



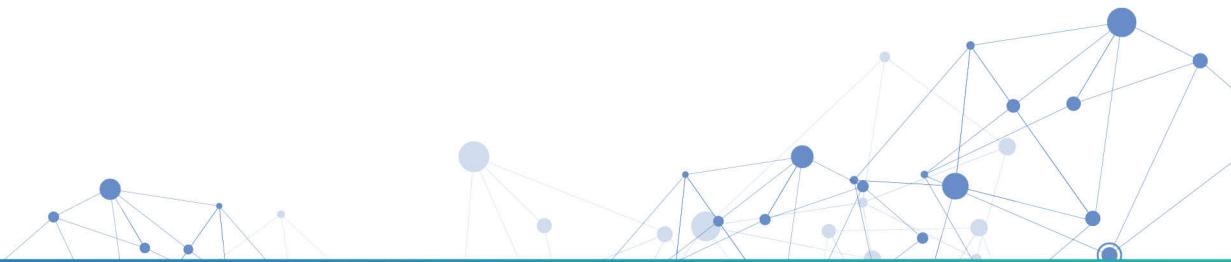
Version
6.13

Financial Crime Compliance Suite

INVESTIGATION CENTER

User Guide

Revision A



Legal Notice:

This document is proprietary & confidential and may only be used by persons who have received it directly from ThetaRay LTD. ("ThetaRay") and may not be transferred to any other party without ThetaRay's express written permission. The document provides preliminary and general information only and is not intended to be comprehensive or to address all the possible issues, applications, exceptions or concerns relating to ThetaRay. All information contained in this document is confidential and shall remain at all times the sole property of ThetaRay. The recipient of this document has no right to disclose any or all of its contents or distribute, transmit, reproduce, publicize or otherwise disseminate this document or copies thereof without the prior written consent of ThetaRay, and shall keep all information contained herein strictly private and confidential. The information is intended to facilitate discussion and is not necessarily meaningful or complete without such supplemental discussion. Please note that the information procedures, practices, policies, and benefits described in this document may be modified or discontinued from time to time by ThetaRay without prior notice. As such, ThetaRay provides the document on an "As-Is" basis and makes no warranties as to the accuracy of the information contained therein. In addition, ThetaRay accepts no responsibility for any consequences whatsoever arising from the use of such information. ThetaRay shall not be required to provide any recipient with access to any additional information or to update this document or to correct any inaccuracies herein which may become apparent.

1. Accessing Investigation Center	18
1.1. Overview of the Alerts List - Landing Screen	19
1.1. Overview	22
2. Managing Alerts List	23
2.1. Alerts List Screen Views	23
2.2. Custom Views	25
2.2.1. Creating Custom Views	26
2.3. Creating a Custom View	27
2.3.1. Editing Custom Views	28
2.4. Working with Custom Views - Additional Notes	29
2.5. Alerts List Screen Filters - By Category Type	29
2.6. Filter Use by Category Type	31
2.6.1. Main Category	31
2.6.1.1. Assignee	31
2.6.1.2. Filter by Assignee	31
2.6.1.3. Filter by Created Date	31
2.6.1.4. Filter by Created Date	32
2.6.2. Filter by Date Range	33
2.6.2.1. Filter by Origin	33
2.6.2.2. Filter by Queue	34
2.6.2.3. Filter by Resolution Code	35
2.6.2.4. Filter by Recommended Resolution Code	35
2.6.2.5. Filter by State	36
2.6.2.6. Filter by SLA Name	37
2.6.2.7. Filter by SLA Stage	38
2.6.2.8. Filter by SLA Status	39
2.6.2.9. Filter by Use Case	39

2.6.3. Monitoring Category	40
2.6.3.1. Filter by Consolidation	40
2.6.3.2. Filter by Severity	40
2.6.3.3. Filter by Relationship	41
2.6.3.4. Filter by Risk Category	42
2.6.3.5. Filter by Risk Name	42
2.6.4. Screening Category	43
2.6.4.1. Filter by Screening Match Score	43
2.6.4.2. Filter by Screening Source Messages	44
2.6.5. CRA Filters	45
2.6.6. CRA Analysis Type	45
2.6.6.1. Filter by CRA Analysis Type	45
2.6.7. CRA Inheritance Type	45
2.6.7.1. Filter by CRA Inheritance Type	45
2.6.8. CRA Risk Classification	46
2.6.8.1. Filter by Risk Classification	46
2.7. Alert Cards Functionality	47
2.7.1. Alert Card - SLA Calendar Settings Functionality	47
2.7.2. SLA Time Remaining Time Display	47
2.7.3. SLA Time Period - Standard Display	50
2.7.4. SLA Time Period - Alternative Display	50
2.7.5. Alert Changing State - Mandatory Note Creation Requirement	51
2.8. Editing an Alert Card	54
2.8.1. Alert State - Change	54
2.8.2. Assignee - Change	57
2.9. Bulk Alert Editing	57
2.10. Working with Bulk Editing Alerts	58

2.10.1. Multiple Changing Alert State	59
2.10.1.1. Bulk Assign to	59
2.10.2. Moving Alerts from the Default Queue to Another Queue	60
2.10.3. Troubleshooting - Bulk Editing	61
2.11. Bulk Download for TM, TS & CS Alerts (System & Manual)	62
2.11.1. Example Downloaded CSV TM Alerts File (Partial)	64
2.12. Example Downloaded System Created CS .csv Alerts File (Partial)	65
2.13. Example Downloaded Manually Created CS .csv Alerts File (Partial)	65
2.14. Example Downloaded System Created TS .csv Alerts File (Partial)	65
2.15. Sorting Alerts	66
2.15.1. Examples of Sorting Capabilities	66
2.15.1.1. Sorting by Alert ID - or Select from List by Ascending or Descending Order	66
Add Sort Field	67
2.15.2. Sort by Assignee	68
2.15.3. Moving the Order of the Sort Field	69
2.15.3.1. Screening Source Messages Sorting	71
2.15.3.2. Sort by SLA Attribute by Remaining Time	71
2.16. Viewing Alerts in Card or Table Format	71
2.17. Viewing, Filtering and Changing Alert State	72
3. Alert Investigation Workflow	73
3.1. Alert State Lifecycle Diagram - Example	74
3.2. Default Workflow	74
3.3. Investigation Center Module Header	75
3.4. Manual Alerts	76
3.4.1. Creating a Manual Alert	76
3.4.1.1. Create an Alert - Additional Information	79

3.4.1.2. Troubleshooting	80
3.5. Re-opening Alerts	80
3.6. Analyst's Workflow	81
3.7. Workflow - Mandatory Notes Completion Tasks	82
3.7.1. Autotext Templates Usage with Mandatory Notes Completion	82
3.8. Supervisor's Workflow	83
4. Alert Details	84
4.1. Tab Navigation Bar	84
4.2. Risk Details Default Tab	85
4.2.1. Alert Card Details	86
4.2.2. Risk Details Overview	86
4.2.3. Essential Evidences	87
4.2.4. Viewing Evidence Data in Table Format	87
4.2.4.1. Quick Transaction Search	88
4.2.5. By Alert Type	89
4.2.6. Viewing Evidence Data in Enlarged or Reduced Mode	89
4.2.7. Downloading Global Transaction Query Content	89
4.2.7.1. Viewing Transactions	90
4.2.7.2. Downloading Transactions	90
Current View Download	90
Custom Download	91
Download Process	91
4.2.7.3. Important Notes	91
4.2.8. Context Rows Query Results	93
4.2.9. Risk Resolution Alert Types and Available Layouts	94
4.2.9.1. Global Transaction Alert Layout Types	94
4.2.9.2. Feature Transaction Alert Layout Types	94

4.2.9.3. Global Layout	96
4.2.9.4. Personal Layout	96
4.2.9.5. Global Layout	96
4.2.9.6. Recent Layout	97
4.2.9.7. Editing a Layout	97
4.2.9.8. Adjusting what Data, and how Data is Presented in Transaction Tables	97
4.2.9.9. Viewing Table Data	99
4.2.10. Risk Details Default Tab (Redesigned)	100
4.2.10.1. Introduction	100
4.2.10.2. Analysis Methods	101
4.2.10.3. Consolidation	102
4.2.10.4. Color Code Legend	102
4.2.10.5. Alert Name and Transaction Date Range	103
4.2.10.6. AI Derived Alerts	103
4.2.10.7. Customer Insights	105
4.2.10.8. KYC & Risk Rating Widget	105
4.2.10.9. Geographical Activity Widget	106
4.2.10.10. Customer Activity Widget	107
4.2.10.11. Historical Alerts Widget	107
4.2.10.12. AI Alert Summary	108
4.2.10.13. Feature Distribution	108
Category Distribution	109
Feature Highlighting	110
Feature Widgets (Essential Evidences)	111
4.2.10.14. Feature Drill Down	113
4.2.10.15. Feature Summary	113

4.2.10.16. Transaction Table	113
Data Manipulation Options	114
Quick Transaction Search	114
4.2.10.17. By Alert Type	115
4.2.10.18. Viewing Evidence Data in Enlarged or Reduced Mode	115
4.2.10.19. Downloading Table Data Content	115
4.2.10.20. Context Rows Query Results	116
4.2.10.21. Risk Resolution Alert Types and Available Layouts	116
Global Transaction Alert Layout Types	116
Feature Transaction Alert Layout Types	117
Global Layout	119
Personal Layout	119
Global Layout	119
Recent Layout	119
Editing a Layout	120
Adjusting what Data, and how Data is Presented in Transaction Tables	120
Viewing Table Data	121
4.2.10.22. Rules Derived Alerts	122
4.2.11. Data Visualization Charts	124
4.2.11.1. Working with Data Visualization Charts	125
Viewing Data and Charts in a Variety of Display Formats	125
Selecting a Display Layout	125
Configuring and Displaying Visualization Charts	127
Selecting Chart Data	127
Selecting a Chart Type	128
Formatting a Chart Layout	130
Chart Formatting	130

Legend	130
Axis	131
Series	131
4.2.11.2. Chart Visualization - Actions Bar	131
Opening and Closing the Chart Menu	131
Downloading a chart in .png Format	131
Expanding selected Chart to Display Full Screen	132
Closing and Removing Created Charts	132
4.3. Alert Details - Custom Tabs	132
4.3.0.1. Viewing Available Custom Tab Customer Data	133
4.4. Risk Details Tab (Manually Created)	134
4.5. Document Tab	135
4.5.1. Document Tab Restrictions	136
4.5.2. Maximum Document Size Permitted in Upload	136
4.5.3. Supported File Extensions:	138
4.5.4. Adding Documents	138
4.5.5. Downloading Viewing and Detaching Documents	138
4.5.5.1. Examples of Viewing Document Types	141
4.6. Related Alerts Tab	143
4.7. Notes Side Panel	145
4.7.1. Notes - Add /Edit Limitations (Roles and Users)	145
4.7.1.1. Examples of Notes Restriction Notices	145
4.7.2. Narrative Text	147
4.7.3. Information/ Process Text	147
4.7.4. Adding New Notes	147
4.7.5. Filtering & Viewing Added Notes	150
4.7.6. Sorting Notes by Order	151

4.7.7. Marking / Unmarking Notes as Deleted	151
4.8. History Side Panel	152
5. Entity Resolution	154
5.1. Introduction	154
5.2. Accessing Entity Resolution Phase 2	155
5.3. Initial landing Screen Layout and functionality	155
5.3.1. Entity Resolution Landing Screen - Functionality Overview	156
5.3.2. Working with the ER Search and Relationship filter	156
5.4. PII Information Management- Mandatory / Optional Requirements Edits	157
5.4.1. Practical Example on Editing Party Address	158
5.4.2. Entity Locking when multiple Users Attempt to Edit PII Simultaneously	159
5.5. Selecting to View / Confirm all Entities for a matched Result	159
5.5.1. Important Points to be aware of when Confirming / Rejecting Matched Entities	160
5.6. Integration of ER Sourced Alerts Into Investigation Center	161
5.6.1. Entity Resolution - Examples of Alert Scenarios in Risk Details Tab	161
6. Operational Dashboard Transaction Business Investigation (BI)	166
6.1. Overview	166
6.1.1. BI and Trends Modules - Functionality Overview	167
6.2. Operational Dashboard - Transaction BI and Trends Modules	168
6.2.1. Transaction BI - Overview	168
6.2.2. Trends BI - Overview	170
6.3. Transaction BI Module - in Detail	173
6.3.1. DPV Select	173
6.3.2. Filters & Download Utility	173
6.3.3. Alert States Widget - Metrics	177

6.3.4. Transaction Monitoring Statistics Widget - Charts and Histogram ..	178
6.3.4.1. Top Risk Widget Data - Further Details	178
6.3.5. Transaction Screening Statistics Widget - Charts and Metric Views	179
6.3.6. Customer Screening Statistics Widget - Charts and Metric Views ...	180
6.3.7. Customer Risk Assessment (CRA) - BI Dashboard Examples	181
6.3.8. SLA Alert Statistics Widget	182
6.3.9. Team Members Widget	183
6.4. Trends Module - in Detail	185
6.4.1. Filter Widgets	185
6.4.2. Trends Example Widgets	187
7. The Case for Network Visualization	192
7.1. Accessing Network Visualization Module	192
7.2. Network Visualization (NV) - Key Module Components	194
7.2.0.1. Graph (Chart) Nodes and Edges	195
7.2.1. Graph Nodes and Edges	196
7.2.1.1. Types of Nodes	196
7.2.1.2. Displaying Alert Id Instead of Alert Name	197
Account and Party Entities - Non Alerted	197
7.2.1.3. Examples - Icon Tagging in Network Visualizations	198
Ability to View Party Accounts Detail on Hover	198
Tool Tip Info Displayed on Hover	199
Account Entity with Related Transaction Icon	199
Country of Origin - Tagged by Flag	199
Country of Origin + Consolidation Indication	200
Meaning of a Plus (+) Icon	200
Alerts Under an Account or Party Entity	201
Hovering on Alert Entity, Displays Alert Details	201

7.2.1.4. Node Size Related to Total Aggregated Amount Range	202
7.2.1.5. Edges	202
7.2.1.6. Direction of Transaction	202
7.2.1.7. Number of Alerts sourced by the Entity under Investigation ..	203
7.2.1.8. Alert Icon - Displayed, if Transaction is Suspected as Being a 'contributor' to Activity	203
7.2.1.9. Amount and Currency of Transaction	203
7.2.1.10. Number of Counter Entity Transactions	204
7.2.1.11. Tool tip / Details if Alert type is Manually Created	204
7.2.2. Controls and Settings Side Panel	204
7.2.2.1. Control Tab	204
7.2.3. Settings Tab	212
7.2.3.1. Auxiliary NV Functionality Components /Tools	212
Key Legend	213
7.2.4. Navigation Utility	214
7.2.5. Node Placement	216
7.2.5.1. Drag and Move Nodes Around Screen	216
7.2.6. Node Search	217
7.2.6.1. Searching for Graph Nodes	217
Node Transaction Direction Flow Select	220
7.2.6.2. Downloading screen graph segments	220
Download Current / Whole Chart View	220
7.3. Working with Network Visualization	222
7.3.1. Investigation Strategy with Network Visualization	222
7.3.2. Visualization Network - Practical Workflow Suggestions - (High level)	223
7.4. Troubleshooting	223

8. Rules Editor - Introduction	225
8.1. Rules Editor Workflow - High Level	225
8.2. Icons Used in the Manual	227
8.3. Editor Access and Initial Orientation	228
8.3.1. Access	228
8.3.2. Rules Editor - Landing Page - Overview	228
8.3.2.1. Rules View	229
8.3.2.2. Key takeaway at this stage:	231
8.4. Editing Rules Parameter Values	231
8.4.0.1. Step #1 - Choosing an analysis	232
8.4.0.2. Selecting a rule	232
8.4.0.3. Activate / inactivate rule	233
8.4.0.4. Editing parameter values	234
8.4.0.5. Suppression Period	234
8.4.0.6. Configuring Suppression	235
8.4.1. Analysis Status indication	235
8.4.2. Testing Evaluation Analyses on System and User Set Values	236
8.4.3. Download Full Results	237
8.4.3.1. Metadata file	238
8.4.3.2. Media file	239
8.4.3.3.	240
8.4.3.4. Applying New Parameter values	240
8.4.3.5. Resetting Values to System Settings	241
8.4.4. Rules Parameter Editor -Troubleshooting	242
8.5. Practical Workflow and Example Scenario	243
8.5.1. Example Test Scenario	244
9. Providing a Recommended Resolution & Closing the Alert	247

9.1. The Analyst Task	247
9.2. The Supervisor's Task	248
10. Browser Support and View Resolution	249
10.1. Browser Support	249
10.2. View Resolution	249
11. Customer Screening Module	250
11.1. Introduction	250
11.2. Overview	250
11.3. Purpose	250
11.4. Analyst's Screening Alert - Lifecycle and Workflow	250
11.4.1. Alert State Lifecycle	251
11.4.2. Alert Default Workflow	251
11.4.3. Whitelisted Call-back Screening Information	252
11.5. Accessing Customer Screening and Overview	252
11.6. Investigation Center - Customer Screening - Landing Screen	253
11.6.1. Customer Screening Landing Page Main Elements Overview	253
11.6.2. Returned Alert Hits Bubble Display Priority	255
11.7. Customer Screening - Managing Alerts	256
11.8. Screening - Relevant Filters	256
11.8.1. Screening Centric Filters	256
11.8.2. Filter by Origin Filter	256
11.8.3. Filter by State	257
11.8.4. Filter by Resolution Code	258
11.8.5. Sorting Alerts	258
11.8.6. SLA	258
11.8.7. Viewing Alerts in Card or Tabular Format	259
11.9. Tab Navigation Bar	259

11.10. Customer Screening Alerts Tab	260
11.10.1. Screened Customer Displayed Data Section - More Information	261
11.10.2. Identification Types	262
11.10.2.1. Individual type	262
11.10.2.2. Organization Type	267
11.10.3. Screening - Dynamic Matched Fields Highlighting	268
11.10.4. Name Match Highlighting in CRA Deployments	269
11.10.5. Additional Information on PEP Data	269
11.10.6. World Check Screening legal Notice Disclaimer	270
11.11. Alert Resolution Process	271
11.11.1. Closing Resolution State - Resolution Rule	273
11.11.2. Additional Info Availability - Post Resolution Stage	275
11.12. Source Messages - Customer Screening	276
11.13. Customer Manual Screening	278
11.13.1. Overview	278
11.13.2. Customer Manual Screening	278
11.13.2.1. Advanced Search Options	280
Search Results	280
Download Search Results	283
12. Adverse Media Screening Module	285
12.1. Adverse Media	285
12.2. Screening - Adverse Media (List Support)	286
13. Transaction Screening Module	292
13.1. Introduction	292
13.2. Overview	292
13.3. Purpose	292
13.4. Contents	292

13.5. Analyst's Screening Alert - Lifecycle and Workflow	293
13.5.1. Alert State Lifecycle	293
13.5.2. Alert Default Workflow	293
13.5.3. Whitelisted Call-back Screening Information	294
13.6. Accessing IC Transaction Screening Module	294
13.7. Investigation Center - Transaction Screening - Landing Screen	294
13.8. Tab Navigation Bar	297
13.9. Transaction Screening Alerts Risk Tab	298
13.9.1. Alert States	298
13.9.1.1. New State	298
13.9.1.2. On Hold State	298
13.9.1.3. Closing Resolution State - Resolution Rule	299
13.9.2. Working with the Screening Alert Resolution Process	299
13.9.2.1. Investigation and Resolution Process - High Level	300
13.9.2.2. Identification Types	301
Individual type	301
Organization Type	306
13.9.2.3. Event Sort by Function	307
13.9.2.4. Investigating Further Evidence	307
13.9.3. Alert Resolution Process	307
13.9.4. Event and Alert Closure Resolution	308
13.9.4.1. Requirement to Provide a Reason for Selected Resolution ..	308
13.9.4.2. Transaction Screening - Additional UI Information	311
13.10. Source Messages Tab - Transaction Screening	312
14. Customer Risk Assessment (CRA) User Guide	314
14.1. CRA Introduction	314
14.2. Purpose and Scope	314

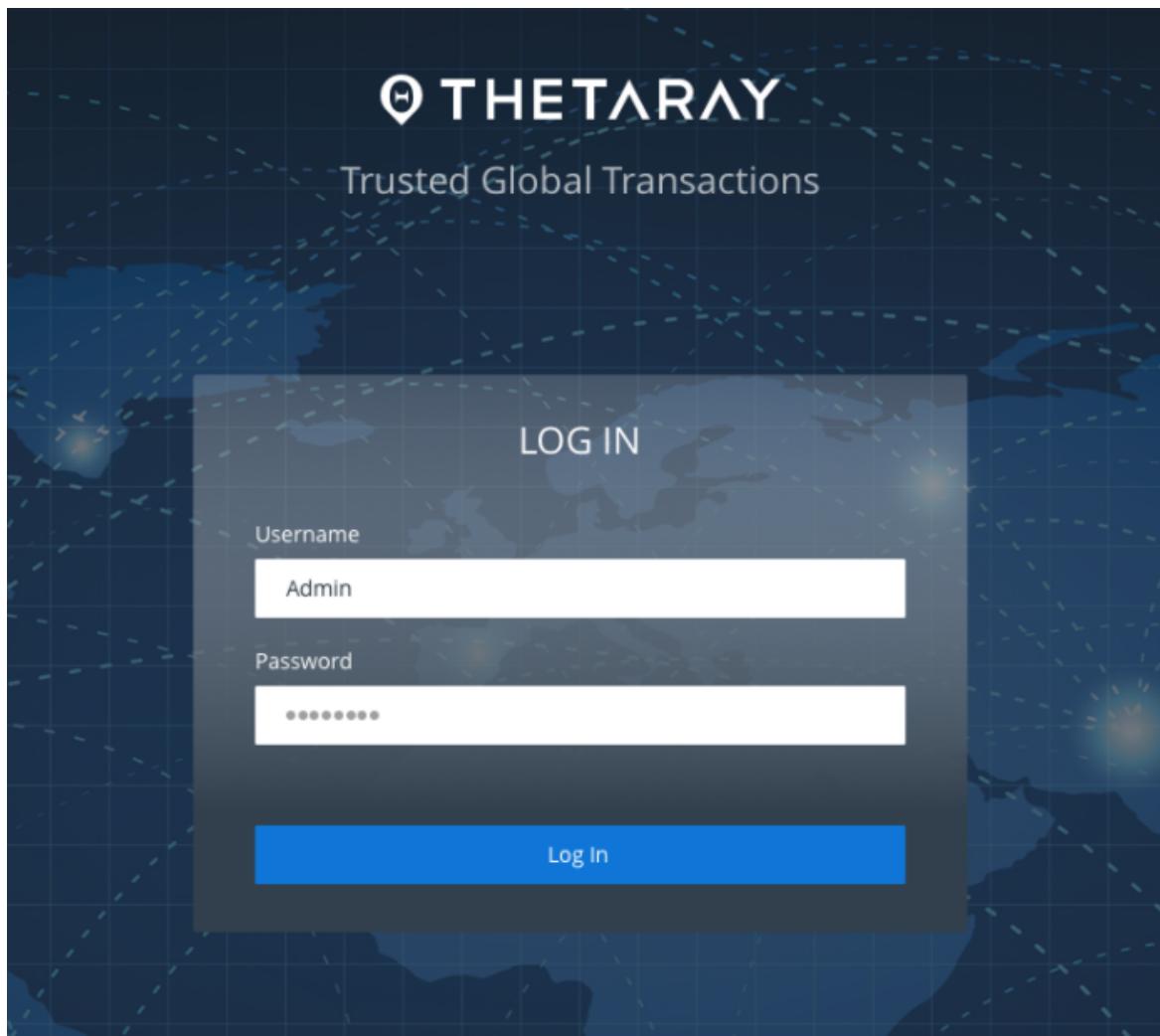
14.3. Customer Risk Assessment (CRA)- Reports	314
14.3.1. CRA Reports- Access, and General Functionality	315
14.3.1.1. Functionality Overview	315
14.3.2. Report Types	316
14.3.2.1. On Demand Reports	316
14.3.2.2. Automated Reports	316
14.3.3. CRA Reports Screen- Overview	317
14.3.4. Selecting Filters	318
14.3.5. Selecting to View Alerts Detail from Reports Module	321
14.3.6. Selecting Download Format & Downloading Reports	322
14.3.7. Troubleshooting CRA Reports	323

1. Accessing Investigation Center

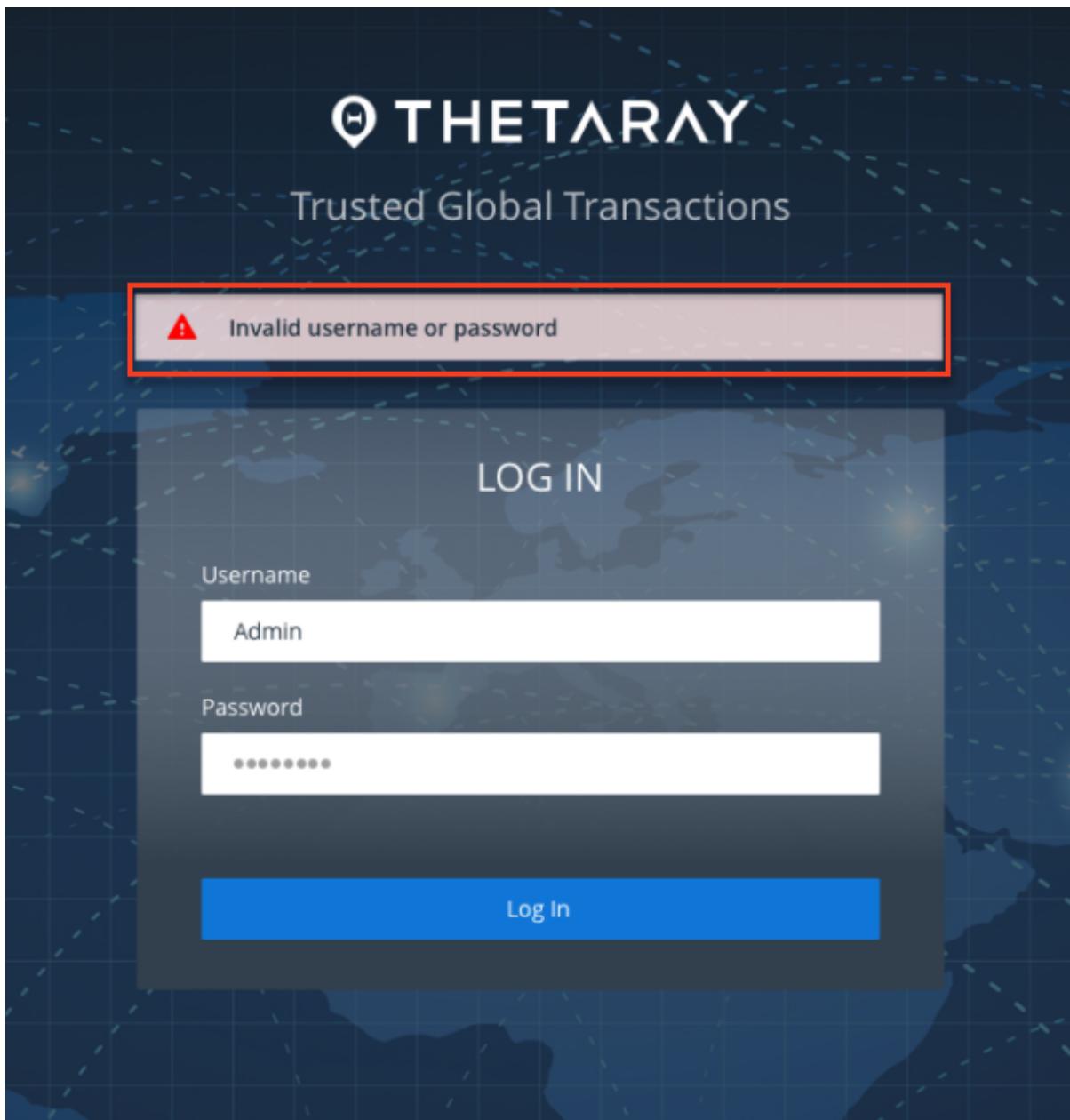
Access to investigation Center is to either company alert investigation personnel (either in the role of system manager or analysts) with appropriate permissions.

» **To access the Investigation Center:**

1. In the ThetaRay log in screen, (shown below) enter your username and password.
2. Click the Log in tab.



In the event of an invalid username or password is entered the following error notification is displayed. Correct and retry.



At successful Login, the **Alerts List** screen is displayed as shown in the following example.

1.1. Overview of the Alerts List - Landing Screen

With reference to the above figure the main elements of the Alert list screen are shown and described briefly below. Further drill down and description of these and associated elements is covered more fully in this guide.

Select Investigation Center (1) - normally selected by default

If Investigation Center Alerts list not displayed by default, select highlighted icon (1) matrix icon as tagged in the Landing screen figure (2nd image figure shown below)

Depending on which product license(s) the customer has subscribed to, the following IC modules may show all or a section of the following icons available for selection.

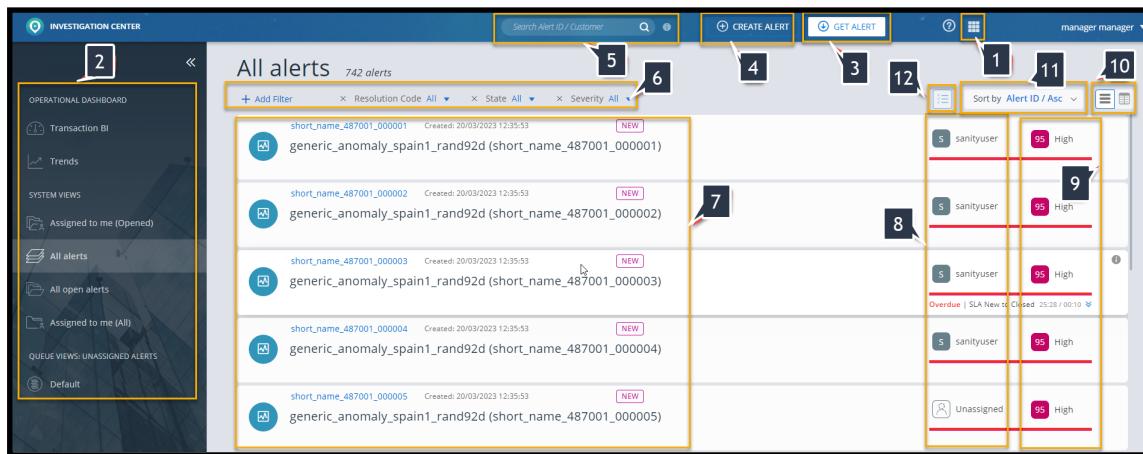
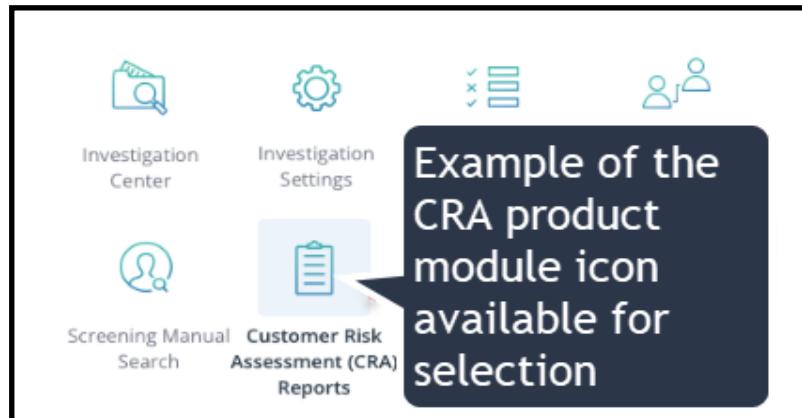


Figure 1: IC Module Landing Screen

As tagged above, the following IC components are displayed

- Alerts View section (2) including;
 - All alerts
 - SYSTEM VIEWS section (including alerts 'assigned to me opened' etc.)
 - QUEUE VIEWS section (Including Default queue)
- GET ALERT (3) - Link to assign an available alert to the signed in user
- CREATE ALERT (4) Create manual alert
- Alerts Search (5)
- Alert filter group (6)
- Alert card(s) (7)
- Alert assignee (8)

- Alert Severity group indication with severity score (9)
- Table / List view toggle (10)
- Sort alert list menu (11)
- View alert list option toggle switch (12)

1.1. Overview

In general, this User Guide provides users tasked with working with the ThetaRay Investigation Center the necessary information to review, investigate and manage Transaction Monitoring system Alerts. The guide presents the Alert management process in a logical fashion, guiding the user through the initial stages of viewing new Alert listings, examining accumulated forensic evidence and then based on the evidence gathered, recommending a resolution to the Alert.

Note: This user guide is primarily focused on providing descriptions and information to the user working with the Transactions Monitoring use case / solution. For specific information on Transaction and Customer Screening or Customer Risk Assessment (CRA) alerts please refer to the appended relevant chapters and subsections of this guide.

2. Managing Alerts List

The alerts list displays all alerts from the currently selected alert view.

Topics covered in this **Managing Alerts List** section include:

- Alerts List Screen Views
- Custom Views
- Alerts List Filters
- Alerts List Screen Filters - by Type
- Alert Cards
- Editing Alert Cards
- Bulk Alert Editing
- Sorting Alerts
- Viewing Alerts in Card or Table Format
- Selecting an alert card to view details
- Bulk Download of Alerts

2.1. Alerts List Screen Views

You can select to view alerts by the following views:

- All Alerts
- SYSTEM VIEWS (including):
 - Assigned to me (opened)
 - Assigned to me (all)
 - All open Alerts
- QUEUE VIEWS: UNASSIGNED ALERTS
 - Default

Note: alerts from all associated use case analysis (if applicable) are available automatically for investigation, without the need to select from a use case list

» To select a list view:

1. From the Alerts List Screen, if the List View menu is not already open click the  icon

The Alerts /Queues List View menu is displayed as shown in the following figure.

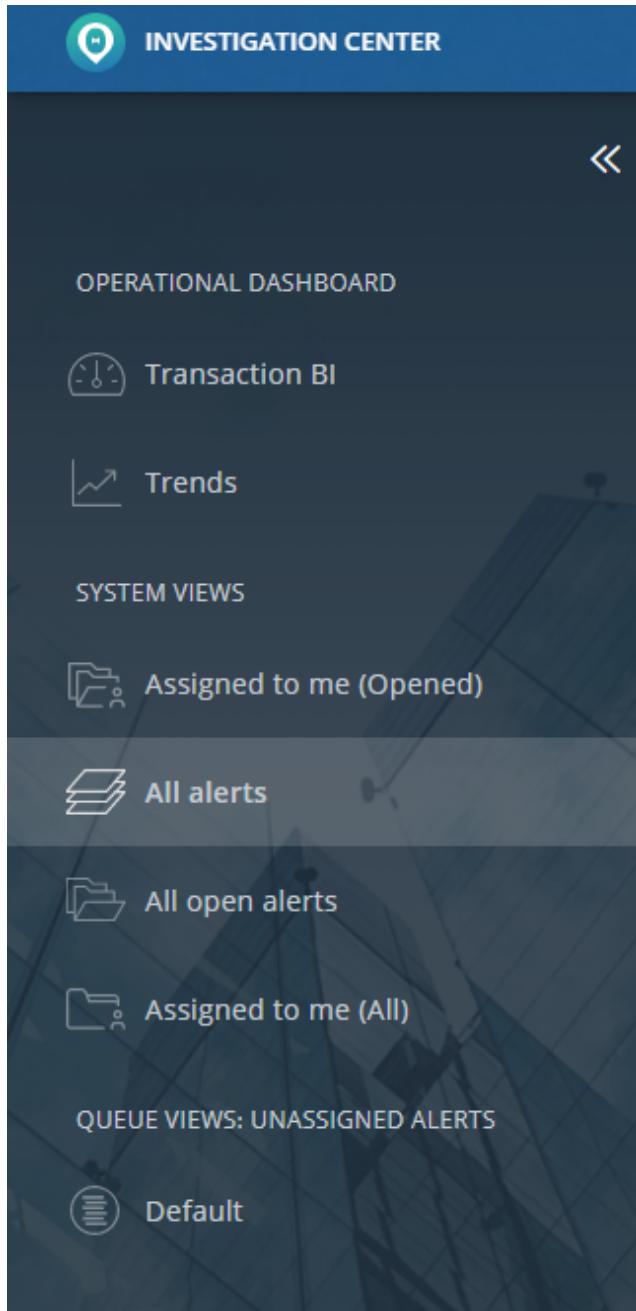


Figure 2: Example - Default Alerts List

2. Select an alerts / queue list to view.

An example Alerts List is displayed below.

Alert ID	Customer	Entity Type	Risk Score	Status
OP_65432432	Land ABC	Company	72	Onboarding (NEW)
OP_65432432	Travis Singleton	Individual	70	Onboarding (NEW)
OP_65432433	Bridget Quinton	Individual	77	Onboarding (NEW)
OP_65432434	Roland Travel	Company	77	Low → High (ESCALATED:COMP)
OP_65432435	Francis Parker	Individual	95	Low → High (NEW)

Figure 3: Example Alerts List Screen Showing Customer Risk Assessment (CRA) Alerts

2.2. Custom Views

To enable you to view previously filtered alert groupings, **Custom Views** can be added to the available system views. Custom views once saved, appear in the **Custom Views** menu located after the System Views menu, as the following example shows.

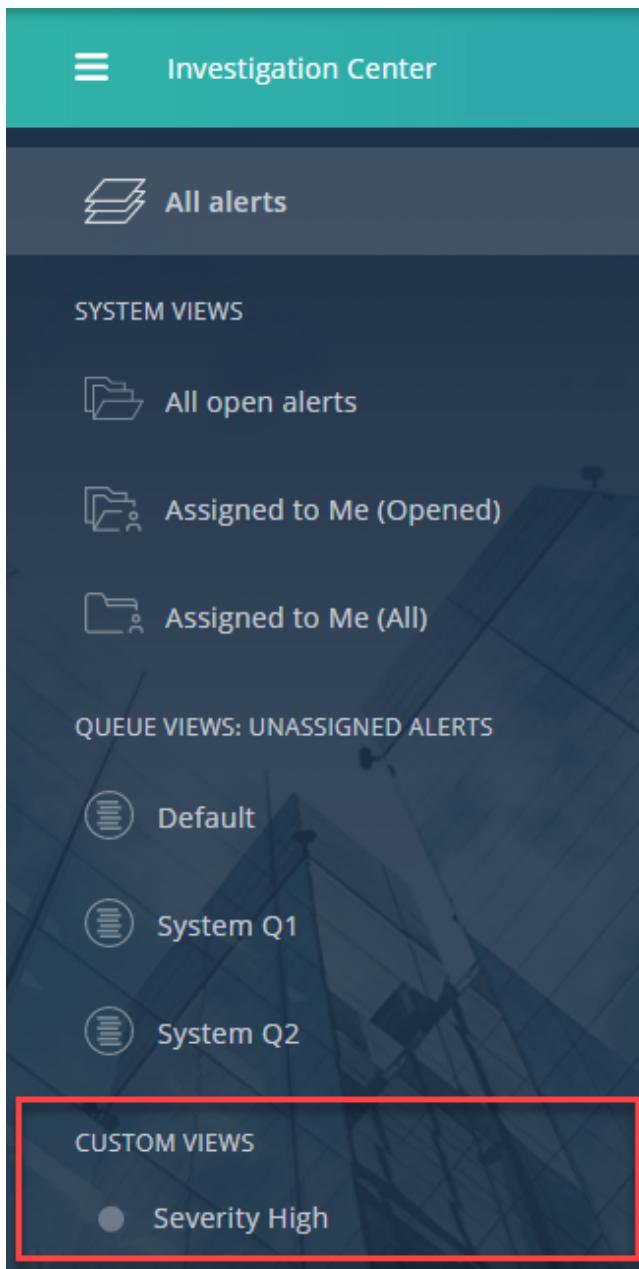


Figure 4: Custom Alert Views

2.2.1. Creating Custom Views

Creating new custom views is quick and easy.

You simply filter or search by criteria to view alerts by similar attributes and once these are displayed, save this filter selection as a custom view for reselection whenever required. This saves the time consuming process of filtering from the list of available alerts at each investigation in the future, and also trying to remember what exact filter settings you used previously.

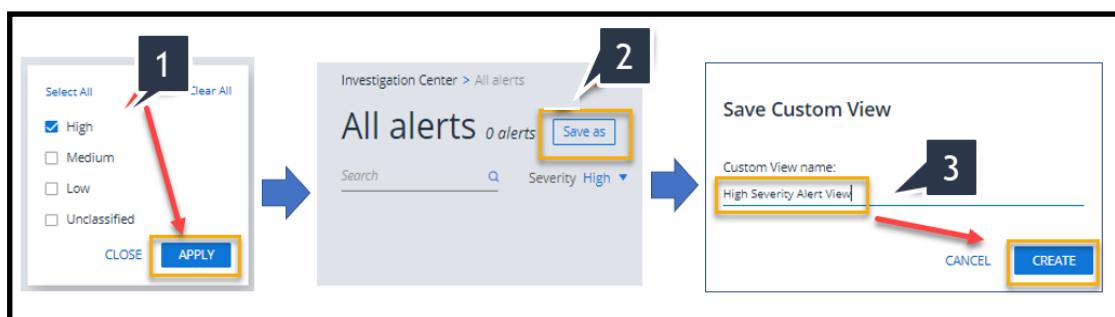
Note: Up to 20 Custom Views can be created. Once 20 views are created, you will need to delete an existing view before you can create a new one.

2.3. Creating a Custom View

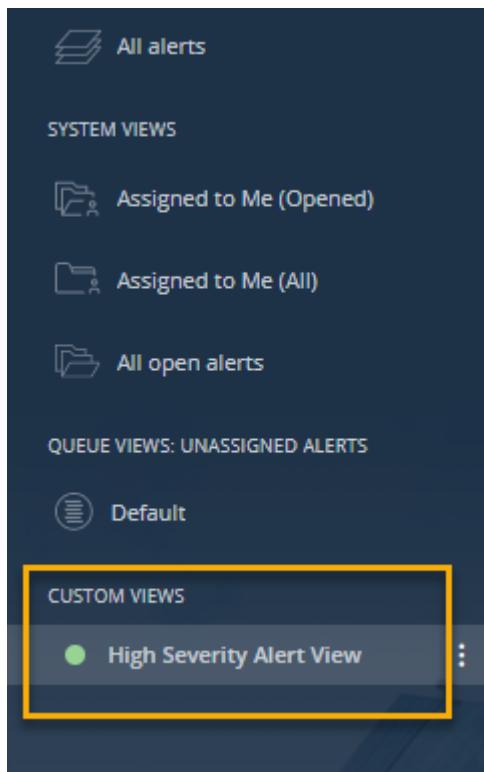
To explain the process, lets create an example custom view that displays all high severity alerts:

1. From the Alerts List screen, select the **All Alerts** View.
2. Open the 'severity' filter and deselect all selected so that only High severity remains and click **apply**(1).
3. Click **Save as** button as shown below in (2).
4. Enter the descriptive name 'High Severity Alert View' in the name field (3) and click **Create**.

The following diagram shows the flow.



5. Check that the newly created 'High Severity Alert View' appears under the newly added Custom Views sub header as shown below.



2.3.1. Editing Custom Views

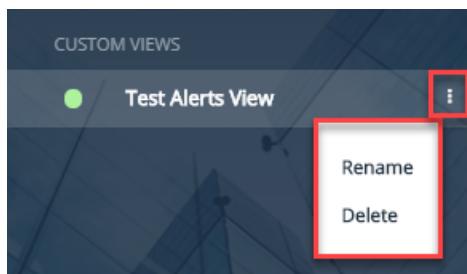
Custom view edit options are as follows:

- Rename
- Delete

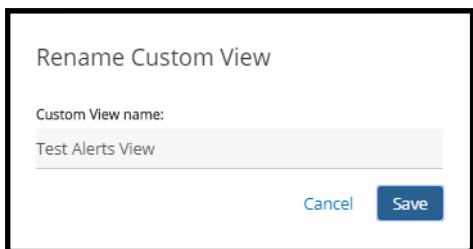
» To edit an existing custom view:

1. Click the 3 dot vertical icon to display edit options for each custom view.

The Edit options are displayed as [2.2.](#) below.



Selecting **Rename**, displays a popup as shown [2.2.](#) below.



2. Type a new name over the existing name (max 25 characters) and click **Save**.

Selecting **Delete** displays a verification popup as shown below.



3. Click **Delete**, or **Keep** to cancel the delete action.

2.4. Working with Custom Views - Additional Notes

1. The Custom View is a personal view, and it is only displayed to the user who created it.
2. The Custom View does not move an alert anywhere, it is, as its name suggests, just a fabricated view displayed on top of the existing alerts.
3. If a Customer View was created to show all the "Under Review" alerts, for example, and the status of an alert was changed to "Recommended Resolution" then this alert will automatically be removed from the view. It is a dynamic view, any change in attributes, will potentially change the content of the view.
4. No special user permissions are needed to create a custom view.

2.5. Alerts List Screen Filters - By Category Type

Before detailing filters individually, here is the complete list of available filters divided into categories:

Filter	Category Type
Assignee	Main
Alert Created Date	
Created Date	
Date Range	
Origin	
Queue	
Resolution Code	
Recommended Resolution Code	
SLA Name	
SLA Stage	
SLA Status	
State	
Use case	
Consolidation	Monitoring
Severity	
Relationship	
Risk Category	
Risk Name	
Analysis Method	
Match Score	Screening
Source Messages	
Analysis Type	CRA
Inheritance Type	
Risk Classification	

2.6. Filter Use by Category Type

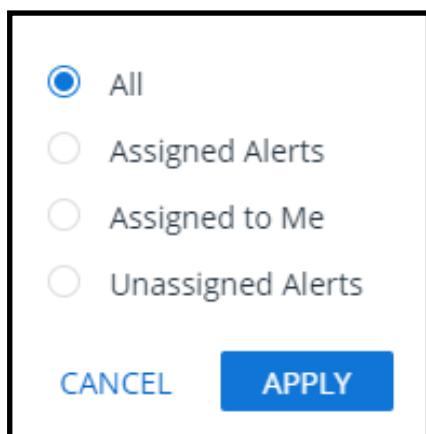
Note: The main category refers to filters that apply to alerts of all origins. The rest of the filter categories alerts of specific origin - Transaction Monitoring, CRA, Transaction Screening and Customer Screening,

2.6.1. Main Category

2.6.1.1. Assignee

Filtering alerts by assignee displays all alerts currently assigned to selected users. An example assignee select filter is shown below.

2.6.1.2. Filter by Assignee



» To filter by assignee:

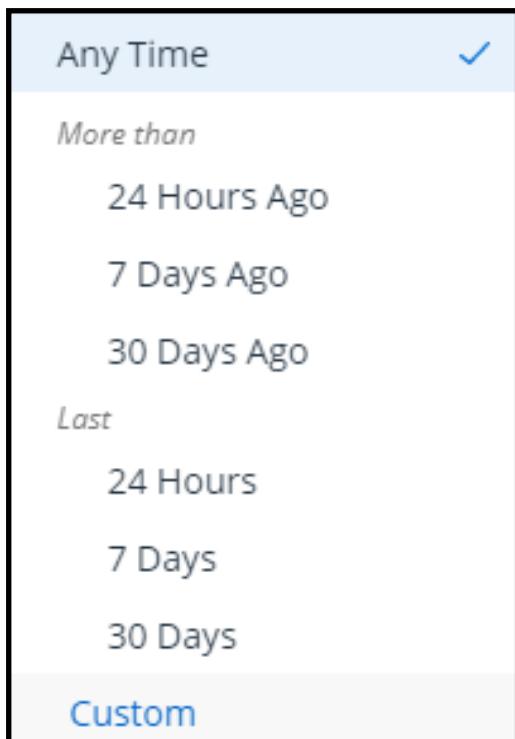
1. Click **Assignee** filter after selecting it from the filter list.
2. Select the attributes to filter by.
3. Click **APPLY**.

2.6.1.3. Filter by Created Date

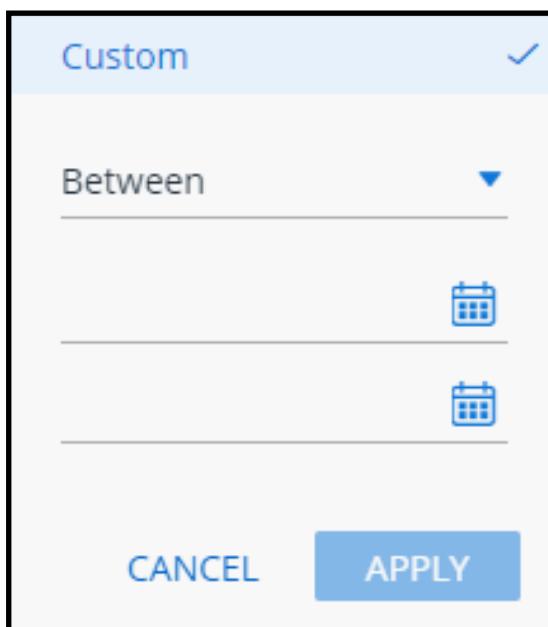
» To filter by Created Date:

1. Click **Created Date** filter after selecting it from the filter list.

Filtering by Created Date supports the following options:



2. Select the time period required, *or*
3. Select Custom, and set the custom 'from' and 'to' period based on created date from the two calendar widgets.



4. Click **APPLY**

2.6.1.4. Filter by Created Date

Info: This filter searches through all data related to the triggering of consolidated alerts

2.6.2. Filter by Date Range

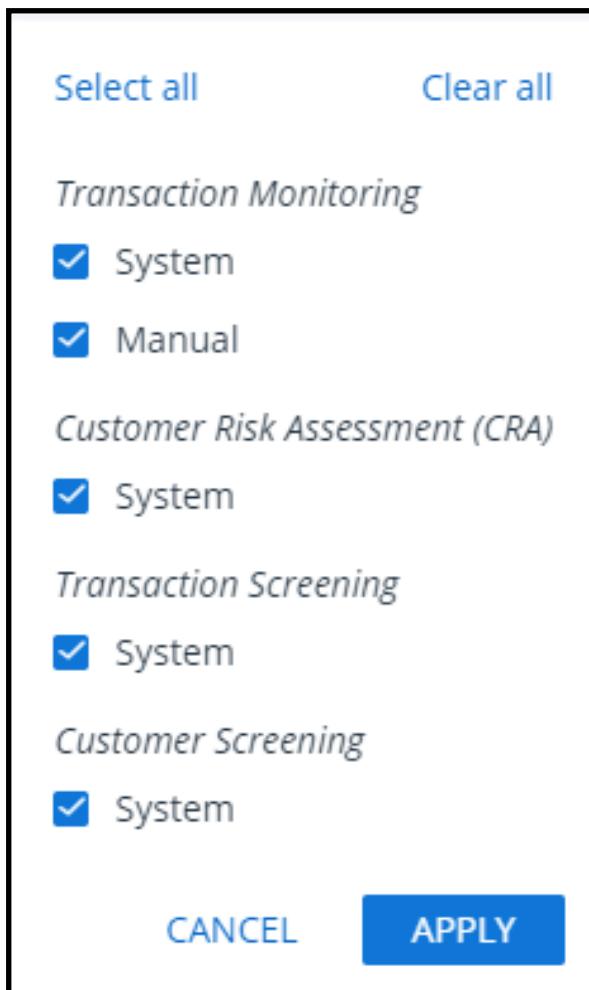
The **Date Range** filter refers to the filtering of alerts with an effective date over a specific preset time period or as a custom time period. The effective date refers specifically to the date when the transaction (that led to the alert identification) occurred on.

Applying this filter is processed in an identical way to how the created date filter is applied.

1. Click Date Created filter after selecting it from the filter list.
2. Select the time period required, *or*
3. Select Custom, and set the custom 'from' and 'to' period based on created date from the two calendar widgets.
4. Click **APPLY**.

2.6.2.1. Filter by Origin

The term *Origin* refers to the solution deployed on your Investigation Center application. (The following images, shows filter by origin examples.



Example Filters by Origin

The origin options currently available are:

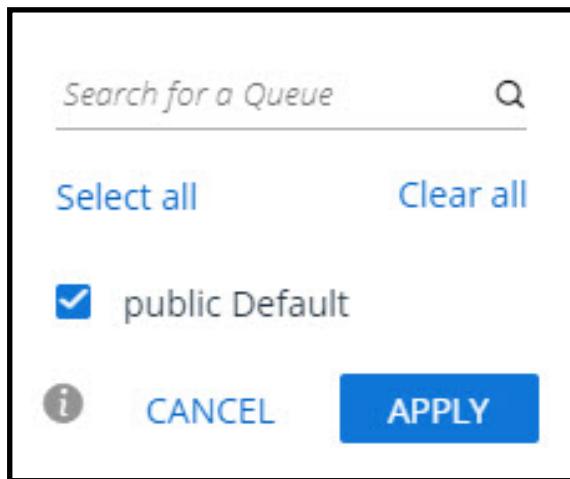
- All origins
- Transaction Monitoring
 - System
 - Manual
- Customer Risk Assessment (CRA)
 - System
- Transaction Screening
 - System
- Customer Screening
 - System

1. Select origin(s) and Click **APPLY** to filter by origins.

2.6.2.2. Filter by Queue

» **To filter by queue:**

1. Click the **Queue** filter after selecting it from the filter list.
2. An example of a queue list is shown below.



Either select the default queue or start typing the characters of a required queue to search for a queue (with auto complete).

2.6.2.3. Filter by Resolution Code

» **To filter by Resolution Code:**

1. From the Alerts List Filter menu, tick select **Resolution Code**.

Note: The list of available resolution codes shown here applies to the current default workflow deployed, and is for example purposes only.

2.6.2.4. Filter by Recommended Resolution Code

Note: The "recommended resolution codes" displayed are configurable by Workflow configuration, so therefore can be different in your environment.

» **To filter by Resolution Code:workflow**

1. From the Alerts List Filter, tick select **Recommended Resolution Code**.
2. To set the filter options, either check the attributes to filter by or enter the search text.
3. When complete click the **APPLY** button to initiate the filter and display related alerts.

