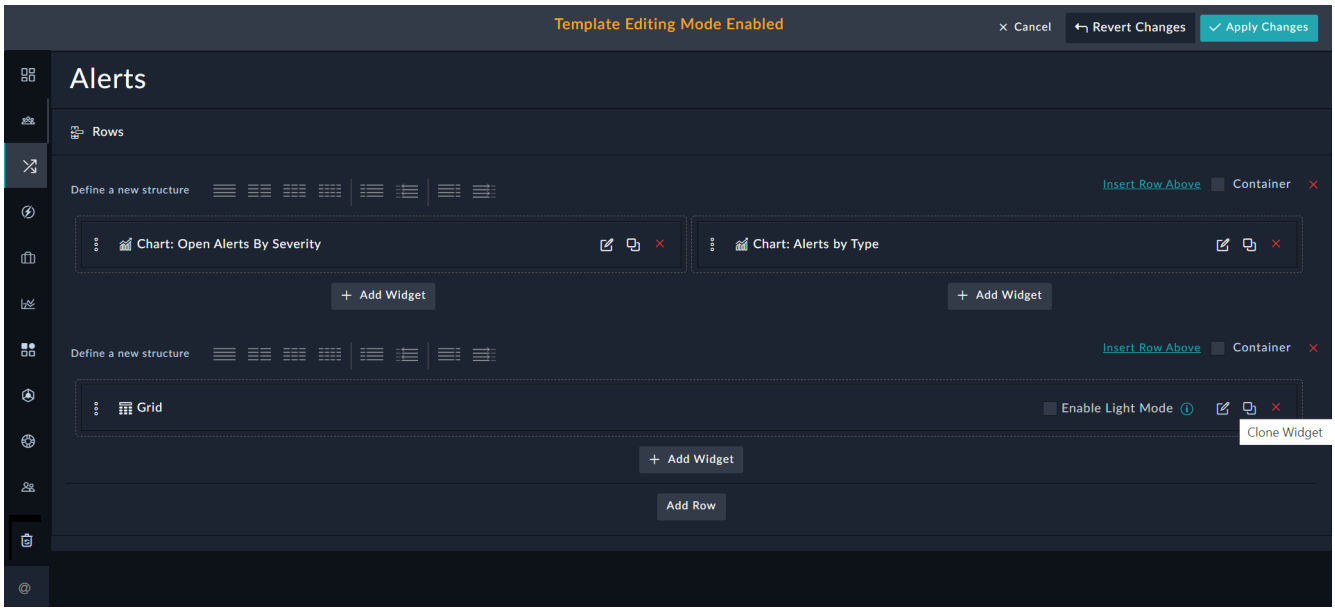
Clearing the **Enable Direct Action Execution Panel** checkbox will remove the Actions button from the detail view of the record.

Clicking the **Enable Recommendation Panel** checkbox (it is cleared by default), enables the **Recommendations** tab, by default, ie., it configures *Similar Records* and *Fields Suggestions* with default criteria, in the **Workspace** panel. For more information on the Recommendations Panel, see the Working with Modules - Alerts & Incidents chapter.

Clicking the **Open Collaboration Panel On First Load** checkbox (it is cleared by default), ensures that on the first load of this module's record the collaboration panel is opened and expanded by default. Subsequent expansion/collapse is determined by the last state of the panel, maintained by each user.

You can perform the following actions while working with Widgets, such as Editable Form Groups, Charts, or Grids:

- Edit Widgets: Click the **Edit Widget** icon to change the fields within the widget or to change the properties of the widget.
- Clone Widgets: Click the **Clone Widget** icon in the row of the widget you want to clone to clone the all the fields and properties of that widget.
- Remove Widget: Click the **Remove Widget** icon to remove the widget.



You can use some common components, such as filter and sort options, and also control the behavior and display of fields across widgets, to create templates and dashboards suit your requirements. For more information, see Common components within Widgets and Display Elements.

Structure

Rows

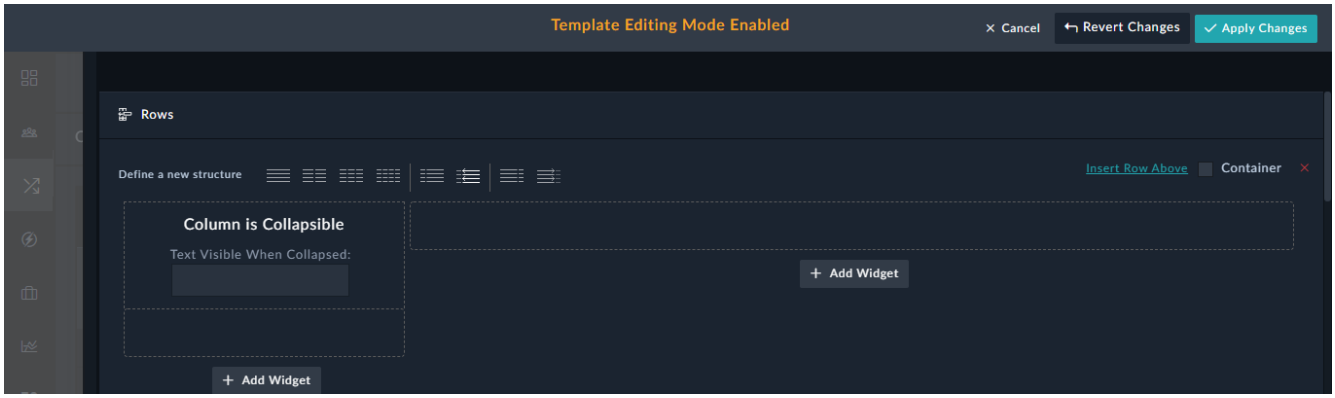
Rows are the foundation widget for organizing a View Template. Rows are the highest-level widget, meaning all View Templates start with a Row. You can nest subsequent Row widgets within the following rows.

Row Layout

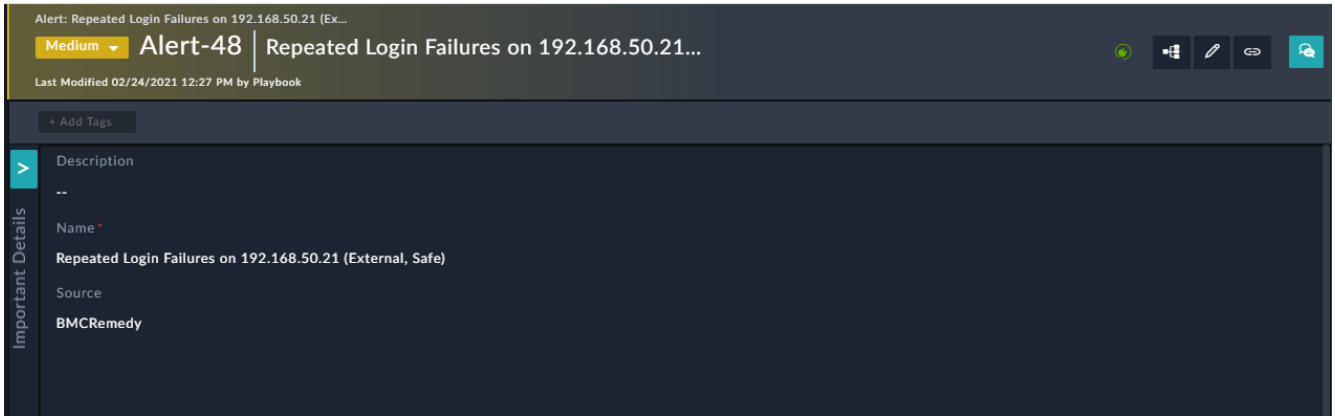
Row widgets have different column layout and width options, such as single-column structure, three-column structure, structures with left or right sidebars etc. You can use any of these options to determine the layout of the row for subsequent widgets, even other rows.

Responsive behavior is built into row layout based on the bootstrap foundation. We recommend viewing the rendered View Template layout across different resolutions after completing to view the behavior corresponds to a desirable method of handling lower resolutions.

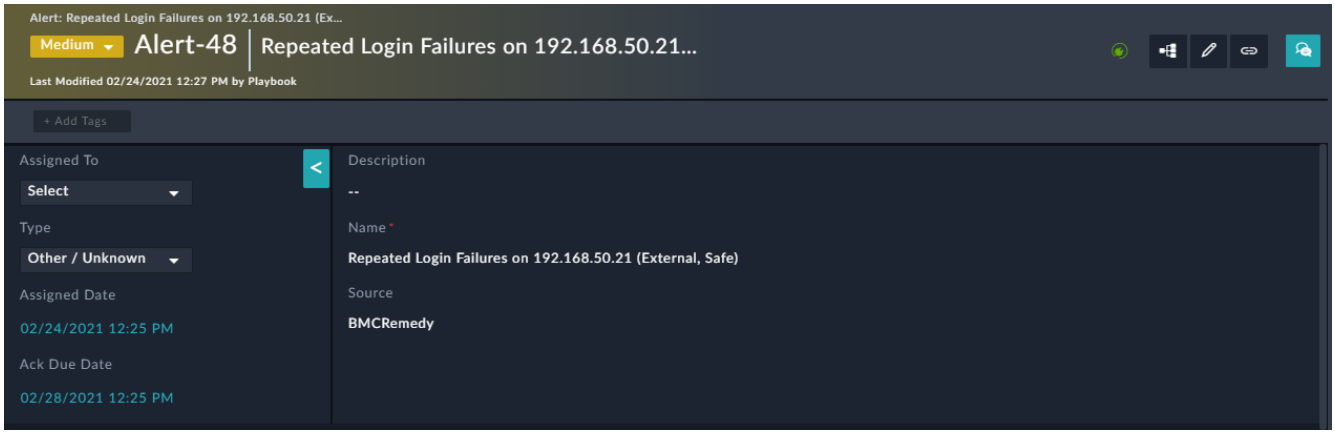
Version 7.0.0 introduces the left-hand or right-hand side "Collapsible Sidebar". Using Collapsible Sidebars, you can expand or collapse the available sidebar space and optimize the available space:



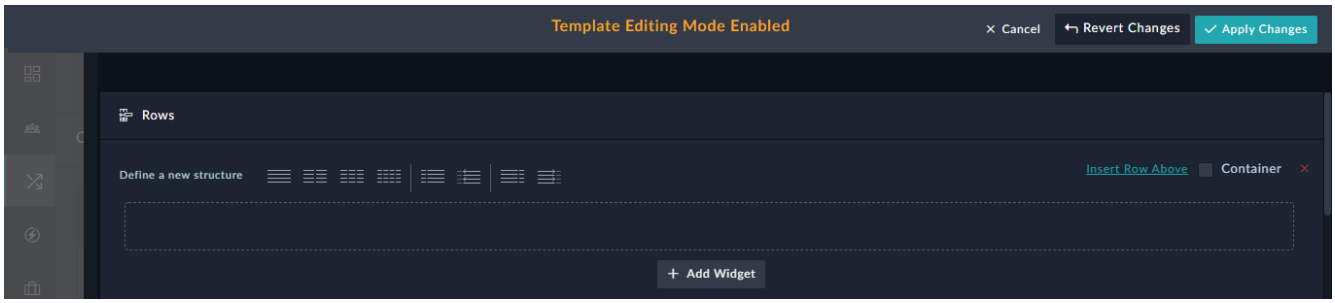
You can enter text that will be visible when the sidebar is collapsed in the **Text Visible When Collapsed** field, For example, his row will appear with the collapsed sidebar in the detail view as follows:



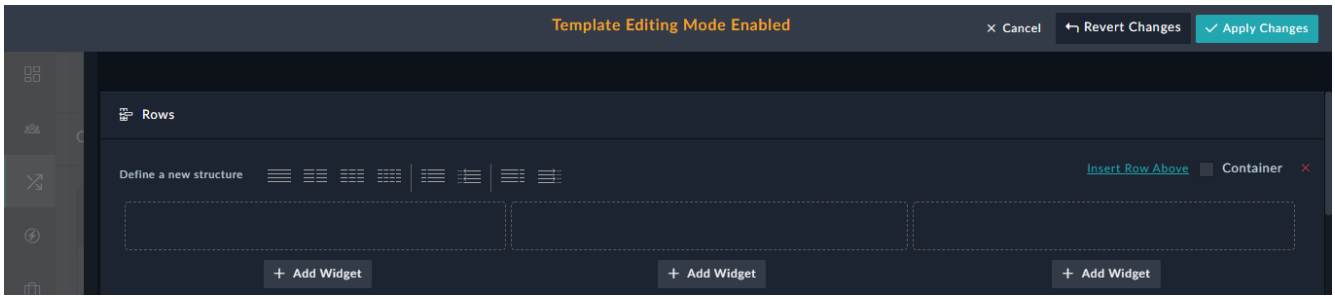
This row will appear with the expanded sidebar in the detail view as follows:



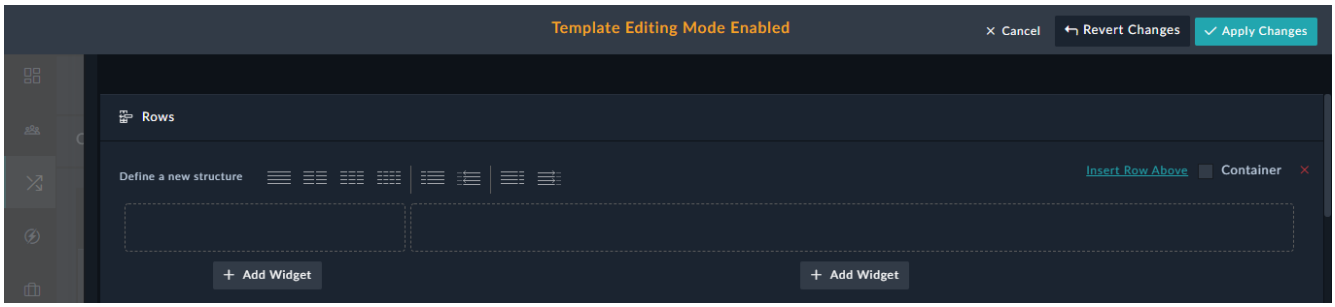
Following are some more examples of row layouts, such as a row layout with a single-column structure:



Row layout with a three-column structure:

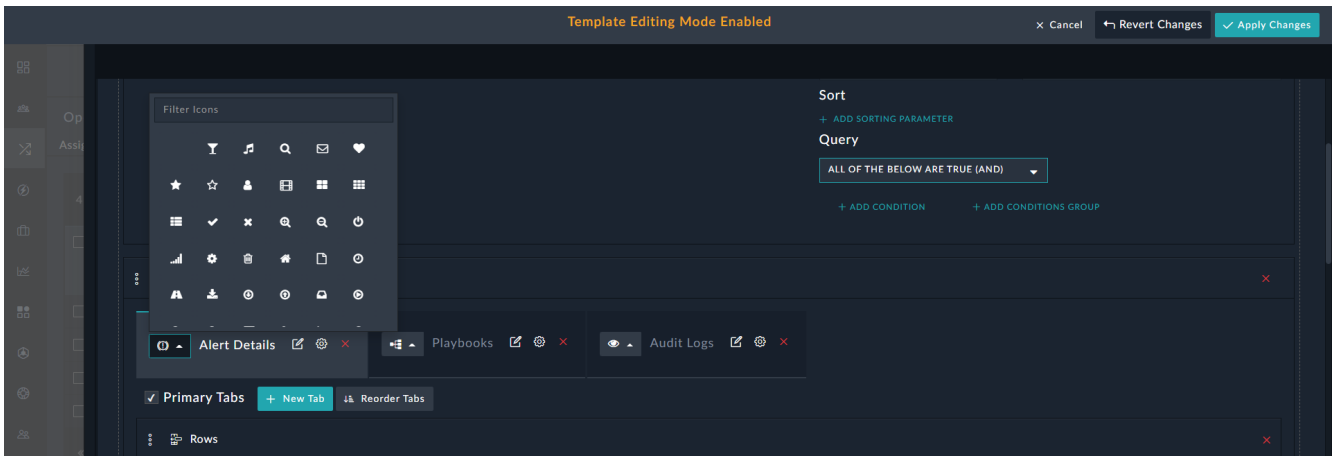


Row layout with a left-hand side static sidebar:

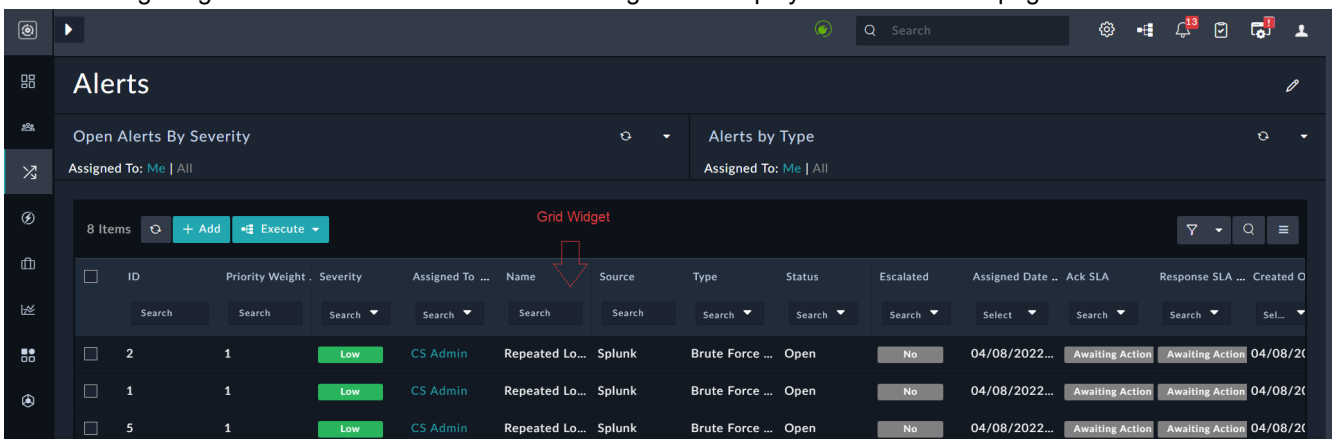


Tabs

Tabs allow for the placement of multiple widgets, including rows, charts, executed playbook logs, etc. Using tabs helps you organize and categorize dashboards and present different types of information on a single page.

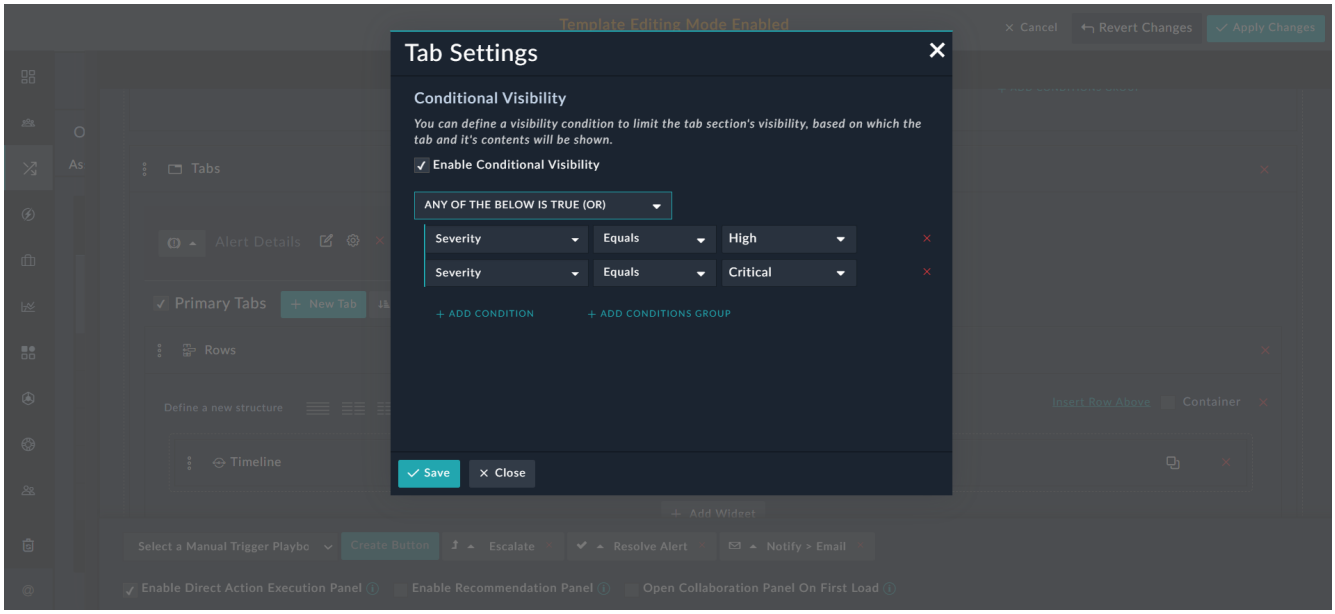


The following images illustrate how the Tab and Grid widgets are displayed on the module page:

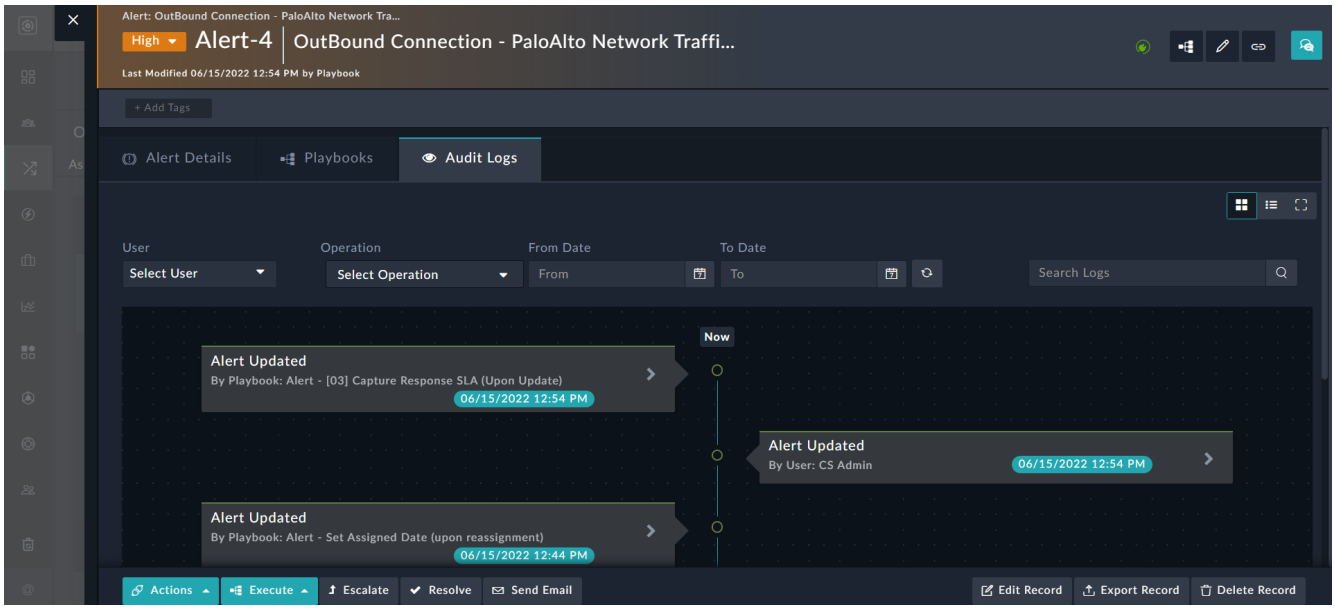


Click **New Tab** to add a tab and enter the tab title in the **Enter tab title** field, and click the green checkbox. Select the **Primary Tabs** option to mark the tab as a primary tab, which then allows you to add a title in the **Enter tab title** and subtitle or description to the tabs in the **Enter tab sub-title** field. If a tab is not a primary tab then you can enter only the title of the tab. You can add icons to your tab titles and filter icons based on icon names as shown in the above image.

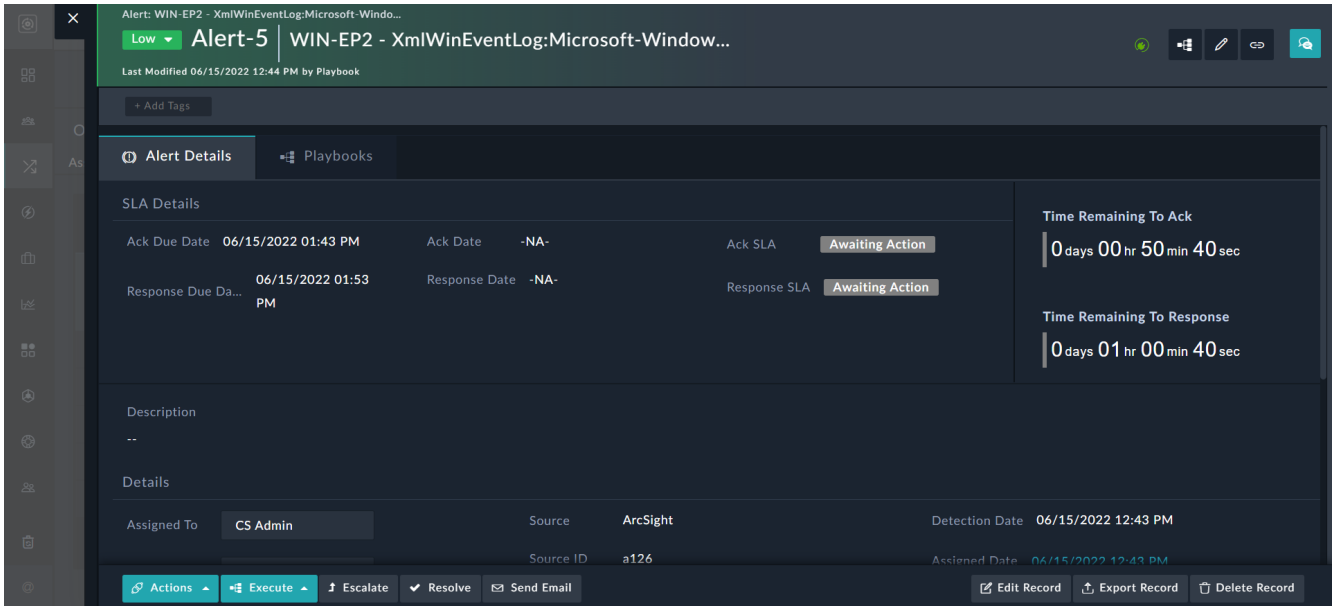
To render tabs based on specified visibility conditions, click the **Settings** icon. For example, if you want alerts to display the 'Audit Log' tab only if the status of the alert is set to 'High' or 'Critical', click the **Settings** icon on the **Audit Log** tab, to display the **Tab Settings** dialog. Select the **Enable Conditional Visibility** option, and then define the condition as '`Severity Equals High`' or '`Severity Equals Critical`' and click **Save**:



Now, the 'Audit Log' tab is visible only if the severity of the alert is high or critical:

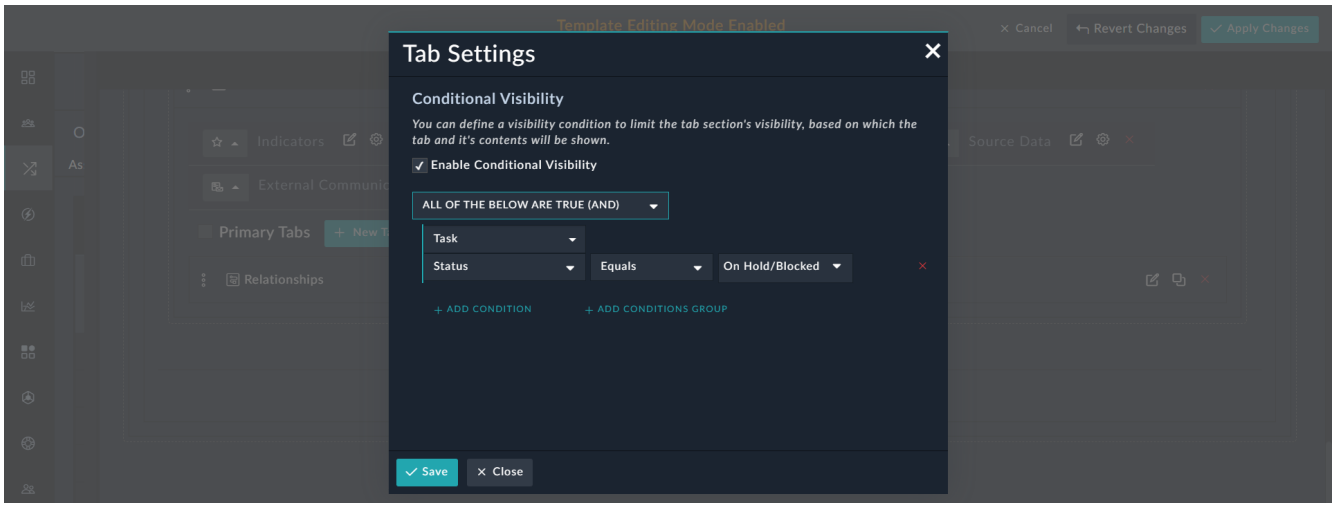


If the severity of the alert is not high or critical, then the 'Audit Log' tab is not visible:



Tabs can also be rendered based on visibility conditions that are specified on relational fields. For example, if you want alerts to display the 'Tasks' tab only if the status of the task is set to 'On Hold/Blocked', click the **Settings** icon on the **Tasks** tab, to display the **Tab Settings** dialog. Select the **Enable Conditional Visibility** option, and then select **Task**, which is part of the Related Modules section and then define the condition as 'Severity Equals On Hold/Blocked' and

click **Save**:



Now, the 'Task' tab is visible on alerts only when the status of the tasks linked to the alerts is set to On Hold/Blocked.

Charts and Metrics

Chart

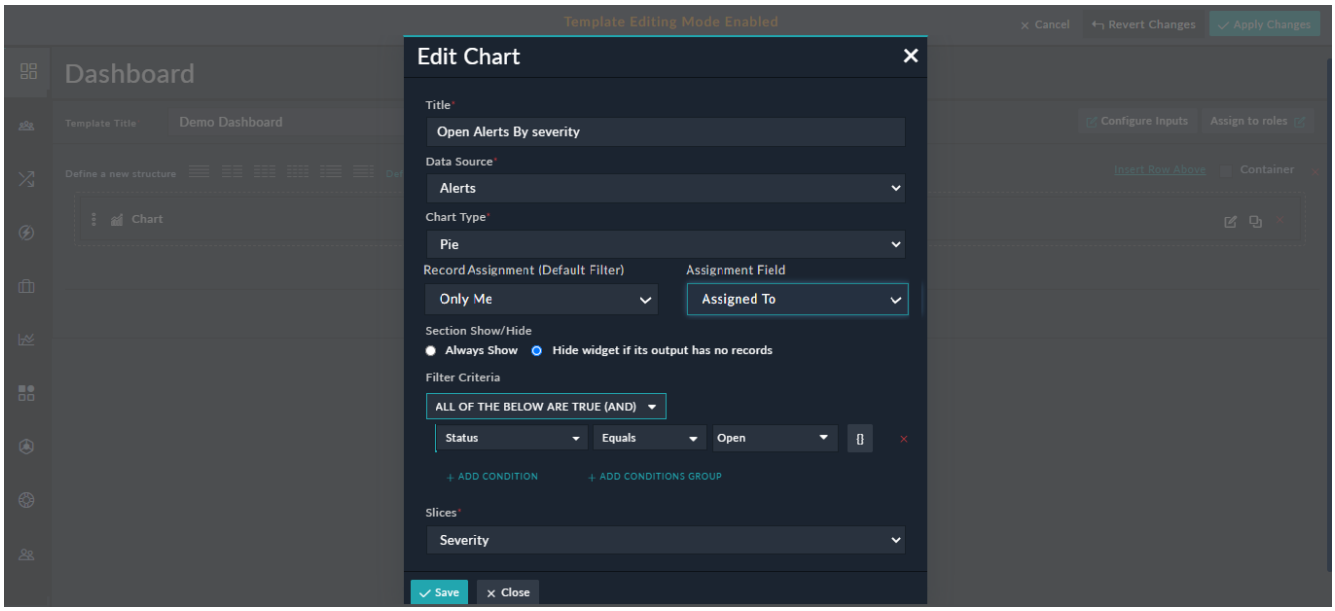
You can represent data using different types of charts, which are Pie, Donut, Average Area, Bar, Timeseries, and Line charts. Each of these types of charts has separate data requirements.

A bar chart or bar graph is a chart or graph that presents categorical data with rectangular bars with heights or lengths proportional to the values that they represent. The bars can be plotted **Vertically** or **Horizontally**. The **Bar** chart widget also allows you to choose all types of fields such as `lookup`, or `text`, for both **Categories** and **Values** Axis, enabling you to be able to display data such as displaying resolved incidents per analyst.

You can select the **Record Assignment (Default Filter)** as **Only Me** or **All**. If you select **Only Me**, then from the **Assignment Field** drop-down list, you must select the assignment on the basis of which you want to filter the dashboard view.

You can choose to either always display the chart or to display the chart only if there is at least one record present in the selected module. This option to show/hide charts is present in the all types of chart widgets in the `Section Show/Hide` section, select the **Always Show** option (default) to always display the chart or select the **Hide widget if its output has no records** option to display the chart only if there is at least one record present in the selected module.

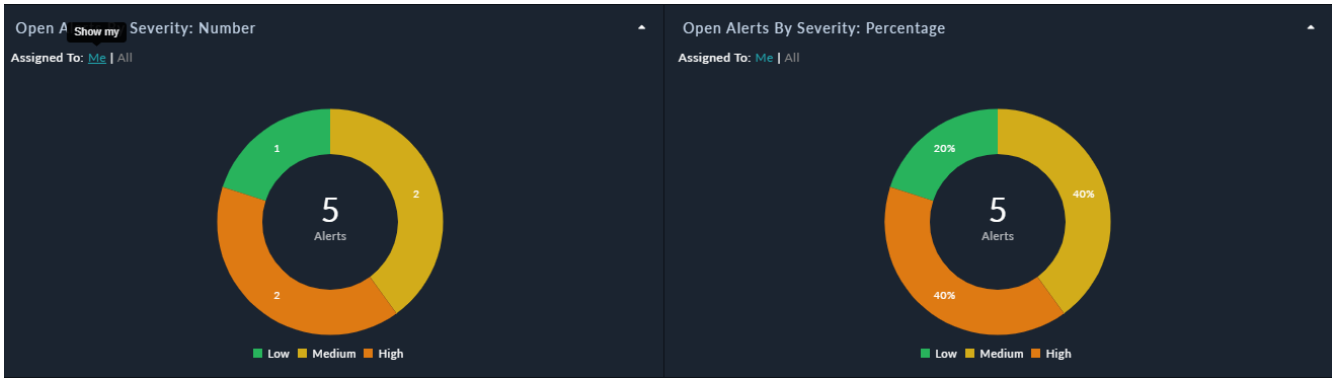
Charts leverage picklist values for discrete representations of color. If you have defined colors for the picklist values, then those values are used. Otherwise, the system automatically colors the values with a standard color palette to preserve visual continuity.



You can click on each section of the chart, for example, slices in a pie chart, and open the corresponding records in the grid view.

A **Donut** chart is a unique type of pie chart with an area of the center cut out. You can use the center of the Donut chart to display information inside the same, making the Donut chart more space efficient. In the case of FortiSOAR, the center area of the Donut chart displays the total number of filtered records present in the selected module or the total number of records present in the selected module (if no filter is applied). For example, if you want to display Alert records whose severity is not critical in a Donut chart, then the center of the donut chart will display the total number of alert records, which are of High, Medium, Low, or Minimal criticality, and the slices of the Donut chart will display the percentages or actual number of the alert records based on severity. If there are a total of 6 alert records, out of which 1 is critical, 2 are high, 2 are medium, and 1 is low, then the center of the donut chart will display 5 alerts, and the slices with discrete colors for severity will display percentages, e.g., 20% in orange for High alerts, 40% in yellow for Medium alerts, and 40% in green for Low alerts. You can also choose to display actual count of records instead of the percentages, by clicking the **Show Actual Number** checkbox in the `Edit Chart` dialog.

The following image illustrates how the Donut chart is displayed on the `Dashboards` page, both with numbers and with percentages, in the dashboard or specific page, after you have selected **Assigned To** in the **Only Me | All (field)** drop-down list:

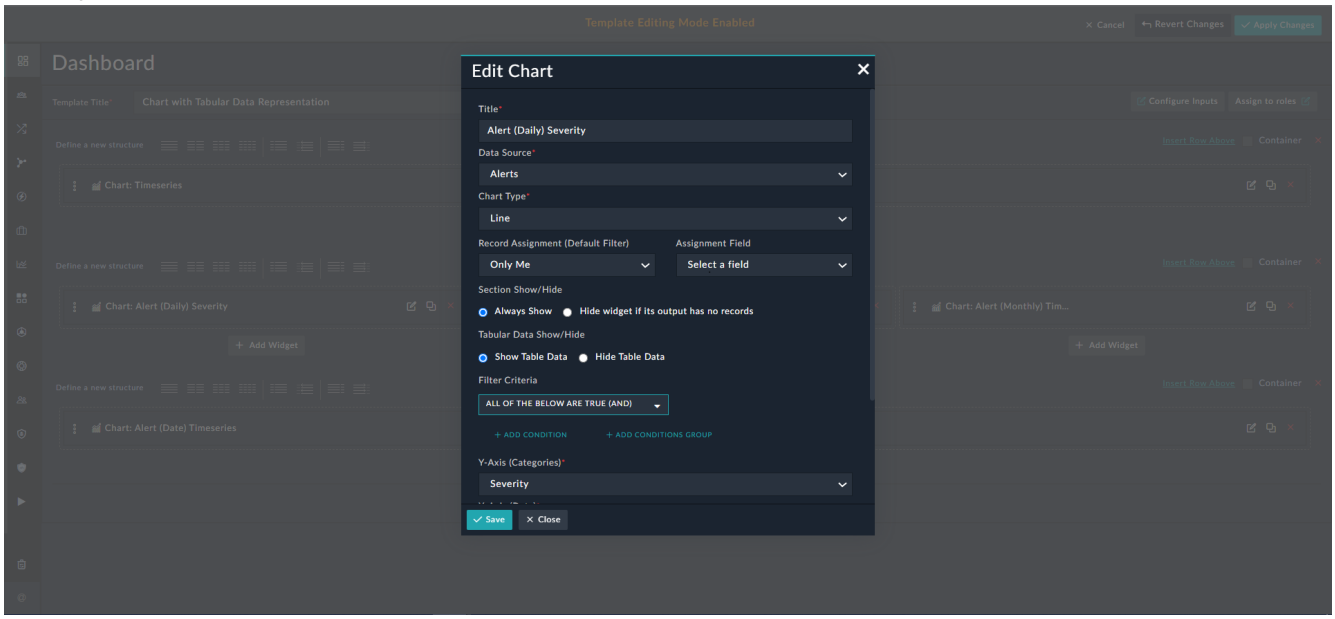


Use the Only Me | All (field) filter, i.e., to toggle the view on dashboards or modules based on this filter, and the Nested Filters components are applicable to Card List widget.

The **Only Me | All** filter is not applicable to Reports, i.e., on the `Reports` page, you cannot toggle the view based on this filter, instead, you must change this in the report template itself when you are adding or editing the Card List widget.

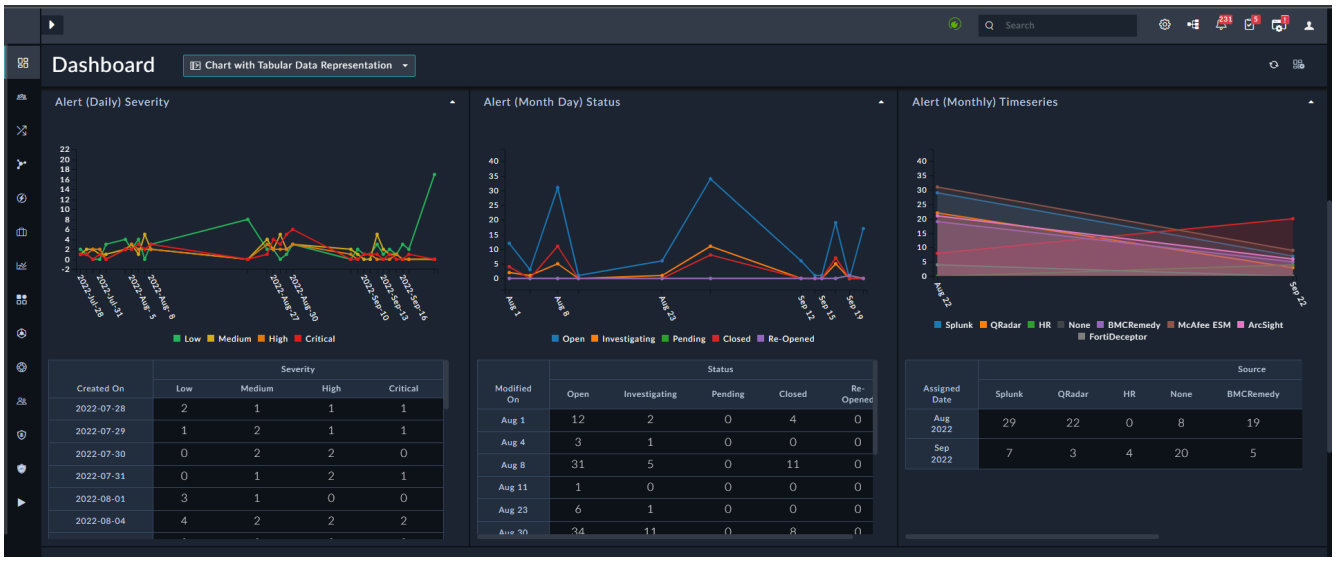
A **Line** chart displays quantitative values over a continuous interval or period. Use a line chart to show trends and analyze how the data has changed over time. You can group data by both picklist and non-picklist values, including integers as well as other field types (except Many to One and Many to Many) in the Y-Axis (categories) drop-down for line as well as 'Timeseries' charts.

A **Timeseries** chart is a line chart of repeated measurements taken over regular time intervals. In the case of the timeseries chart, time is always shown on the horizontal axis, with data points drawn at regular intervals. The timeseries charts help to show trends or patterns. In FortiSOAR release 7.3.0, the 'Line' and 'Timeseries' charts have been enhanced to provide you with a choice of viewing the 'Line' and 'Timeseries' data in a tabular format. Having the data represented in the tabular format helps you to view the varied information in one go without having to hover on the line or timeseries chart.
To view the data of the line or timeseries chart in the tabular format, in the `Edit Chart` dialog, select the **Show Table Data** option and click **Save**.



The following image illustrates how the Timeseries charts are displayed on the `Dashboards` page when you select the 'Show Table Data' option. As you can see in the image, the data gets displayed both as a line graph and in the tabular

format:



Created On	Severity			
	Low	Medium	High	Critical
2022-07-28	2	1	1	1
2022-07-29	1	2	1	1
2022-07-30	0	2	2	0
2022-07-31	0	1	2	1
2022-08-01	3	1	0	0
2022-08-04	4	2	2	2

Modified On	Status				
	Open	Investigating	Pending	Closed	Re-Opened
Aug 1	12	2	0	4	0
Aug 4	3	1	0	0	0
Aug 8	31	5	0	11	0
Aug 11	1	0	0	0	0
Aug 23	6	1	0	0	0
Aug 30	34	11	0	8	0

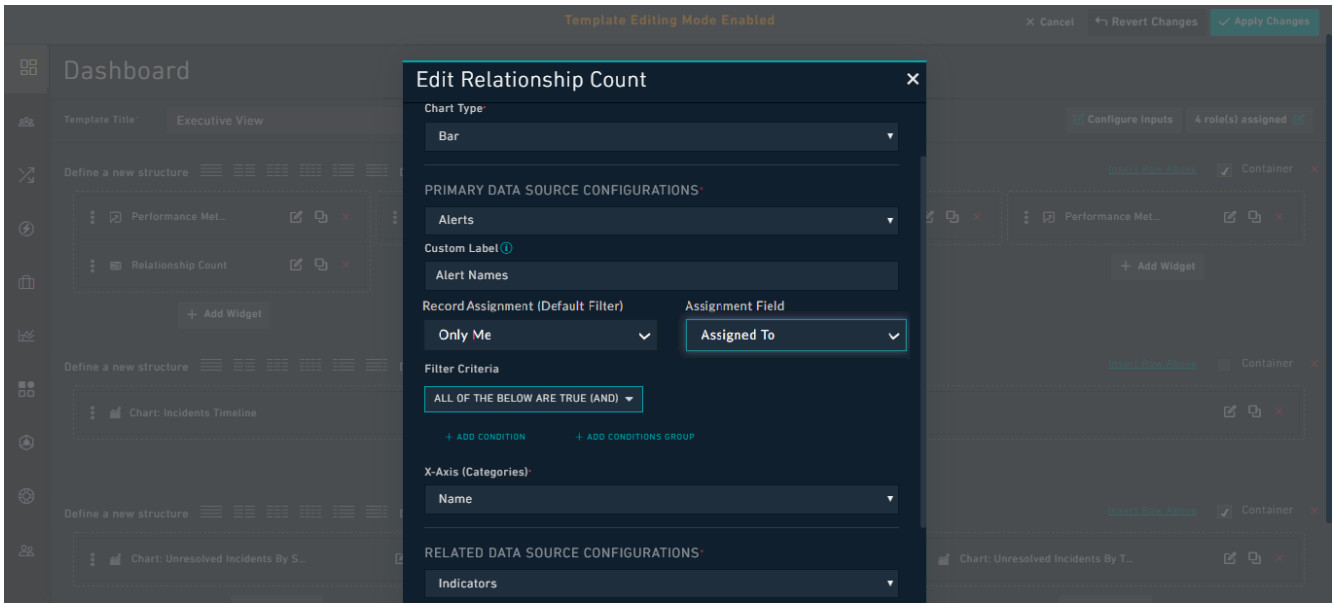
Assigned Date	Source				
	Splunk	QRadar	HR	None	BMCRemedy
Aug 2022	29	22	0	8	19
Sep 2022	7	3	4	20	5

The line graph and the table displayed on a 'Dashboard' are of equal height. If there is a considerable amount of data, then the table on the 'Dashboard' appears with scroll bars. However, line graphs and the tables displayed in a 'Report' are dependent on the amount of data presented. Since 'Reports' cannot have a scroll bar, the table following the line graph displays all the content in a single view.

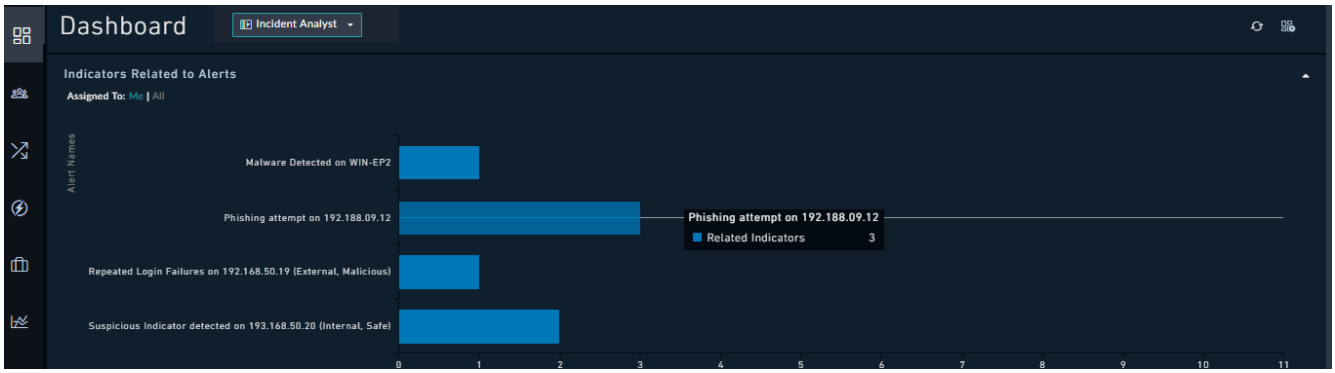
Relationship Count

The Relationship Count chart is a type of bar chart that displays the count of related data records. For example, this widget can display how many indicators are related to alerts.

To configure a Relationship Count widget that will display indicators related to alerts do the following: Edit the Dashboard and select the **Relationship Count** widget. Add the title of the chart and select the **Chart Type** as **Bar**. Then, select Alerts as the data source in the `Primary Data Source Configurations` section. You can also specify a label that will be displayed on the Y axis against the primary data source, in the **Custom Label** field. For our example, type `Alert Names`.
You can select the **Record Assignment (Default Filter)** as **Only Me** or **All**. If you select **Only Me**, then from the **Assignment Field** drop-down list, you must select the assignment on the basis of which you want to filter the dashboard view.
In the **Y-Axis (Categories)** field, choose the field that you want to display on the axis of the bar chart, for example **Name**. Then select the related data source as **Indicators** in the `Related Data Source Configurations` section. You can also specify a label that will be displayed on the X axis against the related data source, in the **Custom Label** field. For our example, type `Related Indicators`. You can define filters for each data source, for example you can filter indicators based on the type of the indicator.



The following image displays the relationship count that displays the indicators related to alerts:



Use the Only Me | All (field) filter, i.e., to toggle the view on dashboards or modules based on this filter. The Nested Filters component is also applicable to Card List widget.

The **Only Me | All** filter is not applicable to Reports, i.e., on the `Reports` page, you cannot toggle the view based on this filter, instead, you must change this in the report template itself when you are adding or editing the Card List widget.

Performance Metrics

Use the Performance Metrics widget to measure efficiencies that security operations gain by using automated workflows and playbooks present in FortiSOAR. The Performance widget is present in the **Dashboard** and **Reports** templates.

The following types of metrics are available in the Performance Metrics widget:

- **ROI**: Displays the return on investment that you gain by using FortiSOAR automation for a specified time period.
- **Playbook Action Count**: Displays the number of playbook steps executed for a specified time period.
- **Time To X**: Displays the Mean, Maximum, or Minimum Time To Restore (MTTR) or the Mean, Maximum, or Minimum Time To Detect (MTTD) taken for a particular activity. For example, you can find out the Mean Time to

Resolution (MTTR) which is the difference between incident creation and incident resolution or MTTD which is incident discovery and incident creation.

- **Aggregate Functions**: Displays the minimum, maximum, mean, median, or sum of record fields (integer or float), for a single record or two records.
- **Ratio**: Displays the relationship between two values. For example, the ratio between the number of alerts escalated to incidents versus the total number of alerts created for a specified time period.
- **Total Count**: Displays the number of records of a specific type on which a specific action is performed for a specified number of days. For example, display the number of escalated alerts for a specified time period.

ROI

Use the ROI widget to display the return on investment or time saved by using FortiSOAR automation, based on the parameters you specify. You need to specify the following parameters:

Title: Title of the ROI widget. For example, `ROI for checking IP reputation`.

Show ROI Measured As: Choose between **Dollar Savings** or **Time Savings**. If you choose **Dollar Savings**, then you have to specify the additional parameter of **$ Value Of Each Hour Of Analyst**: Average cost in dollars that your organization bears for an analyst per hour. For example, `50`. The remaining parameters are the same for both methods of ROI measurements.

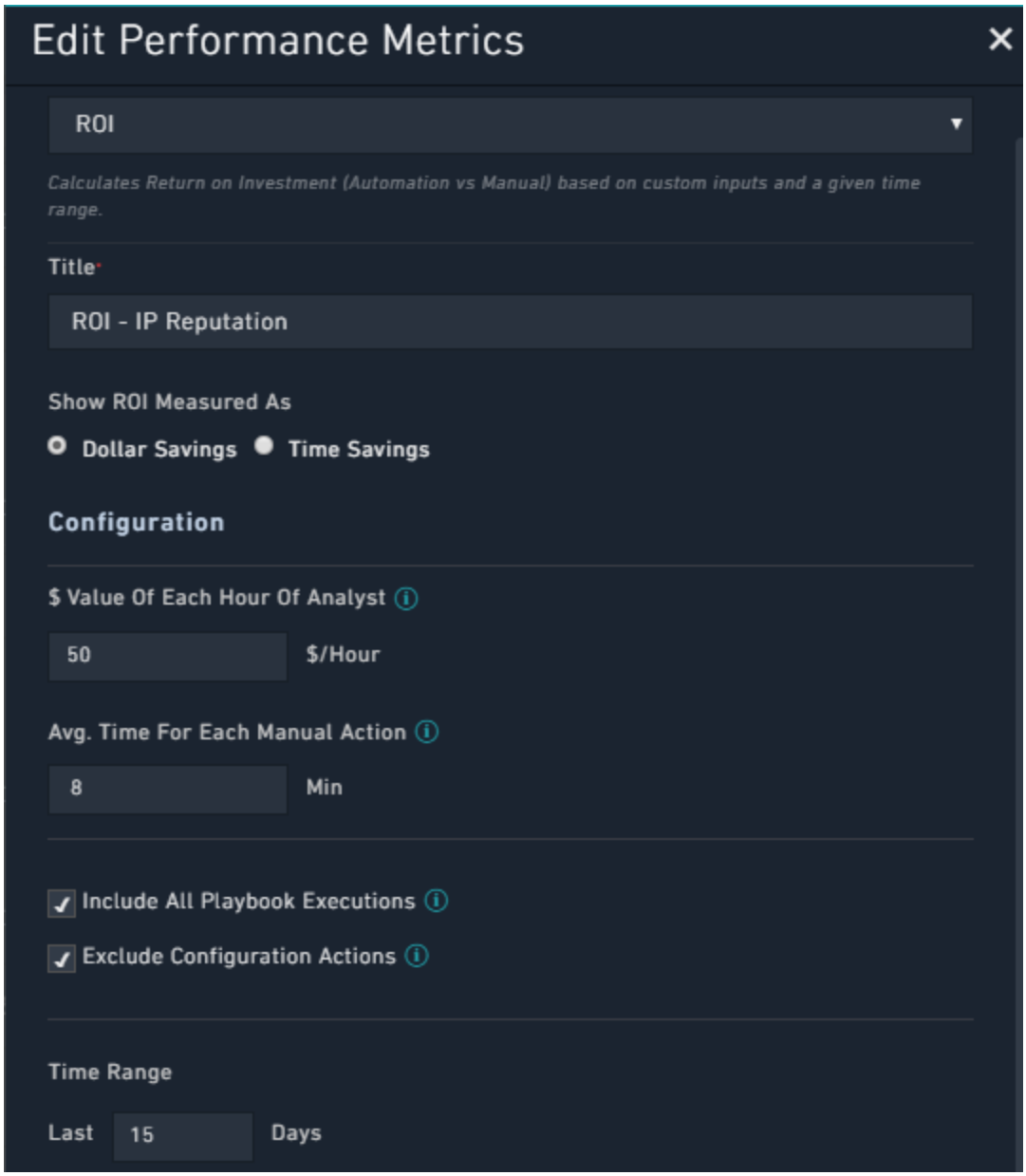
Avg. Time For Each Manual Action: Average time, in minutes, that it takes for an analyst to execute one security investigation action. For example, to check the reputation of IP address in an online tool, such as VirusTotal. For example, `8` minutes.

Include All Playbook Executions: Select this checkbox to determine whether you want to include both the failed and successful playbook executions (this is the default). Clear this checkbox to include only successful playbook executions. This is common parameter across Performance Widgets.

Exclude Configuration Actions: Excludes playbook steps that are used for configuration and which do not add any business value, such as the trigger steps (start), the set variable step, and the steps that are waiting for a decision or approval (this is the default). Clear this checkbox to include all playbook steps. This is a common parameter across Performance Widgets.

Time Range: Specify the time, in days, for which you want to see the ROI. For example, `15` days.

Show Percentage Change: Select this checkbox to show the percentage difference in ROI value between the current ROI value and the previous ROI value for same time span (this is the default). For example, if you have chosen 4 days as the time range, then this will show the percentage difference between the ROI value for the last 4 days compared (example from the 1st to the 4th of June) with the ROI value for the 4 days before this time span (example 28th to 31st May). Clear this checkbox if you do not want to see the percentage change. This is a common parameter across Performance Widgets.



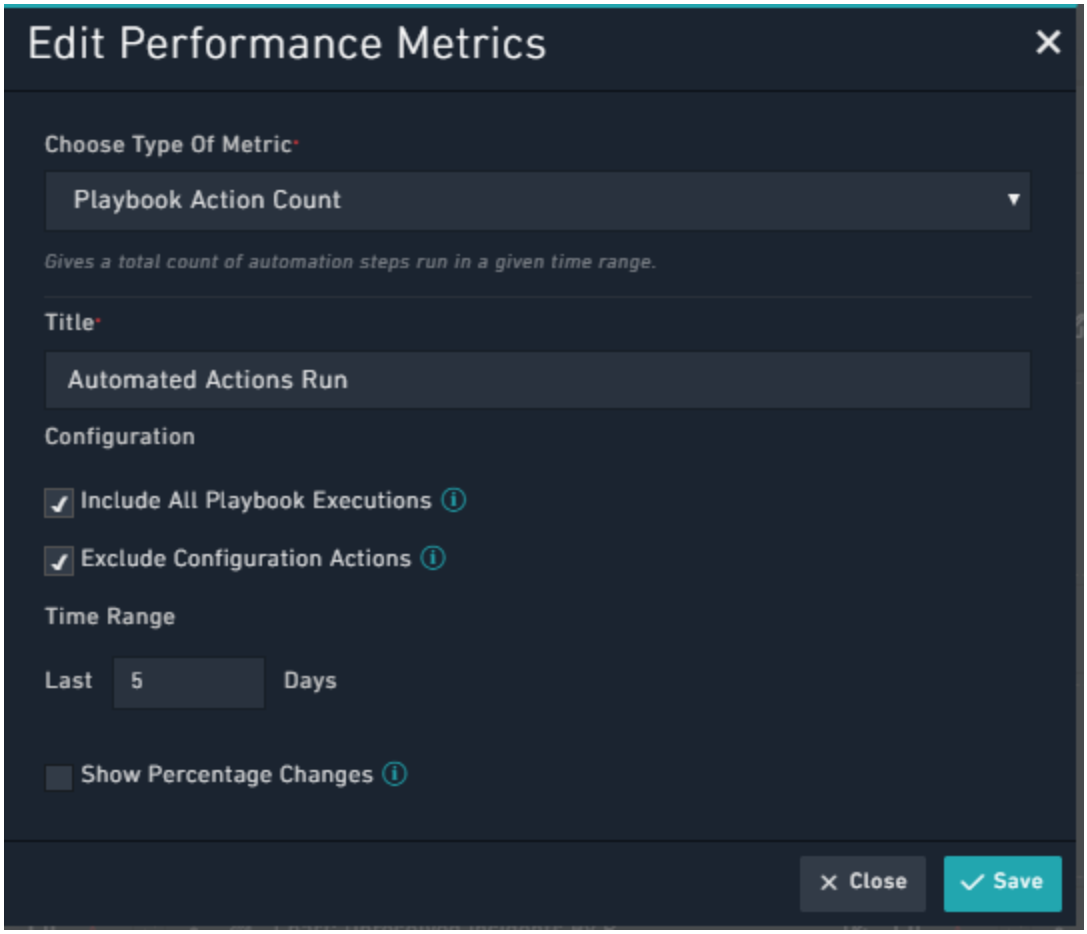
The following image illustrates how the ROI widget is displayed on the `Dashboard` page, if you have chosen the Dollar Savings method of ROI measurement:

Playbook Action Count

Use the Playbook Action Count widget to display the number of playbook steps executed for a specified time period. You need to specify the following parameters, apart from the common parameters of Include All Playbook Execution, Exclude Configuration Actions and Show Percentage Change:

Title: Title of the Playbook Action Count widget. For example, `Automated Actions Run`.

Time Range: Specify the time, in days, for which you want to see the number of playbook steps executed. For example, `5` days.



The following image illustrates how the Playbook Action Count widget is displayed on the `Dashboard` page:

Time To X

Use the Time To X widget to display the MTTR or MTTD for a particular activity. You need to specify the following parameters, apart from the common parameter of Show Percentage Change:

Title: Title of the Time to X widget. For example, `Time to Resolve Incidents - Mean`.
In this case, as an example, we are calculating the Time to X between the Resolved Date and the Discovered Date for Incidents, and we have considered the following types of Time to X, i.e., Mean, Maximum, and Minimum.

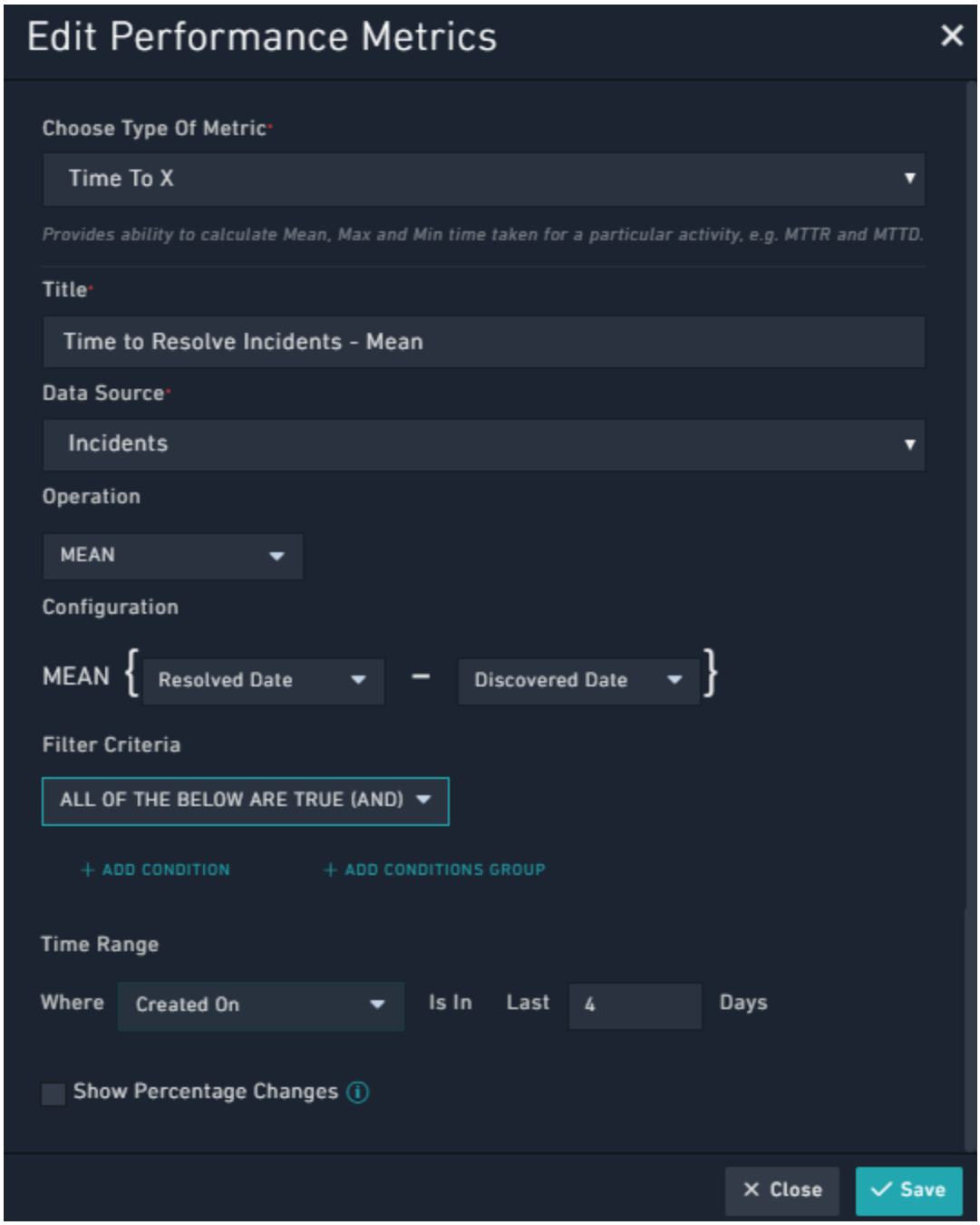
Data Source: The module on whose data you want to calculate the MTTR or MTTD. For example, **Incidents**.

Operation: Select whether you want to calculate the Mean, Median, Maximum, Minimum, or Sum of MTTR or MTTD time. For example, choose **Mean**.
For its configuration, specify **Resolved Date - Discovered Date**.

Filters: (Optional) Specify the filter condition, if you want to apply a filter to the records in the module you have specified.

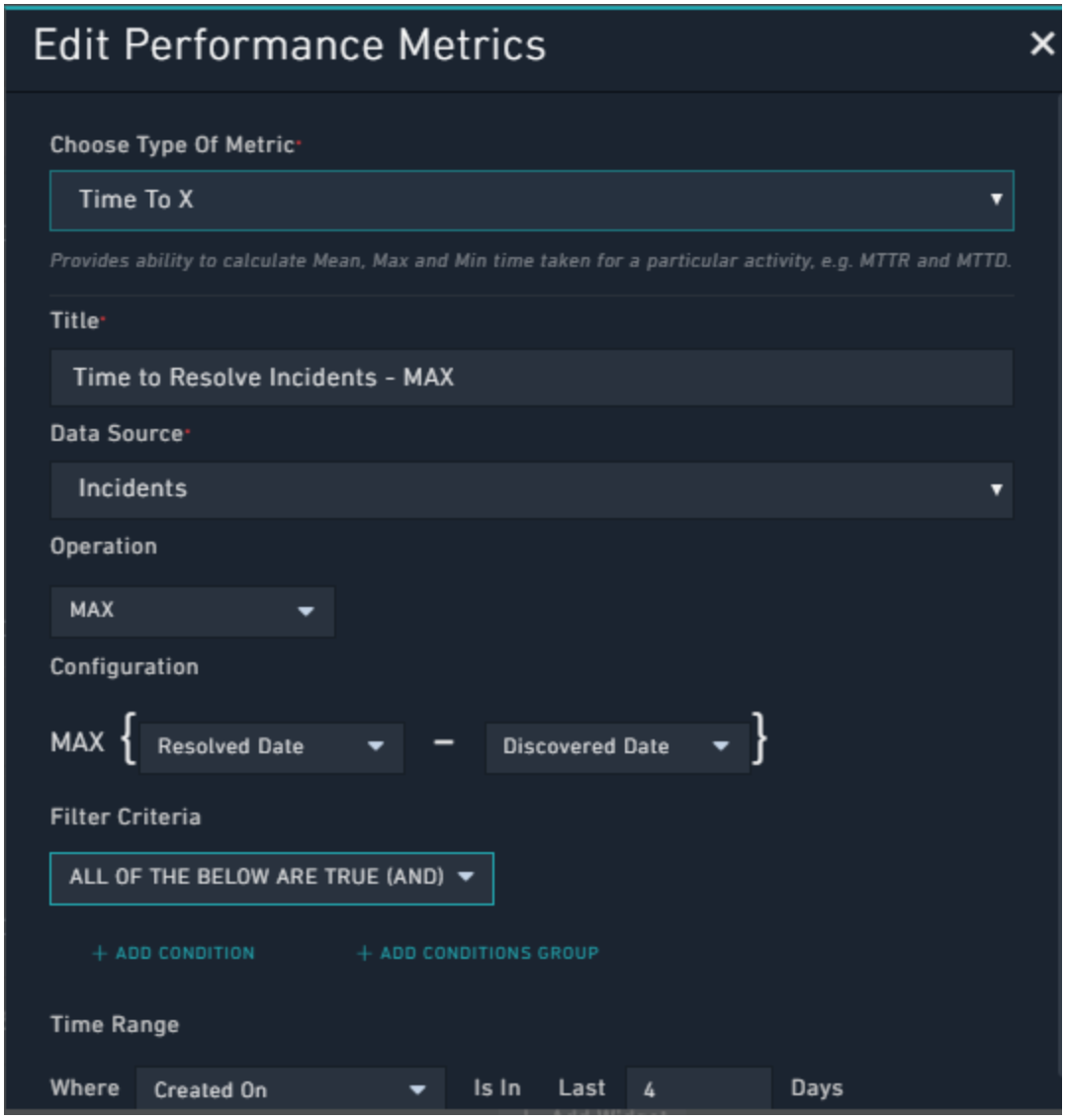
Time Range: Specify the time, in days, and the field based on which you want to calculate the time. For example, `4` days.

Following is an example of the Time To X Mean Template configuration:



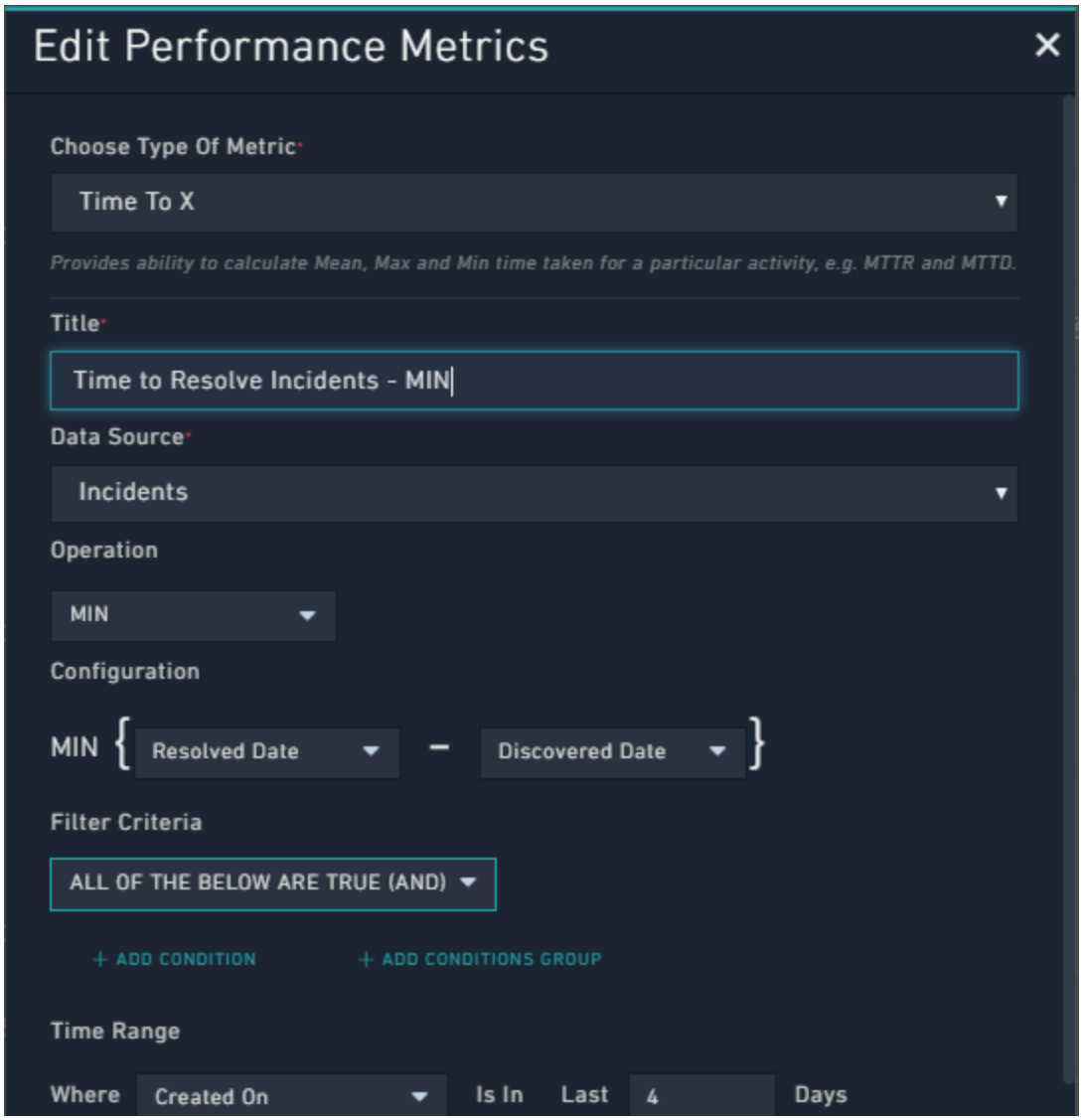
The following image illustrates how the Time To X widget - Mean is displayed on the `Dashboard` page:

Following is an example of the Time To X Max Template configuration:



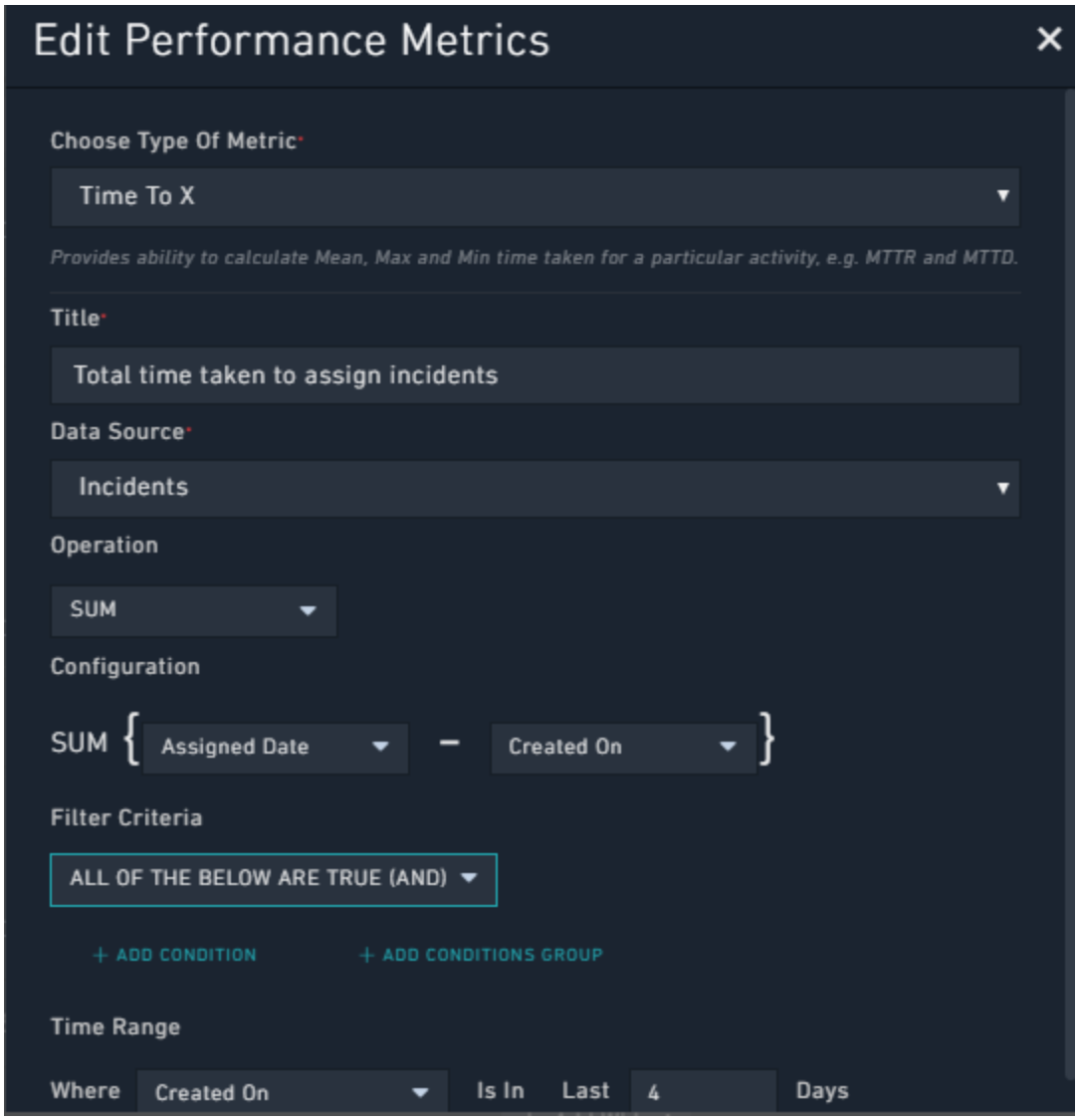
The following image illustrates how the Time To X widget - Max is displayed on the `Dashboard` page:

Following is an example of the Time To X Min Template configuration:



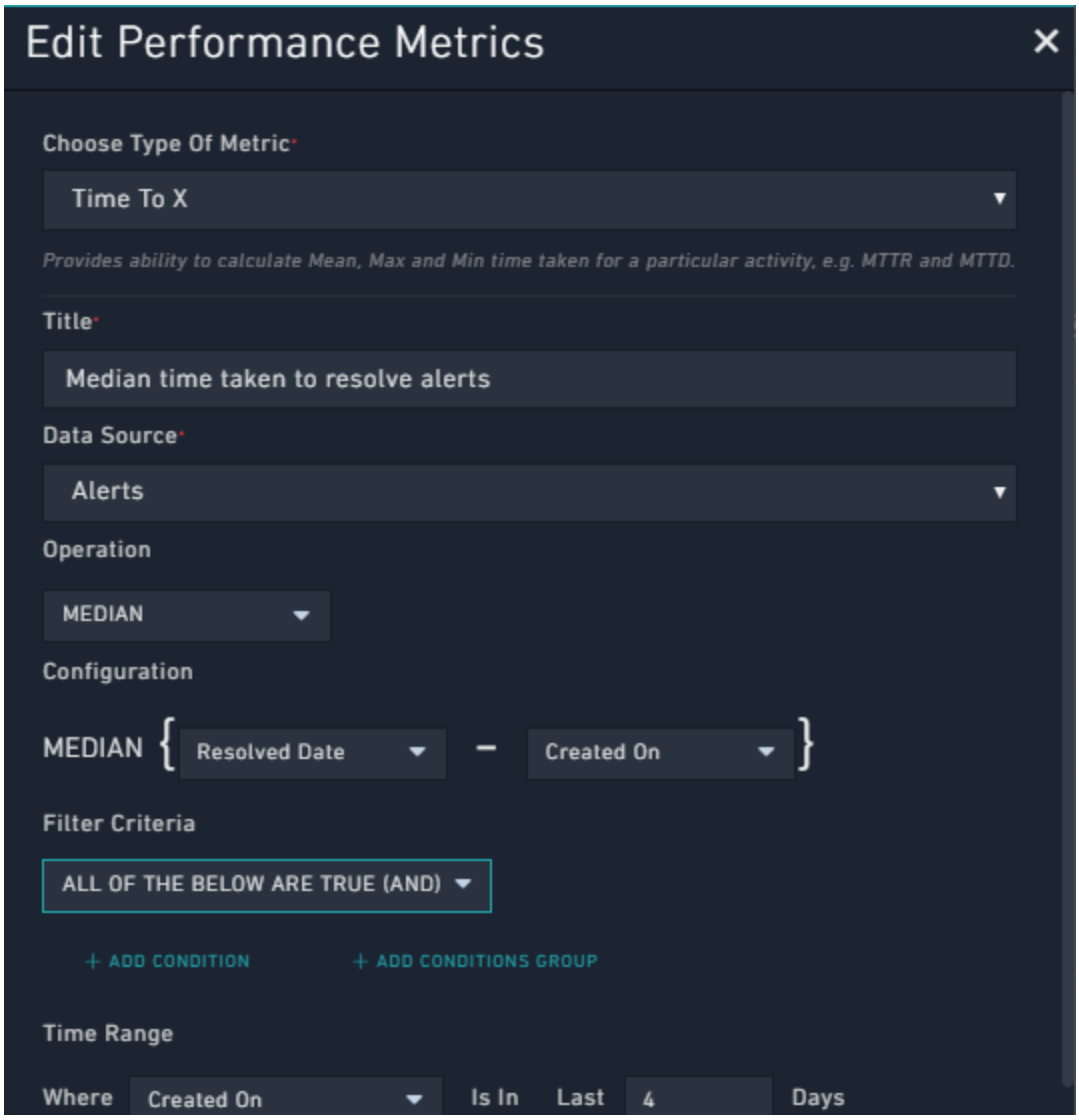
The following image illustrates how the Time To X widget - Min is displayed on the `Dashboard` page:

Following is an example of the Time To X Sum Template configuration that displays the total time taken to assign incidents from the time they are created:



The following image illustrates how the Time To X - Sum widget will appear on the `Dashboards` page. This widget displays the total time taken to assign incidents from the time they are created:

Following image is an example of the Time To X Median Template configuration that displays the median time to resolve alerts, i.e., the median time between the time the alerts are created, and the time alerts are resolved:



The following image illustrates how the Time To X - Median widget will appear on the `Dashboards` page. This widget displays the median time between the time incidents are discovered and the time incidents are resolved:

The "Time To X" widget also supports the following:

- Displaying MTTR values as a Bar Chart, both horizontal and vertical. Earlier this widget could only be displayed using the "Card View".
- Displaying categories within the MTTR view. For example, displaying the time to resolve alerts of different levels of severity by a specific user.

Following is an example of how to create a MTTR dashboard using a Bar Chart that displays the mean time taken for a particular user to resolve alerts of varying severity.

Title: Title of the Time to X widget. For example, `Mean time to resolve alerts by user and severity`.

Data Source: The module on whose data you want to calculate the MTTR. For example, **Alerts**.

Layout: Choose the layout of the widget. You can choose between Card View or Bar Chart. For our example, choose **Bar Chart**.
If you choose Bar Chart, then in the Chart Type choose between Horizontal or Vertical. For our example, choose **Horizontal**.

X-Axis Grouping - 1st Level: Select the field based on which you want to group the records to be displayed in the dashboard. This will form the primary filter for displaying the dashboard. For our example, we require to display the mean time taken by a specific user, for example, `csadmin`, to resolve alerts of varing severity levels. Therefore, for the primary filter, select **Assigned To**.

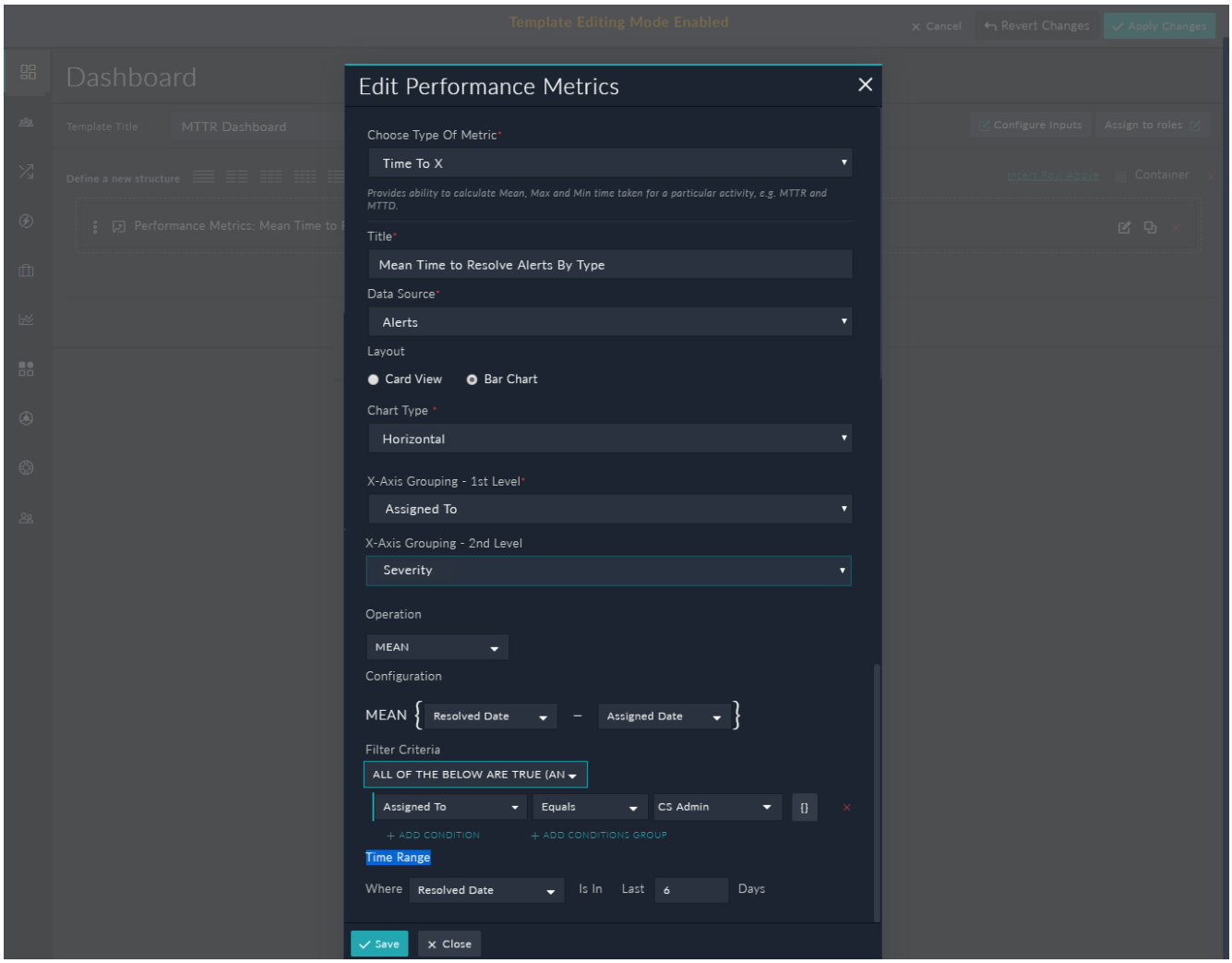
X-Axis Grouping - 2nd Level: Select the field based on which you want to further group the records to be displayed in the dashboard. This will form the second filter for displaying the dashboard. For our example, select **Severity**.
We choose Assigned to and Severity as the primary and secondary filter respectively since we want the MTTR dashboard to display the time taken for resolving alerts grouped the user and severity.

Operation: Select whether you want to calculate the Mean, Median, Maximum, Minimum, or Sum of MTTR or MTTD time. For our example, choose **Mean**.
For its configuration, specify **Resolved Date - Assigned Date**.

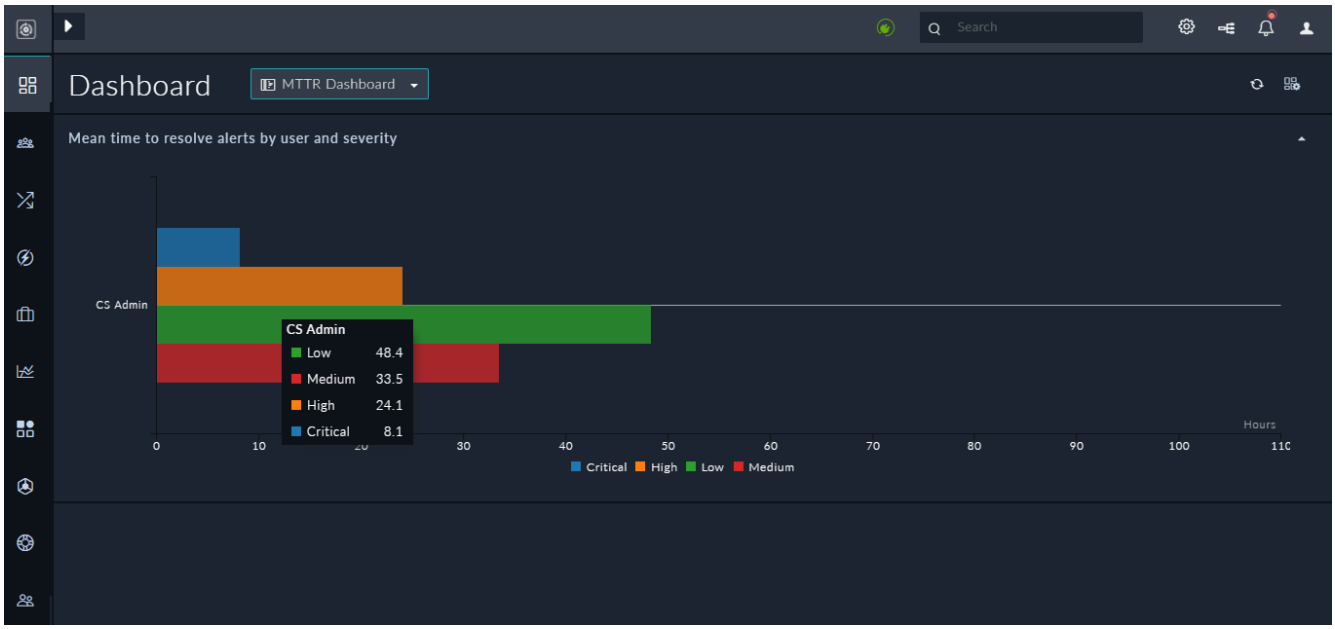
Filters: (Optional) Specify the filter condition, if you want to apply a filter to the records in the module you have specified. In this you can specify the filter `Assigned To Equals CS Admin`, since we want to display how much time the `csadmin` user takes to resolve alerts of varying severity levels.

Time Range: Specify the time, in days, and the field based on which you want to calculate the time. For example, `Resolved Date is in the 6 Days`.

Following image is an example of the MTTR Dashboard configuration that displays the mean time to resolve different types of alerts, i.e., the mean time between the time the alerts are assigned, and the time alerts are resolved:



The following image illustrates how the MTTR Dashboard that displays a bar chart showing the mean time to resolve alerts by type on the `Dashboard` page:



Aggregate Functions

Use the Aggregate Functions widget to calculate and display the minimum, maximum, median, mean, or sum of record fields (integer/decimal), for a single record or for two records. You need to specify the following parameters, apart from the common parameter of **Show Percentage Change**:

Title: Title of the Aggregate Functions widget. For example, `Average time in mins to contain incidents.`

Data Source: The module on whose data you want to calculate the minimum, maximum, average, or sum of integer or float fields. For our example, select **Incidents**.

Operation: Select the operation, which is **MEAN** that you want to perform on the fields and for this operation and then select **Single Record Field**.

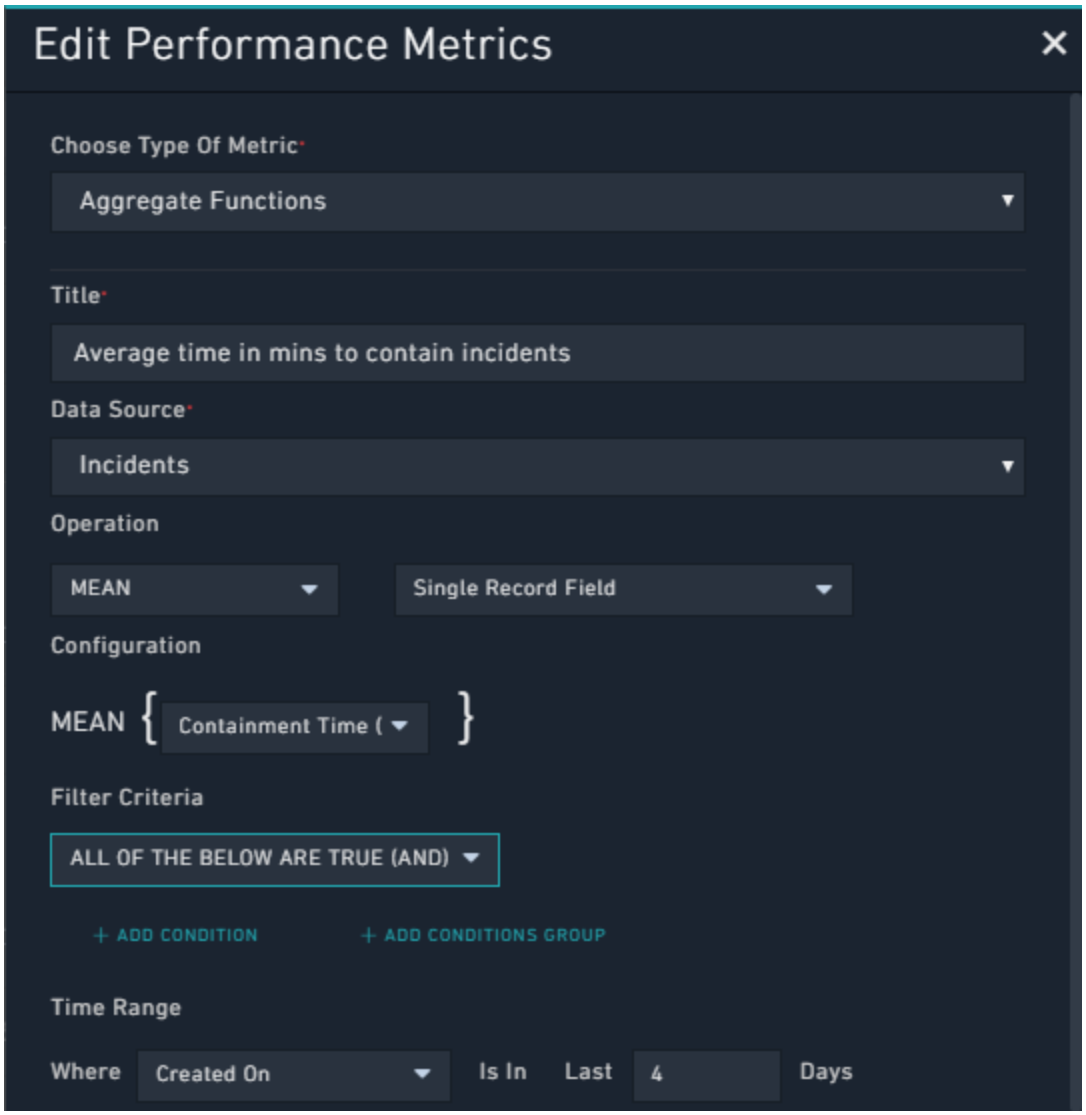
Configuration: In the configuration section, select the field on which you want to perform the operation. The fields must be of type `Integer` or `Decimal`. For our example, select **Containment Time (minutes)**.

It is recommended that when you create an Integer field, you should set its default value as "zero" in the module editor. Since if any column specified in the configuration has NULL values, then the Aggregate Functions might not show the correct value in the dashboards.

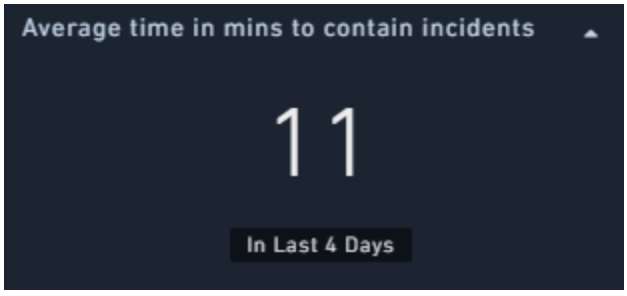
Filters: (Optional) Specify the filter condition, if you want to apply a filter to the records in the module you have specified.

Time Range: Specify the time, in days, and the field based on which you want to calculate the time. For our example, we want to see results of incidents created in the last 4 days.

The following image is an example of the Aggregate Functions widget that has configured according to the above specifications:



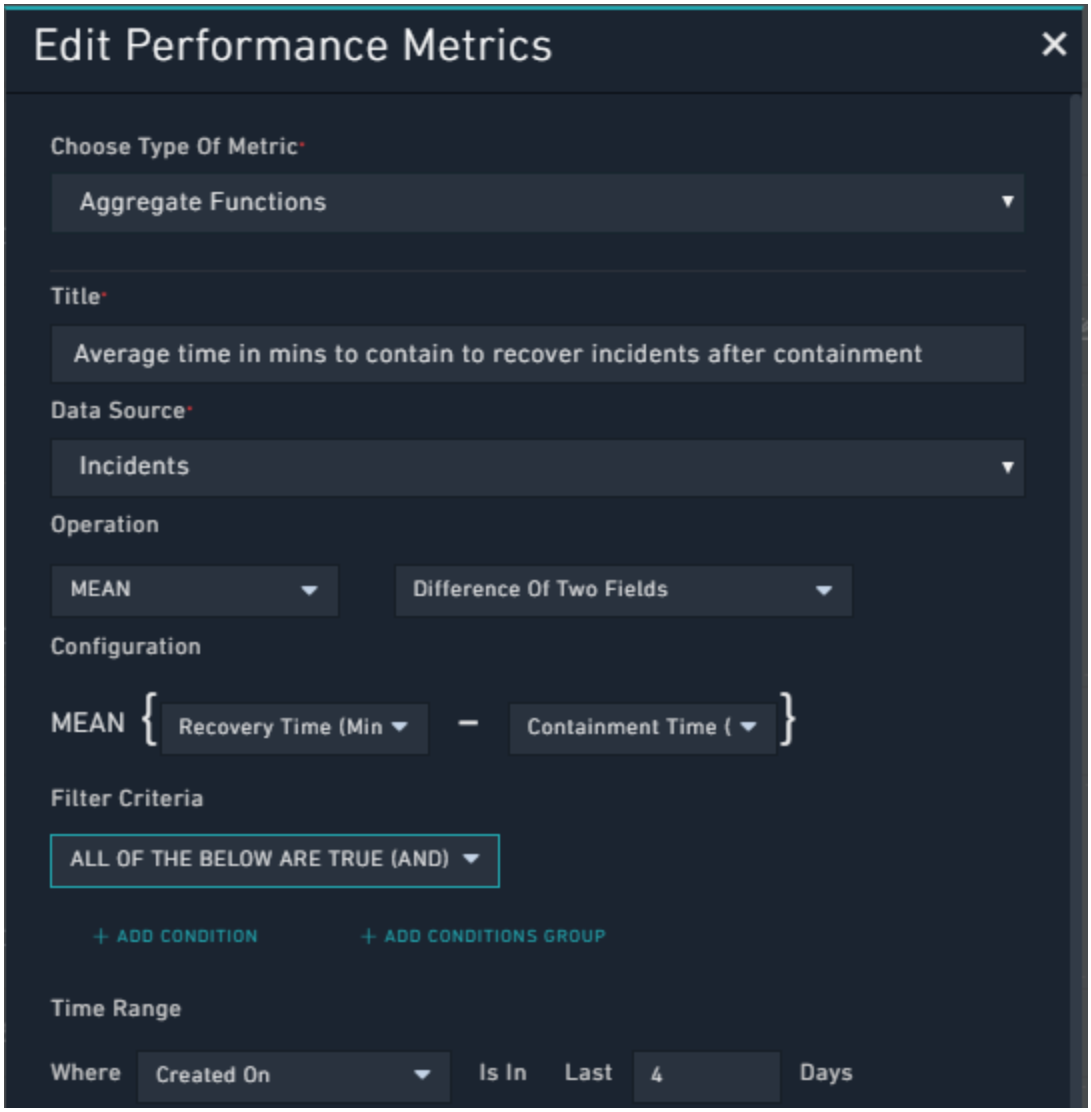
The following image illustrates how the Aggregate Functions widget will appear on the `Dashboards` page. This widget displays the average time, in minutes that it takes to contain incidents, in the last 5 days:



Similarly, you can find out maximum, minimum, median, and sum for integer or decimal fields.

You can also perform an operation that works on two fields and get their maximum, minimum, mean, median, or sum of the difference or aggregation of these fields.

For example, the average difference between the containment time and the recovery time for incidents. The following image is an example of the Aggregate Functions widget configured for this example:



The following image illustrates how the Aggregate Functions widget will appear on the `Dashboards` page. This widget displays the average time, in minutes, to recover after containing incidents, in the last 5 days:

Ratio

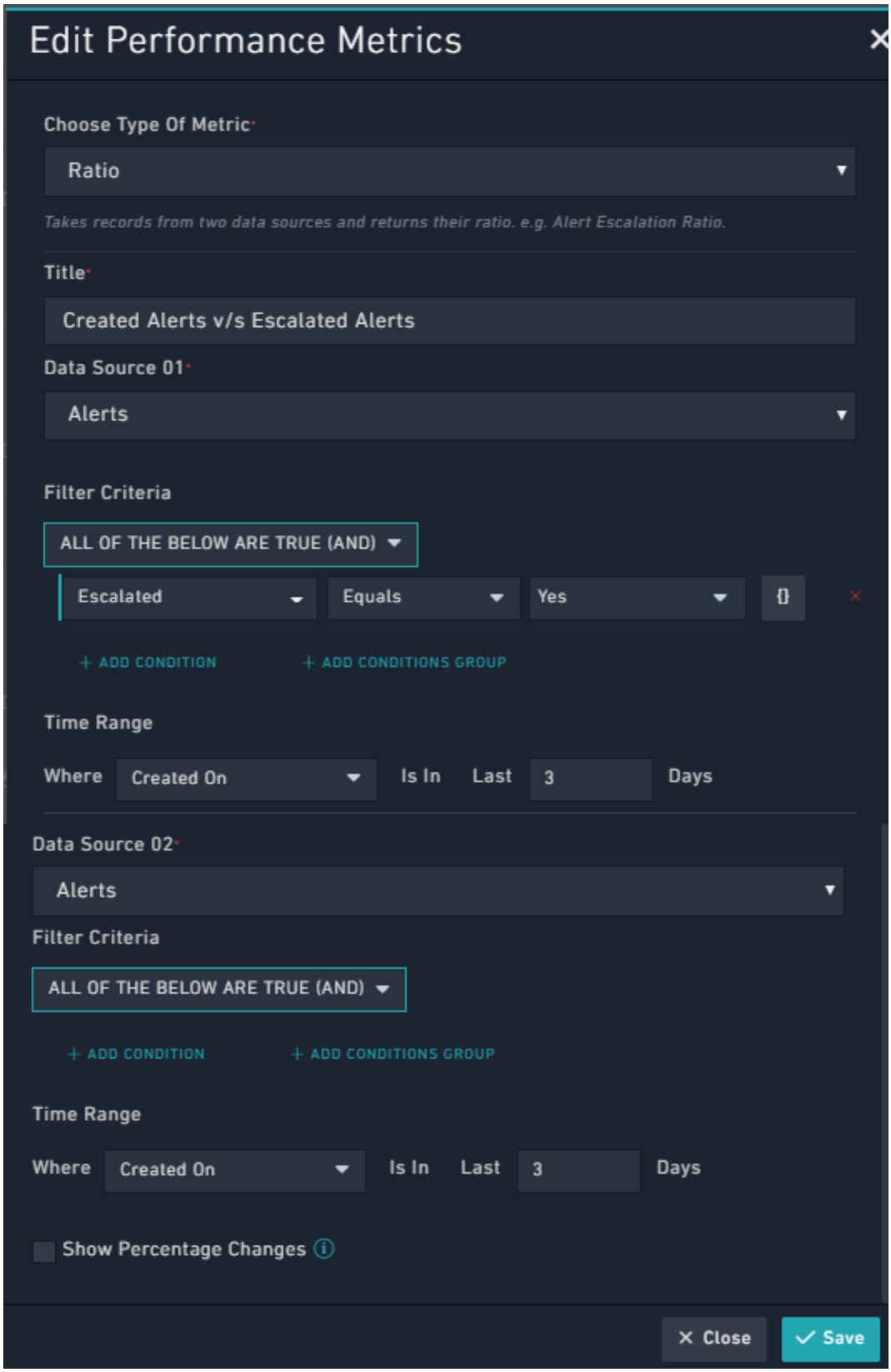
Use the Ratio widget to display the relationship between two values. You need to specify the following parameters:

Title: Title of the Ratio widget. For example, `Created Alerts v/s Escalated Alerts`.

Data Source: The module on whose data you want to calculate the ratio. In the case of the Ratio widget, you must specify two data sources since you require to compare two values. For our example, select **Alerts** as both the data sources.

Filters: (Optional) Specify the filter condition, if you want to apply a filter to the records in the module you have specified. For our example, in one option you do not require to apply any filter since we are comparing all the alerts created and in the other option specify a filter such as `Escalated Equals Yes`.

Time Range: Specify the time, in days, and the field based on which you want to calculate the time. For example, `3` days.



