THETARAY

Version 6.13

Financial Crime Complaiance Suite

INVESTIGATION

Settings - User Guide

Revision A

Publication Date: 2nd April, 2025

Legal Notice:

1. Investigation Settings

1.1. Overview

The Investigation settings module enables you as a business admin user, to configure how alerts in your environment will be formulated for investigation.

At the core of IC settings are three main modules:

1. Templates - define the structure of accumulated alerts and how with a combination of created customized tabs and system static tabs the alert data is presented to the analyst and supervisor for the purposes of efficient investigation and resolution
2. Data Containers - hold evaluation results sourced from selected data sets
3. Mappers - enable data source data to be mapped to the configured customized alert tabs

The cross interconnectivity between each of these core modules is shown diagrammatically in the following figure.

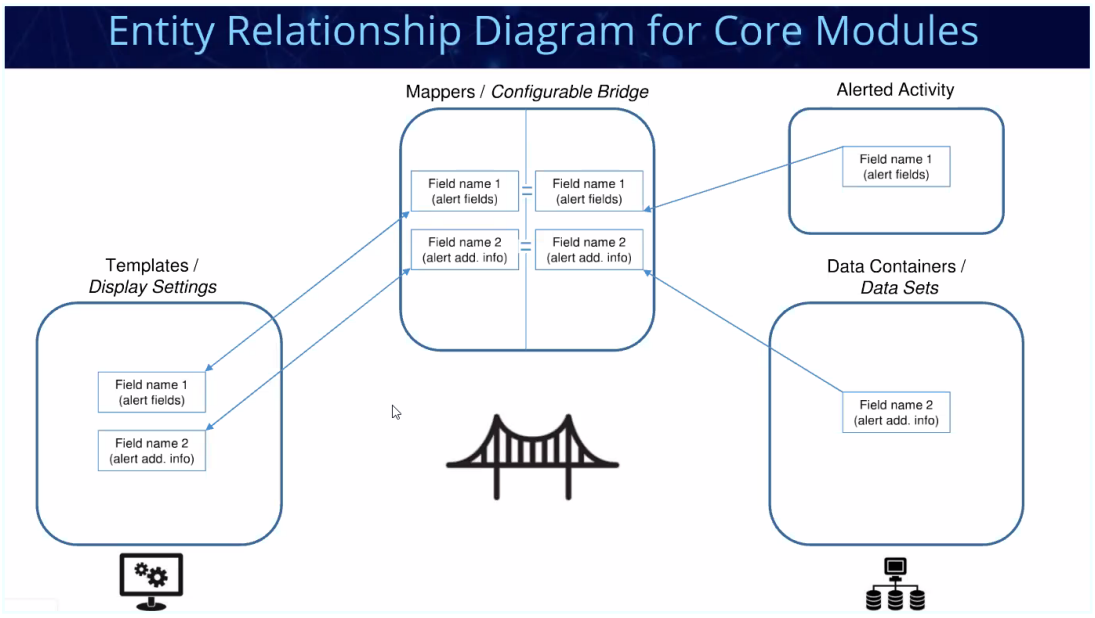


Figure 1: *IC Settings Core modules - Interconnectivity Diagram*

1.2. IC Setting Module

Apart from the Investigation Setting core elements detailed above, the IC settings module includes the following configurable IC setting elements:

- Queues - enable alert list structure for various use cased
  - Default Alert Prioritization - enable alert selection organized by priority

- Workflows - enable alert investigation flow structure according to use case type and requirements
  - Forms Builder - enable creation of time saving forms used in the workflow
- User Attributes. enable users to be organized into logic groups depending on experience level
- General Settings - enable the configuration of additional system utilities used in the application
- Import/ Export - enable quick and efficient transfer of IC configurations from deployment to deployment

1.2.1. Order of Configuration - Best Practices

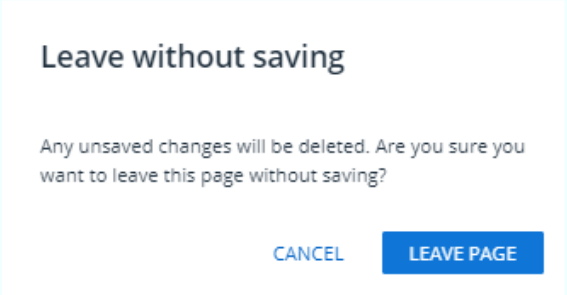
Regarding the available IC setting elements. It is a suggested best practice, for the optimum productivity and efficiency to configure the modules in the order as shown in the following figure, at least at the new installation stage.

Figure 2: *IC Settings - Configuration Order*

Note: Searching for fields etc., uses Autocomplete. Simply start typing text for options to be displayed. If no results are found, a message is displayed.

1.2.2. Leave Without Saving - Caution Message !

The following message is displayed in Investigation Settings if you attempt to quit a section without first saving.



Its purpose is to mitigate data settings loss that can occur if you should inadvertently forget to save your settings before quitting.

1.3. Log in to Investigation Center and IC Settings Module

1.3.1. Prerequisites:

Business admin user: Read/write permission, of IC Setting and read only permission to Investigation Center

To log into IC Settings module:

1. Provide username and password credentials.

The user if designated with IC configuration privileges will be presented with the following access screen as shown below.

2. On clicking the matrix icon (1) the following icon select menu is displayed.

Note: Entity Resolution is an optional module, and may or may not be available in your deployment.

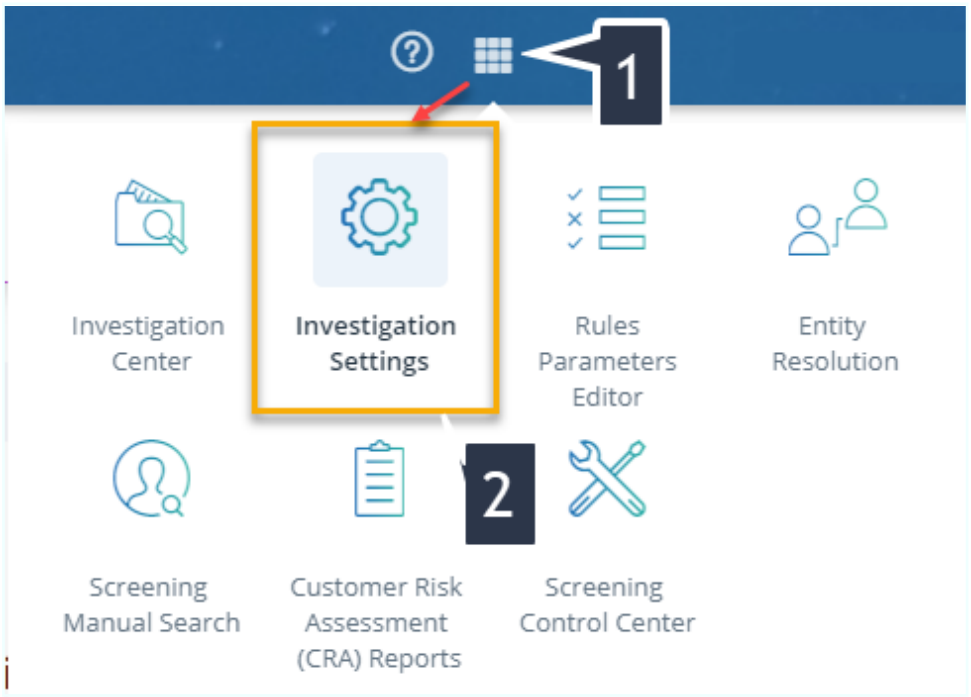


Figure 3: *Matrix Module Select Icon Menu Displayed to the Admin User*

1. To access the Investigation Settings module, click the Investigation Settings link (2).

1.3.2. Investigation Settings Side Panel

On selecting ***Investigation Settings*** option(2) the ***Investigation Setting***s panel is displayed as shown1. with the ***Templates Settings*** option selected and highlighted by default.

2. Templates

Alert templates define how the alert's data will be displayed in the Investigation Center.

The creation of Alert templates enable data to be separated and analyzed by creating and configuring the following components:

- Alert Definition
- Alert Tabs
- Additional

Note: New modification settings made to the module and then applied affect newly published alerts and cannot be applied to previously published alerts. Only Edit of displayed components can be applied.

2.1. Alert Definition

The alert definition process provides the following functionality:

- It allows for the configuration of at least one mandatory primary identifier, and as a best practice, an additional transactional field or fields , depending on use case requirements.
- It enables the template to be configured with a set of more user friendly 'alias' generic field display names. This function will aid the analyst or data scientist in the task of alert investigation to quickly understand and identify the purpose of the data fields under investigation.

We'll start the description of the process at the definition of the template stage.

1. From the sidebar menu click the Templates link to display the default empty template.

In a new deployment, an empty Templates screen is displayed as shown in the following figure.

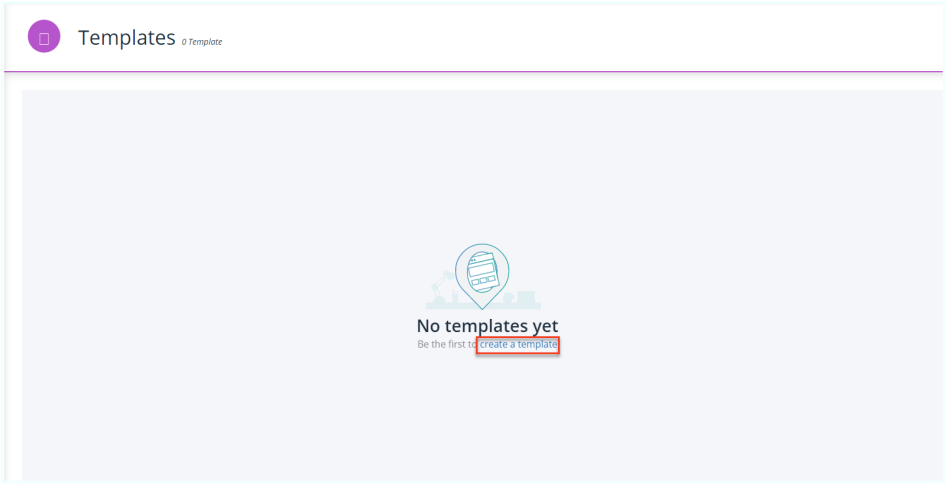


Figure 4: *No Templates yet Configured*

In IC settings, at least one configured use case template is a mandatory requirement.

1. Click the highlighted 'Create a template' link.

An example following create template type select option is displayed as follows:

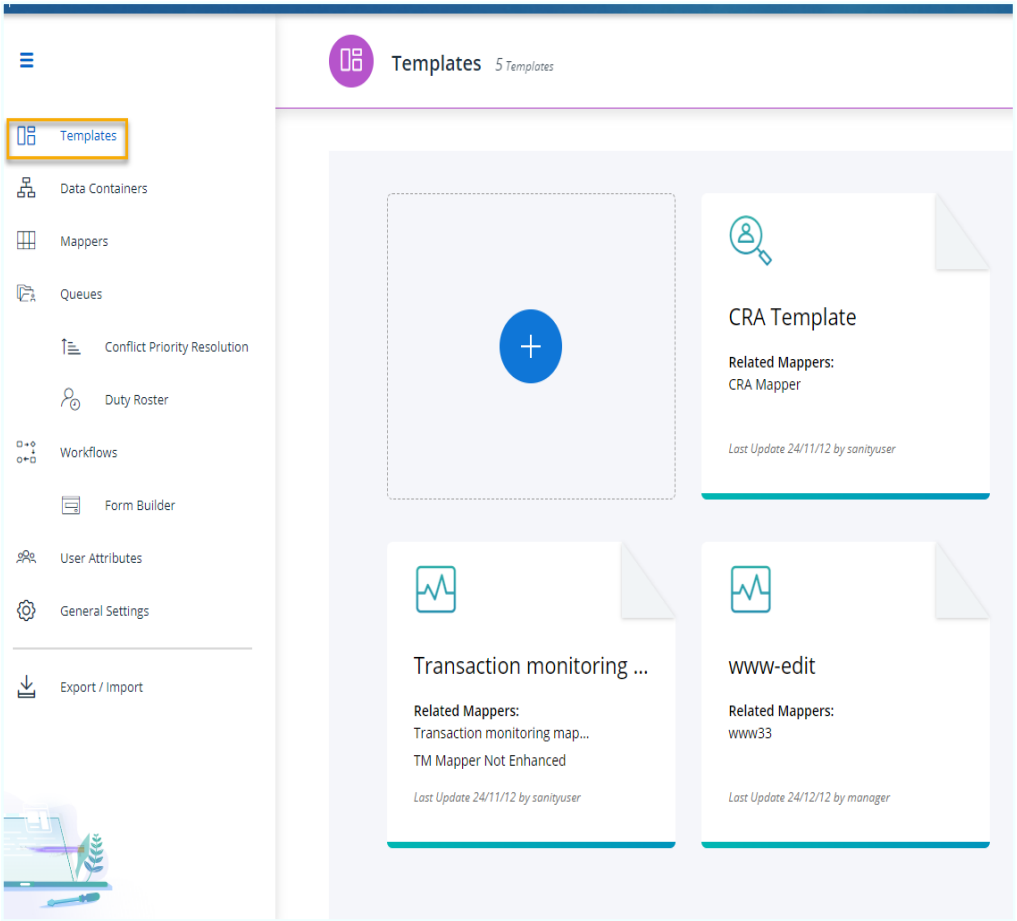


Figure 5: *Example Create New Template Select Screen*

2. Select the type of template required.

The following create template description describes the process when a **Transaction monitoring** template is selected.

A Create Transaction Monitoring template form is displayed as shown below.

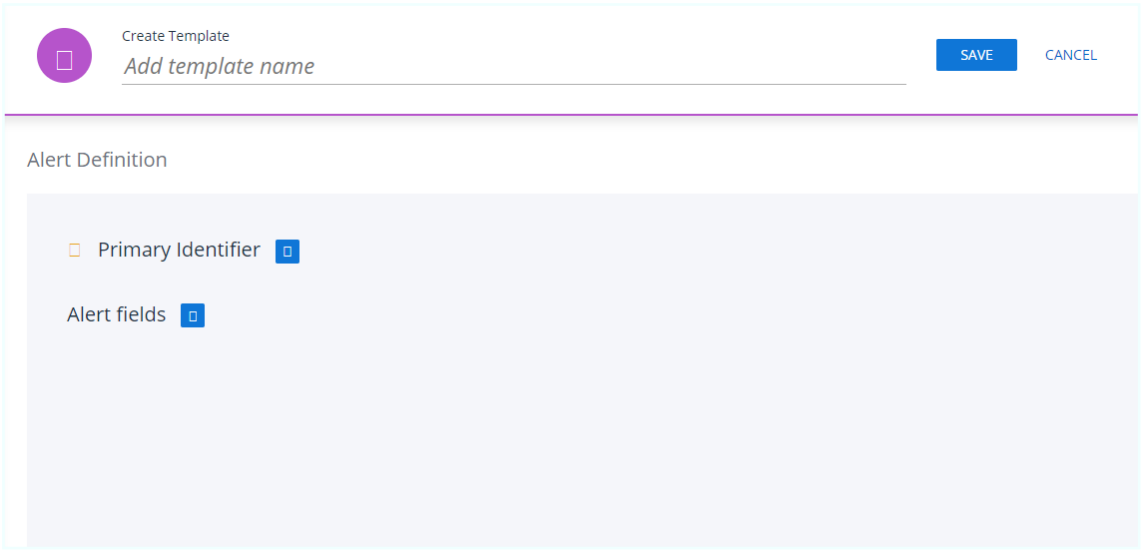


Figure 6: *Create Transaction Monitoring Template - Alert Definition Form*

2.2. Alert Definition

The initial requirement in the alert definition process is to name, configure one primary and save the new template.

To start the definition process:

1. Provide a use case descriptive name (for example: **AML Use Case**)
2. Click in the + Primary identifier icon and type a descriptive name (for example: **account_id).**

Defining a primary identifier automatically makes it the first alert field in the template Alert fields, as shown below.

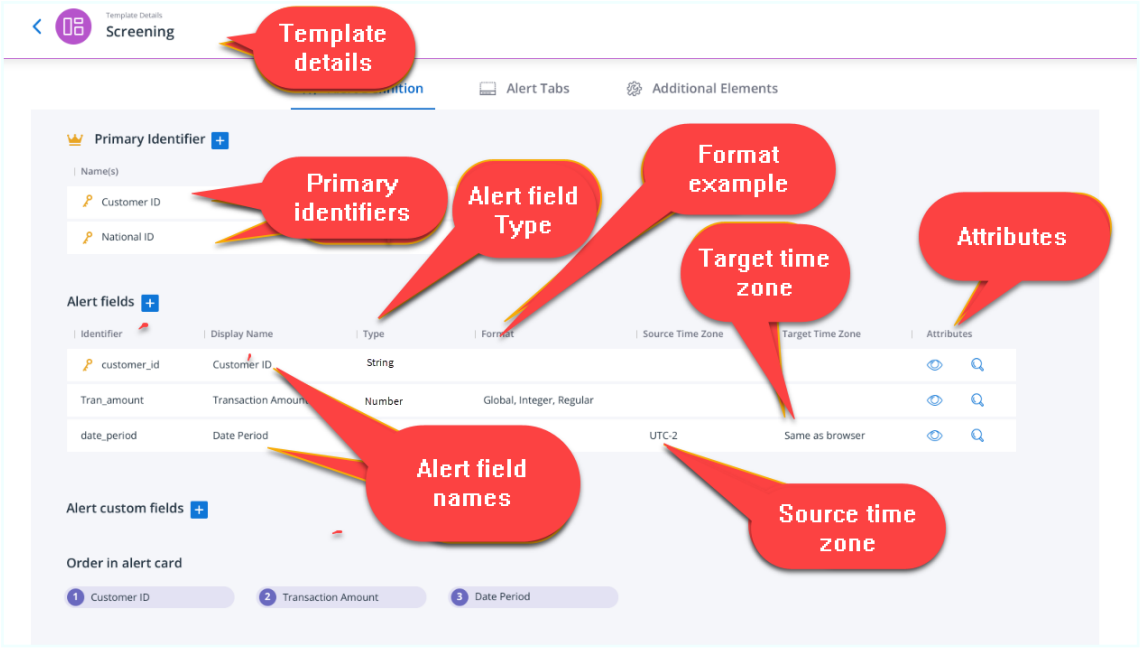


Figure 7: *Alert Definition - Naming and Providing Primary Identifier(s)*

3. Alert Fields showing:
    a. Identifiers
    b. Display Names
    c. Type
    d. Format
    e. Source Time Zone
    f. Target Time Zone
    g. Attributes
4. Click **Save**.

Note: As a best practice, two Primary identifiers should be defined.

2.2.1. Type - Format - Source / Target Time Zone UTC /Default Browser

As shown in the above figure, when setting Alert Definitions in Templates, the admin user can aid investigation efficiency by setting the date format and target time zone of alerts to be aligned with the investigatory analyst's local browser or UTC for a particular global locality. This is particularly effective in deployments that include differing DPVs. This ability ensures the analyst tasked with alert resolution is working in a timezone related to their particular country , region or their default browser setting.
Settings include:

- Format - Global, Integer, and Regular
- UTC time setting selection (time related to UTC time)
- Same as browser settings selction

Thiese configuration options are particularly effective in deployments that include differing DPVs as they ensure that the analyst tasked with alert resolution is working in a timezone related to their default browser and therefore to their country or region.

Once configured, the setting can be viewed in the **General Settings** section under the **Locale Tab.**

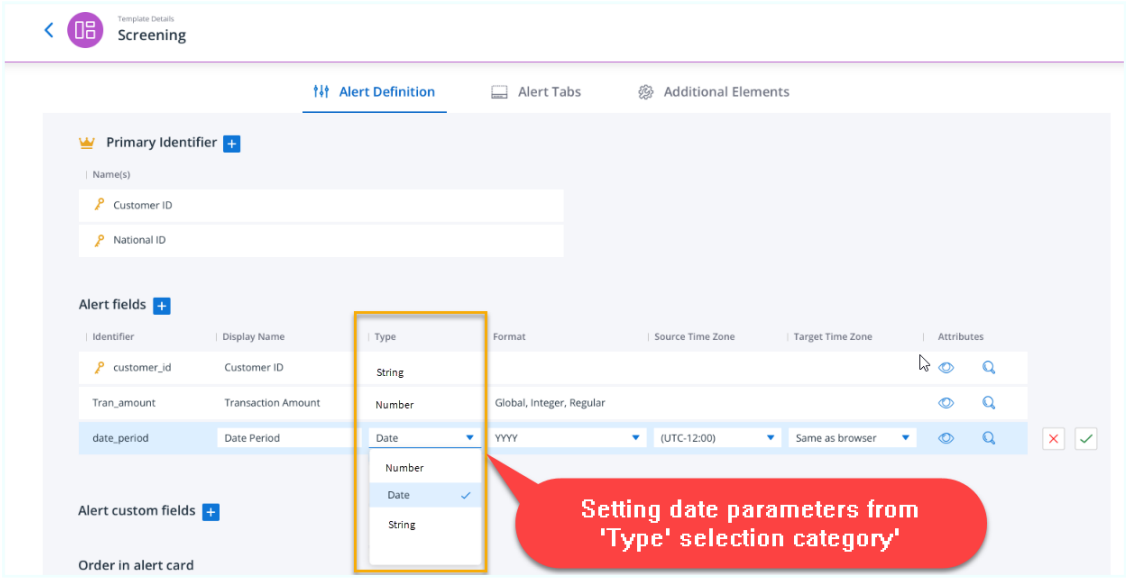


Figure 8: *Selecting Data from the Type Column Category*

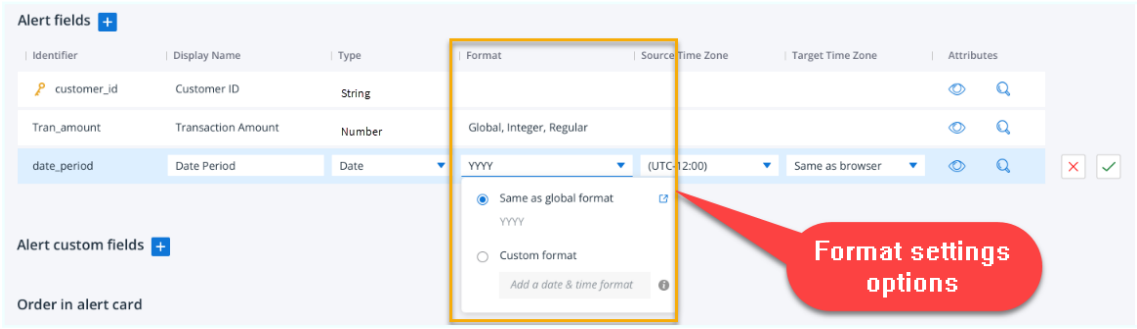


Figure 9: *Selecting Data Format - Global, Integer/ Regular Categories*

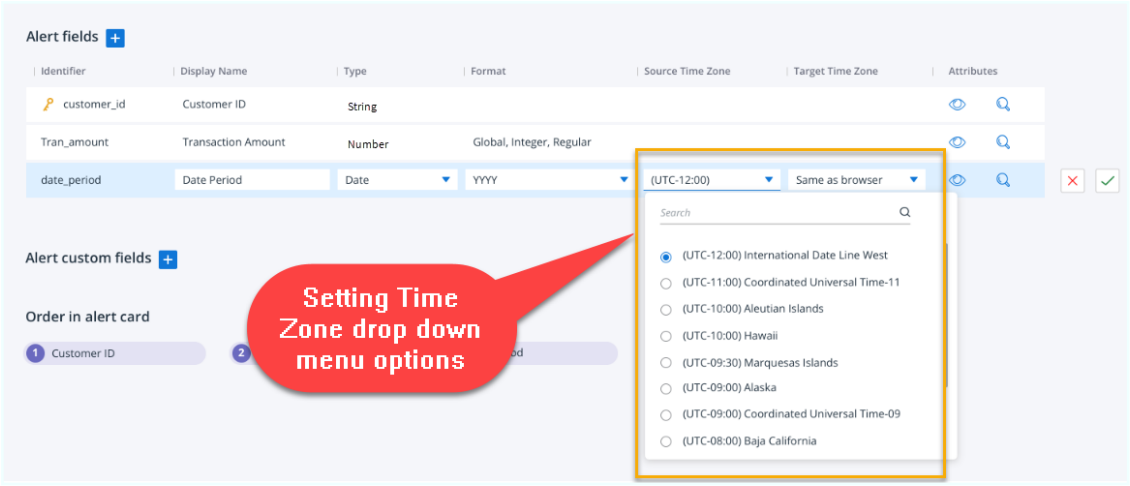
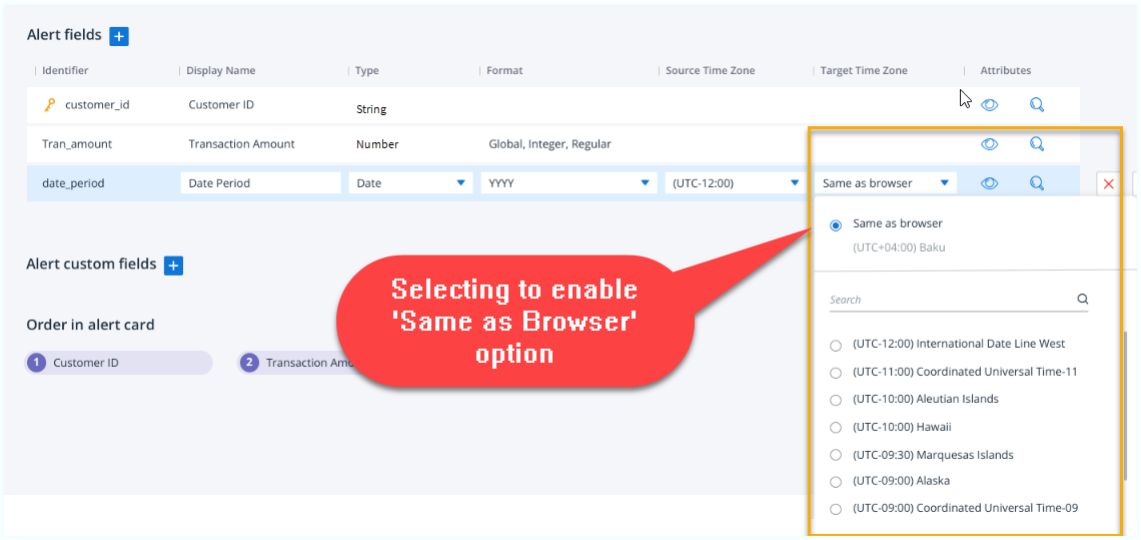


Figure 10: *Selecting Time Zone from UTC Options*



Example - Selecting Time Zone from 'Same as Browser'

Note: When updating Templates it is important to note that if the alert has set definitions which are associated with configured Mappers, updated data is synced with the associated mapper or mappers. This includes all template functionality specific to alert definition and Alert tabs for example, adding, removing, editing alert fields, custom fields, and tabs. A popup similar to the figure below is displayed requiring UPDATE confirmation.

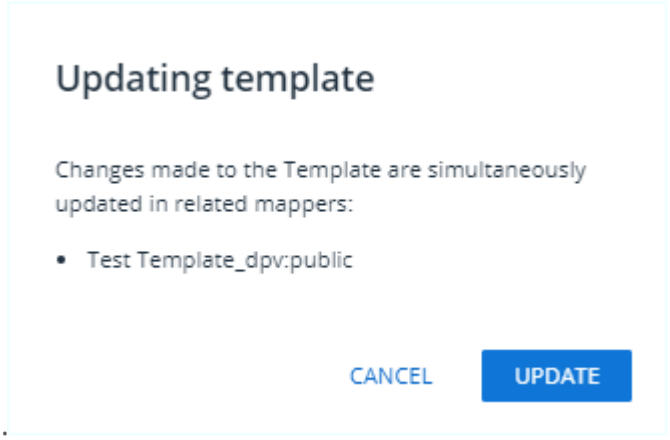


Figure 11: *Saving Template Data Popup when there are Associated Mappers*

2.2.2. Adding Display Names, and Attributes

Referring to the above figure, you can see the Primary Identifier we set and the duplicated name under Fields the Display name.

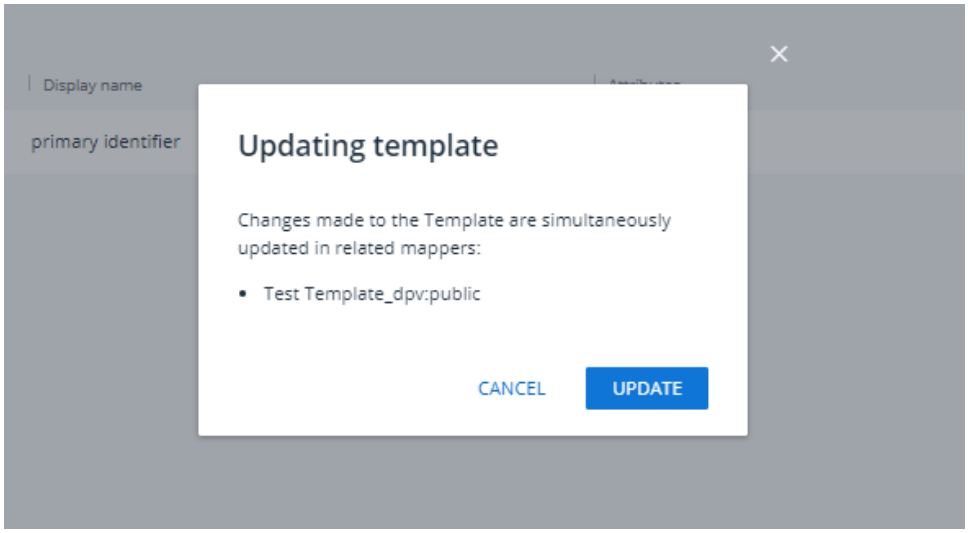
As an example of using Display names and Attributes lets modify the field names and configure display attributes.

1. In the Alert Fields hover over the account_id and when displayed, click the edit pencil icon as highlighted.

Figure 12: *Example - Editing the Display Name and Selecting Attributes*

1. In our example, we will over type the displayed name with **Primary Identifier** and select both the 'View on Alert' card icon and the 'Searchable' icon .
2. Click the green tick to confirm

As mentioned in the above note when there are associated linked mappers a popup similar to that shown below is displayed.



3. Click Update to confirm.

Note: In order to ensure sufficient data is made available to the analyst, it is good practice to add a comprehensive range of data fields to the alert definition. Also note that it is not mandatory to add data fields at this stage, as this task can be completed later.

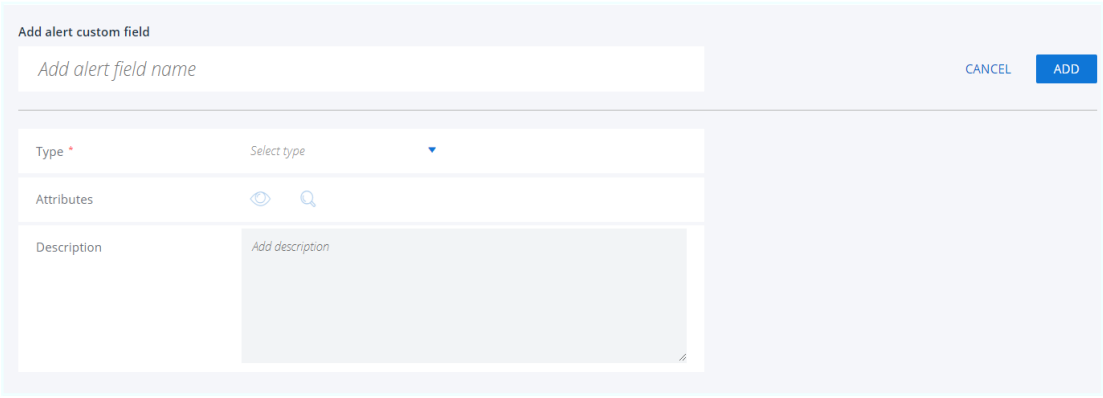
2.3. Adding Custom Fields to the Alert Definition

Adding custom fields in **Alerts Definition** is a straight forward process, but does require some additional configurations.

To add custom fields to the template definition:

1. Click the **Alert custom field +** linkFigure 7: above.

The following custom field configuration form is displayed.



2. In the form that is displayed, provide a name for the Custom field (for example: **Human Trafficking**.
3. From the available data types select (for the purposes of this example) **Boolean.**
4. In the **Default Value** we will in this example, select **True**.
5. Select the required attribute (view, search)
6. Add free text describing the reason and purpose of creating and including this custom field

An example completed form is displayed as shown in the following figure:

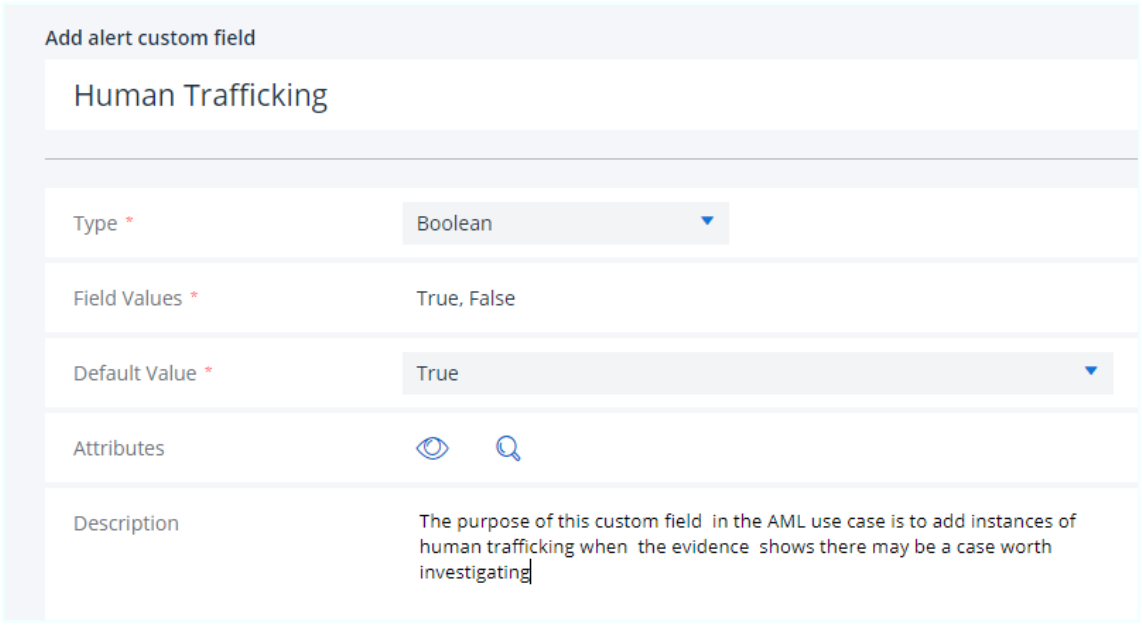


Figure 13: *Adding Alert Custom Field Form*

7. Click **ADD** and confirm that a successful creation message is displayed and the custom alert is added to the configured Alerts Definition

The following example shows the popup displayed when an associated mapper is linked.

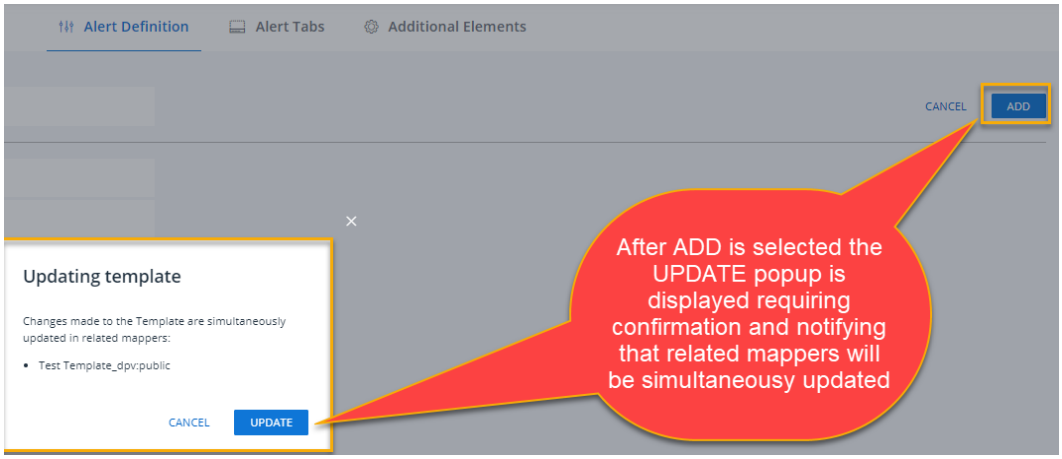


Figure 14: *Example Addition of a Custom alert after clicking* ***ADD***

2.4. Setting Field Order on Alert Card

As alerts are added to the template they are numbered and displayed sequentially. As the alert card can only display up to 4 fields the remainder are stored in a list that can be called up when required for modification.

2.4.1. Reordering

As shown in the following example diagram, the fields displayed on the Alert Card can be reordered. Click the green tick to confirm setting,

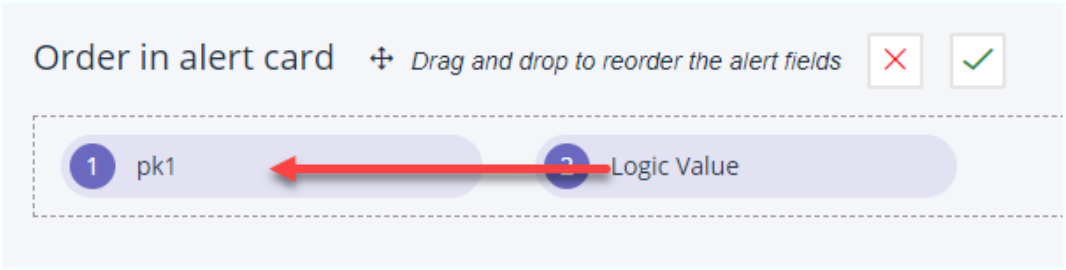


Figure 15: *Reordering Displayed Alerts*

When complete our example **Alert Definition** should look similar to the following.

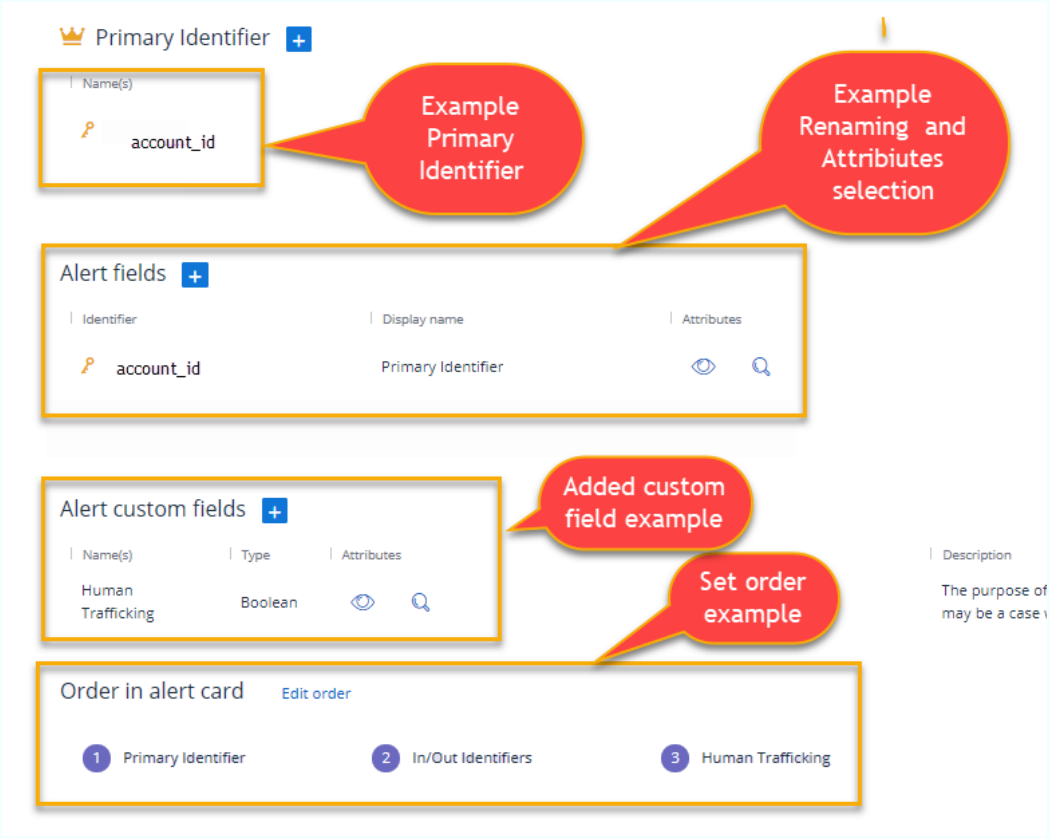


Figure 16: *Example of Alert Definition*

2.5. Alert Tabs

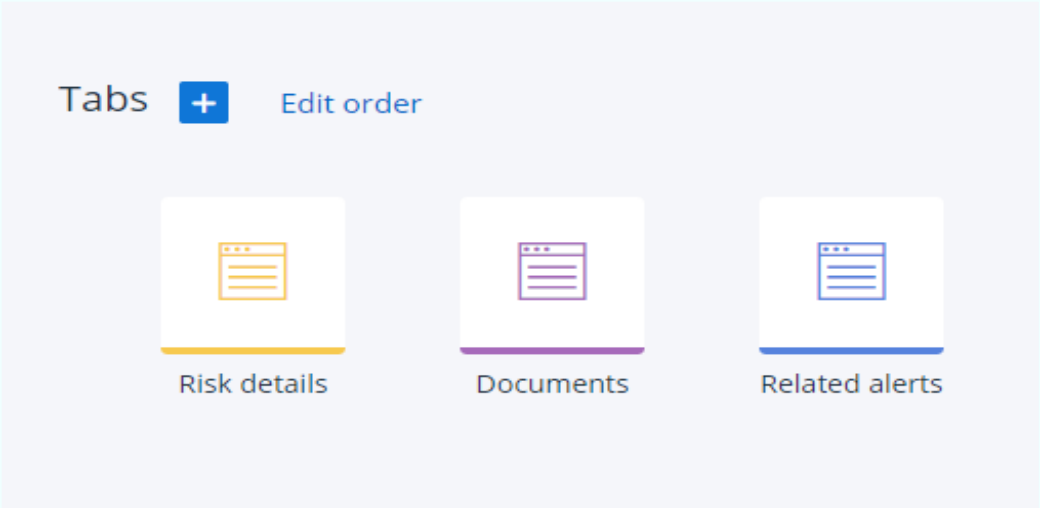
There are two types of alert tabs used in Investigation Center

- System tabs
- Custom tabs

2.5.1. System Tabs

System tabs are supplied with the IC deployment are static and cannot be removed. These are:

- Risk Details
- Documents
- Related alerts



Note: Limitation: Configuration of Risk details is not supported at the moment.

2.6. Custom Tabs

Custom tabs can be added to your Alerts investigation process screen as required via the Template configuration. These provide the ability to customize your alert investigation environment according to your use case needs.

Limitations

- There is no maximum limit to the number of custom tabs that can be added
- Tab elements can be removed only if the tab has not yet been populated with data.

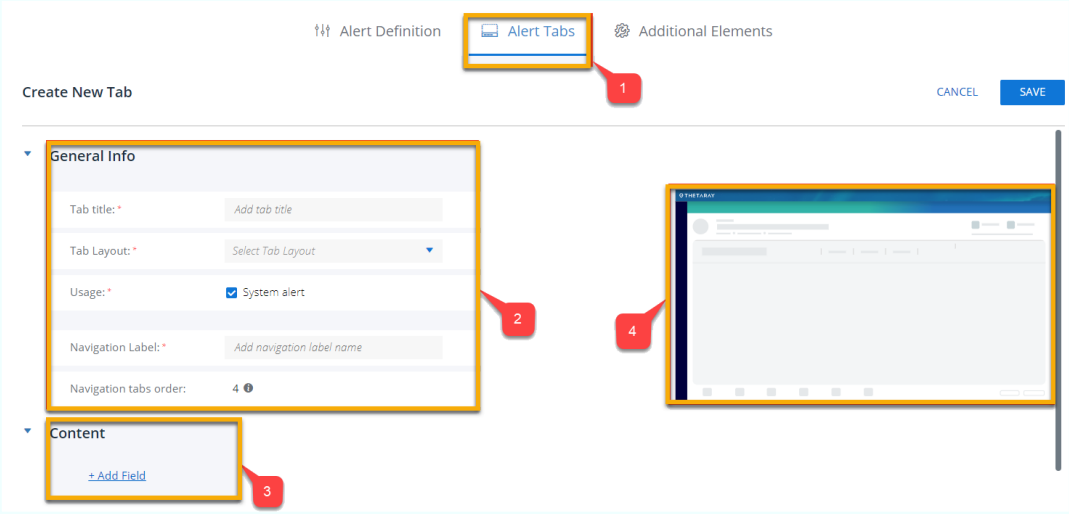
Custom Tabs can be created for Transaction Monitoring, and Sanction Screening use case templates.

2.7. Transaction Monitoring - Custom Tabs

These tabs can be structured in various format layouts as follows:

- Table
- List

1. From the Templates screen click the 'Alert Tabs' link (1).



2.7.1. Element Placement Visualization Aid

When adding elements , the visualization graphic (4) shows you where the element will be placed on the tab, as shown in the following example.

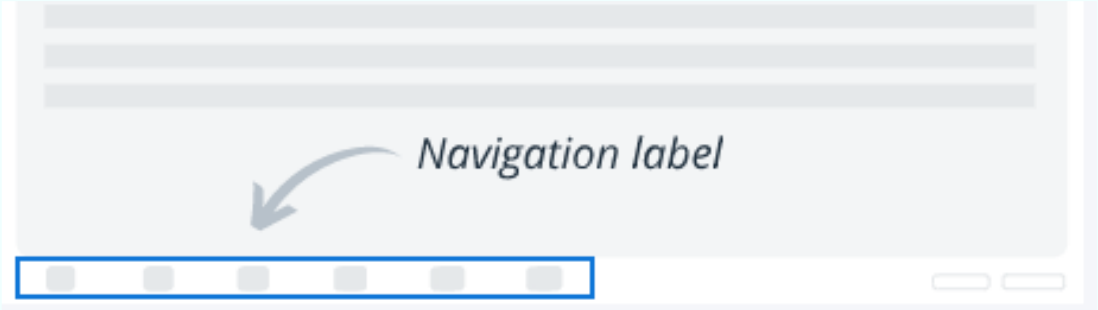


Figure 17: *Visualization Aid (4) - Example*

a. In the Tab title field, provide a tab name (for example, 'BIC')

b. From the Tab layout drop down menu, select the preferred layout:

   - Table *or*
   - List (enables sections)

c. under **Usage**, select the default System alert

d. Provide a **Navigation Label** (i.e. the text that will be displayed on the tab, example: Bank ID) .

e. Navigation tabs order displays the sequential position of the tab in the navigation bar. Reordering of the sequence is accomplished in the main tabs.

f. Collapse the **General Info** block before continuing to allow you more space.

2. Click **Content** to display the Content block (3). This block enables you to enter the field details and parameters for the new tab (Name, Types, Format and Values).

Note: The content block displayed differs depending on whether the tab layout selected is a table or a list.

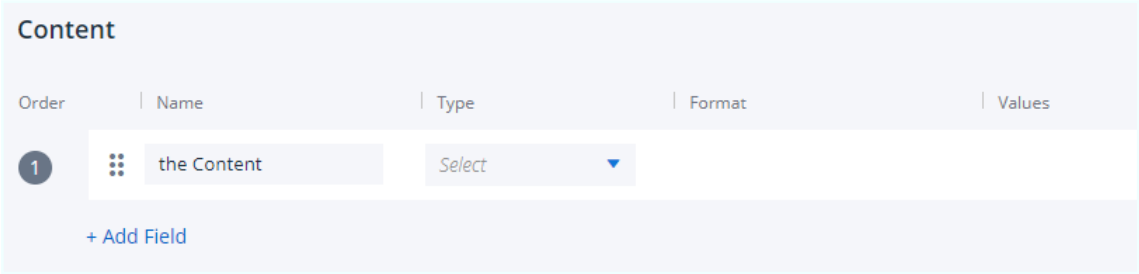


Figure 18: *Content Block for Table Layout - Holds Field Name and Parameters*

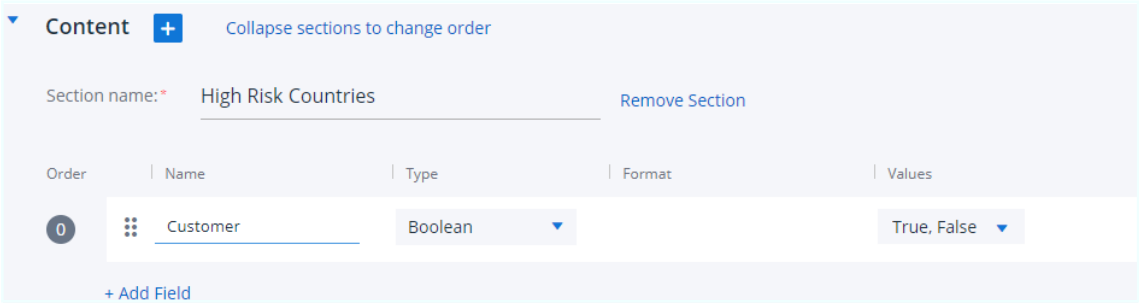


Figure 19: *Content Block for List Layout - Holds Section Name, Field Name and Parameters*

a. Only for list layout provide a name for the section (example: High Risk Countries).

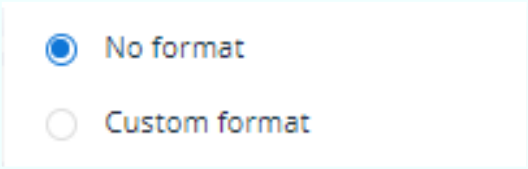
The following steps are common to both layouts:

b. Provide a name for the tab field (example: Customer).

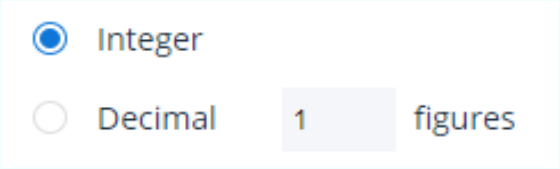
c. Click the **Type** drop down menu and select the field type from: Numeric, Date, Boolean, or Code.

d. If the data type is **Numeric**:

i. first select from the format drop down menu to choose either **No format** or **Custom format**.

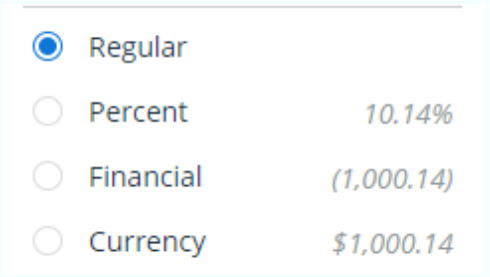


ii. If **Custom format** is selected then select either:
   - **Integer** or **Decimal** format to be used:

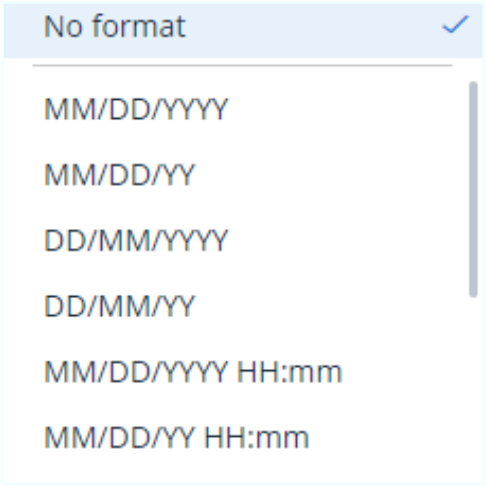


iii. With Custom format, If **Decimal** format is selected, also select the number of figures to be displayed after the decimal point.

iv. With Custom format , if **Integer** format is selected:
   - Choose from the further following format options:

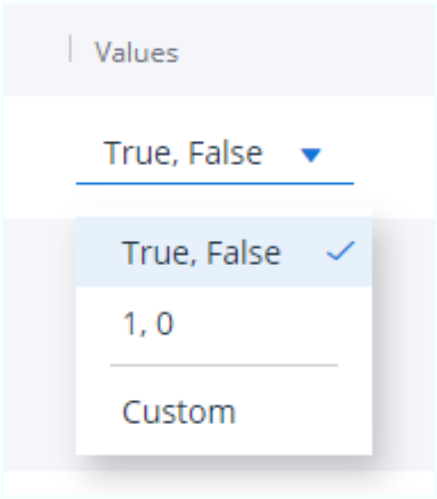


e. If the data type is **Date**, select either, no format or from the displayed list of date formats as shown in the following example:



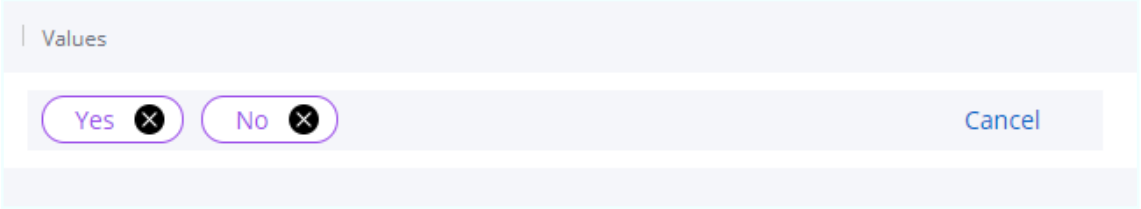
f. If the **Data** type is **Boolean** then continue as follows:

g. Under **Values**, select from the available options to display the Boolean data type:



If the Custom option is selected enter the values you require to denote the two boolean options as follows:

Say we want to use Yes or No to represent True or False, then in the value field type *Yes* click Enter and then *No* and click Enter. The Values field should now display as shown in the following example:

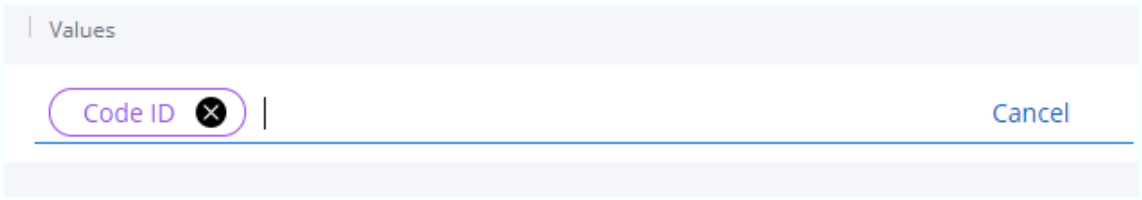


h. If data type is Code, either select:

i. ***No values*** *or*

ii. *click the add values + icon to display the custom code field.*

For the purposes of an example say we want to display **Code ID** on the field header so type Code ID in the Code custom field and click enter.



i. When complete, its important to remember to click **Save**.