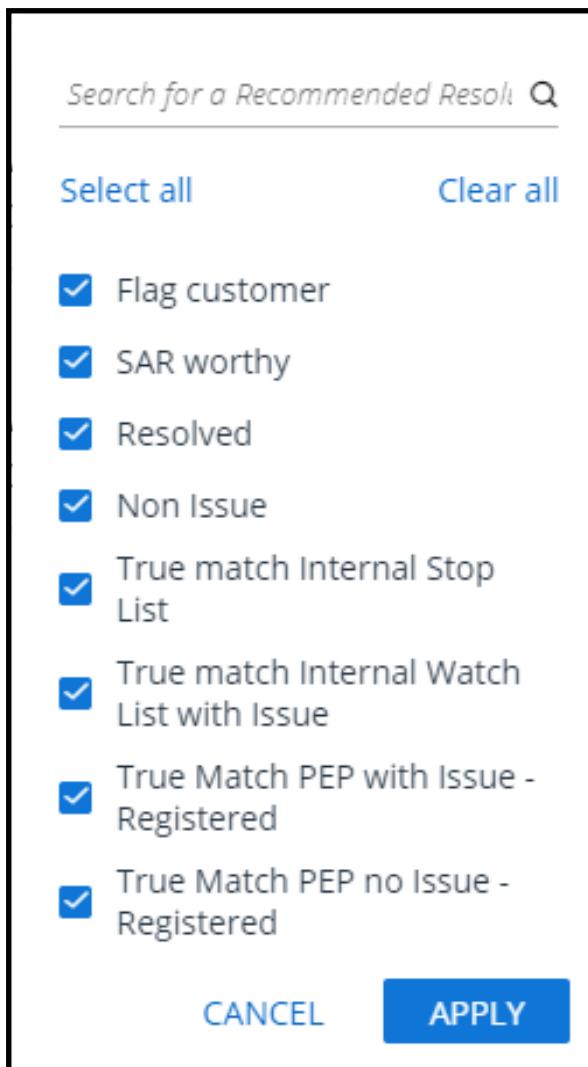


Figure 5: Example - Recommended Resolution Code

2.6.2.5. Filter by State

The State filtering option allows the user to filter displayed alerts by state.

Note: The list of available states shown here applies to the current default workflow deployed, and is for example purposes only.

» To filter by State:

1. From the Alerts List Filter menu, click **State** option.
2. Select each state to filter by.

[Select all](#) [Clear all](#)

Pending_LoD1
 2nd_Review_Comp
 Awaiting_Info_Comp
 New
 Review_SrComp
 Review_LoD1
 2nd_Review_SrComp
 Closed
 Review_Comp
 Escalated_SrComp
 Awaiting_Info_LoD1
 Escalated_Comp

[CANCEL](#) [APPLY](#)

Note: States listed are dependent on use case currently deployed. If the state you are looking for is not displayed, use the search facility (with auto complete).

3. Click **Apply** or **Cancel**.

2.6.2.6. Filter by SLA Name

Note: ThetaRay supports up to 20 SLA Names per Workflow. Regarding display, all names display function dynamically.

» **To filter by SLA Name:**

1. Select **SLA Name** from the main category list of filters.

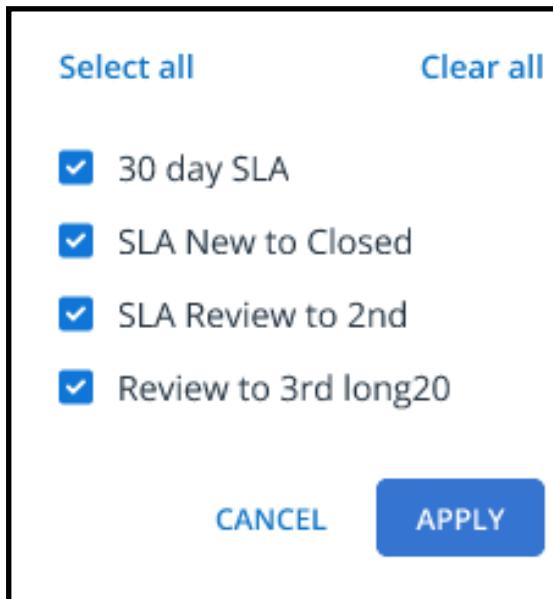


Figure 6: Example list of SLA Names

2. Select the SLA name(s) to filter by,
3. Click **Apply** or **Cancel**.

2.6.2.7. Filter by SLA Stage

» **To filter by SLA Stage:**

1. Select SLA Stage from the main category of filters.

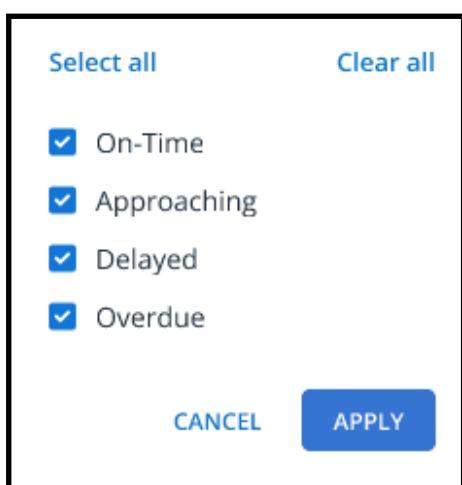


Figure 7: Example SLA Stages Filter

2. Select the SLA stage(s) to filter by,
3. Click **Apply** or **Cancel**.

2.6.2.8. Filter by SLA Status

» To filter by SLA Status:

1. Select **SLA Status** from the main category list of filters.

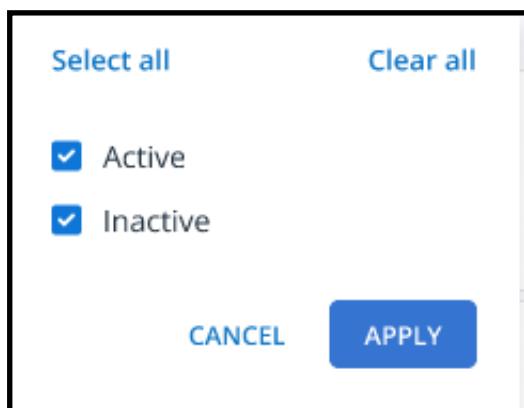


Figure 8: Example SLA Status Filter

2. Select the SLA status filter by.
3. Click **Apply** or **Cancel**.

2.6.2.9. Filter by Use Case

» To filter by Use Case:

1. Click filter by **Use Case** after selecting it from the filter list.

An example of a filter by **Use case** list is shown below.

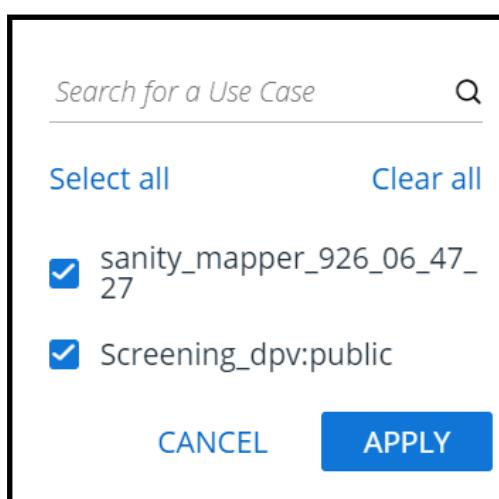


Figure 9: Example Filter by Use Case

2. Select from the displayed Use Cases to filter by, or if the use case is not listed or long, search by making a text search (with auto complete).
3. Click **Apply**.

The next batch of filters are listed under the **Monitoring** Category.

2.6.3. Monitoring Category

2.6.3.1. Filter by Consolidation

» To filter by Consolidation:

1. Click **Consolidation** filter after selecting it from the filter list.

Filtering by Consolidation supports the following options:

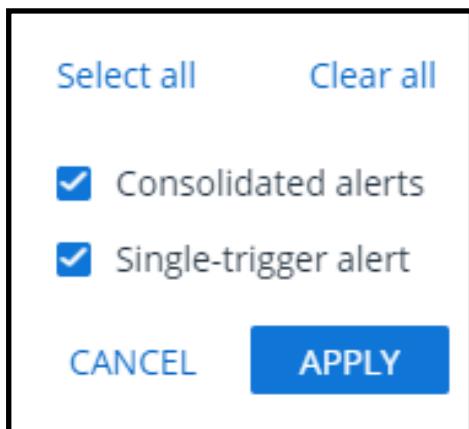


Figure 10: Example Monitoring by Category Filter

2. Select the attributes to filter by.
3. Click **Apply** or **Cancel**.

2.6.3.2. Filter by Severity

Note: This filter pertains exclusively to **Transaction Monitoring** sourced alerts

The severity level represents the specific level of importance. The importance level is signified by:

- Severity Category
- Severity Score

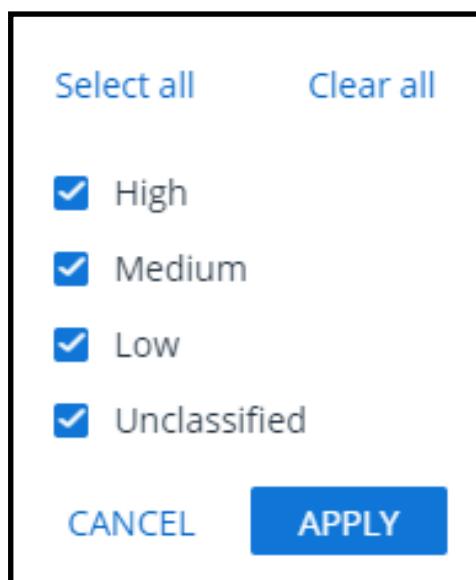
The following table details the relationship between severity category and severity score:

Table 1: Severity - by Category and Score - Default Settings

Severity Category	Severity Score (Indication of severity degree within category)
High	60 - 99
Medium	30 - 59
Low	1 - 29
Unclassified	N/A

» To filter by severity:

1. From the Alerts List Filter options, select the **Severity** filter.
2. Select the severity level(s) to filter by.

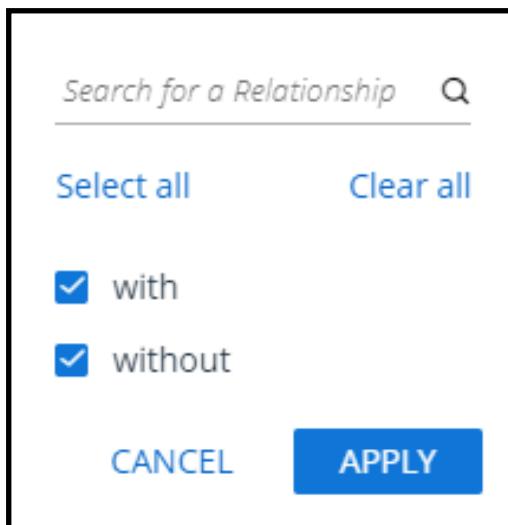
**Figure 11:** Example Severity Filter

3. Click **Apply** or **Cancel**.

2.6.3.3. Filter by Relationship

» To filter by Relationship:

1. From the Monitoring Category, select the Relationship filter.
2. Select the relationship to filter by or make a search in the Relationship field.



3. Click **Apply** or **Cancel**.

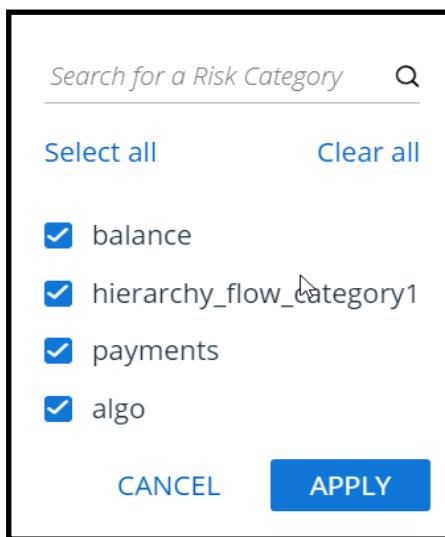
2.6.3.4. Filter by Risk Category

The filter by risk category works by filtering Consolidated alerts associated with the Alert under investigation.

» To filter by Risk Category :

1. Click filter by Risk Category after selecting it from the filter list.

An example of a filter by Risk Category is shown below.



2. Select from the displayed risk of attributes to filter by, or if the Risk category is not listed or is long, search for a risk by making a text search (with auto complete).
3. Click **Apply** .

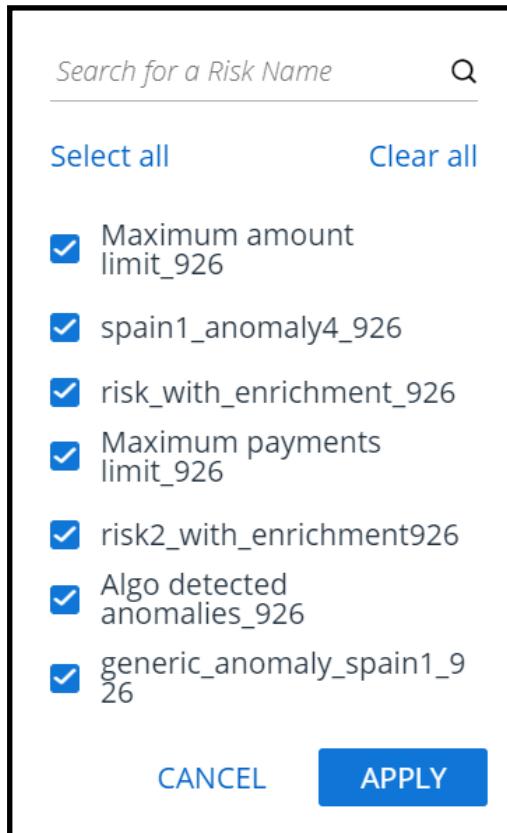
2.6.3.5. Filter by Risk Name

The filter by Risk Name works by filtering Consolidated alerts associated with the Alert under investigation.

» **To filter by Risk name:**

1. Click filter by Risk Name after selecting it from the filter list.

An example of a filter by Risk Name is shown below.



2. Select from the displayed risk of attributes to filter by, or if the risk name is not displayed or the list is long, search for a risk by making a text search (with auto complete).
3. Click **APPLY**.

2.6.4. Screening Category

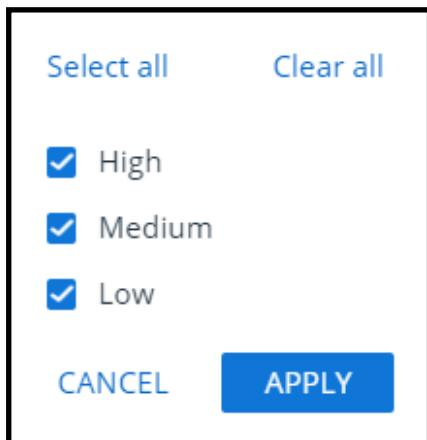
2.6.4.1. Filter by Screening Match Score

The Match Score filter pertains exclusively to the Screening solution

If your IC deployment is set up for multi solutions, in order for this filter to be applied you need firstly to make sure *Screening* is selected in the *Origins* filter.

» To filter by Match Score:

1. Select Match Score filter to add it to the displayed filters on your IC display
2. Open the filter by selecting the 'All' option.



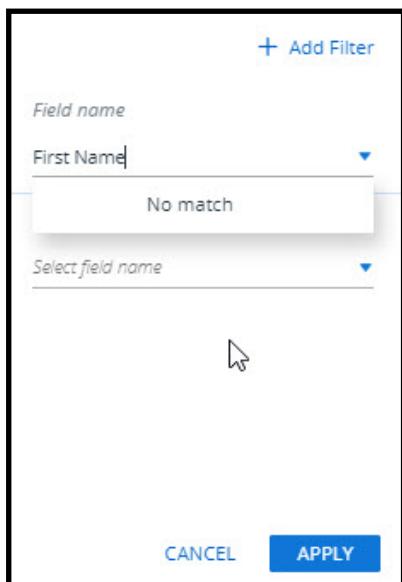
3. Select the required filter attributes and click APPLY.

2.6.4.2. Filter by Screening Source Messages

The **Source Messages** filter enables searching for source messages that contain specific field names.

» To search for *Source Messages* by field name:

1. Select Source message filter.
2. The following filter is displayed .



3. Start to type the field name to search by.

Auto complete will display any matches found as the search name is progressively typed.

4. If fields are matched and displayed, select the required field to search by.

Clicking the **+** **Add Filter** icon displays additional field searches to be made as described in steps 3 and 4.

5. When all the search message by field entries are complete, click **APPLY**.

2.6.5. CRA Filters

Included Analysis Type and Risk Classification

Note: CRA filters are displayed only if the CRA module is included in the deployment.

2.6.6. CRA Analysis Type

2.6.6.1. Filter by CRA Analysis Type

➤ **To filter by CRA Analysis type:**

1. From the CRA filter section, select Analysis Type.

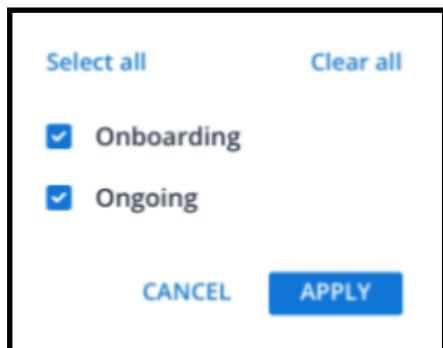


Figure 12: Example Analysis Types Filter

1. Select the analysis type(s) to filter by.
2. Click **Apply** or **Cancel**.

2.6.7. CRA Inheritance Type

2.6.7.1. Filter by CRA Inheritance Type

» To filter by CRA Inheritance type:

1. From the CRA filter section, select Inheritance type.

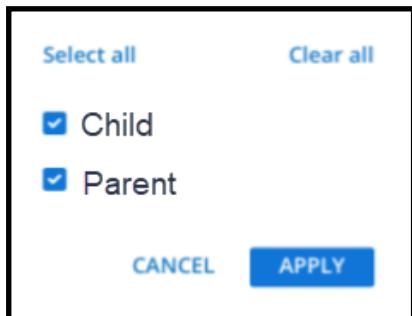


Figure 13: Example InheritanceType Filter Select

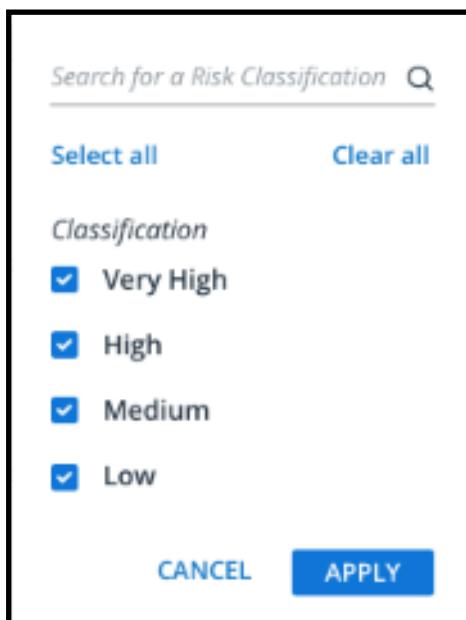
2. Select Inheritance type(s)
3. Click **Apply** or **Cancel**.

2.6.8. CRA Risk Classification

2.6.8.1. Filter by Risk Classification

» To filter by Risk Classification:

1. Select Risk Classification from the CRA Filters section.



2. Select the classification severity to filter by *or*
3. Search for Classification in the search field.
4. Click **Apply** or **Cancel**.

2.7. Alert Cards Functionality

An example alert card is shown as depicted in the following figure.



Figure 14: Example Standard Alert Card Display

2.7.1. Alert Card - SLA Calendar Settings Functionality

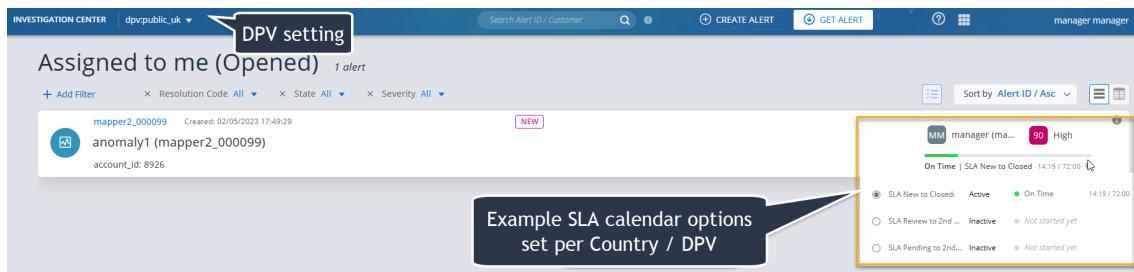


Figure 15: Example Alert Card with SLA Calendar Setting per DPV

The following behavioral points should be noted when working with the SLA Calendar feature:

- SLA settings are applied only to newly created alerts
- A setting applied to a newly created alert will remain for the alert's lifecycle (even if the alert is closed, then subsequently reopened)
- If the setting is removed during the alert lifecycle, created alerts are not effected, but with regard to newly created alerts, these will be assigned the default setting (i.e., the same behaviour as for newly updated settings)

Note: Requests for SLA configuration changes should be made through the Data Science Team.

2.7.2. SLA Time Remaining Time Display

1. The SLA remaining time display provides the analyst to see three SLA time elements:
 - Total SLA time
 - Elapsed time representation
 - Remaining time per color coding
2. On the progress bar analysts can view two of the above elements:
 - Elapsed time

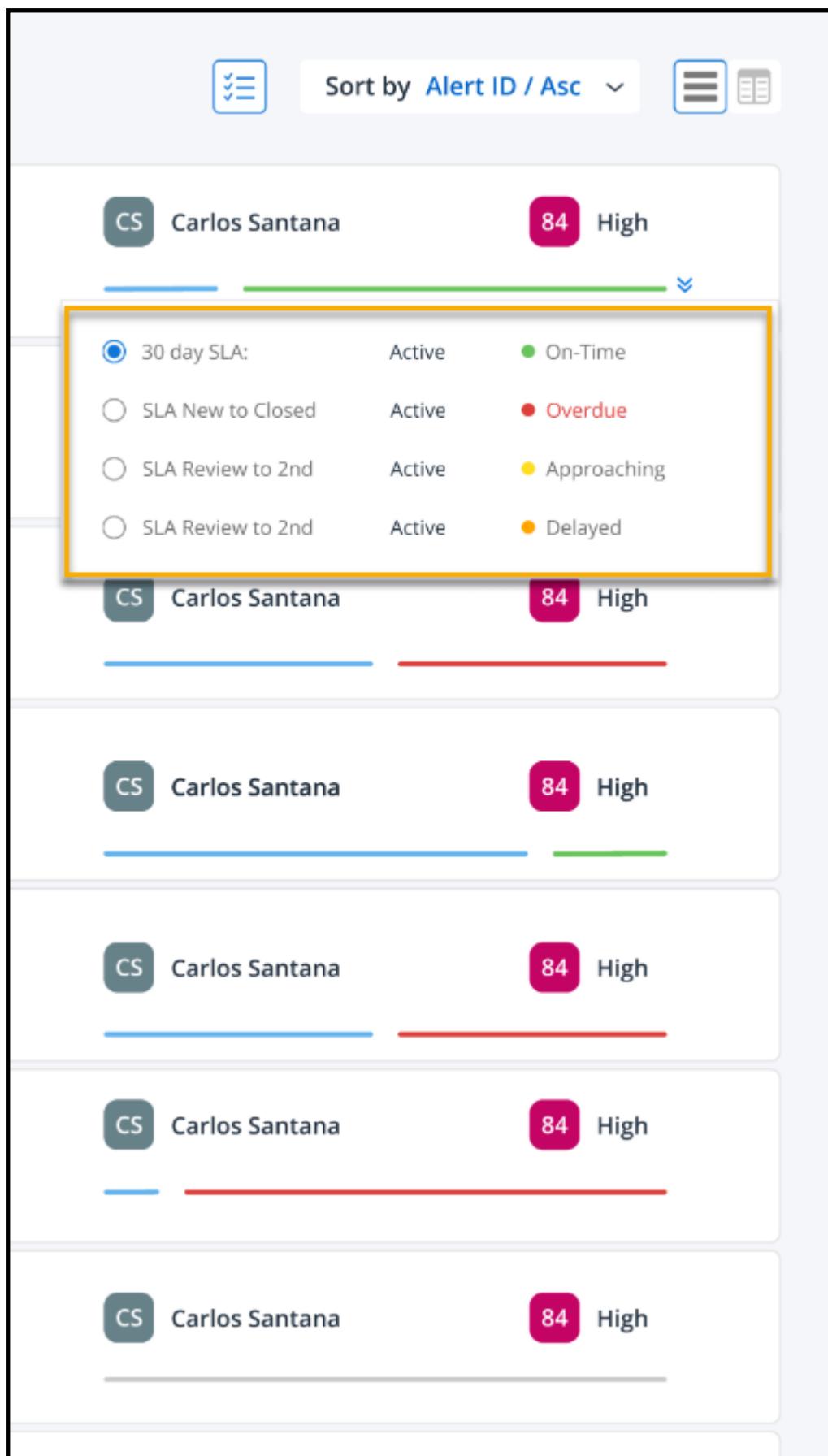
- Remaining time

Additionally, detail of all three elements are viewable as a tooltip upon hover.

3. The time bar shows SLA status color coded as follows:

- Non-started or inactive - gray
- Elapsed - blue
- Remaining mapped with the SLA Stage “On-Time” - green
- Remaining mapped with the SLA Stage “Approaching” - yellow
- Remaining mapped with the SLA Stage “Delayed” - orange
- Overdue (out of the Total SLA) mapped with the SLA stage “Overdue”- red

The following figure shows examples of elapsed time and use of the hover to display elapsed time period and current progress time bar status.



The elapsed (blue) indicator coupled with a remaining time color code - provides the analyst with a visual time overview at each SLA stage how much time has elapsed from the beginning of the stage related to the subsequent following Remaining Time stage.

2.7.3. SLA Time Period - Standard Display

The standard unit of SLA time period used for activated SLAs, is displayed in minutes.

2.7.4. SLA Time Period - Alternative Display

From release version 6.10.1, (and if the related enable flag is set in the deployment) , users can view the SLA time period in a more granular way as follows:

Time Periods are displayed in the following fashion:

- Less than 1 hour - displayed in minutes
- More than 1 hour - displayed in hours
- More than 24 hrs - displayed in days
- More than 30 days - displayed in months
- More than 12 months - displayed in years

Abbreviations used for time cadences:

- Minutes: **min**
- Hours: **hr**
- Days: **d**
- Months: **mth**
- Years: **yr**

Examples of SLA settings with the alternative display in use:

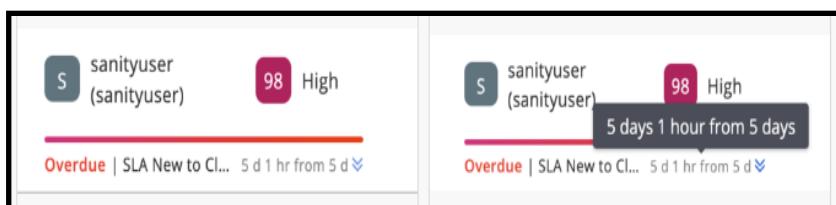


Figure 16: Examples of SLA Settings when Alternative Display Use is Deployed

Note: In IC deployments where SLA is activated, the optional display method is by default disabled, so for customers that require support to enable, please contact your customer success agent if a SaaS customer, and for on-prem customers, refer to the Appendix G chapter of the current Install guide.

2.7.5. Alert Changing State - Mandatory Note Creation Requirement

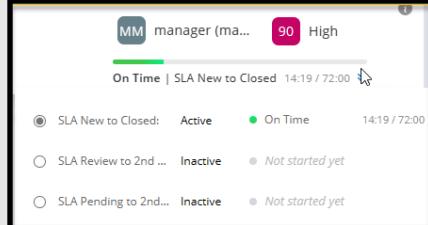
Note: Selecting an alert to change its state requires that a mandatory note be completed that provides the rationale for such a change of state. A mandatory note is provided pre-configured for the purpose.

Elements of the alert card are described and detailed in the following table.

Table 2: Module Header- Element, Description & Detail

Element	Description	Detail
Alert Card Icon	This icon includes metrics such as total number of consolidated alerts, and tagging for unread alerts read alerts, manually created, etc.	<ul style="list-style-type: none">unread alert read alert Manual AlertConsolidated Alert
Alert ID (short name)	System created unique alert ID name and number	Example: short_name_957488_000003
Alert name (full)	Full alert name (description in 'snake' format including short name id)	Examples: mapper1_0000042 (short_name_957488_000003)
account_id	Account Identification	Example: 7049
Date Created	Date and time when the alert was created	Example: Created 25.04.2017 07.05AM
State	The current alert state	Examples: <ul style="list-style-type: none">NEWPENDING_LOD1REVIEW_LOD1REVIEW_SRCOMP2nd REVIEW_SRCOMPESCALTED_COMPESCALATED_SRCOMP

Table 2: Module Header- Element, Description & Detail (continued)

Element	Description	Detail
		<ul style="list-style-type: none"> • AWAITING_INFO
Severity	The severity category and score of the alert Category: low, med, high score: A number between 1 and 100	Examples: <ul style="list-style-type: none"> • 10 Low • 40 Med • 90 High
Assignee	Current alert assignee	Examples: <ul style="list-style-type: none"> • sam developer • Manager • Unassigned
SLA details (if SLA applied)	If included in the use case deployed, the current SLA status (if active) per SLA Calendar settings per country /Region / DPV is shown here Note: Optional Display is by default disabled so if required contact customer success agent.	Examples: <ul style="list-style-type: none"> • On time • Overdue 
Extra Information icon (i)	Hovering over the info icon on the alert card displays extra alert information including: <ul style="list-style-type: none"> • Risk Category • Use Case • Queue association • Assigned team. 	

- If the setting is removed during the alert lifecycle, created alerts are not effected, but with regard to newly created alerts, these will be assigned the default setting (i.e., the same behaviour as for newly updated settings)

Elements of the alert card are described and detailed in the following table.

Table 3: Module Header- Element, Description & Detail

Element	Description	Detail
Alert Card Icon	This icon includes metrics such as total number of consolidated alerts, and tagging for unread alerts read alerts,	<ul style="list-style-type: none"> • unread alert  • read alert  • Manual Alert

Table 3: Module Header- Element, Description & Detail (continued)

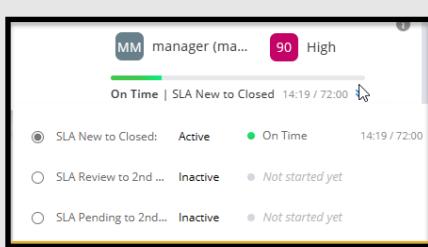
Element	Description	Detail
	manually created, etc.	<ul style="list-style-type: none"> • Consolidated Alert
Alert ID (short name)	System created unique alert ID name and number	Example: short_name_957488_000003
Alert name (full)	Full alert name (description in 'snake' format including short name id)	Examples: mapper1_0000042 (short_name_957488_000003)
account_id	Account Identification	Example: 7049
Date Created	Date and time when the alert was created	Example: Created 25.04.2017 07.05AM
State	The current alert state	Examples: <ul style="list-style-type: none"> • NEW • PENDING_LOD1 • REVIEW_LOD1 • REVIEW_SRCOMP • 2nd REVIEW_SRCOMP • ESCALATED_COMP • ESCALATED_SRCOMP • AWAITING_INFO
Severity	The severity category and score of the alert Category: low, med, high score: A number between 1 and 100	Examples: <ul style="list-style-type: none"> • 10 Low • 40 Med • 90 High
Assignee	Current alert assignee	Examples: <ul style="list-style-type: none"> • sam developer • Manager • Unassigned
SLA details (if SLA applied)	If included in the use case deployed, the current SLA status (if active) per SLA Calendar settings per country /Region / DPV is shown here	Examples: <ul style="list-style-type: none"> • On time • Overdue 

Table 3: Module Header- Element, Description & Detail (continued)

Element	Description	Detail
Extra Information icon (i)	Hovering over the info icon on the alert card displays extra alert information including: <ul style="list-style-type: none"> • Risk Category • Use Case • Queue association • Assigned team. 	

2.8. Editing an Alert Card

From alert cards, you can edit alert attributes of:

- Alert State
- Assignee

2.8.1. Alert State - Change

Note: Selecting an alert to change its state requires that a mandatory note be completed that provides the rationale for such a change of state. A mandatory note is provided pre-configured for the purpose.

As the alert under investigation progresses from starting off in the New State through to the Closed State, its state is changed at each milestone. The changing is normally carried out by the assigned analyst but in certain circumstances it can be changed automatically by the system.

 **To change the state of an alert:**

1. Hover on the state icon and click the edit icon (pencil).
2. According to state change , select available new state.

See example state select as shown [2.8.](#) below:

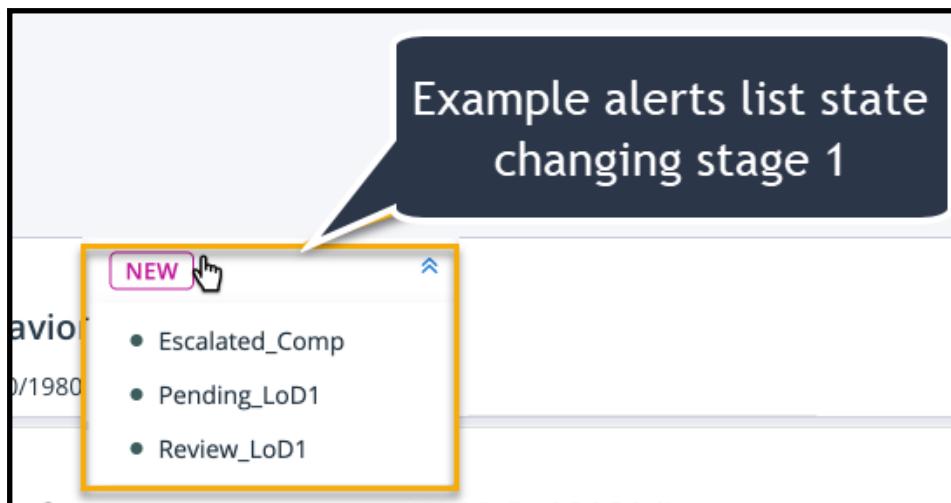


Figure 17: Example Change State Action Stage 1 - from Alert List

Note: The New state cannot be changed manually. Only when the New Alert has been selected and its state changed to Pending or Under Review can further changes be made manually. Refer to Analysts Workflow for further information.

3. Select the appropriate state change option as shown in the following example.

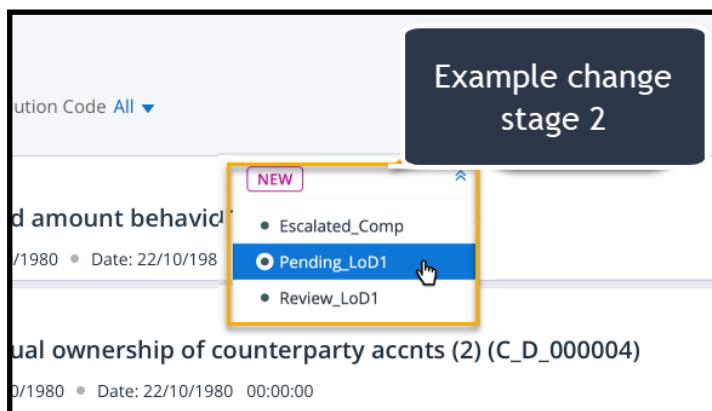


Figure 18: Example State Change Action - Stage 2

4. Select a note option complete the mandatory details, select resolution (if appropriate) and click **APPLY** as shown in the following example.

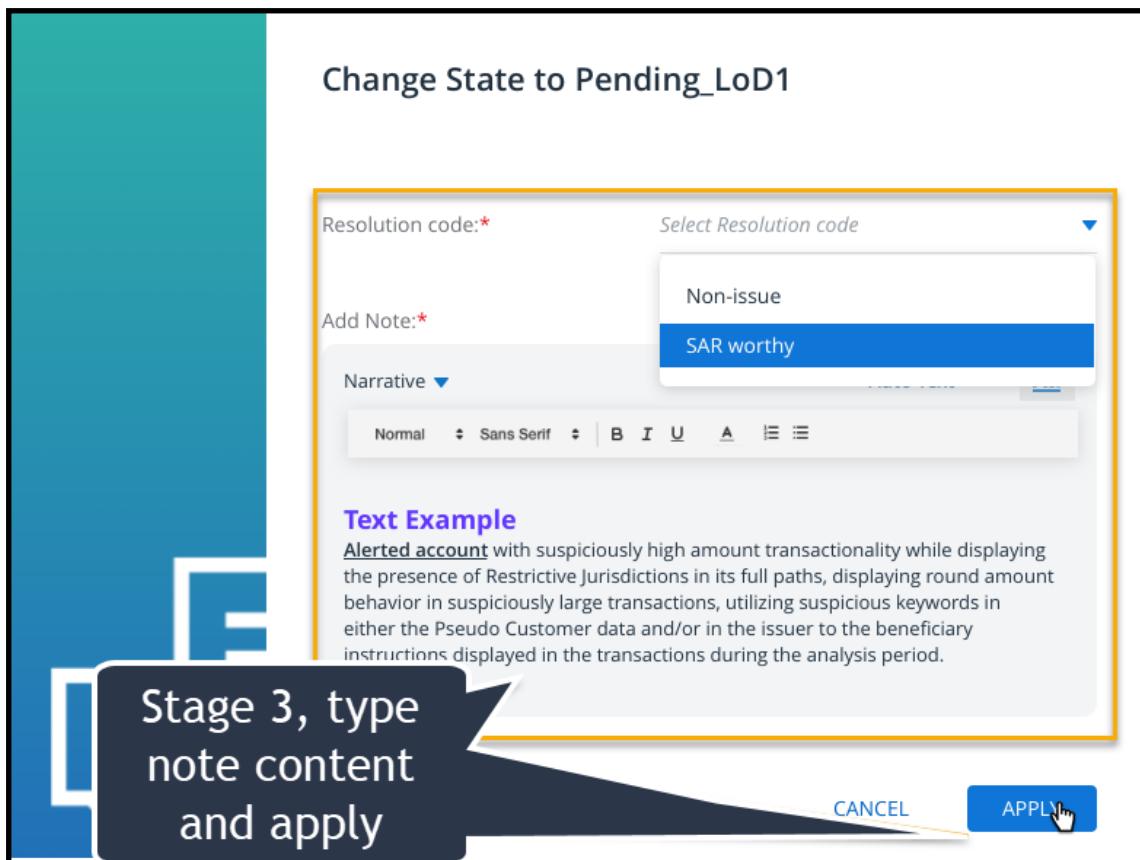


Figure 19: Example Completed Note and Resolution Code Selected

In alerts Details the entered details is available for viewing as shown below.

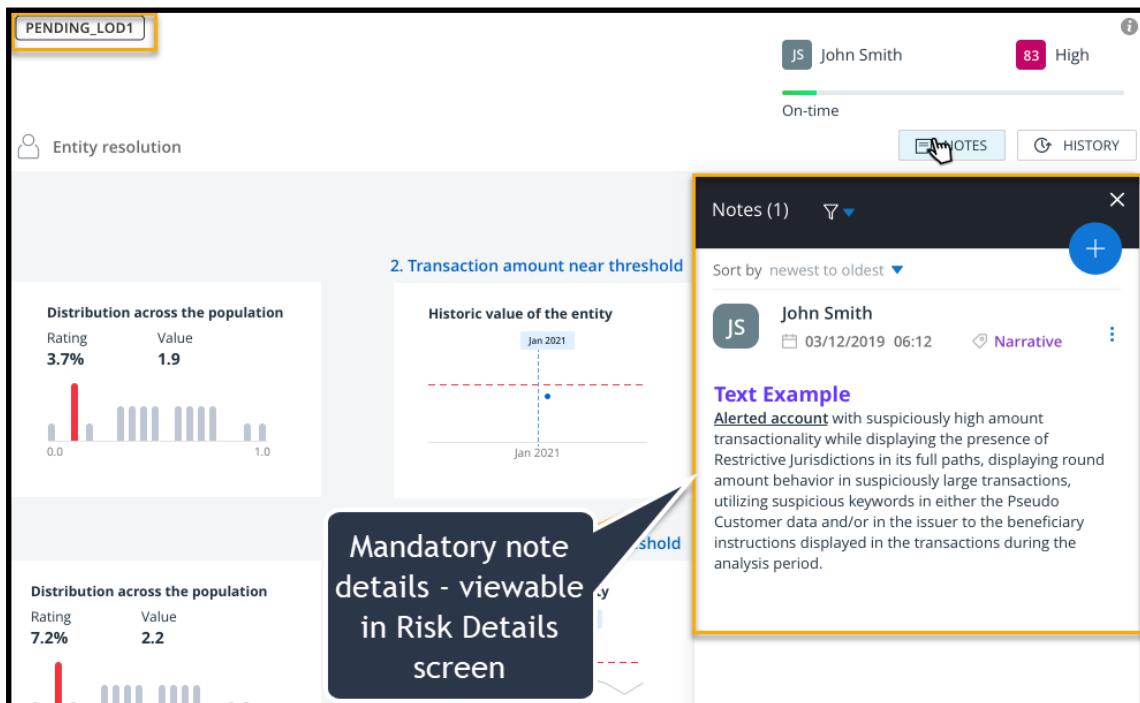


Figure 20: Example Note displayed in Alerts Details

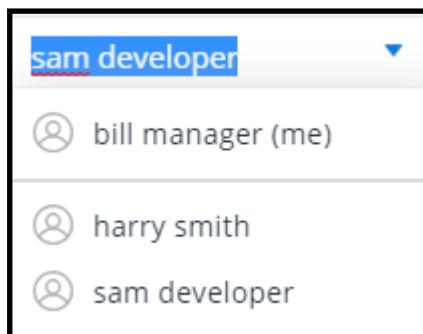
2.8.2. Assignee - Change

In the course of alert investigation it may become necessary to assign the alert to a more experienced investigator.

Note: Changing the assignee is limited to having permissions to assign users and the permissions of these users to be assigned the alert.

» To change Assignee:

1. Hover on the current assignee name and click the currently displayed assignee.
2. From the displayed list of assignees, click the required one (If the list is long use the scroll).
3. If the required assignee is not in the list, enter the first two letters to auto complete.
4. If assigning the alert to yourself, select the first option on the list as shown in the example below.



2.9. Bulk Alert Editing

Bulk editing of alerts allows users with the appropriate data scope permissions and alert assignations to select multiple alerts, and in a single bulk action either:

- Change their assignation
- Move selected alerts from one queue to another

Note: Before using bulk operation, the user should ensure the "public default" group and the filter alerts via Origin filter are selected .
(Choose only one - Screening or System) or Queue filter (choose only one queue).

Note: The maximum number of non-consolidated alerts that can be edited in a single batch is 50. If the required number of alerts to be bulk edited exceeds this amount, further batches can be bulk edited as required.

Note: Bulk Editing of related alerts is also possible. For more information refer to the Related Alerts Tab.

Note: Bulk Alert changes of state does NOT include the use of autotext templates mandatory notes.

2.10. Working with Bulk Editing Alerts

1. From the Alerts List Views in the default screening Alerts List, select alert view required.

Click the **Bulk Edit Icon** as highlighted in the following figure.



Figure 21: Bulk Editing of Alerts in the Alerts list

The alerts list now displays the **Edit Multiple** view as shown 2.9. below.

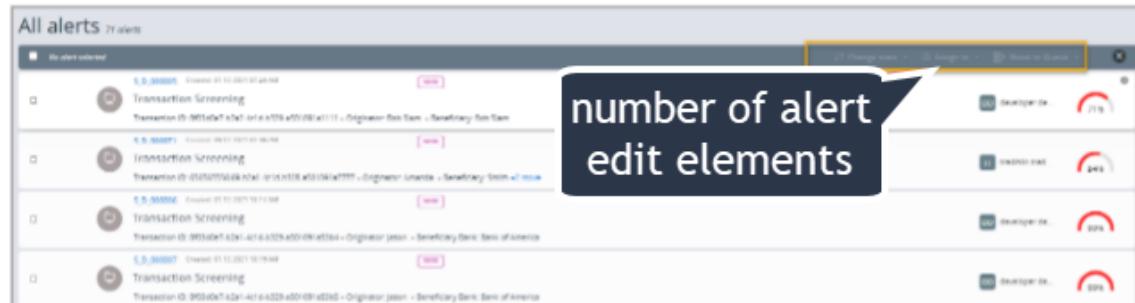


Figure 22: Alerts Edit Multiple View

The three edit element options are displayed (grayed out) in the panel header as follows:

- Change State

- Assign to
- Move to queue

To enable bulk edit, tick the enable box for at least one alert. When enabled, the bulk edit options for which the user has permissions to use are enabled and highlighted.

If one or more edit options are not enabled, it is suggested that a check of allocated permission scopes should be made with the system **Business Admin** user.



Figure 23: Bulk Editing with Change, Assign and Move Enabled

2.10.1. Multiple Changing Alert State

Limitations:

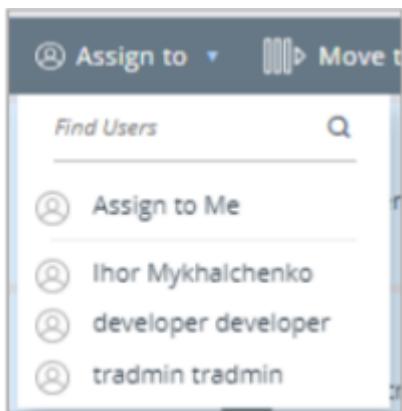
As in individual alert editing bulk change state is not possible in a **Screening Solution** deployment.

2.10.1.1. Bulk Assign to

Note: Bulk edit assigning alerts is only available to users with the appropriate Data scope permission.

» To multiple edit Assign to:

1. Click the Edit Multiple Select button.
2. Click the tick box of the alerts to be bulk assigned.
3. [Bulk Alert Editing](#)
4. From the dropdown list, select the required assignee from the list as shown in the following example:



5. Select the required assignee.

The following message requiring confirmation is displayed.

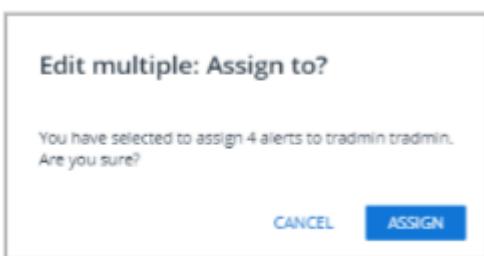


Figure 24: Multiple Assign to Confirmation Request

If the multiple selection completes successfully, the message shown in 2.9. below is displayed.



Figure 25: Bulk Change Success Notification

2.10.2. Moving Alerts from the Default Queue to Another Queue

The ability to bulk move unassigned alerts from one queue to another provides the **Business Admin** user extra flexibility when organizing the alert workload.

Note: Moving alerts from the default alerts queue is only available to users with the appropriate Data permission.

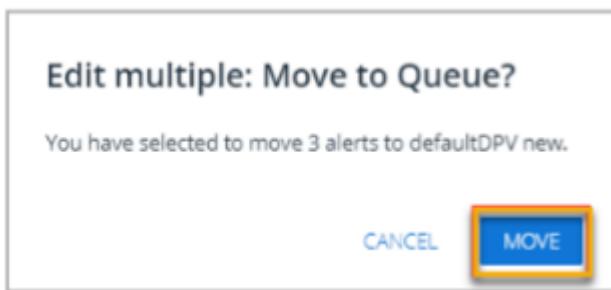
» **To move alerts from the unassigned default queue to another queue:**

1. Select the Move to Queue option from the header bar.
2. Click the tick box of the alerts to be bulk moved from the default alerts queue to the designated queue.
3. Click the **Move to Queue** tab.

4. Select the target queue from the available options.

In the above example, both the existing defaultDPV queue and the single defaultDPV new are displayed. In this instance, only option available for selection is the defaultDPV new queue.

Selecting this option displays the following message requiring confirmation.

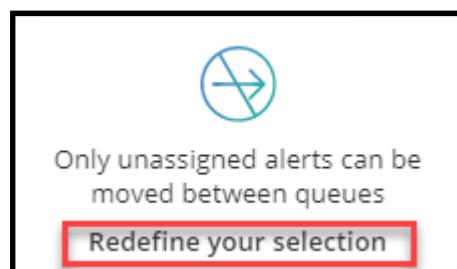


5. Click **Move** to initiate moving alert(s), or **Cancel** to cancel the operation.

2.10.3. Troubleshooting - Bulk Editing

Moving Alerts

Should an alert that is not unassigned be selected for bulk move the following message is displayed:



Solution: Redefine selection and retry bulk move.

General

Inability to perform **Bulk Edit**, verify data permissions with your **Business Admin** user.

2.11. Bulk Download for TM, TS & CS Alerts (System & Manual)

Bulk alert select and download of alerts and associated data to a .csv file provides the analyst with an alternative method of viewing alerts data for further assessment and investigation of various alerts. By using this optional method, it avoids the user having to use the more comprehensive method of deploying the Reports DB application .

Please note that the bulk download of alert types is restricted to downloads of one type per download. That is why it is important to use the origins filter as pointed out in step 1 below, to first select the specific download Origin type.

➤ To select and Download bulk TM, TS and CS alerts:

1. From the origins filter, select one Origin (System or Manual).
2. From the Queues Filter select a queue or queues.
3. Select the multiple icon as shown in the following figure.

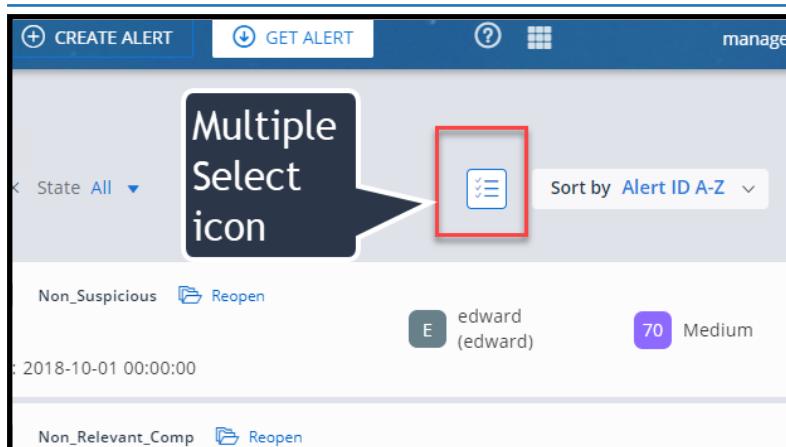
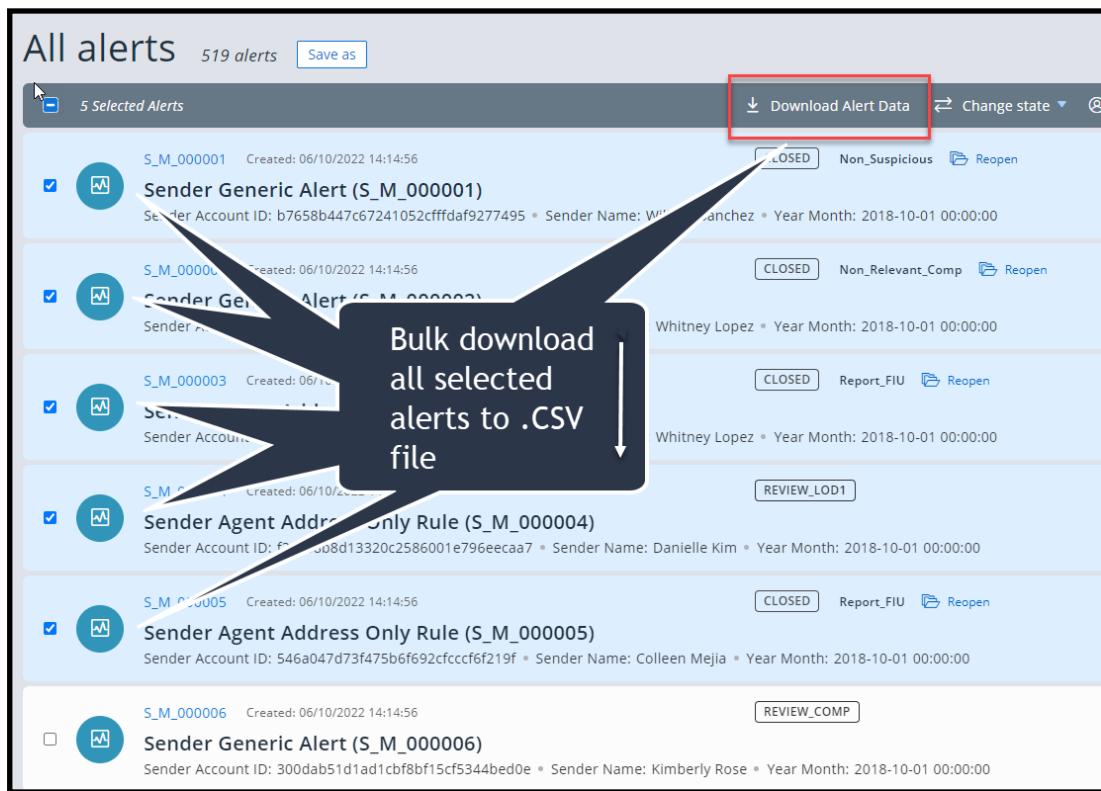


Figure 26: Multiple Select Icon



All alerts 206534 alerts More than 10,000 alerts were found. To refine your search and display results, please use filters. Save as

206534 Selected Alerts More than 10,000 alerts were selected. To refine your search and display results, please use filters. Download Alert Data Change state Assign to Move to Queue X

C_S_000927 Created: 30/01/2025 ... Profile: DEFAULT Hits: 1 SANCTION New mustafa aydin Individual: mustafa aydin Customer ID: fake_46534479549398487061 AA public_default_a... (Analyst Analyst) 100%

C_S_000928 Created: 30/01/2025 ... Profile: DEFAULT Hits: 5 SANCTION New EXIMBANK OF RUSSIA JSC Company: EXIMBANK OF RUSSIA JSC Customer ID: fake_506534504414466709 AA public_default_a... (Analyst Analyst) 100%

C_S_000929 Created: 30/01/2025 ... Profile: DEFAULT Hits: 3 SANCTION New Abdul Jalil Haqqani Wali Mohammad Agent: Abdul Jalil Haqqani Wali Mohammad Customer ID: fake_59466529541431011692 AA public_default_a... (Analyst Analyst) 100%

C_S_000930 Created: 30/01/2025 ... Profile: DEFAULT Hits: 2 SANCTION New VEB ENGINEERING LLC Customer ID: fake_4047559734035806386 Merchant: VEB ENGINEERING LLC AA public_default_a... (Analyst Analyst) 100%

Figure 27: Example Display when Large Amount of Alerts Found and Suggestion to Refine Filters

2.11.1. Example Downloaded CSV TM Alerts File (Partial)

Reported Alert ID	Title	Severity	Severity score	Risk type (OR and AND)	Risk detail info	Risk name	Risk category	State	Resolution Code
28/11/2022	1 S_M_000001	MEDIUM	70 OR	Generic Sender Monthly Anomaly	Sender Generic Alert	remittance	state_closed	Non_Suspicious	
	2 S_M_000002	MEDIUM	70 OR	Generic Sender Monthly Anomaly	Sender Generic Alert	remittance	state_closed	Non_Relevant_Comp	
	3 S_M_000003	MEDIUM	70 OR	Only a registered agent's address has been provided,	Sender Agent Address Only Rule	sender	state_closed	Report_FIU	
	4 S_M_000004	MEDIUM	70 OR	Only a registered agent's address has been provided,	Sender Agent Address Only Rule	sender	state_review_11	Report_FIU	
	5 S_M_000005	MEDIUM	70 OR	Only a registered agent's address has been provided,	Sender Agent Address Only Rule	sender	state_closed	Report_FIU	

Figure 28: Example System TM Partial .csv File Download

All alerts 206534 alerts More than 10,000 alerts were found. To refine your search and display results, please use filters. Save as

+ Add Filter X Origin Customer Screening S... X QUEUE Screening Queue X Clear Edit Multiple Sort by Alert ID A-Z

C_S_000927 Created: 30/01/2025 03:07... Profile: DEFAULT Hits: 1 SANCTION New mustafa aydin Individual: mustafa aydin Customer ID: fake_46534479549398487061 AA public_default_a... (Analyst Analyst) 100%

C_S_000928 Created: 30/01/2025 03:08... Profile: DEFAULT Hits: 5 SANCTION New EXIMBANK OF RUSSIA JSC Company: EXIMBANK OF RUSSIA JSC Customer ID: fake_506534504414466709 AA public_default_a... (Analyst Analyst) 100%

C_S_000929 Created: 30/01/2025 03:08... Profile: DEFAULT Hits: 3 SANCTION New Abdul Jalil Haqqani Wali Mohammad Agent: Abdul Jalil Haqqani Wali Mohammad Customer ID: fake_59466529541431011692 AA public_default_a... (Analyst Analyst) 100%

C_S_000930 Created: 30/01/2025 03:08... Profile: DEFAULT Hits: 2 SANCTION New VEB ENGINEERING LLC Customer ID: fake_4047559734035806386 Merchant: VEB ENGINEERING LLC AA public_default_a... (Analyst Analyst) 100%

Figure 29: Example Bulk Select and download Process Example Partial CS Download .csv file

2.12. Example Downloaded System Created CS .csv Alerts File (Partial)

A	B	C	D	E	F	G	H	I	J	K
Report generated on	Alert ID	Title	Origin	Subtype	Created Date	Profile	List of Matched Sanction Group and Lists	date	third_rein:agent	re
21/02/2025 10:57:00	941 smith a	CUSTOMER_SCREENING	SYSTEM	6/2/2025 8:51	DEFAULT	["label": "PERF PRVT LST", "category": "PERF PRVT LST"]	["label": "PERF PRVT LST", "category": "PERF PRVT LST"]	"dateOfUpload": "2025-02-05T10:27:42.605", "dateOfPublication": null]		
	942 a smith	CUSTOMER_SCREENING	SYSTEM	6/2/2025 8:51	DEFAULT	["label": "PERF PRVT LST", "category": "PERF PRVT LST"]	["label": "PERF PRVT LST", "category": "PERF PRVT LST"]	"dateOfUpload": "2025-02-05T10:27:42.605", "dateOfPublication": null]		

Figure 30: Example System CS .csv File Download Partial

2.13. Example Downloaded Manually Created CS .csv Alerts File (Partial)

A	B	C	D	E	F	G	H
Report generated on	Alert ID	Title	Origin	Subtype	Created Date	Profile	List of Matched Sanction Group and Lists
21/02/2025 10:57:19	43211 putin	CUSTOMER_SCREENING	MANUAL	13/02/2025 15:44:55			["label": "OFAC SDN", "category": "SANCTION"]
	43271 suli	CUSTOMER_SCREENING	MANUAL	13/02/2025 15:45:46			["label": "OFAC SDN", "category": "SANCTION"]
	44139 maria	CUSTOMER_SCREENING	MANUAL	13/02/2025 15:55:06			["label": "OFAC SDN", "category": "SANCTION"]

Figure 31: Example Manual CS Partial .csv File Download Showing Alerts Details

2.14. Example Downloaded System Created TS .csv Alerts File (Partial)

A	B	C	D	E	F	G
Report generated on	Alert ID	Title	Origin	Created Date	Profile	List of Matched Sanction Group and Lists
21/02/2025 10:56:29	1141 Leah Bowman åt* David Cook		SCREENING	7/2/2025 15:50	DEFAULT	["label": "PERF PRVT LST", "category": "PERF PRVT LST"]
	1142 Shawn Ryan åt* Emily Steele		SCREENING	7/2/2025 15:50	DEFAULT	["label": "OFAC SDN", "category": "SANCTION"]
	1143 Kristy Peters DVM åt* Veronica Williams		SCREENING	7/2/2025 15:50	DEFAULT	["label": "OFAC SDN", "category": "SANCTION"]
	1144 Daniel Knight åt* Patrick Jensen		SCREENING	7/2/2025 15:55	DEFAULT	["label": "PERF PRVT LST", "category": "PERF PRVT LST"]
	1145 Tyler Decker åt* Breanna Cunningham		SCREENING	7/2/2025 15:56	DEFAULT	["label": "PERF PRVT LST", "category": "PERF PRVT LST"]

Figure 32: Example System TS Partial .csv File Download Showing Alerts Details

Note: The user should be aware that depending on the factors such as number of alert hits and the variable data loads involved, download time can vary extensively and should be considered when planning to select and download extensive numbers of alerts.