The following image illustrates how the Ratio widget is displayed on the `Dashboard` page:

Total Count

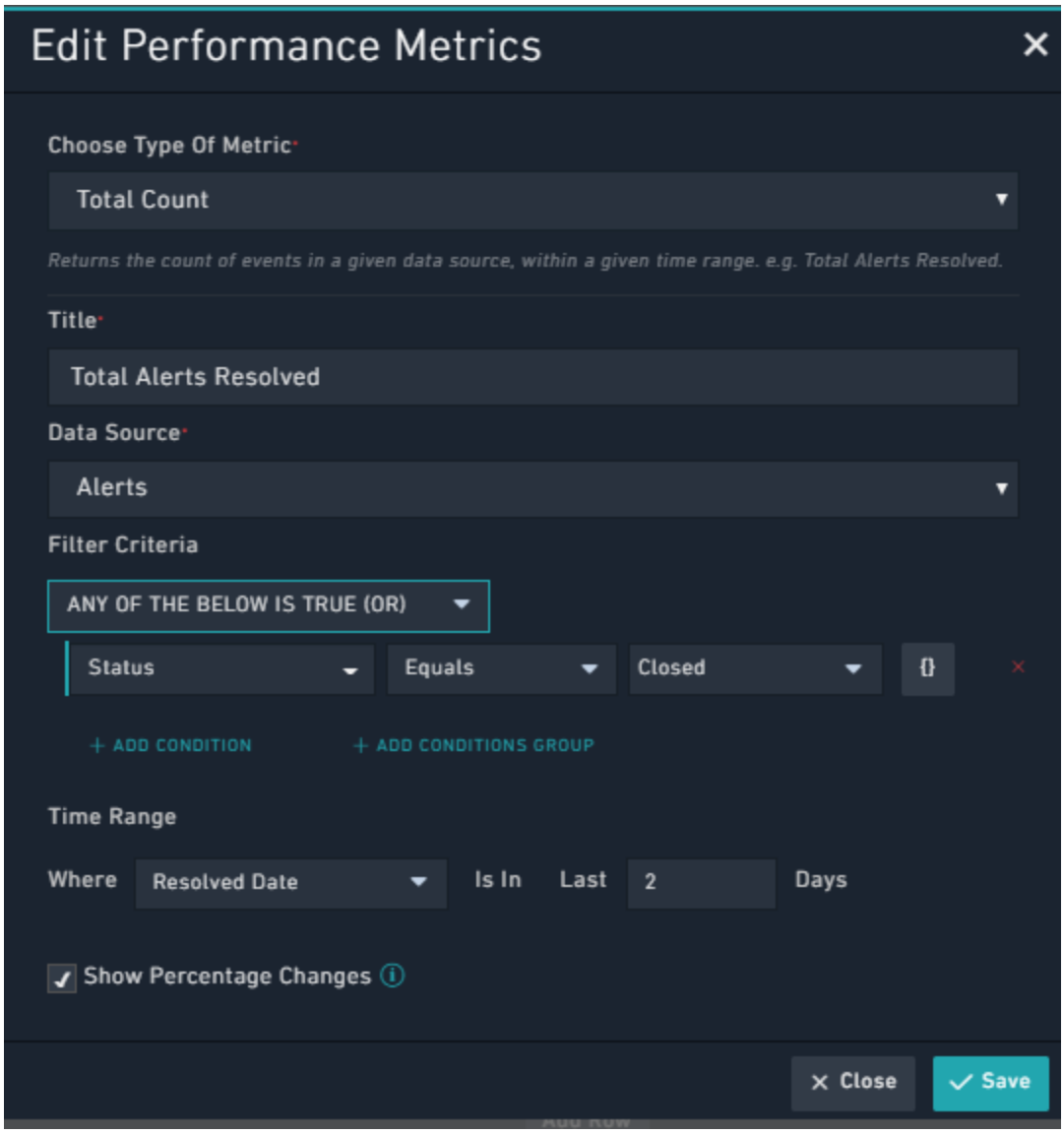
Use the Total Count widget to display the number of records of a specific type on which a specific action is performed for a specified number of days. You need to specify the following parameters, apart from the common parameter of Show Percentage Change:

Title: Title of the Total Count widget. For example, `Alerts Resolved`.

Data Source: The module on whose data you want to calculate the total count. For example, **Alerts**.

Filters: (Optional) Specify the filter condition, if you want to apply a filter to the records in the module you have specified. For example, since we want to get the total count of escalated alerts, specify a filter such as `Status Equals Closed`.

Time Range: Specify the time, in days, and the field based on which you want to calculate the time. For example, `2` days.



The following image illustrates how the Total Count widget is displayed on the `Dashboard` page:

System Monitoring

Use the "System Health Status" Dashboard that is included by default in FortiSOAR to monitor various FortiSOAR system resources such as CPU, Disk Space and memory utilization, and the statuses of various FortiSOAR services. The advantage of having the System Health Status Dashboard is that now you do not require to log into the FortiSOAR server to check the various usage levels and you can also define various thresholds for each system resource and if these thresholds are breached then you can take some corrective actions.

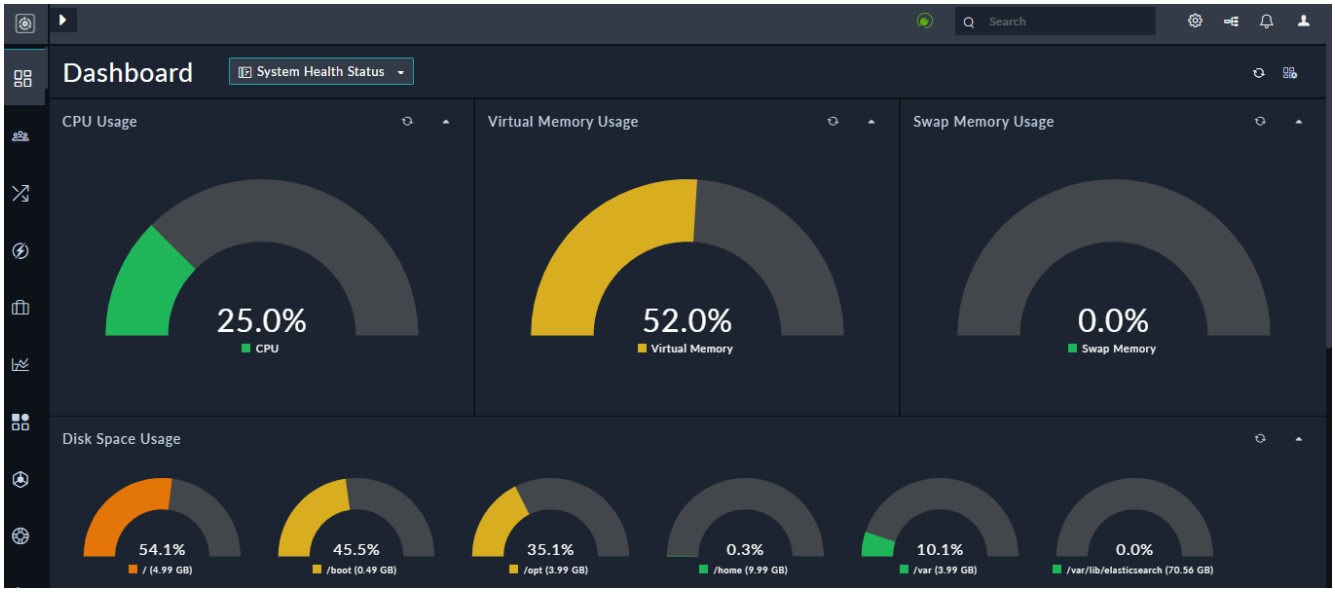
From version 6.4.3 onwards, you should set up system monitoring for FortiSOAR, both in case of a single node system and High Availability (HA) clusters on the `System Configuration` page. To know more about the setting up thresholds and enabling notifications, to effectively monitor various FortiSOAR system resources, see the *System Configuration* chapter in the "Administration Guide."

For versions prior to 6.4.3, you should set up thresholds, schedules, and notifications for the System Monitoring playbook that is included by default with FortiSOAR to effectively monitor various FortiSOAR system resources. To know more about configuring thresholds, schedules, and notifications, see the System Monitoring: Setting up thresholds, schedules, and notifications article present in the Fortinet Knowledge Base.

The following types of system monitoring are available in the System Monitoring widget:

- **CPU Usage**: Displays the percentage (%) of overall CPU utilization.
- **Virtual Memory Usage**: Displays the percentage (%) of overall Virtual Memory utilization.
- **Swap Memory Usage**: Displays the percentage (%) of overall Swap Memory utilization.
- **Disk Space Usage**: Displays the percentage (%) of disk space consumption for different partitions.
- **Service Status**: Displays the status for all FortiSOAR services.

Following is an image of a sample System Health Status Dashboard:



Utilization widgets

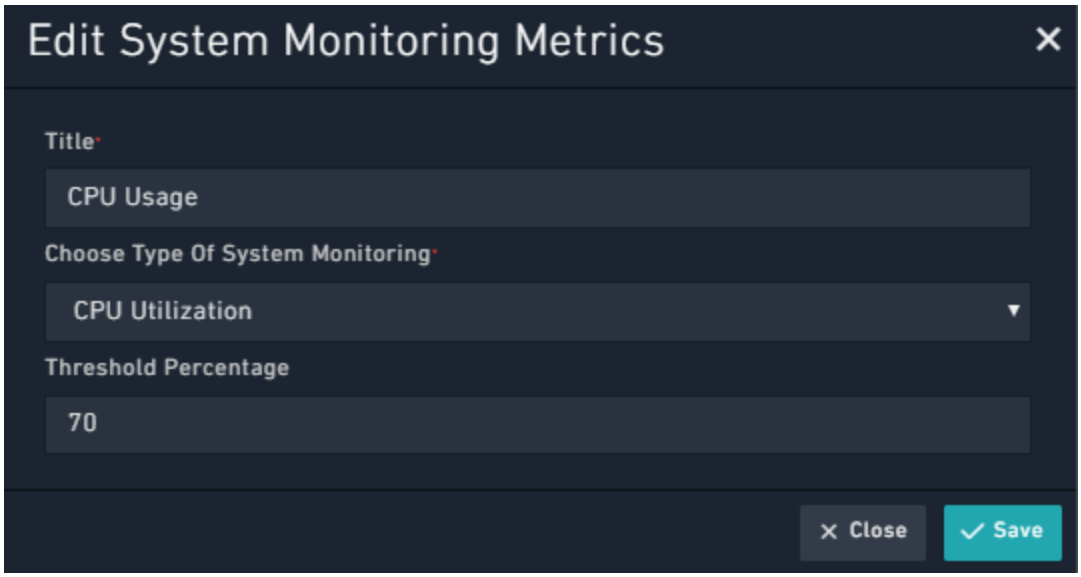
Use the Utilization widgets to display the utilization of various FortiSOAR system resources. Utilization widgets are: CPU Utilization, Disk Space Utilization, and Memory Utilization. These widgets can be configured in a similar manner and are used to display the utilization of various FortiSOAR system resources.

Title: Title of the Utilization widget. For example, if you are selecting the CPU Utilization widget, you can name this widget as `CPU usage`.

Choose Type of System Monitoring: For utilization, you can choose from, CPU Utilization, Disk Space Utilization, or Memory Utilization.

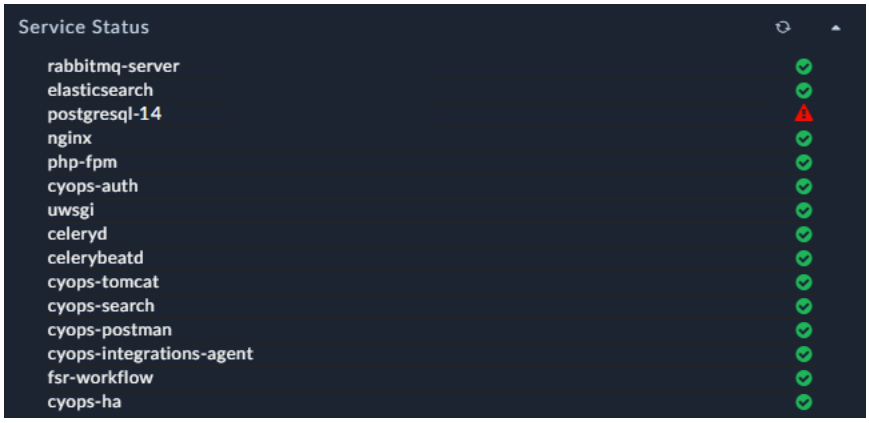
Threshold Percentage: Specify the percentage after which you want to take some corrective action. On the dashboard, the widgets will visually indicate when the threshold is reached or exceeded, in the red color. Similarly, it will display various colors, green, yellow, amber according to threshold value.

Following is a sample image of a configured a CPU Utilization widget:



Service Status widget

This widget displays the status for all FortiSOAR services. Services that are available are displayed with a green circle. If any service is down, then that service will be displayed with a red warning symbol, as is the case with the `postgresql-14` service in the following image:



The `cyops-integrations-agent` service is also monitored. The `cyops-integrations-agent` service supports running actions on remote FSR agents.

Title: Title of the Service Status widget. For example, `Services status`.

Choose Type of System Monitoring: Select **Service Status**.

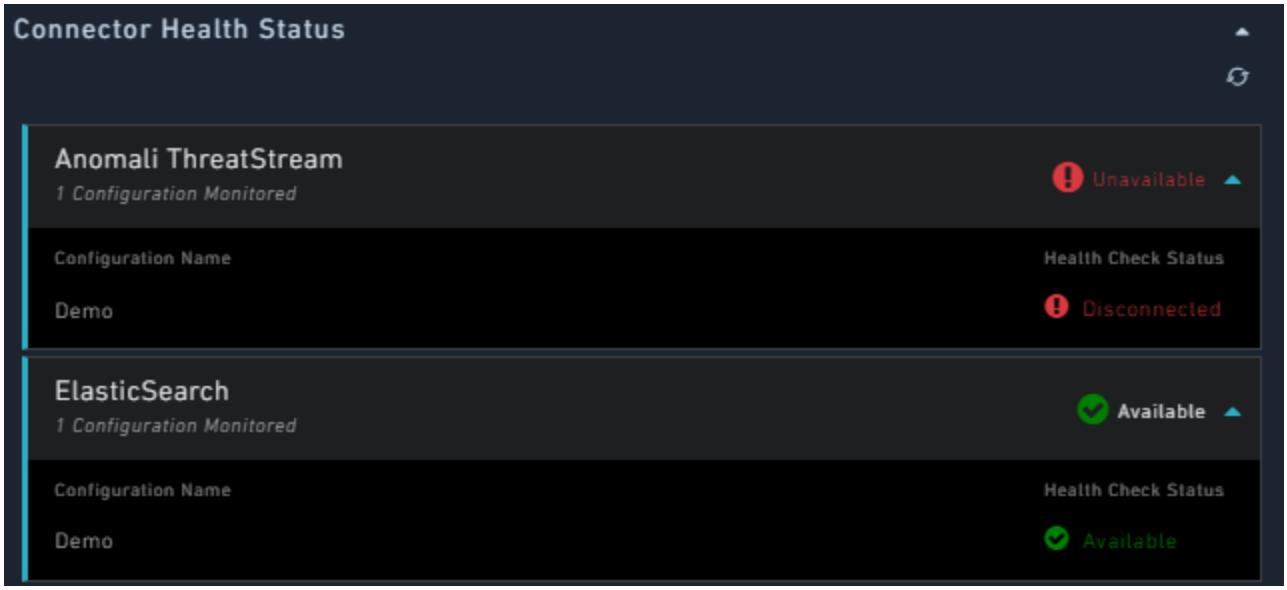
Connector Health

Use this widget to track the health of all the configurations of all your configured connectors. Some system connectors such as BPMN, Report Engine, Utilities, etc. do not require any configuration, therefore this widget does not display the health of these connectors.

The Connector Health widget displays only those configurations that has access to both 'Self' and 'Agent'. For more information on connectors and their configurations, see the "Connectors Guide."

You can edit only the **Title** of this connector.

The following image illustrates how the Connector Health widget is displayed on the dashboard page:



Each connector configuration row will display the number of configurations that are being monitored, for example, in the image above, all the connectors have *1 Configuration Monitored*.

If any of the configurations of a connector is unavailable, then the widget will display "Unavailable" in the red color and the Health Check will be Unavailable. For example, in the above image the configuration of the Anomali ThreatStream connector is unavailable. To view the details of the configuration being unavailable, click the down arrow on the

connector row, to display the Health Check Status of that configuration. You will see that the Health Check Status of this configuration is "Disconnected". You can hover on the warning icon to know the reason for the configuration being disconnected.

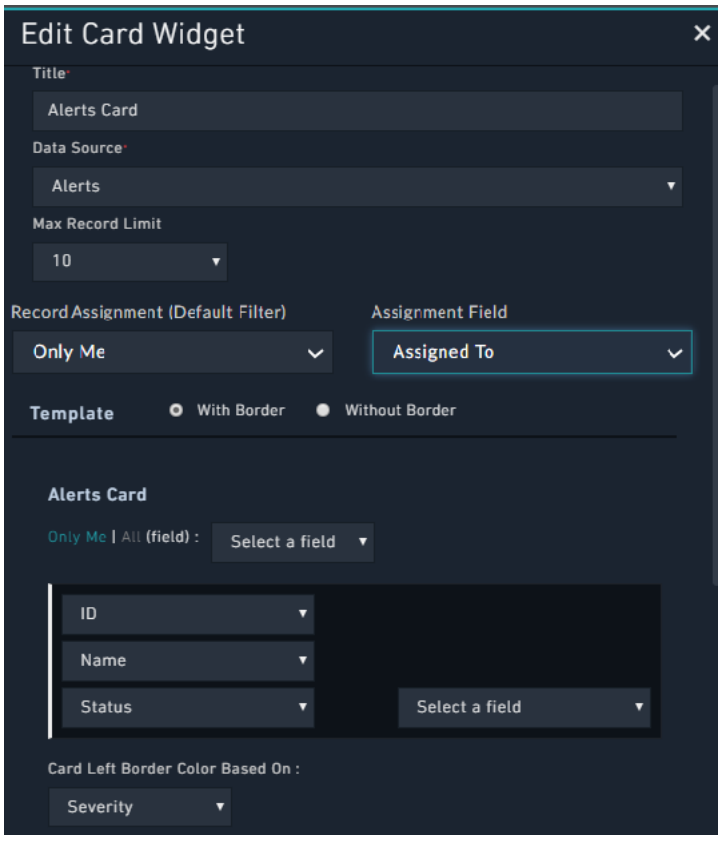
If all the configurations of the connector are available, then the widget will display "All Available" in green color and the Health Check will be "Available". If any configuration is unavailable, then the widget will display "1 Unavailable" in the red color and when you click the down arrow the Health Check Status will display "Available" for the configurations that are available, and display "Disconnected" for the configuration that is unavailable.

If any connector is deactivated, then it will appear as "Deactivated" in red color and the Health Check will display as "Deactivated".

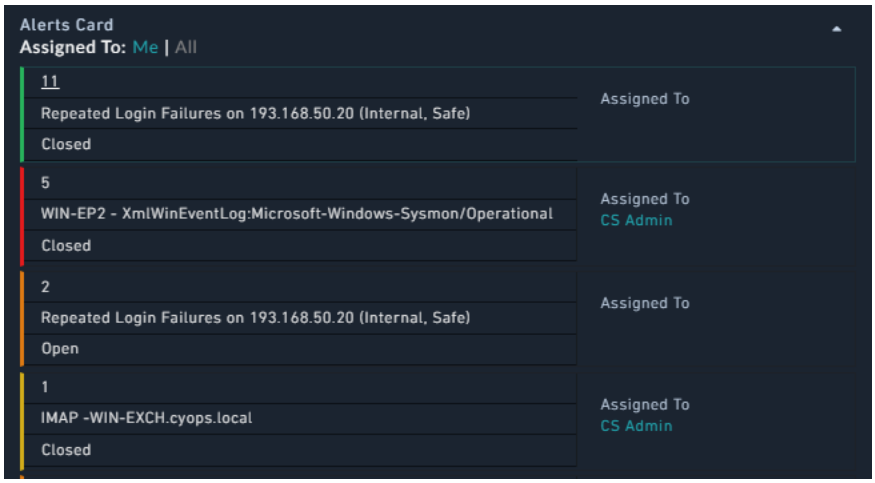
Record - Card View

Card Lists

Cards are like Single Line widgets, but they are in the form of card list in which you have up to four fields in a row. Using the **Card left border Color Based On** drop-down list, you can also choose a color to emphasize fields, such as **Type**, **Severity**, or **Status**.
You can select the **Record Assignment (Default Filter)** as **Only Me** or **All**. If you select **Only Me**, then from the **Assignment Field** drop-down list, you must select the assignment on the basis of which you want to filter the dashboard view.



The following image illustrates how the Card List widget is displayed on the module page:

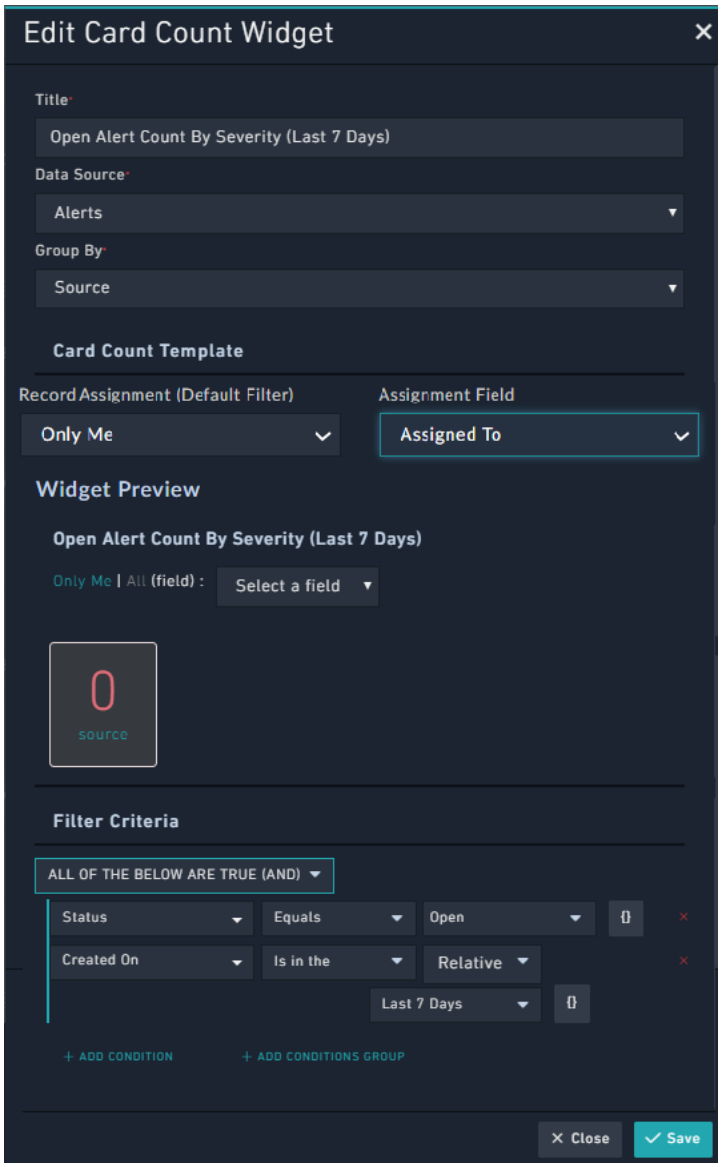


Use the Only Me | All (field) filter, i.e., to toggle the view on dashboards or modules based on this filter. The Nested Filters component is also applicable to the Card List widget.

The **Only Me | All** filter is not applicable to Reports, i.e., on the `Reports` page, you cannot toggle the view based on this filter, instead, you must change this in the report template itself when you are adding or editing the Card List widget.

Card Count

Card Count widgets are simpler forms of the card widget showing a single number representing the total sum of a field on a data model. For example, using the **Group By** field, in the Card Count widget you can get the total count of records assigned to with specific levels of severity.
You can select the **Record Assignment (Default Filter)** as **Only Me** or **All**. If you select **Only Me**, then from the **Assignment Field** drop-down list, you must select the assignment on the basis of which you want to filter the dashboard view.



The following image illustrates how the Card Count widget is displayed on a page:

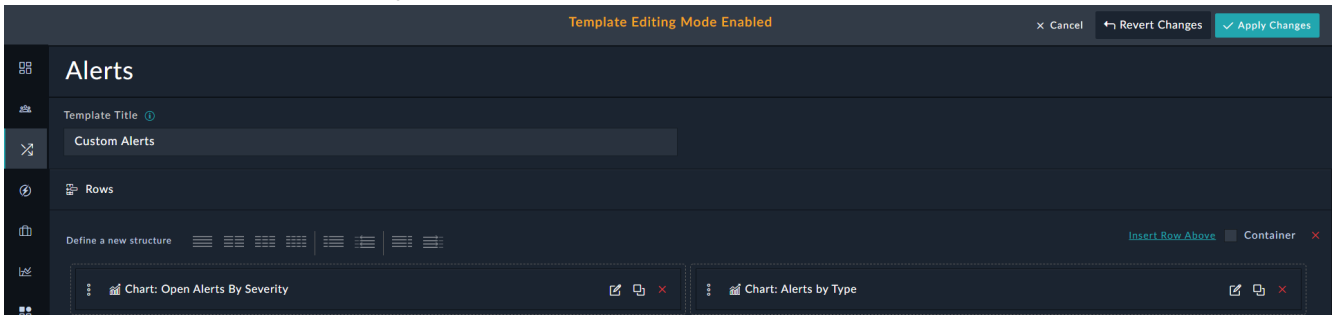
Use the Only Me | All (field) filter, i.e., to toggle the view on dashboards or modules based on this filter. The Nested Filters component is also applicable to Card Count widget.

The **Only Me | All** filter is not applicable to Reports, i.e., on the `Reports` page, you cannot toggle the view based on this filter, instead, you must change this in the report template itself when you are adding or editing the Card widget.

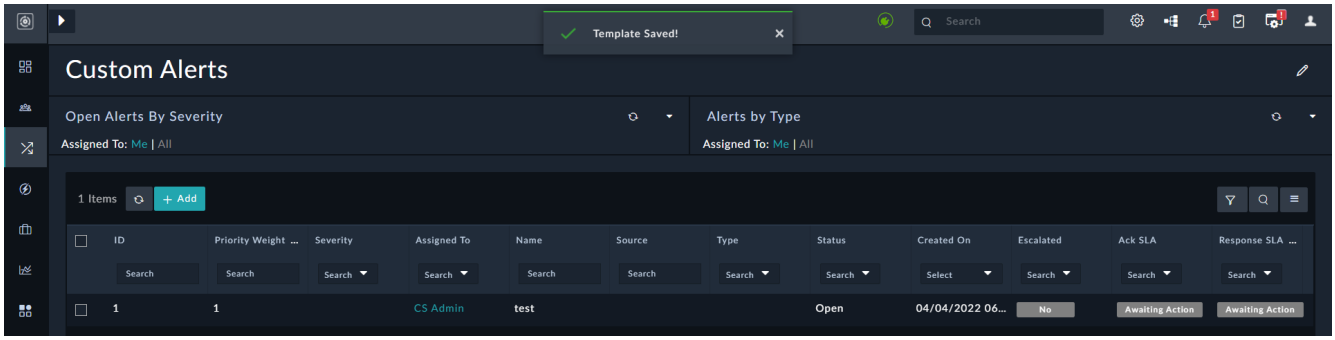
Record - Listing

From release 7.2.0 onwards, you can change the listing page title if you want to name it something other than the plural name of the module. You can change listing page title of modules in Incident Response (Indicators, Tasks, etc.) and Resources (Attachments, etc). However, you cannot change the title of modules in Automation, except the SLA Templates module, or modules such as Reporting, Content Hub, Queue and Shift Management, etc.

For example, if you want to change the name of the Alerts module on the Alerts Listing page to Custom Alerts, click **Alerts** from the left-navigation to view the alert records listing page. Click the **Edit** icon on the top left of the Alerts page, to enter the 'Template Editing' mode. In the **Template Title** field, enter the name of the module that you want to display as the title of the list view. For example, enter `Custom Alerts`:



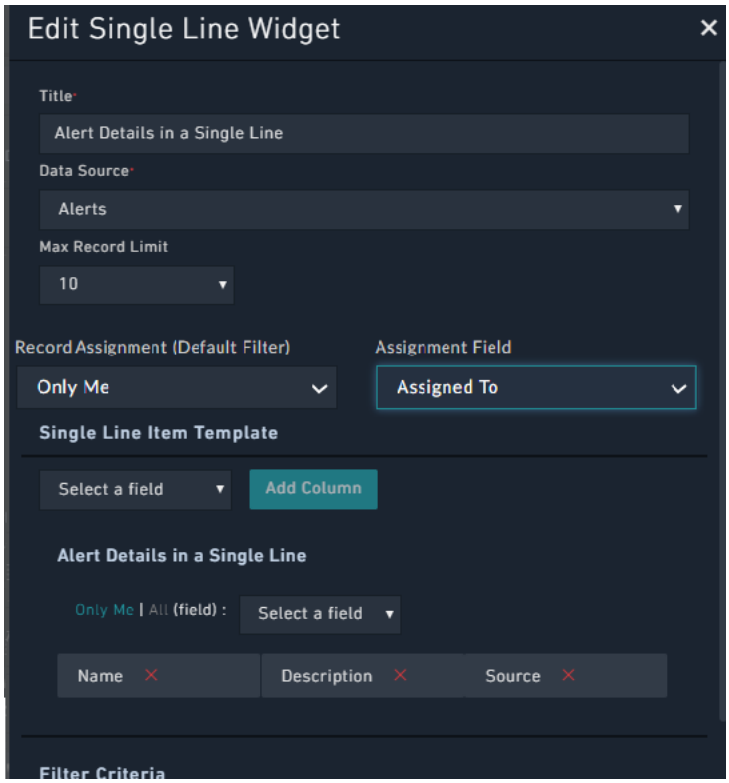
Click **Apply Change** and then click **Confirm** to view the updated list view title:



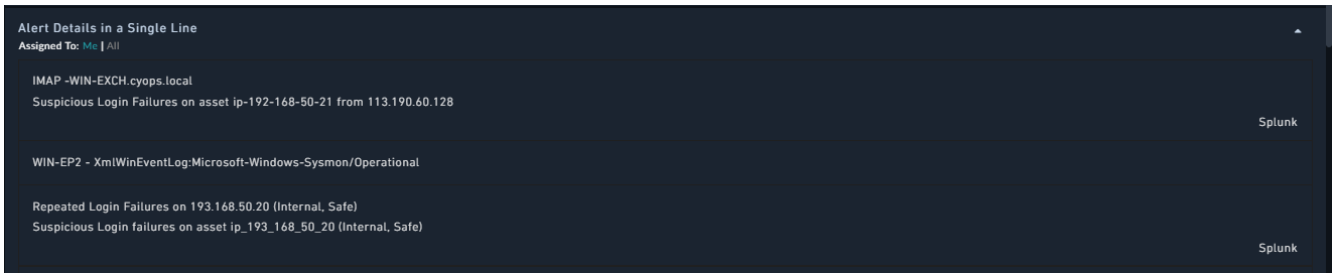
To change the title back to its original, edit the template and clear the text of the **Template Title** field.

Single Line Item

The Single Line widget displays records in a single column. You can use this widget to display records, such as tasks, that are assigned to you and get the complete detail of the tasks in one view.
You can select the **Record Assignment (Default Filter)** as **Only Me** or **All**. If you select **Only Me**, then from the **Assignment Field** drop-down list, you must select the assignment on the basis of which you want to filter the dashboard view.



The following image illustrates how the Single Line Item widget is displayed on the module page:



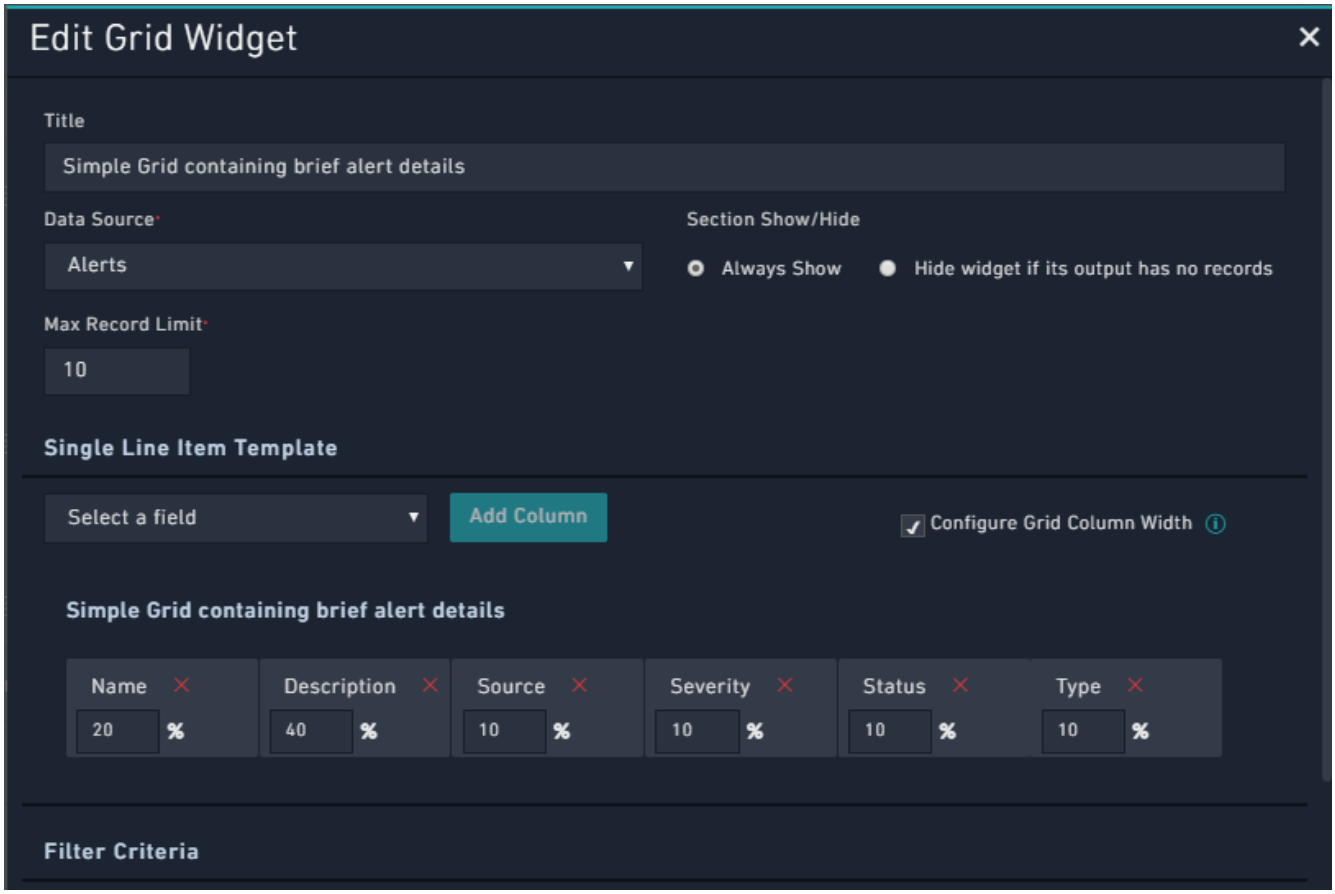
Use the Only Me | All (field) filter, i.e., to toggle the view on dashboards or modules based on this filter. The Nested Filters component is also applicable to Card List widget.

The **Only Me | All** filter is not applicable to Reports, i.e., on the `Reports` page, you cannot toggle the view based on this filter, instead, you must change this in the report template itself when you are adding or editing the Card List widget.

Simple Grid

Use the **Simple Grid** widget to render data in a tabular form in dashboards and reports or wherever you want to render data in the grid format. The Simple Grid widget does not provide any option to search or sort columns or apply filters to records in the List View of the module (as available in the Module List View using the Grid widget). The Simple Grid is a pure display-only grid that gets sorted as per the template specification.

When you are adding or editing the Simple Grid widget in Dashboards or Reports, you must specify the title of the simple grid and the Data Source which will determine the record type that the simple grid will contain. For example, if you select the **Data Source** as **Alerts**, then the widget displays only those records whose type is "Alerts."



In the `Section Show/Hide` section, you can choose to either always display this widget, the **Always Show** option (default), or you can choose to display this widget only if there is at least one record present in the selected module, the **Hide widget if its output has no records** option.

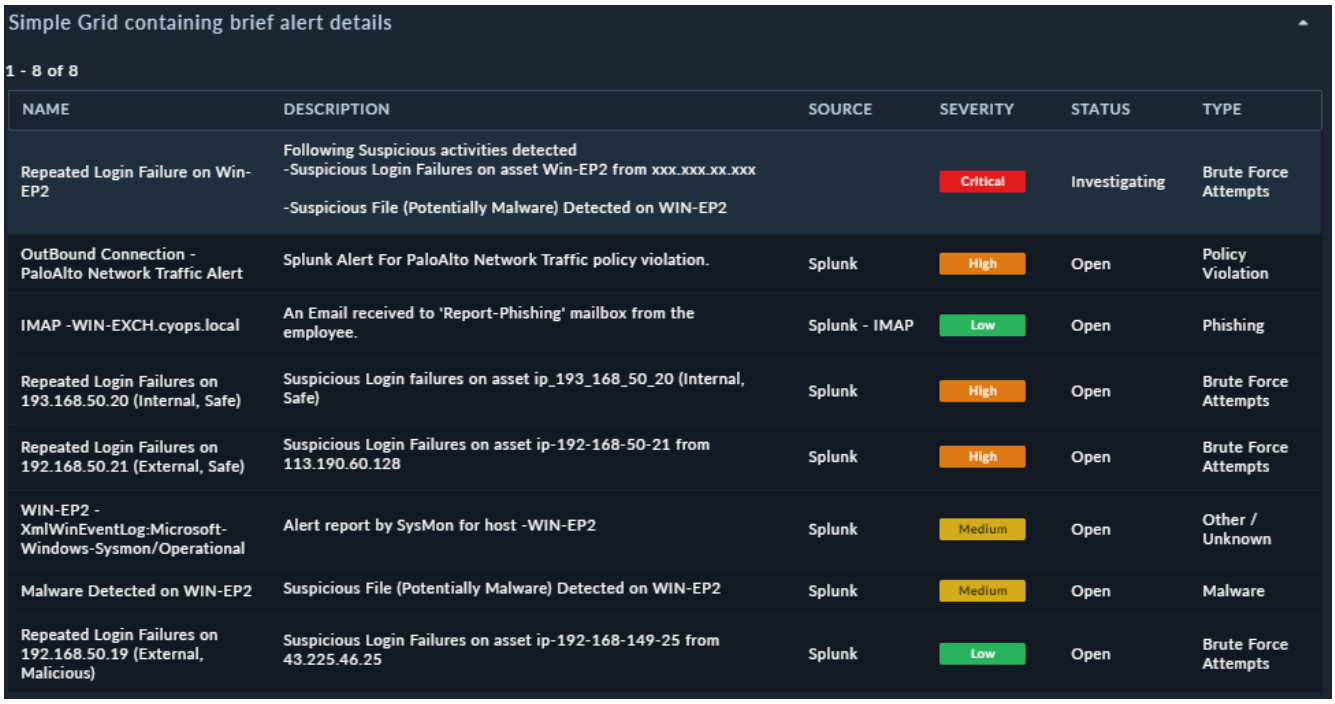
In the **Maximum Record Limit** field specify the maximum number of records that should be displayed in the widget. You can specify any number between 1 to 200. By default, it is set to 10.

In the `Columns` section, select the columns that will be displayed as part of the grid in the `List` view of the module. To add the field as a column, select the field to be part of the grid from the **Select a Field** list and then click **Add Column**. If you want to define the width of the columns in the grid, then select the **Configure Grid Column Width** check box, and this will display a text box in the columns which you have added in which you can specify the width of the columns in the **percentage (%)** format. You can also change the position of how the columns will be displayed in the grid by dragging and dropping the field, add filters to the grid and sort the grid based on a sorting parameter you specify.

From version 6.4.3 onwards, the Simple Grid widget displays the complete text instead of "..." for fields that could contain longer content such as "Description". This enhancement ensures that reports do not contain truncated field content and instead contain the complete content for all fields.

For more information on adding filters and sorting records, see Common components within Widgets.

The following image illustrates how the Simple Grid widget is displayed when used in a dashboard or specific page:

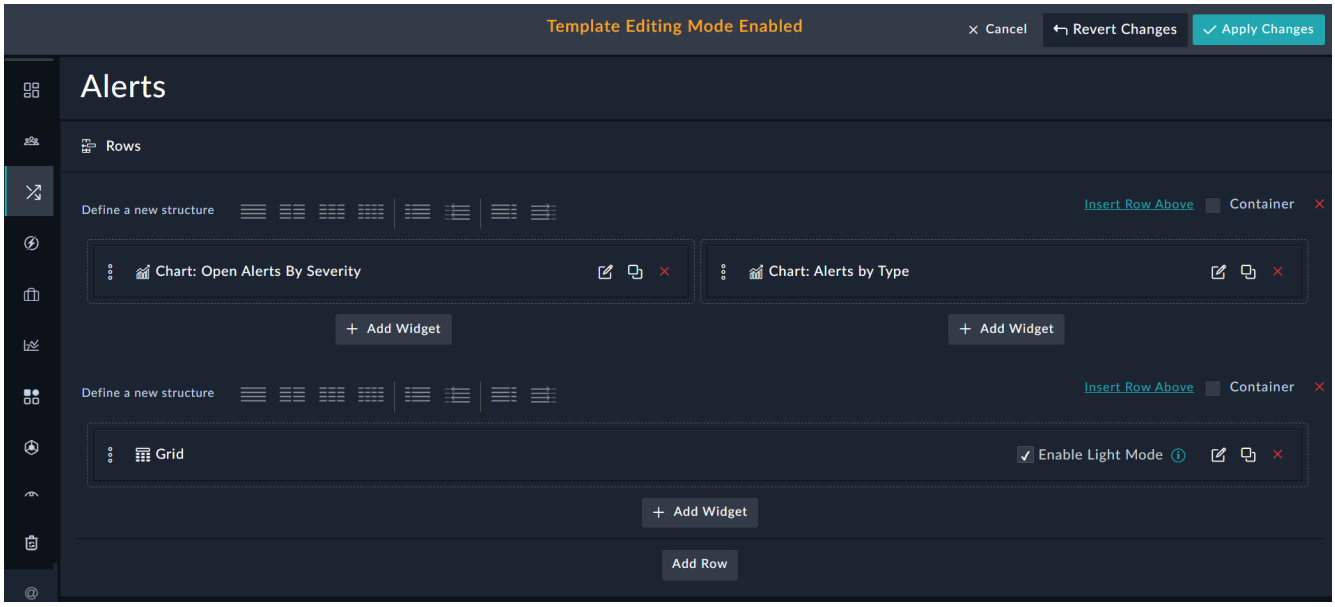


As you can see in the above image, using the Simple Grid you cannot perform any operations, like sorting columns or filtering records, it is only used to display data in the grid format.

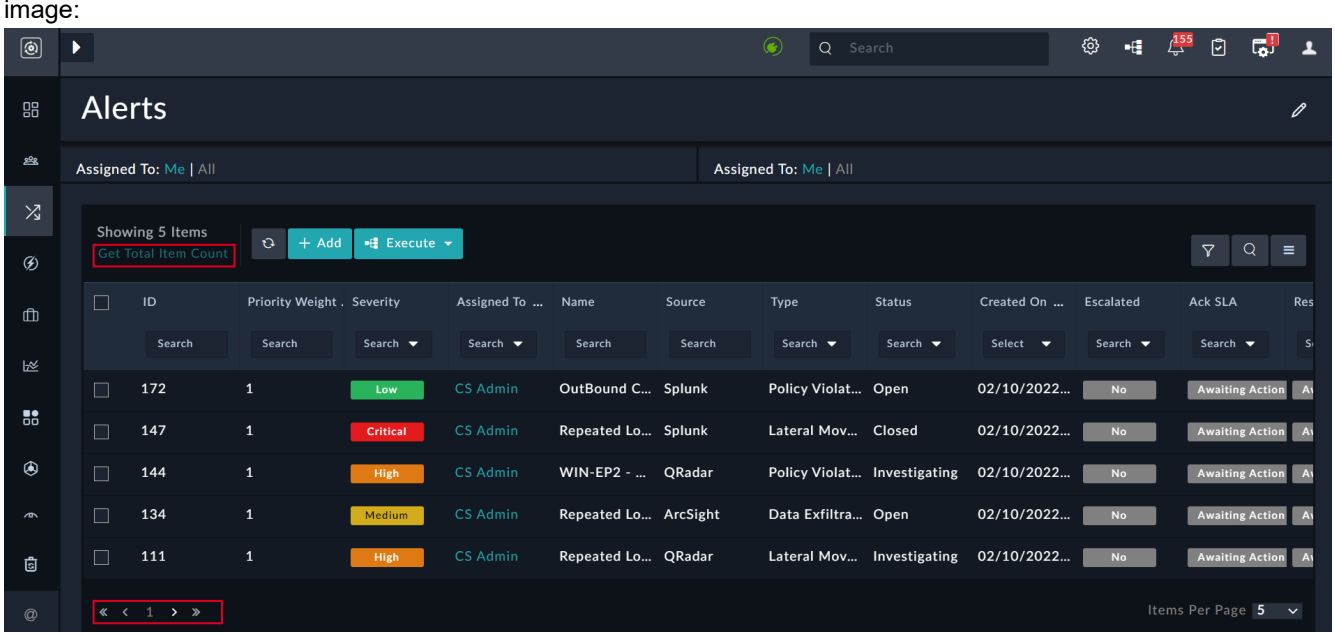
Grid

Grids are tables, with rows representing record instances and columns representing fields.

From release 7.2.0 onwards, you can choose to use a lighter version of the grid widget for better performance and usability. To use the lighter version of the grid widget, click the **Enable Light Mode** checkbox in the **Grid** row:



The performance improvements in the case of the Light Mode are achieved by fetching the total count of records only on demand when the user clicks **Get Total Item Count** at the top of the grid. Also, in this case, the pagination options at the bottom of the grid display the **Next** and **Previous** buttons *without* the total count of pages as shown in the following image:

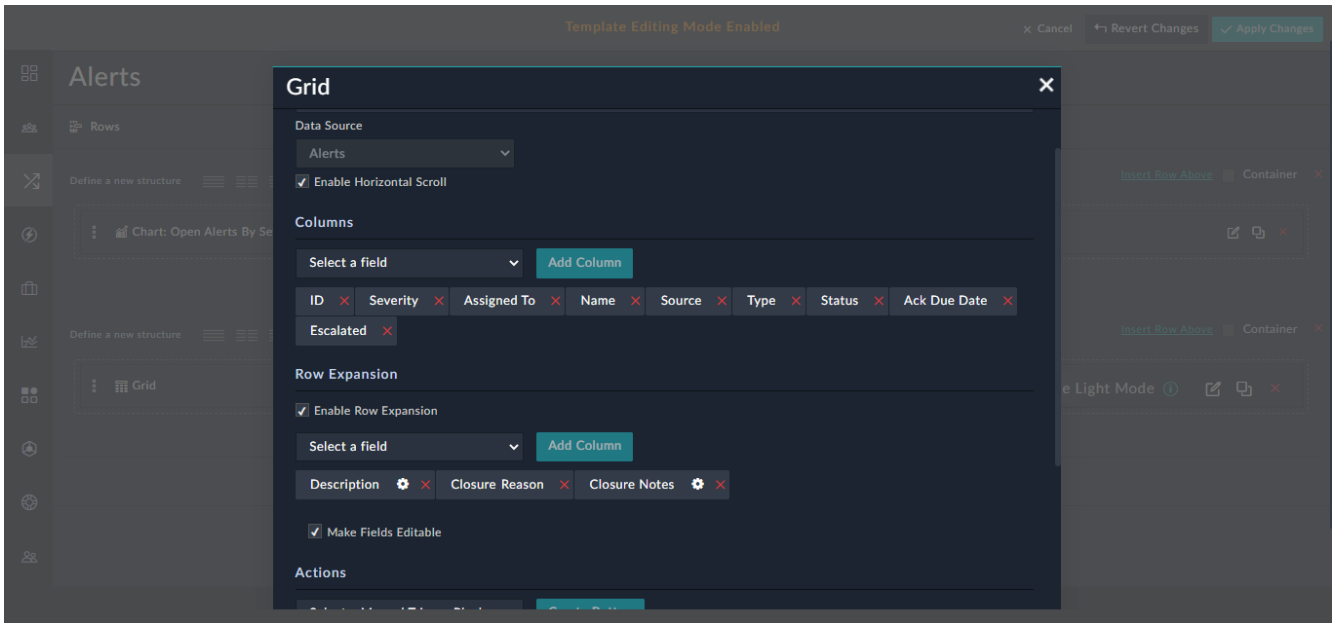


In the case of the Light Mode Grid, users can navigate beyond the last page when the page length and number of records on the last page are equal. For example, the page length is set to 20 records per page and there are 40 records in all, then users can navigate to the 3rd page, where they will see 0 records. However, if there are 30 records in all then this issue will not occur, i.e., the users will be able to navigate only till the 2nd page.

Performance tests run to ascertain the performance improvements achieved while using the Grid in the Light Mode when compared to the normal Grid determined that using the Grid in the Light Mode improved the performance by around 35%. Some numbers that we observed while running is the test are:

- For pages containing 30 records per page, a performance improvement of 65% was observed.
- For pages containing 250 records per page, a performance improvement of 17% was observed.

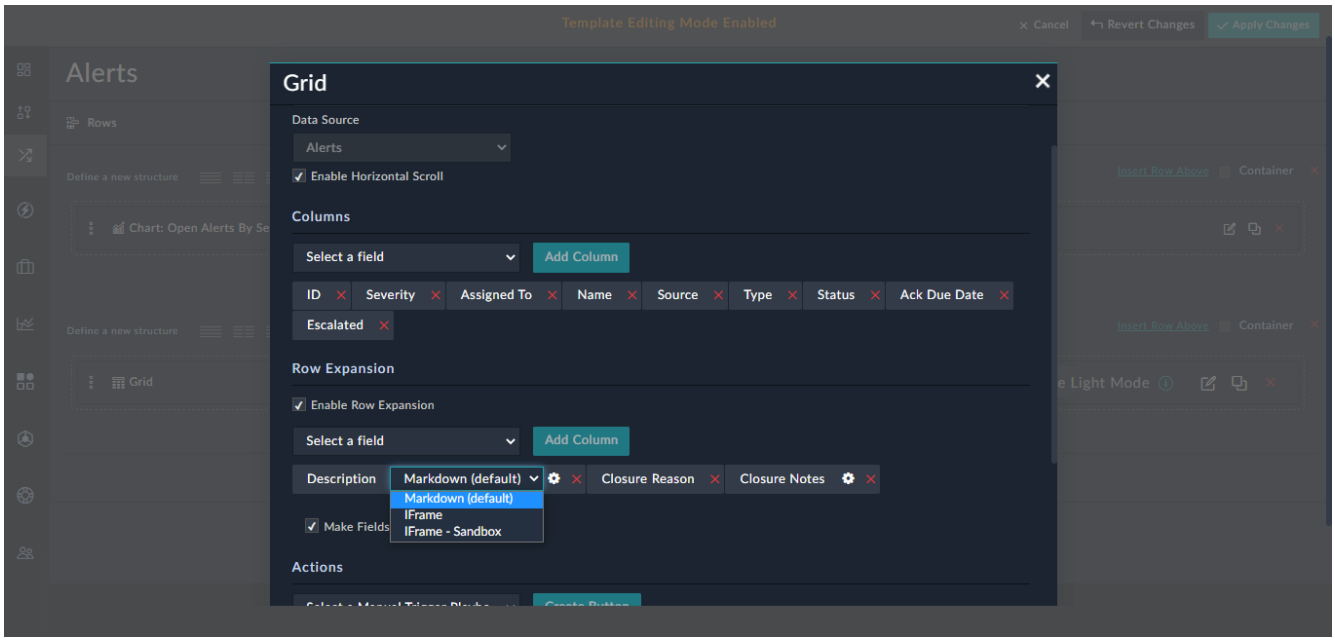
To edit a grid, click the **Edit** icon in the Grid Widget row. A grid holds records belonging to a single record type based "Data Source" that you have specified. For example, if you select the **Data Source** as **Alerts**, then the widget displays only those records whose type is "Alerts."



It is recommended that you should use the Simple Grid widget and *not use* the Grid widget to create Reports.

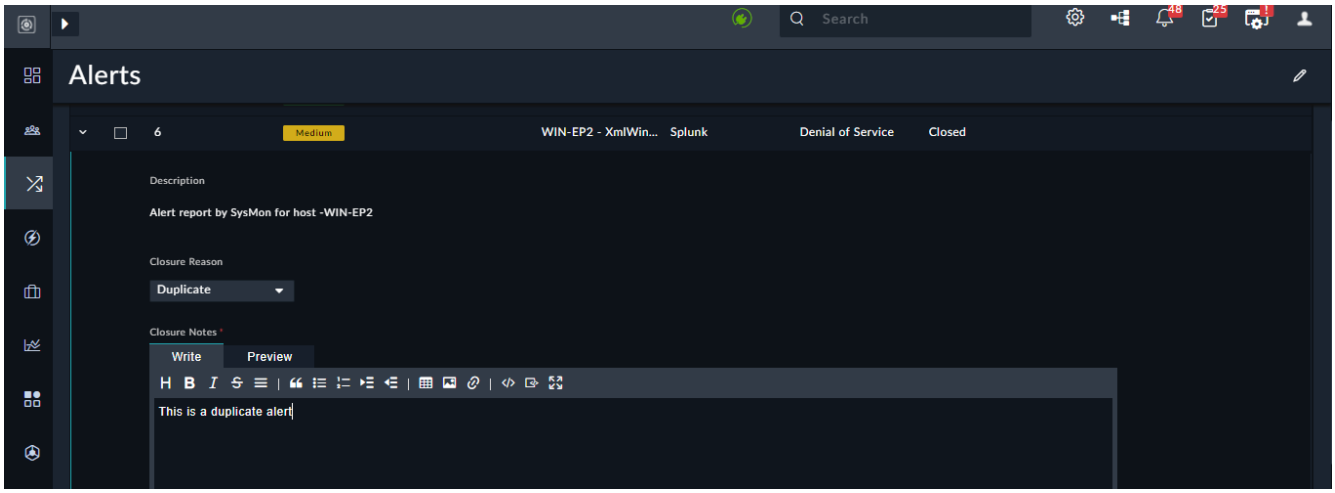
If you want to allow horizontal scrolling in grid views, which provides better usability in scenarios where the data grids that have a large number of columns, then select the **Enable Horizontal Scroll** checkbox. If after enabling the horizontal scroll, you decide that you do not want a horizontal scroll, i.e., you clear the **Enable Horizontal Scroll** checkbox, then all the columns of the grid will go back to having equal width.

If you want to display an overview of record in the grid view itself instead of the user having to open the record in the detail view, then select the **Enable Row Expansion** checkbox. From the **Select a field** list, select the fields that will be displayed as part of the record overview when the user clicks the expand icon (**>**) in the record row. From version 7.2.0 onwards, you can also choose to edit the fields that are part of the expanded row by selecting the **Make Fields Editable** checkbox. This is useful in cases such as, analysts working in the preview mode itself can quickly select the appropriate closure reason for an alert and add the closure notes to the alert. You can also choose how to render a text field that has its subtype set to "Rich Text", either Rich Text (Markdown), which is the default or Rich Text (HTML). For example, in the following image, you can choose how you want to render the "Description" field, from the following options: **Markdown (default)**, **iFrame**, or **iFrame (Sandbox)** by clicking its **Settings** () icon:



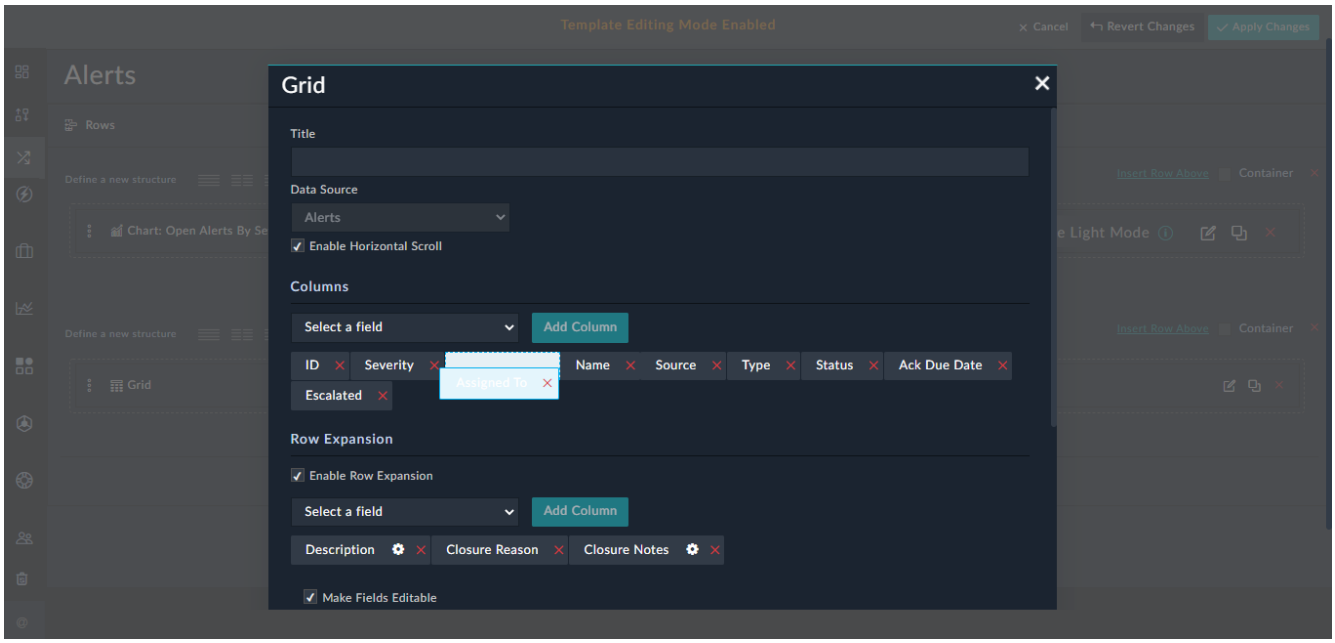
Similarly, if you have a text field that has its subtype set to "Rich Text (HTML)", you can choose how you want to render that field from the following options: HTML (default), iFrame, or iFrame (Sandbox), and if you have a text field that has its subtype set to "Text Area", you can choose to display it in the JSON format.

The following image illustrates how a record with its row expanded is displayed in the Grid view:

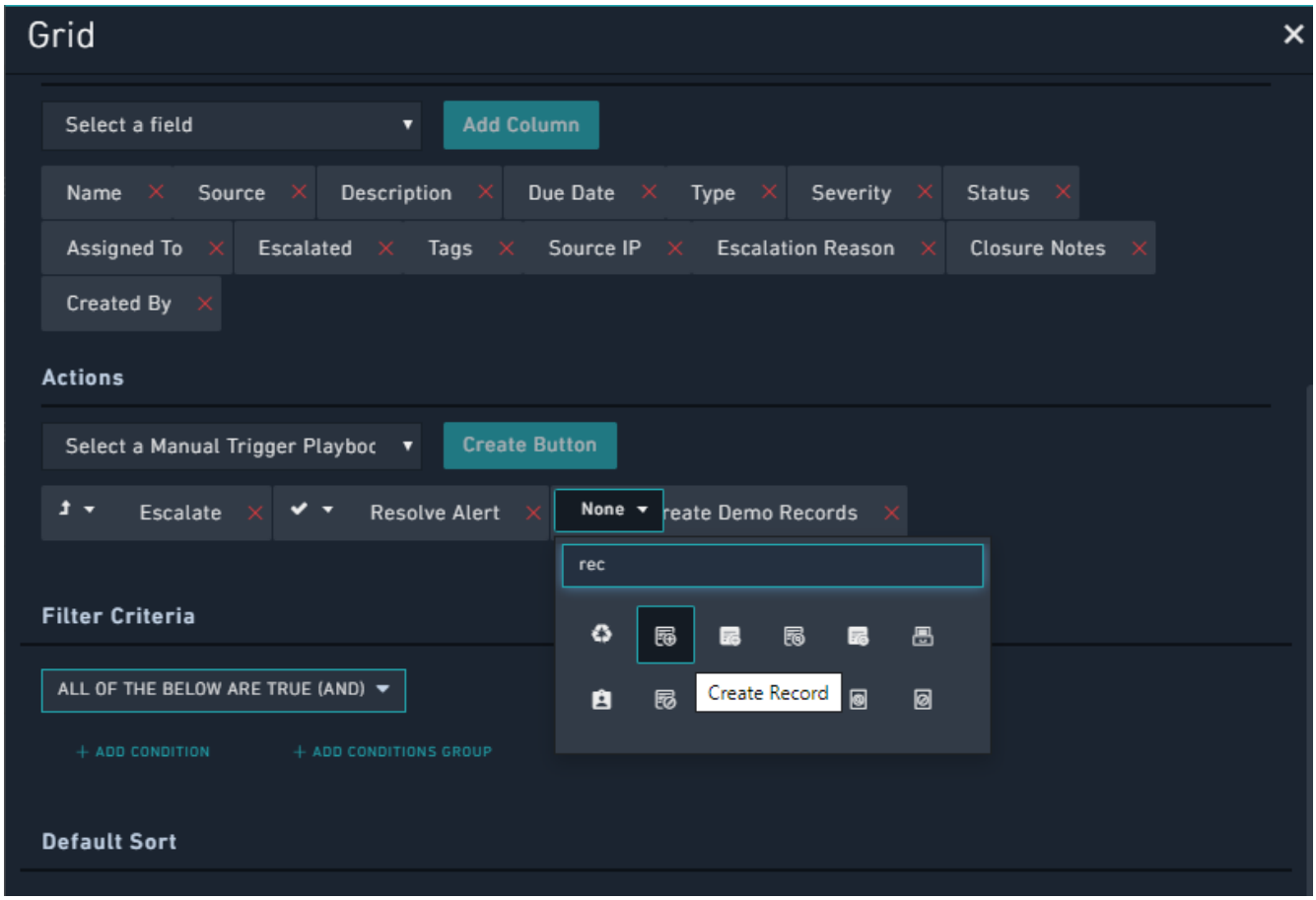


In the Grid widget in Reports and Dashboards, you will find an additional **Limit** field, in which you can specify the number of records that will be displayed on a single page for that module. By default, this is set to `30`.

In the `Columns` section, select the columns that will be displayed as part of the grid in the `List` view of the module. To add the field as a column, select the field to be part of the grid from the **Select a Field** list and then click **Add Column**. You can add tags, which are very useful in locating records, to records by choosing the **Tags** field. You can add special characters and spaces in tags from version 6.4.0 onwards. However, the following special characters are not supported in tags: `'`, `,` , `"`, `#`, `?`, and `/`. Once you add the **Tags** column, you can add and search for tags while adding or editing records. You can also change the position of how the columns will be displayed in the grid by dragging and dropping the field to the appropriate place on the grid as shown in the following image:

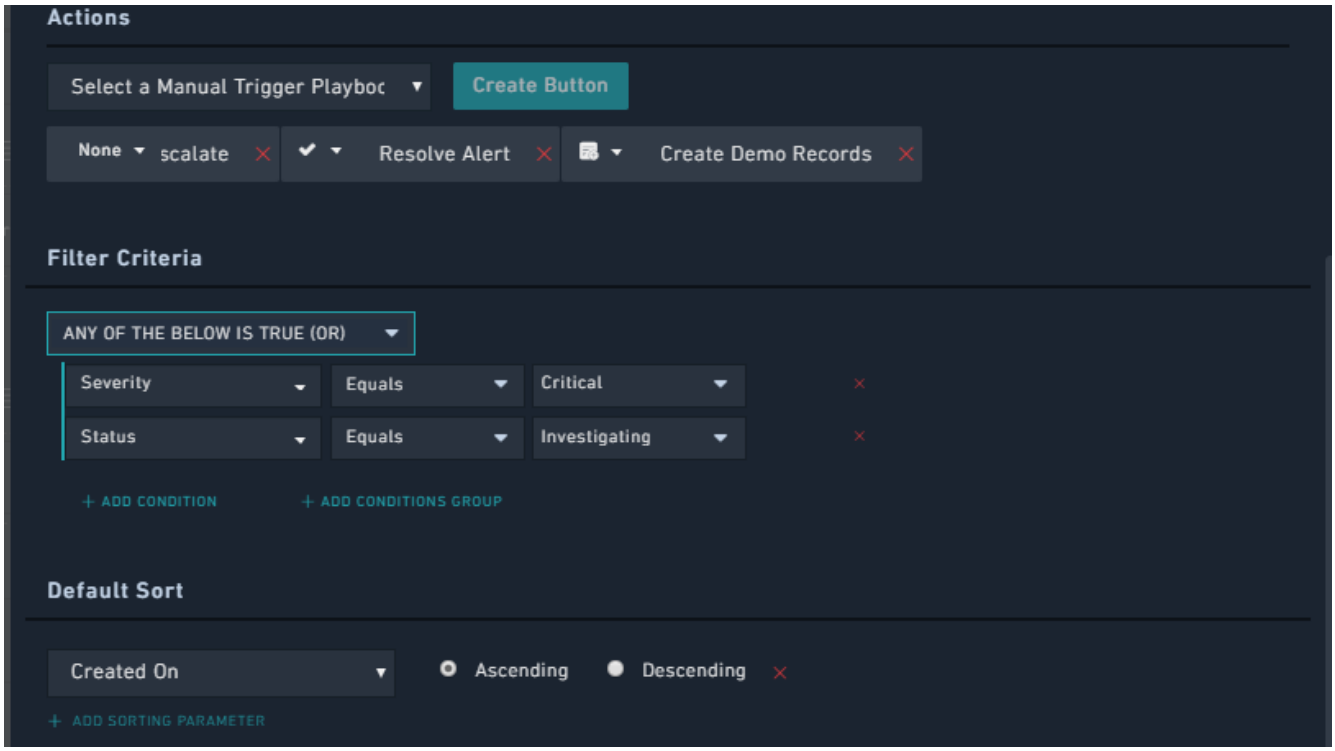


In the `Actions` section, you can create buttons for commonly used actions by selecting a manual trigger playbook from the **Select a Manual Trigger Playbook** list and click **Create Button**. You can search and select an icon that that will be displayed on the action button from the **Filter Icons** list. If you do not want an icon to be displayed, select **None**. The names that are displayed in the **Select a Manual Trigger Playbook** drop-down list, and therefore the name of the manual trigger button, are the names that you have specified in the **Trigger Label Button** field in the playbook.



You can also define filters for records in the Grid widget itself. The Grid Widget includes the Nested Filters component that you can use to filter records in the list view using a complex set of conditions, including the **OR** condition. See the Nested Filters section for more information.

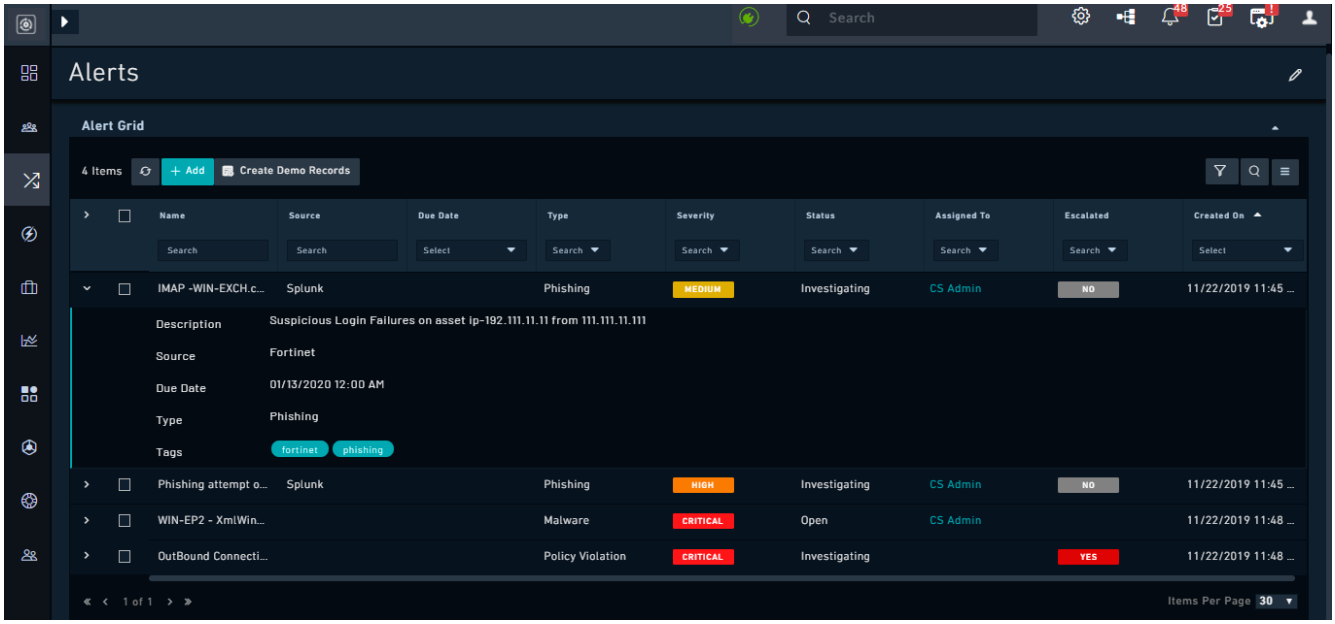
The following image includes a specific filter criterion for filtering records that have `Severity Equal to Critical` **OR** `Status Equal to Investigating`:



You can also use Default Sort to specify fields based on which the records in the module will be sorted by default.

Once you have made all the changes to the Grid widget, click **Save** and **Apply Changes** to view the updates made to the `List View` in the module.

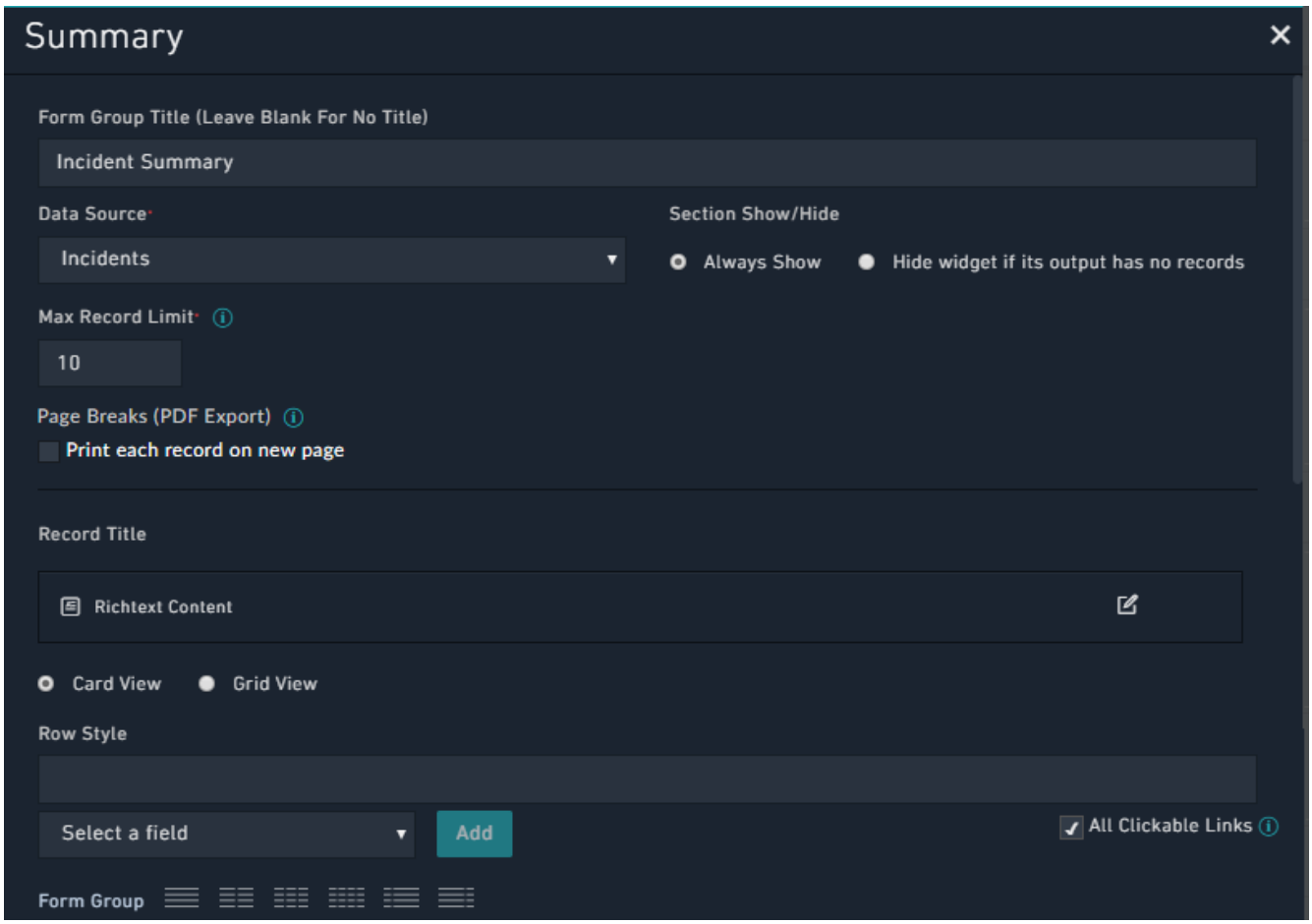
The following image displays the List view of the module, with a record being expanded, in which the `Severity Equal to Critical`**OR**`Status Equal to Investigating` filter has been applied:



Summary

Use the summary widget to display multiple editable fields that you can display in the record detail header, with an aim to summarize the record quickly.

When you are adding or editing the Summary widget in Dashboards and Reports, you must specify the Data Source for which you want to add the summary, and then select and add fields that you want to include as part of the summary, as shown in the following image:



In the `Section Show/Hide` section, you can choose to either always display this widget in the dashboard or report, the **Always Show** option (default), or you can choose to display this widget only if there is at least one record present in the selected module, the **Hide widget if its output has no records** option.

In the **Max Record Limit** drop-down list, you can also specify the maximum number of records you want to see in the summary widget, by default, it is set to **10**.

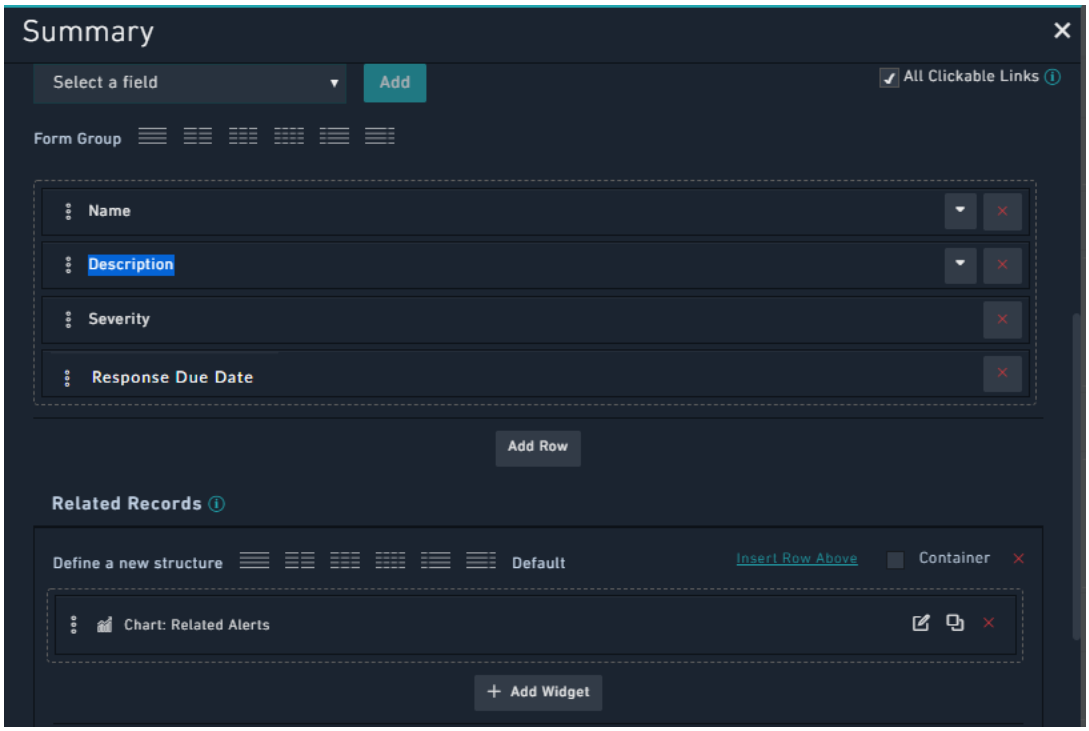
From version 7.0.2 onwards, you can choose to add a page break after each iteration of the Summary widget by clicking the **Print each record on new page** checkbox. If you select this checkbox, then for example, if you have configured your Summary widget to display critical alerts with their related incidents, then the summary of each critical alert along with its associated incidents get displayed in a new page. If you do not select the checkbox, then the critical alerts and their associated incidents are displayed one after the other without any page breaks.

The `Record Title` section contains the `Richtext Content` widget, using which you can define a stylized title for each looping section within the Summary widget. See the Richtext Content section for more information.

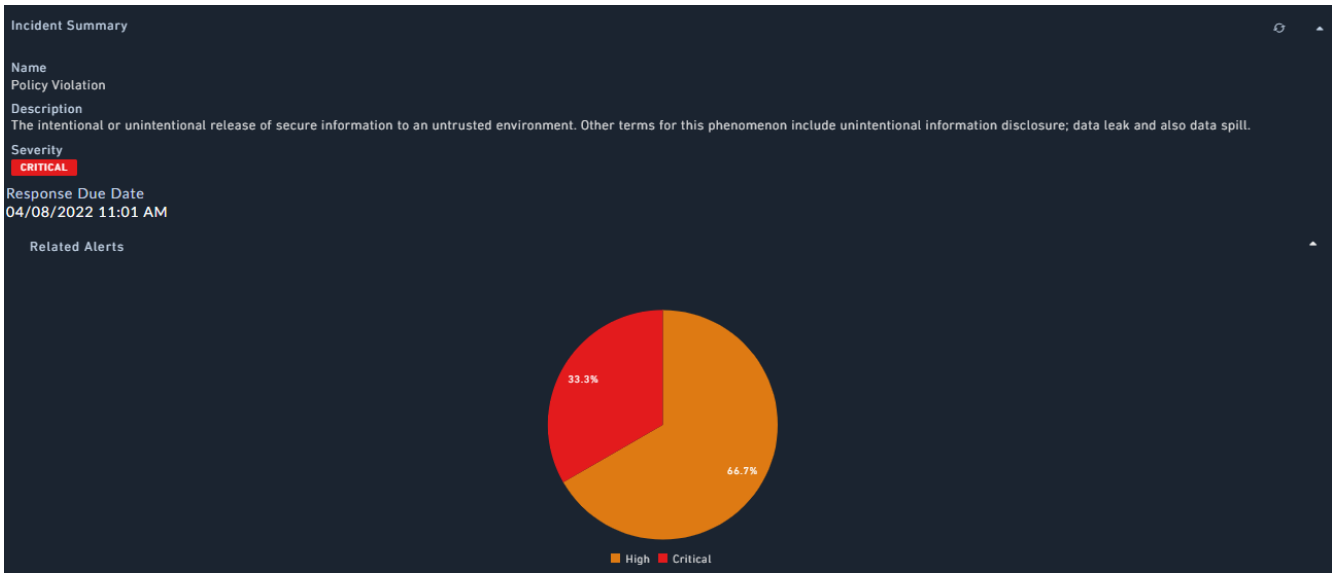
You can choose whether you want to view the Summary in the **Card View** or the **Grid View**.

From the **Select a Field** drop-down list, select the fields that you want to be part of the Summary and click **Add**.

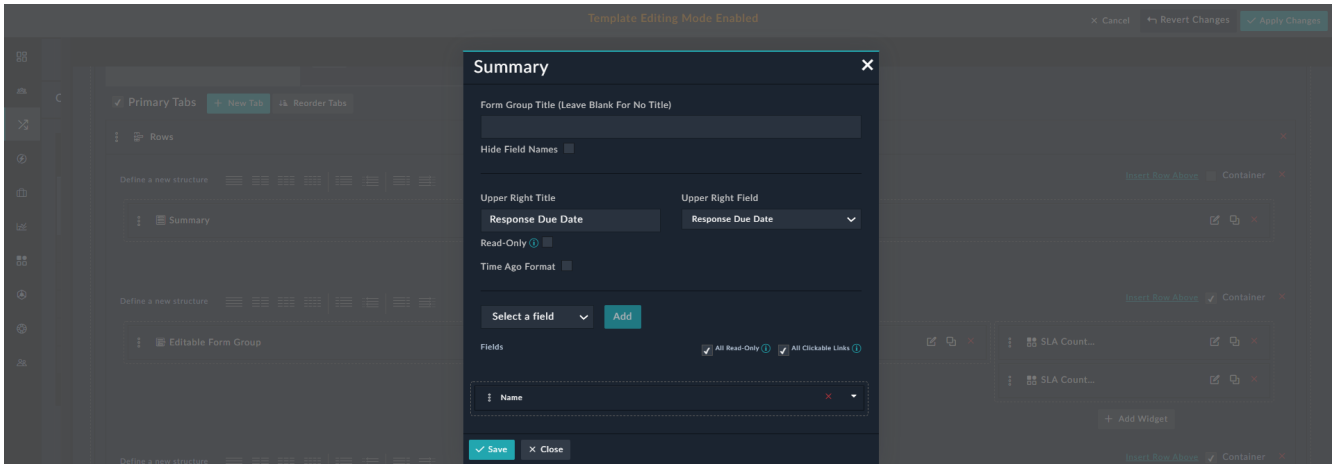
In the `Related Records` section, you can add the widgets of the linked records belonging to the selected record, i.e., you can add related widgets that you require within the Summary widget. For example, if you want to display an incident summary along with all its linked alerts, in a single Dashboard or Report, you can use the Summary widget and in the Related Widgets section, you can add a chart widget that displays linked alerts:



The following image illustrates how the Summary widget that you have defined above will appear in a Dashboard or a report:



In case of the ***Detail*** view, since you are already in a module, you do not need to specify the module. All you need to do is select and add fields that you want to include as part of the summary, as shown in the following image:

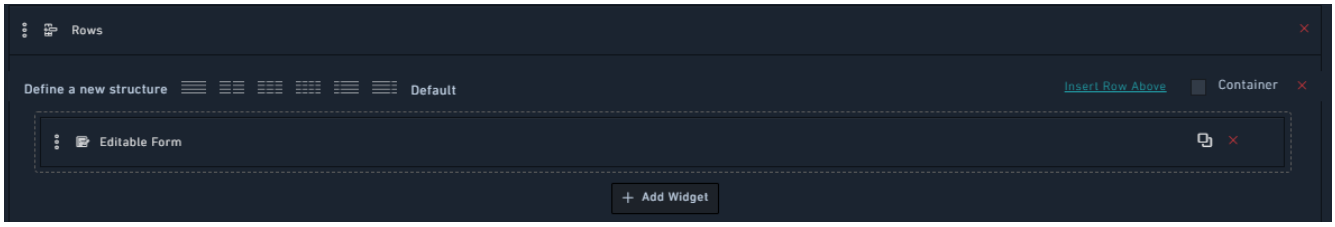


Record Fields

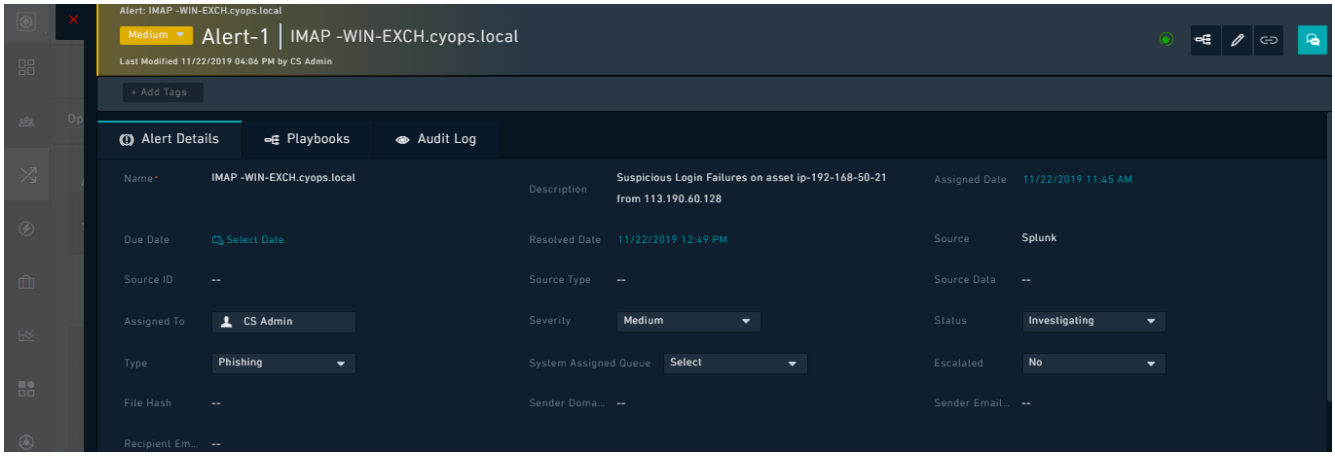
Editable Form and Editable Form Group

Form Group widgets display records as part of an editable form. There are the following types of form widgets:

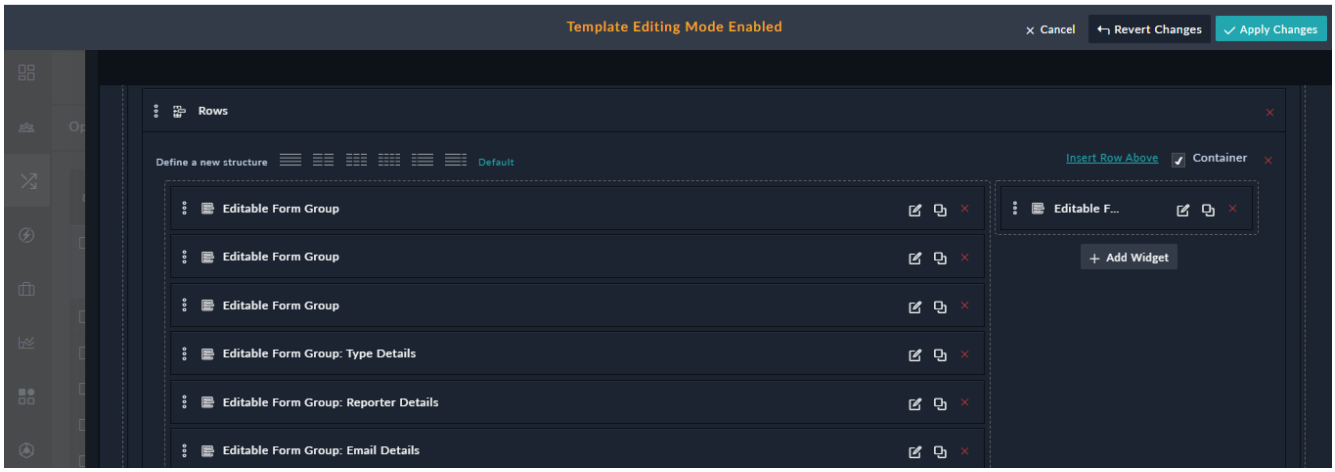
Editable Form widget: Use this widget to insert a form that contains all the editable fields for the Alerts module. You cannot choose fields in this widget and all the editable fields of the current module are included.



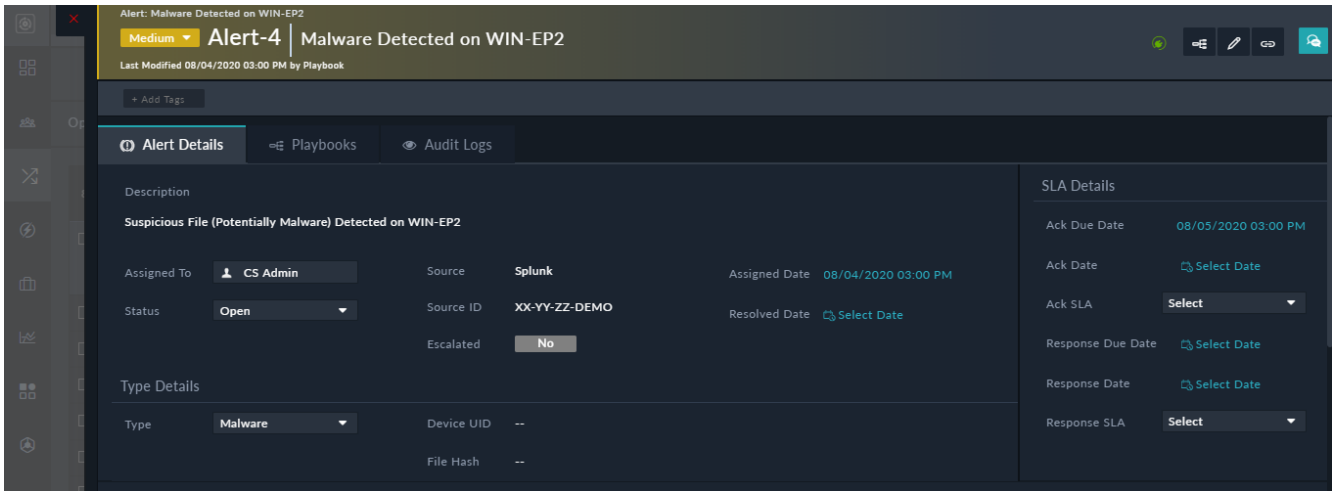
The following image illustrates how the Editable Form widget is displayed in the Detail View of a record:



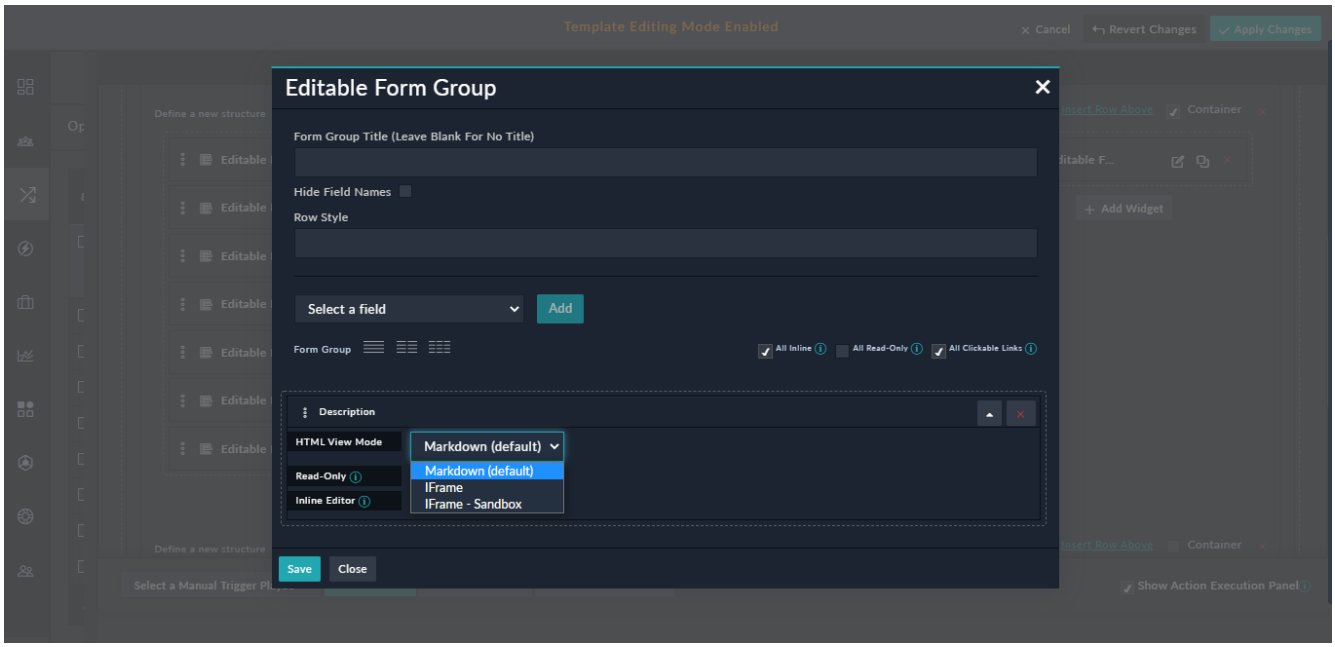
Editable Form Group widget: Use this widget to insert a group of standalone form fields. You can use this widget to create a form that users can use to fill in the details for a record:



The following image illustrates how the Editable Form Group widget is displayed in the Detail View of a record:



If you have a text field that has its sub-type set to "Rich Text (Markdown)" such as the "Description" field, you can choose how you want to render that field from the following options: **Markdown (default)**, **iFrame**, or **iFrame (Sandbox)**:



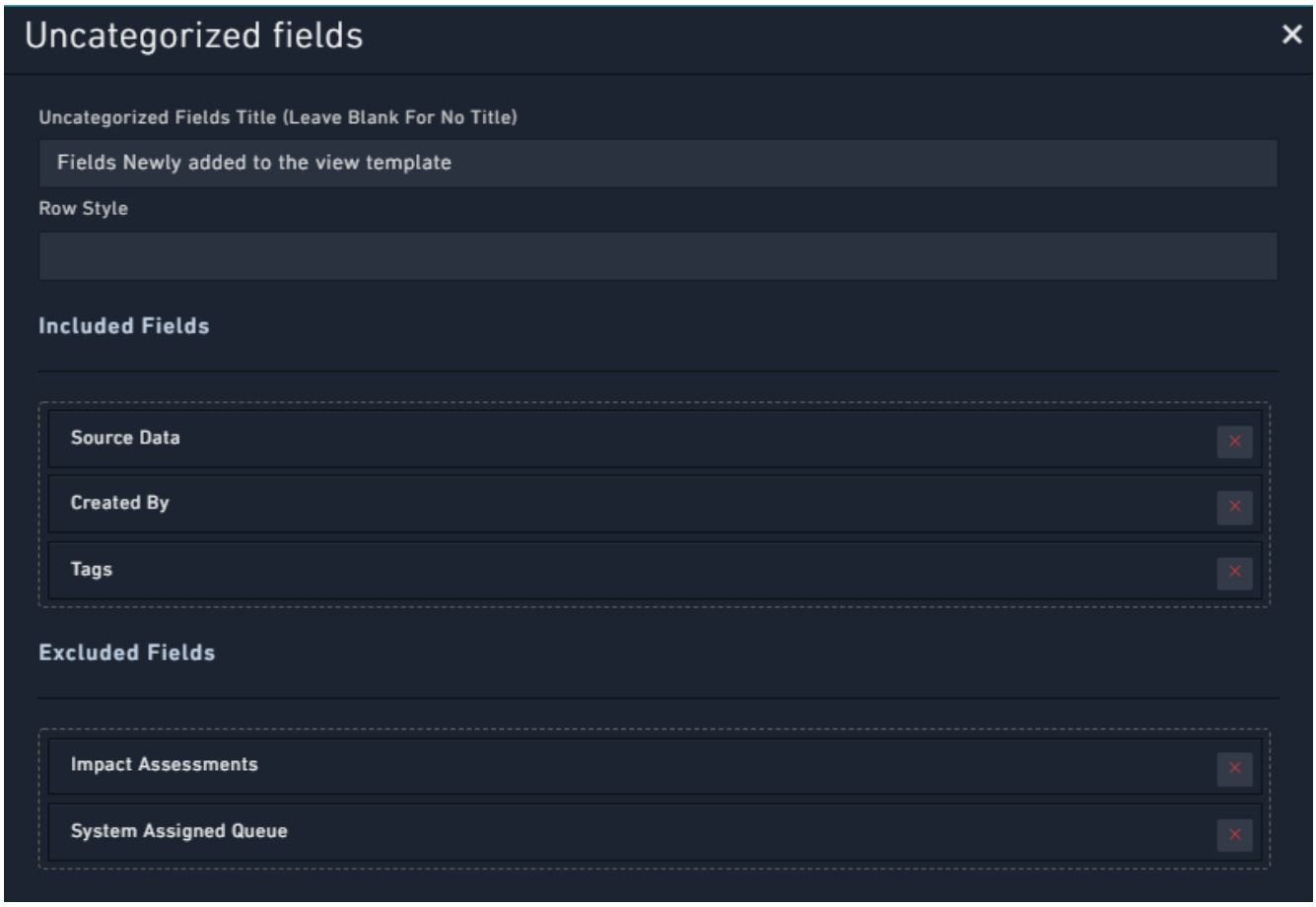
Similarly, if you have a text field that has its sub-type set to "Rich Text (HTML)", you can choose how you want to render that field from the following options: HTML (default), iFrame, or iFrame (Sandbox), and if you have a text field that has its subtype set to "Text Area", you can choose to display it in the JSON format (See Displaying "Text Area" fields in the JSON format).

Important: When the sub-type of a field is set as Rich Text (HTML) or Rich Text (Markdown), and this field expects data to be populated from external data sources using data or email ingestion, then ensure that the System View Template (SVT) of the field is set to 'iFrame', i.e., select **iFrame** as the **HTML View Mode** of this field to prevent any XSS attack attempts or overriding of the parent CSS styling.

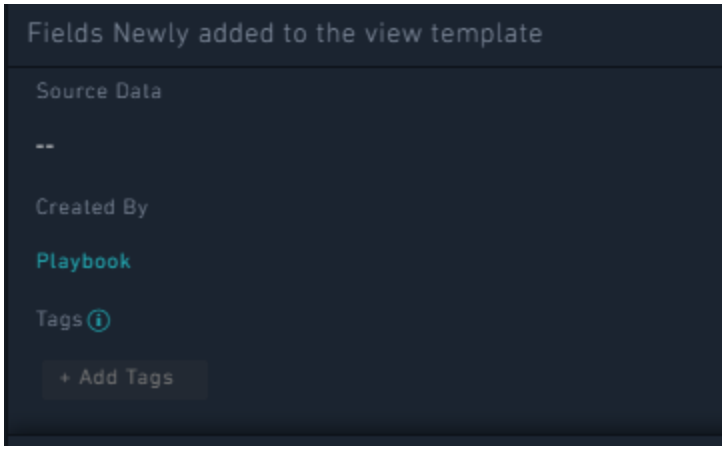
Uncategorized Fields

Use the Uncategorized Fields widget to display fields that have been newly added or the ones that have not been explicitly added to the module layout or view template. This widget evaluates missing fields by comparing the fields in the module mmd with existing fields added in the view panel (module layout) of that module. Similarly, whenever you add any new fields to a module, those also will be displayed in this widget and you can choose to display those fields in the view panel.

For example, if you select the Incident Module and add the Uncategorized Fields widget, you will see the fields that are present in the module but not added in the view panel, which are Source Data, Impact Assessments, System Assigned Queue, Created By, and Tags. The missing fields are shown in the `Excluded Fields` section. To choose the fields that you want to display in the view panel, click the red cross in the row of those fields. These fields will move to the `Included Fields` section and will be shown in the view panel. For example, if you do not want to include the Source Data, Tags, and Created By fields in the view panel, then click the red cross in that row in the `Excluded Fields` section, which will then move these fields into the `Included Fields` section, as shown in the following image:



The following image illustrates how the Uncategorized Fields widget is displayed in the Detail View of a record:



Summary

Use the summary widget to display multiple editable fields that you can display in the record detail header, with an aim to summarize the record quickly. For more information, see the Summary section above.

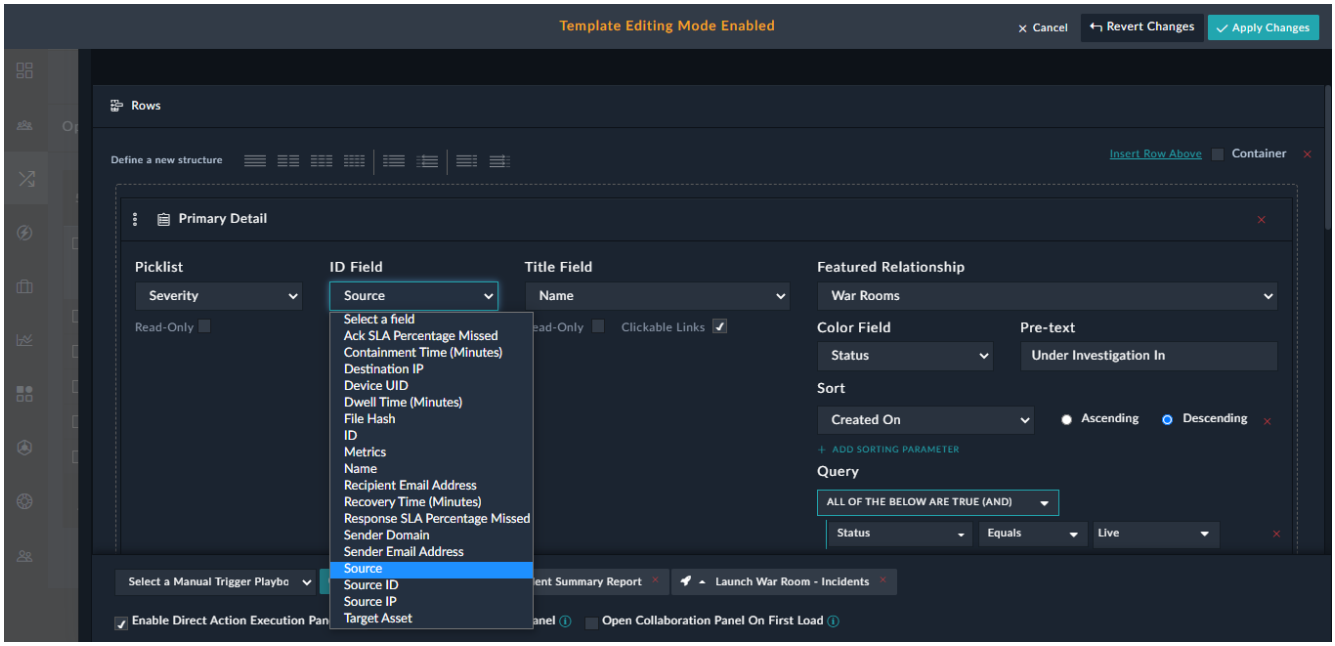
Header Widgets

Primary Detail

Use the Primary Detail widget to add a Header row that is a top-most field to display a record title. You can choose whether this field would be editable or not. If you do not want the Header row items to be editable, then click the **Read-Only** checkbox for the **Picklist** and **Title Field** fields. If you want any URLs in the Header row to be clickable, then click the **Clickable Links** checkbox.

You can choose the ID field that will be displayed in the Primary Details row in the Detail View of a record. The ID field that you can choose is limited to integer fields or text fields. For example, you can choose **Source** as the ID Field to be displayed in the Detail View of a record. By default, the system ID is selected in the ID Field drop-down list.

From version 7.0.0 onwards, a new **Featured Relationship** widget is added to the Primary Detail widget. This widget displays a single related record, which is usually utilized to show any active war room or other investigation. To configure this widget, use the **Select a field** drop-down to select the relationship field you want to display in this record. For example, select **War Rooms**. In the **Color Field** choose the field which will be used to display the color of the indicator circle. In the **Pre-text** field, enter the text that should appear before the record ID. To drill down on the specific record that will be displayed, specify the query filters and sort order. For example, in case of war rooms, this widget gets displayed only if the "*War Room status is set to Live*" and it uses the most recent War Room since the sort is set to *Created On* (descending order).



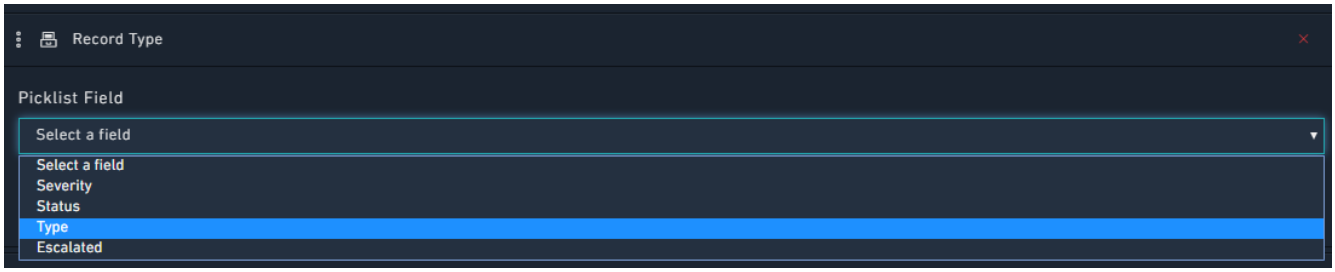
This widget adds a row that has a large font-size and no field label. You will also see **+ Add Tags** field in this row using which you can add tags to the record making it easier for searching and filtering records.

The following image illustrates how the Primary Detail widget is displayed in the Detail View of a record if you have selected **Source** as the ID Field, and the incident is part of War Room-1:

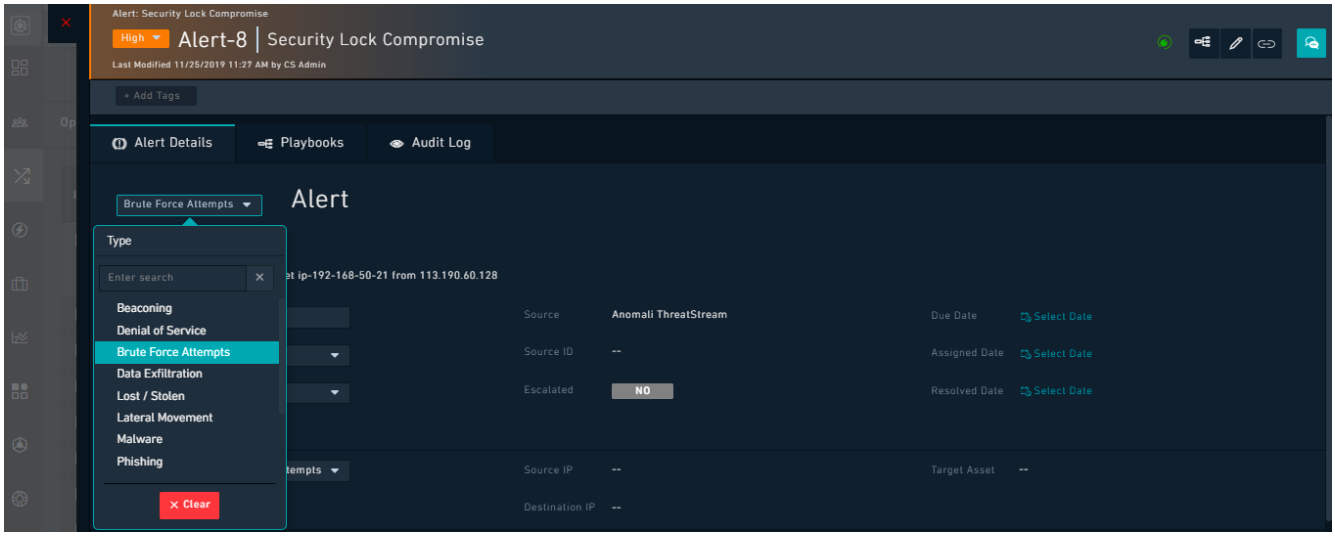
The following image illustrates how the Primary Detail widget is displayed in the Detail View of a record if **ID** is retained as the ID Field, and the incident is part of War Room-1:

Record Type

Use the Record Type to add a stylized field in the top left of the record to display the fields such as severity, status, type, etc of the record.