As with Alert definitions updating custom tabs also requires confirmation as shown in the following example figure.

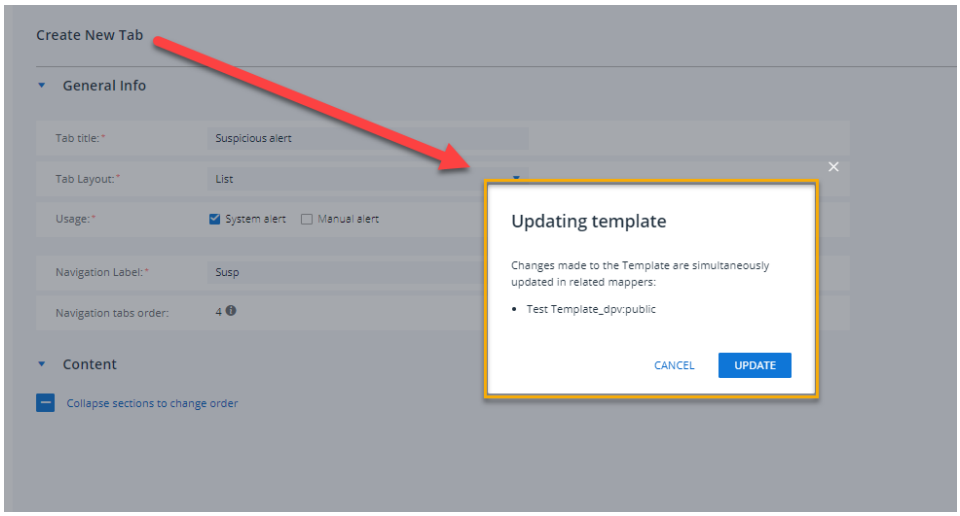


Figure 20: *Updating /Creating a Custom Alert Tab in Templates*

2.7.2. Risk Details - Essential Evidences

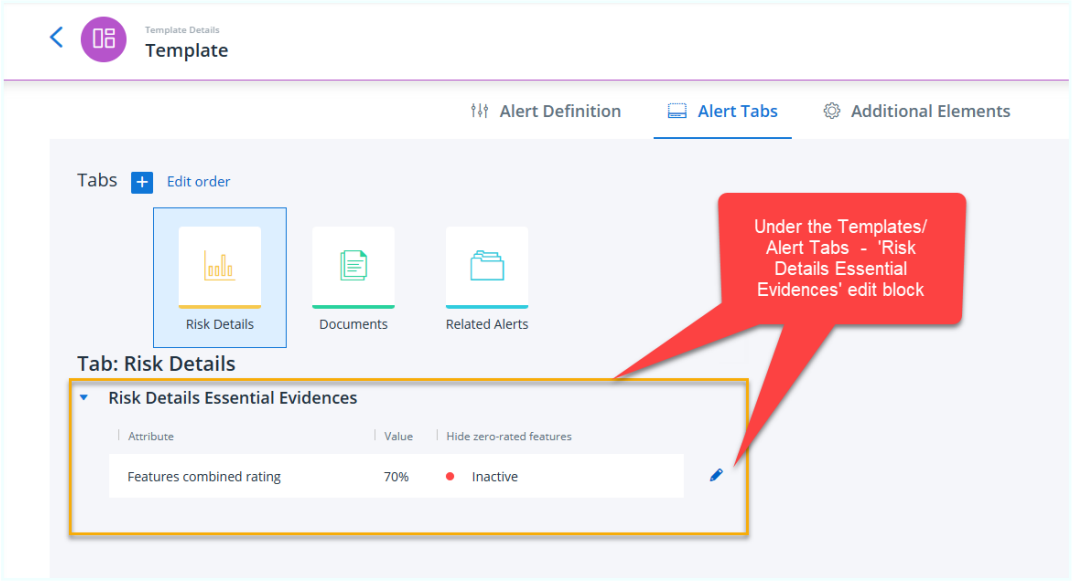
In the Risk Details tab, (IC module) **Essential Evidence Graphs** displayed as feature evidence indicators, assist the analyst in his /her task of alert resolution by enhancing the focus on the core evidences that trigger alerts.
These graphs are created during the alert detection process and play an important role in alert investigation. However, in some instances the amount of essential evidence data gathered can be excessive.
Therefore, in order to help manage the situation and make the analyst's alert resolution task more efficient, it is possible for the admin user (with appropriate permission), to set a threshold limit on the number of essential evidence graphs displayed. The number of graphs shown is calculated by the summing the

percentage values of available graphs, in descending order of magnitude, against the set threshold value.

Note: If the total percentage values of available graphs does not exceed the set threshold value, then the next available graph in order, will be included.

Example : A percentage threshold setting of 90% means that if the three first highest essential evidences ratings for an alert are say 29% , 27% and 25% respectively, summing a combined total of 81%, then the next fourth evidence, with a rating of 15% will be included, even though the total summed percentage is now over the set threshold.

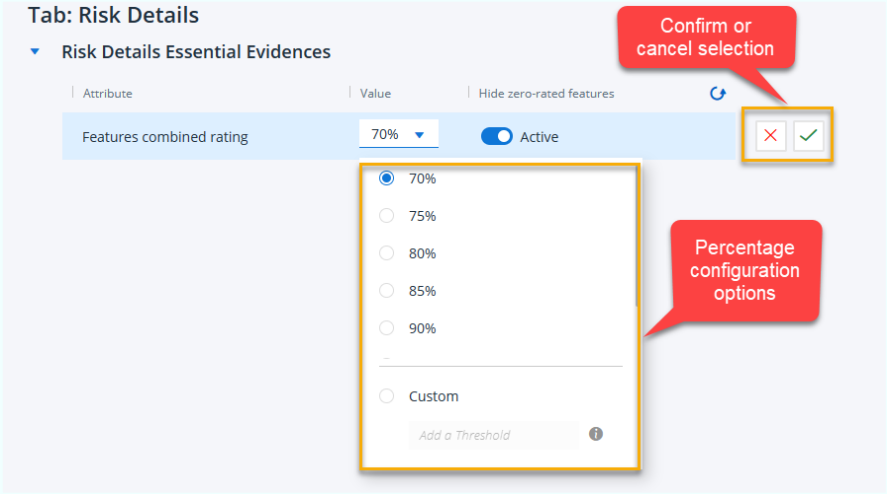
Note: This threshold configuration applies primarily for features generated on algo. Rule-based features are not affected.



To configure Risk Details Essential Evidence Combined Feature Rating:

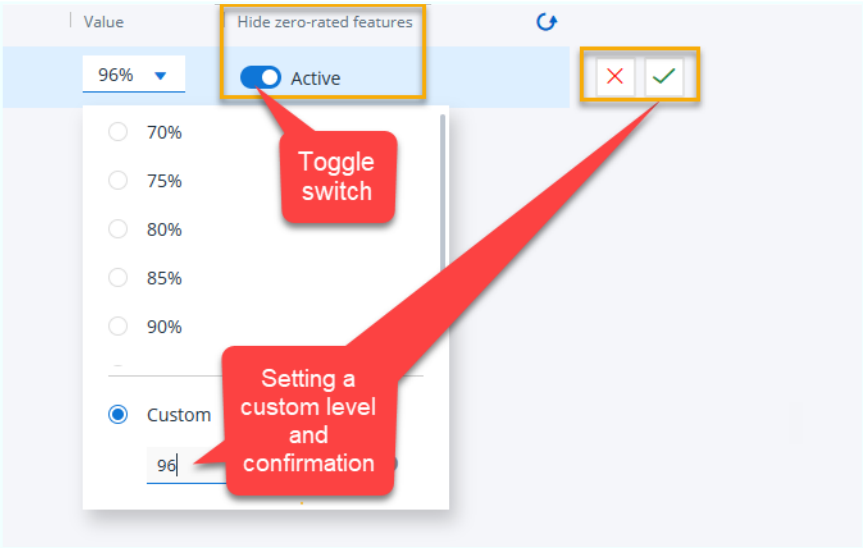
1. Click the Edit pencil indicated in the above figure.

The following configuration popup is displayed:



2. Select from either one of the preset configurations and click the confirm tick green icon.

   If none of the preset configurations suit your requirements, you can always select the **Custom** option as shown below.



3. The default value (if no value is selected) is 80%, and values below 70% cannot be set.
4. Additionally, you can also configure to hide zero- rated features, by activating the **Active** toggle switch highlighted above.

   That's all, navigating away from this tab automatically saves your setting. If required, you can always re-edit these settings at any time.

   Additional Information

Note: Apart from these configured settings limitations, the IC analyst can, if circumstances demand, select to view all evidences locally in the Risk Details section of the IC module. This extra feature ability does not include zero-related features, if set to hide (see step 4 above).

2.8. Screening Templates (Transaction and Customer)

This sub topic describes:

- The default template that comes preset with either Screening add-on deployment
- How to create/add a new Screening template.

2.8.1. Screening Template - (Transaction and Customer)

Selecting to create a screening option in multi solution deployment or at the log in stage when the single screening solution is implemented displays the following landing screen (for transaction screening) with the transaction screening icon shown as highlighted in (1) in the following figure.

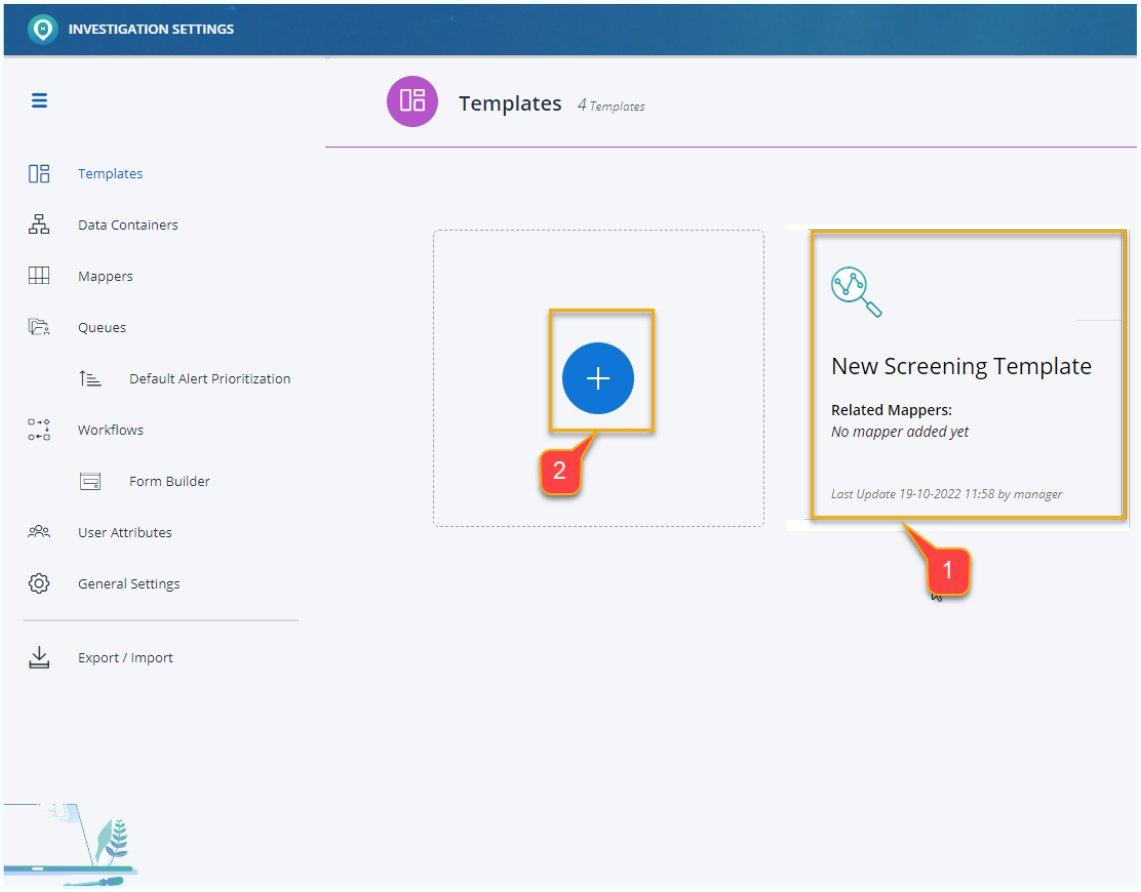


Figure 21: *Screening Templates Landing Screen with Default System Template Icon (1)*

Lets examine the components that comprise the screening definition template.

1. Click the large template icon (1).

The template for a transaction screening template is displayed as shown in the following figure.

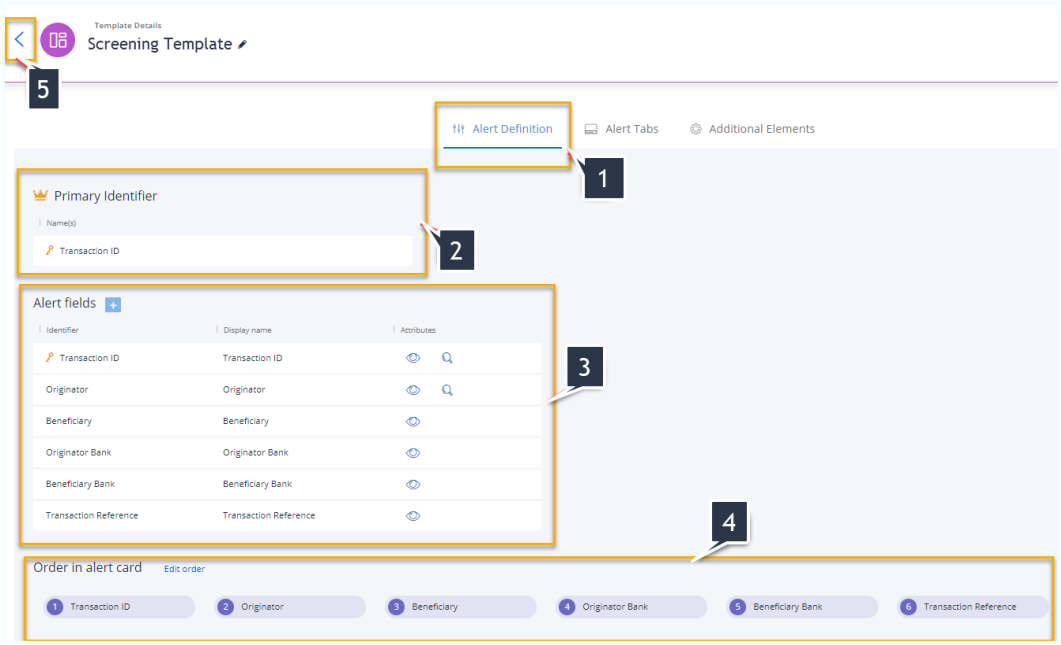


Figure 22: *Default Screening Template Displayed with Key Components*

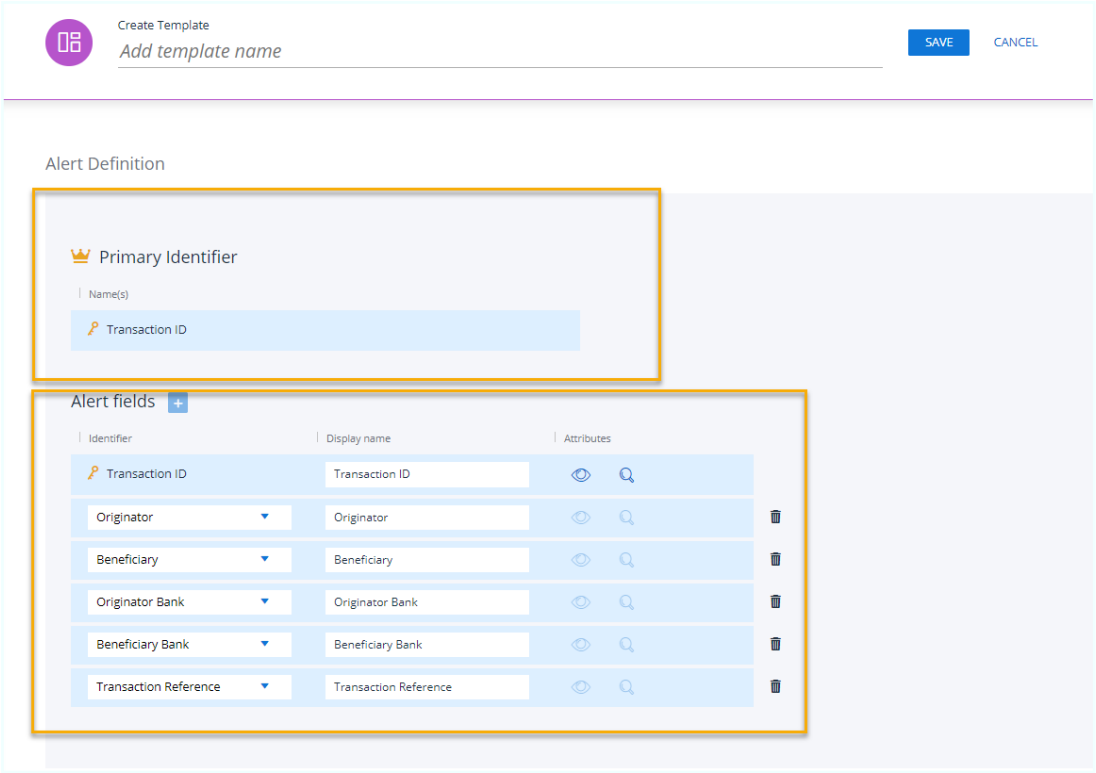
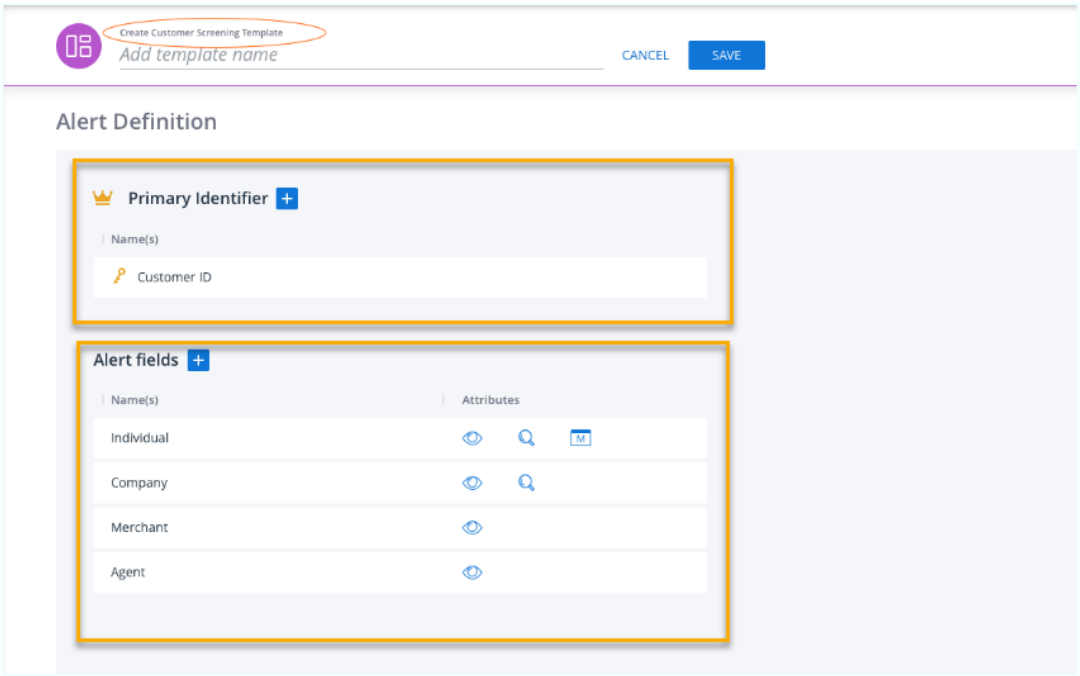


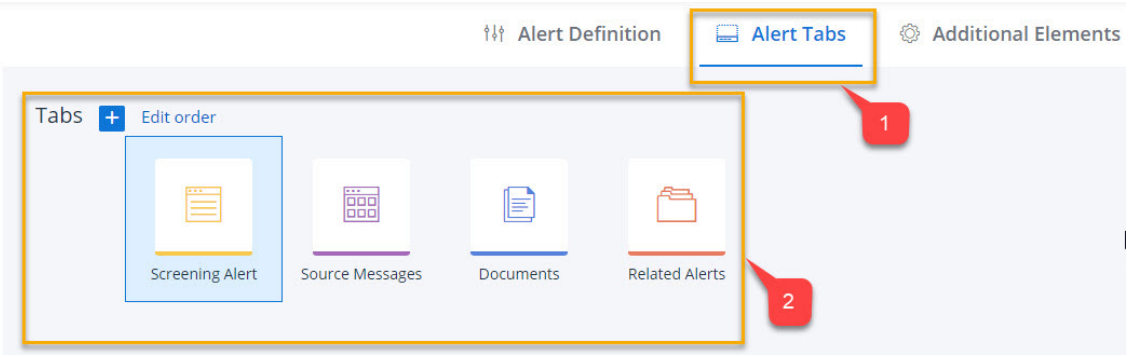
Figure 23: *Example - Create a Transaction Screening Template - Alert Definition Form*



Example - Create a Customer Screening Template - Alert Definition Form

2.9. Sanction Screening Tabs (Transaction and Customer)

If a **Screening** template is selected, available tabs can be displayed for edit by clicking the **Alert Tabs** icon (1) as shown below.



Available tabs under sanction screening (2):

- Screening Alert
- Source Messages
- Documents
- Related Alerts

2.9.1. Screening Alert Tab

Note: This tab is a static tab and as such, its only attribute, is it can be reordered.

2.9.2. Source Messages

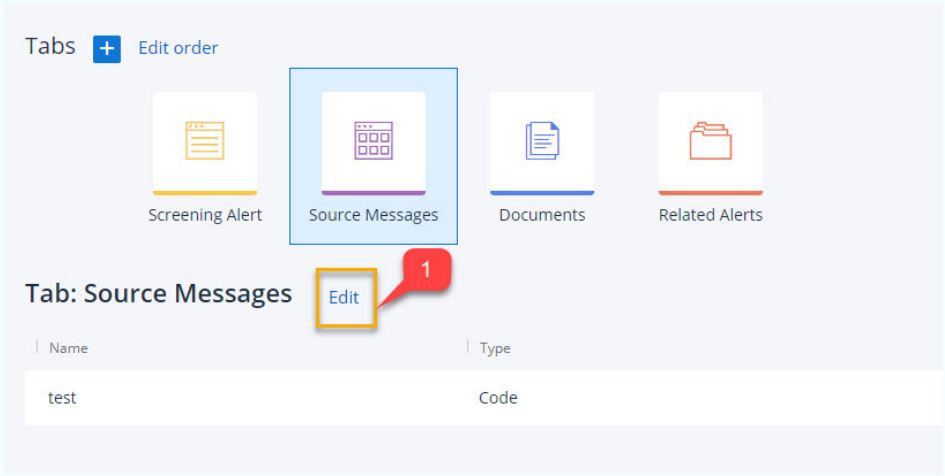
The source messages tab has the following editing attributes:

- Upload additional screening messages, as a CSV file
- Download screening messages, as a CSV file
- Adding new fields to the Source messages on an individual basis
- Reordering

To edit the Source Messages tab:

1. From the Alerts Tab click the Source messages icon.

The **Edit** source messages link is displayed as shown below.



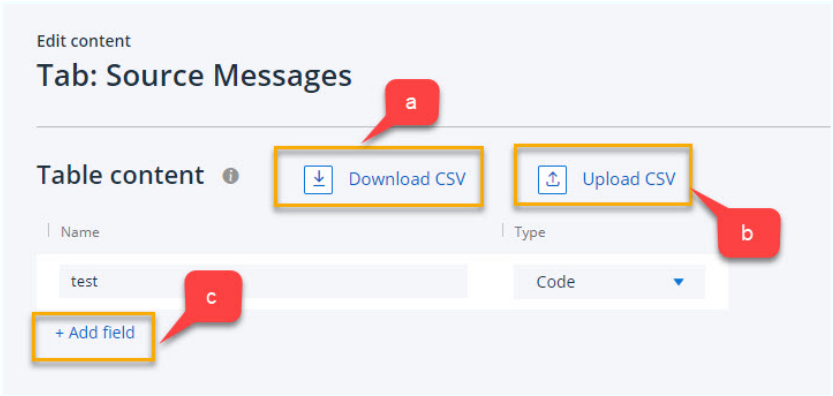
2. Click the Edit link.

The following screen is displayed that enables:

a. Downloading a copy of the current source stored alert source messages.

b. Uploading additional source messages files in CSV format.

c. Adding fields to the current source messages schema.



To download current stored source messages as a CSV file:

1. Click the Download tab (a).
   A CSV file is downloaded to your local computer for investigation purposes.

To upload a saved CSV file with additional source messages:

1. Click the Upload tab (b).
2. When the local document explore opens , search and double click on the CSV source file to upload it.

Note: Uploaded data overwrites previous data.

To Add / a field:

1. Click the **+add** field link (c).
2. Add the field name
3. Add the type (code or date).
4. When complete click Save.

To edit an existing field:

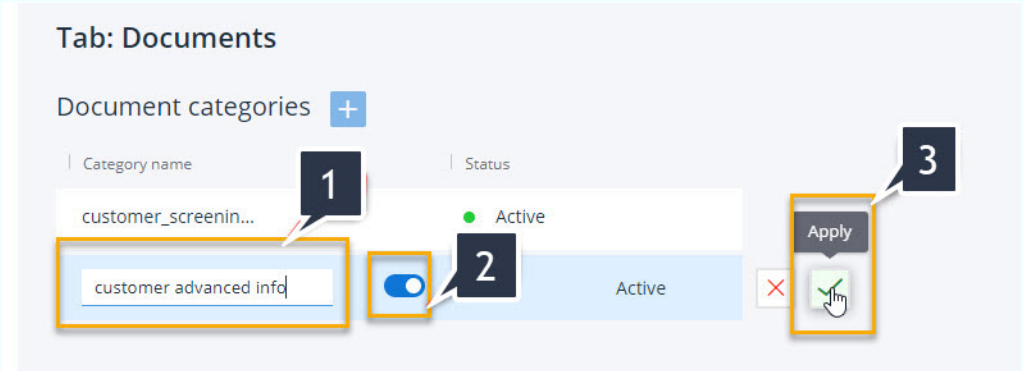
1. Click the Edit link as shown in (1) above
2. Modify the name.
3. Click **Save**.

2.9.3. Documents Tab

The documents tab allows you to add document categories.

To add a document category in the document tab:

1. Click the Document icon.
2. Click the + icon.
3. In the 'Add category name' field (1), type new category name as shown below.



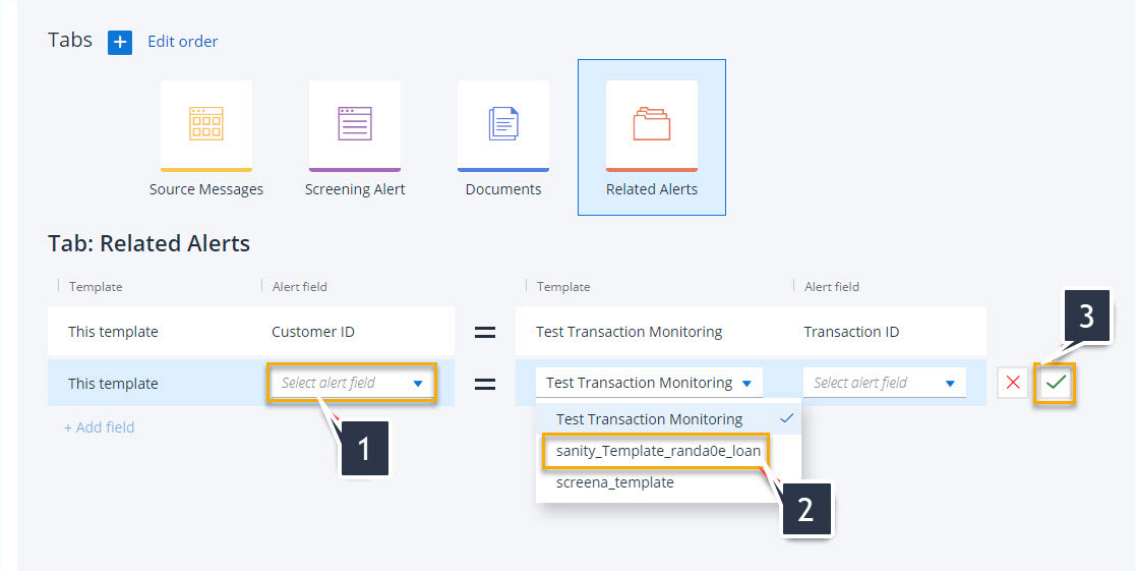
4. Make sure if this category is to be active the switch is enabled (2).
5. Click the green tick icon (3) to add the category and confirm the successful update message is displayed .

2.9.4. Related Alert Tab

The related alerts tab allows you to link to or 'relate' this current alert to other list alerts.

To link the current alert to another alert:

1. Click the Related alerts icon tab.
2. Referring to the example image below: select the alert to relate to as shown.

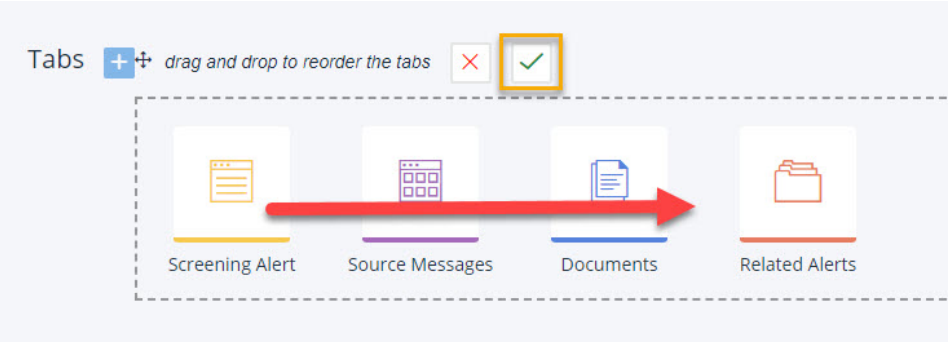


3. Select the current alert from the dropdown (1).
4. From the dropdown list indicated in (2) select the alert to relate to.
5. Click the green tick icon and confirm the successful action. (3).

2.9.5. Reordering the Screening tabs.

To reorder the screening Tabs:

1. From the Alert tabs screen ,click the **Edit order** link
2. Referring to the image below drag the icon to be moved to its new position.



3. Click the green icon to confirm the move and verify the success message.

2.10. Additional Elements - Autotext Templates

This section contains the following topics about Auto text templates:

- Purpose and Benefits
- How to create and use
- Practical Usage Examples

Purpose and Benefits

When investigating alerts, analysts are required to summarize alert details. This is a manual time consuming task and as such impacts negatively on work flow efficiency. The ability to create various custom text templates automates this process and saves the analyst valuable investigatory time.

In the alert resolution workflow, it is now mandatory when changing the alert state, for the analyst to complete a note detailing the rationale for the state change. Auto - text templates are ideally suited to this task, thus providing consistency in messaging and saving the analyst's time in manually creating a new note.

In Investigation Center if assigned to the alert that is being viewed the analyst has the option to create an auto text template note (with rich text formatting if required) of the following types:

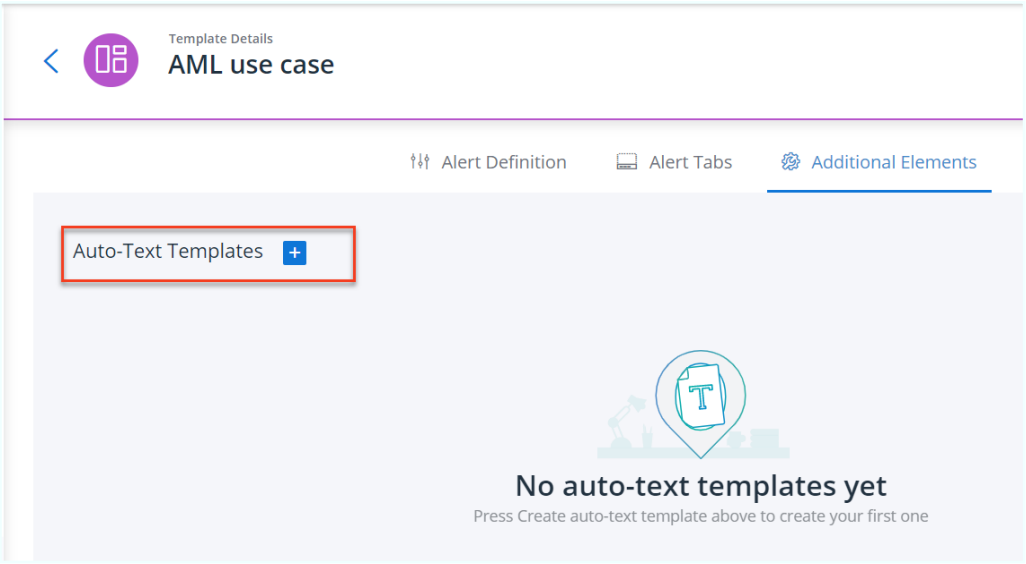
- Narrative
- Information
- Process

Note: For those requiring more detailed instruction on creating Auto Text Templates, refer to the Auto-text templates training video available from the ThetaRay instructional video library.

To create and add an auto-text template:

1. From the Investigation Settings side panel click templates -> Additional Elements.

An Add (+) autotext template is displayed, as shown below.



2. Click the add icon + to display a 'Create auto-text template' form as shown below.

2.10.

Autotext templates are constructed by combining free text with available fields from the drop-down list to create scripts.

2.10.1. Detailed Steps to Create Autotext Templates

With reference to the above figure, steps to create an auto text template include:

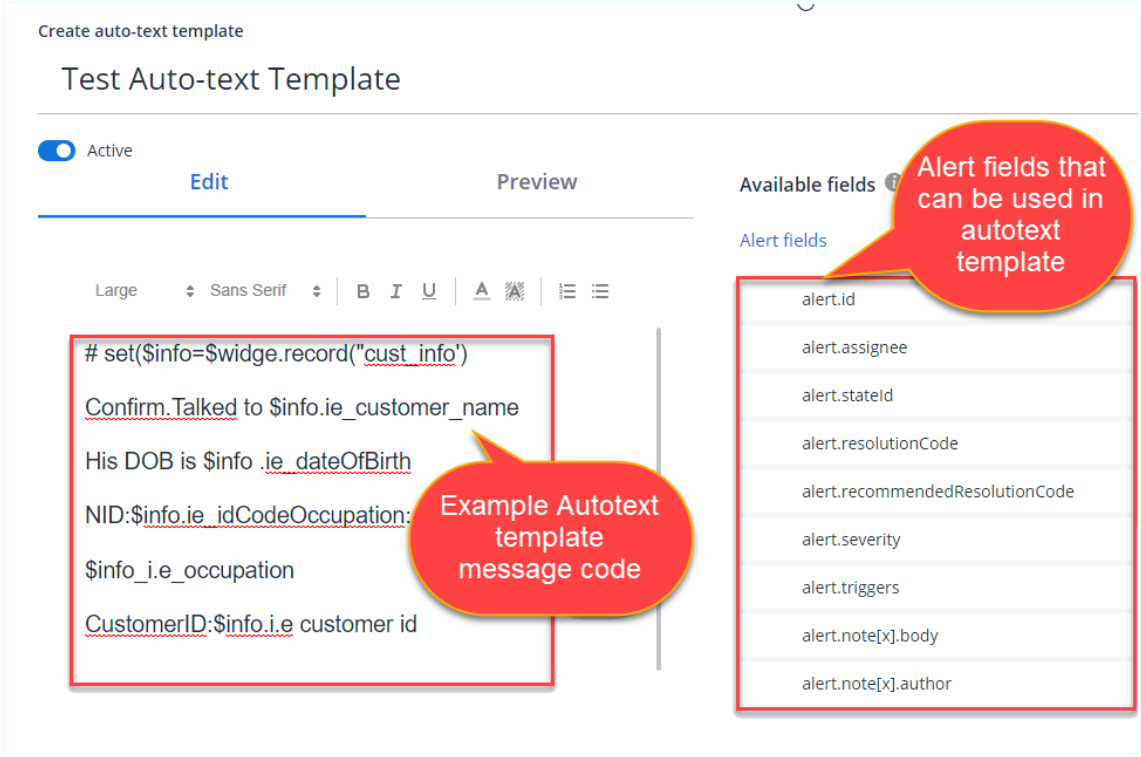
1. Provide a name (1)
    a. Using characters that conform to the character limitations listed in the following bullet list, first provide a meaningful name for your text template.
        - max length 30 chars
        - A-Z, a-z
        - 0-9
        - commas, underscores & hyphens
2. Set Active/inactive toggle switch (2).
3. The content format in auto-text templates can be enhanced with the rich text formatter supplied (3):
    a. Add the free text content in the text workspace area.
    b. Use the Rich text menu to add formatting and preview the final look by clicking the Preview tab (3).
    c. Using the syntax defined in the 'Velocity' language, and using available alerts fields (5), build the required auto-auto text template on the available canvas (4) For
    d. For more information refer to the available ***Auto-text Templates Training Video***available from ***Customer Support.***

e. If including Date and Time elements in Auto Text templates, the following case syntax example provides an example of the syntax that should be used when including an alert 'Occurred On' in the Auto Text Template:

```
$dateTool.createDateStringFromTimestamp($anomaliesDescriptions
[0].occurredOn,"yyyy-mm-dd")
```

For more information on Date and Time formats, refer to the 'Date Time formats Symbols' Description section of the current IC Admin Guide user guide.

4. When finished editing, make sure the template status switch (2) is in the Active position and click Save (7) to add the template to the available templates selection in the Notes tab of IC .
5. It is good practice to open the IC module, navigate to the Notes tab and confirm that the newly created Auto Text is available for selection.



f. If including Date and Time elements in Auto Text templates, the following case syntax examples related to working with dates, provide syntex examples when working with dates.

```
$dateTool.createDateStringFromTimestamp($anomaliesDescriptions
[0].occurredOn,"yyyy-mm-dd")
```

Figure 24: *Date - Occurred on example*

```
id = $alert.idassignee = $alert.assigneestate id = $alert.stateIddate =
$widget.KYC[0].date
```

Figure 25: *Get KYC Related date example*

2.10.2. Viewing , Editing /Deleting a Saved Autotext template

Once saved , you can view, edit and if required, delete the Auto-text template.

2.10.3. Viewing an Autotext Template

Clicking the ***View*** link displays the Auto text templates for further editing if required.

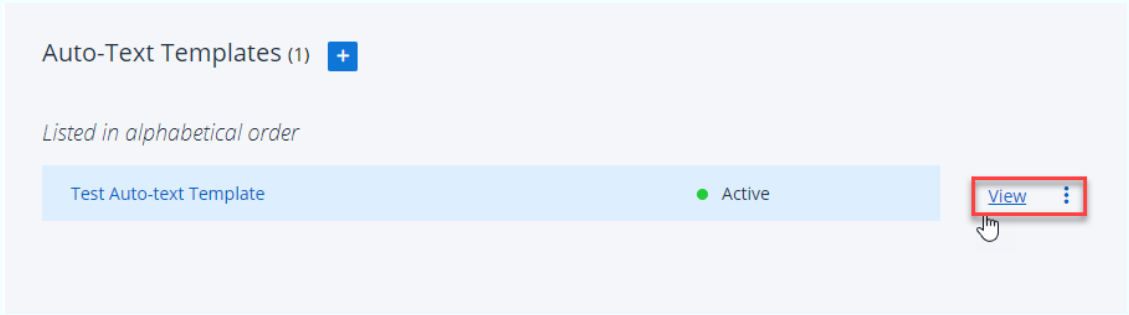


Figure 26: *Example - Access to View Autotext Template*

2.10.4. Editing and Removing Auto-Text Templates

Modifying or removing a configured template is simple and can be performed at any time.

To Edit a configured template

1. Click the **Edit** button on the Auto-Text templates pop-up.
2. Delete (Remove) function is displayed by clicking on the three elipse icon.
3. Make the necessary modifications to the template and click **Save**.

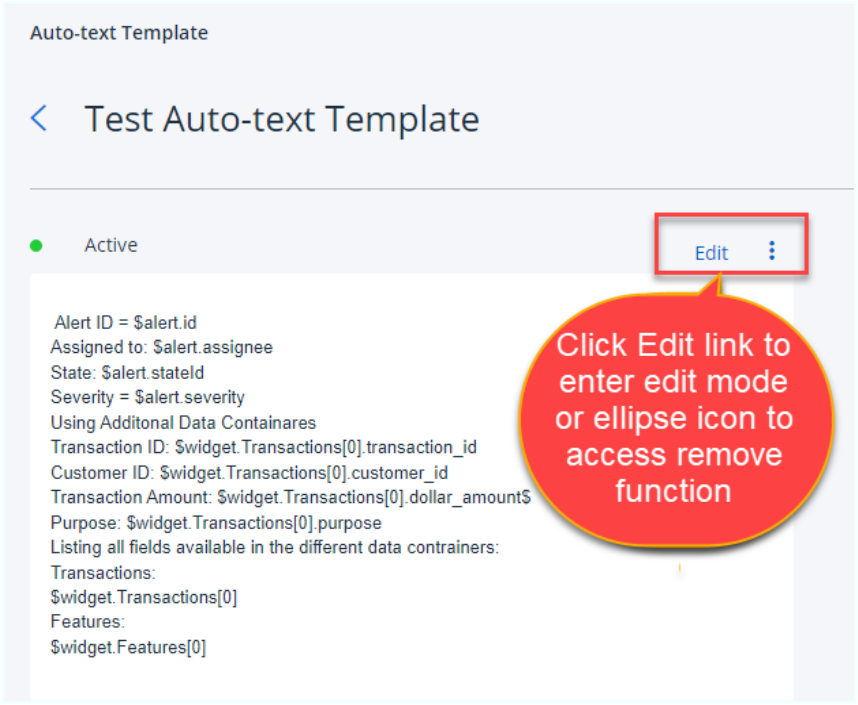


Figure 27: *Example Autotext Template and Accessing Edit / Delete (Remove) Functionality*

2.10.5. Handling Errors

Errors in the construction process are detailed in the Error Details section of the Preview mode.

1. Fix the error(s).
2. If not already activated and the auto-text template is required to be used in the notes tab, move the switch from **Inactive** to **Activate**.
3. Click **Save** to complete the create the autotext template.

Note: Trying to save an autotext template before configuration, results in the following error being displayed.

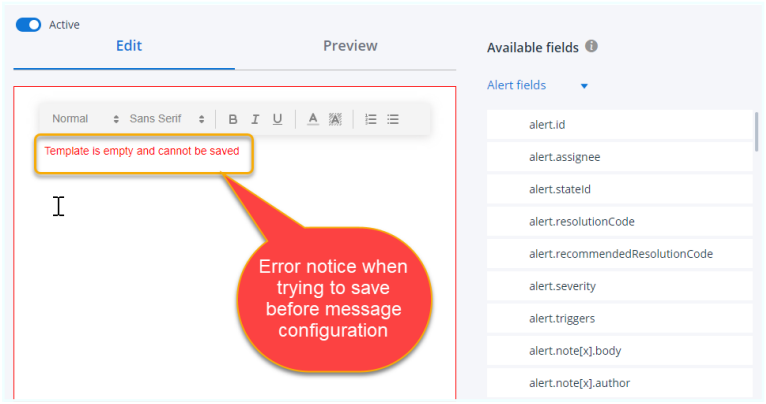


Figure 28: *Example Error Message When Trying to Save Before Configuration*

For more troubleshooting help, refer to Troubleshooting Autotext Template Code Box in the *More Information* section.

2.10.6. Autotext Templates - Event Audit

Be aware that all events that relate to auto text templates (e.g. creation, modification, reopening etc.) are audited.

2.10.7. More Information and Practical Examples

The following five sections provide more information and practical examples on creating auto-text templates and along with a bit of practice, will help you and your analyst team to become more experienced users, and therefore further improve the level of alert resolution efficiency.

- A Quick Introduction to Velocity Syntax
- More Autotext Template Creation Tips
- Finalizing the Autotext Template
- Using Auto-Text Templates to Write Report Notes
- Learn by Doing - Practice with Auto-Text Templates!
  - Example 1: Displaying Data from Data Container and Alert
  - Example 2: Transforming Timestamp to Date Format + Data Dump
  - Example 3: Using Logical Operators and #if clause
  - Example 4: Calculation Operations in Template
  - Example 5: Handling Missing Values
  - Example 6: Printing an Array of Data in a Loop
  - Example 7: Populating and Printing from an Array Example 7: Populating and Printing from an Array
  - Troubleshooting Auto-Text Template Code Box

2.10.7.1. A Quick Introduction to Velocity Syntax

For fuller details about using Velocity, be sure to visit https://velocity.apache.org/engine/2.0/user-guide.html

Syntax	Example
Variables are preceded by $	$anomalyDate
Commands (directives) are preceded by #	#set
#set directive sets the value of a variable or a	#set($name = "Sarah")

Syntax	Example
property inside parentheses. The value, the right side of the equation can be a variable reference, String literal, property reference, method reference, number literal, Array List or Map.	**$name** **Output**Sarah
#if defines a condition to be met before an action can be performed. Each #if block must be closed with an #end directive. An #else or #elseif directive within the #if block are used to specify alternative conditions to act upon.	#set($name = "Sarah") #if ($name == "Dan") Dan #else $name #end Output:**Sarah**
#foreach starts a loop that iterates over elements in a list or array element. Must close with #end.	#foreach($product in $allProducts) $product #end Output: Broom Table Boat Toy ....
Double quotes allow you to use velocity references and directives to interpolate, where the $name will be replaced by the current value before that string literal is assigned. Single quotes will ensure that the quoted value	#set($name = "Sarah") #set($name1 = "$name") $name1 Output: Sarah #set($name2 = '$name') $name2 utput: $name
## and #*...*# can be used to comment text an directives out, so the Velocity engine will not try to process them. ## marks a one-line comment (until the end of the line) #*marks a multi-line comment, until it is closed by *#	#set($name = "Sarah") ##set($name2 = '$name') Comment #* ulti-line comment Thus begins a multi-line comment. This text because will not be displayed because the Velocity Templating Engine will ignore it. *# $name Output: Sarah

2.10.7.2. Finalizing the Auto-Text Template

Now that you have accomplished the most important tasks in creating your new Auto-Text template, let's do the important final steps.

To finalize the Auto Text Template:

1. Save your template (just to be safe). This takes you back to the template menu.
2. Click on the **Edit** button for the next template.
3. Click on **Preview** to discover any problems in your template.

4. If there is anything to correct or tweak:
    - Click Edit and make the required corrections
    - Click **Preview** again
    - Repeat this until the required result is attained
5. Toggle the status switch, located to the right of the Auto-Text Name text box, to **Active**. This makes the template available for use in IC.
6. Click **Save**.

2.10.7.3. More Autotext Template Creation Tips

1. Decide what text and alert fields you need to use in your text and write it in "pseudo-code".

Look at this short example (bold text indicates desired variables):

```
Contacted CLIENT regarding account no.ACCOUNT
```

2. Research and plan how you will obtain the field values that will replace the pseudo-code placeholders of step 1.
    - Data can generally be acquired from 2 sources – Data Containers and anomaly/ alert fields
    - Data Container fields can be copied from the Available Fields pane on the right
3. Set new variables of your choosing to the Data Containers the fields belong to. Variables are indicated by the $ sign preceding them. Setting variables is done by using the #set directive.

In this case we will set $.record(related parties') to $rp by entering the following line in the text box:

```
#set($rp=$widget.record('related parties'))
```

Now you don't need to use $widget.record('related parties') again. $rp can replace it entirely.

Note: $widget.record('related parties') is Velocity syntax. It is a system variable that loads the first record from the source 'related parties'. On the other hand, the $rp variable can have any other name you choose.

4. For each field you need from the related parties list of field use a variable by appending the field name to "$rp" + ".". Attach the fields you need from the Data Container (related parties) to the prefix you set ($rp) with a period. So **$rp.account_id** is shorthand for **[$widget.record('related parties')].account_id**

According to the pseudo-code text you wrote in step 1, you'll understand which fields to append to $rp, for insertion into the Auto-Text template:

Pseudo text:Contacted CLIENT regarding accountno.ACCOUNT. Fields needed: client_Id,account_Id

5. In the code box or any text editor, concatenate the required fields to '$rp.', resulting in:
    - $rp.client_Id
    - $rp.account_Id
6. In the code box, verify that you have the line of code written in Step 3 above, setting the value of $rp to the required Data Container.
7. Add the pseudo text:
   Contacted CLIENT regarding accountno.ACCOUNT.
8. Substitute the concatenated variables from step 5 for the placeholders in the pseudo text, which was Contacted CLIENT regarding account no. ACCOUNT :

```
#set ($rp=$widget.record('related parties'))
Contacted $rp.client_id regarding account no.
$rp.account_id.
```

In preview mode, it will look like this:

```
Contacted 9366 regarding account no. 7562.
```

When used in the Investigation Center as a note for an alert, the text will be exactly as in preview mode (above) except the client id and account id will change according to the specific alert.

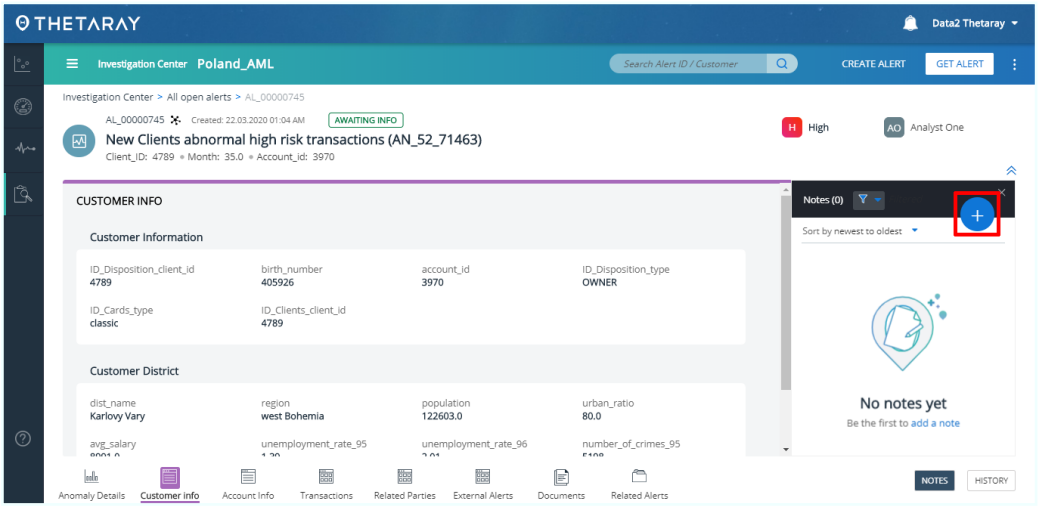
9. Next, we'll continue with the steps for Finalizing the **Auto-Text Template.**

2.10.7.4. Using Auto-Text Templates to Write Report Notes

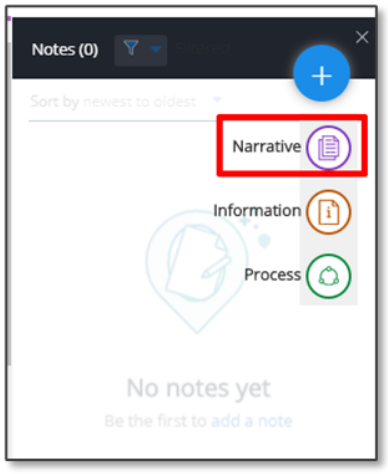
The best part about the Auto-Text Template feature is actually using them in your IC workflow to quickly add meaningful mistake-free, detailed notes to your reports.

To use your Auto-text-Templates in your Investigation Center workflow:

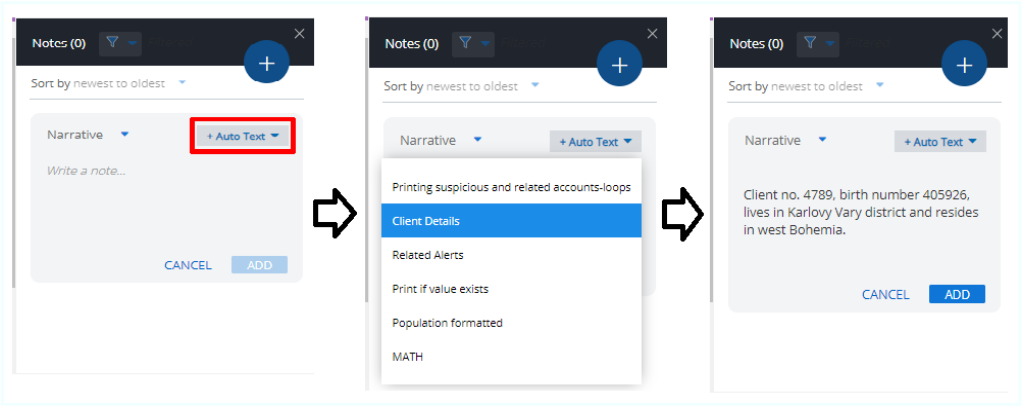
1. Open the Investigation Center.
2. Go to your alerts.
3. Click on an alert to edit it.
4. On the bottom tab bar, click the **Note** button.
   The Notes panel opens.
5. Click on the **Blue Plus** icon at the top of the panel.