Note: In the bulk download of alerts, data related to 'Related Alerts' has been purposefully excluded to optimize download performance and ensure a faster and more seamless user experience. Of course, data related to 'Related Alerts' is included in single alert downloads, ensuring access to comprehensive details when needed.

2.15. Sorting Alerts

To enhance users viewing and processing of alerts list alert sorting includes the following functionalities:

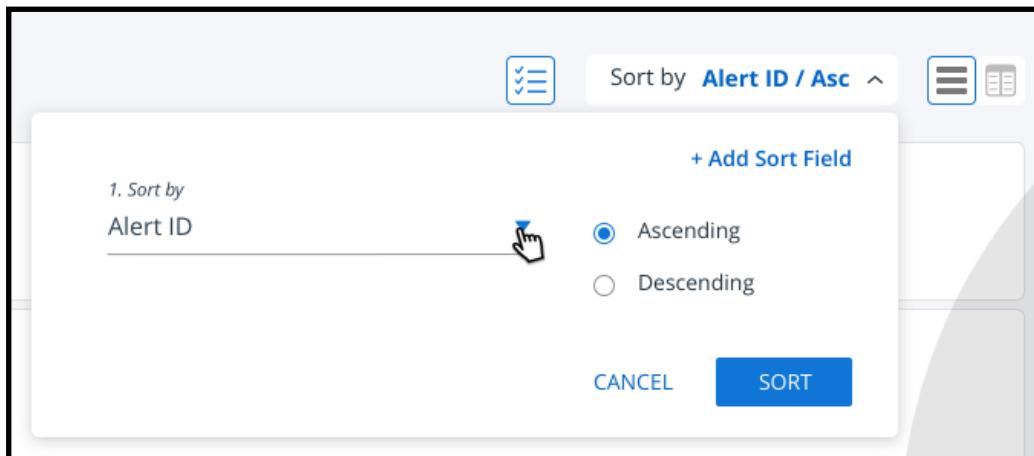
- Sort by field attributes and select sorting order - A to Z or Z to A
- Sort by Assignee - A to Z or Z to A
- For consolidated alerts, sort applied to original Risk
- Up to 4 custom sort by order sequences are possible

2.15.1. Examples of Sorting Capabilities

2.15.1.1. Sorting by Alert ID - or Select from List by Ascending or Descending Order

Alerts can be sorted per attribute by ascending or descending order as follows:

1. Click the down arrow next to the label () to display the Sort by ID / List all drop down menu and Ascending Descending radio button select options as shown below.
2. If the Alert ID is known then enter it or click the dropdown icon to display attribute options.
3. Select ascending or descending order.
4. Click Sort.



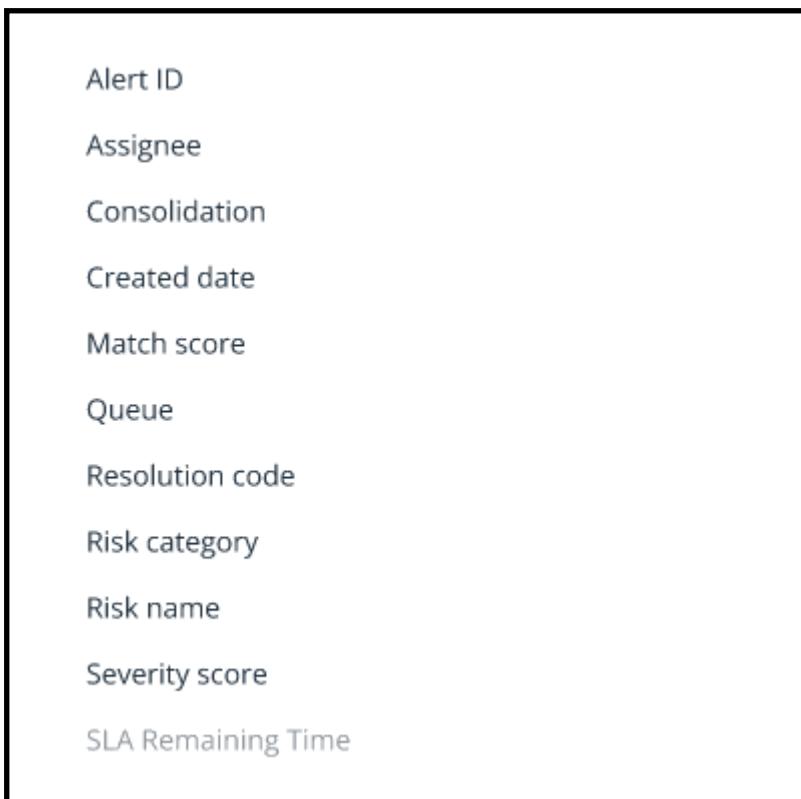
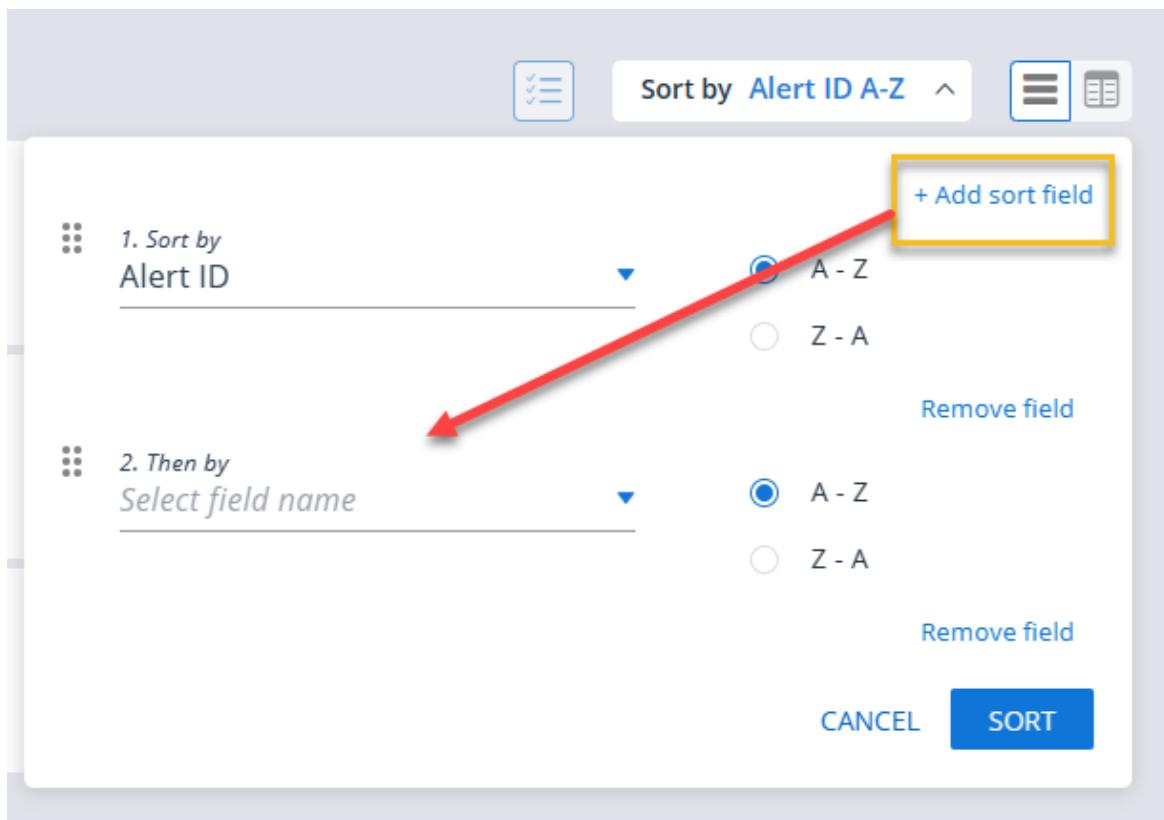


Figure 33: Example Sort by Dropdown List

Add Sort Field

You can select to sort by selecting from a list of provided field names.

1. Click + Add sort field link as highlighted below.



2. Select Field Name and repeat the process for sort by AlertID shown above.

2.15.2. Sort by Assignee

1. To sort by Assignee (analyst).

Enter the assignee by name or select from dropdown list.

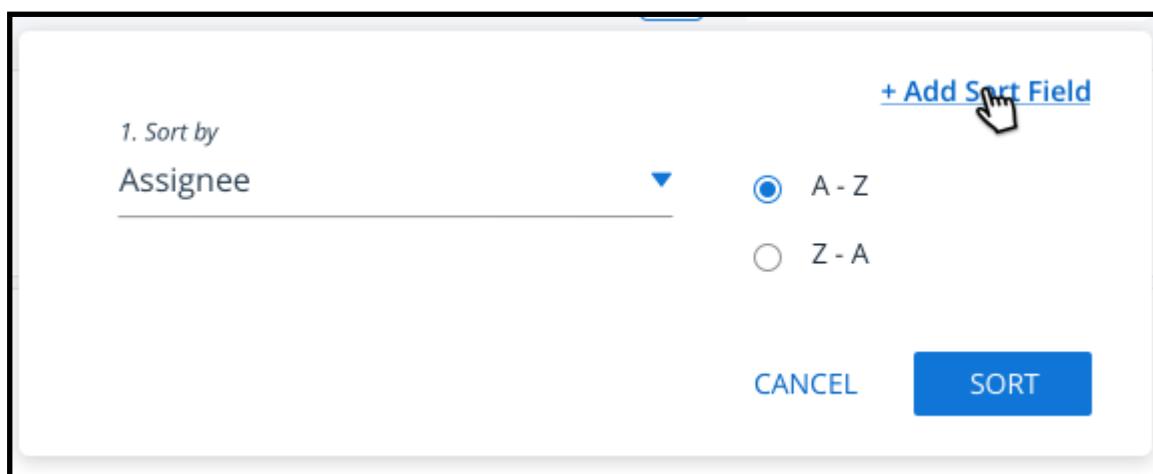


Figure 34: Example of Sorting by Assignee

1. Sort by

Assignee

2. Then by

Select field name

Error text is here

A - Z

Z - A

Ascending

Descending

CANCEL

SORT

Figure 35: Example if Error when Entering Field Name

2.15.3. Moving the Order of the Sort Field

If you require to move the set order of the sort fields, this is easily carried out by a simple drag and drop movement.

Anchor the cursor on the 6 dots element located at the side of the sort field, drag to the required position, then release.

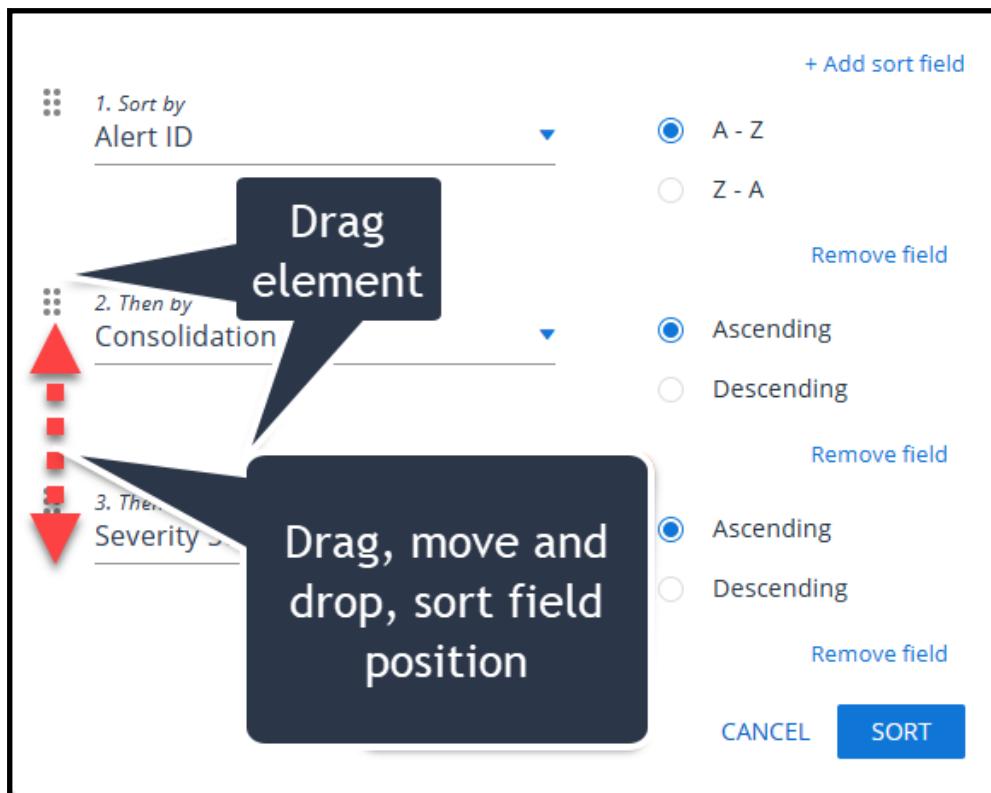


Table 4: Full List of Alert Sorting Attributes

Ref	Attribute
1	Alert ID
2	Assignee
3	Consolidation
4	Created Date
5	Matched Score
6	Queue
7	Resolution Code
8	Risk Category
9	Risk Name
10	Severity Score
11	State
12	Use case

Table 4: Full List of Alert Sorting Attributes (continued)

Ref	Attribute
13	Total number of hits

2. With reference to Table 1, select the attribute to filter by.
3. Select ascending or descending order.
4. Click the green tick to confirm.

Example of Notice Displayed When a sorting list has been removed requiring a new custom view to be saved

2.15.3.1. Screening Source Messages Sorting

This task is restricted to Business Admin personnel. Appropriate personnel should refer to IC settings (Mappers) for more information.

2.15.3.2. Sort by SLA Attribute by Remaining Time

Sorting SLA attributes is possible by remaining time with max or min time in ascending or descending order. By default SLA attributes are sorted by remaining time from min to max in ascending order.

2.16. Viewing Alerts in Card or Table Format

You can view alerts either in:

- Card format
- list table format.

By default alerts are shown in the card format.

1. To toggle the view click the alert view toggle button as shown in the following figure.



An example of alerts in a table list view is shown below.

Origin	Alert ID	Alert title	Assignee	Severity score	Match score	SLA stage	Resolution code
	000001	generic_anomaly_spain1...	Unassigned	95 (High)		Overdue	
	000002	generic_anomaly_spain1...	Unassigned	95 (High)		Overdue	
	000003	generic_anomaly_spain1...	Unassigned	95 (High)		Overdue	
	000004	generic_anomaly_spain1...	Unassigned	95 (High)		Overdue	
	000005	generic_anomaly_spain1...	Unassigned	95 (High)		Overdue	
	000006	generic_anomaly_spain1...	Unassigned	95 (High)		Overdue	
	000007	generic_anomaly_spain1...	Unassigned	95 (High)		Overdue	
	000008	generic_anomaly_spain1...	Unassigned	95 (High)		Overdue	

2.17. Viewing, Filtering and Changing Alert State

Investigating an alert is covered comprehensively in the chapter entitled Alert Details.

Alert Restriction Notice An analyst or supervisor can filter and view all alerts, however only users assigned to an alert and with the appropriate DPV permissions, can change the state of an alert.

Attempts by an unassigned user to select an alert for the purpose of changing its state are denied with following message as shown in the following figure.

The screenshot shows the 'All Alerts' page with 300 alerts. At the top, there are filters for Severity (All), State (All), and Resolution Code (All). Below the filters, two alerts are listed:

- AL_00008897** Created: 10/11/2021 5:14 PM
Jurisdiction risk associated with alerted account
Customer ID: 13000039691 * Customer Name: Jho Low * National ID: 50661316
- AL_65432431** Created: 21/03/2021 8:19 PM
Negative balance for 3 month_05b
Customer ID: 1800062692 * Customer Name: Shoes LTD * National ID: 9944

A modal window is displayed over the second alert, containing the message: "This action is permitted only if the alert is assigned to the user". A hand cursor is hovering over the "UNDER REVIEW" button in the modal. A callout box on the right side of the modal states: "Notice displayed, if alert not assigned to logged in user".

Figure 36: Example of Notice Displayed if an Unassigned User Attempts to Change State

3. Alert Investigation Workflow

On deployment of the Investigation Center, a default workflow is provided. If required, custom workflows can be created by the customer's business administrator's personnel to meet specific alert investigation needs. For more information, refer to the Admin Guide section of this guide > Custom Workflow - Management.

Regardless of the workflow model in place, the alert has a life-cycle, which involves changing through a series of states from new to closed. The first step for the alert is being created as a "NEW" alert, which is the initial state it receives. From this point and on it will change to different states, depending on which workflow is in use either default or custom and the manual changes made by the different assigned users. For example, the alert may be; put on hold, passed to a more senior review expert or closed. Alternatively, and this depends on the designed model workflow in place, the alert can be subject to various automatic system controlled changes such as a "two eyes review".

Additionally, default or custom workflow forms may be used to aid the analyst by semi-automating the task of informing supervisors on the current alert state.

The workflow detailed in this section is for example purposes only, as with most of the sections covered in this user guide, they can be custom designed to meet customer's needs.

In this example, workflow resolution is split between two persona, the Analyst and the Supervisor. The Analyst assigned with the task of reviewing investigating the Alert performs the initial investigatory work before passing the results and a recommended resolution to the Supervisor.

The Supervisor reviews the alert, assesses the recommendation and based on the evidence accrued, makes a decision on how to resolve the Alert.

If the decision is made to close the alert and subsequently, the further forensic evidence is revealed, the Alert can be re-opened for further investigation.

3.1. Alert State Lifecycle Diagram - Example

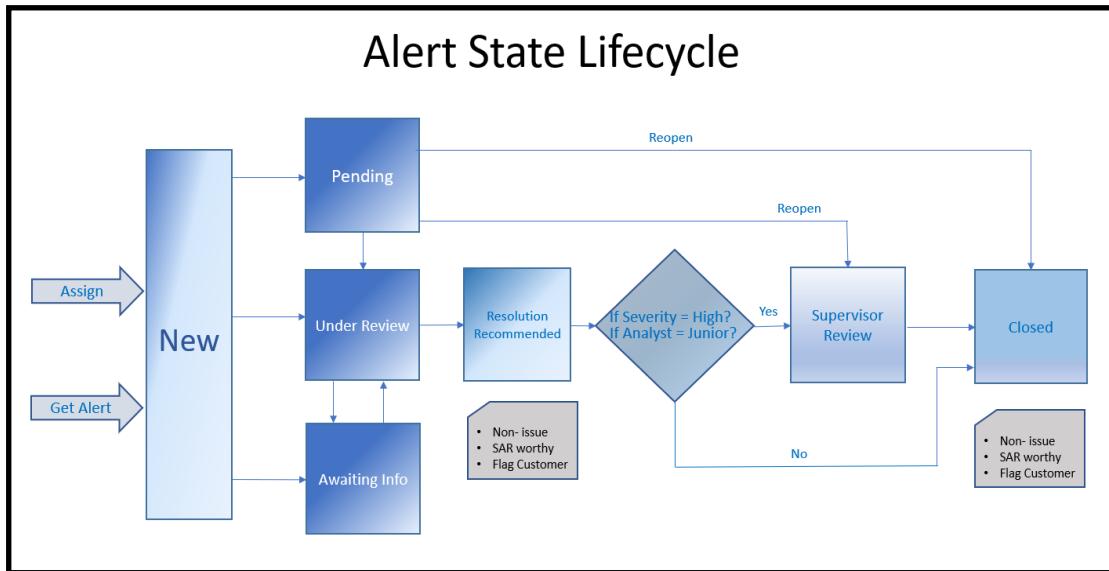


Figure 37: Example Alert State Lifecycle - Simplified Workflow Diagram

3.2. Default Workflow

The current default screening alert lifecycle workflow shown in the following figure. Although this is the OOB workflow included with most new deployments, if necessary and with the support of the Data Science team, the workflow can be customized to meet more complex workflow scenario requirements, and can for example include multiple levels of alert investigation.

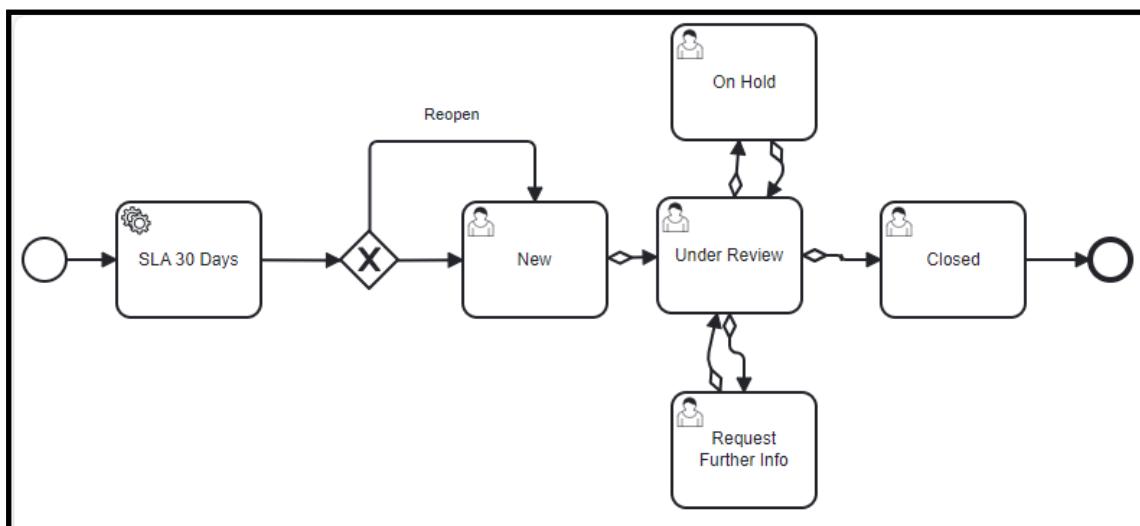


Figure 38: Current Default Workflow Model Included in New Deployments

3.3. Investigation Center Module Header

The Module Header shown in below is common to all views in the Investigation Center. From this header you can carry out the following actions:

- Expand and collapse alert list and queue both default and customized
- Search for alerts by Alert ID / Customer
- Get the next unassigned alert
- Create a new alert manually



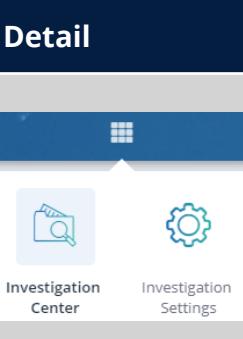
Figure 39: Investigation Center - Alerts Header

The main elements of the Module Header are listed, described and detailed in [Table 5](#): detailed below.

Table 5: Module Header- Element, Description & Detail

Element	Description	Detail
System-wide Alerts search	A text field that is used to search system wide for Alerts by specific parameters	Note: The search will search on all the fields which are marked "searchable" in the IC settings. Examples of Search by: <ul style="list-style-type: none"> • Alert ID • Customer Name • National ID
GET ALERT	The GET ALERT button allows the user to retrieve the next most important alert to be shared as defined by the Admin (Configurable order options)	
CREATE ALERT	The CREATE ALERT button allows the analyst or supervisor to create an alert Manually, and add it to the pool of alerts requiring investigation and resolution	

Table 5: Module Header- Element, Description & Detail (continued)

Element	Description	Detail
Module select matrix icon	At login, the user can select the IC module required (depending on such factors as user's permissions or, any module licensing restrictions in force)	

3.4. Manual Alerts

In general, alerts that populate the IC deployment are system sourced. During the alerts Investigation process there are instances where during the alert investigation process the analyst is made aware of suspicious transactional activity that requires him /her to create an additional alert manually.

The ThetaRay Investigation Center provides for manual alert creation that includes the following scope:

- The user can create a manual alert for each pair of definitions defined in mappers:
- Once created, support is provided for default tabs such as:
 - 'Risk details'
 - 'Related Alerts'
 - 'Documents'
- In addition the user is able to access global transactions via "View Transaction Table"

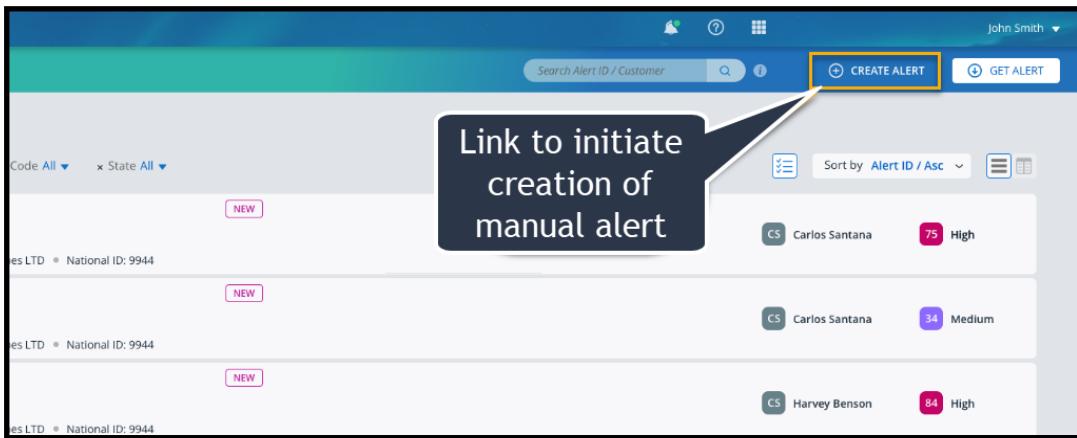
For more information on how the data that is created with manual alerts is used in default tabs refer to the chapter [Alert Details](#) that includes detail on the default tabs related to manual alerts.

Note: Depending on the particular solution or solutions being implemented in your IC deployment, the ability to create manual alerts may be restricted. For example, the creation of screening manual alerts is not possible.

3.4.1. Creating a Manual Alert

To start the creation of a manual alert or alerts, click the CREATE ALERT icon / link located at the top right of the Investigation Center landing screen as

indicated in the following figure.

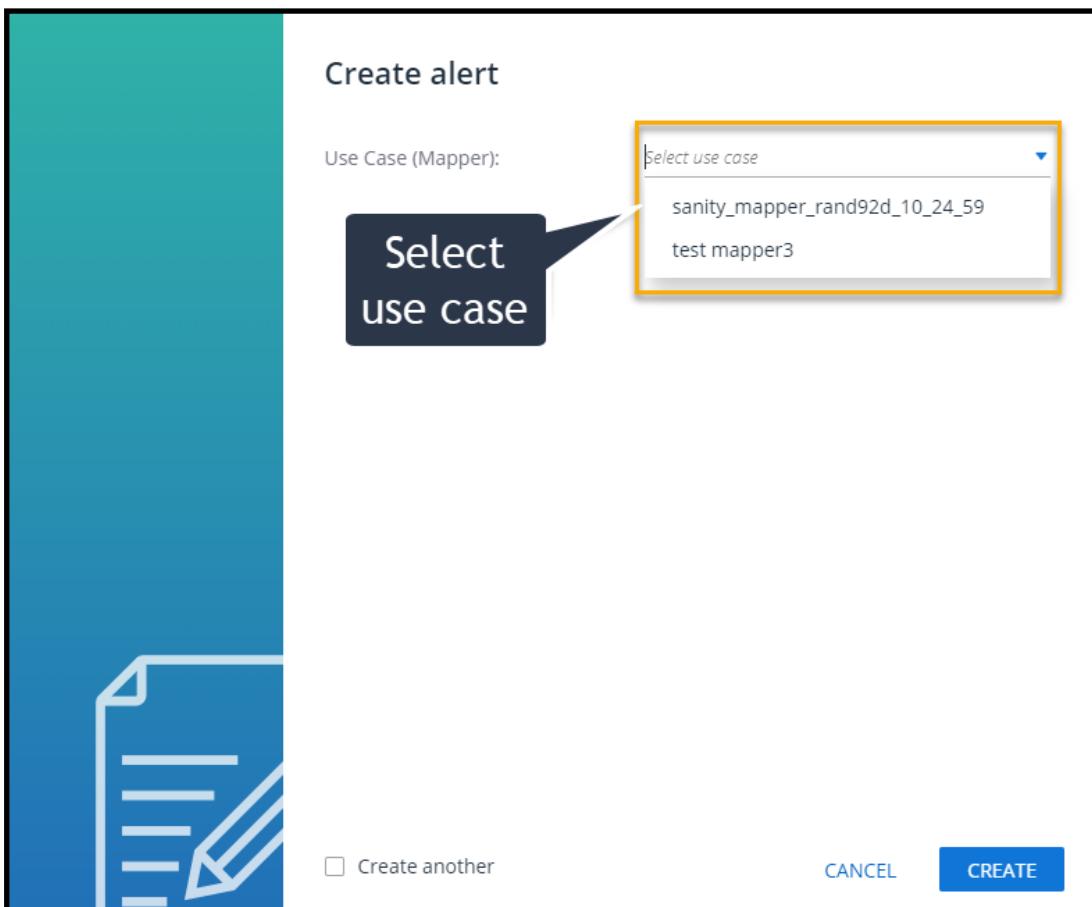


A screenshot of the Investigation Center interface. At the top right, the user 'John Smith' is logged in. Below the header is a search bar labeled 'Search Alert ID / Customer'. To the right of the search bar are buttons for 'CREATE ALERT' (highlighted with a yellow box and a callout bubble) and 'GET ALERT'. The main area displays a list of alerts. The first alert in the list is highlighted with a yellow box and a callout bubble containing the text 'Link to initiate creation of manual alert'. The alert details are as follows:

Code	Customer	Alert ID	Severity
1	Carlos Santana	75	High
2	Carlos Santana	34	Medium
3	Harvey Benson	84	High

Each alert row has a 'NEW' button on the left. The alert list is sorted by 'Alert ID / Asc'.

Figure 40: Location of Link to Initiate Creation of Manual Alert



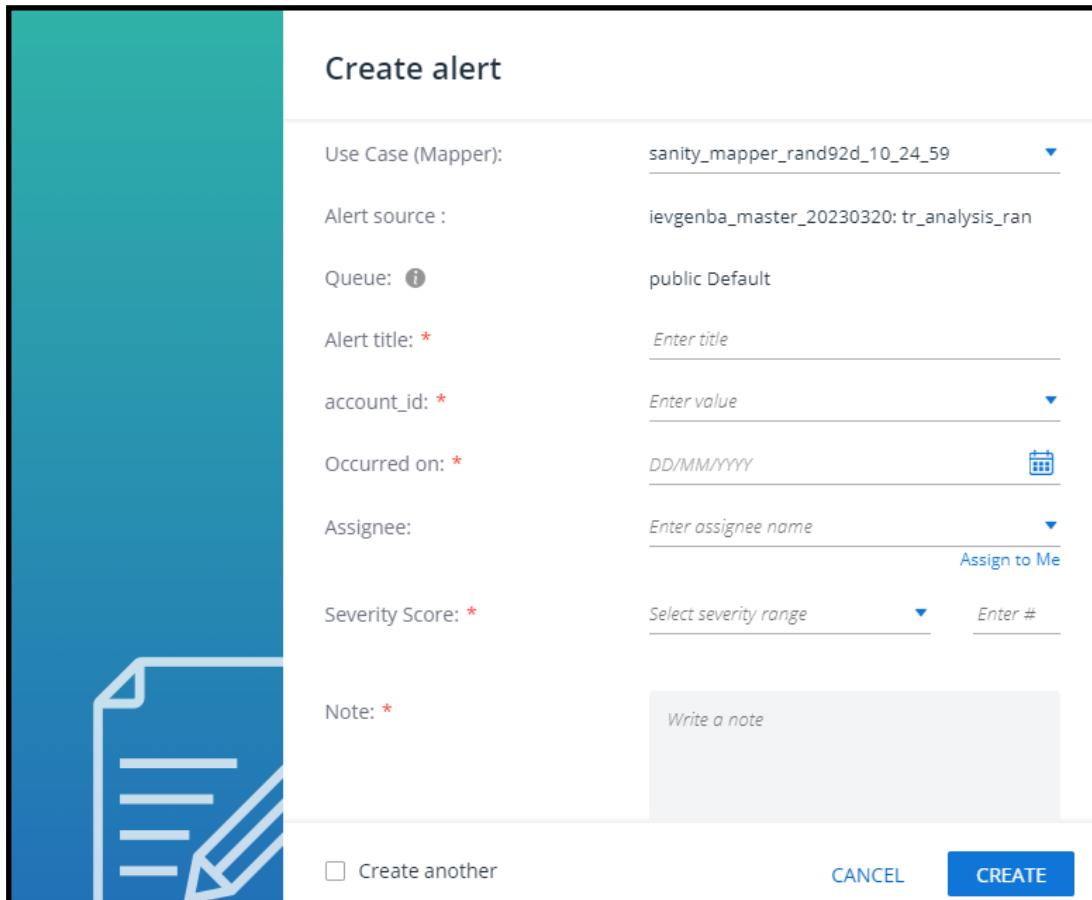
A screenshot of the 'Create alert' dialog box. The title is 'Create alert'. On the left is a large teal sidebar with a document icon. The main area has a label 'Use Case (Mapper):' and a dropdown menu titled 'Select use case' containing the options 'sanity_mapper_rand92d_10_24_59' and 'test mapper3'. A callout bubble highlights the dropdown menu with the text 'Select use case'. At the bottom are buttons for 'CREATE' (blue), 'CANCEL' (gray), and 'Create another' (checkbox).

Figure 41: Example Create Manual Alert (Stage 1 select use case)

» To complete the Create Alert Form as shown above:

1. Select use case.

On selection of a use case, the remainder of the form is displayed as shown below.



The screenshot shows the 'Create alert' form. The 'Use Case (Mapper)' field is set to 'sanity_mapper_rand92d_10_24_59'. The 'Alert source' field shows 'ievgenba_master_20230320: tr_analysis_ran'. The 'Queue' field is set to 'public Default'. The 'Alert title' field is empty. The 'account_id' field is empty. The 'Occurred on' field is empty. The 'Assignee' field is empty. The 'Severity Score' field has a dropdown menu open with options: 'Select severity range', 'High (70 - 99)', 'Medium (30 - 69)', and 'Low (1 - 29)'. The 'Note' field is empty. At the bottom, there are 'Create another' and 'CREATE' buttons, with 'Assign to Me' highlighted.

2. Provide a title for the manual alert.
3. Type the account_id or select from the drop down.
4. Enter the occurred on date manually, or select the date from the provided calendar widget.
5. Enter the alert assignee (for example, name of team member or "assign to me" to self assign the alert.
6. From the drop down menu, select a severity level and severity score as shown in the following example:

If, when entering a severity score value, the number entered is out of the range configured in IC Settings , the following error indication is displayed:

Assignee: [Assign to Me](#)

Severity Score: ⚠

Figure 42: Severity Score Value Entered is out of Range

7. Correct the amount until the red triangle disappears.
8. Add a meaningful descriptive note that provides the rationale for the creation of the alert.
9. In general if the intention is to create further alerts it is a good practice to tag the '**Create Another**' box.
10. Finally click the **CREATE** button and verify that a 'Manual alert <id.xxxxx> was successfully created message is displayed as shown below.

All Alerts 300 Alerts

[Add Filter](#) [Origin All](#) [Resolution Code All](#) [State All](#)

Alert ID	Created	Customer ID	Customer Name	National ID	Severity
AL_0000001	Created: 25/04/2021 5:14 PM	1800062692	Shoes LTD	9944	High
AL_654512431	Created: 21/03/2021 8:19 PM	1800062692	Shoes LTD	9944	Medium
AL_01093424	Created: 13/05/2021 3:43 AM	1800062692	Shoes LTD	9944	High
AL_00372817	Created: 11/03/2021 8:03 PM	1800062692	Shoes LTD	9944	Low
AL_01239876	Created: 09/04/2021 4:14 AM	1800062692	Shoes LTD	9944	Low

Figure 43: Example - Manual Alert Successful Creation Indication

11. If an alert is also required for any subsequent value pairs return to stage 1 select each pair and repeat the process

3.4.1.1. Create an Alert - Additional Information

1. In the alerts list, manually or system created alerts have a specific icon.
2. In the section that allows filtering by alert type, two alert creation types can be selected for filtering manual or System.

In the All Alerts example shown below the icon for manual alerts is shown.

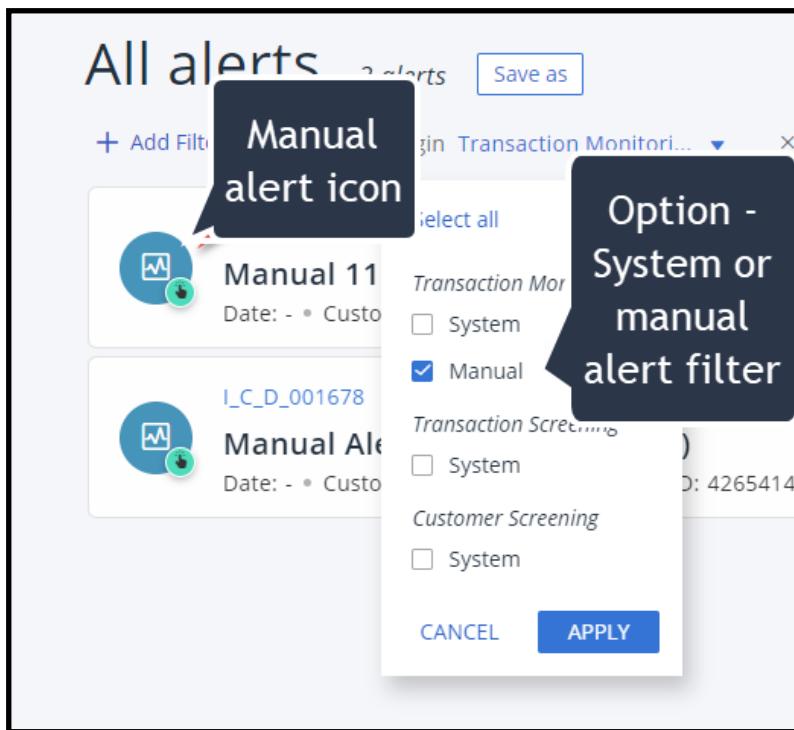


Figure 44: Example manual Alert Icon and Filter

3.4.1.2. Troubleshooting

Error #1 Indication Example :

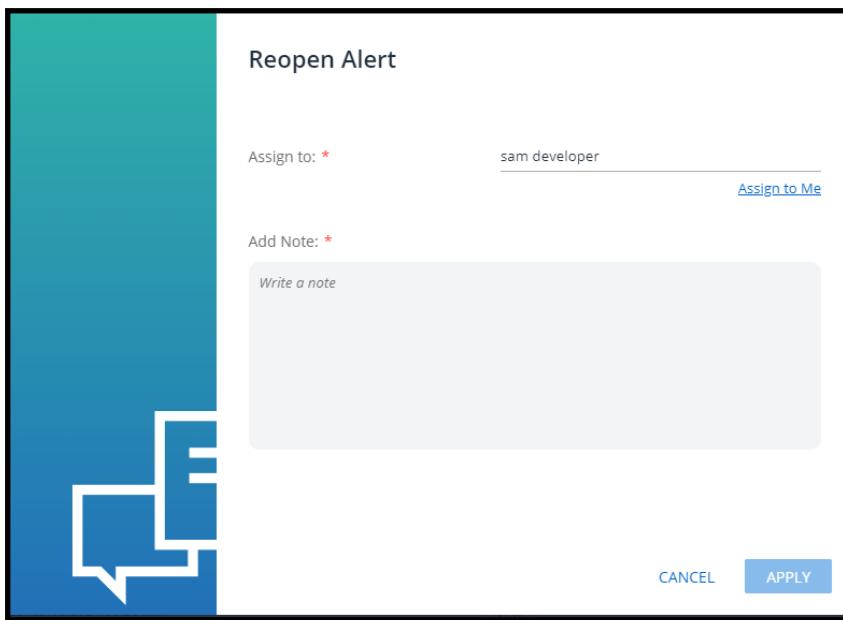
If, when attempting to create the manual alert form , a required field or fields is not included, clicking the CREATE button will highlight the missing fields. Troubleshoot - Fill required field(s) and retry to complete the process.

3.5. Re-opening Alerts

If after closing the Alert, new evidence is revealed, the Supervisor, with the appropriate permission, can if required, re-open the Alert. The Alert history actions are maintained as auditable, so that all the previous forensic evidence is still made available.

Depending on the alert investigation policy in place within the organization, the re-opened alert may be assigned to the original analyst, another analyst with more experience or escalated to a more investigation team. The state of the alert on re-opening is also dependent on the organizational policy. For example in some instances, it may be reopened in the 'Pending' state.

The Reopen form is shown in the following figure.



3.6. Analyst's Workflow

It is recommended to refer to the example while following the Analyst's workflow.

Note: The information provided here is for example purposes only. The exact workflow for an analyst may depend on such factors as:

- Analyst's experience level
- Alert workflow model in place
- Alert state changes mandatory notes requirements

Based on the example in the Alert State Lifecycle diagram shown above, and allowing for variances in deployment, the Analyst's workflow (high level) can be generally summarized as follows:

1. The Analyst, with appropriate permissions, receives the Alert assignment from the Supervisor. It can either be assigned with the task from its manager or pulled using "get Alert". Both will assign the analyst to work on the alert.
2. Selection of the New Alert by the Analyst changes its state to either:
 - a. **Under Review**, if selected by "get alert"- Or
 - b. **Pending**, if assigned by another user.
3. Depending on the investigation use case type, an SLA can be triggered on alert acceptance, to indicate to the assigned analyst the remaining time left for alert resolution.
4. Mandatory notes (with template pre setup in Auto-text Templates) are required to be completed before single or multiple alert state change can be instigated.

5. The Analyst then continues with the investigation process, (changes the status to Under Review).
6. If the investigation process requires querying other forensic evidence, the Analyst changes the status to **Awaiting Info**.
7. When enough evidence is available, the Analyst recommends a resolution and passes the Alert to the Supervisor (status changes to Resolution Recommended then to Supervisor Review)
8. Depending on the amount of experience the analyst has, a 'four eyes' review may be required to be performed by the Supervisor
9. If, during the investigation process evidence is uncovered that requires the creation of an additional alert , then an alert can be created manually. This manual alert is added to the pool of alerts requiring investigation and resolution

For more information on the Analyst's role in providing the alert recommended resolution, refer to the section [Recommended Resolution & Closing the Alert](#)

3.7. Workflow - Mandatory Notes Completion Tasks

As part of current workflow requirements, and to complement the existing mandatory alert closure note, and further improve the analysts work efficiency, the workflow design can include a mandatory note completion for any, or all of the state changes an alert will be subject to, as it passes from state to state.

Best practice Note: This will require the creation of such a set of appropriate auto-text templates to be added to the workflow at system implementation or upgrade.

3.7.1. Autotext Templates Usage with Mandatory Notes Completion

When investigating alerts, analysts are required to provide the rationale for alert closure resolution. This is a manual task and as such is time consuming

Note: Mandatory notes that are used with autotext templates are only applied to single alerts. These are not applied when working with bulk alerts.

3.8. Supervisor's Workflow

After the Analyst has provided a recommended resolution, and depending on the model workflow in place, the alert is normally passed to the Supervisor. The Supervisor, with the appropriate permission, takes control of the Alert's investigation process, releasing the analyst to continue with other alert investigation work. For further reference on the alert workflow, refer to the [Alert State Lifecycle Diagram](#).

The gathered evidence is reviewed by the supervisor and a decision is made on how to proceed. Depending on the workflow model in place and whether an automatic state change is programmed into the workflow, one of the following state changes could be made:

- Perform a 'four eyes' review , if the analyst is of junior status and/ or due to the severity of alert, company policy dictates a further check of the investigation findings is required, (this state change is normally programmed into the model workflow).
- Close the alert as a non-issue
- Open a SAR
- Flag the customer
- Pass the Alert back to the original Analyst for further investigation
- Escalate the alert to a more experienced investigation team
- Reassigning another Analyst with different expertise

For more information on the Supervisor's role in the alert recommended resolution on how to close the alert, refer to the section [Recommended Resolution & Closing the Alert](#)

4. Alert Details

The Alert Details section of the Investigation Center module contains comprehensive data on the Alert under investigation. This includes for example information on the Risk details, customer profile information (for example, solution and evaluation flow) and other important forensic evidence to help you in assessing the validity of suspicious Alerts.

Note: When working with Alert Details and making query requests to the alert database, all actions are logged in the Audit log.

» To display details of a specific Alert:

1. From the Alerts List, select the Alert of interest.

The Risk Details Tab opens (by default) and includes for example:

- Alerts created by the system (the level of risk the system created alert represents)
- Any alerts created manually (a summary of the key information the manual alert is populated with on creation)
- Information such as evaluation flow and source solution
- Essential evidences graphs
- Access to the Navigation bar that holds other static system tabs as well as any other custom tabs created by system admin.

Note: In order to change the state of an alert in Alert Details tab, the user must be assigned to the alert and have the appropriate permission set in user management.

4.1. Tab Navigation Bar

The Tab Navigation Bar provides you with access to the various tabs set for your particular Investigation Center module. As some of these tabs are static (denoted by (*) in the following list), and some dynamic (customizable), the following tabs list is shown for example purposes only:

- Risk Details
- Documents
- Custom tabs (examples; transactions, accounts)
- Transactions
- Notes

- History

An example of the Alerts Tab Navigation Bar with static tabs supplied at deployment is shown in the following figure.



Figure 45: Example Alert Screen Tabs Navigation Bar (Static tabs)

4.2. Risk Details Default Tab

The **Risk Details** tab allows you to view relevant information and evidences regarding the system created alert.

Actions and functionalities available in the Risk Details Tab include:

- Risk features description and details
- Essential evidence cards (by current data histograms and historical linear graphs)
- Added risks (if alert consolidation is enabled in the deployment)
- Viewing (Composite) transactions table
- Enlarging and reducing the transactions table
- Context related transactions time period filter
- Downloading transaction table contents
- Risk Resolution Layouts
- Displaying transactional data in tabular and graphical layouts
- Accessing the Network Visualisations graph data
- Navigation between alerted and non alerted transactions
- Filtering and manipulating data view in tables (including pivot)

To view the Risk details tab click the Risk icon

An example of a Risk Details tab is shown in the following figure.



Figure 46: Example of a Risk Details tab

Lets take a closer look at our alert Risk Details tab example:

4.2.1. Alert Card Details

1. As highlighted, the alert card containing all the alert details such as id, severity etc., as shown in the alerts list screen is redisplayed here (1) for your convenience.
2. Related navigation tabs for further investigation, included by default:
 - a. Customer Info.
 - b. Related parties.
 - c. Documents.
 - d. Related alerts.
 - e. Notes.
 - f. History.

4.2.2. Risk Details Overview

3. The Risk Details section (3) holds a summary of the alert, including:
 - a. High level overview description of the alert.
 - b. The evaluation flow from which the alert risk was identified.
 - c. Source solution.
 - d. Alerted activity unique identity number.
 - e. Alert period.
 - f. To allow you to investigate the alert in more detail (forensic and transactional evidence) a data table displayed along side the graph is

available so that you can drill down and manipulate the data, row by row if necessary.

4.2.3. Essential Evidences

Viewing in Graph Format

In the Essential Evidence section (4) graphs of the main trigger features data results are shown in descending order of importance. There are two graphs, one shows the Historic value and the other the Distribution across data population.

Examples of Essential Evidence graphs are shown below. Included is the metrics for the total number of evidences (trigger features) detected for the alert.



Figure 47: Example Essential Evidence Graphs

4.2.4. Viewing Evidence Data in Table Format

To view Essential Evidence data in a table format, simply click on the graph.

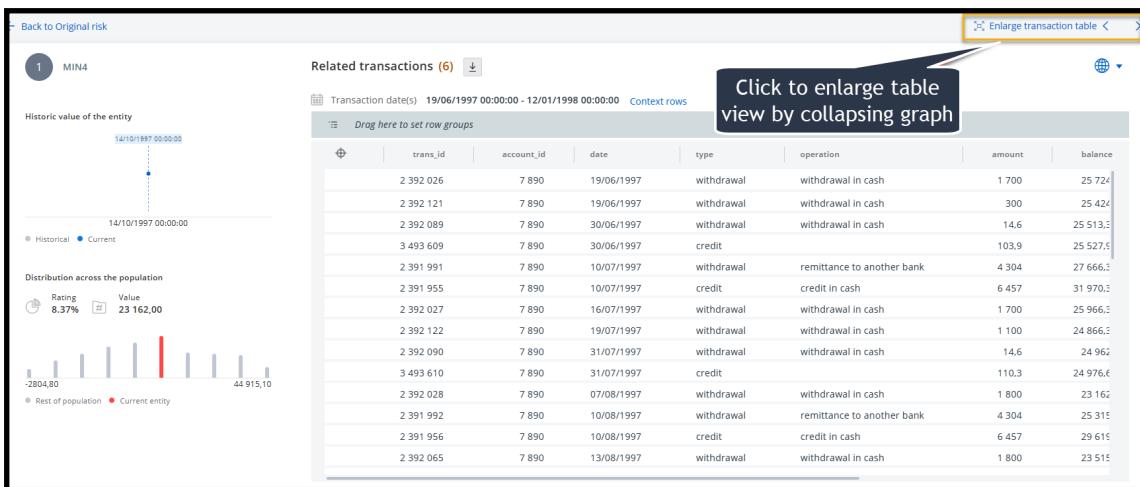


Figure 48: Example - Viewing Essential Evidence Data in Table Format Mode (Default Reduced)

To move to the next or previous table, simply click the Next > or Previous < arrow as shown in the highlighted link above.

4.2.4.1. Quick Transaction Search

To initiate the quick transaction search first click the GOTO link on the Details tab.

The quick transaction search allows you to quickly search and display, alert and non-alert transactions.

To initiate the quick transaction search first click the **Go to** link on the Details tab.

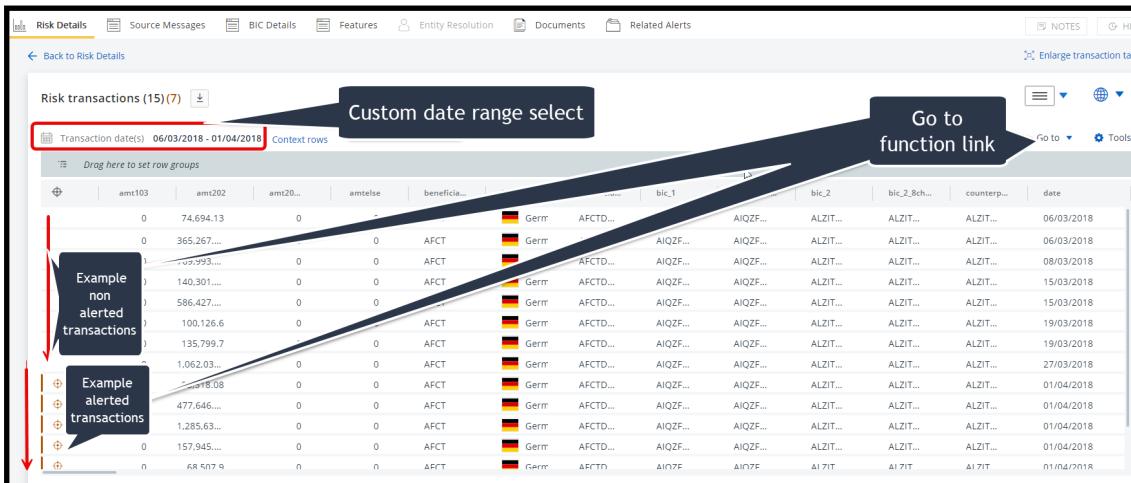


Figure 49: Quick Alert Type Search by Alerted/ Non-alerted Go to Link + Custom Date Range Select

A quick search for transactions is available by the following criteria:

- By alert type
 - By recent time period
 - By custom time period

4.2.5. By Alert Type

Either Alert transaction or non-alert transaction

An example of found alert transaction rows is shown below.