The following image illustrates how the Record type widget is displayed in the Detail View of a record, when **Type** is selected to be displayed:



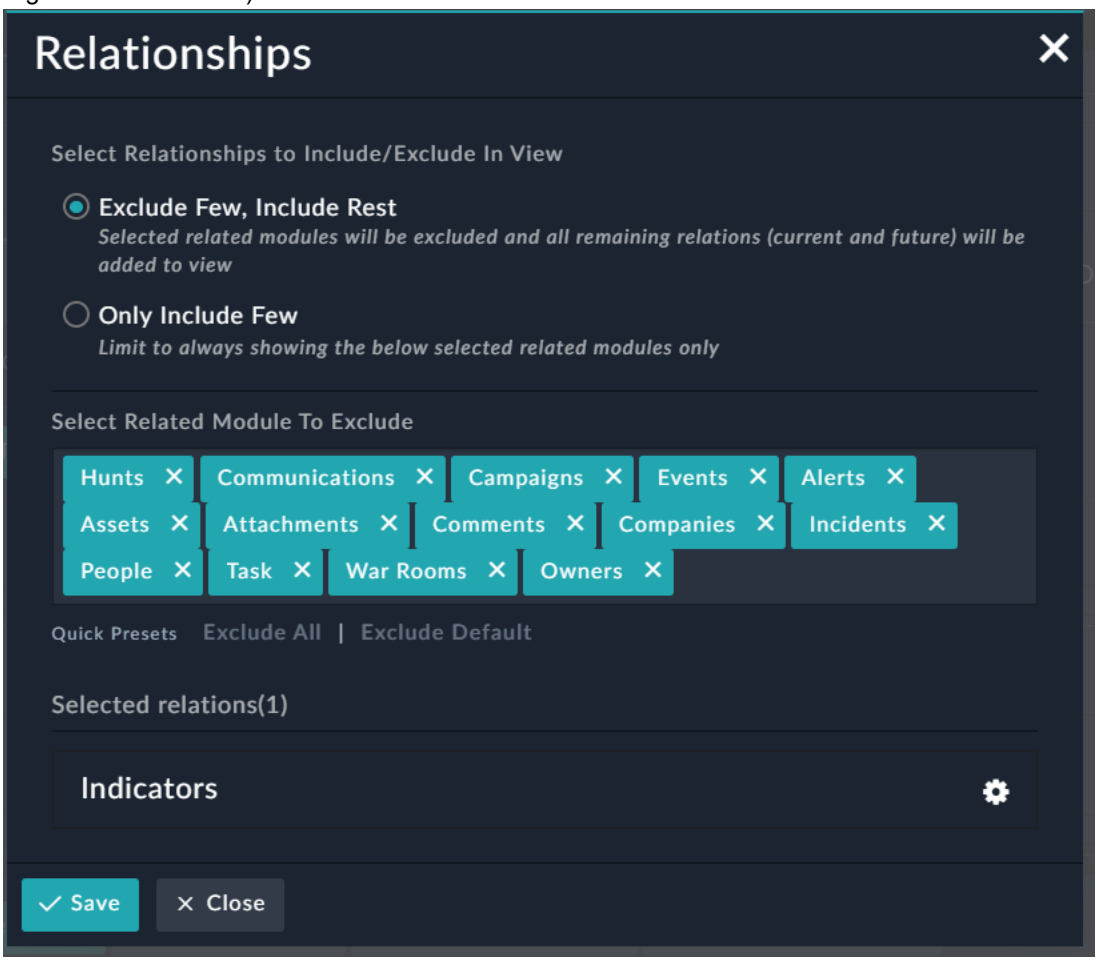
Related Record Listing

Relationships

The Relationships widget displays relationships between the current module and other modules. For example, if the current alert row has a corresponding indicator, then that indicator is displayed as a row, using this widget.

You can select the relationships that you want to include or exclude from the view, i.e. in the **Relationships** tab of the current module. By default, **Exclude Few, Include Rest** option is selected, i.e., by default, a few modules of your choice

are excluded from the view, and all the remaining modules, both current (existing modules) and future (modules that you might add in the future) are included in the view:

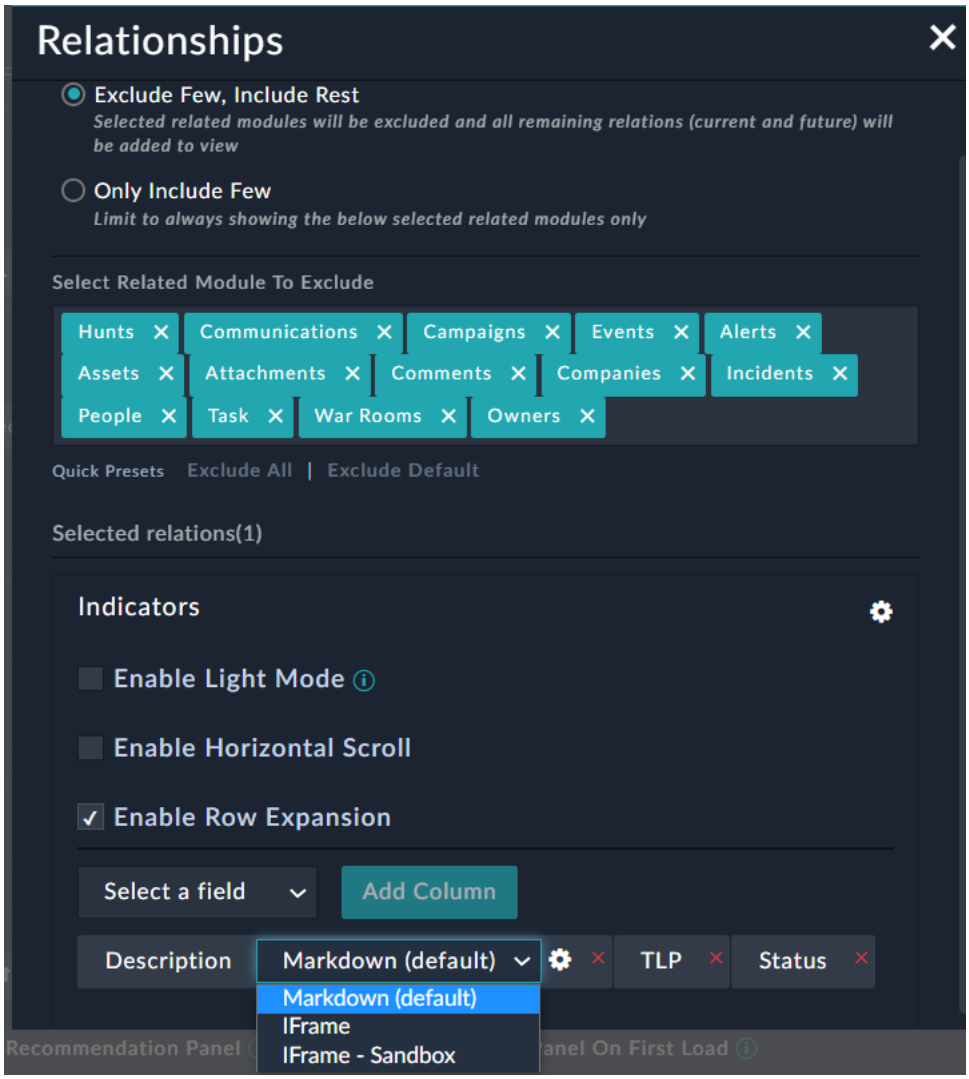


The other option is **Only Include Few**, which limits modules displayed in the view to only those that you explicitly select in the **Selected Relation Modules To Include** list. Therefore, in this case newly added modules do not get included in the view.

The **Selected Related Module To Exclude** lists the modules that will be excluded from view, you can choose to add more modules to this list or remove some modules from this list. You can also use the options present in the `Quick Presets` section to quickly exclude modules to display in the view. Click **Exclude All** to exclude all the modules from the **Relationships** tab of the current module, or click **Exclude Default** to exclude default modules, i.e., Comments and Attachments from the **Relationships** tab of the current module.

Similarly, if you choose **Only Include Few**, then from options in the `Quick Presets` section choose to quickly include modules to display in the view. Click **Include All** to include all the modules from the **Relationships** tab of the current module, or click **Include All (Skip Default)** to include all modules except the default modules, i.e., Comments and Attachments in the **Relationships** tab of the current module.

You can now set up how the relationships are displayed in the current record by clicking the **Settings** ( ) icon in the row of the relationship you want to edit, for example, in the **Indicator** row:

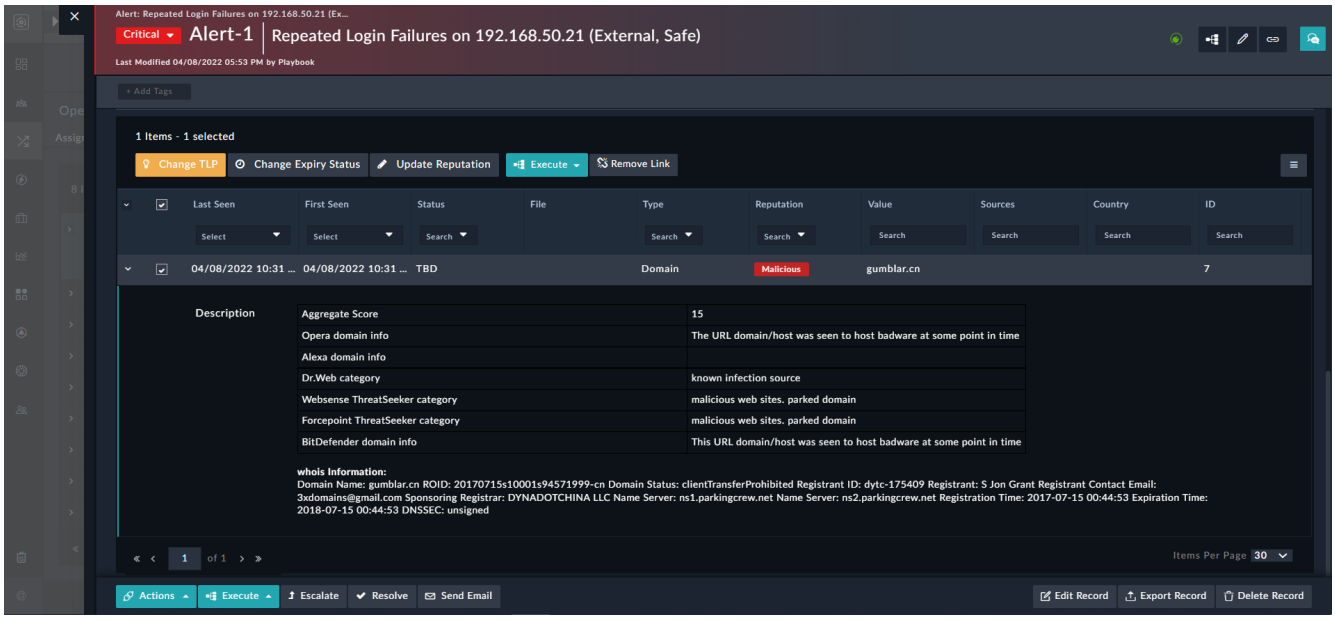


You can set up the following:

- **Enable Light Mode**: Select this option to use a lighter version of this widget for better performance and usability.
- **Enable Horizontal Scrolling**: Select this option to allow a horizontal scroll in the case of a large number of columns
- **Enable Row Expansion**: Select this option to view details of related records in the grid view of the relationship widget itself, instead of having to open the related record in a new window to view its details. Select the **Enable Row Expansion** checkbox and from the **Select a field** list, select the fields that will be displayed as part of the record overview when the user clicks the expand icon (**>**) in the record row.
  You can also choose how to render a text field that has its subtype set to Rich Text (Markdown), which is the default, or Rich Text (HTML). For example, in the above image, the "Description field" is subtype is set to Rich Text (Markdown; therefore, you can choose how you want to render the "Description" field, from the following options: **Markdown (default)**, **iFrame**, or **iFrame (Sandbox).** Similarly, if you have a text field that has its subtype set to "Rich Text (HTML)", you can choose how you want to render that field from the following options: **HTML (default)**, **iFrame**, or **iFrame (Sandbox)**, and if you have a text field that has its subtype set to "Text Area", you can choose to display it in the **JSON** format.

Once you are done with your changes, click **Save**.

The following image illustrates how the Relationships widget is displayed in the Indicator tab of the detail view of an alert record:



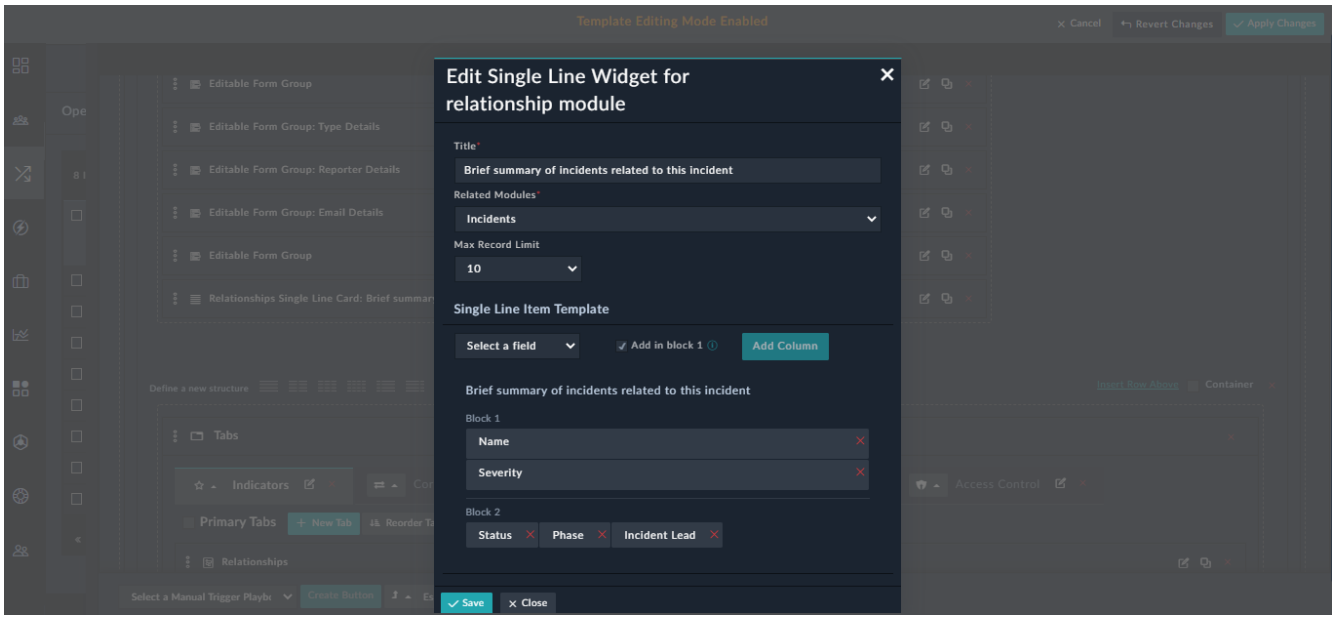
Relationships Single Line Card

The Relationships Single Line Card widget like the Relationship widget displays relationships between the current module and other modules. However, it displays the related records in a single row and column. You can define the fields that you would like to see for the related record in a single view.

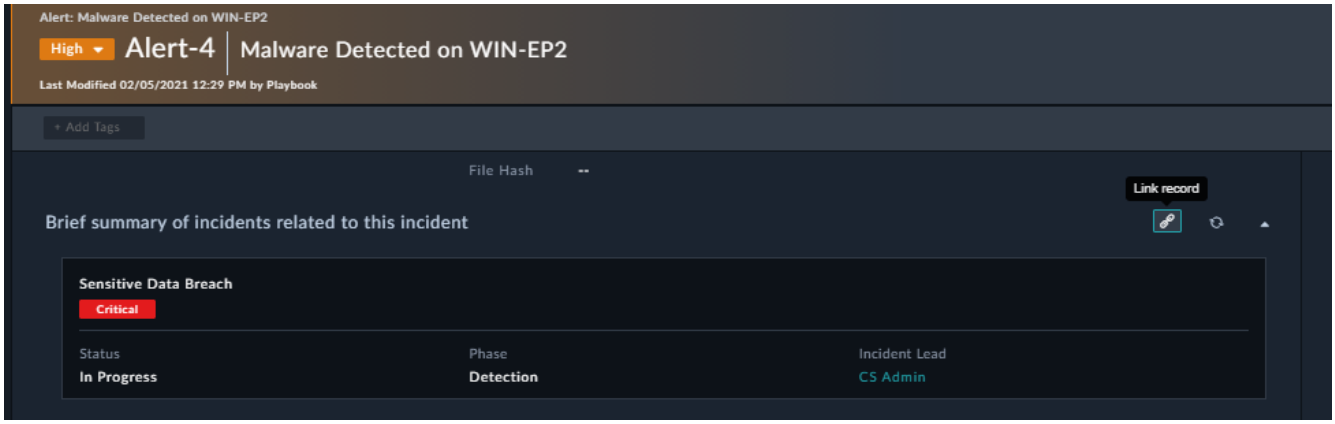
Version 7.0.0 enhances this widget to make it more intuitive and represent relationships in a user-friendly way. You can now link new records from the rendered widget, and also display more fields using this widget with greater control over the layout of the fields.

You can select fields from the **Select a field** drop-down list, and choose which block you want to display that field. To add a field in block one, select the field, and select the **Add in block 1** checkbox, and then click **Add Column**. Each field in Block 1 gets displayed in their own row. To add a field to Block 2, ensure that the **Add in block 1** checkbox is cleared (default). Fields in block 2 get grouped.

For example, in the following image, the Relationships Single Line widget has been defined for alerts with corresponding incidents. Also, the Name and Severity fields have been added to Block 1, and Status, Phase, and Incident Lead field have been added to Block 2:



The following image illustrates how the Relationships Single Line Card widget is displayed in the Detail View of an alert record that has a related incident record:



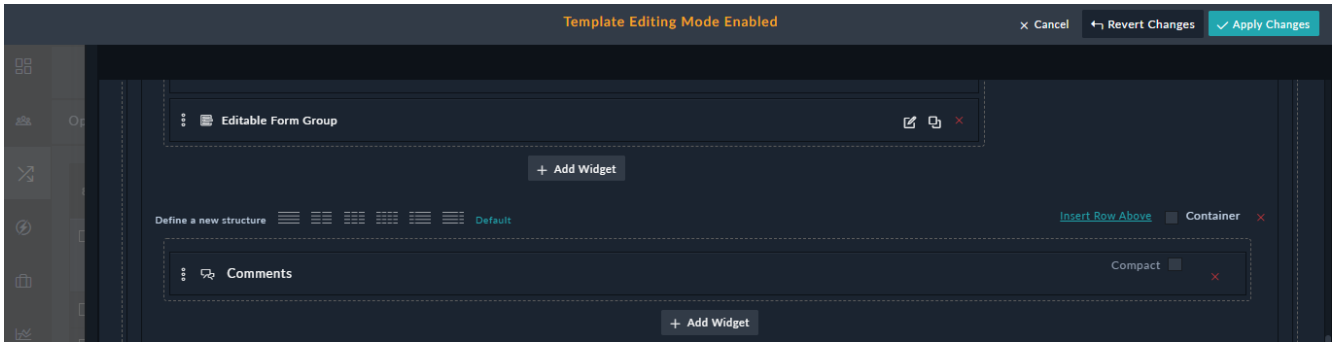
As seen in the above image, the Name and Severity fields have their individual rows, and the Status, Phase, and Incident Lead fields have been grouped in a single row. Also, you can click the **Link Record** icon to link new records from the widget.

Utility Widgets

Comments

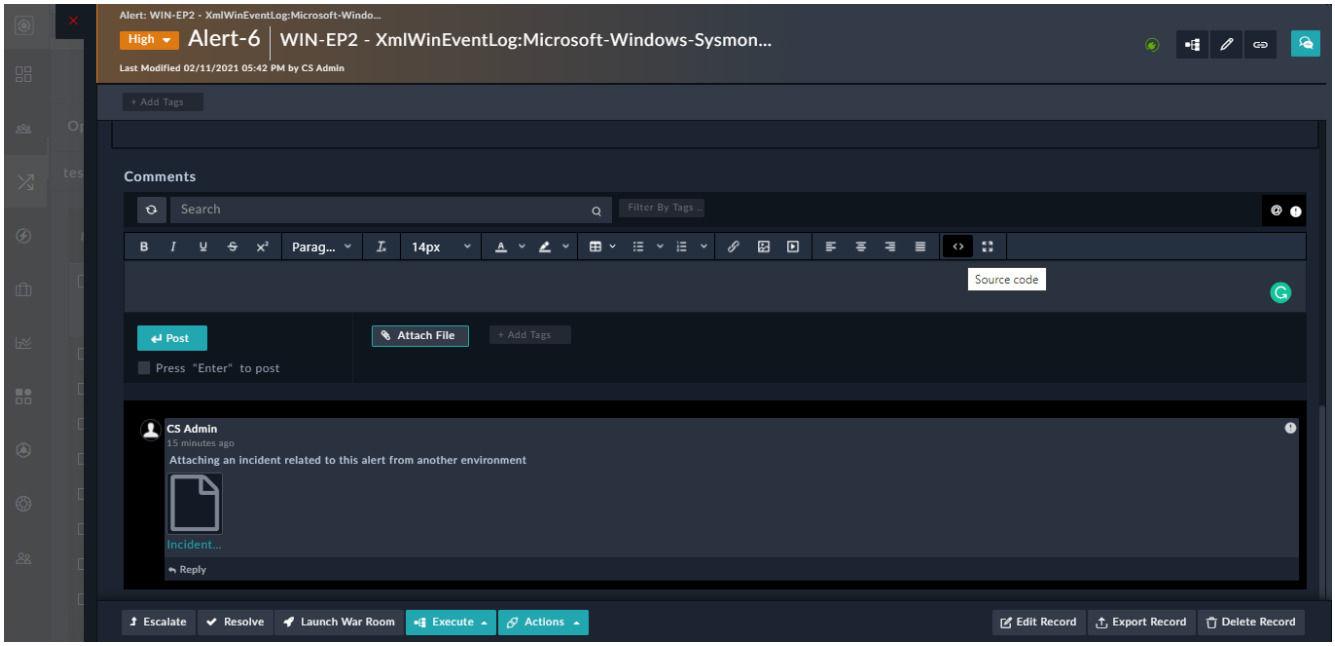
Comments are a unique record type that can be associated with any other record and displayed within the record detail interface. You can place the Comments widget anywhere within a record and comments are added in a rich text format, using formatting styles. You can also embed hyperlinks and media within comments.

Clicking the **Compact** option hides the rich text controls.

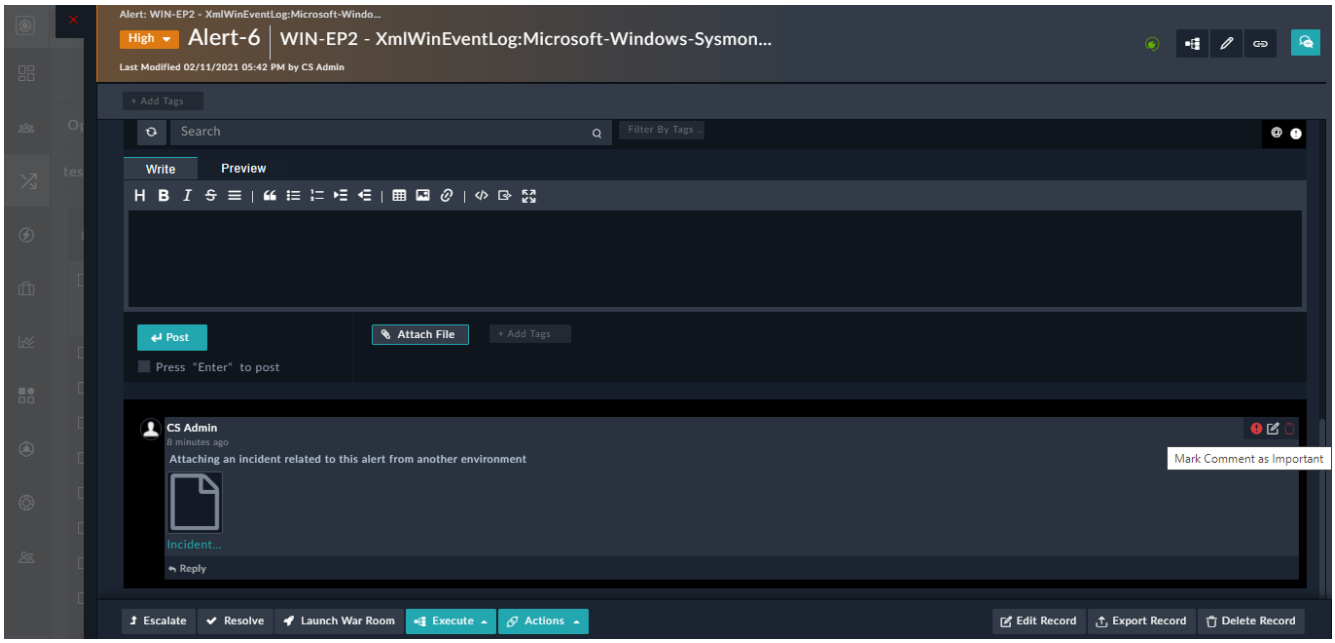


The widget displays the chronological history of all comments on that record. Comments, whether they are added using the comments widget or the collaboration panel, are automatically displayed in the Timeline (Audit Log) of any record.

From version 6.4.3 onwards, you can edit the **Contents** field in the "Comments" module, and choose how this field should be rendered, either Rich Text (Markdown), which is the default or as Rich Text (HTML). The following image illustrates how the Comments widget is displayed in the Detail View of a record, when the "Content" field is set as Rich Text (HTML):



The following image illustrates how the Comments widget is displayed in the Detail View of a record, when the "Content" field is retained as Rich Text (Markdown):



You can format, add links, and inline images to your comment using the "Styling" toolbar. You can add files or images by dragging-and-dropping files or images (these are added as inline images) onto the comments panel, or by clicking the **Attachments** button. You can attach a maximum of five files to a single comment. Both Inline images and images that are attached get appropriately resized within comments. To view the images as per its original size so that it becomes possible to read the contents of the images, click the attachment name to see the enlarged image. In case of inline images, clicking the image name downloads the original image.

Click the **Inline code** or **codeBlock** buttons to add code to the comment. You can preview the comment by clicking on the **Preview** tab and click the **Full Screen** icon to make the workspace cover the complete screen.

To add tags associated with this comment, add the tag in the **+ Add Tags** field. You can search for comments in the search using the **Search** textbox and also filter comments using tags. You can delete or modify your comments based on the settings assigned by your administrator.

Version 7.0.0 introduces some important enhancements to the comments widget such as:

- Support for message threads (or nested replies), which helps to keep track of conversations and makes it easier to respond to a specific thread.
- Ability to mark a comment as important.
- Added support for adding mentions or tagging users in comments by typing `@`, and then selecting the users from the displayed list.
- Added support for filtering comments based on tags, mentions, and the importance flag.

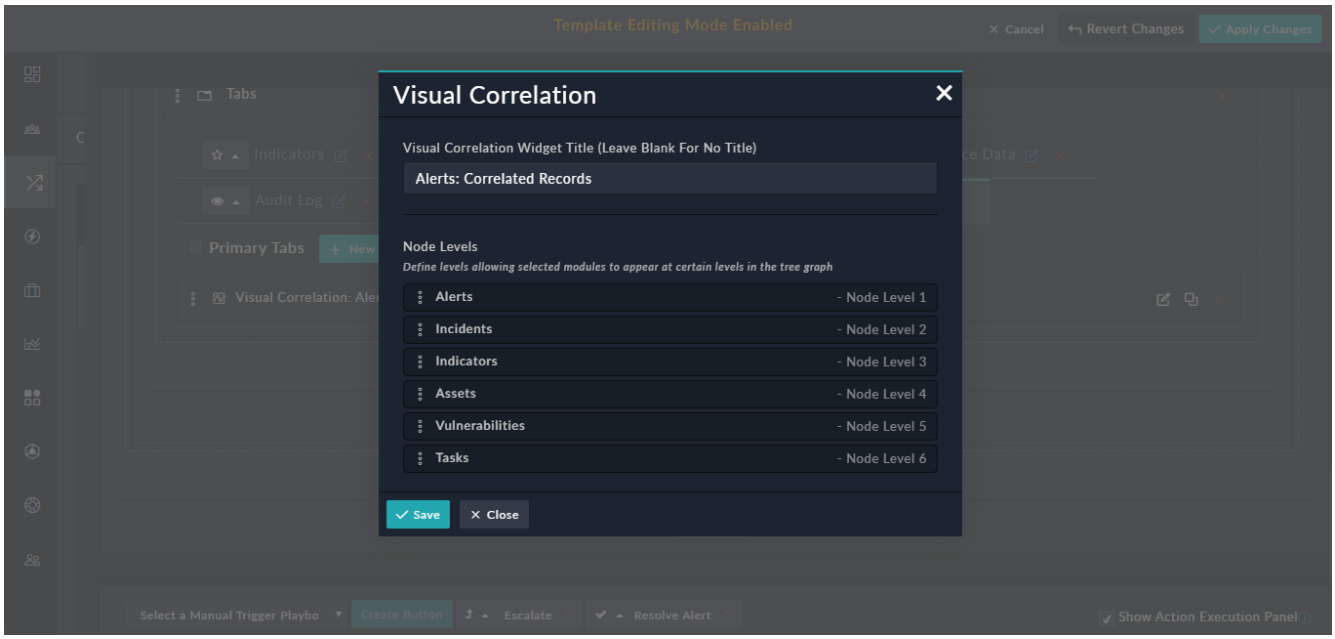
For details on these enhancements, see the Working with Modules - Alerts & Incidents chapter.

If you select the **Press "Enter" to post** option, then comments get posted immediately after the user presses `Enter`. In this case, if the user wants to add a new line, the user must use "Shift + Enter."

Visual Correlation

Use the Visual Correlation widget to visually display the nodes related to a particular record, i.e., to view the visual relationship in a graph format.

If you are adding Visual Correlation as a tab, then click **New Tab** and enter the name of the tab, for example, Visual Correlation, select an icon associated with this tab, and then click the green check mark. Click **Add Widget** in this tab and then select **Visual Correlation** in the `Choose Widget` dialog to add the visual correlation widget in the detail view of the record. You can edit this widget to add a title to the Visual Correlation graph, by clicking the **Edit** icon in the widget's row, and enter the title in the **Visual Correlation Widget Title** field, for example, `Alerts: Correlated Records`. From version 6.4.0 onwards, you can define the levels at which various nodes will be displayed in the "Tree" view of the graph. You can change the levels by dragging and dropping the nodes at the level you want to display the nodes in the "Tree" view of the graph. Click **Save** to save the changes to the Visual Correlations widget.



As shown in the above image, we have set Alerts as Node Level 1, Incidents as Node Level 2 and so on.

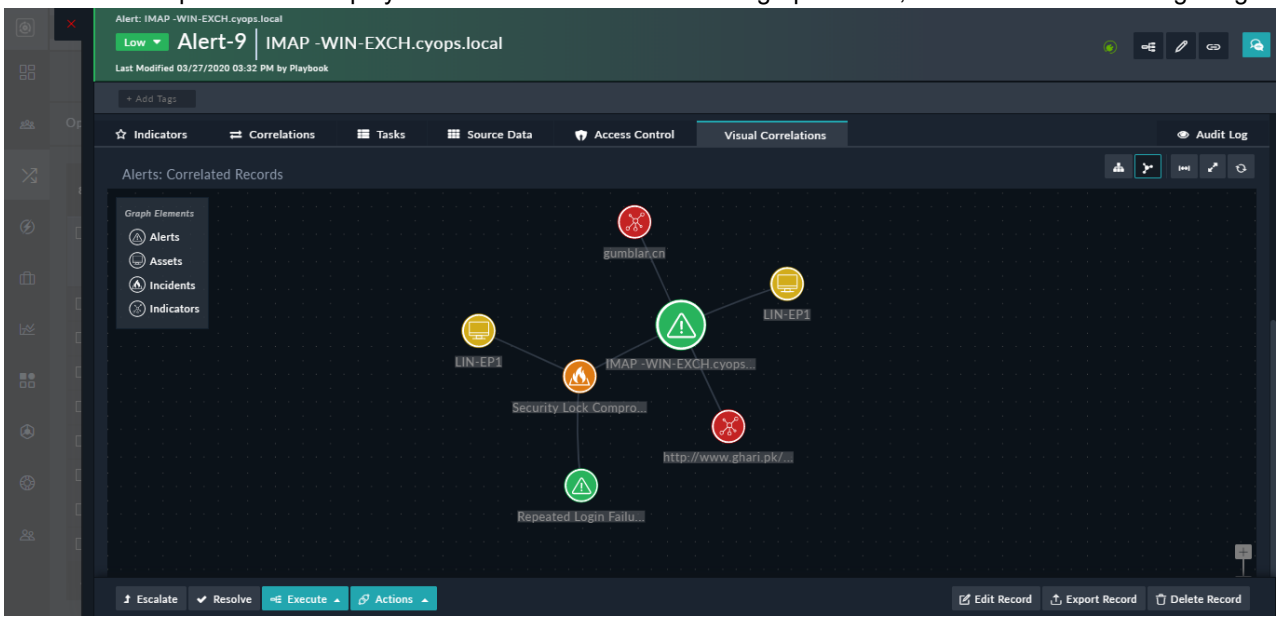
Your administrator must configure settings for the correlations for this widget to be displayed in the detail view of the record. For more information, see the *Application Editor* chapter in the "Administration Guide."

If the correlations settings are done, then you can see the Visual Correlation widget in the detail view of an "Alert" record as shown in the images in the following list.

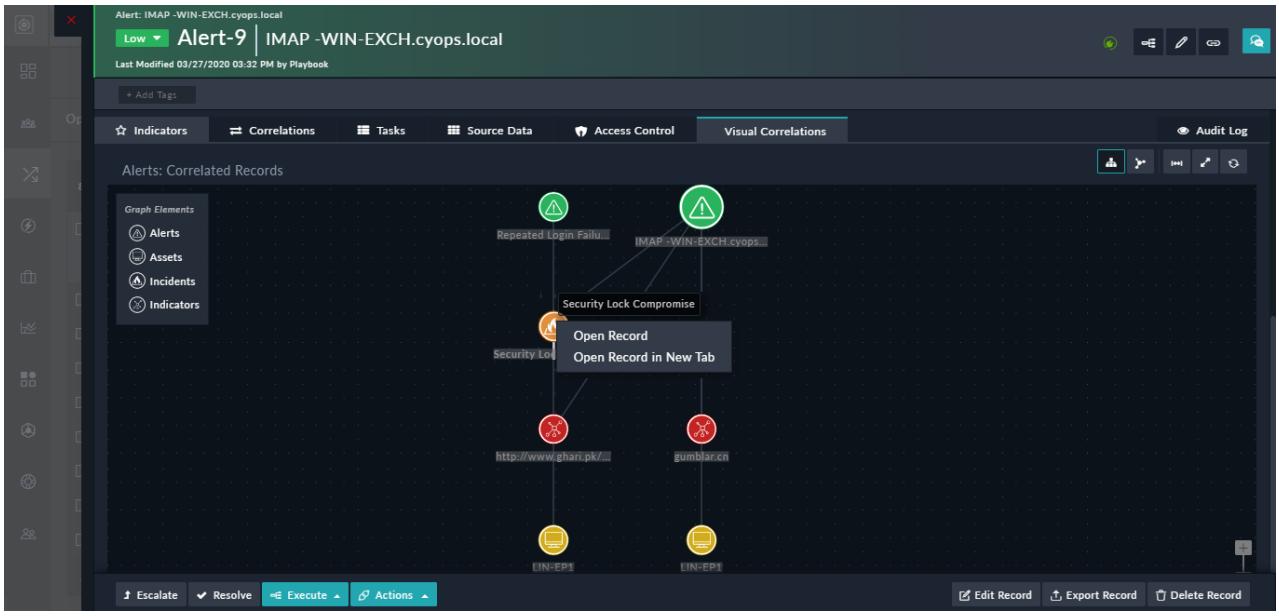
The Correlations Graph also includes the following:

- A legend that describes the node types of the related records to left of the Correlations Graph.
- The ability to fit the graph on the screen by clicking the **Fit in view** button and other usability enhancements such as zoom and pan tools.
- The ability to toggle between the **Tree** view and the **Hub and Spoke** view. The "Tree" view, which is the default view displays the nodes in a hierarchical manner. The hierarchy in which the nodes are displayed is defined when you add the Visual Correlation widget.
  In our case we have defined "Alerts" as Node Level 1, "Incidents" as Node Level 2, "Tasks" as Node Level 3, "Indicators" as Node Level 4, and so on, as shown in the following image:

The "Hub and Spoke" mode displays the nodes in a circular network graph format, as shown in the following image:



- A "context menu" to the related nodes that contains options to open the related record as shown in the following image:



You can choose to open the record in the current tab itself by clicking the **Open Record** option in the context menu or you can open the record in the new tab by clicking the **Open Record in New Tab** option. This is especially useful in cases you want to perform certain actions on the related record, such as blocking an indicator without losing the context of the main record. The main node does not have the context menu since the main record is already open.

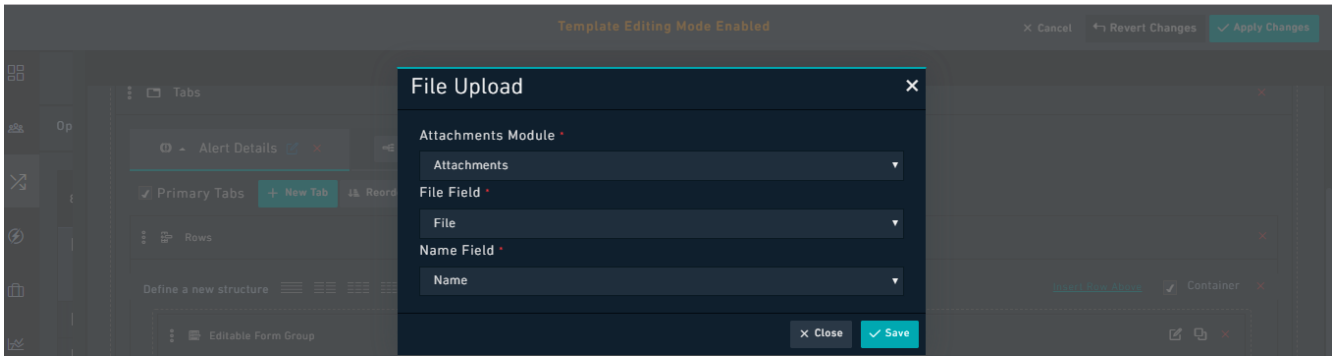
You can view the Visual Correlations graph in the full-screen by clicking the **Full-screen Mode** button. To exit the full screen, press `ESC`.

File Upload

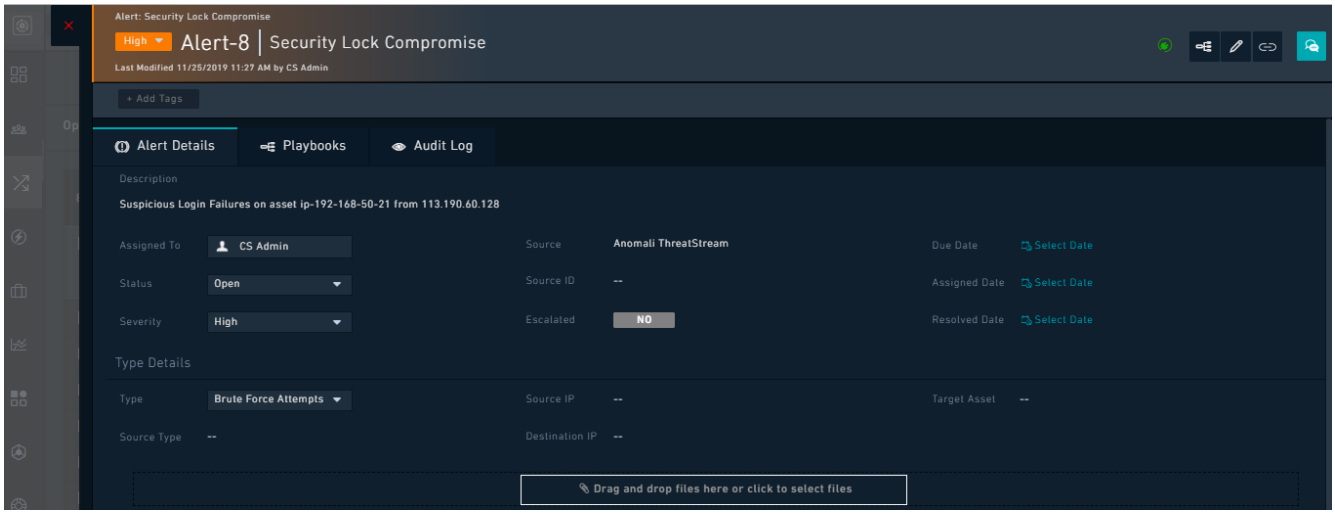
Use the File Upload widget to provide users with an area to attach file records. You can upload files to this area by either dragging and dropping files or by clicking and browsing to a file.

All files uploaded are referenced in Attachments using the File API.

In the **File Upload** widget, you can specify the module in which you want the files to be saved in the **Attachments Module** field. By default, this is set as Attachments, i.e., when you upload files, using the File Upload widget, the files become part of the Attachments record. Retain the values of the File Field and Name Field as default:



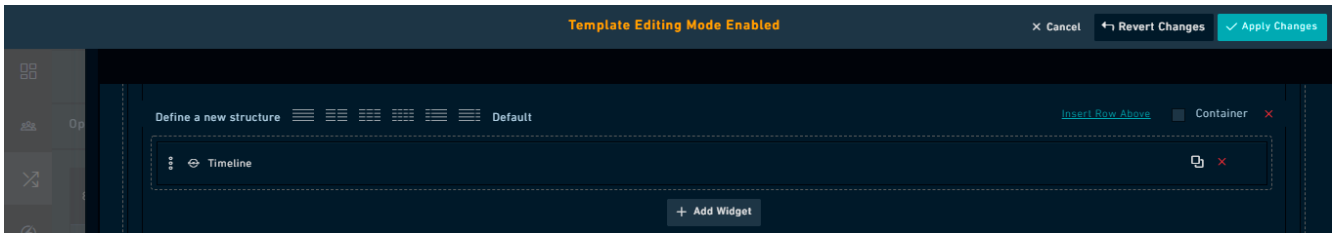
The following image illustrates how the File Upload widget is displayed in the Detail View of a record:



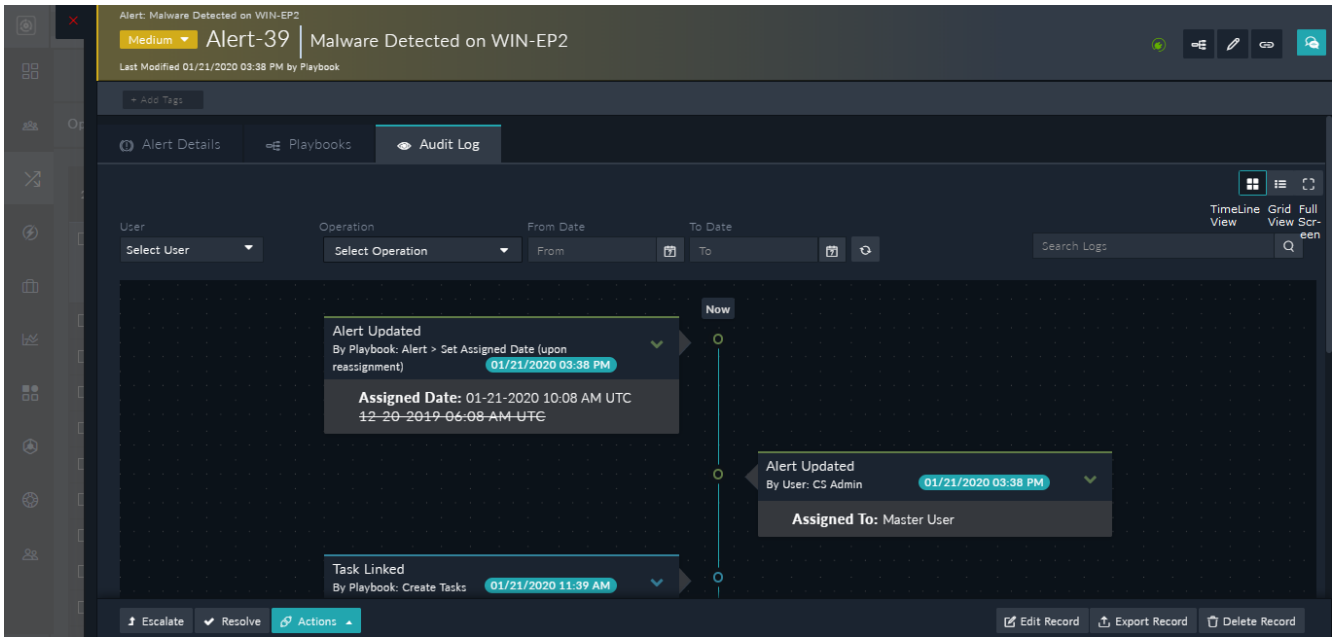
Note: You can also edit the template of the add/edit form for any module and add the **File Upload** widget to that form. This is useful when you want to create a record with attachments without having to create a many-to-many relationship between the record and the attachments.

Timeline

The Timeline widget inserts a historical timeline for the current record. The Timeline widget is added by default for records created in modules which are installed when you deploy FortiSOAR. If a user creates a new module and publishes that in FortiSOAR, then the Timeline widget is not present. Users must edit the record template for the newly created module and add this widget so that the timeline for records is available. You cannot edit the Timeline widget.

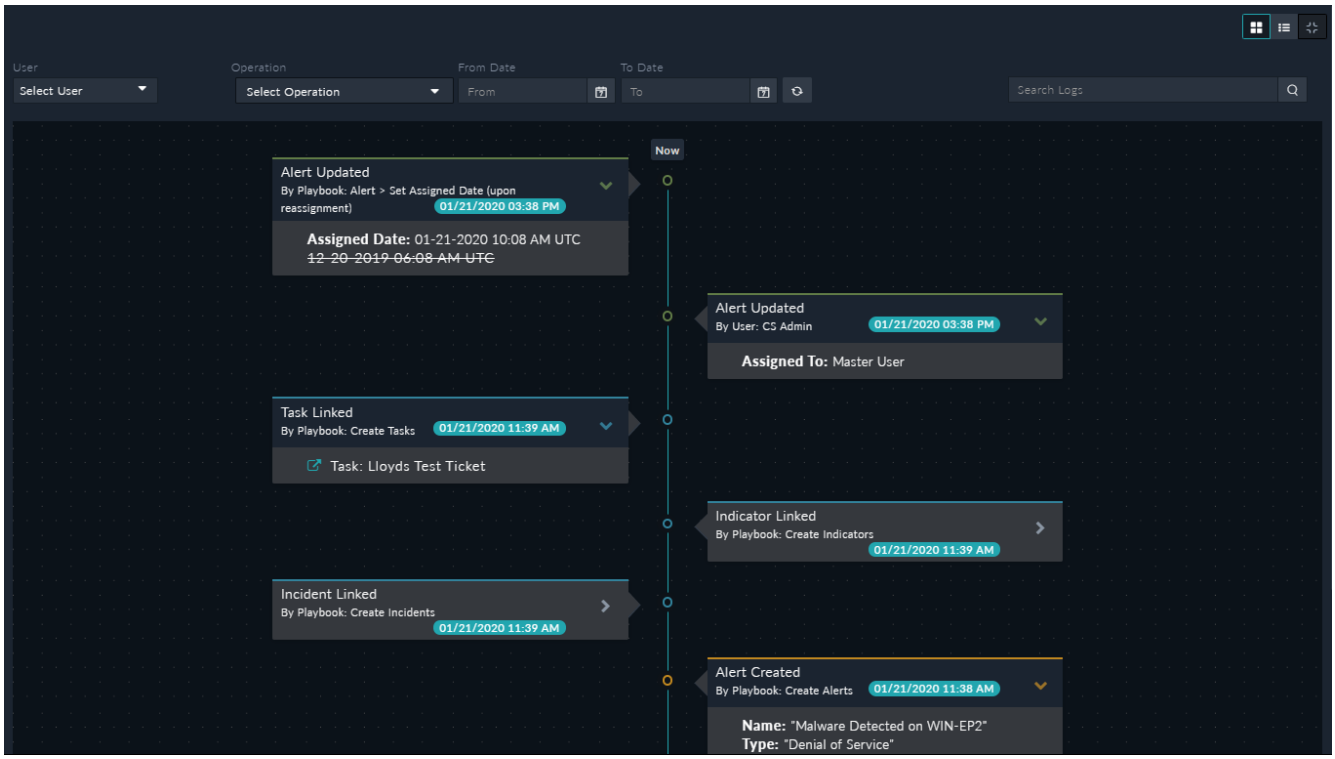


The Timeline widget appears in the **Audit Log** tab for records created in modules which are installed when you deploy FortiSOAR. The following image illustrates how the Timeline widget is displayed in the Detail View of a record:



If you link a record that contains Unicode or non-English characters, then in the Timeline widget, you will not see that event (the link event), or you will not be able to see the details of that event. If you link a record with only English characters, the Timeline widget displays correctly.

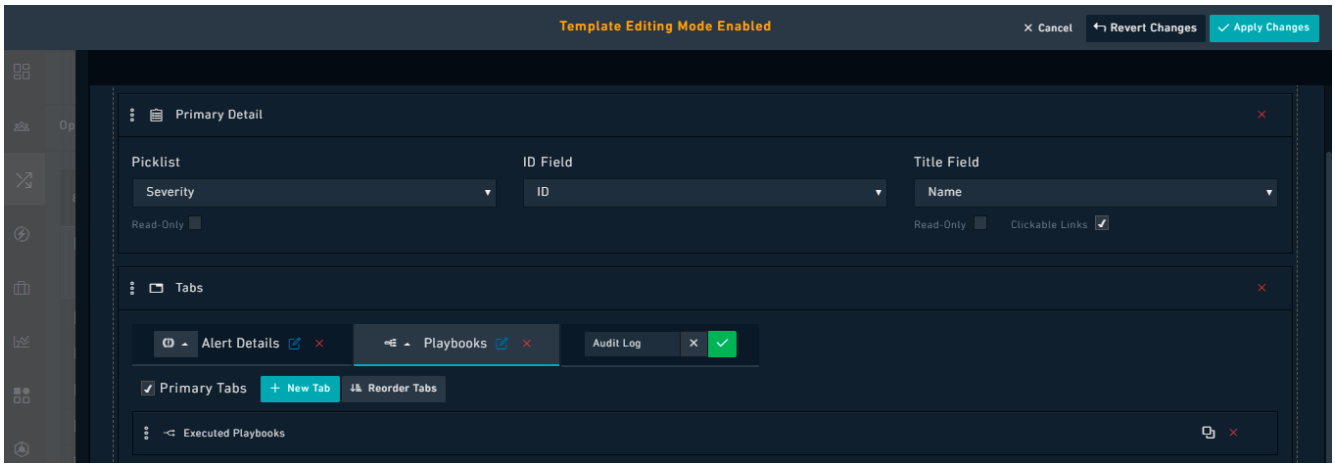
You can toggle between the timeline view, grid view, and full-screen view of the of the audit log tab. To move to a full screen view of the audit log, click the **Full-screen Mode** icon, which opens the audit log in the full screen as shown in the following image:



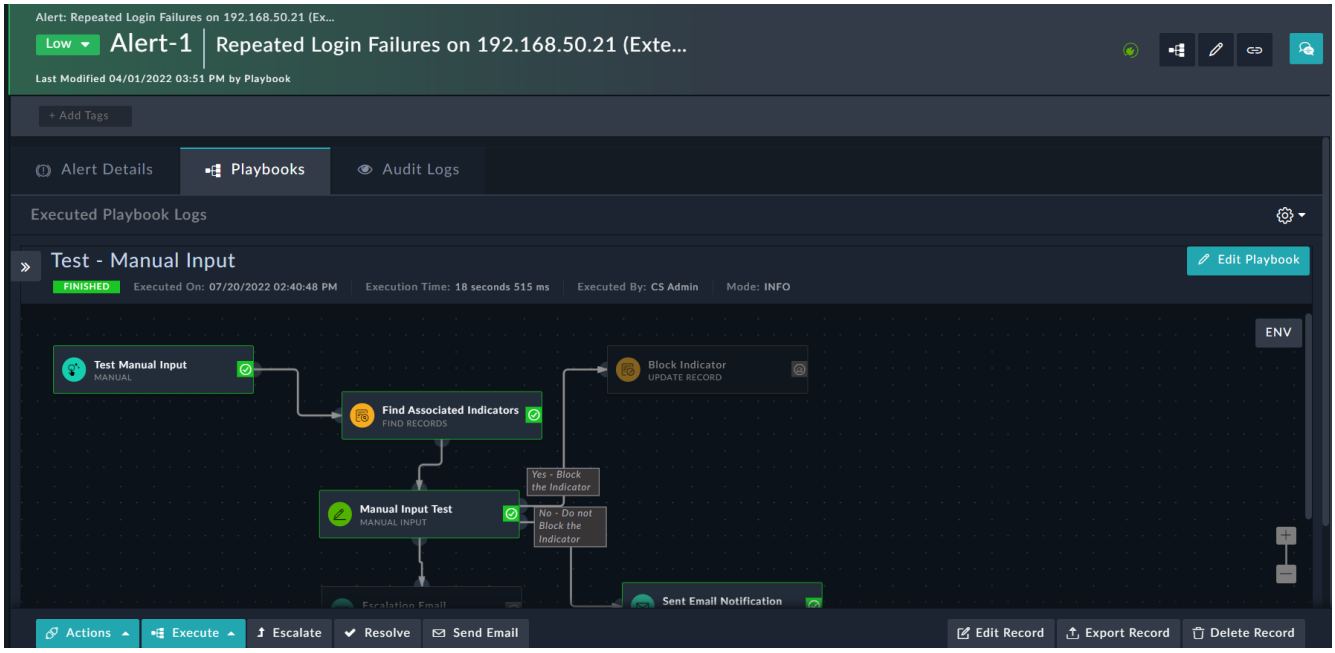
You can click the side arrows to view details of the event as shown in the above image. To exit the full screen, press `ESC`, or click the **Exit full-screen mode** button.

Executed Playbooks

Use the Executed Playbooks widget to view the executed playbook logs associated with the current record or entity. The Executed Playbooks widget is added by default for records created in modules which are installed when you deploy FortiSOAR. If a user creates a new module and publishes that in FortiSOAR, then the Executed Playbooks widget is not present. Users must edit the record template for the newly created module and add this widget if they want to view the executed playbooks logs associated with the current entity. You cannot edit the Executed Playbooks widget.



The Executed Playbooks widget appears in the **Playbooks** tab for records created in modules which are installed when you deploy FortiSOAR. The following image illustrates how the Executed Playbooks widget is displayed in the Detail View of a record:



Recommendation Settings

You can add the Recommendation Settings widget in the detail view of a record to display similar records and predict values of fields. You can turn this widget on or off as per your requirement and also configure the settings for displaying similar records and predicting values of fields. For more information on how to configure this widget, see the Working with Modules - Alerts & Incidents chapter.

Custom Content

iFrame

You can use the iFrame widget to display any external HTML page inside an HTML iFrame component. The iFrame widget is present in the **Dashboard** and **List Views** templates.

Use the iFrame widget responsibly. FortiSOAR has no control over and assumes no responsibility for, the content, privacy policies, or practices of any third-party websites. Ensure all external HTML pages are verified and approved by your organization's Legal and IT teams.

You should not add a Dashboard page as a URL in the iFrame Widget, since adding a dashboard page can lead to recursive calls to other pages, which could cause the iFrame to respond very slowly and FortiSOAR to become unresponsive.

An example of how you can use iFrame widgets would be that you could embed URLs of external cyber security tools (e.g., hex to ascii or url decoding services) that you often use within this widget. Then, when an alert comes into the system, you can gather the data from the alert and paste it into the iFrame and quickly get analysis for the same, instead of having to jump back and forth between tabs or windows. In some cases, it also helps to avoid using the API route, which has its own limits.

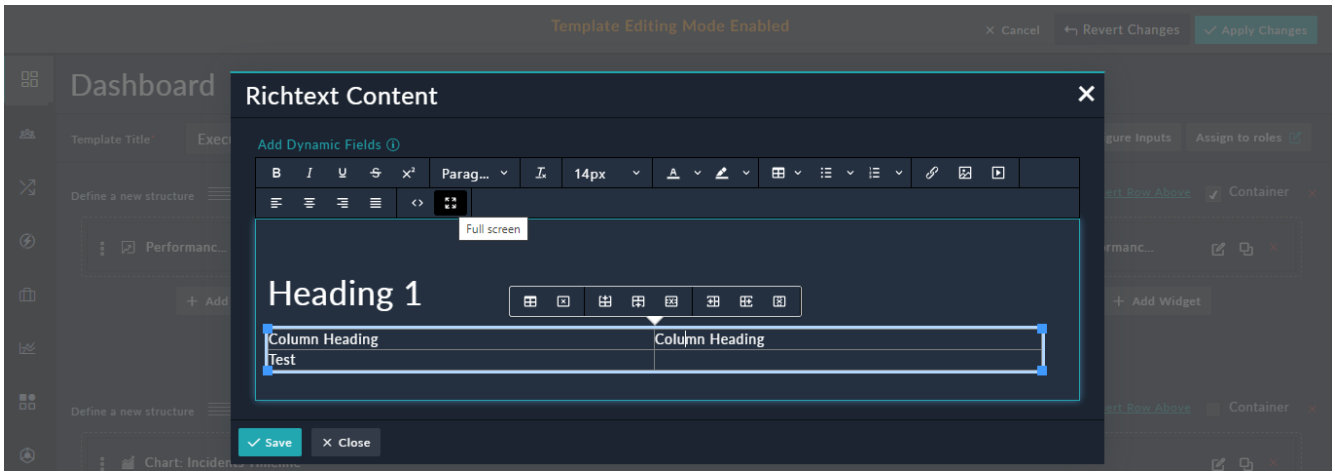
The iFrame Widget supports websites that have CORS enabled. If FortiSOAR displays a blank frame or an error in the iFrame then check the browser developer tools for more information.

Richtext Content

Use the Richtext Content widget to include formatted content, including lists and tables, images, and source code in your **Dashboard**, **List Views**, and **Details View** templates.

From version 6.4.3 onwards, the Richtext Content widget contains a "HTML WYSIWYG" editor for rendering rich text. An "HTML WYSIWYG" editor is extremely easy to use and it renders the content in HTML and therefore can be used easily at places where HTML needs to be rendered, for example, in an email, without the need for users to write code.

You can add styles such as headings, bold, italics, add lists, tables, and insert links, media, etc. using the "Styling" toolbar provided in the widget. To get help on what an icon in the styling toolbar represents, hover your mouse over that icon. Click the **Full Screen** icon to move to the full screen view of the widget.

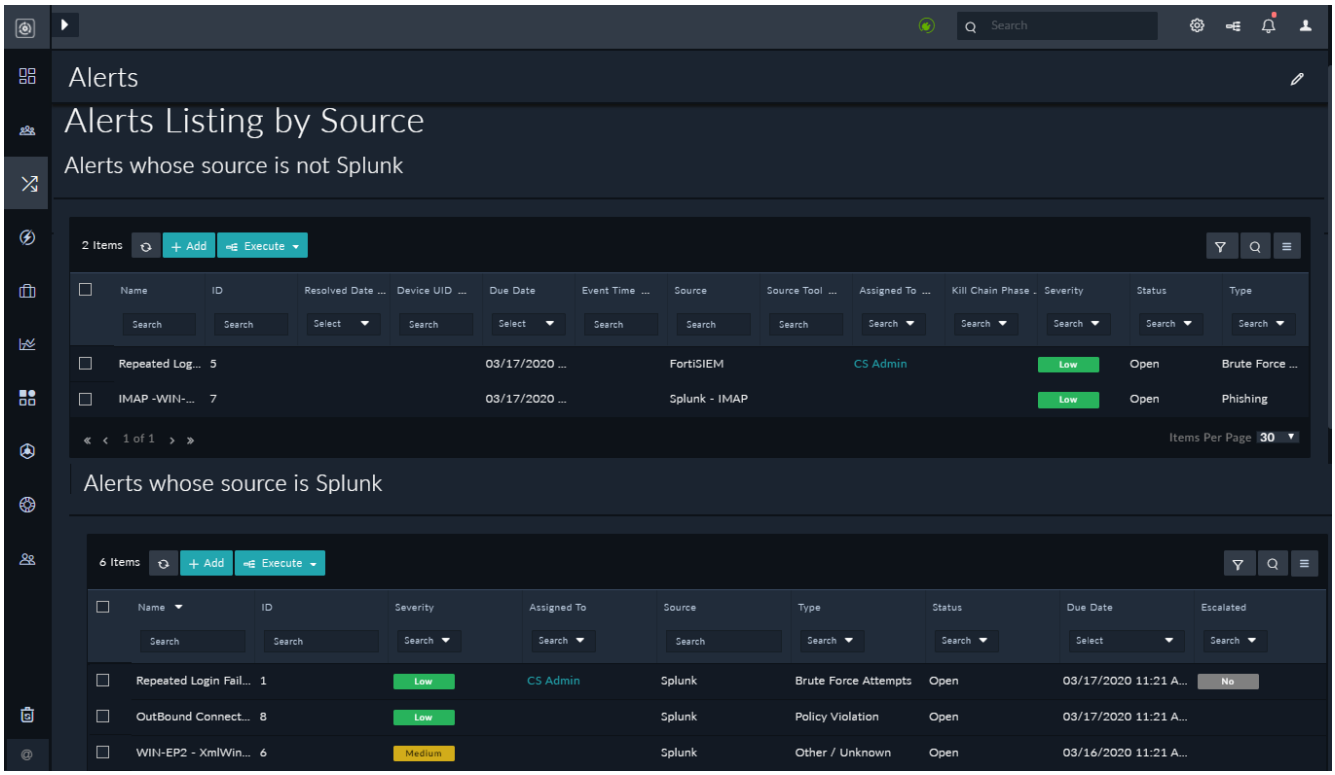


Click the **Source code** button to view the HTML source for the above content:

Example of using Richtext Content Widget

In our example, we have arranged alerts according to their source, for example, alerts that are from Splunk in one category and alerts from another source in another category as shown in the following image:

The Alerts Details Listing view will appear as follows, based on the template you have defined:



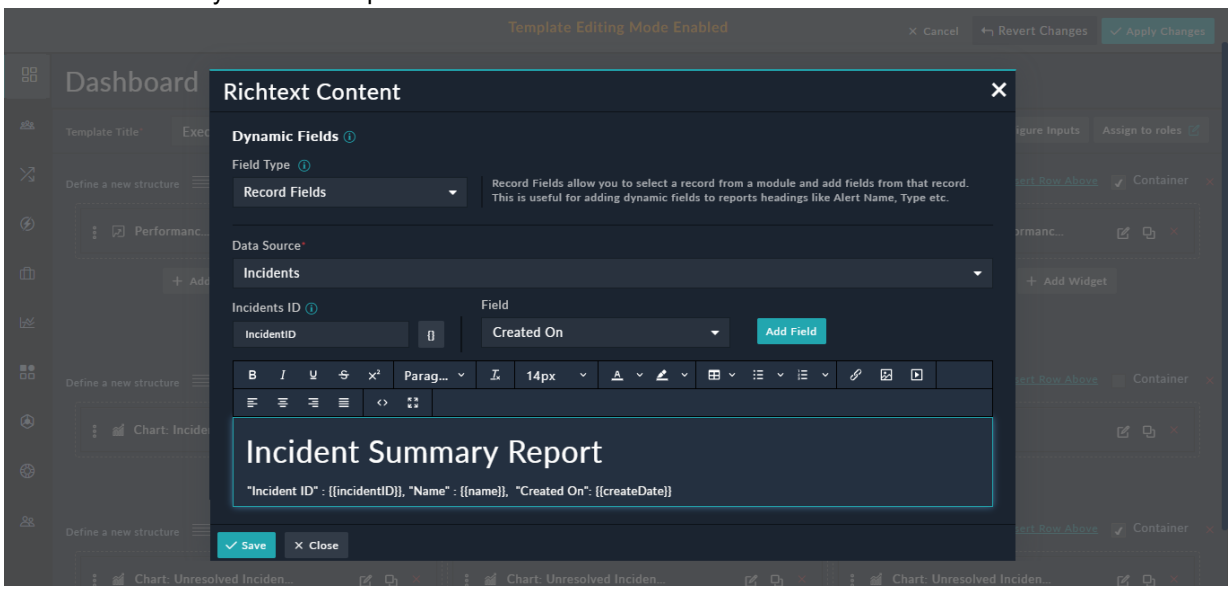
In the context of Dashboards or Reports, you can also use the identifiers defined in the input variables as part of the Richtext Content. For more information, see the Input Variables in Dashboards and Reports section.

For example, if you are creating a dashboard or a report for a particular Incident ID, then you can add the identifier (`{{identifier}}`) for the Incident ID that you have defined as the input variable to the Richtext content as `Incident Id: {{identifier}}`. Based on the value you have specified in **Inputs** (for example `626`), the Richtext content will display **Incident ID: 626** on the report or dashboard you are creating. For more information, see the Related Records Filter in Widgets section. Similarly, you can also use `{{todayDate}}` to display the current date in a dashboard or report.

In the context of Dashboards or Reports, you can also choose the dynamic fields that you want to display in the Richtext Content, making it simpler and efficient for you to add dynamic fields to the Richtext Content.

Do the following, if for example, you want to add a Richtext Content widget, in the *Incident Summary Report*, which contains the following fields: name of the incident and the date the incident was created on.

1. Click the **Add Dynamic Fields** link that appears at the top of the RichText Content Widget.
2. From the **Field Type** drop-list, select the type of dynamic field you want to add. You can choose from Record Fields, Configured Input Fields, or Utility Fields.
   Record Fields are fields that are part of the module that you select from the **Data Source** drop-down list. Based on the module that you select and the provided record ID, using either a specific record ID or a pre-defined configured input variable, you can add fields from the records.
   Configured Input Fields are fields that you have defined earlier as input variables (see Input variables). These fields allow you to add defined report input fields, and pull the value dynamically based on the input parameters specified at the time of running the report.
   Utility Fields are dynamic fields commonly used to add dynamic content, such as `todayDate` and `timezone`.
3. For our example, we need to add the name of the incident and the date the incident was created on. To add the `Name` and `Created on` fields in the Richtext Content widget, do the following:
   a. From the **Field Type** drop-down list, select **Record Fields**.
   b. From the **Data Source** drop-down list, select **Incidents**.
   Once you click **Incidents**, the **Incidents ID** field is displayed. The Incidents ID field is the `<Module ID>` field that specifies the ID of the record from which you want to pick up the content of the dynamic field. You can either provide a unique ID (i.e., the ID of a particular incident like `626`) or select an ID dynamically from the list of input parameters you have configured. In case of our example, an identifier, **IncidentID**, has been defined as an input variable. Therefore, in our example, the **Incidents ID** field is displayed with `ID` selected. You should click the **Add Custom Expression** button and from the **Select variable** drop-down list, select **IncidentID**. This means that users will provide the Incident ID (`{{incidentID}}`) at the time they run the *Incident Summary Report*.
   c. To add the `Name` field, from the **Field** drop-down list, select **Name** and then click **Add Field**.
   This will paste the jinja value of the Name field, i.e., `{{name}}` in the Richtext Content widget on the location where your cursor is placed.
   d. To add the `Created On` field, from the **Field** drop-down list, select **Created On** and then click **Add Field**.
   This will paste the jinja value of the Created On field, i.e., `{{createDate}}` in the Richtext Content widget on the location where your cursor is placed.



Important Points:

- Once you add a dynamic field to the Richtext Content widget, you cannot edit this field, also when you hover on the added field, you will see the context of field. In the above image, the Incident ID is undefined since we have used an input variable in the Incident ID field, which means that the user running the record will require to provide the Incident ID at the time of running the report by clicking **Input** and entering the Incident ID.
- In case of **Record Fields**, you must add dynamic fields for a single module, for example the name and description of an incident record. If you add dynamic fields for multiple modules, the dynamic fields for the last specified module are considered.
  For example, if you have added the name field for the incident module and then you add the name field for the alert module, the Richtext Content widget will display the name only of the alert record and not of the incident record.

Widget Library

You can add widgets such as Access Control, Task Management, etc from the widget library to the detail view of a record. For more information, see the Widget Library chapter.

Common components within Widgets

You can use common components that are part of widgets in the same way across Dashboards and Templates. Some of the common items are:

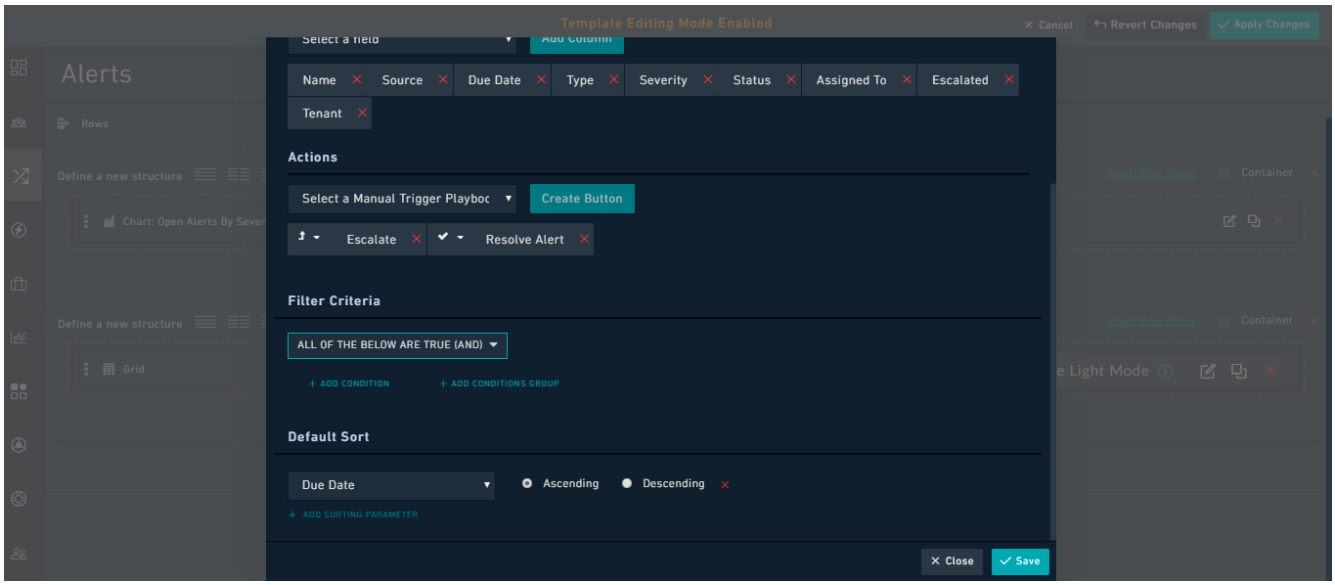
- Default Sort
- Nested Filters

Default Sort

Default sort is part of the **Grids**, **Card Lists**, and **Single Line Items** widgets. Use **Default Sort** to specify fields based on which the records in the module will be sorted by default.

Following example describes how to use default sort in a **Grid** widget:

In the `Default Sort` section, you can specify fields based on which the records in the module will be sorted by default. Click the **Add Sorting Parameter** link to get a drop-list of all fields for that module. Select the field based on which you want to sort the records, for example, **Due Date**, and then select whether you want the records to sort in the **Ascending** or **Descending** order.



Nested Filters

Nested Filters is part of all the widgets, except the **Custom Content** and **Structure** Widgets. Use **Nested filters** to filter records using a complex set of conditions. Nested filters group conditions at varying levels and use **AND** and **OR** logical operators so that you can filter down to the exact records you require.

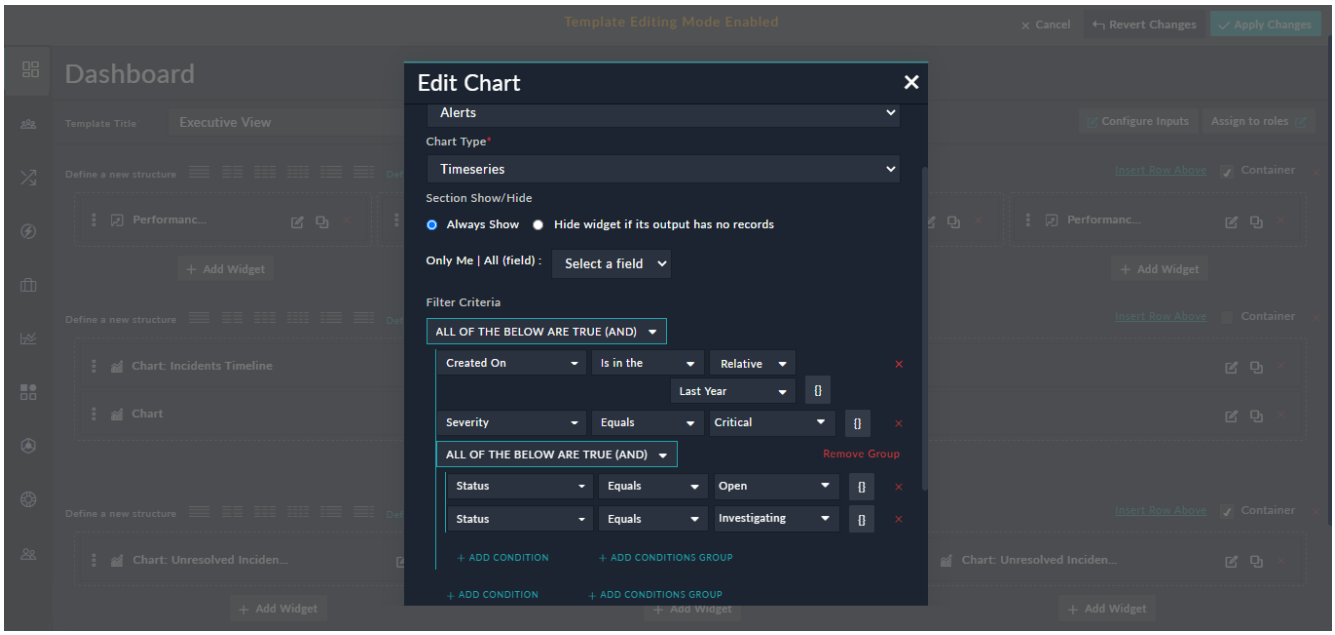
You cannot search or filter encrypted fields. Also, if you want to apply a filter with an `Equals` or `Not Equals` logical operator to a richtext content field, such as **Description**, you must enclose the content you want to filter in `<p>...</p>` tags.

The Nested Filters component also has the ability to display fields with many-to-many relationships. Earlier, only primitive types and one-to-many relationship fields were displayed in the Nested Filters component. For example, now you can use this component to display all alerts that are associated with a specified Incident ID. An example of this is included in the Related Records Filter in Widgets section. The **Select a field** drop-down list in `Filters` now also categorizes fields into `Primary Fields` and `Related Modules` making it easier for you to understand whether a field is a field of that module or a field of a related module. For example, for the `Incidents` Module, **Assigned To** and **Created On** would be listed in the `Primary Fields` section, and **Alerts** and **Assets** would be listed in the `Related Modules` section.

Following example describes how to use Nested Filters in a **Chart** widget:

In the `Filters` section, you can add conditions by clicking the **Add Condition** link or add a condition group by clicking the **Add Conditions Group** link.

For example, if you want to display alerts in a chart that have been created in the last calendar year and whose severity is critical and whose status is open or investigating, you would create a filter as shown in the following image:



To create nested filters based on the example, perform the following steps:

1. In the `Filters` section, select the logical operator, **All of the below are True (AND)**, or **Any of the below is True (OR)**. For our example, we require the AND operator, since we want alerts that were created in the last 30 days and whose severity is critical, so select **All of the below are True (AND)**.
2. Click the **Add Condition** link and create a filter for alerts that have been created in the last year.
   From the `Select a field` drop-down, select **Created On**, from the `Operator` drop-down list select **Is in the**, select **Relative** and then from the `Created On` drop-down list select **Last Year**. For more information on date/time ranges, see Support for Custom Time Ranges in Filters.
3. Click the **Add Condition** link and create another filter for alerts whose severity is critical.
   From the `Select a field` drop-down, select **Severity**, from the `Operator` drop-down list select **Equals** and, in the `Severity` drop-down list select **Critical**.
4. Create a condition group for the status condition, since you require to choose between two conditions in `Status`.
   Click the **Add Conditions Group** link and select the logical operator. For our example, we require the OR operator, since we want alerts whose status is Open or Investigating, so select **Any of the below is True (OR)**.
5. Click the **Add Condition** link and create a filter for alerts whose Status is Open.
   From the `Select a field` drop-down, select **Status**, from the `Operator` drop-down list select **Equals** and, in the `Status` drop-down list select **Open**.
6. Click the **Add Condition** link and create a filter for alerts whose Status is Investigating.
   From the `Select a field` drop-down, select **Status**, from the `Operator` drop-down list select **Equals** and, in the `Status` drop-down list select **Investigating**.
7. Click **Save** to save the filter.

Nested filters display logical operators depending on the type of field selected as a filter. For example, if you select a `Date/Time` field, then you will see the following operators:

- Is in the
- Is Null
- Equals
- Not Equals
- Before
- On or Before

- After
- On or After

Similarly, if you select a field of type `Integer` you will see the following logical operators:

- Equals
- Not Equals
- Less Than
- Less Than or Equal To
- Greater Than
- Greater Than or Equal To
- Is Null

Or, if you select a field of type `Picklist` or `Lookup` you will see the following logical operators:

- Equals
- Not Equals
- Is In List (Added in version 7.0.2)
- Is Not In List (Added in version 7.0.2)
- Is Null

Or, if you select a field of type `Text` you will see the following logical operators:

- Equals
- Not Equals
- Contains
- Does not Contain
- Matches Pattern
- Does Not Match Pattern
- Is In List (Added in version 7.0.2)
- Is Not In List (Added in version 7.0.2)
- Is Null

The **Matches Pattern** and **Does Not Match Pattern** operators allow you to use basic pattern matching in conditional statements using the percent (`%`) or underscore (_) wildcards. The `%` sign represents zero, one, or multiple numbers or characters. The _ sign represents a single number or character.

Support for Custom Time Ranges in Filters

You can define a date range, for `Date/Time` fields, using the operators mentioned earlier and filter records using the following types of filters:

- **Relative Date Ranges**, A custom relative date, or a relative date range. A relative date is a date that is relative to the current date. In case of a custom relative date range you define your own relative date range, for example, filtering records in the last 4 days. In case of the relative date range, you can choose from a list of predefined options such as, Last Year.
- **Today**, i.e., 00:00 hours of the current day to 23:59 hours of the current day.
- **Static Date Ranges**, For example, filtering records for December 2018, i.e., from 1st December 2018 00:00 hours to 1st January 00:00 hours.

Definitions of time ranges while using the `Is in the` operator:

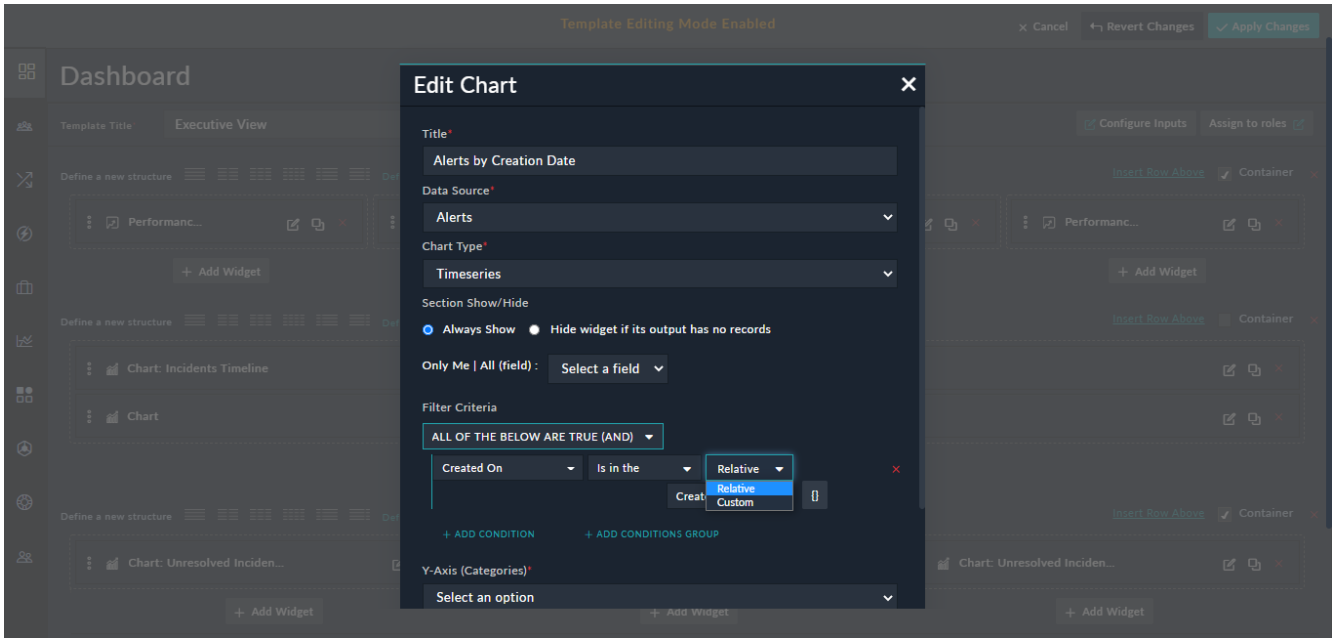
- **Years** and **Months**: Is the calendar year or months. This filter considers the current year and month, and then applies the filter. For example, if you apply the **Last Year** filter on 1st February 2019 09:00 hours, then it would be to

filter records from 1st January 2018 00:00 hours to 1st February 2019 09:00 hours. Similarly, if you apply the **Last Month** filter on 1st February 2019 09:00 hours, then it would filter records from 1st January 2019 00:00 hours to 1st February 2019 09:00 hours.

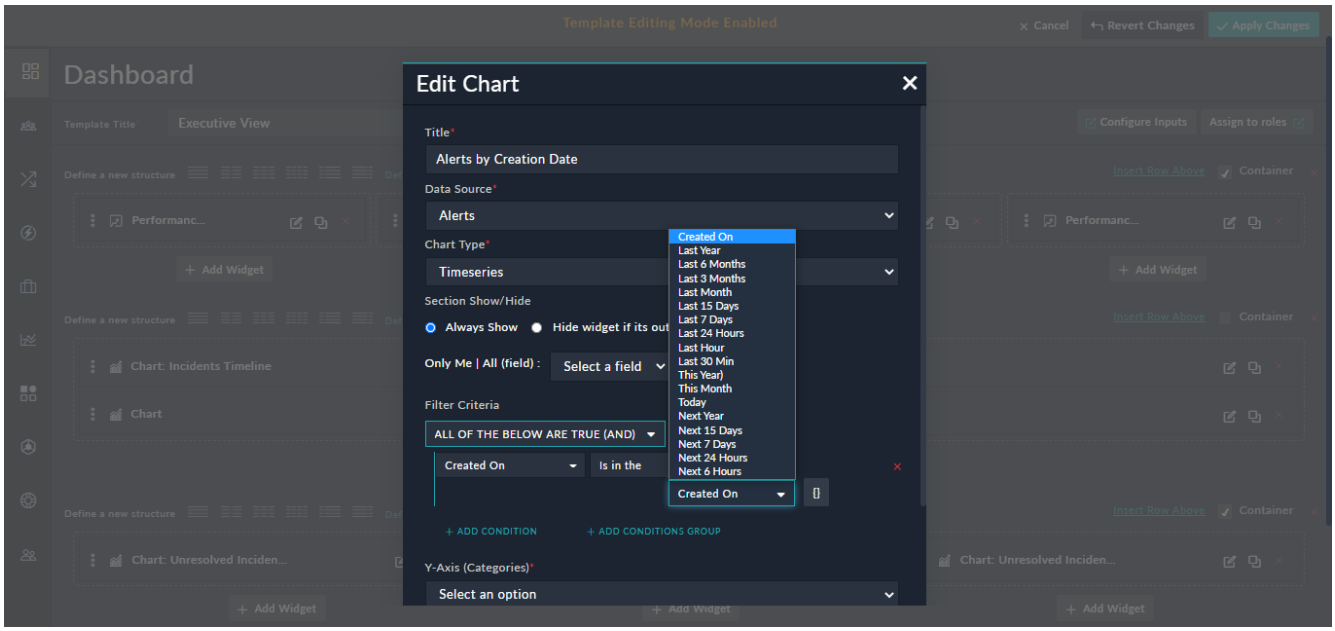
- **Days**: Is the number of days for applying the filter. This filter considers the current day and time and then applies the filter. For example, if you apply the **Last 7 Days** filter on 4th February 2019 09:00 hours, then records from 29th January 2019 00:00hrs to 4th February 2019 09:00 hours will be considered.
- **Hours** (and **Minutes**): Is the hours and minutes for applying the filter. This filter considers the current hour and minute and then applies the filter. For example, if you are applying the **Last 24 Hours** filter on 5th February 2019 15:30 hours, then records from 4th February 2019 15:00 hours to 5th February 2019 15:30 hours will be considered.

Important: The definition of the relative date time ranges has been simplified and changed in version 6.4.3 to include the current unit of time, for example in case of last x years/months/days/hours/minutes, etc. Earlier the definition used to exclude the current unit of time, for example, the filter would exclude the current hour in case the **Last 24 Hours** filter was applied. Due to this change if you have used the `Is in the` operator and you have upgraded your environment from a version prior to 6.4.3, then data will differ after the upgrade.

For the `Is in The` operator you can choose a relative date or a custom date to filter records. For example, if you have a chart that displays alerts according to the created date, then in the `Filter Criteria` section when you select the **Created On** field and the **Is in the** operator, you will see **Relative** and **Custom** options:

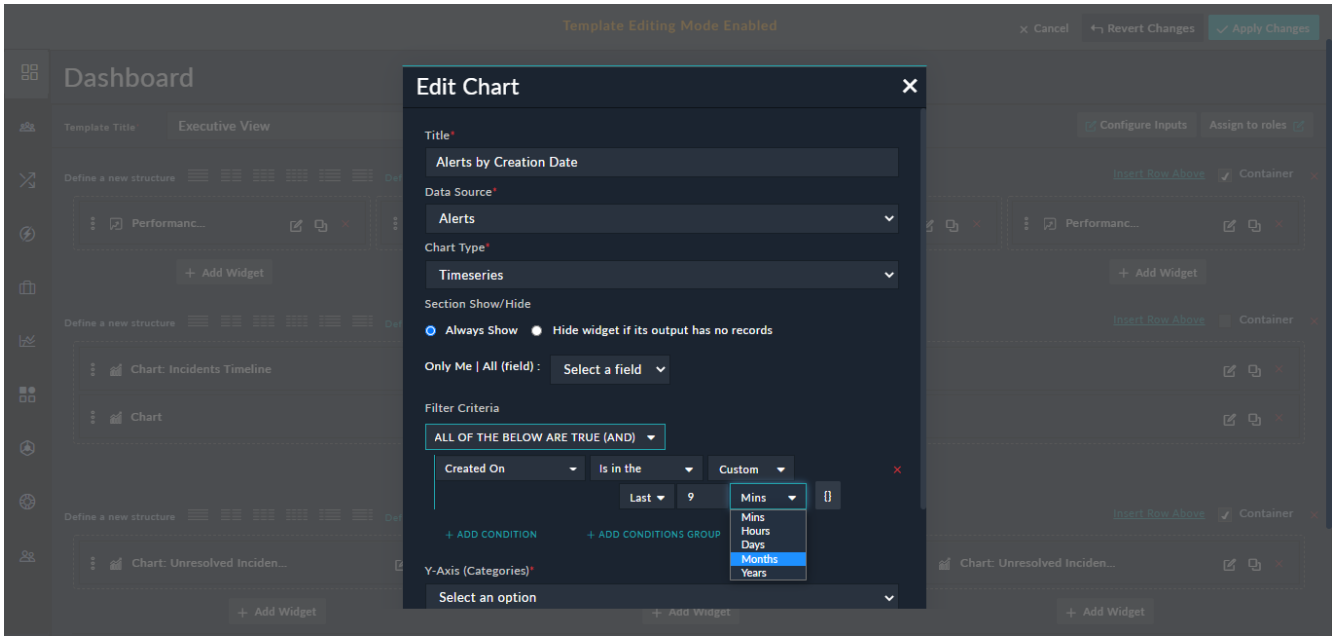


If you want to filter records based on a relative date and time, i.e, date and time relative to today, for example, you want the dashboard or report to display all the alerts that were created in the last six months, then click **Relative** and then select the **Last 6 Months** option.



Based on this filter the dashboard will display a timeseries of all alerts that were created in the last 6 months. For example, Last 6 Months would be 1st July 2019 00:00 hours to 1st January 2019 09:00 hours, if you are applying this filter on 1st January 2020 09:00 hours.

If you want to filter records on a custom relative date, i.e., if the datetime for which you want to filter records is not present in the predefined list of relative dates, then you can choose the **Custom** option and specify the relative datetime. For example, if you want the dashboard or report to display all the alerts that were created in the last nine months, then click **Custom** and then select **Last**, type **9** in the next text box, and then select **Months**.



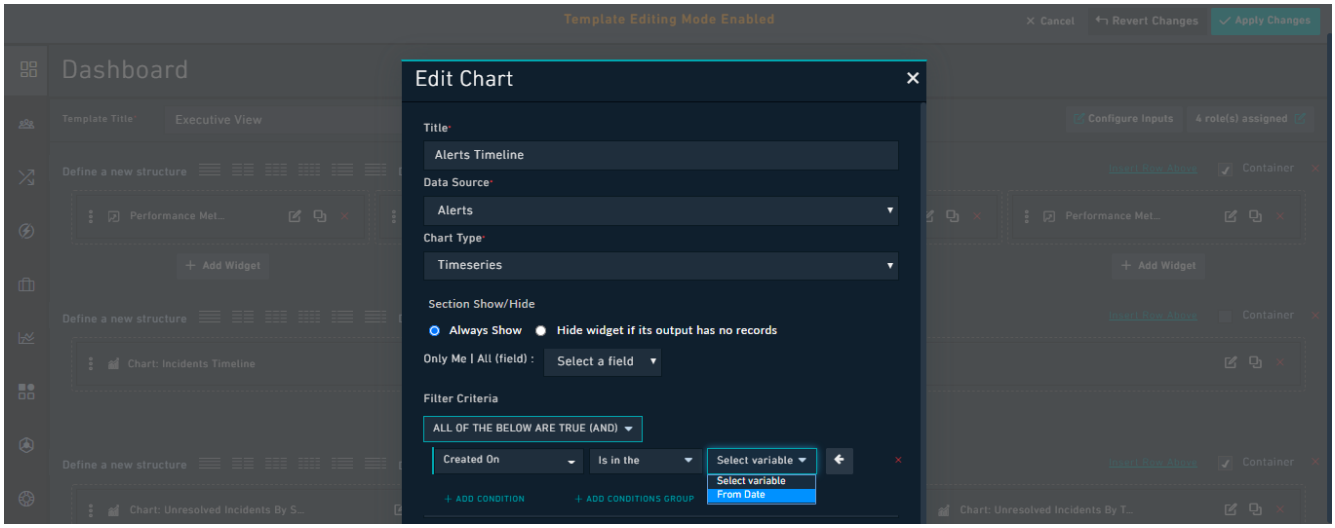
Based on this filter the dashboard will display a timeseries of all alerts that were created in the last 9 months. For example, Last 9 Months would be 1st April 2019 00:00 hours to 1st January 2020 09:00 hours, if you are applying this filter on 1st January 2020 09:00 hours.

When you are using the `Is in the` operator and you specify a Custom filter with the same time range as the options present in the Relative filters, then after you save the filter, the filter changes from Custom to Relative. This does not impact any functionality. For example, if you have specified a Custom filter as `Is in the Last 1 hour`, then after saving this filter when you reopen the template you will observe that the filter has changed to a relative filter since the Last 1 hour option is present in the pre-defined list of Relative filters.

For the `Before`, `On or Before`, `After`, or `On or After` operators you can also choose a static date or a relative date based on which you can filter records.

In case you have upgraded to a version later than 5.0.0, then you will have to reselect your datetime filters, since the new datetime filters are not backward compatible. You will be able to see the older applied datetime filter in the FortiSOAR reports and dashboards. However, if you want to edit these filters, then you will have to reselect all the datetime filters in that dashboard or report. Similarly, if you import a report or dashboard into version 5.0.0 or later, it will work fine. However, if you want to edit the datetime filter, you will have to reselect all the filters in that datetime dashboard or report.

You can also use variables that you have defined in the Input variables in the Nested Filter component. To use defined input variables, click the **Add Custom Expression** icon and select the defined input variable. For example, if you have defined the **From Date** input variable to be used in Dashboards or Reports, select this variable, as shown in the following image:



Behavior of Nested Filters in case of records that have 'null' value

Records that have a 'null' value in a field are not displayed when you filter records using the *Not Equals* operator.

Example:

If you want to define a filter that will retrieve all records whose severity is not equal to critical, you must add the following two conditions to ensure you retrieve all records: **Severity Not Equals Critical**, and **Severity Is Null True**. If you add only the **Severity Not Equals Critical** condition, then records that do not have any Severity assigned to them (null records) will not be retrieved.

Display Elements

You can use the following display elements within widgets to control the behavior and display of fields within widgets:

- All Inline or Inline Editor
- All Read-Only or Read-Only
- All Clickable Links

All Inline or Inline Editor

Selecting the **All Inline** or **Inline Editor** checkbox treats all the fields within the widget as inline fields. Inline fields are editable by clicking the fields. If a field is not inline then to edit that field, you must click the **Edit** button that appears alongside the field.

Read-Only

Selecting the **Read-Only** checkbox treats all the fields within the widget as read-only fields, irrespective of the permissions assigned.

Clickable Links

Selecting the **Clickable Links** checkbox converts any URL or email address present in `text` and `textarea` fields to hyperlinks, which are clickable.

Note: Links in `richtextarea` fields are not converted into hyperlinks and therefore not automatically clickable.

Container

Selecting the **Container** checkbox arranges and styles the widget, which it contains appropriately such that they appear as one cohesive unit.

Insert Row Above

Click the **Insert Row Above** link to insert a blank row, wherever required.

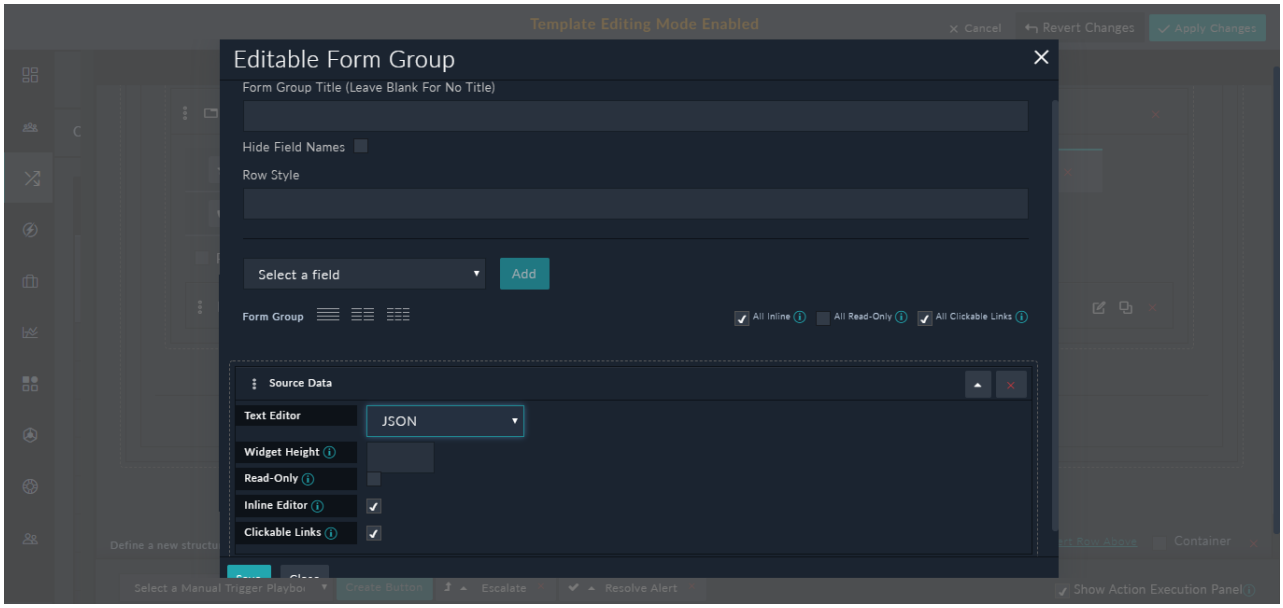
Displaying "Text Area" fields in the JSON format

You can use the "JSON field" type to store data in the JSON format directly for fields such as `Source Data` that commonly store data in the JSON format.

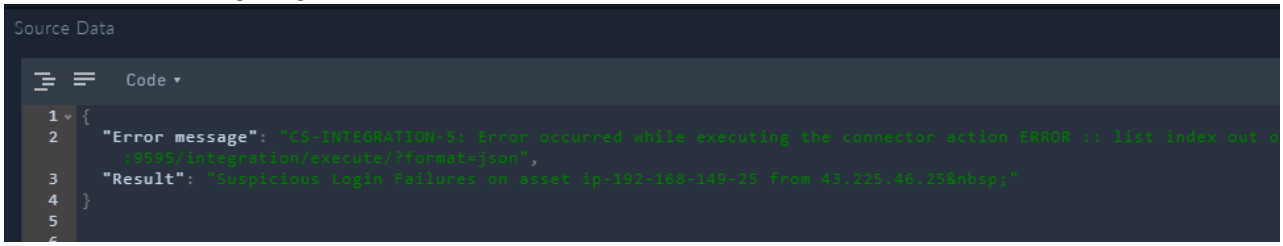
The `Editable Form Group` widget provide you with the ability to display JSON data in the JSON format for fields that have their field type set as `Text Area`. For example, if alert data is forwarded from a SIEM to FortiSOAR in the JSON format, you can change the `Editable Form Group` widget to display this data in the JSON format in a JSON viewer instead of the string format.

To enable the option for the JSON viewer in case of `Editable Form Group` widget:

1. Navigate to the module where you want the data to be displayed in JSON format, for example, `Alerts` and click a record in this module to open the `Detail` view of this module.
2. Click the **Edit Template** icon to open the Template Editor and modify the interface.
3. Click **Edit** in the `Editable Form Group` and modify the field, whose field type is set as `Text Area`, for example, **Source Data**, for which you want to display the data in the JSON format.
   Click the **v** icon in the **Source Data** field to display more options and from the **Text Editor** drop-down list select **JSON**:



   In the **Widget Height** field, you can define the height, in pixels, of the JSON editor.
4. Click **Save** and **Apply Changes**.
5. Open the record in the `Detail` view; you will see the field that you have modified is displayed in the JSON viewer as shown in the following image:



   You can edit the JSON directly in the JSON viewer, and if you have made any errors while editing the JSON, the JSON viewer will display a red cross on that line.

Content Hub

FortiSOAR release 7.2.0 introduces the 'Content Hub' using which you can find, view, install, create, out-of-the-box reference material and product add-ons such as connectors, widgets, and solution packs.

Use the Content Hub from within FortiSOAR to seamlessly browse, build, install, create, and support upgrades for the Solution Packs, Connectors, and Widgets. Prior to release 7.2.0, connectors and widgets used to be managed using different stores, and there was no management of Solution Packs. Now, the 'Content Hub' provides a consolidated place for managing all types of product add-ons.

The Content Hub is also available publicly at: https://fortisoar.contenthub.fortinet.com/, which also provides users with a consolidated view of all the listings of all FortiSOAR add-ons and reference information helping users leverage all that FortiSOAR has to offer more effectively by increasing the utilization of FortiSOAR.

The Content Hub data gets synchronized from the FortiSOAR repository, currently, at the thirtieth minute of every hour (for example, 1:30, 2:30), so that the content displayed in the content hub is always up-to-date.
You must ensure that repo.fortisoar.fortinet.com is reachable from your FortiSOAR instance. Otherwise, you will see a blank page when you click **Content Hub** in the left navigation. If FortiSOAR is deployed using offline repo, you must ensure that your repo is synchronized with repo.fortisoar.fortinet.com.

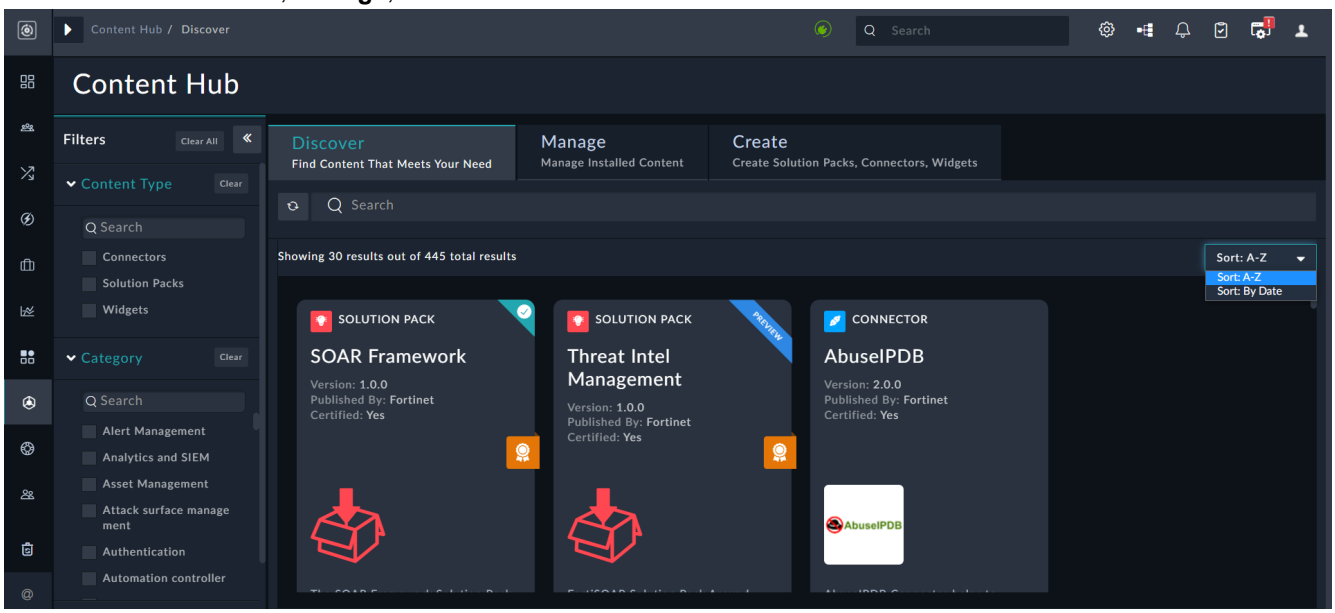
Permissions required for using Content Hub

- To view the Content Hub and changes made in the Content Hub, you must be assigned a role that has a minimum of `Read` permission on the `Content Hub` and `Applications` modules, and a minimum of `Create`, `Read`, `Update` permissions on the `Solution Packs` module. If users do not have `Read` permission on the `Content Hub` module, then such users cannot view the Content Hub and it will not be available in the left navigation.
- To view the content, i.e., the widgets and connectors that are part of the Content Hub, you must be assigned a role that has a minimum of `Read` permission on the `Content Hub`, `Solution Pack`, `Widgets`/`Connectors`, and `Applications` modules. Apart from this if you need to work (create, edit, delete) with the content, then you need appropriate permissions on the respective modules.
- To install content from the Content Hub or to or upload content to the Content Hub you must be assigned a role that has a minimum of `Read` permission on the `Security` module.