6. From the three icons displayed, click on Narrative.

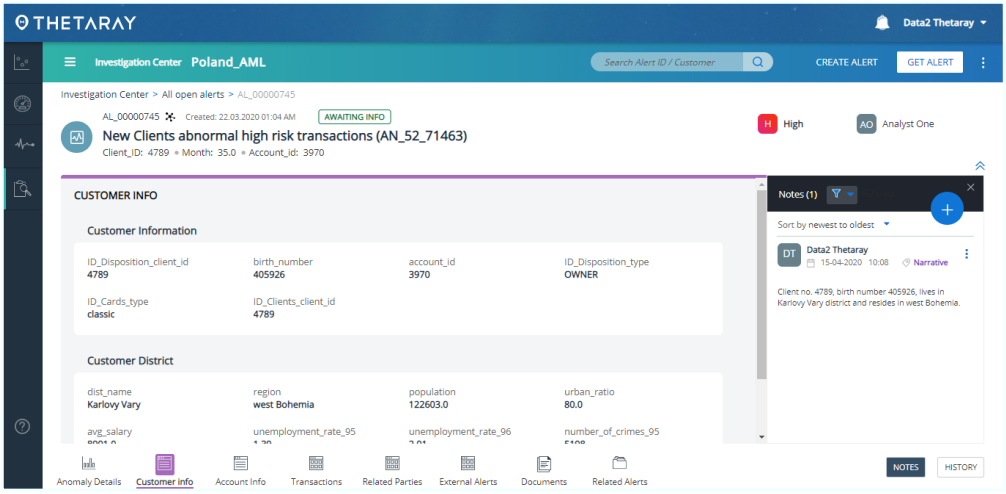


6. Click on the **Auto Text** drop down and select the required Auto-Text by title. Remember, only Auto-Text templates that are set to Active in the Auto-Text Template UI are listed and selectable.
   After selecting the title of your Auto-Text, the text you created is displayed, and all the fields you added in Edit mode, specific to this alert are displayed.



7. Click **Add** if you wish to add the text to your alert notes.

The note is added:



2.10.7.5. Learn by Doing - Practice with Auto-Text Templates!

The series of Auto-Text templates below can be used in your templates or as standalone learning exercises to copy, paste into the template editor, modify and preview. For each example below, you will see its:

- Goal /scenario expressed in the title
- Edit mode view
- Preview-mode view
- Some helpful comments

2.10.7.6. Example 1: Displaying Data from Data Container and Alert

This example shows how to display a list of attributes for a client and an alert, using data from 2 (or more) containers.

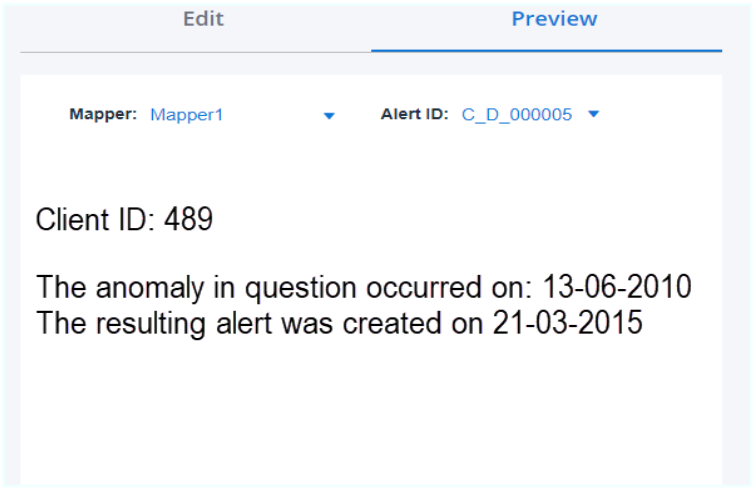
```
Client ID: $widget.record('client info').ID_Clients_client_id

The anomaly in question occured on:
$dateTool.createDateStringFromTimestamp($anomaliesDescriptions
[0].occurredOn, 'dd-MM-yyyy')

The resulting alert was created on:
$dateTool.convertDateTimeFormat($createdDate,  "yyyy-MM-
dd'T'HH:mm:ss.SSSZ",  'dd-MM-yyyy')
```

The example retrieves data from 2 data sources – the 'client info' data container and the properties of the specific anomaly / alert the user is working on.

Addressing each of these sources is slightly different, as you can see above.

The **$dateTool** function allows you to set the desired format for date data. We will discuss it in the next example.

Preview Mode:



2.10.7.7. Example 2: Transforming Timestamp to Date Format + Data Dump

This example shows how a timestamp can be displayed as a formatted date.

Edit Mode:

```
This alert was generated on:
$dateTool.createDateStringFromTimestamp ($anomaliesDescriptions
[0].generatedOn, 'yy-MM-dd')
Severity rating: $severity.
$anomaliesDescriptions[0]
```

The instruction $anomaliesDescription[0] dumps many properties of the anomaly, including the date for the record. This allows the user to select any property, like viewing the original timestamp inside the data, while scripting the template. The analyst would not normally include this dump in a template to be used in reports. This is for training purpose only.

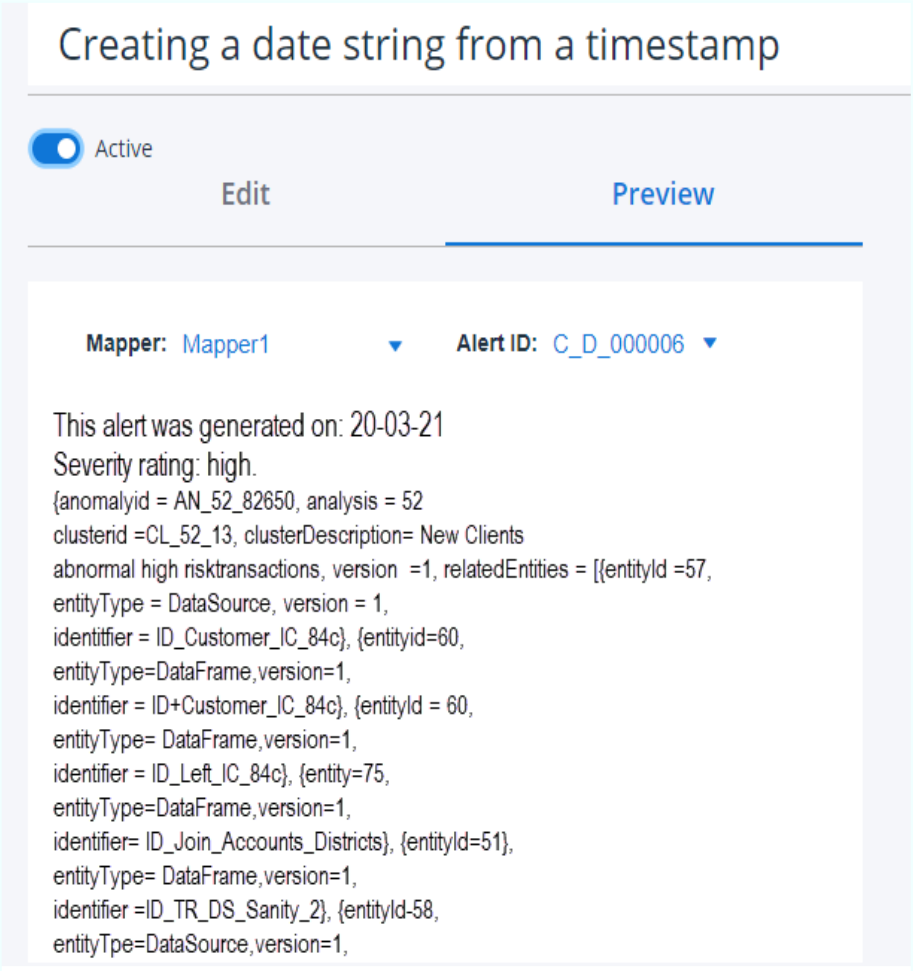
The following are the methods exposed by $datetool on note templates.

All results will be retrieved as formatted date strings.

Method	Arguments	Description
convertDateTimeFormat	1. String dateString - the date to format 2. String initialFormat -	Converts supplied date string (arg 1) in specific format

Method	Arguments	Description
	the current format 3. String desiredFormat - the result format	(arg 2) to the desired format (arg 3)
createDateStringFromTimestamp	1. Long timeStamp - date as Epoch 2. String format - result format	Formats number epoch date: (arg 1) to desired format (arg 2)
now	1. String format - result format	returns current time at provided format

Preview Mode:



2.10.7.8. Example 3: Using Logical Operators and #if clause

This example shows how you can use logical operators like AND (&&) OR (||) and NOT (!) to determine conditions for taking an action.

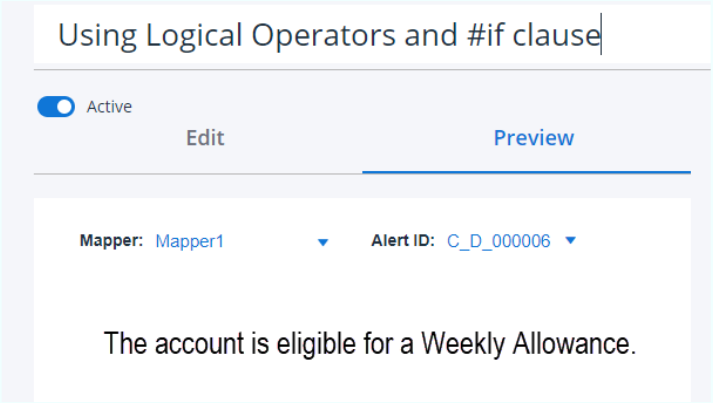
We use #if and #elseif statements to create the different options. The #end statement has to come at the end of every #if block.

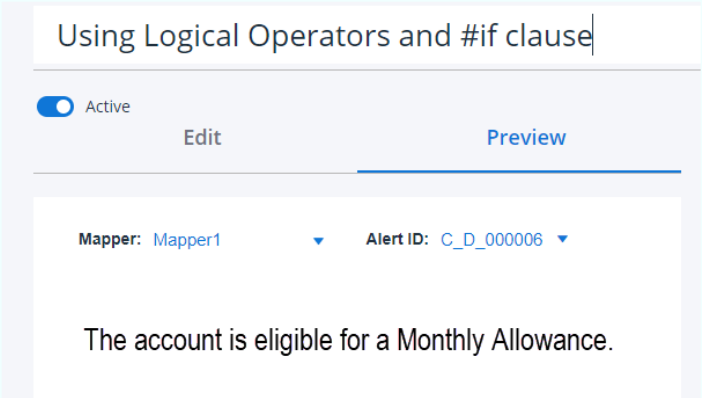
Edit Mode:

```
#set($info=$widget.record("account info"))
#set($freq=$info.frequency)
#set($avg=$info.avg_salary)

#if ($freq == "Monthly issuance" && $avg >= "8000")
The account is eligible for a Monthly Allowance.
#elseif ($freq == "Monthly issuance" || $avg >= "6000" && $avg
<= "7000")
The account is NOT eligible for a Monthly Allowance.
#elseif ($freq != "Monthly issuance" && $avg >= "8000")
The account is eligible for a Weekly Allowance.
#else
The account is eligible for no Allowance.
#end
```

The different combinations of $freq and $avg allow you to set flexible scenarios and act on each one differently.

Preview Mode:





2.10.7.9. Example 4: Calculation Operations in Template

In this example, we show how to run basic calculations on data acquired from the containers.

Edit Mode View:

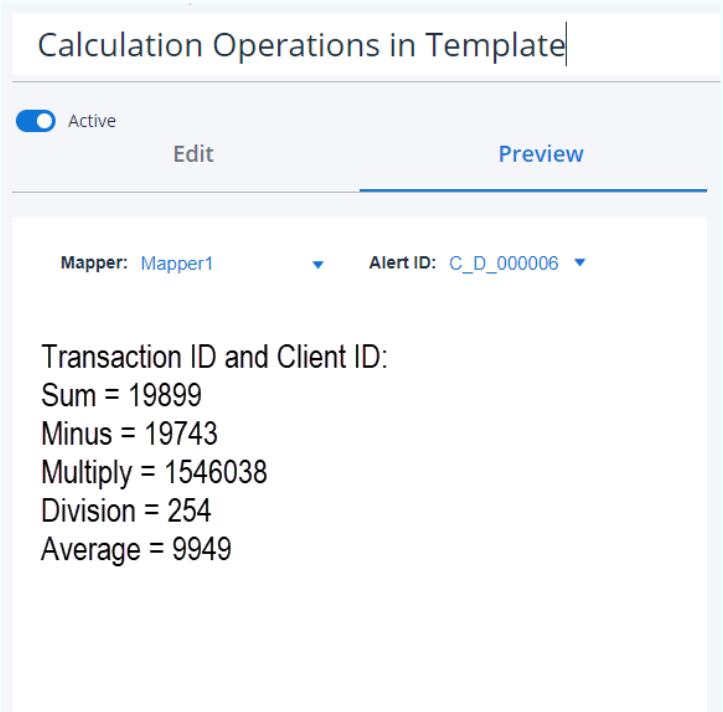
```
#set($alerts = $widget.table("alerts"))
#set($a = $widget.record("alerts").trans_id)
#set($b = $widget.record("alerts").client_id)
#set($Integer = 0)
#set($numa = $Integer.parseInt($a))
#set($numb = $Integer.parseInt($b))
#set($array1 = [$numa,  $numb])
#set($arrsize = $array1.size())
Transaction ID and Client ID:

#set ($sum = $numa + $numb) Sum = $sum
#set ($min = $numa - $numb) Minus = $min
#set ($mul = $numa * $numb) Multiply = $mul
#set ($div = $numa / $numb) Division = $div
#set ($ave = $sum / $arrsize) Average = $ave
```

We get the alerts table, then the required records.

$Integer.parseInt($a) is required to cast the string into an integer (proper number), so calculations are possible.

The array ($array1) is useful for getting the number of items, to calculate the average.

Preview Mode:



2.10.7.10. Example 5: Handling Missing Values

Example for running a check to see if a row is empty:

Edit Mode:

```
#if ($myMap.isEmpty())
...
#end
or
#if ($myMap.size() == 0)
...
#end-2-end-demo
```

2.10.7.11. Example 6: Printing an Array of Data in a Loop

Example of getting value from each row (get loan_id from each row):

Edit mode:

```
    #foreach ($lo in $widget.loan)
    $lo.loan_id
    #end
```

2.10.7.12. Example 7: Populating and Printing from an Array

Example on how to sum values:

Edit Mode:

```
$alert.id
#set($env = 50)
#foreach ($lo in $widget.loan)
$lo.loan_id
#set($res = $lo.loan_id + $env)
#end
$res
```

2.10.7.13. Troubleshooting Autotext Template Code Box

Syntax Errors are indicated in the Error Details section of the Preview.

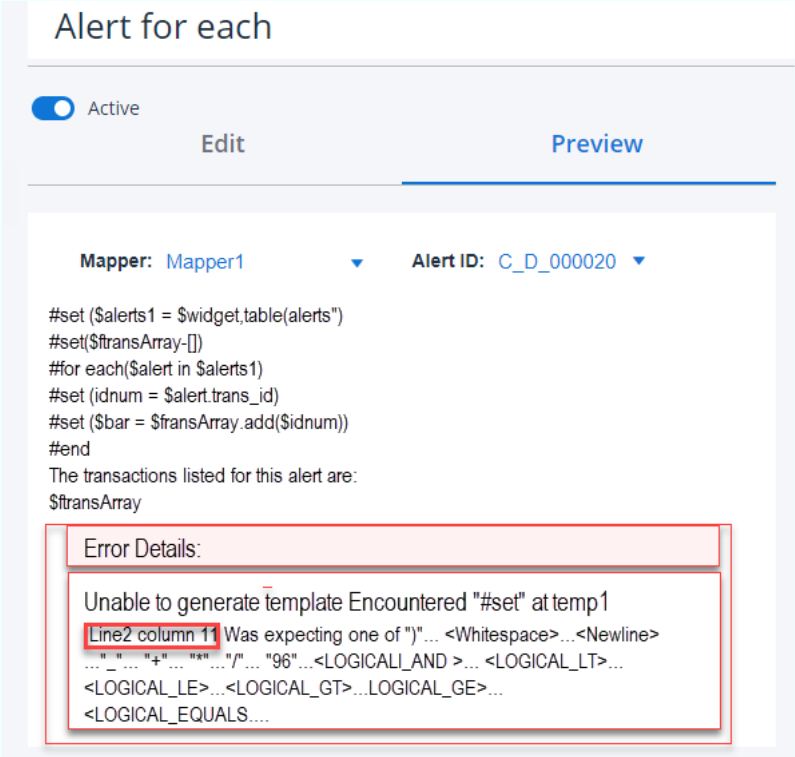


Figure 29: *Example Trouble Shooting Error Details Screen*

Depending on the error, you may get a more specific error message, as above.

Here, the system is telling you where the error is located – line 2, column 11.

It also indicates that it was expecting any of the listed characters and did not find any.

That usually means that you forgot to close a statement or a variable properly. In this example, the second closing) is missing after “alerts”).

Here are some other things to try:

1. Compare your code directives with code directives in a script that is working.
2. Check your syntax against the Velocity User Guide.
3. Check the names of the Data Containers you are accessing are specified without spelling errors.
4. Do not use the '.' character in property names. For property names, use the same rules as for the template title.
5. Be aware that once a variable has been assigned to some value using #set, it cannot then be removed from the context (set to null).
6. If your problem does not get solved quickly within your team, don't hesitate to escalate it to ThetaRay Customer Support.

3. Containers

A Container in the alert data flow is used to map to a source of data information that is required to be utilized and displayed in an alert. Once created, configured and populated with data set fields they provide the created template (via the mapper) with a range of internal and external data set sources to facilitate the alert investigation process in your environment.

A single data container can be used in multiple different IC settings and in some instances can serve clients which are not related to alert investigation.

For a general view of how containers are used in the broader data flow, refer to the Data Flow Example diagram located in the data flows introductory section of IC Settings.

Limitations

A data container although subject to certain caveats is subject to standard operations

- Creating
- Reading
- Updating (note: removal of a field from a data container is only possible if the field is not used in any tab.
- Deletion

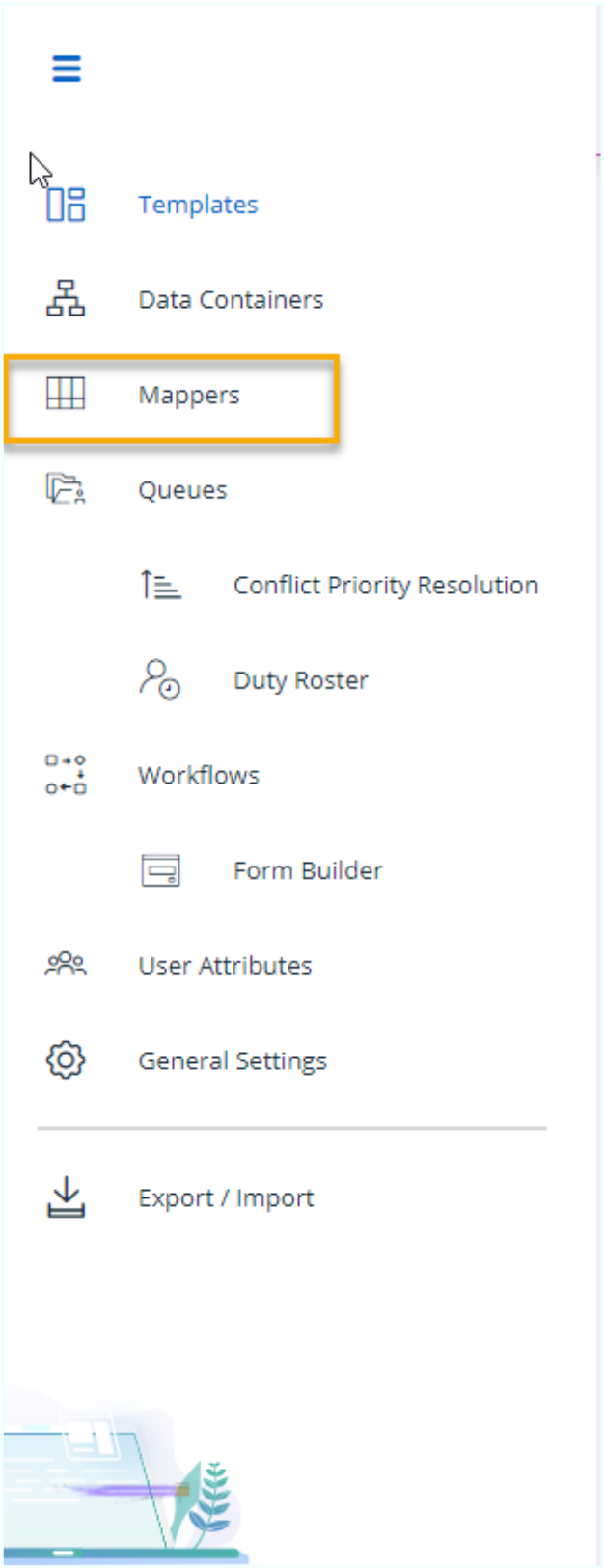
Data container parameters include:

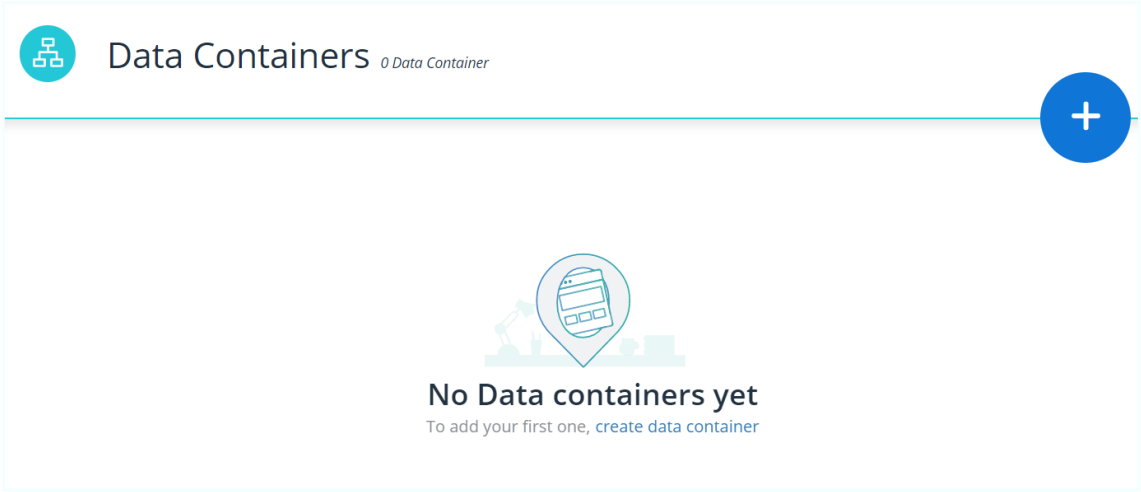
- Solutions
- Data Set
- Field name
- Field type

Note: Tabs which used the data container, will be automatically updated to the new name.

To create a Data Container:

1. Click the Data Containers Icon from the Side Pamel.

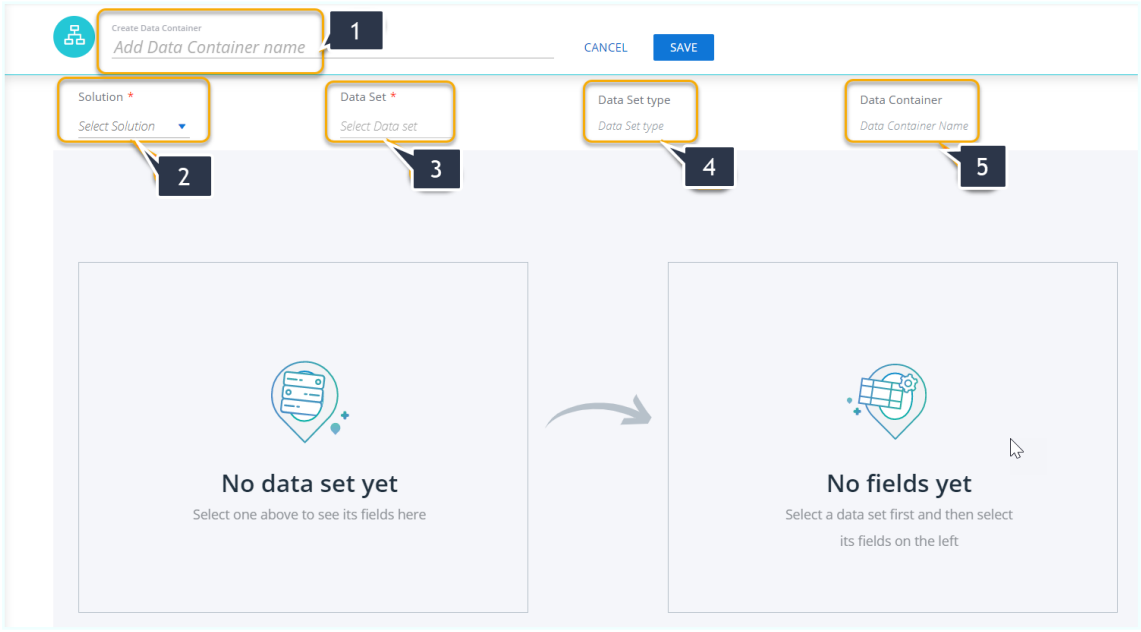




As can be seen from the above figure no containers have yet been configured.

Let's create our first container.

2. Click the create data container link (+) on the upper right of the screen to display the create container form.



3. Provide a descriptive name for the container, (for example: Accounts, Features, BICs AML solution (that will contain many data sets)(1).
4. Click the Solution dropdown menu (2) select a solution.
5. From the Data Set dropdown menu (3) select a Data Set from the available sets.

Note: The Data Set Type is automatically selected to match the Data Set (OVERWRITE, APPEND, or UPDATE)

There are two methods of selecting fields to populate the container:

1. By text search query (1).
2. Selecting from a list of fields from each available data set (2).

A list of example available transaction related fields (including their data types) is displayed below on the left as follows:

Figure 30: *Container Field selection Example for a Transaction Data Set*

3. Either search for a field if the displayed list is long, or click the boxes next to the fields to be added to the container(Note: selecting the first box selects /deselects all fields).

Note: The text search option includes auto complete so that when you start to type the required field name, auto complete will display available field names as you type.

Once you select a single or multiple fields, the Add (number) Fields button is displayed.

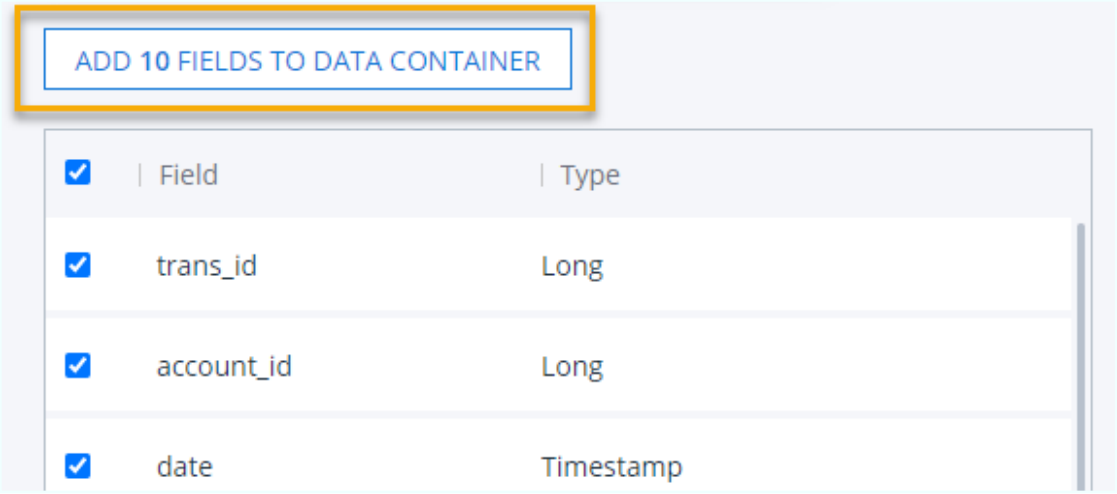


Figure 31: *Add Field Button Displayed when a Field Selection is Made*

4. To move selected fields to the right panel:
   a. Click the **Add Fields to Data Container** button *or*,
   b. Click the **+** icon on each item individually.

The selected fields are now added to the container as shown below.

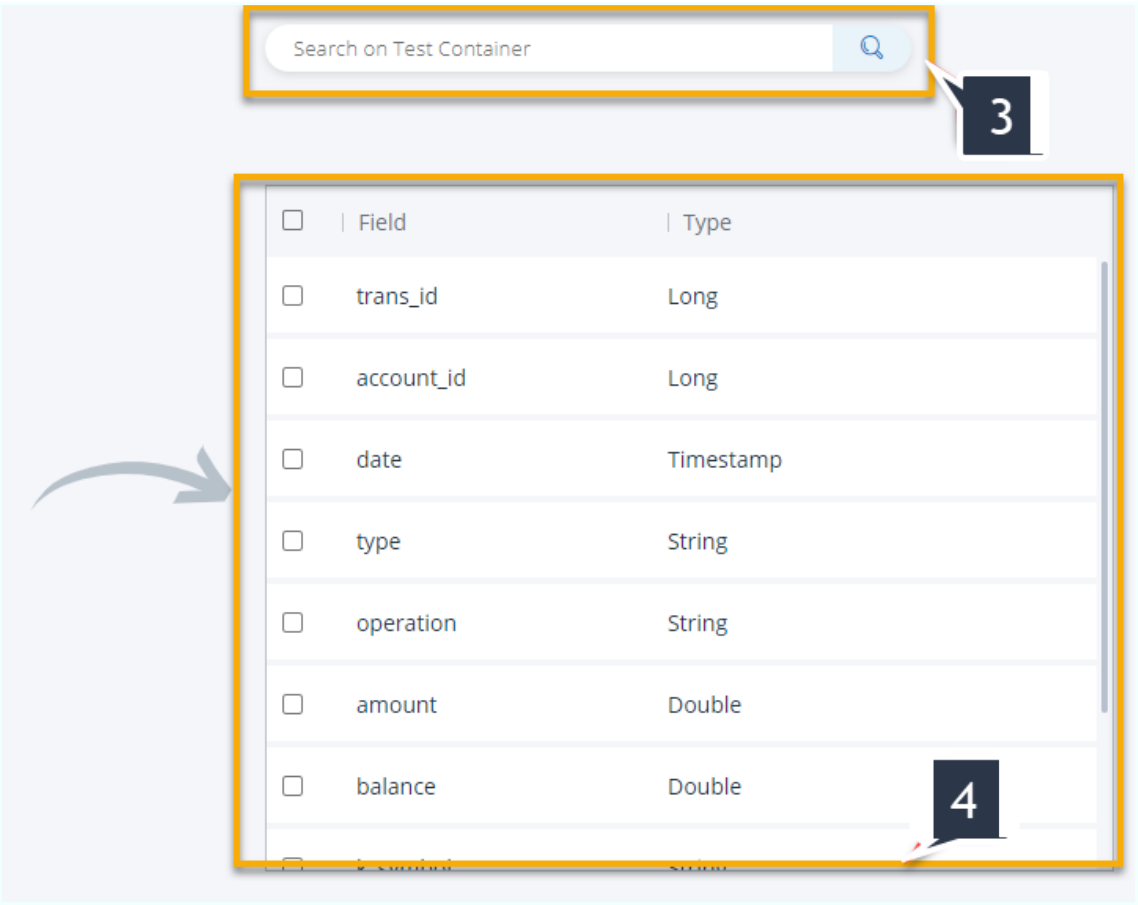


Figure 32: *Selected Fields Added to Container*

3.1. Removing Added Fields from Container List

Once the fields have been added to the container, you can if you wish select and remove unwanted fields.

To remove an added field or fields:

1. Select the fields to be removed.
2. Click the remove link displayed above the list or click the delete icon next to the each individual field to remove unwanted fields.
3. Searching for added fields to remove is the same process as described in 3. above.
4. When the Container is complete, remember to **Save**.

3.2. Working with Containers - Summary

From the example process previously described, continue to create and populate data containers as required.

It is suggested that the example process on container creation and population described in this topic should be adopted in your container management tasks for your environment.

Additionally, to make the process of managing alert data as efficient as possible, it is suggested that separate data containers be created for each data category type, with each container holding related fields.

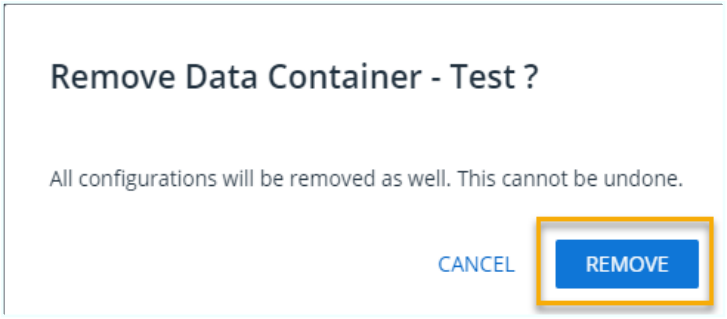
3.3. Removing a Container

Note: Once the IC module is in use (populated with data), If required to remove a container or data fields from a container you first need to remove the association between the relevant mapper and the container.

To remove a data container that has not yet been populated with data:

1. Select the Data container from the list of data containers.
2. Click the delete icon next to the entry.

The following confirmation popup is displayed.



3. Either confirm removal or cancel.

4. Mappers

Mappers are used to enrich the data an alert card can hold by enabling the configuration of multiple paths or maps to be created between detected alerts and a wide range of available data sources both internal and external, stored in a data container or containers.

In essence once configured , they provide the necessary channeling of the data source held in a container and connect its content to a destination field in the template.

Most of the work in the mapper maps between logical fields which were defined in the template and their location.

Multiple mappers can co-exist and generate alerts of the same structure - but with different data sources (containers).

The split between templates and mapper also allows greater flexibility in terms of the ability to display in one tab input which comes from different data sources.

The Mapping process includes:

- Mapper definition
- References
- Alert Definitions
- Alert Tabs

Mappings - Key Points to Note:

- Once configured, link data held in containers to the default tabs included in the deployment, however you as a system administrator can select to refine your alert investigation strategy by mapping data to specific custom tabs
- It is not a must to use all the tabs or fields which are defined in the template It is possible to inactivate a specific tab or field in a specific mapper.
- It is possible to mix between data containers/references which are used and display one form with mixed sources
- It is possible to prepare the mapping outside of the system in a CSV file. This should ease the work if and when a tab includes high amount of fields which are not different from their data container and providing manually
- References - try to map between alert fields in mapper and data container, not template display names shown in the template

Prerequisites:

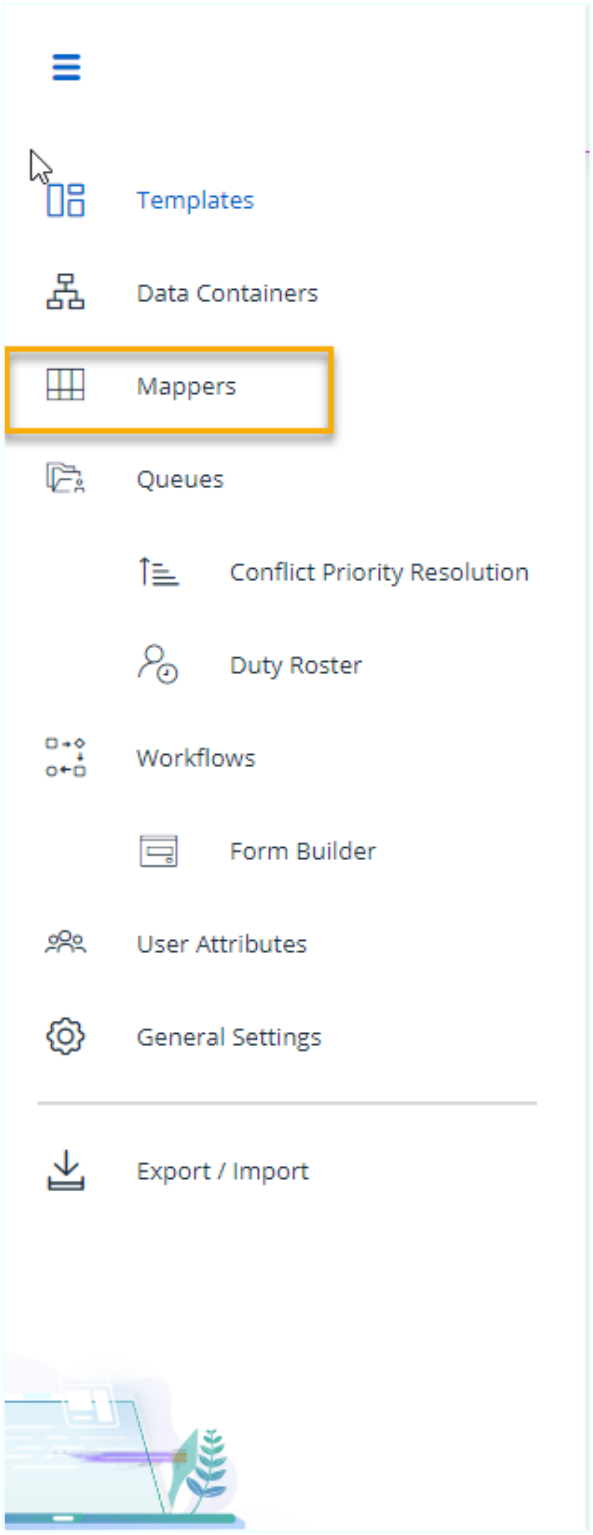
A user with permissions to "Settings:WRITE" can generate / update mappers.

Mappers in New Deployments

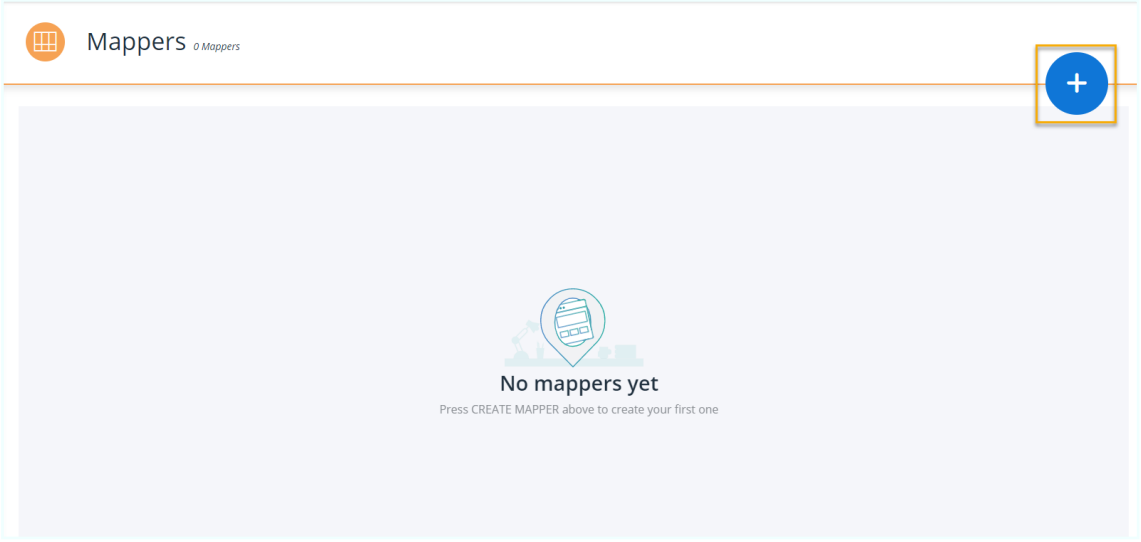
In new deployments, mappers will need to be created. The following image is displayed in new deployments where mappers have not yet been created.

To create or edit a mapper:

1. Click the Mappers Icon in the Side Panel.



The mappers create edit screen is displayed. In the example shown below no mappers have yet been created.



4.1. Mapper Definition Tab

The first stage when creating mappers, is to define the mappers.

Mappers Definition enable alert consolidation from different evaluation flows into a single alert, so that analysts can optimize the investigation and resolution of alerts.

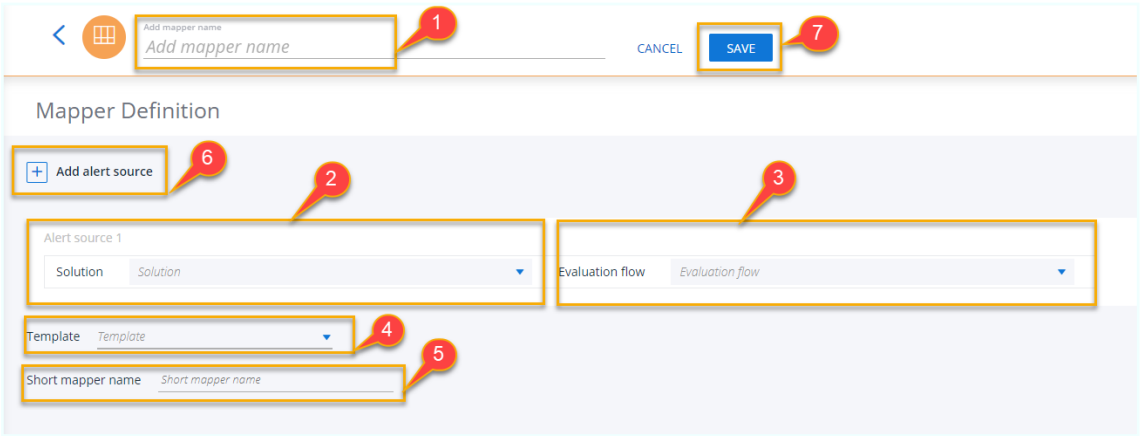
To configure a mapper definition:

1. From the side bar menu, select the 'Mappers' option.

The Mapper Definition tab is selected by default.

2. Click the + icon.

A Mappers Definition configuration form is displayed.



To create a new mapper definition:

1. With reference to the above form, provide the following information.
   a. A name for the mapper (1).
   b. Solution (Alert Source) (2).
   c. An available evaluation flow (analysis) (3).
   d. A template (4).
   e. Provide a 'short mapper name'(prefix) or use the system given one (to ensure the overall mapper name is unique (5).
   f. If more that one alert source is to be mapped to the same or different evaluation flow, click the + icon 'Add Alert Source" (6) and repeat process from step (2).

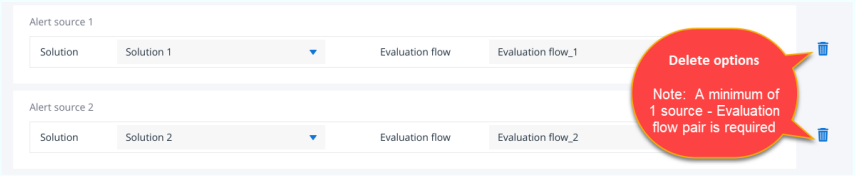


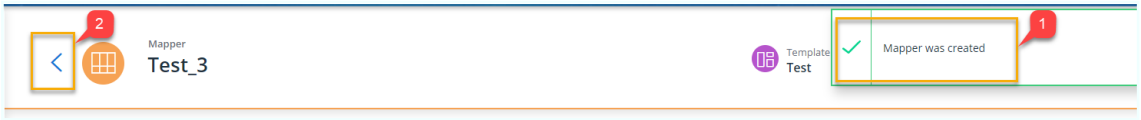
Figure 33: *Example of Two Alert Source - Evaluation Flow Configurations*

   g. When complete, don't forget to click **Save**.

Note: To help ensure all the fields are completed as required , pressing **Save** prematurely results in an error notifications in the required fields.

4.1.1. Mapper Definition Configuration Verification

If the mapper is created successfully the following success message is displayed as shown in (1) in the figure below.



To view the table of created mappers, click the back arrow as shown in (2) in the above figure.

The current list of related mappers and configurations is displayed as shown below.

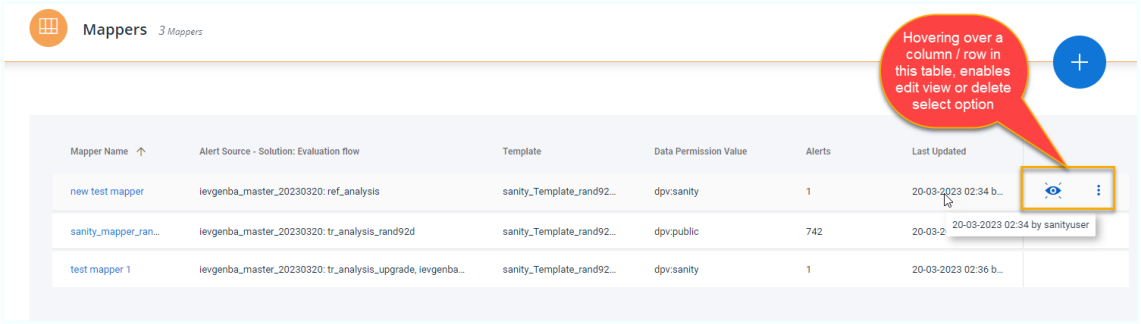
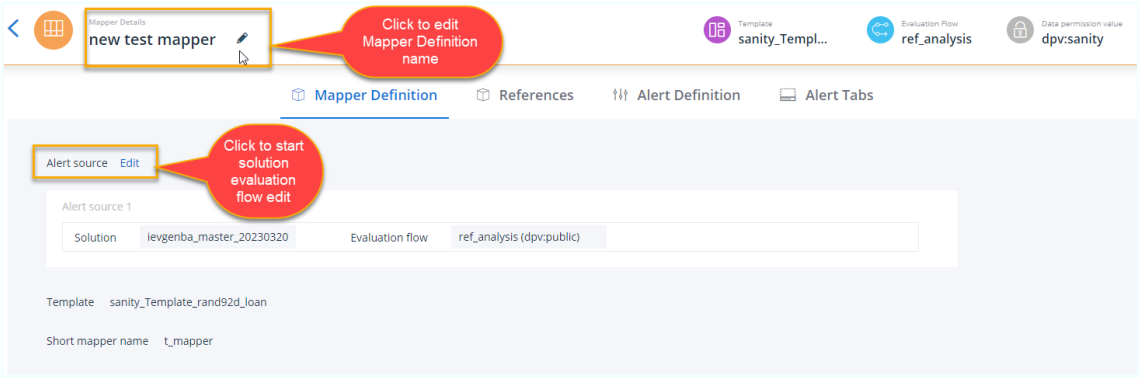


Figure 34: *Example List of Created Mappers*

4.1.2. Editing Mapper Definitions

Mapper definitions can easily be modified. Clicking a mapper definition from the available list of created mappers, or clicking the show icon (as displayed in the previous image) , displays the configured definition as shown in the following example.



To edit just the mapper definition name:

1. Click the pencil edit icon.

2. Change the mapper name then click the green (confirm) tick.

A confirmation message is displayed.

To edit the mapper definition pair setting:

1. click the ***Edit*** link to enter Edit Mapper Definition mode.

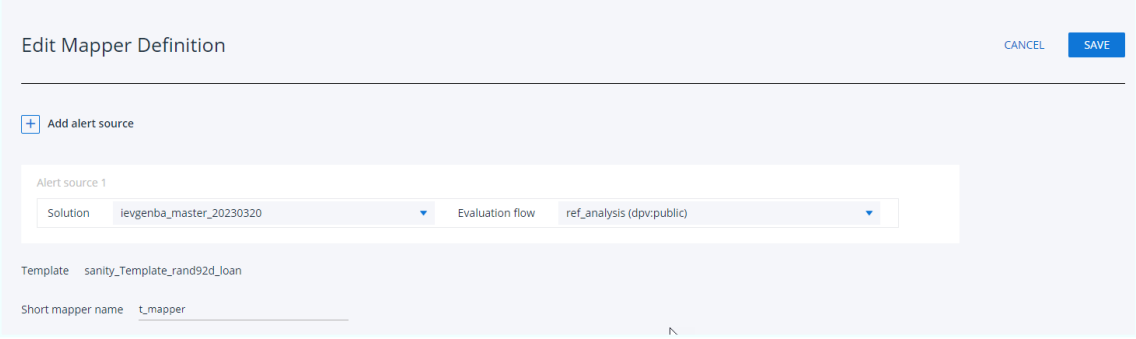


Figure 35: *Mapper Definition - Edit Mode*

Edit mode enables the following functionality:

- Change the Source
- Change the Evaluation flow
- Add additional alert source definitions from scratch

2. When complete , don't forget to click **Save**.

Note: Deletion and removal of a created mapper does not affect already published alerts

---

4.2. Mappers - References

The following are the key points regarding references:

- A reference has a name which is used to map a field in the mapper to a source
- References allow the definition of what data containers will be used by the mapper and what is their relationship with the investigated entity
- Each reference includes mapping between the alerted activity fields (key or non-key) and between fields of the data container
- Mapping links can be configured based on one or more fields
- Adding external data containers is managed outside the scope of the mapper's scope

4.2.1. Adding References

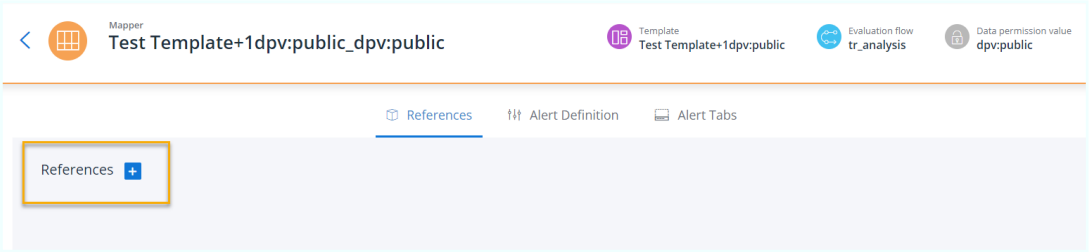
Mapper references enable the data scientist or data engineer to map source data stored in container fields to specific alert fields located on static or custom created

alert tabs.

To display the references add mapper screen:

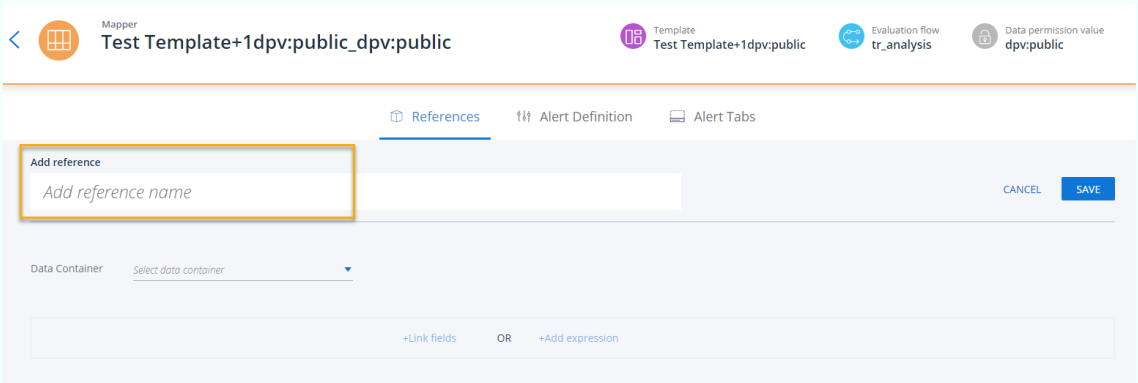
1. Either click the mapper name link under the **Mapper Name** or click the view icon displayed by hovering the cursor over the mapper listing as highlighted below.

The Reference configuration screen is displayed as shown below.



To best describe the mapping process task, we will first add a reference and then continue to map some example data fields to our system tabs.

2. To start, click the highlighted 'References +' link to display the following configuration screen.



1. Click in the 'Add reference name' field.
2. Provide a unique name / id for this reference.

Referring to the following figure, for the purpose of our example we will name our reference, **ref1** (1).

3. Now to start the mapping process click the data container dropdown menu, select a data container(2).

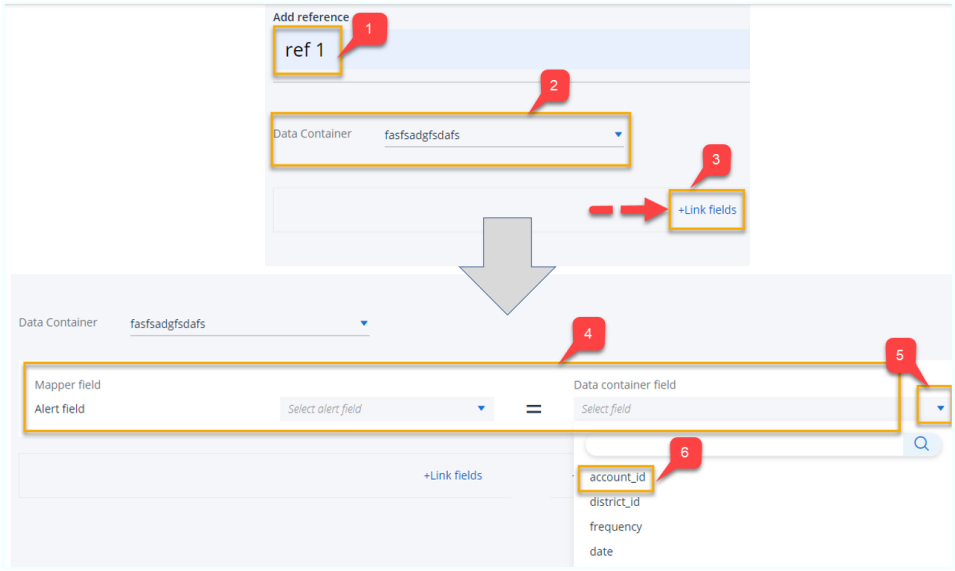
The mapping process provides for two options:

a. To map data in a container to a specific field located on tabs *or,*

b. The setting of expressions, so that if a condition is met, the source data in the container will map to a specific field or fields located in a system tab or tabs.

Example #1 - mapping directly to a tab field

To simplify the process we will start by mapping data in a container to directly to a listed field:
Click the **+Link fields** link (3).