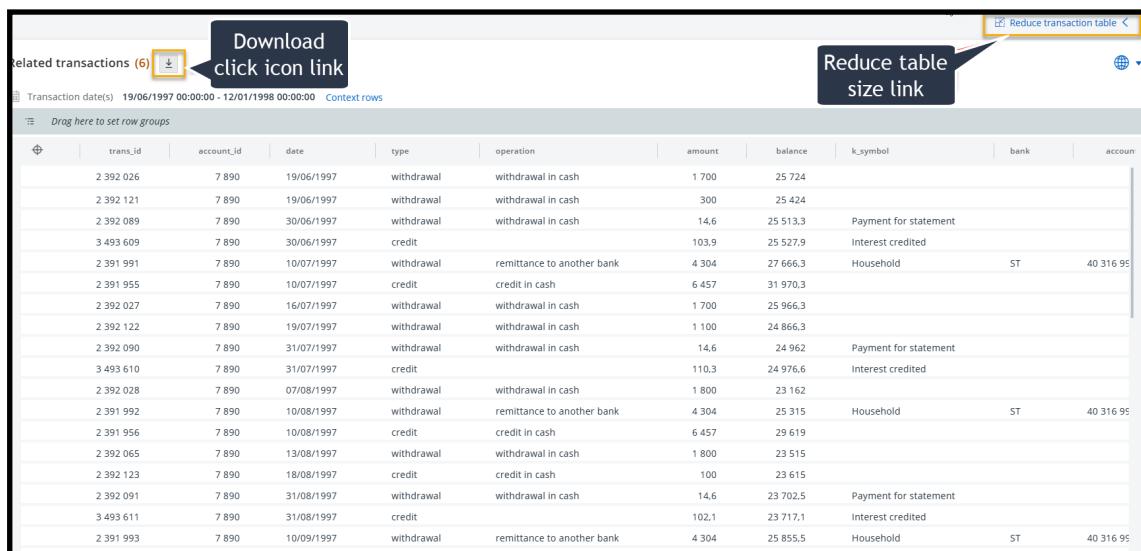
④ F1923474	Aug-2017	6,655	John Coltrain
④ F1923474	Aug-2017	6,655	John Coltrain
④ F1923474	Aug-2017	6,655	John Coltrain

Figure 50: Example List of Alert Transactions Found in a Quick Alert Search

4.2.6. Viewing Evidence Data in Enlarged or Reduced Mode

To view the essential the evidence table in an enlarged view, simply click the link shown in the above figure.

The graph collapses allowing the table to expand to fill the available space.



trans_id	account_id	date	type	operation	amount	balance	k_symbol	bank	account
2 392 026	7 890	19/06/1997	withdrawal	withdrawal in cash	1 700	25 724			
2 392 121	7 890	19/06/1997	withdrawal	withdrawal in cash	300	25 424			
2 392 089	7 890	30/06/1997	withdrawal	withdrawal in cash	14.6	25 513.3	Payment for statement		
3 493 609	7 890	30/06/1997	credit		103.9	25 527.9	Interest credited		
2 391 991	7 890	10/07/1997	withdrawal	remittance to another bank	4 304	27 666.3	Household	ST	40 316 95
2 391 955	7 890	10/07/1997	credit	credit in cash	6 457	31 970.3			
2 392 027	7 890	16/07/1997	withdrawal	withdrawal in cash	1 700	25 966.3			
2 392 122	7 890	19/07/1997	withdrawal	withdrawal in cash	1 100	24 866.3			
2 392 090	7 890	31/07/1997	withdrawal	withdrawal in cash	14.6	24 952	Payment for statement		
3 493 610	7 890	31/07/1997	credit		110.3	24 976.6	Interest credited		
2 392 028	7 890	07/08/1997	withdrawal	withdrawal in cash	1 800	23 162			
2 391 992	7 890	10/08/1997	withdrawal	remittance to another bank	4 304	23 315	Household	ST	40 316 95
2 391 956	7 890	10/08/1997	credit	credit in cash	6 457	29 619			
2 392 065	7 890	13/08/1997	withdrawal	withdrawal in cash	1 800	23 515			
2 392 123	7 890	18/08/1997	credit	credit in cash	100	23 615			
2 392 091	7 890	31/08/1997	withdrawal	withdrawal in cash	14.6	23 702.5	Payment for statement		
3 493 611	7 890	31/08/1997	credit		102.1	23 717.1	Interest credited		
2 391 993	7 890	10/09/1997	withdrawal	remittance to another bank	4 304	25 855.5	Household	ST	40 316 95

Figure 51: Example Essential Evidence Data in Table Format (Enlarged)

To return the table to default (reduced mode), click the link highlighted in the above figure.

4.2.7. Downloading Global Transaction Query Content

The Global Trace Query feature allows you to view and download transaction data from the Risk Details tab in TM alerts. The system behavior adapts based on the volume of transactions being queried.

- The number of transactions viewable is set by default at 50K.
- This threshold is customizable by system administrators

If required to modify the limit the deployment admin user should reach out to the customer support representative, who can arrange for this limit to be modified.

Examples of accessing and viewing the Global page are shown below

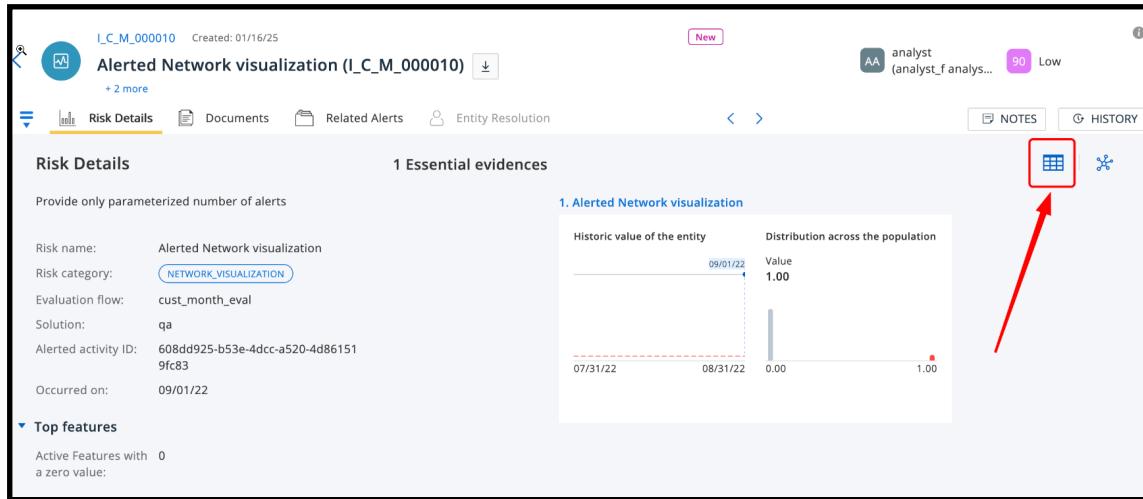


Figure 52: Example showing access the Global Trace Query Transaction Page from the Risk Details Tab

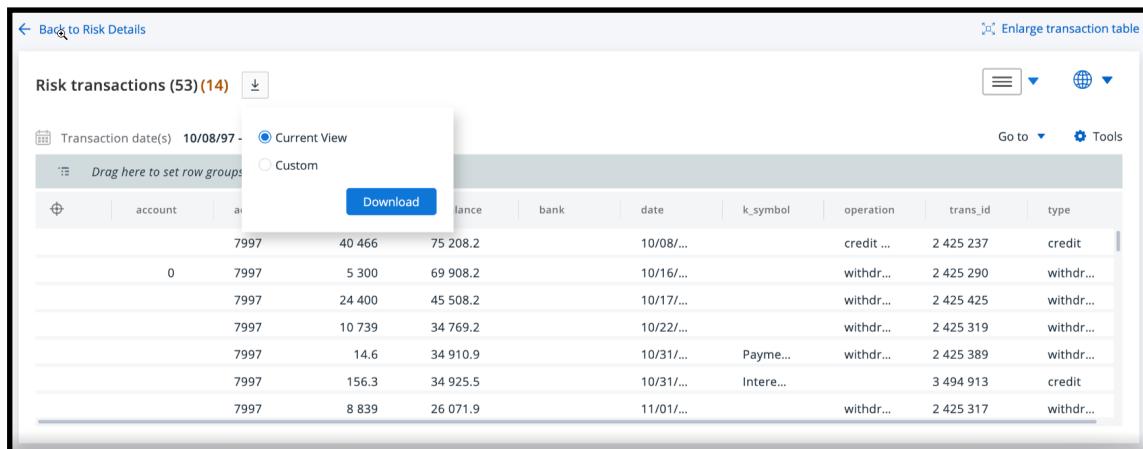


Figure 53: Example Global Transaction Page View

4.2.7.1. Viewing Transactions

For Queries Under 50,000 Transactions - No restrictions

For Queries Over 50,000 Transactions:

1. The transactions table will show an empty state
2. Table functionality is disabled
3. Only the Custom Download option is available

4.2.7.2. Downloading Transactions

Click the download button to access two download options:

Current View Download

1. Downloads the exact content displayed in your table
2. Includes any applied filters, groupings, or context rows
3. Only available for queries under 50,000 transactions

Custom Download

1. Available for all query sizes
2. Allows date range selection
3. Default dates match your trace query period

Using Custom Download

1. Date Selection
2. Click the date fields to open the date picker
3. The date picker automatically shows the trace query period
4. You must include the original transaction period in your selection
5. Selected "From" date must be earlier than the start of the transaction period, and selected "To" date must be later than the end of the transaction period.
6. Dates display in your system's global date format

Download Process

1. Click "Download" to initiate
2. The download button shows a loading animation
3. Downloads run in the background
4. You can navigate away or log out - the download will continue
5. When complete, if you remain on the same page, the file is downloaded through the browser.

4.2.7.3. Important Notes

- All downloads maintain existing encryption and user permission requirements
- The system enforces date range restrictions to ensure data integrity
- Downloads are browser-based and will complete even if you navigate away

The following example shows the situation where the maximum limit has been exceeded.

S_M_000003 Created: 06/10/2022

CLOSED Report_FIU Reopen

Sender Agent Address Only Rule (S_M_000003)

Receiver Name: John Smith

Risk Details Documents Related Alerts Entity Resolution

Risk transactions (210,178) (198,156) ↴

Transaction date(s) 03/10/2018 - 02/01/2019 Context rows

Sender ID Receiver ID Transaction Amount Transaction Currency

The requested number of transactions exceeds the allowed limit and therefore cannot be viewed. Please use the download option to view the transactions.

As shown above in this scenario when the limit is exceeded instead of transactions being displayed, instead the 'exceeded limit' note is shown.

(210,178) (198,156) ↴

03/10/20

Current View

Custom

From

Select or Type

To

Select or Type

Download

Figure 54: Example where Limit Exceeded leaving only Custom View Enabled

To enable you to investigate the table data in another application (e.g. Excel) you can download the content in a zipped CSV (,) comma delimited file format.

Note: The limit downloading transactions to view as an Excel formatted file is ~ 1 million transactions.

Troubleshooting Note: In general if there are any other issues relating to viewing Global Trace Query transactions it is suggested to check permissions to verify that the user in question has the necessary permissions to view data that has been encrypted.

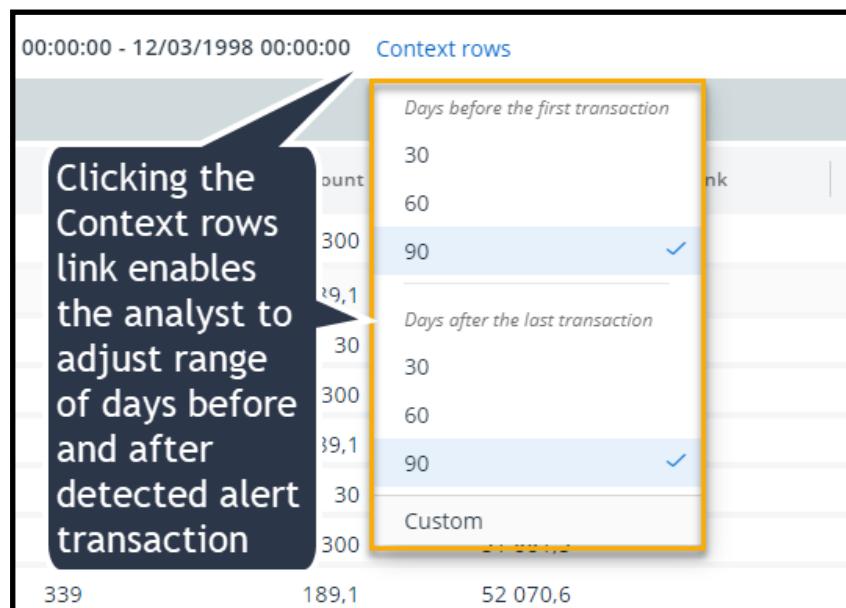
To ensure correct functioning of table and report downloads, commas used in numbering notation (as employed in certain countries or regions) are removed.

Data content from the viewed table is downloaded to your local machine.

Note: Only Table data that has been filtered can be downloaded. Pivoted data can **not** be downloaded (exported). If the download button is disabled, check the table is not displaying the results of a pivot function.

4.2.8. Context Rows Query Results

The range of related days before and days after the first and last transaction context rows can be configured from each feature table, by clicking on the Context rows link as shown in the following figure.



4.2.9. Risk Resolution Alert Types and Available Layouts

The goal of the layout capability is to enhance and expedite the investigation process of the global transaction table, focusing on the triggering of the entire alert, as well as feature-level tables that present transactions related to the triggering of a particular feature.

Each layout group has its own sub-levels, which are described in the tables below.

4.2.9.1. Global Transaction Alert Layout Types

Global Transaction Layouts			
Personal		Global	
Risk Name	General info	Risk Name	General info
A user saves a defined table layout for all their alerts with the same risk name as the current alert under investigation. This layout always supersedes the Personal General Layout, as well as the Global Risk Name and General Layouts.	A user saves a defined table layout for all their alerts, regardless of the risk name. A user saves a defined table.	A user saves a defined table layout for all their alerts with the same risk name as the current alert under investigation, making it available to all analysts on their team.	A user saves a defined table layout for all their alerts, regardless of the risk name, making it available for all analysts on their team.

4.2.9.2. Feature Transaction Alert Layout Types

Feature Transaction Layouts					
Personal			Global		
Risk Name	Feature Name and Risk Name info	General info	Risk Name	Feature Name and Risk Name info	General info
A user saves a defined table layout for all features and alerts with the same feature name as the current alert under investigation.	A user saves a defined table layout for all their alerts with the same feature name and risk name as the current alert under investigation. This layout always supersedes the Personal General Layout, as well as the Global Feature Name, Feature Name and Risk and General Layouts.	A user saves a defined table layout for all features, regardless of the name.	A user saves a defined table layout for all features and alerts with the same feature name and risk name as the current alert under investigation.	A user saves a defined table layout for all their alerts with the same feature name and risk name as the current alert under investigation, making it available to all analysts on their team.	A user saves a defined table layout for all features, regardless of the name, making it available to all analysts on their team.

Layout Selection is located under the Disk Details tab, provide the supervisor / analyst with the choice of either resolving alert risks in a global or personal configuration. To assist the analyst selecting a personal layout the **Recent Layout** (refer to the sub topic detailed below) feature enables the user to select a recently

modified layout to run and test the suitability before deciding to save it as the optimal personal layout.

Available layouts and options are shown in the figure as shown below.

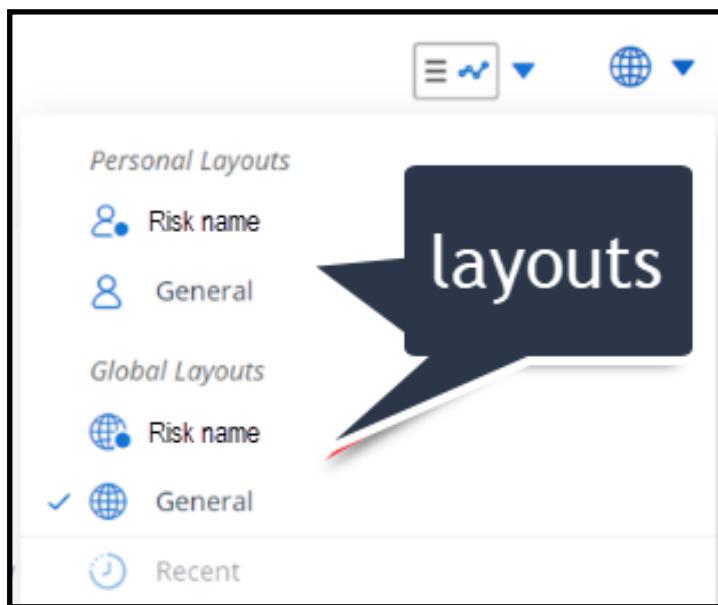


Figure 55: Layout Options, Personal, Global and Risk Types and Recent

4.2.9.3. Global Layout

The global layout is the default layout provided at deployment. This generic layout can be modified by Analysts and Supervisors with the appropriate permission. A Global layout that is modified and re-saved is applied to other analysts working on the same use case.

4.2.9.4. Personal Layout

The Personal layout enables each analyst to configure a custom layout to suit individual needs and preferences.

Note: A Personal layout supersedes a Global Layout in terms of display priority

Note: Once a personal layout is configured by the analyst, it takes priority becomes the new default layout and cannot be overwritten.

4.2.9.5. Global Layout

The global layout is the default layout provided at deployment. This generic layout can be modified by Analysts and Supervisors with the appropriate permission. A Global layout that is modified and re-saved is applied to other analysts working on the same use case.

4.2.9.6. Recent Layout

To make the transition from a global to a customized personal layout as smooth as possible, the user can modify the global layout in gradual steps , test out the modifications over a period of time, and when the optimal layout is achieved, save the changes as the preferred personal layout.

Note: Be aware, changes to your layout while in 'Recent layout' mode are temporary and only last until you log out or change alert, at which point any changes made to the layout are removed.

4.2.9.7. Editing a Layout

The current layout can be modified or deleted, by an Analyst or Supervisor (with permissions).

» To edit a layout:

1. From the Alert Details screen, select a tabular tab (e.g. **Transactions**).
2. Configure the tab layout to your preference.
3. Click the down arrow next to the layout icon displayed (Global  Personal  or Recent ) as shown in below
4. Select a layout from the layout categories available and click **Save as**.

A change layout popup message, requiring verification is displayed as shown similar to the figure shown [Figure 56](#): below.

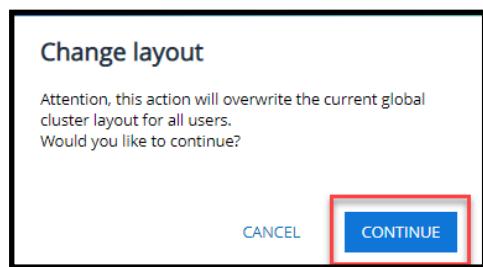


Figure 56: Change Layout Verification Popup Message

4.2.9.8. Adjusting what Data, and how Data is Presented in Transaction Tables

Regarding the Transaction tables structure, (eg column order, filtering, conditions etc.) the table structure is built according to the current standard 'AG-Grid' table

structuring technology, so the analyst can adjust the table structure to best filter display and compare the available data.

Filtering and column sorting menus are listed below.

Column Functions Including:

- Pin Column
- Autosize This Column
- Autosize All Columns
- Group by Data Type
- Rest Columns

Filter by Conditions Including:

- Equals
- Not Equal to
- Starts with
- Ends with
- Contains
- Not Contains

Filter by Columns

List of all available columns to select for filtering as shown in the example depicted below.

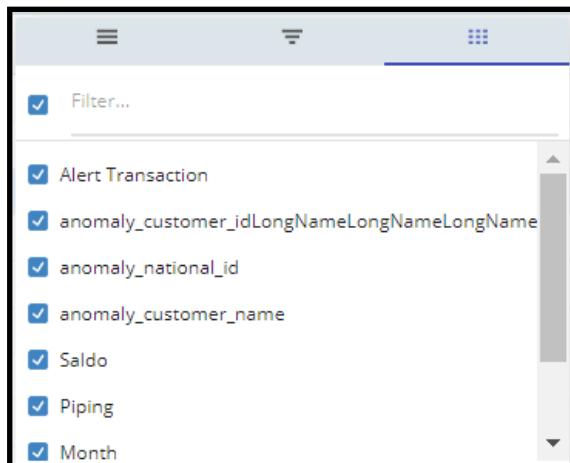


Figure 57: Filters Menu Options

» To access the filter options:

1. In the table, click to the right of the Column label to reveal the  menu.
2. Click the menu icon to display the Columns Filter and other options as shown in [Figure 57](#): above.
3. Click the  menu again to close the filters menu.

» To sort columns by order:

1. Toggle the selected Column label to sort by ascending or descending order.

4.2.9.9. Viewing Table Data

Data displayed in tabular tabs can be viewed as is, after filtering or aggregation (pivot)

Filtering columns to view is done via the Tools settings menu as shown in below.

» To select Tools menu:

1. Click the Tools icon .

The Tools menu is displayed as shown in below.

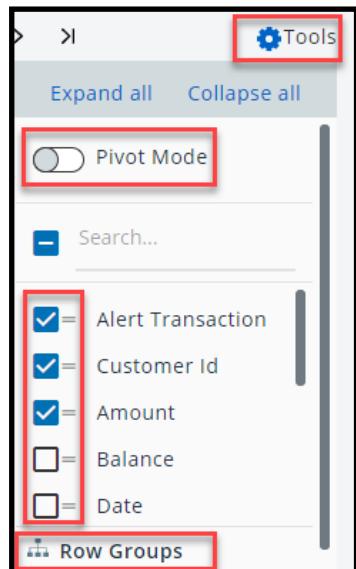


Figure 58: Tools Menu Example

2. To filter by selected columns, select the columns to filter by..
3. To pivot on table data, drag the column labels to the Row groups section or the Values section to aggregate results, then click the pivot box.

Data content from the viewed table is downloaded to your local machine.

Note: Only Table data that has been filtered can be downloaded. Pivoted data can **not** be downloaded (exported). If the download button is disabled, check the table is not displaying the results of a pivot function.

4.2.10. Risk Details Default Tab (Redesigned)

4.2.10.1. Introduction

The Transaction Monitoring Risk Details tab in the detailed view of the alert has been redesigned to include an updated outlook for alert analysis. The prime incentive for this upgrade option is to offer our customer's analysts a more intuitive way to investigate alerts.

Introducing a cutting-edge upgrade to our Transaction Monitoring alerts, designed to streamline and enhance the analysis of suspicious activity. This update introduces new visualizations that provide intuitive insights into alert patterns, along with an improved user experience to facilitate seamless navigation through alert details. Leveraging advanced AI capabilities, the system now includes summarization features that distill key information, enabling faster and more accurate decision-making. Together, these enhancements empower users to understand and resolve alerts with greater efficiency and confidence.

Note: With the introduction of the Risk Details design, existing deployments will of course be able to use the previous design for as long as necessary even after upgrading. In order to enable the redesign, configurations must be done on the platform and the view must be enabled in the IC settings. The redesign view will affect only newly created alerts from the enablement, the previous alerts will remain in the previous layout before upgrading. New customers deployments will be able to take advantage of the new design during the implementation.

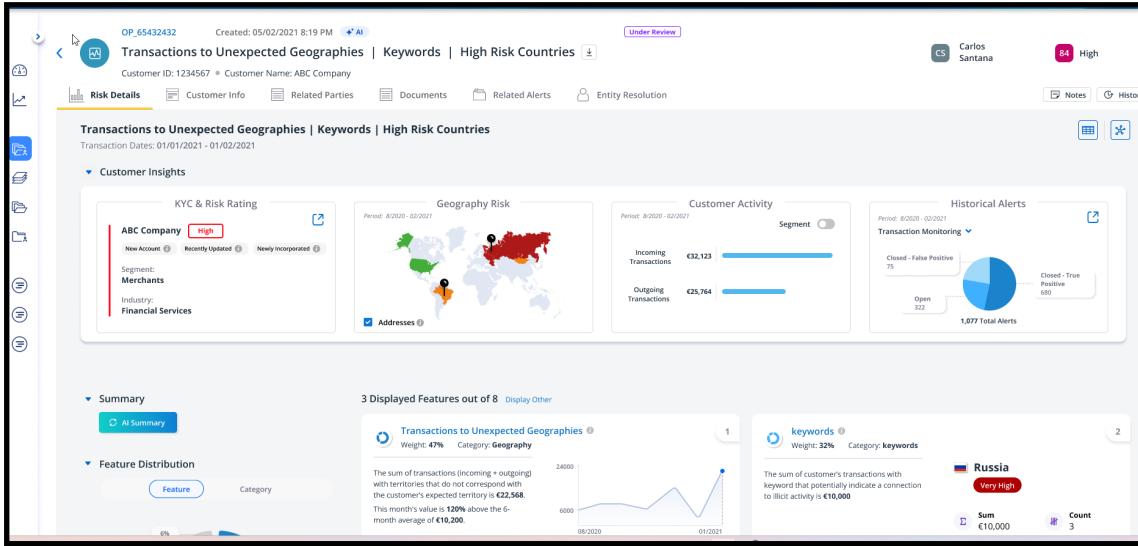


Figure 59: Example Landing Page Showing the Key Layout Features of the New Paradigm Risk Details Tab

In addition to the multiple enhancements the redesign includes, the Transaction Monitoring alert view has been split to support two main views, one for AI derived alerts and one for Rule derived alerts.

To better understand how to deal with AI and Rules derived of alert types let's drill down and take a closer look at the methodology associated with presenting the data contained in both alert types.

4.2.10.2. Analysis Methods

An AI-derived transaction monitoring alert is a notification generated by advanced artificial intelligence algorithms that analyse transactional data to identify patterns, anomalies, or behaviors, indicative of potentially suspicious or high-risk activities.

A rule-derived transaction monitoring alert is a notification triggered by predefined criteria or business rules, such as specific transaction amounts, frequencies, or geographic locations, to flag activities that may warrant further investigation.

Each alert is assigned an analysis method during its creation, which dictates its explainability layout and can be used to filter alerts in the all alert view as well.

Part of Analysis methods, both derived alert types can be filtered for under the System View side panel -> All Alerts -> + Add Filter as shown in the following figure:

All alerts

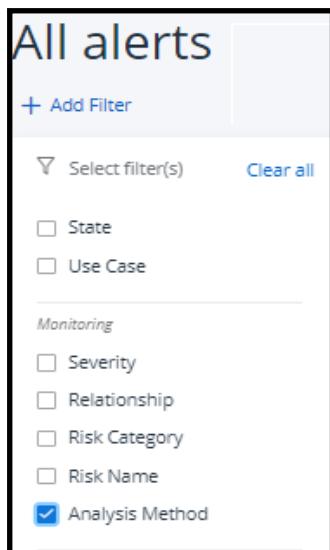
[+ Add Filter](#)

[Select filter\(s\)](#) [Clear all](#)

State
 Use Case

Monitoring

Severity
 Relationship
 Risk Category
 Risk Name
 Analysis Method



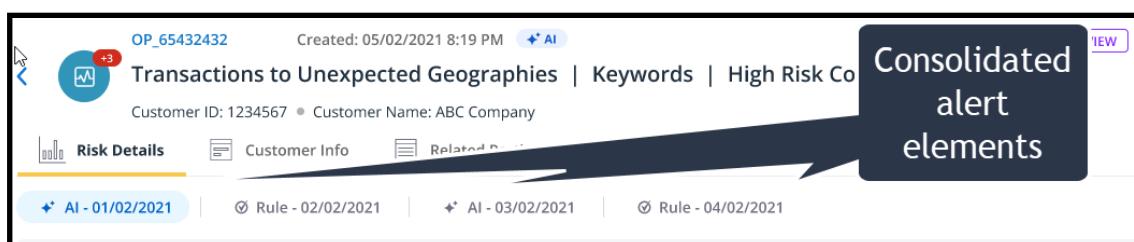
Alert Type	Alert ID	Created	Action
Rule Anomaly	asd_000009	11/11/2024 15:24:11	Rule
AI Anomaly	asd_000010	11/11/2024 15:24:11	AI

Figure 60: Example of Filtering for AI and Rule Alerts by Analysis Method

4.2.10.3. Consolidation

Alert consolidation methods are also applied to AI and Rules derived alerts throughout the IC module. The relevant analysis method and the creation date have been added to the consolidation tab in order to provide further insight into the nature of the consolidated alert.

Note: Consolidation between previous and redesigned alerts is not supported.

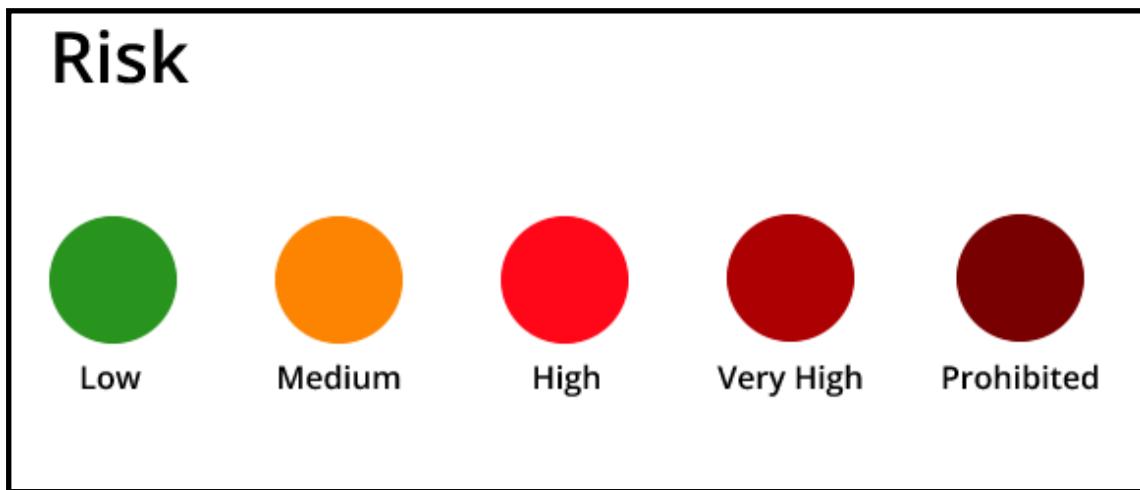


Alert Type	Creation Date
AI	01/02/2021
Rule	02/02/2021
AI	03/02/2021
Rule	04/02/2021

Figure 61: Example Consolidated Alerts of AI Based Alert

4.2.10.4. Color Code Legend

Throughout the Risk Details tab redesign feature it is important to note how color coding is used to signify severity levels across all graphs.



4.2.10.5. Alert Name and Transaction Date Range

4.2.10.6. AI Derived Alerts

Let's take a closer look at AI derived alerts. The AI alert card shown below is an example taken from a queue list.

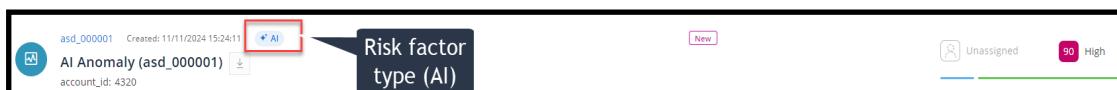


Figure 62: Example AI Derived Alert Card from Alerts Queue / List

Once entering the detailed view, the upgraded **Risk Details** tab allows you to view relevant information and evidences regarding the AI derived alert, including:

- Display of analysis method in the alert header
- Risk Name and Transaction Dates
- Customer Insight Widgets
- AI Alert Summary
- Feature Distribution
- Displayed Explainability Widgets

To view the Risk details tab click the Risk icon

Let's take a closer look at the redesigned enhanced Risk Details tab and discover how the task of distilling alert evidence more efficiently is achieved.

With reference to the tagged figure shown below:

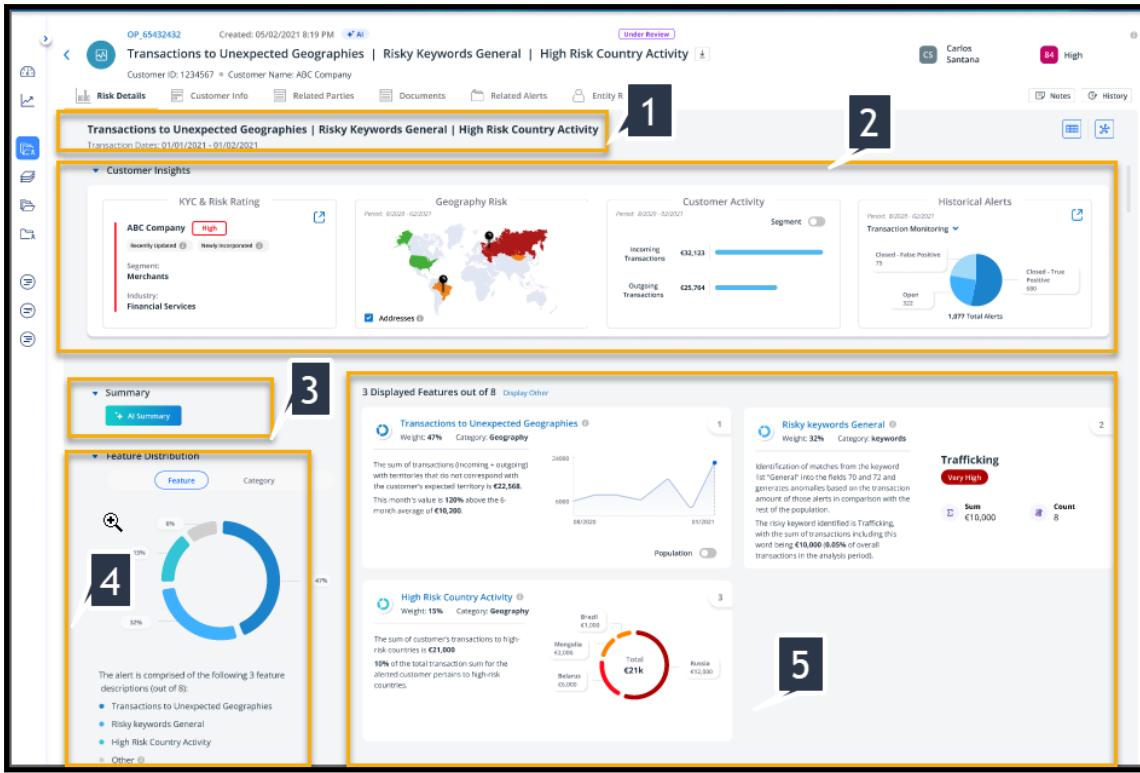


Figure 63: Example AI derived Alert

1. The feature risk name along with transaction dates signifying the transactions that were included in the analysis that resulted in the current investigated alert.
2. Customer Insights Widgets of the following types:
 - a. KYC information on the investigated entity.
 - b. Countries transacted with in the set time period, color coded according to risk level, and pinned significant addresses.
 - c. Transactional activity subdivided into incoming and outgoing transactions and showing the values and volumes of each subdivision. In addition, population data for comparison will be provided when available.
 - d. Historical alert information showing the number of alerts per status, for all applicable origins.
3. Licensed add-on that provides an AI sourced summary of the alert
4. A color coded 'donut' chart that shows all features contributing to the alert detection both as features and as categories.
5. Feature explainability widgets detailing information on the contributing features to the alert, including robust visualization options.

The alert name is present in the alert header as well as in the risk detail tab. In case of a consolidated alert, the alert header contains the name of the original alert and the additional alert names will be present in the relevant risk details tabs

Transaction Date Range reflects the dates of the transactions included in the analysis that produced the alert. Monthly or weekly analyses will present a date range, whereas a daily or real time analysis will show one date. The dates conform to the global date format selected.

4.2.10.7. Customer Insights

This section is common to both alert types, so the following description applies to both AI and Rules derived alerts.

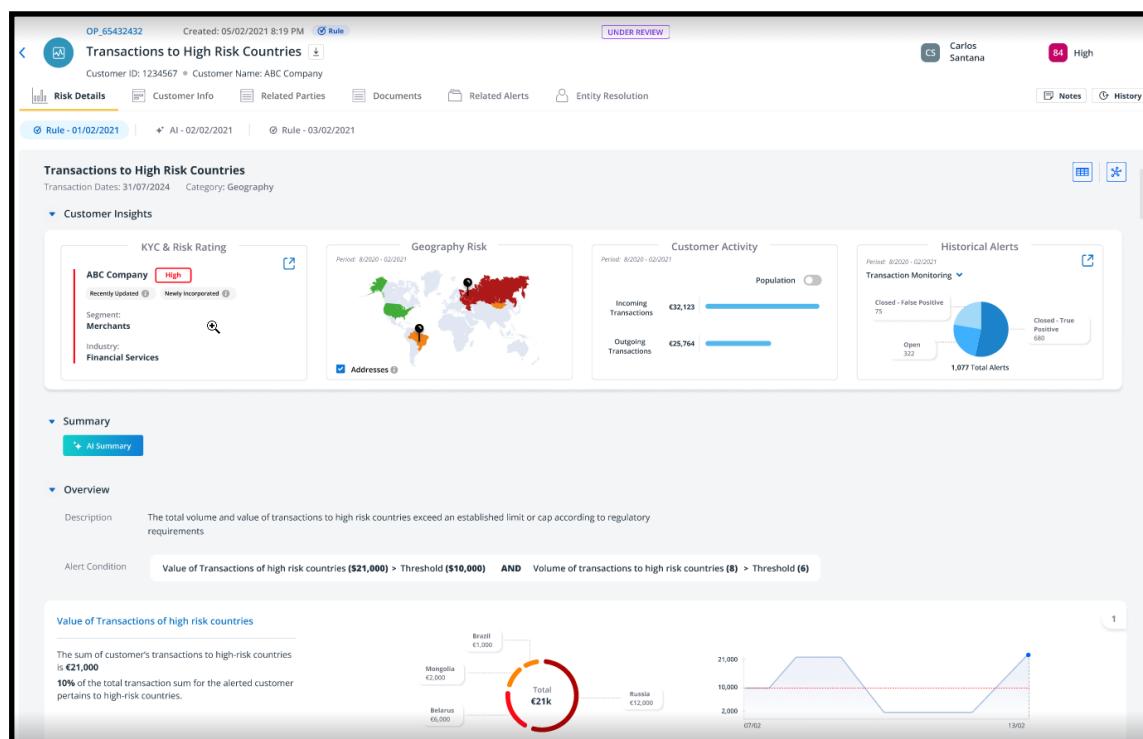


Figure 64: Example Customer Insights Relevant to both Alert Derivations, using Information Widgets

It provides the analyst via a set of varying information widgets, providing insightful information that combine to help the analyst grasp the key fundamental forensic evidence related to each alert and helping to make a more informed judgement on the validity of the created alert.

Customer insight widgets are meant to provide a high level view of the investigated customer, including overviews into the transactional activity, risk level, KYC details, etc.

The four types of Widgets shown in the example are detailed as follows:

4.2.10.8. KYC & Risk Rating Widget

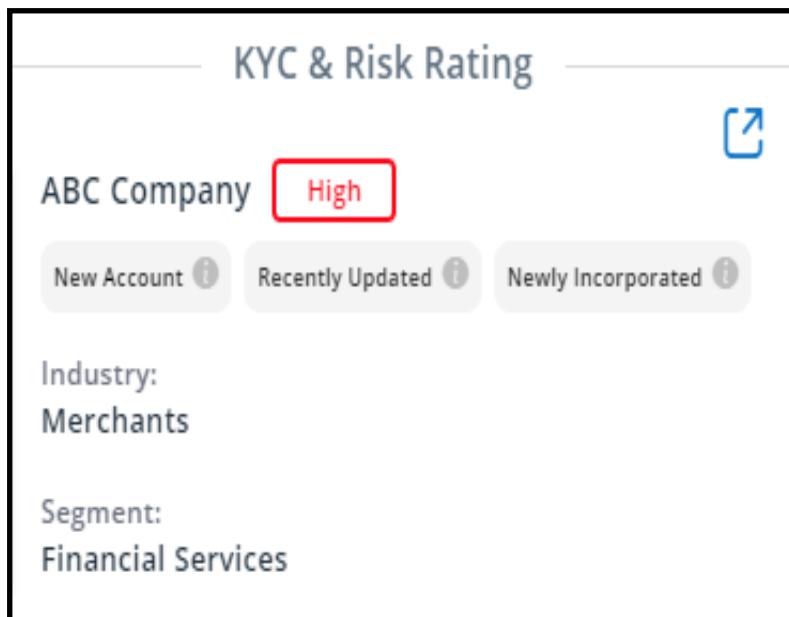


Figure 65: Example KYC & Risk Rating Widget of Alert Insights

The KYC & Risk Rating widget includes:

The widget will always include the investigated customer's name and key attributes such as Industry, Occupation, Segment, etc. The key attributes can be set at a project level, and different ones can be shown depending on the customer type (individual or business).

In addition, the risk level will be present if available from the KYC data.

KYC tags

New Customer - will be shown in case the customer has recently been added, the timeframe is configurable.

New Account - will be shown in case the account related to the current alert is considered to be new. The time frame for this is configurable as well.

Recently Updated - will be shown if any data for the customer has been recently updated, in the configured time frame.

Newly Incorporated - will appear if the customer (of type business) has their incorporation date with the configured time frame.

4.2.10.9. Geographical Activity Widget



Figure 66: Example Geographical Activity Map Widget of Insights

The geographical widget provides the analyst with a global overview of the customer's transactional activity per region, with each region represented by a color indicating the level severity risk. In addition to highlighting the countries transacted with in the given time period, important addresses are marked with pins on the map. An option to remove the pins is present in the "addresses" checkbox at the bottom of the widget.

4.2.10.10. Customer Activity Widget

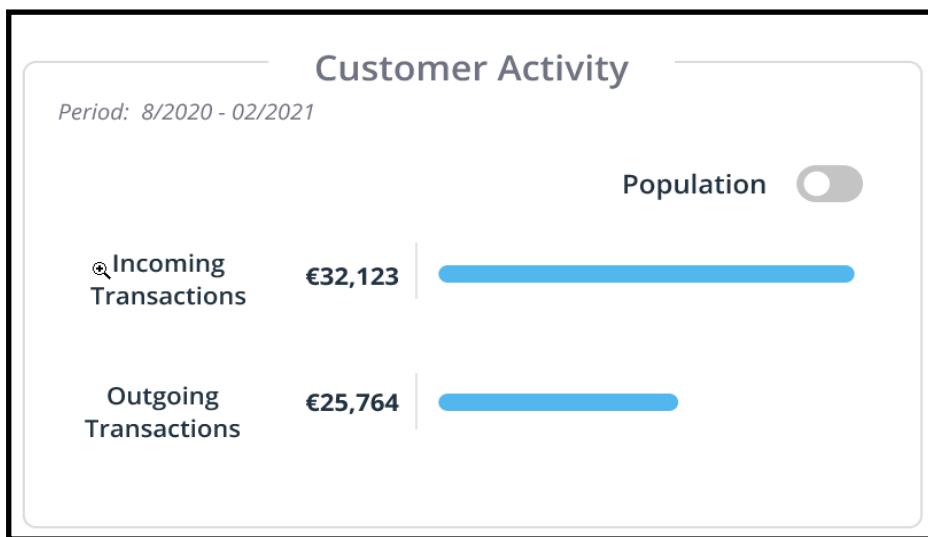


Figure 67: Example Customer Activity Widget of Insights

The Customer activity widget provides the analyst with separate outgoing and incoming Transactional statistics and bar charts indicating relative volumes for comparison purposes. These are displayed for a specific time period and an additional overlay of population behavior within the time period can be added via the checkbox if the data is available.

4.2.10.11. Historical Alerts Widget



Figure 68: Example Historical Alerts Widget of Insights

The historical alerts widget provides the analyst with a status breakdown of the additional alerts triggered for the same investigated customer. The widget shows data for a specific time period, similar to the previous two widgets. The historical alerts are shown by origin, if there is more than one, for example, Transaction Monitoring, Customer Screening, etc. The status breakdown provides insights to whether the additional alerts are Open, meaning still under investigation, Closed False Positive or Closed True Positive.

4.2.10.12. AI Alert Summary

An alert summary using Open AI is a licensed add-on, which if included in the deployment provides the user with an in depth summary of the AI derived alert.

It is activated by clicking on the AI Summary button icon .

For deployments with the add - on feature enabled clicking on the AI Summary reveals in- depth information.

4.2.10.13. Feature Distribution

AI alerts are comprised of features and their weighted contribution. The chart shows the leading features that contributed to the creation of the AI Alert, and they are the main ones that explain it as they received the highest weights. The threshold for displaying the features is configurable via the IC Settings. If the threshold is set to 70% for example, the features shown are the ones that add up to at least 70% of the overall feature weights. The additional features with lower weights, can be found in the "other" section of the chart.

As an AI derived alert is feature source oriented, it is differentiated from a Rules alert by the inclusion of the feature distribution section which includes information about the relevant features that contributed to the alert's creation displayed either

with its percentage contribution percentage indicated on a doughnut chart and legend list as shown in the following example:

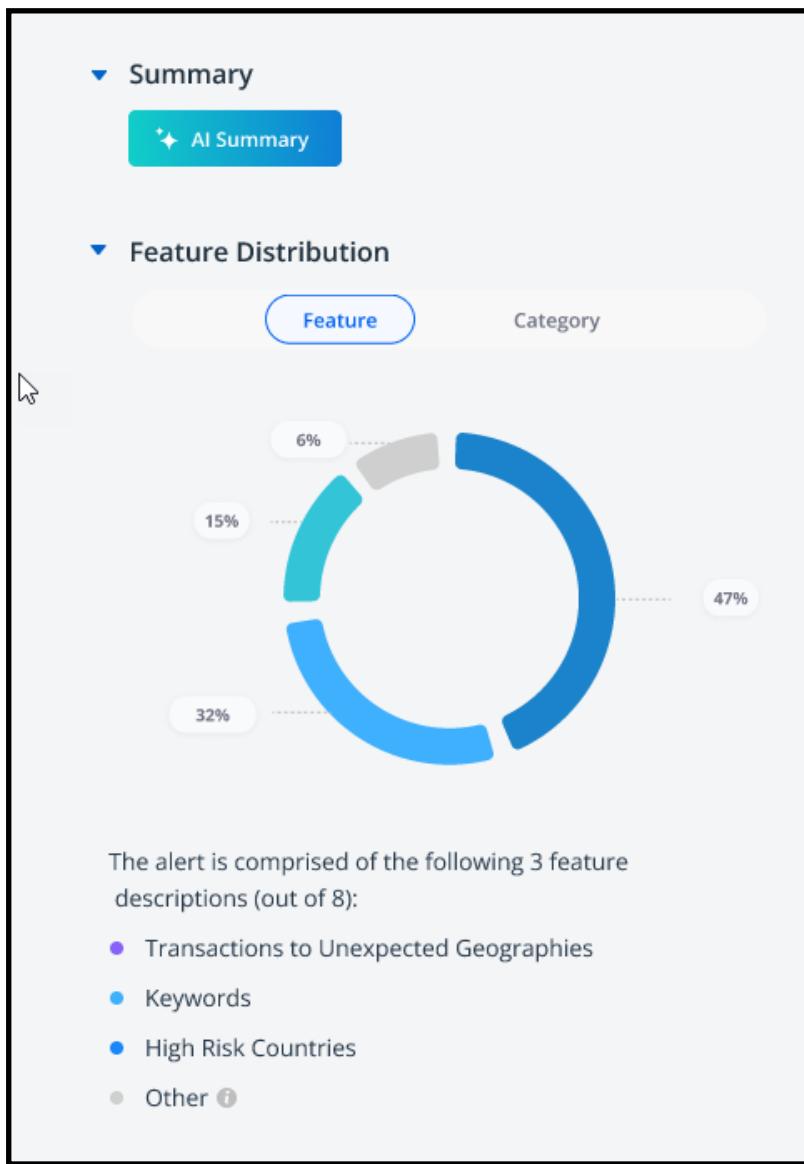


Figure 69: Example AI Feature Distribution Showing Related Features with Legend Color Identification

Category Distribution

Apart from Feature statistics view in the graph donut, the user can select to view the displayed feature distribution by Category view, as shown in the following example figure.

Each feature has a category aligned with the relevant associated risk. The category distribution chart shows the leading category of the features contributing to the alert. As it's possible for features to share the same category, it provides insights as to the nature of the alert. In the example below we can see that more than 50% of the features belong to the Geography category.

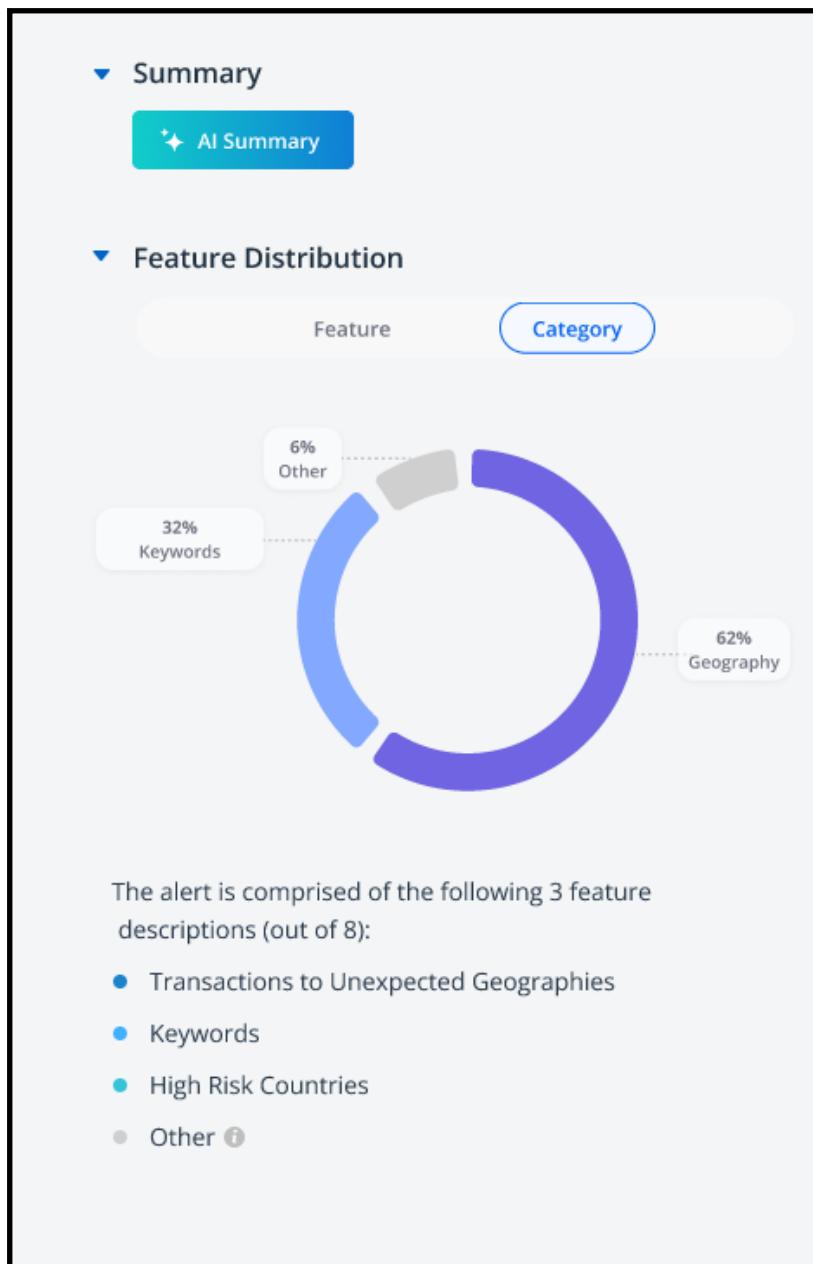


Figure 70: Example Donut Chart Selected to View by Category

Feature Highlighting

Regardless of which donut view is selected, to help the analyst get a quick view of data stats in context, hovering over the data stats highlights where else the data is used in the feature distribution description. In both Feature and Category donut views, hovering over a section highlights the corresponding feature or category name in the legend underneath the chart, as well as the corresponding feature widget. For the category distribution, if more than one feature belongs to the category, both feature explainability widgets are highlighted.

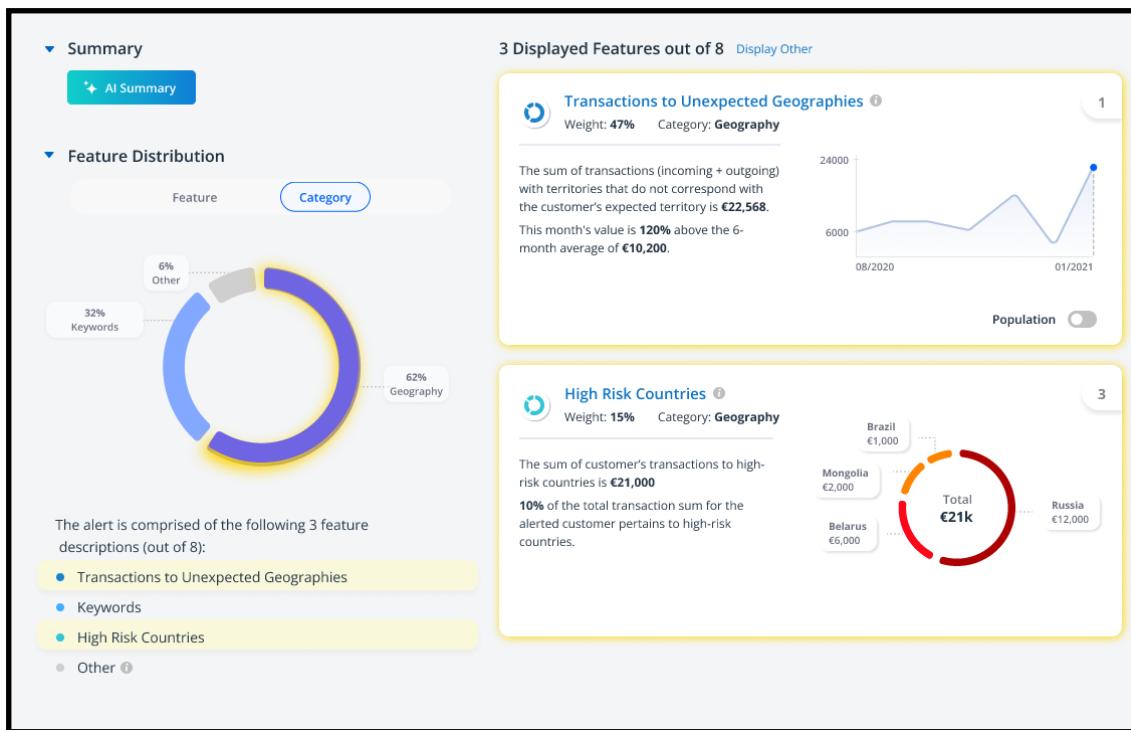


Figure 71: Example - Hovering over Stats, Highlights more Instances where Alert Sub features are Used

Feature Widgets (Essential Evidences)

Feature Widgets provide essential forensic evidences that include:

- **Feature Icon**- Donut image of various colors that is color coded to represent the corresponding color on the feature distribution donut chart
- **Feature Name** - name of the feature, eg. Transactions to High Risk Countries
- **Feature Description** - can be found when hovering over the info icon following the feature name. This description pertains to the feature itself
- **Feature Weight** - Expressed as a percentage indicating the proportion to which the feature contributed to the creation of the alert, e.g. 5%.
- **Feature Category**- Client specific designated category, e.g. Geography, Transactional, etc.
- **Feature Dynamic Description**- A detailed description of the feature with relevance to the investigated alert. This description includes data relevant to the alerted customer and the transactions that caused this feature to contribute to the alert.
- **Feature Explainability Visualisation** - various types of charts that show visually a specific aspect of the feature either from a historical , categorical, binary, or some form of behavioral change point of view.