By default, for fresh installations of FortiSOAR the FSR Content Hub role is added and assigned to the 'Playbook Appliance'. Therefore, if you remove the FSR Content Hub role from the playbook appliance, then you must add relevant permissions to the playbook appliance.

Content Hub

Click **Content Hub** in the FortiSOAR left navigation to display the `Content Hub` page, which contains a **Filter** panel on the left and the **Discover**, **Manage**, and **Create** tabs.



You can use the **Search** box to search across all the tabs and sort the content alphabetically (A-Z) or by date.

Using the **Filters** panel, you can filter the content displayed in all the tabs. To clear all your filters, click **Clear All**. To clear filters for a particular category, click the **Clear** button in that category. You can use the **Search** box in each of the filter criteria to search for content in that particular filter criterion. You can collapse or expand the **Filters** panel, by clicking the **<<** arrows. If you have filtered the content based on any criteria, then you can view the filters that you have added in the **Filtered by** list.

You can filter content (add-ons) based on the following:

- **Content Type**: Filter the content based on the type of content with which you want to work, by selecting the required add-ons from the listed content types. Currently, Connectors, Solution Packs, and Widgets are the add-on content types present in FortiSOAR.
- **Category**: Filter the content based on the categorization of the content. Content is categorized based on the type of operations that the add-ons can perform. Examples of categories are Enrichment, Endpoint Management, Malware Analysis, etc.
- **Publisher**: Filter the content based on who is the publisher of the add-on. The add-ons can be developed and published by Fortinet or Community (anonymous) or by various contributors such as Bay Dynamic, Eclecticiq, etc.
- **Tags**: Filter the content based on the tags (exact match) associated with the content.

The `Content Hub` page contains the following tabs:

- **Discover**: Displays all the add-ons that are available in the Content Hub.
- **Manage**: Displays all of your content, i.e., all the add-ons that you have installed on the FortiSOAR instance.
- **Create**: Displays the add-ons that you are creating or editing, i.e., it displays the add-ons that you are working on and which are yet not published.

Discover tab

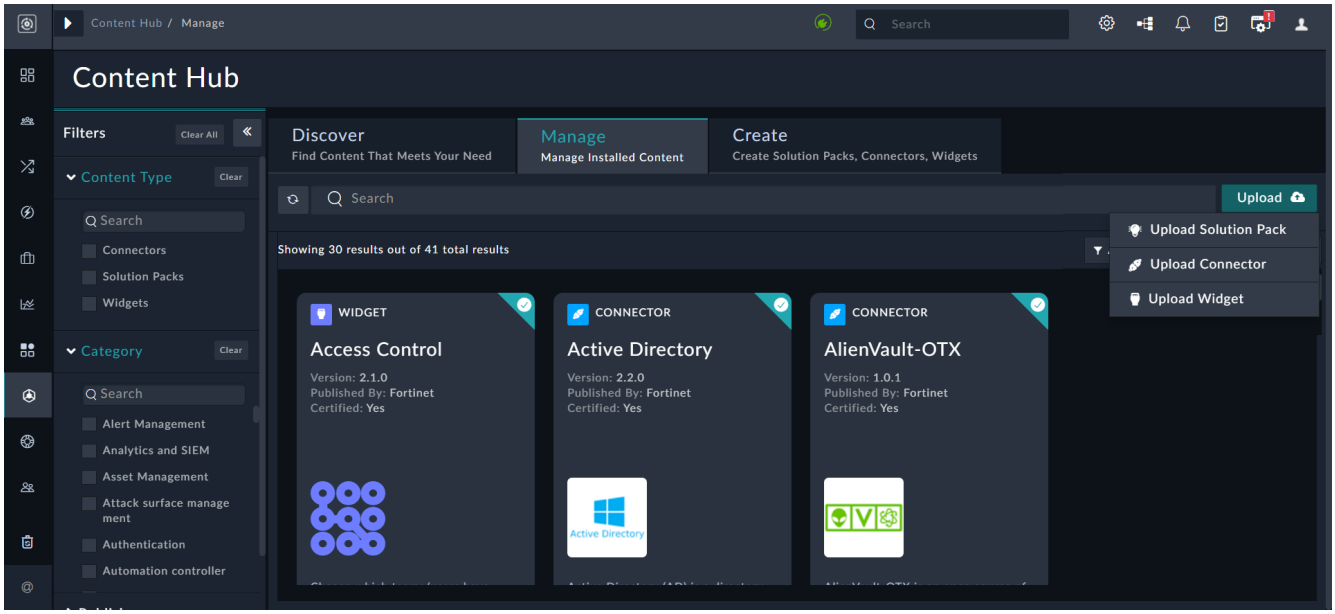
The **Discover** tab displays all the add-ons that are available in the Content Hub. Click on a tile to open the add-on popup, which displays the information about the add-on and using which you can install and export connectors, solution packs, or widgets.

Users who are upgrading to release 7.2.0 or later from a release prior to 7.2.0, will observe that connectors that they had installed prior to the upgrade are missing from the Content Hub. To resolve this issue, users have to assign appropriate permissions on the `Solution Packs` module to the 'Playbook Appliance'. For more information, see the "Upgrade Guide."

Manage tab

The **Manage** tab displays all of your content, i.e., all the add-ons that you have installed on the FortiSOAR instance. It also contains upgrade notifications for any of the add-ons that you have installed. You can search for an add-on by its name in the **Search** box and sort the add-ons either alphabetically or by date. Similarly, you can filter the installed add-ons that have an upgraded version, by selecting **Update Available** from the drop-down list.

To upload a custom add-on, connector, widget, or solution pack, click **Upload** and then select the type of add-on you want to upload:



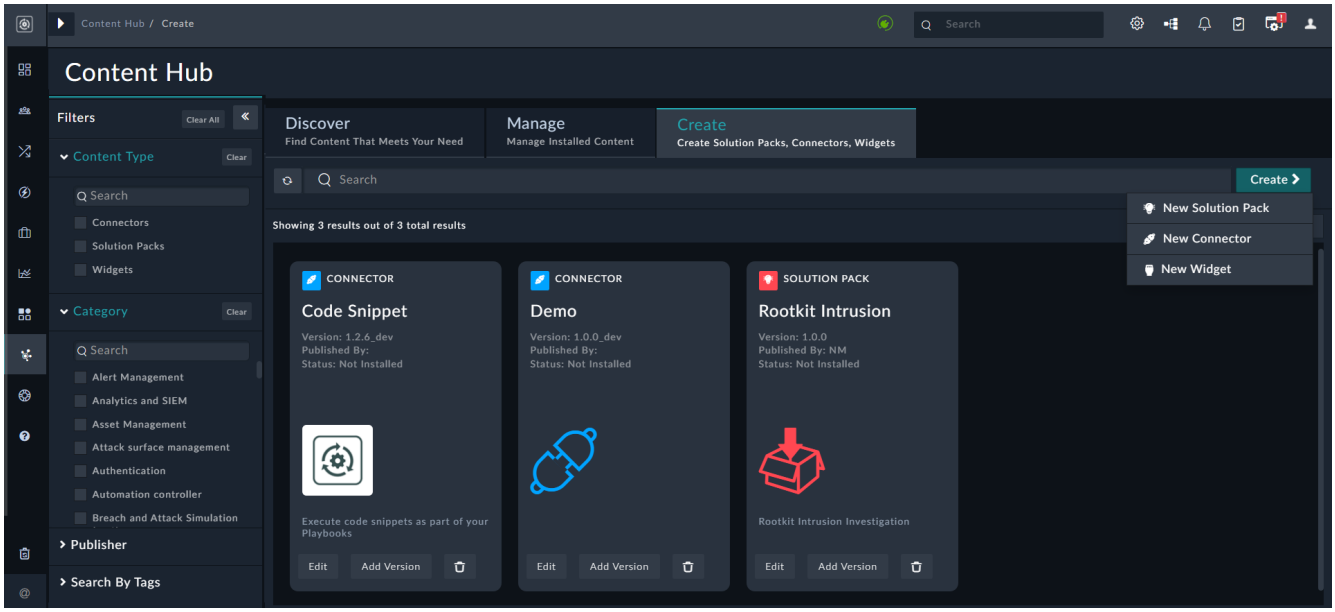
Clicking **Upload** > **Upload <ContentType>** opens the Upload <ContentType> popup, where you can drag-and-drop the .tgz or zip file of the add-on or browse to the .tgz or zip file to add the add-on in FortiSOAR. If you have an existing version of the connector, widget, or solution pack on your system, then you can click the **Replace existing version** checkbox to replace that version of the connector, widget, or solution pack.

Ensure that all the dependencies for the add-on gets installed. If the dependencies are not installed for connectors, then you can install them using the CLI. In the case of Solution Packs and widgets you can try to install them using the UI.

Click on a tile to open the add-on popup, which displays the information about the add-on, and using which you can perform various actions such as editing, cloning, exporting, uninstalling (or deleting) the add-ons.

Create tab

The **Create** tab displays the add-ons on which you are currently working and which have not been published:



You can perform the following operations from the add-on card in the Create tab:

- **Edit**: This allows you to edit the add-on, which in the case of connectors and widgets opens the code editor interface and in case of solution packs opens the `Edit Solution Pack` wizard.
- **Add Version**: This allows you to add a version for the add-on, which in the case of connectors and widgets opens the `Clone <add-on>` dialog and in the case of solution packs opens the `Clone Solution Pack` wizard.
- **Delete**: This allows you to delete the add-on.

You can also create new add-ons by clicking **Create New** and then selecting the type of add-on you want to create. Clicking **Create New** > **New <ContentType>** opens the wizard for that particular add-on using which you can create the add-on.

For more information on Widgets and Solution Packs, see the Widgets and Solution Packs chapters respectively, and for Connectors, see the "Connectors Guide."

Content Hub Portal

The Content Hub is also available publicly at: https://fortisoar.contenthub.fortinet.com/, to view out-of-the-box reference material and product add-ons like connectors, playbooks, solution-packs, widgets, etc.

The Content Hub portal displays FortiSOAR highlights, such as featured solution packs, curated solutions, information about FortiSOAR community, its forums, etc. It also contains a **Search** box (minimum three characters are required to search) using which users can search through the complete Content Hub portal.

The Content Hub portal contains all reference material and add-ons offered by FortiSOAR, including connectors, solution packs, widgets, how to's, etc. The Content Hub portal allows you to search and filter content using various

criteria such as the content type (connectors, solution packs, how-tos, etc.), category of the content. On the listing page for a particular content type, you can click a card to displays the detailed page for that content. For example, clicking on a connector card, for example, Fortinet FortiSIEM opens a page containing a brief introduction about the connector, the release highlights for that particular version of the connector, etc. It also contains a drop-down list of the previous versions for that connector. Clicking on a previous version opens a page containing information for that version of the connector.

You can also experience the Content Hub portal on your mobile and with the same pages, listings, and details as is present in a browser

Troubleshooting Tips

Unable to see updates for your entities in Content Hub

If you are unable to see updates for your entities such as connectors, widgets, etc. in Content Hub, it could be because the Content Hub data is not synced with the FortiSOAR repository.

Resolution

To resolve this issue, you can wait for the next synchronization cycle between Content Hub and the FortiSOAR repository. The Content Hub data gets synchronized from the FortiSOAR repository, currently, at the thirtieth minute of every hour (for example, 1:30, 2:30).

Or, you can manually force the synchronization using the following command:

```
sudo -u nginx php /opt/cyops-api/bin/console app:contenthub:sync --force
```

Solution Packs

FortiSOAR is built using modular architecture and solution packs are the implementation of best practices to configure and optimally use FortiSOAR. The solution packs also contain a lot of sample/simulation/training data that enables you to experience FortiSOAR without having all the devices. FortiSOAR provides several out-of-the-box (OOB) solution packs to facilitate users to get started easily and effectively.

Only certified Solution Packs are eligible for support. Support is limited to only the pack functionality in ideal environments and does not apply to any resolving system conflicts or changes that might have taken place due to the pack installation. Since a solution pack can require changes in system configurations and views, we strongly recommend that before you install a solution pack, you should review the solution packs and their dependencies before installation, take system backups, and test the solution pack in staging/development environments.

Some of the out-of-the-box (OOB) solution packs include:

- **SOAR Framework**: Enables users to experience the power of FortiSOAR incident response. This Solution Pack (SP) is the **Foundational** Solution Pack that creates the framework, including modules, dashboard, roles, widgets, etc., required for effective day-to-day operations of any SOC. As the Incident Response modules, i.e., Alerts, Incidents, Indicators, and War Rooms are not part of the FortiSOAR platform, it becomes essential for users to install the SOAR Framework SP to optimally use and experience FortiSOAR's incident response. For detailed information about the SOAR Framework SP, see the SOAR Framework SP documentation.
  Note: *From release 7.2.0 onwards, the SOAR Framework Solution Pack (SP) is installed by default with the fresh installations of FortiSOAR*. If you have upgraded your FortiSOAR system from release 7.2.0 to a release later than 7.2.0, for example, 7.2.1, and if the SOAR Framework SP has an updated release, for example 1.0.1, then in the Manage tab, an **Update Available** link is visible on the SOAR Framework SP's card. Similarly, if you have a freshly installed FortiSOAR release 7.2.1 system, then by default release 1.0.1 of the SOAR Framework SP is installed.
- **Multi Tenancy**: Enables users to experience the power and capability of FortiSOAR incident response in a multi-tenant architecture.
- **MITRE ATTACK Enrichment Framework**: Enables users to use the information and knowledge base that's provided by the MITRE ATTACK Framework to its full extent.
- **Knowledge Base**: Enables users to configure and optimally use FortiSOAR based on best practices. It provides users with information about different things like (triage processes, tools, etc.) used in a SOAR.

Many more out-of-the-box (OOB) solution packs are included with FortiSOAR and documentation comes bundled with each solution pack.
Content Hub contains the complete listing of all the solution packs. FortiSOAR allows users to edit out-of-the-box (OOB) solution packs if users want to customize a solution pack to suit their requirements and even build new packs for custom use cases.

Permissions required for using Solution Packs

Following are the permissions that you must be assigned to perform operations on solution packs:

- To install a solution pack from the Content Hub, you must be assigned a role that has a minimum of `Create`, `Read`, and `Update` permissions on the `Security` module, `Create` and `Read` permissions on the `Solution Packs`

module, and `Read` permission on the `Application` and `Content Hub` modules.

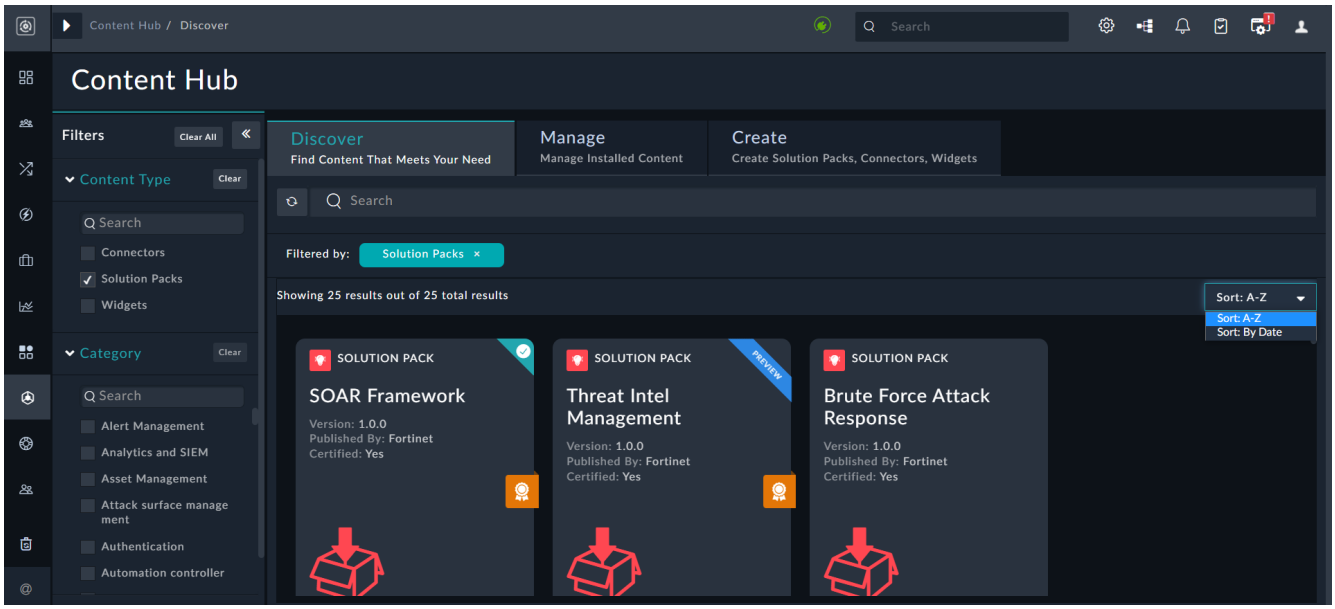
- To import a solution pack, you must be assigned a role that has a minimum of `Create`, `Read`, and `Update` permissions on the `Application` and `Security` modules, `Create` and `Read` permissions on the `Solution Packs` module, and `Read` permission on the `Content Hub` module.
- To create a new solution pack, you must be assigned a role that has a minimum of `Create` and `Read` permissions on the `Security` and the `Solution Packs` modules, and `Read` permission on the `Application` and `Content Hub` modules.
- To edit Solution Packs, i.e., view the solution packs listed in the Content Hub and changes made to the Content Hub, you must be assigned a role that has a minimum of `Read` permission on the `Application` and `Content Hub` modules, a minimum of `Create`, `Read`, and `Update` permissions on the `Security` module, and `Update` and `Read` permissions on the `Solution Packs` module.
- To clone Solution Packs, you must be assigned a role that has a minimum of `Read` permission on the `Application`, `Security`, and `Content Hub` modules, and a minimum of `Create`, `Read`, `Update` permissions on the `Solution Packs` module.
- To export Solution Packs and download the zip file of solution packs, you must be assigned a role that has a minimum of `Read` and `Update` permissions on the `Application` and `Security` modules, a minimum of `Read` permission on the `Solution Packs`, `Content Hub`, and `File` modules.
- To delete Solution Packs, you must be assigned a role that has a minimum of `Read` permission on the `Application` and `Content Hub`, and a minimum of `Read` and `Delete` permissions on the `Solution Packs`and, `Security` modules.

Apart from above permissions you also must have appropriate permissions for all the entities, i.e., modules, connector, widgets, dashboards, etc. that are used in solution packs. If you do not have the appropriate permissions then those entities (modules, connectors, widgets, etc) are skipped while working (cloning, editing, creating, etc) with the solution packs. If you do not have appropriate permissions for all the entities, then you will be unable to import and install solution packs.

You must ensure that repo.fortisoar.fortinet.com is reachable from your FortiSOAR instance. Otherwise, you will see a blank page when you click Content Hub in the left navigation.

Viewing Solution Packs in Content Hub

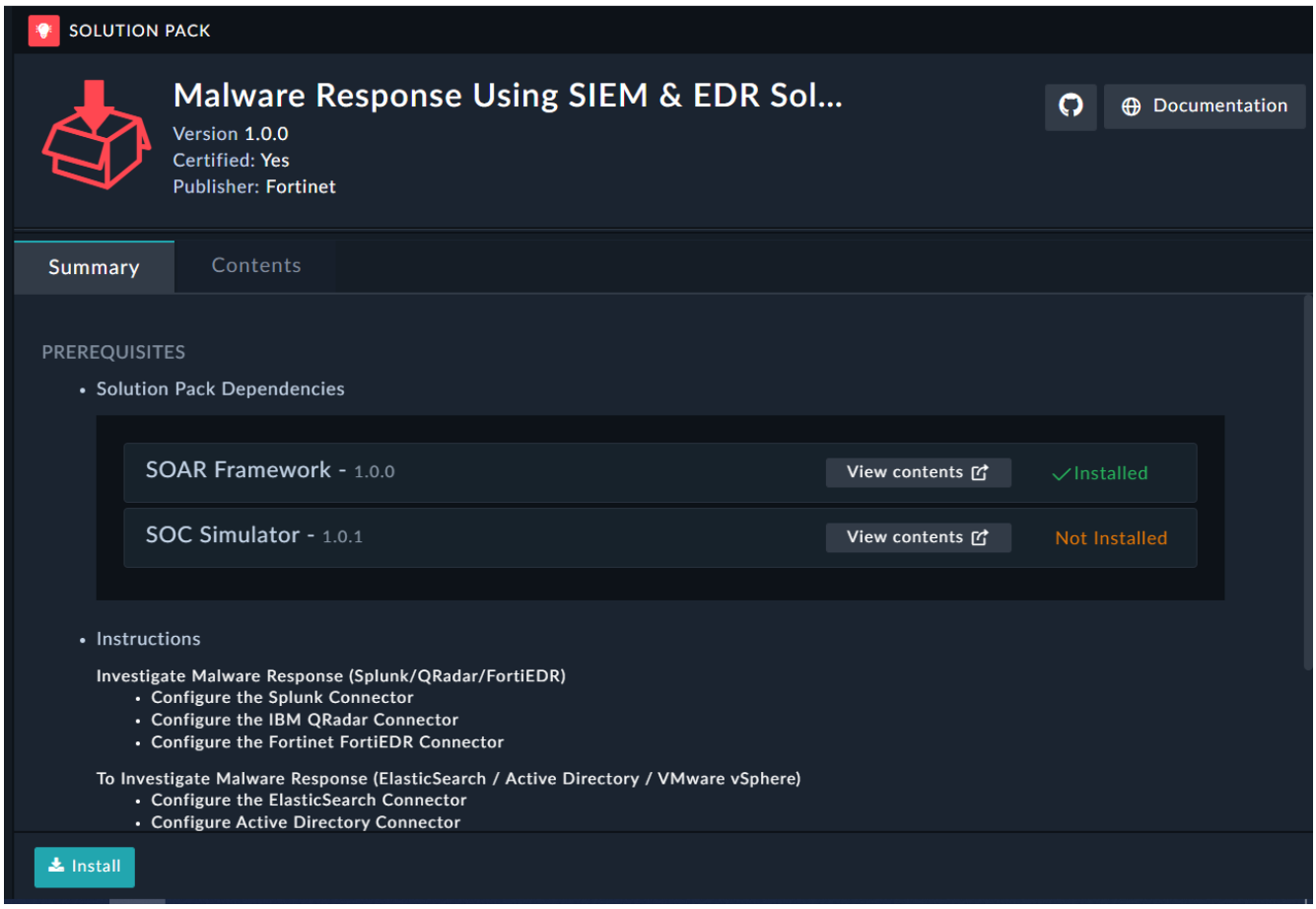
To view solution packs, on the FortiSOAR left navigation, click **Content Hub**. On the `Content Hub` page, from the **Filter** panel choose **Solution Packs** to view the list of all currently available solution packs:



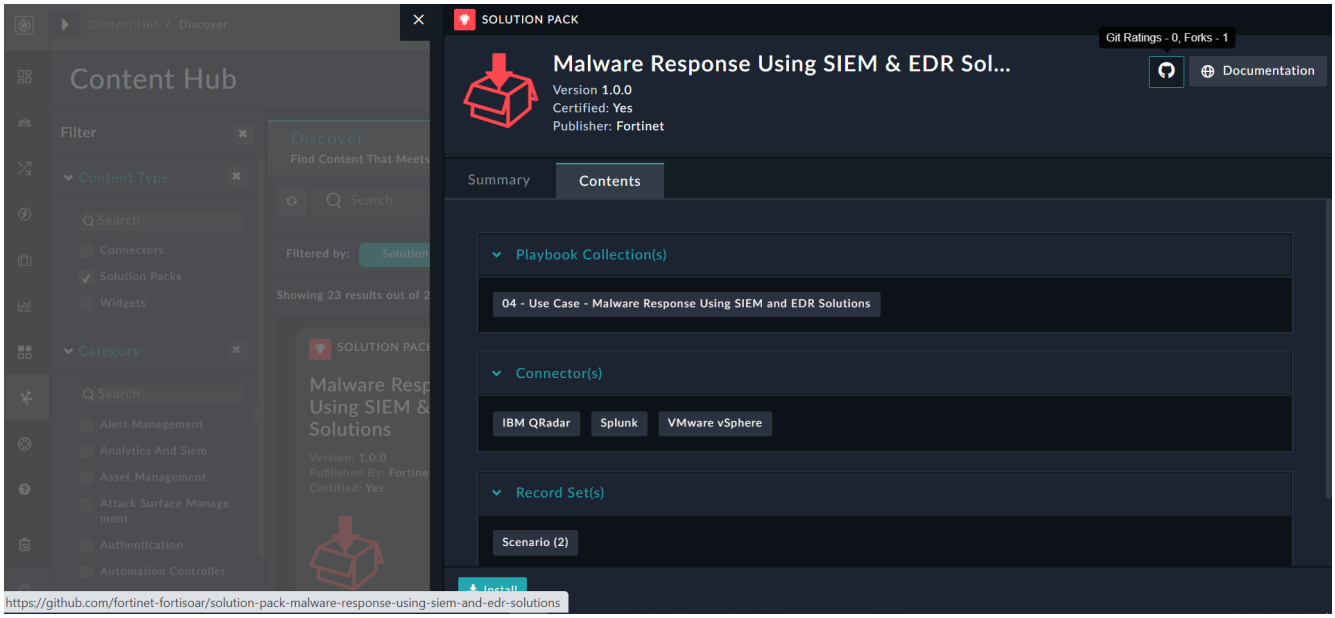
You can search for a solution pack using the **Search** field and sort the solution pack alphabetically (A-Z) or by date. Using the **Filters** panel, you can filter the solution packs displayed in all the tabs based on varied criteria. Solution packs that are installed appear with a tick on their card, for example the SOAR Framework solution pack in the above image. Some Solution Packs (SP) have an orange icon, which signifies a 'Featured' SP, for example the SOAR Framework SP. Featured SPs are those SPs that are significant to SOAR operations and therefore have been highlighted. Similarly, some SPs have a 'Preview' ribbon which signifies that these SPs are being released like a "BETA" version with more enhancements being planned for subsequent releases to make them more comprehensive and robust, for example the Threat Intel Management SP. For more information on Content Hub, see the Content Hub chapter.

Working with Solution Packs

Click **Content Hub** > **Discover** to view a list of available SPs. To view the details of the solution pack and to perform actions on the solution pack, click the card of the solution pack. The solution pack popup contains a Summary tab and a Contents tab. The **Summary** tab contains a brief description of the solution pack, additional information such as the category of the solution pack and support contact information, and prerequisites or dependencies that must be fulfilled before installing that solution pack, as well as instructions on what steps must be performed for the solution pack to work:



Click **View Contents** to open the SP in the new window and install that SP or view its contents.
The **Contents** tab lists the contents of the solution pack, i.e., it displays the list of modules schemas, record sets, roles, playbook collections, widgets, connectors etc. that are part of that solution pack:



To install a solution pack, click **Content Hub** > **Discover** and then click on the card of the solution pack that you want to install to open that solution pack's popup, and then click **Install**.

Other ways that you can install a Solution Pack are:

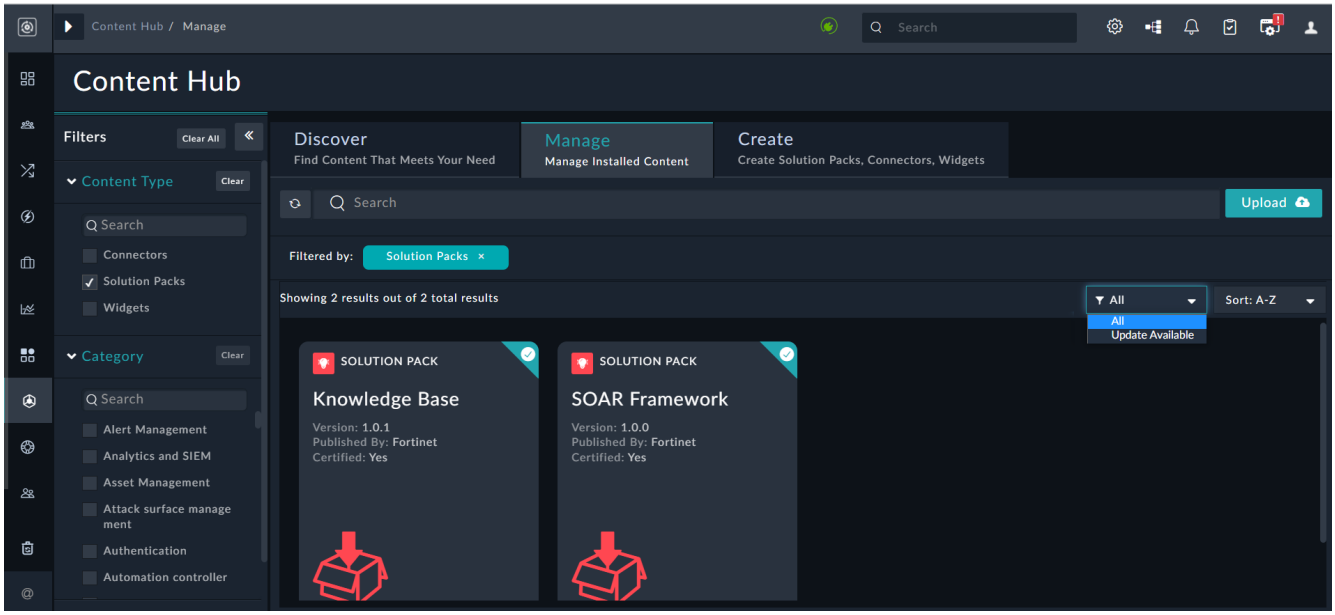
- Import (Upload) a Solution Pack (.zip file) on the **Content Hub** > **Manage** tab. The process of the same is explained later in this topic.
- Import the Solution Pack using the Import Wizard. The process of importing and exporting entities is explained in the Application Editor chapter in the "Administration Guide."
  Note: It is not recommended to import a Solution Pack using the Import Wizard, since only the Solution Pack data gets imported into the system, but the Solution Pack template is not created and the Solution Pack does not get created in the Content Hub. Therefore, in this case, you can only use the imported entities (widget, connectors, reports, etc), but not the Solution Pack template.

Before you install a Solution pack, consider the following:

- Solution packs that contain "Module Schema(s)" (**SP dialog** > **Contents**) replace the settings and views of the following in your existing system:
  - 'System View Template' including the view of the specified schema
  - 'Action Buttons' displayed on top of the grids
  - 'Recommendations Settings' that provide the similarity suggestion
- Install Solution packs in test environments and take system backups before installing a solution pack - Since solution packs can potentially alter your existing configurations and views, it is recommended to install Solution Packs in test environments and have system backups in place, such as backing up your System View Templates using the Import Wizard before installing a solution pack to avoid rework on manual adjustment of the settings to meet your requirements.
- Some solution packs might need a 'System Publish' activity, causing the system to be unavailable for as long as a few minutes, and all the users will need to wait for this process to complete before resuming usage.

Once installed the solution packs appear in the **Manage** tab.

On the **Manage** tab, you can view the content that is installed, in our example, you can view the installed solution packs:



You can search for a SP by its name in the **Search** box and sort the SPs either alphabetically or by date. Similarly, you can filter the installed SPs that have an upgraded version, by selecting **Update Available** from the drop-down list. On

the SP's card, you can also see if any SP that is installed on your system has an upgraded version. For example, if you have installed the Knowledge Base v1.0.1 solution pack on your system and v1.1.0 is available, you will see an **Update Available** link, which you can click to open the solution pack's popup. On the solution pack's popup, you will see an **Update to <version number>** button, clicking which upgrades the solution pack to the newer version.

To upload a custom solution pack (.zip) that you have already created, click **Upload** > **Upload Solution Pack**. This opens the `Upload Solution Pack` popup where you can drag-and-drop the .zip file of the solution pack or browse to the .zip file to add the solution pack in FortiSOAR. If you have an existing version of the solution pack on your system, then you can click the **Replace existing version** checkbox to replace that version of the solution pack.

Notes:

- If there is any depenedency associated with the custom solution pack, the you must install that dependency before importing the solution pack.
- If your custom solution pack has a dependency on a solution pack that is part of the repository, for example, MITRE Framework, then the repo solution pack gets installed (if not already installed) when the custom solution pack is installed.
- If you are exported a repository solution pack, for example MITRE Framework SP, and imported the same to another system, then that imported solution pack is considered as local custom solution pack and you will not get further updates to that solution pack.

You can perform the following actions on the popup of an installed SP:

- **Edit**: To edit an installed repository solution pack to suit your requirements, click **Edit**, to open th confirmation dialog for creating a local copy of that solution pack. Clicking Confirm opens the **Clone Solution Pack** Editor. For details on editing solution packs, see Editing an existing Solution Pack. In the case of custom (local) solution pack, you can simply edit the solution pack; a local copy does not get created.
- **Export**: To export a solution pack in the `.zip` format so that it can be used in another environment, click the **Export** button. Once the solution pack is saved as a `.zip` file, you can import the same using **Upload > Upload Solution Pack.**
- **Delete**: To delete an installed solution pack, click **Delete Template** which displays a `Confirmation` dialog. Click **Confirm** on the dialog to uninstall the solution pack.When you perform the delete operation, the the solution pack template gets deleted, and data associated with the installed solution pack, such as the data of the associated connectors, widgets, etc, are retained on your system.

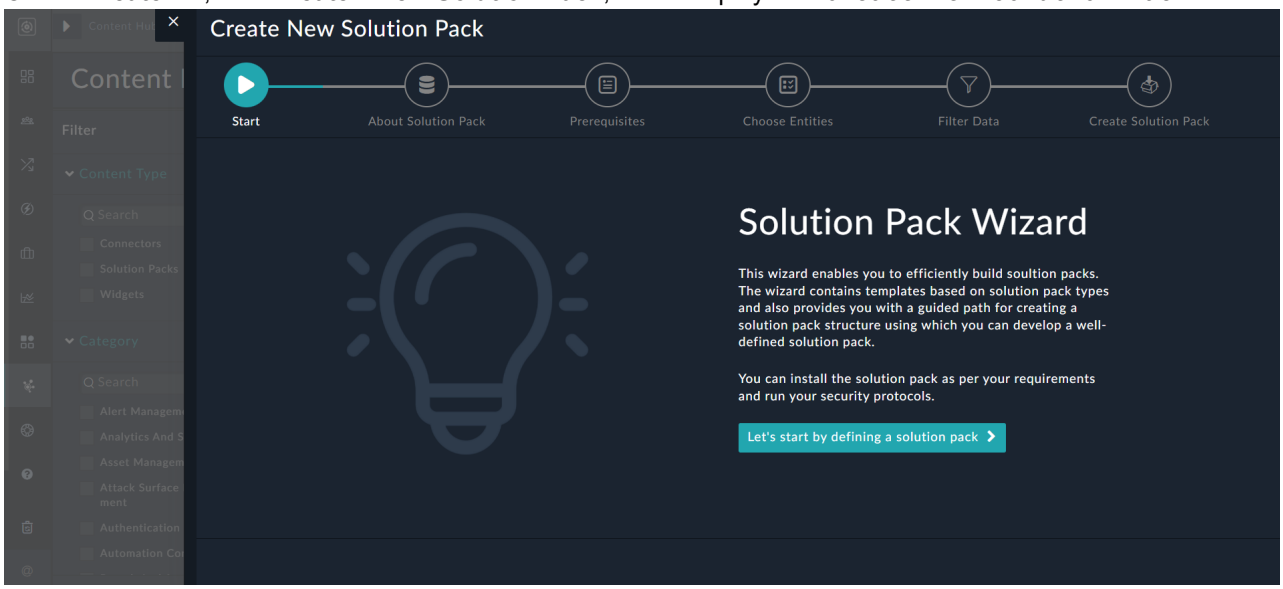
Apart from this, the solution pack also contains a link to its **Documentation** and its **GIT** repository, if that solution pack is part of the public GIT repository. When you hover on the **GIT** icon you can see the ratings of that solution pack and the number of forks that have been created from that solution pack.

Creating Solution Packs

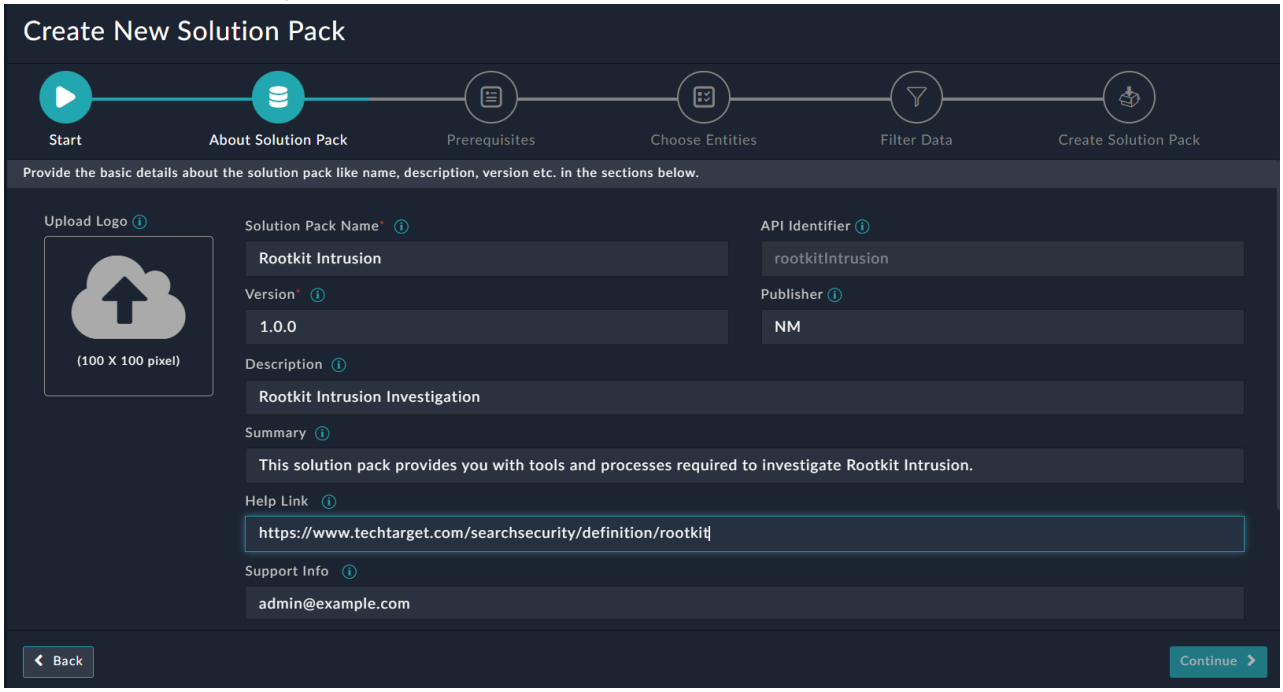
Use the Solution Pack Building Wizard to efficiently create new Solution Packs.

To create a new Solution Pack, do the following:

1. On the FortiSOAR left-navigation, click **Content Hub** > **Create**.
2. On the **Create** tab, click **Create** > **New Solution Pack**, which displays the `Create New Solution Pack` Wizard.



3. Click **Let's start by defining a solution pack** to open the **About Solution Pack** screen where you can provide the metadata for the solution pack such as the title, version, etc.



Details that you can provide are:

a. Upload a logo for the solution pack.

b. In the **Solution Pack Name** field, enter an appropriate title for your Solution Pack.
Note: Supported characters for the title, alphanumeric characters, spaces, colon, hyphen, ampersand (&), or underscores. Also, the value that you enter in this field must not match the name of any other Solution Pack that is available in the Content Hub. For example, you cannot enter `SOAR Framework` in this field, since the SOAR Framework Solution Pack is available in the Content Hub.

c. In the **API Identifier** field contains an auto-populated name based on the name that you specify for the solution pack. The API Identifies is used as a variable in the Solution Pack code to reference this Solution Pack

d. In the **Version** field, enter the version of the Solution Pack in the x.y.z format. For example, `1.0.0`. As a good practice, you should always increase the version number before making changes to an installed solution pack.

e. (Optional) In the **Publisher** field, enter the name of your organization as the publisher of this Solution Pack. The publisher of the Solution Pack is responsible for maintaining and supporting the Solution Pack.
If you want to keep the Solution Pack anonymous, then you can add the "Community" keyword. If this field is left blank, again the Solution Pack's publisher is automatically set to "Community".
Note: Do not enter "Fortinet" in this field.

f. (Optional) In the **Description** field, enter information for the Solution Pack that you are creating. The Description is displayed on the Solution Pack card on the Content Hub listing page and enables users to understand more about the Solution Pack.

g. (Optional) In the **Help Link** field, you can enter the links of the web pages that contain the details of the solution pack.

h. (Optional) In the **Support Info** field, you can enter support email IDs that users can contact if they have any issues with the solution pack.

i. (Optional) From the **Category** list, select the categories in which you want to place this solution pack. For example, Authentication, Centralized Security Management, Threat Intelligence, etc.

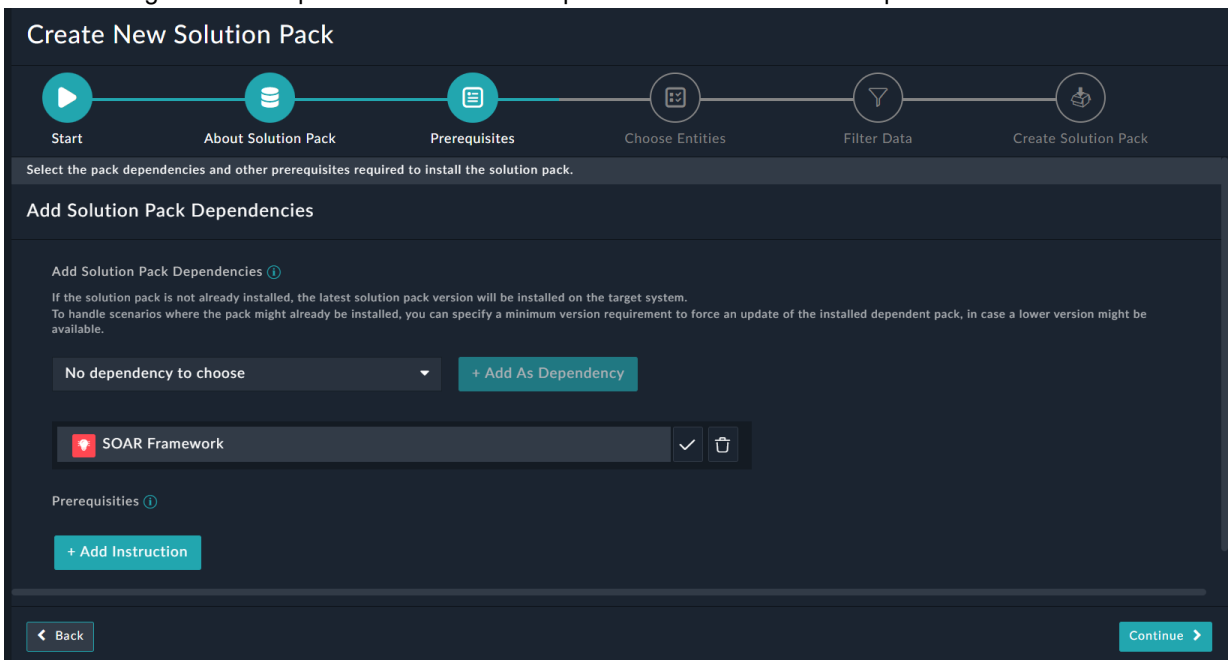
j. (Optional) In the **Tags** field, enter the keywords that you want to associate with the Solution Pack. Tags make it easier to search and filter solution packs.

k. Click **Continue** once you have completed entering the details.

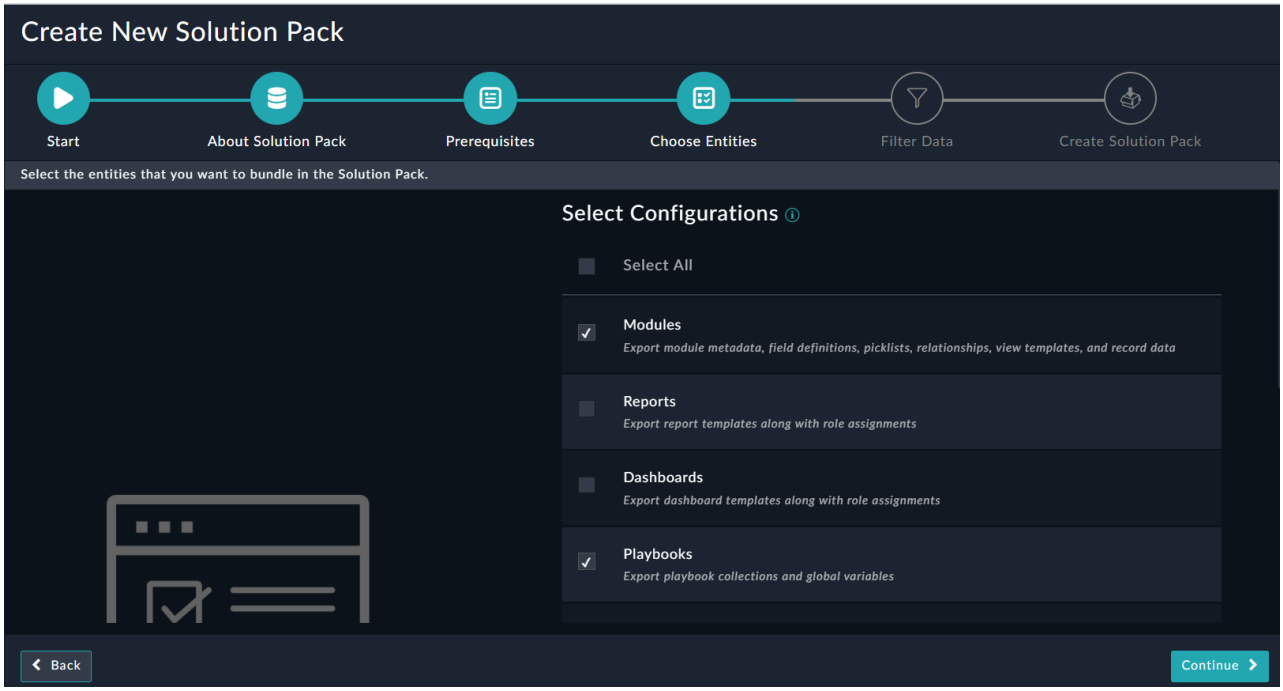
4. On the **Prerequisites** screen, add the dependencies and other prerequisites that are required to install the solution pack:

a. From the **Select Solution Pack** list, select the solution packs that must be installed by users on their system before installing this solution pack, and then click **Add as Dependency**.

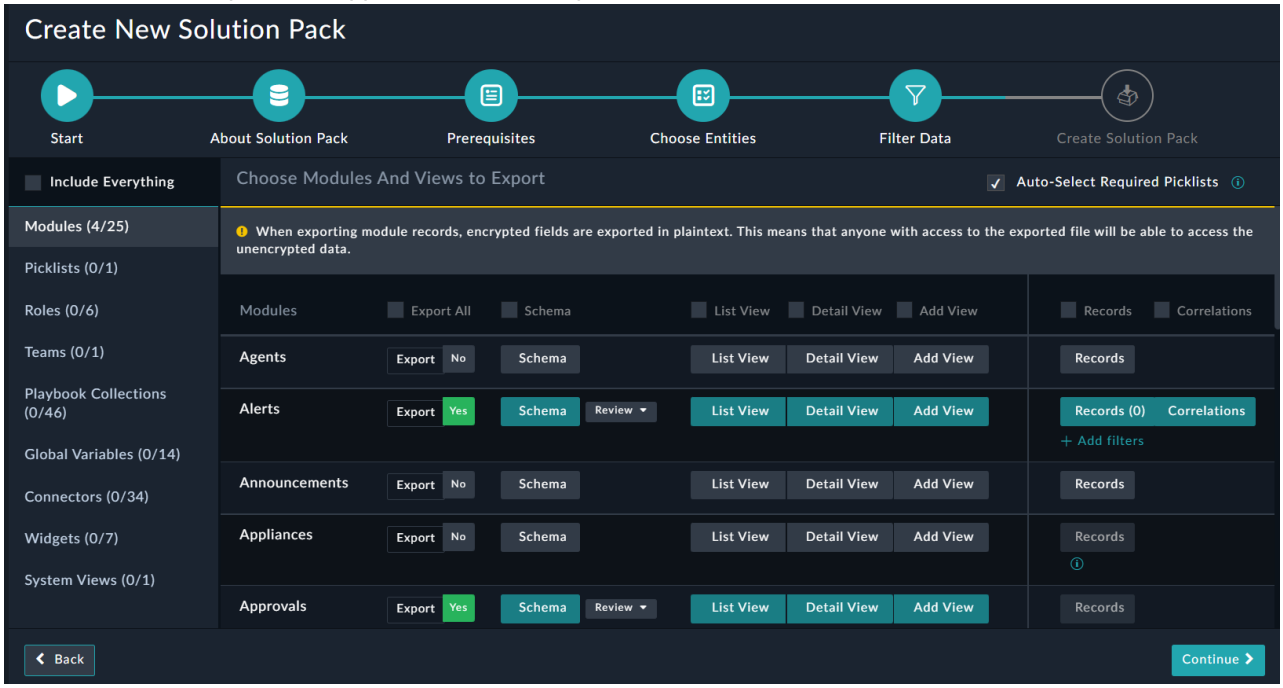
b. In the **Prerequisites** section, click **+ Add Instruction** to add instructions that require to be followed by users for the solution pack to work, and then click **Continue**. Examples of this could be simple code snippets or commands that users need to run after installation of the solution pack, or a list of steps users should follow after installing the solution pack. You can add multiple instructions for a solution pack.



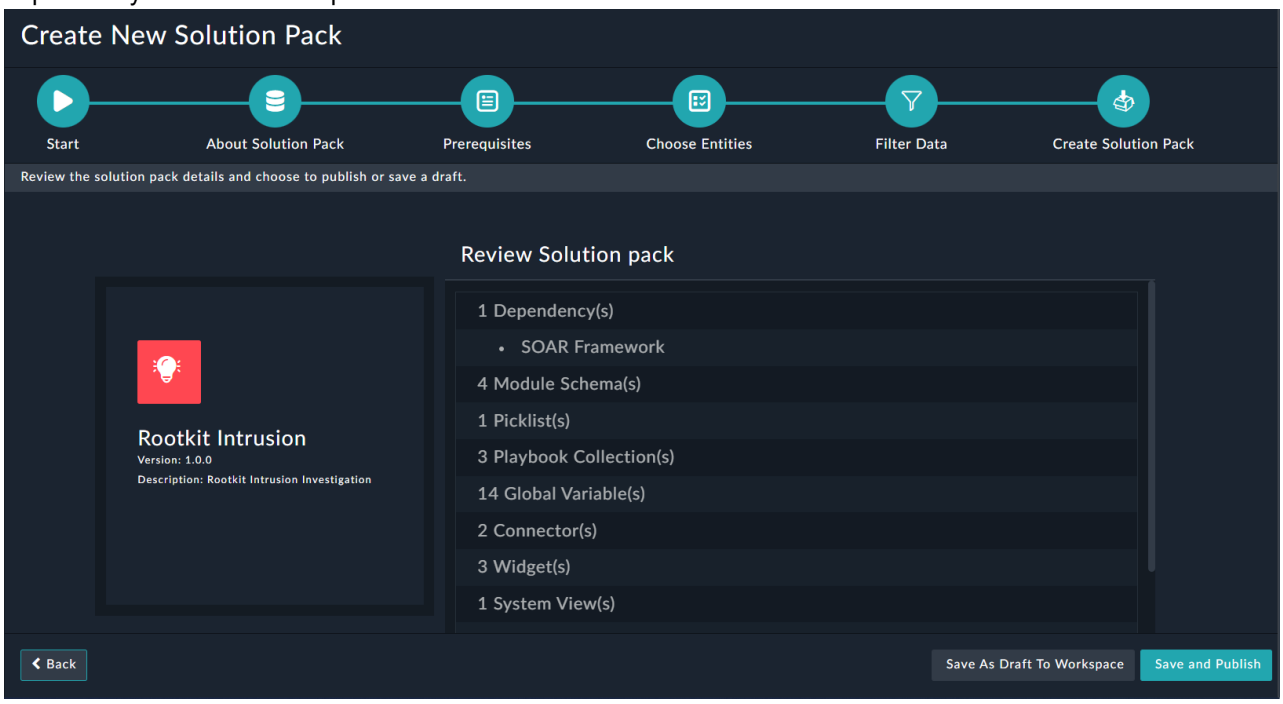
5. On the **Choose Entities** screen, select the entities such as modules, playbooks, connectors, administrative and security settings, etc., that you want to bundle with the solution pack, and then click **Continue**.



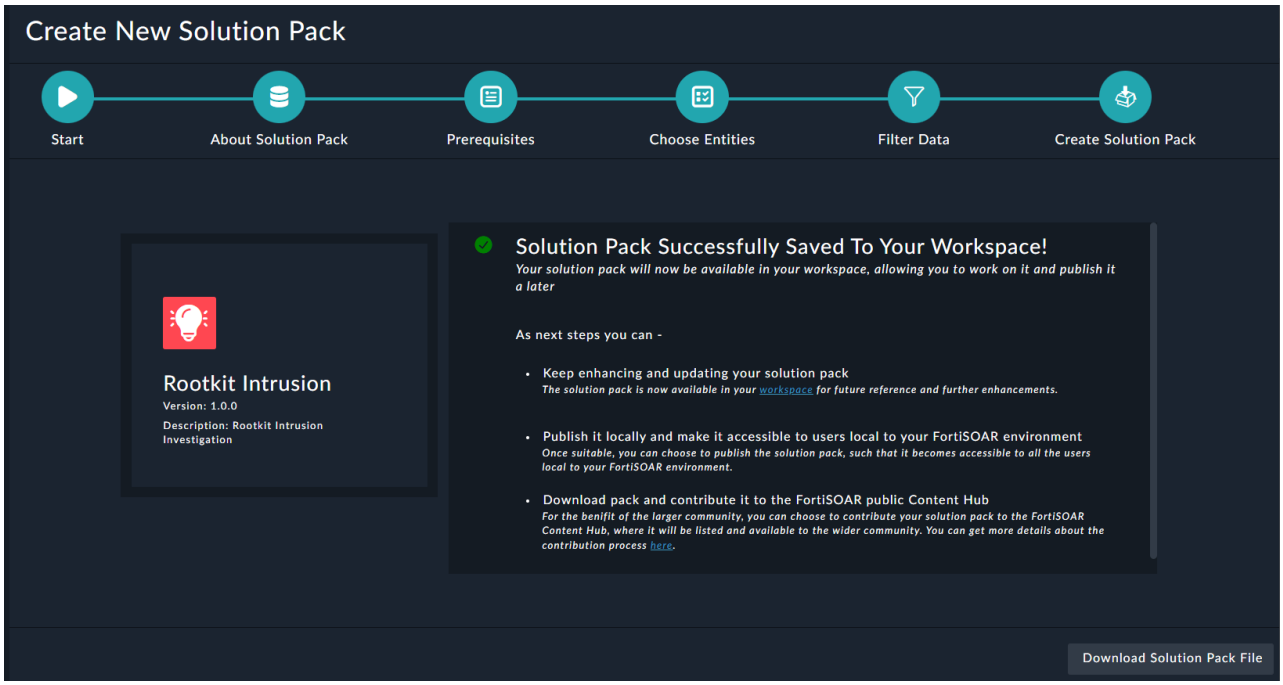
6. On the **Filter Data** screen, you can choose the granular details of the entities that you want to include in the solution pack and then click **Continue**. The entities displayed on this screen are dependent on the entities that you have selected on the **Choose Entities** screen. For example, if you only want a specific set of modules to be part of the solution pack, then you can select only those modules, such as Alerts, Approvals, Incidents, Tasks, etc. You can also choose the fields that you want to include in a selected module by clicking **Review**. To include record sets, click **Records**, and to include their correlations, click **Correlations**.
The Filter Data screen is the same as is present in the Export Wizard. For details on the Filter Data screen, see the `Export Wizard` topic of the *Application Editor* chapter in the "Administration Guide".



7. On the **Create Solution Pack** screen, you can review the solution pack contents and details of the solution. Click **Create a Draft To Workspace** saves the solution pack in the **Create** tab where you can continue to refine the solution pack. Solution Packs that are in the '**Draft**' state are not available for local users to include in their solution packs, i.e., they cannot be included in any other solution pack as a dependency; though they can make edits to the solution pack in the Create tab. Click **Save and Publish** to publish the solution pack and add this solution pack in the **Manage** tab. Publishing makes the solution pack available to other users who are local to your FortiSOAR environment, i.e., users who are locally present in your FortiSOAR environment can select the solution pack as a dependency for their solution packs.



8. For our example, we clicked **Create As Draft To Workspace**, which displays a screen mentioning the next steps that you can perform with the solution pack. You can also click **Download Solution Pack File** to download a zip file of your solution pack.



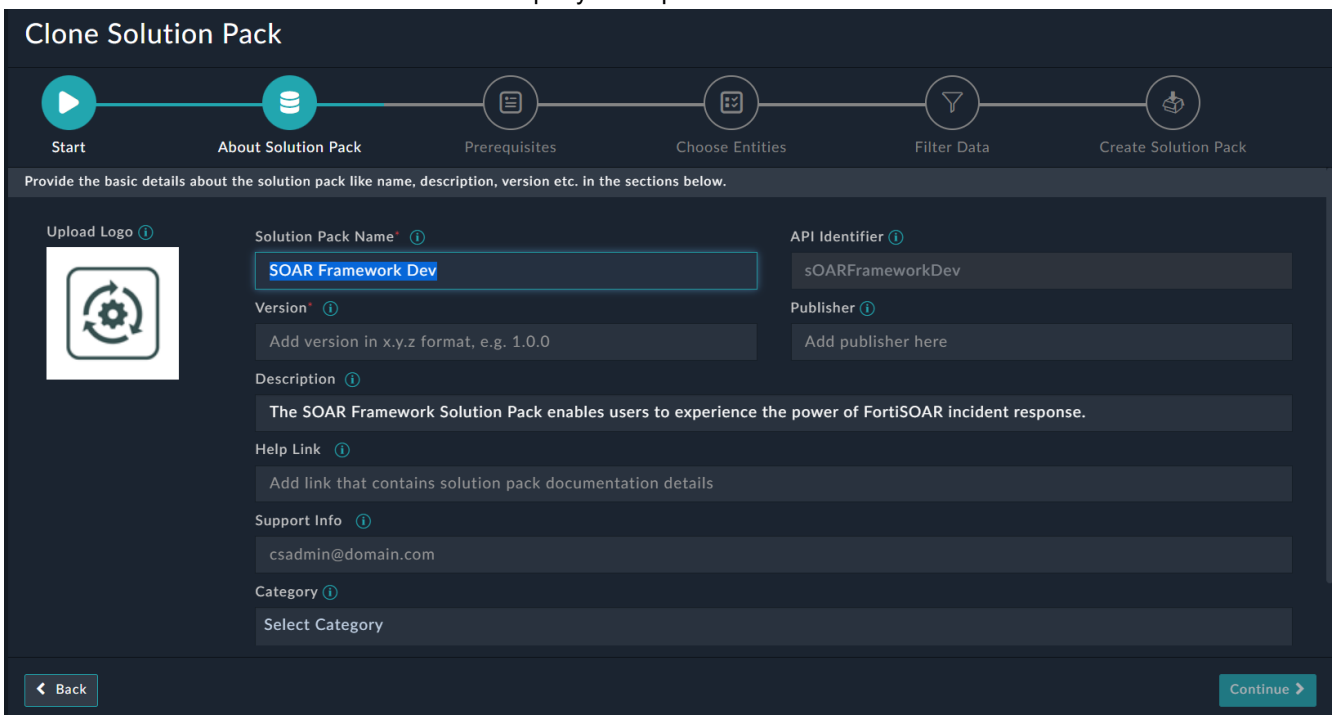
The next steps that you can perform are:

- Keep enhancing and updating the solution pack in your WorkSpace tab.
- Publish the solution pack and make it accessible to users local to your FortiSOAR environment.
- Download the solution pack and contribute it to the FortiSOAR public Content Hub. This option contains a link that opens a GIT repository that contains instructions on how a user can contribute to the public Content Hub.

Editing an existing Solution Pack

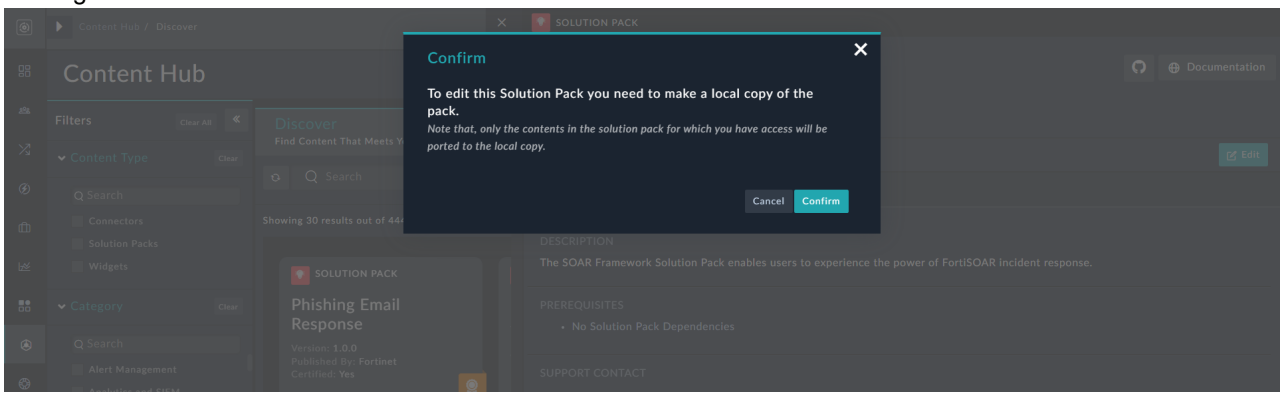
To edit a solution pack that is in your local environment (and not published), go to the **Create** tab, and click edit on the solution pack card to open the **Edit Solution Pack** wizard. You can also create a new version of the solution pack by clicking **Add Version** on the solution pack card. This opens the **Clone Solution Pack** wizard, where you can add a new

version of the SP and continue to edit the SP as per your requirements:



To edit a solution pack from the repository to suit your requirements, do the following:

1. On the FortiSOAR left-navigation, click **Content Hub** > **Manage.**
2. On the **Manage** tab, click the card of the solution pack that you want to edit to open the solution pack popup, and then click **Edit**. When you click **Edit**, FortiSOAR displays a confirmation dialog box to get a confirmation on creating a local copy of the solution pack that you can edit, so that you can edit an existing solution pack without impacting the original one:



3. Click **Confirm** to open the **Clone Solution Pack** wizard.
4. Edit the solution pack as required and then either save the solution pack as a draft in the Create tab or publish the solution pack. The Clone Solution Pack wizard contains the same screens and fields as the **Create New Solution Pack** wizard. For more information on the screens and field, see the Creating Solution Packs topic.
   Note: It is recommended that you increase the version number before making changes to an installed solution pack.

Widgets Library

FortiSOAR allows users to edit out-of-the-box (OOB) widgets and build new widgets for custom use cases. FortiSOAR provides many OOB widgets for graphs, charts, utilities, etc., however, there are always customizations and new use cases that are required to meet the user expectations. This feature provides more control to users and allows them to shape the widget based on their available data. For more information on the OOB widgets available in FortiSOAR, see the Dashboards, Templates, and Widgets chapter.

If you have upgraded your instance to FortiSOAR 6.4.1 or later from a version earlier than 6.4.1, then you will not be able to view widgets, due to missing permissions on the `Widgets` module. Administrators require to assign appropriate permissions to users according to the operations using the widgets.

From release 7.2.0 onwards, you can use the Widget Library or Content Hub to view, search, install, upgrade, and uninstall widgets that are part of the FortiSOAR OOB widget library.

In Release 7.2.0, the Widget Library navigation take you to the Content Hub with the relevant 'Widgets' filter selected for browsing ease.

Permissions required for using Widgets

Following are the permissions that you must be assigned to perform operations on widgets:

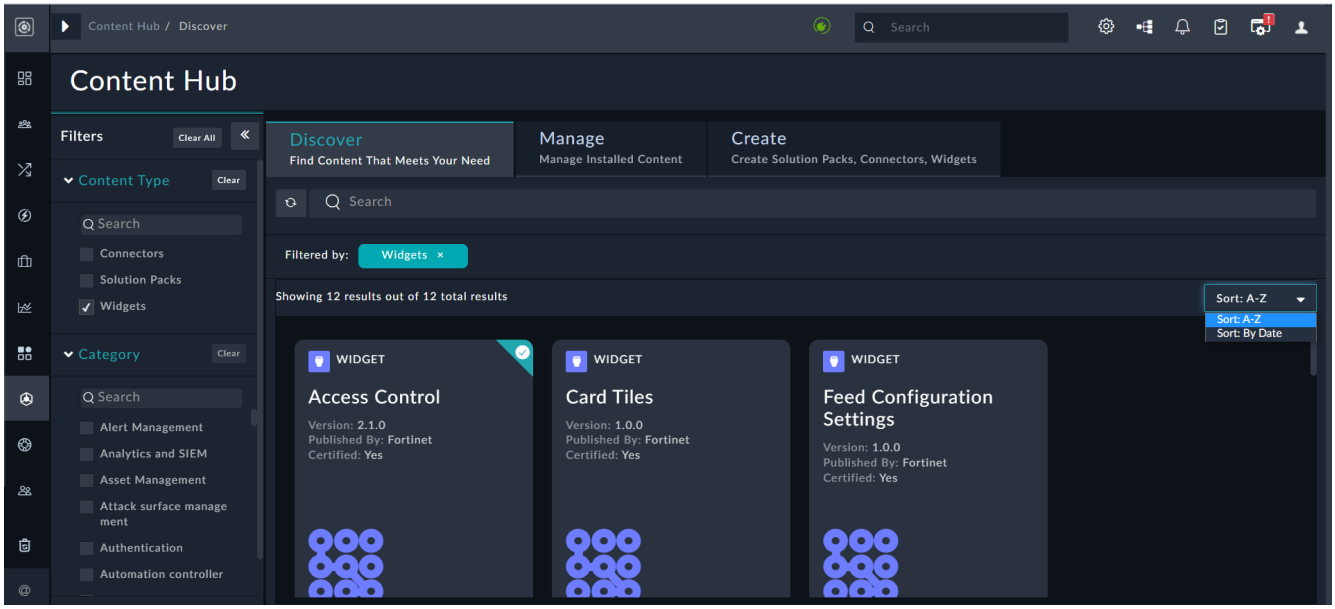
- To work with widgets, i.e., view the widgets listed in the Content Hub and changes made to the Content Hub, you must be assigned a role that has a minimum of `Read` access on the `Application`, `Widgets`, and `Content Hub` modules, a minimum of `Create`, `Read`, `Update` permissions on the `Solution Packs` module.
- To install a widget from the Content Hub or to or to upload a widget to the Content Hub you must be assigned a role that has a minimum of `Read` permission on the `Security` module.
- Apart from the above, to work with widgets, you need appropriate permissions on the `Widgets` module, such as to install a widget or create a new custom widget, you must be assigned a role that has a minimum of `Create`, `Read`, `Update` permissions on the `Widgets` module, or to upgrade and configure a widget, you must be assigned a role that has a minimum of `Update` and `Read` access on the `Widgets` module, etc.

Once you create a new widget or edit an existing OOB widget, and you want to display that widget in dashboards, reports, view panel, listings, etc., you also require appropriate permissions to the FortiSOAR page in which you want to display the widget.

You must ensure that repo.fortisoar.fortinet.com is reachable from your FortiSOAR instance. Otherwise, you will see a blank page when you click Content Hub or Widget Library in the left navigation.

Viewing Widgets

To view widgets, on the FortiSOAR left navigation, click **Content Hub** or **Widget Library**. The **Widget Library** is filtered to display only widgets, whereas the **Content Hub** displays all the out-of-the-box reference material and product add-ons such as connectors, widgets, and solution packs. In this chapter the screenshots included are from the **Content Hub** page; similar screens are displayed in the **Widget Library** page. On the `Content Hub` page, from the **Filter** panel choose **Widgets** to view the list of all currently available widgets:

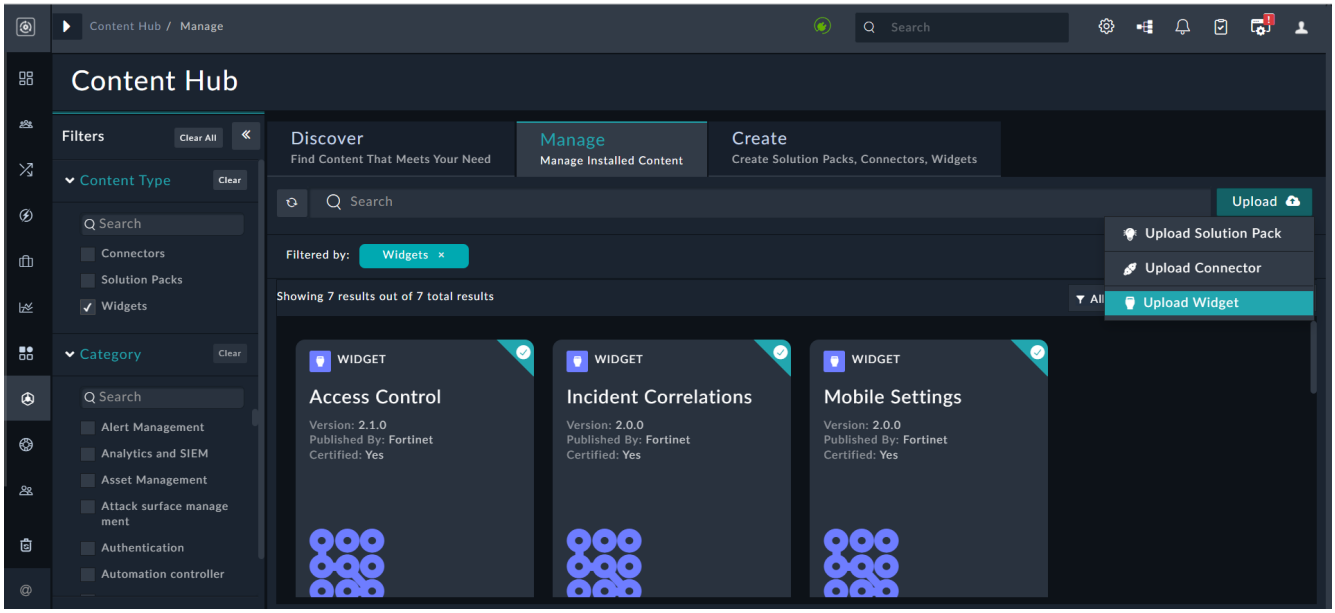


You can search for a widget using the **Search** field and sort the widgets alphabetically (A-Z) or by date. Using the **Filters** panel, you can filter the widgets displayed in all the tabs based on varied criteria. Widgets that are installed appear with a tick on their card, for example, the Access Control widget in the above image. For more information on Content Hub, see the Content Hub chapter.

Working with Widgets

To install a widget, click **Content Hub** > **Discover** or **Widget Library** > **Discover.** Click on the card of the widget that you want to install to open that widget's popup, and then click **Install**. Once installed the widgets appear in the **Manage** tab.

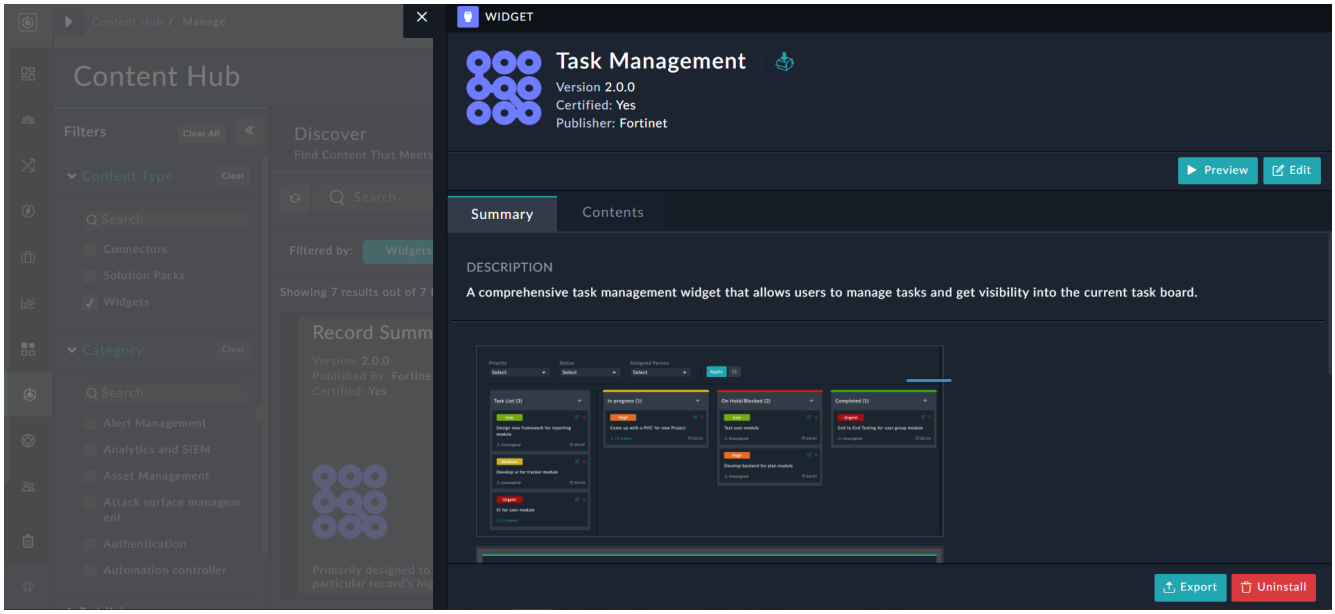
On the **Manage** tab, you can view the content that is installed, in our example, you can view the installed widgets:



You can search for a widget by its name in the **Search** box and sort the widgets either alphabetically or by date. Similarly, you can filter the installed widgets that have an upgraded version, by selecting **Update Available** from the drop-down list. On the widget's card, you can also see if any widget that is installed on your system has an upgraded version. For example, if you have installed the Access Control v2.0.0 widget on your system and v2.1.0 is available, you will see an **Update Available** link, which you can click to open the widget's popup. On the widget's popup, you will see an **Update to <version number>** button, clicking which upgrades the widget to the newer version.

To upload a custom widget (.tgz) that you have already created, click **Upload** > **Upload Widget**. This opens the `Upload Widget` popup where you can drag-and-drop the .tgz file of the widget or browse to the .tgz file to add the widget in FortiSOAR. If you have an existing version of the widget on your system, then you can click the **Replace existing version** checkbox to replace this version of the connectors.

To view the details of a widget and to perform actions on the widget, click the card of the widget:



The **Summary** tab contains a brief description of the widget, its compatibility information, information on which FortiSOAR pages, such as dashboards, add forms, etc., on which the widget will be displayed, and an example of the widget usage along with a sample screenshot of the widget. The **Contents** tab contains the feature list for the widget. You can perform the following actions on the widgets popup:

- **Edit**: To edit a widget to suit your requirements, click **Edit**, which if you are editing a local widget, opens the code editor interface, or asks you to change the version of the widget; or if you are editing a widget from a repository clones the repository widget and then opens the code editor interface. For details on editing widgets, see Editing an existing widget.
- **Preview**: Some fields of the widget such as its title, the fields based on which the widget content is filtered or grouped, etc are editable based on the configuration of that widget. To such editable fields, click the **Preview** button.
- **Export**: To export a widget in the `.tgz` format so that it can be used in another environment, click the **Export** button. Once the widget is saved as a `.tgz` file, you can import the same using the **Upload > Upload Widget** button.
  Important: If the Data Import JSON file contains a version of the widget that is not available in the FortiSOAR repository, then the latest available version of that widget gets installed. For example, if you are trying to import the JSON file that contains *userAssignments* 1.0.0 widget that is not available in the FortiSOAR repository; but, version 1.1.0 is available, then version 1.1.0 of the *userAssignments* widget gets installed.
  Note: If you export a widget from the 'Managed' tab, i.e., an installed widget, and you import that widget, then such widgets get directly installed, i.e., they appear in the **Discover** tab; however, if you export a widget that has not been published , i.e., from the 'Create' tab, then such widgets are added to the 'Create' tab.
- **Uninstall**: To uninstall an installed widget click **Uninstall** which displays a `Confirmation` dialog. Click **Confirm** on the dialog to uninstall the widget.

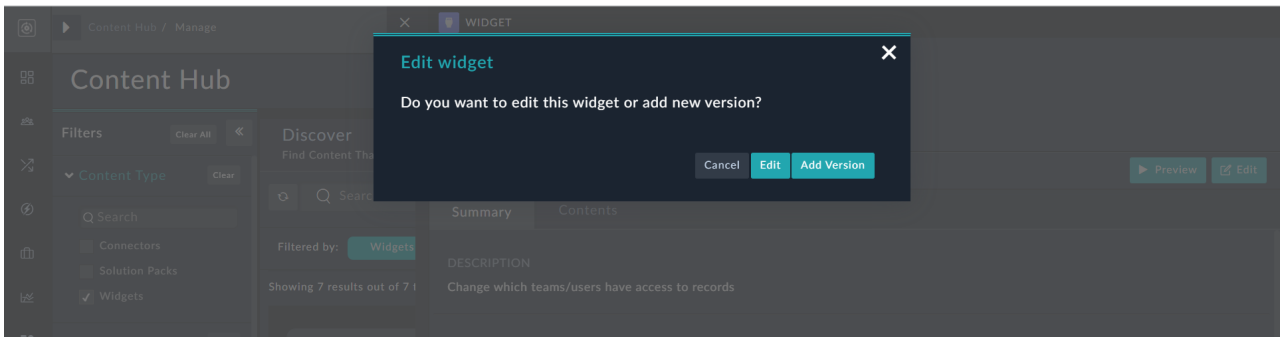
You cannot uninstall system widgets such as the Mobile Settings widget or the Task Management widget.

You can add the installed widgets to FortiSOAR pages, such as reports, view panel, etc., based on the widget configuration specified.

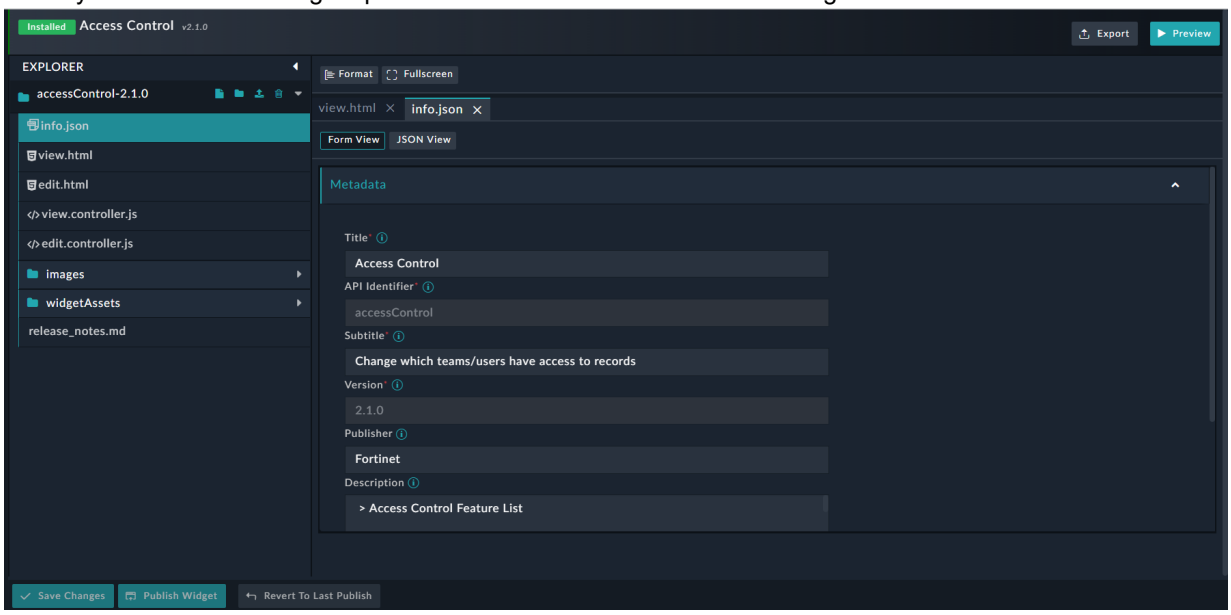
Editing an existing widget

To edit a widget from the repository to suit your requirements, do the following:

1. On the FortiSOAR left-navigation, click **Content Hub** > **Manage** or **Widget Library** > **Manage**.
2. On the **Manage** tab, click the card of the widget that you want to edit to open the widget's popup, and then click **Edit**. When you click **Edit**, FortiSOAR displays a confirmation dialog box that lets you choose whether you want to edit this widget or add a new version for the widget:

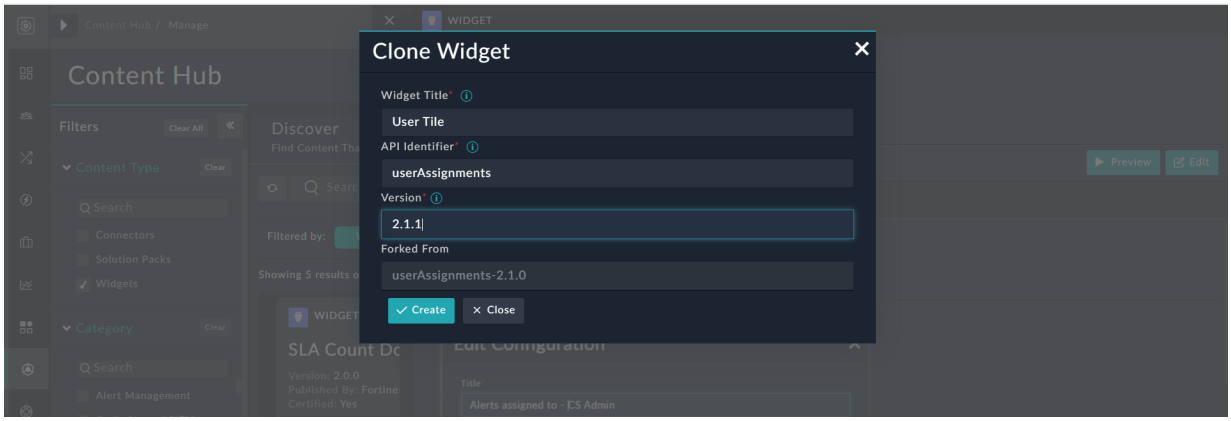


a. When you click **Edit** the widget opens in the code editor interface and also gets saved in the **Create** tab:

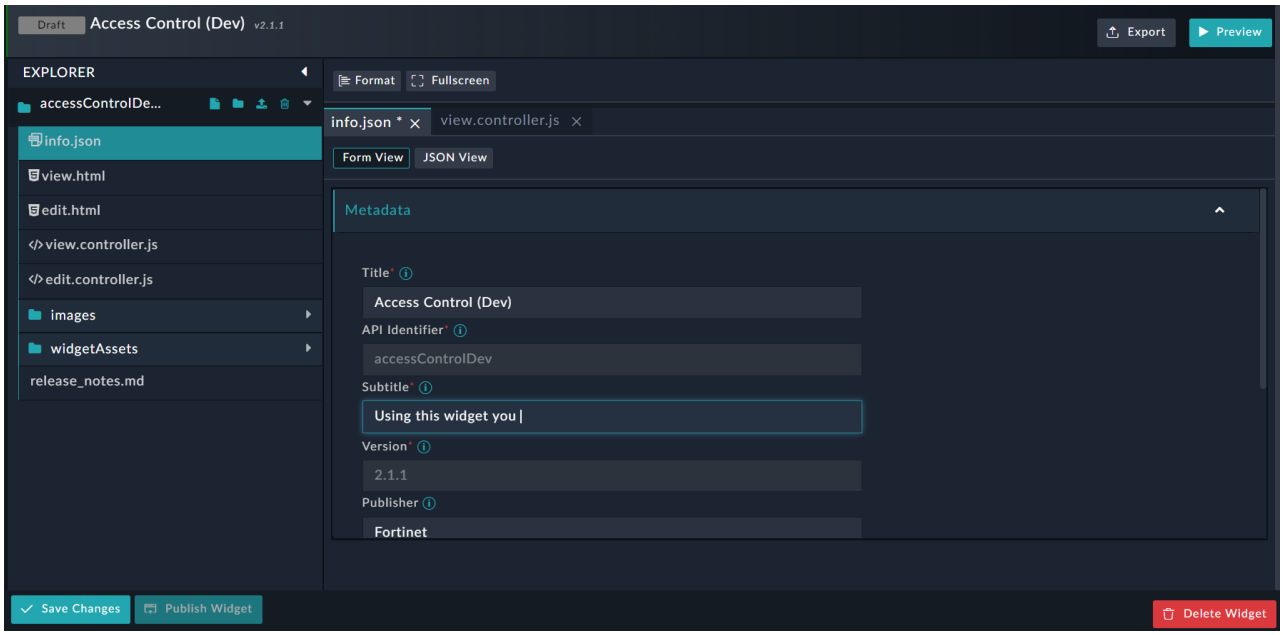


The directory structure for widgets is explained in the Directory structure and contents for widgets section.

b. When you click **Add Version** a `Clone Widget` dialog appears in which you can enter details such as the title and version of the widget that you want to edit, etc., and then click **Create**. The widget with the specified version gets saved in the **Create** tab.



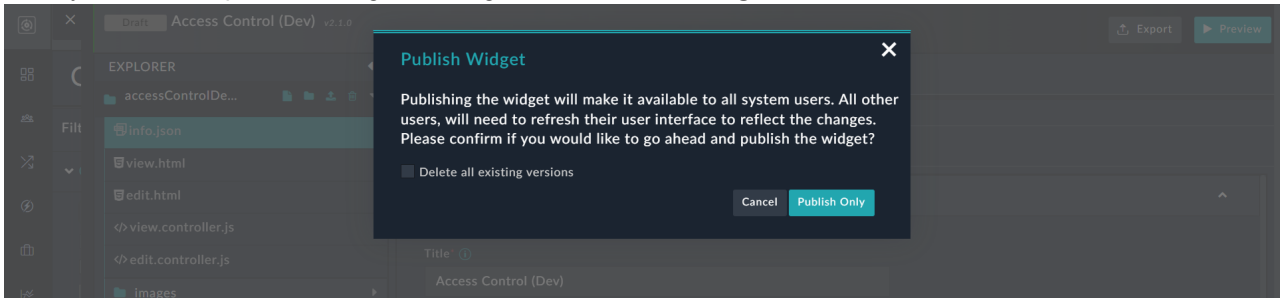
3. Edit the existing widget as required.
Note: You cannot change the 'Title', 'API identifier', and 'Version' of a widget once it is set.
From version 7.0.2 onwards, you can click the **Form View** button to edit the `info.json` file in a **Form** view, instead of editing the file in the raw JSON format:



Once you have completed making the changes click **Save Changes**.
You can also perform the following operations on the code editor interface:

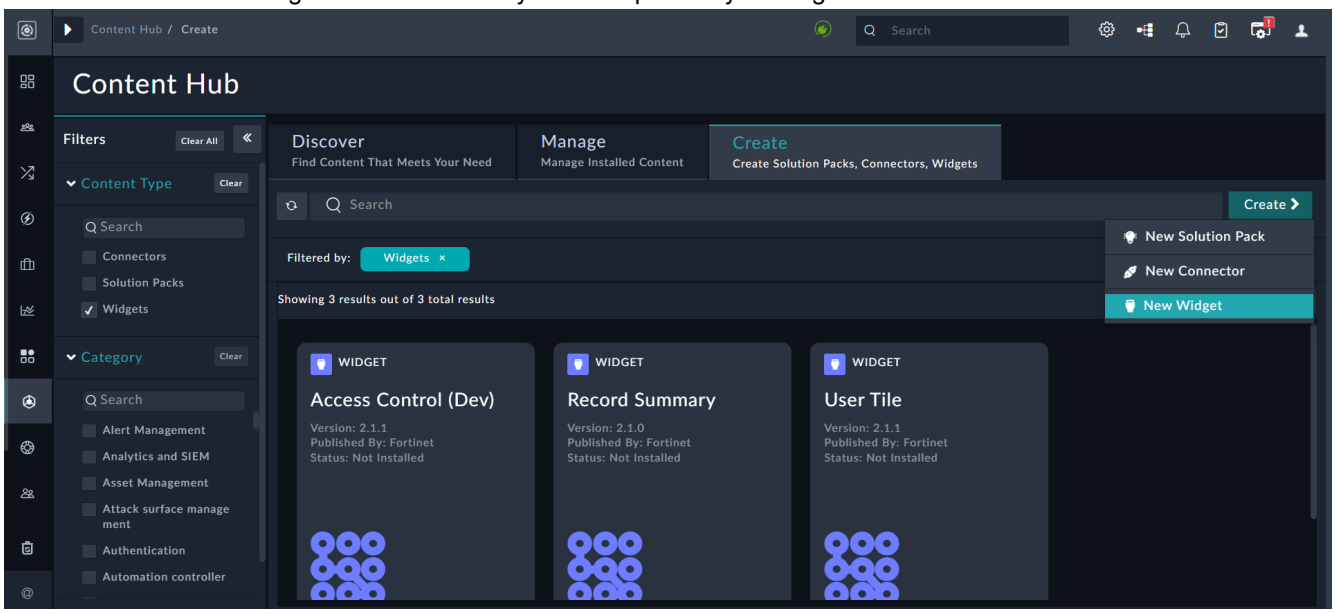
- **Code Formatting**: To lint your code automatically and make the code more human-readable and error-free (programming and programming errors), select the entire code in the editor and click the **Format** button.
- **Full Screen**: To get a better working view and make the editor go full-screen, click the **Fullscreen** button. To exit the full screen, press `ESC`.
- **Export**: To export the widget as a `.tgz` file, click the **Export** button. You might want to import the exported widget's `.tgz` file into another system.
- **Preview**: To preview the widget development progress, at any time during the development, so that it becomes easier to make changes, click the **Preview** button.
- **Delete Widget** or **Uninstall Widget**: To delete a widget that is not installed or uninstall a widget that is installed. Clicking **Delete Widget** or **Uninstall Widget** displays a `Confirmation` dialog, and you can click **Confirm** to delete or uninstall the widget.

4. Once you have completed making the changes, click **Publish Widget**.



Click **Publish Only** to publish the widget and make it available on the **Discover** tab for all the users of the system and enables usage of this widget on the pages as specified in the widget configuration. However, a working copy for the same is also maintained in the **Create** tab.
To delete all existing versions of the widget from your system, select the **Delete all existing versions** checkbox.
After you have published the widget, you will also see a **Revert To Last Publish** button on the code editor interface. Clicking **Revert To Last Publish** clears any changes made to the widget code since the last `Publish` event.

You can also view the widgets that are currently in development by clicking **Content Hub** > **Create**:



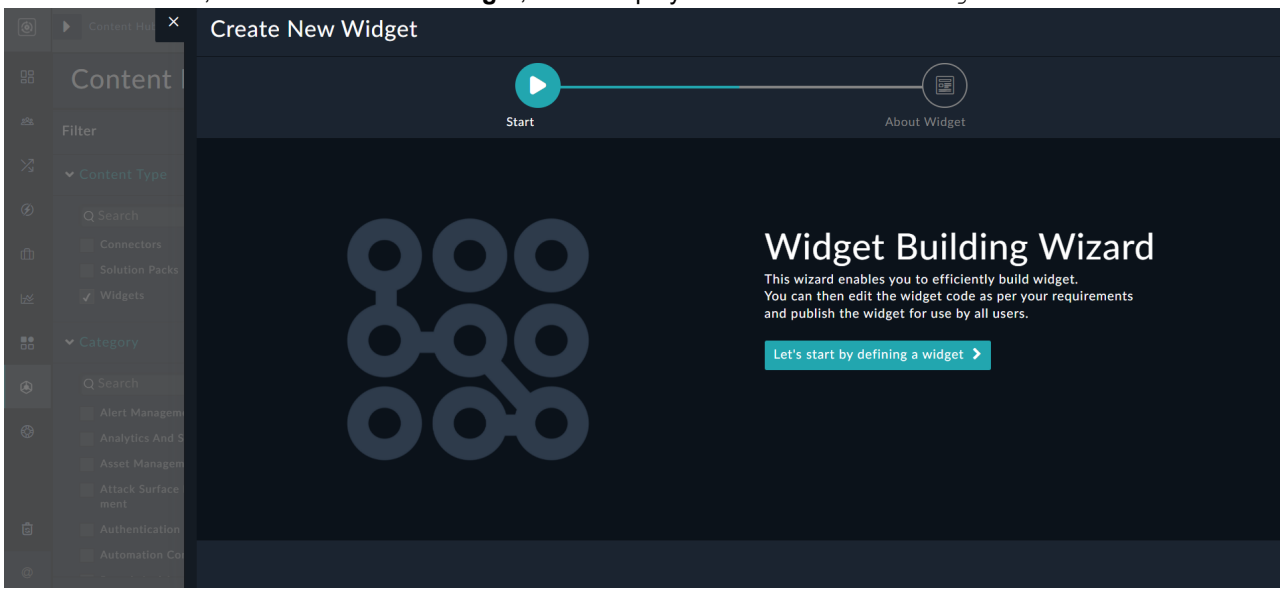
To edit a widget, click **Edit** on that widget's card, which opens the code editor interface. To add a new version for a widget click **Add Version**, which displays the `Clone Widget` dialog. To delete a widget, click the **Delete** icon.

Creating Widgets

Use the Widget Building Wizard to efficiently create new widgets.

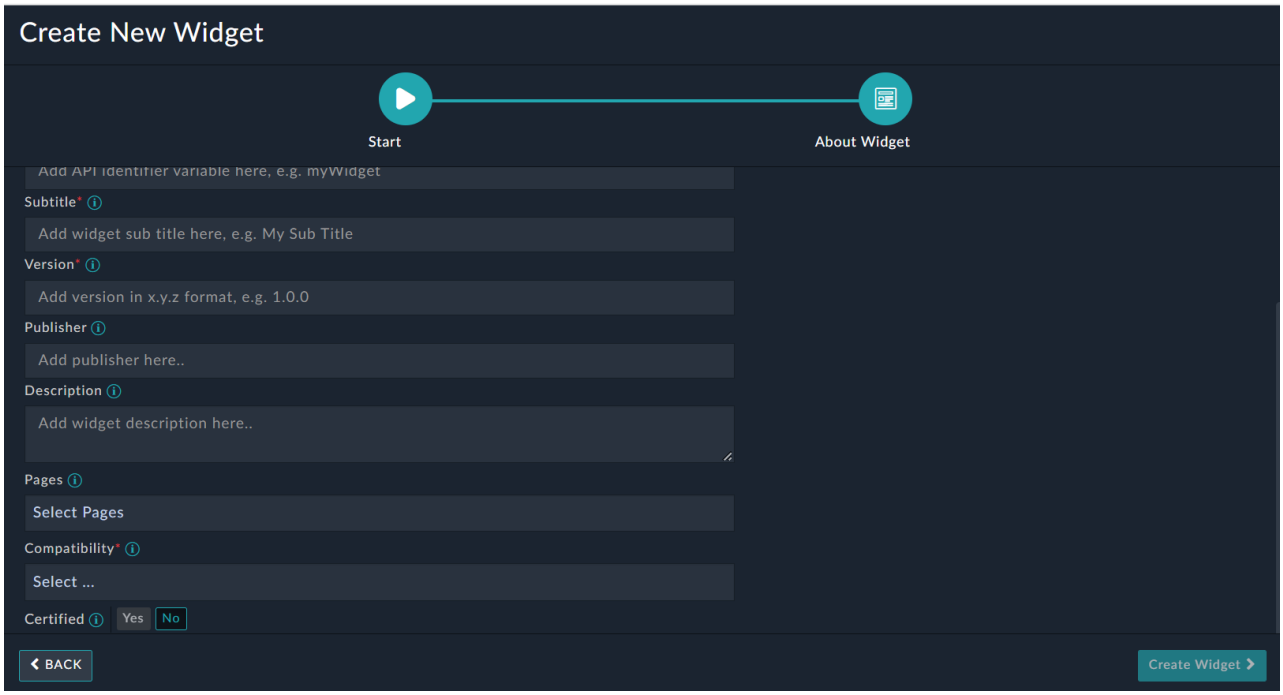
To create a new widget, do the following:

1. On the FortiSOAR left-navigation, click **Content Hub** > **Create** or **Widget** Library > **Create**.
2. On the **Create** tab, click **Create** > **New Widget**, which displays the `Create New Widget` Wizard.



Prior to version 7.0.2, the code editor interface with the contents of the default "Hello World v1.0.0" widget would be displayed.

3. Click **Let's start by defining a widget** and to open the **About Widget** screen where you can provide the metadata of the widget such as the title, version, etc., and then click **Create Widget**.



Details that you can provide are:

   a. In the **Title** field, enter the title of your widget.
   b. In the **API Identifier** field, enter a name that would be used as a variable in the widget code to reference this widget. The variable that you use here can be alphanumeric; however, it should not contain any special characters and it must not start with a number.
      Also, note that the value that you enter in this field must not match the name of any other widget that is available in the Content Hub. For example, you cannot enter `mobilesettingdev` in this field, since the Mobile Settings widget is available in the Content Hub.
   c. In the **Subtitle** field, enter the subtitle of your widget.
   d. In the **Version** field, enter the version of the widget in the x.y.z format. For example, `1.0.0`.
   e. (Optional) In the **Publisher** field, enter the name of your organization as the publisher of this widget. The publisher of the widget is responsible for maintaining and supporting the widget.
      If you want to keep the widget anonymous, then you can add the "Community" keyword. If this field is left blank, again the widget's publisher is automatically set to "Community".
      Note: Do not enter "Fortinet" in this field.
   f. (Optional) In the **Description** field, enter information for the widget that you are creating. The Description is displayed on the Widget card on the Widget Library listing pages and enables users to understand more about the Widget.
   g. (Optional) From the **Pages** list, select the pages in FortiSOAR such as Dashboard, Listing, Add Form, etc., on which you want to display this widget.
   h. (Optional) In the **Compatibility** field, enter the FortiSOAR version, in the x.y.z format, with which this widget is compatible.
   i. Toggle **Certified** to **Yes** or **No**, depending on whether you want to publish the widget as certified or uncertified.

4. Once you click **Create Widget**, the widgets open in the code editor interface and you can edit the widget as per your requirements. For details of the directory structure of the code editor interface, see the Directory structure and

contents for widgets. Details on editing widgets are present in the Editing an existing widget section.
Once you have completed editing the widget, click **Save Changes**.

5. Once you have completed making the changes, click **Publish Widget**.
Click **Publish Only** to publish the widget and make it available on the **Discover** tab for all the users of the system and enables usage of this widget on the pages as specified in the widget configuration. However, a working copy for the same is also maintained in the **Create** tab.

Directory structure and contents for widgets

widgetname folder

```
--+ editController.js
--+ edit.html
--+ images
---+ imagefiles
--+ info.json
--+ viewController.js
--+ view.html
--+ Widget Assets
---+ css
---+ html
---+ js
```

Controller and view files

The controller and view files are used to define and stylize the widget. The `view.html` and `viewController.js` define the output of the widget, i.e., how the widget will be displayed on the specified FortiSOAR pages. The `edit.html` and `editController.js` define the settings of the widget.

You can also include CDNs (Content Delivery Networks) in `edit.html` and `view.html` by using standard link syntax

Images

The images folder contains any image that is associated with the widget. For example, sample screenshots of how the widget will be displayed on FortiSOAR pages.

info.json

The `info.json` file contains information about the name, title, subtitle that represents a brief description of the widget and the version of the widget. In its `metadata` section, it contains a comma-separated list of FortiSOAR pages, such as dashboards, view panels, etc., in which you can add and display the widget. For example:

```
"pages": [
   "Dashboard",
   "View Panel"
  ]
```

It also contains the following information for the widget:

- The `certified` parameter contains information on whether the widget has been certified by FortiSOAR.
- The `snapshots` parameter contains the path of the screenshots that are part of the widget.

- The `description` parameter contains the feature list of the widget.
- The `help_online` parameter contains the link to the widget documentation added to the `help_online` parameter.
- The `compatibility` parameter contains a comma-separated list of FortiSOAR versions with which the widget is compatible.

Widget Assets

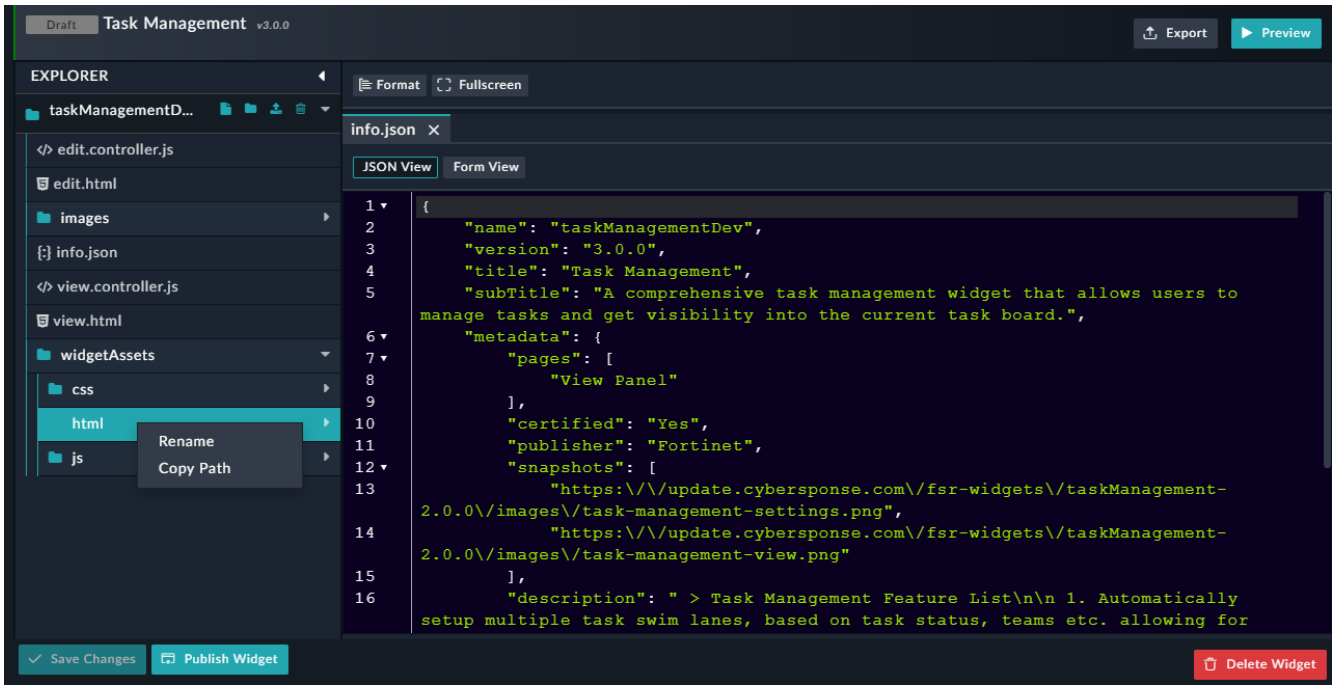
Use the "Widget Assets" folder to create or import external assets that can be leveraged to build widgets, which enables you to create complex widgets and expands the capabilities of the "Widget Library." You can also create your own library and from version 7.0.2 onwards, you can create new files or folders in the *root* folder itself. To use an uploaded or created JS library, right-click the respective file, select the **Copy Path** item, and then include the path in the "src" of the `script` tag in `edit.html` or `view.html` according to your requirement.

The Widget Assets folder, by default, contains the css, html, and js subfolders. You can create or import files such as external JS files (external libraries), image files, etc. directly to any folder or sub-folder.

Actions that can be performed in the code editor interface

You can perform various actions such as creating or importing files or folders in the code editor.

- **Create File** - Creates a file in the root (*widgetname*) folder or in the folder you have selected. For example, if you have selected the Widgets Assets folder then this action creates the file in the selected folder. All the actions work in a similar way.
- **Create Folder** - Creates a folder in the root folder or in the folder you have selected.
- **Upload File** - Imports a file to the root folder or in the folder you have selected.
- **Delete File or Folder** - Deletes the selected file or folder. If you have selected a folder, and you click the **Delete** button, then this action will delete all files within the selected folder.
  Important: The root folder and the info.json, view.html, edit.html, view.controller.js, and edit.controller.js files cannot be deleted.
- **Rename or Copy the Path of a File or folder** - Right-click a file or folder to rename the file or folder or copy its path.