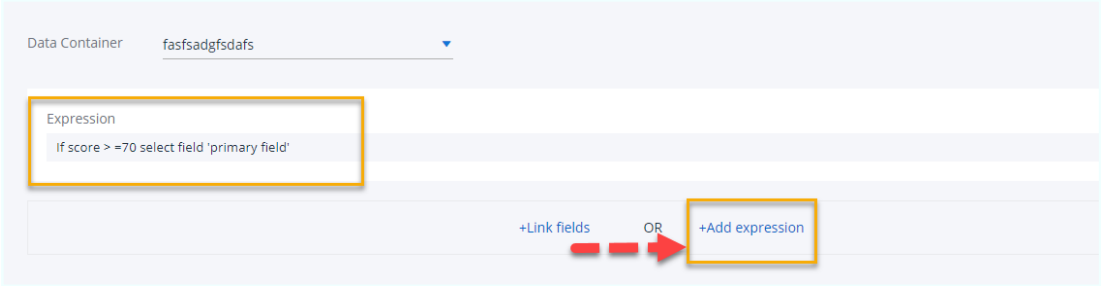
The source /destination mapping statement is now displayed as highlighted in (4). It now requires the data source and alert field selections to be made.

4. Click the Container field dropdown menu and for the purposes of the exercise we will select 'account id' from the displayed fields as our source field(6).
5. In the tab field we will select Primary ID as the mapped alert.
6. In a normal process the mapping process continues until all the configurations are complete.
7. Don't forget to click save when complete.

Example #2 - Mapping with a Conditonal Statement

For example: Test all data results for a score greater than 75 and if 'true'. map to a field in the template named "high score".

The mapping process is similar to that described in example except the Expression link should be selected and a conditional statment entered in the input field as shown below.



8. When complete click **Save**.

Note: Removing Mappers can only be achieved if there are no alerts yet associated with the mappers configurations.

4.3. Mappers - Alert Definitions Tab

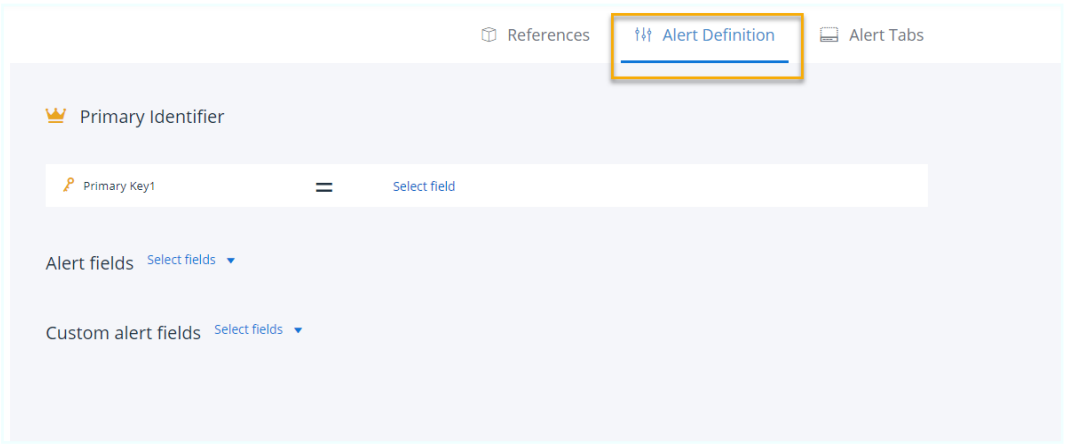
Mappings to alert definitions should configured as follows:

- From the primary key identifier(s) to fields listed in associated containers
- Alert fields defined by conditional usage, either basic and/ or custom should be mapped from the created template to related fields configured in created containers

When working with mappers, mapping to alert fields that have been defined also enhances the overall alert investigation process.

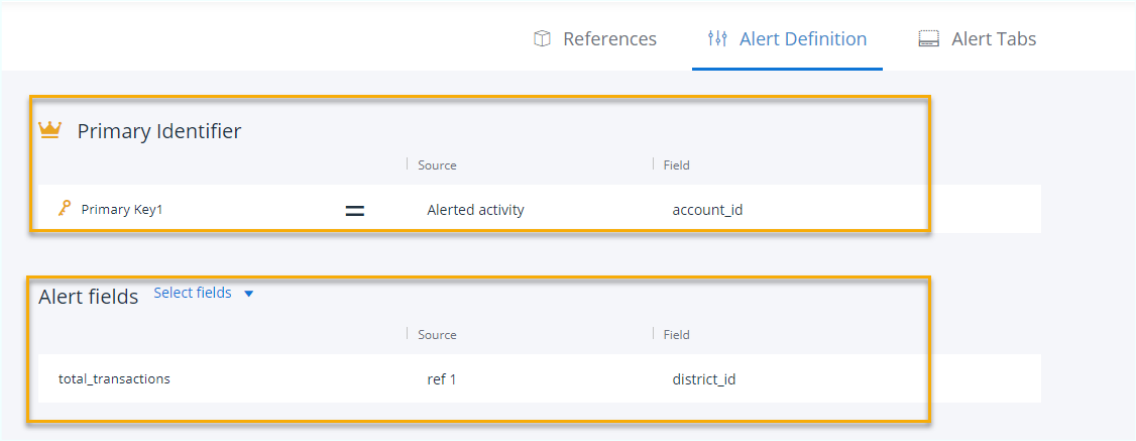
To set up alert definitions for static system or custom fields:

1. From the mappers screen click the alert definitions tab as shown below.

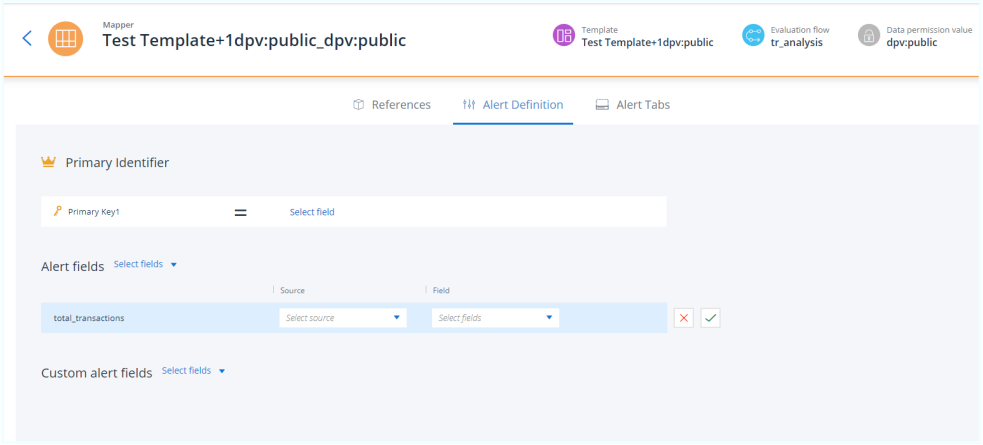


2. Select fields to map to and add sources and extra fields as required as shown in the following example.

Note: When selecting the source be aware of the difference between selecting 'Data Container' data added as the reference is created in the mapper and 'Alerted Activity' data which in some instances may hold more insightful information that was used initially to trigger the alert at the anomaly / alert detection stage.



3. When complete, click **Save**.



Note: Removing Mappers can only be achieved if there are no alerts yet associated with the mappers configurations.

4.4. Alert Tabs - Default

In the Mappers section of IC Settings, under Tabs, there two types of Alert Tabs:

- Default
- Custom

This subsection of Mappers, details the default tabs provided with every deployment.

- Risk Details Tab
- Documents Tab
- Related Alerts Tab
- Entity Resolution Tab (requires license)

4.4.1. Risk Details Tab

The Risk details tab is used in the Investigation Center to provide the analyst with insightful evidence when investigating discovered alerts.

The admin user as part of his /hers work flow tasks is required to ensure the Risk Details tab is configured to maintain maximum efficiency.

Currently, there are two configuration duties that involve the Mappers module and the Risk Details tab:
Global Time Setting: The first is to set the Occurred on - date format for tab trigger details..

Enable Enhanced UI: The second is to enable and configure elements of the enhanced Risk details tab UI which provides the analyst with a much more defined approach to understanding the alert risk evidence gathered in the alert discovery process.

The following image shows the default alert tabs as they are displayed under Tabs of Mappers in IC settings.

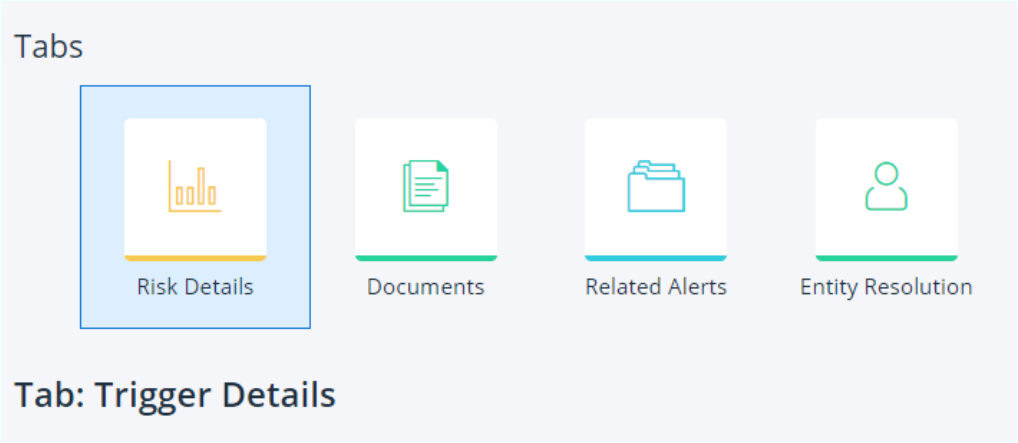
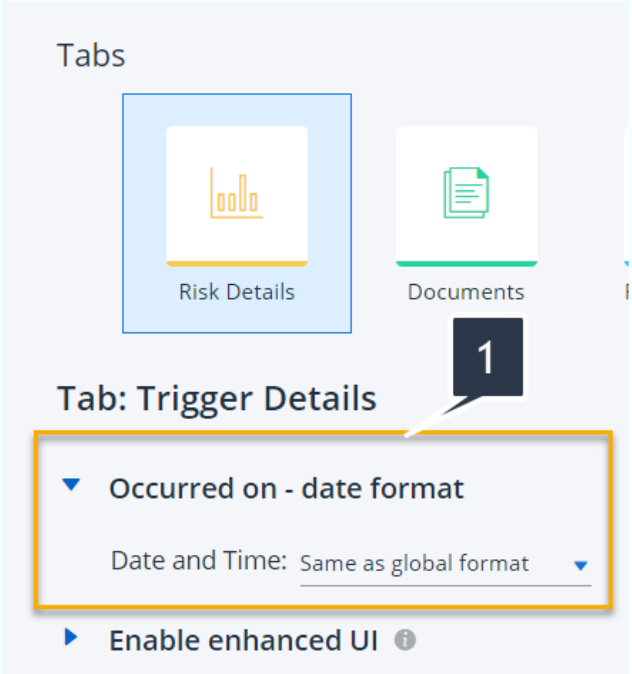


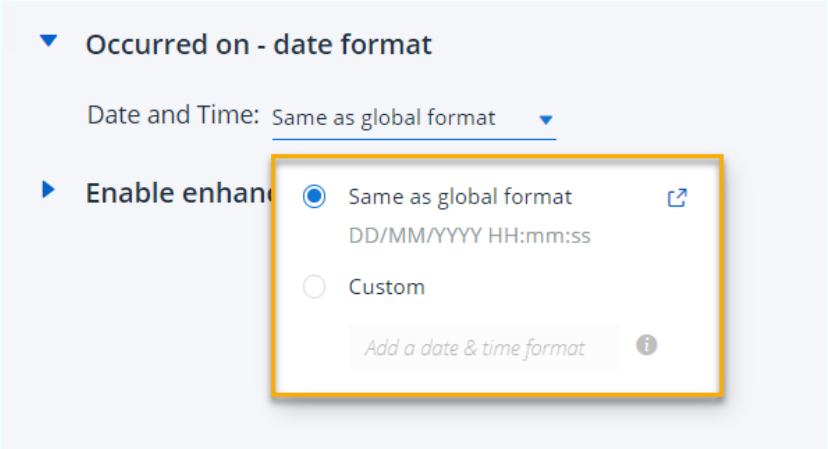
Figure 36: *Example of Tabs section of Mappers Showing Default Tabs and the Risk Details Tab Highlighted*

4.4.1.1. Setting Occurred on Date Format (1)



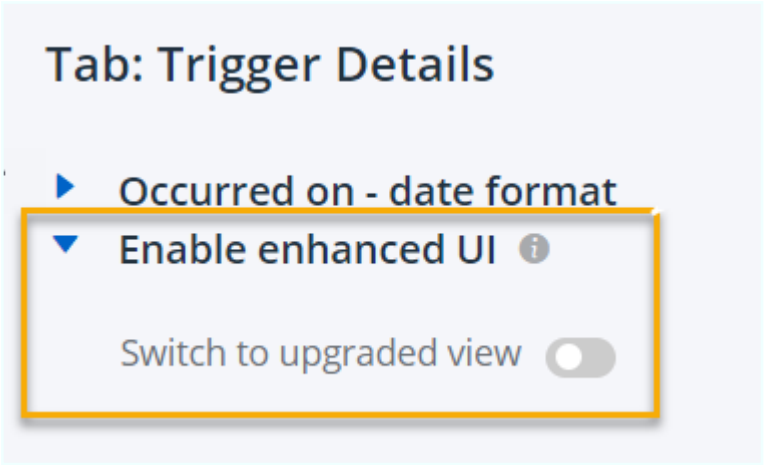
To set Occurred on date format:

1. With reference to the above image, click the down arrow.



2. As can be seen in the above image, you have the option of selecting to set up your analysts to use the global format, or alternatively, a custom format, where you can configure other formats that may better suit your location. (Note, that if you select to configure a custom format, after configuration the suggested format is verified for format compliance.)

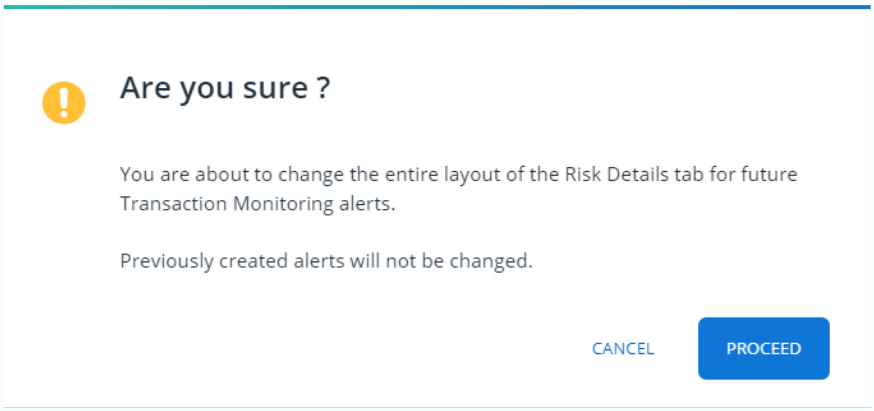
4.4.1.2. Enable Enhanced UI (2)



The process of enabling the enhanced UI requires initially for the Details tab to be first switched over to the upgraded view.

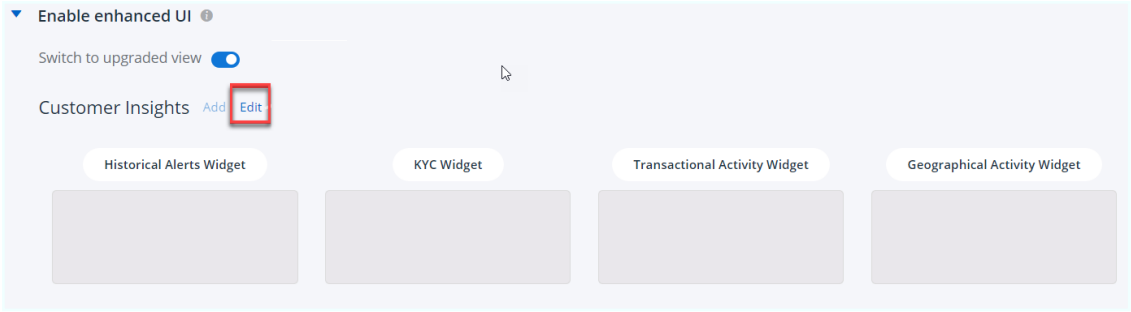
To switch over to the upgraded view:

1. Slide the toggle button shown above, to the right.
2. A caution before proceeding notice as shown below is displayed.

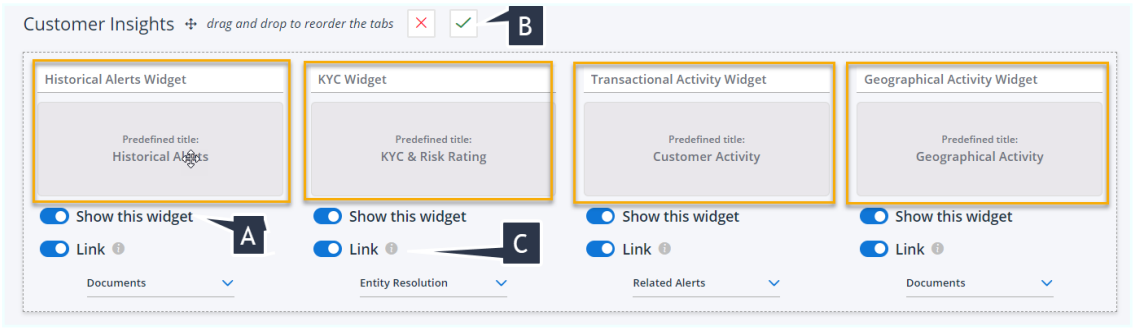


3. Only apply once you have confirmation that all of the necessary configurations have been done on the platform side to support enabling the enhanced UI. Enabling the enhanced UI will only affect new alerts created after enabling. Existing alerts will retain their previous layout.

The following example of enhanced widgets are displayed.



4. Clicking the **Edit** icon as highlighted above, displays the widget types which are employed in the enhanced UI.



With reference to the above image, let's take a closer look at what you can configure in the Enhanced UI settings of the Risk Details tab.

The four example widgets as shown are:

- Historical Alerts widget
- KYC Widget
- Transactional Activity widget
- Geographical Activity widget

Widgets in each deployment can vary depending on customer use case, environment etc.

Note: These examples will only show if they are configured in the platform

---

Depending on your companies Risk Alert resolution strategy, you as system admin can:

- **A** - Configure to show all or just some of the widgets in the IC alerts resolution UI deployment
- **B** - Reorder (drag-n drop) the widgets to be displayed in order of deployement importance
- **C** - Link the widgets to other default tabs

- **D** - Rename the widgets

Additional notes on Enhanced UI configuration:

1. Showing Widgets - The toggle switch setting can also be used to redisplay widgets that have been turned off.
2. Any changes made to the configuration requires setting configuration by clicking the green tick.
3. Linking to other tabs, - to display link selection push the toggle to the right and click the down arrow and select the tab to display other available tabs to link to, then select as required.

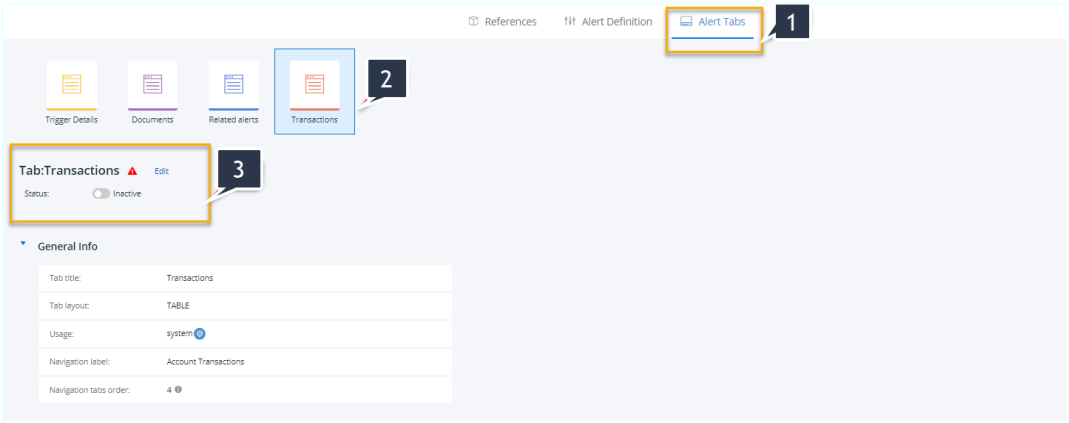
4.5. Alert Tabs - Custom

This subsection of Mappers, details an example of a Custom Tab

Custom tabs are created and configured in the Templates section of the IC Settings module and can be viewed, edited, activated or deactivated as required.

To view custom alert tabs:

1. Click the alert tabs link as shown below (1).



To modify the settings of the Custom tabs in the mapper (for example, tab and field activation, data field mapping etc,)

2. Select the tab to modify mapper settings.
    a. Ensure tab is activated
    b. Click edit.

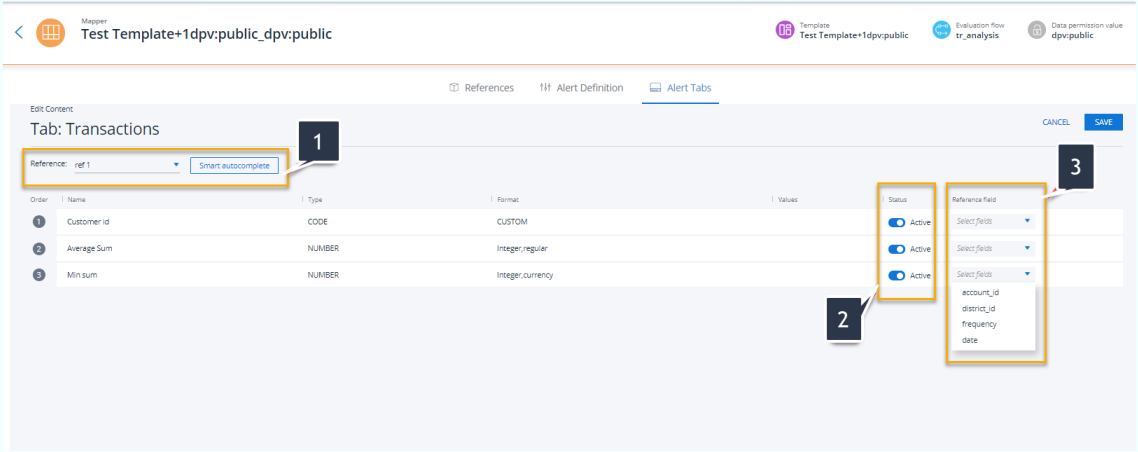
The Custom tab (in this example in tabular format) is displayed as shown below.

3. Referring to the following figure:
    a. Select reference fields to map to (1).
    b. Activate or deactivate fields (2).

c. Select the reference field dropdown menu that you require to modify the associated fields (3).

d. Modify the fields as required.

e. Click **Save**.



4.6. Mappers - Custom Sorting Sequence Setting

Multi level sorting of Source Messages in Mappers is achieved by ordering and enabling attributes in Mappers.

The source message tab has been extended by the addition of three fields:

- Number
- String
- Date

4.6.1. Hierarchical Multi level Sorting

Hierarchical multi- level sorting, enables the screening admin user to custom preset screening source message filter by priority sequences. Once set and saved analysts can use these customized sort sequences to save workflow time when working with large amounts of screening source messages.

These sequences can be set up to 4 levels deep and can be removed and replaced as required. Any message fields can be selected as sort attribute values.

Note: Available sorting attributes are aligned with the origin filter selection, so be aware that if a field you are looking to select is not displayed, it is probably because it is non - relevant and not necessarily a functionality issue.

Note: Be aware, as the process of saving the new config is not automatic, once a custom sort configuration is removed and another configuration made, a reminder to save the new configuration is displayed as shown in the following message

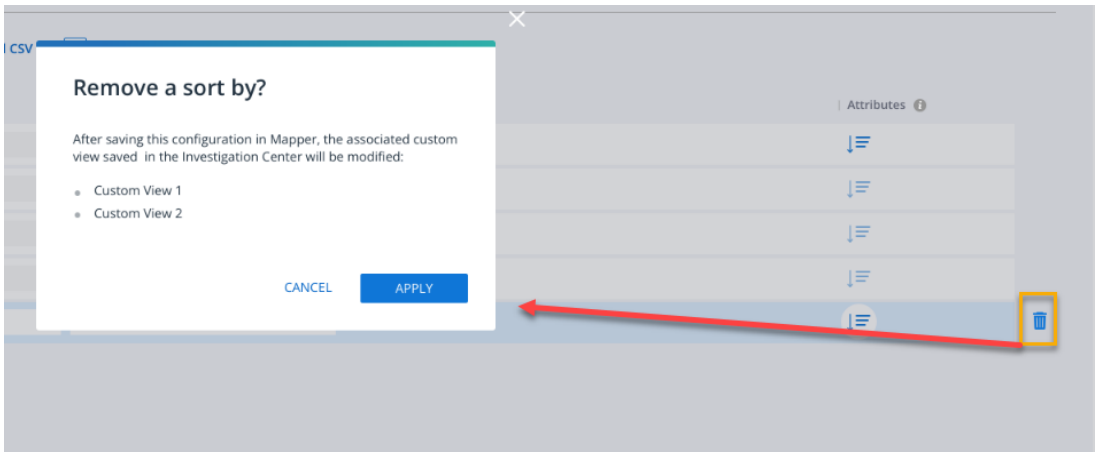


Figure 37: *Example - Reminder Message , Alerting the user to Save the New Configuration*

To Configure a sort sequence:

1. Under the Screening Template, open the ***Tab Source Messages*** screen.
2. Click the ***Number*** dropdown list.
3. Select the 'order to filter by' sequence number.
4. Click the attribute icon at the end of the row that displays the field attribute you wish to select.
5. In deployments with a high volume of messages, you can limit the filter period by clicking the ***Date*** icon and setting the 'Cut off' Period'.
6. You can if required continue this procedure o another 3 times.
7. When complete, do not forget to click **SAVE.**

The delete (remove) icon is available as shown, to remove a custom setting.

Once saved, the sequence is made available to your screening analysts in the in the filter section of the IC module deployment.

The following image shows ***Tab Source Messages*** screen and key components.

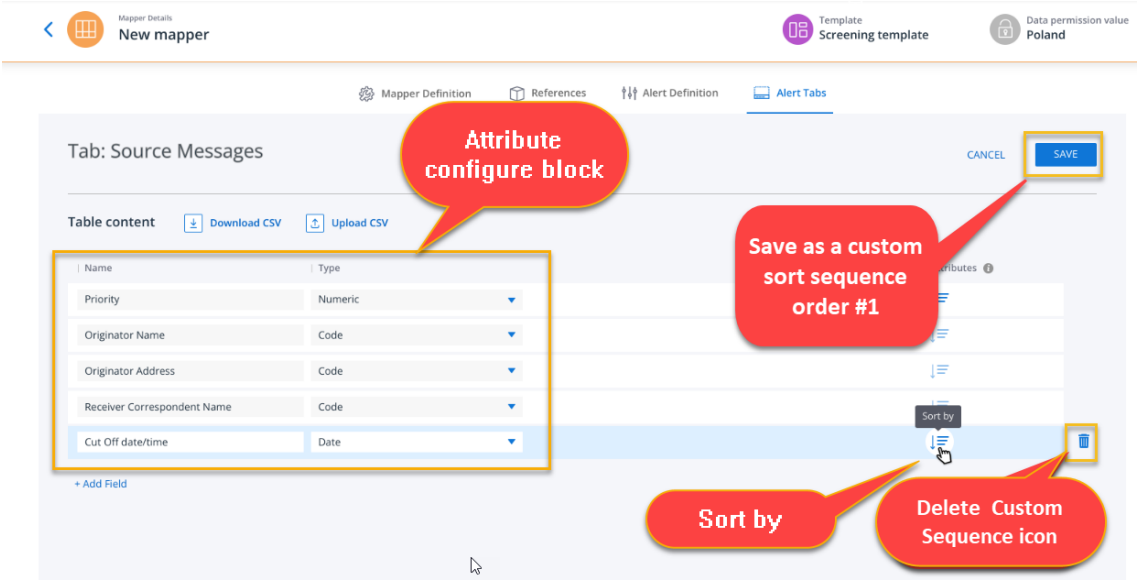


Figure 38: *Example #1 - Custom Sort Key Components*

5. Investigation Center - Teams and Queues

5.1. Introduction

Investigation Center is aimed at supporting large groups of analysts working on investigating alerts in their organization. In many instances, these analysts are required to work on different use cases that may also span diverse geographical regions.

The fundamental, requirement is for an efficient system that organizes analysts into groups according to their field of expertise and permission level as well as ensuring that each group only receives targeted specific alerts.

5.2. Solution Overview - Teams & Queues

The requirement to organize analysts working on similar use case alerts is solved by enabling the organization's business admins to create implement and mange teams with different data permissions and different tasks.

The requirement to ensure that each team only receive specific alerts is solved by enabling business admins to segregate existing and new alerts regardless of the analysis they are sourced from and channel them into alert data queues.

With the implementation of Teams and Queues , Analysts will not be left with too many options and confusions regarding what they should be working on next.

- Teams (groups) management is covered fully in User management, Keycloak
- Queues Management is covered in the following topic

5.3. Usage Example

To best explain Teams & Queues in operation the following usage example is provided:

'Blue Horizons' Bank is a bank that is located in the Bahamas. The bank has branches in Nepal, Congo and Bahutan.

The bank is focused on 3 use cases:

1. Retail AML (for all 4 jurisdictions)
2. Internal fraud (Bahamas only)
3. Correspondent banking (for all 4 jurisdictions)

Pseudo customers (Nepal and Congo)

The bank has a team of 30 analysts.

The analysts are split into 4 teams:

1. **Bahamas Regular Team**

The team's queues are:

- Retail AML - covers all the cases of non VIP customers
- Bahamas CB - all cases except for VIP customers.

2. **Bahamas Experts Team.**

The team's queues are:

- VIP Retail AML
- VIP CB
- Internal Fraud

CB Global Team

The team's queues are:

- CB of Nepal, Congo and Bahutan
- Pseudo customer for Nepal and Congo
- Retail global team. The team's queues are:
- Retail AML of Nepal, Congo and Bahutan

Retail Global Team

The team's queues are:

- Nepal Retail AML
- Congo Retail AML
- Bahutan Retail AML

6. Queues Management

The ability to create Queues helps the Business Admin user to optimally organize generated alerts into lists that can be best handled by available supervisors and analyst teams.

Please note, Queues management is relevant for organizations with multiple teams. For small scale organizations, a single default queue is generated automatically, so there is no need to create more queues

---

Note: The example layouts and options shown in this section depict environments that incorporate such features as data permission values, alert queues and also alert segregation . If the environment you are working with does not include all the functionality that is shown , this is normally due to a more basic implementation of the platform.

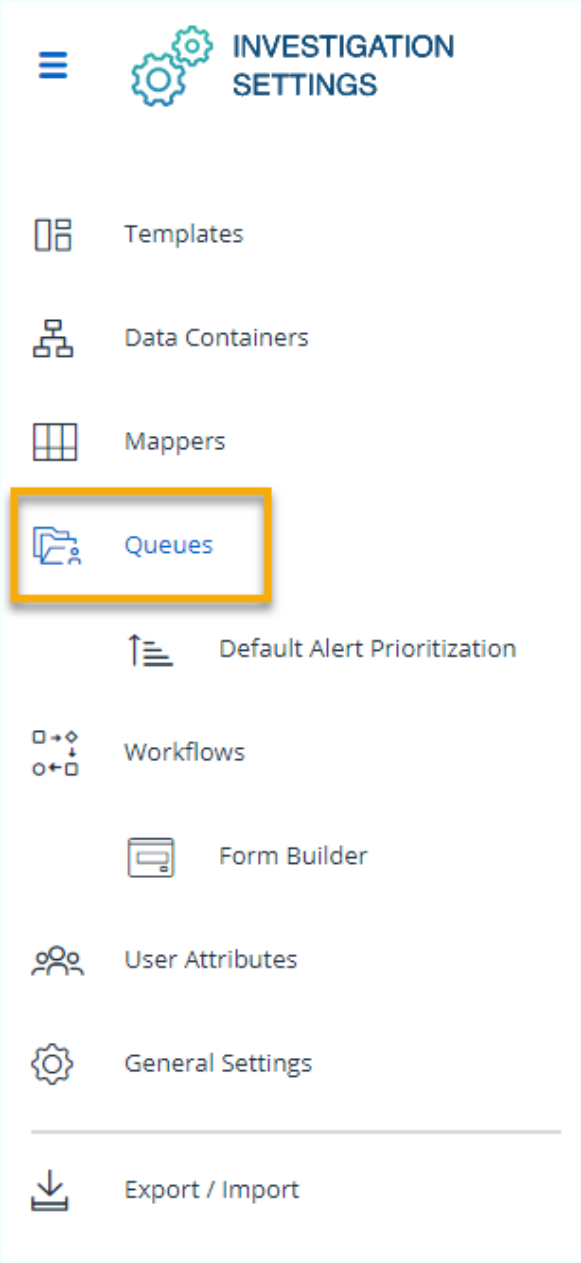
6.1. Creating and Managing Queues

Queues are defined, created and manged in Queue Management by a Business Admin user or senior team analyst leader with experience in queues management and appropriate data permissions.

Once created a new queue is added to the existing Queue Management list.

To create a new queue:

1. Click the Queues icon link from the Investigation Settings side panel as shown below.



The **Queue Management** list is displayed as shown below and includes:

- Queue segregation toggle switch
- Number of alerts in each queue
- All queues by name - including default and created
- Team(s) assigned to handle the queue
- Distribution Criteria
- Workflow
- Data Permission Value
- Queue segregation toggle switch

- View Distribution Centers
- Add Queue Create Button

An example of a Queue Management list is shown below.

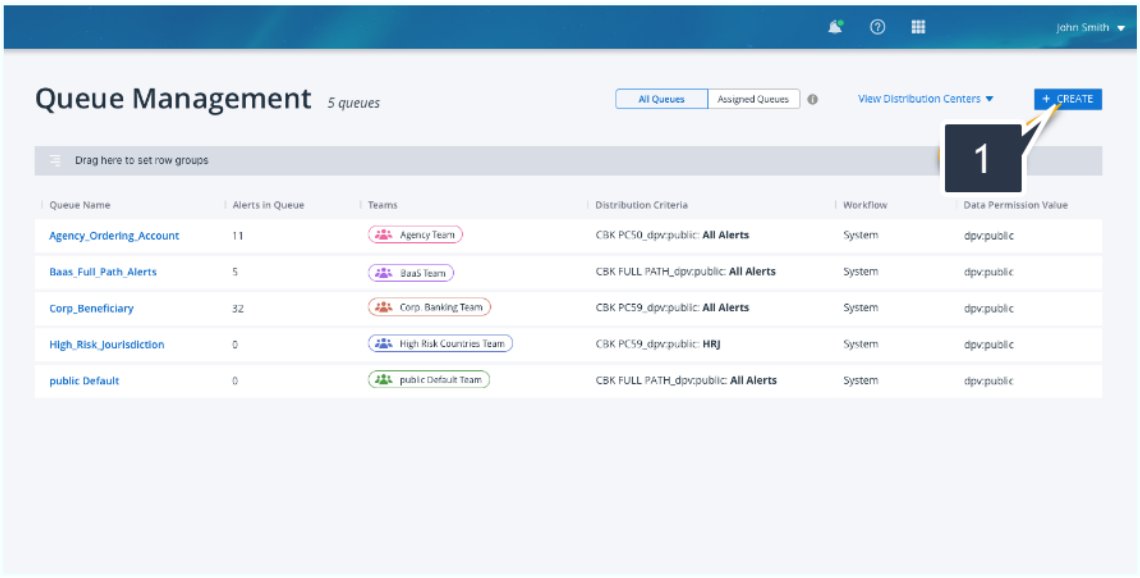


Figure 39: *Queue Management List Table Example*

To create a new queue:

1. Click the **+ Create** button (1) above.

The **Create Queue** form is displayed as shown below. We will initially configure the basic queue parameters including:

- Queue name
- Data permission value
- Associated workflow
- Associated Teams

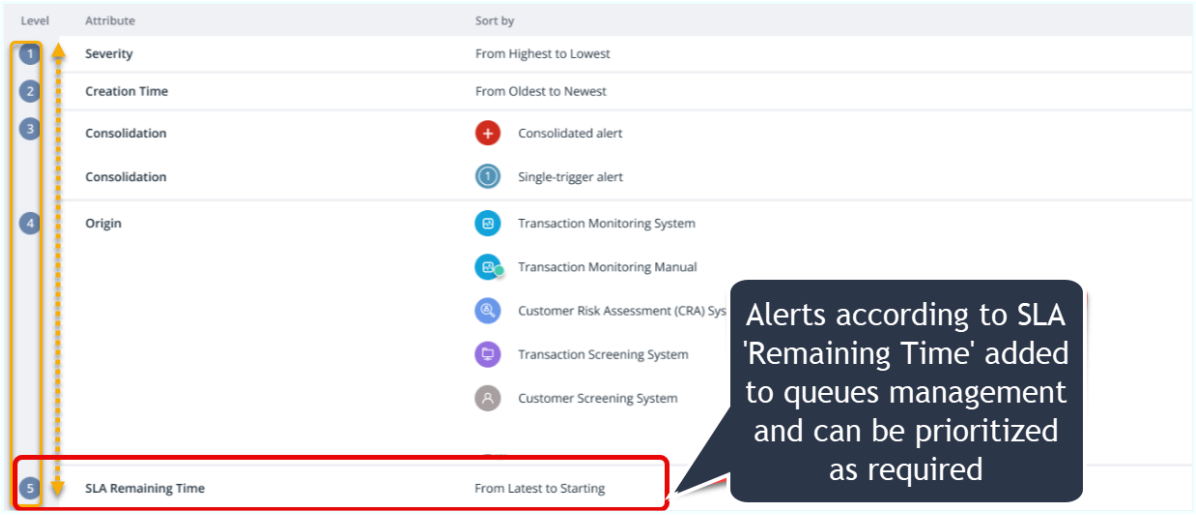


Figure 40: *Example: Creating a New Queue Configuration*

2. Provide a descriptive name for the queue (1)(max 50 characters).
3. *Select a **Data Permission Value** from the Drop-down list if no other options are available select the default value (2).*
4. *Select the workflow from the available list of workflows (3).*
5. From the Teams dropdown menueither*:*
   a. Select a Team or Teams that the new queue will be assigned to *or,*
   b. Type the name of a new Team to add to the list of available teams (max 50 characters) and click **Apply**.
   c. Click **Save**.
6. Verify the new queue with associated attributes is added to the **Queue Management** list.
7. If required, select either the *All Queues / Assigned Queues* toggle switch (as shown below), to select if the listed team users can view *all queues*, or only *assigned queues*.

6.1.1. Queue Segregation

Queue segregation enables the business admin user to configure whether analyst teams can view all queues or just assigned queues.

Configuration of either option enabled by switching the All Queues / Assigned Queues toggle switch ,as shown below.

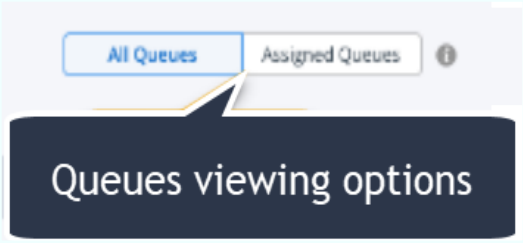


Figure 41: *Queue Segregation Toggle Switch*

6.1.2. Additional information on Queue Segregation

- By default, queue segregation is set to disabled (all Queues in the dpv are viewable)
- When enabled, queue segregation also impacts on the alerts viewable by users such as in Alert Views, BI Dashboard etc.

6.2. Setting Distribution Criteria and Queue Order

Now that we have set the basic attributes of our new queue, to maximize its usability we can configure the distribution criteria that determine:

a. What portion (segment) of available alerts it will contain (1) *and,*

b. What prioritizes the order of alert selection, within the queue (2),

---

Note: When setting SLA queues, users have the option to choose the alerts order in ascending or descending order based on SLA Remaining Time

---

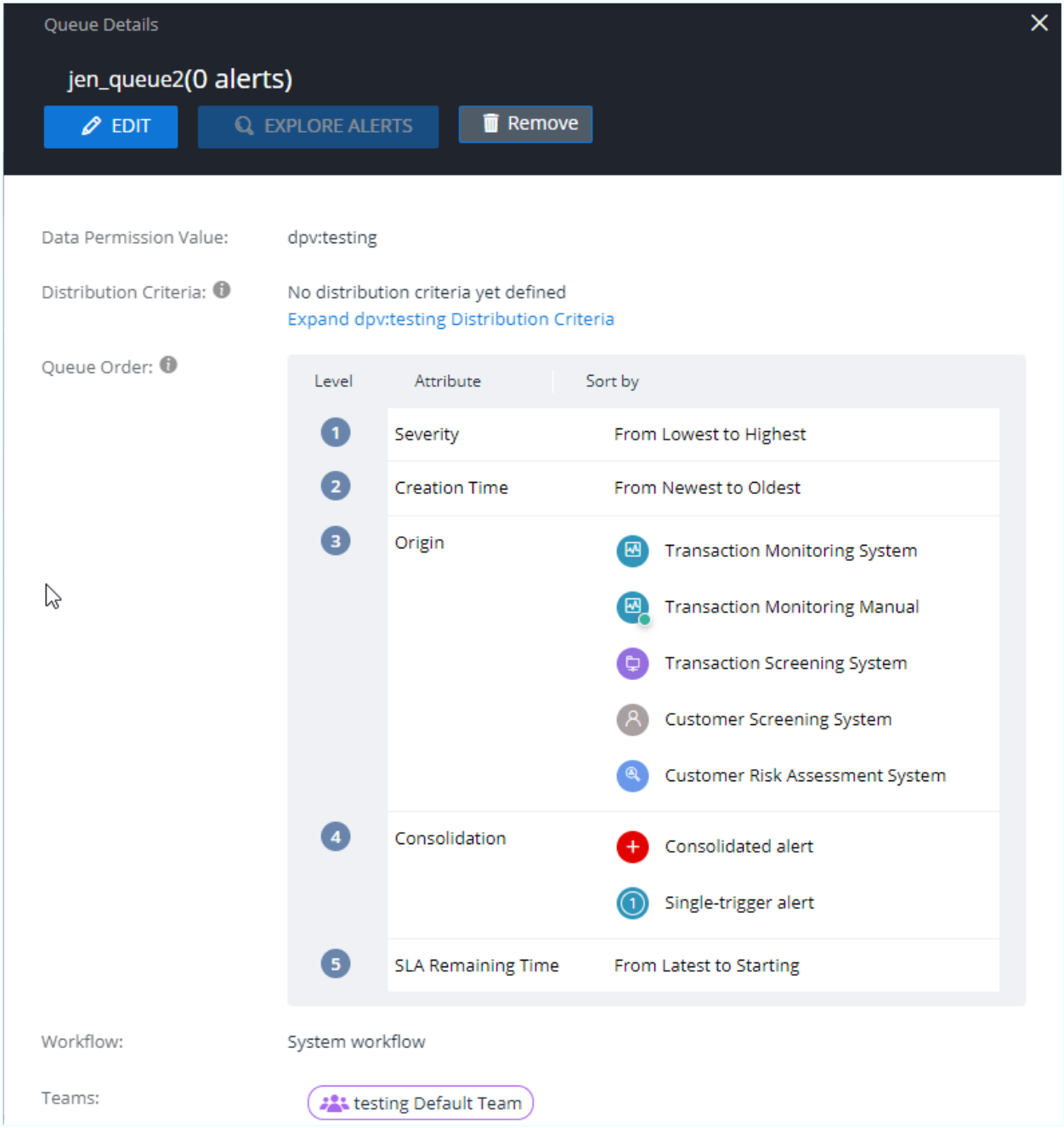


Figure 42: *Example Queue, Distribution Criteria and Alert Order of Selection Setting*

The next step is to select the Distribution Type required. There are currently two types:

- All alerts
- Segment

Selecting **All Alerts**, allows you to create a queue containing all the alerts contained in the analysis.

Selecting **Segment**, allows you to create a queue containing a segment of alerts contained in the analysis, defined by a condition or conditions.

All Alerts Option:

To create a queue containing all alerts from an evaluation analysis, continue as follows:

1. Select the Medium Severity queue from the Queue Management list.

Figure 43: *Queue Header*

2. Click the Edit button. from the Queue header shown above.
3. Click Expand Distribution Criteria link (1) to display the Select Analysis and Select Distribution Type drop down menus.

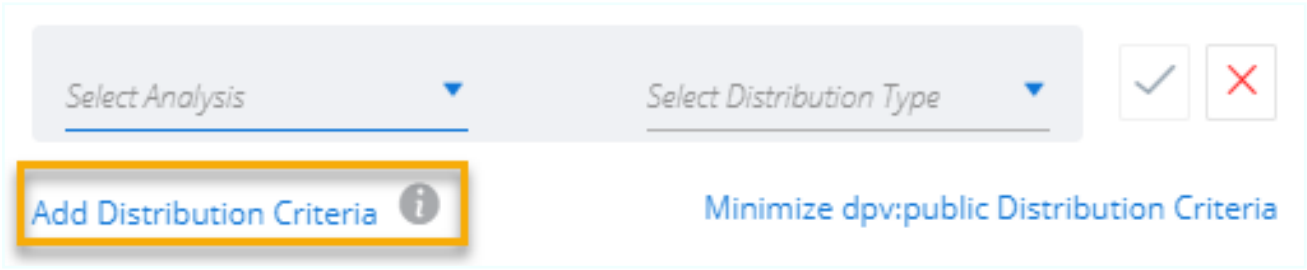
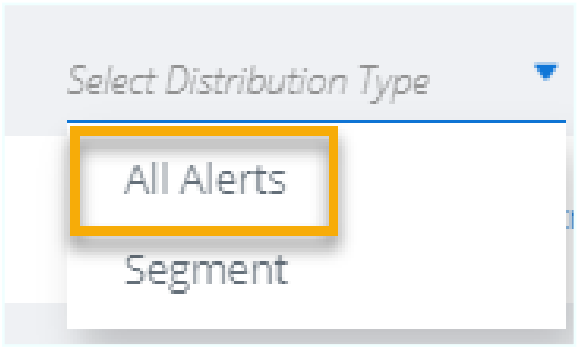


Figure 44: *Select Analysis and Select Distribution Type Links*

4. From the Select Analysis (Evaluation) drop down menu select the required Analysis evaluation
5. From the Select Distribution Type select the **All Alerts** option.



6. Click **Save**.

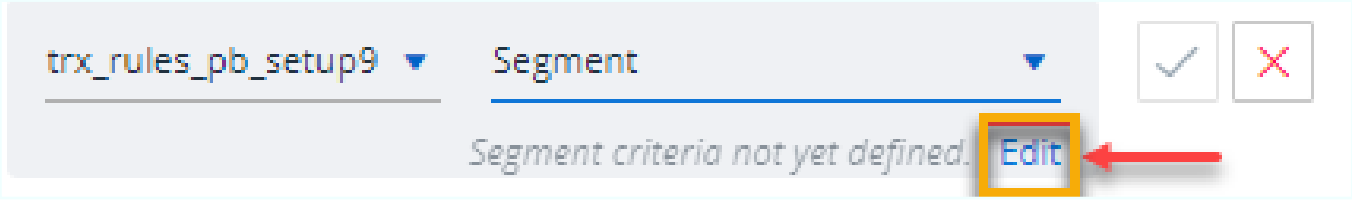
Segment Option

When Creating a segment queue, bear in mind the following:

- When conditions are applied, all incoming new alerts are checked for condition(s) matching. If an alert does not match any condition it is added to the default queue list.
- Configuring conditions requires a basic understanding of the 'Groovy' programming language.

To create a queue containing a segment of analysis alerts, continue as follows:

1. Click the **Edit** button (shown below) to begin to define the segment criteria.



The Edit segment criteria panel is displayed as shown in the following figure.

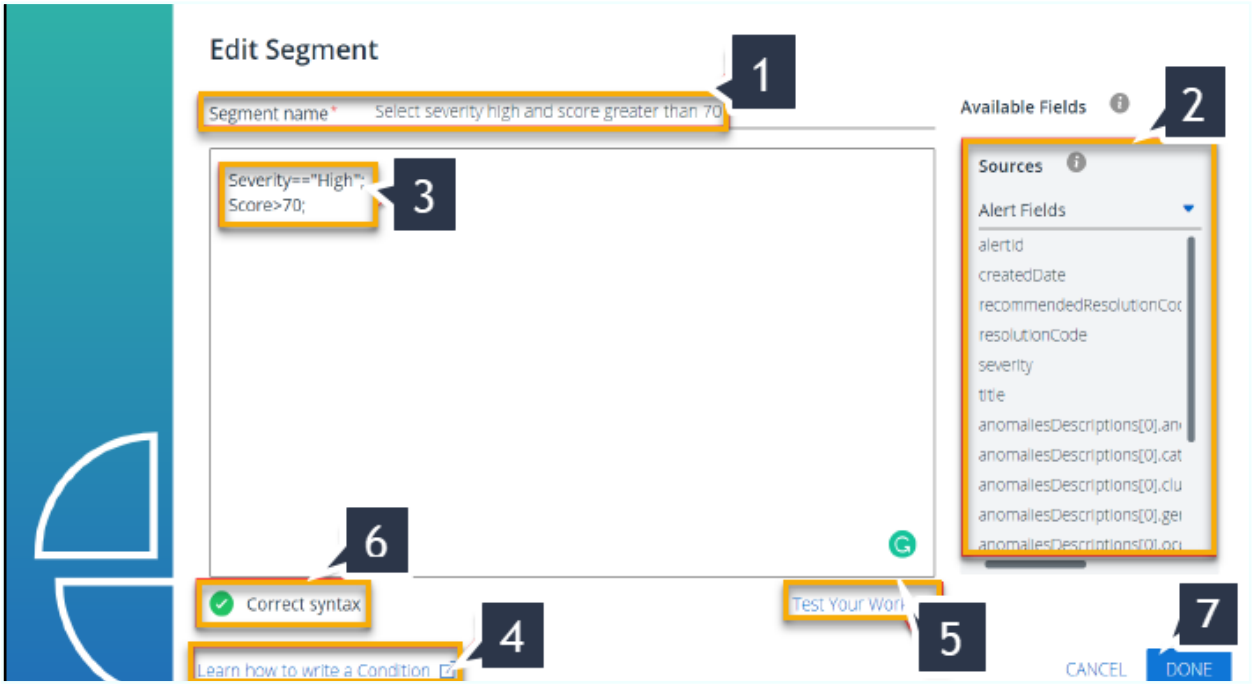


Figure 45: *Example Criteria Condition Code and verification*

To edit the segment criteria:

1. Enter a descriptive name for the segment (1).
2. View from **Sources**, the elements to apply conditional values to(2).
3. Build statement conditions according to the designed selection strategy(3).

For example, set the level of severity and /or the score greater than value as a condition, as shown in the following example:

```
severity == "High";
score > 50;
```

and displayed in the **Edit** segment figure above.

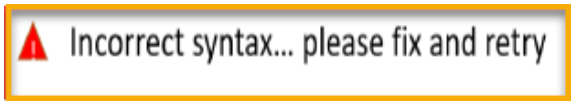
c. If required, click the **Learn how to write a condition** link for more information on creating conditions (4).

d. Test the syntax by clicking the **Test your Work** link(5).

- Click Check Syntax.

If the syntax is correct, this is indicated by a green tick as shown in (6).

If there are syntax errors in **Edit Segment**, this is indicated as shown below.



e. Fix syntax error(s) and retry.

f. When complete, click **Done**(7).

To help you assess if the condition(s) you have set are effective and show how many alerts will move from the default queue of the same DPV to the new queue you are about to create, you can download a **Distribution Criteria Evaluation** in the form of a report.

g. If required to download a **Distribution Criteria Report**, click the **Test Your Work** link then the **Evaluate Distribution Criteria** link as indicated inthe following figure.

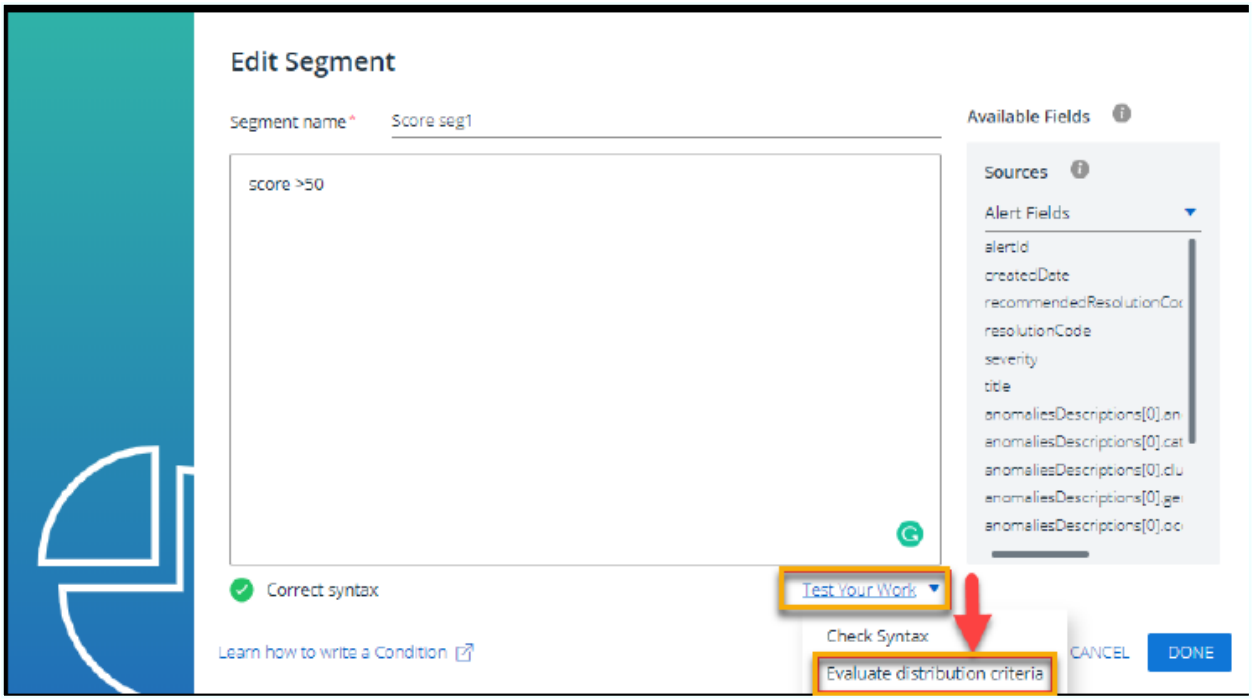


Figure 46: *Edit Segment Condition Code Evaluation*

4. Return to the Queues Details (Edit Mode):
    a. Confirm the Segment edit by clicking the green ok tick next to the Distribution type.
    b. The newly created segment name is displayed.
    c. Click **Save**.
    d. Verify the new Segment queue is now added to the **Queue Management** list as shown in 6. Figure 47: .