The example shown below is the key Essential evidence feature and other relevant evidence examples are also shown .



Figure 72: Explainability Example 1

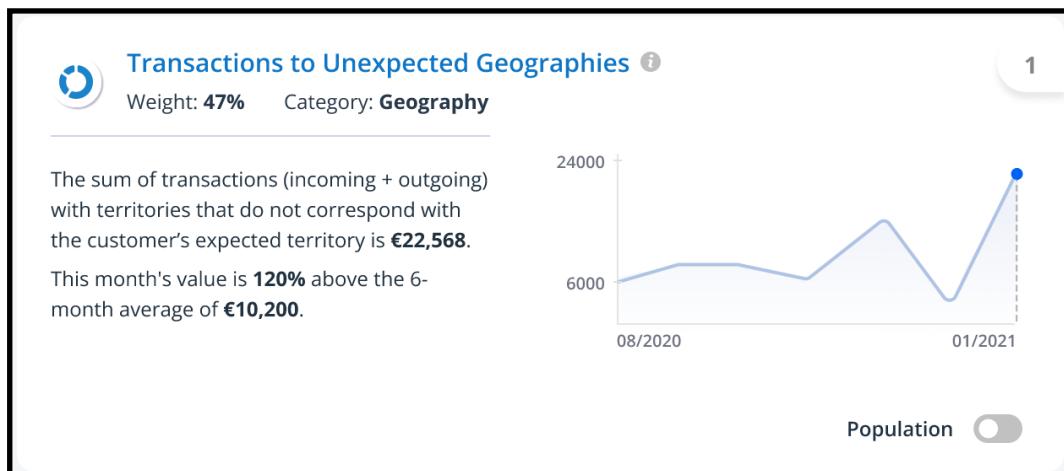


Figure 73: Historical Explainability

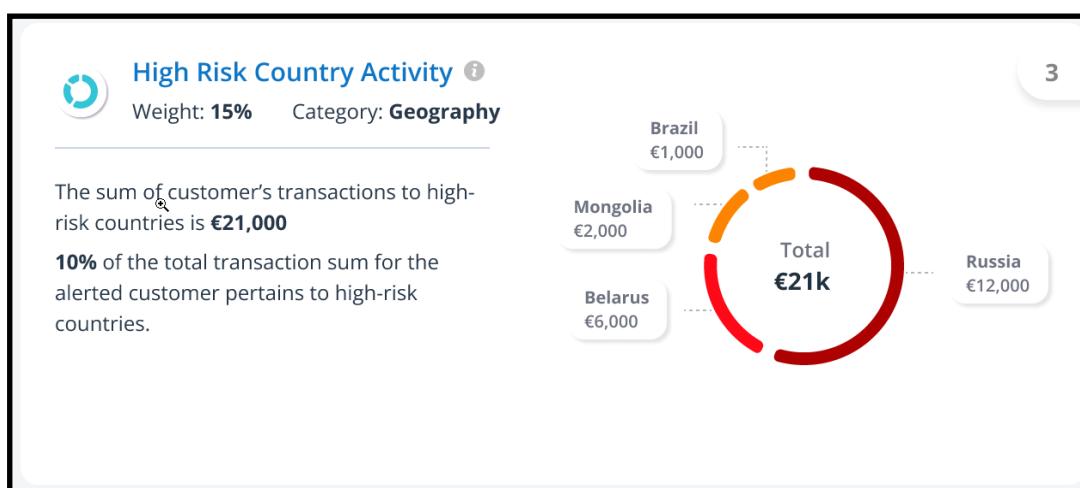


Figure 74: Categorical Explainability

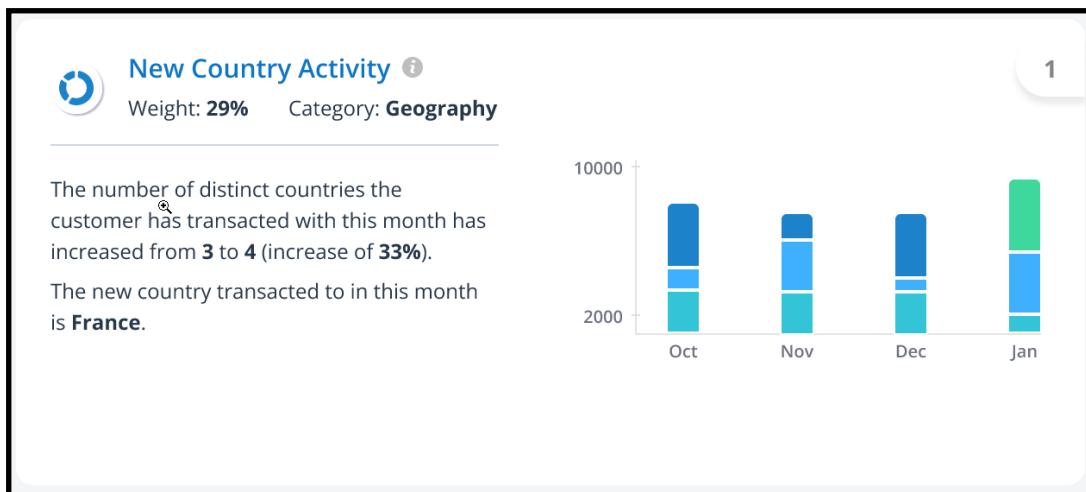


Figure 75: Behavioral Change Explainability

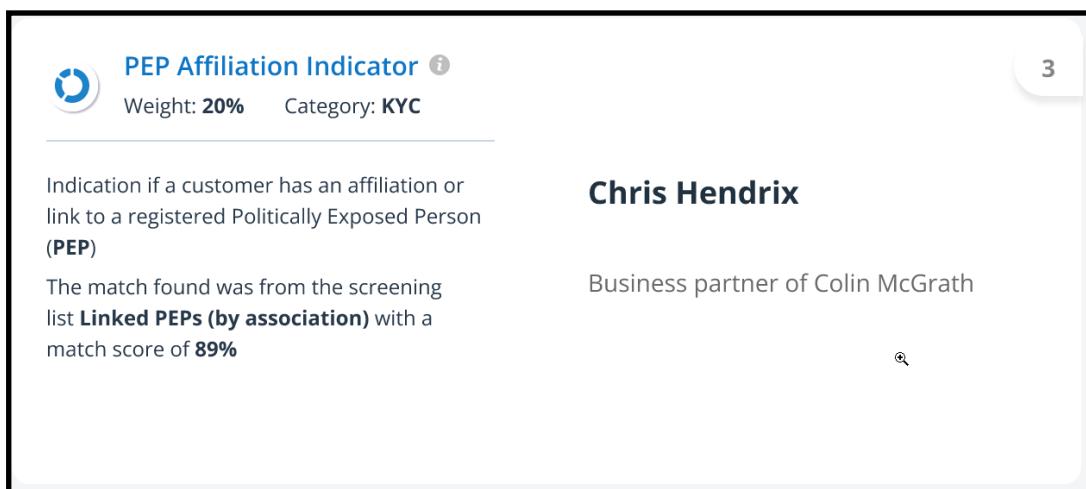


Figure 76: Binary Attribute Explainability

4.2.10.14. Feature Drill Down

- Feature drill down can be accessed by clicking on the arrow at the right of the feature widget on hover. The feature drill down contains the transactions relevant to the features as well as the summary from the feature widget.

4.2.10.15. Feature Summary

The feature summary that is found on the explainability widget from the previous screen, is shown here as well so as to maintain the context of the analyzed feature. This includes all elements of the feature explainability widget, including feature name, weight, category, descriptions and visualizations. If any more visualizations are configured for the feature, these will be shown here as well.

4.2.10.16. Transaction Table

The feature transaction table offers the analyst the ability to manipulate the displayed data, including such functionality as listed in the bullet list below.

Data Manipulation Options

If required, feature data can be displayed and manipulated as was in the case of the original Tab display layout design, which included:

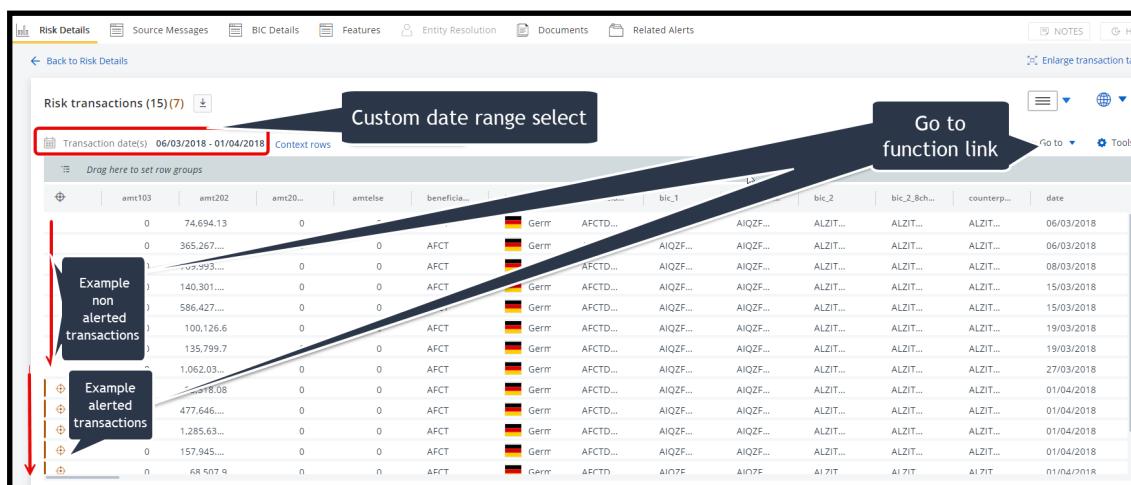
- Quick Alerts search - goto function etc.
- Viewing Evidence Data in Enlarged or Reduced Mode
- Data rows download as CSV files
- Viewing transactions by alert type
- Risk Resolution Alert Types and Available Layouts
- Context rows query results
- Global Layouts
- Table column resorting as provided for in standard AG functionality
- Data Manipulation tools - eg. aggregation, pivot grouping etc.

Quick Transaction Search

To initiate the quick transaction search first click the GOTO link on the Details tab.

The quick transaction search allows you to quickly search and display, alert and non-alert transactions.

To initiate the quick transaction search first click the **Go to** link on the Details tab.



The screenshot shows a transaction table with various columns including amt103, amt202, amt20..., armtseis, benefici..., bic_1, bic_2, bic_2_Bch..., counterp..., and date. The table contains numerous rows of transaction data. Two specific rows are highlighted with callouts: one for 'Example alerted transactions' and another for 'Example non alerted transactions'. The 'Go to' link is located in the top right corner of the table area, and the 'Custom date range select' input field is also highlighted with a callout.

Figure 77: Quick Alert Type Search by Alerted/ Non-alerted Go to Link + Custom Date Range Select

A quick search for transactions is available by the following criteria:

- By alert type

- By recent time period
- By custom time period

4.2.10.17. By Alert Type

Either Alert transaction or non-alert transaction

An example of found alert transaction rows is shown below.

⌚ F1923474	Aug-2017	6,655	John Coltrain
⌚ F1923474	Aug-2017	6,655	John Coltrain
⌚ F1923474	Aug-2017	6,655	John Coltrain

Figure 78: Example List of Alert Transactions Found in a Quick Alert Search

4.2.10.18. Viewing Evidence Data in Enlarged or Reduced Mode

To view the essential the evidence table in an enlarged view, simply click the link shown in the above figure.

The graph collapses allowing the table to expand to fill the available space.

trans_id	account_id	date	type	operation	amount	balance	k_symbol	bank	account
2 392 026	7 890	19/06/1997	withdrawal	withdrawal in cash	1 700	25 724			
2 392 121	7 890	19/06/1997	withdrawal	withdrawal in cash	300	25 424			
2 392 089	7 890	30/06/1997	withdrawal	withdrawal in cash	14.6	25 513.3	Payment for statement		
3 493 609	7 890	30/06/1997	credit		103.9	25 527.9	Interest credited		
2 391 991	7 890	10/07/1997	withdrawal	remittance to another bank	4 304	27 666.3	Household	ST	40 316 95
2 391 955	7 890	10/07/1997	credit	credit in cash	6 457	31 970.3			
2 392 027	7 890	16/07/1997	withdrawal	withdrawal in cash	1 700	25 966.3			
2 392 122	7 890	19/07/1997	withdrawal	withdrawal in cash	1 100	24 866.3			
2 392 090	7 890	31/07/1997	withdrawal	withdrawal in cash	14.6	24 952	Payment for statement		
3 493 610	7 890	31/07/1997	credit		110.3	24 976.6	Interest credited		
2 392 028	7 890	07/08/1997	withdrawal	withdrawal in cash	1 800	23 162			
2 391 992	7 890	10/08/1997	withdrawal	remittance to another bank	4 304	23 315	Household	ST	40 316 95
2 391 956	7 890	10/08/1997	credit	credit in cash	6 457	29 619			
2 392 065	7 890	13/08/1997	withdrawal	withdrawal in cash	1 800	23 515			
2 392 123	7 890	18/08/1997	credit	credit in cash	100	23 615			
2 392 091	7 890	31/08/1997	withdrawal	withdrawal in cash	14.6	23 702.5	Payment for statement		
3 493 611	7 890	31/08/1997	credit		102.1	23 717.1	Interest credited		
2 391 993	7 890	10/09/1997	withdrawal	remittance to another bank	4 304	25 855.5	Household	ST	40 316 95

Figure 79: Example Essential Evidence Data in Table Format (Enlarged)

To return the table to default (reduced mode), click the link highlighted in the above figure.

4.2.10.19. Downloading Table Data Content

To enable you to investigate the table data in another application (e.g. Excel) you can download the content in a CSV (,) comma delimited file format.

Simply click the download icon (6)  highlighted in the figure above. The contents are downloaded by default to your *Downloads* folder in your local machine.

To ensure correct functioning of table and report downloads, commas used in numbering notation (as employed in certain countries or regions) are removed.

Data content from the viewed table is downloaded to your local machine.

Note: Only Table data that has been filtered can be downloaded. Pivoted data can **not** be downloaded (exported). If the download button is disabled, check the table is not displaying the results of a pivot function.

4.2.10.20. Context Rows Query Results

The range of related days before and days after the first and last transaction context rows can be configured from each feature table, by clicking on the Context rows link as shown in the following figure.

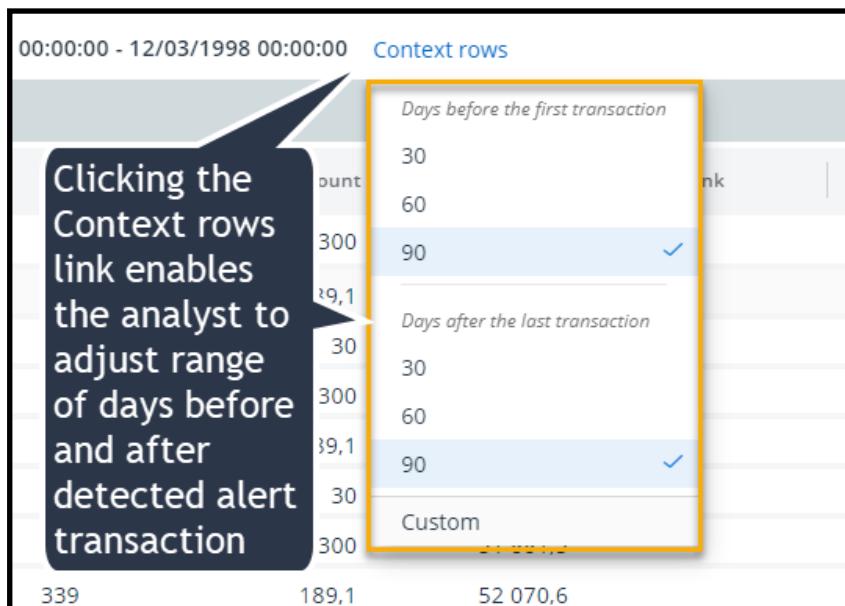


Figure 80: Example Context Rows Configuration Setting

4.2.10.21. Risk Resolution Alert Types and Available Layouts

The goal of the layout capability is to enhance and expedite the investigation process of the global transaction table, focusing on the triggering of the entire alert, as well as feature-level tables that present transactions related to the triggering of a particular feature.

Each layout group has its own sub-levels, which are described in the tables below.

Global Transaction Alert Layout Types

Global Transaction Layouts			
Personal		Global	
Risk Name	General info	Risk Name	General info
A user saves a defined table layout for all their alerts with the same risk name as the current alert under investigation. This layout always supersedes the Personal General Layout, as well as the Global Risk Name and General Layouts.	A user saves a defined table layout for all their alerts, regardless of the risk name. A user saves a defined table.	A user saves a defined table layout for all their alerts with the same risk name as the current alert under investigation, making it available to all analysts on their team.	A user saves a defined table layout for all their alerts, regardless of the risk name, making it available for all analysts on their team.

Feature Transaction Alert Layout Types

Feature Transaction Layouts					
Personal			Global		
Risk Name	Feature Name and Risk Name info	General info	Risk Name	Feature Name and Risk Name info	General info
A user saves a defined table layout for all features and alerts with the same feature name as the	A user saves a defined table layout for all their alerts with the same feature name	A user saves a defined table layout for all features, regardless	A user saves a defined table layout for all features and alerts with the same feature name as the	A user saves a defined table layout for all their alerts with the same feature name and risk name	A user saves a defined table layout for all features, regardless

Feature Transaction Layouts					
Personal			Global		
Risk Name	Feature Name and Risk Name info	General info	Risk Name	Feature Name and Risk Name info	General info
current alert under investigation.	and risk name as the current alert under investigation. This layout always supersedes the Personal General Layout, as well as the Global Feature Name, Feature Name and Risk and General Layouts.	of the name.	current alert under investigation, making it available to all analysts on their team.	as the current alert under investigation, making it available to all analysts on their team.	of the name, making it available to all analysts on their team.

Layout Selection is located under the Disk Details tab, provide the supervisor / analyst with the choice of either resolving alert risks in a global or personal configuration. To assist the analyst selecting a personal layout the **Recent Layout** (refer to the sub topic detailed below) feature enables the user to select a recently modified layout to run and test the suitability before deciding to save it as the optimal personal layout.

Available layouts and options are shown in the figure shown below.

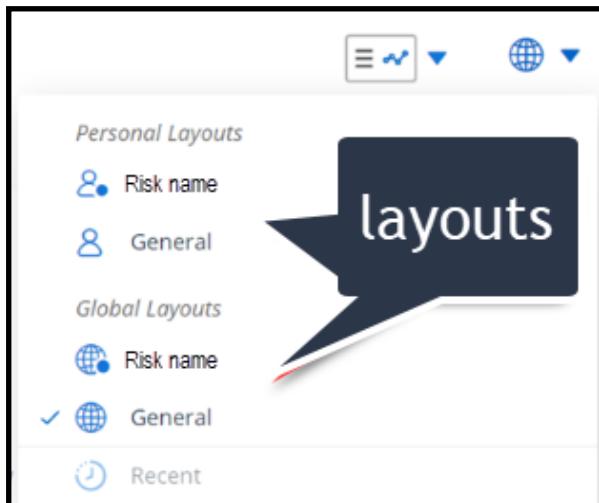


Figure 81: Layout Options, Personal, Global and Risk Types and Recent

Global Layout

The global layout is the default layout provided at deployment. This generic layout can be modified by Analysts and Supervisors with the appropriate permission. A Global layout that is modified and re-saved is applied to other analysts working on the same use case.

Personal Layout

The Personal layout enables each analyst to configure a custom layout to suit individual needs and preferences.

Note: A Personal layout supersedes a Global Layout in terms of display priority

Note: Once a personal layout is configured by the analyst, it takes priority becomes the new default layout and cannot be overwritten.

Global Layout

The global layout is the default layout provided at deployment. This generic layout can be modified by Analysts and Supervisors with the appropriate permission. A Global layout that is modified and re-saved is applied to other analysts working on the same use case.

Recent Layout

To make the transition from a global to a customized personal layout as smooth as possible, the user can modify the global layout in gradual steps , test out the

modifications over a period of time, and when the optimal layout is achieved, save the changes as the preferred personal layout.

Note: Be aware, changes to your layout while in 'Recent layout' mode are temporary and only last until you log out or change alert, at which point any changes made to the layout are removed.

Editing a Layout

The current layout can be modified or deleted, by an Analyst or Supervisor (with permissions).

» To edit a layout:

1. From the Alert Details screen, select a tabular tab (e.g. **Transactions**).
2. Configure the tab layout to your preference.
3. Click the down arrow next to the layout icon displayed (Global  Personal  or Recent ) as shown in below
4. Select a layout from the layout categories available and click **Save as**.

A change layout popup message, requiring verification is displayed as shown similar to the figure shown below.

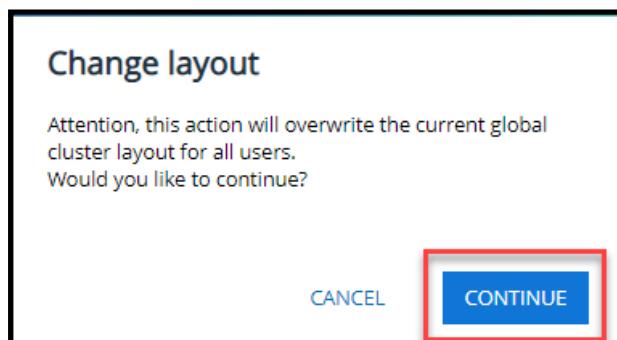


Figure 82: Change Layout Verification Popup Message

Adjusting what Data, and how Data is Presented in Transaction Tables

Regarding the Transaction tables structure, (eg column order, filtering, conditions etc.) the table structure is built according to the current standard 'AG-Grid' table structuring technology , so the analyst can adjust the table structure to best filter display and compare the available data.

Filtering and column sorting menus are listed below.

Column Functions Including:

- Pin Column
- Autosize This Column

- Autosize All Columns
- Group by Data Type
- Rest Columns

Filter by Conditions  **Including:**

- Equals
- Not Equal to
- Starts with
- Ends with
- Contains
- Not Contains

Filter by Columns 

List of all available columns to select for filtering as shown in the example depicted below.

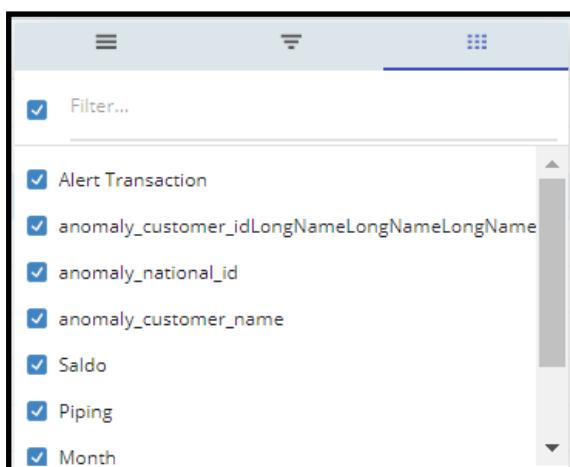


Figure 83: Filters Menu Options

» To access the filter options:

1. In the table, click to the right of the Column label to reveal the  menu.
2. Click the menu icon to display the Columns Filter and other options as shown in [Figure 83: above](#).
3. Click the  menu again to close the filters menu.

» To sort columns by order:

1. Toggle the selected Column label to sort by ascending or descending order.

Viewing Table Data

Data displayed in tabular tabs can be viewed as is, after filtering or aggregation (pivot)

Filtering columns to view is done via the Tools settings menu as shown in below.

» **To select Tools menu:**

1. Click the Tools icon  Tools.

The Tools menu is displayed as shown in below.

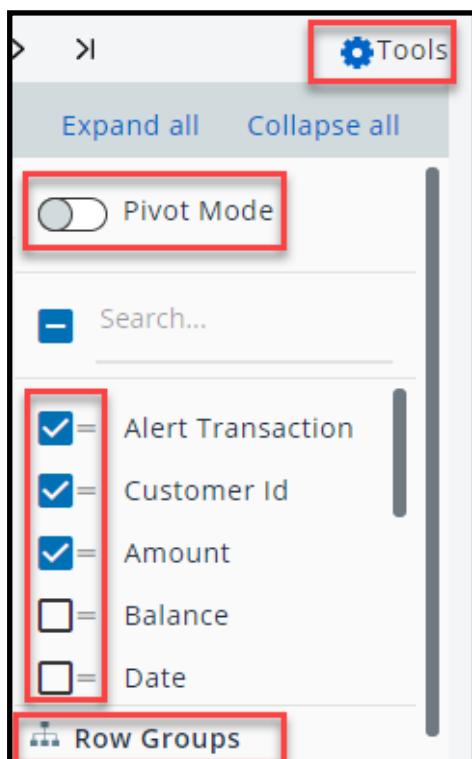


Figure 84: Tools Menu Example

2. To filter by selected columns, select the columns to filter by.
3. To pivot on table data, drag the column labels to the Row groups section or the Values section to aggregate results, then click the pivot box.

Data content from the viewed table is downloaded to your local machine.

Note: Only Table data that has been filtered can be downloaded. Pivoted data can **not** be downloaded (exported). If the download button is disabled, check the table is not displaying the results of a pivot function.

4.2.10.22. Rules Derived Alerts

Note: This section details a rule derived alert, which shares the Customer Insights widget component with the AI derived alerts, and therefore for expediency sake and not wishing to simply duplicate content this is mentioned where necessary, and only explicit rule derived information is covered here.

Rule(s) derived alerts are created alerts that are triggered when the KPI(s) associated with the rule is /are exceeded.

Example

Shown below is an example of an alert detected and added to the alerts list queue when the conditions of a rule or rules are met.



Figure 85: Example Rule Derived Alert Card Listed in Alerts Queue / List

As briefly covered in the opening screenshot, we can see the anomaly title and some basic information are displayed, such as the related date or dates range, say the alert includes associated consolidated alerts, plus the alert category.

Each rule derived alert card in the alerts list /queue is distinguishable by its analysis method tag.

Clicking the alert card of interest displays a related risk details tab as shown in the example below.

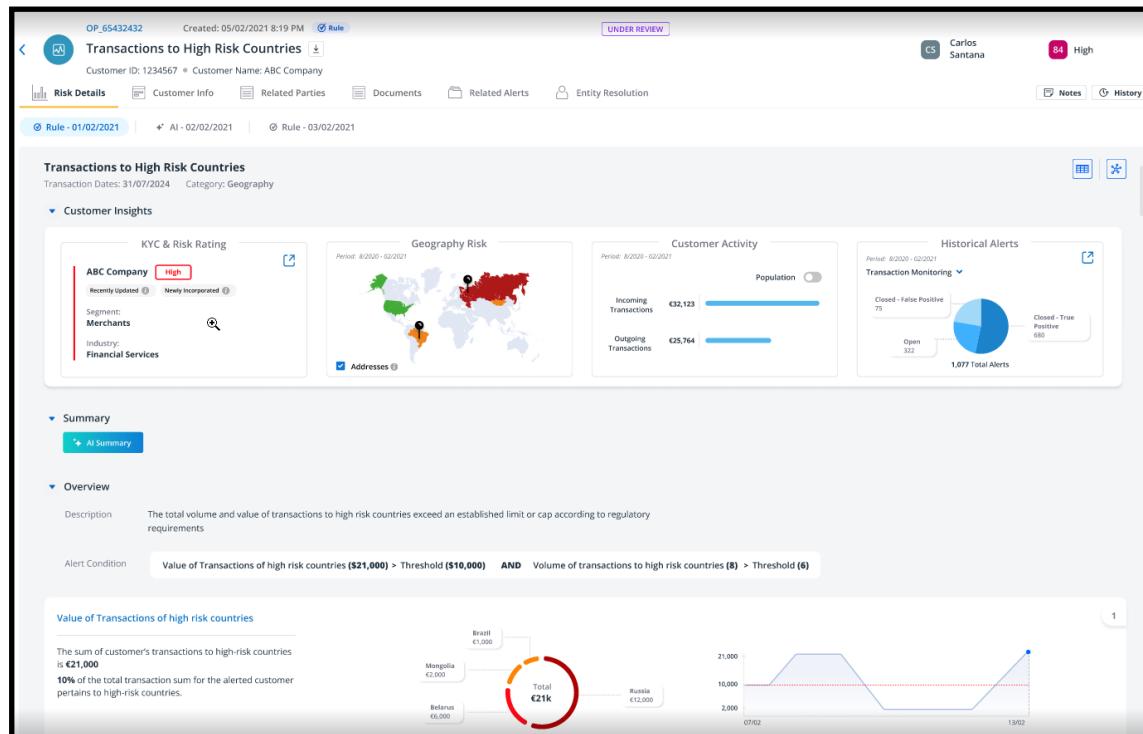


Figure 86: Rules Derived Overall Example

Including:

- Alert Name
- Transactions Date Range
- Category

Customer Insights

As previously mentioned and described the customer insights section of the rule derived alert is the same as provided in the section on AI based alerts.

Summary

The AI alert summary using OpenAI models is present here as well and the details can be found in the AI derived alert section.

Rule Overview

- Description - description of the rule and it's triggers
- Alert condition that triggers the alert, example The value of transactions to high risk countries exceeds the allowed threshold and the volume of transactions to high risk countries exceeds the allowed threshold

The conditions found in the alert condition section are further enhanced upon using the explainability widgets. Similar to the feature explainability widgets found in the AI derived alerts, the rule widgets include:

1. The explainability name, for example Value of Transactions to High Risk Countries
2. Dynamic description, including data pertaining to the current alert and additional insightful calculations
3. Explainability visualizations - these will customarily include an historical chart with the threshold, and an additional visualization where configured.

The explainability widgets intend to provide further clarity into making a swift and informed decision as to the validity of the alert.

As with the AI Rule Feature information Summaries, clicking the explainability widgets as shown in the examples below provides the analyst with graph and table drill down and access to original tab layout data manipulation tools (e.g. pivot, aggregation etc.)

4.2.11. Data Visualization Charts

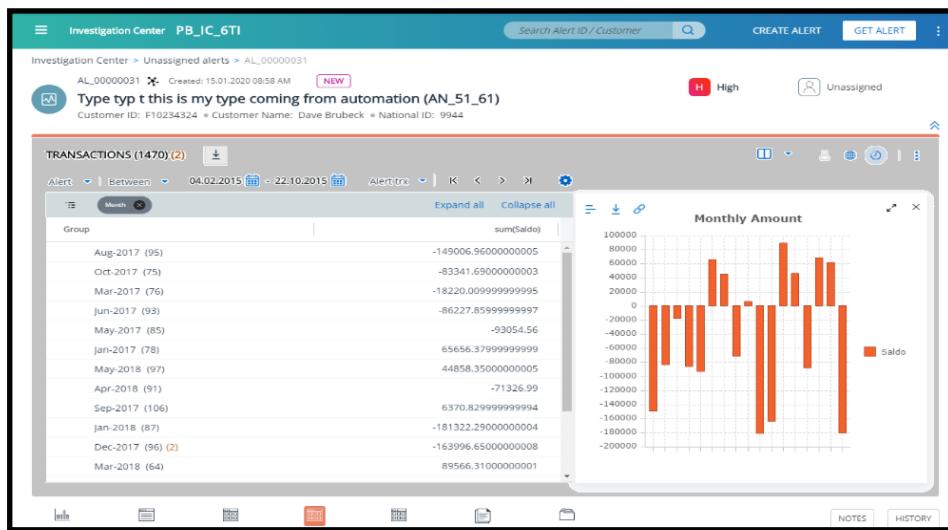
What are Data Visualization Charts?

Data Visualization charts provide a graphical representation of the data displayed in the tabular tabs used in the Investigation Center. They extend the ability to

comprehend transactional data by allowing you to view and compare features displayed as a graph over a specific time period.

Additionally, as the graphs are driven by the data stored in the data tables, changes or manipulations made to the data, such as filtering, grouping or by pivoting are immediately reflected in the chart output.

An example of a alert details tab showing data in a table and as chart is displayed as shown below:



4.2.11.1. Working with Data Visualization Charts

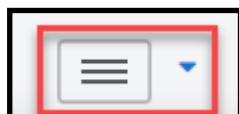
This remainder of this topic describes and details:

- Viewing data and charts in a variety of display formats
- Configuring charts
- Downloading created charts in .png format
- Viewing charts in full screen format
- Closing and removing charts

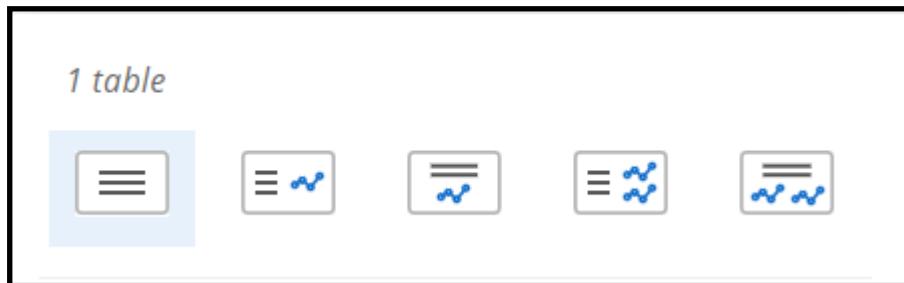
Viewing Data and Charts in a Variety of Display Formats

Selecting a Display Layout

Available display formats are selected from the highlighted icon displayed in the Risk Details tab menu image as shown below.



Click the dropdown icon to display the layout options as shown below.



Available display layouts are as shown and described in the following table:

Table 6:

Display Layout Options	Description
	Single table option only
	Dual horizontal layout pane: Tabular data on the left Chart on the right
	Dual vertical layout pane: Tabular data on the top Chart on the bottom
	Tri-pane layout #1: Tabular data on the left Two charts on the right vertically
	Tri-pane layout #2: Tabular data on the top Two charts on the bottom horizontally

» **To select the display layout:**

1. Click the display icon drop-down as highlighted above.
2. Select the required display option.

If a chart is not currently configured, the Create New Chart /Duplicate prompt is displayed as shown below.



Figure 87: Create New /Duplicate Chart Prompt

Configuring and Displaying Visualization Charts

Configuring and displaying a chart requires three steps:

- Selecting the data to be displayed
- Selecting a chart type
- Formatting a chart layout

Selecting Chart Data

Displaying data as a chart requires the selection of a numerical data field or fields that will form the Chart 'X' axis (Series).

These 'X' axis chart components can then be tagged with a suitable Category label.

➤ To select the data to display in the chart:

1. Select the desired layout format.
2. In the empty state chart area, Click the **Create New Chart** link or click the graph menu icon  .
3. With the data tab selected, scroll down to the section labeled **Series**.
4. Select as many of the available numerical data fields as required to render the chart 'X' axis.
5. Scroll up and tag the x axis chart elements by one of the available categories, e.g. transaction date, id etc.
6. Click the chart menu icon  to collapse the menu selection options.

An example column oriented data chart is shown below.[4.2.11](#).

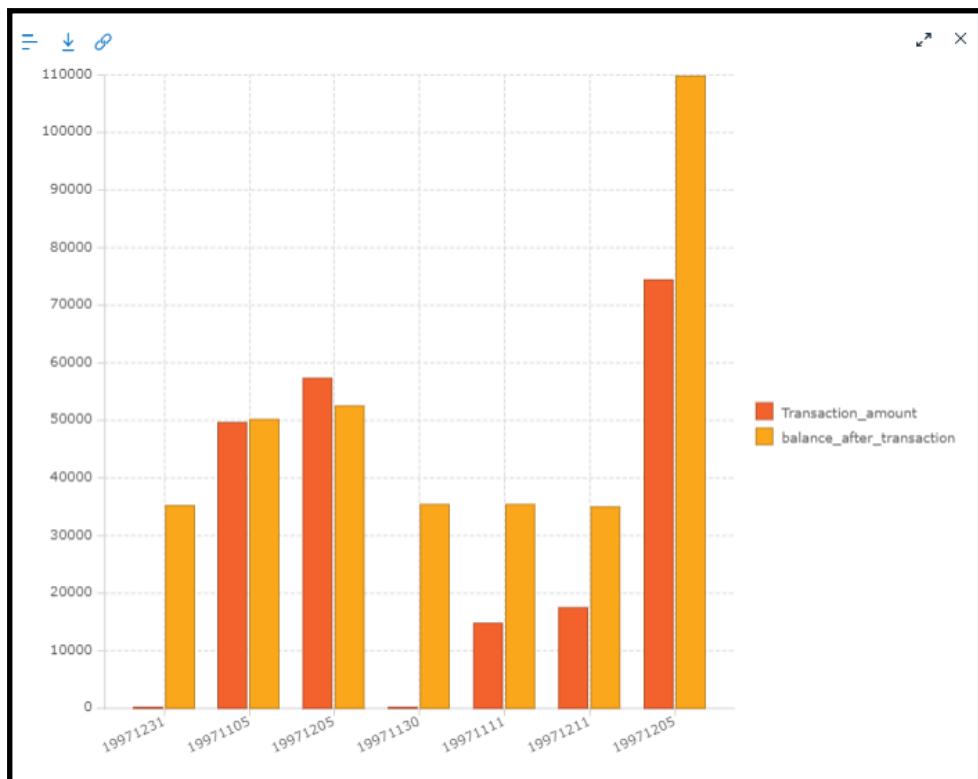


Figure 88: Example Column Chart (Dual Horizontal) that Compares two Data Fields Tagged with ID

Selecting a Chart Type

Once created, the chart can be viewed in a variety of chart types. Depending on the data under investigation, the experienced chart analyst will have a good idea which chart type to use that will produce the most meaningful visualization.

The range of available chart types that can be selected are detailed in the following table:

Chart Types	Variants	Example Image
Column	Grouped	
	Stacked	
	100% Fully Stacked	

Chart Types	Variants	Example Image
Bar	Grouped	
	Stacked	
	100 % - Stacked Bar Chart	
Pie	Pie	
	Doughnut	
Line	None	
X Y Scatter	Scatter	
	Bubble	
Area	Grouped	
	Stacked	
	100 % - Stacked Bar Chart	

➤ **To change the selected chart type:**

1. With the chart displayed, click the chart menu icon to display the menu.
2. Select the Settings tab to display the available Chart Type options.

3. Click the Chart Type of interest to display the original selected data as a new chart type.
4. Click the chart menu icon  to retract the menu and maximize the new chart type display.

An example of the same data used in the above column chart but now displayed as a Line Chart is shown below.

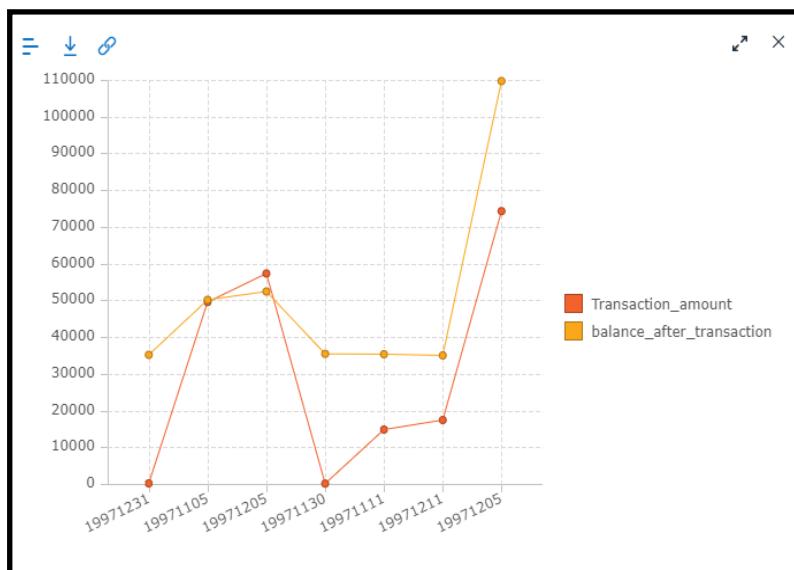


Figure 89: The Same Data as Used in the Previous example, but Displayed as a Line Type Chart

Formatting a Chart Layout

Formatting a chart layout enables you to fine tune the layout of the created chart.

The following chart visualization functionality is available under the chart menu

Format tab:

- Chart formatting
- Legend formatting
- Axis styling
- Series styling

Chart Formatting

Chart formatting includes the ability to set the following attributes:

- Chart title
- Font type and size
- Chart padding
- Chart background and color

Legend

Legend customization includes the ability to set the following attributes:

- Legend enable /disable and positioning
- Legend padding
- Font type and size

Axis

Axis formatting includes the ability to set the following attributes:

- Axis color, thickness, width and length
- Font type size and XY rotation
- Axis padding

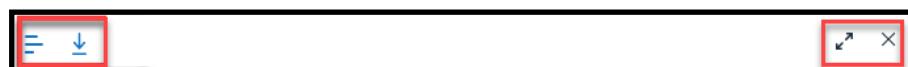
Series

Series customization includes the ability to set the following attributes:

- Tool tips enable/disable and line width
- Markers enable/disable size and stroke width

4.2.11.2. Chart Visualization - Actions Bar

This section details the auxiliary actions available from the Visualization chart **Actions Bar** as displayed below



The Chart Visualization actions menu (from left to right) includes the ability to :

- Open and close the **Chart Menu**
- Download charts in .png format
- Expand the selected chart to display full screen
- Close and remove charts

Opening and Closing the Chart Menu

In order to configure a new or reconfigure an existing chart, select the chart type or format the chart layout access to the chart menu is required.

➤ To open or close the chart menu:

1. From the **Chart Actions** menu, click the **Chart Menu** icon  to toggle between open and close mode.

Downloading a chart in .png Format

» To download a chart image:

1. From the **Chart Actions** bar, click the download icon  to download the chart as a .png image to your local machine.

Note: Downloading an image captures the current dimensions of the chart. The result will be larger if you are viewing the chart in full screen mode.

2. If required to download the chart as an expanded full size image, first select  to display the image full size, then click the download icon .

Expanding selected Chart to Display Full Screen

Created charts can be expanded to full pane size to enhance the clarity of the chart detail.

» To expand a chart:

1. From the **Chart Actions** menu, click the Expand icon  to expand the standard size chart to fill the full pane.

Note: Charts in the full pane size will, if selected for printing, print the chart as a full pane .png image.

Closing and Removing Created Charts

When the current created chart is no longer required, it can be closed and deleted.

» To close and delete a chart:

1. From the **Chart Actions** menu, click the close icon  to close and remove the current displayed chart.

4.3. Alert Details - Custom Tabs

In any IC deployment the user can create custom tabs that fit with his /her company's use case. For more information please refer to current IC Settings User Guide.

The **Alert Details** custom tab or tabs allow you to view relevant information and evidences regarding the system created alert.

The key actions and functionality available in the Alert Details custom tab are the same as provided for the Alert Details default tab plus the extra ability to select to view available custom tab data by date and time.

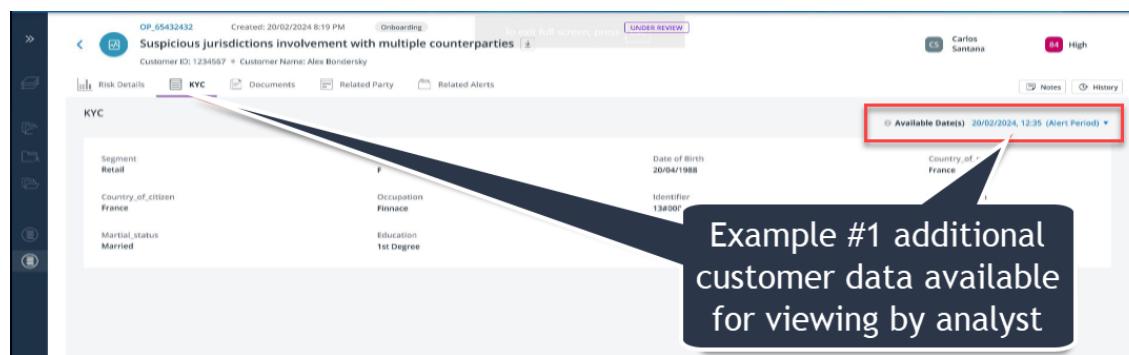
To avoid unnecessary content repetition, as the description of viewing essential evidences in graph mode and table mode , viewing evidence data in enlarged or reduced mode and downloading viewed data, are the same as described for the default risk details tab, for the custom tab overall action and functionality please refer to the previous risk details tab section.

4.3.0.1. Viewing Available Custom Tab Customer Data

To further aid the analyst in the course of his alert investigation duties, available related historical custom tab data can be selected and viewed by created date and time. This feature provides the analyst with an extra important layer of forensic alert evidence in the alert resolution .

The following list details this feature's overall scope and capability:

- Applicable to the alerts of all origins.
- Available for all custom tabs based on overwrite /update datasets
- Depending on the alert, the user can navigate available data and select to view per time and date
- Available data entries are listed in chronological order - from the most recent to the oldest via a drop-down menu
- The date of current alert under investigation date is highlighted
- The default view of the custom tab is related to the time of the alert with the relevant indication
- When a user exits an alert, the custom tab display returns to the default view



OP-65432432 Created: 20/02/2024 8:19 PM Onboarding Customer ID: 12345678 - Customer Name: Alex Banderky

Risk Details KYC Documents Related Party Related Alerts

KYC

Segment: Retail

Country_of_citizen: France

Marital_status: Married

Date of Birth: 20/04/1988

Occupation: Finance

Identifier: 1234567890

Education: 1st Degree

Notes History

Available Date(s) 20/02/2024, 12:35 (Alert Period) ▾

Example #1 additional customer data available for viewing by analyst

Figure 90: Example Additional Custom Tab Link Indicating Additional Available Data

Figure 91: Example Additional Available Data Displayed by Date and Time

Figure 92: Example Specific Data Display when Selecting from Dropdown List of Available Data

4.4. Risk Details Tab (Manually Created)

The RISK DETAILS screen displays a summary of the manual alert details entered on alert creation, as well as a link to view global transactions related to the manual alert.

Details include:

- Date and time Created
- Alert status
- Alert Number
- Customer ID
- BIC Code

A summary description of the main forensic evidence why the manual alert was created and any other relevant and support information.

Additionally the following information is included:

- Risk name
- Solution
- Evaluation flow
- Alerted activity ID

- Occurred on date and time
- Link to view related transactions table

The figure below shows an example of a Risk Details screen for a manually created alert.

The screenshot shows the 'INVESTIGATION CENTER' interface for 'Bahamas'. The main content area displays a 'Manual Alert #000001' with the following details:

- AL_0001201** Alert created: 25/04/2021 5:14 PM
- Customer ID:** 1800062692 • **BIC Code:** 23456789876
- Alert card information** (highlighted)
- RISK DETAILS** (highlighted)
- Alert description** (highlighted): Alerted Account with transaction volumes flowing from higher to lower risk jurisdictions in full path, with several amounts near known thresholds in period of analysis, with several P_Customer names and-or addresses
- Alert details** (highlighted):
 - Risk name: Manual Alert #000001
 - Risk category: MANUAL DEFAULT RISK
 - Evaluation flow: tr_analysis
 - Alerted activity ID: AL_0001201
 - Occurred on: 01/04/2021 09:54:02
- Transaction table link details** (highlighted): [VIEW TRANSACTION TABLE](#)
- Risk Details** (highlighted)
- Documents**
- Related Alerts**
- Custom Tab 2**
- Custom Tab 1**

Figure 93: Example - Manually Created Alert Details Screen

As in the system created Risk Details screen related tab links are also displayed.

4.5. Document Tab

The Document tab enables you to:

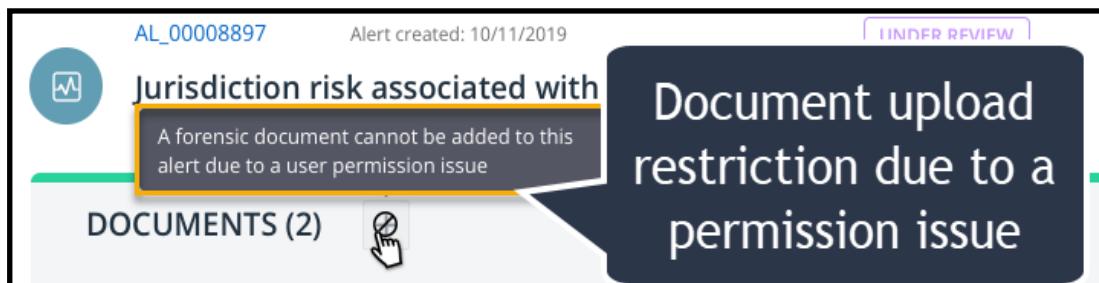
- View uploaded Alert related documents
- Download Alert related documents
- Upload new documents that will provide additional forensic evidence

4.5.1. Document Tab Restrictions

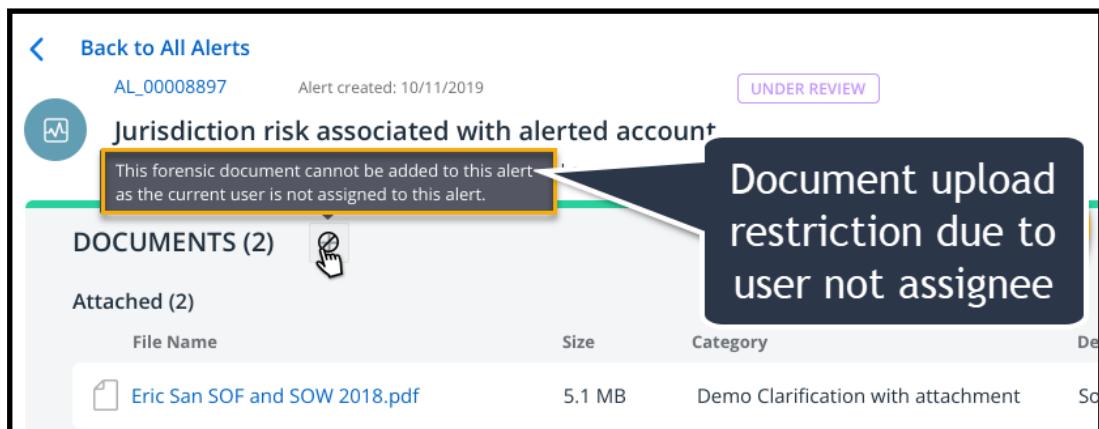
Uploading /downloading documents as forensic evidence is restricted to a user that is:

- Granted the appropriate user management permission
- Assigned to the alert

Example restriction notice - When the user does not have the required user management permission.



Example restriction notice - When the user is not assigned to an alert.



Note: Document download can also be restricted for the same reasons as described above, when attempting to upload forensic documents.

4.5.2. Maximum Document Size Permitted in Upload

The maximum document size that can be uploaded is 10 MB per document.

The elements of the Documents tab are described and detailed in the following table. [Table 7](#): below.

Table 7: Documents Tab – Elements, Description and Details

Element	Description	Details
Add Documents Icon +	This icon when clicked enables the user to browse to and select the document to upload	
File Name	Filename and type used in file provided as evidence once the document is successfully uploaded, it is listed under the File Name column and the File Name is displayed as download link	Format: <File name>.<file type suffix>
Size	File size	Example Units: Megabytes
Category	Categories drop down menu used to tag type of document	Example Types: <ul style="list-style-type: none"> • ID documents • Account movements • List of contact movements • FIOC • Evidence provided by customer • Anomalies report • Others
Description	Provided description of document	Up to a max of 500 characters can be used in the description text field
Added by	Name of role group active in system	Name of group, either system default or Admin created that has permissions to upload Alert related documents
Date added	Date when document uploaded	Example Format: dd:mm:yyyy hh:mm (AM/PM)
Actions	Settings that allows for the document to be uploaded, attached or detached	Options: <ul style="list-style-type: none"> • Upload (downloadable) • Detach (Due to regulatory requirements gathered forensic investigation such as documents can not be deleted.)

Table 7: Documents Tab – Elements, Description and Details (continued)

Element	Description	Details
		These are marked as detached and are not downloadable)

4.5.3. Supported File Extensions:

The following table details supported document type file extensions:

Supported File Type Extensions				
txt	rtf	csv	tsv	json
xml	doc	docx	xls	xlsx
ppt	pptx	one	vsd	pdf
xps	jpc	jpeg	tif	tiff
png	gif	bmp	zip	rar
7Z	msg			

4.5.4. Adding Documents

» To upload a new document:

1. From the Documents tab either click the add icon + or the Add Document link.
2. Browse to and select the document to upload.
3. From the Category drop-down menu, select the appropriate document type.
4. Provide a name for the document (max 200 chars).
5. Add a meaningful description of the document.
6. Click the Upload button.

4.5.5. Downloading Viewing and Detaching Documents

Once a forensic document has been uploaded, depending on the customer's security policy various document actions can be performed as follows:

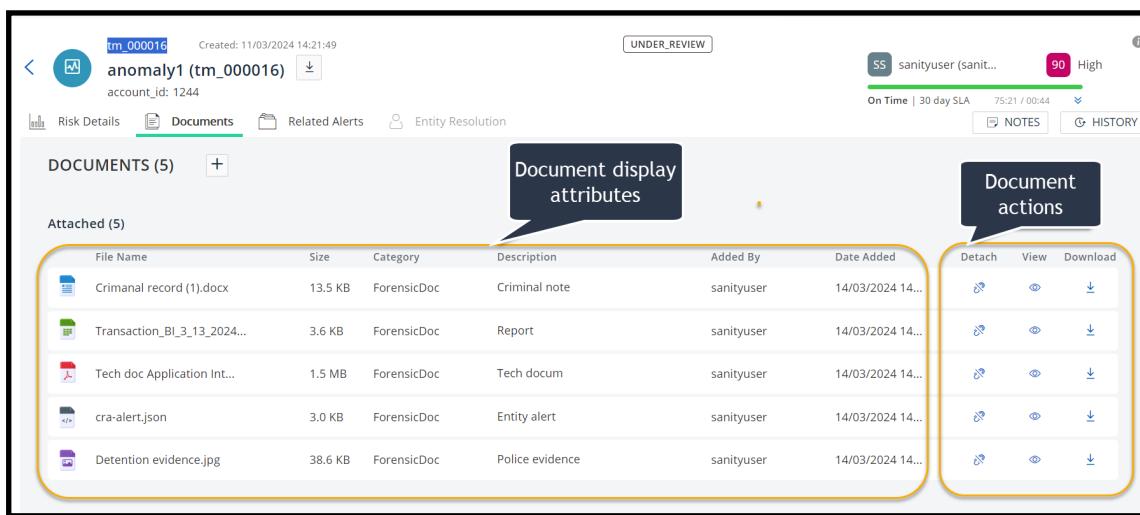
- Download
- View only

- View before download (with the correct permissions)
- Detach

» To display the available forensic documents:

1. From the Navigation bar, click the Documents link icon .

The Documents tab is displayed with any uploaded documents listed, similar to the example shown below.