Once you have created or imported the required files you can use them in the widget. You can also edit the imported files in the code editor interface and can perform all the operations such as formatting the code, previewing the code, etc. as described in the Editing an existing widget section.

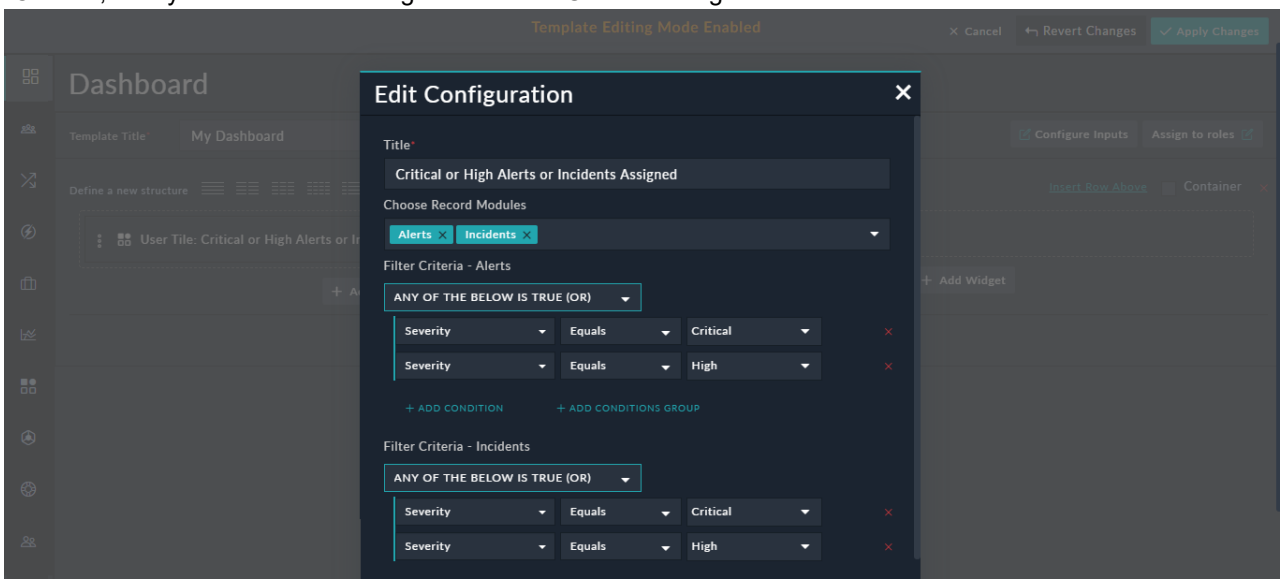
Using a widget in FortiSOAR pages

To use a FortiSOAR OOB widget or to use a custom widget that you have created, click the FortiSOAR page in which you want to add the widget. Then in the edit view of that page, add and configure the widget.

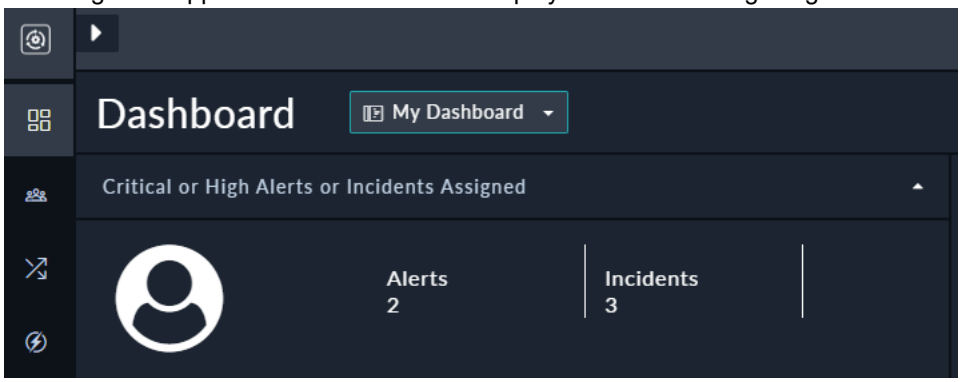
Let us take the example of the "User Tile" widget, which is used to view the logged-in user's assigned records across multiple modules along with the user's avatar. It also supports the filtering of records. If you want to add this widget to your dashboard, then do the following:

1. Click **Dashboard** and to edit an existing dashboard, click the **Actions** icon ( ), and then click **Edit Dashboard**.
2. Click **Add Widget** and from the `Widget Library` section, click **User Tile**.
3. Edit the configuration of the widget as per the settings defined in the widget configuration. Details on editing widgets are present in the Editing an existing widget section.
   In the case of the "User Tile" widget, you need to provide the widget with a title, then choose the modules for whose records you want to view and you can also define filter criteria for filtering records of the selected module. For example, if you want to display Alerts and Incidents that are assigned to you, whose severity is set to "High" or

"Critical", then you can edit the configuration of the User Tile widget as follows:



4. Click **Save** and **Apply Changes**.
The widget will appear in the dashboard as displayed in the following image:



Important: To view the custom widgets that are part of FortiSOAR pages such as `Dashboards` and `Reports` you must be assigned a role that has a minimum of `Usage` access on the `Widgets` module.

Modules

Modules provide access to individual data models within the FortiSOAR database, such as `Incidents`.

Default Modules

You will see the following default modules in case of a fresh install of FortiSOAR and if you have installed the SOAR Framework Solution Pack.

From release 7.2.0 onwards, the SOAR Framework Solution Pack is installed by default with the fresh installations of FortiSOAR

The SOAR Framework SP is the **Foundational** Solution Pack that creates the framework, including modules, dashboard, roles, widgets, etc., required for effective day-to-day operations of any SOC. As the Incident Response modules, i.e., Alerts, Incidents, Indicators, and War Rooms are not part of the FortiSOAR platform, it becomes essential for users to install the SOAR Framework SP to optimally use and experience FortiSOAR's incident response. For detailed information about the SOAR Framework SP, see the SOAR Framework SP documentation.

In FortiSOAR, the left navigation bar categorizes the modules as follows:

- **Dashboard**
- **Queue and Shift Management**
- **Incident Response**
  Alerts
  Incidents
  Tasks
  Indicators
  Campaigns
  Hunts
  War Rooms
- **Automation**
  Playbooks
  Connectors
  Data Ingestion
  Schedules
  SLA Templates
- **Resources**
  Attachments
  Email Templates
- **Reports**
- **Widget Library**
- **Content Hub**
- **Help**

Dashboard

Dashboards are generally the users' default home page. Administrators create dashboards that are applicable throughout the application and are assigned to users based on their roles. For more information, see the Dashboards, Templates, and Widgets chapter.

Queue and Shift Management enables you to automatically assign records to users within a queue using queues and shifts. For more information, see the Queue and Shift Management chapter.

Incident Response

The Incident Response Component is a collection of all modules typically related to Security Incidents. You might work on the entire Incident lifecycle from within this component.

This component underpins the operational side of your SOC. The standard flow starts within the `Alerts` module.

Alerts

Alerts in FortiSOAR are essentially notifications indicating that an attack has been directed at an organization's systems. Alerts are related to events and often contain essential information for addressing the attack by including vulnerabilities and exploits being leveraged by the potential attack.

Incidents

Incidents represent a collection of information discovered during an Incident Response investigation. Incidents are triggered based on the suspicion or confirmation of a security breach. Incidents can be related to cyber or physical security.

Tasks

Tasks represent a discrete action taken by either an individual or automated response. Tasks might link to outside systems, such as ticketing systems, to track specific actions beyond that of your SOC team.

Tasks might also be created to represent actions taken automatically as a part of a response policy enacted by a Workflow. This requires that the Workflow must have a step to insert a Task as a record of an action undertaken by an external system, such as adding an IP address to the denylist in the firewall ruleset.

Indicators

Indicators contain details of all the data that is collected from system log entries or files, which identify potentially malicious activity on a system or network. It contains records of identifiable information regarding a threat, such as an IP or URL.

Once an alert is created FortiSOAR extracts the metadata from the raw alert data and creates indicators, with details such as type of indicator, i.e. IP address, URL, attachment, domain, etc., the value of the indicator, such as the IP address number, the domain name, whether this indicator has been sighted any other alerts, and what is the IOC status of that indicator.

Campaigns

Campaigns represent a collection of Incidents that can be tied to a single Threat Actor. Seemingly disparate Incidents might be related attempts from a malicious attacker attempting to probe and gain access to your network.

It is generally difficult to determine if Incidents themselves are related and roll them into a Campaign. Typically, they would be linked by a known, single threat actor based upon some uniquely identifiable piece of information that ties the Actor across multiple Incidents. Note that Campaigns are not part of default modules.

Hunts

Hunts is a module where you can store and organize your hunts. The hunt you create becomes a central repository where you can link all Alerts, Assets, Users, and other modules' records associated with your hunting activity.

War Rooms

War Rooms in FortiSOAR is a collaborative space that enables SOC teams to mitigate a critical cyber threat scenario or campaign. FortiSOAR makes it easy for analysts to quickly and easily provision a War Room that allows participation of all stakeholders to analyze and collaborate to quickly mitigate the threat and restore the services. For more information, see the War Rooms chapter.

Automation

The Automation Component is a collection of modules that you can use to automate your security operations.

Playbooks

Playbooks in FortiSOAR allows you to automate your security processes across external systems while respecting the business process required for your organization to function. For more information, see the *Playbooks Guide*.

Connectors

Connectors provide you with the ability to retrieve data from custom sources and perform automated operations. FortiSOAR has already developed a number of connectors and also provides you with a Connector Building wizard using which you can develop custom connectors that can retrieve data from custom sources. For more information, see *Connectors Guide*.

Data Ingestion

Data Ingestion enables you to use the FortiSOAR Data Ingestion Wizard to ingest data from external SIEM solutions and other third-party sources like threat intelligence platforms, email solutions, etc. The wizard also takes care of the scheduling of data ingestion into FortiSOAR, if the connector is enabled for scheduling. For more information, see *Connectors Guide*.

Schedules

Schedules in FortiSOAR allow you to schedule playbooks to run at regular intervals. For more information, see the Schedules chapter.

Schedules as a module is removed, i.e., you will not find schedules on the `Modules` page and you cannot modify the mmd of the schedules using the Application Editor.

SLA Templates

SLA Templates in FortiSOAR can be used to create an in-built SLA management for incidents and alerts. For more information, see the *SLA Management* chapter in the "Administration Guide."

Resources

The Resources Component is a collection of all modules typically related to components stored in FortiSOAR such as attachments and templates.

Attachments

Attachments represent files that are uploaded and stored in FortiSOAR. You submit files that are available in the FortiSOAR `Attachments` module to 3rd-party tools to scan and analyze suspicious files and retrieve reports for the submitted samples.

You can add a file up to the maximum file size of **100 MB** in the Attachments module.

Email Templates

Email Templates represent templates that are stored in FortiSOAR that you can use when you want to send emails from FortiSOAR. For example, if you have created a rule that requires FortiSOAR to send an email automatically if a particular condition is met, then you must create a template for the email and save that email in the Email Templates module.

Email Templates contain a set of standard templates included with FortiSOAR. Standard templates include emails that are sent by FortiSOAR when a new user is added in FortiSOAR or an email that is sent to users when they forget their passwords and send a request to reset the FortiSOAR password.

Reports

Reports represent FortiSOAR Reports that you should use for your reporting purposes. You can easily create rich reports and dashboards in FortiSOAR. You can also schedule reports, view historical reports and also search for text in

the report PDF, which is in the text PDF format. For more information, see the Reports chapter.

Widget Library

Widgets allow users to edit out-of-the-box (OOB) widgets and build new widgets for custom use cases. Users can use the widget library to customize existing widgets or build new widgets as per their requirements. For more information, see the Widgets Library chapter.

Content Hub

Content-Hub contains out-of-the-box reference material and product add-ons like solution packs, connectors, widgets, etc.

Solution Packs are the implementation of best practices to configure and optimally use FortiSOAR enabling users to get started easily and effectively. The solution packs contain a lot of sample/simulation/training data that enables you to experience FortiSOAR without having all the devices.
Connectors provide you with the ability to retrieve data from custom sources and perform automated operations. For more information, see *Connectors Guide*.

Widgets allow users to edit out-of-the-box (OOB) widgets and build new widgets for custom use cases. For more information, see the Widgets Library chapter.

Help

The **Help** component contains the Knowledge Base, which is the FortiSOAR Product documentation, along with small tutorials and examples, to help you work effectively with FortiSOAR.

Additional Modules

In addition to the default modules, the installation of solution packs (SP) provides you with corresponding modules. For example, if you install the Vulnerability Management SP, the Vulnerability Management modules get installed or if you install the SOC Simulator SP, the Scenarios/Simulations module gets installed. Detailed documentation comes bundled with each solution pack.

Vulnerability Management

Vulnerability Management is a collection of all modules typically related to vulnerabilities that exist in your system.

Vulnerabilities

Vulnerabilities represent a collection of weaknesses in your systems that can lead to security concerns. You can configure vulnerability scans to run periodically on your network, creating an inventory of the vulnerabilities for your specific assets.

Assets

Computers represent the Assets of your organization. Assets represent a unique piece of hardware and any information known about that hardware, such as MAC address, hostname, or IP address. Assets preferably have a unique identifier.

Assets typically are only stored within FortiSOAR as records related to Incidents, Alerts, or Vulnerabilities. Asset information may be pulled from a CMDB or other resource available with knowledge of the asset characteristics, such as an ARP table or DHCP records.

In the case of large networks, Asset tracking is often a complicated process and plagued with limitations. We recommend that Asset creation involve corroboration between multiple unique sources of data that build a level of confidence in the accuracy of the Asset information, as single sources can be unreliable with respect to data integrity and accuracy.

Scans

Scans contain the details of all the scans that you run on your systems. It contains records of a bulk scan from scanners.

Scenarios

The Scenarios module allows you to run various Simulations. It contains simulation data and utilities that demonstrate FortiSOAR capabilities around several important SOC use-cases without the need to integrate with actual device endpoints.

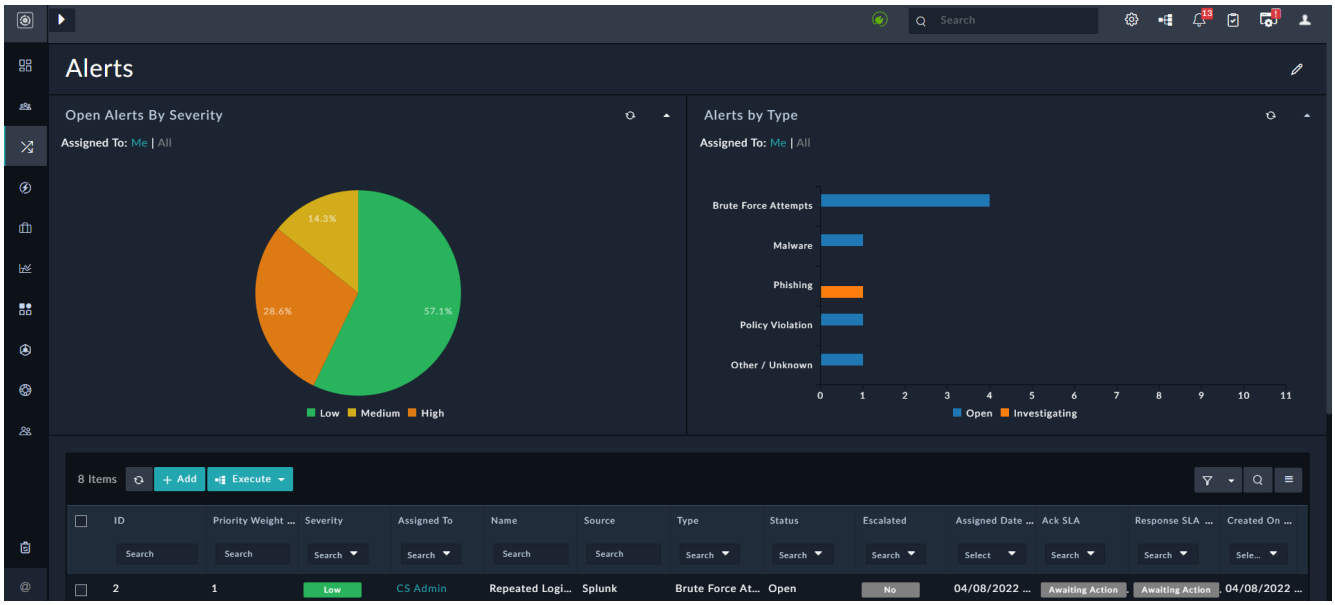
Working with Modules - Alerts & Incidents

Alerts

Alerts in FortiSOAR are essentially notifications indicating that an attack has been directed at an organization's systems. Alerts are related to events and often contain essential information for addressing the attack by including vulnerabilities and exploits being leveraged by the potential attack.

Alerts Dashboard

The *Alerts Dashboard* is a collection of graphs and charts showing visual representations of specific incident activity in the module. An example of the collection of graphs and charts that the system can display by default can be *Open Alerts By Severity* and *Alerts By Type* as shown in the following image:



You can customize the graph and chart display to meet your individual team or organization's needs. For more information on `Dashboards`, see the Dashboard, Template, and Widgets chapter.

Incidents

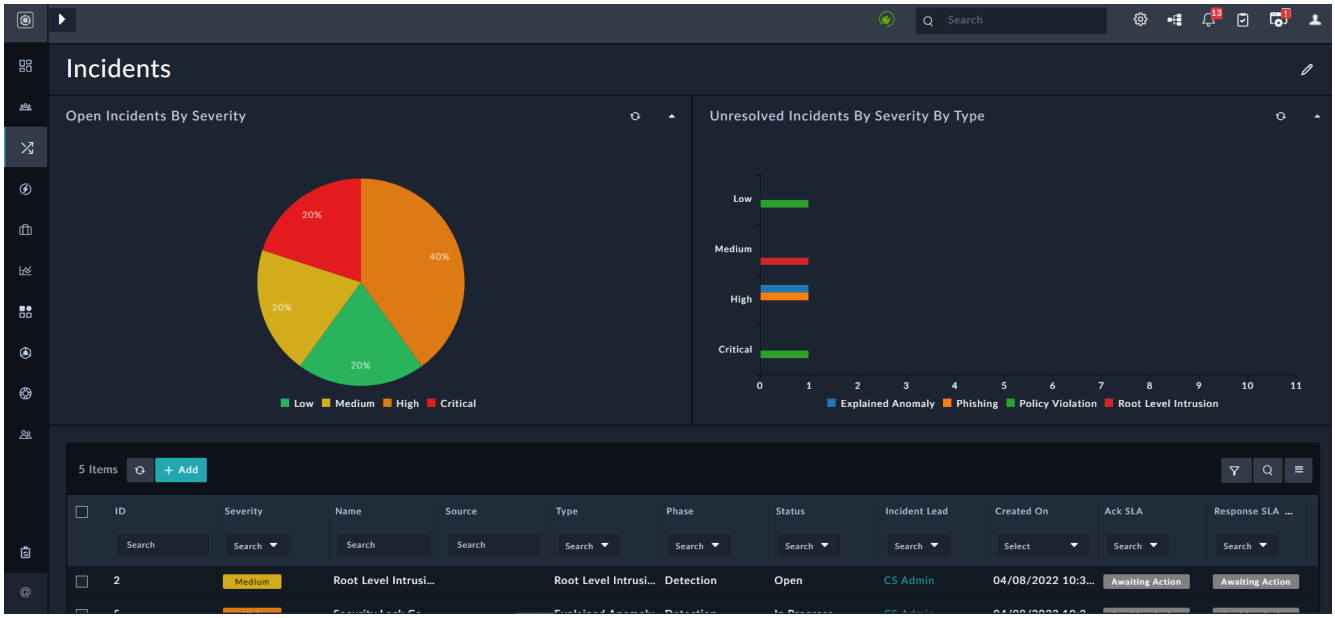
Incidents represent a collection of information discovered during an Incident Response investigation. Incidents are triggered based on the suspicion or confirmation of a security breach. Incidents may be cyber or physical security related.

Incidents in FortiSOAR document vital information related to cybersecurity violations and attacks that threaten the integrity of your systems and/or data. Critical information such as origin points, severity, and source allow SOC users to

assess the scope and reliability of breach while tracking various data such as containment and recovery times help teams identify efficiency trends and gaps in efficiency.

Incidents Dashboard

The Incidents Dashboard is a collection of graphs and charts showing visual representations of specific incident activity in the module. An example of the collection of graphs and charts that the system can display by default can be *Open Incidents By Severity* and *Unresolved Incidents By Severity By Type* as shown in the following image:



You can customize the graph and chart display to meet your individual team or organization's needs. For more information on `Dashboards`, see the Dashboard, Template, and Widgets chapter.

Working with Alerts and Incidents

In FortiSOAR, modules have a `List View` and a `Detail View` as described in the following sections. Modules that are used for automation, such as `Playbooks` and `Schedules` have been described in the other chapters in this guide.

In this chapter, we have taken the example of the 'Alerts' Module and described how you could work with alerts. You can work the same way with other modules such as 'Incidents.'

Alerts List View

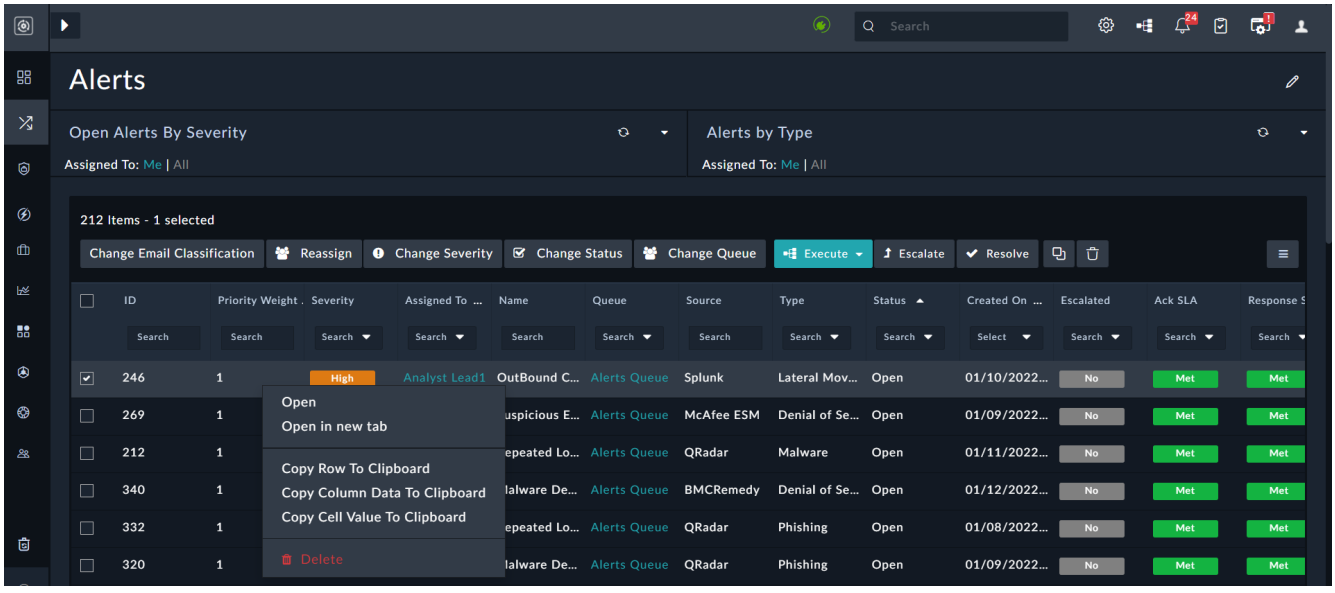
The Alerts List View shows the user all the existing alerts the current user's teams own and high-level detail about each alert.

To add an alert in FortiSOAR, click **Add Alert** in the top bar of the `Alerts` Module to open the `Create New Alert` form. Fill in the required details the `Create New Alert` form and click **Save** to create an alert. If your administrator has configured default values for any fields, then that default value will be displayed in the `Create New Alert` form. For example, if your administrator has set the default value of the **Status** field as **Open**, then when you create a new alert, by default, the **Status** field is already set as **Open**.

The Alerts List View displays records that are sorted by modified date/time with the most recently created/edited alert first. You can change the sort order by clicking on the column headers and specifying the sort criterion. For example, you can sort the `Created On` column to display either the oldest or the most recent created alerts first. Your administrator can also specify fields based on which the records in the module will be sorted by default. For more information on `Default Sort`, see the Dashboards, Templates, and Widgets chapter.

From release 7.2.0 onwards, `DateTime` fields, such as 'Created On', 'Modified On', etc are stored with milliseconds precision (earlier it was seconds). Advantages of having a more precise time include the ability to accurately sequence comments that have been simultaneously written, correctly paginate records when records are created or updated at a very high frequency, etc.
If you have upgraded to 7.2.0, and users add new values to any existing `DateTime` fields, then those are stored with milliseconds precision; however, values in the `DateTime` fields that were present before the upgrade would yet be present in the old format, i.e., stored with the seconds precision.

You can right-click an alert in the grid view to display the new context menu options that have been added that enable you to copy record details to the clipboard. **Copy Row To Clipboard**, **Copy Column Data To Clipboard** and **Copy Cell Value To Clipboard** are the context menu options that you can use to copy data for a single row, single column, and single cell respectively. These options do not copy a blank row, a blank column, or a blank cell.



The **Copy Row To Clipboard** option copies the data only for the *visible columns* of the selected row to the clipboard in the JSON format. JSON format makes it very easy for you to understand the field name and its value. If you want to copy data other than those of the visible columns, then you must make those columns visible by adding them to the grid in the UI. Use the **More Options** icon ( ) to the right of the table header to hide and unhide columns. Visible columns appear with a green tick icon and hidden columns appear with a red cross icon.

The **Copy Column Data To Clipboard** option copies the data of the selected column to the clipboard in the newline-separated format.

The **Copy Cell Value Clipboard** option copies the data of the selected cell to the clipboard.

You can add tags while creating records, enabling you to search for records in FortiSOAR using tags, making tags very useful in searching and filtering records. You can create tags that have a minimum of three characters. You can add special characters and spaces in tags from version 6.4.0 onwards. However, the following special characters are not supported in tags: `'`, `,` , `"`, `#`, `?`, and `/`. The **Tag** field gets auto populated based on tags that are already created. Tags are case insensitive; however, if you create two tags with different case, for example, BFA and bfa, FortiSOAR will display results containing both "BFA" and "bfa".

Administrators can also configure grid and relationships templates so that horizontal scrolling in grid views gets enabled, which provides better usability to users in scenarios where the data grids that have a large number of columns. For more information on how to configure templates, see the Dashboards, Templates, and Widgets chapter.

To edit the template for any module, including `Alerts`, click the **Edit Template** icon that is present in the upper right-hand corner. For more information on `Templates`, see Dashboards, Templates, and Widgets chapter.

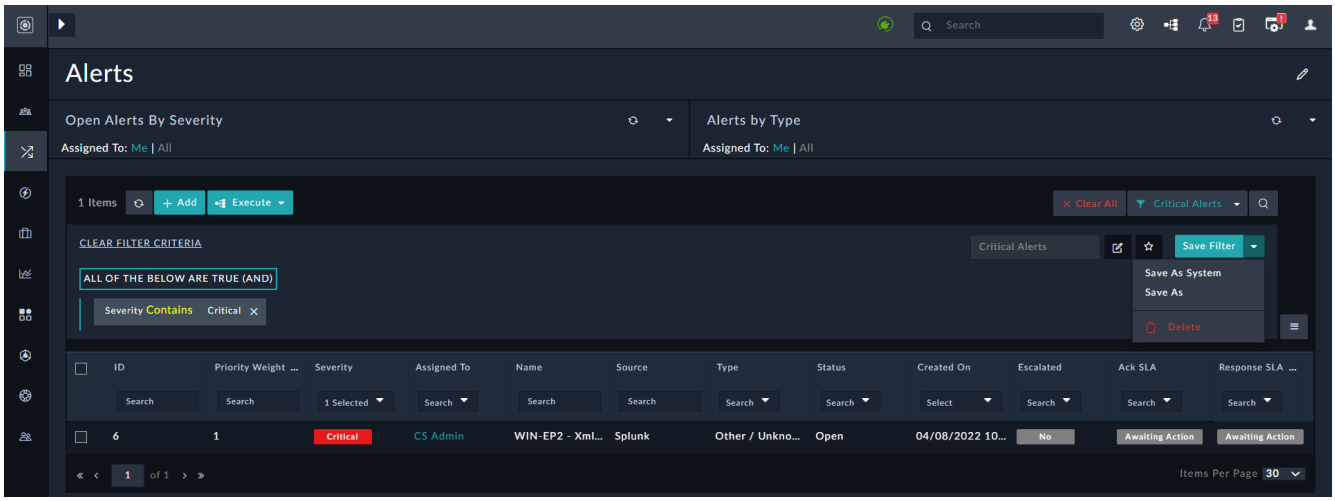
Searching and Filtering Alerts

Users can search for a specific alerts within the list (grid) view using the following:

- **List View Search** - enter text in the search field and click on the search icon to search every column in the list view for the data criteria.
- **Filter Search** - enter text in the search criteria row underneath the column header or select one or more options from the picklist under the column header. To search the grid whose lookup or pickup fields are not set or empty, you can select the **Not Set** option from the picklist under the column header. For example, to search for alerts whose 'Status' or 'Type' is not set.
  Note: You cannot search or filter encrypted fields.

You can also customize or select system filters by clicking the **Filter** icon next to the list view search field. Then either enter a filter criterion or select a filter from the drop-down menu from the search criteria row underneath the column header or select column filters to customize a view and click the **Save Filter** button. Clicking **Save Filter** opens a `Save New Filter` Dialog in which you must assign a name to the newly created filter.

For example, in the following image, a filter is being created for alerts whose `Severity` is **Critical**.



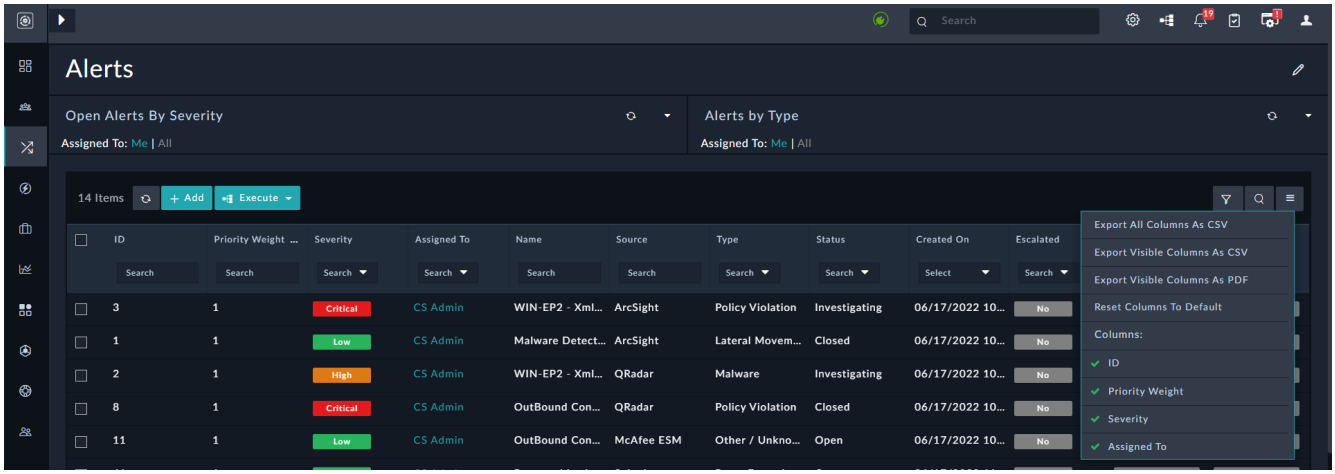
Click **Clear All** to remove the filter.

You can also define filters for records in the Grid Widget itself. The Grid Widget includes the Nested Filters component that you can use to filter records in the list view using a complex set of conditions, including the **OR** condition.

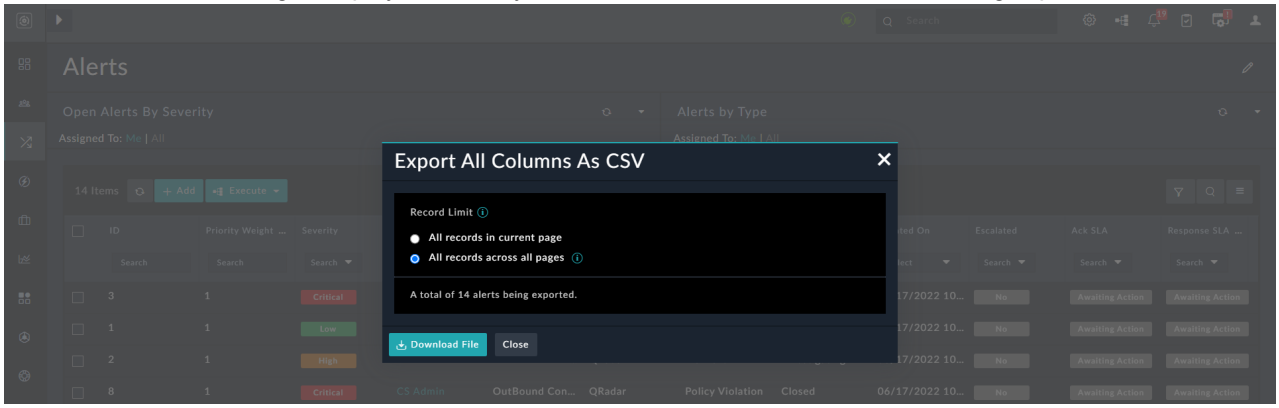
See the Searches and Filters and Dashboards, Templates, and Widgets chapters for more information on searching and filtering records.

Exporting Records from the List view

To export records using the grid view, click the **More Options** icon ( ) to the right of the table header:



- **Export All Columns as CSV**: Use this option to export data from all columns, i.e., data from both *visible* and *hidden* columns matching the currently set filter (if any) from the alerts grid get exported to a `.csv` file. Also, if you have applied any saved filters then they also get applied while exporting the records. List views of modules have a maximum shown record count of 250 records, which meant that earlier only 250 records could be exported using the other export options available on the **More Options** menu. When you select this option, the `Export All Columns As CSV` dialog is displayed, where you can choose to limit the record data being exported.



  Select the **All records in current page** to export data from the records on the current page, or select **All records across all pages**, to export all the record data.
  Important: If you select the **All records across all pages** option, you must have `Create` and `Read` permissions on the `Files` module and `Execute` and `Read` permissions on the `Playbooks` module.
  Click **Download File** to download the CSV file containing the exported records.
- **Export Visible Columns as CSV**: Use this option to export visible columns of the alert record to a `.csv` file. The visible columns appear with a green tick icon.
  Note: You can hide columns by deselecting a column from the list of columns present within the **More Options** menu. The hidden columns appear with a red cross.

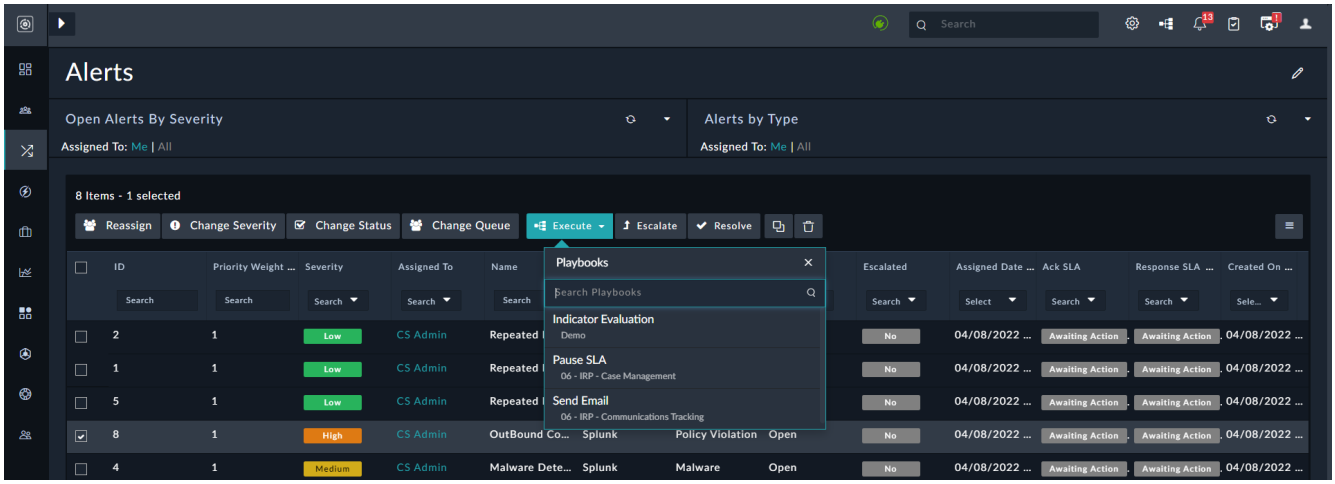
- **Export Visible Columns as PDF**: Use this option to export visible columns of the alert record to a `.pdf` file.
  Note: If you want to export records from the record's grid and view panel that contain unsupported character sets such as Korean or Chinese, then your administrators require to perform additional configurations. For more information, see the 'Configurations required for exporting of records with unsupported character sets in the PDF format' topic in the *Debugging, Troubleshooting, and optimizing FortiSOAR* chapter of the "Administration Guide."
- **Reset Columns To Default**: Use this option to reset the alert record fields to the default fields specified for the alert module.

The following additional options are visible if you select the row(s) in the grid:

- **Export Selected Rows as CSV**: Use this option to export selected rows in the alerts grid to a `.csv` file.
- **Export Selected Rows as PDF**: Use this option to export selected rows in the alerts grid to a `.pdf` file.

Editing a record in the List view

Select a record in the list view to delete, clone, perform bulk and automated actions, on that record as shown in the following image:



To reassign a record to another user(s), select the record(s) and click the **Reassign** button. Clicking the **Reassign** button displays the `Assigned To` list. Select the user to whom you want to reassign the record(s) and click **Reassign**.

To delete a record, select the record and then click the **Delete** button.

Deleting a record deletes the data and the relationships to the record, but not the entities to which the record is related.

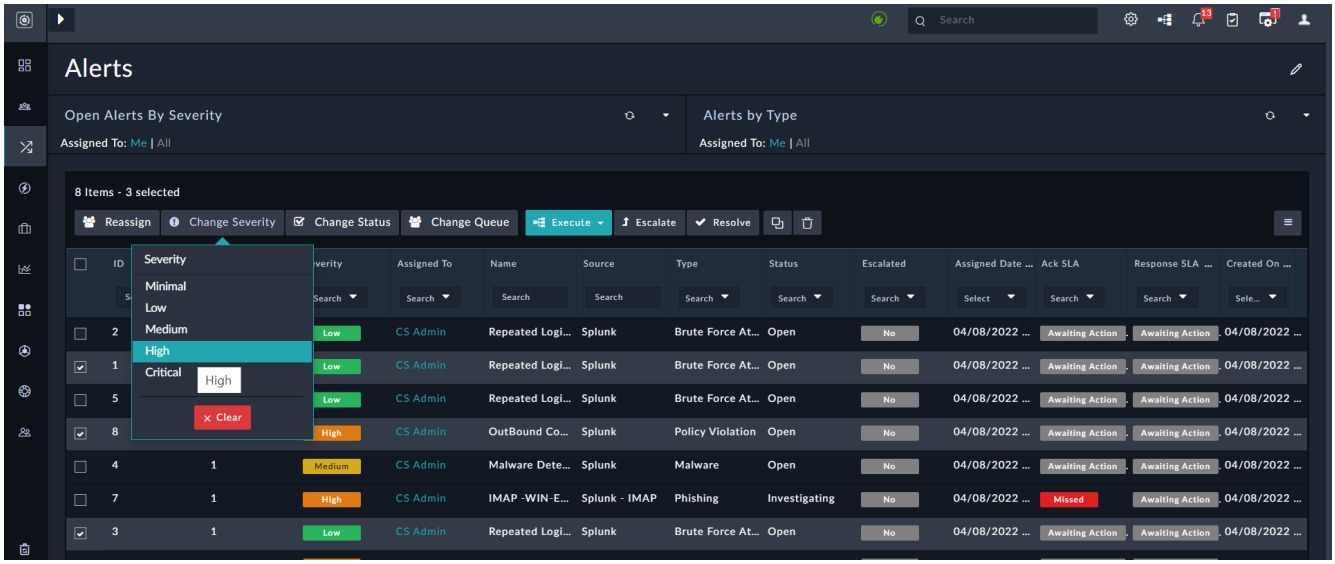
To clone a record, select the record and then click the **Clone** button, which opens a `Clone Records` dialog. In the `Clone Records` dialog choose whether you want to clone only the record, or also the related records for that record; if you want to clone the related records also, select the **Include Relationships** checkbox and click **Confirm**. Once you clone a record, you can edit it as per your requirements. FortiSOAR names the cloned record as `Copy of <content of the Name field>`. In case the record does not have the **Name** field in its MMD, then FortiSOAR picks up the value of the first field that is of text format. For example, in the case of the `Indicator` module, **Value** is the first field that is of text format. So, if you clone an indicator record, the cloned record will be named as `Copy of <content of the Value field>`.

You can clone only up to 100 records in a single selection. Select 100 records or less to perform the clone operation.

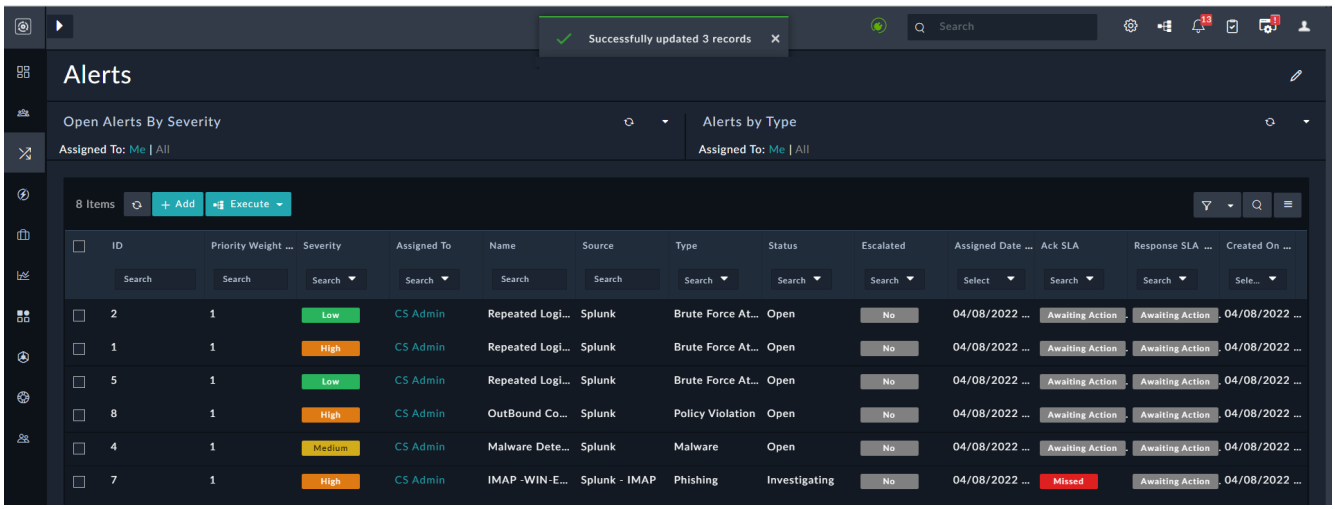
Executing default actions on records in bulk

If your administrator has configured bulk edit on a field in a particular module, then you can modify those records in bulk. The **Change Email Classification** (introduced in 7.2.0), **Reassign, Change Severity**, **Change Status**, **Change Queue** (introduced in 7.2.0), **Execute**, **Escalate**, and **Resolve** buttons are bulk operation buttons, which are included by default in FortiSOAR. For example, you can update the email classification of records to Phishing or Non Phishing, by selecting the records and clicking **Change Email Classification**, and then selecting **Phishing** or **Non Phishing**. Or, you can change the queue to which the records are assigned by selecting the records and clicking **Change Queue** and then selecting the queue to which you want to assign the records.
Your administrator can also configure the bulk edit operation on any other field, such as **Type**, in the `Alerts` module, then you can select multiple records and perform a bulk change on that field. Administrators can refer to the *Application Editor* chapter in the "Administration Guide" for the process of configuring `Bulk Edit`.

Example of the working of Change Severity: In case of Change Severity, you can select multiple records and change their `Severity` to the same particular severity level. Select multiple records and click the **Change Severity** button, which displays a `Severity` dialog box. The `Severity` dialog box contains the severity options configured, for example, Critical, High, Medium, etc. Select the severity level that you want to set for the multiple records, for example, select **High**.



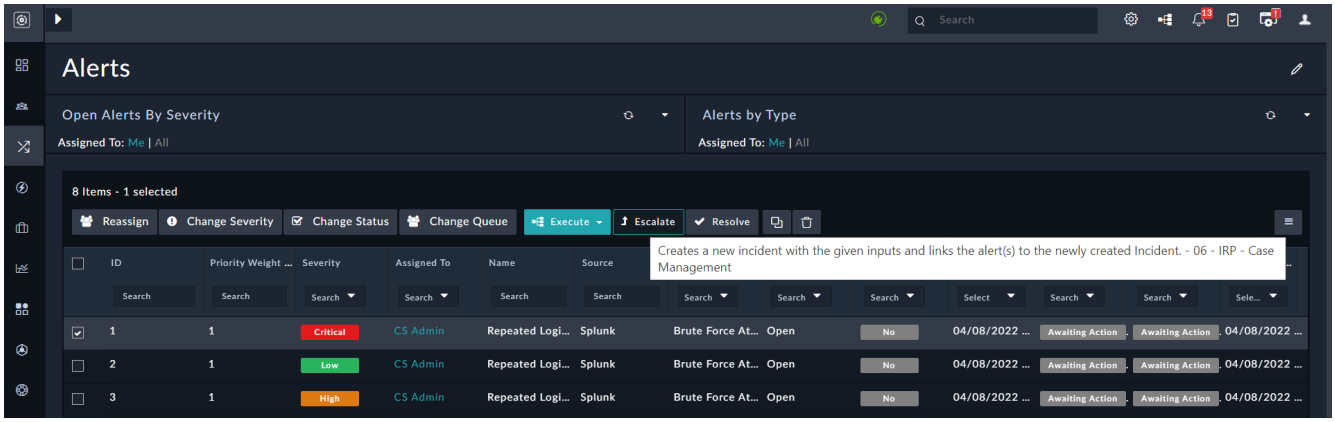
Once you click the severity that you want to set for the records, you will see a `Success` message, and see that the `Severity` level of the selected records has all been modified to **High**, as shown in the following image:



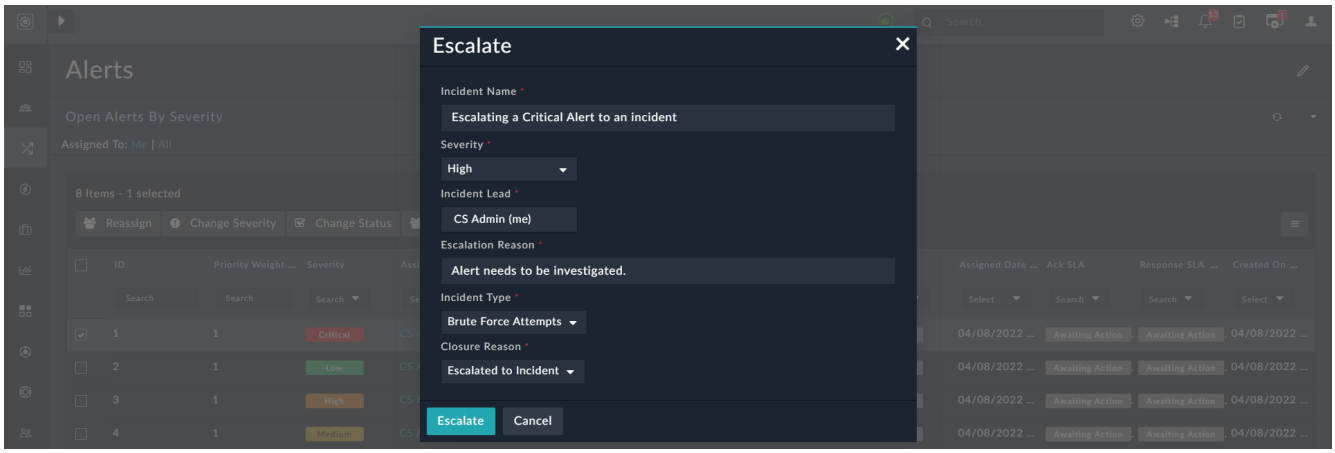
You can also change the status of multiple records to the same particular status level in the same way and also perform a bulk reassign to records to a particular person. You can also close multiple records in bulk by selecting multiple records and then clicking the **Resolve** button. Once you click the **Resolve** button FortiSOAR displays a `Resolve` dialog in which you are required to add the reason for closing the alerts in the **Closing Reason** field and click the **Execute** button. This reason that you add for closing the alert is included in the **Closure Notes** fields, and the status of the records is changed to **Closed**.

Example of escalating an alert to an incident: When your administrator is editing the template for a module, the administrator can create buttons for commonly used actions on that module. For more information on editing templates, see the Dashboard, Templates, and Widgets chapter. For example, the **Escalate** button for the Escalate manual trigger on the `Alerts` module, which escalates alerts to incidents is included by default in FortiSOAR.

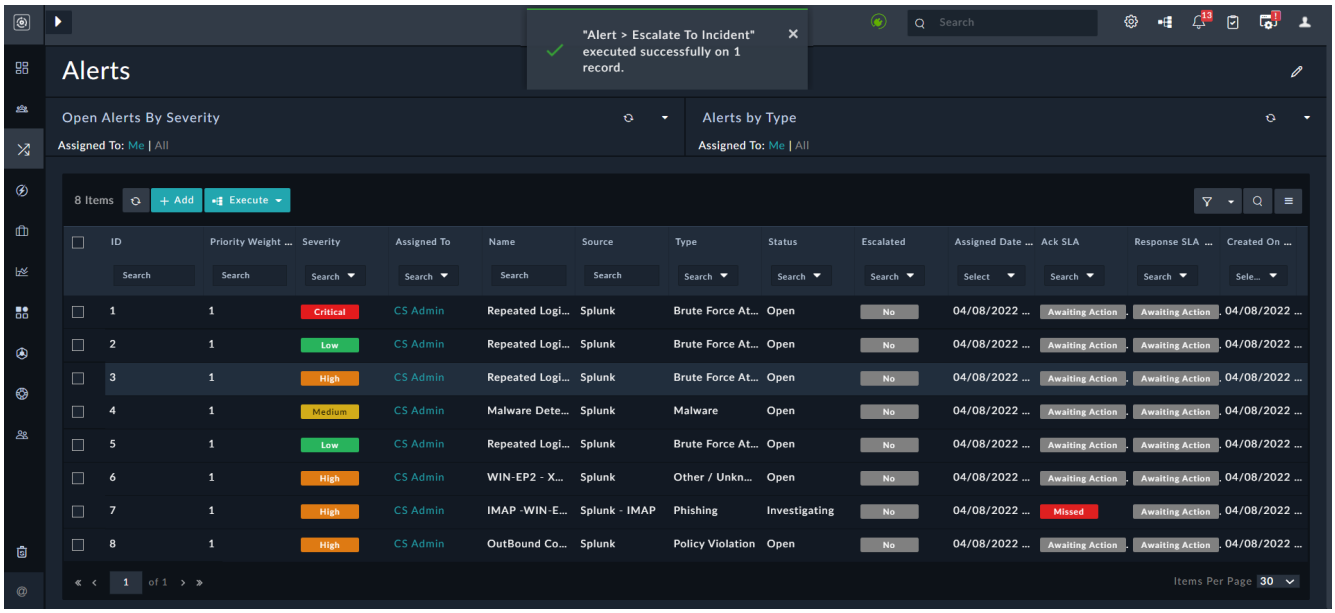
You can select an alert record or records in the grid view and click the **Escalate** button to create a new incident based on the provided inputs and link the alert to the newly created incident.



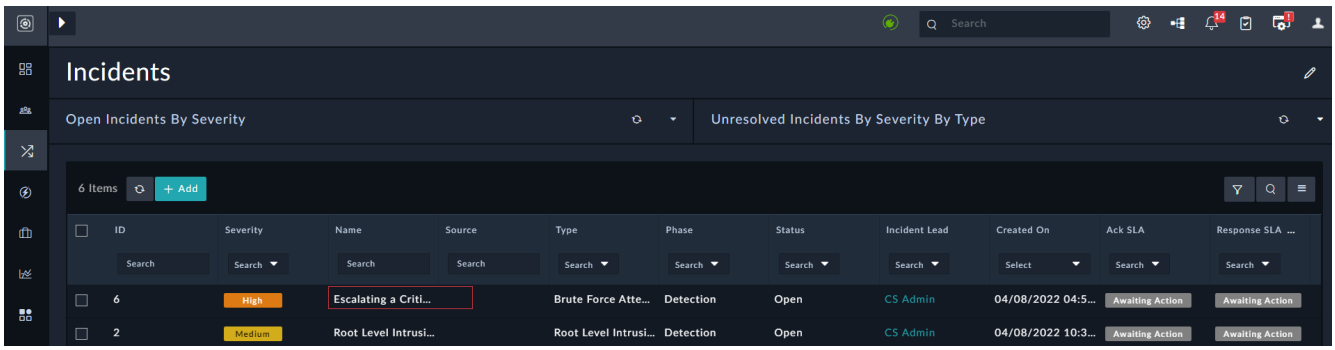
For example, if you want to escalate a `Critical` alert to an incident, you must select that record from the grid and then click the **Escalate** button. This triggers the Escalate playbook and based on the configuration of this playbook; you must specify the value of specific fields, such specifying the name and severity (default set to "Medium") of the incident that will be created by the playbook, the person to whom this incident will be assigned, and the reason for escalation (default set to "Alert needs to be investigated.").



Click **Escalate** to run the playbook and based on whether the playbook runs successfully or not, you will get an appropriate message, success in our example, as shown in the following image:

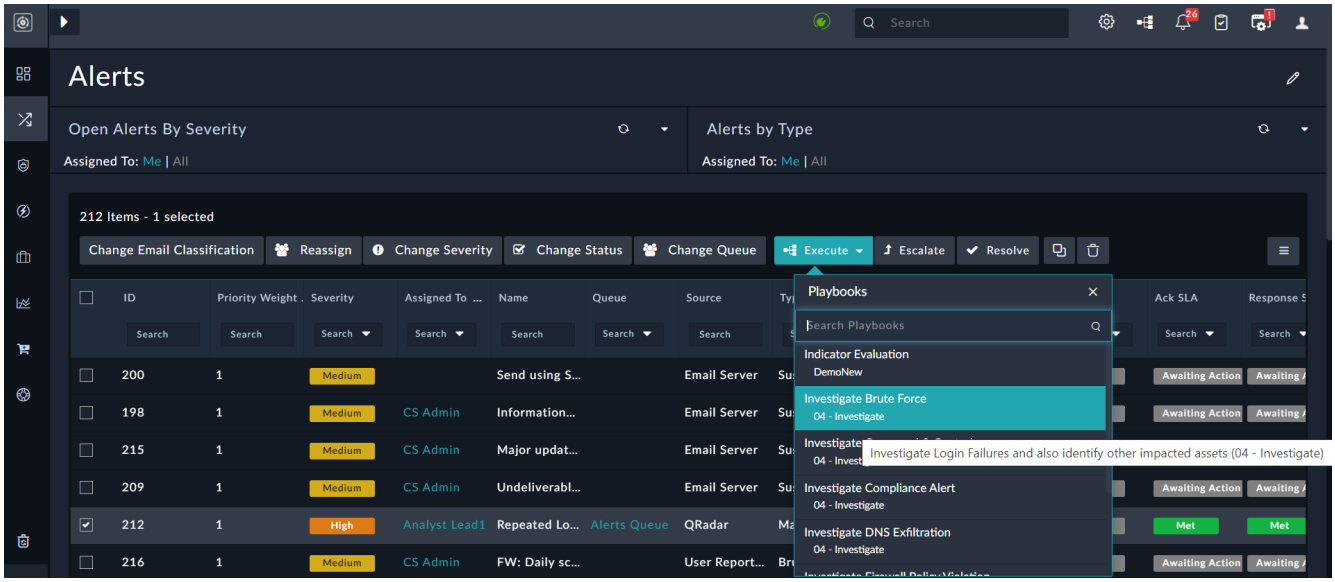


You will see **Yes** in the `Escalated` column in the row of the alert that you have escalated. You can see that an incident is created based on your inputs by either clicking the **Go to result** link as shown in the previous image or by opening the Incidents module. In our example, we named the incident as `Escalating a Critical Alert to an Incident`, and the following image displays this newly created incident:



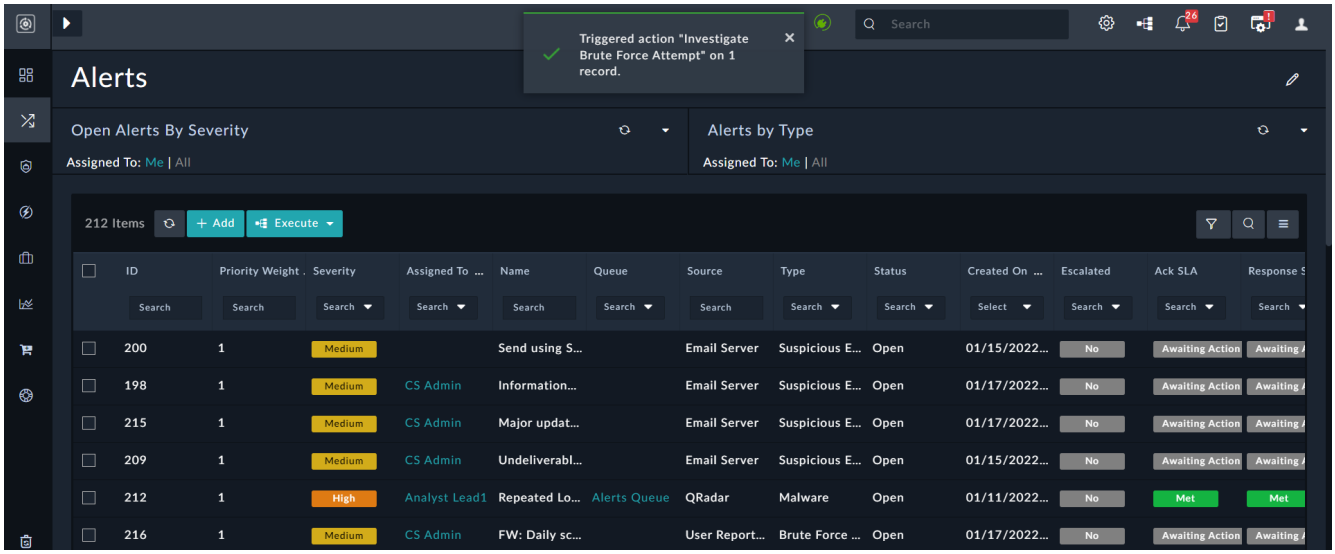
Executing playbook actions on a record

If you have registered any manual triggers on the module, in this case, the `Alerts` module, and you select a record, then you can see those actions listed in the `Execute` drop-down list. If you want to run any action against the selected record, then click **Execute** and select the action that you want to execute.



The names that are displayed in the **Execute** drop-down list are the names that you have specified as the playbook name or the name that you have specified in the **Trigger Label Button** field in a manual trigger playbook. If you have specified both, then the name you have specified in the in the **Trigger Label Button** field will be displayed in the Execute drop-down list. For more information about playbooks and triggers, see the *Triggers & Steps* chapter in the "Playbooks Guide."

For example, if you want to investigate a repeated login failure then select the alert for which you want to run the investigation and click the **Investigate Brute Force** option from the `Execute` drop-down list. This will run the `Investigate Brute Force` playbook as shown in the following image:

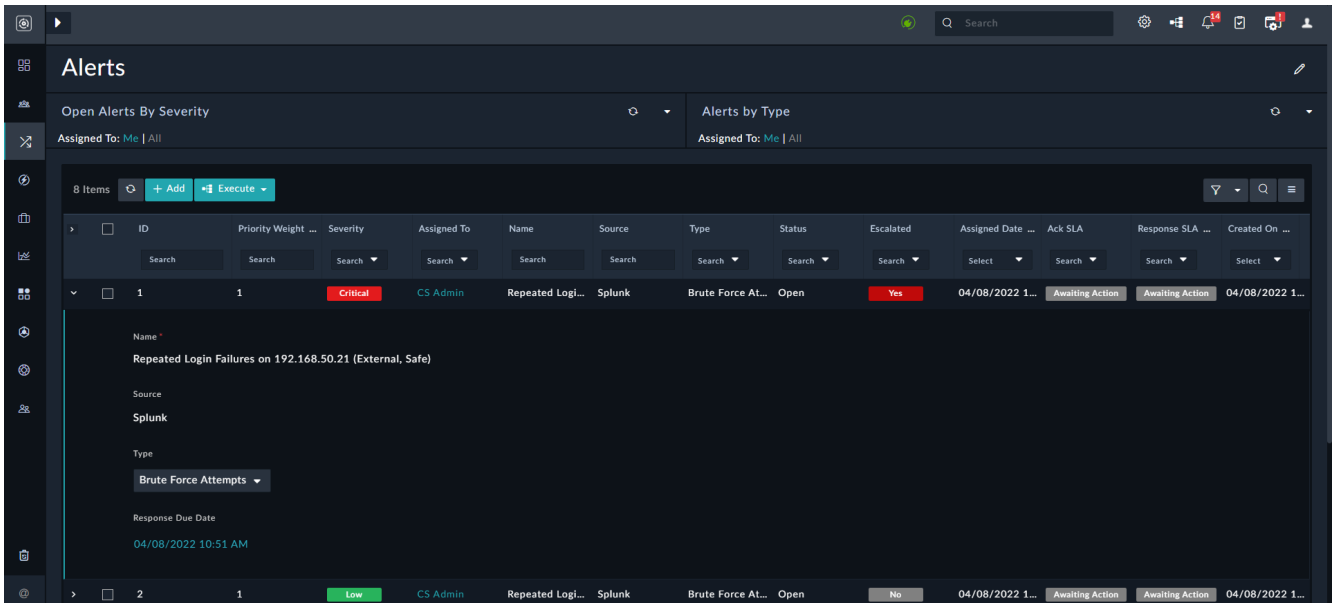


Important: FortiSOAR implements RBAC for playbooks, including the ability to define the ownership, Public or Private, for playbooks. A "Private" playbook is one that can be executed only by those teams to which it is assigned. A "Public" playbook is one that can be executed by all (if they have other appropriate rights). Execute actions include actions such as **Escalate**, **Resolve**, or any actions that appear in the **Execute** drop-down list on module records are shown based on ownership. For example, if you have created a **Private** playbook with a Manual Trigger on the `Alerts` module, and if you go to the alerts module and select the record, then the **Execute** drop-down list will contain only those playbooks that belong to your team(s). Also, you can only execute playbooks, if your administrator has assigned you a role that has the Execute permission selected for the Playbooks module.

Using Row Expansion in Grids

Administrators can also configure your template to display the overview for records, such as incident or alert records, without having to open that record in the detail view. For more information on how to configure the template, see the Dashboards, Templates, and Widgets chapter. If the template is configured for grid expansion, then you can click expand icon (**>**) in the record row to display the details for that record. The fields that are displayed here is dependent on what your administrator has configured in the template.

The following image illustrates how FortiSOAR displays the detail view of an alert whose template has been configured for grid expansion:

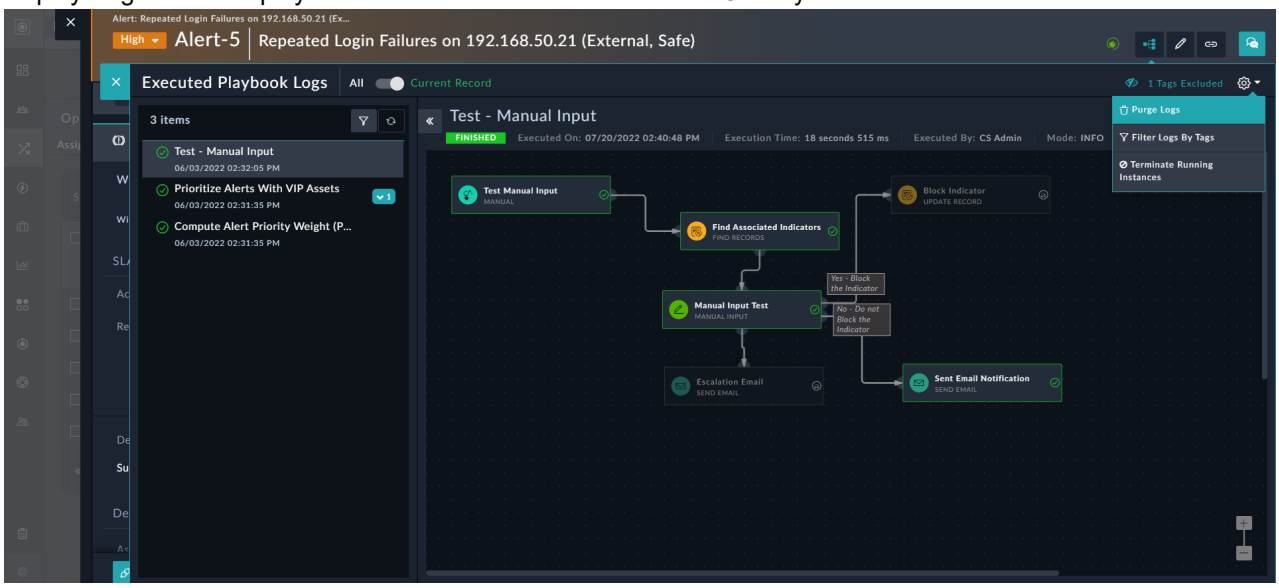


Alert Details View

When you click an alert in the list view, it opens the alert in the `Detail` view. You can view in-depth information about the alert as well as review comment activity and any records related to the alert (attachments, tasks, etc.). The details of the alert such as Severity, ID, Name, and the DateTime when the alert was last modified. You can also add or view tags associated with the record in the detail view. You can click icons that appear on the top right of the detail view to perform various actions:

- Click the **Executed Playbook Logs** icon ( ) to view the logs and results of playbooks that have been executed on that alert record in the flowchart format. You can toggle between **Current Record** and **All**. The 'Current Record' view displays only the logs of the playbooks that are executed on that particular record whereas, the 'All' view

displays logs for all the playbooks that are executed on the FortiSOAR system.



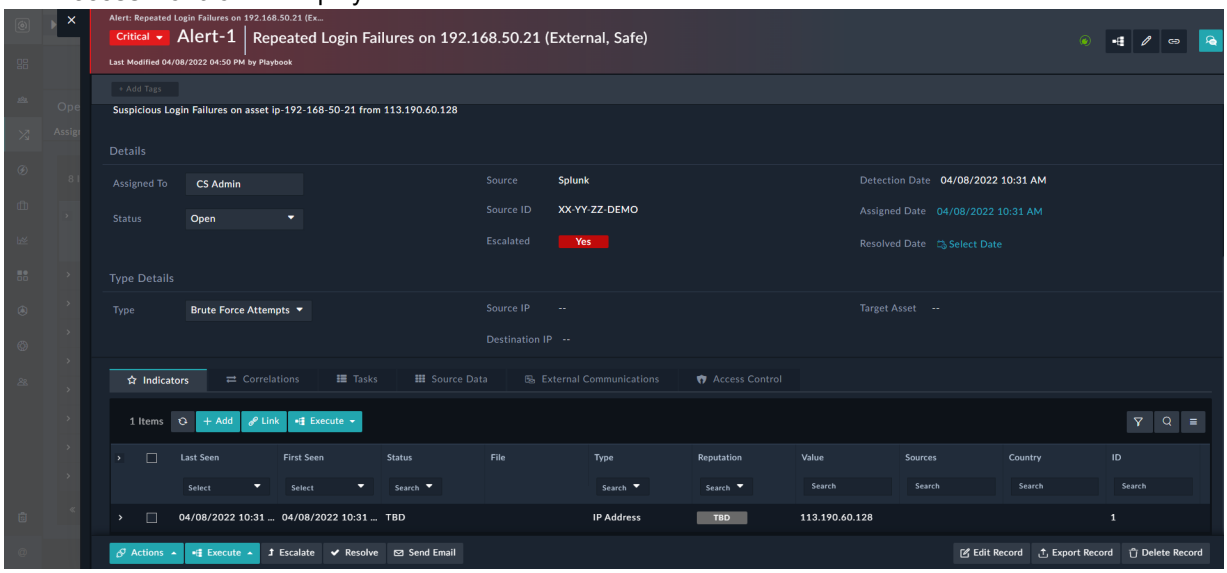
You can also purge Executed Playbook Logs for a particular alert by clicking the **Settings** icon on the top-right of the `Executed Playbook Logs` dialog in the Detail view of that alert, and then selecting the **Purge Logs** option, which displays the `Purge Playbook Execution Logs` dialog. In the `Purge Playbook Execution Logs` dialog, select the time frame (using the calendar widget) before which you want to clear all the executed playbook logs. For more information on all the **Executed Playbook Logs**, see the *Debugging and Optimizing Playbooks chapter* in the "Playbooks Guide."

- Click the **Edit Template** icon to design the detail view using templates. For more information on templates, see the Dashboards, Templates, and Widgets chapter.
- Click the **Copy Record Link** icon ( ) to copy the record link to the clipboard and share the record. The record link gets copied to the clipboard as follows: `https://{*Your_FortiSOAR_IP*} /modules/{*module_name*} /{*record_ID*}`. For example, `https://xx.xx.xx.xxx/modules/alerts/5f213267-8683-43c4-8560-b45eda413145`.

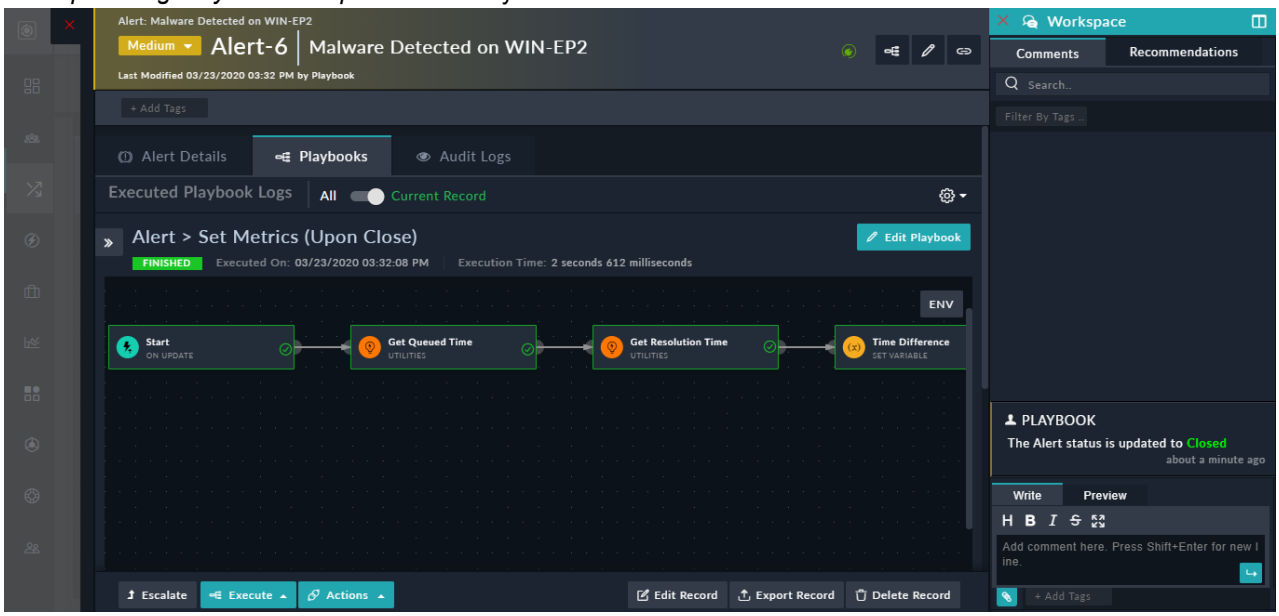
The `Details` view by default has the following tabs:

- The **Alert Details** tab displays details of the alert such as to whom the alert is assigned, the status, severity, type, source, etc of the alert. The Alerts Details tab contains the following tabs:
  - The **Indicators** tab displays the indicators such as URLs and IP addresses, which are linked to that alert record.
  - The **Correlations** tab displays subtabs that display the entities to which the alert is actively related.
  - The **Tasks** tab displays the tasks that are linked to that alert record.
  - The **Source Data** tab displays the raw data of that alert record.
  - The **External Communications** tab displays any external communication associated with that alert record.

- The **Access Control** tab displays the owners of that alert record.

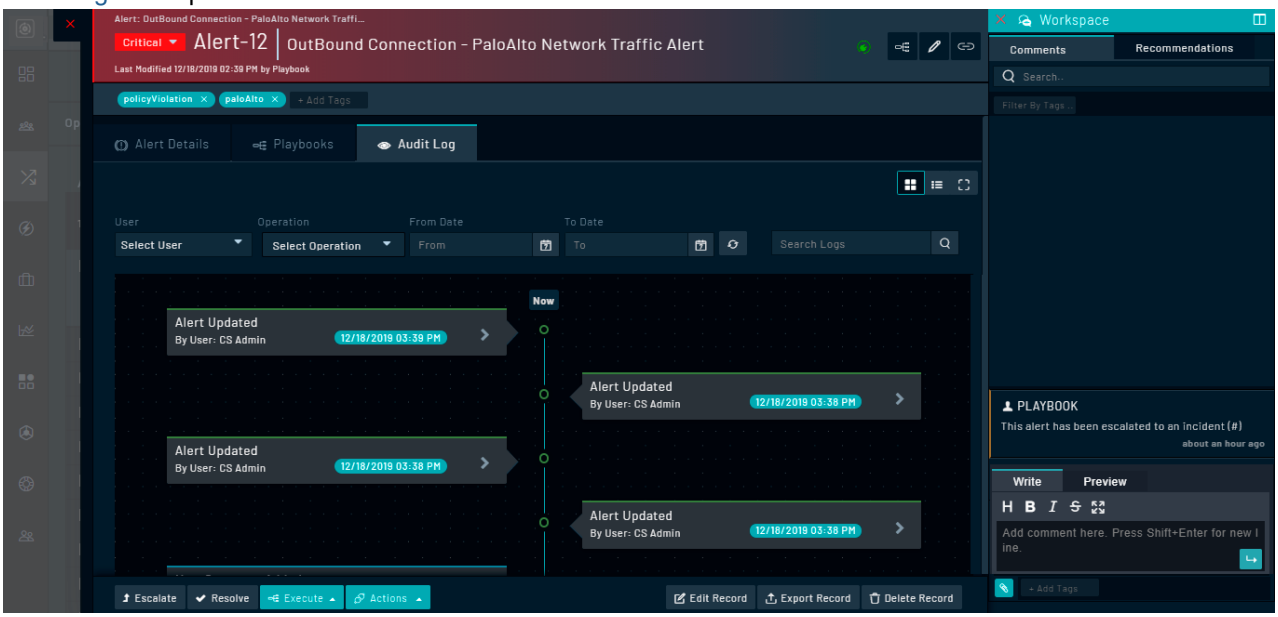


- The **Playbooks** tab displays the logs and results of playbooks that have been executed on that alert in the flowchart format, as is displayed in the **Executed Playbook Logs**. This makes it easier for users to view the flow of playbooks, especially useful for viewing the parallel execution paths in playbooks. The same view can be seen when you click the **Executed Playbook Logs** icon on the top right of the Detail view.
  For more information on all the **Executed Playbook Logs** and the details of the playbooks tab, see the *Debugging and Optimizing Playbooks chapter* in the "Playbooks Guide."



- The **Audit Log** tab displays the historical timeline, in a graphical format, for the current record. Click the **Full-screen Mode** button to view the audit log in the full-screen mode. You can expand and collapse the entries in the timeline (audit log) to view the details of the changes. For more information on `Timeline`, see the Dashboards, Templates,

and Widgets chapter.



Editing a record in the Alert Details tab

Overview

To edit the template for any module, including `Alerts`, click the **Edit Template** button. For more information on `Templates`, see the Dashboards, Templates, and Widgets chapter.

You can run actions on the record, such as escalating an alert to an incident by clicking the **Escalate** button. Or, you can resolve an alert by clicking the **Resolve** button. The **Escalate** and **Resolve** buttons have been explained in the `Alerts List View` section.

Click the **Delete Record** button to delete the alert record from the `Details` page.

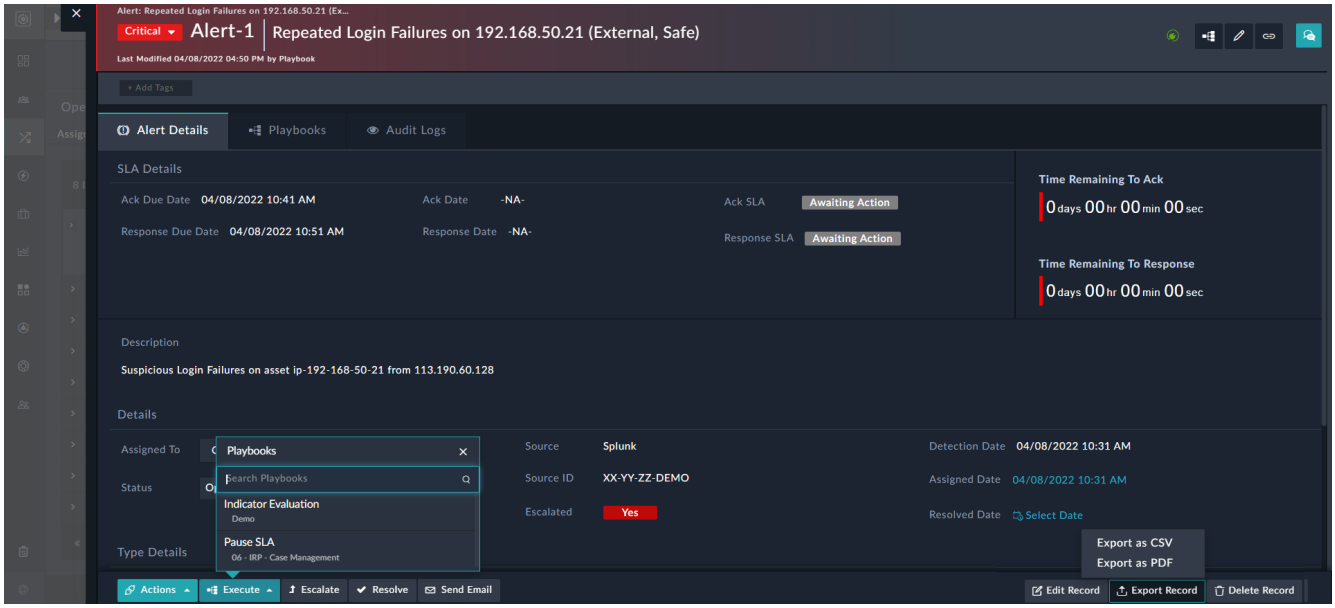
Deleting an alert record deletes the alert data and the relationships to the record, but not the entities to which the alert is related.

You can export the detailed information of the alert in the `.csv` and `.pdf` formats, by clicking the **Export Record** button.

If you want to export records from the record's grid and view panel that contain unsupported character sets such as Korean or Chinese, then your administrators require to perform additional configurations. For more information, see the 'Configurations required for exporting of records with unsupported character sets in the PDF format' topic in the *Debugging, Troubleshooting, and optimizing FortiSOAR* chapter of the "Administration Guide."

From version 6.4.0 onwards, you can view fields related to SLA management in you alert or incident records. You will see fields such as Ack Due Date, Ack Date, Ack SLA, Response Due Date, etc. using which you can track whether or not the SLAs have been met. For more information, see the *SLA Management* chapter in the "Administration Guide."

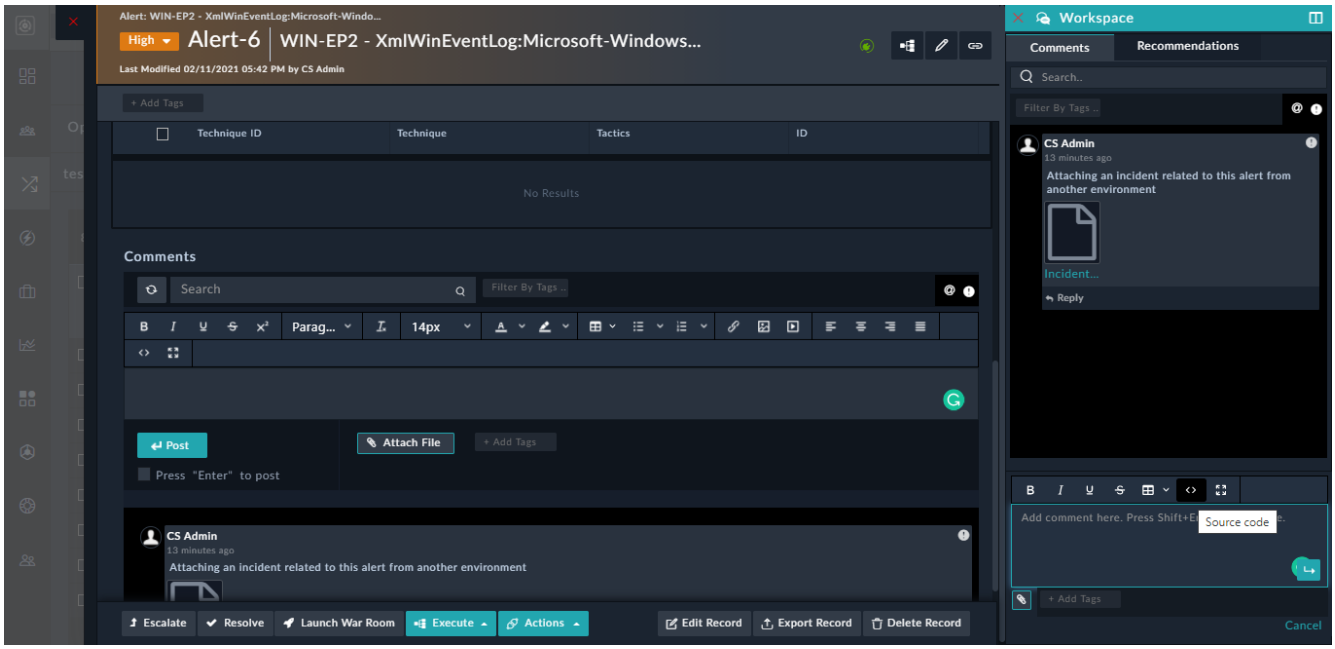
You can execute a playbook on the record by clicking the **Execute** button and selecting the playbook that you want to run on the record. From version 6.4.0 onwards, you can also search through the list of playbooks by typing the search keywords in **Search Playbook**.



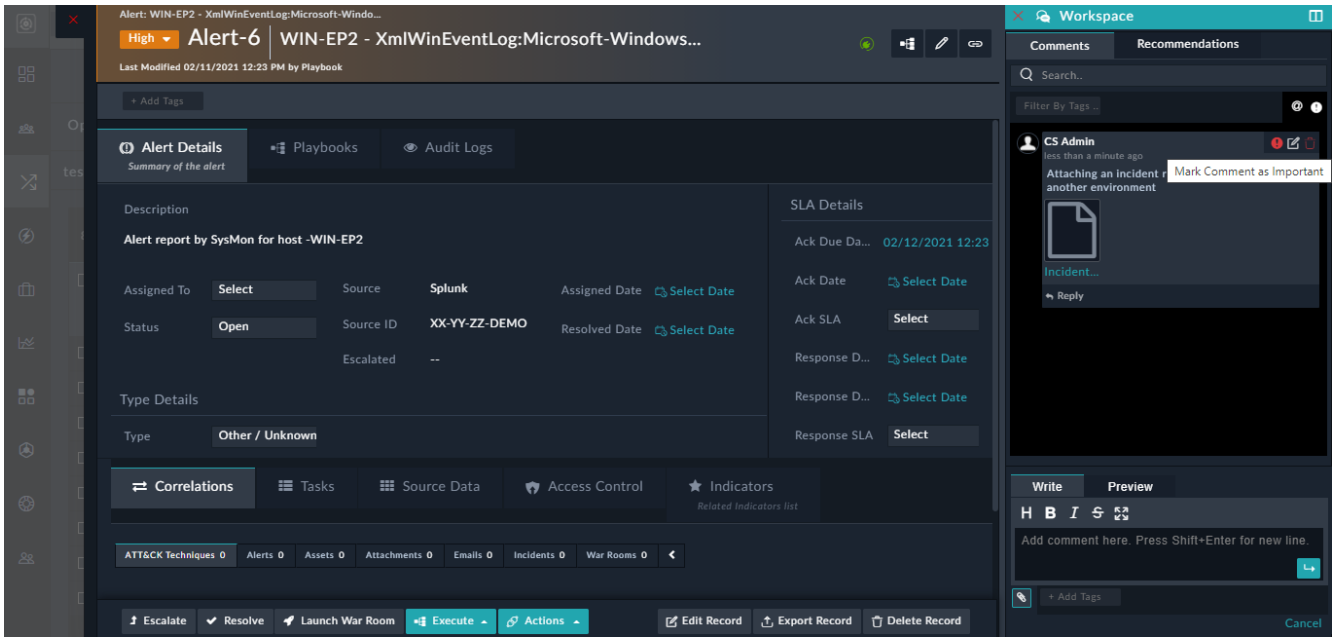
Click the **Workspace** icon ( ) to view the Workspace panel, which appears on the right side of the Detail view of a record and consists of the Comments tab and the Recommendations tab. You can use the **Comments** tab of the Workspace to add comments and attachments to the record. The **Recommendations** tab of the Workspace provides you with a list of similar records.

In the **Comments** tab, you can add comments and attachments to the record. Use the "Styling" toolbar to apply some formatting, such as bold, italics, underline, and strikethrough to the content that you add as a comment. From version 6.4.3 onwards, you can edit the **Contents** field in the "Comments" module, and choose how this field should be rendered, either Rich Text (Markdown), which is the default or as Rich Text (HTML).

The following image illustrates how the Comments widget is displayed in the Detail View of a record, when the "Content" field is set as Rich Text (HTML):

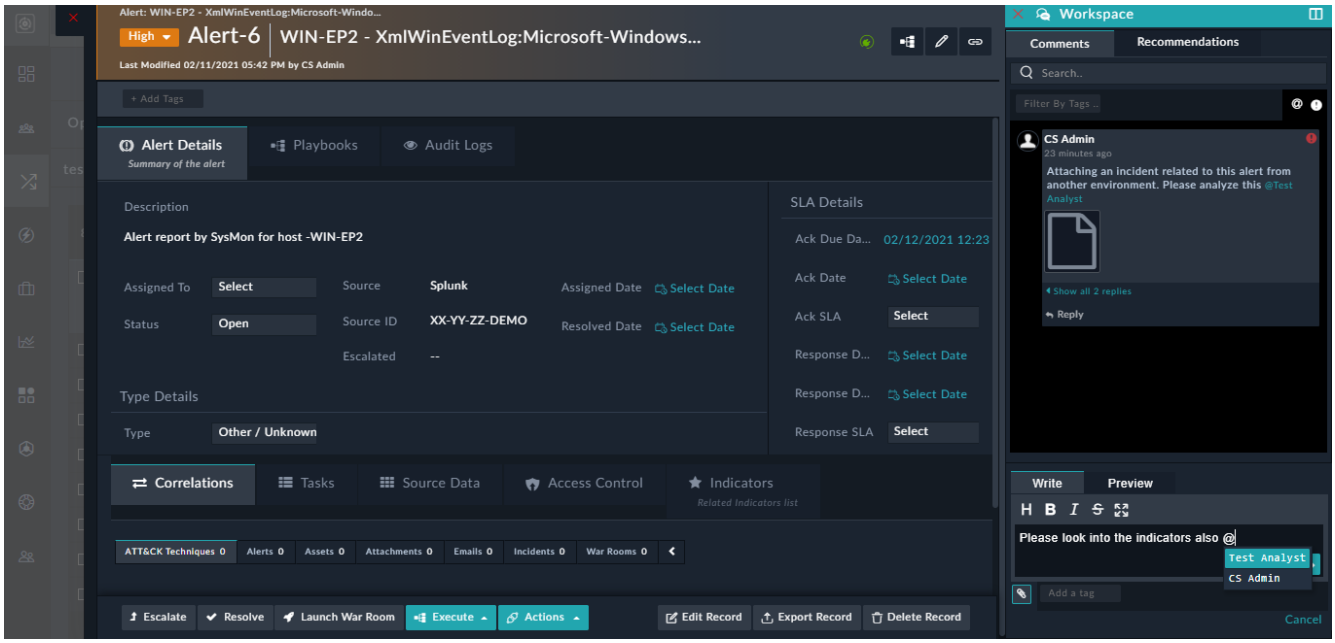


The following image illustrates how the Comments widget is displayed in the Detail View of a record, when the "Content" field is retained as Rich Text (Markdown):



You can mark a comment as important, by clicking the **Mark Comment as Important** icon. You can *search* for comments and also *filter* comments based on tags, mentions, and the importance flag.

From version 7.0.0 onwards, you can add mentions or tag users in comments. Typing `@` in the comments displays the list of active users, with their first and last names highlighted in blue. Select the user who you want to tag from the list, which results in the IRI of the user being linked to that comment. Users who are tagged get notified of their mentions by email.



Message Threads or Nested Replies are introduced in comments to help in keeping track of conversations and making it easier to respond to a specific thread. Now, when users reply to a comment, the reply will be displayed as an indented (only a single level indent) comment. which helps in clear identification of replies to a comment and a new comment thread as seen in the above image. The first comment contains a message thread whose entire conversation you can view by clicking **Show all <number of replies> replies**. You can reply to the conversation by clicking **Reply**.

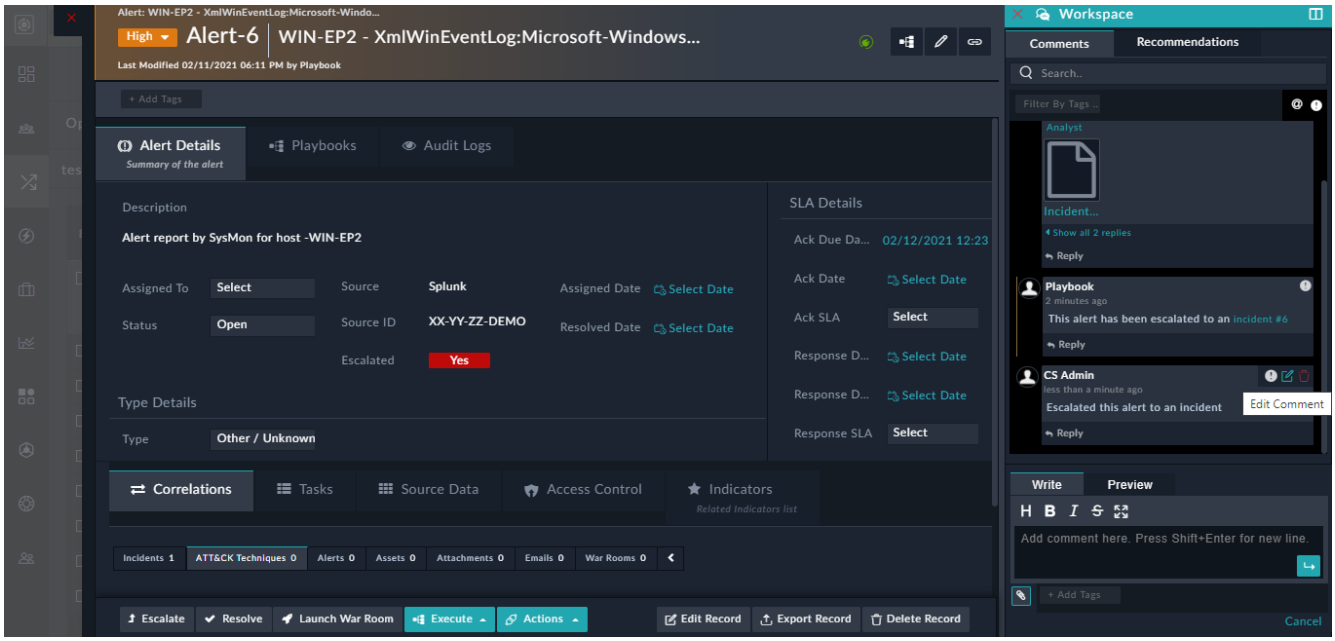
If you have large files or images to be added to comments, you can add them as attachments to the comments. Add files or images by dragging-and-dropping files or images (these are added as inline images) onto the comments panel, or by clicking the **Attachments** button. You can attach a maximum of five files to a single comment. Both Inline images and images that are attached get appropriately resized within comments. To view the images as per its original size so that it becomes possible to read the contents of the images, click the attachment name to see the enlarged image. In case of inline images, clicking the image name downloads the original image.

You can preview the comment by clicking on the **Preview** tab and click the **Full Screen** icon to make the workspace cover the complete screen. Press `Enter` or click the **Post Comment** icon to add the comment to the collaboration panel. Press `Shift + Enter` to add a new line.

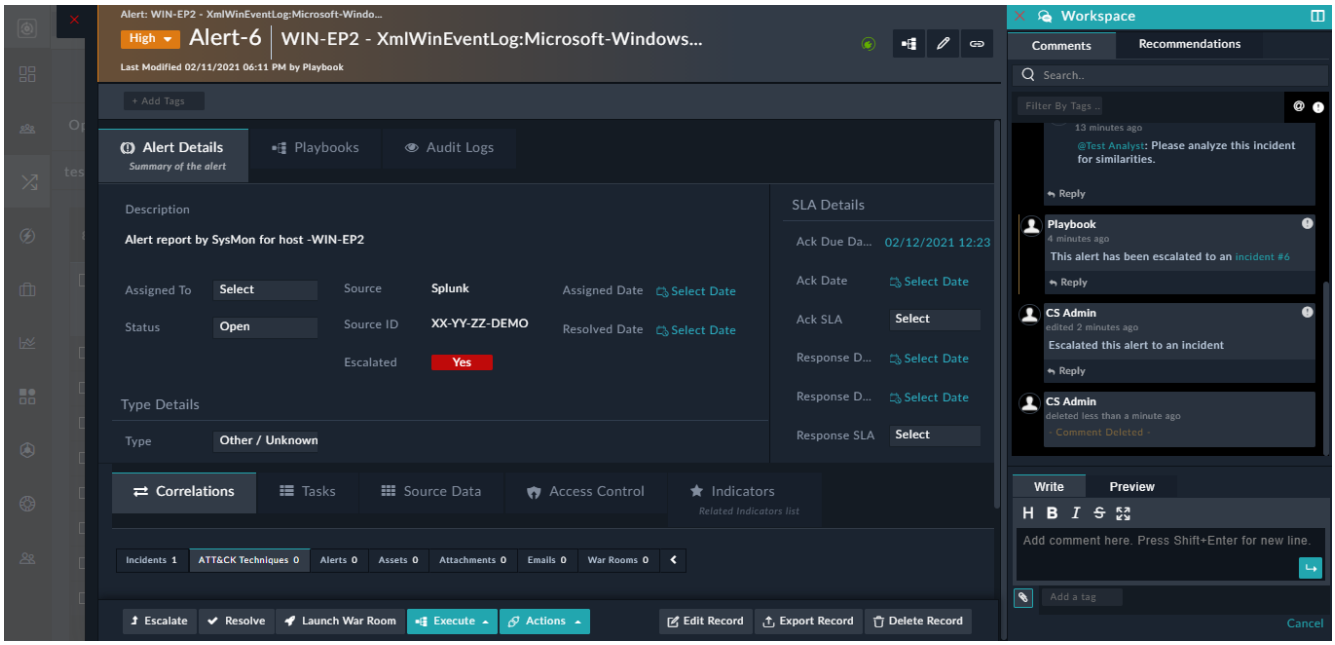
You can increase the width of the workspace panel by clicking the **Expand** icon ( ). The Comments panel displays the latest 30 comments, and if you want to view older comments, then click the **View More** link that at the top of the Comments panel.

You can edit and delete your own comments if your administrator has enabled the settings for comment modification and if you have appropriate CRUD permissions on the `Comments` module. You can edit or delete your comments within the time duration that your administrator has set, by default this is set to "5 minutes". This means that you can edit and delete your comments within 5 minutes of adding the comment.

If you want to edit a comment, click the **Edit** icon within the comment, make the necessary modifications to the comment and press Enter. The Collaboration Panel would now display the modified comment with the `Modified <time when the comment was modified>`, for example, `Modified less than a minute ago`, content appearing under the modified comment, as shown in the following image:



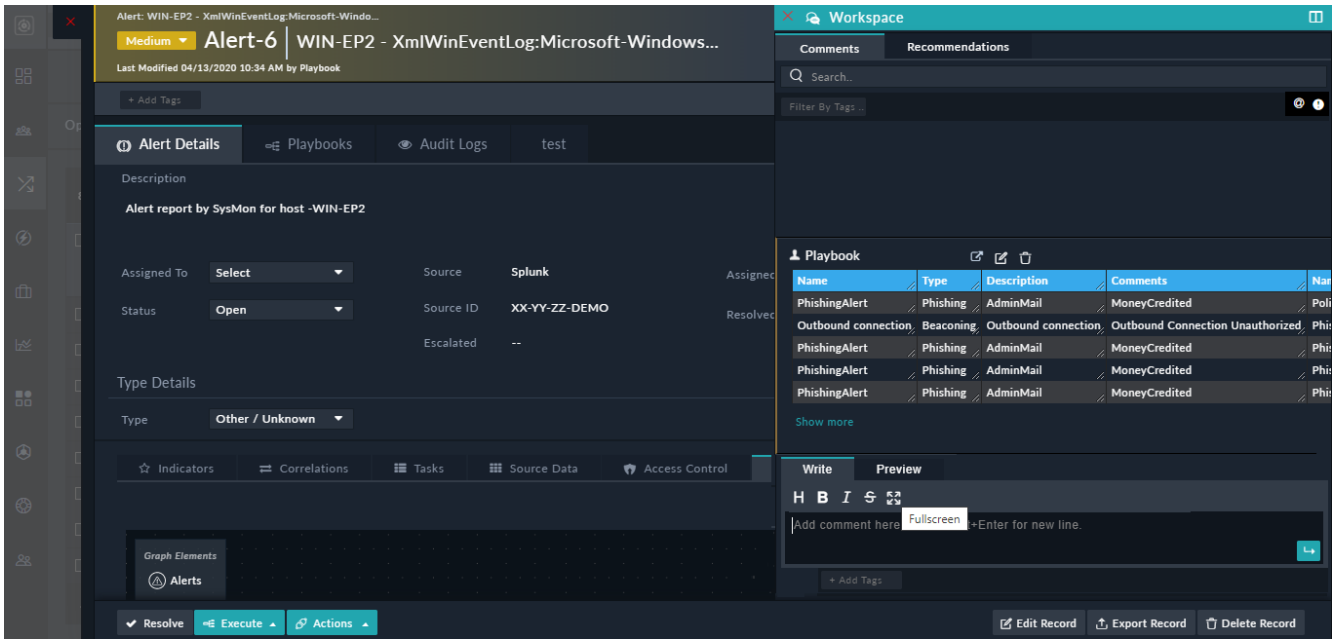
If you want to delete a comment, click the **Delete** icon within the comment and in the Confirmation dialog, click **Confirm**. Then Collaboration Panel would display the comment as – `Comment Deleted` – under the username, as shown in the following image:



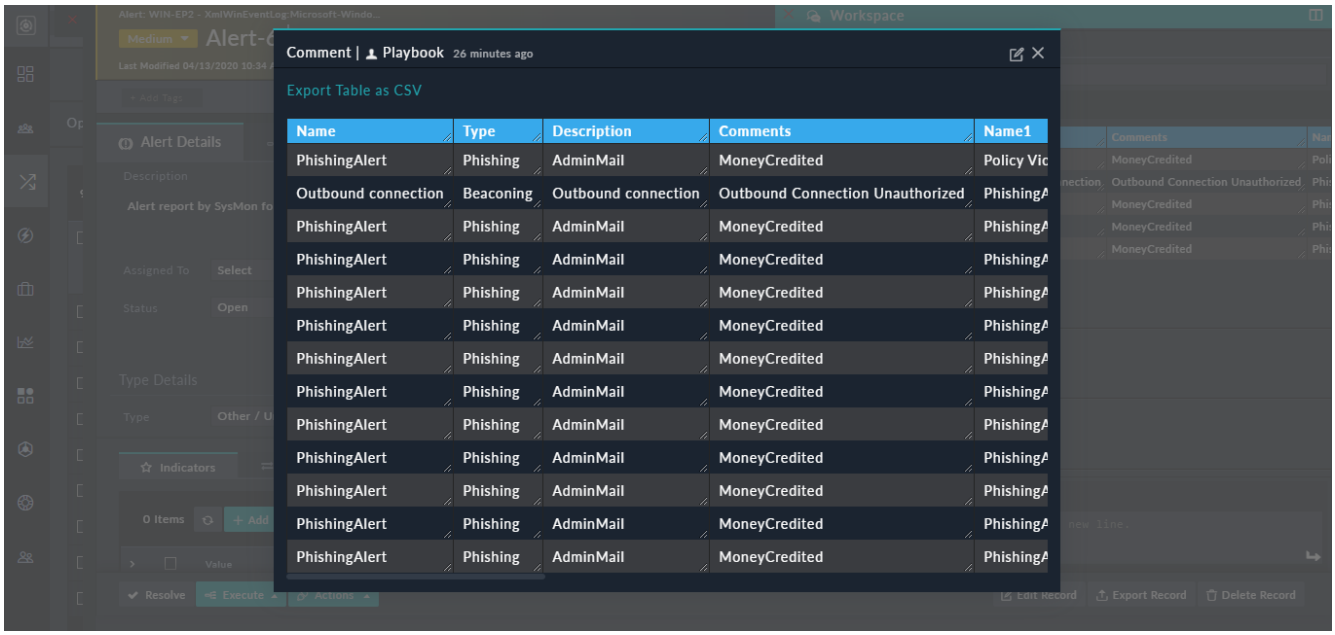
You will observe the same behavior in case the **Comments** widget has been added in the detail view of the record.

Related records permissions are defined by the parent record, and therefore comments are associated with the record instead of the module. Therefore, anybody who can see the record as per ownership or team hierarchy can see all the comments added to that record irrespective of who added the comments to that particular record.

From version 6.4.0 onwards, the table view has been enhanced to allow for editing a table in the Collaboration Panel by clicking the **Edit** icon and also for viewing the table in the full screen by clicking the **Full-Screen** icon as shown in the following image:



Clicking the **Full-Screen** icon opens the table in the full screen as shown in the following image:

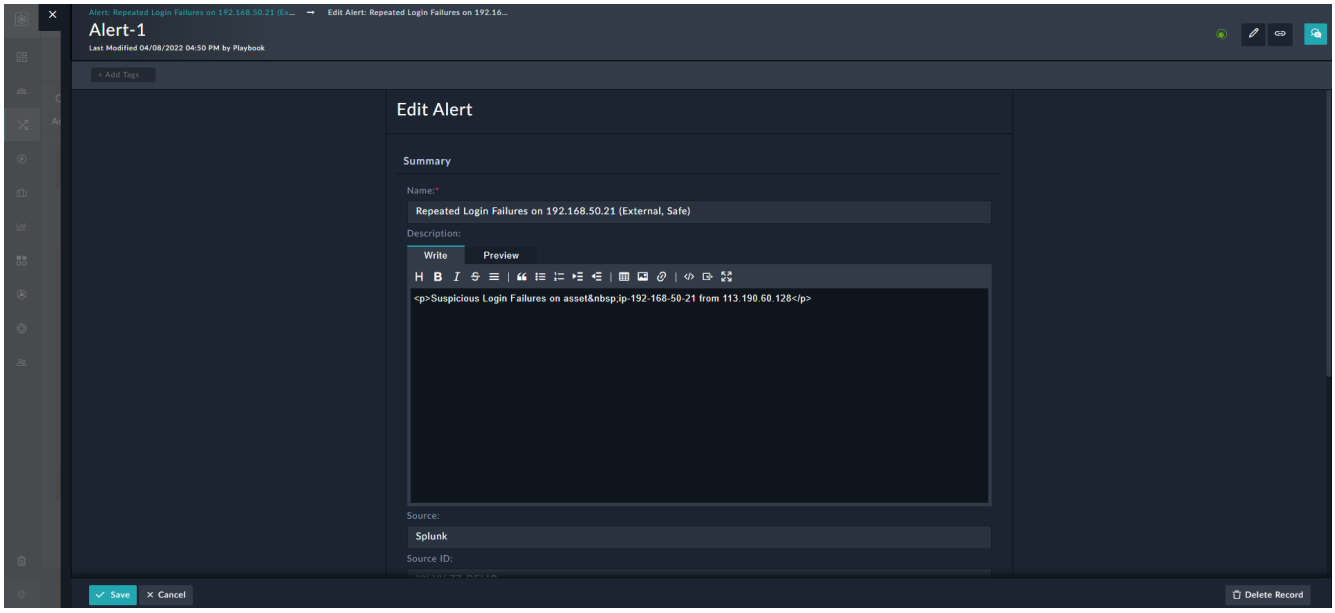


This enhancement makes it easier for you to view and edit large tables in the Collaboration Panel, especially those that have been converted from JSON to HTML using the "Util: Convert JSON into an HTML Table" action of the "Utilities" connector and added into the alert using a playbook as shown in the above image. In the full-screen mode also you can edit the table and you can export the table in the `.csv` format by clicking the **Export Table as CSV** link. Also, if there are more than "5" rows in the table then a **Show More** link will be displayed, clicking which you can view all the rows of the table.