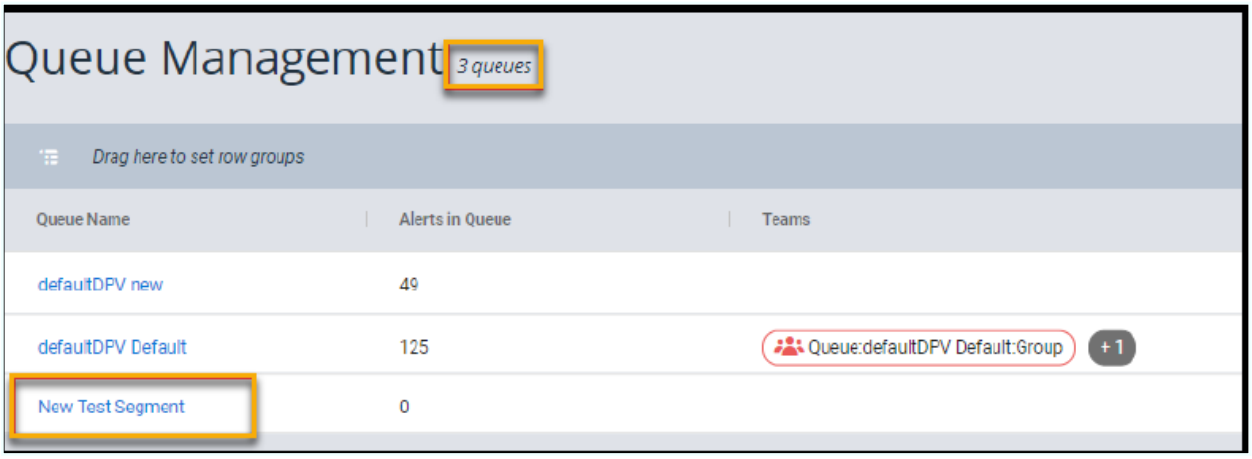


Figure 47: *Updated Queue Management List*

6.3. Segments - Special Case Priority Setting

When more than one segment queue is created where both use the same analysis, the potential exists for a priority conflict. In such a scenario, the order of priority can be changed by editing the selection order.

In the first segment, the configured conditions test for alerts with two severity conditions and a score value over a threshold of 50.

In the second segment, the configured condition tests for alerts whose score is less than 80.

This situation may call for the order of selection priority to be changed.

To change the priority order of segments:

1. Expand the Distribution Criteria by clicking on the **Expand Distribution Criteria** link as shown in the following figure.

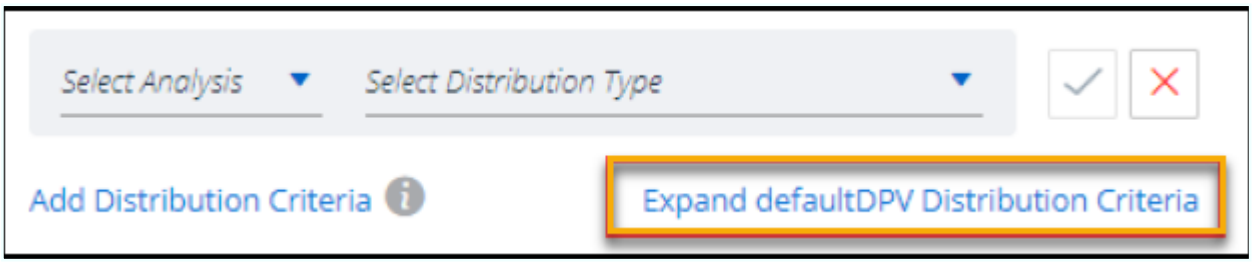
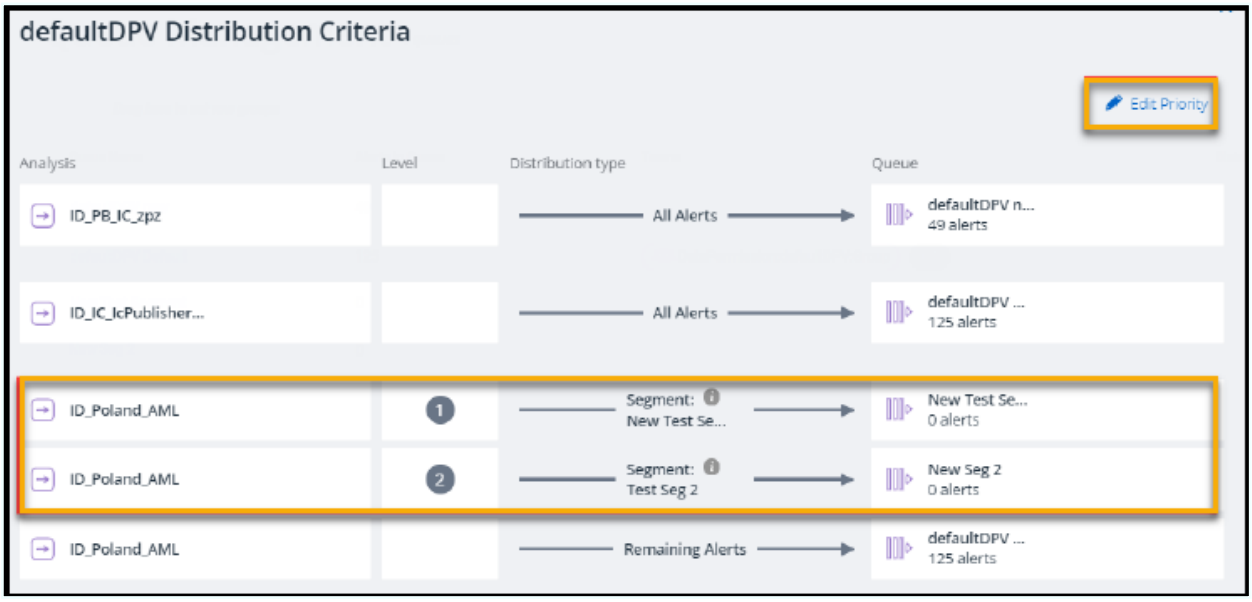
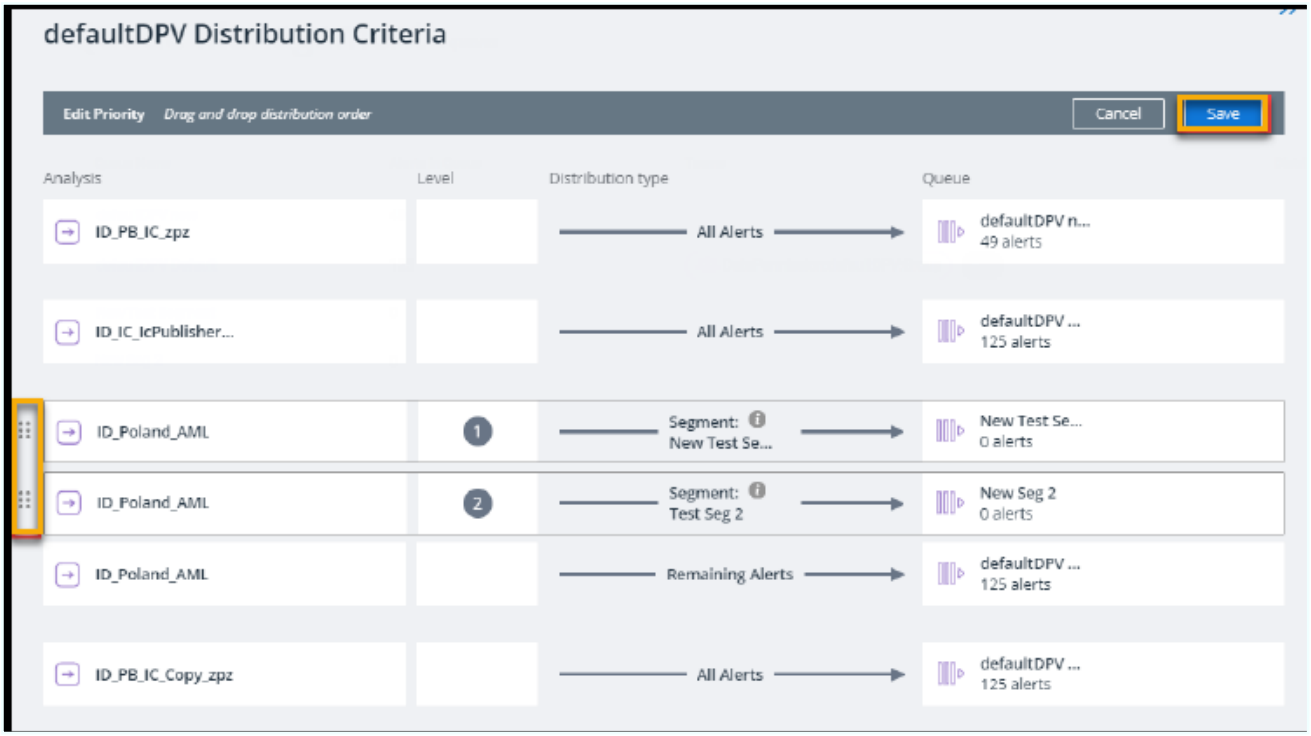


Figure 48: *Link to Expand the Distribution Criteria Panel*

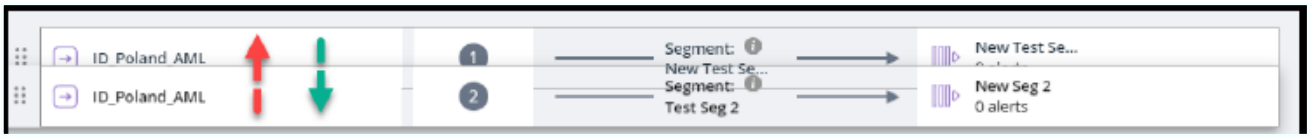
The **Distribution Criteria** panel opens as shown6. below.



2. Click the **Edit Priority**pencil link enables the edit mode with drag 'n drop handles and the **Save** status button as shown6. below.



Changing the order is accomplished simply by a drag-n-drop action as shown below.



3. When complete click **Save**.
4. *Toggle the **Expand Distribution Criteria** link again to collapse the Distribution Criteria panel.*

Note: Changes made to the distribution criteria will only impact new alerts that come in. Existing alerts will always reside in the same place they were, You can move them manually if needed, but changing distribution criteria will not move them.

6.4. Re-ordering Queue Parameters

Reordering of the sections and sub parameters within each queue enables alert order prioritization. This process is covered previously in this chapter in related subjects and also in the following sub-chapter Conflict Priority Resolution. However for convenience, a brief example is provided here as well.

To reorder the priority of sections and parameters you simply drag 'n drop the section or parameter to the new priority position as required as shown inthe following figure.

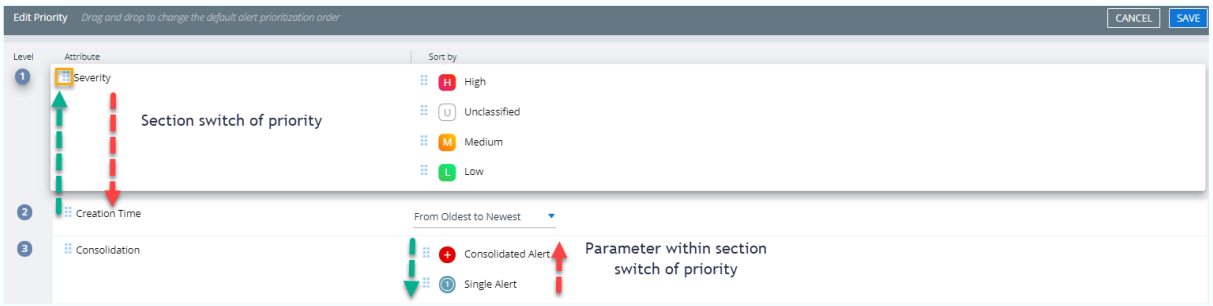


Figure 49: *Example of Changing the Priority of Queue Elements*

6.5. Queues Management - Details Panel

The **Queues Management Details Panel** provides:

- A simplified summary report of queue statistics
- Links to edit, add and explore alert queues

To Open the Queues details Panel:

1. From the **Queues Management** list, click any of queue names displayed.
2. The Queue Details panel for the selected queue is displayed as shown in the following figure.

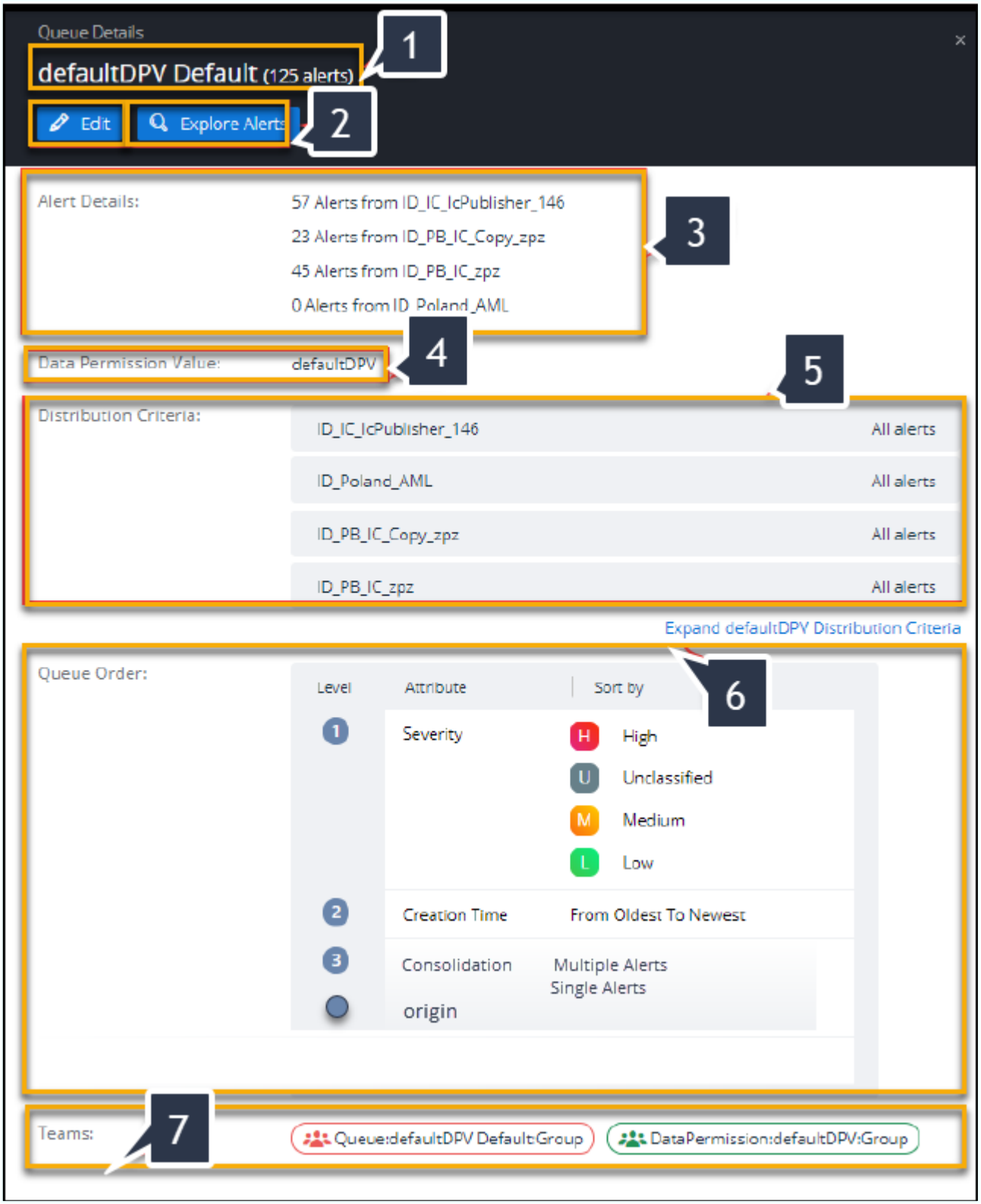


Figure 50: *Example Queues Details Panel*

The following table provides a description of each of the panel's section details.

Table 1: *Queue Details = Description per Section*

Ref Number	Description
#1	**Queue Name**+ total number of associated alerts
#2	**Edit / Explore Alerts**- open queue for editing and exploring alert views links
#3	**Alert details** - including number of alerts per analysis
#4	**Data Permission Value** listed by name
#5	**Distribution Criteria**- name and type
#6	**Queue Order** - Attributes and sub attributes selection order
#7	**Teams** - assigned teams to queues

3. Referring to the **Queue Order** section (5) you can, reorder (drag and drop) the attributes priority displayed so that the next alert available for investigation will be selected by the system accordingly.
4. From the Teams dropdown menu either:

6.6. Auto-assignment Days

This parameter for deployments where this feature is active determines the relative time horizon in days (0- 365) for the queue that the system considers when calculating an analysts availability for the auto- assignment process. An example configuration time period is shown below.

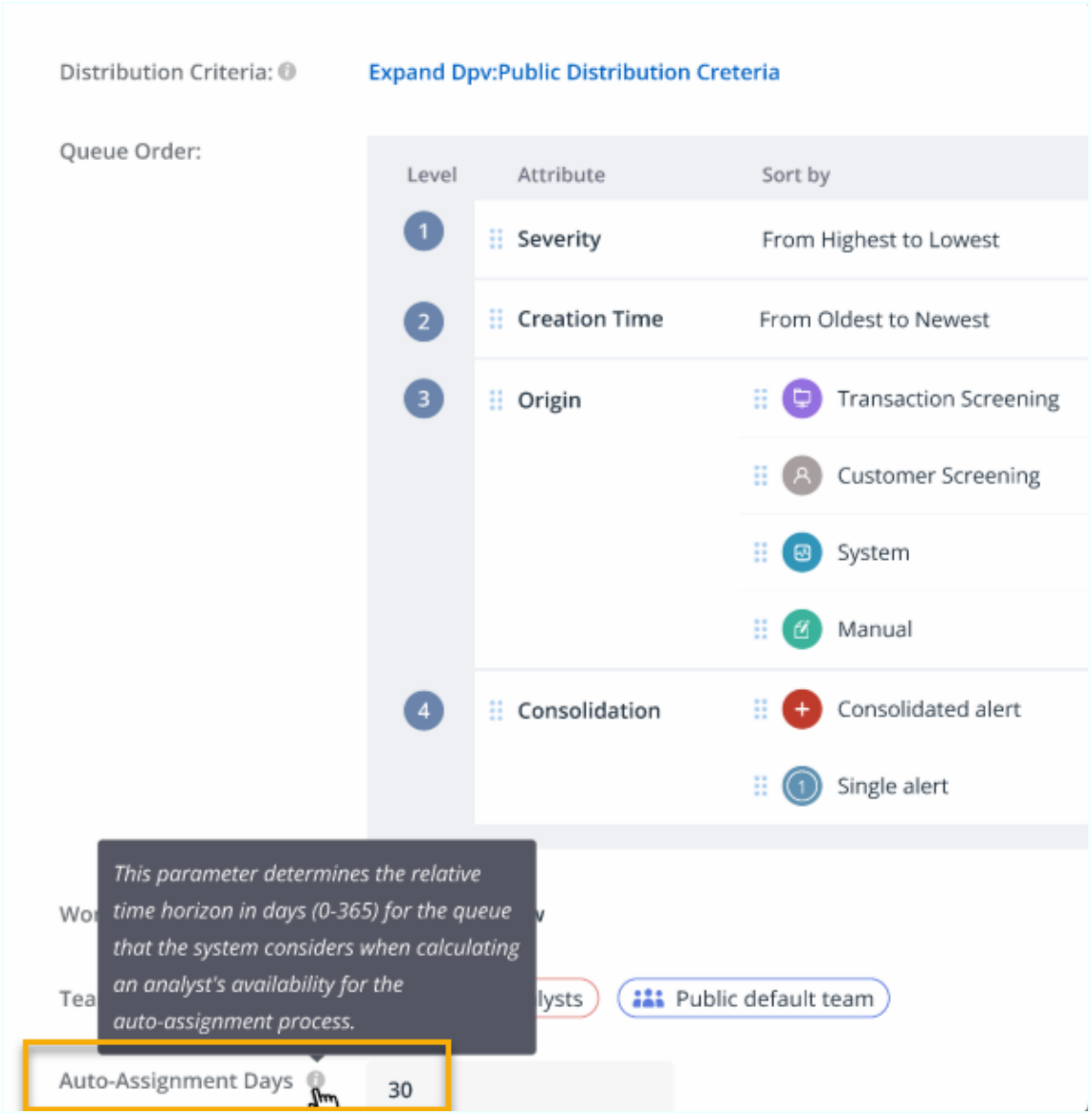


Figure 51: *Example Auto -assigment Configuration for Specific Queue*

6.7. Conflict Priority Resolution

6.7.1. Overview

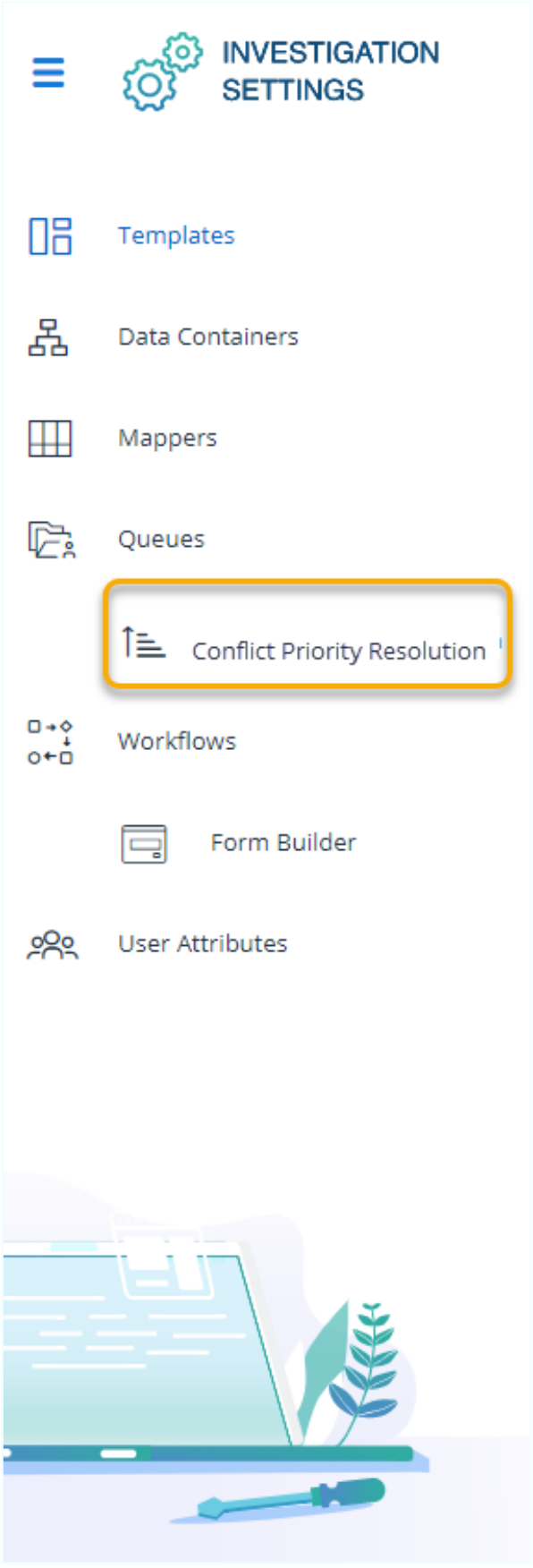
In the Investigation Center, unassigned alerts are organized into queues or lists to facilitate an efficient method of alert delegation to analysts. In general, this method of work delegation works well, and allows analysts who require the next unassigned alert to 'get' the next alert from the top of the queue. Occasionally though, a conflict situation may arise where analyst users are assigned alerts from more than one queue. To mitigate the chances of this occurrence, the following reordering processes are made available in the Conflict Priority Resolution screen:

- Reordering of the prioritization attributes
- Resorting of sub attributes within the prioritization attributes

This task is carried out by users with appropriate permissions (e.g. **Business Admin** users).

To access the set default order of alert attributes:

1. From the Investigation Settings side panel menu click the Conflict Priority Resolution link as highlighted in the following figure.


INVESTIGATION SETTINGS
Templates
Data Containers
Mappers
Queues
Conflict Priority Resolution
Workflows
Form Builder
User Attributes

The Default Alert Conflict Priority Resolution screen is displayed as shown in the following figure.

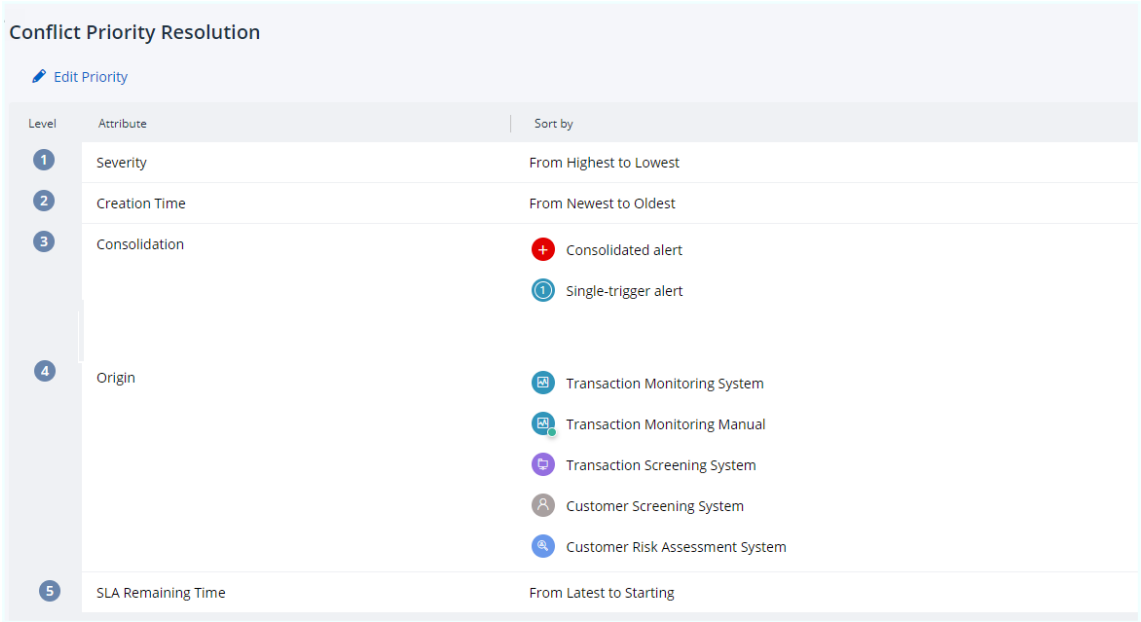


Figure 52: *Conflict Priority Resolution - Showing the Default Priority Order*

6.7.2. Alert Selection Process - How it works

This section explains how the selection process works when the user selects to 'get' the next alert from the queue.

Selection is determined in a cascading manner so that when a selection conflict occurs (i.e. more than one alert meets the selection requirements), the next level down is used in the select decision process and so on.

Based on the 'out of the box' settings the following would be the selection process used:

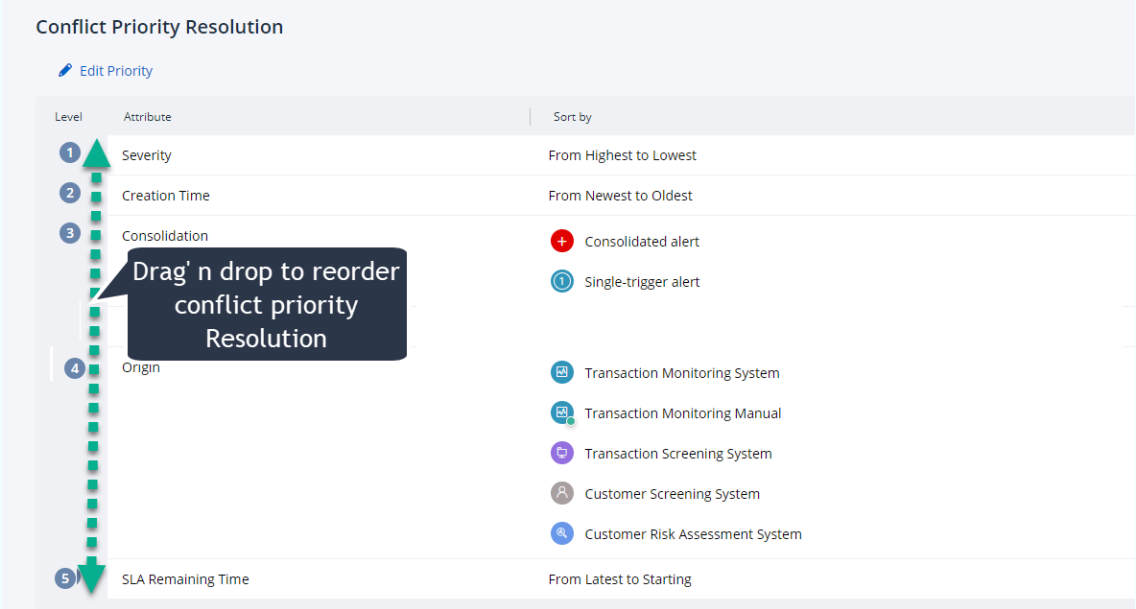
1. Alert conflict Priority Resolution selection is based initially on **Severity** from highest to lowest. Should a select conflict exist for each level then the selection process moves to step 2.
2. Alert priority is based on **Creation Time**, (most recent time to latest time). Should a conflict exist in Creation time selection , as described in the previous step, the selection process moves to step 3.
3. Alert priority is based on alert **Consolidation**.
4. Origin - prioritize according to alert origin.
5. SLA Remaining Time - further explanation:

a. **Latest**: Alerts that have the least remaining time until the end of the set SLA.

b. **Starting**: Alerts with the most remaining time, indicating these have been recently started.

To re-order the attribute levels:

1. Click the **Edit Priority** pencil icon, as highlighted above.
2. Position the cursor over the matrix icon of the level to be moved then 'drag and drop' the item to be moved or sorted to the new position as shown below.



3. Sort menu items first sub attributes and then main attributes by the drag and drop method previously described, or tick the option to be displayed first in the list.
4. When the attributes have been reordered, click **Save**.
5. As a best practice, re-enter the **Conflict Priority Resolution** panel and confirm settings.

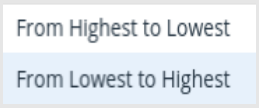
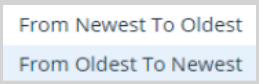
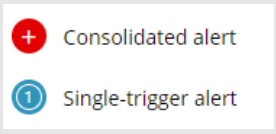
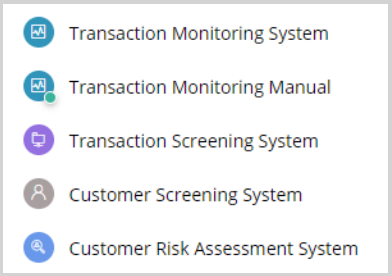
Note: When creating a new queue in **Queues Management**, the queue prioritization will reflect the current **Conflict Priority Resolution** setting.

Note: Attributes and sub attributes can be re prioritized at any time, and changes made are implemented when settings are saved.

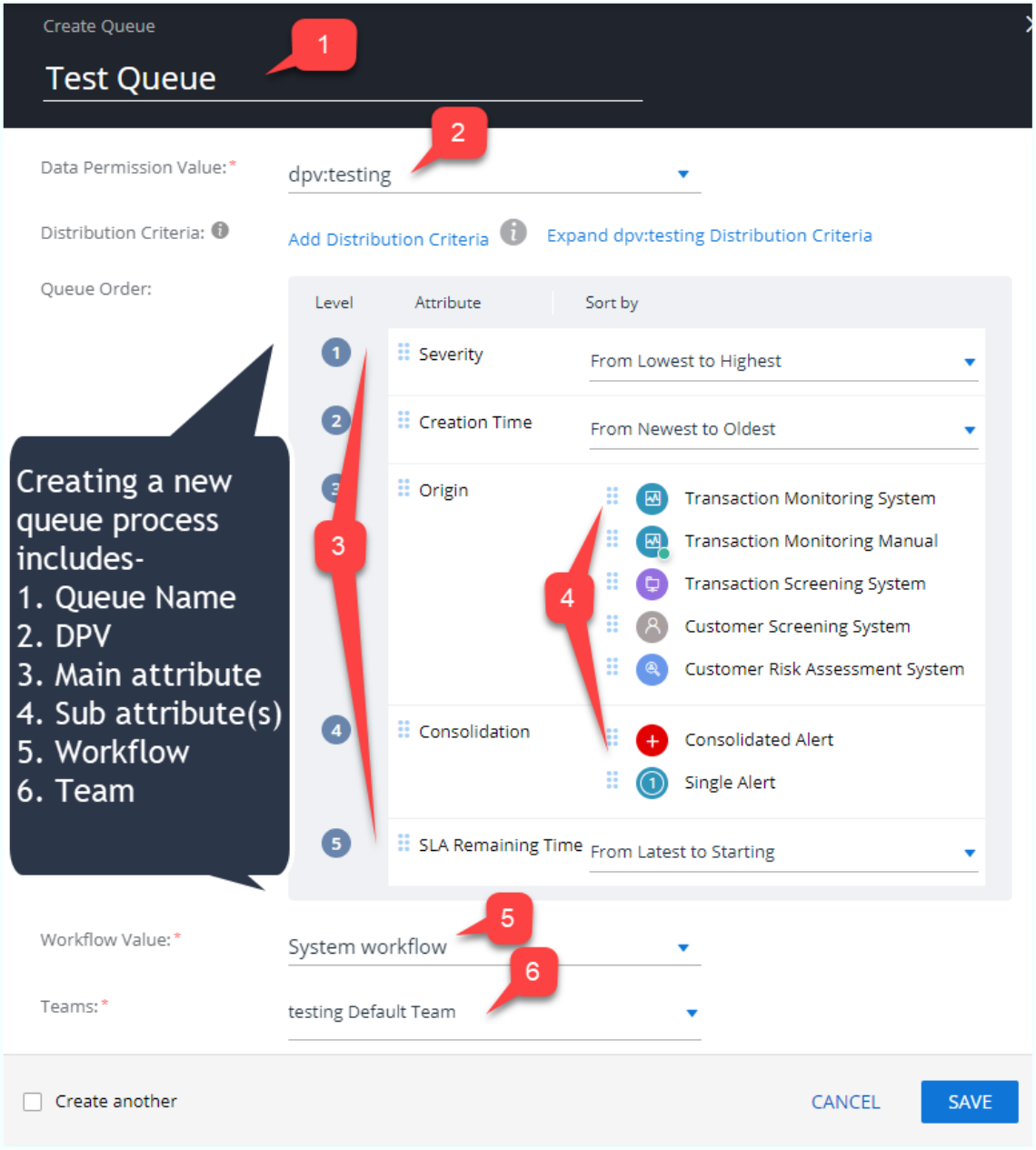
6.7.3. Attributes Available for Conflict Priority Resolution

Attribute and sub attribute menu items available for ordering and sorting are listed in the table6.7. below.

Table 2: *Queue Attributes and Sub Attribute Details*

Attribute	Sub Attributes - Options	Details
Severity	• Highest to Lowest • From Lowest to Highest	
Creation Time	• Newest to Oldest • Oldest to Newest	
Consolidation	• Consolidated alert • Single trigger alert	
Origin	• All • Trx Monitoring - System • Trx Monitoring - Manual • Transaction Screening • Customer Screening • Customer Risk Assessment System	
SLA Remaining Time	• From Latest to Starting • From Starting to Latest	Default: From Latest to Starting

Also note in queues management, the user can decide, say when creating a new queue, what queue order shall be set by the main and sub priority attributes.



6.8. Alert Auto - Assignment - Overview

The prime objective of alert auto - assignment is to ensure maximum alert resolution workflow efficiency, by automating the alert distribution process based on severity /match /risk scores. This enhanced system significantly:

- Improves efficiency
- Reduces delays
- Reduces manual intervention in the distribution process, which minimizes errors
- Ensures timely investigations of alerts

Now, depending on the analyst roster in place, analyst team members only receive alerts ordered into queues by severity and other criteria and with a distribution process that is setup to work dynamically in accordance with each individual deployment's available manpower resources.

A step by step overview of the flow is as follows:

1. Detected alerts are first distributed to the IC module.
2. In the IC module, alerts are segmented into queues by severity /match /risk scores
3. A dynamic duty roster is created depending on availability criteria such as analyst productivity, days off, and seasonal holidays depending on location. Specifically, availability criteria parameters include:
    a. Work capacity - mandatory
    b. National calendar - optional
    c. Time Zone - optional
    d. Non working days - optional

    Note: The contents of this roster is added into the alert resources schedule per deployment.

4. Depending on the calculations taken from the previous steps, each alert is designated a weight value, which aids in accurate distribution of alerts to the appropriate analyst

Note: This capability detailed above is not activated by default and if required, should be enabled by your Business Admin. When deciding whether or not activation is beneficial or not for your deployment, the user is advised to factor in such variables as deployment size and manpower resource availability against the extra overhead of maintaining the auto alert assignment feature. For more advice, reach out to your customer support representative.

The following flow diagram shows the alert auto distribution process high level:

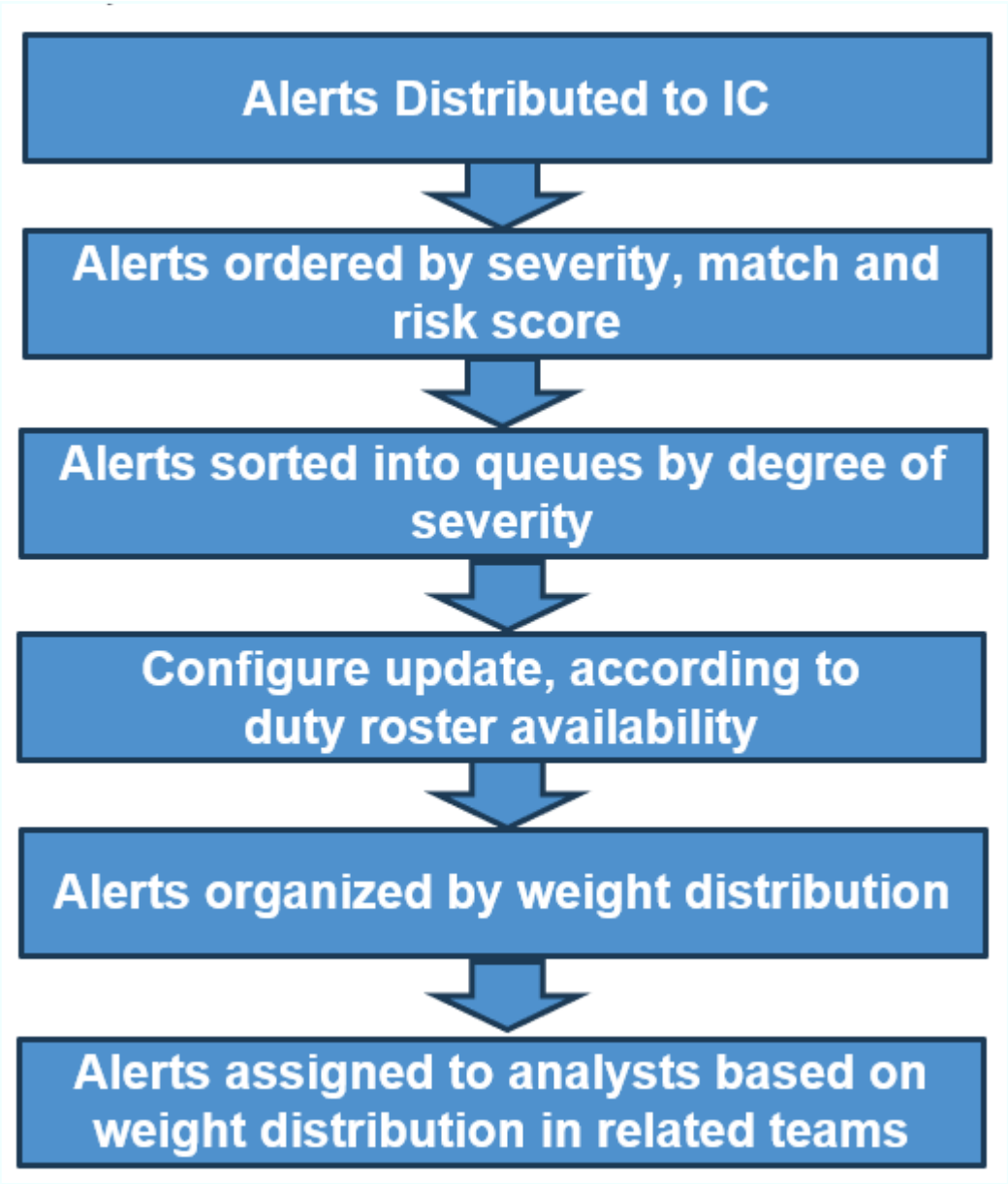


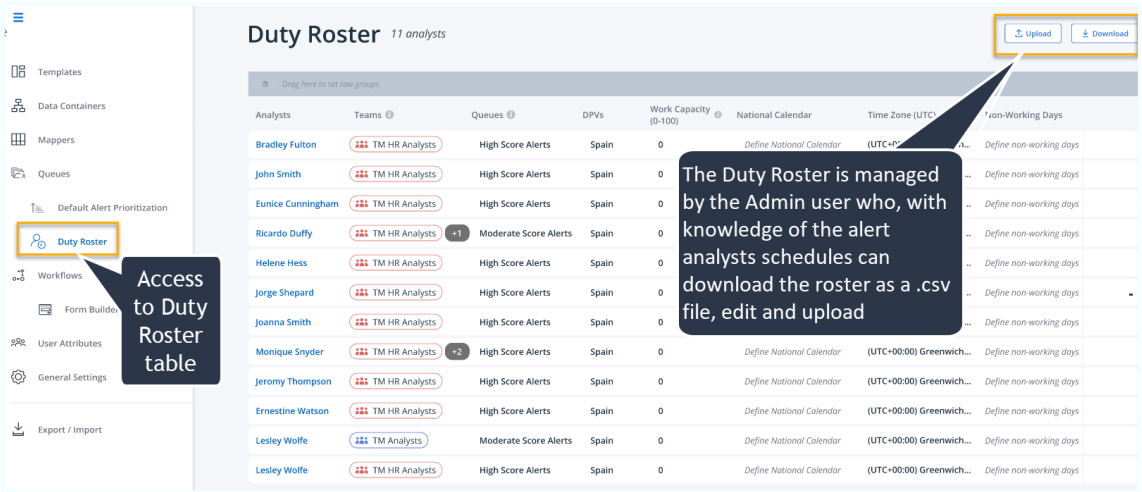
Figure 53: *High Level Flow-Alert Auto-Assignment by Severity Score, other Criteria and Analyst Availability*

6.9. Duty Roster

The Duty Roster sub section of the Queues Management section of Investigation Settings helps Business Admin users to improve organizational efficiency when managing available analyst resources in ThetaRay Alert resolution deployments.

Important:: It is important to note that the auto assignment capability can only be enabled by adding the relevant service task during the workflow design, and configuration of the Duty Roster section in particular, the analyst Work Capacity section.

Access to and example of, a Duty Roster is shown below.



As the example table shows, analyst resources for an organization are listed and detailed including:

- Analyst by full name
- Team membership
- Additional team(s) the analyst is a member of (e.g.,+2)
- Related Queue or queues
- DPVs
- Work Capacity (0-100)
- National affiliated calendar
- Time Zone (UTC) Non - working Days

Additional Notes on Work Capacity

This purpose of configuring the Work Capacity column is to enable the setting the analyst's work capacity in the most efficient manner, please note the following points:

- Work capacity is indicated by a number between 0 and 100
- A value of 0 indicates the analyst is unavailable for alert assignment
- If all analysts in the queue have a capacity of 0, alerts are distributed to the queue as unassigned

- The maximum capacity for n analyst in a single queue is 100
- If an analyst belongs to multiple queues, their total capacity accross all queues must not exceed 200

To summarize the purpose of this column is to aid the Business Admin user fine tune the duty roster to meet occurring non standard resource demands. With an in depth knowledge of available analysts, the user can indicate instances where some analysts are not fully employed and therefore have spare capacity that can be leveraged to meet varying excess resource demands.

6.9.1. Editing Duty Roster

Editing the duty roster can in some instances be a time consuming task, especially for large alert resolution organizations. To ease the task, the most time efficient method is to download the duty roster data table as a .csv file, edit the content and perform re- upload.

6.9.2. Supervisor's Participation in Duty Roster Management.

Additionally, analyst supervisors can also help manage the resources of analysts and queues under their supervision by being delegated limited managerial access to specific analyst duty roster entries.
This ability aids alert resolution efficiency by removing some of dependency on Business Admin in having to handle all analyst resources in a specific organization. For more information, refer to the section, Supervisors Workflow located in the current Investigation Center User Guide.

7. Workflow Management

7.0.1. Introduction

This section provides an overview to default and customizable workflows.

The Investigation Center is deployed with a default workflow as shown in the following figure.

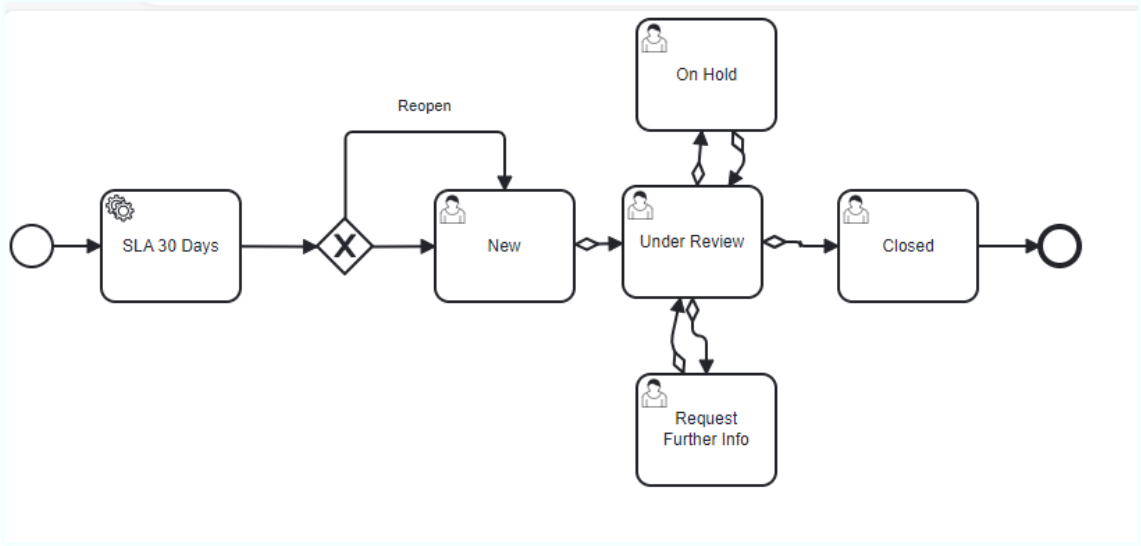


Figure 54: *The Current Default Workflow*

As with many of the elements of the investigation Center, if the default option does not completely suit your alert investigation needs, you can either build a new one from scratch, or modify the existing model (if this exists).

Note: If you require a Custom Workflow then please contact your ThetaRay Customer Support representative.

7.0.2. The Custom workflow

The workflow determines the process path of an alert as it passes through the investigation process from the new state through various state changes to closure with a recommended resolution. Through the workflow process, decisions on the next stage are made either manually or by the system according to a preset program. The workflow can also include a "four eyes" review when a resolution is proposed by a junior analyst and this decision needs to be confirmed by a more senior supervisor.

The system of creation, implementation and management of customizable workflows is designed to offer maximum flexibility with regard to maintaining and

improving the level of effectiveness and ability to support the company's specific work pattern requirements.

The task of creation and management of these workflows should ideally be handled by Business Admin personnel who have the in depth knowledge of their organization and the level of experience on how to best utilize available workforce resources and maximize alert resolution efficiency.

7.0.3. Workflow Creation - Guidelines

- Various stakeholders ranging from developers to managers collaborating to produce a workflow model that meets the company's alert investigation policy needs
- A new workflow model is designed by the appropriate personnel (e.g. Business Admin) which includes the following steps:
    - Producing a model graph which includes:
        - The various hierarchical levels used in the workflow model
        - All symbols that map the process flow from start to end, activity states and SLA values for each stage, and where appropriate recommended resolution codes
        - Manual and automatic system path handovers
    - Verifying the connection graph with all company stakeholders
    - Creating a .bpmn xml file from the verified graph, ready for upload to the Workflow Management platform
    - Automation of Status Change following Get Alert
    - Uploading the .bpmn workflow, States, Resolution code and configured JSON files for these workflow elements
- Running and testing the workflow for any process logic issues that may exist
- Fixing issues, uploading modified list elements and re-testing the workflow for compliance to the original design

The remainder of this section covers the following topics:

- Workflow Implementation process overview
- Workflow model - requirements
    - States and resolution code lists
- How to access, upload new and edit existing workflows
- Associating a queue with a workflow
- Mandatory state change completion notes

7.0.4. Custom Workflow - Implementation Process

In the custom workflow implementation, the following components are required:

- Custom workflow model in .bpmn format
- A list of states that match each possible state the alert can be assume
- A list of recommended resolution codes used by analysts or supervisors when proposing a resolution to the alert
- Selection of autotext template notes to be available to analysts for /all any alert state changes as part of the workflow

7.0.5. Custom Workflows

A workflow model can be designed and created with any compatible third party graphic / xml engine / editor. Before expending the time and effort in changing the Workflow, consider consulting ThetaRay's Customer Success to see if there is a ready made similar file available.

Once completed, the .bpmn file should be saved anywhere ,but for convenience a local computer is recommended where it can be accessed for uploading to the Investigation Center as part of the mandatory workflow required components.

Additionally, and as a best practice, it is also advised that a graphic chart of the workflow from which the xml file is produced is also saved in the new project folder. Although not required in the implementation process, it is a useful asset in the overall model design process when collaborating with other project stakeholders, to make sure their design requirements are also addressed in the custom workflow solution.

In the Workflow management section, some practical guidance and structure ideas are provided to help you understand the principles of workflow model creation.

For more detailed information about creating custom workflows contact Customer Support and request a copy of the Activiti Tool User guide.

7.0.5.1. Workflow Elements - States and Resolution Codes

The created workflow requires , apart from the configured .bpmn file, two additional maintainable workflow elements:

- A list of alert states that are used throughout the workflow to define the current alert state
- A list of recommended resolution codes that can be suggested by the analyst as a possible final resolution to the alert

When creating a new custom workflow, two default sets of states and resolution codes are made available and if these meet workflow design requirements, can

simply be selected at the create and upload stage. Alternatively, if the workflow design requires a new custom design built from the ground up, a new set of workflow elements can be created and used in the workflow implementation. The important point here, is that what ever workflow elements are incorporated in the model layout, are selected from the default list in the upload process.

7.0.5.2. States - Overview

A master list of states is maintained from the states contained in each custom workflow. Maintaining a centralized list not only enables sharing and reusability between different workflows but also facilitates displaying data about alerts from different workflows in the same report or dashboard.

7.0.5.3. Default Workflow - State Requirements

- "New"
- "Under Review"
- "On Hold"
- "Request Further Information"
- "Closed"

7.0.5.4. States - Attributes and Limitations Details

The following table lists and details State attributes and limitations.

State Attributes	Details
ID	The current status of the State Example from the default workflow: "state_new",
Identifier	Used by the system to identify the workflow. This attribute if required, can be moved from one environment to another Example from the default workflow : "ID_state_new",
Display name	For custom states : • Can be updated and changed by admin • Up to 30 chars max • All characters are allowed • Name must be unique Example default workflow :"New"
Type	Whether the state is changed by the system or user: Options: • System • Manual
Active / deleted	Denotes whether the state is in use or not

State Attributes	Details
	Boolean value options: • true • false
Roles	The id value of the role which is associated with the state
Teams	The id value of the team which is associated with the state
Workflows	The id value of the workflow that is associated with the state

An example of default workflow states file in a JSON script is shown below:

```
[
    {
        "id": "state_new",
        "identifier": "ID_state_new",
        "name": "New",
        "type": "SYSTEM",
        "active": true,
        "deleted": false,
        "roles": [],
        "teams": [],
        "workflows": []
    },
    {
        "id": "state_under_review",
        "identifier": "ID_state_under_review",
        "name": "Under Review",
        "type": "CUSTOM",
        "active": true,
        "deleted": false,
        "roles": [],
        "teams": [],
        "workflows": []
    },
    {
        "id": "state_request_further_info",
        "identifier": "ID_state_request_further_info",
        "name": "Request Further Info",
        "type": "CUSTOM",
        "active": true,
        "deleted": false,
        "roles": [],
        "teams": [],
        "workflows": []
    },
    {
```

```
        "id": "state_hold",
        "identifier": "ID_state_hold",
        "name": "On Hold",
        "type": "SYSTEM",
        "active": true,
        "deleted": false,
        "roles": [],
        "teams": [],
        "workflows": []
    },
    {
        "id": "state_closed",
        "identifier": "ID_state_closed",
        "name": "Closed",
        "type": "SYSTEM",
        "active": true,
        "deleted": false,
        "roles": [],
        "teams": [],
        "workflows": []
    }
]
```

7.0.5.4.1. Workflow Resolution Codes

As with custom states, when working with custom sets of resolution codes these are also required to be created a JSON script file.