File Name	Size	Category	Description	Added By	Date Added
Criminal record (1).docx	13.5 KB	ForensicDoc	Criminal note	sanityuser	14/03/2024 14...
Transaction_BI_3_13_2024...	3.6 KB	ForensicDoc	Report	sanityuser	14/03/2024 14...
Tech doc Application Int...	1.5 MB	ForensicDoc	Tech docum	sanityuser	14/03/2024 14...
cra-alert.json	3.0 KB	ForensicDoc	Entity alert	sanityuser	14/03/2024 14...
Detention evidence.jpg	38.6 KB	ForensicDoc	Police evidence	sanityuser	14/03/2024 14...

Figure 94: Example of Documents Tab

Let's take a closer look at the documents list, its attributes and the actions that a user with the appropriate scope can perform.

Display Attributes

Working from left to right:

- The document icon (if doc of type where an icon is delegated) is displayed.
- The document name and type suffix is displayed
- The doc category (provided at upload is displayed)
- The doc description (provided at upload is displayed)
- The user that added the doc is displayed next
- Date uploaded

Document Actions

The actions block has three available actions that can be enabled dependant on user scope and application deployment security restrictions:

- Detach, View and Download

From left to right:

Detach - To detach (but not remove) a document):

1. Click the 'Detach' icon of the specific document - The document is now disabled

View - Some notes regarding viewing documents:

Note: Whereas several file types can be viewed, (as shown in the following examples) it should be noted that limitations do exist when attempting to view some older Microsoft files formats.

Microsoft File Types Supported in Preview doc

images (.png, jpg, gif and svg)

PDF

CSV

JSON

ML

Excel (xlxs)

Word (docx)

email supported formats:

*HTML

*MME

*MSG

*EML

Microsoft File and Image Types Not Supported in Preview doc

.doc

.xls

.tif

Note: Horizontal and vertical scrolling is enabled for large files.

Note: Please be aware that for PIP security reasons, users cannot copy data of previewed files.

» To view a file:

1. Click the View icon of the specific document - A preview of the document is displayed.

4.5.5.1. Examples of Viewing Document Types

Example Preview of .csv File

INVESTIGATION CENTER				CREATE ALERT	GET ALERT	DevMode	?	
Alert ID	Assignee	Creation date	Date of occurrence	Information from History Tab			Information from Notes Tab	
1 189	analyst	21/02/2024 14:49:06	02/09/2022 00:00:00	<pre>[{"id":188,"mapperIdentifier":"1691913151334","alertId":"000189","userName":"System","action":"Alert Created","time":"21/02/2024 14:49:06","parameters": [{"type":"TYPE_STRING","name":"Queue","previous":null,"current":"1691913154335"}, {"type":"TYPE_STRING","name":"State","previous":null,"current":"state_new"}, {"type":"TYPE_STRING","name":"Severity","previous":null,"current":"90"}], [{"id":2771,"mapperIdentifier":"1691913151334","alertId":"000189","userName":"System","action":"Alert fetched from queue","time":"27/02/2024 08:24:16","parameters": [{"type":"TYPE_STRING","name":"Assignee","previous":null,"current":"analyst"}]}, {"id":2772,"mapperIdentifier":"1691913151334","alertId":"000189","userName":"analyst","action":"Add Note","time":"27/02/2024 08:24:27","parameters":[]}]}]</pre>			<pre>[{"author":"analyst","addedAt":"27/02/2024 08:24:27","categoryType":"Information","body":"ya9e1sb26bl21scfm0g0ry4d6t7co8us712tqlvg4n8iagoxj6w95ujqeieph1ecten35b41n50kqzkleqzvehg5wvgsprk6j6pgcj08ejb11gz75joai5auvgt1xykgjsvwifmbu6ubudb68lu8tisda7rzhun9uczzktkrbr3x76q59hez2tzdt1npld6y8_442993"}]</pre>	

Figure 95: Example Preview of .csv File

Example Preview of PDF File

THE TARAY

One Level Deeper

Customer Risk Assessment (CRA)

The ability of financial institutions to manage the possible risk factor presented by their new and existing customer base represents a major part of running and controlling any efficient financial service.

The addition of a CRA service to its product range, means that Thetaray can now move towards 'closing the circle' in its goal of meeting all financial service needs requirements of its ever growing diverse client base.

The new CRA service is well matched and technologically engineered to either integrate into its existing product range such as transaction monitoring, and transaction and customer screening or if a client requests, can be deployed as a stand alone service.

Once CRA is deployed, and supporting datasets integrated, a client's customers either at the onboarding or ongoing stage are subject to risk scans by a combination of specially engineered algorithms and deterministic rules that determine the customer risk level. Result reports are available post scan either automatically or on demand for download and review.

The client's analyst team is fully supported with an easy to use UI/UX that enables data filtering that aids in the alert investigation process and alert closure with an

Figure 96: Example Preview of PDF File

Example Preview of Excel File

	First Name	Last Name	Gender	Country	Age	Date	Id
5	Gaston	Brumm	Male	United States	24	21/05/2015	2554
6	Etta	Hurn	Female	Great Britain	56	15/10/2017	3598
7	Earlean	Melgar	Female	United States	27	16/08/2016	2456
8	Vincenza	Weiland	Female	United States	40	21/05/2015	6548
9	Fallon	Winward	Female	Great Britain	28	16/08/2016	5486
10	Arcelia	Bouska	Female	Great Britain	39	21/05/2015	1258
11	Franklyn	Unknow	Male	France	38	15/10/2017	2579
12	Sherron	Ascencio	Female	Great Britain	32	16/08/2016	3256
13	Marcel	Zabriskie	Male	Great Britain	26	21/05/2015	2587
14	Kina	Hazelton	Female	Great Britain	31	16/08/2016	3259
15	Shavonne	Pia	Female	France	24	21/05/2015	1546
16	Shavon	Benito	Female	France	39	15/10/2017	3579
17	Lauralee	Perrine	Female	Great Britain	28	16/08/2016	6597
18	Loreta	Curren	Female	France	26	21/05/2015	9654
19	Teresa	Strawn	Female	France	46	21/05/2015	3569
20	Belinda	Partain	Female	United States	37	15/10/2017	2564
21	Holly	Eudy	Female	United States	52	16/08/2016	8561
22	Many	Cuccia	Female	Great Britain	46	21/05/2015	5489
23	Libbie	Dalby	Female	France	42	21/05/2015	5489
24							

Figure 97: Example Preview of Excel File

Example Preview of Email File

From	John Doe
To	sales@bitdaddys.com
Subject	(outlookEMLandMSGconverter Trial Version Import) BitDaddys Software
Dear BitDaddys Corp., We have added your software to our approved list. Thank you for your efforts, Sincerely, John Doe Some Server Company	

Figure 98: Example Preview of Email File

Example preview of json file

```
[  
  {  
    "id": "state_new",  
    "identifier": "ID_state_new",  
    "name": "New",  
    "type": "SYSTEM",  
    "active": true,  
    "deleted": false,  
    "roles": [],  
    "teams": [],  
    "workflows": [{"id": "1"}],  
    "updateTime": "2022-05-01 08:10:49",  
    "fileName": "states.json"  
  },  
  {  
    "id": "state_closed",  
    "identifier": "ID_state_closed",  
    "name": "Closed",  
    "type": "SYSTEM",  
    "active": true,  
    "deleted": false,  
    "roles": [],  
    "teams": [],  
    "workflows": [{"id": "1"}],  
    "updateTime": "2022-05-01 08:10:49",  
    "fileName": "states.json"  
  },  
  {  
    "id": "state_pending_l1",  
    "identifier": "ID_state_pending_l1",  
    "name": "Pending_LoD1",  
    "type": "CUSTOM",  
    "active": true,  
    "deleted": false,  
    "roles": [],  
    "teams": [],  
    "workflows": [{"id": "1"}],  
    "updateTime": "2022-05-01 08:10:49"  
  }  
]
```

Figure 99: Example Preview of json File

➤ To download a document:

1. From the Documents tab click the name of the file to download.

The document is downloaded to your local download directory.

Troubleshooting Note: If the file you require does not respond to an action (for example, view or download) you should check with your IT department, if the problem is related to a permissions issue or your company's PIP security policy

4.6. Related Alerts Tab

Related alerts are alerts that share the exact same primary identifier with the current investigated entity.

The alerts from all the analysis which are mapped by the admin to explain their relationship will appear as related alerts.

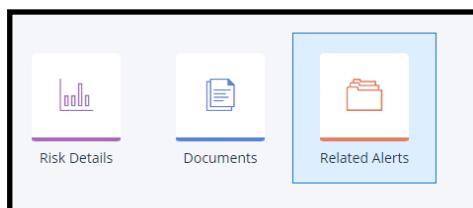
You can view all available analyses or select a specific publisher to filter the displayed list.

Related alert cards show the same properties as standard alert cards plus:

- Use Case Name/ID
- Total number of all use case related alerts
- All available related alerts in drop-down list to view by
- Option to bulk edit related alerts

» **To display the Related Alerts tab:**

1. From the Navigation bar, click the Related Alerts link icon  in the Navigation bar as shown in the following example:



An Example of a **Related Alerts** tab screen is displayed below.

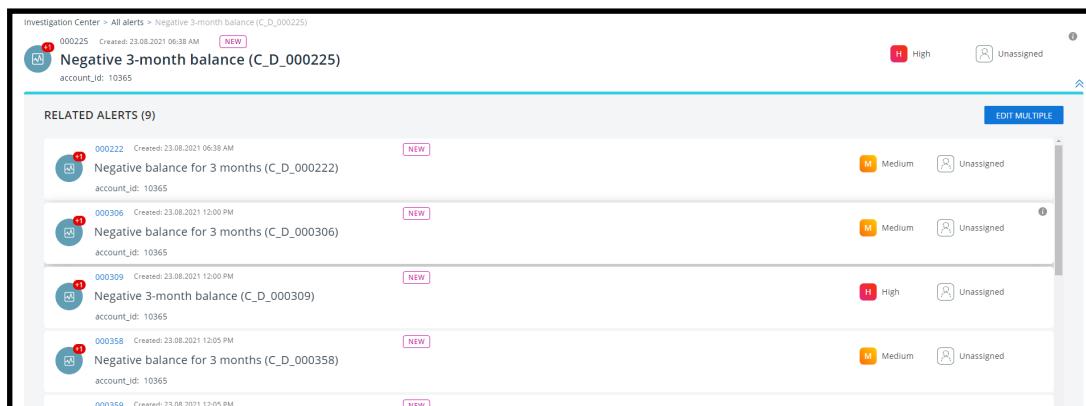


Figure 100: Example of a Related Alerts Tab Screen

Related Alerts tab elements are listed, described and detailed (where appropriate) as shown in Related Alerts Tab

Table 8: Related Alerts - Elements, Description & Details

Element	Description	Details
Alert Card	The Alert card of the alert under investigation	
Related Alerts (stats)	Total number of related alerts	e.g.: Related

Table 8: Related Alerts - Elements, Description & Details (continued)

Element	Description	Details
		Alerts (50)
Sorted by Creation Date	List of all related alerts according to the selection in the dropdown list	Options: <ul style="list-style-type: none">• Ascending• Descending

4.7. Notes Side Panel

The Notes tab side panel allows you to:

- Add new notes as required
- View added alert notes
- Sort by oldest /newest
- Mark notes as deleted

4.7.1. Notes - Add /Edit Limitations (Roles and Users)

Control over notes edit privileges has been modified to introduce a level of admin the analyst deals with notes (add and edit).

Depending on the analyst's role and by extension, permission level in general, an analyst will be able to:

- View all notes
- Will only be able to edit notes for alerts assigned to him /her

General Edit permissions:

Action	Permissions
View	Assigned and unassigned user
Adding a note	Only assigned user
Editing a note	Only assigned user
Changing note state (e.g. 'mark as deleted')	Only assigned user

4.7.1.1. Examples of Notes Restriction Notices

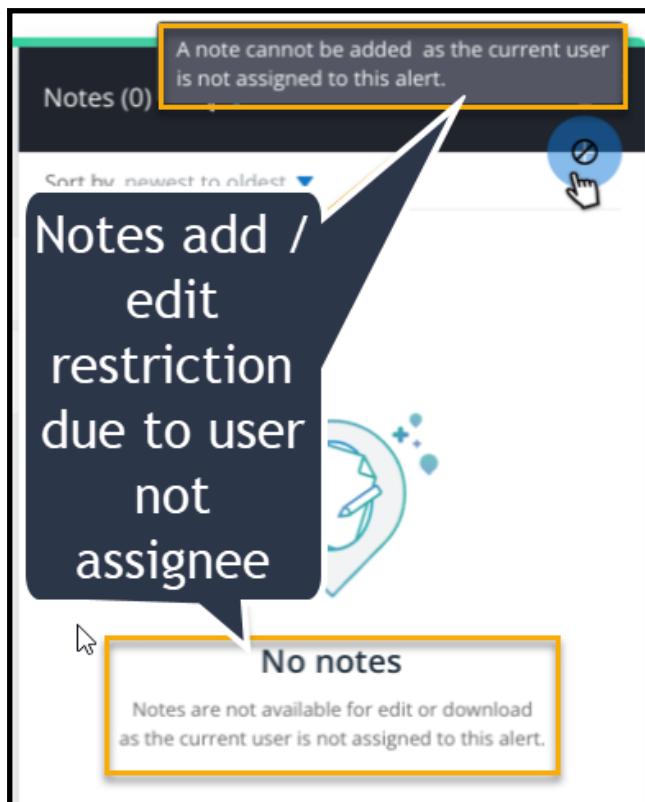


Figure 101: Example Notes Add Restriction Notice

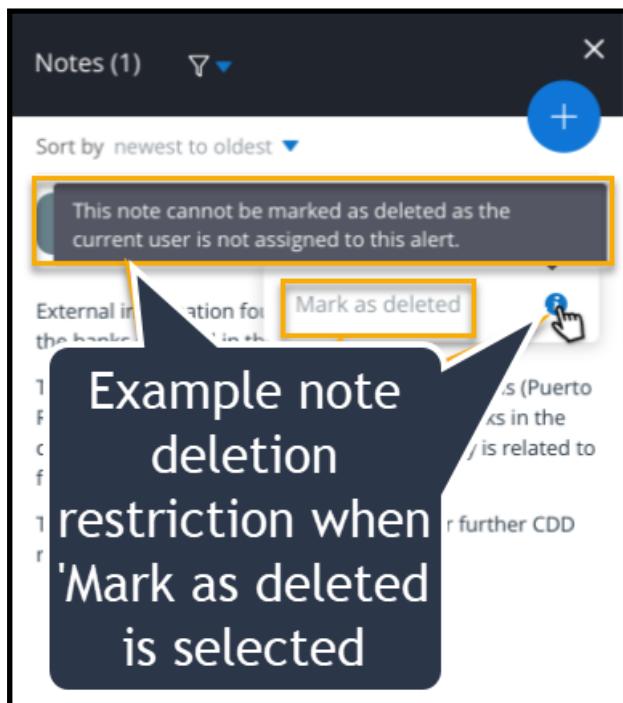


Figure 102: Example Restriction Notice when Unassigned user Attempts 'Mark as Deleted'

Notes can be populated with two main types of text:

- Narrative
- Process/ Information

4.7.2. Narrative Text

Narrative text is preset generated text, specific to the alert under investigation. It saves the analyst time manually collecting and adding supportive information concerning the investigated entity. Narrative custom texts are designed and developed in IC settings by the organizations business admin users who configure Auto Text Template scripts utilizing the data made available post analysis from both anomalies and alerts

An example of a narrative is shown below:

Confirm. Talked to Dave Brubeck, his DOB is: 08/23/1974, NID: 23495215W, Occupation: Bank worker).

4.7.3. Information/ Process Text

Information and process text is free text added by the user.

Process text is generally specific to the alert status.

Information text is any descriptive information about the alert or customer whereas

(Process example: Waiting for verification from a Supervisor with a recommended resolution.

(Information example: The validity of the Alert is by the available forensic evidence.)

4.7.4. Adding New Notes

» To add a new note to the Alert:

1. From the Navigation bar, click the Notes icon .
2. Click the blue **Add +** icon.
3. From the drop-down menu as shown in the following figure select note Type (Narrative /Information /Process).

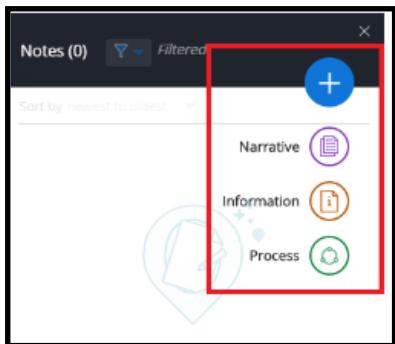


Figure 103: Note Type Select Options

4. If Narrative note type is selected the following panel is displayed as shown in the following figure.

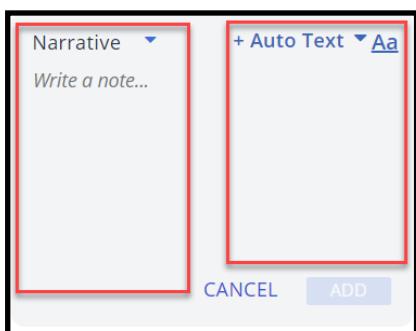


Figure 104: Narrative Notes - Create manually or by Auto Texts

Creating a Narrative note manually

5. From the **Narrative** dropdown menu select type of note from :
 - Narrative (manually created text)
 - Information (descriptive information about the alert)
 - Process (alert status)
6. If the Narrative type is selected there is an additional option to add formatting via the Aa html menu as shown in the following figure.

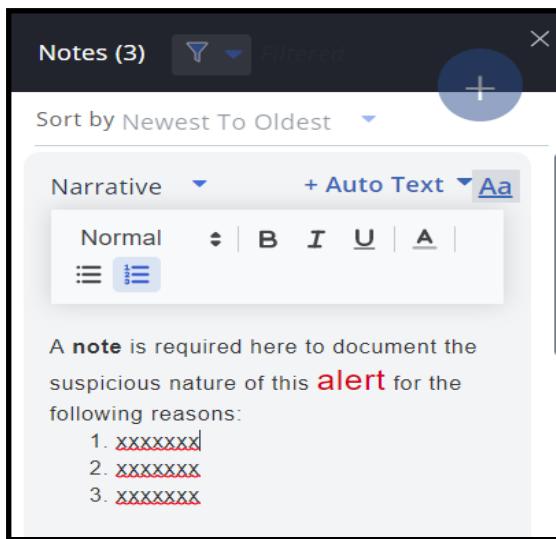


Figure 105: Example of Creating a formatted Narrative Note Manually

7. When complete click **Add**, to add the note.
8. If an Information or Process explanation type note is required , formatting is not enabled, simply type content and click **Add**.
9. To select a created **Auto Text**, click the dropdown menu to display available Auto Text Templates that were created in IC Settings as shown in figure 4 below.

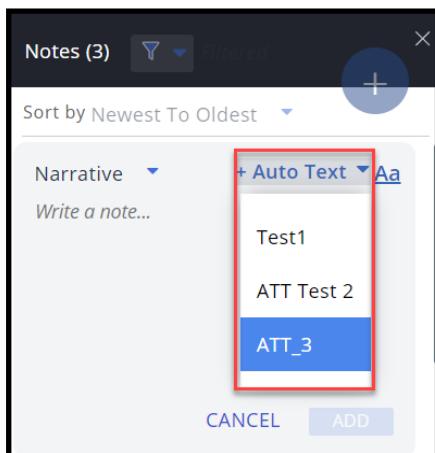
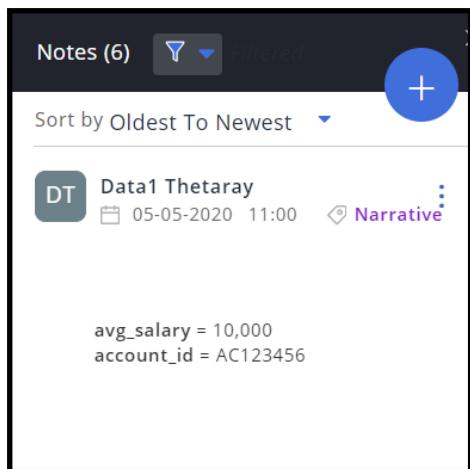


Figure 106: Auto Text Templates Selection

In this example we will select the ATT_3. auto text pre created by an admin user in Investigation settings.

10. As can be seen the Narrative is shown in the Edit mode, if the template does not need further edits click **Add** to add auto text and view formatted note.
11. If the Narrative requires further HTML formatting , edit, then click **Add**.



4.7.5. Filtering & Viewing Added Notes

Before viewing added notes you can set the optimum view filters according to your standard work flow.

➤ **To set the available view filters:**

1. From the Notes side panel click the filter icon .

The set view filters side panel is displayed as shown in the following figure.

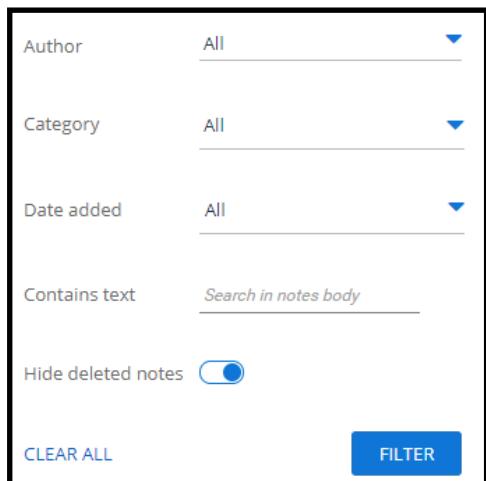


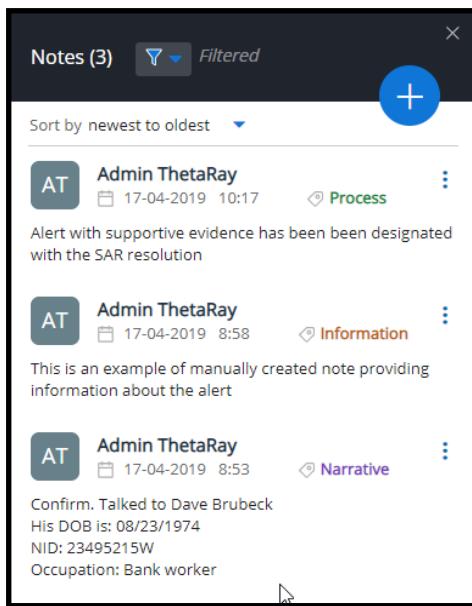
Figure 107: Filter Configuration Drop Down Menu

Set the configurations as required and click the **Filter** button

➤ **To view Notes created for the current Alert:**

1. From the Navigation Panel, click the Notes icon

Saved notes are displayed according to filter settings in the Notes side panel as shown in the following figure.



Notes (3) Filtered

Sort by newest to oldest

AT Admin ThetaRay 17-04-2019 10:17 Process

Alert with supportive evidence has been designated with the SAR resolution

AT Admin ThetaRay 17-04-2019 8:58 Information

This is an example of manually created note providing information about the alert

AT Admin ThetaRay 17-04-2019 8:53 Narrative

Confirm. Talked to Dave Brubeck
His DOB is: 08/23/1974
NID: 23495215W
Occupation: Bank worker

Figure 108: Example List of Created Notes

4.7.6. Sorting Notes by Order

Notes can be sorted by:

- Oldest to newest, or
- Newest to oldest

» To sort by newest to oldest (or vice versa):

1. Click the Sort by the Newest to Oldest icon:
2. Select the option required.

4.7.7. Marking / Unmarking Notes as Deleted

As mentioned previously in this section only assigned users can mark or unmark notes as deleted.

Due to regulatory constraints, once a note has been added it cannot be deleted. However notes that are deemed no longer relevant by the user, can be marked as deleted. Once marked as deleted, the note will still be readable although appear grayed out.

» To mark / unmark a note as deleted:

1. Select the **More Actions** button next to the note
2. Depending on the note status click the **Mark / Unmark as Deleted** button

Note: Depending on the View filter settings, the grayed out note may or may not be displayed.

4.8. History Side Panel

The History side panel allows you to review alert actions activity made during the investigation process. The amount of detail displayed depends on the alert, activity and activity source.

An example of a side panel displaying alert actions historical activity, is shown below.



Figure 109: Example Alert Historical data

5. Entity Resolution

5.1. Introduction

This chapter of the Investigation Center describes the Entity Resolution (ER) feature as provided in phase 2. As Entity resolution is now fully integrated into the Investigation Center's package of anomaly investigation discovery tools, it provides the analyst with that extra important wider and deeper interactive layer of anomaly resolution capability, thus enriching and improving their level of workflow productivity.

The key topics covered in this section include:

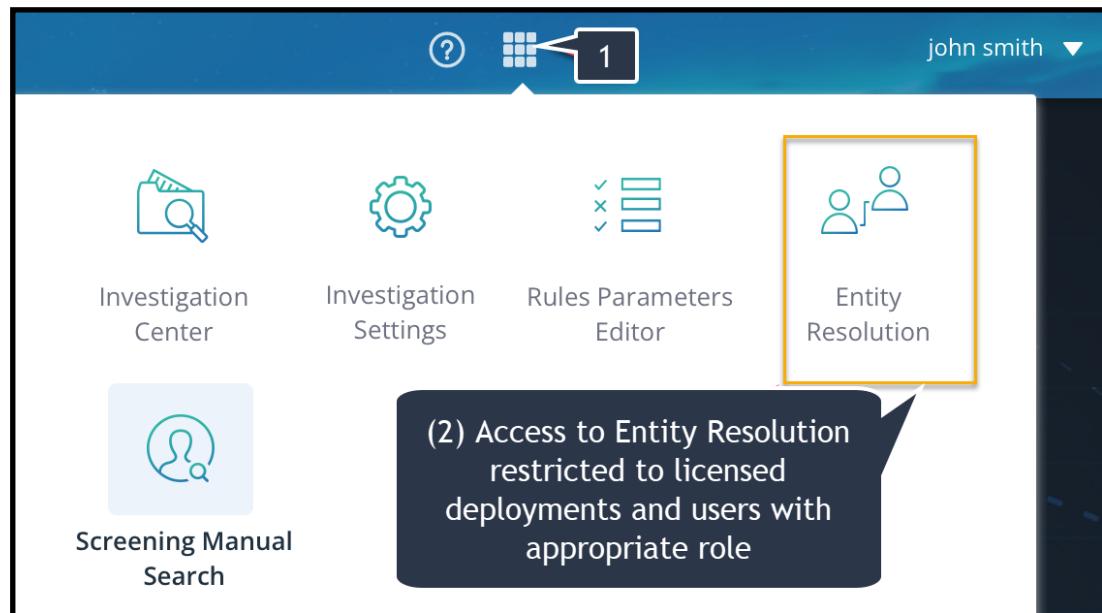
- Accessing the ER module
- Initial landing screen layout and functionality
- Working with the ER Search and Relationship filter
- PII Information - mandatory requirements and optional edits
- Matched entity drill down and confirmation / reject procedures
- Integration of ER sourced alerts into Investigation Center
- How ER alert consolidation / added risks are managed with example scenarios

Note: Only deployments that have the license for Entity Resolution will have access to the ER module and module users must have the appropriate permissions.

5.2. Accessing Entity Resolution Phase 2

» To access the Entity Resolution module:

1. From The IC Log-in, click the matrix icon (1).



2. Select the Entity Resolution (ER) module from the Matrix Icon (2) as shown above.

5.3. Initial landing Screen Layout and functionality

On selection of the ER module, a landing screen is displayed , similar to the following screen.

(1) Entity resolution - Landing Screen with two initial displays limited to two entities per alert

(2) Entity Resolution filter by options

(3) icons indicating auto match confirmation mode enabled to confirm match Note: Can be manually overridden

4

Entity Resolution

5.3.1. Entity Resolution Landing Screen - Functionality Overview

1. To make the task of confirming or rejecting matched entities more simplified and efficient, the initial landing screen displays only two matched entities per entity resolution.
2. Filter by option tabs to enable results to be filtered.
3. Automatic confirmation is enabled to aid efficiency, although the analyst can if he / she (with knowledge of data and customers) feels the auto confirmation is not accurate enough, can override this setting and confirm or reject the matches manually.
4. To initialize the match / reject process for each result, click the edit icon pencil.

5.3.2. Working with the ER Search and Relationship filter

In the **Entity Resolution** module, searches for specific entity results can be made by selecting from available filter categories (and then by listed parameters).

Filter Categories are as follows:

- Threshold Score
- Generated Date
- Modified Date
- Party Status

The screenshot shows the Entity Resolution module with several filtering options highlighted:

- Filter by more than score range:** A dropdown menu for 'Threshold Score' is open, showing options like 'All', 'More than 80', '85', '90', and 'Custom'. The 'More than' option is selected.
- Filter by time range:** A dropdown menu for 'Generated Date' is open, showing options like 'Any Time', 'More than 24 Hours Ago', '7 Days Ago', '30 Days Ago', and 'Custom'. The 'Any Time' option is selected.
- Filter by Party status:** A modal dialog for 'Party Status' is open, showing 'Select all' and 'Clear all' buttons. It lists 'New (22,046)', 'Processed (10,321)', and 'Updated (1,354)' with checkboxes. The 'New' checkbox is selected.
- Relationship filter:** A dark blue callout box points to a section of the interface, likely referring to the list of relationships or entities shown below the filters.

5.4. PII Information Management- Mandatory / Optional Requirements Edits

The personal information (PII) available regarding each Party candidate is designated by one of two categories:

- Mandatory or
- Optional

Mandatory:

Each matched entity displayed in the ER module must have as a mandatory requirement, a unique identity number and a party name. These cannot be modified.

Optional:

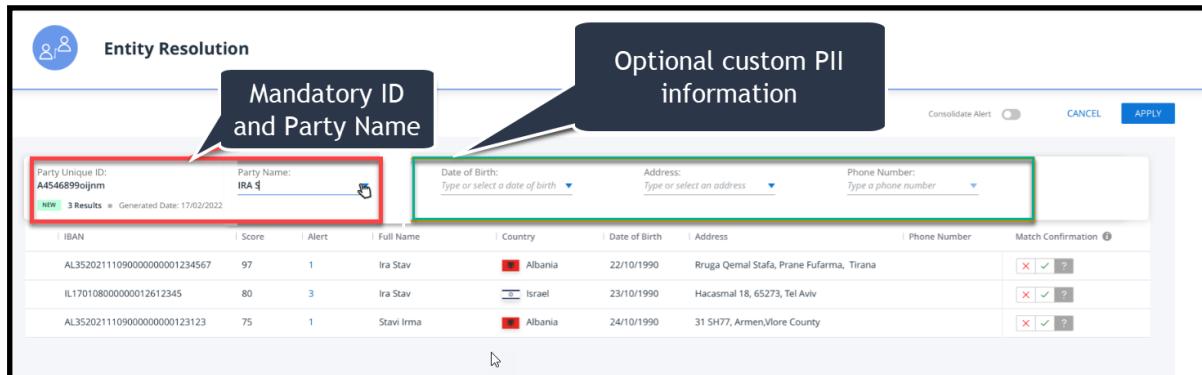
In the example provided, there are three optional / custom fields shown as follows:

- Date of Birth
- Address
- Phone Number

These can be modified by the user in one of two ways:

1. By selecting from one of the listed alternatives (if available)
2. By entering a free text alternative (If the analyst has additional information available, gathered in the course of his /her investigation)

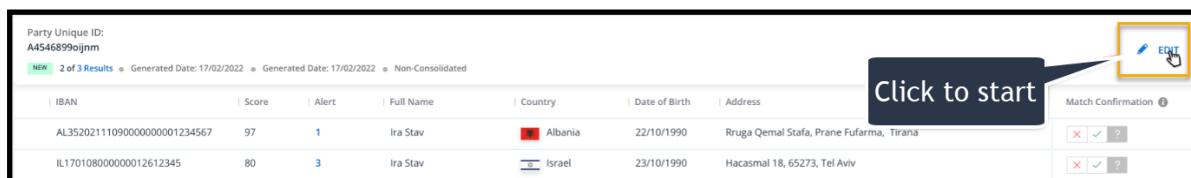
Note: The extent of the optional fields can vary depending on use case.



The screenshot shows the Entity Resolution interface. At the top, there are two sections: 'Mandatory ID and Party Name' (highlighted with a red box) and 'Optional custom PII information' (highlighted with a green box). The 'Mandatory ID and Party Name' section contains fields for 'Party Unique ID' (A4546899ojnm) and 'Party Name' (IRA 5). The 'Optional custom PII information' section contains fields for 'Date of Birth', 'Address', and 'Phone Number'. Below these sections is a table of search results. The table includes columns for 'IBAN', 'Score', 'Alert', 'Full Name', 'Country', 'Date of Birth', 'Address', 'Phone Number', and 'Match Confirmation'. The results show three entries for 'Ira Stav' from different countries (Albania and Israel) with varying scores and addresses.

5.4.1. Practical Example on Editing Party Address

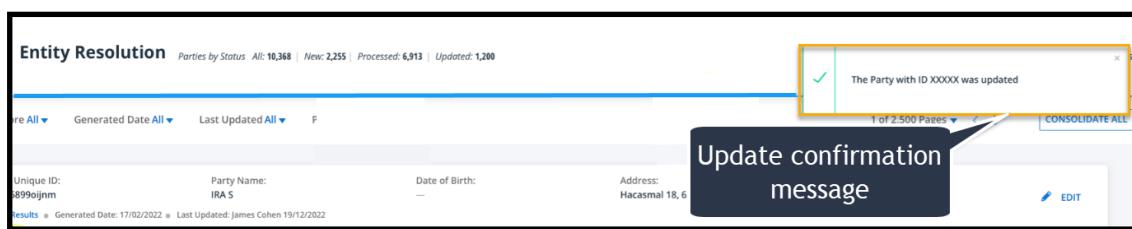
1. To start the edit process click the **EDIT** pencil icon for the entity, as shown below.



The screenshot shows the Entity Resolution interface with the 'EDIT' pencil icon highlighted for the first entity in the list. A callout box says 'Click to start'. The table below shows two entries for 'Ira Stav' from different countries (Albania and Israel) with varying scores and addresses.

2. On the **Address** field, click the down arrow to display available addresses, select one or add a custom address as free text.
3. When complete, click **APPLY** to modify the entry.

The modification process if successful, is confirmed by a successful confirmation message.

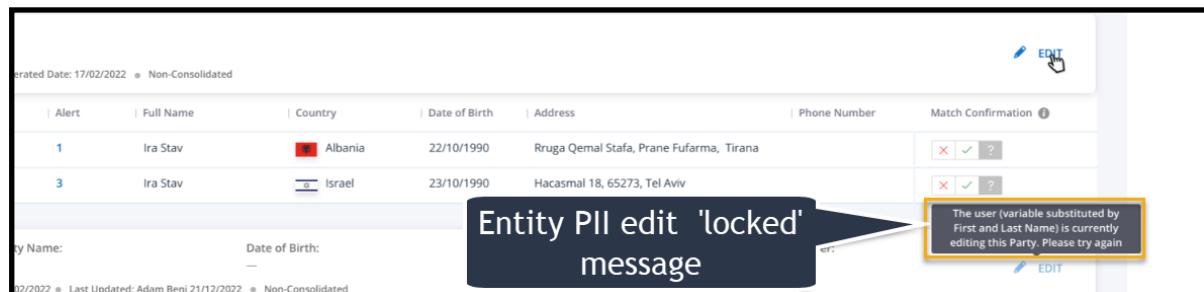


The screenshot shows the Entity Resolution interface with a confirmation message box: 'The Party with ID XXXXX was updated'. A callout box says 'Update confirmation message'. The table below shows the updated address for the entity.

Note: This modification can subsequently be modified by other analysts /Supervisors working on ER investigations in the same team.

5.4.2. Entity Locking when multiple Users Attempt to Edit PII Simultaneously

As a feature design requirement, in Entity Resolution only one user can edit Party candidate PII at a time. Therefore, when an analyst is working on editing PII the entity is effectively 'locked' and attempts to access the entity result in the following message being displayed to the analyst attempting to edit PII.

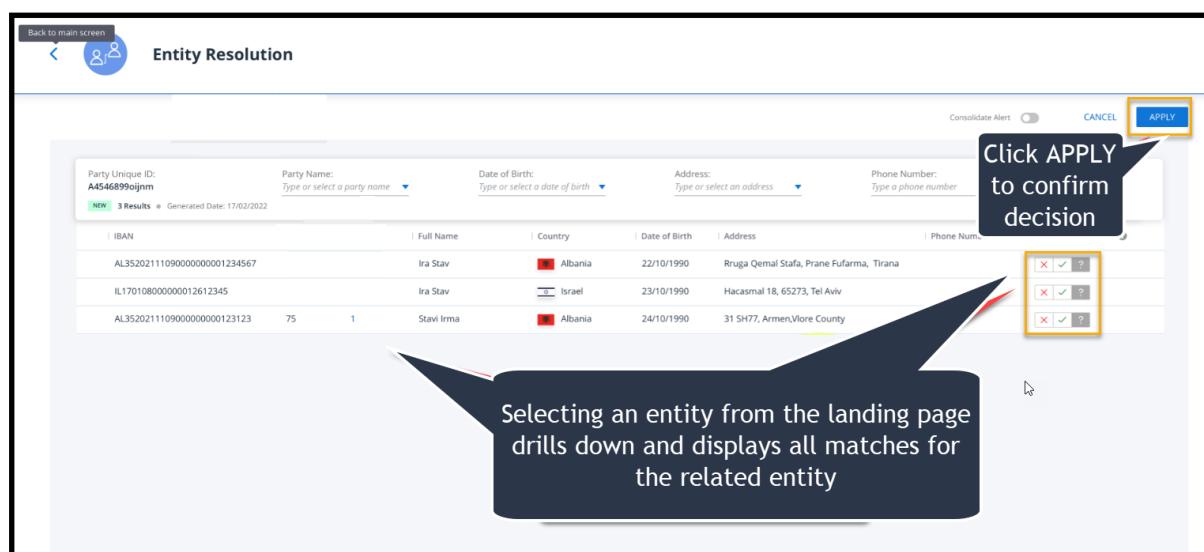


5.5. Selecting to View / Confirm all Entities for a matched Result

» To view all detected entities for a match:

1. Click the match on the Landing Page.

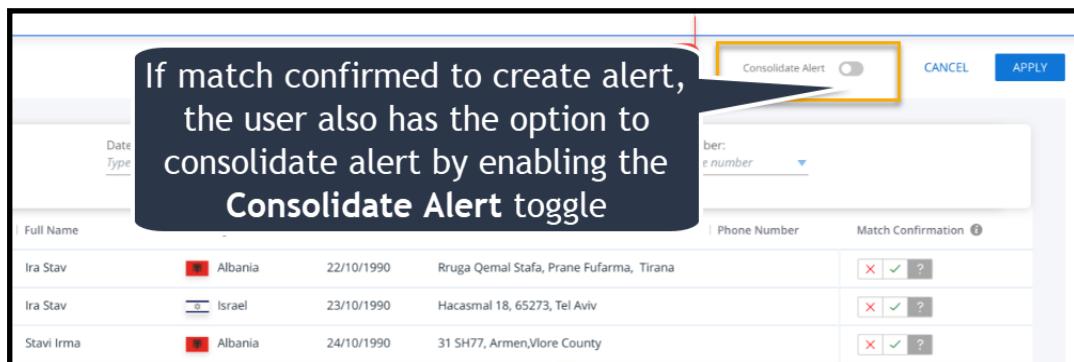
As an example, the following full list of 3 results are displayed.



2. Reject (X) Confirm (tick) match or select 'On hold; and click **APPLY**.

A confirmation message is displayed

3. Additionally, if match is confirmed the user can at this stage, decide to consolidate just the alert to be created, or consolidate all as shown in the following two examples displayed below.



Example - Consolidate the Individual Alert to be Created

Entity Resolution Parties by status: All: 1375 | New: 1375 | Processed: 0 | Updated: 0 Last Update: July 07, 2023 13:07 Refresh

Threshold Score All ▾ Generated Date Any Time ▾ Last Update Any Time ▾ Party Status New (1375) ▾ 1 of 344 Pages ▾ < > CONSOLIDATE ALL

Party Unique ID:	Party Name:	Party Address:	Party Country:	Match Confirmation		
39e66dad-f12c-4264-aab8-fad70aabb8b1	—	—	—	<input checked="" type="checkbox"/>	<input type="checkbox"/>	?
46CF6A9B3B9ED26B8E...	99	ANGIE GIORGINI	Andorra	71 ENCHANTMENTS V...	<input checked="" type="checkbox"/>	?
700B4A68D7640A3A9A1...	99	ANGIE GIORGINI	Serbia	71 ENCHANTMENTS V...	<input checked="" type="checkbox"/>	?

Party Unique ID: 3adb74b-3e9b-463b-b709-f7006fc96ebf Party Name: — Party Address: — Party Country: —

EDIT

Option to consolidate all created alerts

Figure 110: Example - Consolidate All Option

5.5.1. Important Points to be aware of when Confirming / Rejecting Matched Entities

1. A minimum of two candidate confirmations are required to enable the creation of an ER alert.
2. If all candidate accounts are declined, the suspected Party is not displayed in the ER module in the next run.
3. When one account is declined and the second is under review, the suspected Party is not displayed in the ER module in the next run.
4. When one account is declined and another is confirmed, the suspected Party is not displayed in the ER module in the next run.

5. Party alerts, account alerts with Party, account alerts with Party can be grouped by the filter Relationship.
 - a. Tags can be customly defined in IC settings.

5.6. Integration of ER Sourced Alerts Into Investigation Center

The integration of Entity Resolution sourced alerts into Investigation Center provides for their investigation and resolution as with other alert types (for example, Transaction Monitoring sourced alerts). From the analyst's point of view, they should be handled in a similar manner as other IC alerts. Their alert cards are identical, except for the addition of ER related tags such as **Party** and **Account with Party**, that signify they are ER sourced alerts.

Example Alert Card List with Entity Resolution (ER) deployed including ER Relationship filter

Examples of Entity Resolution sourced alerts integrated into a standard Transaction Monitoring alerts list

Other Entity Resolution artifacts are included for example in the Filters Section of IC module and as you will see in the following section, in the Alerts Details section as covered in the next topic of this chapter.

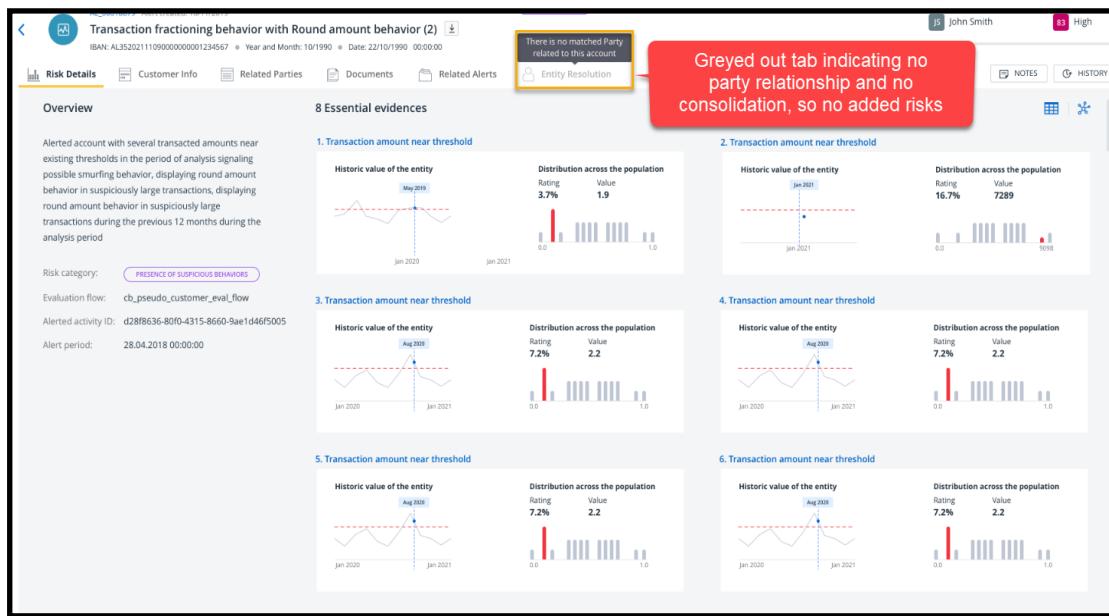
5.6.1. Entity Resolution - Examples of Alert Scenarios in Risk Details Tab

As detailed in the previous topic, ER sourced alerts are managed in a similar fashion to other IC alerts. Apart from being listed in the alerts list, they are also details in the Alerts Detail tab.

In this topic we will show examples and briefly cover each possible scenario where ER alerts both consolidated and non consolidated could appear in the in the Investigation Center Alert Details Tab.

Example Scenario #1 - Alerted Account with no Party - alert not consolidated

In this first example, where ER is enabled, but available case evidence does not indicate a Party relationship and therefore **not** ER related, and as such, this is indicated by a greyed out Entity Resolution tab as shown in the following figure.



Example Scenario #2 - Tab active ((Account alerted and consolidated but with no Party))

In this second logical scenario, let's take a look at an example where a matched candidate reflects an account candidate where the Account is not related to a Party it has triggered an alert but in this instance there are consolidated alerts indicated by the presence of displayed added risks.

Round amount behavior with Differences in counterparty data (2) (C_D_0001977)

Customer ID: 13000039691 • Customer Name: Jane Doe • National ID: 50061316

Risk Details Customer Info Related Parties Documents Related Alerts Entity Resolution

Original Risk Added Risk 1 Added Risk 2 Added Risk 3 Added Risk 4 Added Risk 5 Added Risk 6 Added Risk 7 Added Risk 8

Overview

Alerted account with several transacted amounts near existing thresholds in the period of analysis signaling possible smurfing behavior, displaying round amount behavior in suspiciously large transactions, displaying round amount behavior in suspiciously large transactions during the previous 12 months during the analysis period

Risk category: **PRESENCE OF SUSPICIOUS BEHAVIOR**

Evaluation flow: cb_pseudo_customer_eval_flow

Alerted activity ID: d28f636-80f0-4315-8650-8ae1d46f5005

Alert period: 28.04.2018 00:00:00

There is no matched Party related to this account

Entity Resolution

Grayed out tab indicating no party relationship but added risks indication consolidation

8 Essential evidences

1. Transaction amount near threshold

Historic value of the entity

Jan 2020 Jan 2021

Distribution across the population

Rating	Value
3.7%	1.9
16.7%	7289

2. Transaction amount near threshold

Historic value of the entity

Jan 2021

Distribution across the population

Rating	Value
16.7%	7289

3. Transaction amount near threshold

Historic value of the entity

Jan 2020 Aug 2020 Jan 2021

Distribution across the population

Rating	Value
7.2%	2.2

4. Transaction amount near threshold

Historic value of the entity

Jan 2020 Aug 2020 Jan 2021

Distribution across the population

Rating	Value
7.2%	2.2

5. Transaction amount near threshold

Historic value of the entity

Jan 2020 Aug 2020 Jan 2021

Distribution across the population

Rating	Value
7.2%	2.2

6. Transaction amount near threshold

Historic value of the entity

Jan 2020 Aug 2020 Jan 2021

Distribution across the population

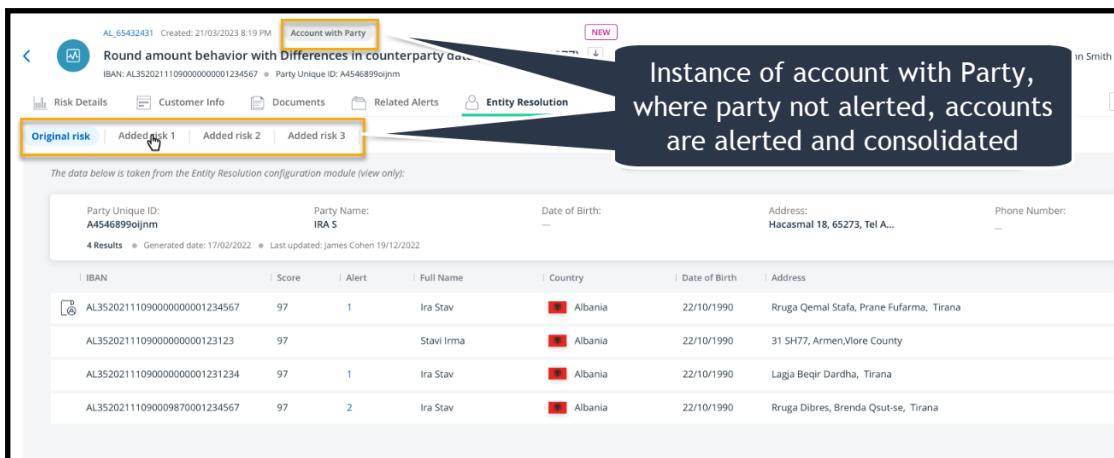
Rating	Value
7.2%	2.2

Example Scenario #3 - Tab active (Party not alerted with related account that is alerted but not consolidated)

In this scenario example a Party with an associated alerted account was matched but the user had previously reset consolidation (i.e consolidation set to zero (off) in IC settings).

Example Scenario #4 -Alerted Account and consolidated with Party (Party not alerted)

In this instance there are consolidated alerts and a party that is not alerted.



AL_65432431 Created: 21/03/2023 8:19 PM Account with Party NEW

Round amount behavior with Differences in counterparty data
IBAN: AL35202111090000000001234567 • Party Unique ID: A4546899ojnm

Risk Details Customer Info Documents Related Alerts Entity Resolution

Original risk Added risk 1 Added risk 2 Added risk 3

The data below is taken from the Entity Resolution configuration module (view only):

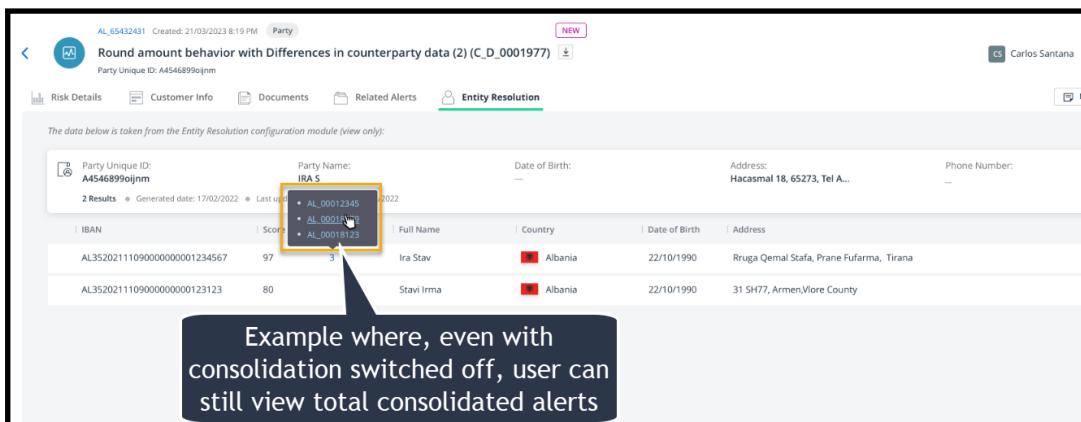
Party Unique ID:	Party Name:	Date of Birth:	Address:	Phone Number:
A4546899ojnm	IRA S	—	Hacasmal 18, 65273, Tel A...	—

4 Results • Generated date: 17/02/2022 • Last updated: James Cohen 19/12/2022

IBAN	Score	Alert	Full Name	Country	Date of Birth	Address
AL35202111090000000001234567	97	1	Ira Stav	Albania	22/10/1990	Rruga Qemal Stafa, Prane Fufarma, Tirana
AL3520211109000000000123123	97	—	Stavi Irma	Albania	22/10/1990	31 SH77, Armen,Vlore County
AL35202111090000000001231234	97	1	Ira Stav	Albania	22/10/1990	Lagia Beqir Dardha, Tirana
AL35202111090009870001234567	97	2	Ira Stav	Albania	22/10/1990	Rruga Dibres, Brenda Qsut-se, Tirana

Example Scenario #5 Party alerted and related accounts are not consolidated

In this instance there are accounts related to a party that are all alerted and consolidated



AL_65432431 Created: 21/03/2023 8:19 PM Party NEW

Round amount behavior with Differences in counterparty data (2) (C_D_0001977)

Party Unique ID: A4546899ojnm Carlos Santana

Risk Details Customer Info Documents Related Alerts Entity Resolution

The data below is taken from the Entity Resolution configuration module (view only):

Party Unique ID:	Party Name:	Date of Birth:	Address:	Phone Number:
A4546899ojnm	IRA S	—	Hacasmal 18, 65273, Tel A...	—

2 Results • Generated date: 17/02/2022 • Last updated: James Cohen 19/12/2022

IBAN	Score	Alert	Full Name	Country	Date of Birth	Address
AL35202111090000000001234567	97	3	Ira Stav	Albania	22/10/1990	Rruga Qemal Stafa, Prane Fufarma, Tirana
AL3520211109000000000123123	80	—	Stavi Irma	Albania	22/10/1990	31 SH77, Armen,Vlore County

Example where, even with consolidation switched off, user can still view total consolidated alerts

Example Scenario #6 -Party alerted and related accounts are consolidated

In this instance there are accounts related to a party that are all alerted and consolidated.

AL_65432431 Created: 21/03/2023 8:19 PM **Party** NEW

Party Unique ID: A4546899ojjm Party Name: Ira Stav

Risk Details Customer Info Documents Related Alerts Entity Resol

Original Risk | Added Risk 1 | Added Risk 2 | Added Risk 3 | Added Risk 4 | Added Risk 5 |

The data below is taken from the Entity Resolution configuration module (view only):

IBAN	Score	Alert	Full Name	Country	Date of Birth	Address	Phone Number
AL35202111090000000001234567	97	1	Ira Stav	Albania	22/10/1990	Rruga Qemal Stafa, Prane Fufarma, Tirana	
AL3520211109000000000123123	97		Stavi Irma	Albania	22/10/1990	31 SH77, Armen/Vlore County	
AL35202111090000000001231234	97	1	Ira Stav	Albania	22/10/1990	Lagja Beqir Dardha, Tirana	
AL35202111090009870001234567	97	1	Ira Stav	Albania	22/10/1990	Rruga Dibres, Brenda Qsut-se, Tirana	
NO8330001234567	97		Ira Stav	Norway	22/10/1990	Søraugleite 185, Haugesund	
CZ550800000001234567899	97	2	Ira STAVI	Czech Republic	22/10/1990	Na Loučkách 604, Rájec-jestřebí	
AL3520211109000055001234567	97	1	Irya Stav	Albania	22/10/1990	Lagja nr 2 Prane spitalit, Tirana	
LV97HABA0012345678910	97	1	Ira Stav	Latvia	22/10/1990	Raunas, bld. 33, Riga	

Instance of accounts with party alerted and also consolidated

6. Operational Dashboard Transaction Business Investigation (BI)

Note: If this module is not available as part of your IC deployment, and attempts to access it result in an error message, this may be due to a licensing issue.