Editing Records

Editing the complete record

To edit the complete record, click the **Edit Record** button, which opens the `Edit Alert` dialog that contains the details of the alert in a form. You can edit multiple fields at one time for the record and then click **Save** to save the changes to the record.



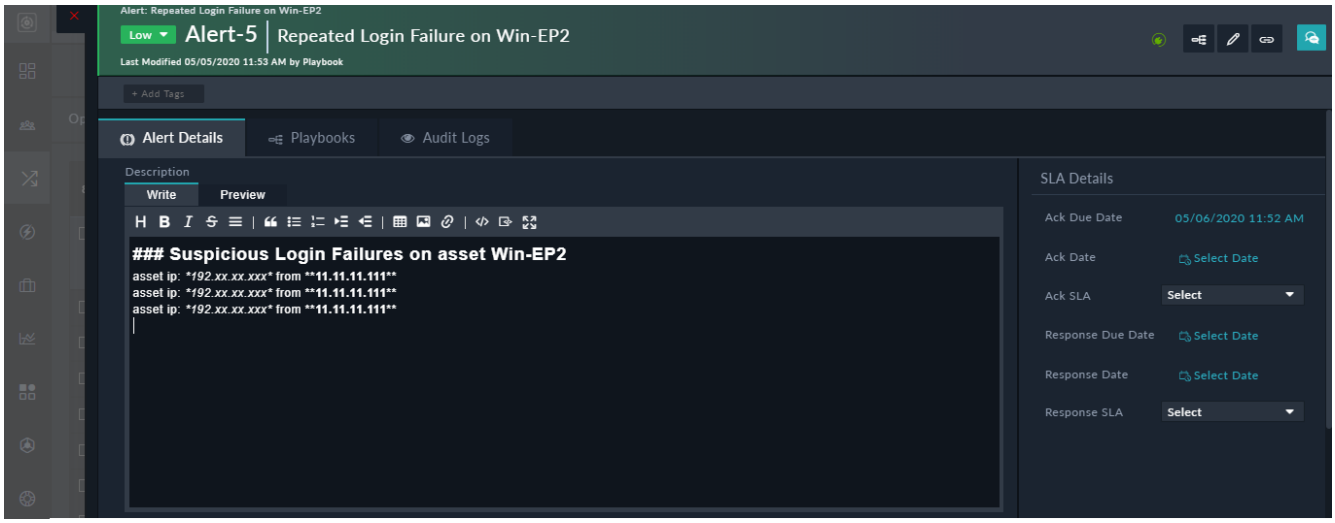
Editing Fields

To edit any fields in the record, go to that field, and if that field is an editable field then you can click and change the value of that field either by typing content in the text field or by selecting a value from a drop-down list.

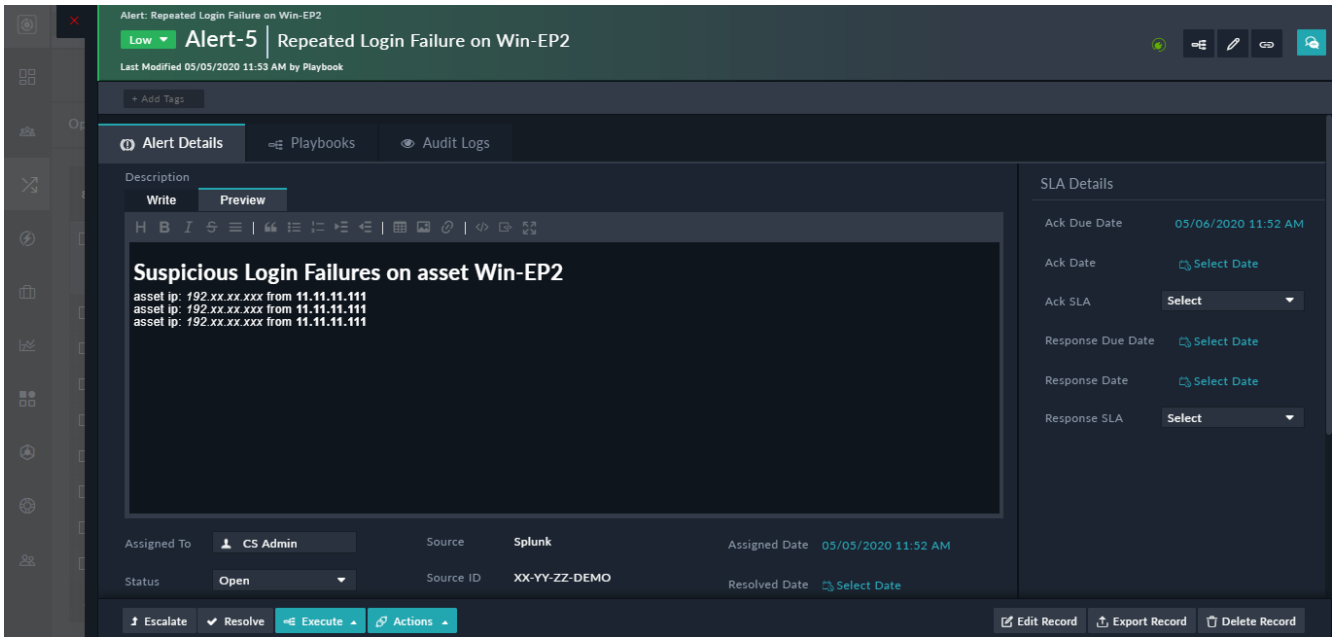
The alerts detail view contains a **Description** field that provides the description of the alert and it is generally a "Rich Text" field. Rich Text fields allow you to apply formatting to the content entered in this field. Rich Text fields can either have a "Markdown" editor or an "HTML WYSIWYG" editor, based on the sub-type that is set for this text field. The default editor is set as "Markdown" for all modules, which can be changed to the "HTML" editor using 'Module Editor'.

You can add styles such as headings, bold, italics, add lists, tables, and insert links, images, attachments etc. using the "Styling" toolbar provided in the rich text field in both the Markdown and HTML editors. Note that video is not supported in the "Markdown" editor.

In case of the Markdown editor, you can write in markdown in the "Write" mode and click **Preview** to view how your content will be displayed. The following image displays content in the "Write" mode:



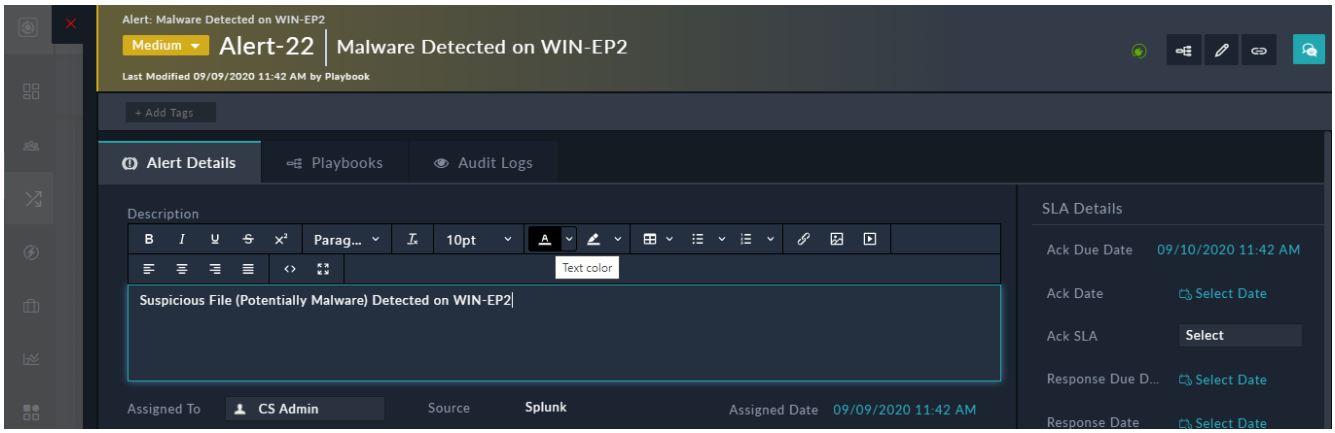
The following image displays content in the "Preview" mode:



You can also add an inline css or add inline styles such as `"style="color:blue;""` to your content in the Rich Text field.

Some tags such as script, iFrame, textarea, form, select, meta, style, link, title, embed, object, details, and summary and some attributes such as onLoad are not supported in the Rich Text (Markdown) field and the Richtext Content widget. If you want to use these tags or attributes, contact FortiSOAR support.

The following image displays editing of content of a rich text field using the HTML editor:

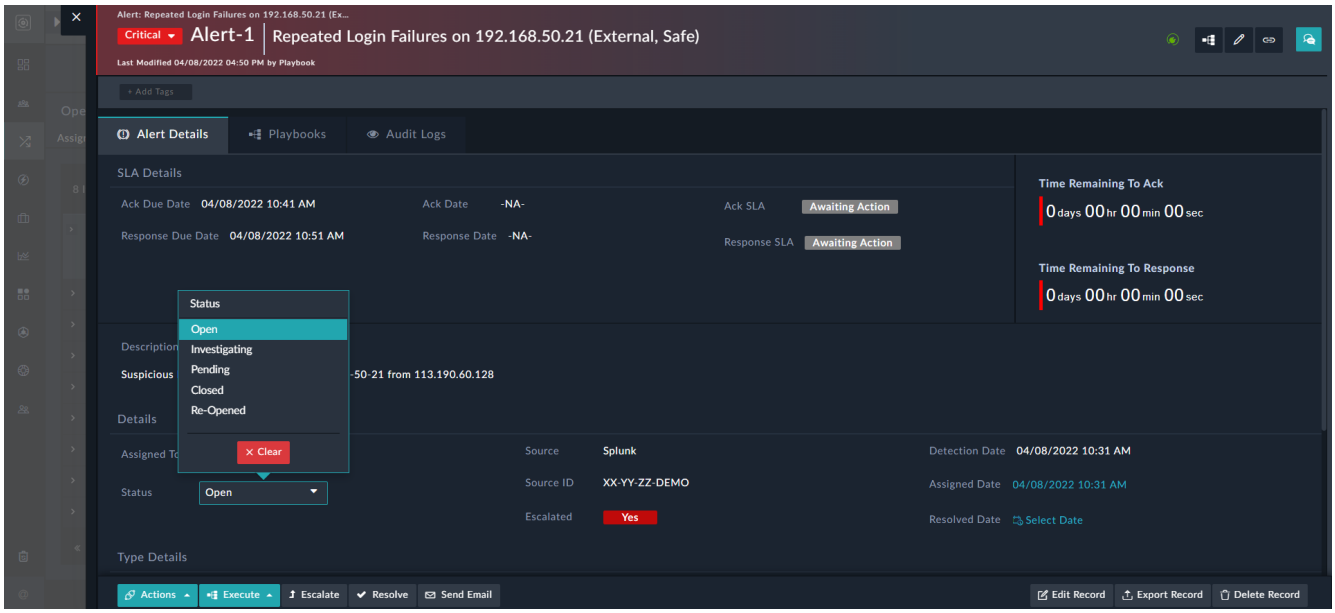


If the editor of the "Rich Text" field is changed from Markdown to HTML or vice-versa, note the following:

- If the content was in the HTML format and you change the format to Markdown, then the Markdown editor will display the HTML code in "Write" mode and the "Preview" will work fine.
- If the content was in Markdown format and you change the format to HTML, then the HTML editor will show the Markdown code in the source code mode; however, the content will not get rendered. You must convert the markdown code to HTML code for the content to correctly render the content.

Editing picklists or lookups

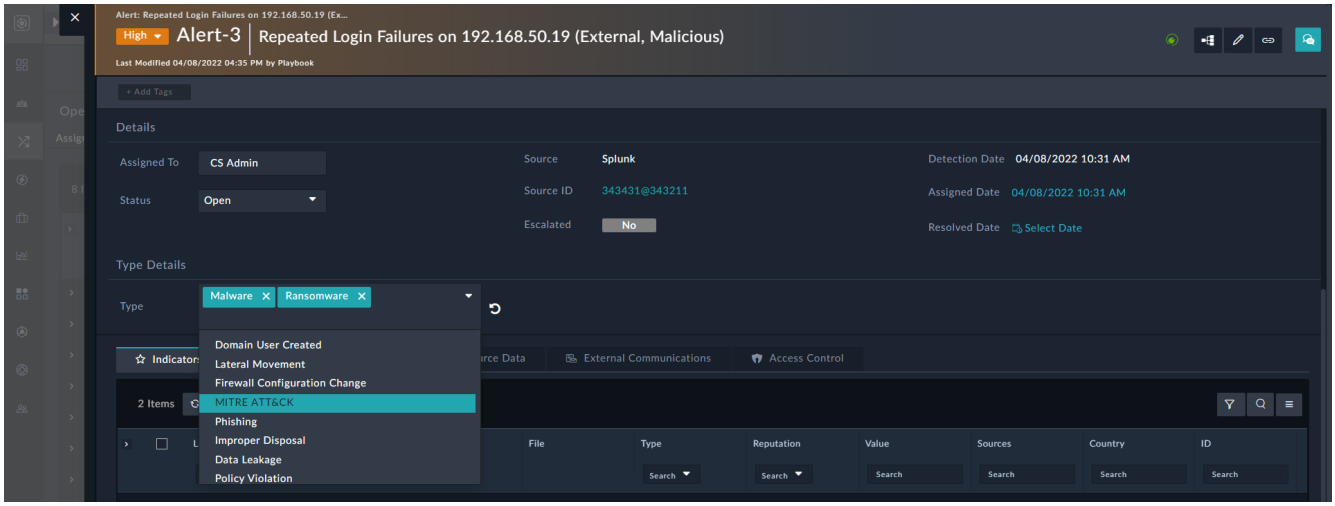
To change a value of a picklist or a lookup, select the required value from their respective drop-down list as shown in the following image:



By default, `lookup` fields in FortiSOAR display only the first 30 items. To search for more than 30 items, use the `Search` text box. For example, the `Status` list in the above image will display only the first 30 users.

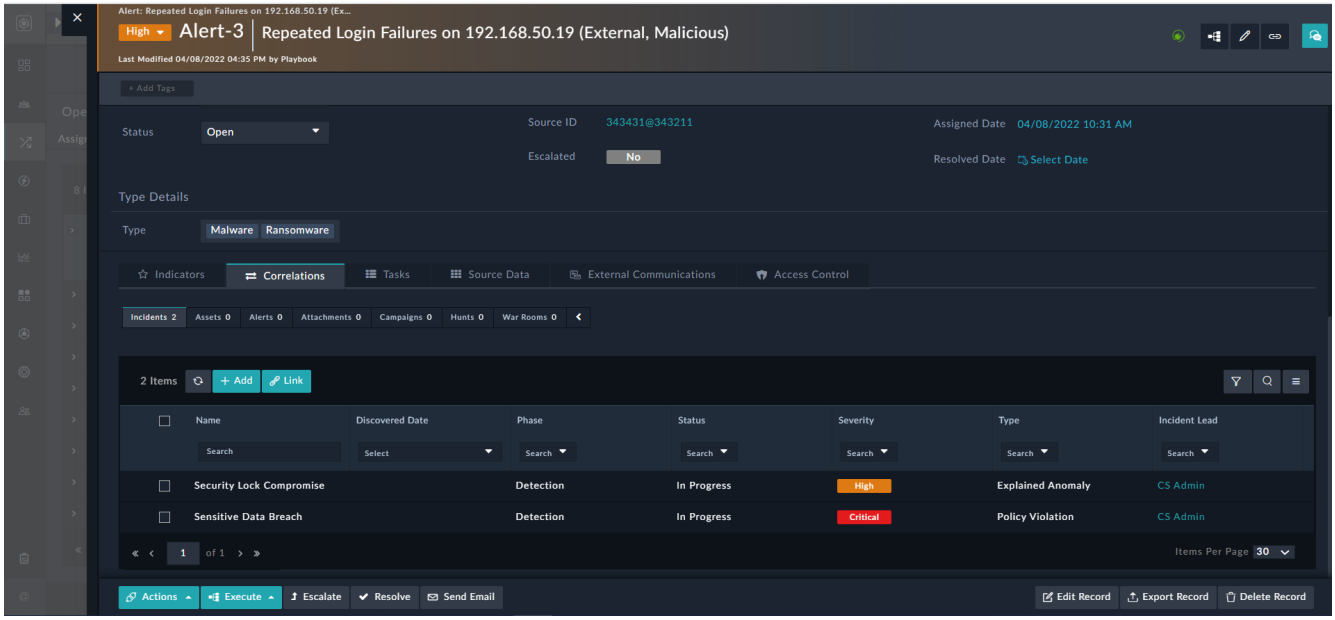
The `lookup` fields for the `People` module, such as **Assigned To** or **Incident Lead**, also contains a **View** button. Clicking the **View** button opens the `User Profile` page for that user.

FortiSOAR also supports a special type of picklist, called "Multiselect Picklist". You can use the multiselect picklist for fields that can contain more than one value. For example, you can have an alert be assigned more than one "Type", i.e., an alert can be of type Brute Force Alert and Malware. If your administrator has assigned "Multiselect Picklist" field type to any picklist, then you can assign more than one value to that field as shown in the following image:



Working with Related Records

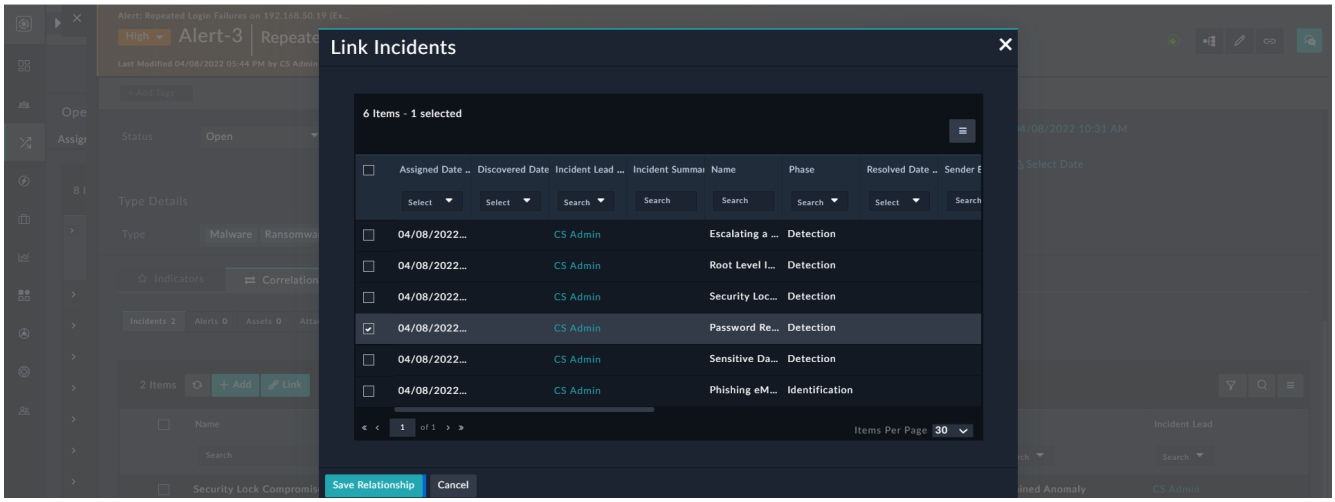
Clicking the **Correlations** tab displays subtabs that contain the entities, such as incidents or emails or events, to which the alert is actively related.



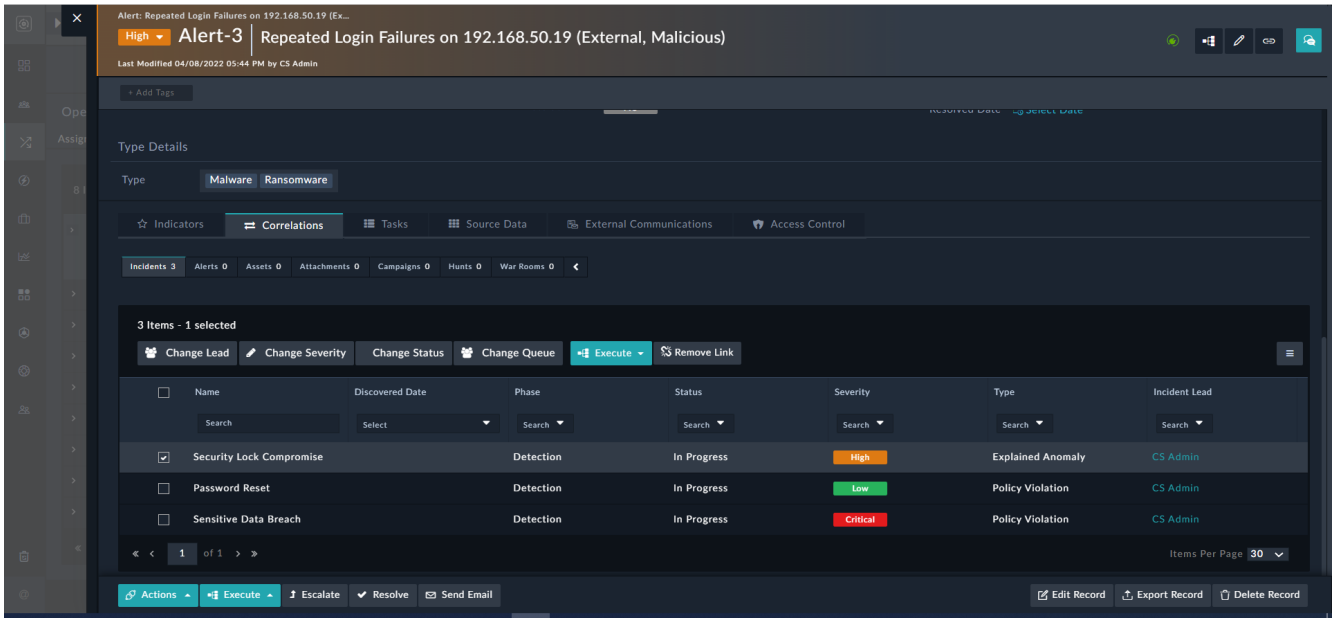
Clicking the **<** icon collapses the subtabs and displays entities to which the alert has an active relationship and clicking **>** icon expands the subtabs displaying all the entities.

If you want to add relationships to any other entity, click that entity and then click the **Link {Entity}** button. For example, to link an incident to an alert click **Incidents** and then click the **Link Incidents** button. This displays the `Change`

`Relationship` dialog which displays the list of Incidents. Click the incident that you want to link to the alert and then click **Save Relationship** to add the incident as a related record to the alert.



You can perform update field operations on the related item, such as change status, change severity and change lead, by clicking the respective buttons. The operation of these fields is similar to Executing default actions on records in bulk. To remove a relationship, select the related item and click **Remove Link**.



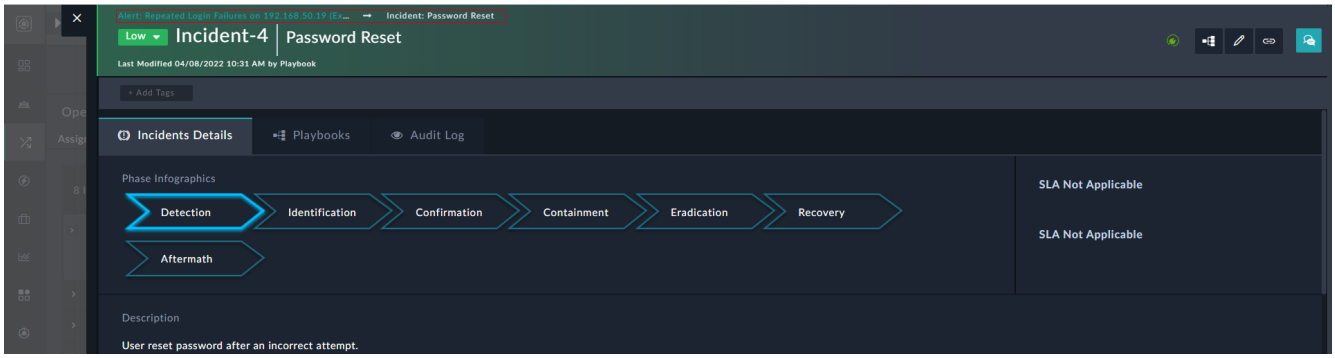
Related records permissions are defined by the parent record. For example, if there is an alert record that contains a related incident record to which you do not have permissions, you will be able to view that incident record (read-only permissions) in the **Related Records** tab.

You can also view the relationships of a particular record in a graphical format, by adding the Visual Correlation widget to the detail view of the records. For more information, see the Dashboards, Templates, and Widgets chapter.

Viewing Breadcrumbs

FortiSOAR displays breadcrumbs in the top bar of a record so that you can view your navigational trail and immediately know your location within FortiSOAR. Using the breadcrumbs, you can navigate easily through several related records and come back to your original record.

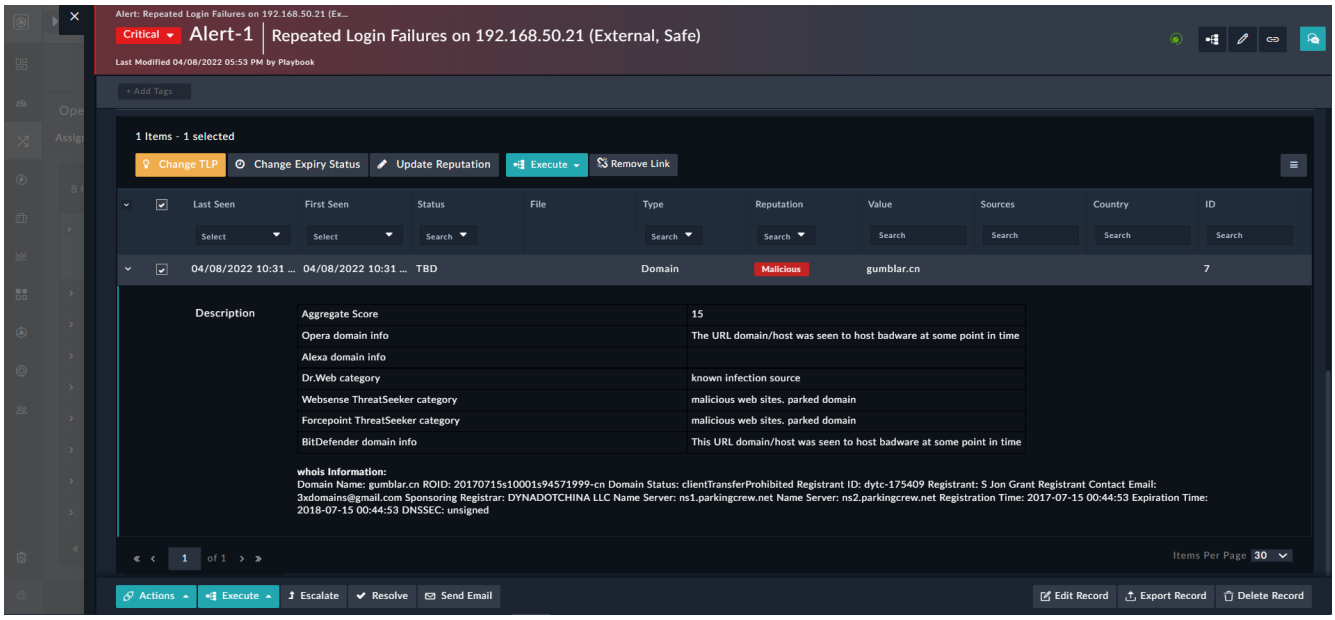
For example, click a record in a module, for example, `Alerts`, then click the **Related Records** tab, click the **Incidents** subtab, select the related incident. You will see the breadcrumbs in the top bar of the record, as shown in the following image:



Using Grid Expansion in Relationships

If your administrator has configured your template to display the overview of related records in the detail view of the record itself without having to open the related record in a new window. For example, you can view the details of an incident related to an alert in the alert detail view itself, without having to open the incident record in a new window. For more information on how to configure the template, see the Dashboards, Templates, and Widgets chapter. If the template is configured for grid expansion, then you can click expand icon (**>**) in the related record row to display the details for that record. The fields that are displayed here is dependent on what your administrator has configured in the template.

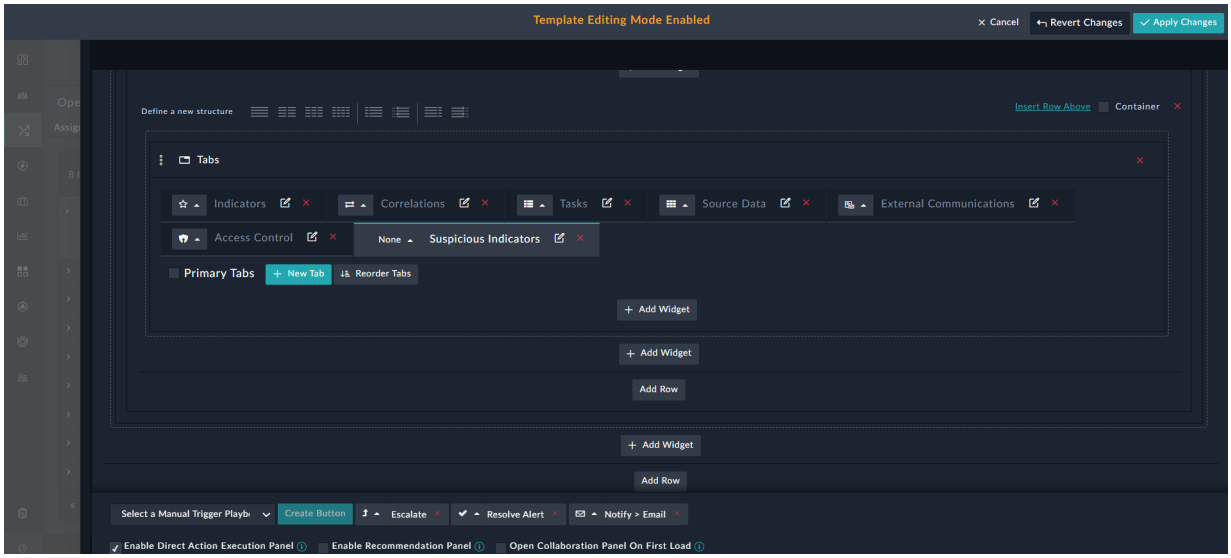
The following image illustrates how FortiSOAR displays the detail view of an alert and its **Related Records** tab, with the **Incidents** tab selected. The Incidents records have been configured for grid expansion:



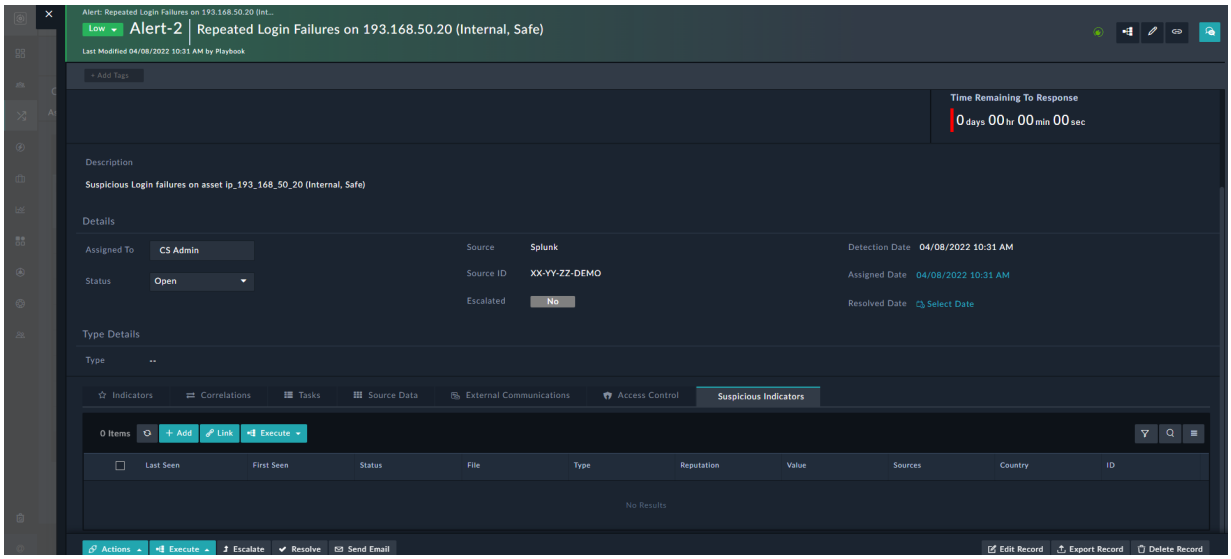
Applying different default filters for each relationship grid

You can apply different default filters for each relationship grid widget. For example, if in the alert details, you want one relationship grid to display only "Suspicious" Indicators and another to display only "Malicious" Indicators, this can be achieved as follows:

1. In the alerts detail view, add a relationship grid for Indicators, named "Suspicious Indicators" as follows:
   a. Open an alert in the detail view and click **Edit Template**.
   b. In the Template Editing Mode, go towards the end of the template, where various tabs for related records are present, and click **New Tab**, and enter the title as `Suspicious Indicators` and click the **green** checkbox. Then, click **Add Widget** in the Suspicious Indicators tab and optionally add an icon for this tab. rom the `Choose Widget` dialog, select **Relationships**. Click **Edit** in the Relationships grid, and in the `Relationships` dialog, click **Remove All** and then from the **Select a module** drop-down list, select **Indicators**, click **Add To View** and click **Save**.

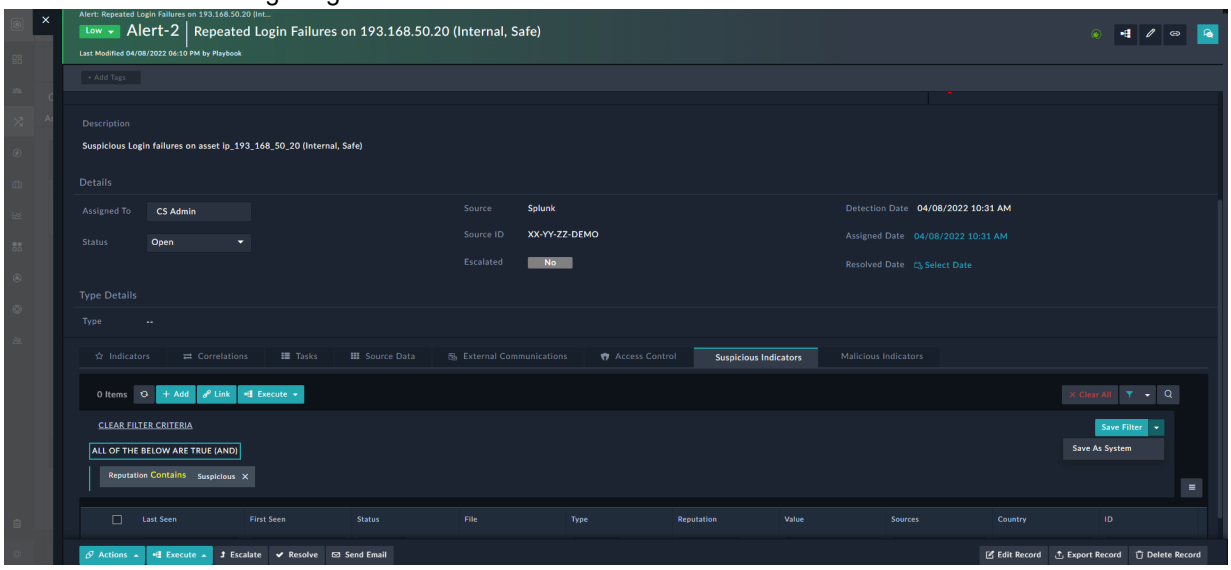


   This creates a tab called **Suspicious Indicators** in the `Related Records` section in the alert details page.



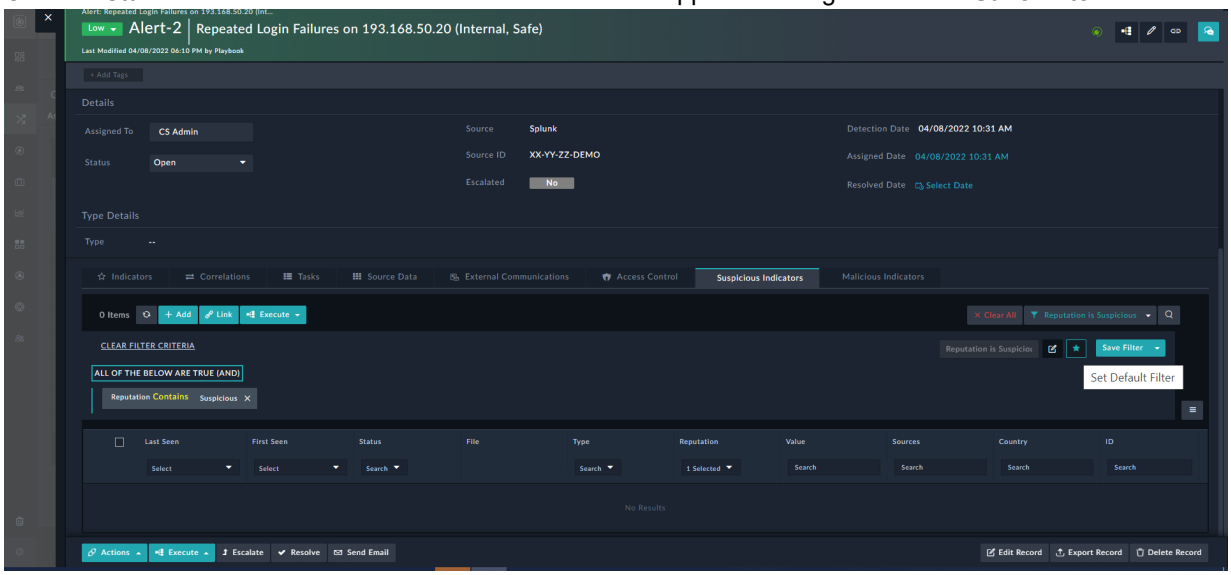
Similarly, perform the above steps for creating the **Malicious Indicators** tab.

2. In the Suspicious Indicators tab, create a filter for "Reputation = Suspicious" as follows:
   a. Click **Filters** and from the **Reputation** drop-down list select **Suspicious** and click **Apply**. This creates a filter as shown in the following image:

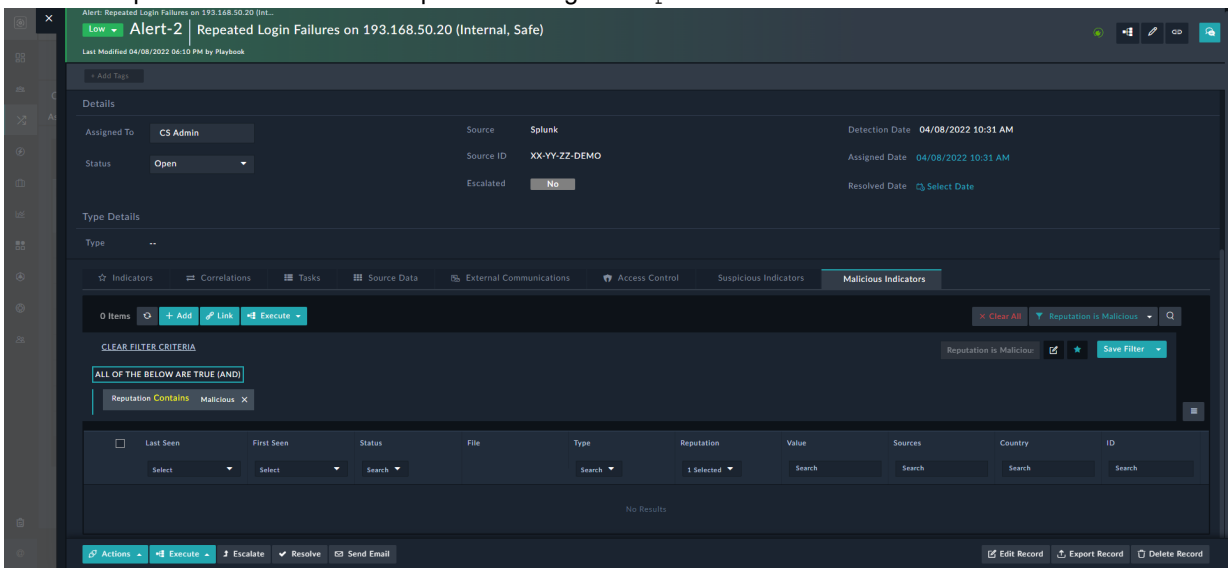


   b. Click the **Save Filter** drop-down list as select the **Save as System** option (if you want this filter to be applicable to all users) which opens the `Save As System Filter` dialog, in which enter the name of the filter such as, `Reputation is Suspicious`, and click **Save**.

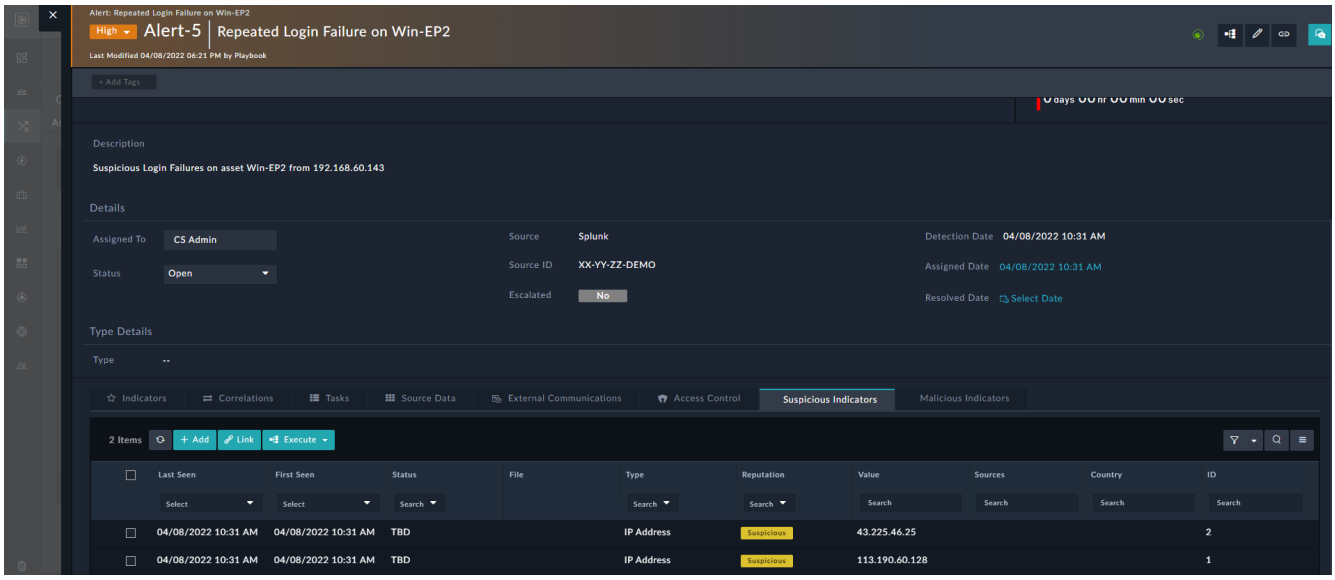
c. Click the **star** icon to save this filter as the default filter to be applied to this gird and click **Save Filter**.



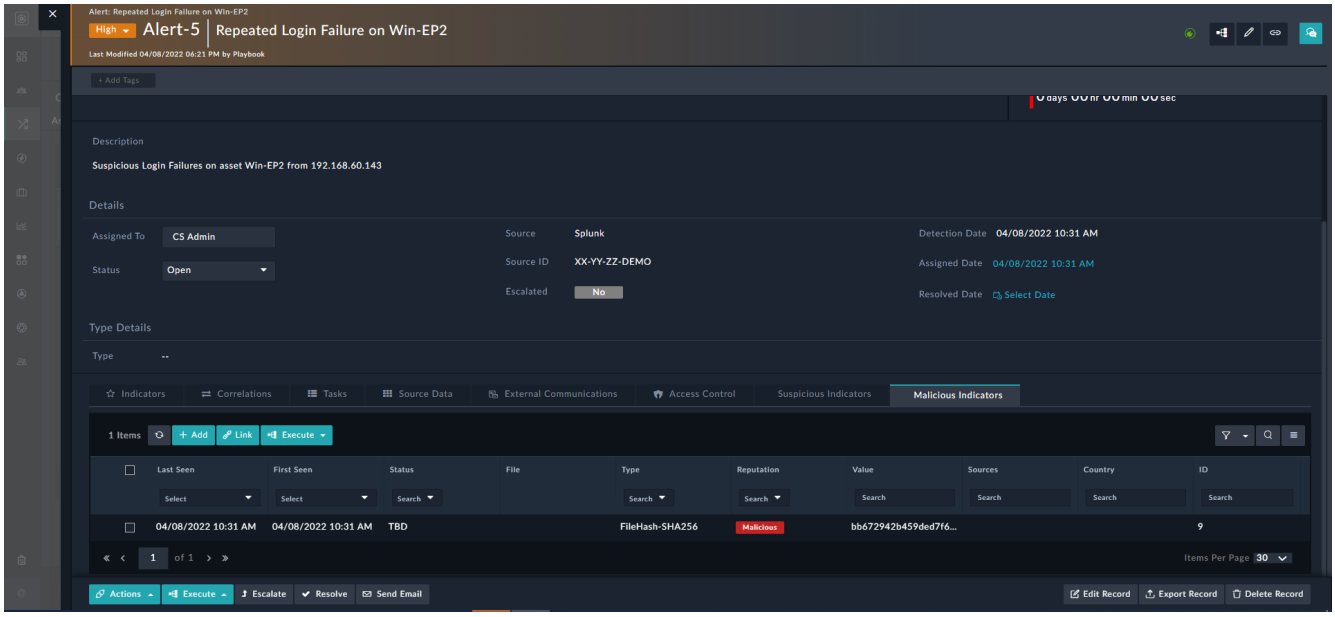
d. Perform steps similar to the above steps for creating the `Reputation is Malicious` filter.



Once you have added these default filters, you will observe that the relationship grid in the Suspicious Indicators tab will contain only those indicators whose reputation is suspicious.



Similarly, you will observe that the relationship grid in the Malicious Indicators tab will contain only those indicators whose reputation is malicious.



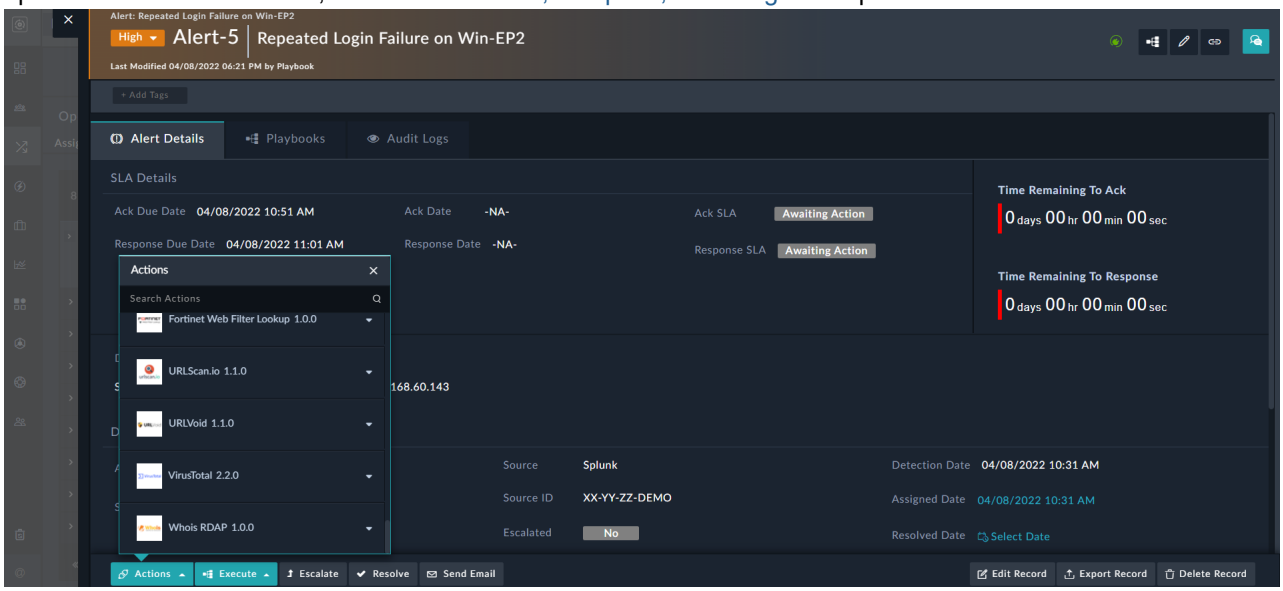
Invoking connector actions directly on a record

You can invoke connector actions directly in the detail view of a record and investigate the alert without the need of writing a playbook.

To run connector actions on the record, you must be assigned a role that contains `Read` and `Execute` permissions on the "Connectors" module. Also, if the connector action has roles defined for its execution, then the roles of the logged in user will be matched against the roles permitted for the action, and if the roles match, then the user can execute that particular action.

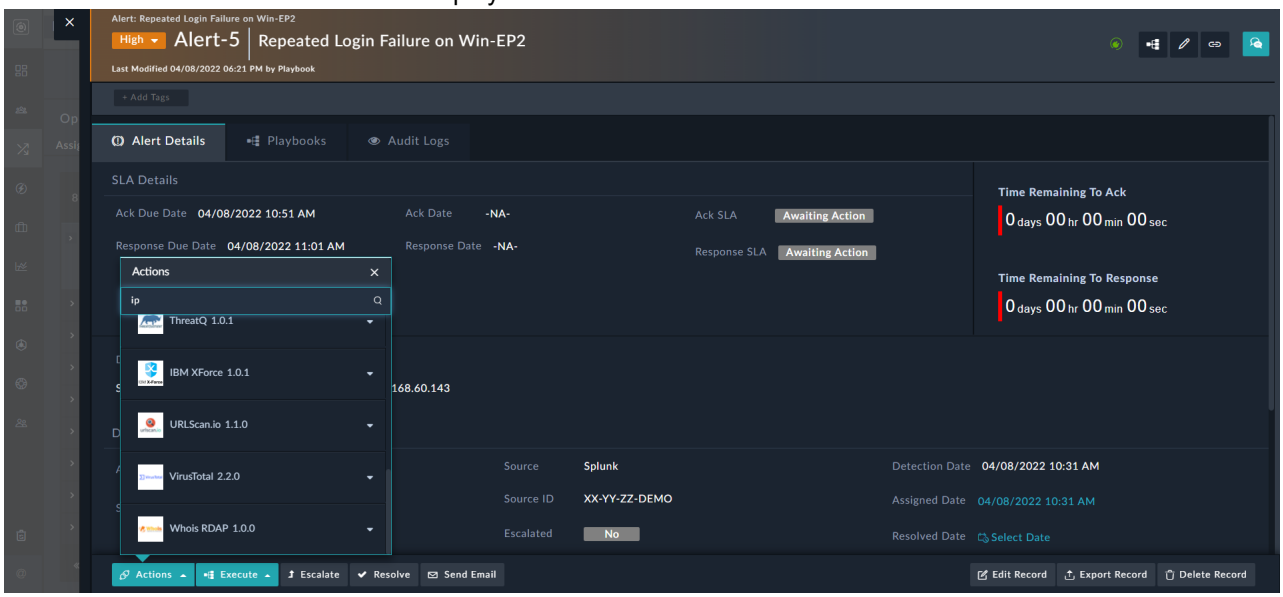
For example, if want to retrieve the reputation of a source IP address in an alert from a threat intelligence tool such as VirusTotal, you can do the following:

1. Open the detail view of the alert record on which you want to run the connector action.
2. Click the **Actions** button.
   You will see the Actions button, if the **Show Action Execution Panel** checkbox is selected, which is the default option. For more information, see the Dashboard, Template, and Widgets chapter.

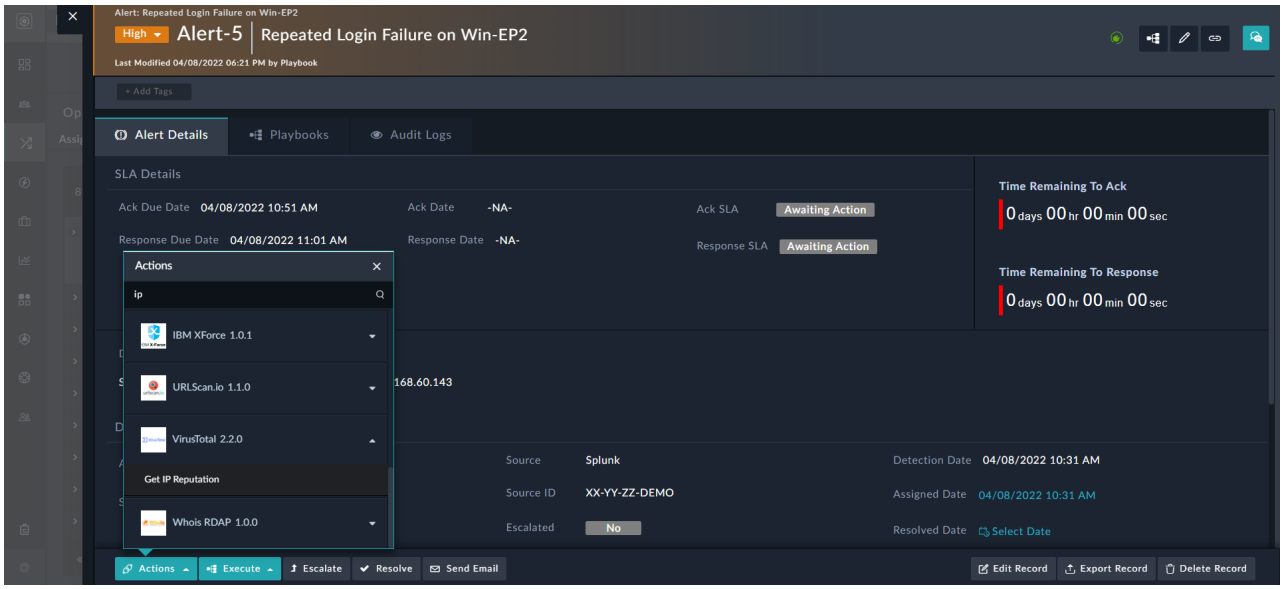


Note: The **Actions** list only displays the active and installed connectors.

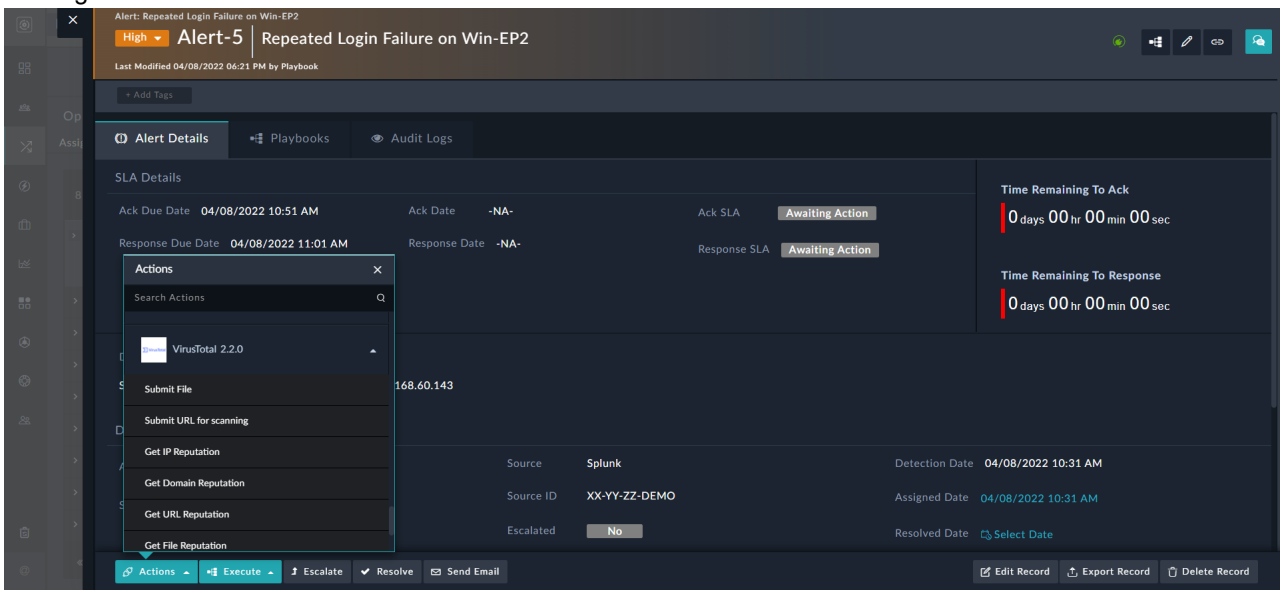
3. Search for actions that you want to perform using the **Search Action** box. For example, if you want to search for a reputation of an IP address, then you can type `IP` in the **Search Action** box, and the connectors that have any action related to an IP address will be displayed:



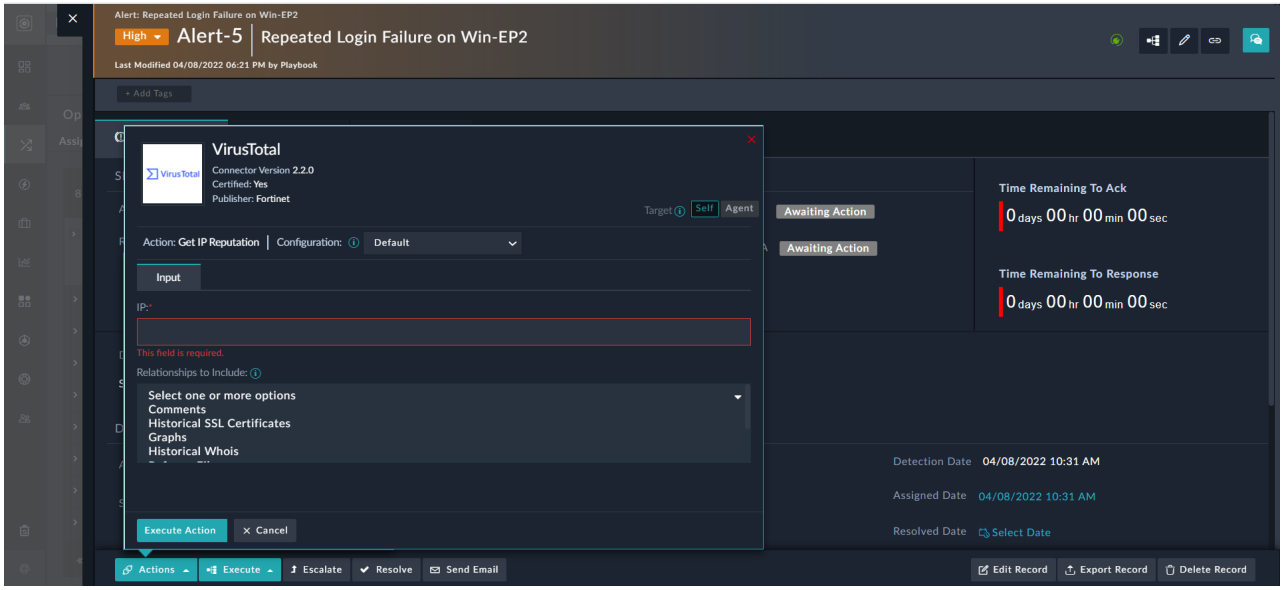
As shown in the above image, VirusTotal, IBM XForce, URL Scan.io, etc connectors have "IP" in their actions. Click the down arrow to view the actions associated with IP for each connector. For example, if you click VirusTotal, you will see the "Get IP Reputation" action:



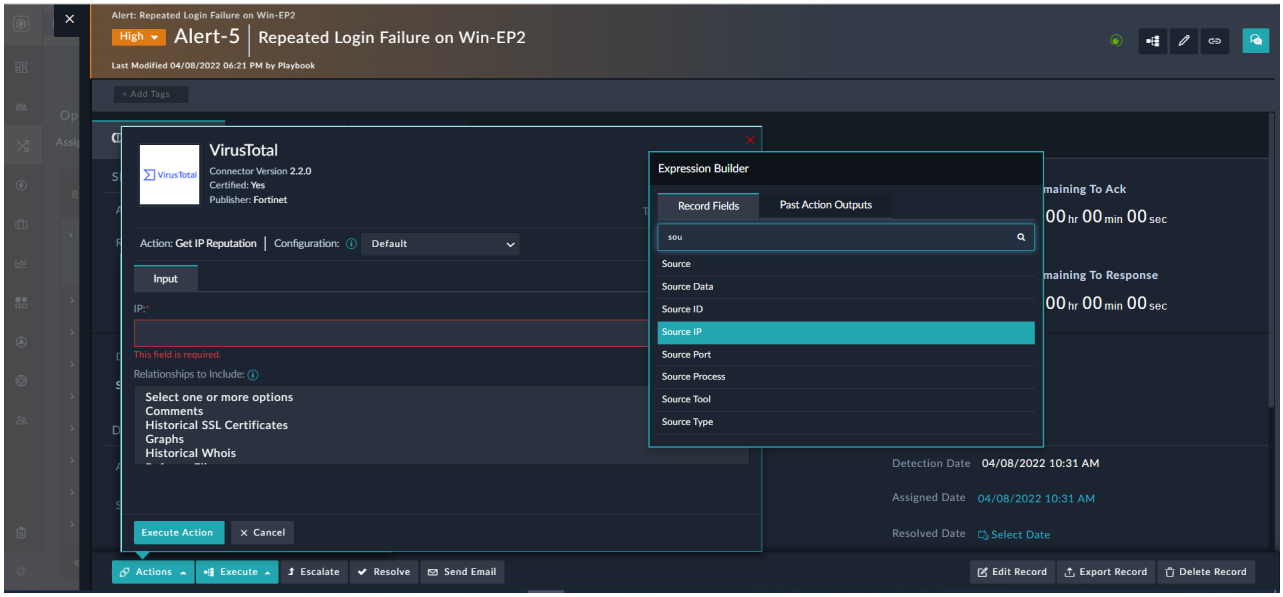
You can also clear the filter and view all the actions associated with a connector by clicking the connector and viewing its actions:



4. Click the action that you want to perform on the alert. For our example, click **Get IP Reputation** (associated with VirusTotal), which displays the VirusTotal dialog. From version 6.4.1 onwards, you are required to specify whether you want to run the direct connector action on the current FortiSOAR node or remotely on the FSR agent node by clicking the **Self** or **Agent** buttons besides `Target`. By default, **Self** is selected, which means that the connector action will run on the current FortiSOAR node, then you must select the configuration using which you want to run the connector action since the FortiSOAR node can have multiple configurations. If you click **Agent**, then you can select the FSR agent on which you want to run the connector action and you must also select the configuration using which you want to run the connector action since FSR agents can have multiple configurations. For more information on FSR agents and how to run direct connector actions using FSR agents, see the *Segmented Network support in FortiSOAR* chapter in the "Administration Guide." For our example, we have chosen **Self**.

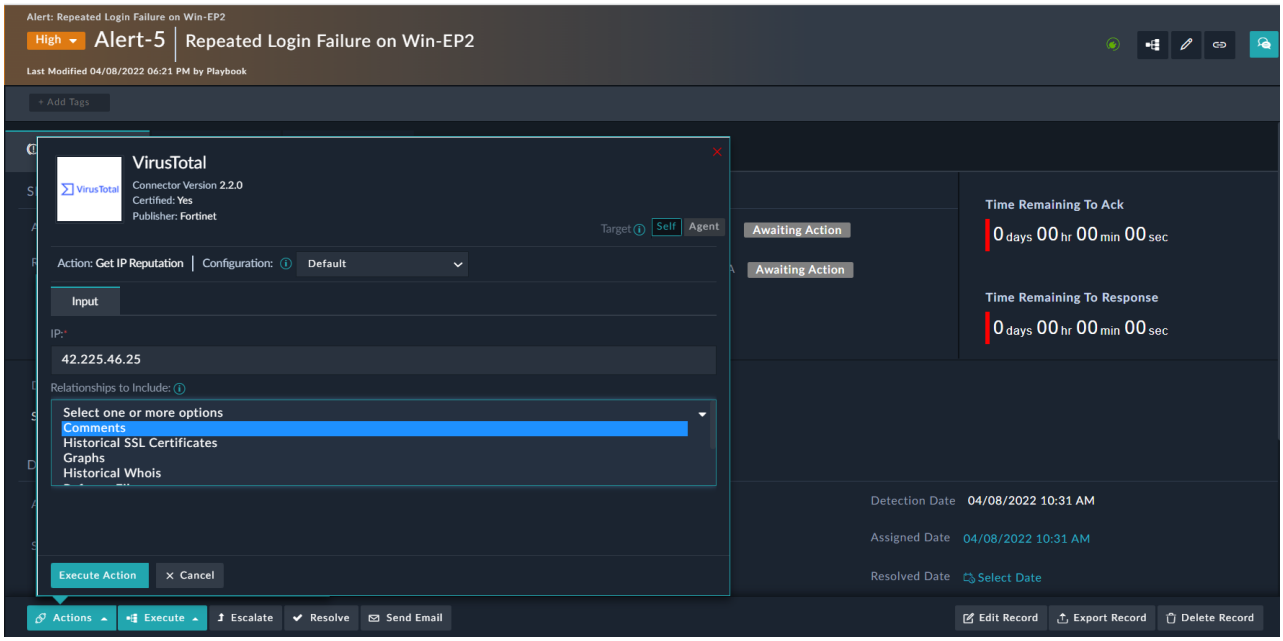


Next, in the Input tab, in the IP field, either enter an IP address or use the value of a record field. For our example, we will use the value of the IP address that is present in the Source IP field. To input the value from a record field, in the `Input` tab, click the **IP** field, which displays an `Expression Builder` dialog. On the **Record Fields** tab, select or search for the record field, using the **Search Fields** box, that you want to add as the input to the connector action. For our example, select Source IP:

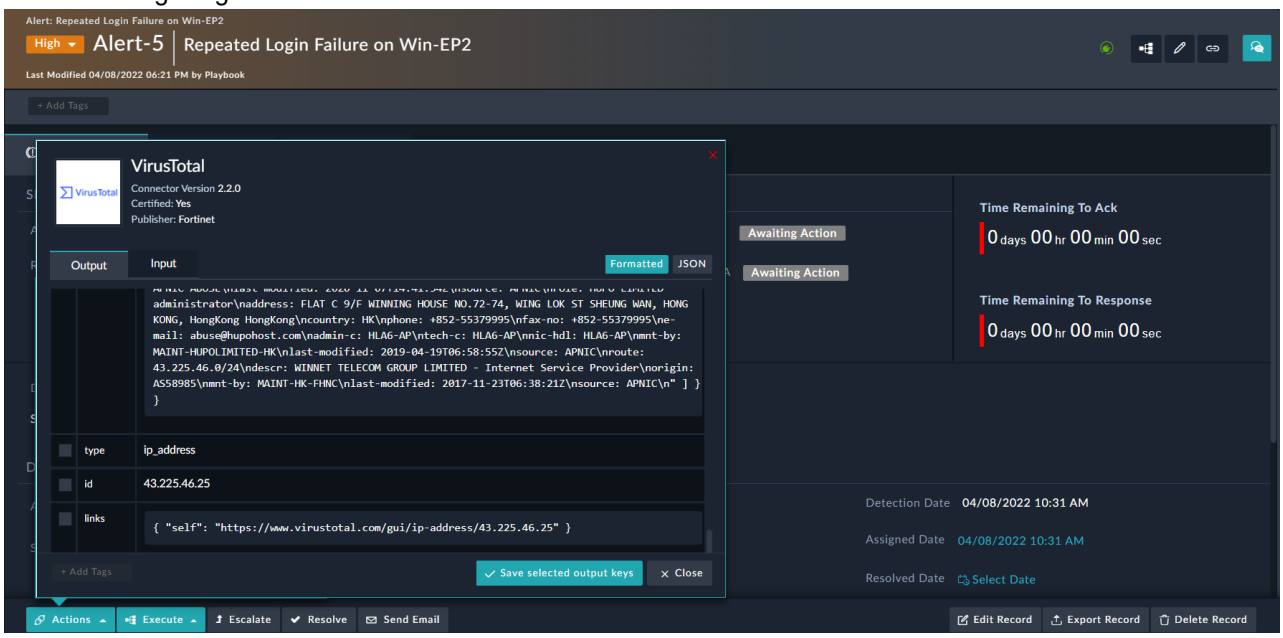


From the **Relationships to Include** list, you can also select the relationships such as Comments, Graphs, etc that you want to include in the output.

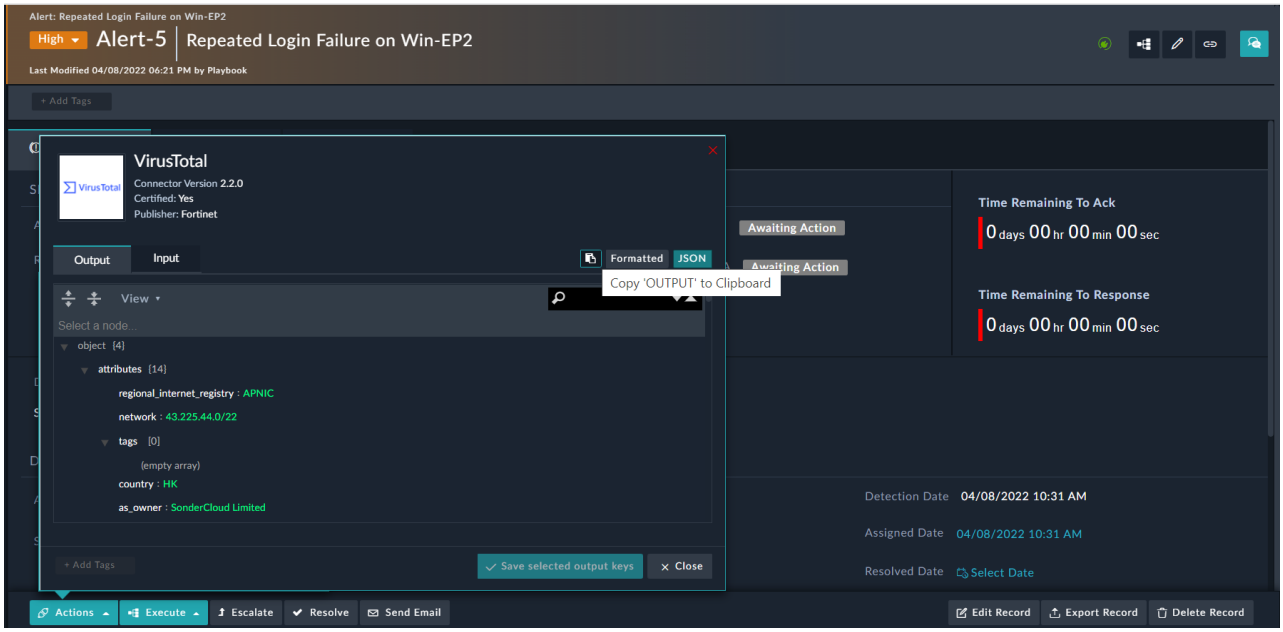
5. To run the connector action, click **Execute Action**.



6. Once the connector action is executed, you can see the formatted output of the action, in a tabular format, as shown in the following image:

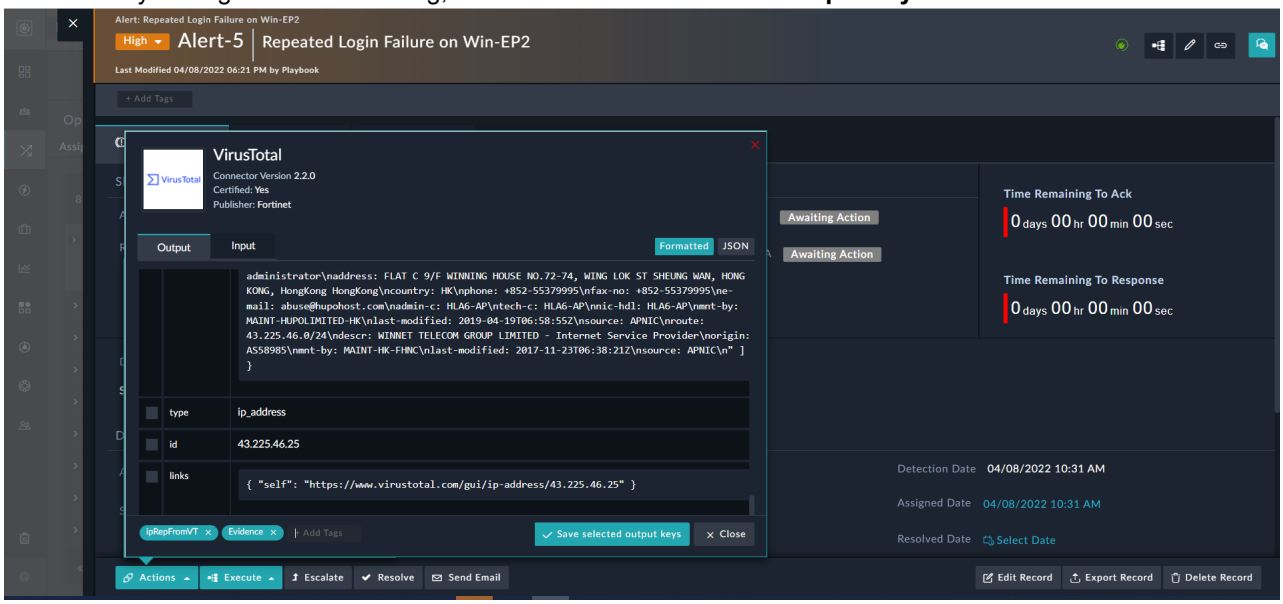


You can also view the output and in the JSON format:

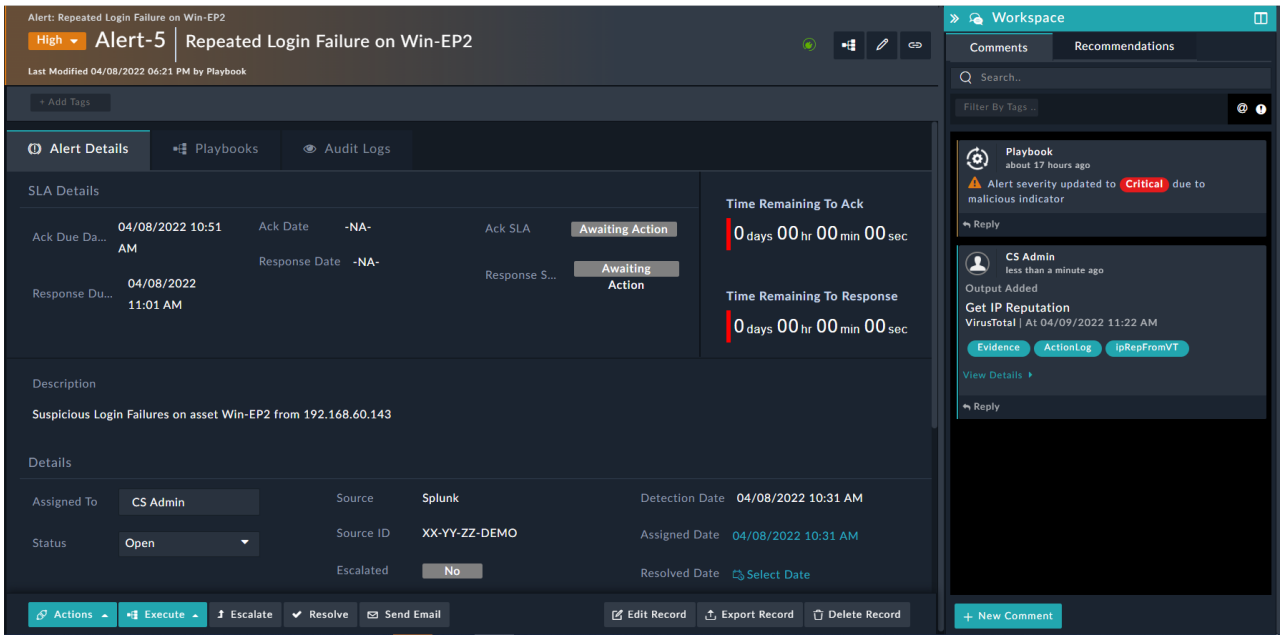


You can also copy the output to the clipboard.

Select the output keys that you want to save, for example **attributes**. You can also add tags such as `Evidence` to the results making it easy for you to search for and filter the outputs. For example, you can add a tag `ipRepFromVT` to mark that the reputation of the specified IP address is got from VirusTotal, and also mark this action log as 'Evidence' by adding the `Evidence` tag, and then click **Save selected output keys**.

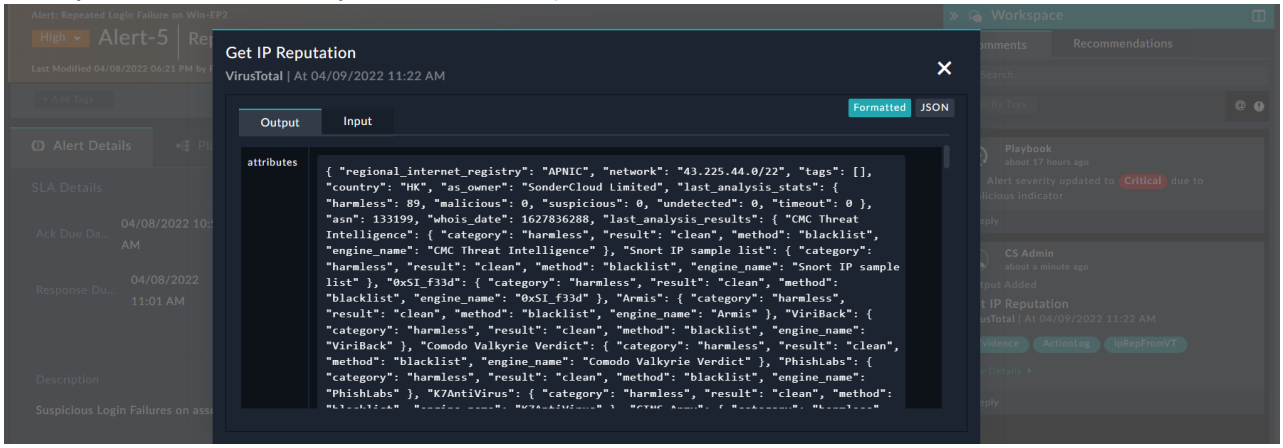


The output keys get saved as **Action Log** in the **Comments** tab in the Workspace section:

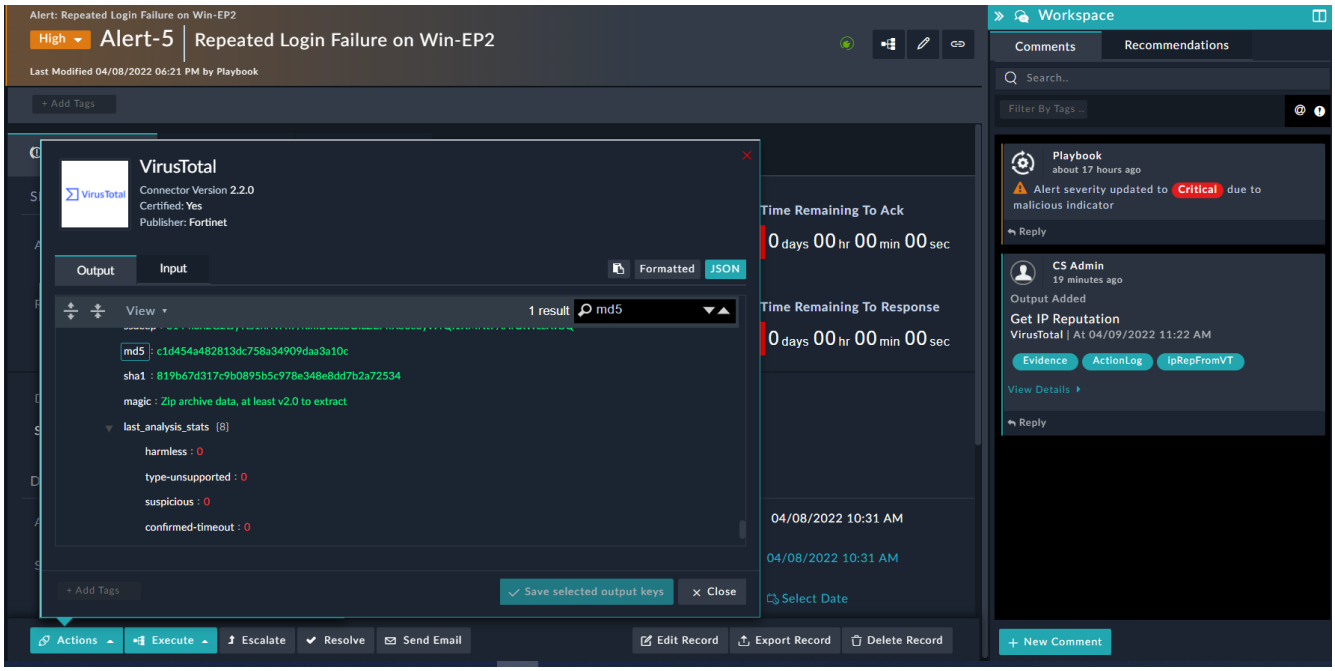


Also, since we also added a tag to the output, you can see the **ipRepFromVT** and **Evidence** tags added to the entry in the Comments tab.

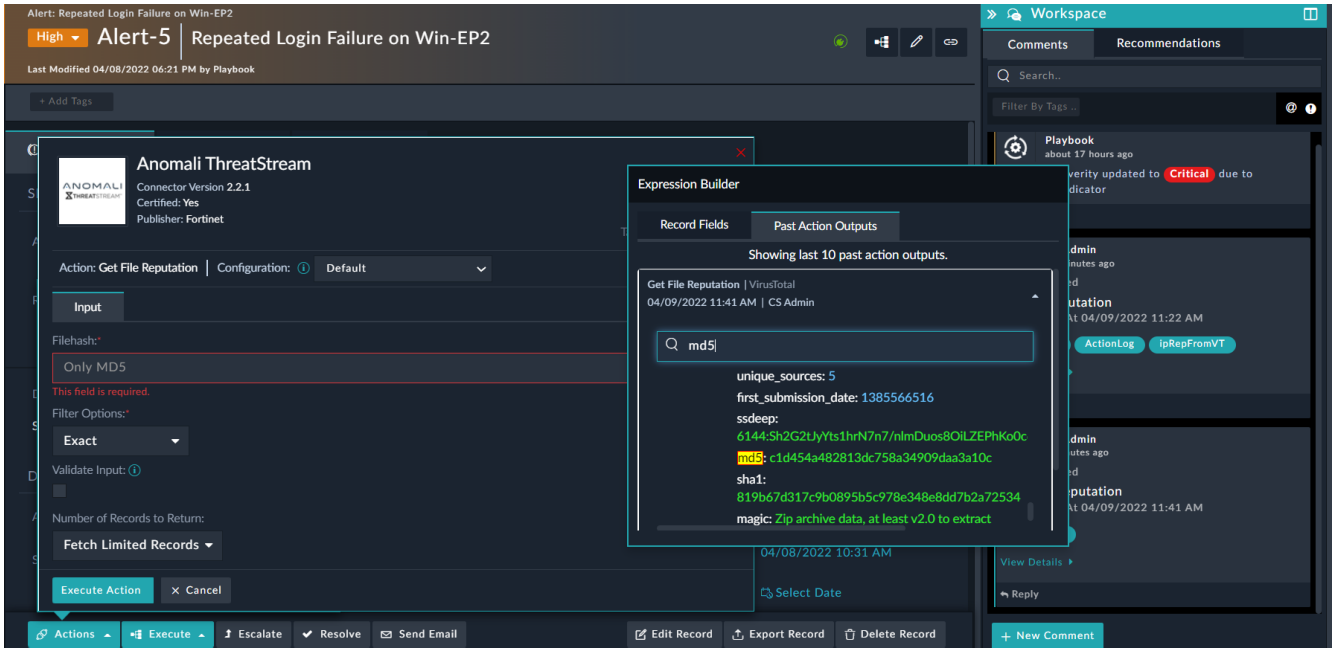
When you click **View Details**, you can see the output that has been saved:



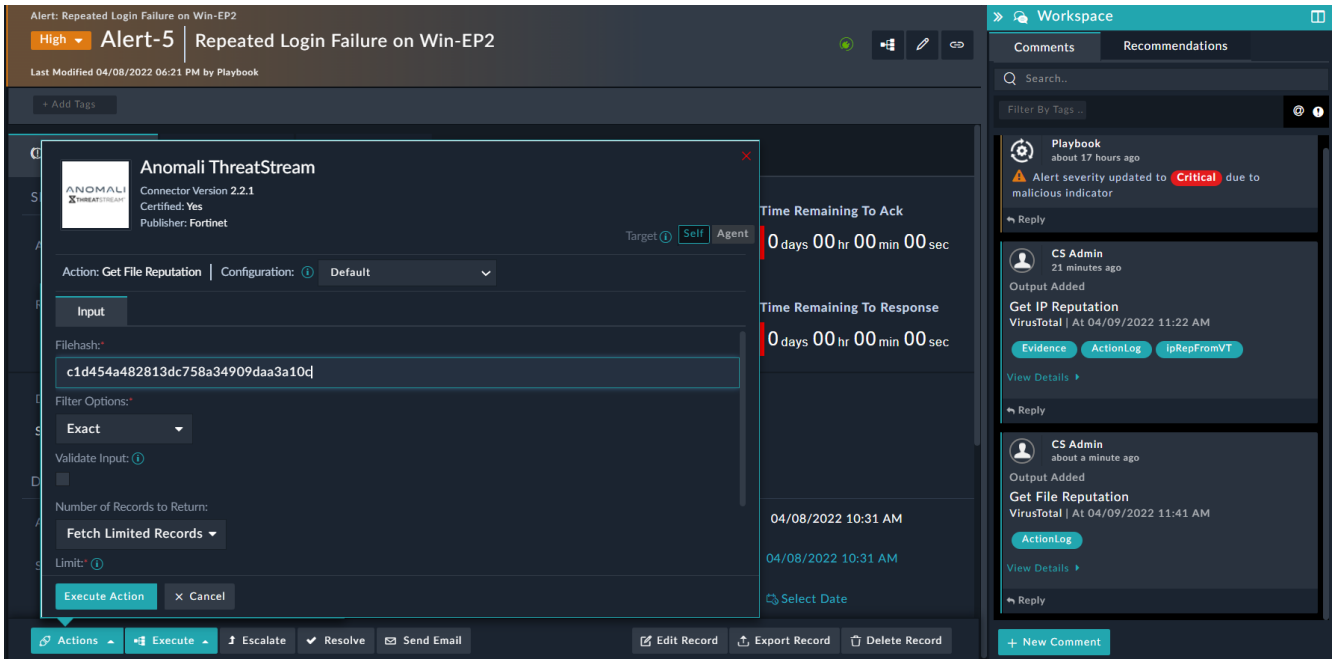
You can also consume the saved output for past connector actions as an input to another connector action within the record. For example, you want to get the reputation of a filehash using the Anomali ThreatStream connector, which supports only the MD5 as a filehash value and you have only the SHA256 value. In this case, you can extract and save the MD5 value from a filehash using the **Get File Reputation** action in VirusTotal:



Then, you can use the saved MD5 value to get the reputation of this filehash from Anomali ThreatStream, by clicking the **Actions** button and selecting the **Get File Reputation** action from the Anomali ThreatStream. In the **Input** tab, click the **Filehash** field, which displays the `Expression Builder`. Click the **Past Action Outputs** tab, where you can view the saved output of the past 10 actions. Select the action whose output you want to consume, in our example, choose the Get File Reputation action (from VirusTotal) and select or search for the parameter ("md5") that you add to the field:



To run the action on the record and retrieve the reputation of the MD5 filehash from Anomali ThreatStream, click **Execute Action**:



You can then check the output of the connector action and further perform actions as described earlier, including adding output keys to the action log and adding tags for future processing.

Using record similarity

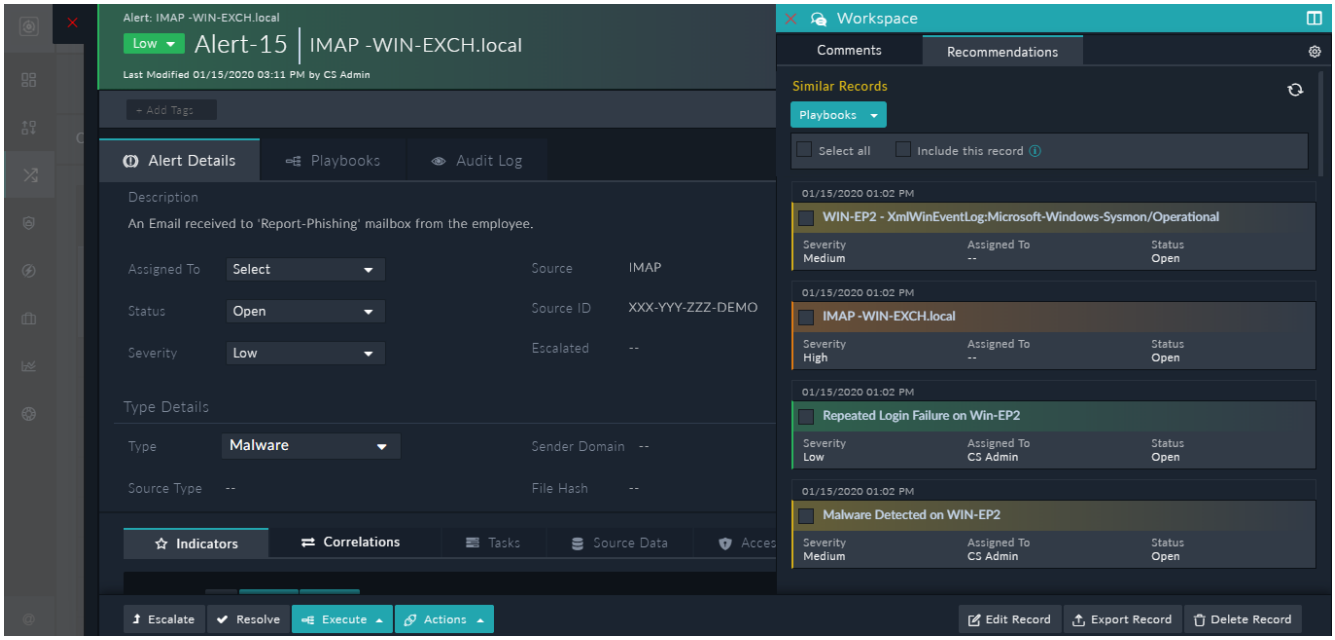
FortiSOAR displays records that are similar to the record on which you are working. For example, FortiSOAR will display alerts that contain similar file hashes, source IP, domains, etc. based on the similarity criteria you have defined.

A scenario where analysts can use this feature would be the case of a Phishing alert being created in FortiSOAR from your Email Gateway. Users might click the URLs which in turn will create multiple Malware alerts from your SIEM (or Endpoint Detection Response tools). Therefore, a single event, i.e., a Phishing email generates alerts of different types (Malware, Policy Violation, Suspicious Email, etc) in FortiSOAR. Since FortiSOAR displays similar alerts to the alert an analyst is working on, it provides the analyst the complete picture of the event and makes it easier for the analyst to take remedial action.

The Recommendation Panel can be enabled and configured with default criteria if the **Enable Recommendation Panel** checkbox is checked in the template of a module. For more information, see the Dashboards, Templates, and Widgets chapter

From version 7.0.0 onwards, two strategies are supported by FortiSOAR: Elasticsearch Based Text Classification (*default*) and Machine Learning Based Clustering for the similarity feature. For more information on these strategies, see the 'Recommendation Engine' topic in the *Application Editor* chapter in the "Administration Guide."
Also, note soft-deleted records, i.e., records in the recycle bin, will not be visible in the similarity results; immediately in the case of Elasticsearch Based Text Classification and after re-training the data in case of Machine Learning Based Clustering. For more information on the recycle bin, see the *Recycle Bin* chapter in the "Administration Guide."

Administrators define the similarity criteria based on which the **Recommendation** pane displays similar alerts. For example, administrators can define similarity criteria is based on the source and indicators of the alert. Therefore, alerts whose source or indicators, such as domains, IP addresses, URLs, etc., match the source or indicators of the alert record on which you are working get displayed in the `Similar Records` list:



As seen in the image above, the alerts that match the "Indicator" criteria (which are `gumblar.cn`, `http://ghari.pk`, etc.) are displayed first and then the alerts that match the "Source" criteria (which is IMAP), since the settings are such that the indicator criteria have been given greater weight than the source criteria.

The **Playbooks** drop-down list displays the list of playbooks that you had specified while configuring the recommendation settings. In our example, we had selected the `Indicator Evaluation` playbook, which gets displayed in the Playbooks drop-down list. You can select a similar record or click **Select All** to select all the similar records, and then click Indicator Evaluation to execute the playbook on that record(s). To execute the `Indicator Evaluation` playbook on the current (parent) record also, i.e., `Alert 15...` in the above image, select **Include this record** checkbox. Therefore, you can choose to execute the selected playbook on the current record as well as the selected similar record(s).

You might also want to perform an action, for example, *Resolve*, on similar alerts (records) but you do not want to resolve the current (parent) record, i.e., `Alert 15...`. However, you do want to link the similar records to the parent record, then in the `Resolve Alert` playbook, which is present in **Playbooks > 08 - Escalation** playbook collection, open the "Update Record" step and in the **Alerts** field (under `Correlations` section), enter `vars.request.data.__parentId`. This is also useful if you want to resolve duplicate records and keep only the parent record open.

Predicting values of field values in a record

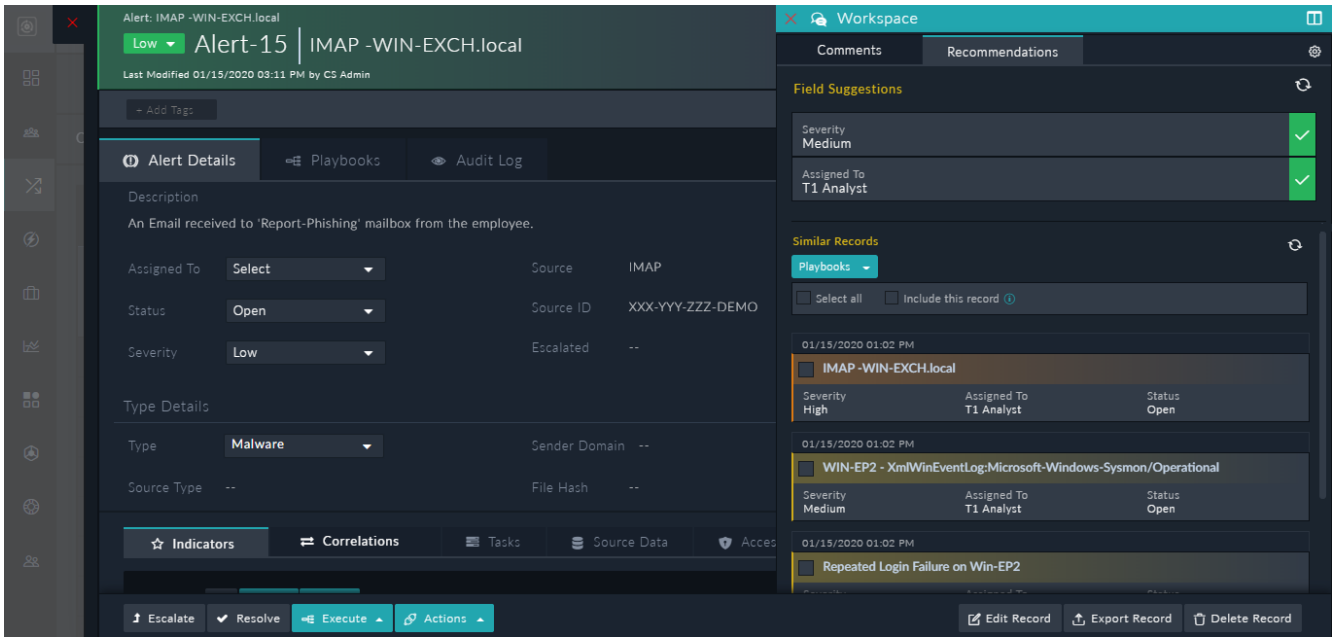
FortiSOAR predicts values of fields of your choice within a record from the values of fields of existing records based on the criteria you have defined, making it easier for analysts to make informed decisions.

A scenario where analysts can use this feature would be the case of an alert, where you want FortiSOAR to predict the severity and assign the alert to a particular user, based on matching the alert's indicators and type.

From version 7.0.0 onwards, two recommendation strategies are supported by FortiSOAR: Elasticsearch Based Text Classification (*default*) and Machine Learning Based Clustering. For more information on these strategies, see the 'Recommendation Engine' topic in the *Application Editor* chapter in the "Administration Guide."

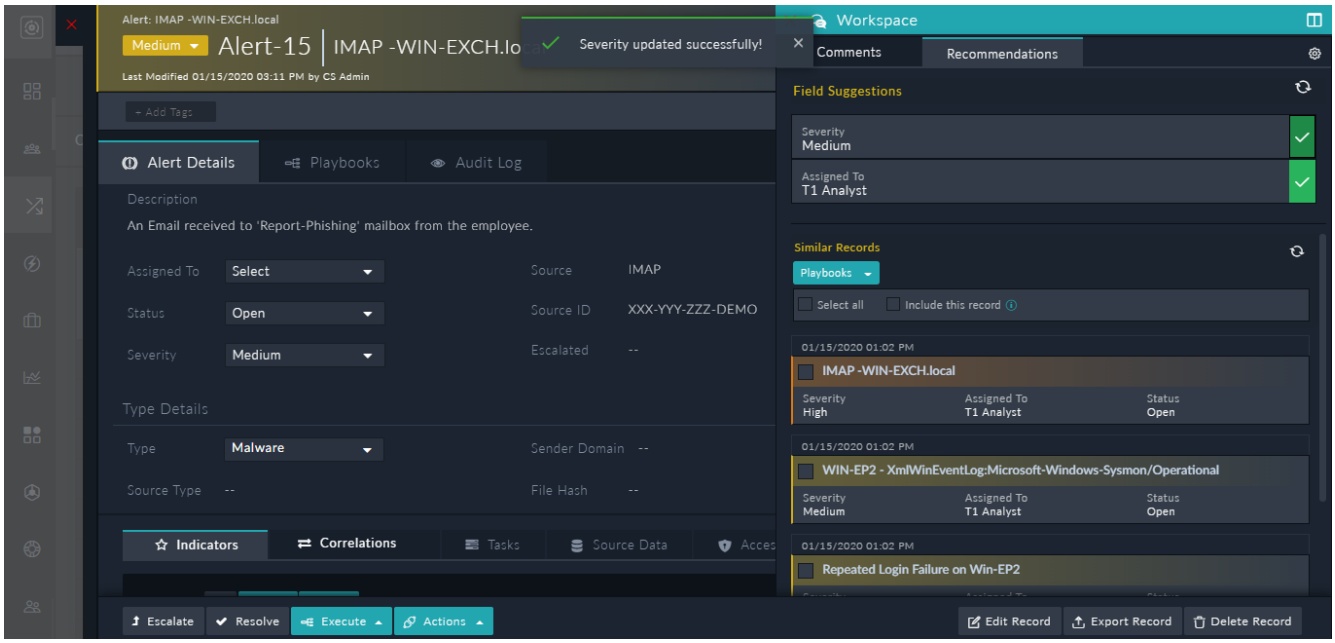
Also, note that the recycle bin data is not visible in the results displayed by the recommendation engines; immediately in case of Elasticsearch Based Text Classification and after re-training the data in case of Machine Learning Based Clustering. For more information on the recycle bin, see the *Recycle Bin* chapter in the "Administration Guide."

Administrators define the field suggestions criteria based on which the **Recommendation** pane displays suggestions for field values. For example, administrators can define that the Severity and Assigned To fields can be predicted from the Type and Indicators fields. Based on the prediction criteria that has been defined, the **Recommendation** pane can display field value suggestions as follows:



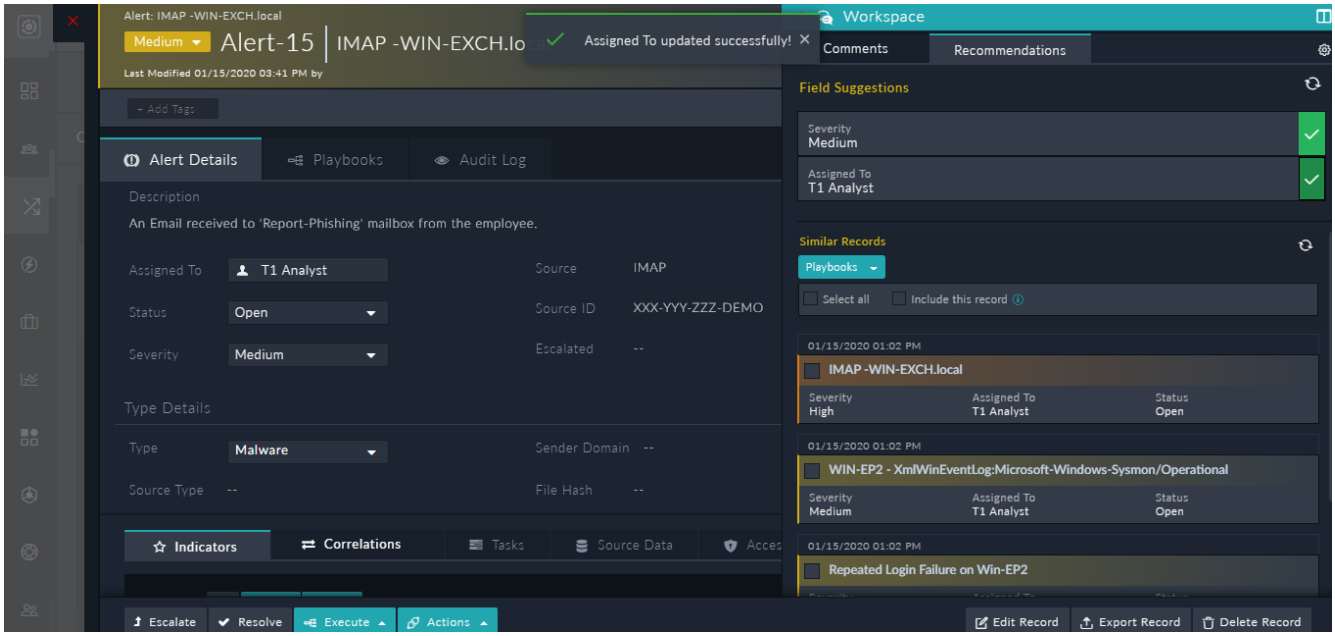
As shown in the above image, FortiSOAR recommends that the severity of the record should be set to "Medium" and the record be assigned to "T1 Analyst". FortiSOAR makes these predictions based on the criteria that the administrators have set, and the ranking that is given to matching records.