Following is an example script of default resolution codes.

```
[
    {
        "id": "Flag_customer",
        "name": "Flag customer",
        "classification": "PRODUCTIVE",
        "active": true,
        "deleted": false,
        "roles": [],
        "teams": [],
        "workflows": [],
        "updateTime": null,
        "fileName": null
    },
    {
        "id": "SAR_worthy",
        "name": "SAR worthy",
```

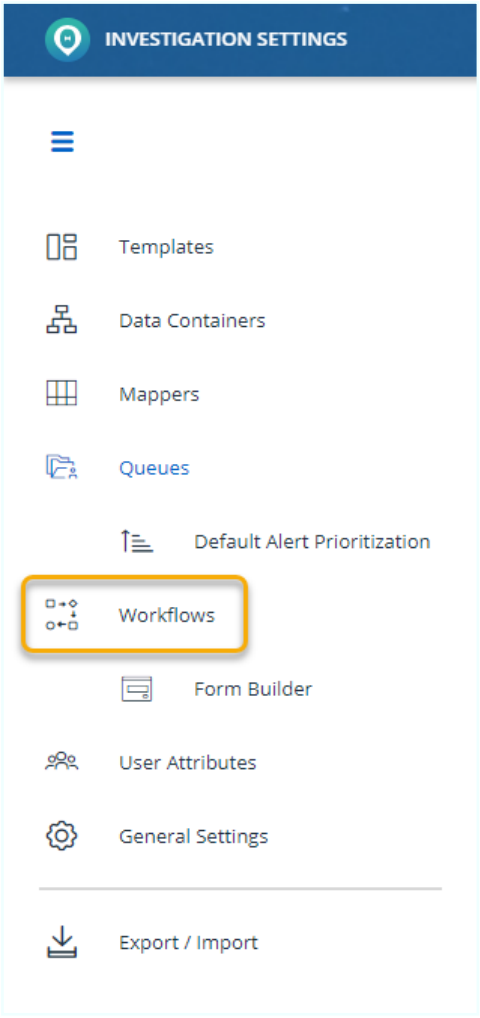
```
        "classification": "PRODUCTIVE",
        "active": true,
        "deleted": false,
        "roles": [],
        "teams": [],
        "workflows": [],
        "updateTime": null,
        "fileName": null
    },
    {
        "id": "Resolved",
        "name": "Resolved",
        "classification": "PRODUCTIVE",
        "active": true,
        "deleted": false,
        "roles": [],
        "teams": [],
        "workflows": [],
        "updateTime": null,
        "fileName": null
    },
    {
        "id": "Non_Issue",
        "name": "Non Issue",
        "classification": "NON_PRODUCTIVE",
        "active": true,
        "deleted": false,
        "roles": [],
        "teams": [],
        "workflows": [],
        "updateTime": null,
        "fileName": null
    }
]
```


7.0.5.5. Working with Workflow Management

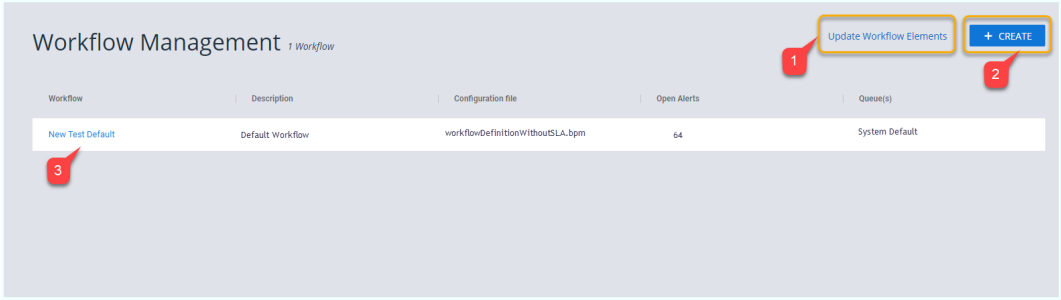
Workflow Management is available to Business Admin users with the appropriate permission.

To access the Workflow Management module:

1. From the Investigation Settings side panel, click the **Workflow Management** tab as highlighted in the figure below.



The Workflow management table is displayed including the supplied default workflow (3) as shown below.



From this dashboard you can carry out the following actions:

- Create a new workflow (2)

- Update existing workflow elements (1)
- View the current list of created workflows (3) including:
  - Workflow name
  - Workflow description
  - Configuration File
  - Number of open alerts in each workflow
  - Alert queues associated with each workflow

If extra support in creating your specific custom workflow is required please contact **ThetaRay Customer Support.**

7.0.5.6. Creating a New Workflow

The basic process of creating and uploading a new workflow involves the following steps:

1. Create or edit your flow using a wokflow creation /edit tool (for example: activiti)
   a. For more information on 'activiti', refer to the current version of the '**activiti**' workflow creation tool user guide, available from ThetaRay Customer Support.
2. Upload the JSON files for States and Resolution Codes

- Select a configured .bpmn or bpmn20.xml workflow file for upload

To create (upload) a new workflow process model:

3. Click the **+ Create** button (2) on the Workflow Management table as shown above.

The Create a new workflow form is displayed as shown below.

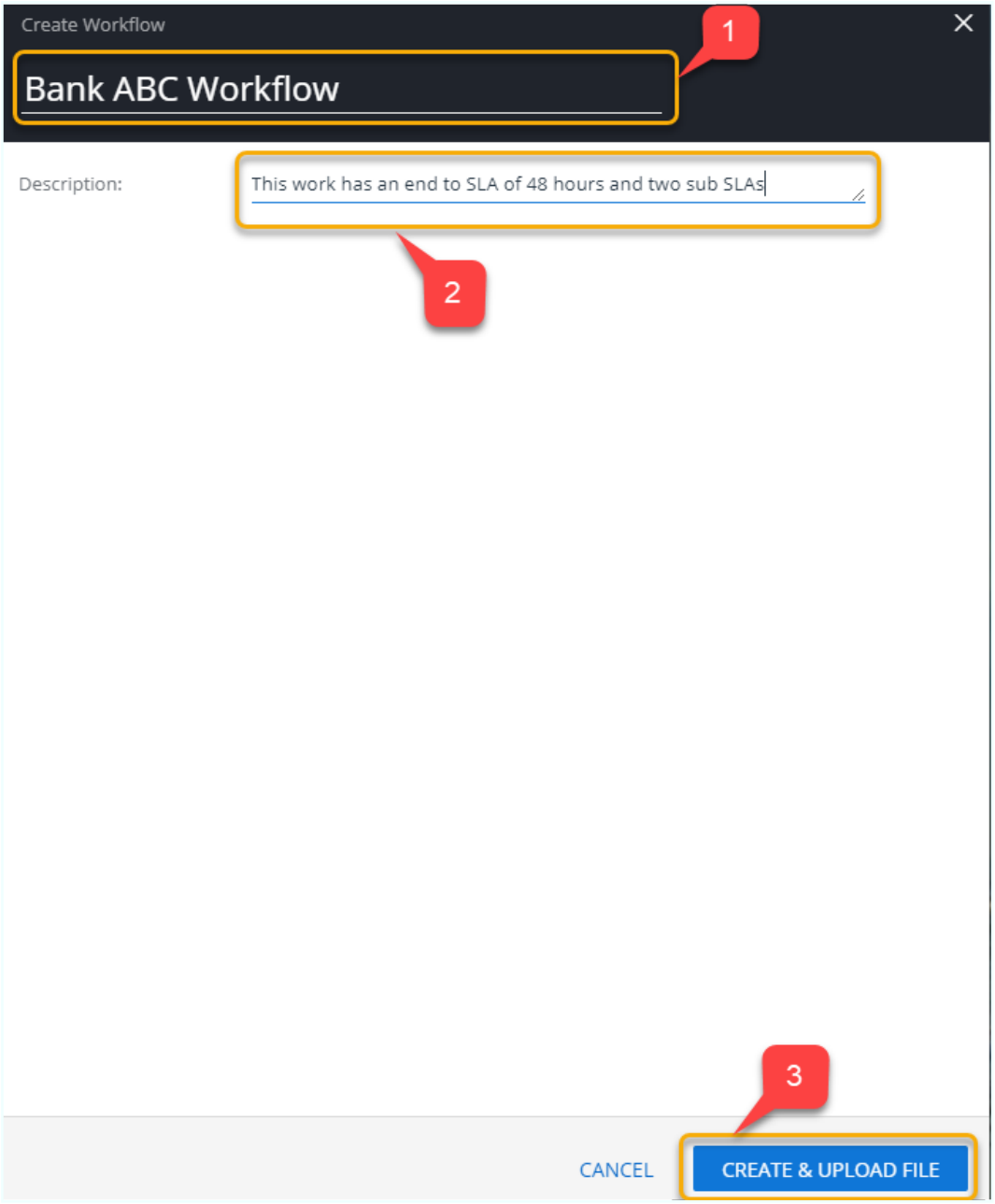


Figure 55: *Create New Workflow Model Form*

4. Provide a name for the workflow (max 50 characters) (1).
5. Add a description of the workflow (max 500 characters) (3).
6. When complete click the **Create & Upload** button (4).

The following **Upload New File** popup is displayed:

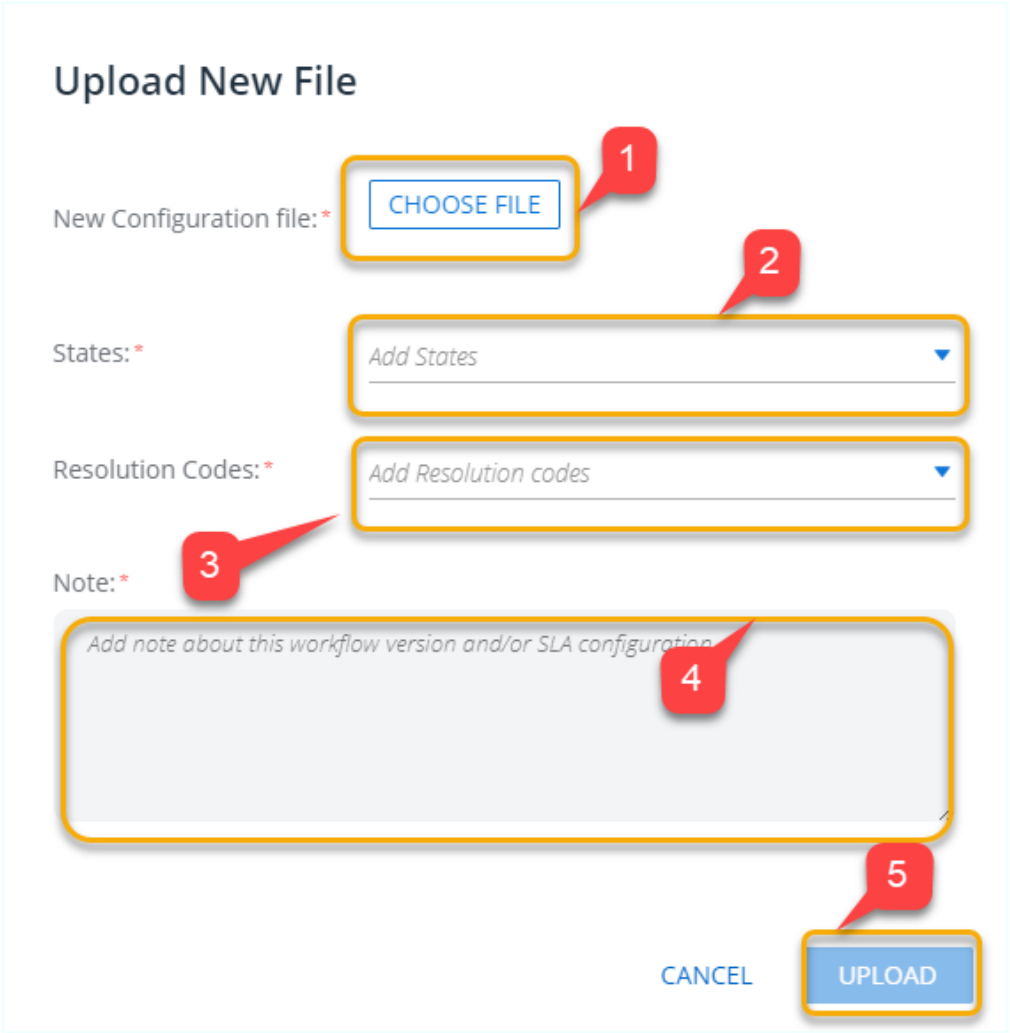
7.0.5.7. Uploading Support Workflow Elements (States and Resolution Codes)

When selecting the Sates and Resolution Codes to support the Workflow XML the user has two options:

1. With Custom Workflows the user is required to create two JSON files:
   a. States JSON.
   b. Resolution Codes JSON

These should be saved in the local computer and then when required for upload, clcik CHOOSE FILE, navigate to and select custom files for upload then click the UPLOAD button.

2. If saving a default workflow, the user should select available States and Resolution codes from the available dropdown lists shown in the following figure (2. and 3)



3. Click the **Choose File** link, navigate to the workflow .xml file and select.
4. Click the **Add States** drop down menu and select the states that are used in the workflow then click the X icon to close the dropdown menu.

An example of the available default states are displayed as shown in Figure 56: below.

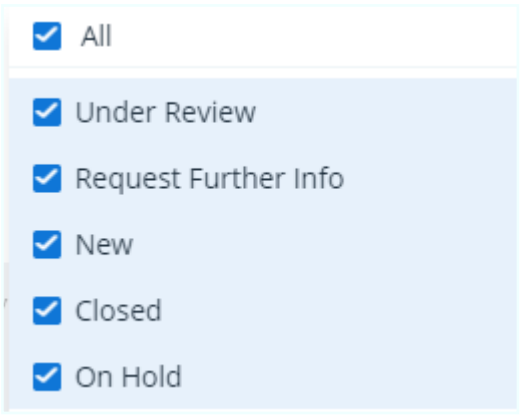


Figure 56: *Example Alert States*

5. Click the **Add Resolution Codes** drop down menu (3) and select codes that are used in the .bpmn file then click the **X** icon to close the dropdown menu.

An example of the available default resolution codes are displayed as shown in Figure 57: below.

Figure 57: *Example Resolution Codes*

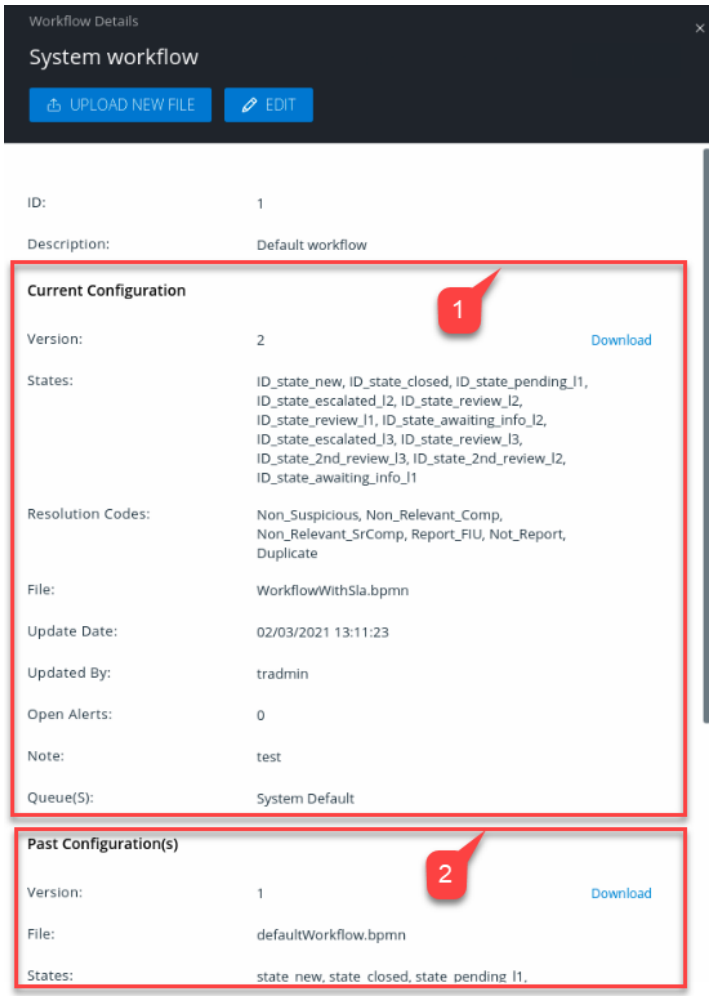
Warning: The upload process does not verify elements in the custom model match those listed in the additional uploaded workflow, it is important, as a best practice, before uploading states and resolution code elements to ensure that no differences exist between both entities.

6. When complete, click the **Upload** button to upload the workflow to the ThetaRay IC module and add it to the list of available custom workflows displayed in the **Workflow Management** screen.
7. It is considered a best practice at this stage to check the workflow is as designed.

7.0.6. Maintaining Workflow Versions (Custom Workflows)

Note: A workflow that is edited and re-uploaded from the Model editing tool being used and with the same name, is stored as the Current Configuration V2 (1) and a previous version is tagged as a **Past Configuration** and listed below and labeled as V1 (2), as shown 7. below.

This method of maintaining previous versions of a workflow enables model rollback, if post update, it is decided that a previous model version is actually a better version than the current version.



7.0.6.1. Editing a Workflow

A comprehensive range of editing functions is available to ensure optimum workflow management is maintained. These include:

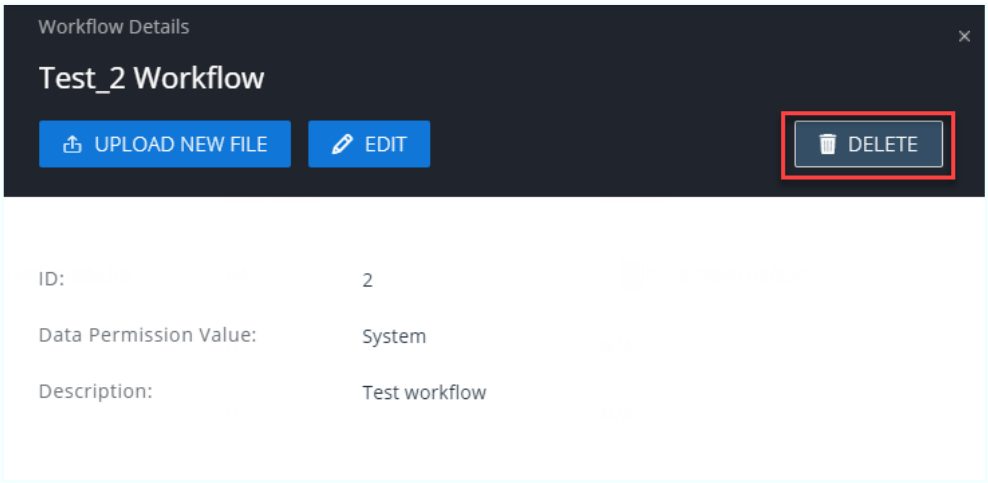
- Deleting unwanted workflows

- Adding and modifying custom workflow elements if the workflow contains workflow elements that are not listed in the default list

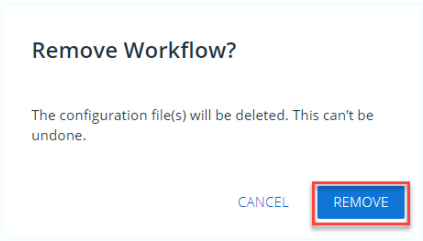
7.0.6.2. Deleting a custom workflow

To delete a custom workflow from the Workflow list table:

1. From the workflow management table, highlight the workflow to be deleted.
2. From the Edit /Delete popup that is displayed as shown below, click **Delete**.



An action confirmation popup in some cases is displayed requiring either confirmation or cancellation as shown in the following figure:



3. Click **Remove**, to delete the workflow.

7.0.6.3. Associating a Created Workflow with Alert Queues

A custom workflow is required to handle specific types of alerts that have been grouped together in a single queue .

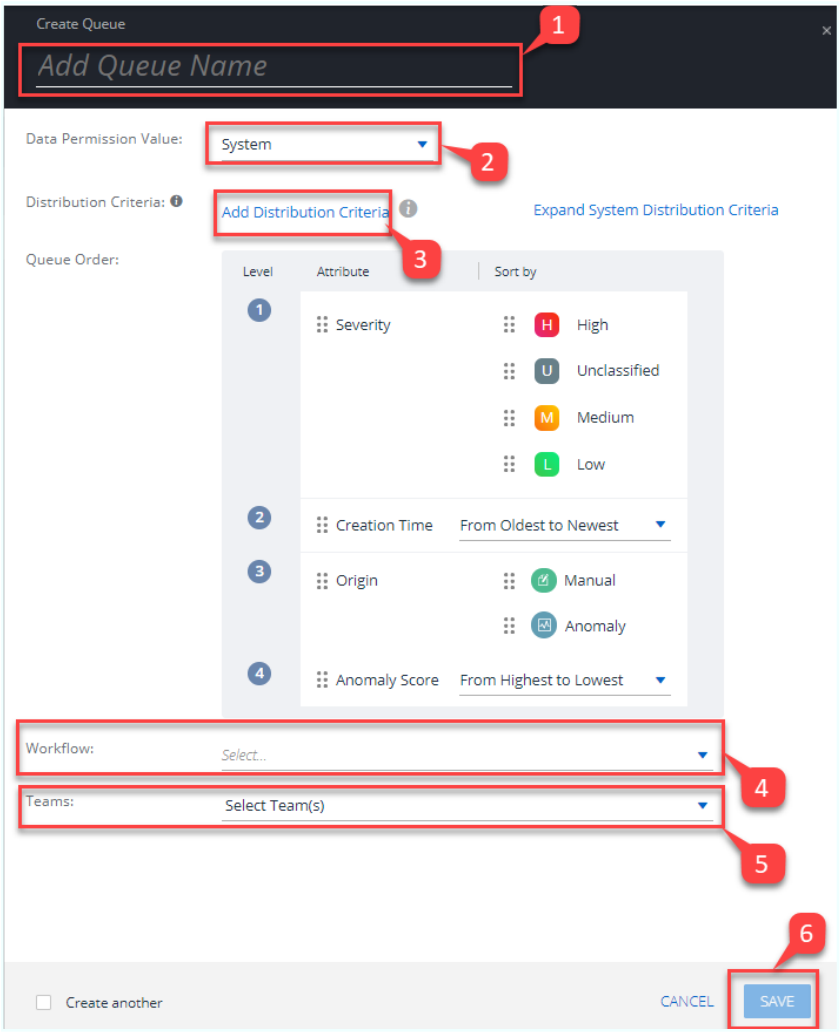
As an example, it maybe decided in your alert investigation domain that alerts of "High" severity should be investigated and resolved in a custom designed workflow.

Continuing with this example, let's create and associate a new queue with our custom workflow.

To create an alert queue that is associated with a specific workflow, proceed as follows:

1. From the Queues Management screen, click the **+ create** icon.

The **Create Queue** popup is displayed as shown below.



If necessary to obtain more details refer to Create a Queue section of Queues Management:

7.0.7. Additional Information

7.0.8. Process Flow - Example Structure

In workflow model creation, adopting a hierarchical process structure helps organize the alert resolution lifecycle in a structure which maximizes manpower resources in an effective manner

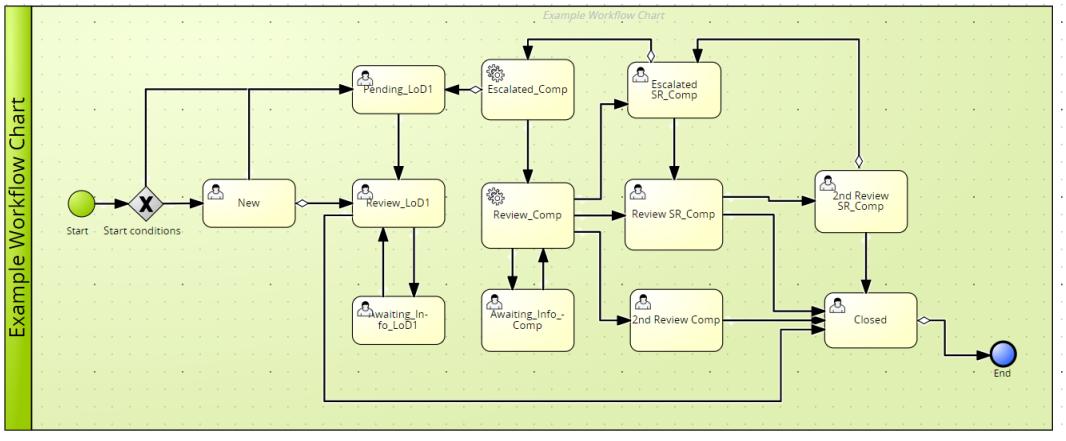
The following example uses graded levels in the alert resolution process and could provide a workable approach to the task of alert handling within a corporate structure. In this example there are three levels of investigation.

Level #1 Starting with level #1 alerts handled by entry level analysts who would normally handle the bulk of low severity alerts. If after investigation they are deemed to be classed as false positive can be closed relatively quickly at this stage of analysis investigation.

Level #2 If during level #1 investigation there are alerts of medium severity and potentially more suspicious, these can be passed to level #2 analysts who have greater experience in investigating more serious alerts. These. after further analysis may could be closed as not providing enough current evidence of wrong doing although the customer in question could be tagged as suspicious and the alert or alerts could be reopened later if more suspicious transactions linked to the marked customer are uncovered.

Level #3 level #3 investigation is reserved for high severity alerts that may be deemed SAR Worthy and require a much more intensive investigation process. This analysis work is the task of specialist analysts with the highest level of expertise in investigating serious financial crime (e.g.: AML, terrorism or human trafficking etc.)

An example workflow model diagram is shownFigure 56: below.



7.0.8.1. XML File - Contents

Once the custom workflow has been approved , to be adopted into the ThetaRay Investigation Center it requires to be converted to a .bpmn xml file for upload.

The xml file contains the following components:

- The workflow process logic that drives the various stages of the alert investigation

- The SLA timings per as they apply to the various service tasks integral to the design
- Within the main workflow sub workflows are used to handle other procceses in parallel such as passing the alert to a supervisor for 4 eyes review

A segment of a .bpmn compliant file is shown7. below.

```
<serviceTask id="auto_pass_four_eyes_review" name="4 Eyes Review" activiti:expression="${alertHandlingService
<sequenceFlow id="flow36" sourceRef="auto_pass_four_eyes_review" targetRef="auto_pass_to_supervisor">
  <conditionExpression xsi:type="tFormalExpression"><![CDATA[${conditionResult eq 'true'}]]></conditionExpres
</sequenceFlow>
<sequenceFlow id="flow37" sourceRef="auto_pass_four_eyes_review" targetRef="state_closed">
  <conditionExpression xsi:type="tFormalExpression"><![CDATA[${conditionResult eq 'false'}]]></conditionExpre
</sequenceFlow>
<serviceTask id="auto_pass_to_supervisor" name="Pass to Supervisor" activiti:expression="${alertHandlingServi
<sequenceFlow id="flow32" sourceRef="auto_pass_to_supervisor" targetRef="state_resolution_recommended"></sequ
<serviceTask id="auto_pass_to_analyst" name="Pass to Analyst" activiti:expression="${alertHandlingService.pas
<sequenceFlow id="flow33" sourceRef="auto_pass_to_analyst" targetRef="state_pending"></sequenceFlow>
<exclusiveGateway id="start_exclusive_gateway" name="Start conditions"></exclusiveGateway>
<sequenceFlow id="flow34" sourceRef="start_exclusive_gateway" targetRef="state_new">
```

7.0.9. Workflow Forms

To help automate the alert resolution process and status communication between analyst and supervisor/compliance personnel a set of workflow forms can be integrated into the workflow model. These can be set up a pre-requisite to the next alert's state so that the analyst's input can be collected and the system supervisor can be updated. For more information on creating and using workflow forms, refer to the topic: Workflow Forms.

7.1. Workflow System-Driven Automated Tasks

- Service tasks are tasks which are done automatically without human intervention.
- In an organization’s workflow model, certain tasks can be automatically triggered.
- Embedding these system-triggered tasks is normally part of the workflow model design handled by an appropriate Business Admin user.
- This automated decision-making ability not only saves on valuable alert investigation time resources, but also helps mitigate the possibility of errors introduced by the user when making next step process decisions manually.

For more information, and full list of automated service tasks, refer to the current Activiti user guide.

The following table lists and details examples of some automatic service tasks currently available for inclusion in an alert investigation workflow model:

Table 3: *Example Automatic Service Tasks listing and details*

Service Task	Details
Four eyes review	The four eyes review service task will reassign an alert to a user who is: • Holding a supervisor role. • Is in the team. • Is not the analyst who assigned the alert. • Has data permission to the alert. It is possible to combine this service task with a condition that filters the alerts which should go through such process. A decision could be made, for example, to only review the high- risk alerts and/or to only review alerts which were analyzed by junior analysts and/or to only review alerts from specific clusters which are specifically important.
Queue assignment	The assign to a queue service task, will receive a name of a queue, move the alert to this queue and unassign the alert. This way, an alert can be escalated to a more senior team for example, and reside in the queue until one of the senior team members selects it for review. This service task can be combined with a form where the user picks a queue name to move the alert to, or that the queue to move the alert to is pre-defined and is stated in the workflow itself.
RealTime	In order for RealTime Transaction Monitoring to be enabled in your BPMN workflow, its associated service task requires to be included in the workflow model design. Related instructions for enabling such a service task refer to the current version of the ***activiti user guide***.
Automation of Change State	This capability is relevant to the first state of the determined queue and triggered by Get Alert button • This capability encompasses only adjacent states. E.g. if two consecutive states are New and Under Review, o Under Review when an analyst presses the button Get Alert •**Note**: There is only one workflow path after the initial state Related instructions for enabling such a service task refer to the current version of the ***activiti user guide***.

7.2. Automatic Workflow State Changing

Automatic State changing in workflows is an optional feature that customers can incorporate in their system deployment to provide greater alert resolution throughput efficiency.
The automation feature works by enabling some initial alert state changes in a queue, to be executed as part of the workflow when the analyst clicks the 'Get Alert' button. For example from the New state the workflow can for example be set up to skip the 'Pending' state and jump directly to the 'Under Review' state.

1. For on-prem customers, please refer to the Activiti User guide that has a dedicated sub chapter that provides details on how your workflow

deployment engineers can integrate this feature into your specific on prem deployment.

2. For SaaS customers interested in incorporating this feature in their deployment, please contact their customer support representative for assistance.

7.3. Workflow - Forms

7.3.1. Introduction

Workflow Forms allow you to further enhance the usability of your custom workflows. By including a range of easy to use system designed forms specific to your alert investigation schema, you can streamline the processes of :

- Information gathering from your analysts and teams
- Provide analysts and supervisors with a more efficient method of requesting further information about the alerts under investigation
- Improve the level of interoperability between collaborating teams

As you will see when you delve further into **Forms,** you have the choice of selecting already designed standard forms, further customizing set up basic default forms or, if you require a special form that does not exist, you can design a form from the ground up by selecting form elements from a form element building block repository.

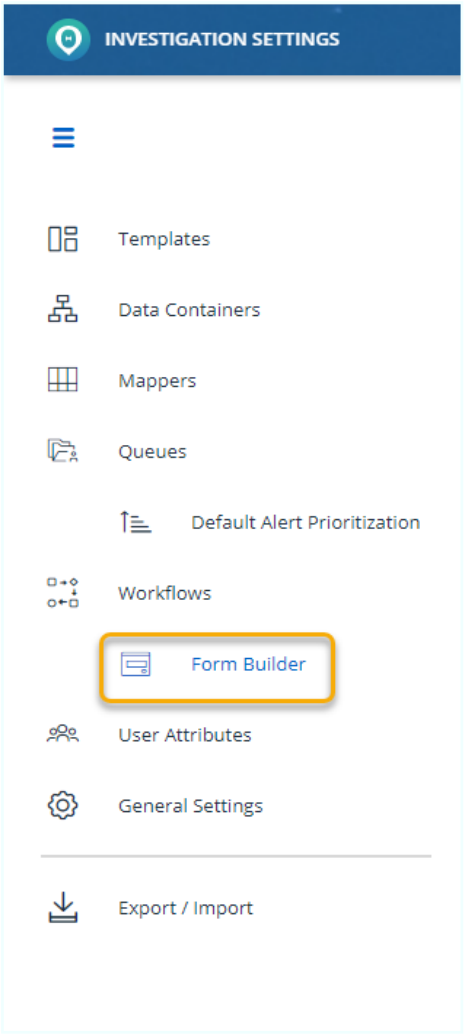
Once your ideal forms have been selected or designed and tested , you can then incorporate them as objects into your workflow model.

As with all elements of the flexible customizable **Workflow** elements, if needed, you can modify the forms in use, if and when your alert schema changes due to changes in on- going work flow patterns.

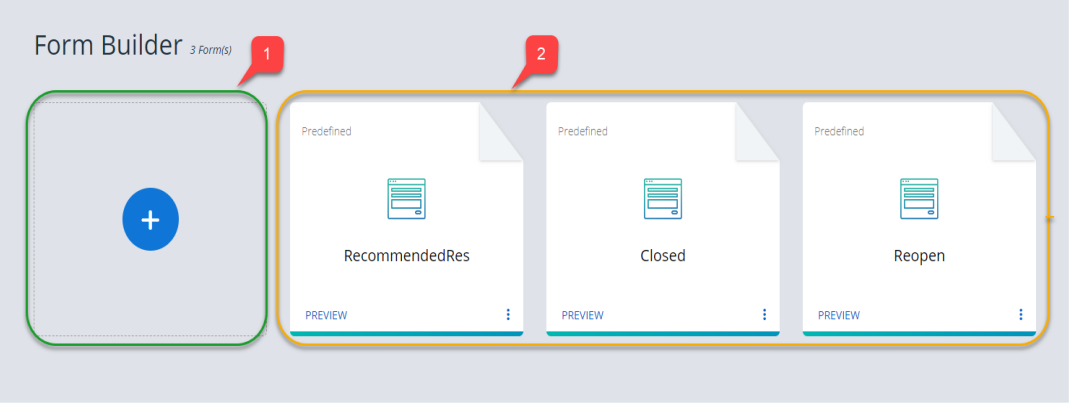
7.3.1.1. Accessing Forms

To access Forms:

1. From the Investigation Settings side panel shown below, click the highlighted **Workflow Builder** tab as highlighted.



An example of a **Form Builder** menu is displayed below.



Referring to the example forms builder screen shown above three out of the box predefined forms (2) are shown, as well as the add new Form icon (1):

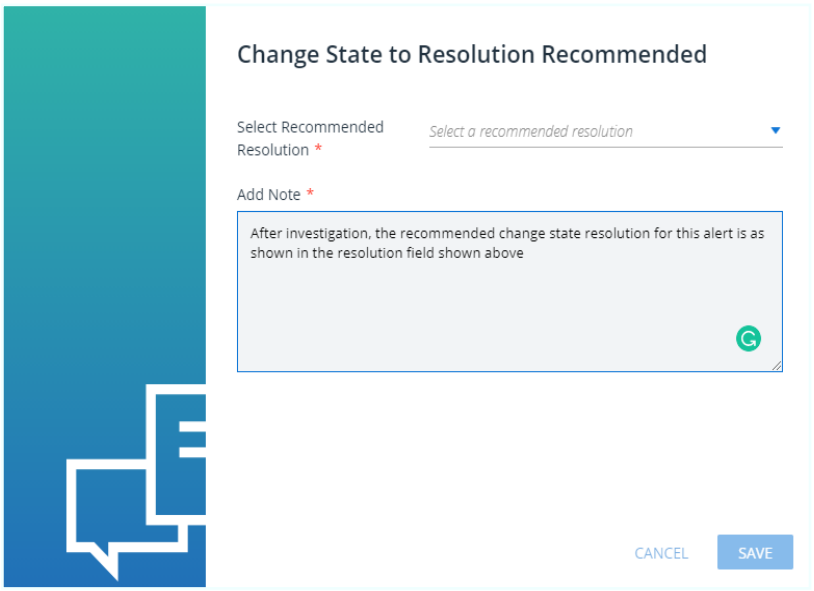
7.3.1.2. Predefined Forms

Predefined forms are preset. They cannot be modified or deleted.

The basic template used in predefined forms usually represents a specific alert status resolution and includes a free text description field where the reason for the particular selection should be detailed.

Once completed and saved the contents of the form are uploaded to the system via the workflow model logic in place and when completed by the user is offered up to to the team supervisor for resolution consideration.

An example of a predefined default form is shown below.



7.3.1.3. Adding a New Form + (Options)

If the predefined forms do not meet your requirements sufficiently, as a Business Admin user with appropriate permissions you can if required either:

- Build and add a new form almost from scratch
- Duplicate an existing form, rename, then edit as required

In the form creation process, you can select from various elements to configure the form as required.

Included in the selectable elements is a 'free text' description field which is included as a mandatory requirement.

- This option shall include the possibility to select specific resolution codes while creating a form in the "Form Builder" of IC Settings.
- There is a need to attach a selected set of resolution codes for specific forms in one workflow that differ from each other.
- In custom forms all resolution codes shall be unselected. A user is required to select at least one resolution code to save a form.
- In the predefined forms, all resolution codes shall be listed as before and a user can modify the selection.
- When creating Custom forms the IC admin user can manage his team of analysts more efficiently in by configuring which recommended 'codes' the analyst can select from per custom form
- All other elements of the predefined forms shall not be editable.
- The resolution codes shall be listed from A to Z.
- a user can create multiple forms that differ from each other with specific resolution code sets for one workflow

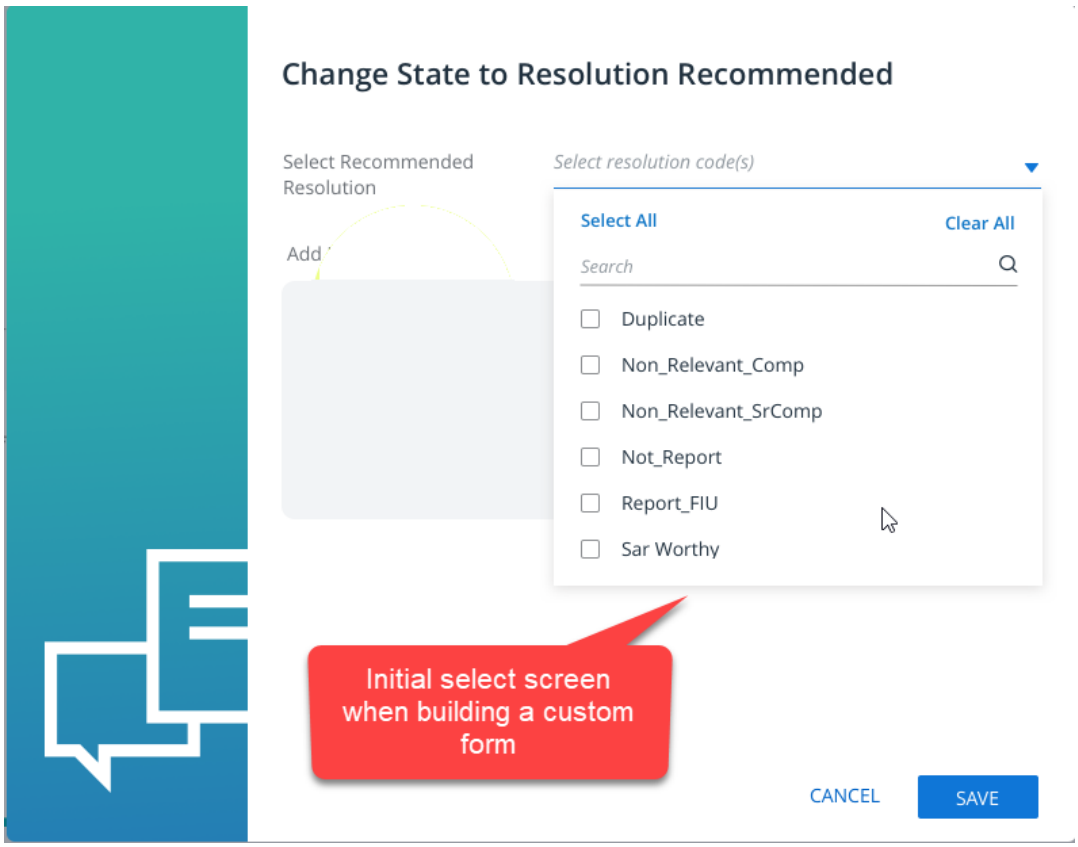
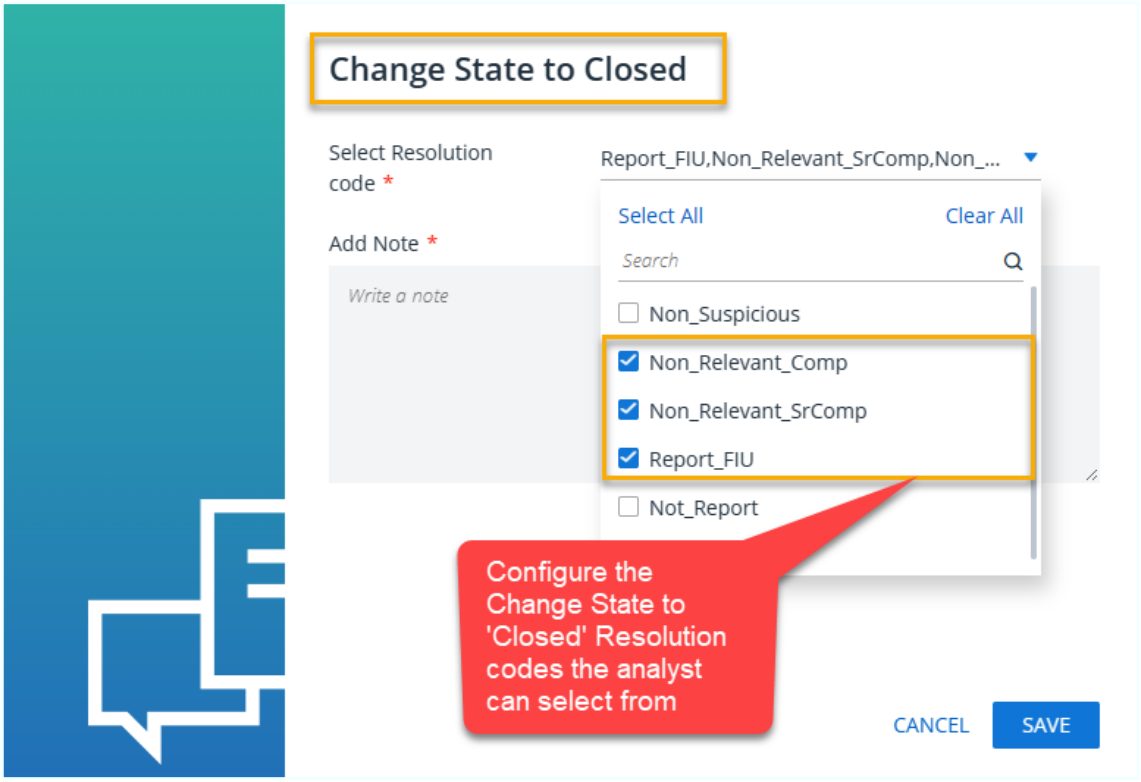
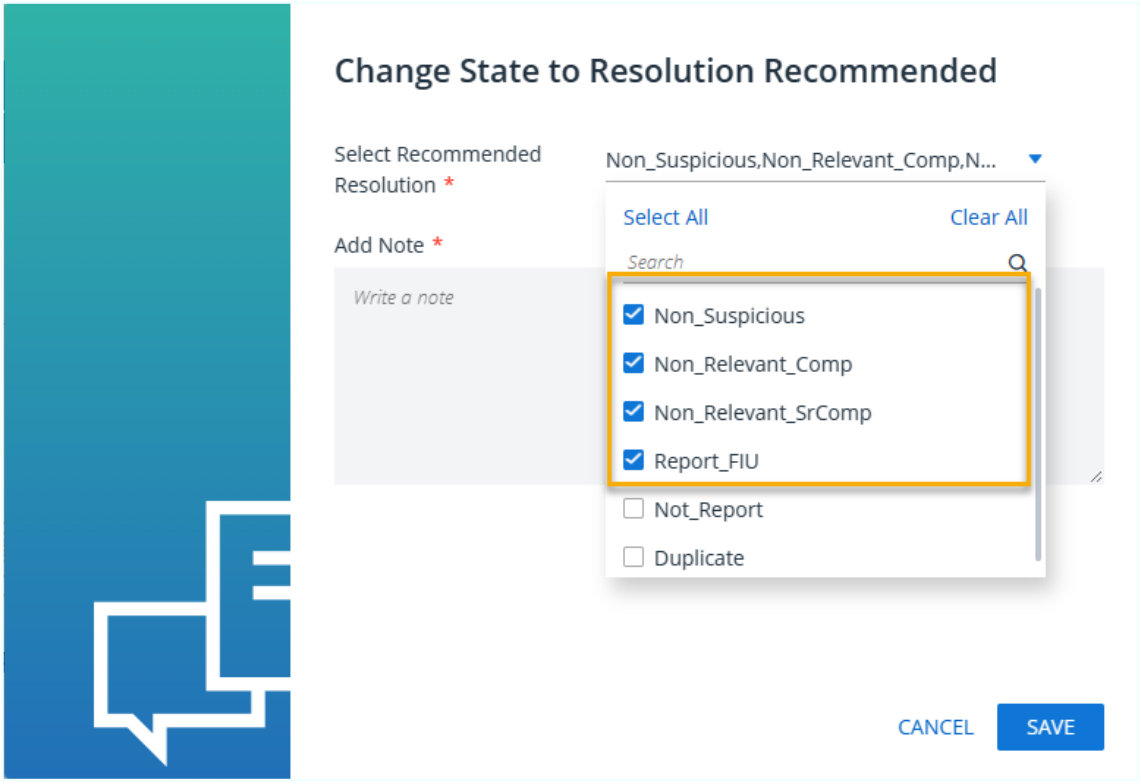
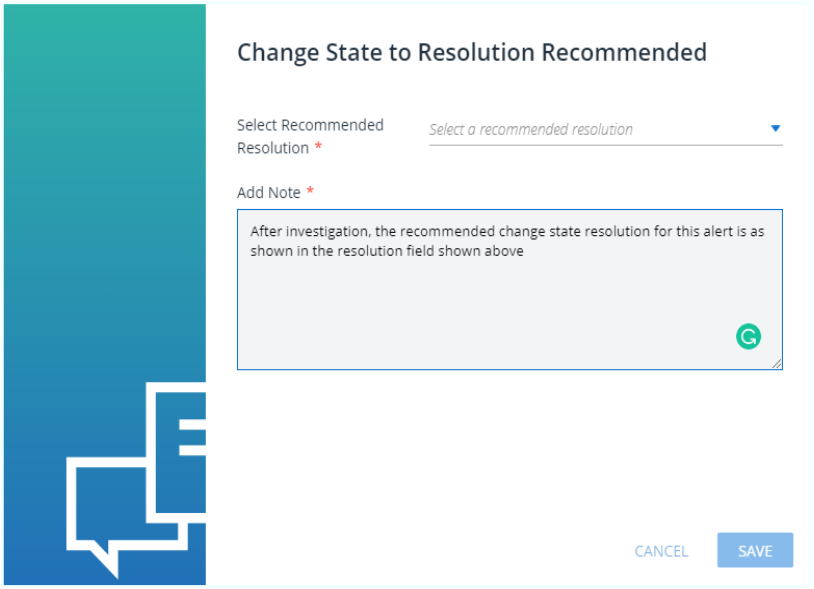


Figure 58: *Initial Form Display with no Codes Selected for Analyst Selection*





default form is shown below.



7.3.1.4. Adding a New Form + (Options)

If the predefined forms do not meet your requirements sufficiently, as a Business Admin user with appropriate permissions you can if required either:

- Build and add a new form almost from scratch
- Duplicate an existing form, rename, then edit as required

In the form creation process, you can select from various elements to configure the form as required.

Included in the selectable elements is a 'free text' description field which is included as a mandatory requirement.

Note: This type of form, although enabling maximum design options, does include basic immutable elements that are required as part of the workflow model.

An example of a configured form is shown in 7.3. below.

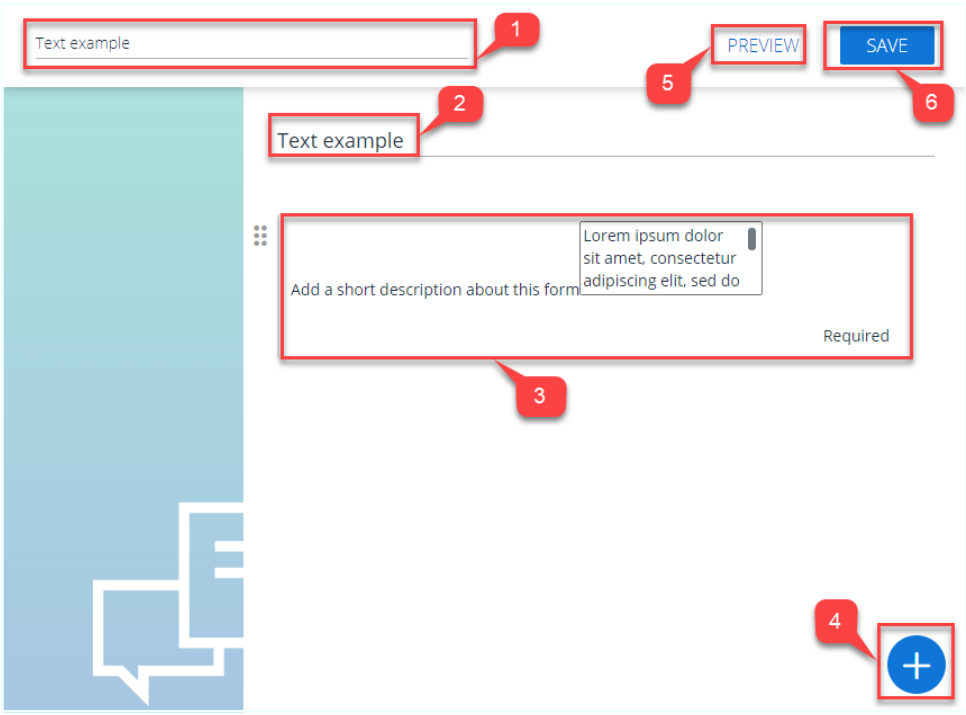


Figure 59: *Configurable Form - Edit Mode*

The example form shown above contains the following elements:

- **Name**: Name of Form, (max 100 chars.) (1).
- **Title**: Form title, (max 100 chars.) is mandatory and must be unique(2)
  - Example: in this instance both the form title and name could be the same or the title can be different (for example the form name could be **Required Feedback from Team** and the title could be **Number of Alerts Resolved**

- **Description**: Free test for adding a description Normally required in most alert investigation deployments (max 1024 characters)(3)
- **Add Icon +** to allow more form elements to be added to form (4)
- **Preview**: Provides a preview of the form layout, as it will be displayed in the environment workflow (5)
- **Save**: When the form editing is complete, a save is required to make sure that it is added to the library of available forms in the workflow

7.3.1.5. Adding a New Form - Practical Example.

The creation of a new form is provided as a practical example:

To create a new form by adding available elements (example):

1. Click the + icon in the Create form screen.

The basic new form layout is displayed as shown inthe following figure.
Figure 60: *Create New Form - Basic Layout and Selecting First Form Component*

2. Enter a form name (max 100 characters) e.g., required feedback from team.
3. Enter a title for the specific form.(max 100 chars) e.g. number of alerts resolved.
4. Click the + add icon.

In this example, we will first select a Note field element from the list of available elements, to enable us to describe the new form that is being created.

5. Select the **Note Field** element.

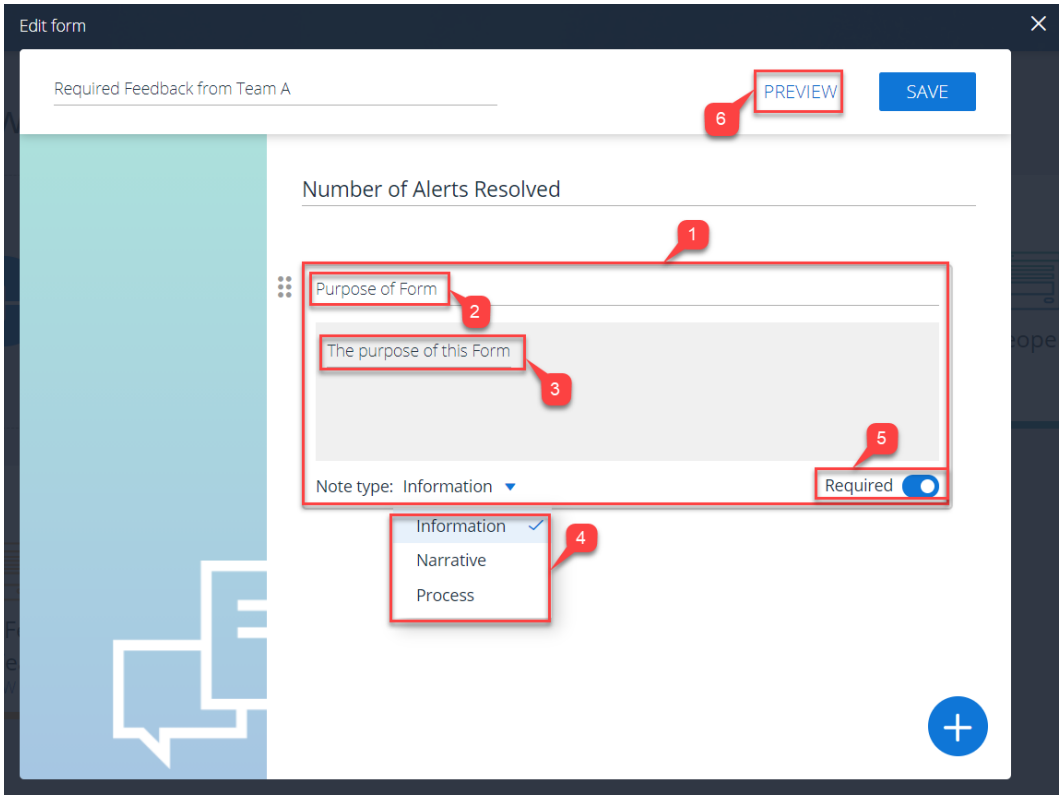


Figure 61: *Example Adding a Note Field Element*

A note field element is added as shown in Figure 61: above (1).