6.1. Overview

The Investigation Center BI Operational Dashboard, is a data visualization and analysis tool that displays on various screens the status of key performance indicators (KPIs) and other important business metrics and data points encompassing the Thetaray's alert investigation process.

Its core purpose is to help and aid Investigation Center persona, Team managers, tasked with running a team or teams of analysts, to monitor their operational status, take appropriate action when necessary and, in short to ensure all analysts achieve maximize efficiency as they carry out their daily alert resolution duties.

Data is displayed on the operational dashboard metric widgets that include the following data types:

- Transaction Monitoring
- Transaction Screening
- Customer Screening
- Customer Risk Assessment

The Operational Dashboard consists of three modules:

- Operational Dashboard - Transaction BI
- Operational Dashboard - Trends
- Operational Dashboard - Configuration

The first module listed in the bullet list, 'Transaction BI', provides Supervisors and Team managers with the ability to monitor current alerts statistics on an ad-hoc basis . The second module listed, 'Trends', provides statistics from an historical viewpoint. Both these topics are described in detail in the remainder of this chapter.

The third module listed above , 'Configuration', enables persona with appropriate role/ permission to make specific configurations to the KPIs and value parameters that are used to define the operational dashboard settings. These settings are configured in the General Settings section of the Investigation Settings Module. For more information, refer to the current version of the *Investigation Settings*

6.1.1. BI and Trends Modules - Functionality Overview

In the BI and Trends modules the following functionalities are now included:

- Ability to switch on /off sections of the Operational Dashboard which prevents blank displays for deployments that do not include all features or products
- Customer Risk Assessment (CRA) alerts data
- Status of teams investigating CRA alerts
- Dedicated tab for alert origins
- All tab with core widget for all origins
- Drag 'n drop functionality to reorder displayed tabs

6.2. Operational Dashboard - Transaction BI and Trends Modules

Access

The Operational dashboard is accessible to Alert Investigation Supervisors and Team Managers with appropriate permission.

Access to both BI and Trend dashboard modules is via the Alerts View Side panel as shown below.

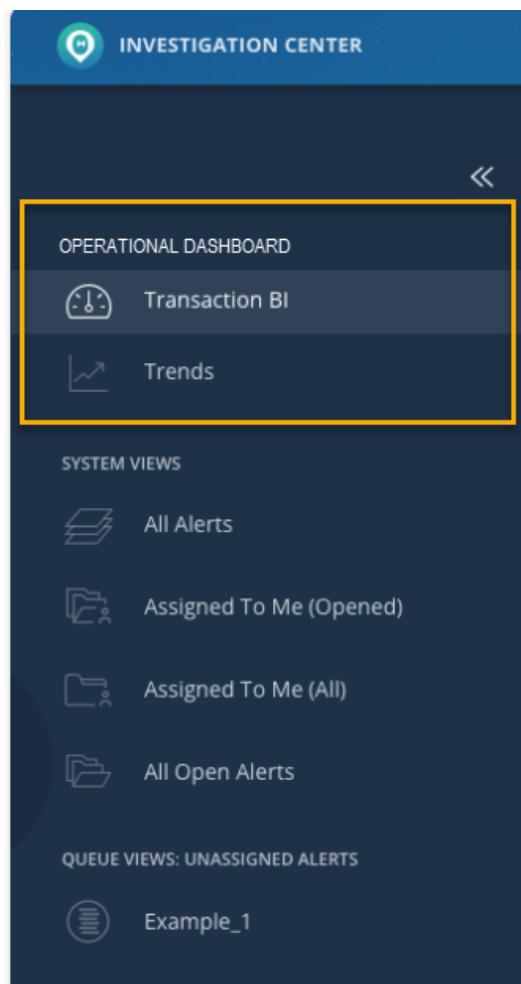


Figure 111: Operational Dashboard - Access to Transaction BI Landing page or Trends Module

6.2.1. Transaction BI - Overview

Firstly to view BI data, clicking the TRANSACTION BI tab displays a landing page similar to the following:

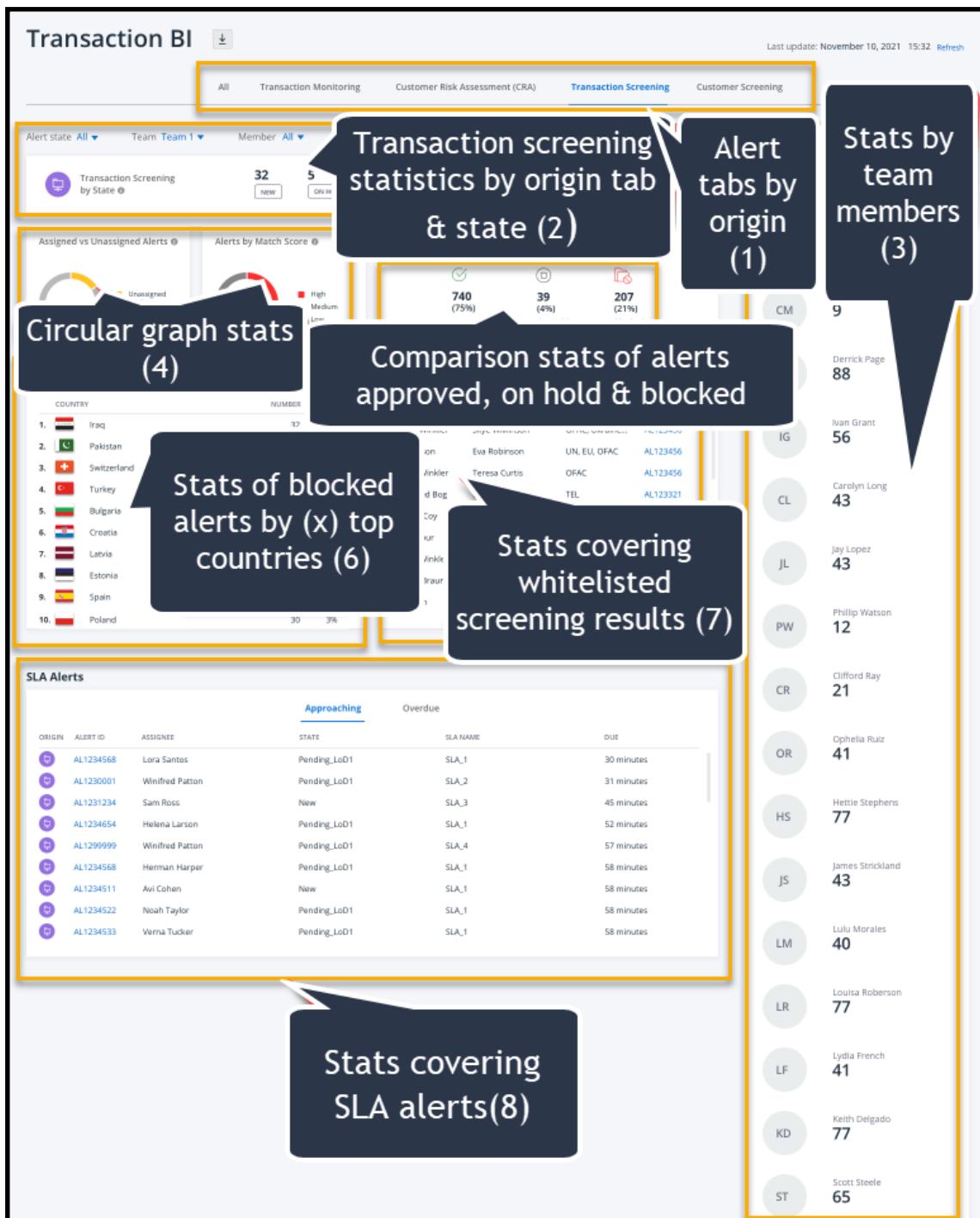


Figure 112: Example - Transaction BI Landing Page

With reference to the above image, before we cover the BI module in detail, let's familiarize ourselves with a high level overview of the Transaction BI module layout and provided key statistical sections.

Viewing from top down, alert related statistics are displayed by:

Alerts by origin tabs (1)

These tabs are displayed for selection:

- Transaction Monitoring
- Transaction Screening
- Customer Screening
- Customer Risk Assessment

Screening alert states (2)

This data block displays alerts states statistics for new and on hold screening alerts, depending on which Screening tab is selected.

Team member statistics (3)

Stats by individual team members are displayed on a right side bar column for quick comparison and assessment of each team members performance.

Circular graph statistics (4)

Circular graph statistics display statistics of alerts assigned versus unassigned and alerts by match score and as either high medium and low severity.

Screening alerts status by state (5)

Screening alerts statistics by current state- Approved, On Hold and Blocked shown by metrics and as a percentage.

Blocked alerts by (x) top countries (6)

List of 10 countries shown in descending order by number of blocked alerts, by country flag, name, metrics and as a percentage of overall total.

Whitelisted entities (7)

List of whitelisted entities displayed by user id, name, sanction list and alert id.

SLA Statistics (8)

SLA information shown either by SLA category - Approaching or Overdue and including alert origin, alert id , assignee, current state, SLA name and time till time set expiry.

6.2.2. Trends BI - Overview

Alternatively, to viewing the BI Trends module, clicking the TRENDS BI tab displays a landing page similar to the following:



Figure 113: Example - Trends BI Landing Page

With reference to the above image, similarly to our quick preview of the Transaction BI now let's familiarize ourselves with a high level overview of the Trends BI module layout and provided key statistical sections.

Alerts tab by origin (1)

- Transaction Monitoring
- Transaction Screening
- Customer Screening
- Customer Risk Assessment

Average time by state (2)

Average time by state graphs show trends in a histogram graph by state, over a selected time period.

Examples:

- New
- Pending
- Review

- Awaiting

Closed alerts by Resolution code (3)

This trends information is displayed in point to point graphic charts

Examples:

- Report FIU
- Not relevant
- Not report
- Not suspicious

Generated vs assigned vs closed alerts (4)

This information is displayed in a histogram format, and can include generated vs assigned vs closed alerts,

Transition by state (5)

Transition by state is shown between selected states by column graphs. The value length of the each column is an indication of number of alerts passed between each state column over a specific time period.

Average investigation time by category (6)

This trends graph indicated by comparison point to point line graphs the average investigation time per category.

6.3. Transaction BI Module - in Detail

The Transaction BI module comprises the following widgets:

- Filters and download widget
- DPV select where multi DPV s exist
- States - metrics widget (Transaction Monitoring Screening and CRA)
- Transaction Monitoring statistics widget - charts and histogram views
- Transaction Screening statistics widget - chart views and metrics
- Customer Risk Assessment (CRA) statistics widget - chart views and metrics
- SLA Alert Statistics widget
- Team members data widget
- Analysis download per tab

6.3.1. DPV Select

In deployments where multi Data Permission Values (DPVs) exist, the user can select to display data from a specific DPV .

Deployments where this option exists are enabled with an additional drop down select menu, as indicated in the following image.

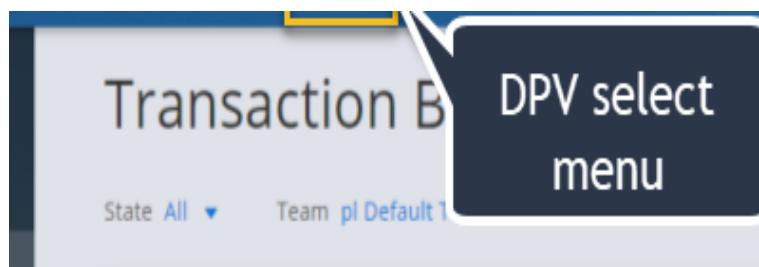


Figure 114: Example Transaction BI with DPV Menu Option

6.3.2. Filters & Download Utility

As an alerts investigation supervisor or team manager, to help you quickly understand and remedy issues that are impacting negatively on effective alert resolution, the Operational Transaction BI, comes equipped with a comprehensive set of data filters.

These filters enable you to deep dive, query and view results by an individual entity or by a cross section of entities.

To further help you understand the available statistics you can also download data reports as CSV formatted files. The filter and download widget is shown in the following figure.



The screenshot shows a header with the title 'Transaction BI' and a downward arrow icon. Below the header are three filter dropdowns: 'State All ▾', 'Team public Default Team ▾', and 'Member All ▾'.

Available Filters

Available filter categories are by:

- State
- Team
- Member

Using filters is easy:

1. Select the dropdown menu of the filter of interest.
2. Click to display the menu contents.
3. Check the box or boxes next to the items to filter by, and click APPLY.

The displayed metrics, graphs and analytics displayed in the widgets will change according to the filter applied.

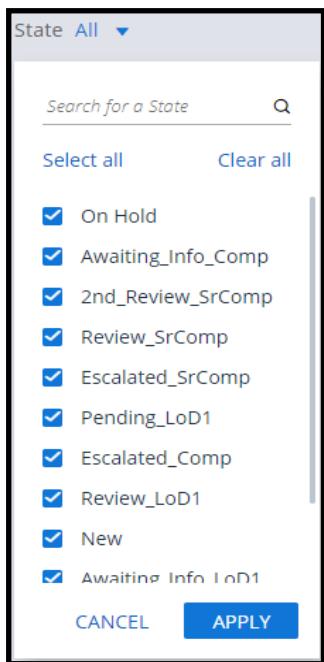
State Filter

➤ For example, to filter by state:

1. Click the State drop down menu.

An Alert state filter by menu is displayed similar to the following example. The actual filter shown will depend on whether the default workflow or a custom workflow is deployed on your environment.

The following filter by select menu example depicts a filter where a custom workflow is in place.



For this example, the table below details the full list of State filters available.

Ref	Filter by
1	On Hold
2	Awaiting_Info_Comp
3	2nd_review_SrComp
4	review_SrComp
5	Escalated_SrComp
6	Pending_LoD1
7	Escalated_Comp
8	Review_LoD1
9	New
10	Awaiting_Info_LoD1
11	2nd review_Comp
12	Review_Comp

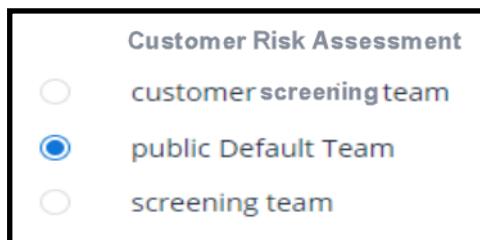
2. To filter results, check the box or boxes next to the states to filter by, or
3. Type the first few chars in the *Search for a State* field to search by autocomplete.
4. Click **APPLY**.

Note: As mentioned above, States shown in the dropdown list can vary depending on the solution(s) deployed on your environment.

Team Filter

Example Team filter select display

Select the team to filter by (Apply is automatic)



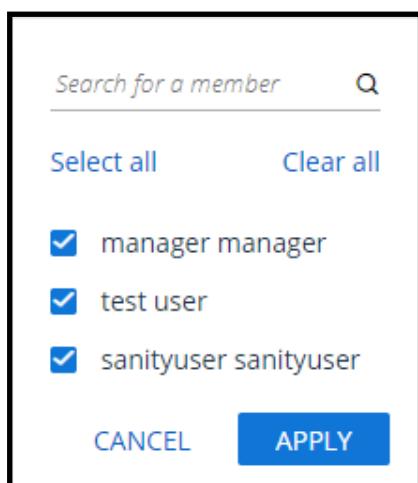
Note: When selecting to filter by teams, only one team at a time can be selected for filter and the members filter will show only selected members belonging to that specific team.

Member Filter

» For example, to filter by member

1. Click the **Member** drop down menu.

The Member filter by menu is displayed, similar to the following example:



2. Check the box or boxes next to the Members to filter by, or
3. Type the first few chars in the *Search for a member* field to search by autocomplete.
4. Click **APPLY**.

Downloading Analytic Reports

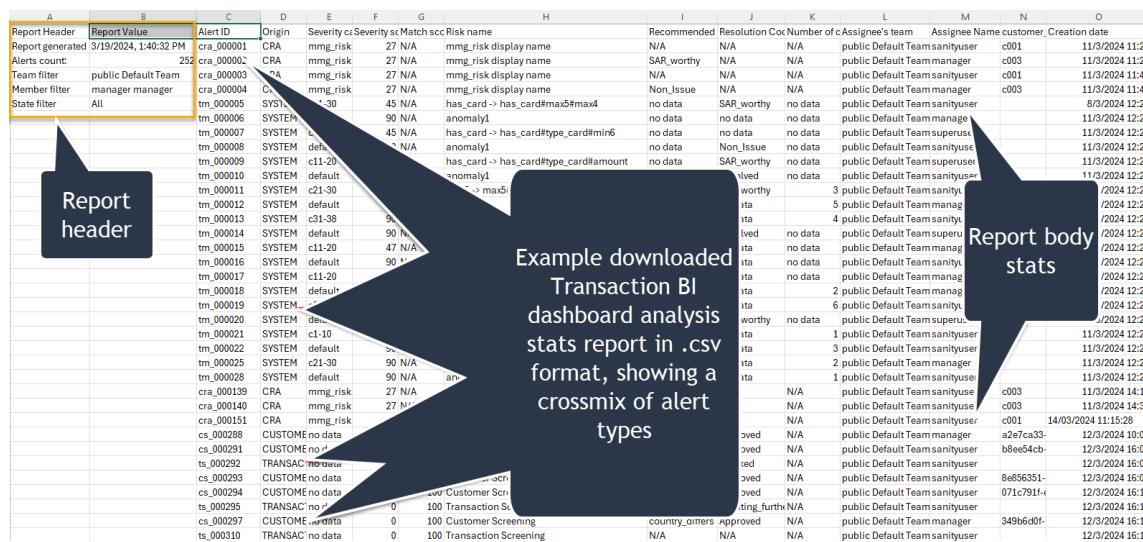
Note: Users download analytics per tab csv, so that the download only contains analysis of the tab specific content

» To download the current viewable analytical data report :

- With the results analytical data displayed, click the download icon 

The viewed page is converted to a .csv file, downloaded and is available for printing or viewing.

An example of a downloaded .csv file is shown below.



Report Header	Report Value	Alert ID	Origin	Severity	Severity	Match	sc Risk	Risk name	Recommended	Resolution	Co	Number of c	Assignee's team	Assignee Name	customer, Creation date
Report generated	3/19/2024, 1:40:32 PM	cra_000001	CRA	mmg_risk	27	N/A	mmg_risk	display name	N/A	N/A	N/A	public Default Team	sanityuser	c001	11/3/2024 11:2
Alerts count:	252	cra_000002	CRA	mmg_risk	27	N/A	mmg_risk	display name	SAR.worthy	N/A	N/A	public Default Team	manager	c003	11/3/2024 11:2
Team filter:	public Default Team	cra_000003	CRA	mmg_risk	27	N/A	mmg_risk	display name	N/A	N/A	N/A	public Default Team	sanityuser	c001	11/3/2024 11:4
Member filter:	manager manager	cra_000004	CRA	mmg_risk	27	N/A	mmg_risk	display name	Non_Issue	N/A	N/A	public Default Team	manager	c003	11/3/2024 11:4
State filter:	All	tm_000005	SYSTEM	c11-30	45	N/A	has_card-> has_card#max5#max4	no data	SAR.worthy	no data	no data	public Default Team	sanityuser	8/3/2024 12:2	
		tm_000006	SYSTEM	90	N/A	anomaly1			no data	no data	no data	public Default Team	manager	11/3/2024 12:2	
		tm_000007	SYSTEM	45	N/A	has_card-> has_card#type_card#min6			no data	no data	no data	public Default Team	superuse	11/3/2024 12:2	
		tm_000008	SYSTEM	default	27	N/A	anomaly1		Non_Issue	no data	no data	public Default Team	sanityuse	11/3/2024 12:2	
		tm_000009	SYSTEM	c11-20	45	N/A	has_card-> has_card#type_card#amount		SAR.worthy	no data	no data	public Default Team	superuse	11/3/2024 12:2	
		tm_000010	SYSTEM	default	90	N/A	anomaly1		Non_Issue	no data	no data	public Default Team	sanityuse	11/3/2024 12:2	
		tm_000011	SYSTEM	c21-30	45	N/A	has_card-> has_card#max5#max4		Non_Issue	no data	no data	public Default Team	manager	11/3/2024 12:2	
		tm_000012	SYSTEM	default	90	N/A	anomaly1		Non_Issue	no data	no data	public Default Team	superuse	11/3/2024 12:2	
		tm_000013	SYSTEM	c31-38	90	N/A	anomaly1		Non_Issue	no data	no data	public Default Team	superuse	11/3/2024 12:2	
		tm_000014	SYSTEM	default	90	N/A	anomaly1		Non_Issue	no data	no data	public Default Team	superuse	11/3/2024 12:2	
		tm_000015	SYSTEM	c11-20	47	N/A	90	**	Non_Issue	no data	no data	public Default Team	superuse	11/3/2024 12:2	
		tm_000016	SYSTEM	default	90	N/A	anomaly1		Non_Issue	no data	no data	public Default Team	superuse	11/3/2024 12:2	
		tm_000017	SYSTEM	c11-20	47	N/A	90	**	Non_Issue	no data	no data	public Default Team	superuse	11/3/2024 12:2	
		tm_000018	SYSTEM	default	90	N/A	anomaly1		Non_Issue	no data	no data	public Default Team	superuse	11/3/2024 12:2	
		tm_000019	SYSTEM	c21-30	45	N/A	90	**	Non_Issue	no data	no data	public Default Team	superuse	11/3/2024 12:2	
		tm_000020	SYSTEM	default	90	N/A	anomaly1		Non_Issue	no data	no data	public Default Team	superuse	11/3/2024 12:2	
		tm_000021	SYSTEM	c1-10	45	N/A	90	**	Non_Issue	no data	no data	public Default Team	superuse	11/3/2024 12:2	
		tm_000022	SYSTEM	default	90	N/A	anomaly1		Non_Issue	no data	no data	public Default Team	superuse	11/3/2024 12:2	
		tm_000023	SYSTEM	c21-30	90	N/A	90	**	Non_Issue	no data	no data	public Default Team	superuse	11/3/2024 12:2	
		tm_000024	SYSTEM	default	90	N/A	anomaly1		Non_Issue	no data	no data	public Default Team	superuse	11/3/2024 12:2	
		tm_000025	SYSTEM	c1-10	45	N/A	90	**	Non_Issue	no data	no data	public Default Team	superuse	11/3/2024 12:2	
		tm_000026	SYSTEM	default	90	N/A	anomaly1		Non_Issue	no data	no data	public Default Team	superuse	11/3/2024 12:2	
		tm_000027	SYSTEM	c1-10	45	N/A	90	**	Non_Issue	no data	no data	public Default Team	superuse	11/3/2024 12:2	
		tm_000028	CUSTOMER	no data	90	N/A	90	**	Non_Issue	no data	no data	public Default Team	superuse	11/3/2024 12:2	
		tm_000029	CUSTOMER	no data	90	N/A	90	**	Non_Issue	no data	no data	public Default Team	superuse	11/3/2024 12:2	
		tm_000030	CUSTOMER	no data	90	N/A	90	**	Non_Issue	no data	no data	public Default Team	superuse	11/3/2024 12:2	
		ts_000292	TRANSA	no data	0	100	Customer Screening	country_owners	Non_Issue	no data	no data	public Default Team	superuse	12/3/2024 16:0	
		cs_000293	CUSTOMER	no data	0	100	Customer Screening	country_owners	Non_Issue	no data	no data	public Default Team	superuse	12/3/2024 16:0	
		cs_000294	CUSTOMER	no data	0	100	Customer Screening	country_owners	Non_Issue	no data	no data	public Default Team	superuse	12/3/2024 16:1	
		ts_000295	TRANSA	no data	0	100	Customer Screening	country_owners	Non_Issue	no data	no data	public Default Team	superuse	12/3/2024 16:1	
		cs_000296	CUSTOMER	no data	0	100	Customer Screening	country_owners	Non_Issue	no data	no data	public Default Team	superuse	12/3/2024 16:1	
		ts_000310	TRANSA	no data	0	100	Customer Screening	country_owners	Non_Issue	no data	no data	public Default Team	superuse	12/3/2024 16:1	

Figure 115: Example of a Downloaded Analytics Report in CSV format

Note: Best practices and key takeaways from displayed analytics. As you work through analytic result monitoring, be aware of statistics indicating workflow bottle necks, or other issues requiring action on your part to mitigate the situation.

6.3.3. Alert States Widget - Metrics

The following example widget shows:

- Transaction monitoring alerts by state
- Transaction Screening alerts by state (if use case includes transaction screening)
- Customer Screening alerts by state (if use case includes customerscreening)

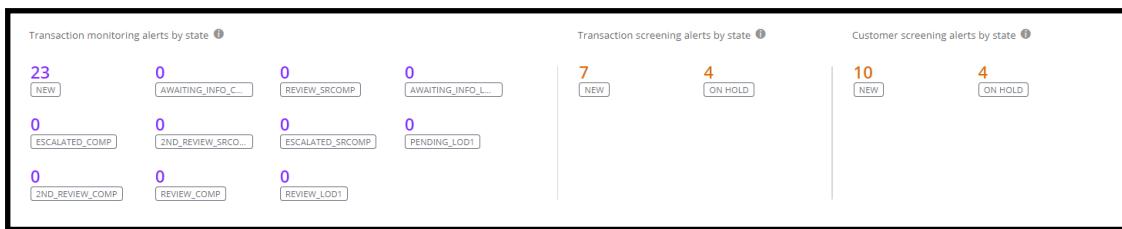


Figure 116: All Alert Categories - State Statistics

Update to include CRA

This widget displays both charts segmentation and a histogram to demonstrate and highlight key Transaction Monitoring alert statistics and data distribution output over time.

6.3.4. Transaction Monitoring Statistics Widget - Charts and Histogram

This widget displays both charts segmentation and a histogram to demonstrate and highlight key Transaction Monitoring alert statistics and data distribution output over time.

The example widget shown below displays:

- Distribution comparison chart of assigned versus unassigned alerts
- Distribution comparison chart of alerts by severity (High, Med, Low)
- Histogram of top risk categories
- Listed and detailed in order of risk importance (top 9)

6.3.4.1. Top Risk Widget Data - Further Details

- The Top Risk widget displays the list of the top nine risks of alerts during the last 24 hrs
- A user has the ability to navigate to and examine the filtered list of alerts in IC that contain top risks
- Indication of the number and percentage of alerts in which the risks were identified.
- The order of the top risks in the list is descending based on the number of alerts in which risks were identified.

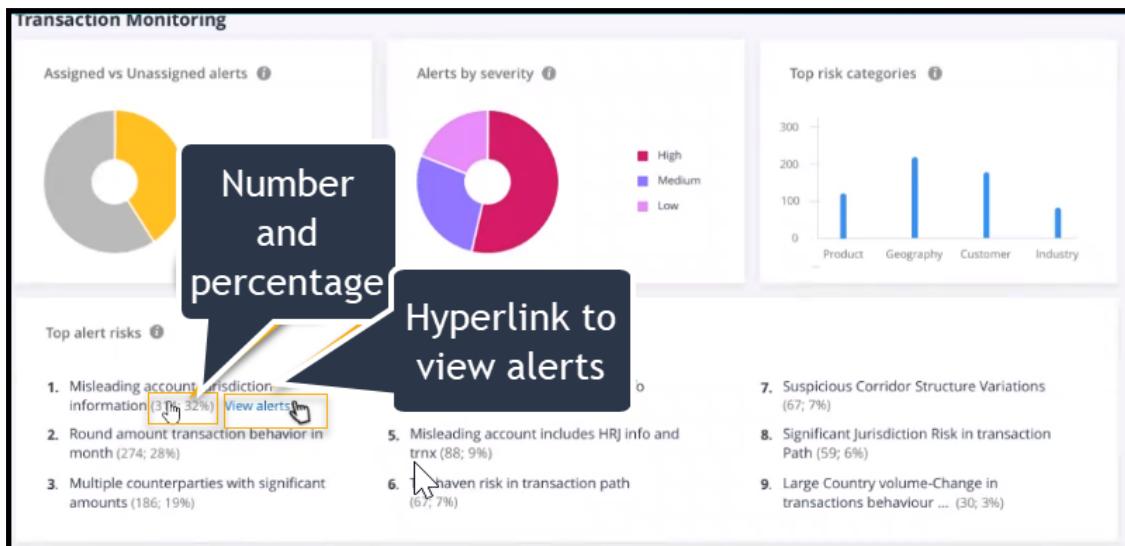


Figure 117: Example Transaction Monitoring Distribution Chart, Histogram and Top Risk Order

Note: Also, as shown in the above figure, the number and percentage of risk alert categories are displayed, plus a hyperlink is included to enable associated alerts to be viewed.

6.3.5. Transaction Screening Statistics Widget - Charts and Metric Views

This section (if deployed) uses both comparison charts showing segmentation and metrics to demonstrate and highlight distribution comparison by chart of related Transaction Screening alert statistics.

The following example widget shows:

- Comparison chart of Assigned versus Unassigned alerts
- Comparison chart of alerts by match score (High , Med, Low)
- Metrics and percentage value of approved vs on hold vs blocked alerts
- List of countries where blocked alerts originate from, in descending order of default, and including metrics and percentages
- Last 24 Hours of whitelisted entities

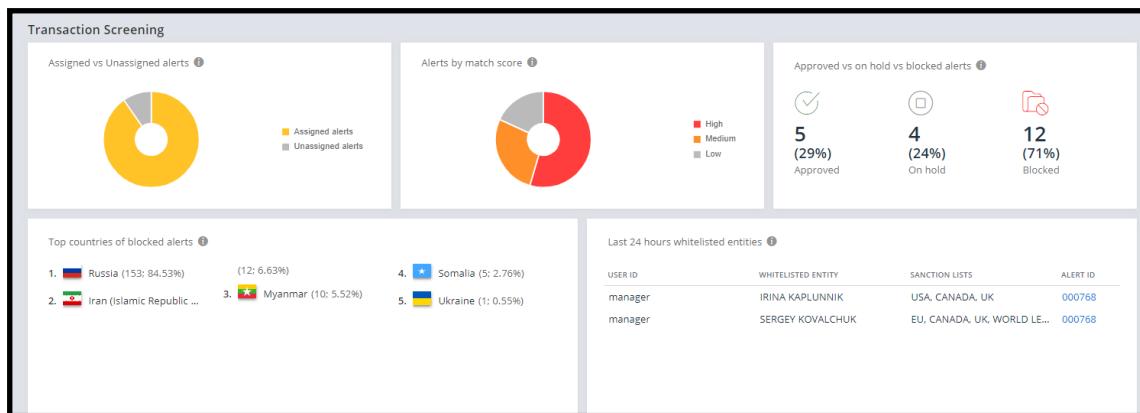


Figure 118: Example Transaction Screening Results Widget Showing Related Statistics

Note: As a best practice if **Transaction Screening** is not included in the deployment and to avoid a blank widget being displayed, the section should be made **inactive** in the Investigation Settings under General Settings.

6.3.6. Customer Screening Statistics Widget - Charts and Metric Views

This section (if deployed) uses both comparison charts showing segmentation and metrics to demonstrate and highlight distribution comparison by chart of related Customer Screening alert statistics.

The following example figure shows:

- Comparison chart of Assigned versus Unassigned alerts
- Comparison chart of alerts by match score (High, Med, Low)
- Metrics and percentage value of approved vs on hold vs blocked alerts
- List of countries where blocked alerts originate from, in descending order of default, and including metrics and percentages.
- Last 24 Hours of whitelisted entities

Note: As a best practice if **Customer Screening** is not included in the deployment and to avoid a blank widget being displayed, the section should be made **inactive** in the Investigation Settings under General Settings.

6.3.7. Customer Risk Assesment (CRA) - BI Dashboard Examples

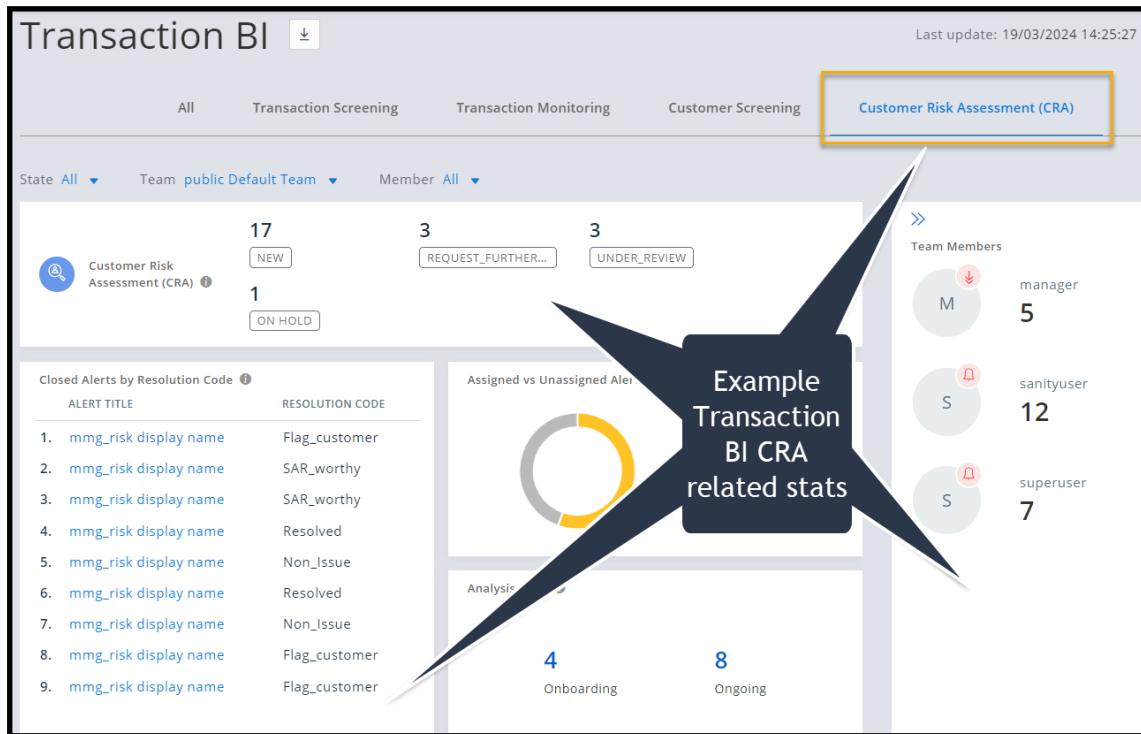


Figure 119: Example #1- CRA stats in Transaction BI Module

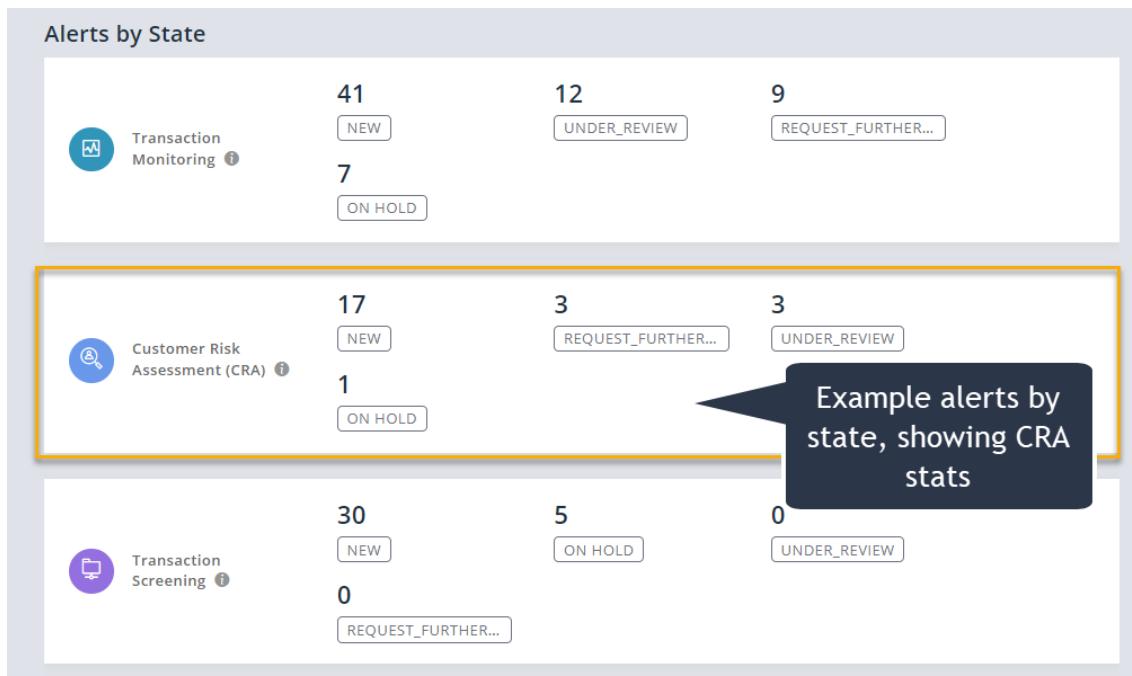


Figure 120: Example #2 - Highlighted Screenshot Showing CRA States Statistics

ORIGIN	ALERT ID	ASSIGNEE	STATE	Approaching		Overdue
				SLA NAME	DUE	
🔍	000680	sanity		2 day SLA	a day	
🔍	000681	super		2 day SLA	a day	
🔍	000682	super		2 day SLA	a day	
🔍	000683			2 day SLA	a day	
🔍	000684	mana		2 day SLA	a day	
🔍	000685	sanity		2 day SLA	a day	
🔍	000686	superuser	state_new	2 day SLA	a day	
🔍	000687	superuser	state_new	2 day SLA	a day	
🔍	000688	manager	state_new	2 day SLA	a day	
🔍	000689	manager	state_new	2 day SLA	a day	

Figure 121: Example - CRA Alert in CRA with Handy Link to Open Alert in IC Details

6.3.8. SLA Alert Statistics Widget

This widget displays a list of SLA statistics for alerts that are either in the crucial category stages of 'Approaching' or 'Overdue'.

Each alert is tagged with an origin icon indicating if it is a Transaction Monitoring, Transaction Screening or Customer Screening alert. Included in the list where appropriate are assignee, current state as well time due or overdue.

Approaching alerts ⓘ					Overdue alerts ⓘ				
ORIGIN	ALERT ID	ASSIGNEE	STATE	DUE	ORIGIN	ALERT ID	ASSIGNEE	STATE	OVERDUE
🔍	000005	manager	SLA Review to 2nd Review	2 minutes	🔍	000071	developer	SLA Pending to 2nd Rev... a day	
🔍	000005	manager	SLA Pending to 2nd ReviewComp	2 minutes	🔍	000071	developer	SLA Review to 2nd Rev... a day	
🔍	000009	manager	SLA Pending to 2nd ReviewComp	a minute	🔍	000072	manager	SLA New to Closed	a day
🔍	000009	manager	SLA Review to 2nd Review	a minute	🔍	000073	developer	SLA New to Closed	a day
🔍	000046	manager	SLA Review to 2nd Review	2 minutes	🔍	000074	manager	SLA Review to 2nd Rev... 19 hours	
🔍	000046	manager	SLA Pending to 2nd ReviewComp	2 minutes	🔍	000074	manager	SLA Pending to 2nd Rev... 19 hours	
🔍	000050	manager	SLA Review to 2nd Review	a minute	🔍	000074	manager	SLA New to Closed	a day
🔍	000050	manager	SLA Pending to 2nd ReviewComp	a minute	🔍	000075	developer	SLA New to Closed	a day
🔍	000056	manager	SLA Review to 2nd Review	2 minutes	🔍	000075	developer	SLA New to Closed	a day
🔍	000056	manager	SLA Pending to 2nd ReviewComp	2 minutes	🔍	000078	manager	SLA New to Closed	a day
🔍	000079	manager	SLA Pending to 2nd ReviewComp	2 minutes	🔍	000079	developer	SLA New to Closed	a day
🔍	000079	manager	SLA Pending to 2nd ReviewComp	2 minutes					

Figure 122: Example SLA Alerts in 'Approaching' or 'Overdue' SLA State for all types of alerts Monitoring/ Screening

6.3.9. Team Members Widget

In this final widget of the Operational Dashboard Transaction BI module , all team members are listed.

Data included in the Team members list includes full name, initials and number of alerts currently opened and assigned to each member as shown in the following example figure.

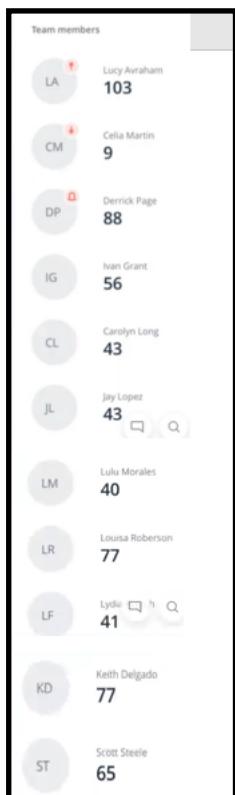


Figure 123: Example Team Members List

Team / Member Status Icons

Regarding teams, and by association members of each team, these can assume one of the following workload states:

- Normal - no workload issues (no icon tag)
- () Overload -The number of alerts assigned to a team member that is above the threshold
- () Idle - The number of alerts assigned to a team member that is below the threshold
- () Warning - alert SLA(s) that are logged as approaching , delayed or overdue

Icon levels and warning alarm SLAs are configured in the General Settings section of Investigation Settings by Settings admin user with the required permissions.

They are set per the rules listed above.

6.4. Trends Module - in Detail

To Access the Trends module , click the Trends link in the alert select side panel of the Investigation Center. The Trends access link and module is displayed as shown in the following figure.

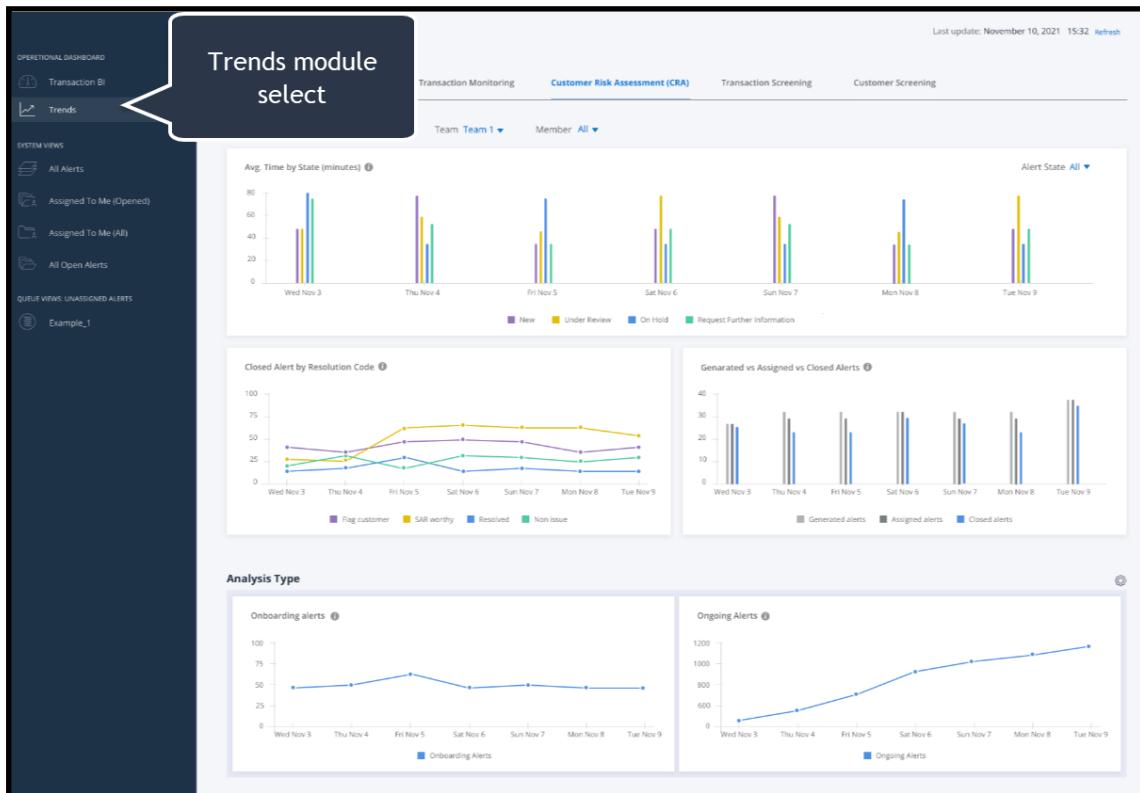


Figure 124: Accessing The Trends Module of the Operation Dashboard

The Trends dashboard module provides the Teams Manager with an Historical perspective on the workflow currently being employed in their alert resolution deployment.

The Trends module (like the Transaction BI) also provides filters , display widgets and a utility to download detailed widget content per tab as reports in .csv format.

A notable feature of the Trends module is its ability for the user to set up trial iterations of results using combinations of various filters (for example, by using the recent time periods filter and viewing comparison results gain a more insightful understanding of underlying and emerging trends).

6.4.1. Filter Widgets

Various filters including time period, teams and members, and including the download reports icon are located at the module header.

Additionally, a an alert state filter is included with the State analytics widget.

Time Period Filter

The time period filter provides the user the ability to filter the widget display by configurable :

- Days
- Weeks
- Months

The following figure shows an example of the Time Period Filter. The time period can be set numerically or by using the *From* and *To* calendar select widgets.

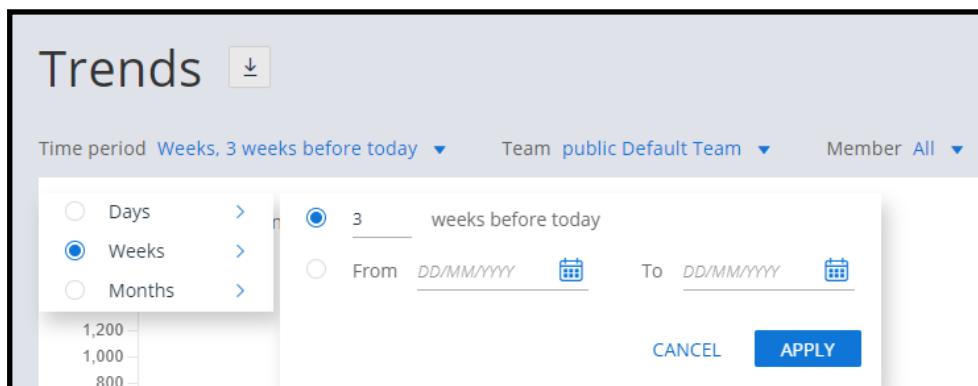


Figure 125: Example of the Time Period Filter in Trends Module

The Team / Member Filter

As in the BI module the Team and Members filters provide the option to filter by team and member(s).

Downloading Analytic Reports

Note: Users download analytics per tab csv, so that the download only contains analysis of the tab specific content

» To download the current viewable analytical data report :

1. With the historical results analytical data displayed, click the download icon



The viewed page is converted to a .csv file, downloaded and is available for printing or viewing.

An example of a downloaded historical data .csv file is shown below.

Report No	Report Value	Alert ID	Origin	Severity category	Severity scor	Match score	Risk name	Recomm. Resolution	No. of consol.	Assignee	Na transaction_id	Sanction	Country	Creation date	Last update
Report ger 3/19/2024, 1:55:54 PM		000292	TRANSAC	no data	0	100	Transaction Screening	N/A	N/A	public Del sanituser	a3989393-491b-452-9849-dee27a1f8 EU	RU	12/2/2024 16:09	13/03/2024	
Start date	3/12/2024	000292	TRANSAC	no data	0	100	Transaction Screening	N/A	N/A	public Del sanituser	a3989393-491b-452-9849-dee27a1f8 EU	RU	12/2/2024 16:09	13/03/2024	
End date	3/19/2024	000292	TRANSAC	no data	0	100	Transaction Screening	N/A	N/A	public Del sanituser	a3989393-491b-452-9849-dee27a1f8 EU	RU	12/2/2024 16:09	13/03/2024	
Alerts cou	33	000295	TRANSAC	no data	0	100	Transaction Screening	N/A	N/A	public Del sanituser	d0407322-c2d-4ba1-ac9d-db133a EU	RU	12/2/2024 16:10	14/03/2024	
Team filter	public Default Team	000336	TRANSAC	no data	0	100	Transaction Screening	N/A	N/A	public Del sanituser	d27922f-hb2-409-8214-74b8b8ec EU	N/A	13/03/2024 14:34:39	13/03/2024	
Member filter	public Default Team	000338	TRANSAC	no data	0	100	Transaction Screening	N/A	N/A	public Del sanituser	0501090-49a5-448-980-4098888 EU	RU	12/2/2024 16:09	13/03/2024	
Time reso	7 DAY	000338	TRANSAC	no data	0	96	Transaction Screening	N/A	N/A	public Del sanituser	86265590-9d81-4f05-453a-1b3243 UK	N/A	13/03/2024 15:22:18	13/03/2024	
Example Trends analysis .csv report header stats		000339	TRANSAC	no data	0	100	Transaction Screening	N/A	N/A	public Del sanituser	5e14d3b-1081-44f0-8517-09631905 EU	N/A	13/03/2024 15:34:09	13/03/2024	
		000436	TRANSAC	no data	0	100	Transaction Screening	N/A	N/A	public Del sanituser	78a-2229-c66-44d3-876d-1b42656 EU	RU	14/03/2024 14:30:48	14/03/2024	
		000437	TRANSAC	no data	0	100	Transaction Screening	N/A	N/A	public Del sanituser	aef4d49-1768-4969-beff-a1d8b77 EU	MM	14/03/2024 14:33:11	14/03/2024	
		000448	TRANSAC	no data	0	100	Transaction Screening	N/A	N/A	public Del superuser	b3e79347-1b09-4a76-a952-9b66777 EU	RU	14/03/2024 15:13:49	14/03/2024	
		00452	TRANSAC	no data	0	100	Transaction Screening	N/A	N/A	public Del sanituser	97a6b730-6c6f-4c85-a9b3-917e1c EU	RU	14/03/2024 15:33:25	14/03/2024	
		00607	TRANSAC	no data	0	100	Transaction Screening	N/A	N/A	public Del sanituser	3786957-6356-4ac5-82fc-a939fa83d EU	CU	15/03/2024 16:48:41	15/03/2024	
		00608	TRANSAC	no data	0	88	Transaction Screening	N/A	N/A	public Del sanituser	051090-49a5-448-980-4098888 EU	RU	15/03/2024 16:47:12	15/03/2024	
		00610	TRANSAC	no data	0	100	Transaction Screening	N/A	N/A	public Del sanituser	2fa9a67-5cd4-493e-960a-cc71c87 EU	UZ	15/03/2024 16:48:15	15/03/2024	
		00611	TRANSAC	no data	0	100	Transaction Screening	N/A	N/A	public Del sanituser	c4-1781-4c6-4451-ac5-6014ca EU	RU	15/03/2024 16:48:40	15/03/2024	
		00612	TRANSAC	no data	0	100	Transaction Screening	N/A	N/A	public Del sanituser	b4126b-4c7-493-916b-516b71 EU	RU	15/03/2024 16:48:42	15/03/2024	
		00613	TRANSAC	no data	0	98	Transaction Screening	N/A	N/A	public Del sanituser	b77-397-453a-881-4-04-04-04 EU	RU	15/03/2024 16:48:42	15/03/2024	
		00617	TRANSAC	no data	0	93	Transaction Screening	N/A	N/A	public Del sanituser	d77c-cc-9b-411-3-b-07-1-cd8b7c EU	IT	15/03/2024 16:55:27	15/03/2024	
		00618	TRANSAC	no data	0	100	Transaction Screening	N/A	N/A	public Del sanituser	22d5d-6-cd4-44b-0-791-ec84702 EU	RU	15/03/2024 16:55:57	15/03/2024	
		00619	TRANSAC	no data	0	100	Transaction Screening	N/A	N/A	public Del sanituser	35d-3-ae-1b1-4055-16-6-0-0-0-0-0-0 EU	RU	15/03/2024 16:56:22	15/03/2024	
		00620	TRANSAC	no data	0	67	Transaction Screening	N/A	N/A	public Del sanituser	c7aha24-4385-4d3-929-92b-ecb95f5 EU	AZ	15/03/2024 16:56:53	15/03/2024	
		00705	TRANSAC	no data	0	100	Transaction Screening	N/A	N/A	public Del sanituser	c3b5b89-0321-42x-9-8b-0-bcb3d0 EU	RU	18/03/2024 14:34:10	18/03/2024	
		00707	TRANSAC	no data	0	100	Transaction Screening	N/A	N/A	public Del sanituser	de5ca6b-95b4-4384-baf1-513-0-7e EU	ME	18/03/2024 14:35:21	18/03/2024	
		00708	TRANSAC	no data	0	100	Transaction Screening	N/A	N/A	public Del sanituser	03030-5-609-4b7b-bd-0-0-6268 EU	RU	18/03/2024 14:35:56	18/03/2024	
		00710	TRANSAC	no data	0	100	Transaction Screening	N/A	N/A	public Del sanituser	c5c8d8f-6-2b1-4055-16-6-0-0-0-0-0 EU	RU	18/03/2024 14:36:52	18/03/2024	
		000712	TRANSAC	no data	0	100	Transaction Screening	N/A	N/A	public Del sanituser	1419083-abc-4617-8677-8-17c76 EU	RU	18/03/2024 14:39:22	18/03/2024	
		000713	TRANSAC	no data	0	100	Transaction Screening	N/A	N/A	public Del sanituser	34c395-e549-46a7-94aa-a97c7c2 EU	RU	18/03/2024 14:39:39	18/03/2024	
		000714	TRANSAC	no data	0	100	Transaction Screening	N/A	N/A	public Del sanituser	dad46fc-2-8b-41a-1-8485-9-4-9-9 EU	RU	18/03/2024 14:39:50	18/03/2024	
		000736	TRANSAC	no data	0	100	Transaction Screening	N/A	N/A	public Del sanituser	77854-2-8b-41a-1-8485-9-4-9-9 EU	RU	18/03/2024 14:39:51	18/03/2024	
		000737	TRANSAC	no data	0	100	Transaction Screening	N/A	N/A	public Del sanituser	028a8-6694-46-2-4-2-1-aa-1-1 EU	AM	18/03/2024 14:39:52	18/03/2024	
		000738	TRANSAC	no data	0	100	Transaction Screening	N/A	N/A	public Del sanituser	233040-ec-1f-429-9-6-7-1-ec-1-0 EU	RU	18/03/2024 14:47:07	18/03/2024	
		000739	TRANSAC	no data	0	100	Transaction Screening	N/A	N/A	public Del sanituser	0dc550da-4463-40-6-0-9-7-0-0 EU	RU	18/03/2024 14:47:39	18/03/2024	

Figure 126: Example of Trends Historical Analytics Report in .csv File Format

6.4.2. Trends Example Widgets

To demonstrate example historical analytical trends that can be displayed in this module, the following example widget views are provided:

Example #1 - Average time by state over a period of the last 7 days.