If you agree to the suggestions and want to make the change in the record, click the green checkbox in the row of the field, which in turn will update or add the field value in the record. For example, if you want to update the value of the severity of the record to match the suggested similarity, then click the green checkbox in the severity row:



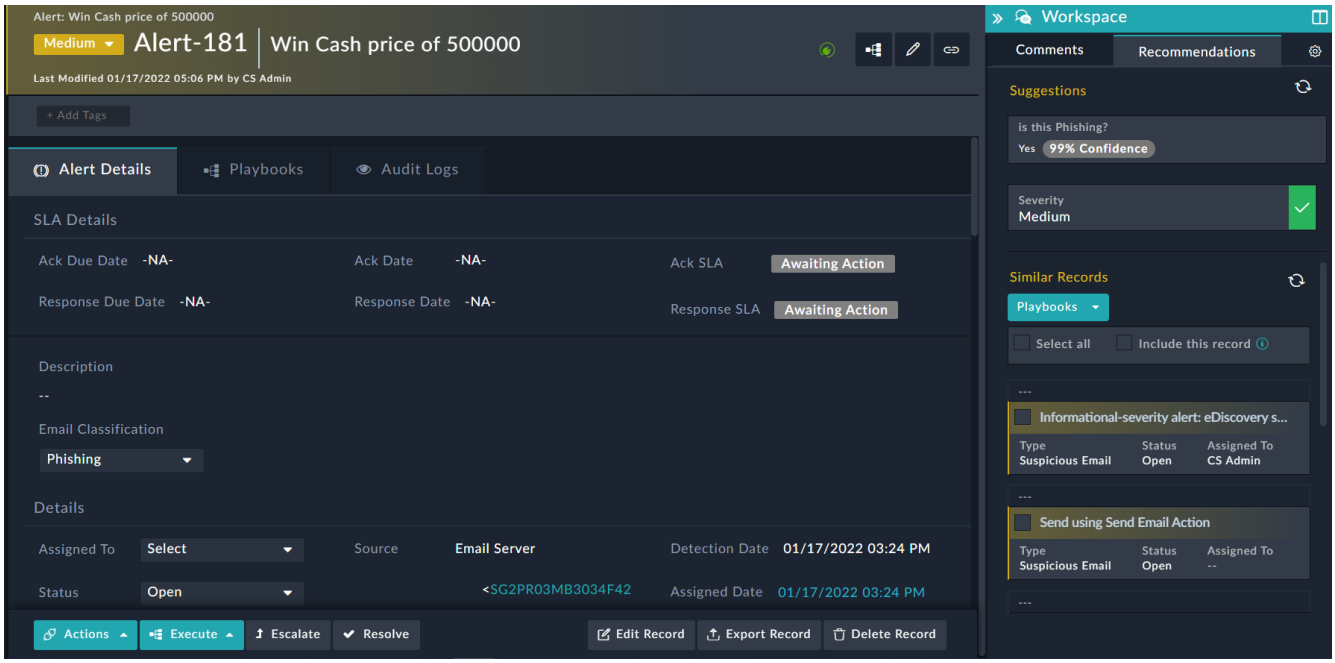
As shown in the above image, once you click the green checkbox, the value of the severity field changes from Low to Medium as per the predicted field value.

Similarly, you can also add T1 Analyst in the Assigned To field:



Viewing Suggestions for Phishing Classifications

From release 7.2.0 onwards, if your administrator has set up the 'Phishing Classification' feature, then in the **Recommendation** tab of the Workspace panel, you can also see suggestions on whether or not an alert record can be classified as a 'Phishing' record as shown in the following image:



You will see a `Suggestion` section with contains the `Is this Phishing?` question followed by the answer to that question and the corresponding confidence level. For example, in the above image, the answer to the `Is this Phishing?` question is `Yes`, with `99%` confidence that it is a phishing email (record). You will also see that the Email Classification drop-down list has been set to 'Phishing'. Using this suggestion and its corresponding confidence value it becomes easy for you to classify records into 'Phishing' and 'Non Phishing' and accordingly proceed with the investigation process.

If you have installed and configured the Phishing Classifier connector on an agent node, and not on the FortiSOAR (base) node, then suggestions are not displayed in the **Recommendations** tab on the `Workspace` pane; however, you can use the agent configuration in connector actions in playbooks to get predictions.

Queue and Shift Management

Queues provide managers a view that answers questions like, "what are my resources working on currently?", "how many tasks are pending?", and "do any tasks require reallocation?". Queues provide users a view that answers questions like "what is my work?", "how much of my work is pending?", and "what is the priority of my tasks?".

Using Queues and Shifts you can automatically assign records to users within a particular queue. For assignment automation, queues and shifts can be explained as follows:

Queues:

- A list of records assigned using the criteria you have defined.
- When a record is added to a queue, it is also assigned to a user based on the criteria that you have set for assignment of records.

Shifts:

- A set of users available for assignment at certain times of the day and certain days of the week.
- Records are not assigned to a shift rather, they are assigned to individual users using queues but, with the requirement that the users must be on shift.

It is highly recommended that you use the 'Assignment' feature in place of queue management, which has been deprecated from release 7.2.0. The legacy queue management page has been deprecated as automated record assignments were not supported in Queue Management.

In release 7.2.0, automation has been added as a central function of queue and shift management to include the ability to auto-assign the following:

- New records to queue based on custom filters such as type, severity, etc you have defined.
- Records to individual users within a queue using methods such as round-robin or to queue or shift leaders.
- Records to new assignees based on shift changes (shift handover) or other criteria such as how long the record has remained open, etc.

A queue leader is any active user or queue member to whom records can assign records. Any active user, even those who do not have permissions on queues and shifts, can be added as queue members or queue leaders for default assignment of records.

Permissions required for working with queues and shifts

- To manage with queues and shifts you must have `Create`, `Read`, `Update`, and `Delete` permissions on the `Queues` and `Shifts` modules, and `Read` permission on the `People` module.
- To view queues and shifts you must have `Read` permission on the `Queues`, `Shifts`, and `People` modules.
- Any team that is added as an owner of the queue, must be linked to appliance "Playbook". If not, queue assignment will not work for that team.

Prerequisites to automating assignments

Before you can automate assignments and use queue and shift management, you must ensure that the module whose records you want to auto-assign using queues is 'Queueable', i.e., while creating or configuring queues, the module must be displayed as an option for auto-assignment.

By default, the 'Alerts', 'Incidents', and 'Task' modules are 'Queueable'.

To use queue and shift management, follow the given steps to make a module 'Queueable'. In the following example, we are making the 'Events' module 'Queueable'

1. User must be assigned the role that has `Create`, `Read`, `Update`, and `Delete` (`CRUD`) permissions on the `Application` module.
2. Click **Settings** and click **Modules** in the `Application Editor` section, to open the Module Editor.
3. On the `Modules` > `Summary` page, from the **Select a module to edit or create a new module** drop-down list, select the module that you want to make queueable.
   For example, select **Events**.
4. In the `Additional Setting` section, select **Queueable**.
5. Click **Save** and **Publish** the module.
   Once the module has been published, you can associate records of the **Events** module with queues.

Managing queues and shifts

To automate assignments, you have to create queues and generate shifts.

Creating Queues

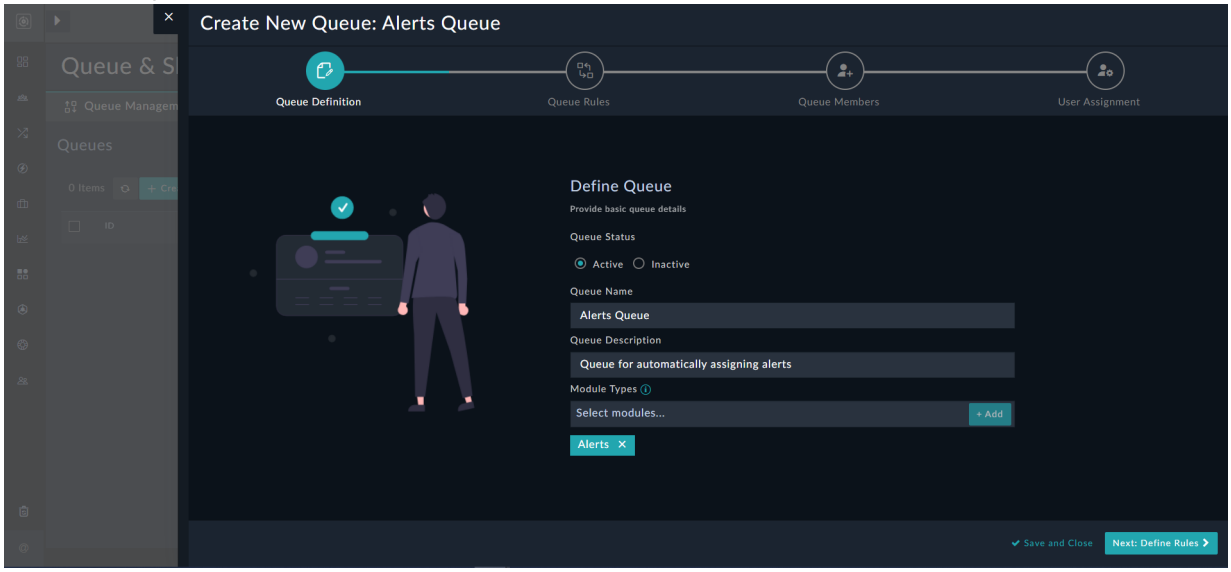
Permissions required for creating queues:

- User must be assigned the role that has `Create`, `Read`, `Update`, and `Delete` (CRUD) permissions on the `Queues` module and at the minimum `Read` permissions on the `Applications` module.
- Appropriate permissions to any module whose records you want to associate with queue must be added to the 'Playbook' appliance for queues to work on that module. For example, if you have a custom module, 'CustModule1', then ensure that you assign a role with appropriate permissions on 'CustModule1' to the 'Playbook Appliance'.
- In addition to the above permissions, it is also good to have `Read` permissions on the `Security` module as then it becomes possible to add teams as queue owners, and then add the whole team as a shift or queue member all at once.

To create queues, do the following:

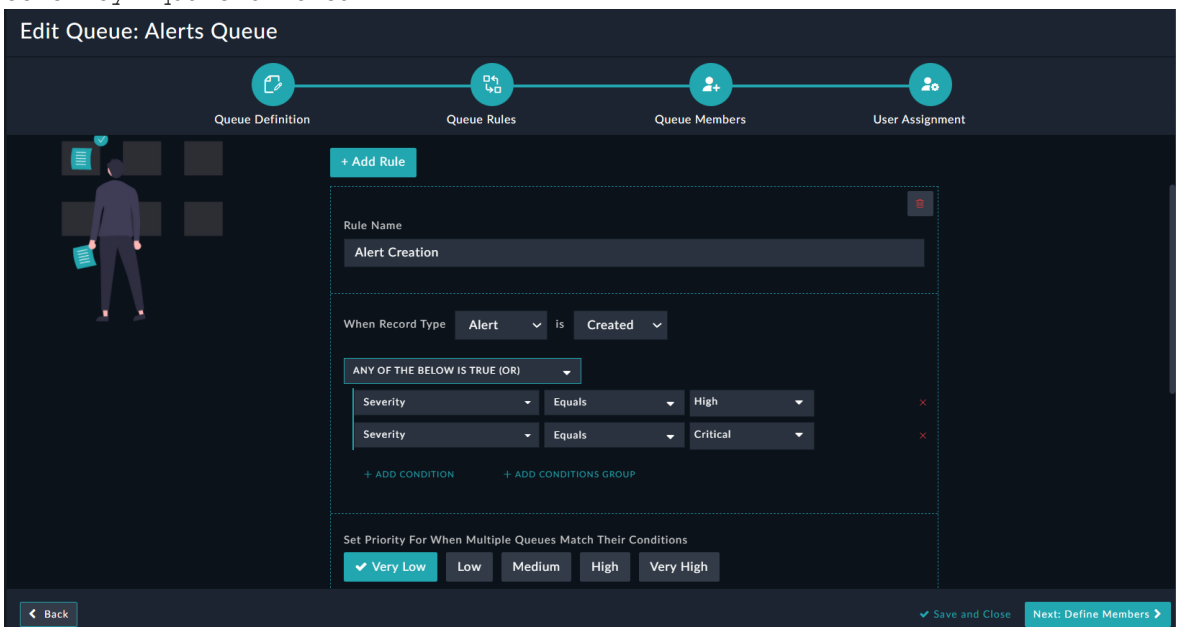
1. Click **Queues & Shift Management** in the left navigation bar to open the `Queue & Shift Management` page.
2. To create a new queue, click **Create New Queue** to open the `Create New Queue Wizard`.

3. In the `Create New Queue Wizard`, on the `Queue Definition` screen, define the queue:
   a. To create the queue in the 'Active' state, ensure that **Active** is selected for **Queue Status**.
   b. In the **Queue Name** field, enter a name that describes the queue. For example, if you are creating a queue for automatic assignment of alert records, then you can name the queue as '`Alerts Queue`.'
   c. In the **Queue Description** field, enter the description of the queue. For our example, you can enter `Queue for automatically assigning alerts.`
   d. From the **Module Types** list, select the modules whose records you want to associate with this queue.
   Note: Only modules that are marked as Queueable will be listed in this drop-down list. By default, the 'Alerts', 'Incidents', and 'Tasks' are marked as 'Queueable.'
   For our example, select **Alerts** and then click **Add:**



   e. Once you have completed providing the basic details for the queue, click **Next: Define Rules**.
4. On the `Define Queue Rules` screen, define the rules for adding records to this queue.
   To add a rule, click **Add Rule**, which displays a Rule Block:
   a. In the **Rule Name** field, enter a name that describes the rule. For example, if you want to assign only High and Critical alerts to this queue, then you can name the rule as '`Rule for High and Critical Alerts`.'
   b. From **When Record Type** list, select the record type to associate with the queue. For our example, since we have chosen only the 'Alerts' module, only '**Alerts**' is present in the **When Record Type** list.
   By default, rules are added for the 'Creation' action, i.e., when the selected record type, **'Alert' is 'Created'**, they are assigned to the queue.
   c. Define additional criteria to the default rule. For example, if you want to assign only High or Critical Alerts to the queue, then you can define the criteria as:
      i. From the Logical Operation drop-down list, select the **Any of the below is True (OR)** operator.
      ii. Click **Add Condition** and then add the following conditions:
      `Severity Equals High`

`Severity Equals Critical`



d. From the `Set Priority For When Multiple Queues Match Their Conditions` list, select the priority of this queue. By default, it is set to **Very Low**. Priority for queues is useful when a record matches rules of multiple queues, in which case it will be added to queue with highest priority.

e. You can also add more rules for the assignment of records to the queue by clicking **Add Rule** to display a new Rule Block. For example, if you want to assign alerts to this queue when particular fields are updated, do the following:

i. In the **Rule Name** field, enter a name that describes the rule. For example, '`Rule for Updated Alerts`.'

ii. From **When Record Type** list, select the record type to associate with the queue. For our example, since we have chosen only the 'Alerts' module, only '**Alerts**' is present in the **When Record Type** list, and select the action as **Updated** option.

iii. From the **Select Record Fields to Monitor For Updates** list, select the fields, which when updated, should move the records to the queue. For example, select **Severity**, **Type**, and **Response Due Date**.

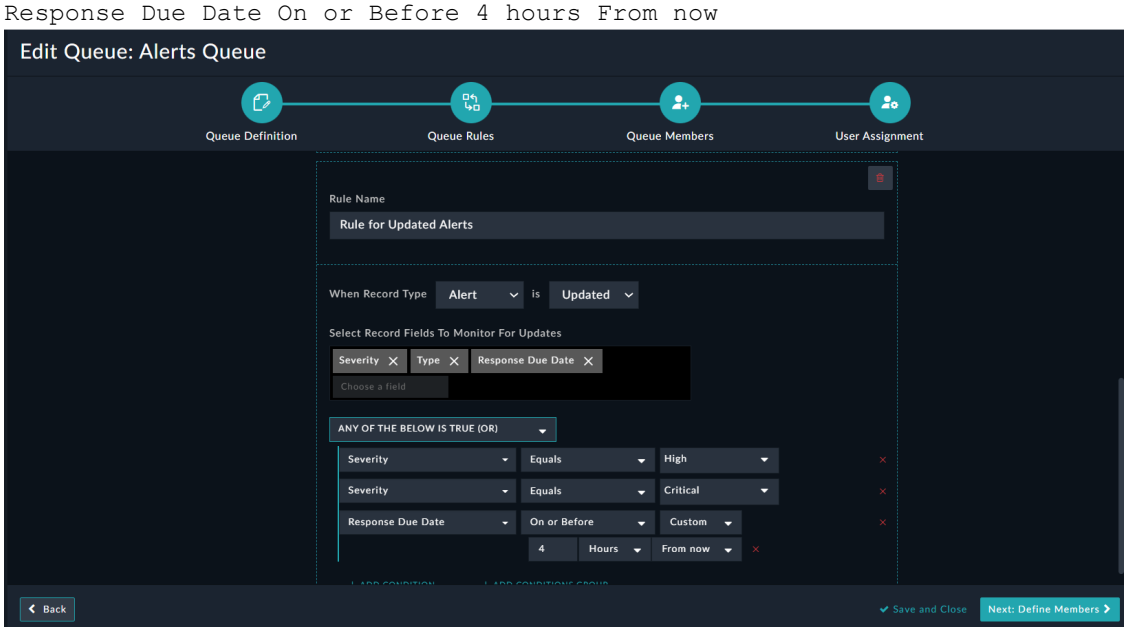
iv. Define the criteria for the assignment of alerts to this queue. For example, if you want to move alerts to this queue only if their severity is updated to high critical or if their response due date is in 4 hours, then add the following criteria:

i. From the Logical Operation drop-down list, select the **Any of the below is True (OR)** operator.

ii. Click **Add Condition** and then add the following conditions:

`Severity Equals High`
`Severity Equals Critical`

`Response Due Date On or Before 4 hours From now`



v. From the `Set Priority For When Multiple Queues Match Their Conditions` list, select the priority of this queue. By default, it is set to **Very Low**. Priority for queues is useful when a record matches rules of multiple queues, in which case it will be added to queue with highest priority.
Similarly, you can define additional rules for the assignment of alerts or other record types such as Incidents to the queue.

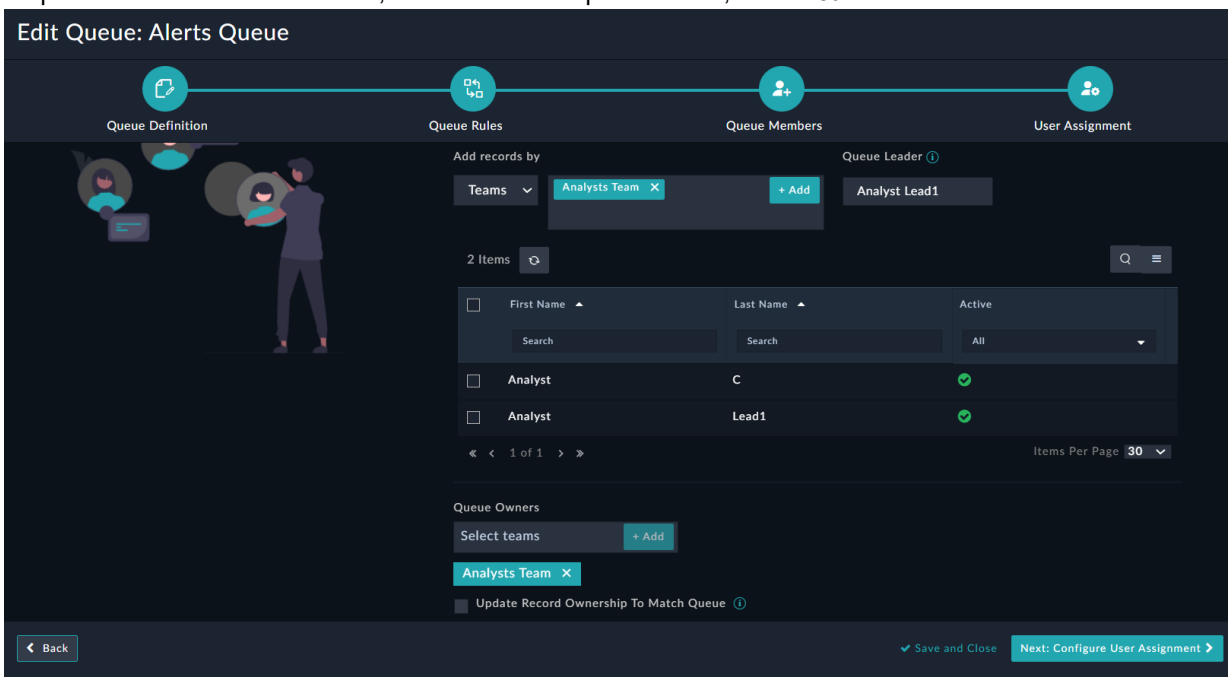
vi. Once you have completed defining rules you can click **Next: Define Members**.

5. On the `Queue Members` screen, select the members and optionally the queue leader of the queue as follows:

   a. In the `Queue Members and Ownership` section, you can choose to add members of the queue as individual Users or add a Team. If you choose to add a team, then all users who are part of that team get added as members of the queue. To add queue members from the **Add records by** drop-down list, select **Users** or **Teams**. Based on your choice, a list of users or teams gets populated in the **Select users** or **Select teams** list. Select the users or teams that you want to add as members to this queue and click **Add**.
   Note: The **Select users** and **Select teams** lists display only active users.
   To remove users, select the users that you want to remove and click **Remove**.

   b. Optionally, from the **Queue Leader** list, you can select the user who you want to assign as a queue leader.
   Note: The queue leader can also be a queue member. To change the queue leader, from the **Queue Leader**

drop-down list select another user, or to remove the queue leader, click **Clear**.

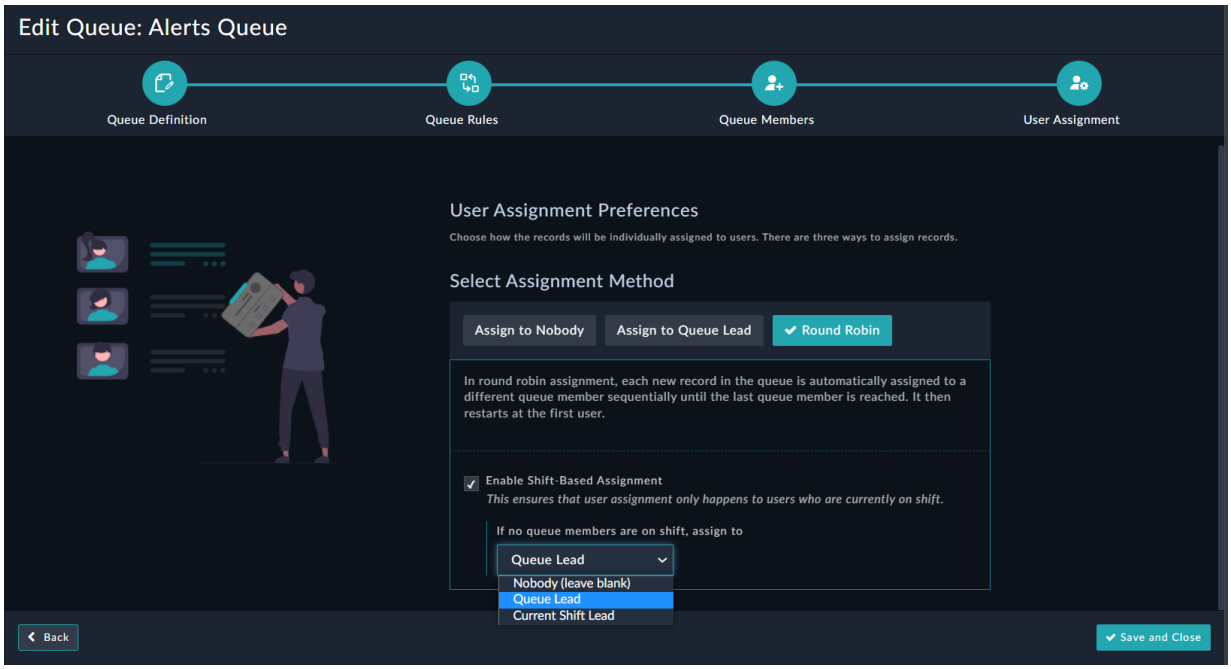


c. Optionally, from the **Queue Owners** list, you can select the teams that you want to assign as the owners of the queue and click **Add**.

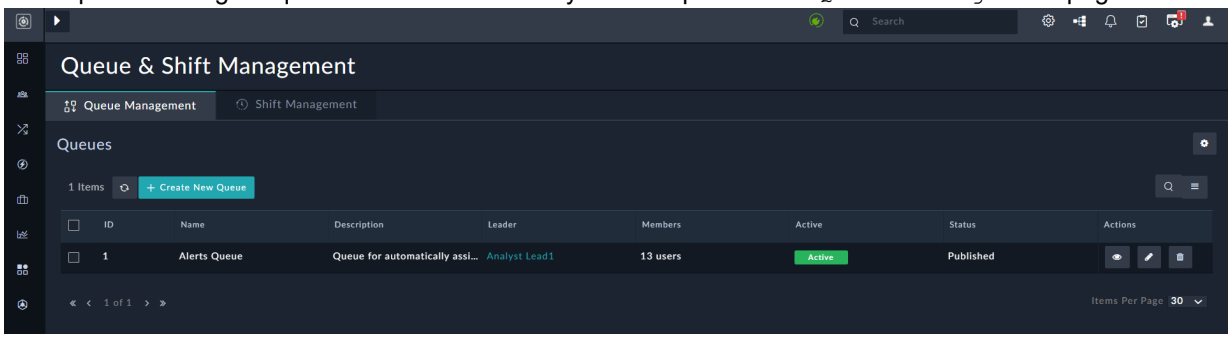
d. Select the **Update Record Ownership To Match Queue** checkbox to add the teams who are associated with the queue as owners of the record, when the record moves to this queue. This ensures that team members can view the records that are assigned to the queue.
Once you have defined queue membership, click **Next: Configure User Assignment**.

6. On the `User Assignment` screen, define how records are to be individually assigned to users. In the `User Assignment Preferences` section, define the following:

a. From the **Assignment Method** drop-down list, choose the method of assignment. You can choose between **Assign to Queue Lead**, **Round Robin**, or **Assign to Nobody**.
Assign to Nobody: Records user assignment field is left blank.
Assign to Queue Lead: Records get assigned to the Queue Lead.
Note: Select the **Enable Shift-Based Round Robin Assignment** checkbox to ensure that records get assigned only to members who are currently on shift. If you select the **Enable Shift-Based Assignment** checkbox, then select the user who would be assigned records if the queue lead is not on shift. You can select between **Nobody (leave blank)** or **Current Shift Lead**.
Round Robin: Each new record in the queue is automatically assigned to different queue members sequentially until the last queue member is reached, and then it restarts with the first member.
Note: Select the **Enable Shift-Based Assignment** checkbox to ensure that records get assigned only to members who are currently on shift. If you select the **Enable Shift-Based Assignment** checkbox, then select the user who would be assigned records if queue members are not on shift. You can select between **Nobody (leave blank)**, **Queue Lead**, or **Current Shift Lead**.



Once you have completed defining how records are to be individually assigned to users click **Save and Close** to complete creating the queue. This adds the newly created queue to the `Queue Management` page:



On the `Queue Management` page, you can view existing queues and also click the **Settings** icon to view or change the queue management settings. You can perform various actions in the queue's record such as:

- To view the details of the queue, including the records assigned to that queue, members of the queue, etc., click the **View** icon.
- To change or edit an existing queue, click the **Edit** icon.
- To delete the queue, click the **Delete** icon.

Queue Management Settings

You can define various settings for queue management including, defining the global criteria for the removal of records from all the queues and how records are displayed in all the queues. To edit queue management settings, do the following:

1. On the `Queue Management` page, click the **Settings** icon ( ) to display the `Queue Management Settings` dialog.
2. On the **Automatic Queue Exit Criteria** tab, you will see the modules whose records you can auto-assign using queues. By default, the 'Alerts', 'Incidents' and 'Tasks' modules are visible. Use this tab to define the criteria for the

removal of records from all the queues of the modules. For our example, we will define the criteria for removing 'Alert' records:

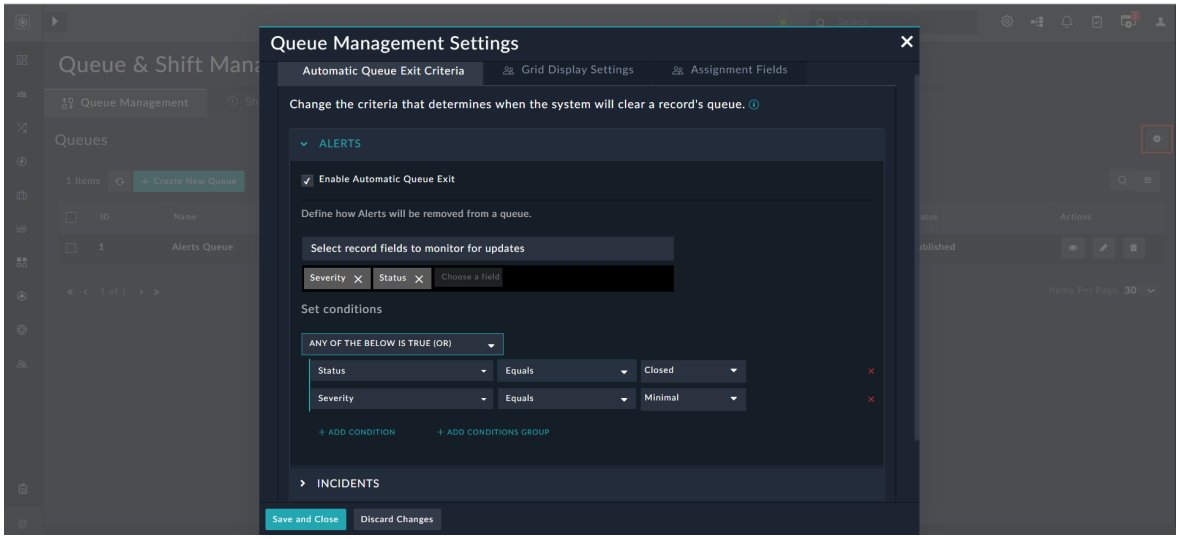
a. In the **Alerts** section, select the **Enable Automatic Queue Exit** checkbox.

b. In the `Define how Alerts will be removed from a queue` section, in the **Select record fields to monitor for updates** field, select the fields, which when updated would remove the alert records from all the queues. For example, select **Status** and **Severity**.

c. In the `Set Conditions` section, add the conditions which when met would automatically remove the record from queues. For example, if you also want to remove alert records from all queues when the Status of the Alert is closed or when their severity is 'Minimal', do the following:

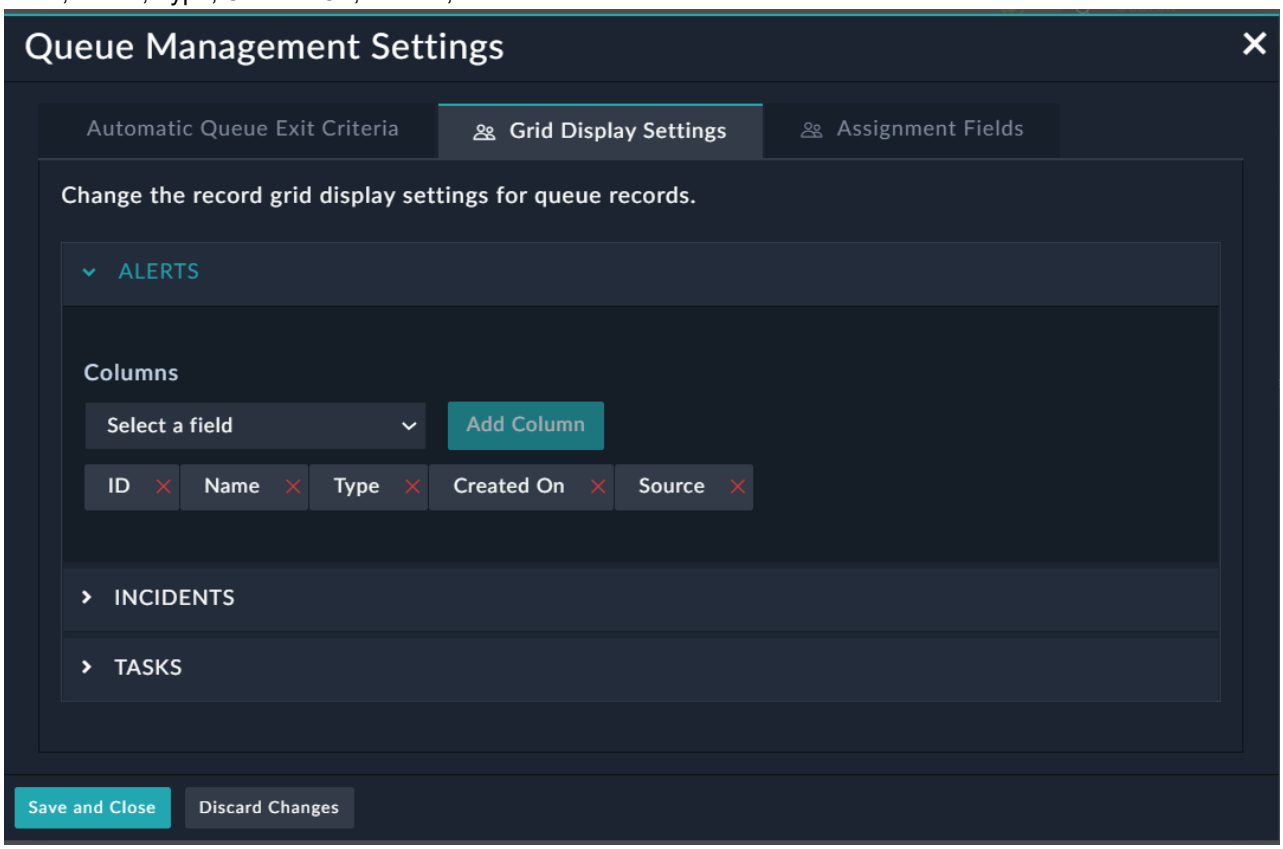
   i. From the Logical Operation drop-down list, retain the selection of **Any of the below is True (OR)** operator.

   ii. Click **Add Condition** and add the following condition:
   `Status Equals Closed`
   `Severity Equals Minimal`



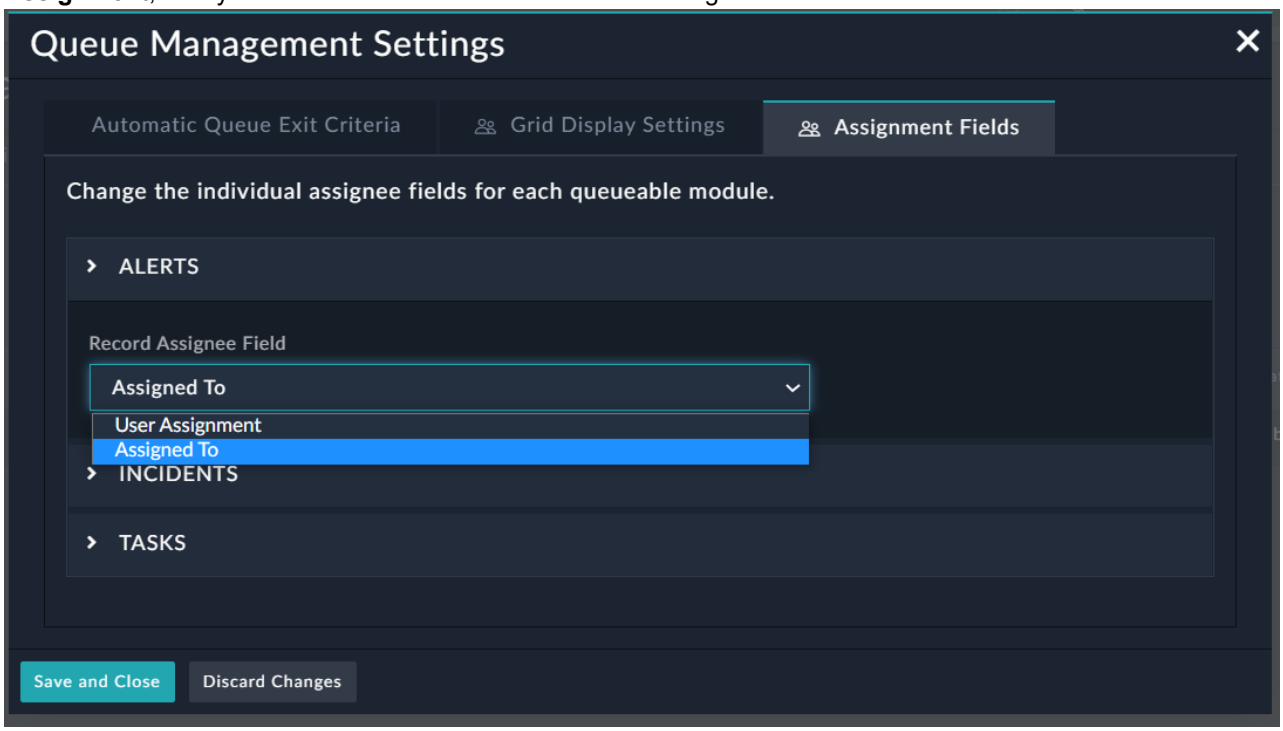
3. Click the **Grid Display Settings** tab to define how the card for records is displayed in all the queues. For our example, we will define how cards for 'Alert' records are displayed in queues. From the **Column** list select the fields that you should be added to the alert card in the queue and then click **Add**. For example, select and add fields such

as ID, Name, Type, Created On, Source, etc.:



4. Click the **Assignment Fields** tab to view or change the field that is used for the assignment of records for each queueable module. By default, the 'Alerts', 'Incidents' and 'Tasks' modules are visible. For example, if in case of alerts you have defined two fields that are used for assigning records to users **Assigned To** (default) and **User**

Assignment, then you can select either one of them as the assignee field for the record:

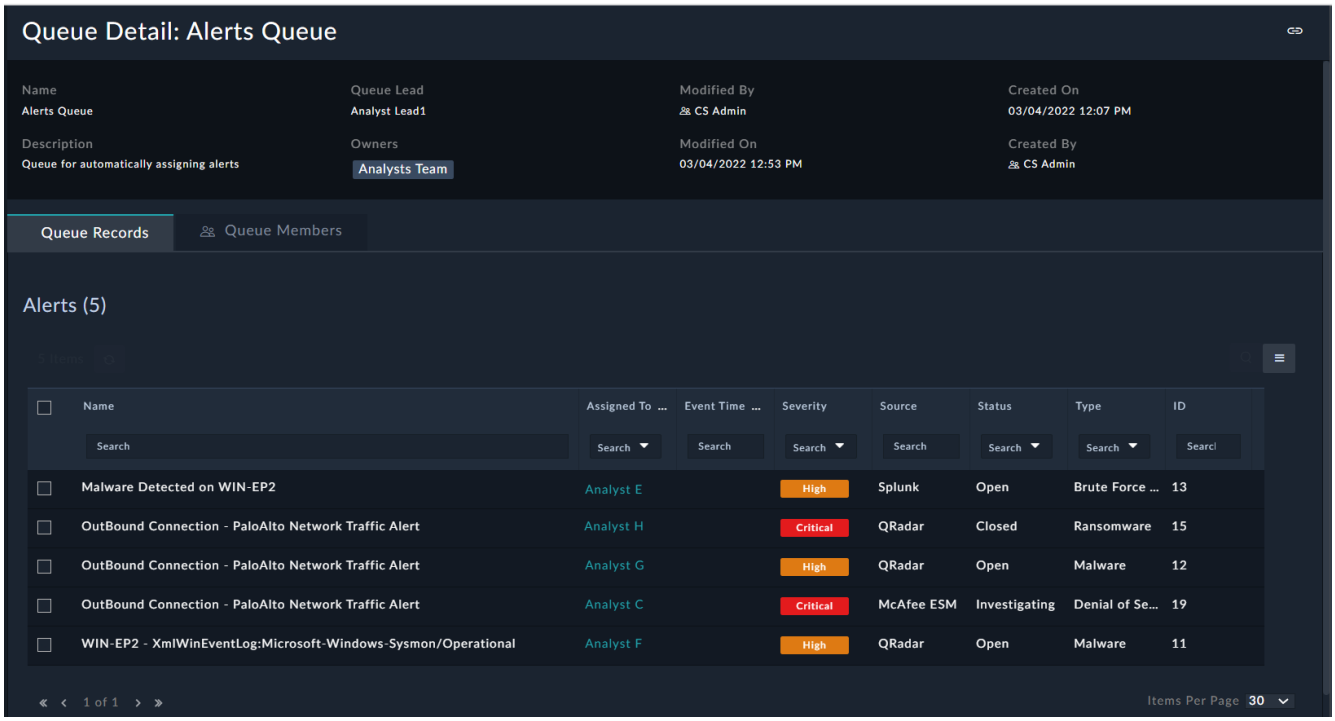


5. Once you have completed updating the queue management settings, click **Save and Close**.

Working with Queues

On the `Queue Management` page, you can see existing queues. To view details of the queue such as records that are assigned to the queue, members of the queue, etc., click the **View** icon in a queue record. In the following image the **Alerts Queue** is the active queue whose details, i.e., records assigned to the queue and members of the queues are

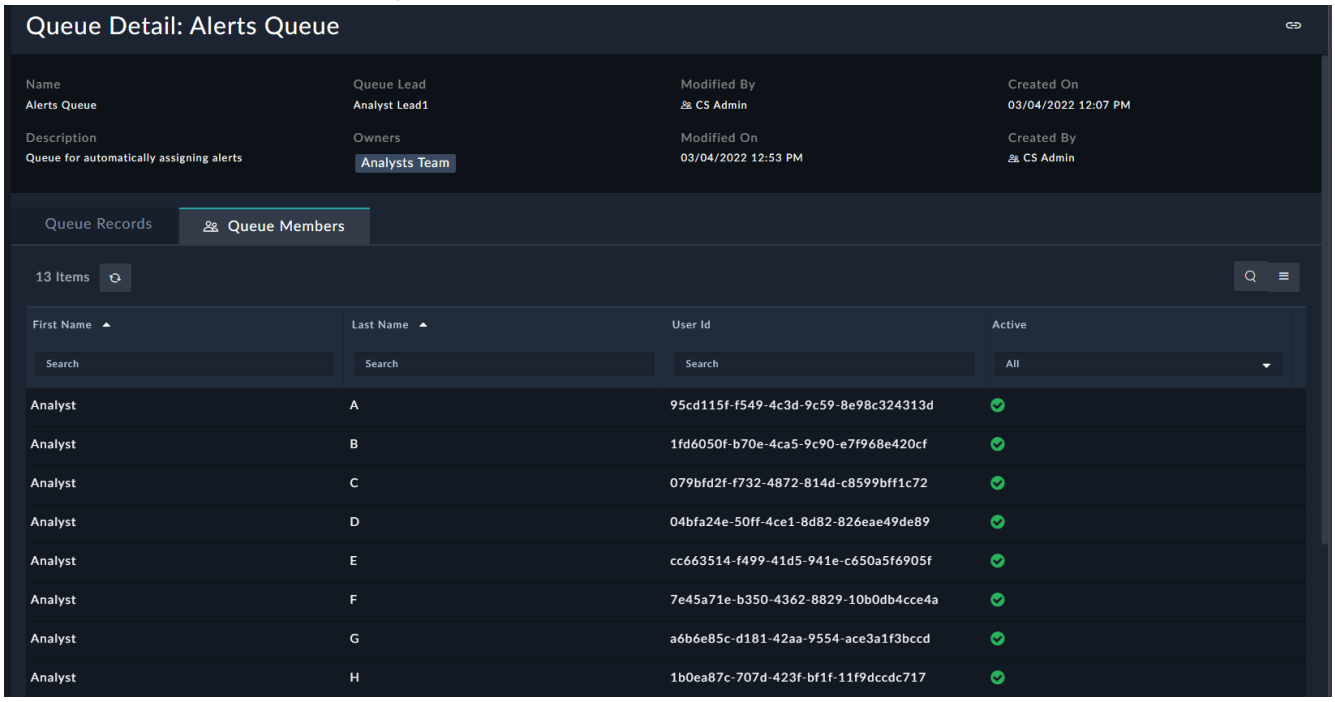
displayed:



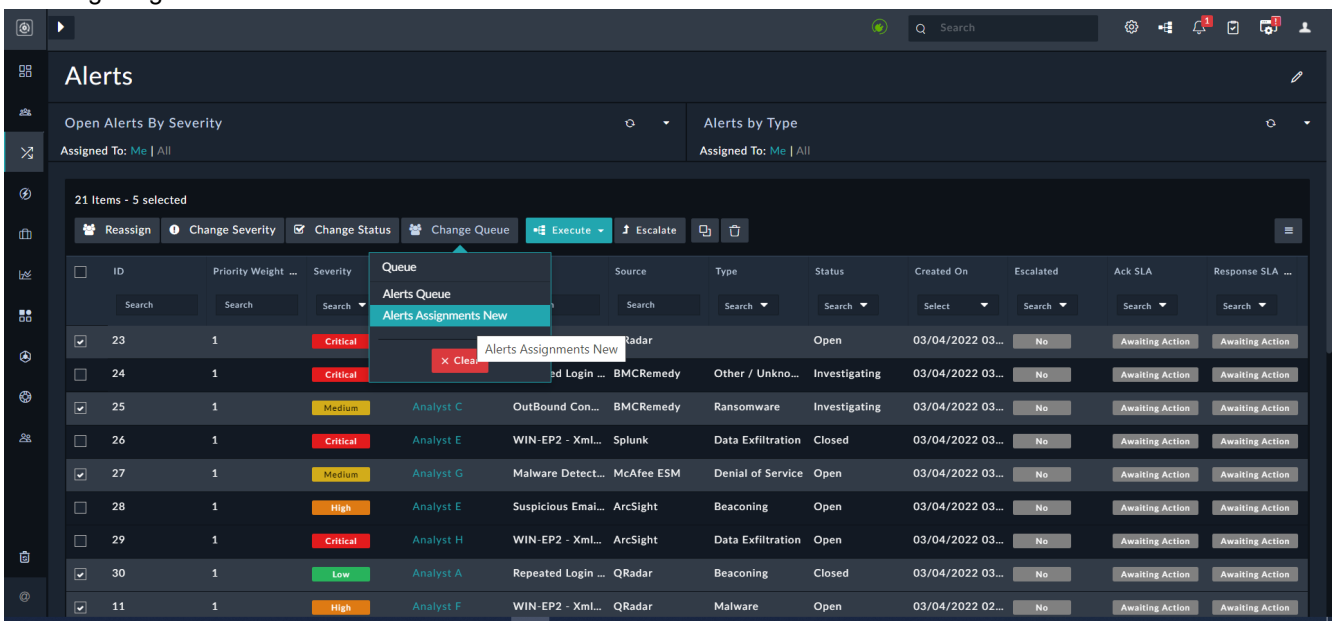
The list of alert records that are assigned to this queue is displayed in the **Queue Records** tab. Each alert record in the list is displayed as defined in Queue Management Settings, i.e., these settings define which fields are displayed in the alert record and how they are displayed. Also, as defined in the queue rules (in our example), alerts that are created are assigned to users who are part of the queue and are in that shift using the round-robin assignment method.
To view the details of a record, or to reassign a record, click the alert record in the alerts list grid, which opens the detail view of the record in which you can manually assign records to individual users or queues. For more information on the detail and list view of records, see the Working with Modules - Alerts & Incidents chapter.

To delete records from the queue, select that record and click **Remove Link.**

To view the members of the active queue, click the **Queue Members** tab:



You can also perform operations on the records from their respective views. For example, to manually reassign an alert record to another user or queue, you can click the alert record, and update the **Assigned To** or **Queue** fields. Similarly, to bulk assign records to different queues, click the **Change Queue** option in the record list view as shown in the following image:



As shown in the above image, the records have been assigned to the 'Alerts Queue'; however, if you want to assign some records to another queue, for example, 'Alerts Assignments New', then you can select the records, click **Change Queue**, and select the **Alerts Assignment New** queue. The selected records then move to the 'Alerts Assignments New' queue. For more information on the detail and list view of records, see the Working with Modules - Alerts & Incidents chapter.

You can export or import Queues and Shifts using the FortiSOAR Export and Import Wizards. Queues and Shifts are exported as records and the configuration of the Queue Management page is exported using the System View Template. While exporting Queues or Shifts, ensure that you select Queues and Shifts modules as well as their records in the Export Wizard. For more information on the Export and Import Wizards see the Application Editor chapter in the "Administration Guide."

Working with Shifts

Permissions required

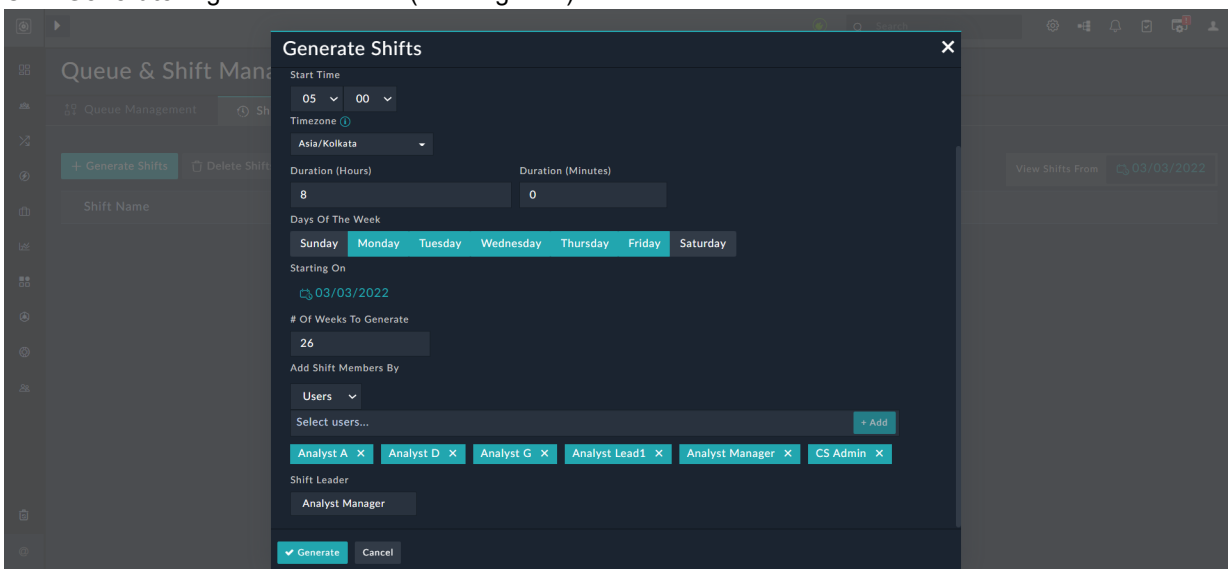
- To generate and delete shifts, the user must be assigned the role that has `Create`, `Read`, `Update`, and `Delete` (CRUD) permissions on the `Shifts` module and at the minimum `Read` permissions on the `Applications` module.
- To view the shift roaster, you need `Read` permissions on the `Shifts` module and at the minimum `Read` permissions on the `Applications` module.

Generating Shifts

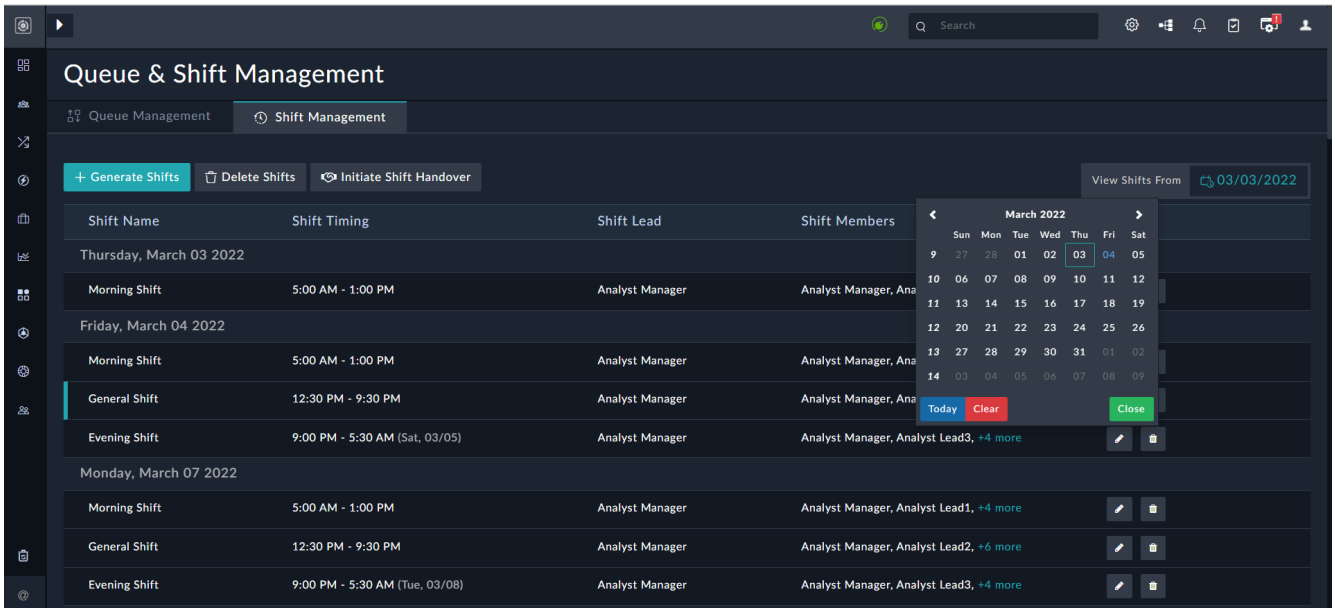
Queues and Shifts work together for the assignment of records. To create shifts, do the following:

1. Click **Queues & Shift Management** in the left navigation bar, then click the **Shift Management** tab.
2. To add shifts, on the `Shift Management` page, click **Generate Shifts**.
3. In the `Generate Shifts` dialog add the following:
   a. In the **Shift Name** field, add the name of the shift. For example, `Morning Shift`.
   b. In the **Start Time** field, select the time (in the 24-hour format) from when the shift will start. For example, 5:00 (for 5 am).
   c. From the **Timezone** field, search and select the time zone in which you want to apply the generated shift times.
   d. In the **Duration (Hours)** field, enter the duration of the shift in hours. You can enter the minutes in the **Duration (Minutes)** field. For example, if the shift is 8 hours, enter 8 in the Duration (Hours) field and 0 in the Duration (Minutes) field. However, if the shift is of 8 hours 30 minutes, then enter 8 in the Duration (Hours) field and 30 in the Duration (Minutes) field.
   e. In the `Days Of The Week` section, select the workweek, i.e., the days of the week for your organization. By default, Monday to Friday are selected. However, you can select the workdays according to the region as well, for example, Sunday to Thursday is the workweek in some Middle Eastern countries.
   f. From the **Starting On** date field, select the date from when you want to start the shift.
   g. In the **# Of Weeks To Generate** field, enter the number of weeks for which you want to generate this shift. For example, you might want to generate a shift for 6 months, in regions where daylight saving is applicable. Since you will need to change the shift timings every 6 months. To generate the shift for 6 months, enter 26 weeks.
   h. From the `Add Shift Members By` section, you can choose to add individual users or teams to the shift. If you choose to add a team, then all users who are part of that team get added to the shift. To add users to the shift from the **Users** drop-down list, select **Users** or **Teams**. Based on your choice, a list of users or teams gets populated in the **Select users** or **Select teams** list. Select the users or teams that you want to add as members to this queue and click **Add**.
   Note: The **Select users** and **Select teams** lists display only active users.

i. From the **Shift Leader** drop-list, select the user who is assigned as the leader of this shift.
j. Click **Generate** to generate this shift (Morning Shift).

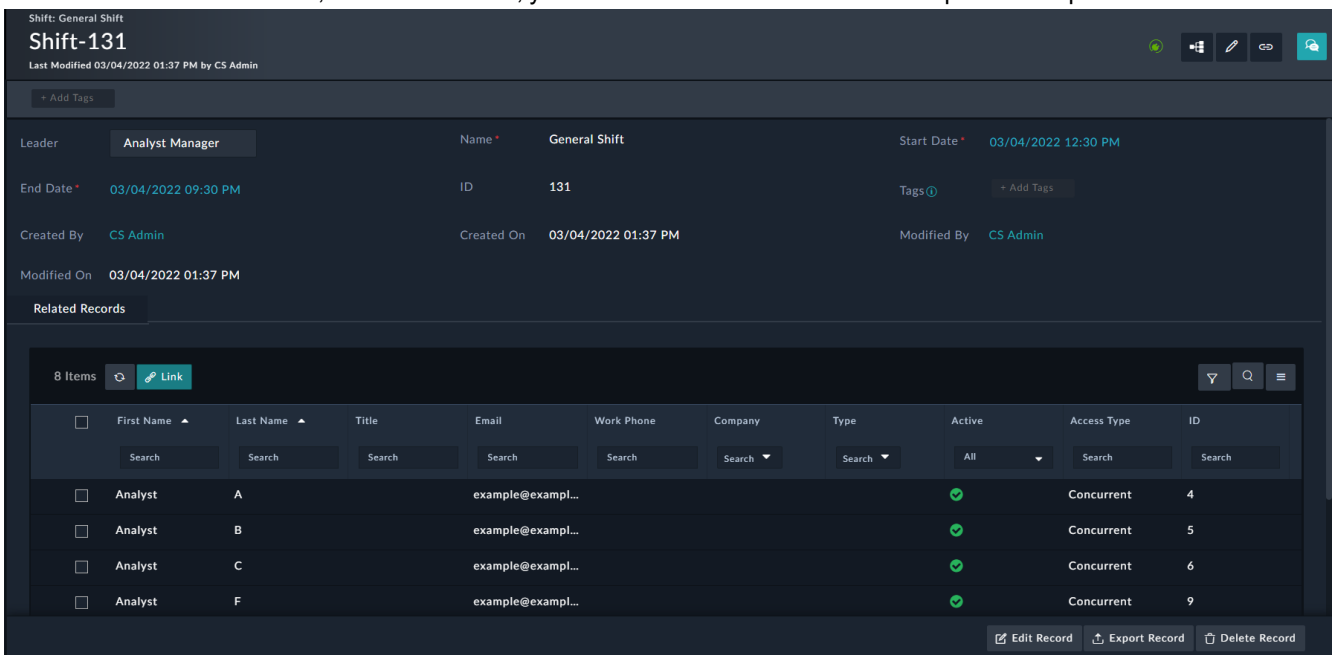


This adds the shift roster on the `Shift Management` page:



To view shifts older or historical shifts, click **View Shifts From** and select a date on the calendar.
To view the list of users that are part of a shift, click the **Edit** icon on the shift record to open its detail view. In the

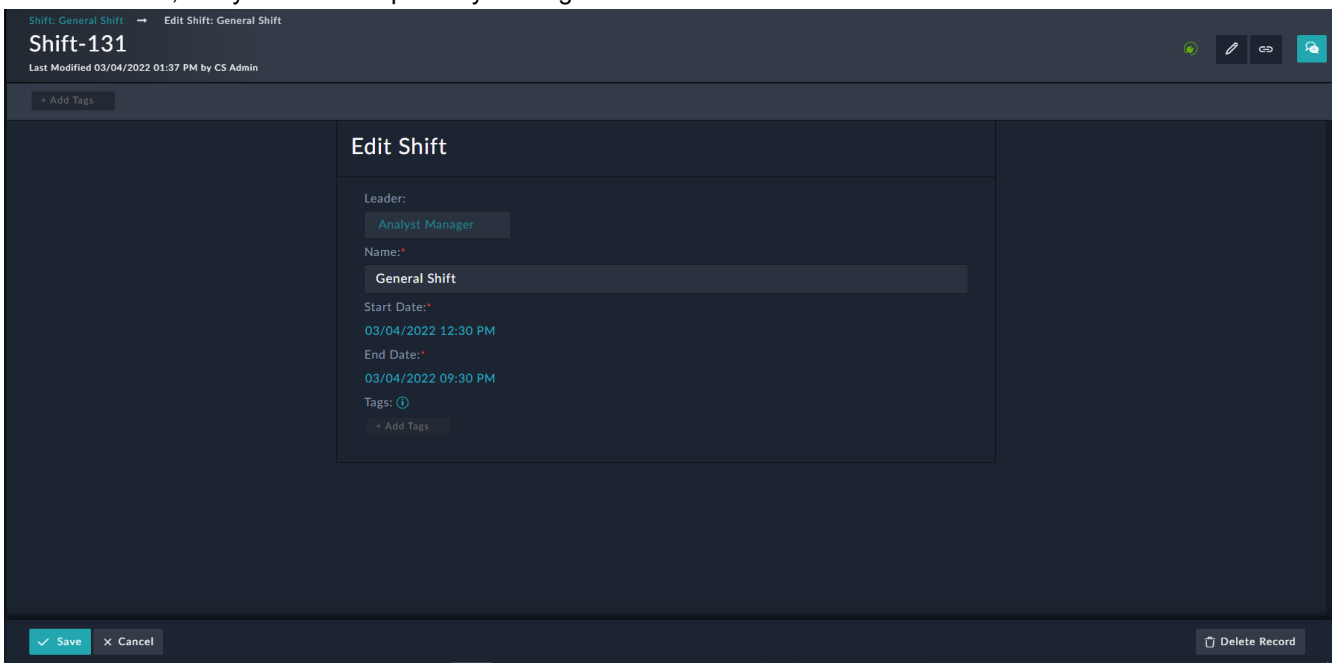
`Related Records` section, on the **Users** tab, you can view the list of users who are part of that particular shift:



To add existing users to the shift, click **Link**, to open the `Link People` dialog, in which you can select users to add to the shift, and then click **Save Relationship**. Similarly, to remove users from the shift, select the users and then click **Remove Link**.

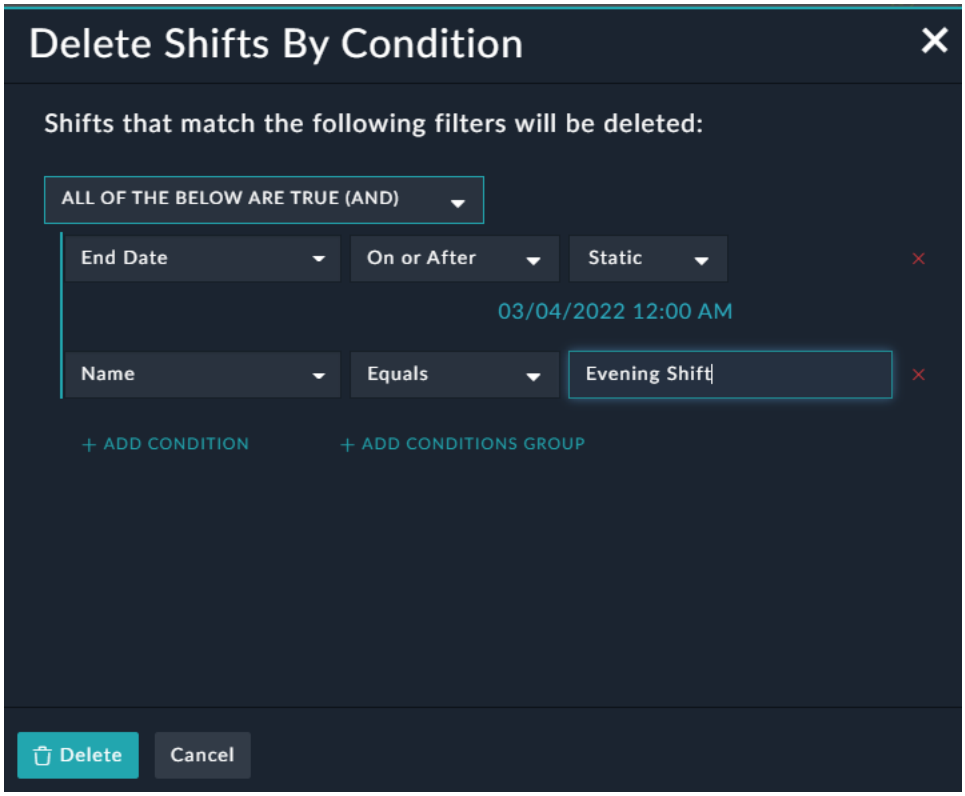
To delete a record for a particular shift, either click the **Delete** icon on the grid view of the record or click the **Delete Record** button on the detail view of the record and click **OK** on the confirmation dialog. To export a shift record in the CSV or PDF format, click the **Export Record** button in the details view of the shift record.

You can also edit some details of the shift by clicking the **Edit Record** button in the details view of the shift record. Details of the shift that you can change are the leader of the shift, the name of the shift, the starting and ending date and time of the shift, and you also can optionally add tags for the shift:



Deleting Shifts in bulk

To delete shifts in bulk and based on some condition, click the **Delete Shifts** button. In the `Delete Shifts By Condition` dialog, enter the criteria based on which you want to delete the shifts. By default, a condition for deleting shifts that existed in the past is added. In addition to the same, if for example, your organization has removed the Evening Shift, then you can add a condition such as `Name Equals Evening Shift` and click **Delete**:



Click **Confirm** on the confirmation dialog to delete all the records associated with the 'Evening Shift.'

Initiating Shift Handovers

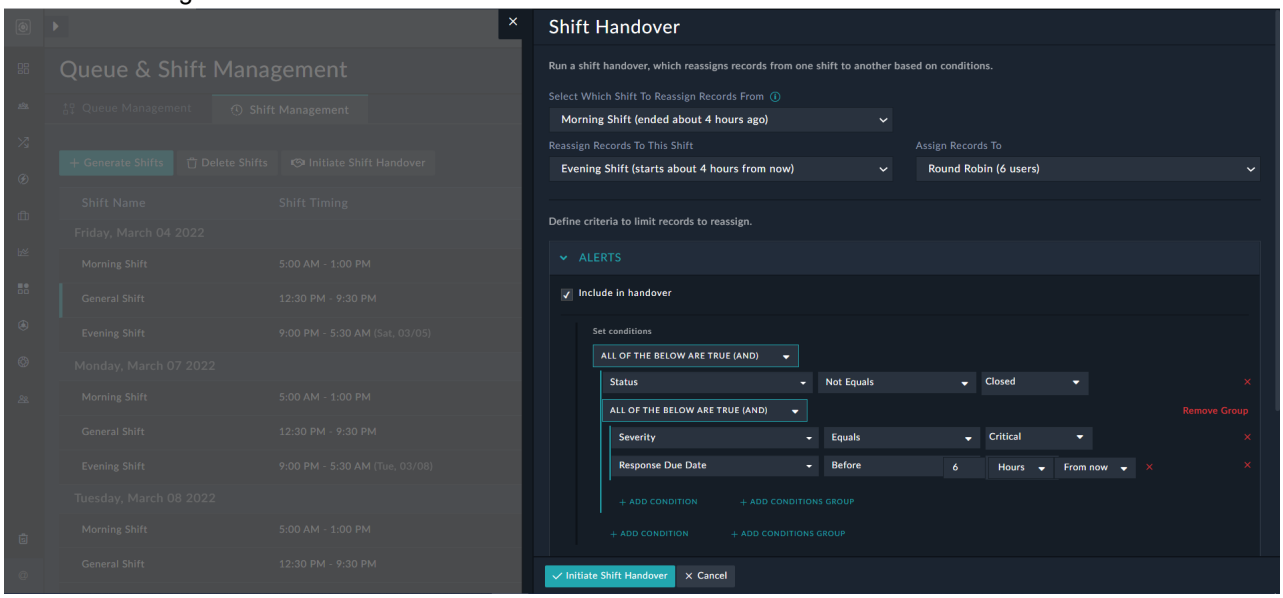
You can also define rules for shift handovers, i.e., based on the specified criteria, the filtered items would be handed over or reassigned to the members of the next shift.

For example, a queue leader is working in the 'General Shift' might want to reassign all Alerts whose status is not 'Closed' and whose Severity is 'Critical' or whose 'Response Due Date' is in or less than 6 hours to members of the 'Evening Shift'. To initiate shift handovers:

1. Click **Queues & Shift Management** in the left navigation bar, then click the **Shift Management** tab.
2. Click **Initiate Shift Handover**.
3. In the `Shift Handover` slider, define the rules for shift handover:
   a. From the **Select Which Shift To Reassign Records From** drop-down list, select the shift whose records you want to hand over. For example, **Morning Shift** (ended about 3 hours ago).
   b. From the **Reassign Records To This Shift** drop-down list, select **Evening Shift** (starts in about 5 hours from now)

   c. From the **Assign Records To** list, select to whom you want to assign the records. You can choose to assign the records to the manager of the shift to which you are handing over the records, **Shift Manager** or assign the records in the **Round Robin** method, or choose to not assign the records to anyone, **Nobody (leave blank)**.

4. The `Define criteria to limit records to assign` section displays all the modules whose records you can auto-assign using queues. For our example, click the down (**v**) arrow in the **Alerts** row, and define the criteria as follows:
   a. Click the **Include in handover** checkbox to include the records in the handover based on the defined conditions.
   b. Add the conditions based on which you want to assign records to members of the selected shift. For our example, click **Add Condition** and then enter the condition `Status Not Equals Closed`.
   Next, click **Add Conditions Group**, select the **OR** operator and add the following conditions:
   `Severity Equals Critical`
   `Response Due Date On or Before 6 hours from now`
   Similarly, you can define criteria for other modules whose records you can auto-assign using queues.
5. From the **Only Include Records Created In The** field, choose **Relative** or **Custom** and then select the number of days to be considered for alert creation while handing over alerts to different shifts.
6. In the **Add Comment To Reassigned Records**, you can add a note, for example, `Reassigned via shift handover` that gets added as a comment in the records.



7. To initiate the shift handover, click **Initiate Shift Handover**.
   This begins the process of reassigning records to the shift and FortiSOAR displays a toaster message containing the number of records that were reassigned to the specified shift. When you open the detail view of records that were re-assigned using shift handover, you will see the comment, for example, `Reassigned via shift handover` added to the record.

Reports in FortiSOAR

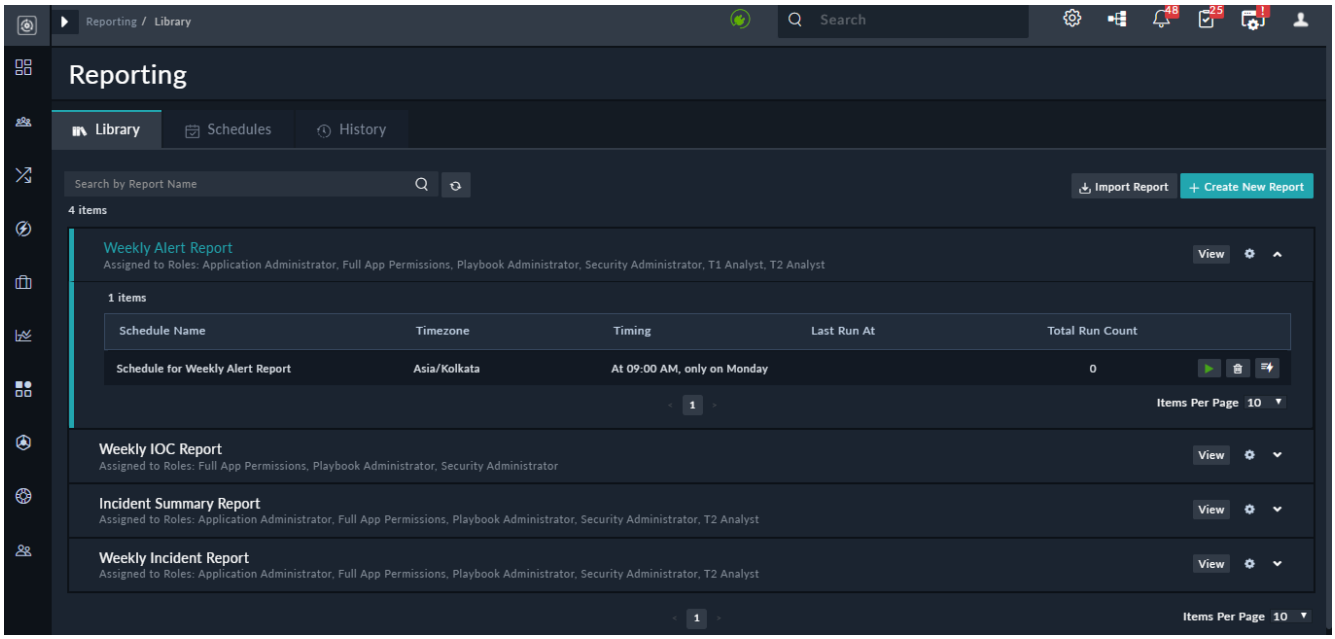
You should use FortiSOAR Reports for your reporting purposes since you can easily create rich reports and dashboards in FortiSOAR. You can also schedule reports, view historical reports and also search for text in the report PDF, which is in the text PDF format.

You can design your report to include a date or date range as an input parameter to a report; i.e. define a date range, date, or filter criterion in the template for reports. Similarly, users of the report can also specify a date range and filter data in the report whose template have the date or filter parameter defined. For information on how you can define and use dates or date ranges to filter data in the reports, see the Dashboards, Templates, and Widgets chapter. You can also specify the timezone in which you want to export your reports.

Dashboards and reports have good performance since only the required content is loaded and lazy loading of the content is enabled.

Click **Reports** in the FortiSOAR left navigation to display the `Reporting` page, which the following tabs:

- **Library**: Centralized repository of all reports. The Library page displays a list of reports and its associated schedules. To see the details of schedules associated with a report, you can click the down arrow in the reports row. You can also view the generated reports from this page and also see the roles that have been assigned to a particular report. You can create new reports, edit and manage reports, and search for reports on this page. You can also import a valid JSON report template on this page.
- **Schedules**: Lists all the created schedules on this page. You can click **View Details** in a schedule row to view the detail schedule record page. Using the schedule detail record page, you can view the logs of the playbooks (by clicking the **View Executed Playbooks**) that were executed using this schedule, and also perform actions such as stopping, updating, or starting the schedule using this page. You can also search for schedules by schedule name, and filter schedules by status and report on this page.
- **History**: Lists all created (historical) reports on this page. You can search for report using its historical name and filter reports and schedules by various criteria. You can also download a pdf version of the historical report from this page.



Pagination is enabled on all pages within Reporting, i.e., on the Library, Schedules, and History pages for better navigation and also on the item rows within the report rows, for example, the schedule entries within a report row.

Permissions required for working with reports

Only when an administrator modifies reports, those modifications are applicable across the system and applicable to users, based on their roles.

- To view reports, you must be assigned a role that has `Read` permissions on the `Application` and `Reporting` modules, and the report must be assigned to your role.
- To create and edit reports, you must be assigned a role that has `Read`, `Create`, and `Update` permissions on the `Reporting` module and `Read` permission on the `Application` module. Additionally, if you also want to delete reports and configurations, you must be assigned a role that has `Read`, `Create`, `Update`, and `Delete` permissions on the `Reporting` module and `Read` permissions on the `Application` module.
- To customize only your own reports, i.e., the changes made in the reports would not be visible to any other user, a role with `Read`, `Update` and `Create` permission on the `Reporting` module and `Read` permission on the `Application` module is sufficient. If such a user (a non-admin user) changes the dashboard, then a copy of the original dashboard is created and those changes are visible to only that particular user and not to other users.
- To customize reports, i.e., the changes made in the reports would be visible to all users who have access to that report, a role that has `Read` and `Update` permissions on the `Reporting` module and `Read` permissions on the `Application` and `Security` modules must be assigned. If you have these permissions, then the changes are made in the original dashboard and these changes are visible to all the users who have access to the dashboard.
- To create a schedule, you must be assigned a role that has `Read`, `Create`, and `Update` permissions on the `Schedules` and `Read` and `Create` permissions on the `Playbooks` module. To delete schedules, you must be assigned a role with `Delete` permissions on the `Schedules` module.
- To view saved reports, you must be assigned a role that has `Read`, `Create`, and `Update` permissions on the `Saved Reports` module. To delete saved reports, you must be assigned a role with `Delete` permissions on the `Saved Reports` module.
- To export your reports as a PDF file, you must be assigned a role that has `Read` permissions on the `Application` and `Reporting` modules, `Create`, `Read`, and `Update` permissions on the `Saved Reports` modules, `Read` and `Execute` permissions on the `Playbooks` module, and `Create` and `Read` permissions on the `Files` module.

In addition to the appropriate permissions mentioned above, users also require to have appropriate rights on the module for which they want to create or edit reports. Since if users do not have `Module Read` permissions on the module that they want to consume in the report, then they will not be able to view the details of that module in the report. For example, if you have `Module Read` permissions on the **Alerts** module but not on the **Incidents** module, then you can update reports that consume Alerts as their data source. However, if you try to update a report that consumes Incidents as the data source, FortiSOAR displays a message such as `You do not have necessary permissions for Incidents`.

Working with reports

To create a new report, click **Reports** in the FortiSOAR left navigation, which displays the **Library** tab on the `Reporting` page, and click the **+ Create New Report** button.

The **Library** tab contains a list of reports that have been created. You can search for reports by report name using the **Search** box and refresh the `Library` page using the **Refresh** icon. You can also edit existing reports and perform other operations from this page.

To view the details of the schedules associated with a report, click the down arrow in the report row whose associated schedules you want to view or modify, and then click on the schedule row. This will display the `Schedule Details` dialog, using which you can view or modify the schedule. One report can have multiple schedules, but one schedule can only be associated with a single report.

Importing a report template:

Use the export and import template feature to share reports across users. If you see a report that a colleague has created that you feel would be useful to you as well, then instead of you having to recreate the report, your colleague can export the report, and you can import it and start using the same.

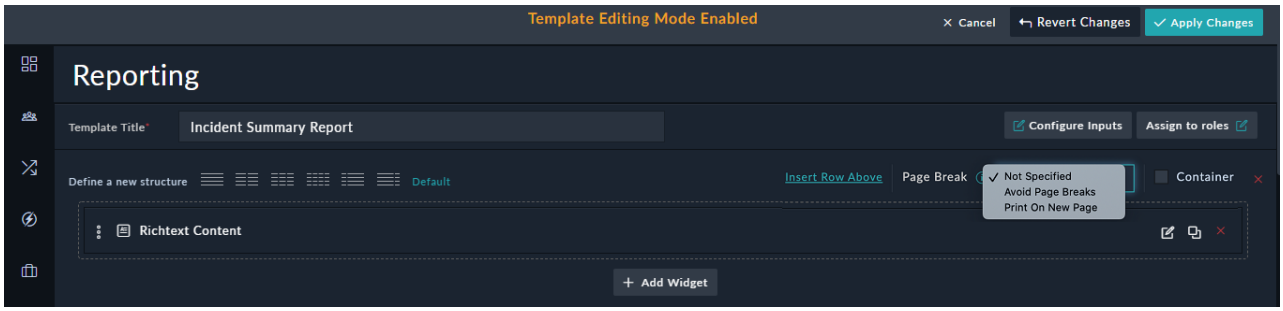
You can only import a valid JSON template. The template that you import is only applicable to your report. Administrators must import, update, and assign reports for the changes to apply to all users.

1. Log on to FortiSOAR and click **Reports** in the left navigation.
2. On the `Library` page, click **Import Report**.
3. In the `Import Report Template` dialog box, drag-and-drop the JSON template file, or click to browse to the JSON template file.
4. Click **Import**.
   If the file is in the appropriate JSON format, FortiSOAR displays `Template Imported successfully!`

Based on the permissions that are set for you, you can perform the following operations on the `Library` page:

Adding or Editing Reports on the Library page

1. Log on to FortiSOAR and click **Reports** in the left navigation.
2. To create a new report, click the **+ Create New Report** button on the `Library` page. To edit an existing report, click the **Actions** ( )icon, in the row of the report that you want to edit, and click **Edit Template**.
   Templates are JSON definitions of the interface structure composed of widgets. Widgets are configurable interface elements that are used to represent data, such as charts or lists visually. For more information on Templates and Widgets, see the Dashboards, Templates, and Widgets chapter.
   From version 6.4.4 onward, reports are enhanced to support page breaks, by providing a **Page Break** option on the `Edit Template` page. To insert page breaks for reports (rows in report), you can choose from the following options:
   - **Not Specified**: In this case, page breaks are not added, i.e., this option allows page breaks within rows.
   - **Avoid Page Breaks**: In this case, page breaks are avoided, i.e., if a page break occurs within a row in a report, then the row automatically gets printed on a new page.
   - **Print On New Page**: In this case, page breaks are added between rows, i.e., each row of a report is printed on a new page.



Note: If you have changed a report that an administrator has assigned to you, then you will not be able to view the administrator changes to that report. To reset the administrator changes to the report, click **Actions** > **Reset to Original State**, i.e., the changes that the administrator made will be visible and your changes will be lost.

3. In the **Template Title** field, enter the template title.
4. Click **Add Row** and structure the row by defining the number and layout of columns from the options displayed in **Define a new structure**.
5. Click **Add Widget** and from the **Choose Widget** dialog box, select the appropriate widget.
   For more information on Templates and Widgets, see the Dashboards, Templates, and Widgets chapter.
6. Click **Edit Widget** to configure or reconfigure the widget properties and click **Save**.
   Note: The **Only Me | All** filter is not applicable to Reports, i.e., on the `Reports` page, you cannot toggle the view based on this filter, instead, you must change this in the report template itself when you are adding or editing a widget. For more information on Widgets, see the Dashboards, Templates, and Widgets chapter.
7. Click **Apply Changes**.
   To revert the changes, you have made to the template, click **Revert Changes**.

To add a report heading, you can use the Richtext Content widget. You can also add fields (choose fields) from modules that you want to display in the Richtext Content widget making it simpler and efficient for you to add fields in the Richtext format. For more information on the Richtext Content widget, see the Dashboards, Templates, and Widgets chapter.

To clone a report template:

1. Log on to FortiSOAR and click **Reports** in the left navigation.
2. On the `Library` page, click the **Actions** icon, in the row of the report that you want to edit, and click **Clone Template**.
3. Update the template title.
   By default, the template title appears as **cloned: name of the original template**.
4. Update the template and widgets as required.
5. Click **Apply Changes**.

To export a report template:

Report templates get exported as a JSON template.

1. Log on to FortiSOAR and click **Reports** in the left navigation.
2. On the `Library` page, click the **Actions** icon, in the row of the report that you want to edit, and click **Export Template**.
   FortiSOAR downloads the template on your machine in the JSON format.

To remove a report template:

You can only remove reports that you have added. You cannot remove reports created by an administrator or by any other user.

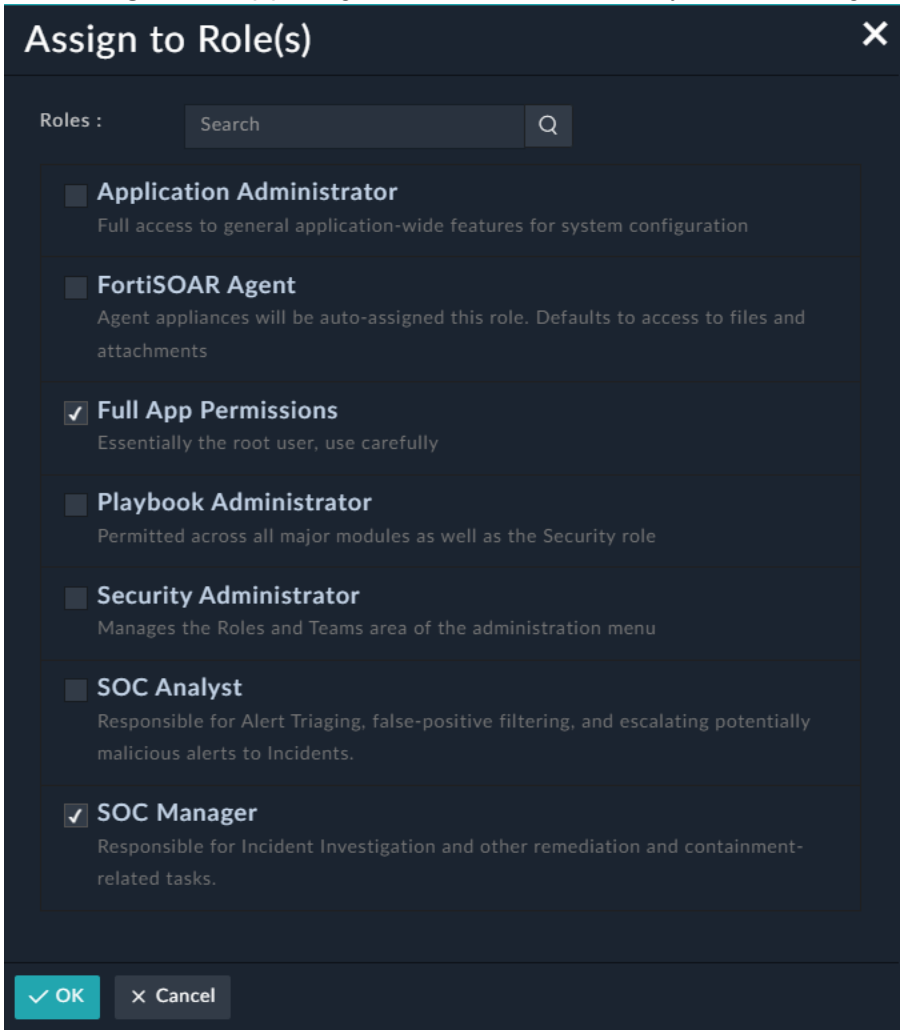
1. Log on to FortiSOAR and click **Reports** in the left navigation.
2. On the `Library` page, click the **Actions** icon, in the row of the report that you want to remove, and click **Remove Template**.
3. On the **Confirm** dialog, select **Confirm**.

To assign roles to reports

You must have a minimum of `Read` permission on the "Security" module, apart from other appropriate privileges to perform this task.

1. Log on to FortiSOAR and click **Reports** in the left navigation.
2. On the `Library` page, click the **Actions** icon, in the row of the report to which you want to assign a role, and click **Assign to Role**.
   This displays the Assign to Role (s) dialog in which you can select the role(s) to which you want to assign the report.

3. In the **Assign to Role(s)** dialog box, select the role to which you want to assign the report.



4. Click **OK**.
   Users having the role specified will be able to see the report(s) associated with that role the next time they log on to FortiSOAR.

Performing operations on the Report Page

To view the generated report

To view the generated report, on the `Library` page, click **View** in the row of the report that you want to view. This displays the *Report Page*. You can also perform the Assign to Role (if you have administrative privileges), Edit Report, New Report, Clone Report, Export Report, in the JSON format, and Remove Report operations by clicking the **Actions** ( ) icon on the *Report Page*. In addition to these operations, you can export a report as a pdf.

To go back to the `Library` page, click **Back to Library**.

To export a report as a PDF

On the *Report Page*, you can download the report in a `.pdf` format by clicking the **Export As PDF** button. The report is exported in text PDF format, which enables you to search text in the report PDF and also reduces the file size of your report as compared to an image PDF.

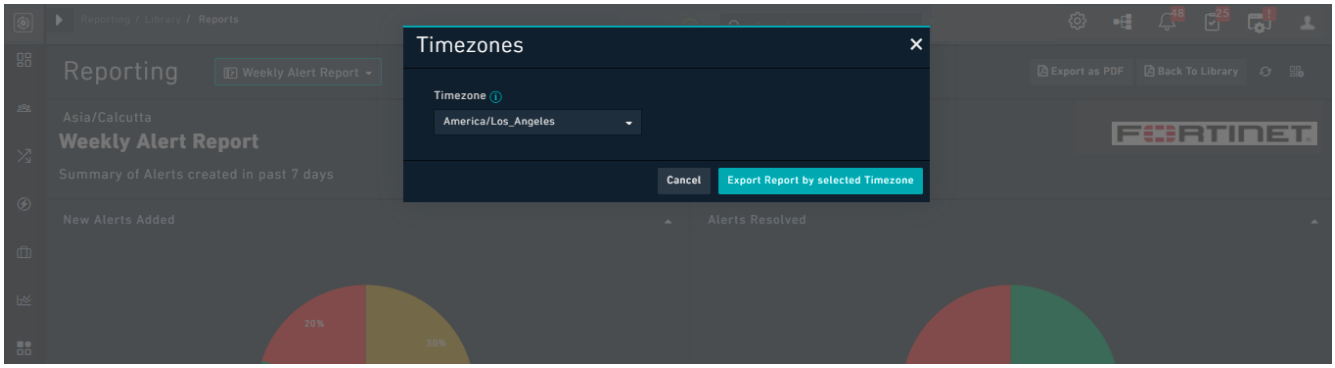
The PDF report that you export might not exactly match with the report view that you see on the FortiSOAR UI. This happens if the data that is used to create the report gets updated from the time you have viewed the report till the time the report is exported.

By default, reports are exported in the light theme. This report gets downloaded on your machine. This report also gets saved and is available in the `History` page (**Reports** > **History**).

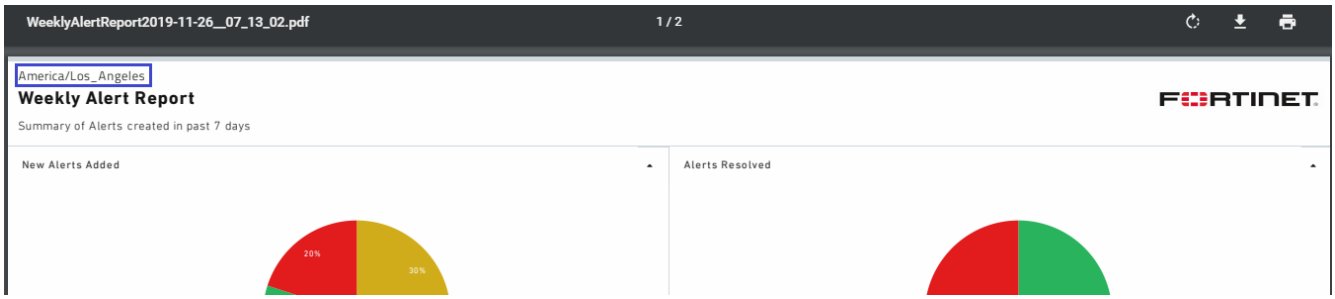
You can export a FortiSOAR report that contains more than one page in the PDF format, i.e., the exported report PDF can consist of multiple pages. However, note that report pages are split into multiple pages based on the height of the report. Therefore, you must arrange your widgets, especially widgets in the *Chart* category, in the report in such a way that widgets are not placed between two pages, else the data of that widget will get split into two parts.

If you have manually exported the report, i.e, by clicking the **Export As PDF** button on the *Reports* page, then the report is generated by default in the timezone that is set by your administrator. If the administrator has not set any timezone, then the report is generated in the timezone of the user's browser. Administrators can define a timezone that will be used by default for exporting reports. This timezone will be applied by default to all reports that you export from the *Reports* page. For more information, see the *System Configuration* chapter in the "Administration Guide."

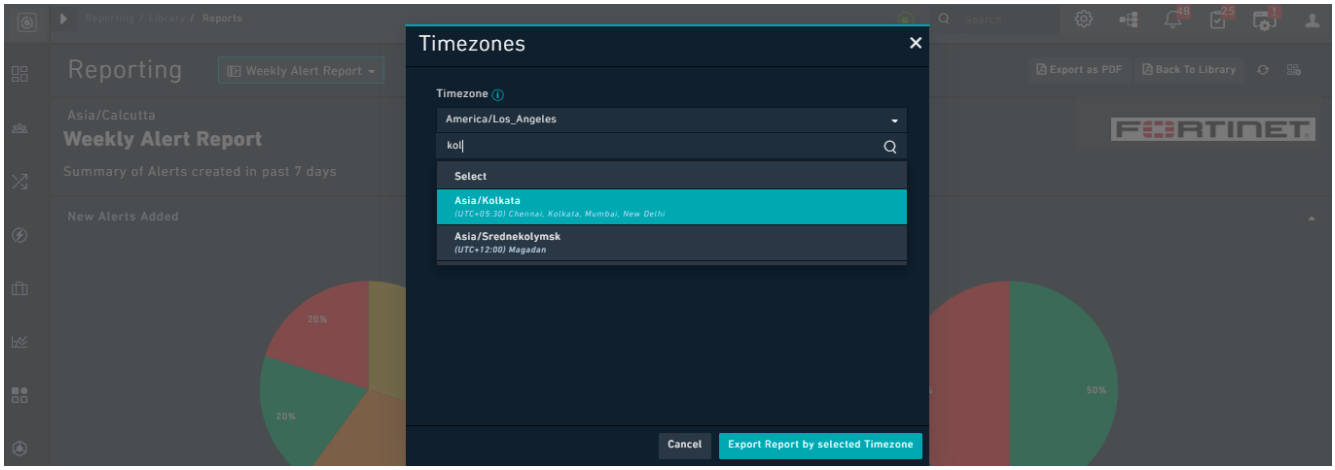
If your administrator has set the default timezone in which to export reports, then that timezone is displayed when you click the **Export As PDF** option. The default timezone set will be displayed in the `Timezones` dialog:



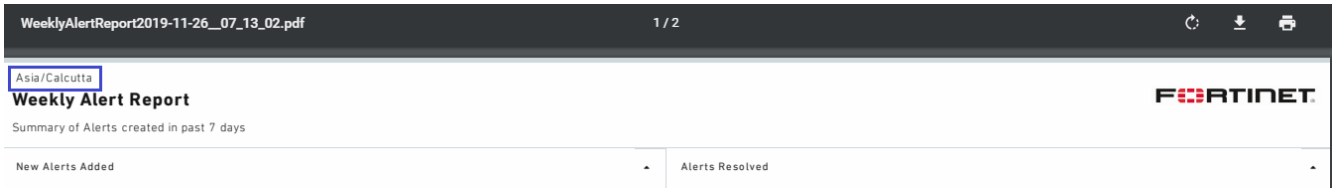
Either retain the default timezone or change the timezone using the **Timezone** drop-down list, and then click the **Export Report By Selected Timezone** button in the `Timezones` dialog. For our example we have retained the default timezone. Therefore, the report will be exported in the default timezone (America/Los_Angeles), which is visible on the exported report as shown in the following image, if you have added timezone as part of the report. For more information see Displaying of timezone within exported reports.



If you want to export the report in the timezone other than the default timezone, then in the `Timezones` dialog that appears when you click the **Export As PDF** option, choose the required timezone. In the `Timezones` dialog, you can search and select the timezone in which you want to export the report. For our example the default timezone is set as America/Los_Angeles and if for example, you want to export the report in the Asia/Kolkata timezone, then type `kol` in the search box below the Timezone field to find the correct timezone, as shown in the following image:



Now, click the **Export Report By Selected Timezone** button. This will export the report and you will be able to see this timezone (Asia/Calcutta) on the exported report as shown in the following image, if you have added timezone as part of the report. For more information see Displaying of timezone within exported reports.

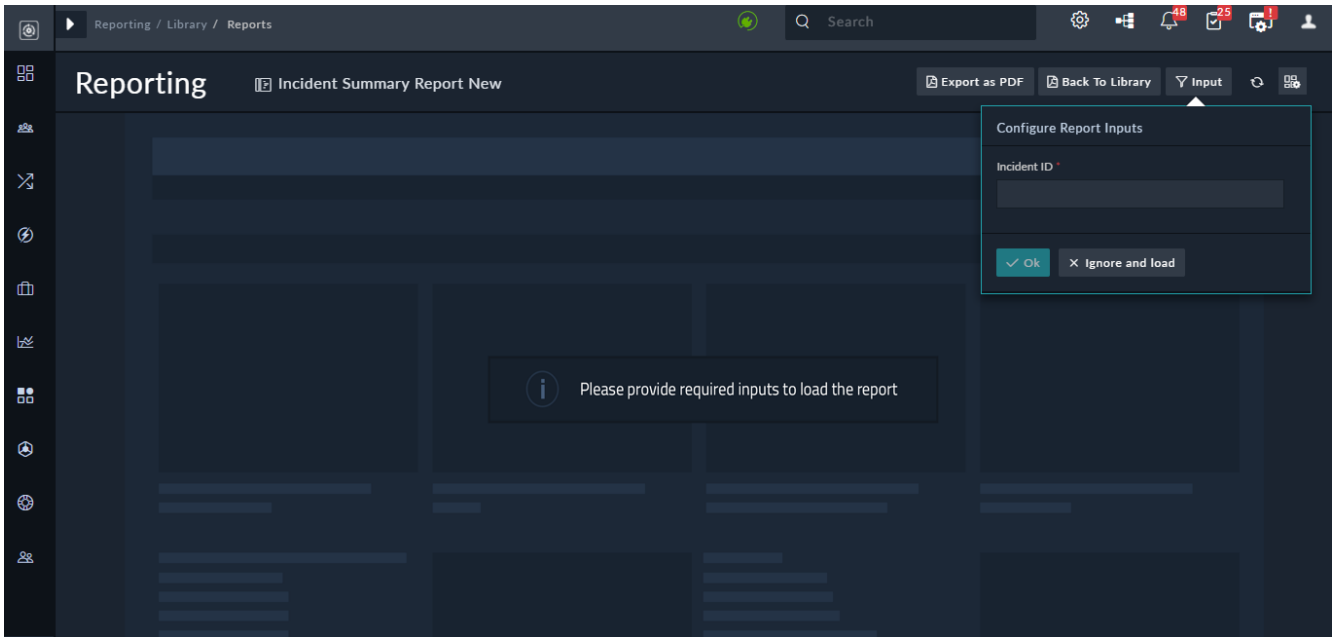


Input Variables in Dashboards and Reports

You can define variables that you can use in widgets as filters to consume inputs and create a dashboard or a report dynamically. Using input variables, you can filter data in a dashboard or report to display a particular set of data without having to define the same criteria in each widget in the dashboard or report. Once you configure the variable as a filter in widgets, the dashboard or report is displayed according to the filter value you have specified. You can also specify inputs for dashboards or reports, based on which dashboard or reports are updated dynamically to display the dashboard or report according to the updated input values.

For more information and examples of input variables, see the Dashboards, Templates, and Widgets chapter.

From version 6.4.0 onwards, the user experience of working with reports that need input to load has been improved. If a report, for example, Incident Summary Report was configured such that no default incident ID was specified and required the user to provide the incident ID before the report could be displayed, then earlier FortiSOAR would display messages such `Widget not configured properly`. Now, FortiSOAR displays a message such as `Please provide required input to load the report` and prompts you to enter the **Incident ID** in the `Configure Reports Inputs` dialog, as shown in the following image:

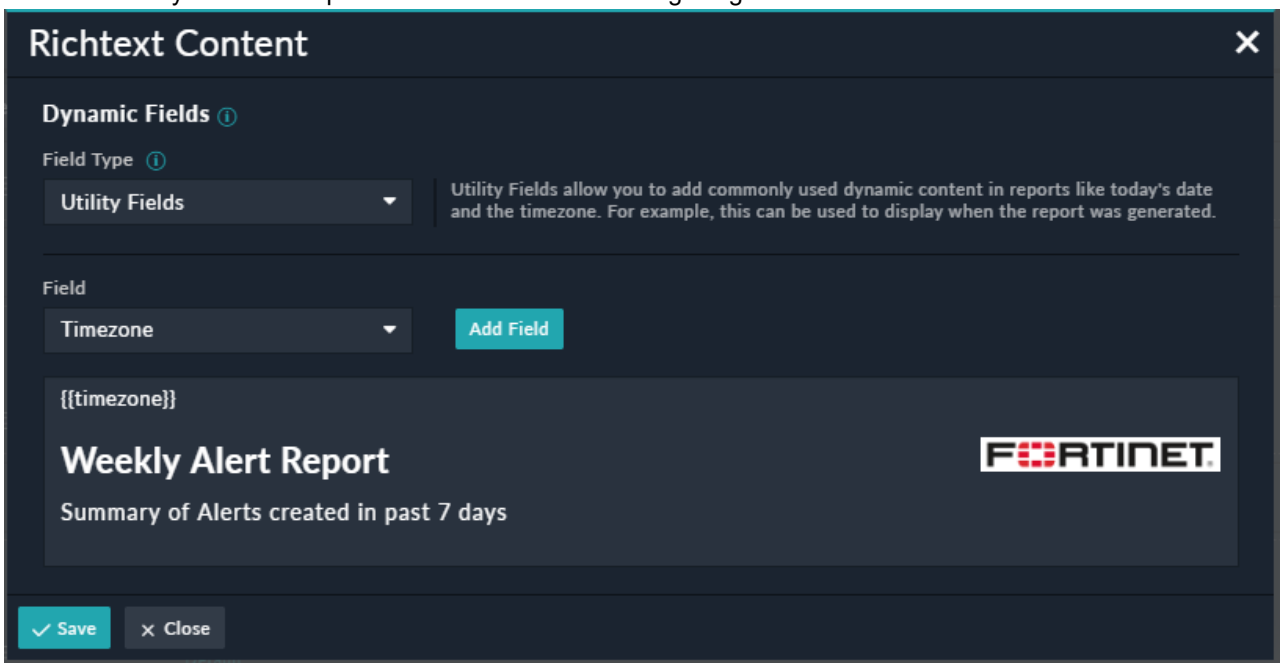


Displaying of timezone within exported reports

If you want to display the timezone in which the report (.pdf) has been exported, do the following steps in the template of the report in which you want to display the timezone:

1. On the `Reports` page, in the report row in which you want to display the timezone, click the **Actions** icon, and then select **Edit Template**.
   Generally, you will find that the heading of the report is displayed using the Richtext Content widget.
2. In the **Richtext Content** widget row, click the **Edit** icon.
3. In the Richtext Content widget, click the **Add Dynamic Fields** link.
   For more information on templates and widgets, see the Dashboards, Templates, and Widgets chapter.
4. From the **Field Type** drop-down list, select **Utility Fields**.
5. From the **Field** drop-down list, select **Timezone**, and click **Add Field**.
   This will paste the jinja value of the Timezone field, i.e., `{{timezone}}` in the Richtext Content widget on the

location where your cursor is placed as shown in the following image:



6. Click **Save** to save the updates to the reports template.

If your report has been scheduled using the timezone as Asia/Kolkata, then you will be able to see this timezone (Asia/Calcutta) on the exported report as shown in the following image:

Scheduling Reports

You can schedule reports to run automatically at specific times and also automatically send reports to the relevant users. For example, you can schedule a report that contains Critical Open Alerts to be sent out to, for example, managers in a SOC team, at 8 am in the morning on Mondays.

You can create multiple schedules for a single report.

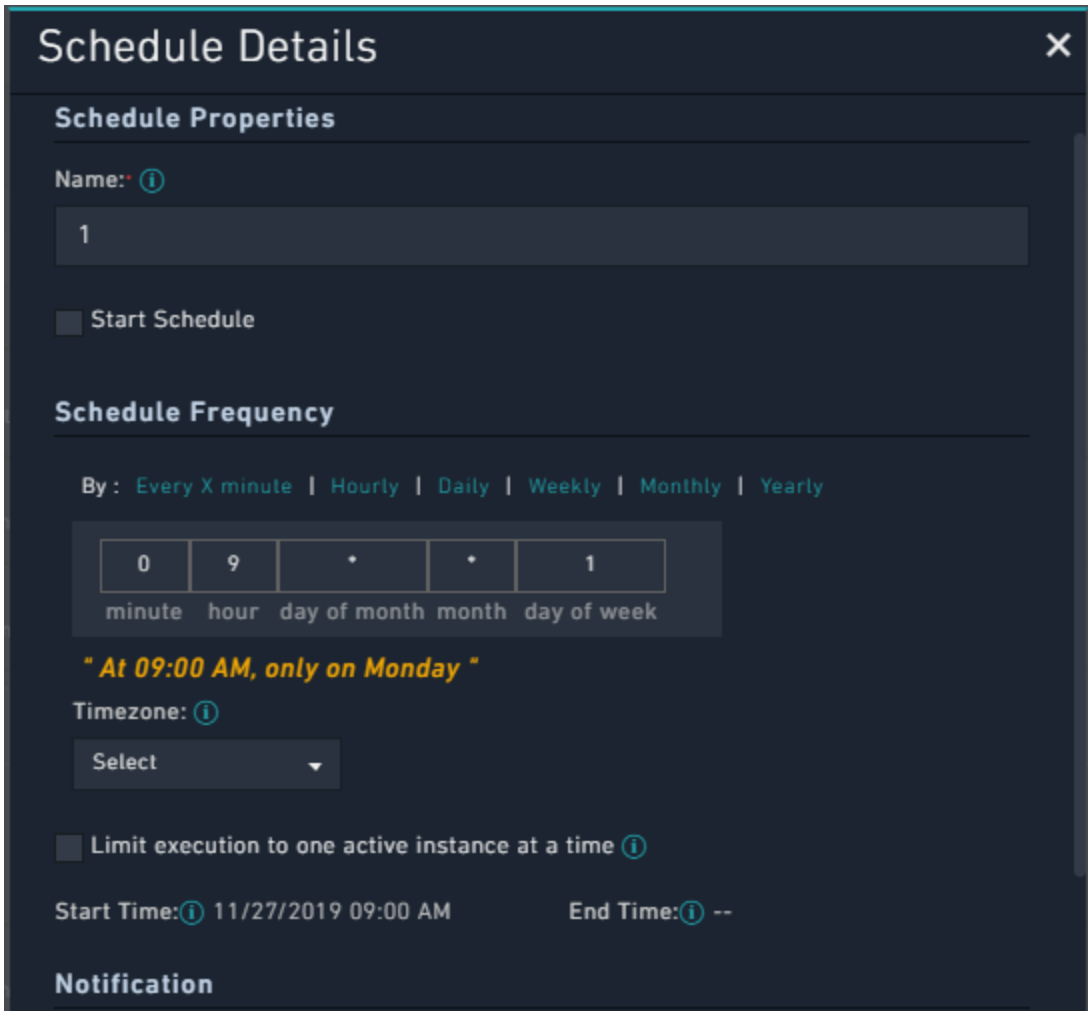
When you click **Reports** in the left navigation, the `Reporting` page with the **Library** tab selected is displayed.

On the `Library` page, you can see the list of reports and its associated schedules. You can also add new schedules to a report or modify existing schedules on this page.

To schedule a report you must be assigned with the appropriate role associated with that report, and also appropriate permissions on the `Schedules` and `Saved Reports` modules.