6. Complete the Note Element labels (for the purposes of this example) as follows:
    a. Purpose of Form label (2).
    b. A field in which to describe the purpose of the Form (3).
    c. Type of Note (Informative, Narrative or Process) (4).
    d. A toggle switch to make the requirement of this mandatory or optional (5).

Note: By enabling the requirement switch the user will not be able to complete and send this form unless this mandatory requirement is met.

When the note element is complete, it is a good practice to preview the Form (so far) by clicking the **Preview** button (6).

An example **Preview** of the partially created form is displayed in our example as shown Figure 62: below.

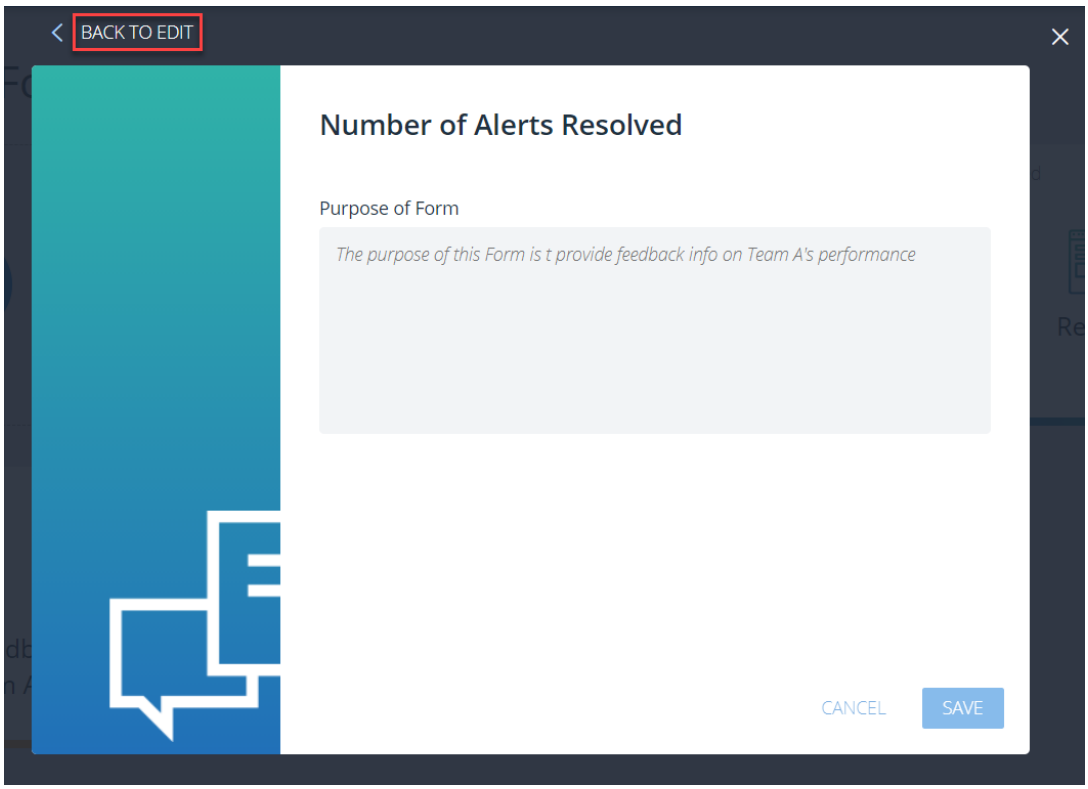


Figure 62: *Viewing a Preview of an Example Form*

7. To make further edits (Modify existing Element or Add a new Element), click the **Back to Edit** link.

Now in our example, lets add a dropdown select menu to enable our users to add other attributes to our form.

8. Click the add + icon.

For the sake of this example , we want our users to be able to add an assignee to the form by selecting from a list of environment analyst assignee users displayed in our dropdown menu. For that we need to:

a. Click Drop-down menu from the types available.

A Drop-down menu is added to our form as shown in 7.3. below.

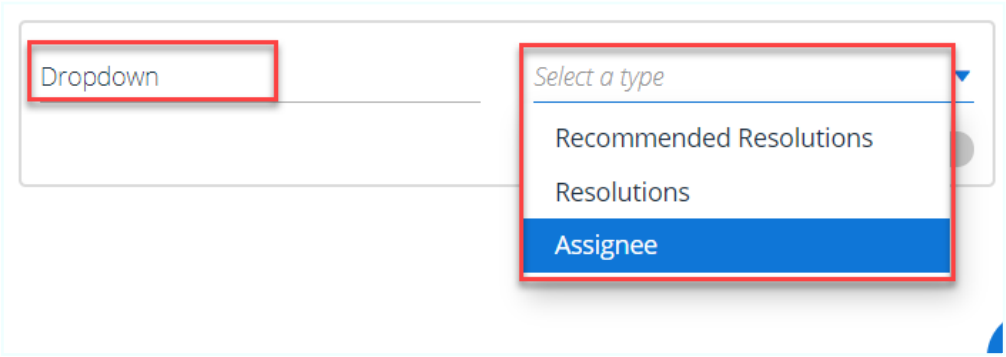


Figure 63: *A Drop-down Menu is Added to our Example New Form*

b. Provide a name (e.g., Assignees) for our dropdown menu.
c. Select **Assignee** from the available menu options.
d. When you think the form is complete, click **Preview** to preview it.
e. When all form features meet design specifications, click **Save**. to add the form to the form library.

7.3.1.6. Summary of Form Options

The table below provides details of all form elements available.

Form Element Categories	Options	Details
Initial form elements	Dropdown	Dropdown Menu title
	Note Field	Note title
	Description	Details of form purpose
Note Field Types	Information	General alert case support information
	Narrative	Alert information in the form of a story
	Process	System process information
Dropdown menu types	Recommended Resolutions	Suggested alert resolution (from analyst)
	Resolutions	Alert Resolution final (Supervisor decision)
	Assignee	To whom the alert is assigned to

8. User Custom Attributes

8.1. What are User Attributes used for?

In the current 6.2 release, the main purpose of assigning users custom attributes, is to provide the implemented alert quality control feature in the current workflow with the necessary percentage levels of each individual analyst team member. This level dictates the split level on how many alerts require further supervisor verification.

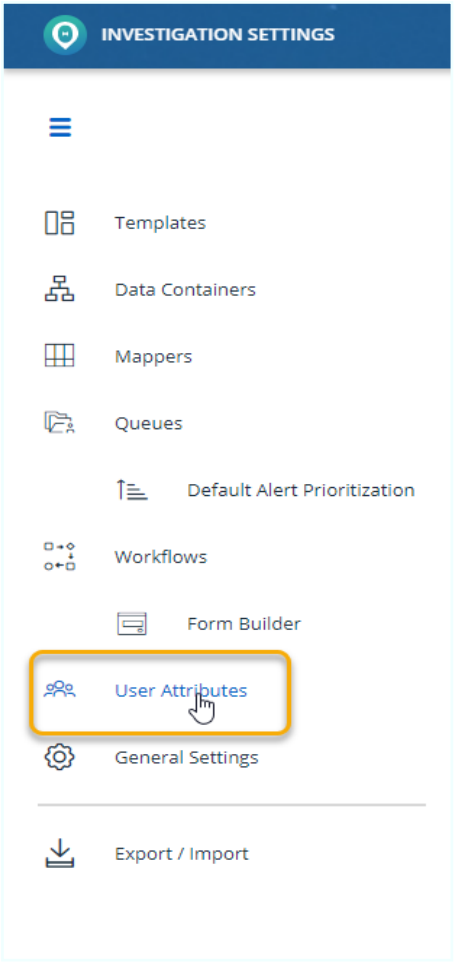
For more information on how the quality control scheme works , refer to the documentation section under workflows labeled *Workflows Quality Control* and for information on adding Quality Control verification stages into the current workflow refer to the current *Activiti user guide* .

This section of the Investigation Settings module, describes and details how to set the percentage levels for each analyst in the team.

Once set and in use, these set percentages can be monitored and if necessary, modified to achieve maximize team performance levels.

8.2. Who can configure Attributes & how to Access User Attributes?

The task of configuring user custom attributes is normally undertaken by an admin user, with appropriate read/ write permissions.
Access is from the IC Settings side bar menu as shown below.



To access the Attributes table.

1. click the User Attributes link highlighted above.

An example user attributes table is displayed below.

The table Displays the following information:

- Edit Select box
- User ID
- Username
- First name
- Last name
- Status: Active or Inactive
- Select Settings select panel icon

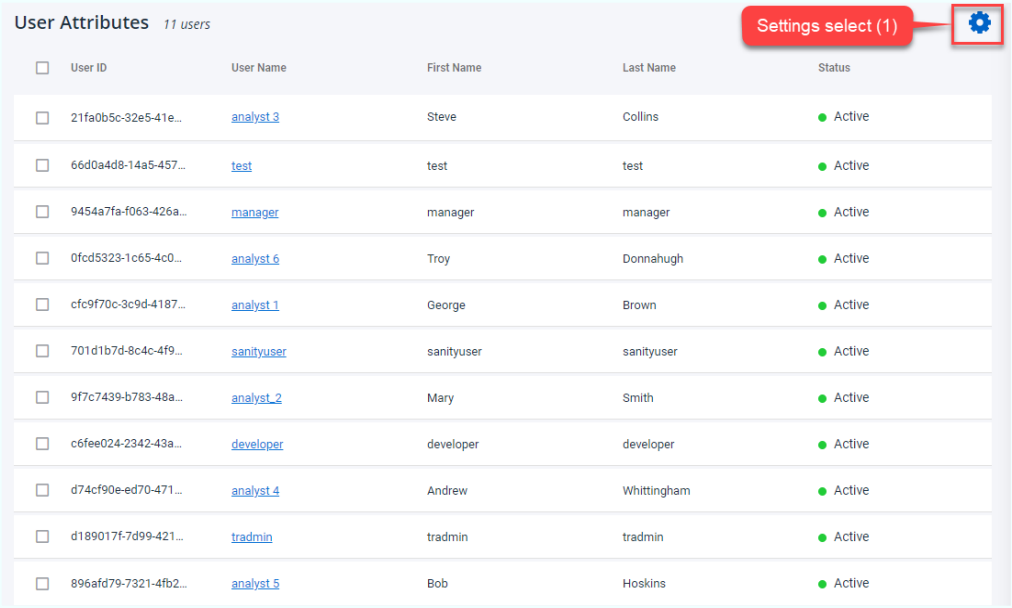


Figure 64: *Example User Attributes table showing User Details , Status and Settings Panel Select Icon*

8.3. Configuring User Percentage Levels

Configuring user attributes percentage levels for the first time, requires that you need to first configure the *Settings* panel.

8.3.1. Configure the User Attributes Settings Panel

To configure the *Settings* panel:

1. Click the *Settings* select icon (1) as shown above.

The Add User Custom Attributes Settings panel is displayed as shown below.

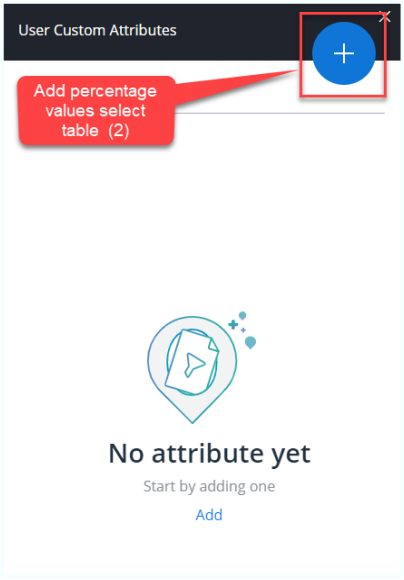
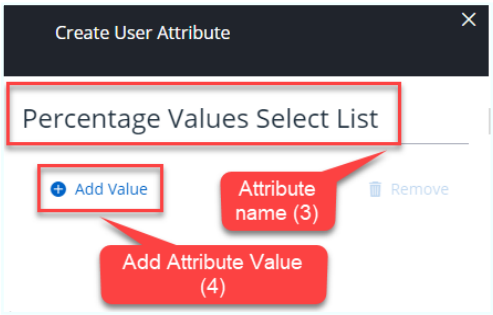


Figure 65: *Add Percentage Attributes*

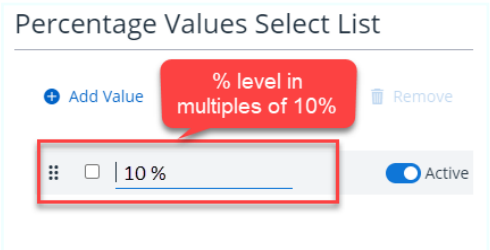
Before we can assign percentage values to our analyst users let's configure a percentage option table.

2. Click the *Add* icon as highlighted in (2) above. to display the User Attributes
    a. First we need to name the attribute - As we want to set up various percentage select values for our analysts we will name the attribute - *Percentage Values Select List* , as shown below (3).



    b. To set our range of values click the *Add Value* link as shown above (4).

The configure value field is displayed as shown below:



To complete the percentage value list we will,for the sake of completeness add values from 0 - 100 %, although note that it is not an intial requirement to enter all incremental values as shown below.

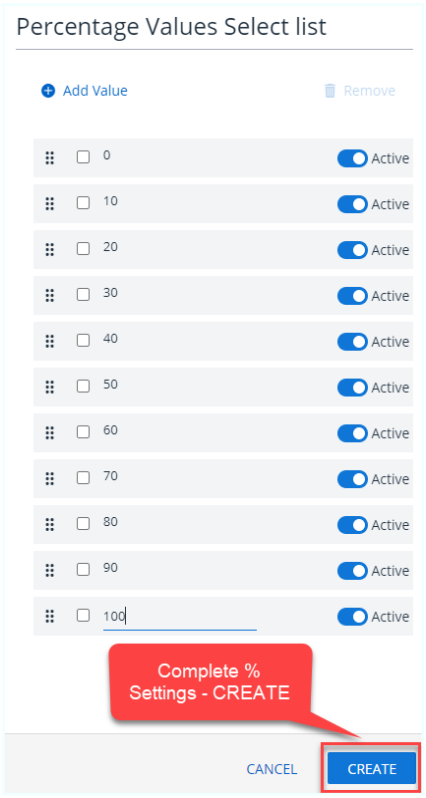
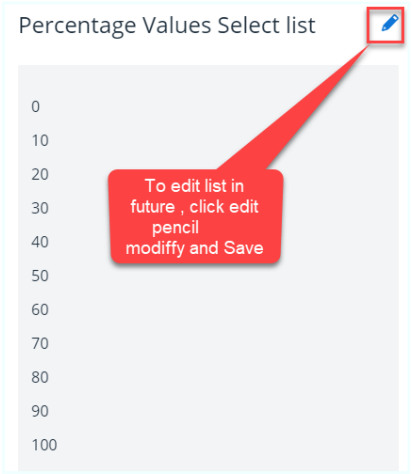


Figure 66: *Percentage QC Levels Configuration in the Settings Panel*

c. When complete click the CREATE button.

When CREATE is clicked, the following summary screen is displayed.



d. If required to edit set values, click the edit pencil , modify and Save.

Note: Also in the *Settings configuration edit mode*, users can be acivated or deactivated by toggling their Active switchin the Edit Mode. Don't forget to click *Save* when complete.

8.3.2. Configuring Percentage Levels per User

To configure a percentage level attribute to an individul user:

1. From the User attributes screen, click the Edit Icon pencil for the user you wish to assign percentage.

The User Attributes' panel with the Quality Control edit panel is displayed as shown below.

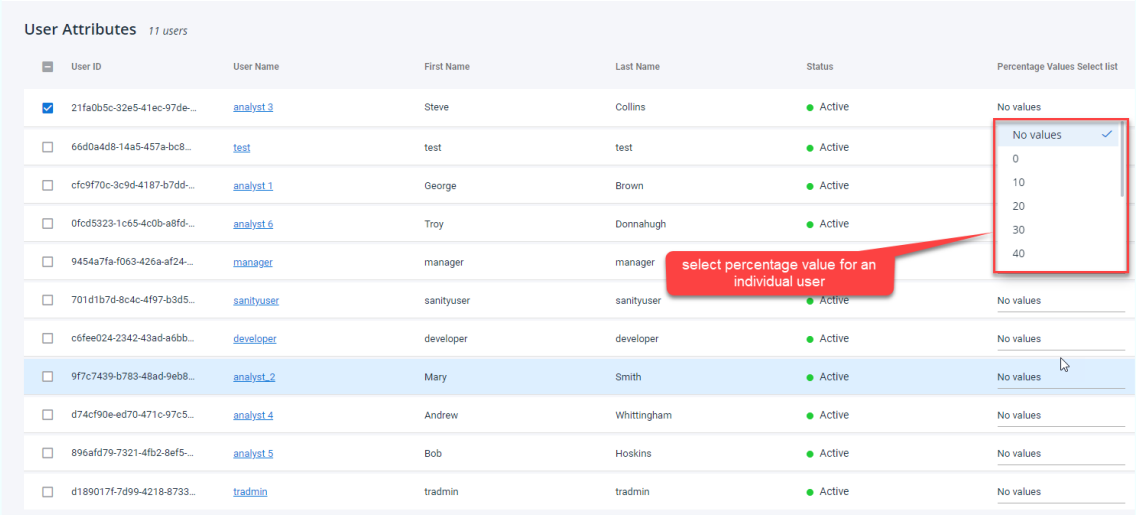
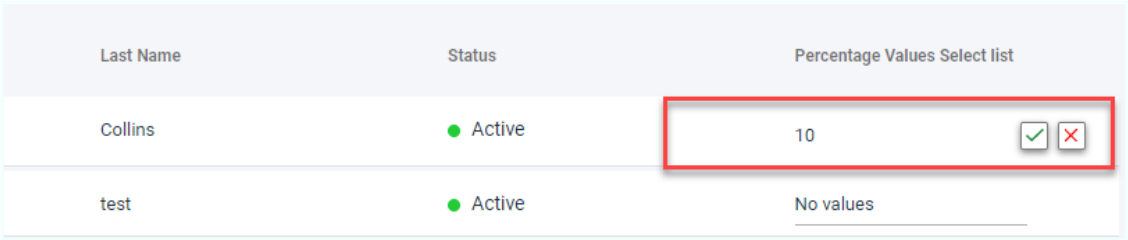


Figure 67: *Example Configuring Quality Control Percentage level for an Individual User*

2. Select the required percentage per user (in this example we will configure a level of 10% (As a reminder of QC functionality - this configuration means that for this user, 1 in every 10 alerts will be verified).



3. When complete, click the green tick icon to save setting.

Note: If required after configuration is saved, you can test the implementation on the workflow, by clicking refresh (f5) to apply the new settings

Note: when percentage values are set for users, these settings are not applied retrospectivley (i.e. the new settings do not do not impact on previous alerts, only on newly selected alerts).

8.4. Editing User Attributes - Bulk Operation

In large organizations where there are many registered users, the time consuming task of assigning attributes can be managed more efficiently by bulk assigning attributes.

To bulk assign QC percentage levels:

In this example shown we bulk assign 3 users a percentage level of 30%.

1. We tick the boxes for our similarly experienced users (1)

(Notice, after more than 1 user is selected the Edit Attributes button is activated.)

2. Click the *Edit Attributes* button to display the bulk edit popup (2).
3. From the Edit Attributes popup we select 30% percentage level from the dropdown menu (3).
4. Click the box next to the Percentage value select
5. When complete, click *Save*to apply (4).

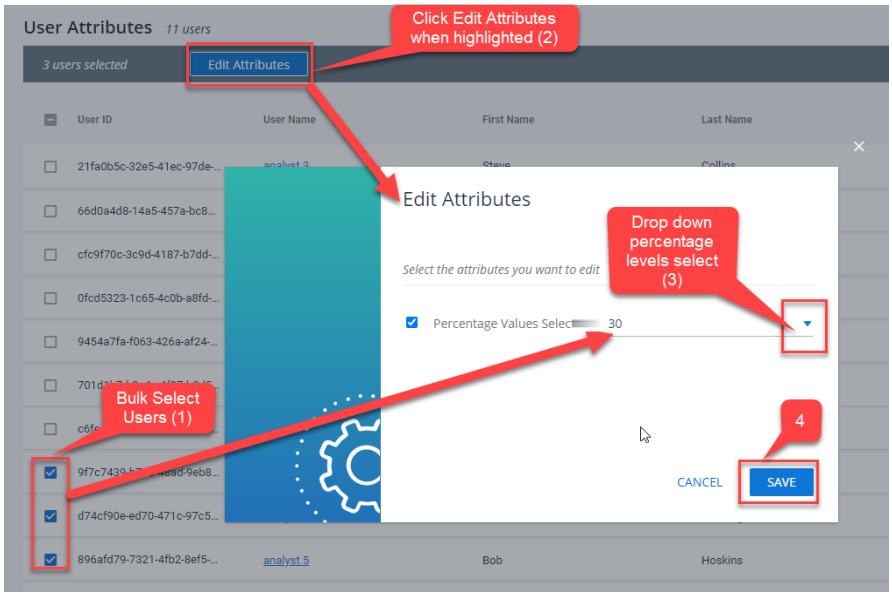


Figure 68: *Bulk - Quality Control Percentage Level Settings*

8.5. Modifying User Attribute Percentage levels

Cofigured percentage values can be modified at any time.

1. Select the Edit pencil for individual users or use the bulk edit function.
2. Don't forget to apply new settings by clicking the green tick icon when editing individual users or *Save* when bulk editing.

9. General Settings

The General Settings chapter enables the IC admin user with permissions to configure auxiliary investigation center functions that are not included in the main IC setting categories.

General Settings enables the following configurations:

- Control - This configuration enables alert editing as whether an alert is assigned to the analyst or not
- Locale - enables specific date/ time and number formats and SLA calendars to be configured and implemented
- Operation Dashboard Configuration - controls widget views
- Consolidation - controls alert consolidation
- Match Score - sets the level of alert definition in the screening solution
- Severity Score - sets severity definition levels in IC
- Alert Externalization - sets required parameters to externalize alerts covering all origins

To access General :

1. Click the tab highlighted in the following figure.

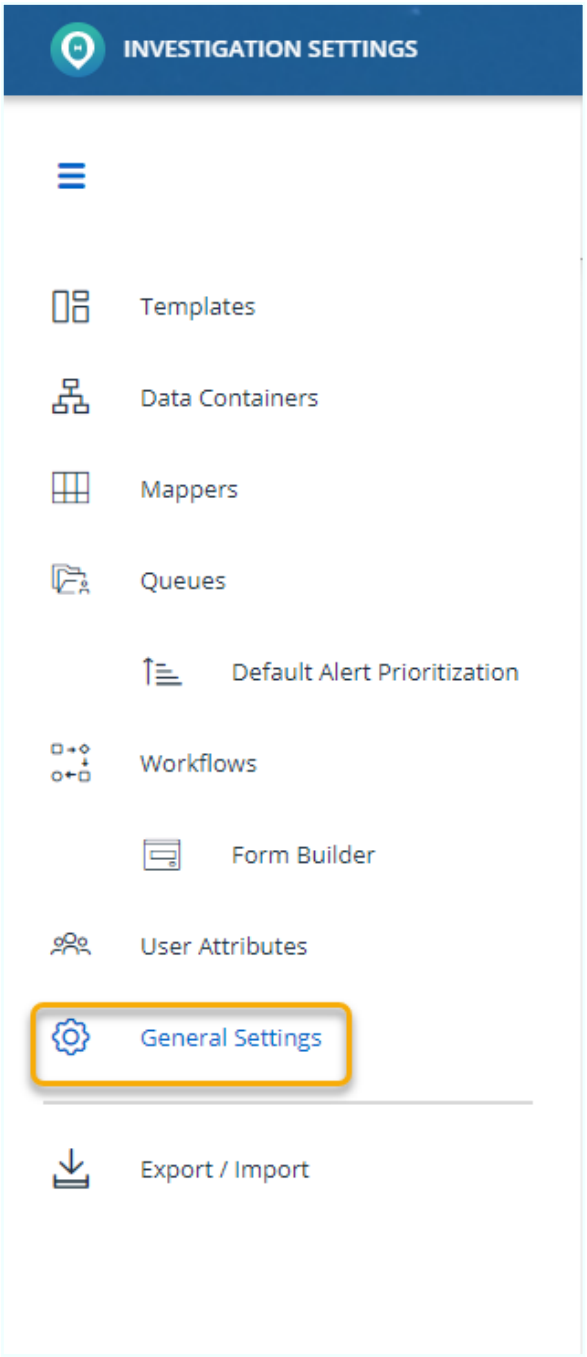
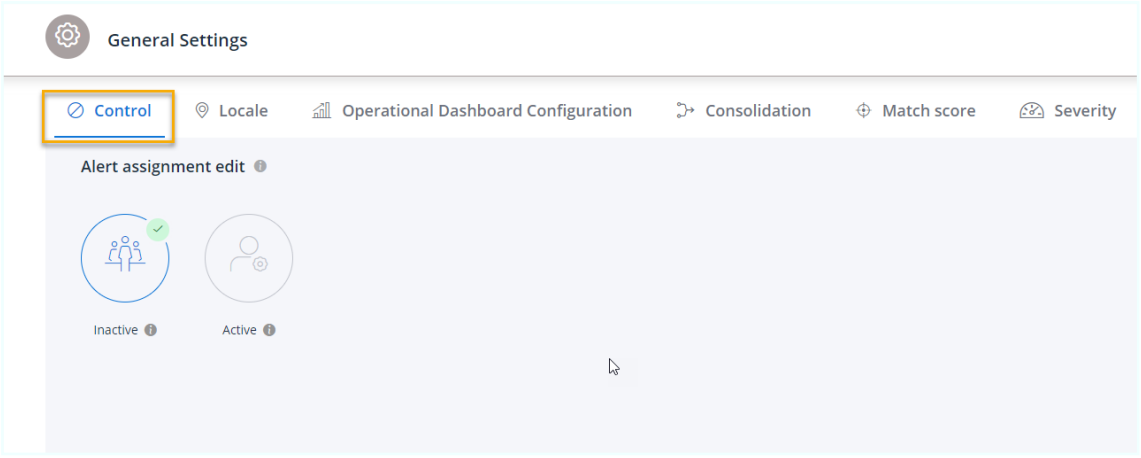


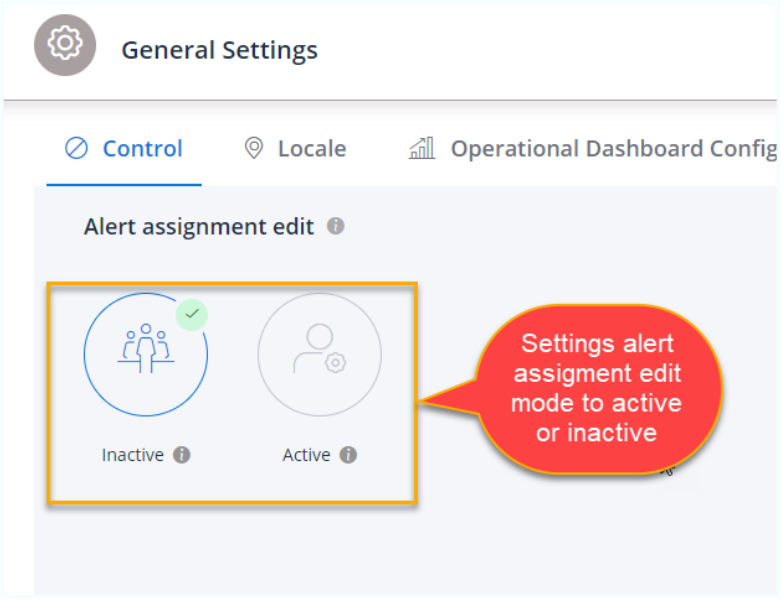
Figure 69: *Clicking on* ***General Settings*** *displays the following screen with the* ***Control*** *tab selected by default.*



General Setting Default Display on Selection

9.1. Control

The purpose of the **Control** tab, is to enable two permission modes active or inactive for a user depending on whether an alert is assigned to them or not. By default, the ***Inactive*** setting is enabled, as shown in the figure below.



Inactive mode - No editing limitations so that a user can:

- Edit notes for any alert in alert queue
- Upload forensic documents to any alert in the alert queue
- Change the state of any alert in an alert queue

Active mode - Editing Limitations so that assigned users can:

- Edit notes for alerts assigned to them
- Upload forensic documents only to an alert assigned to them

- Change the state of an alert assigned to them

9.2. Locale

As the ThetaRay Alert solution is deployed globally in multiple regions, it is an important requirement to be able to display entities such as date / Time and numbers in a format that is applicable to each specific geographical region or country.

The **Locale** tab in **General Settings** enables the business admin user to define the date/time zone / number formats applicable to his / her IC alert deployment according to locality.

9.2.1. Date / Time/ Local Browser Set Formats

With reference to the figure shown below, to view and set the applicable date time and numbering formats click the highlighted dropdown icon as shown in (1, a & b).

In addition, the user's local browser (UTC) time zone (set in IC Settings Templates and Mapper configuration), is displayed.

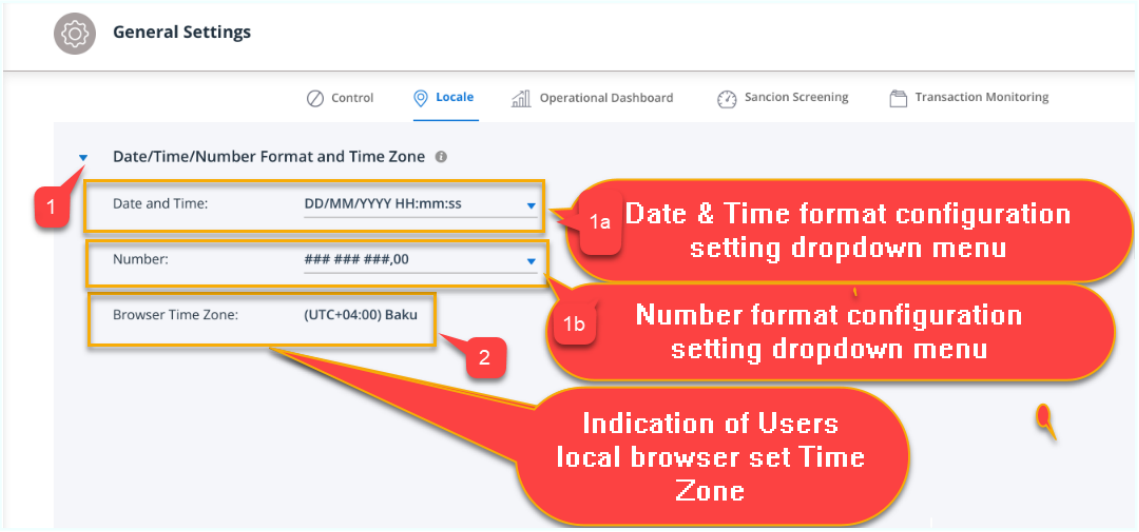


Figure 70: *Locale Settings Configuration / Browser Indication*

When selected the Date/Time format select block is displayed as follows:

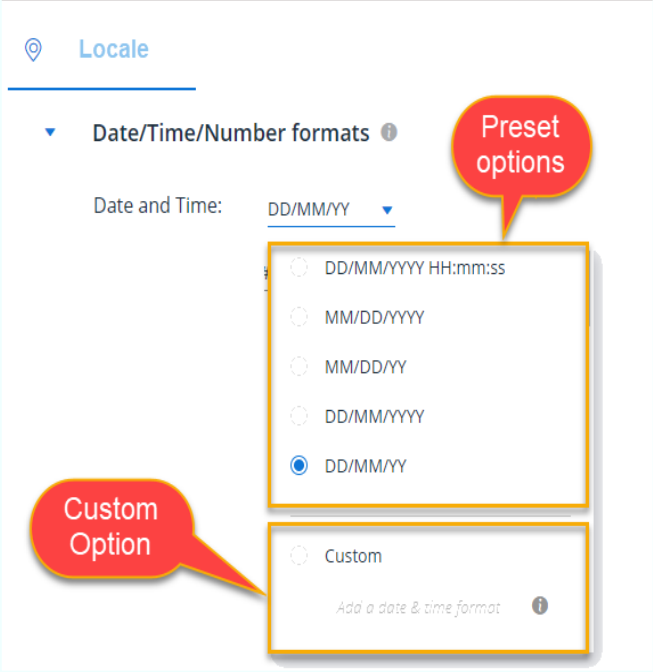


Figure 71: *Preset and Custom Sections Select*

The above figure highlights the two **Date and Time** format setting options:

- Preset
- Custom

9.2.2. Preset

Scrolling down the range of preset time and date formats reveals all the options as detailed in the following table.

Table 4: *Preset Format Options Table*

Ref	Date Format	Time format
1	DD/MM/YYYY	HH:mm:ss
2	MM/DD/YYYY	N/A
3	MM/DD/YY	N/A
4	MM/DD/YYYY	HH:mm
5	MM/DD/YY	HH:mm
6	MM/DD/YYY	HH:mm:ss
7	MM/DD/YY	HH:mm:ss
8	MM/DD/YYYY	HH:mm:ss XM
9	MM/DD/YY	HH:mm:ss XM
10	DD/MM/YYYY	HH:mm
11	DD/MM/YY	HH:mm

Table 4: *Preset Format Options Table (continued)*

Ref	Date Format	Time format
12	DD/MM/yy	HH:mm:ss

Selecting to set from one of the preset options is simple. Identify the date and time format that suits your locale, click the associated radio button - that's it !

9.2.3. Custom

If none of the preset options meet your requirements, try the custom option.

To set a custom format:

1. Click the radio button in the Date and Time **Custom** format section.
2. Type your custom format making sure the following guidelines are followed:
   a. The day is denoted by DD (capitals with a (/),(.),(-) inserted between date entities).
   b. The Month is denoted by MM (capitals with a (/),(.),(-) inserted between date entities).
   c. The Year is denoted by YY or YYYY (capitals with a (/),(.),(-) insterted between date entities).
   d. The Hour is denoted by HH (capitals with (:) inserted between time entities).
   e. Minutes are denoted by mm (lower case with (:) inserted between time entities).
   f. Seconds are denoted by ss (lower case with (:) inserted between time entites).
   g. XM can stand for AM or PM and can be included to refer to after midnight, but still on the same schedule day.
3. When custom format is complete, click **Enter**.

Note: When either a preset or custom date and time format is selected, it immediately becomes the new Investigation Center wide global setting format which is used to display the date and time throughout the alert Investigation Center deployment.

The following table details where the date and time format is applied in the Investigation Center and Settings.

Table 5: *Date and Time Format used in the Investigation Center and Investigation Settings - per Section*

Section	Module	Comments
Alert Card List	Investigation Center	All relevant card details
Risk details and evidence elements	Investigation Center	Includes graphs, histograms, (includes days)
Notes tab log details	Investigation Center	Where the selected format does not include time, the displayed time uses the default format
History tab log details	Investigation Center	
Date range filters	Investigation Center	including custom option
Rules Editor	Rules Editor	last updated & date range
Network Visualization data	Network Visualization	Nodes and edges
Trace queries date range	Investigation Center	global and feature level
Templates	Investigation Settings	Date and time format in alert tabs of Templates with overwrite capability
Mappers	Investigation Settings	Date and time format in alert tabs of Mappers with overwrite capability
Operational Dashboard	BI and Trends	last update time stamp (both modules), reports in Transaction BI and Trends modules

Note: In global and feature transactions, risk details and evidence elements are not covered by preset and custom date/time/number configuration. This category of data is received from customers and processed by data engineers.

Note: The default preset date and time format is: DD/MM/YYYY HH:mm:ss

Note: When trying to set a custom date and time format, and any components are entered that are not acceptable, a red warning triangle is displayed as shown below. Click the **(i)** tool tip icon to display a message detailing the correct custom requirements.

Note: Additionally, the Transaction BI and Trends reports time reports data down loadable from the Operational Dashboard is not included by the date/time/number global format selection / configuration.

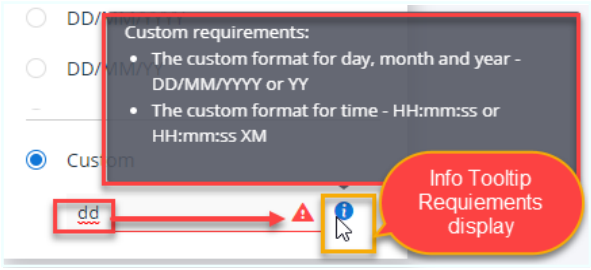


Figure 72: *Example Display Showing Requirements*

To resolve the issue check the requirements and guidelines listed above.

9.2.4. Number Formats

Number formats are in general used to denote amount values (either monetary or quantity)

To configure the numbers format used in your deployment:

1. Referring to the figure below, click the drop down icon (2).

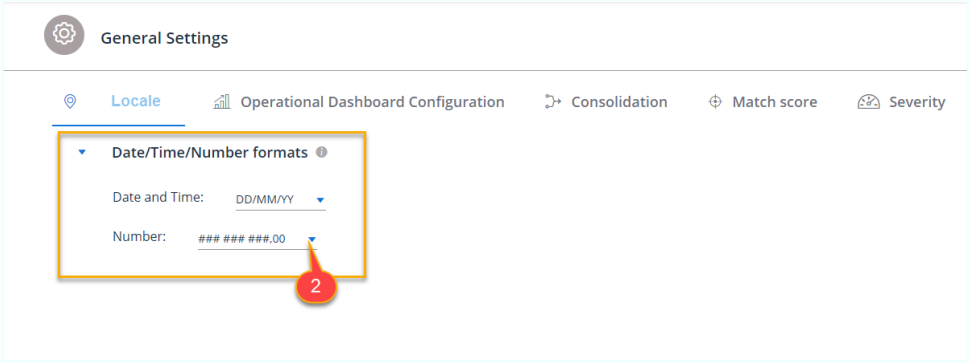


Figure 73: *General Settings - Number Format Options Menu Select*

The numbers format option select menu is displayed as shown below.

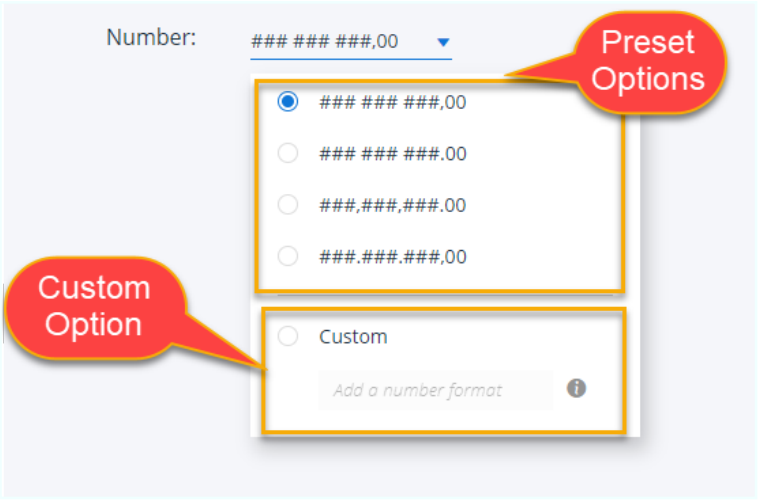


Figure 74: *Custom Number Select Options*

The above figure highlights the two **Number** format setting options:

- Preset
- Custom

9.2.5. Preset

Selecting to set from one of the preset options is simple. Identify the number format that suits your locale, click the associated radio button - that's it !

9.2.6. Custom

If none of the preset options meet your requirements, try the custom option.

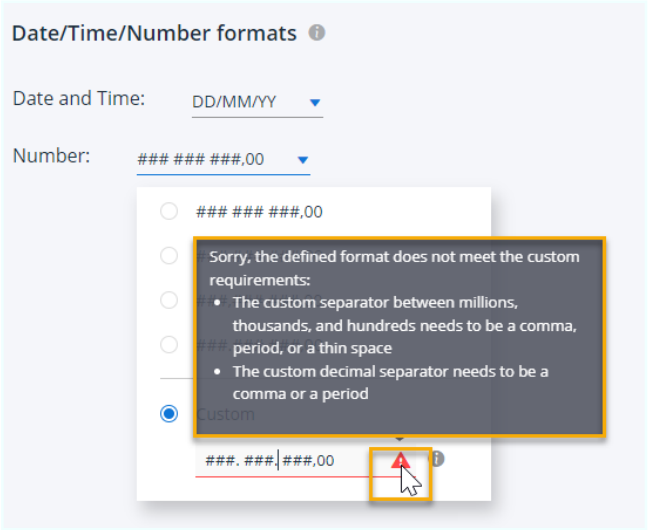
To set a custom format:

1. Click the radio button in the **Custom** number format section.
2. Type your custom format making sure the following guidelines are followed:
   a. The customer separator between millions, thousands and hundreds requires to be a comma, period or thin space.
   b. The custom decimal separator / delimiter requires to be a full stop or comma.

Note: As with the Date and Time format selection the newly selected numbers format is applied immediately to all sections of the Investigation Center and Settings modules. As a guideline also, the sections where the new number format is applied is in general the same as detailed in the date and time details table shown above.

Note: The default preset number format is: ### ### ###,00

Note: When trying to set a custom number format, and any number components are entered that are not acceptible, a red warning triangle is displayed as shown below. Clicking the **(i)** tool tip icon displays a message detailing the correct custom requirements.



9.2.7. Local Browser Setting Display

To facilitate and enhance the analysts alert investigation task, displayed alerts can be viewed relevant to the analyst's local time zone. So for example, in a globally diverse deployment, shared alerts from different DPV's can be investigated according to the analysts own browsers time zone.

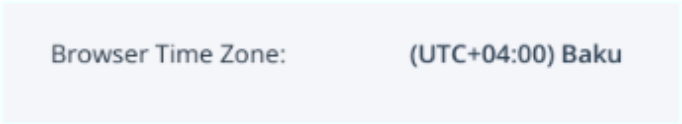


Figure 75: *Example Browser (UTC) Time Zone Setting*

For more information on setting local time zones, refer to ***IC Settings Templates and Mappers*** configurations sections.

9.3. National Calendar SLA (Per DPV)

This section facilitates the configuration of deployments, depending on the extent of geographical coverage to pair different countries or regions with a specific DPV or DPVs that enables each pairing to use local calendar settings that are custom aligned with such work trend variables as for example, local holidays, normal work day patterns etc.

To initialize the SLA configuration:

1. Click the Locale Tab, then the SLA tab menu dropdown.

The following screen is displayed:

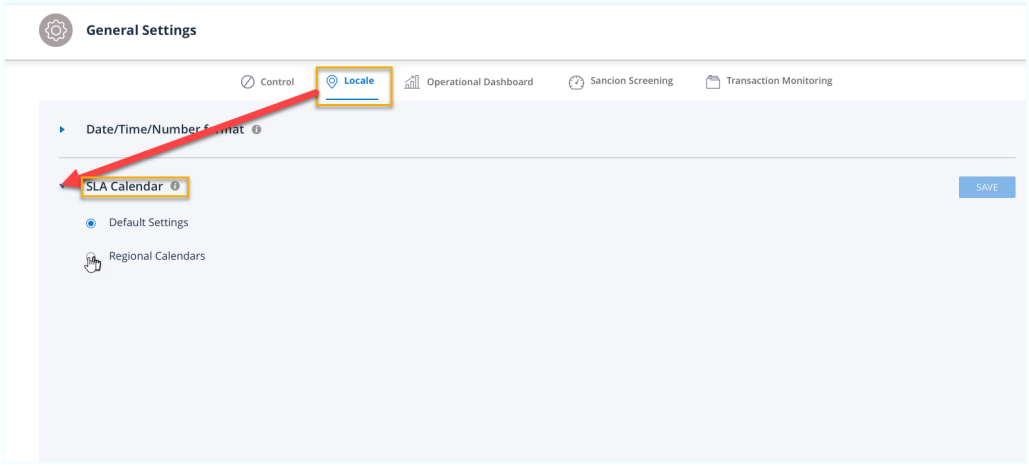


Figure 76: *SLA Calendar Initial Configuration Screen*

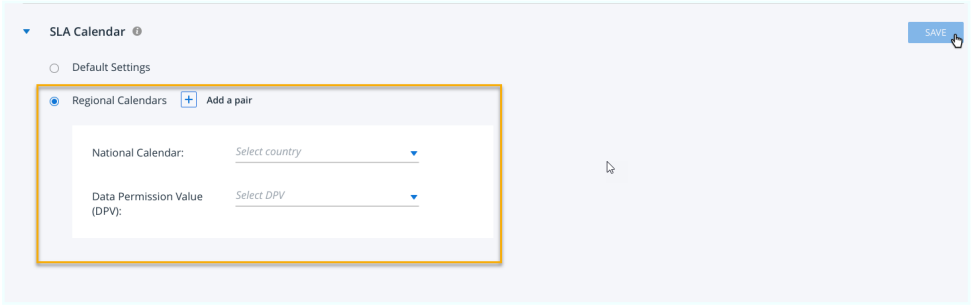


Figure 77: *Example Initial Selection to Add a Country / DPV pairing*

2. Select the Regional Calendars to deselect the default settings and begin the process to add a paring configuration.
3. Click the Add a Pair + icon.
4. Click the Select country drop down menu.

A country list is displayed as shown in the following example.

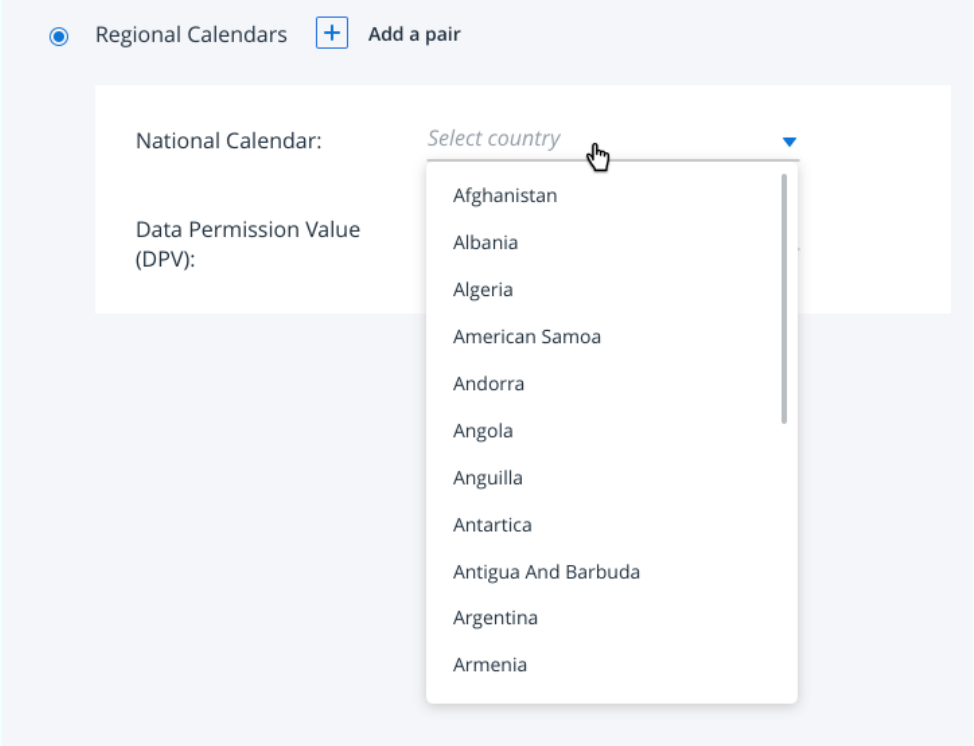


Figure 78: *Example National Calendar Country Selection from Available Options*

As an alternative to selecting the required country from the available list you can, where there are many countries in the list, use the auto complete function to search and display a country or countries that match the first few entered characters, as shown in the following example.

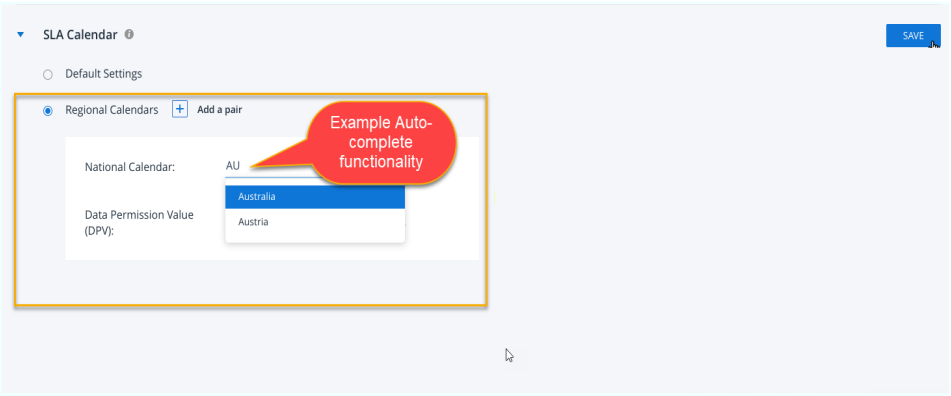


Figure 79: *Example Searching for a Country Using Autocomplete*

When the country is selected, selecting the DPV drop down menu displays all available DPVs included in the your specific deployment, as shown in the following example.

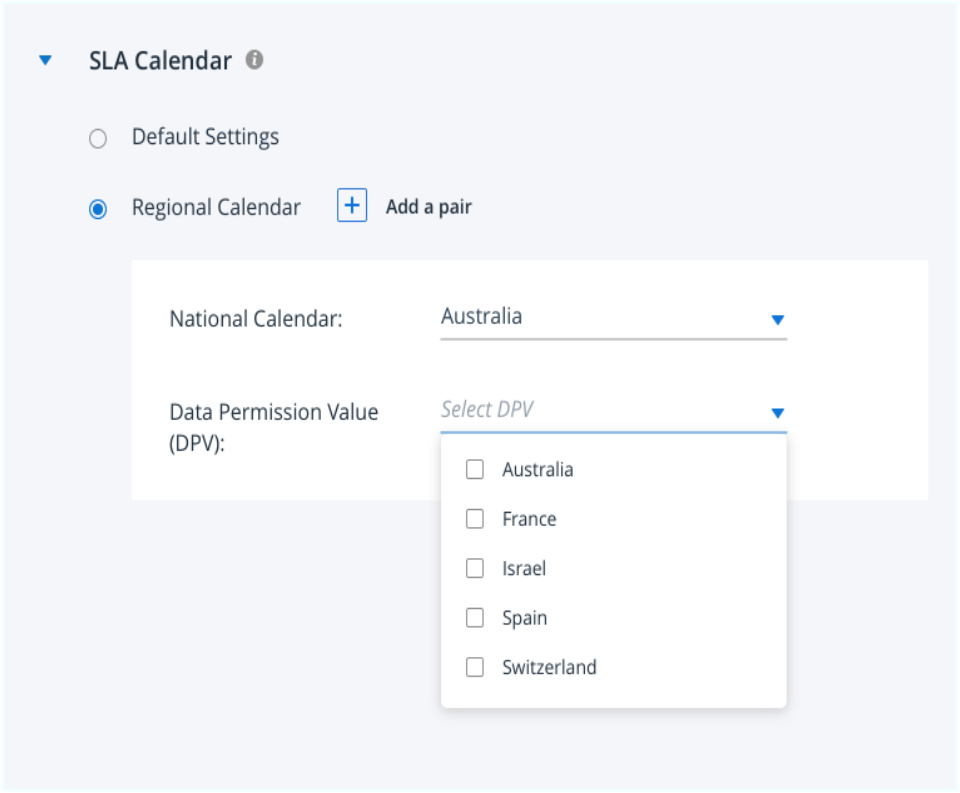


Figure 80: *Example Configuration Pairing of National Calendar with Multiple DPVs*

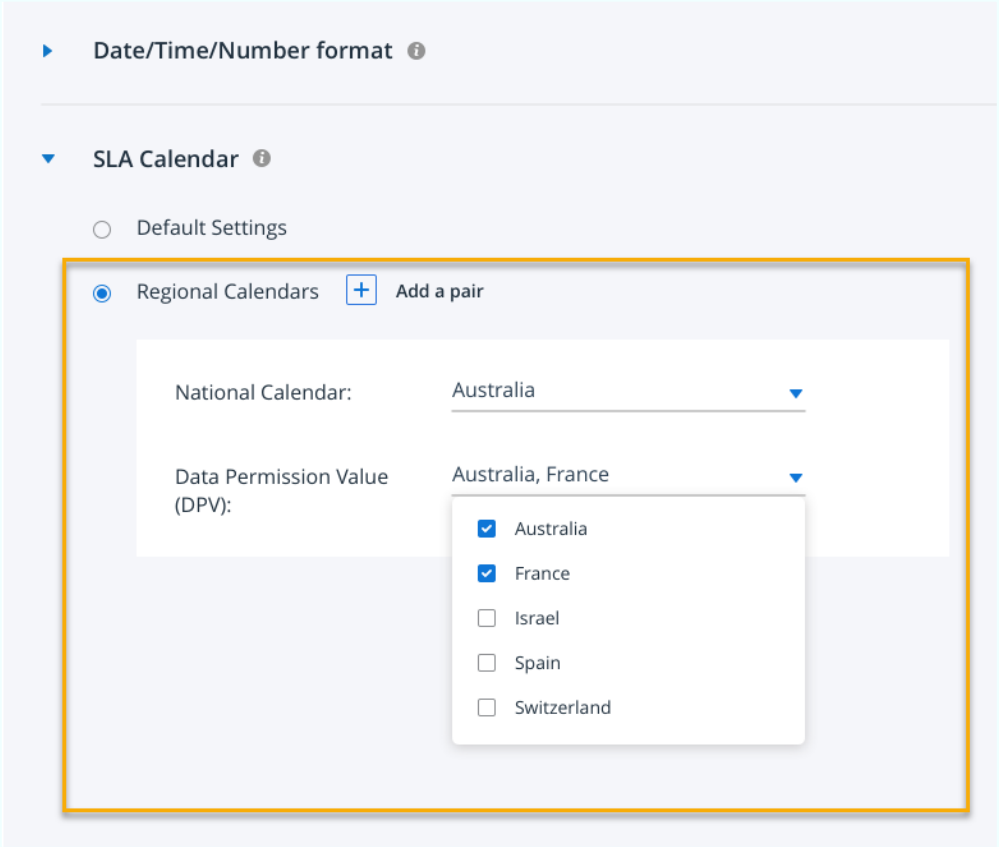


Figure 81: *Example of Configuring a Single Country - DPV Pairing*

It is also possible in large deployments that cover many countries and there are multiple DVPs, to configure multiple pairings, as shown in the following example.

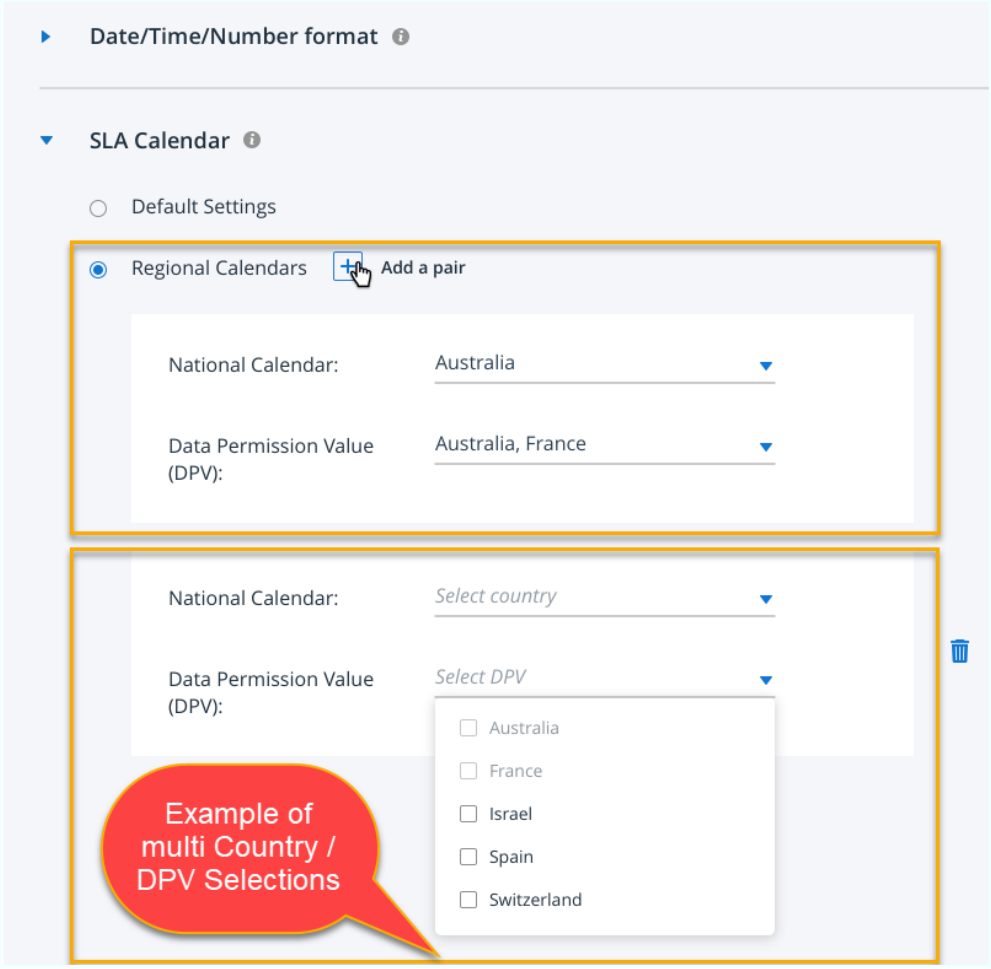


Figure 82: *Example of Configuring Multiple Country- DPV Pairings*

9.4. Operational Dashboard Configuration

This section of **General Settings** enables the various elements of the **Operational Dashboard** to be configured. At present these elements include:

- **Section Display tabs On /Off** - settings that control which operational dashboard tabs , and by association which widgets and data are displayed should be switched on or off.
- **Alarm Status Configuration** - settings that define alarm status values used in the Investigation Center Operational Dashboard BI module.

9.4.1. BI Dashboard - Display Tabs ON / OFF Switching

The display tabs on /off switching functionality in the BI and Trends modules is designed to allow each Thetaray client to control which BI and Trends elements to display depending on which data modules their deployment supports.

An example of a default settings screen is displayed below.

Some points to note on the designed BI and Trendsmodules layout and functionality

1. The on /off switching controls which tabs will be displayed on your Investigation Center BI /Trends modules
2. When a tab is made active or inactive the switching process is immediate so once modified, the user can navigate to the associated screen and verify the results of the switching modification.
3. As an aid to the setup process, the data origins are organized into two columns roughly dependent on alert classification:
   a. The left column contains:
      - ALL tabs - Enables all tabs to be displayed with one single setting
      - Transaction Monitoring Tab - Standard transaction alert monitoring (OOB)
      - Customer Risk Assessment Tab - CRA alerts (if licensed module included)

Note: ALL tabs relate to Transaction BI module only, TM, CRA, TS and CS are relevant for both modules.

---

   b. The right column is dedicated to the two Screening sections:
      - Transaction
      - Customer

To set alert origin BI and Trends tabs to on or off status:

1. Select Operational Dashboard tab in General Settings.
2. Click the Display On /Off dropdown arrow to display settings options:
3. Select the tab settings to suit your data type setup

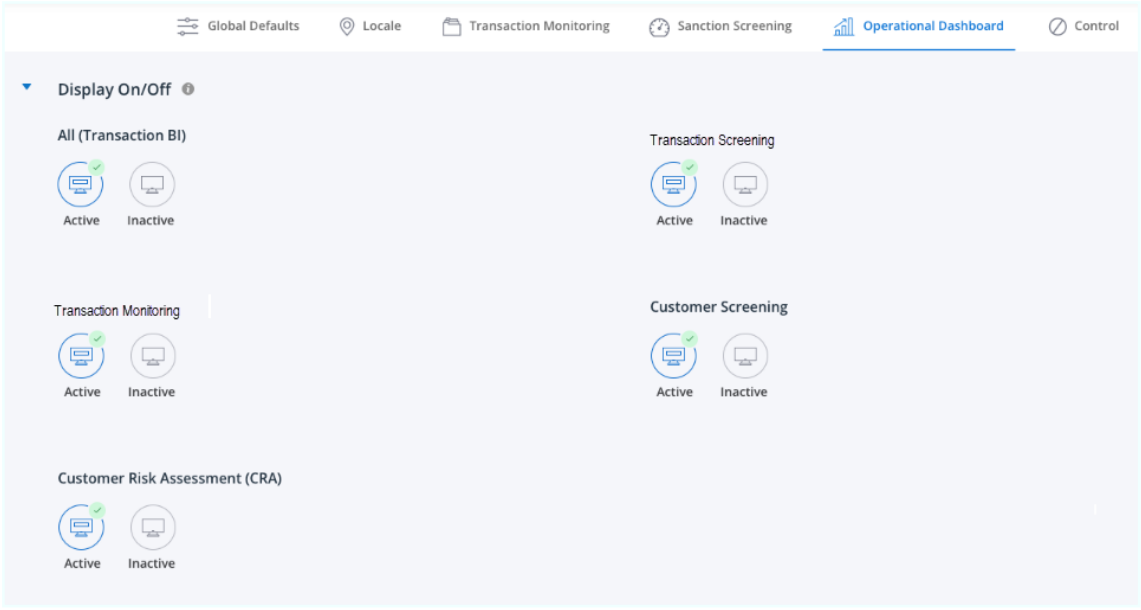
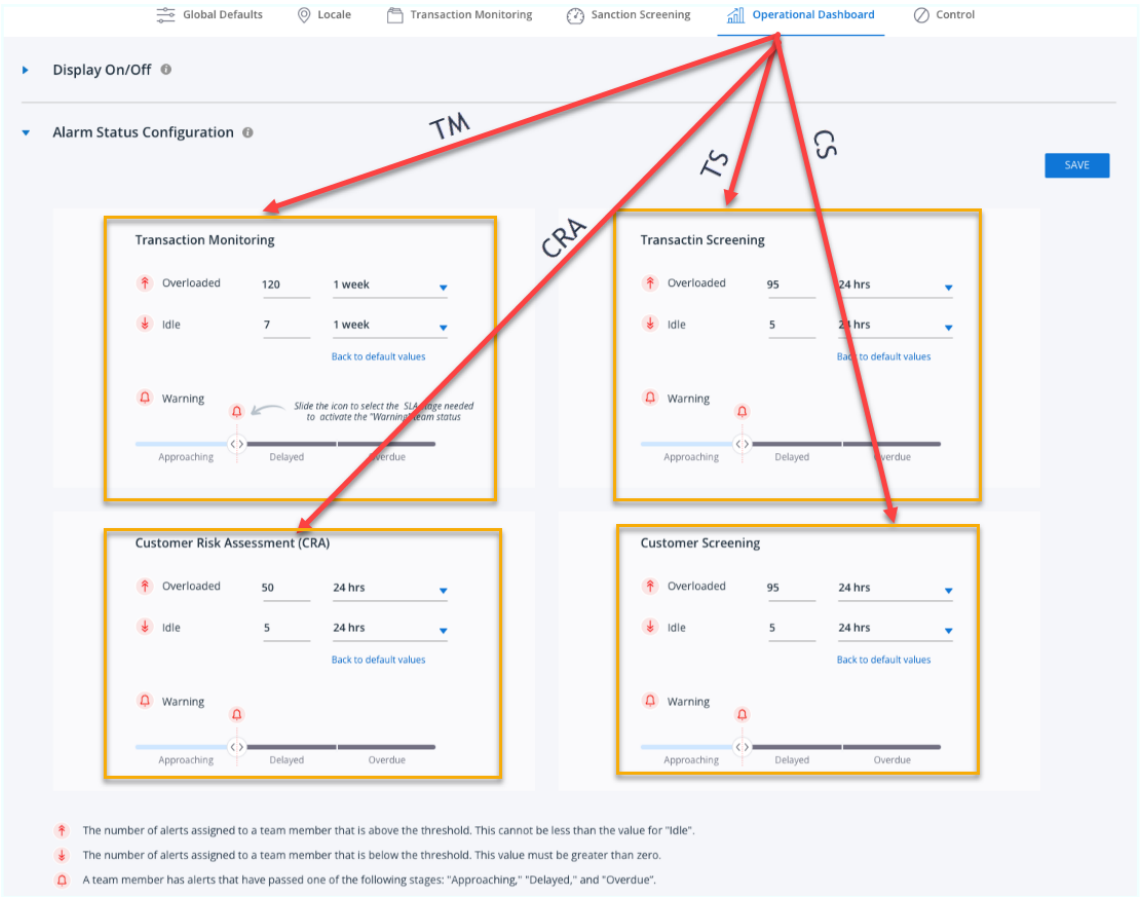


Figure 83: *Default BI Dashboard Display On/ Off Settings Screen*

Note: The list of alarm status for teams displayed for configuration depends on the active/inactive tabs per origin, setting as described in the above section.

On selection of this sub section module, the following example image is displayed:



In deployment, settings levels take default settings as shown in the following figure. This configuration section details how and what values can be applied.

9.4.2. Value Settings - Icons and Rules

Before configuring Alarm Status value settings in the Operation Dashboard Transaction BI module, note the following guidelines and rules:

- Customized settings can be made for the following types of sourced alerts:
  - Transaction Monitoring
  - Transaction Screening
  - Customer Screening
  - Customer Risk Assessment

There are three alarm statuses associated with the above alert types handled by team members:

- Overloaded
- Idle
- Warning

The following tagged icons and rules apply:

- ( ) Overloaded -The number of alerts assigned to a team member that is above the threshold. This cannot be less than the value of 'Idle'.
- ( ) Idle - The number of alerts assigned to a team member that is below the threshold. This value must be greater than zero.
- ( ) Warning - A team member has alerts that have passed one of the following stages: 'Approaching' , 'Delayed' and 'Overdue'.

To set values for 'Overloaded' and 'Idle ' statuses:

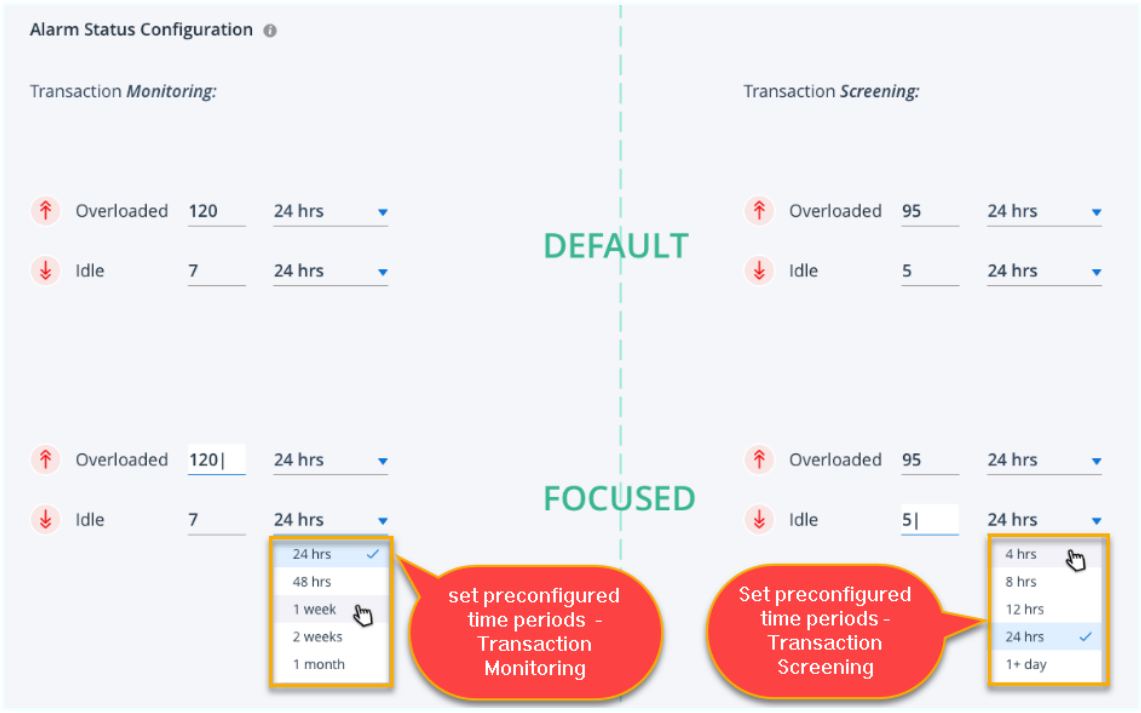


Figure 84: *Example Showing Configuration for TM Alerts, other Alert Categories are Configured Similarly*

Note: If required to revert back to default settings, click the link(s) displayed in the following figure.

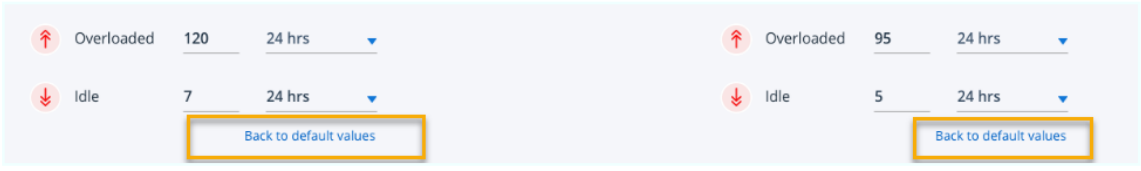


Figure 85: *Back to Default Value Links*

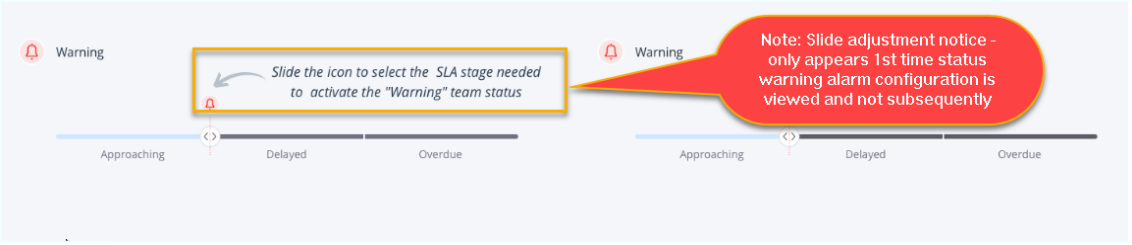
9.4.3. Warning Icon Configuration

The Warning icon can be configured to display in one of three SLA stages (for both Transaction Monitoring and Transaction Screening).

- Approaching, Delayed and Overdue
- Delayed and Overdue
- Overdue

As you will see when you configure this setting, removing 'Overdue' is not an option.

Note: The first time the warning icon is configured an instruction notice is displayed. On subsequent opening of the alarm status section, it is not displayed.



1. If required to custom configure the warning SLA 'bell' status, slide the bell to the required stage.

9.4.4. Saving Settings

Some Alarm Status configurations require setting metric values, 'SAVE' is required when complete.

Note: Save will not complete if there are configuration errors. Refer to the list of additional configuration rules/ troubleshooting error message notes listed below, modify settings and retry.

9.4.5. Error Message Troubleshooting

1. The difference between the 'idle and Overloaded' stages, must be at least 2 units such that they cannot be configured as 10-11, 120-121, etc.
2. The value for 'Overloaded' cannot be less than the value for 'Idle'.
3. The value for 'Idle must be greater than zero.

9.5. Consolidation

The process of consolidating related alerts helps reduce the overall alert investigation workload by just displaying the original risk.

Additional discovered alerts which are related by a common entity and which may be important as forensic evidence, are also made available to the analyst in the Risk Details panel as shown in the following example below.

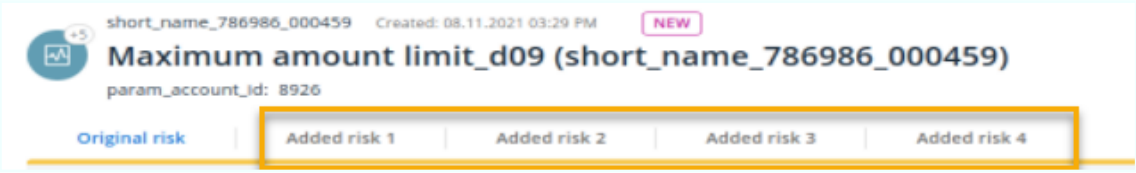


Figure 86: *Example displayed Consolidated Alerts*

To maximize investigation efficiency each use case may require a different maximum number of consolidated alerts available for further viewing.

The IC admin user / Data Scientist, who have a good knowledge of the specific use case and deployment, is required to set this maximum value.

9.5.1. Consolidation Tab Alert Value Setting and Consolidation by State

The consolidation value setting sets the maximum number of consolidated alerts that will be displayed in the Alerts Risk Details screen and thus provides a more precise definition for existing and new alerts.
This enables the analyst or supervisor to further drill down and investigate the alert under suspicion by examining the details of listed consolidated associated alerts. Consolidation by workflow and state provides the admin user with further fine control of the alert consolidation process by enabling the selection of specific workflow states to introduce alert /risk consolidation.

9.5.1.1. Pre Consolidation Considerations

Before configuring the consolidation level there are some important points to bear in mind:

1. When a user selects certain states of the workflow to apply consolidation these settings, will only be consolidated into newly created only when the next dataset batch is processed and published into IC.
2. Existing alerts that have already been consolidated are not affected by the change in the configuration setting.

9.5.1.2. Conditions for consolidation:

- Same entity / primary identifier
- A different risk
- Alerts must be open and not in the closed state

To set the maximum level of displayed consolidated alerts:

1. Click the Consolidated tab (1).

The following screen is displayed.

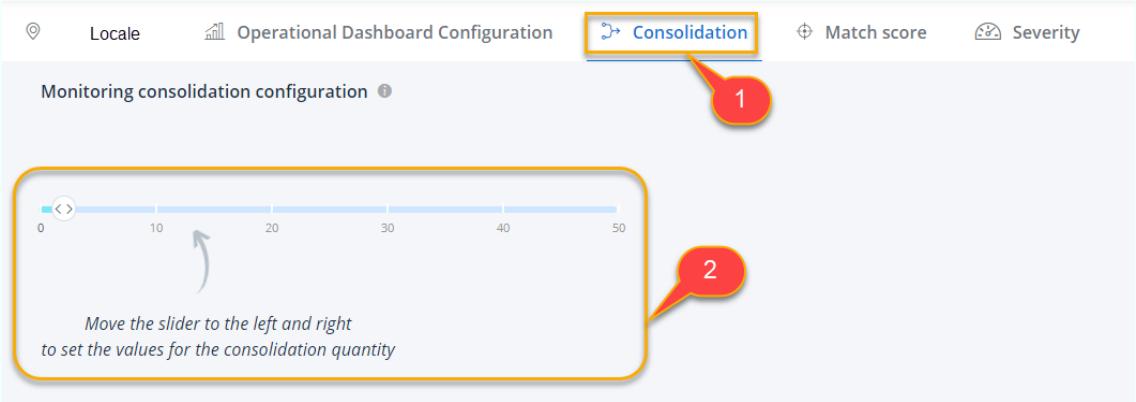


Figure 87: *Setting the Consolidation Level*

2. Adjust the slider to set the maximum value(2).

Note: Maximum configurable value is 50.

The admin user (with appropriate permission) can additionally manage alert consolidation settings by workflow state.

Configuring Consolidation by Workflow State:

Selecting to consolidate alerts in a specific state or states per workflow, is a simple task, as shown in the following example images and steps detailed below.

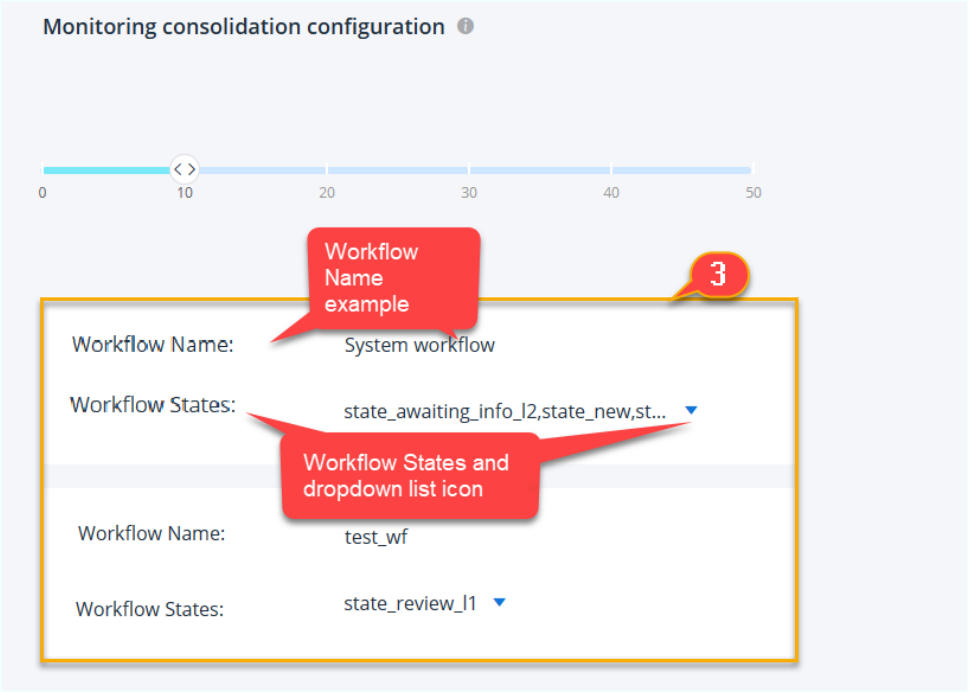
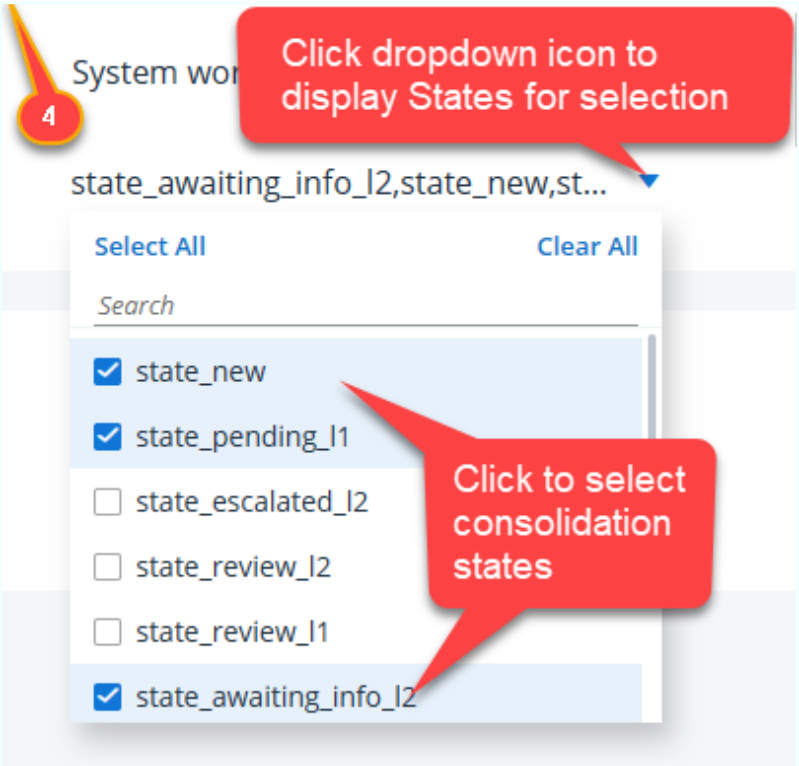


Figure 88: *Example Consolidation by State per Workflow - Initial Screen*

1. To start configuration, click the Dropdown icon as highlighted (3).
2. Click to select state(s) to consolidate alerts by per workflow (4).



The following points should be noted:

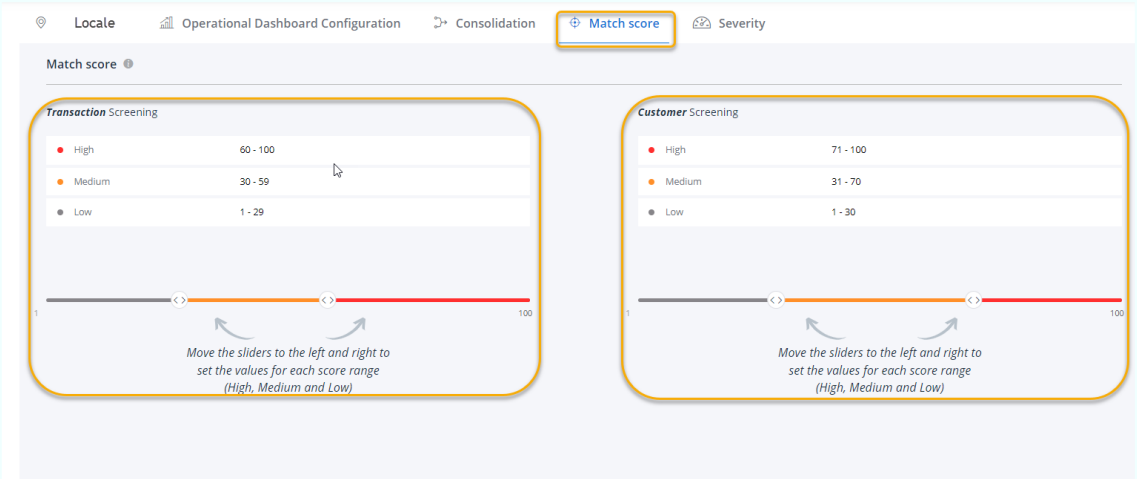
- There is no consolidation for the state "Closed" (reason for non inclusion in the dropdown menu)
- This configuration menu is not be displayed if a user indicates "0" alerts/no consolidation in the Monitoring consolidation slide bar configuration
- When a user moves an alert to another queue linked to another workflow, the alert continues to use the old workflow until it is resolved (closed)
- Only newly created alerts/risks are affected by the configuration, existing alerts are not
- Be aware that if no selections are made then **ALL** states are selected
- Only new risks of the existing consolidated alerts will be affected by the configuration.

Note: Saving settings is automatic when the user navigates away from the ***Consolidation*** tab.

9.6. Match Score

Match score configuration (where the screening solution is deployed) enables the definition of what represents a high, medium or low match score.

1. Clicking the *Match score* setting tab in **General Settings** displays the following example configuration screen.



2. Slide the <> arrows to the left and right to adjust the required values.

Note: Saving the configuration is automatic when you quit General settings.

Note: Further changes in Match score values can be made at any time.

9.7. Severity Score

Alert severity is measured by two parameters:

- **Category** - High, Medium, Low and Unclassified
- **Score** - A numerical range that indicates the degree of severity within each category

The default score values per category are as follows:

- High: 60 -99
- Medium: 30 - 59
- Low: 1 - 29

These values can be adjusted to meet the individual requirements of ThetaRay's customers.

To adjust the score range of each Severity category:

1. Verify the user has the appropriate admin role(s) set in User management application.
2. Click the Severity link in **General Settings**

The severity adjustment configuration widget is displayed as shown in the following figure.

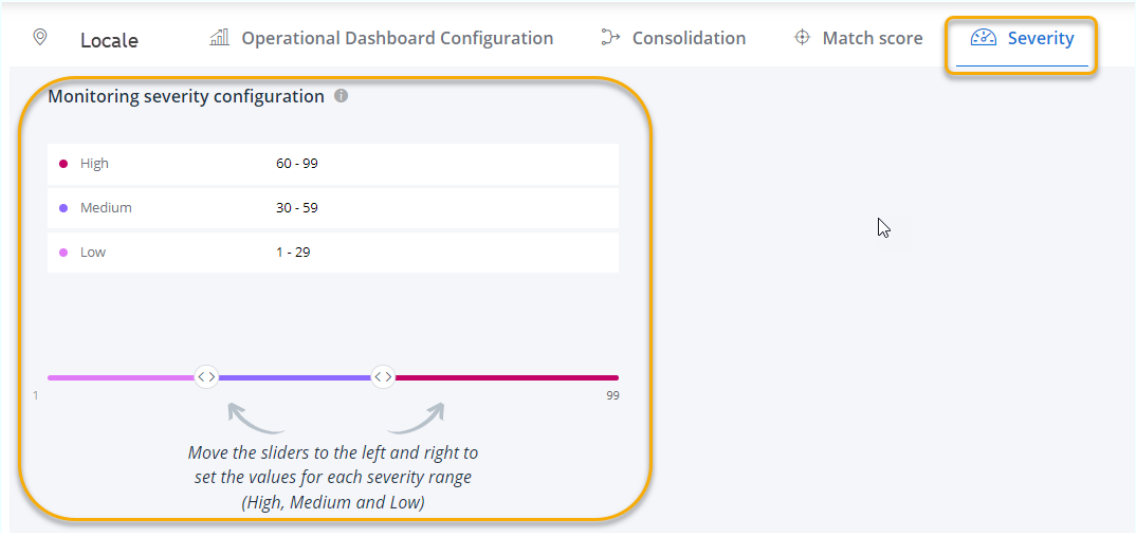


Figure 89: *Severity Score Adjustment Widget*

3. Slide the <> arrows to the left and right to adjust the required values.

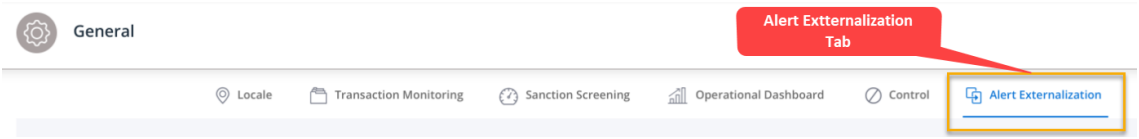
That's all, although changes in the IC module, will not be seen until a new batch of alerts updates the alerts list.

Note: Further changes in score values can be made at any time.

Note: Saving the configuration is automatic when you quit **General Settings**.

9.8. Alert Externalization

Following the Severity tab the Alert Externalization is next.



Alert Externalization in the General Settings, deals with managing alerts that are handled by customers using a 3rd party Case Manager instead of the default ThetaRay built in Case Manager.

In such a scenario, access to various services provided case managers is handled by a configured API. As a security compliance requirement, using a service requires either a password or API key to be encrypted.
Working with the API involves setting various parameters in the mappers configuration, section as described and shown here.

9.8.1. Adding Parameters Set

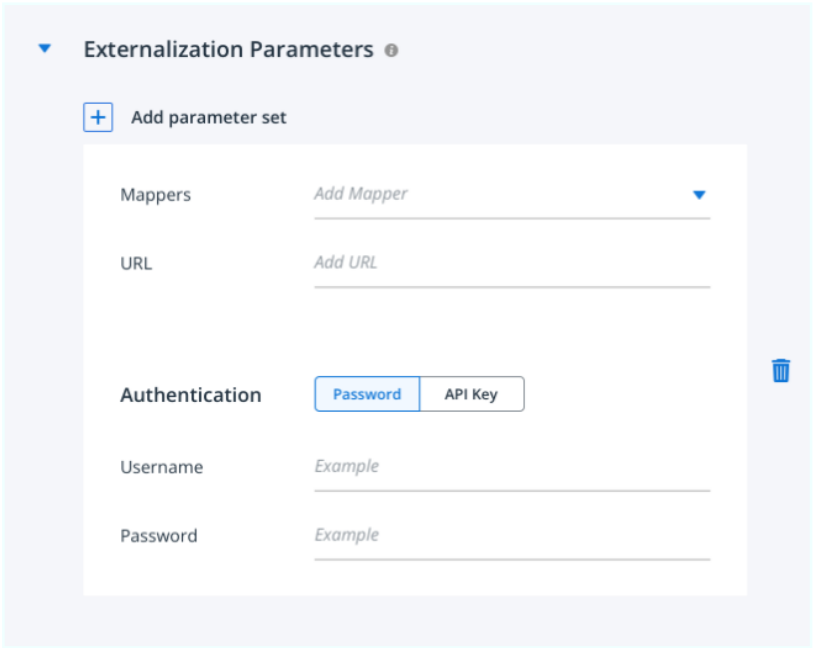


Figure 90: *Example - Add new parameter*

To add a parameter set:

1. Click the plus + icon
2. From the Add Mapper drop down menu, select a mapper or mappers to be appended with the parameter set.

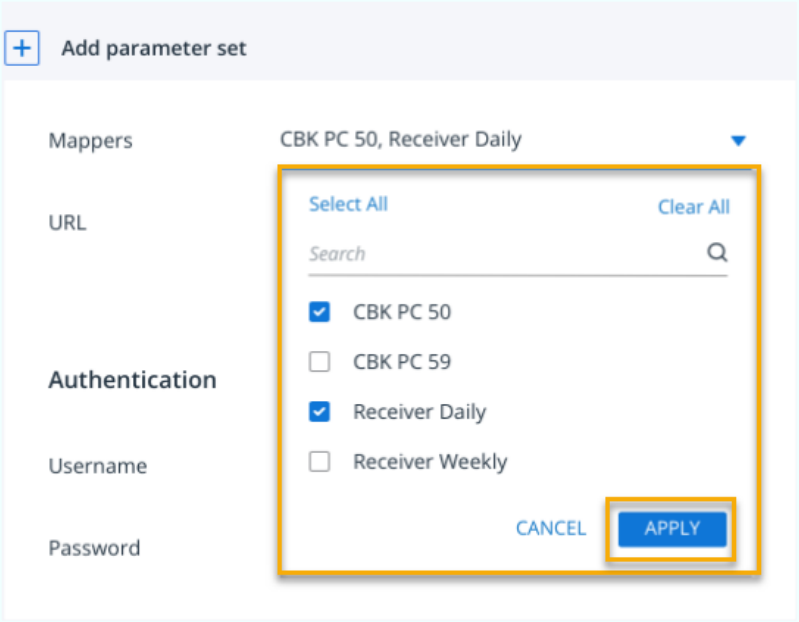
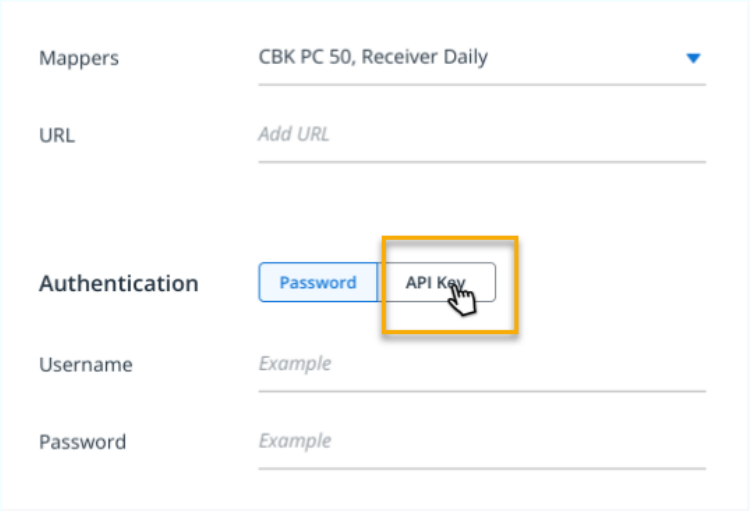


Figure 91: *Example Select Mappers from Dropdown Menu*

3. Click, **APPLY**
4. In the URL field enter the 3rd party Url.
5. If using password authentication, enter your Username.
6. If you wish to gain access to the service via the API Key click the API key option.



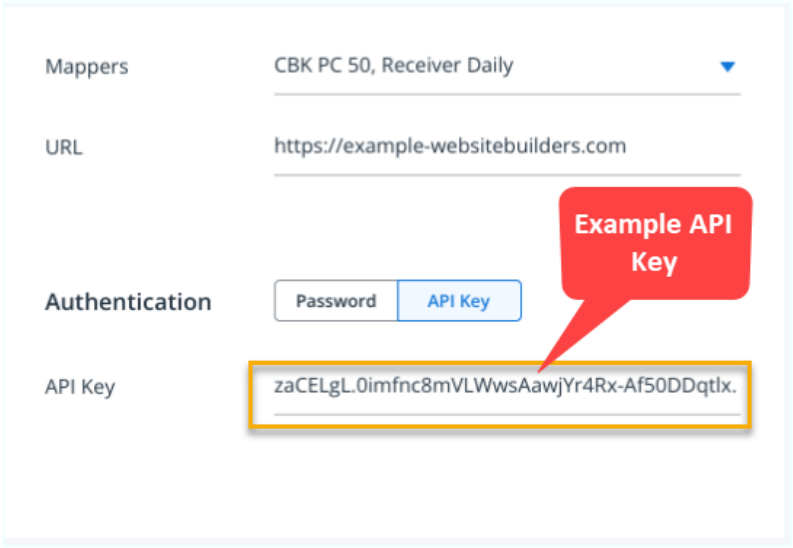


Figure 92: *Example Using an API Key for Access*

7. Enter a valid password.
8. Click Save when complete.
9. If it is required, you can delete a parameter set by clicking the **Delete** icon.

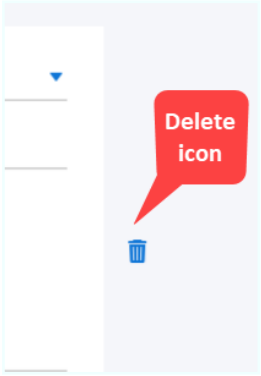


Figure 93: *Delete (Trash Bin)*

10. Export / Import

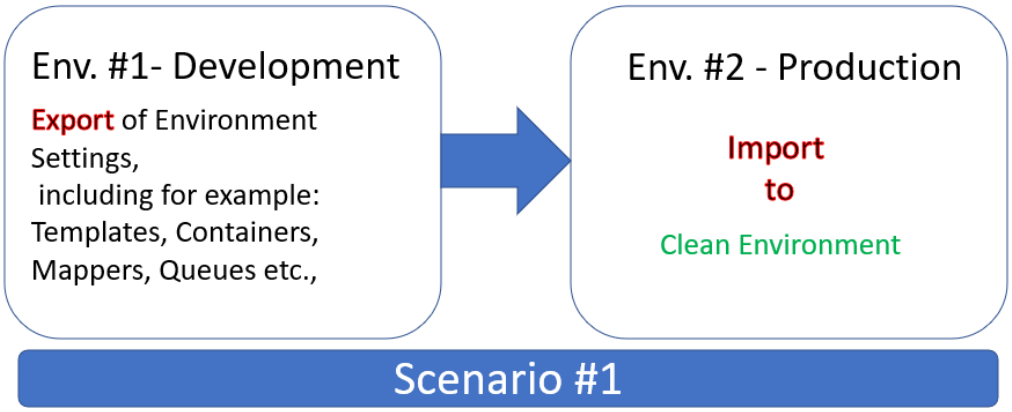
10.1. Introduction

The Export / Import facility in Investigation Settings at its core provides system admin with the ability to move all definitions made from environment to environment without the need to redefine settings from scratch, saving resources and preventing human errors.

In summary, It enables exporting and importing IC configurations and user management entities.

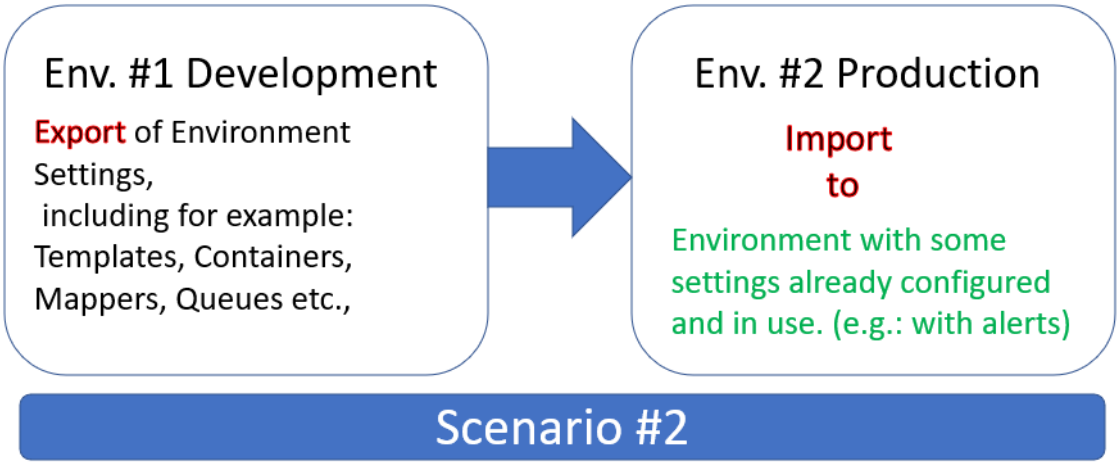
When exporting and importing, there are two possible export - import scenarios:

1. Exporting from an environment, for example a development environment that has been tested and is now ready for deployment in a new clean environment.



This is by far the most straight forward method of moving settings between environments.

2. Exporting from an environment, for example a tested development environment and it's now required to transfer the settings to an existing production environment that already contains set IC entities perhaps with active alerts.



This method , if carried out correctly is also straight forward. However, before you attempt to export and import settings as shown in scenario #2, it is important that we fully understand whats going on 'under the hood' when exporting / importing.

10.1.1. Uniqueness issue

If the destination environment already contains an entity with name X and identifier Y and the import also includes entities with the same name and different id, (meaning that the entity was created manually via the UI), the import will fail.

Example case
To highlight a possible issue that can occur in scenario #2, let' s take for example the case where we have an IC Queue named ***high_ severity*** created in the source environment. The queue not only has this name but also an identity id.
In the recipient environment there is also an IC Queue named ***high _severity***. Both entities were created manually, and as such, both were tagged with unique system identity ids. Being unique, these identities will not match and the outcome when attempting to import settings, will be import failure.

Warning: When working on building a test development environment with the intention of exporting finally tested settings to an existing production environment, bear in mind the above example, plan ahead, and do not manually create entities in your production environment.

10.1.2. IConfigurations Export/Import Entities:

- IC Templates
- IC Data Containers
- IC Mappers
- User Attributes

- Queues
- Workflows
- Forms
- Custom views
- Layouts

User Management Export/Import Entities:

- Users
- User Roles
- Teams
- Data Permission Values
- Roles (including composite roles)

10.1.3. Additional Info and Limitations

Specific to Import - be aware of the following:

- Upon import, if the entity does not exist in the destination - it will be created.
- Upon import, if the entity does exist in the destination - it will be updated.
- Not all changes are acceptable by import and if attempted my result in import failure

---

Note: As a rule of thumb: if something is not editable via the UI of the IC settings, it is also not supported as part of the import process.

- For example - primary keys of a template cannot be changed
- Some entities depend on others, for example - a mapper expects a template and an analysis to exist. If they don't (e.g. if a mapper is imported and it misses the template it expected import may fail)
- Keycloak updates are not transactional and therefore should first be checked before import is attempted
- An entity can only be removed if it could have been removed via the UI. For example - a queue with alerts, cannot be deleted
- The recipient site must share the same namespace as the source site
- As the export /import process transfers only the meta data and not the actual data itself, then the recipient site must have access to the same datasets as that held in the source site

10.2. Accessing Export / Import

From the Investigation Settings side panel click the Export / Import Icon as highlighted in the following figure.

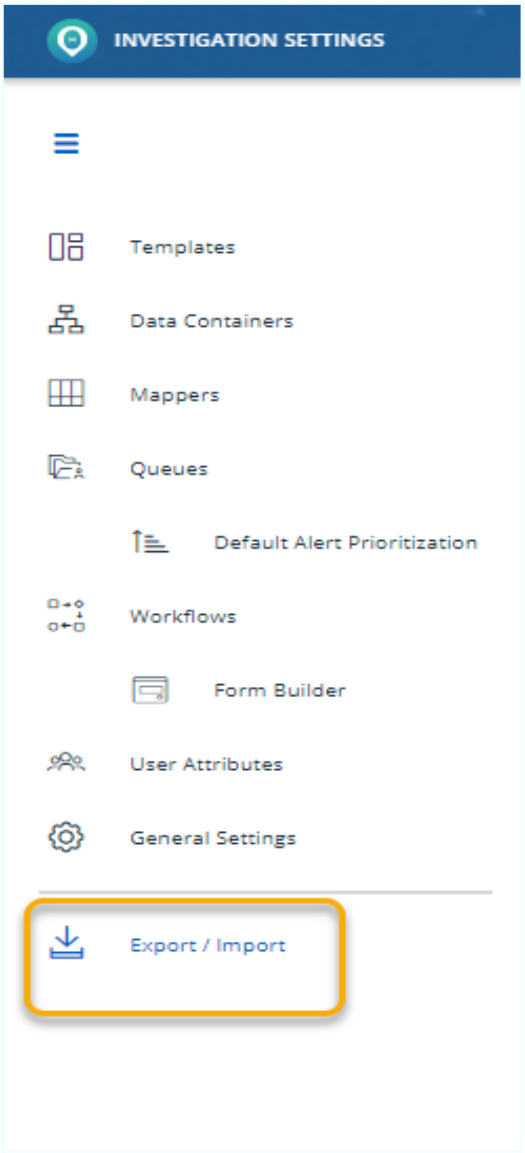


Figure 94: *Export Import Select Link in Investigation Settings Side Panel*

The Export /Import configuration Screen is displayed as shown in the following figure.

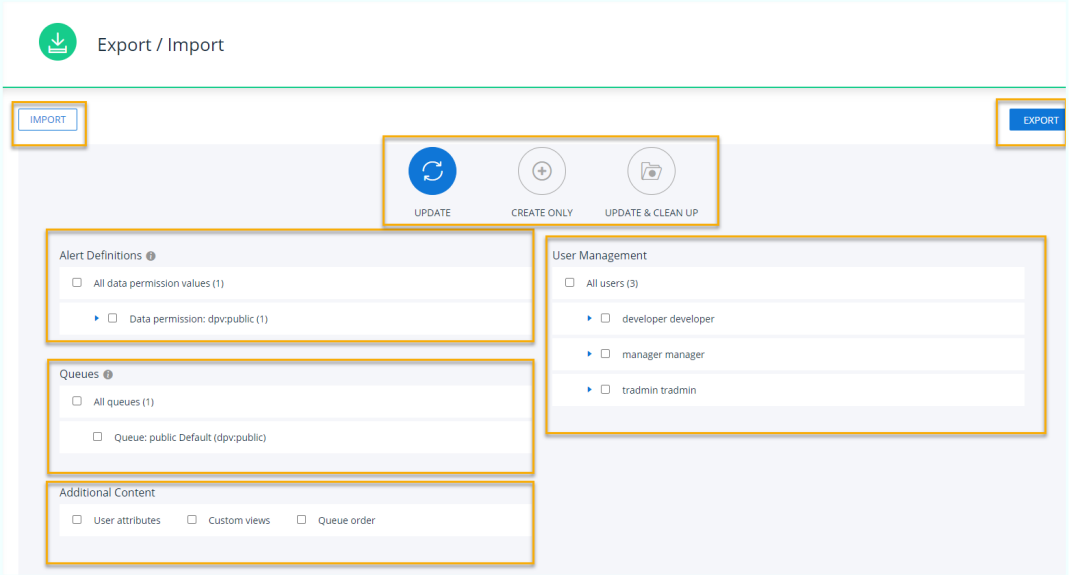


Figure 95: *Example -Export Import Configuration Screen*

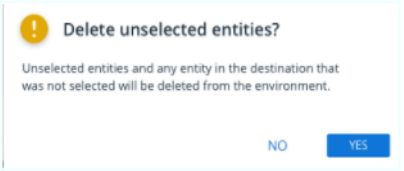
10.3. Exporting

By default , the Export / Import configuration screen displays the Export option (2).

If required to change to Import, click the Import link

3. To configure the export set up:
    a. Select the export mode required(3):
        i. Either to *update* an already exported package, or
        ii. *Create* a new export package, or
        iii. Update and perform a clean up operation to remove unselected entities.

Note: If update and perform clean up is selected, the following confirmation popup is displayed for verification:



    b. Under the *Alert Definitions* block, select to export the dpvs required.
    c. Under the *Queues* block, select to export the queues to export .
    d. Under the *Additional Content* block , and if required, select to include:

i. User Attributes
ii. Custom Views
iii. Queue order

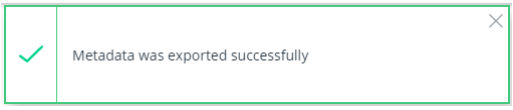
e. Under the User Management block , select to:
i. Include all users and all roles *or,*
ii. Individual users and selected roles,

4. When the export configuration is complete trigger export and download the export package by clicking the **Export** button

---

Note: Export is verified by a successful metadata export message as shown in the following example

---



On success the export file is downloaded to your Downloads folder.

5. Copy the downloaded exported package file:
   a. First to a local folder, and then subsequently to :
   b. A folder in the destination computer, for importing.

An example of an exported file (part) is shown in the following figure.

```
{
  "importType": "CREATE",
  "alertMappers": [
    {
      "id": null,
      "name": "sanity_mapper_8ba_07_27_09",
      "dataPermission": "dpv:public",
      "identifier": "1636874829548",
      "solution": "harveybe_product1233",
      "alertTableName": "tr_alert_table_1636874829548",
      "template": {
        "id": 1,
        "identifier": "91400adc-f15d-434c-b4f8-08e8281a1802",
        "name": "sanity_template_8ba_loan",
        "alertTemplateConfigurations": [
          {
            "id": null,
            "version": 1,
            "alertFields": [
              {
                "identifier": "param_account_id",
                "displayName": "param_account_id",
                "type": "PRIMARY",
                "summaryPosition": null,
```

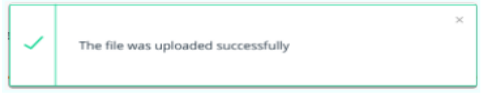

Figure 96: *Example (Partial) Exported file (XML)*

10.4. Importing

Once the export configuration file has been copied to the recipient computer it can be imported as follows:

1. Access the IC settings in a similar fashion as in the export function.
2. Click the *Import* button (1).

The file explorer opens to allow you to search for the exported JSON file.Search for the exported data JSON file and select it to initialize the import process. A successful import is confirmed by the following message:



10.5. Troubleshooting Unsuccessful Imports

In the event that the import was not successful, an error message is displayed along with information on the issue and where possible, some useful resolution tips.

For example failure to import may throw the following error message:

```
Queues with name(-s) {0} found with another identifiers
```

Solution:

1. Refer to Uniqueness issue and example use case detailed under the Introduction section of this chapter to better understand the root cause of the issue.
2. To correct the issue: remove the entity in the recipient environment and and then retry export /import.
3. If the issue still remains, contact *Customer Support.*

The following table details the range of fail messages:

Result Type	Micro-Copy - Possible Message Texts
Toaster message - failure	*"Sorry, we could not upload this file. Try saving it in CSV format and upload again."*
	"An unexpected error occurred while uploading this file. Please try again later."
	"The file is damaged and cannot be uploaded. Please try fixing it and upload it again."
	"Sorry, the file could not be uploaded. The number of rows does not match the predefined format."
	"Sorry, the file could not be uploaded. The number of columns does not match the predefined format."
	"Sorry, the file could not be uploaded. The name "valueX" does not exist. Please fix row "X"."
	"Sorry, the file could not be uploaded. There is a duplicate usage of name "valueX" in the column "Name". Please check rows "X" and "Y"."
	"Sorry, the file could not be uploaded. The value in the column "Status" does not match the required "Active or Inactive" entry. Please fix row "X"."
	"Sorry, the file could not be uploaded. The reference field name "fieldX" does not exist in the indicated reference. Please fix row "X"."
	"Sorry, the file could not be uploaded. There is a duplicate usage of reference field name "fieldX". Please check rows "X" and "Y"."
	"Sorry, the file could not be uploaded. The correct format of entries for "Link values" is "value1:linkedValue1|value2:linkedValue2|". Please fix row "X"."
	"Sorry, the file could not be uploaded. There is no such value "valueX" in the field "fieldX". Please fix row "X"."
	"Sorry, the file could not be uploaded. Entries for "Link values" only apply to "BOOLEAN" and "CODE" fields. Please fix row "X"."
Under the field message - failure	*"Please select a reference from the dropdown"*