To add a new schedule, do the following:

1. On the `Library` page, in the report row for which you want to add a new schedule, click the **Actions** icon, and then select **Schedule Report**.
2. In the `Schedule Details` dialog, configure the following parameters
   a. In case of a report that takes input variables, you must specify the required inputs in the `Report Inputs` section.
   For example, if a report requires the incident id as an input parameter, then you must enter the Incident ID in the Report Inputs section.

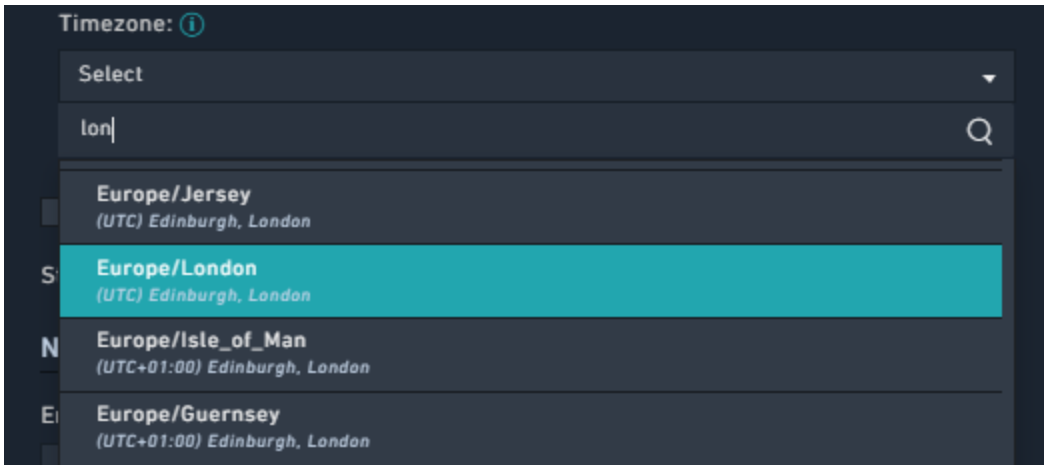


b. In the **Schedule Name** field, enter the name of the schedule.

c. If you want to start the schedule immediately after creating the schedule, click the **Start Schedule** checkbox.

d. In the `Cron Expression` section, add a valid cron expression to schedule the report.
Cron expression is a string consisting of up to five subexpressions (fields) that describe individual details of the schedule.
In the Cron Expression section, you can click the Hourly, Daily, Weekly, Monthly or Yearly links in the `By` row to schedule your report and define the schedule for your report. For example, to schedule a report to run weekly at 9:00 am in the morning every Monday, click the **Weekly** link and in the hour box type `9`, in the minute box type `0`, and in the day of the week type `1` (0-Sunday, 1-Monday, 2-Tuesday...6-Saturday) as shown in the above image. A short description of the schedule also appears below the cron expression box, in our example, it appears as `At 9:00 AM, only on Monday`, which means the report will run every Monday at 9 am as shown in the above image.
Note: The schedule runs as per the timezone selected in the **Timezone** drop-down list.

e. From the **Timezone** drop-down list, search for and select the timezone in which you want to export the report. For example, if you want to search for the timezone of London, you can type `lon` in the search box below the Timezone field to find the correct timezone.



The time that is displayed in the generated reports, i.e., reports that are present in the **History** tab, will be based on the timezone you have selected.
If you do not select any timezone, then by default, the timezone is set as UTC.

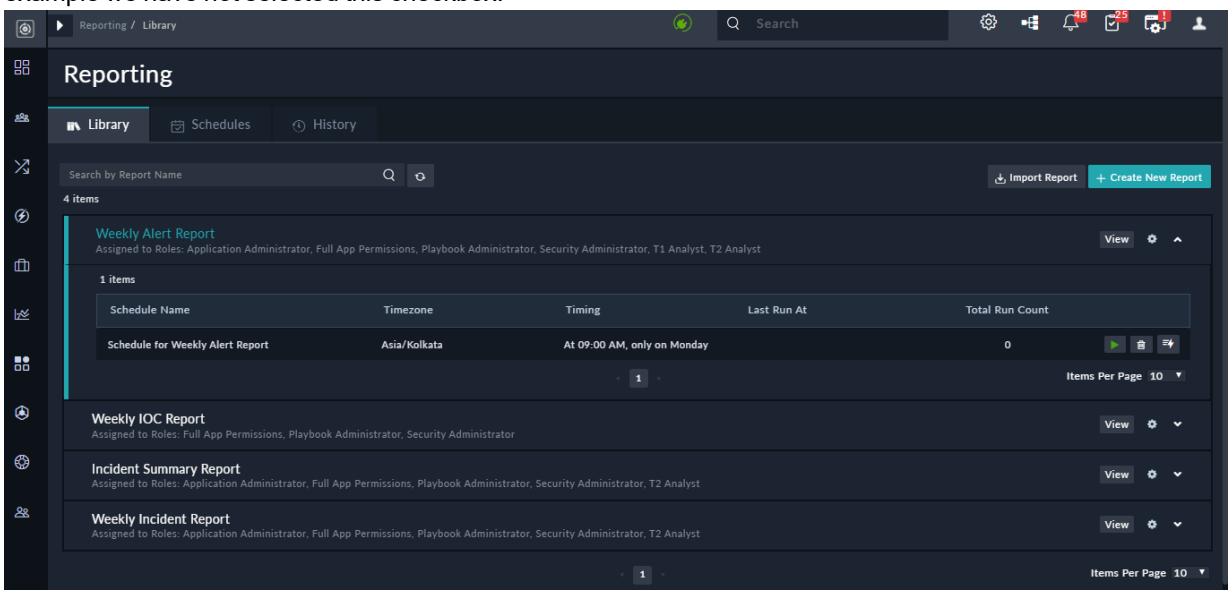
f. If you want to ensure that you do not rerun the workflow, if previous scheduled instance of the report is yet running, then click **Limit execution to one active instance at a time**.

g. (Optional) In the **Start Time** field, you can specify the date and time from when the schedule will start running.

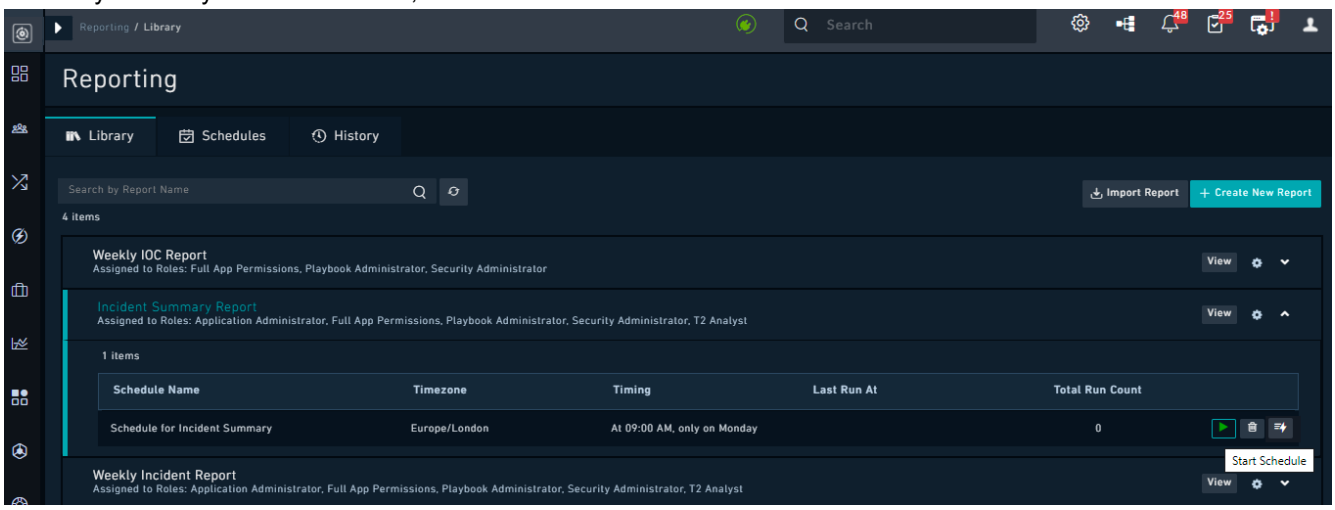
h. (Optional) In the **End Time** field, you can specify the date and time after which the schedule will not run, i.e., the date and time to stop the schedule.
Note: Once a schedule reaches the specified end time, then the schedule displays **Yes** in the Expired column on the schedules listing page. It is recommended that you should make the expired schedules "Inactive".

i. In the **Email Address** field, enter a semicolon-separated list of email IDs to whom you want to send this scheduled report.
Note: Ensure you provide valid email addresses.

j. Click **Save** to save this schedule.
You can also choose to immediately run and display the report, i.e., run the report schedule immediately (outside of its scheduled time) by clicking the **Run Schedule Now** button.
The schedule is saved in the **Inactive** state if you have not selected the **Start Schedule** checkbox. In our example we have not selected this checkbox.

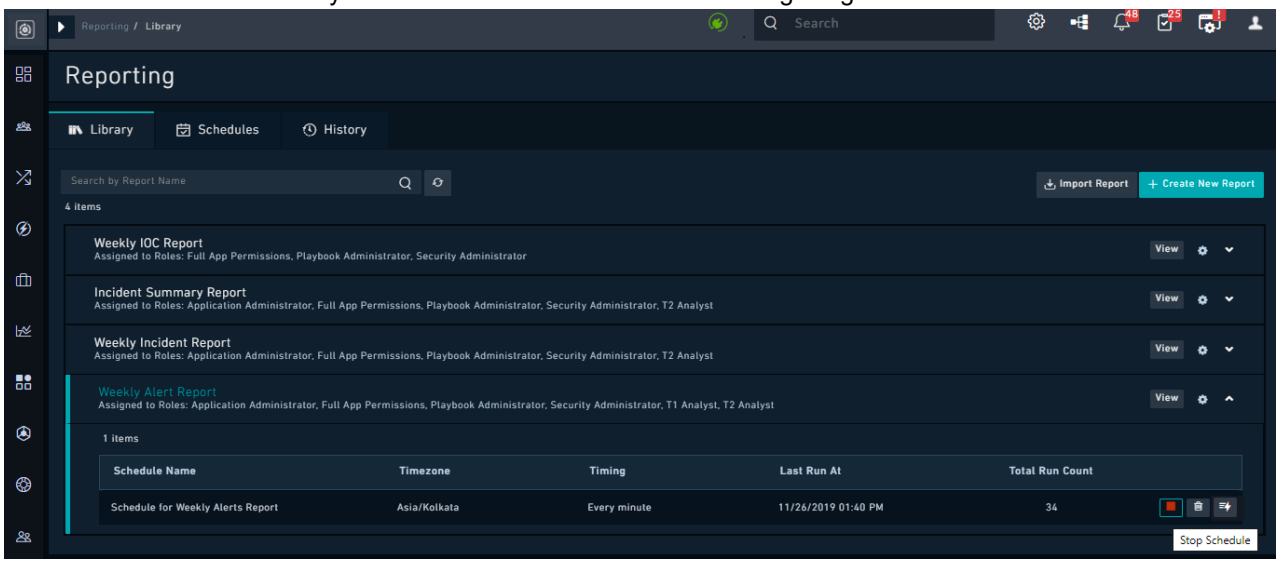


To start your newly created schedule, click the **Start Schedule** button in the schedule row:



To perform other actions, on the `Library` page, do the following:

- To view schedules associated with reports and the details of the schedule, click the down arrow in the report row whose associated schedules you want to view as shown in the following image:

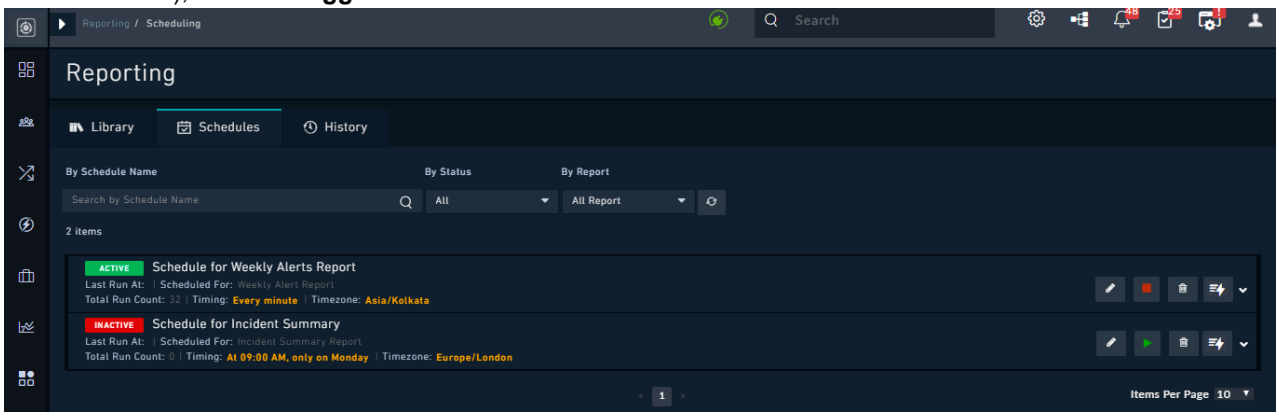


  The schedule details include information such as, the name of the schedule, the schedule timezone, the timing of the schedule, the last run of the schedule, and the total run count of the schedule. You can also stop a running schedule using the **Stop Schedule** button; similarly, you can also start a stopped schedule using the **Start Schedule** button. If you want to immediately view a report (outside of its scheduled time), click the **Trigger Schedule Now** icon, which immediately triggers the schedule associated with the report.
  Note: When you stop a schedule the value, i.e., datetime of the **Last Run At** field becomes blank.
- To modify a schedule, click the down arrow in the report row whose associated schedules you want to modify, and then click on the schedules row. This will display the `Schedule Details` dialog, using which you modify an existing schedule.

Click the **Schedules** tab, to do the following:

- View a list of all the schedules associated with reports, i.e., all schedules that have been created for reports are visible on this tab.
- Search for schedules by schedule name.

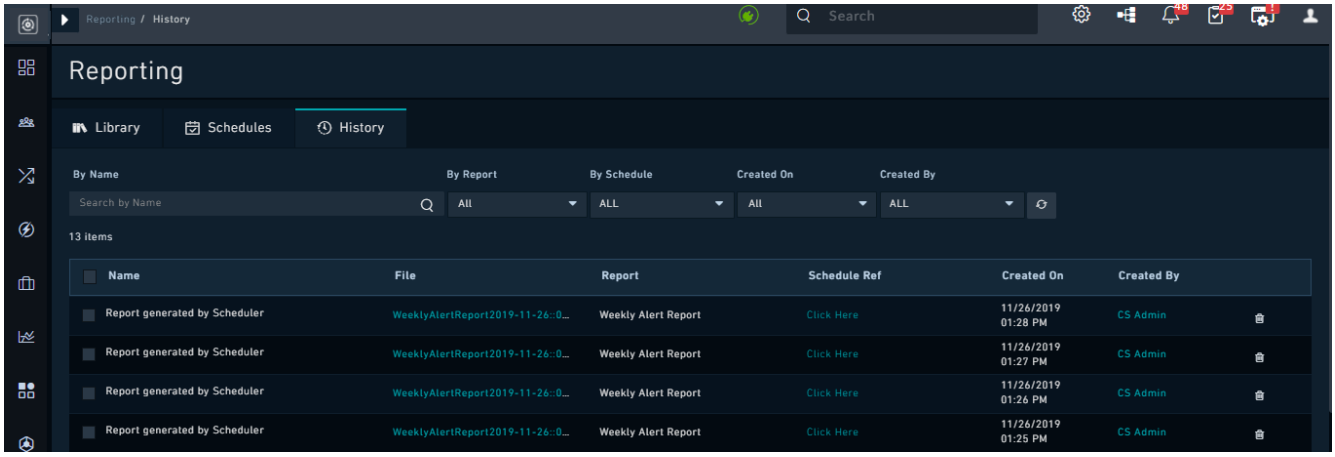
- Filter schedules by Status and Report name. Filtering by Report name will display the schedule associated with the report. One report can have multiple schedules, but one schedule can only be associated with a single report.
- Refresh the `Schedules` page using the **Refresh** icon.
- Perform the following actions in a particular schedule row: Stop a running schedule using the **Stop** button in the schedule row; similarly, you can also start a stopped schedule using the **Start** button. Update a schedule, by clicking the **Edit** icon. Clicking the **Edit** button, displays the `Schedule Details` dialog, using which you can update the schedule. Delete a schedule by clicking the **Delete** icon. To run a schedule immediately (outside of its scheduled time), click the **Trigger Schedule Now** button.



- View brief details of the reports associated with the schedule by clicking the down arrow in the row of the schedule whose report details you want to view.
  The report details include information such as, name of the playbook that ran for the schedule, a link to the PDF version of the report, the name of the report, the date on which the schedule was created, and the name of the user who created the schedule. Clicking the report link in the `File` column downloads the PDF version of the historical report associated with the schedule.

Historical Reports

Click the **History** tab to view a list and details of all created (historical) reports on this page, as shown in the following image:



The historical report details include the name of the playbook that ran for the schedule, a link to the PDF version of the report, the report name, a link to the `Schedule Details` dialog using which you can update the schedule of the report,

the datetime when the historical report was created, and the name of the user who created the report. Clicking the report link in the `File` column downloads the PDF version of the historical report.

You can refresh the `History` page using the **Refresh** icon. To delete a historical report click the **Delete** icon in the row of the historical report you want to delete.

You can search for historical reports by the report's historical name and also filter reports and schedules on this page based on the following criterion:

- **By Report Name**: Enter the name of the saved report that you want search.
- **By Report**: Select the name of the report from this drop-down list to filter reports.
- **By Schedule**: Select the name of the schedule from this drop-down list to filter reports.
- **Created On**: Select the relative date range within which you want to search for created reports, for example, all reports created in the Last 30 Mins.
- **Created By**: Select the user from this drop-down list to filter reports based on the user who has created the reports.

War Rooms

Overview

War rooms enable SOC teams to get into a collaborative space to mitigate a critical cyber threat scenario or campaign. FortiSOAR makes it easy for analysts to quickly provision a War Room and ensures that the task force is well-equipped to handle and coordinate all aspects of critical situations. FortiSOAR enables stakeholders to analyze and collaborate to quickly mitigate the threat.

To effectively run a war room, you must be able to communicate effectively to both internal and external stakeholders. You must also be able to coordinate between teams, investigate the root cause, and resolve the problem by allocating tasks to specialists, agreeing on milestones, taking notes of technical analysis and solution proposals, and getting feedback on all points. It is also important to be able to escalate issues to executive management so that the management team can decide on the next course of action.

FortiSOAR provides you with the war room framework and allows you to define policies to achieve the functionality required to effectively run the war room. This ensures that members of your SOC team can handle major incidents or threats faster.

The process that is generally followed for threat mitigation is as follows:

1. Create a Response Team who will be owners of the threat and responsible to respond to the threat. In a FortiSOAR War Room record, using the **Dashboard** screen, you can create a response team easily and add or remove users and/or teams. For more information, see the Gather a response team section.
2. Assign Tasks: Create a task list of all activities that are generally required to respond to a threat and assign those to appropriate members of the response team. You can easily achieve this using the Task Management tab in the war room record.
3. Investigate the incident: Investigate the threat or incident to find out the root cause and provide the mitigation for the threat. Using the Investigate tab, you can look at related incidents, alerts, indicators, and the assets involved in the investigation. This enables you to look at the bigger picture and assist in investigating and mitigating the threat.
4. Reporting: Timely threat reporting to stakeholders is of utmost importance. You can use the Communication tab in a war room record to view the summary and current status of this threat, send email updates, and also specify the next steps and notes for activities undertaken.

Communication is the key that ties all the above steps mentioned and it is essential for effective mitigation of threats. You should be able to share information and send updates to all the stakeholders with ease. This includes recording and coordinating all activities, such as the context of the issue, the timeline to fix the issue, and the overview of the impact. In this way, when any new team members join the war room, they can quickly be brought up to speed and become an active contributor. Use the Workspace panel to collaborate among stakeholders by adding comments, tagging users, and adding attachments. You can also convey messages and announcements related to the threat to all the stakeholders using the Communication tab, and view the chronological history of all the activities that were performed in the war room using the Timeline tab.

The below sections define how to setup this general flow; however, this flow can be customized to include your changes or additions. You can also customize the War Room module as per your requirements by adding, removing, or modifying fields, picklists, widgets, etc.

You can also repurpose war rooms to set up processes for Business continuity planning (BCP).

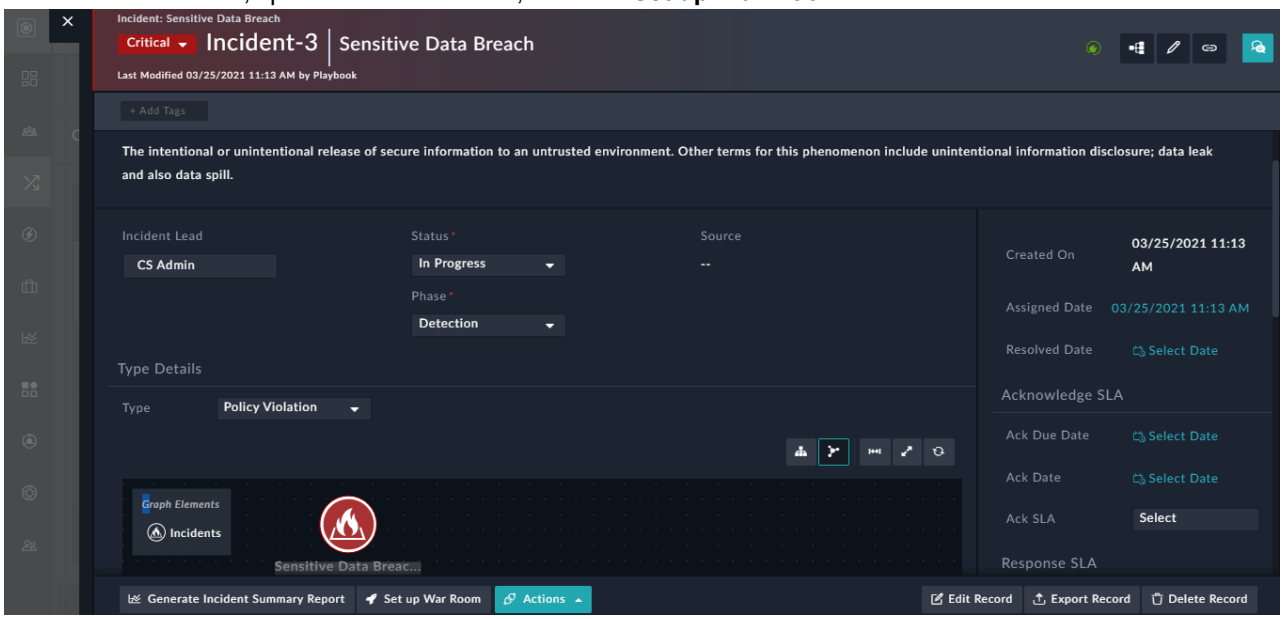
Permissions required

War rooms have their own RBAC settings. To create and use War Rooms, you require CRUD permissions on the War Room module. Teams that have access to War Rooms depend on the team that sets up the war room. Also, in case of War Rooms, you can have user-based ownership in addition to team-based ownership.

In case of a fresh installation of FortiSOAR, the default roles are given access to the War Room module. In case of a FortiSOAR upgrade, users have to enable access to the War Room module.

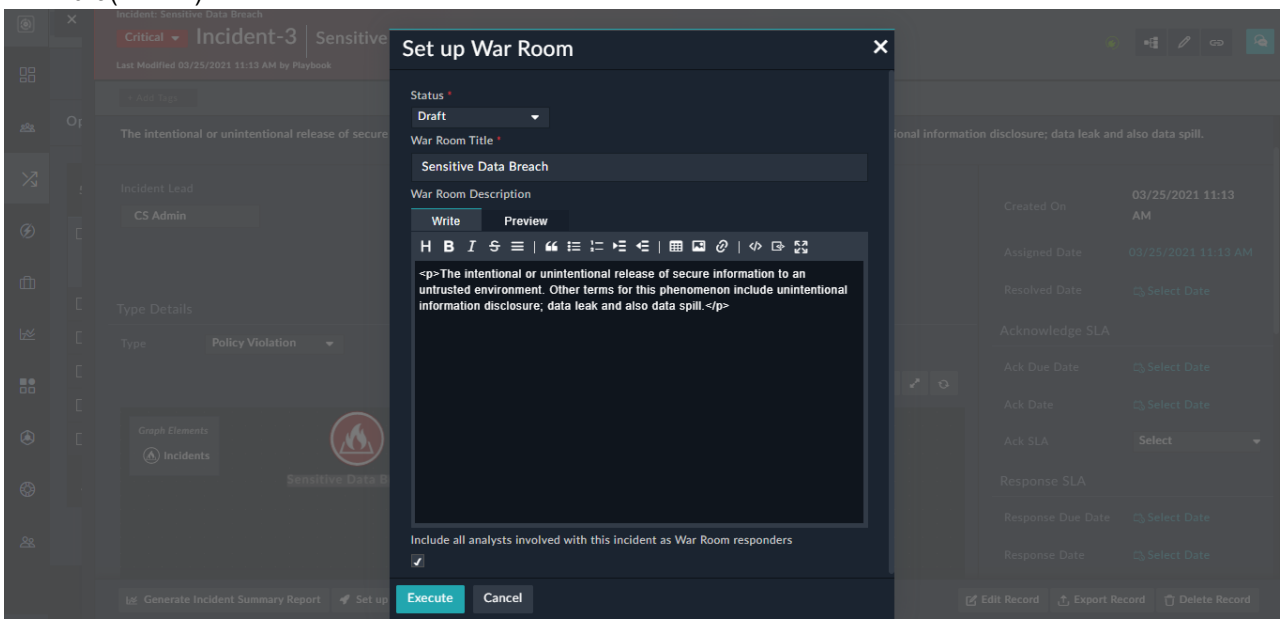
Launching War Rooms

1. To launch a war room, open an incident record, and click **Set up War Room**.

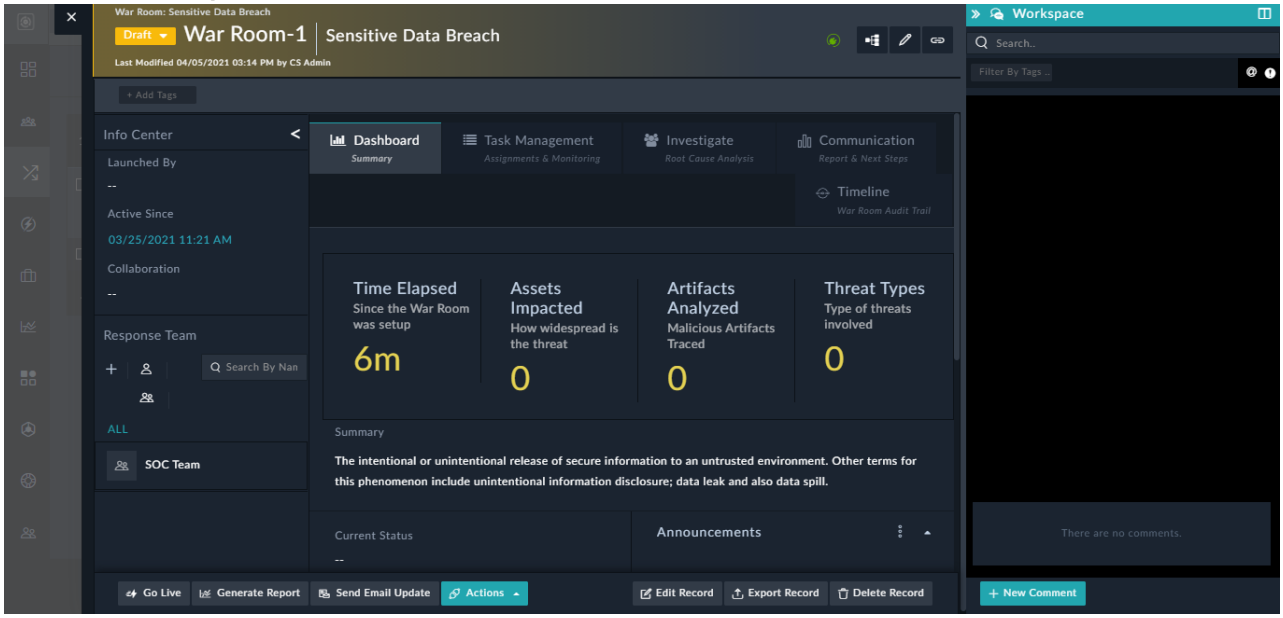


2. In the *Set upWar Room* dialog, enter an appropriate name and description for the war room. Also, ensure that the **Include all analysts involved with this incident as War Room responders** checkbox is selected (default) to include all the users who are part of the team that owns this incident, and then click **Execute** to create a war room in

the **Draft** (default) state.



3. To open the War Room record either click on the link that appears on the incident once the war room is created or click **Incident Response** > **War Rooms** and click the created War Room record:



A link to the war room record is also added to the Workspace of incident.

4. The war room record opens at the **Dashboard** tab which contains the summary of the incident. It is also the place where you can create the response team and assign ownership of this incident to particular users or teams. The war room record also contains other tabs - these are explained in the Setting Up War Rooms section.
Once you have completed setting up the war room, you can begin sending notifications to all the stakeholders, click the **Go Live** button. Apart from this you can edit, export or delete the record. You can also leverage FortiSOAR'playbook/connector framework to rapidly mitigate and contain the threat by directly running playbooks using the **Execute** button. Similarly, you can run connector actions directly on the incident by clicking the **Actions** button. For more information all these operations, see the Working with Modules - Alerts & Incidents chapter.

Once you click **Go Live**, the `Go Live` dialog is displayed. You can add an external collaboration link to collaborate with stakeholders that are not part of FortiSOAR and then click **Go Live**. Once you click **Go Live**, the status of the war room turns from "Draft" to "Active", notifications are sent to all the members of the war room, and the incidents that are linked to the war room display the active War Room in the header widget.

Setting up War Rooms

You can begin setting war rooms by adding team members, assigning tasks, collaborating between the teams, investigating the incident, etc. To facilitate these activities, the war room record contains the Dashboard, Task Management, Investigate, Communication, and Timeline tabs. It also includes a Workspace panel that helps in collaboration. Details of each tab follow:

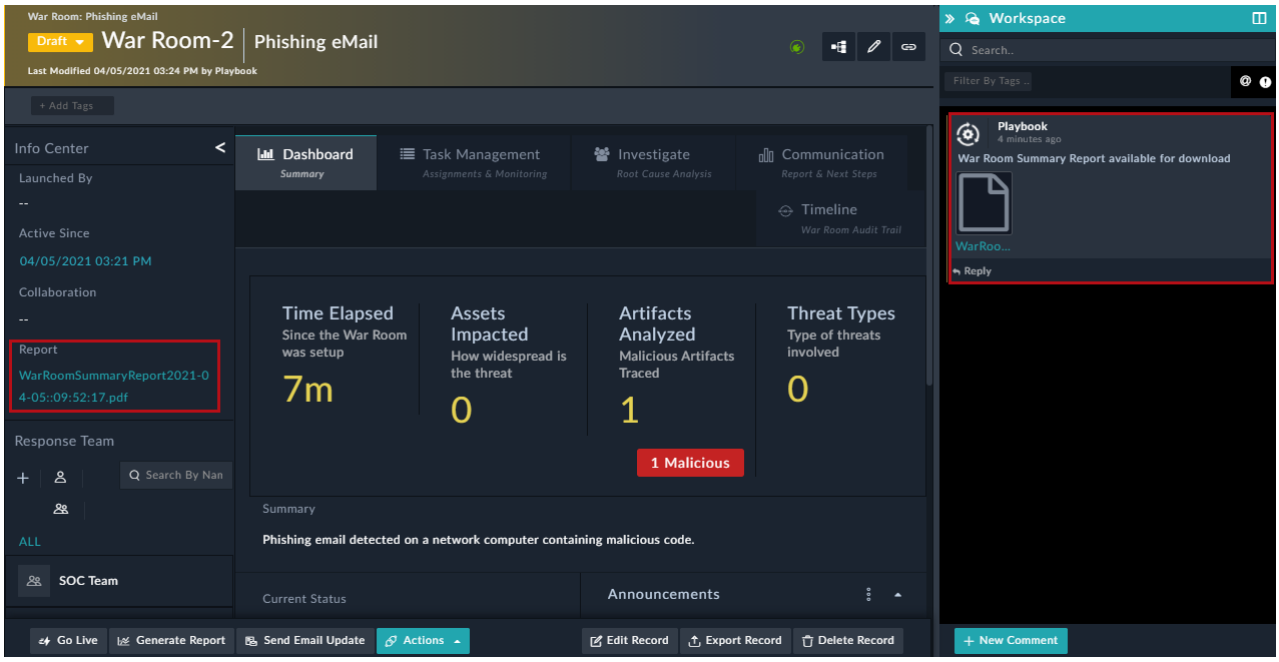
Dashboard

The **Dashboard** tab contains details of the incident such as the description and current status of the incident, time elapsed since the time of the incident, assets impacted by the incident, etc. It also contains the incidents, alerts, indicators, and artifacts that are related to this incident, etc. You can link records to this incident by clicking the **Link record** icon in the *Incidents, Indicators, Assets & Other Artifacts Involved* section.

All modules whose records are related to the war room must be made 'User Ownable'. This is required if you want the records to be viewed by all the responders of the war room.

In the footer of the War Room Record, you can use the following buttons to perform operations:

- **Generate Report**: Click to generate reports and metrics for this threat. When a report is generated, a **Report** field is added to the Info Center and the playbook responsible for generating the report also adds a comment in the Workspace. You can download the generated report, in the PDF format, from the link in the **Report** field or by using the **Download File** link the **Workspace**:

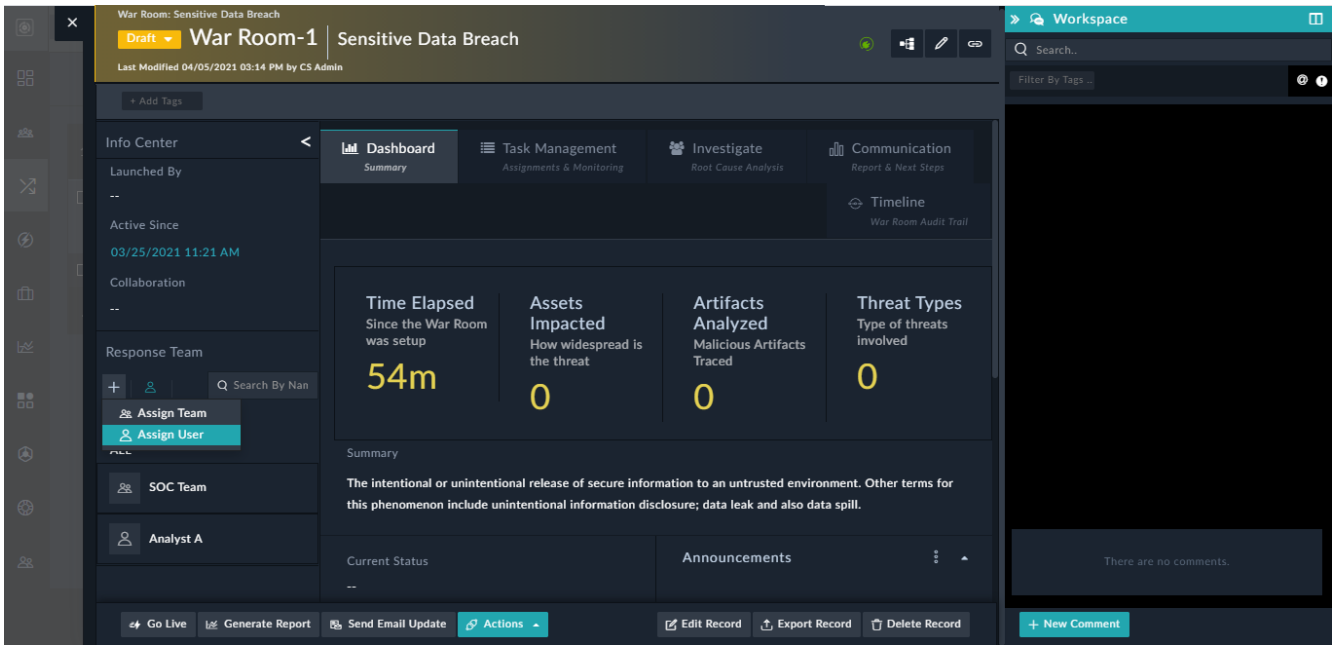


- **Execute**: Click to execute playbook actions on the record.
- **Actions**: Click to execute connector actions directly on the record. You can also add tags to the result of the action making it easier to filter the action logs. You can also add the `Evidence` tag, to mark the result as evidence, which then gets added to the **Evidences** tab within **Investigate**.
  To know more about the **Execute** and **Action** buttons and operations, see the Working with Modules - Alerts & Incidents chapter.
- **Edit Record**: Click to edit the war room record in the Form format.
- **Export Record**: Click to export the war room record in the CSV or PDF format.
- **Delete Record**: Click to delete the war room record.

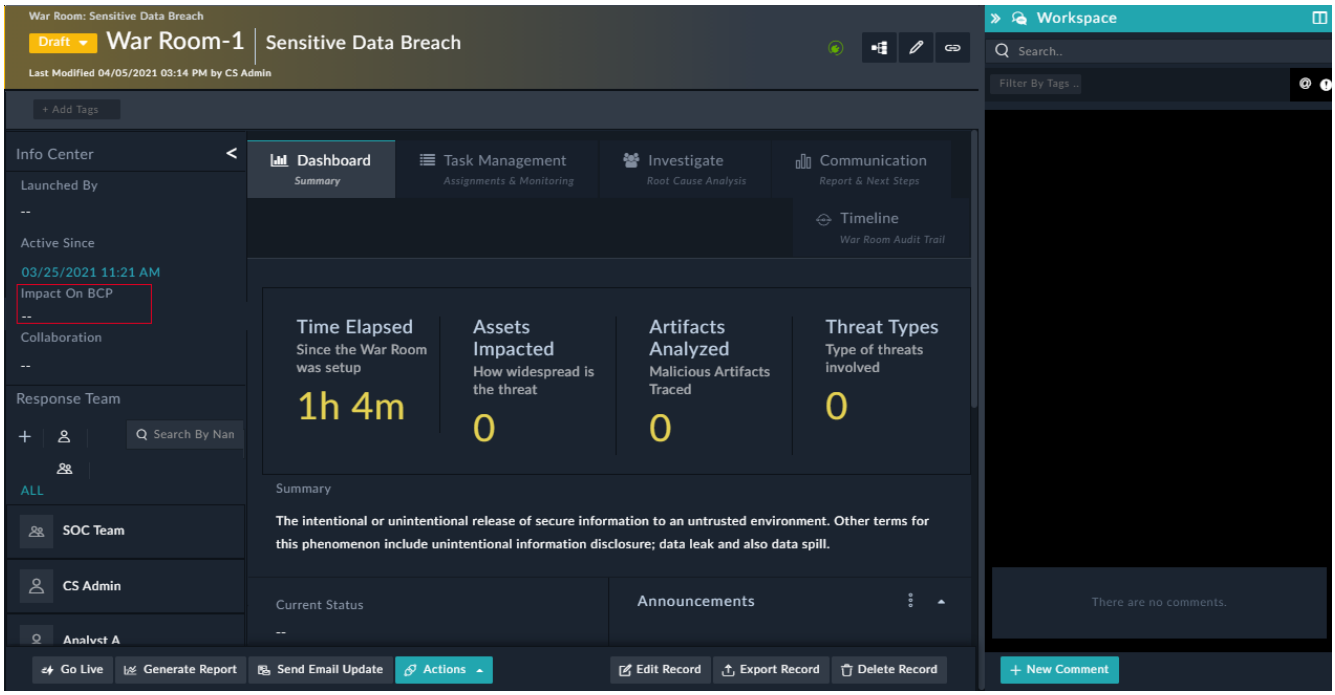
Gathering a response team

The **Info Center** panel is a collapsible panel on the left side of the detail view, and it contains information such as who has launched or set up the war room, from when the war room has been active, and the conference bridge and collaboration details.

It is also where you can find the details of the response team, i.e., the teams and users who are owners of this war room and are responsible to provide a response to this incident. You can assign both teams and users, for example, you have a SOC team that is part of the response team, but you also want Analyst A (who is not part of the SOC) to be an individual owner, then you click the **Users** field and select **Analyst A** from the drop-down list.



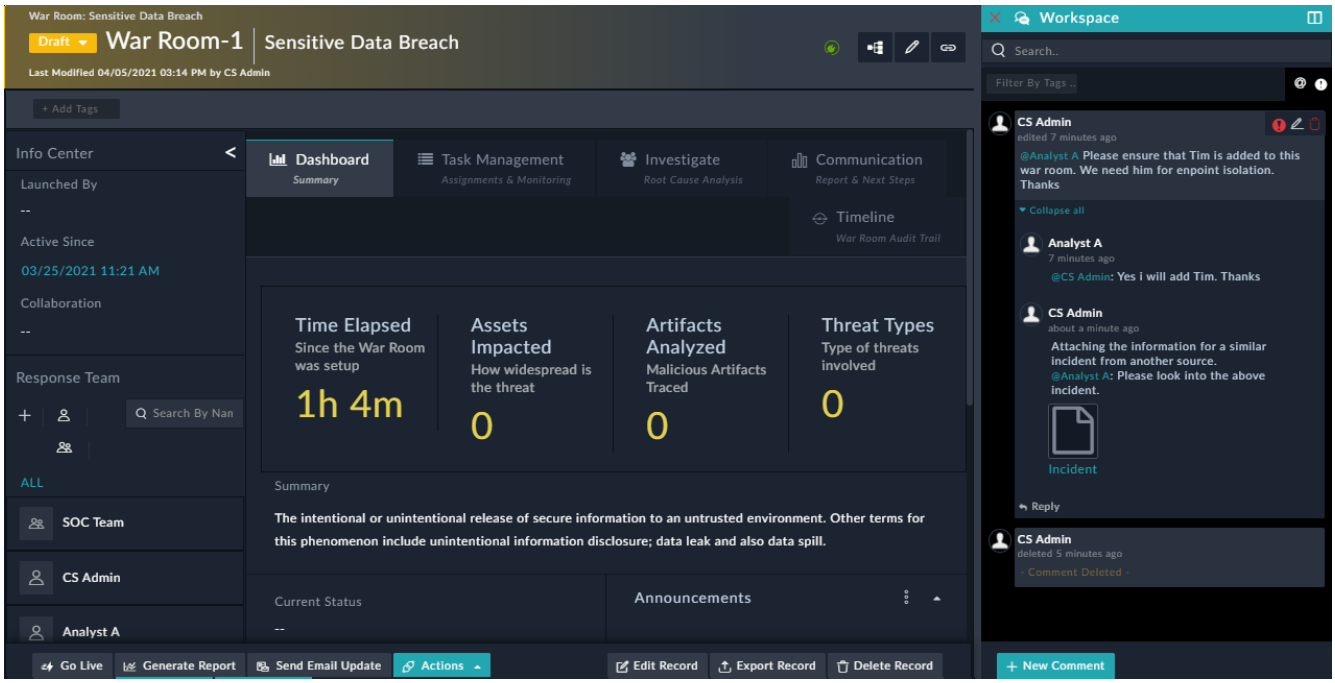
You can edit the form to add or remove fields and widgets to the War Room record as per your requirements. You can add fields to the War Room module, using the Module Editor, for example, you can add a field name 'Impact on BCP' and add this field to the War Room template. You will then be able to see the 'Impact on BCP' field in the war room record, as showing in the following image:



For information on the Module Editor, see the *Application Editor* chapter in the "Administration Guide" For information on editing SVT and widgets, see the Dashboards, Templates, and Widgets chapter.

Workspace - Enabling Communication

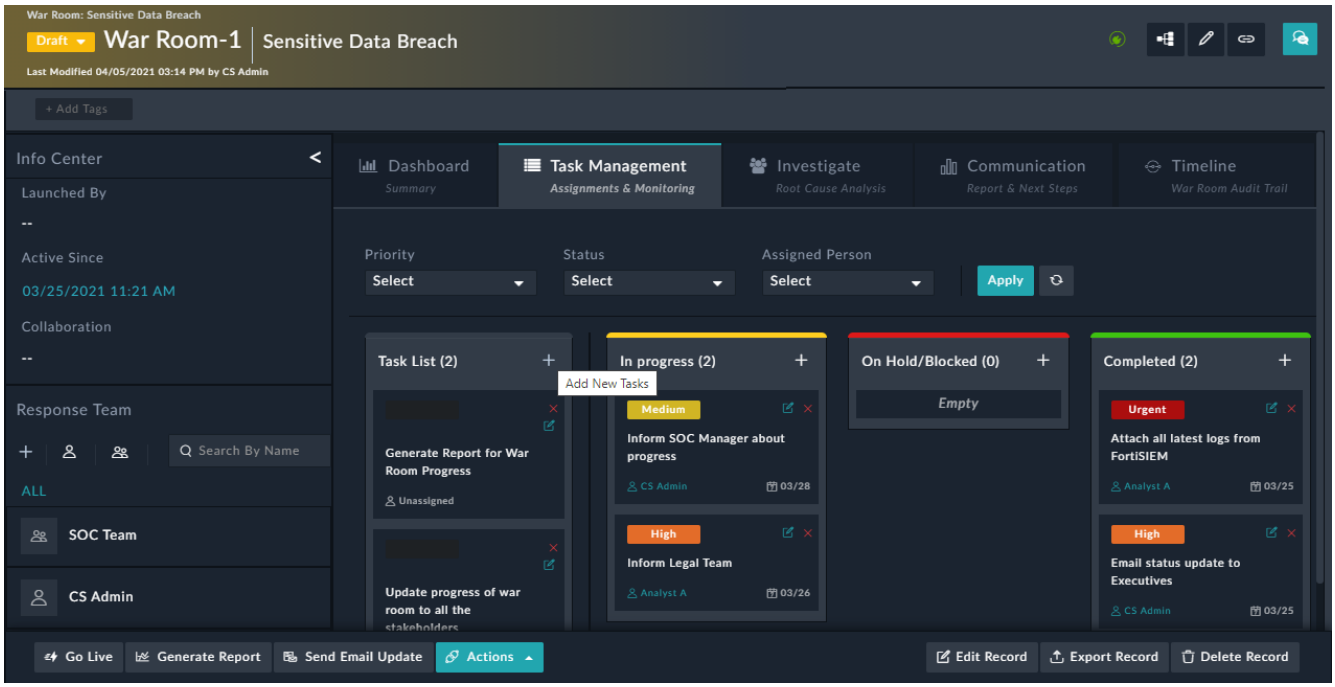
The **Workspace** panel is a collapsible panel on the right side of the detail view, using which collaboration can be easily achieved between various stakeholders by adding comments to the record. This enables participation of various stakeholders and team members across the organization. FortiSOAR supports message threads, which helps in keeping track of conversations and makes it easier to respond to a specific thread. You can add mentions or tagging users in comments by typing @, and then selecting the users from the displayed list, and can also mark a comment as important. Users who are tagged get notified of their mentions by email.



For more information on how comments work in a record, see the Working with Modules - Alerts & Incidents chapter.

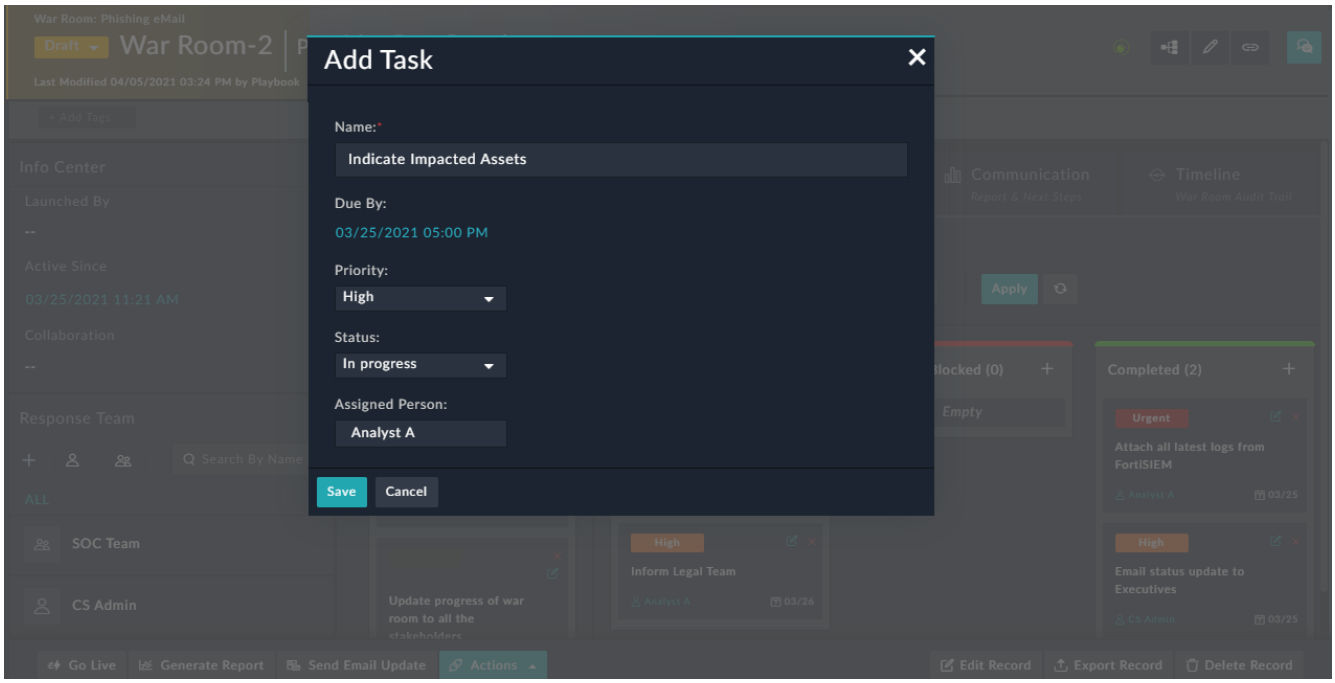
Task Management

Use the **Task Manager** tab to manage all tasks related to the war room. This is where you can create a task list and manage task assignments and track tasks till their completion. The Task Manager contains various task that are grouped by fields such as the **Status** of the task. As shown in the following image, task cards are grouped together based on the status of the task, which are In progress, On Hold/Blocked, and Completed:



Tasks are grouped by **Status** by default, however you can change the grouping as per your requirements, for example, group by **Type**, and can also choose the fields that you want to display on the card, by editing the 'Task Management' widget in the war room record template. For information on editing templates and widgets, see the Dashboards, Templates, and Widgets chapter. FortiSOAR also contains a "Widget Library" that allows you to edit out-of-the-box (OOB) widgets such as the 'Task Management' widget, and build new widgets for custom use cases.

You can create a task list of activities for mitigating the threat and assign it to various members of the team. To create task, click **+** (**Add new tasks**) in the card group/bucket in which you want to create the task:



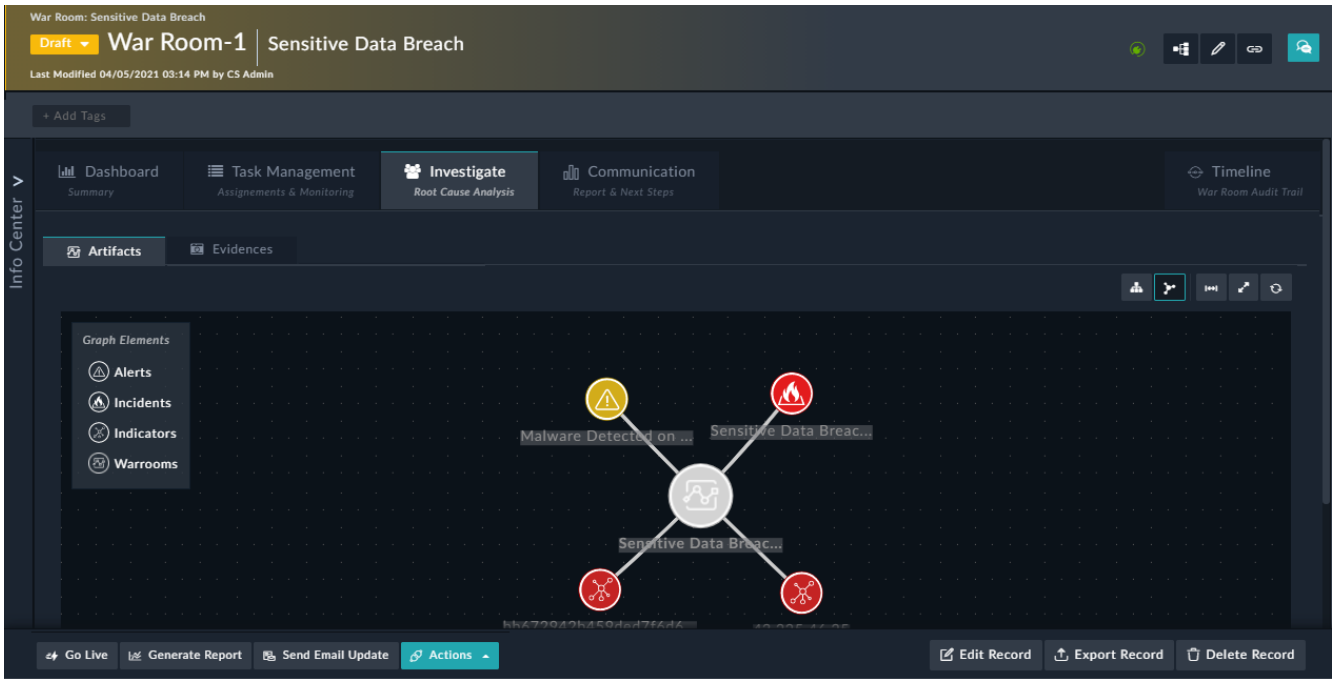
In the **Add Task** form fill in the fields such as name of the task, its due date, priority, and status, and select the person to whom you want to assign the task. You can also leave the task unassigned and assign it to a team member at a later time. Click **Save** to add the card to the task list in the bucket specified by the status you have selected. For example, in the above image the created task will be added to the **In Progess** bucket and the user to whom it is assigned, i.e., **Analyst A** will receive an email notification of the task assignment.

You can also drag and drop cards from one bucket to another to quickly change the task states.

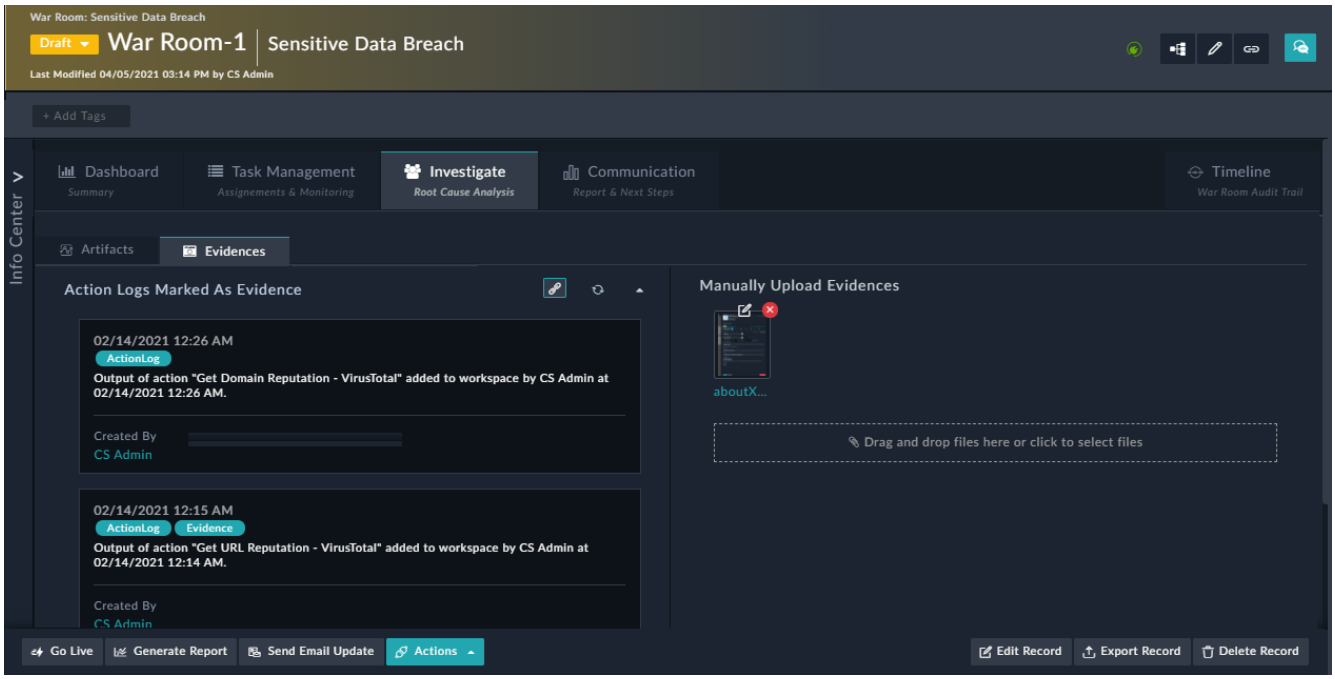
Investigate

Use the **Investigate** tab to investigate the incident and perform root cause analysis. It contains all the records and evidence linked to that particular incident, giving you a complete picture of all the events that lead to the security thread.

It displays an **Artifacts** tab that contains a graphical representation of all the records that are linked to this incident as shown in the following image:



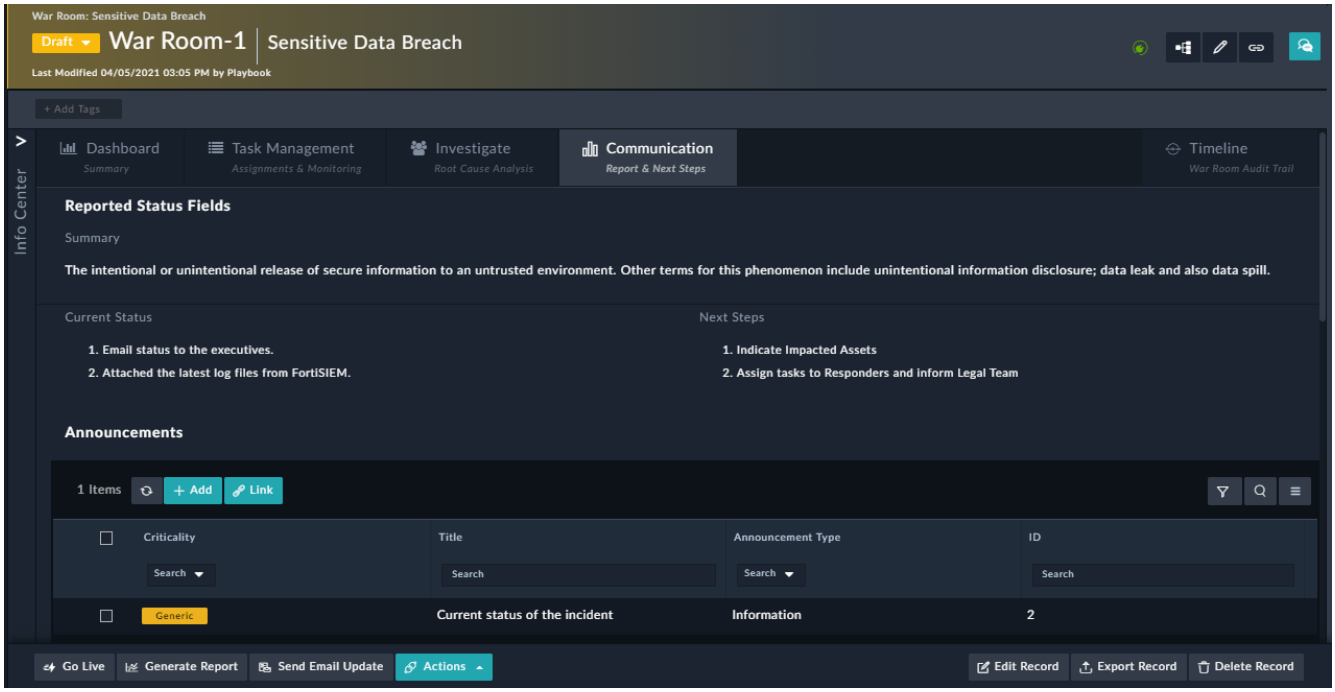
It also contains an **Evidence** tab, where you can view all evidence related to this threat. You can investigate the war room by executing playbooks or connector actions directly on the war room record. For example, you could directly run a 'Get Domain Reputation' action that belongs to the *VirusTotal* connector on this record, and if the result of the action has an impact on this threat, you can tag the result of the action as `Evidence`, which then gets added to the **Evidences** tab. You can also manually upload evidences in this screen, by dragging or dropping the evidence file, or browsing to the evidence file. For more information on action logs and marking an action log as evidence, see the Working with Modules - Alerts & Incidents chapter.



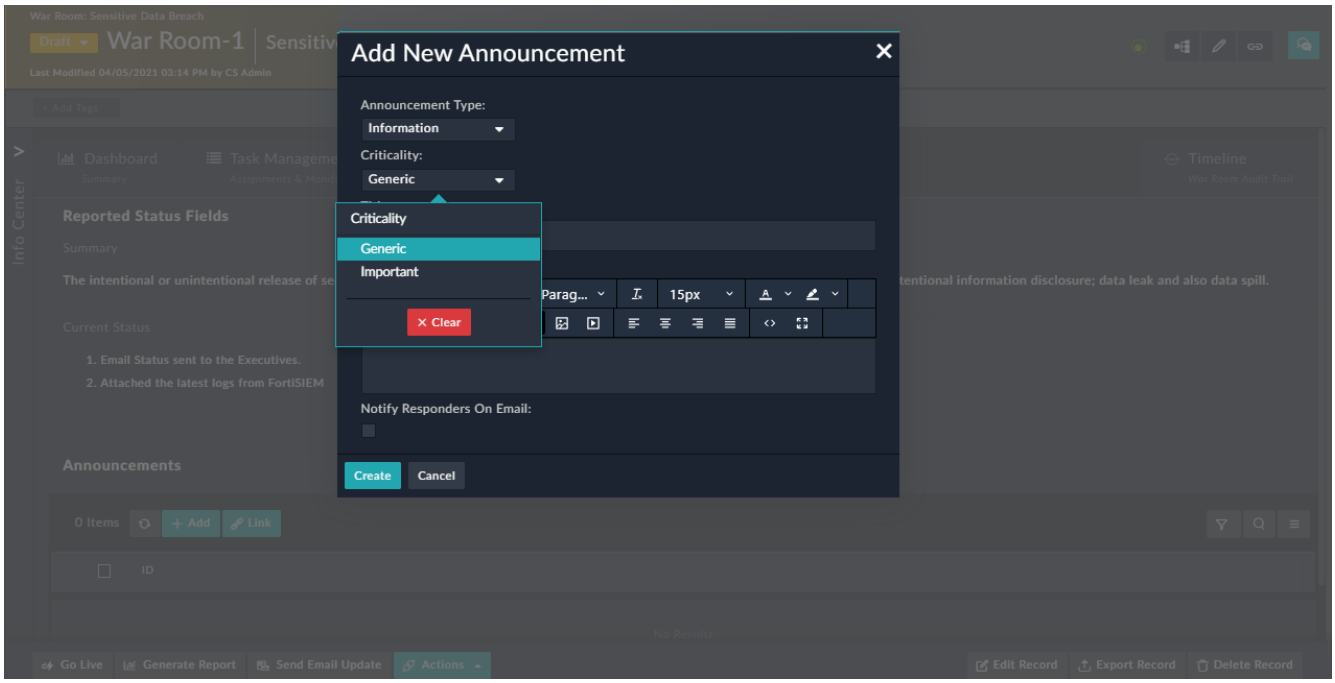
Communication

Use the **Communication** tab to view the summary of the incident, attach or send announcements associated with this threat, and define next steps for the threat. The Communication tab also contains a summary of the threat and its current status.

In the **Next Steps** section, you can add a list of pending tasks, or add notes for the activities undertaken.

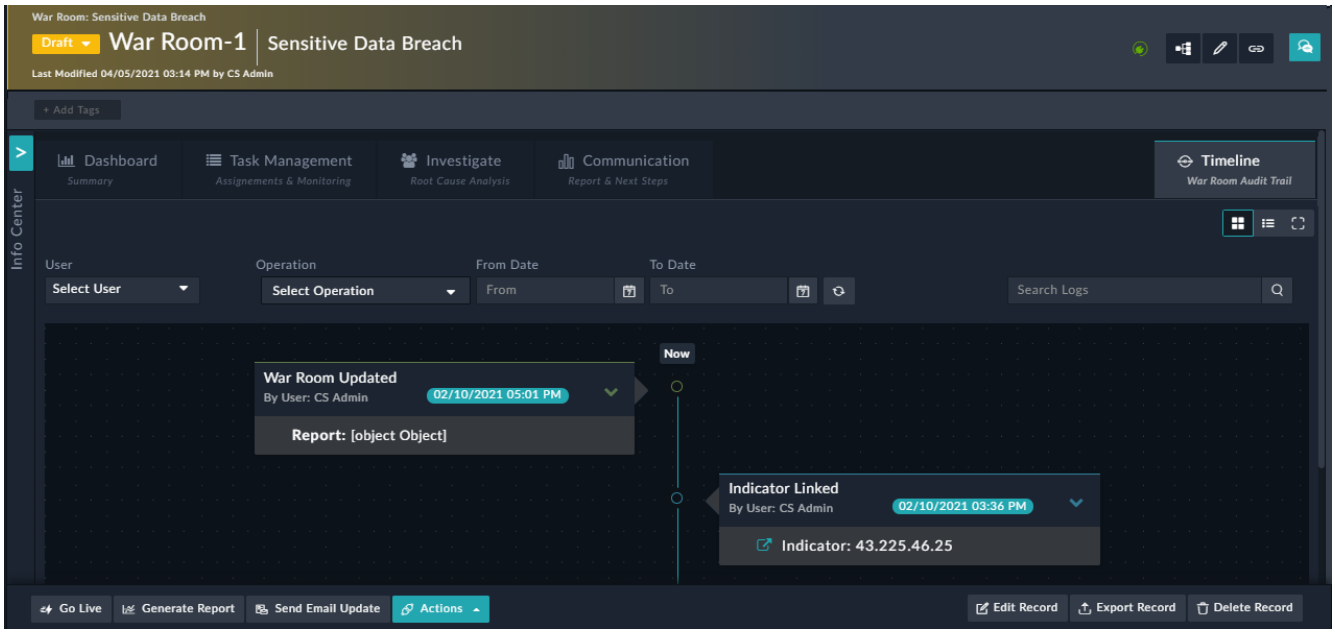


You can also link or send announcements to all the members of the response team. To add an announcement, click the **Add** button, to display the `Add New Announcement` dialog. Select the announcement type, criticality of the announcement, and then enter the title and description for the announcement. **Announcement Types** can be **Meeting**, **Information**, or **Generic**, and its **Criticality** can be **Generic** or **Important**. If you also want to notify the responders by email, then select the **Notify Responders On Email** checkbox:



Timeline

The Timeline tab displays a historical timeline for the current war room, i.e., it displays the chronological history of all the activities that were performed in the war room:



Detailed information of the Timeline widget is present in the Dashboards, Templates, and Widgets chapter.

Schedules

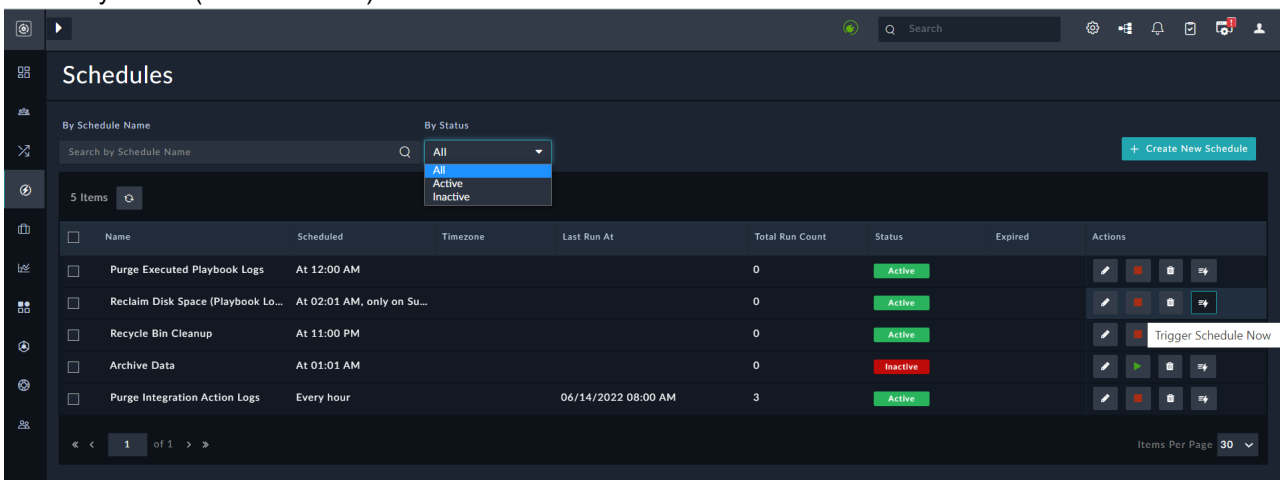
FortiSOAR provides you with a `Schedules` module that allows you to schedule playbooks to run at regular intervals.

Permissions required for working with Schedules

- To access the `Schedules` page, you must be assigned a role with minimum `Read` permission on the `Playbooks` module, which means that this permission must be assigned to users who require to perform any operations such as view, create or update schedules.
- To create and update schedules; you must be assigned a role with a minimum of `Create`, `Read`, and `Update` permission on the `Schedules` module. To modify schedules, you must be assigned a role with a minimum of `Read` and `Update` permission on the `Schedules` module. To view the existing schedules, you must be assigned a role with a minimum of `Read` permission on the `Schedules` module. To create and delete schedules, you must be assigned a role with a minimum of `Create`, `Read`, `Update`, and `Delete` permission on the `Schedules` module.

Working with Schedules

1. Click **Automation** > **Schedules** in the left navigation bar.
   On the `Schedules` page you can see the list of schedules created. You can also filter schedules by schedule name and/or By Status (Active/Inactive):

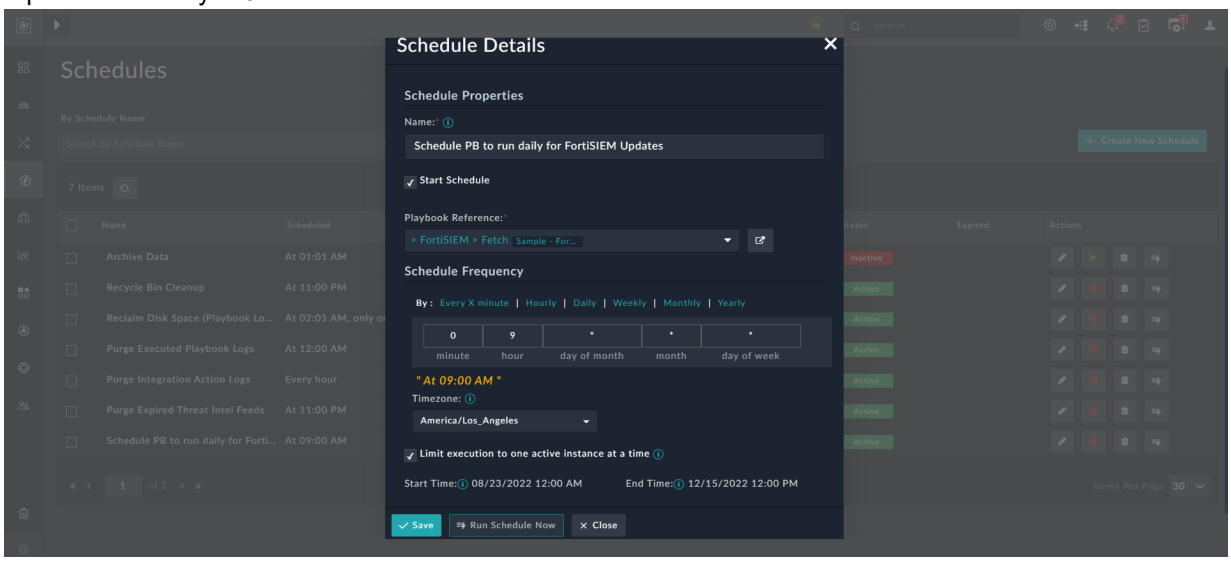


2. To define a new schedule for a periodic playbook, on the `Schedules` page, click **Create New Schedule**.
3. In the `Schedule Details` dialog, enter the following details:
   a. In the **Name** field, add the name of the schedule.
   Note: Schedule names must be unique and comprehensive. You should be able to understand what the purpose of the schedule is by reading the name of the schedule. For example, if you want a playbook to run every day and connect to your SIEM, for example, FortiSIEM, and gather incidents from FortiSIEM, and then make the corresponding updates in the FortiSOAR `Alerts` module, you can name such a schedule as `Schedule PB to run daily for FortiSIEM Updates`.

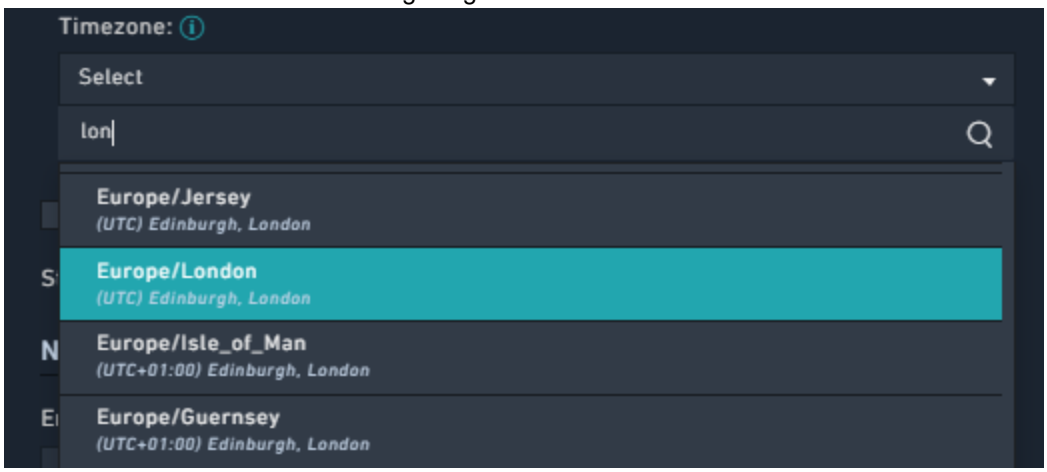
b. If you want to start the schedule immediately after creating the schedule, click the **Start Schedule** checkbox.

c. From the **Playbook** drop-down list, select the playbook that you want to schedule.

d. In the **Schedule Frequency** field, add a valid cron expression.
Cron expression is a string consisting of six or seven subexpressions (fields) that describe individual details of the schedule.
In the Cron Expression section, you can click the **Every X minute**, **Hourly**, **Daily**, **Weekly**, **Monthly**, or **Yearly** links in the `By` row to add a schedule.
For example, to schedule a report to run daily at 9:00 am in the morning, click the **Daily** link and in the Minute box type `0` and in the Hour box, type `9`, as shown in the following image. A short description of the schedule also appears below the cron expression box, in our example, it appears as `At 9:00 AM`, which means the report will run daily at 9 am.



e. From the **Timezone** drop-down list, search for and select the timezone in which you want to export the report associated with this schedule. By default, the timezone is set as UTC. You can search for a timezone in the **Search** box as shown in the following image:



f. If you want to ensure that you do not rerun the workflow, if previous scheduled instance of the schedule is yet running, then click **Limit execution to one active instance at a time**.

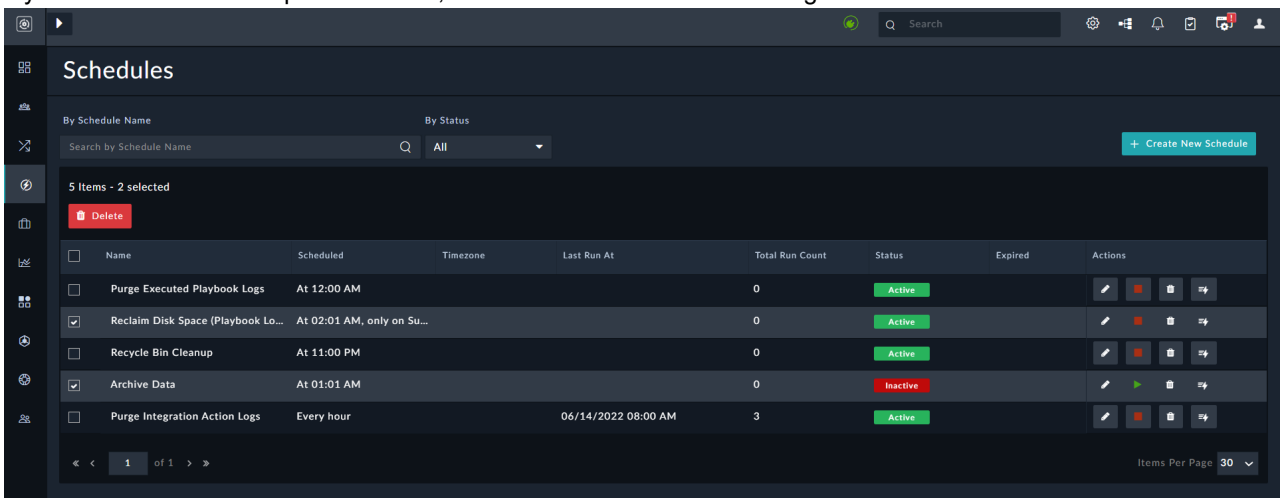
g. (Optional) In the **Start Time** field, you can specify the date and time from when the schedule will start running.

h. (Optional) In the **End Time** field, you can specify the date and time after which the schedule will not run, i.e., the date and time to stop the schedule.

Note: Once a schedule reaches the specified end time, then the schedule displays **Yes** in the Expired column on the schedules listing page. It is recommended that you should make the expired schedules "Inactive".

i. Click **Save** to save the schedule.
To run the schedule immediately, click the **Run Schedule Now** button.

4. Once you create a schedule, if you have not selected the **Start Schedule** checkbox, then the schedule remains in the **Inactive** state until the schedule starts at the date and time you have specified in the Start Time field. You can also manually start the schedule by clicking the **Start Schedule** icon (green play icon) in the `Actions` column.
To stop an **Active** schedule, click the **Stop Schedule** icon (red stop icon) in the `Actions` column.
Note: When you stop a schedule the value, i.e., datetime of the **Last Run At** field becomes blank.
To edit a schedule click the **Edit** icon in the `Actions` column, which will display the `Schedule Details` dialog in which you can edit the schedule properties.
To delete a schedule click the **Delete** icon in the `Actions` column, which will display the `Confirmation` dialog and once you click **OK** in it the schedule gets deleted.
If you want to delete multiple schedules, then select the schedules in the grid view and click **Delete**.



To run a schedule immediately (outside of its scheduled time), click the **Trigger Schedule Now** icon in the `Actions` column.

On the `Schedules` page, you will see a schedule named "Integration Action Log Purge" active on the `Schedules` page by default, which is scheduled to run every hour and purge action integration logs. When any interaction is performed using a FSR Agent, for example, invoking a direct connector action using an FSR agents, such requests are first stored in the `connector_executeaction` database table in the base FortiSOAR node with its state set as "In Progress". Once the response is received from the FSR agent then the state of this entry is updated to "Finished". The "Integration Action Log Purge" schedule clears these logs since they tend to grow after some time. Note that this action log is an event details store in the database and *not* a log file in the system. This schedule is associated with the "Purge Integration Logs" playbook that is part of the System Fixtures (**Settings** > **System Configuration** > **System Fixtures** > **Schedule Management Playbooks**).

Tutorial: Creating an Incident Form for the Phishing Type of Incident

Purpose

This tutorial aims at walking you through the steps you require to create Incident forms for various types of incidents, such as Phishing, using FortiSOAR.

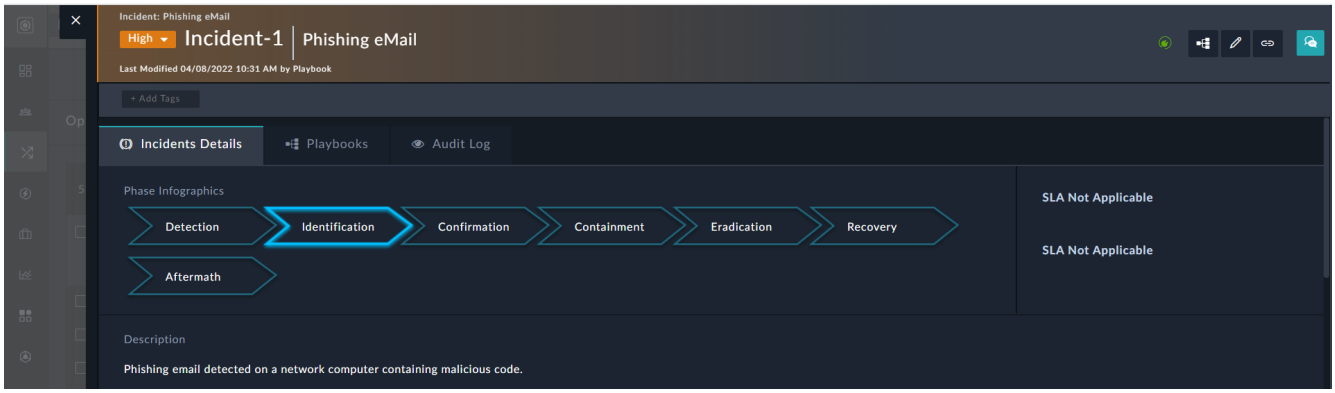
Incidents represent a collection of information discovered during an Incident Response investigation. Incidents are triggered based on the suspicion or confirmation of a security breach. Incidents can be cyber or physical security related.

This document assumes that you have completed the installation and configuration of your FortiSOAR instance and now you are ready to create records in FortiSOAR.

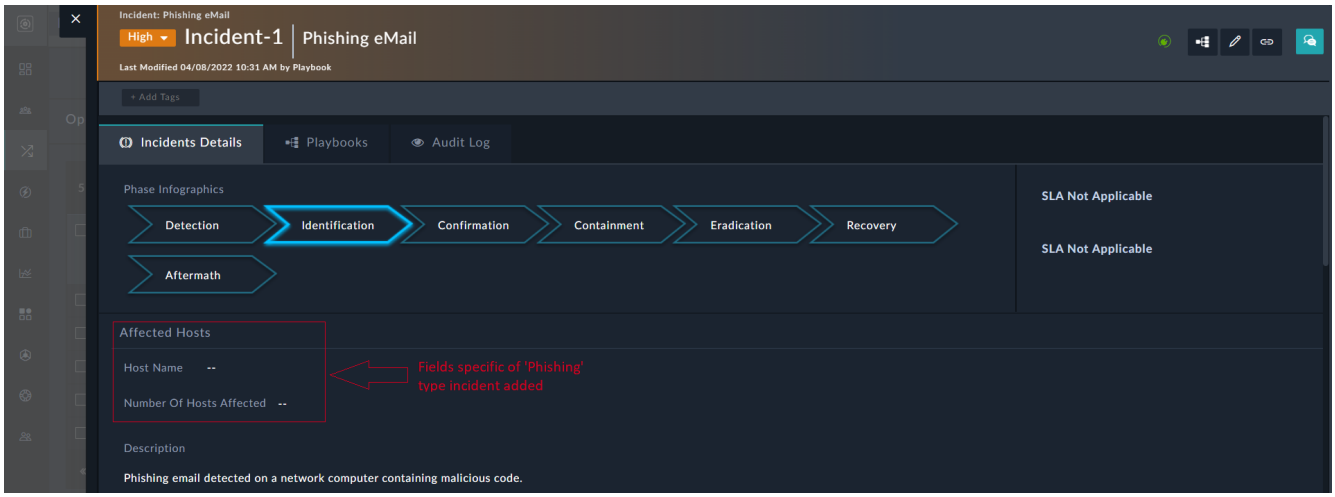
Phishing Type of Incident should have the following additional fields, apart from the general fields of the Incident Record:

- Host Name
- Number of Hosts Affected

The Phishing Type of Incident Record without the above fields is displayed as follows:



The Phishing Type of Incident Record with the above fields will be displayed as follows:



These records will only be displayed in forms when the Incident Type is set to "Phishing."

To achieve this, we will have to perform the following steps:

1. Add the required fields to the Incident of type "Phishing" using the Module Editor.
2. Publish the Incidents module.
3. Update the System-View Templates (SVT) for the Incidents module.

Adding required fields to the Incident of type "Phishing" using the Module Editor

Use the Module Editor in FortiSOAR to add new modules, add new fields, and edit existing fields within a module. In our case, we assume that the Incident Module is already created with default fields and we require to add specific fields for the Phishing Type Incident. See the *Application Editor* chapter in the "Administration Guide" for information on how to add modules.

1. Log on to FortiSOAR using your credentials.
2. Click the **Settings** ( ) icon that appears on the top-right corner in FortiSOAR and in the `Application Editor` section, click **Modules** to open the `Modules` page.
3. To add fields to the Incidents module, select **Incidents** from the Modules drop-down list, click the **Fields Editor** tab on the `Modules` page and click the Add (**+**) icon beside Fields.
4. To add the **Host Name** field, configure the following properties for the field:
   a. **Field Type**: The type of field; it specifies the type of form used to render this attribute. For example, a checkbox, a picklist, or a Text field.
   For the Host Name field, select **Text Field**.
   b. **Sub-Type**: This is the sub-type of the Field Type that narrows down the input format to any specific type such as Text Field, Phone Field, Email Field etc. For the Host Name field, select **Text Field**.
   c. **Field Title**: A short display name describing the field.
   For the Host Name field, type `Host Name`.
   d. **Editable**: Selecting this option allows you to modify the field after the creation of a module record. If this option is not selected, then you cannot modify the initial value after the record is created.
   For the Host Name field, ensure that the **Editable** checkbox is selected.

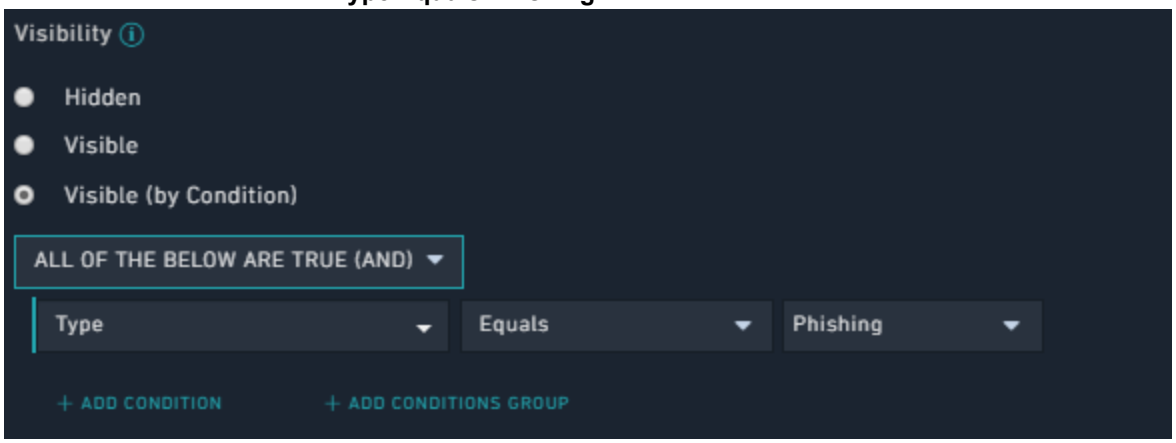
e. **Searchable**: Selecting this option makes this field searchable in the grid view.
Check the Searchable option for the Host Name field. For the Host Name field, ensure that the **Searchable** checkbox is selected.

f. **Default Grid Column**: Selecting this option makes the field appear as a column by default in the grid view.
For the Host Name field, ensure that the **Default Grid Column** checkbox is cleared.

g. **Encrypted**: Selecting this option enables encrypting of field values before storing in the database for enhanced security.
For the Host Name field, ensure that the **Encrypted** checkbox is cleared.

h. **Required**: Specifies whether the field is a required field.
Select **Not Required** for the Host Name field.

i. **Visibility**: Specifies whether the field is visible or not. For the Host Name field, select **Visible (by Condition)**.
In the condition builder select **Type Equals Phishing**.



This means that the Host Name field will only be visible when the Incident type is set as Phishing. Note that the `IncidentType` is a Picklist type of field and using FortiSOAR you can define your incident types by editing this picklist or creating new picklists.
See the *Application Editor* topic in the "Administration" guide for information on how to create picklists and use condition builder and also for detailed explanations on fields and their properties.

j. **Default Value**, **Tooltip**, and **Length Constraints**: For the Host Name field, for the purpose of this example, leave these field blank.

k. **Allow Bulk Edit**: Selecting this option allows the bulk edit operation on the selected field, this means that you can select multiple records in the **Incidents** grid view and change the value of this field in a single click.
For the Host Name field, for the purpose of this example, do not select this option.

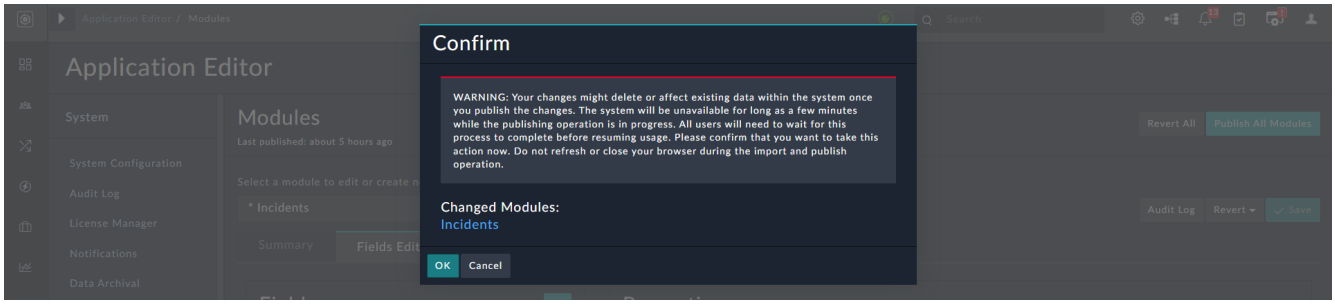
l. Click **Apply** to add the Host Name field to the `Incidents` module.

5. Click **Add Field** to add the Number of Hosts Affected field and configure similar properties for these fields:
   a. **Field Type**: select **Integer**.
   b. **Field Title**: type `Number of Hosts Affected`.
   c. Configure the remaining properties for the Number of Hosts Affected field, similar to that of the Host Name field, including setting the Visibility of these fields to **Visible (by Condition)** and in the condition builder select **Type Equals Phishing**, to ensure that these fields are also only visible if the Incident Type is Phishing.
   d. Click **Apply** to add the Number of Hosts Affected field to the `Incidents` module.
6. Click **Save** to save the changes to the `Incidents` module.

Publishing the Incidents Module

Whenever you change a field or a module and click **Save**, the change is staged but is not yet live in the system. You must perform a Publish to ensure that the changes are made in the system.

You initiate a publish action by clicking the Publish All Modules button at the top-right of the Module Editor page. Publishing pushes the changes that you have made to fields and modules to the database. Up until the Publish point, all changes to the data model in the Module Editor are saved as metadata, which is information that describes the structure of other information.



Updating the System View Templates (SVTs)

The FortiSOAR interface is rendered using Templates, which can be modified as needed to suit your specific purposes better. You can structure and style forms with varied types of fields by modifying templates according to your requirements. The system interface is composed of View Templates, which are JSON definitions of the interface structure composed of widgets. Widgets are configurable interface elements that are used to represent data, such as charts or lists visually.

Widgets are used to render information for visual display inside View Template. Widget types vary such that specific widgets only correspond to certain view types. For example, detail view has some exclusive widgets.

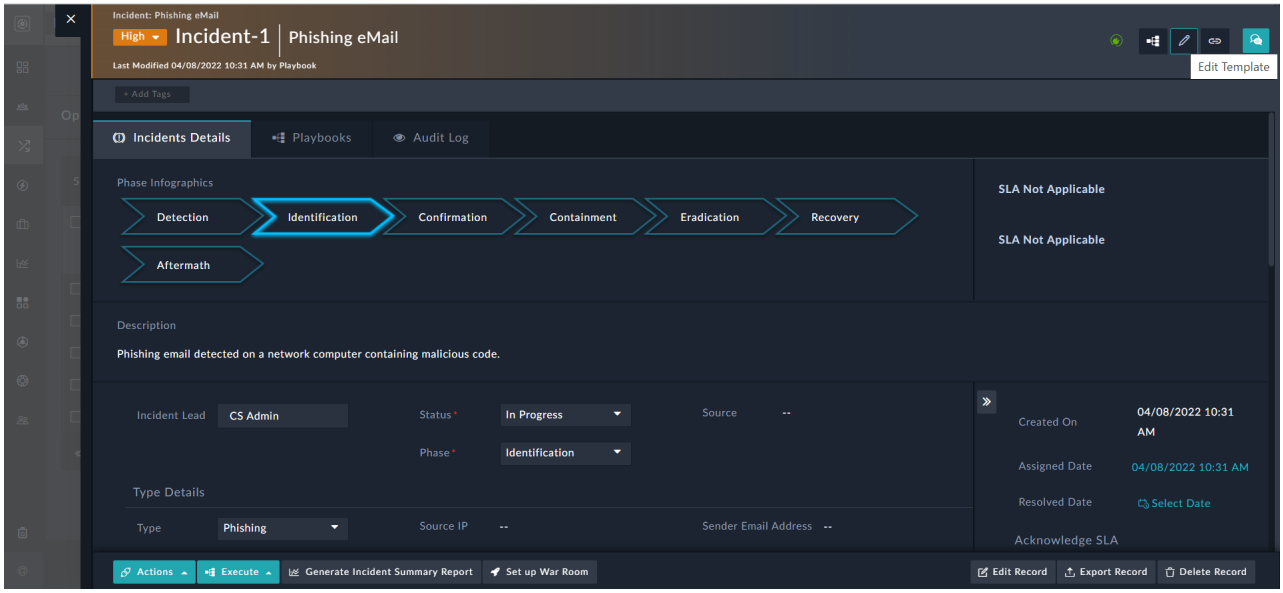
See the Dashboards, Templates, and Widgets chapter, for a detailed explanation on how to use templates and widgets.

Editing the Detail view of the Incidents Module

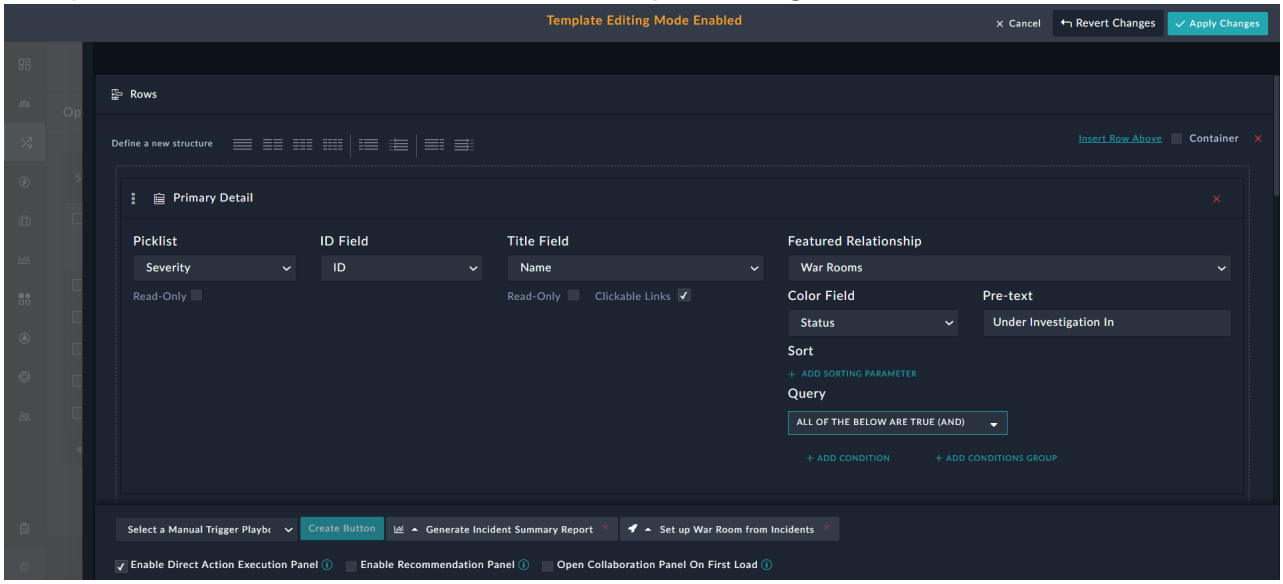
To view the Sender Domain, Sender Email Address, and Recipient Email Address fields that we have added using the Fields editor on the FortiSOAR UI we have to add these fields to the Detailed view of incident records by updating the SVT for the Incident Module.

1. Log on to FortiSOAR using your credentials.
2. Click **Incident Response** > **Incidents** in the left-navigation to open the Incidents module in the list view.

3. Click on a record to open the detailed view of an incident record and click the **Edit Template** icon in that record.



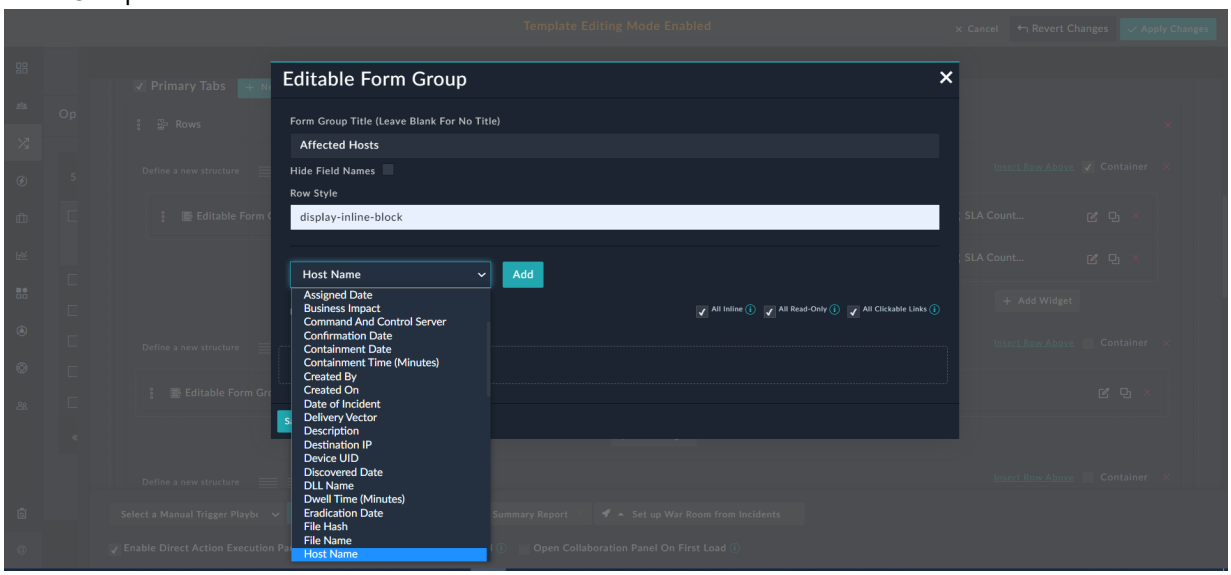
This opens the detail view of the incident record in the **Template Editing** mode:



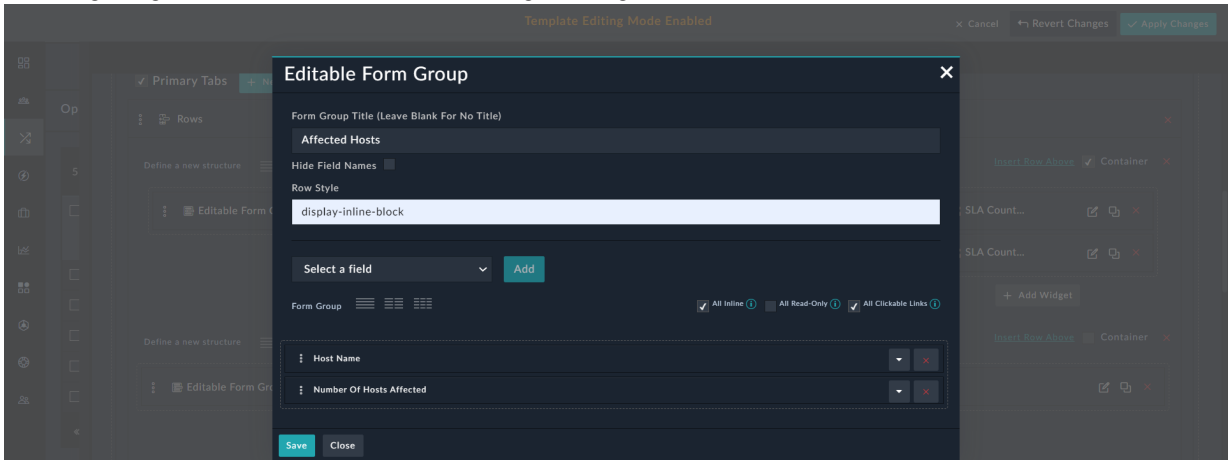
Now you can begin editing the template using Widgets.

4. In our example, we want a row to be added in which we can add the information for the **Host Name** and **Number of Hosts Affected** fields.
   To achieve this, click the **Insert Row Above** link or **Add Row** button, depending on where you want to place these fields in the template. This will add a row and within this row, click **Add Widget**.
5. From the `Choose Widget` dialog, select **Editable Form Group** widget. This opens the Editable Form Group template for configuration. You can also click on the **Edit Widget** icon in this row to modify the widget later.
6. Configure the Editable Form Group as follows:
   a. Type `Affected Hosts` in the **Form Group Title** field and type `display-inline-block` in the **Row Style** field.

b. Then from the **Select a Field** drop-down list, select **Host Name** and click **Add** to add this field to the Editable Form Group.

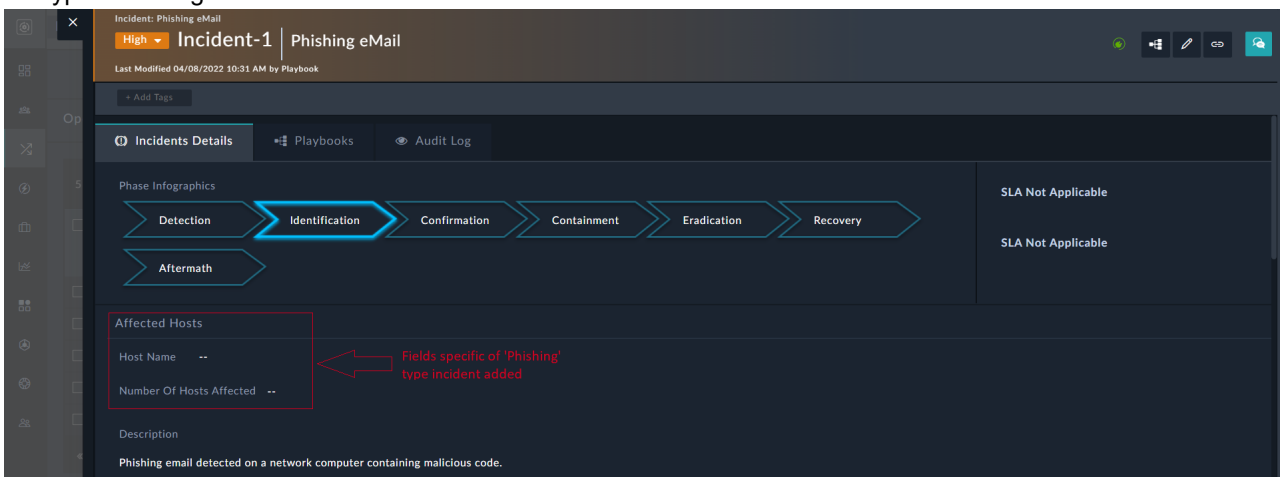


c. Similarly, select the **Number of Hosts Affected** field and then click **Add** to add in the widget.
This adds both the Host Name and Number of Hosts Affected fields to the Editable Form Group as shown in the following image, and click **Save** to save the widget configuration:



7. On the template editing page, click **Apply Changes** to save changes to your template.
Now, you can see the fields that you have defined to be displayed in the detailed view of an incident record that has

the type "Phishing."



Conclusion

This tutorial demonstrates the flexibility that FortiSOAR provides for incident response.

Using this flexibility, you can create very customized forms for various types of records, each catering to your specific requirements. Fields can be customized at a very granular level using properties that can be conditional, such as the *Required By* condition.

www.fortinet.com