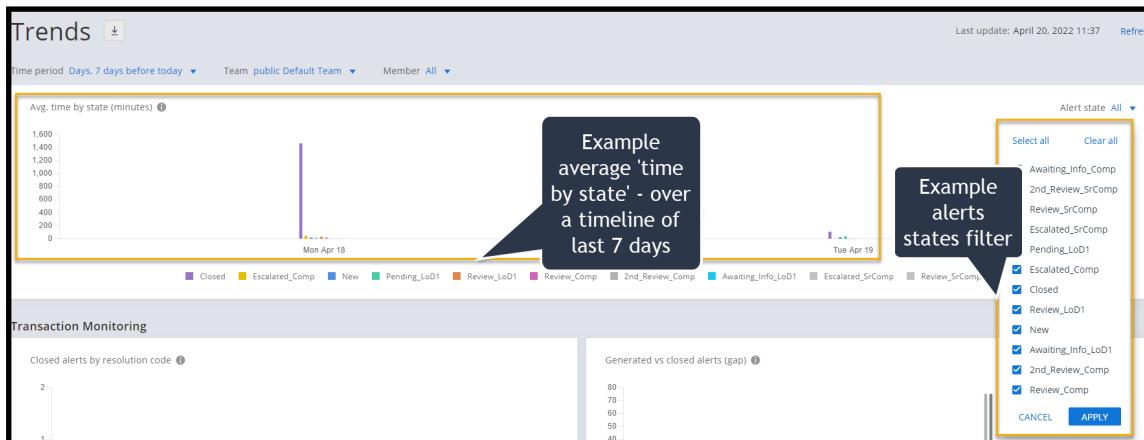


Figure 127: Example #1 - Average time by state over a period of the last 7 days

Example #2 - Transaction Monitoring - Generated vs Assigned vs Closed Alerts

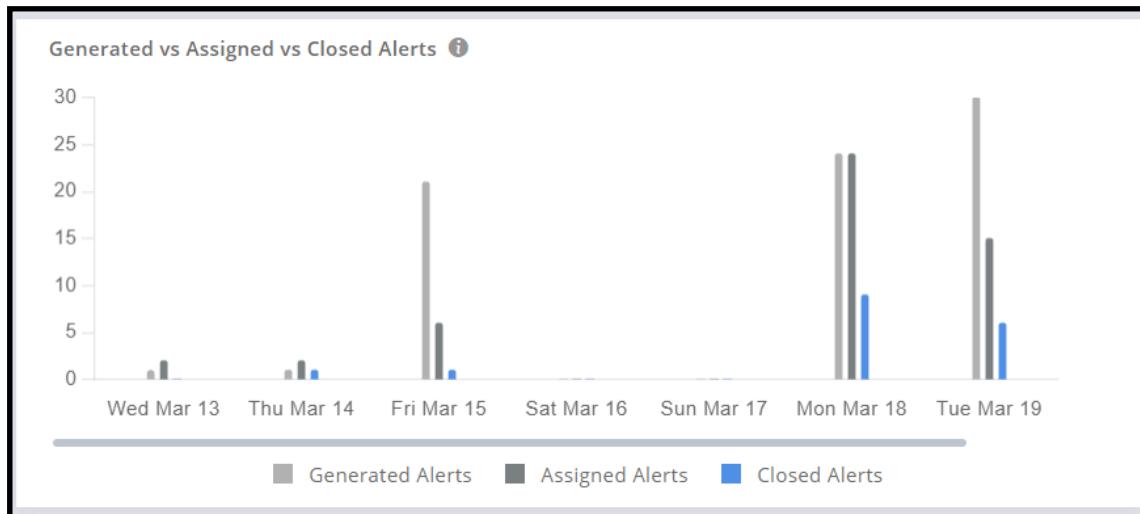


Figure 128: Example #2 - Generated vs Assigned vs Closed Alerts also Showing Information Tool-tip

Example #3 - Transaction Monitoring - Average investigation Time by Category (minutes)

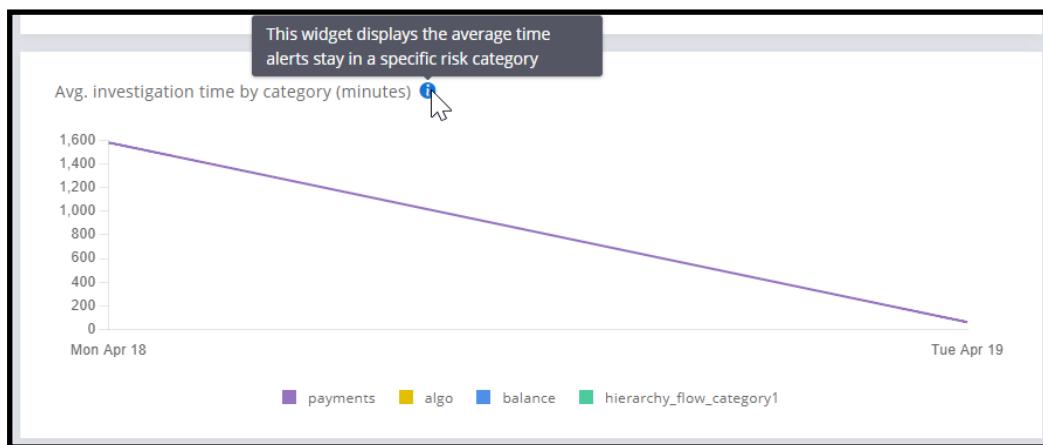


Figure 129: Example #3 - Average Investigation Time by category

Example #4 - Transaction Screening - Closed Alerts by Resolution Code



Figure 130: Example #4 Transaction Screening - Closed Alerts by Resolution Code

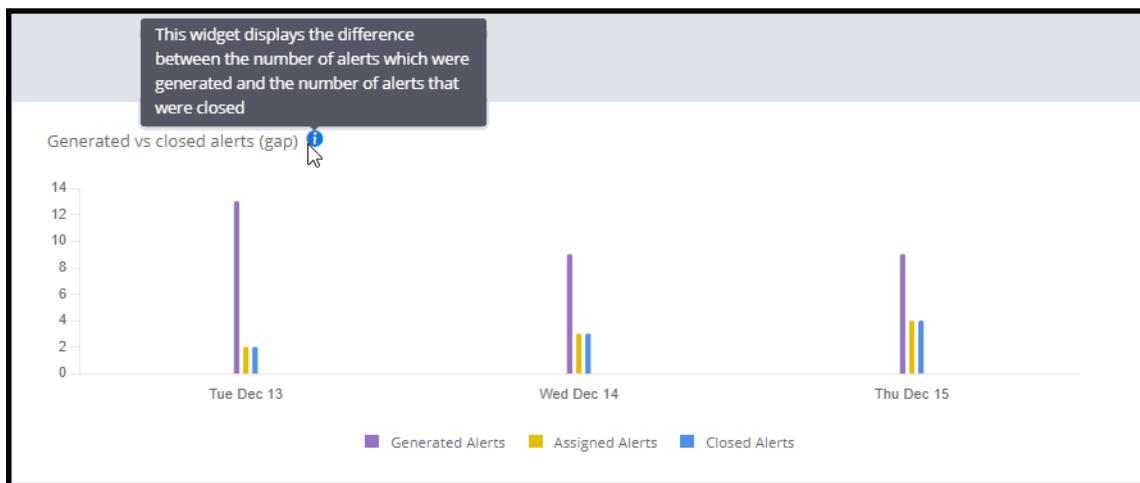


Figure 131: Example #4 Transaction Screening - Difference between Number Generated / Closed Alerts Trend

Example #5 - Transaction Screening - Top Countries of blocked alerts



Figure 132: Example #5 Top Three Countries - Blocked Alerts Trend

Example #6 - Transaction Screening - Whitelisted Trends



Figure 133: Example 6 - Whitelisted Alerts - Trend

Customer Screening

Example #7 - Customer Screening Closed Alerts by Resolution code

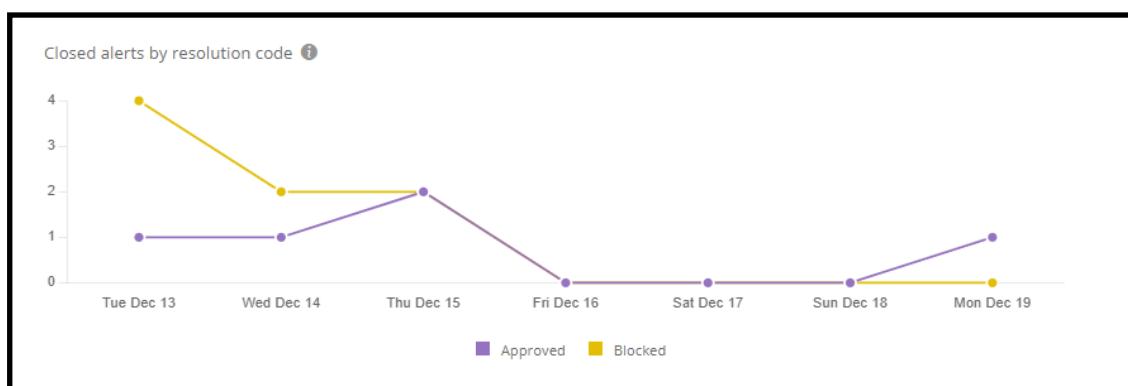


Figure 134: Example 7 - Customer Screening - Alerts Closed by Resolution Code Trend

Example #8 Customer Screening - Number of Alerts Activated vs Closed

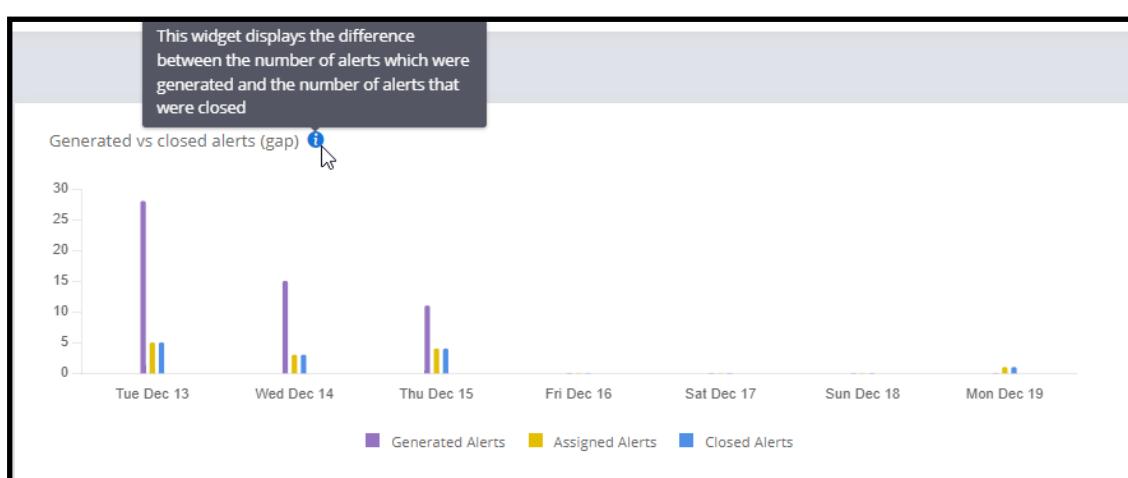


Figure 135: Example 8 - Customer Screening - Number of Alerts Activated vs Closed Trend

Example #9 Customer Screening - Top three Sanction Screened Lists



Figure 136: Example 9 Customer Screening - Top Three Sanctioned Lists Trend

Example #10 Customer Screening - Whitelisted Trend

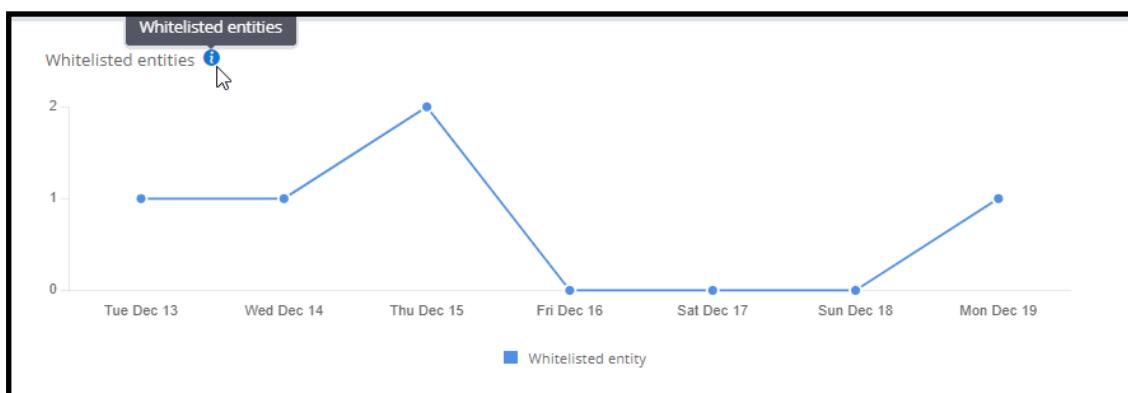


Figure 137: Example 10 Customer Screening - Whitelisted Trend

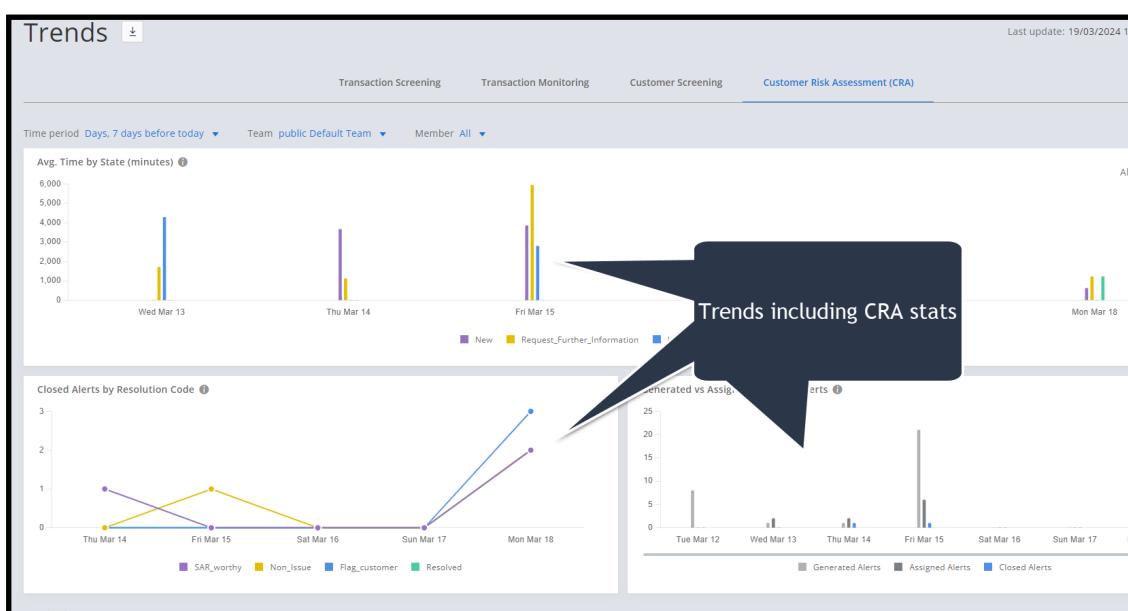


Figure 138: Example CRA Metrics Shown in Trends Module

7. The Case for Network Visualization

Before we explore how to use network visualizations in your alert investigation environment, lets take a brief look at the key challenges faced by companies working with alert resolution.

Whatever your role within the alert resolution process, as an analyst, supervisor or perhaps as a business admin user, the fundamental challenges faced daily by all concerned are how to improve efficiency, by speeding up the alert resolution process while maintaining a high level of risk assessment accuracy.

Network Visualization, enables the analyst or supervisor to view transactions and their interconnectivity by means of a network graph. The graph consists of a matrix of nodes that shows related parties in a transactional network and includes such statistics such as the sender and receiver for each transaction, and other relevant information and forensic evidence that reveals suspicious transactional patterns. The graph matrix is super effective in providing the investigator with a fast and informative insight into what is 'going on' and to quickly understand the overall activity pattern.

Armed with this enhanced information, analysts can then make their workflow more efficient, by helping to speed up the process of making more informed decisions about the validity of the risk under investigation quicker, and with a higher degree of accuracy.

7.1. Accessing Network Visualization Module

From the introduction, you should better understand what Network Visualizations are, let's access this module and learn how to use its functionality.

Note: If this module or part of its functionality is not as described in this chapter and not available as part of your IC deployment, this may be due to a licensing issue.

» To access Network Visualization in your IC deployment:

1. From the Alerts list , click the Alert of Interest to open its *Risk Details* page.

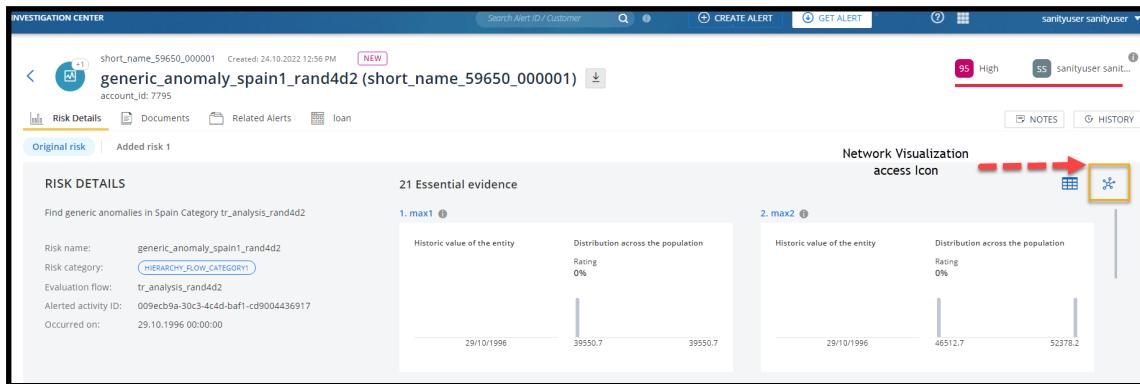
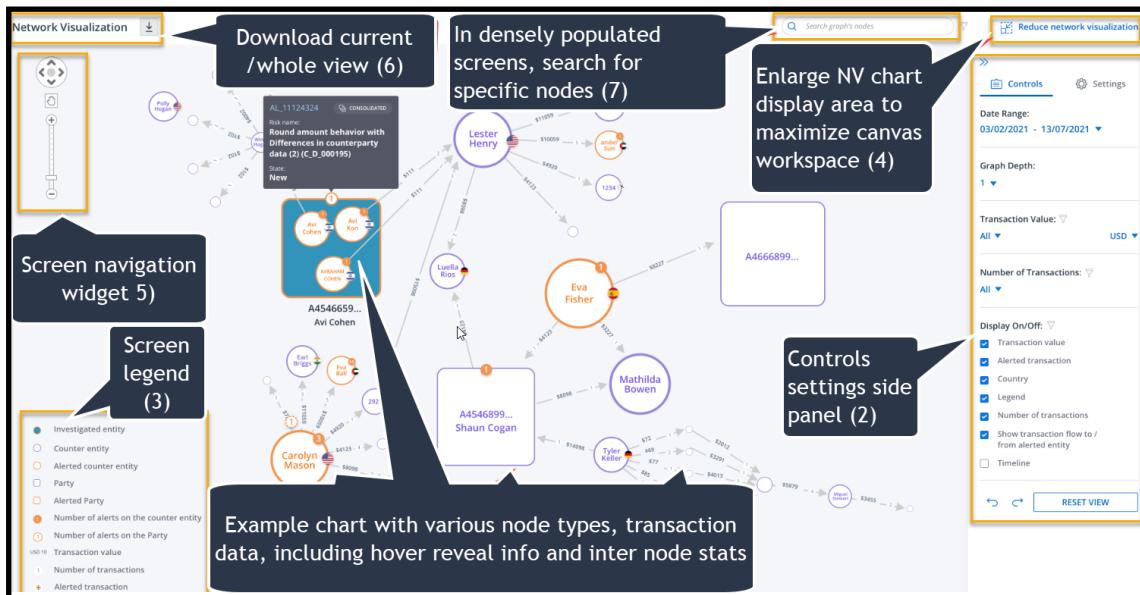


Figure 139: Network Visualization Icon, that Provides Access to the Alert Transaction Entity Connection Graph

The highlighted network icon is our key to accessing Network Visualization for the selected alert.

2. Hovering over the icon reveals the 'View Network Visualization' information tool tip.
3. Clicking the icon opens the Network Visualization 'Landing page' similar to the following.

Figure 140:



Network Visualizations - Example Landing Page

We will cover each of the main highlighted landing screen components in detail in a moment, but first let's orientate ourselves with the general landing page layout:

- **Main Chart Elements / Entities** (1) - Example key central elements of the network visualization module and along with associated linked entities that shows various node types, statistics data and transaction flows
- **Controls and Setting Side Panel** (2) - This side panel contains the chart controls and settings that are used by the analyst to filter and configure the NV display. This is especially important with alerts, that in some instances can contain excessive data which may cloud the investigation process. Filtering and configuration helps provide visually a clearer understanding of the alert, and key related associated transactions
- **Key Icon Legend** (3) - Provides a key description for each symbol used in the NV chart
- **Enlarge / Reduce Network Visualization** (4)- with two display options:
 - a. **Enlarge Network visualization** - Used with side panel collapse option maximizes graph screen to help focus investigation on transactions flow
 - b. **Reduce Network Visualization** - Reduces graph screen to default size that enables access to related tabs (for example, Documents, Risk details, Related alerts, Notes etc.) and also alert card details
- **Zoom and Screen Navigation** (5) - Enables zoom and navigational movement around the screen canvas
- **Download** (6) - Download current / whole chart view in various formats
- **Search Graph Nodes** (7) - For alerts that are data intensive, locating a specific node maybe challenging, so to mitigate this possible issue you can make searches via this provided search field located at the top of the NV screen

7.2. Network Visualization (NV) - Key Module Components

Now that we have taken a brief look the NV module layout, we need to dig a bit deeper into each key module component before attempting some practical example working procedures.

The highlighted NV functionality components mentioned in the Accessing Network Visualization chapter module are described in the following sub sections topics .

These elements can be categorized as follows:

- Graph (Chart) Nodes and edges
- Controls and Settings side panel
- Auxiliary Components (screen functionality)

7.2.0.1. Graph (Chart) Nodes and Edges

Let's take a close look at the 'make up' of a network graph.

The network graph, constructed from alert data, is made up of multiples of two basic elements:

- Nodes
- Edges

Nodes

A node, can signify the key transaction 'player' (under investigation) or related transaction players.

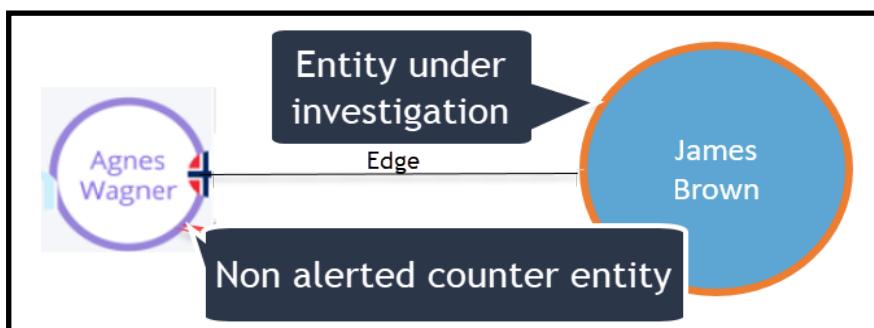
Both 'player' types can be either a transaction sender or transaction recipient.

Additionally a node usually holds related alert information about the 'player' (example: Country of origin, total number of co-related transactions (sender or recipient) and, if it is an alerted entity or party.

Edges

Edges contain transactional direction plus other relevant statistics

Let's take a closer look at a simple section of a graph diagram that depicts two nodes (key player and co-respondent joined by an edge).



Lets drill down deeper into graph nodes and their connecting edge entities.

A **node** contains details and icon tags that provide:

- Name of entity under investigation
- Name and type of node (entity and party)
- Country of origin-flag icon, (if available)
- Nodes can be on the account level and depending if the customer has the ER license also at Party node level
- A + plus icon on the entity border indicates other related transactions exists in the database (**Note:** The plus sign will appear by hovering over the entity and only if there is a related transaction at a higher depth level ++++). Also,

note that the + sign can be configured to show always. For more info, refer to section Meaning of a Plus (+) Icon

- The relative size of the entity node is indicative of the total monetary value magnitude
- **Note:** The size of the party node is not related to any other related node value
- If the entity has a numbered tag on its border this indicates the number of transactions under the entity. Clicking this tag reveals more information about the transaction (example: id number)
- Hovering on alert number entity displays a detailed info tool tip

An **edge** contains tags and icons that provide:

- Direction of transaction single direction or a double edge if transactions exist in both directions
- Alert icon if transaction is suspected as being a "contributor" to the alert
- Amount and currency of transaction(s) - aggregated sum
- Number of transactions both for entities and parties
- Animation display to and from the entity

7.2.1. Graph Nodes and Edges

The following section shows examples of graph nodes and edges and how they are represented in a Network Visualizations graph

7.2.1.1. Types of Nodes

Nodes displayed in a Network Visualizations graph are differentiated by shape and color. These can be categorized as an entity or as a party.

The following two example images, show both types, their different shapes indicating what category of nodes they belong to but their common border color indicating their alert status.

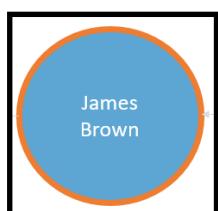


Figure 141: Example - Account Entity under investigation (Alerted)

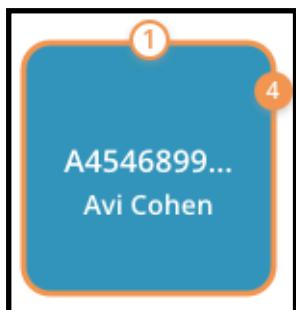


Figure 142: Example - Party Entity under investigation (Alerted)

7.2.1.2. Displaying Alert Id Instead of Alert Name

if it aids the investigation process, the analyst can select to show the Alert Id in NV instead of Alert Name.

Refer to Control panel on how to configure.

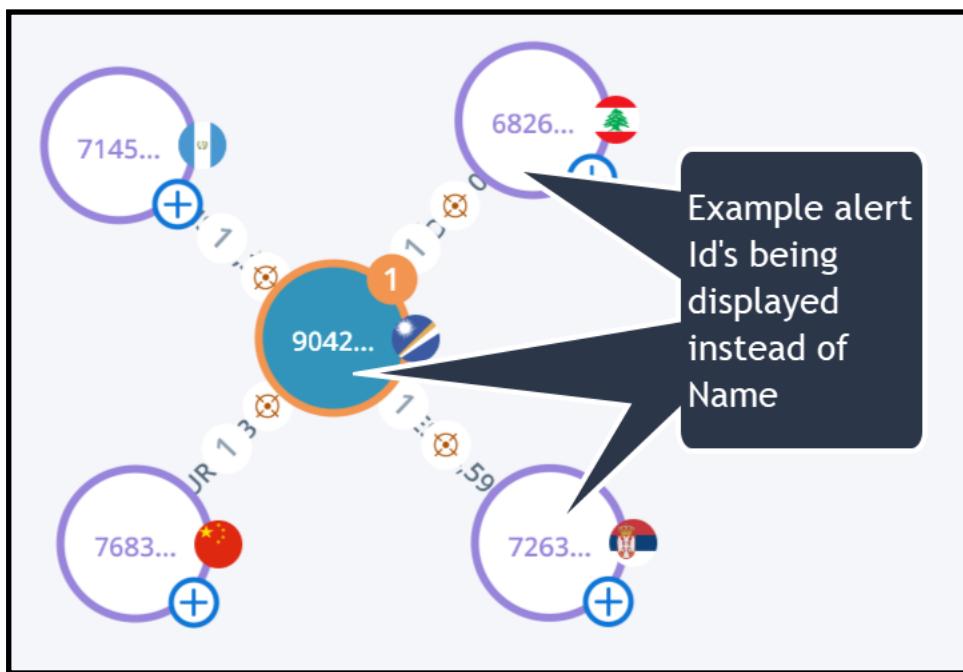


Figure 143: Nodes Displaying Alert Id Instead of Alert Name ()

Account and Party Entities - Non Alerted

In Network visualizations non alerted entities and parties are represented by similar shaped nodes as indicated in the above alerted examples, but are differentiated by border and background color as shown in the examples below. These entities can be of type sender or recipient



Figure 144: Example Non- alerted Account Entity

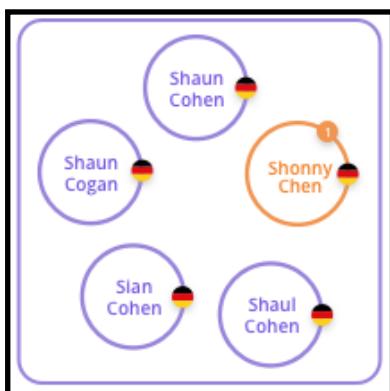


Figure 145: Non Alerted Party Entity with Individual Party Related Accounts displayed

7.2.1.3. Examples - Icon Tagging in Network Visualizations

Although described briefly in the opening section of this chapter, and also detailed in the graph legend, the extensive use of tagged icons throughout the network visualization graph requires additional information to aid the analyst in the task of alert investigation when working with the further 'drill down' detail.

Ability to View Party Accounts Detail on Hover

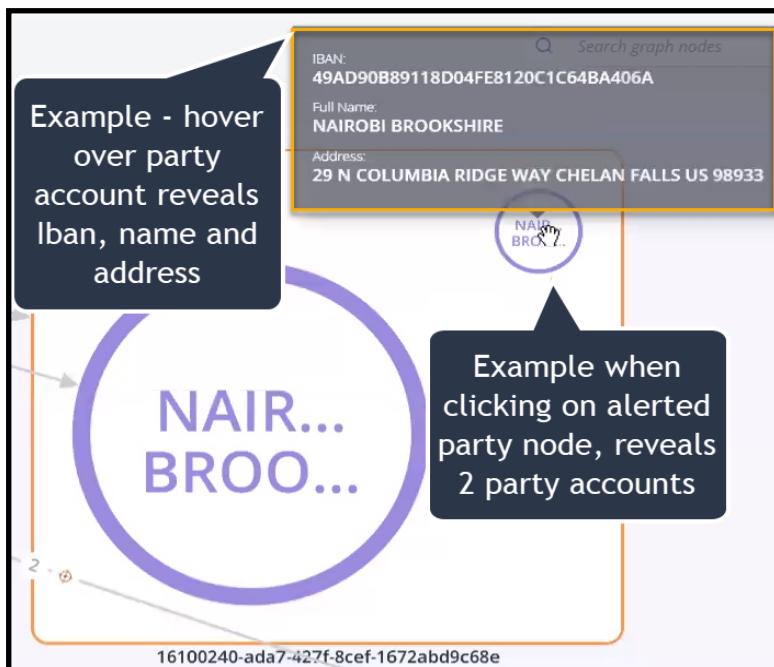
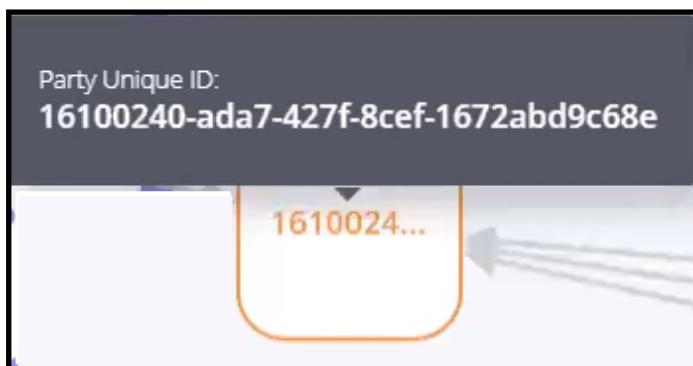
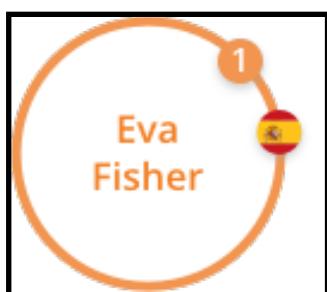


Figure 146: Example- Alerted Party (Orange Border) with 2 Accounts Detail with Transactions

Tool Tip Info Displayed on Hover



Account Entity with Related Transaction Icon



Country of Origin - Tagged by Flag

Each counter party is also tagged by his / her main country of origin (if exists in database). Hovering on this icon reveals the country of origin

This indication can help in the investigation process, as historically some countries can be classified as being in a high risk category.

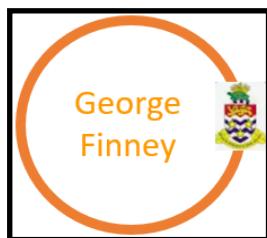


Figure 147: Example of Account Entity - from Cayman Islands with flag tag

Country of Origin + Consolidation Indication

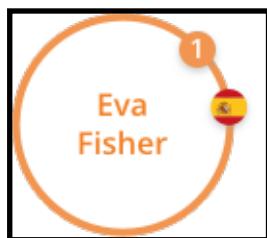


Figure 148: Example of Entity with Country of origin Flag and Border Icon indicating Consolidation

Meaning of a Plus (+) Icon

In Network Visualizations a very effective feature is the + icon on the entity border. This icon indicates that this entity is linked to at least one other entity. The number of linked entities is only limited by the amount of related data in the database and is not restricted by the 'Graph Depth' level. The analyst as part of his investigation strategy should use this feature to '*follow the money trail*' to see where it leads and what insightful information it provides.

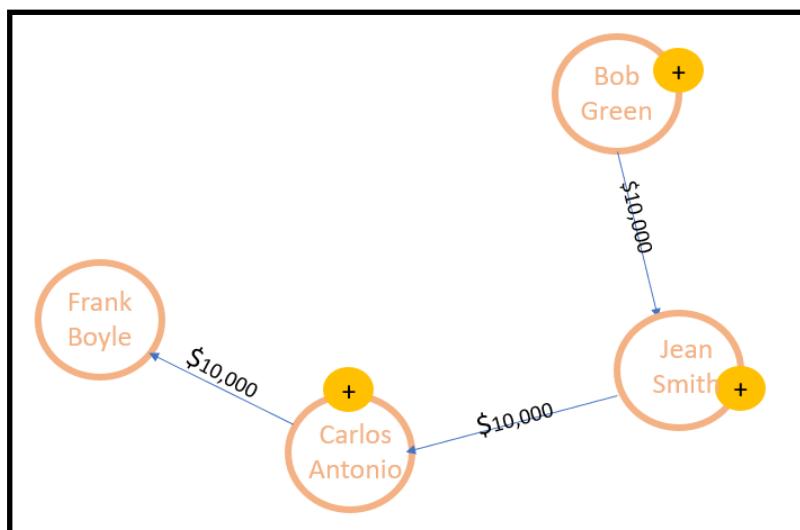


Figure 149: Example of Entities revealed by the + icon that Provide a 'Money Trail' to Follow

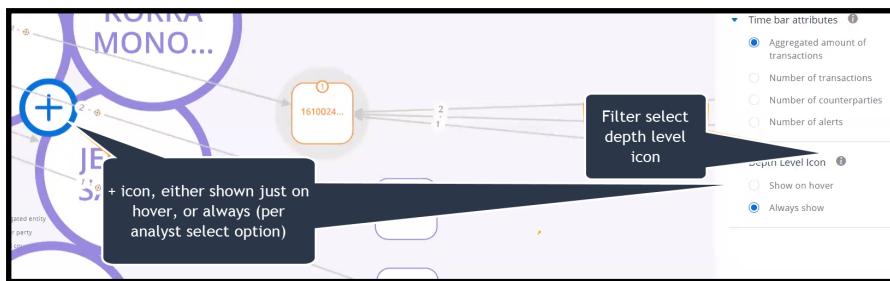


Figure 150: Example - (+) Icon on Border(Shown on hover or Always) - Indicating Node Accounts

Alerts Under an Account or Party Entity

If there is a numbered tag shown on a node entity, this indicates that more information on each alert is available by clicking on the tag.

In the following example, where 3 related alerts are indicated on the tag, clicking on the number tag, information such as the alert id is displayed.

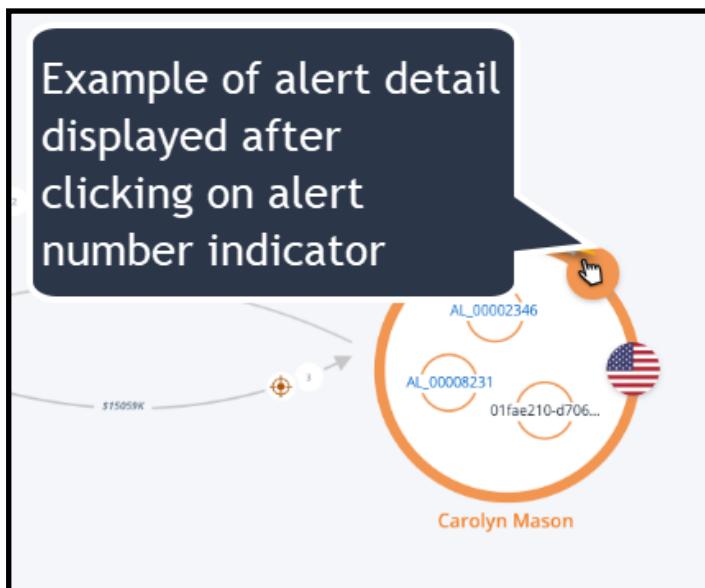


Figure 151: Example of Alert Node Number indication, Revealing more Detail

Hovering on Alert Entity, Displays Alert Details

Numbered tags can also when hovered over reveal summary alert detail such as:

- Alerted activity ID
- Risk Name
- Alert id
- if the activity contains regular, consolidated or suppressed alerts
- Alert status

Note: The provided tool tip can in some instances contain details of multiple activities. If so, simply use the scroll function to view all data.

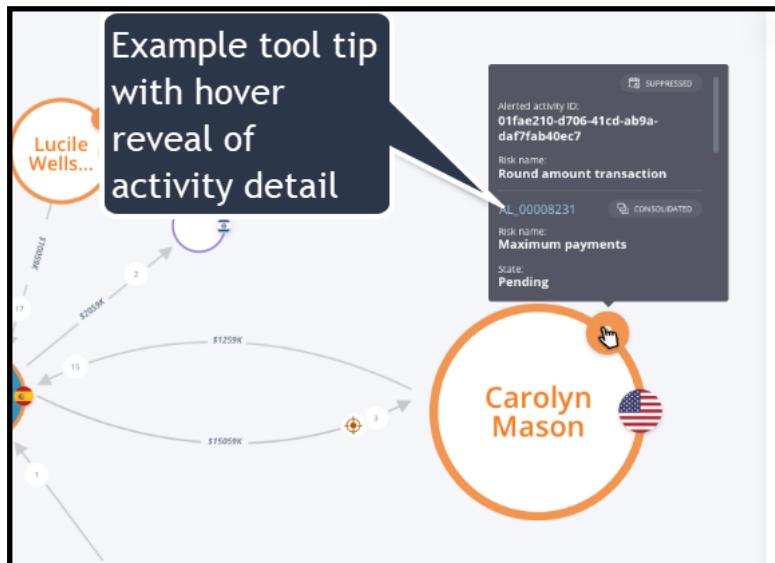


Figure 152: Hovering on Node Transaction Tag Reveals Activity Detail

7.2.1.4. Node Size Related to Total Aggregated Amount Range

The node size relationship to the total aggregated amount for displayed entity nodes is detailed in the following table:

Note: Node size relationship indication, only applies to single account entities and not to Party entity nodes

Ref	Node Size	Total Aggregated Amount Range
1	Small	0 - 250k USD
2	medium	250k - 500K USD
3	Large	500k - 750k USD
4	X - large	750k +

7.2.1.5. Edges

The graph edges link the graph nodes together and contains information on the data that is being transmitted between entities.

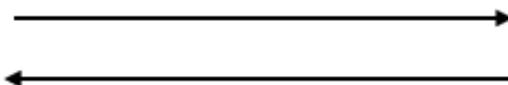
7.2.1.6. Direction of Transaction

Transactions between entities are indicated by arrows as follows:

- One way - single arrow



- Both ways - double arrows



7.2.1.7. Number of Alerts sourced by the Entity under Investigation

Included in the edge is a numbered icon that indicates the total number of transactions between two entities.



Figure 153: Example - Entity sourced transactions

7.2.1.8. Alert Icon - Displayed, if Transaction is Suspected as Being a 'contributor' to Activity

If the transaction is suspected as being a 'contributor' to the alert activity, the following icon is included in the edge:



Figure 154: Example of Target Icon Indicating a transactional alert

7.2.1.9. Amount and Currency of Transaction

Included in the graph edge is the amount and currency of the transaction.

If several transactions are included in the edge, the amount shown is an aggregated total.

The transaction currency is also indicated:

Examples:

- Euros - 25000
- \$ 100,000

- yen - 5000

7.2.1.10. Number of Counter Entity Transactions

Included in the edge is a numbered of counter party sourced transactions that are being sent either to the entity being investigated or to other counter parties.



Figure 155: Example of Counter Entity Sourced Transactions

7.2.1.11. Tool tip / Details if Alert type is Manually Created



Figure 156: Graph Segment with Popup Indicating Inclusion of Manually Created Alert

7.2.2. Controls and Settings Side Panel

7.2.2.1. Control Tab

The main functionality provided under the Control Tab provides the ability to filter the various aspects available in the Network Visualizations display.

The figure below shows an example Control Tab.

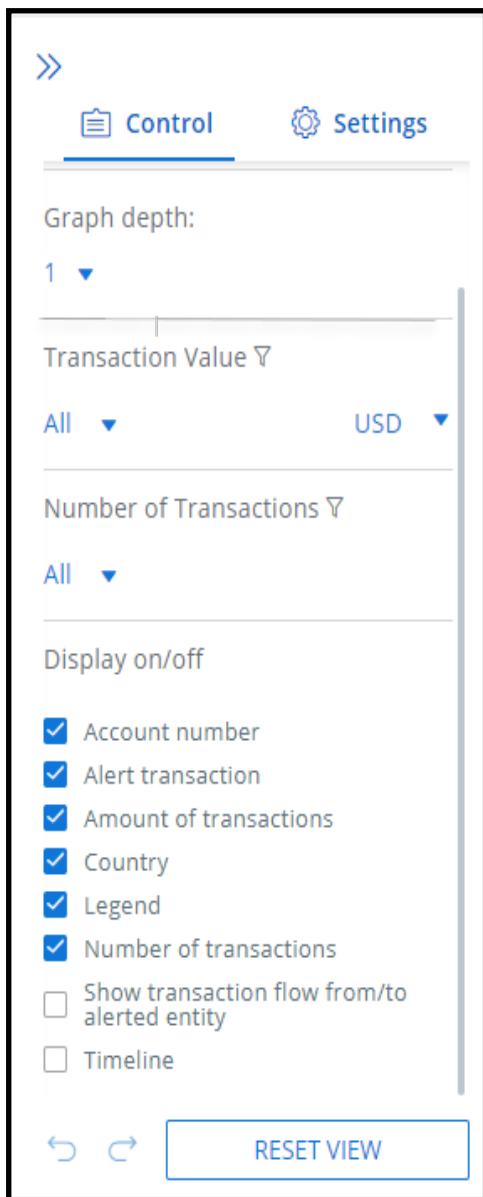


Figure 157: Example - Control Tab with Account Id selected instead of Name

Lets take a moment to review the key elements of the Control Tab.

With reference to the above image, the following bullet list briefly details elements of the control tab:

- **Date Range** - Select the date range capture window parameters
- **Graph Depth** - Select the level of graph connections to display
- **Number of Transactions** - Select to include transaction number statistics per grouping
- **Transaction Value** - See detailed description below
- **Display On /Off** - Switch on / off entire segments of display data

- **View Options** - includes options to view previous or next set view or to make complete reset to default view

Transaction Value - Filter Setting Guidelines

Please Note:

1. The Transaction Value has two sub-filters:
 - a. The first defines the condition for the total transaction value.
 - b. The second defines the expected currency of the total transaction value.
 2. The default filter currencies are USD, GBP and EUR.
 3. If other currencies are included in the transaction, these will be displayed in the filter.
 4. Edge-displayed currencies remain unchanged.
 5. Transactions in currencies other than the selected currency are converted in the background.

Important notice:

- Transaction values are aggregated
 - Once the currency filter is set the graph displayed data will vary depending on the currency selected

Date Range Filter

Enables graph to show graph data just from a particular selected date range.

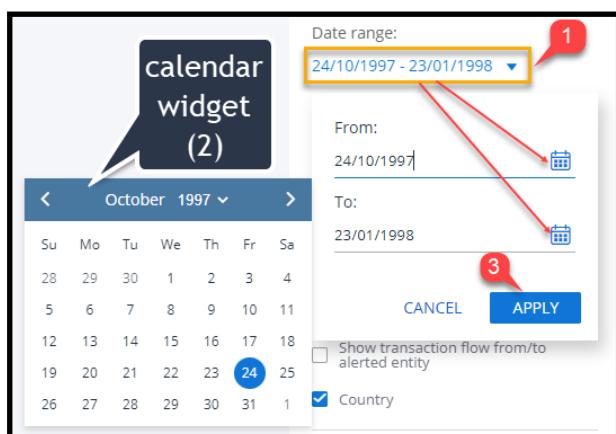


Figure 158: Select Date Range Filter

➤ To filter by date range in Network Visualization:

1. Click the Date Range dropdown menu (1).
 2. From the calendar widget (2) select the 'from' and 'to' dates.
 3. Click **APPLY** (3).

The graph data is displayed between the selected dates.

Note: Expanding the date range can impact significantly on performance, as there will be probably more entities to process.

Graph Depth

The graph depth menu has 4 levels. Each incremented level displays an increase in outlying counter entity connection activity. Its main purpose is, to enable the analyst to view the alert picture connectivity wise and increase his / her 'birds eye view' of the risk under investigation.

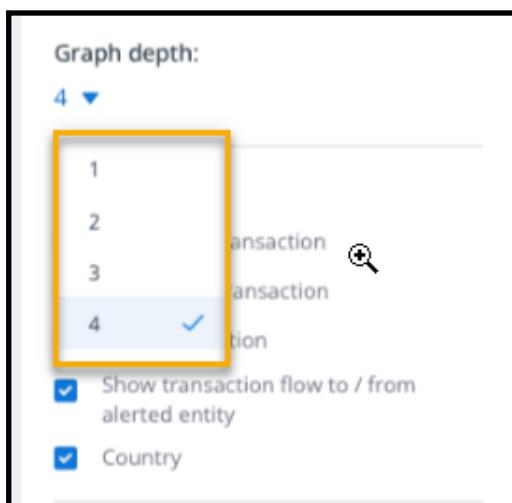


Figure 159: Graph Depth Level Menu

» To select a depth level:

1. Click the **Graph Depth** drop down menu.
2. Select new level.

When the Graph Depth is modified, the displayed graph is updated immediately

Examples of Graph Depth levels from 1 to 4 :

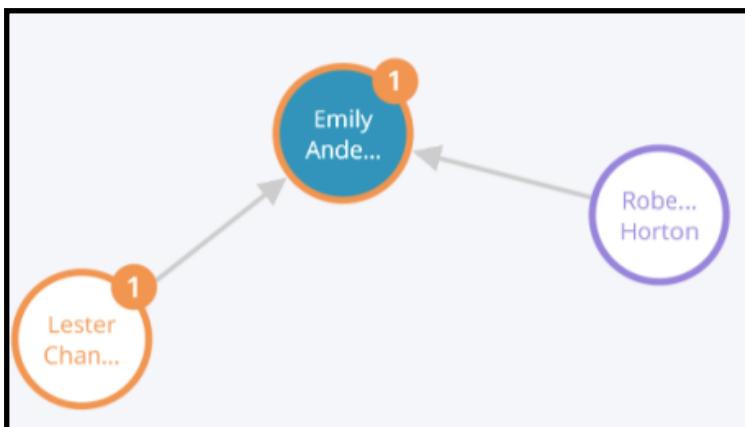


Figure 160: Example Graph Depth - Level 1

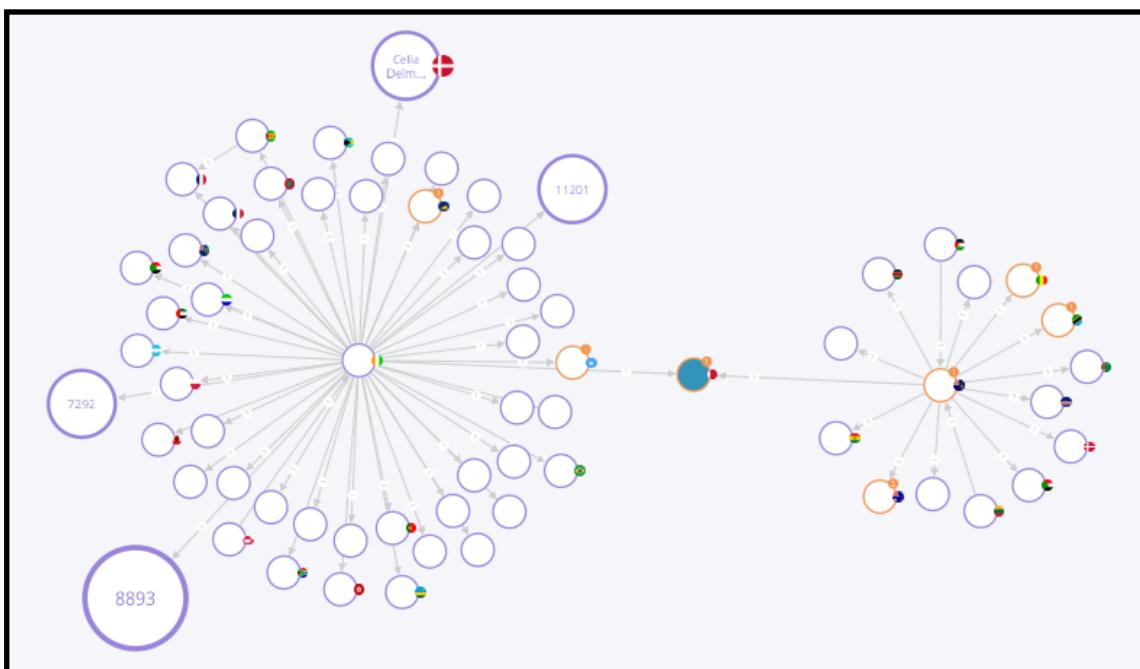


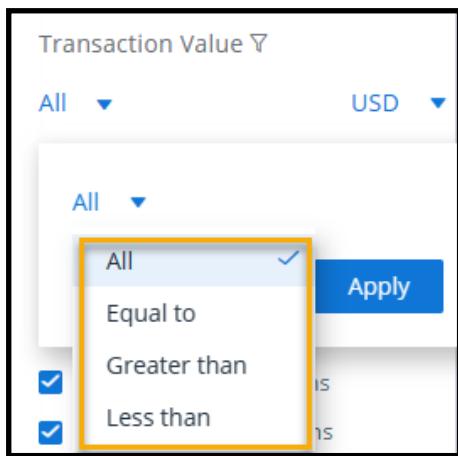
Figure 161: Example Graph Depth - Level 2

Note: When using the upper levels of the Graph Depth options and the new (extended) graph is initially a bit challenging to assimilate, you can drill down and view the new areas of the graph, by clicking on nodes of interest to select, expand and navigate around the new local network area.

Note: Be aware, depending on the size of the network, selecting level 4 may impact on graph clarity view ability.,

Value of Transaction Filter

The NV graph can be filtered by transaction value

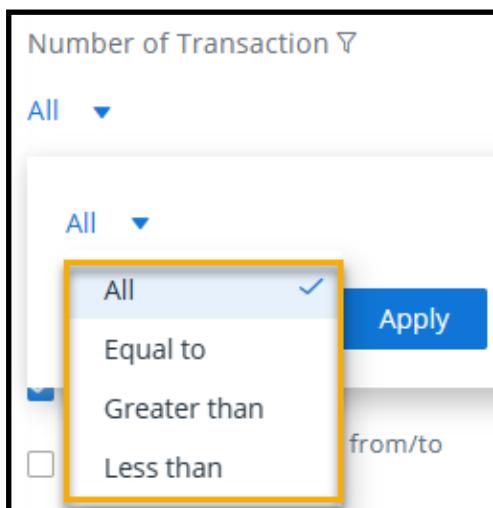


To filter the NV Graph by transaction value

1. From the number of transaction filter, click the All dropdown menu icon on the **Controls** side panel. I
2. Either select to include all values or select from available options as shown in the above image or select another option e.g over xxx under xxx , and enter a value .

Number of Transactions Filter

The NV graph can be filtered by number of transactions



To filter the NV Graph by number of transactions:

1. From the number of transaction filter, click the All dropdown menu icon on the **Controls** side panel.
2. Either select to include all number values or select from available options as shown in the above image and enter a value .

Display On /Off) Filtering by adding or removing graph elements enables the analyst (by trial and error), to 'switch off' and remove certain graph data (example: amount and number of transactions).

An example of the display on off filter block is shown below.

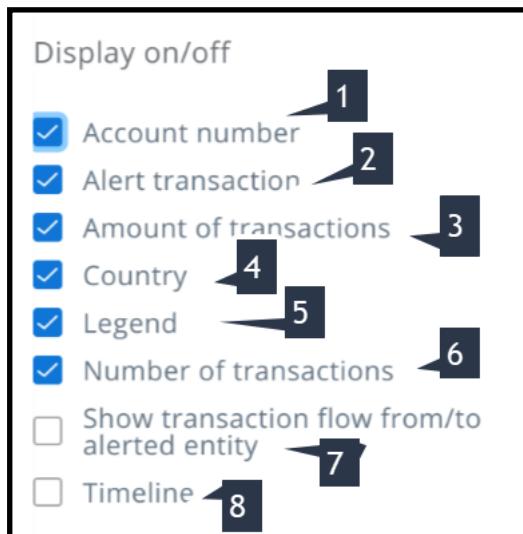


Figure 162: Example On /Off Display Filter Select

Display on /off filters in Network Visualization provide you with necessary tools to make transaction flow investigation more efficient by allowing you to focus on specific data displayed in the Network Visualization screen.

In summary, available filters enable the following main functionalities:

- Filter out some displayed data - useful when investigating crowded graphs
- Configure timeline graphs to highlight specific attributes in the display
- Configure the graph time period range
- Select a graph depth level to show more /less alert transaction connections
- Switch viewable attributes on /off
- Undo /redo viewing steps and if required reset the current view

Let's take a closer look at this extremely useful filter panel detailed below.

In some instances, data included with a high density can be excessive, and it would in most cases be beneficial to the analyst to gain a clearer picture of the underlying suspicious transactions and trends between entities by being able to simply deselect a category or categories

As per the tagged call outs on the above image:

1. When ticked, shows the Alert Id instead of Name
2. Transaction amount displayed on the graph.
3. Number of transactions.

4. Alerted transactions.
5. Show transaction flow, to and from alerted entity.
6. Country.
7. Legend switch on /off.
8. Timeline switch on /off.

Note: On access the 'Show transactions flow to /from alerted entity ' filter is not enabled.

Undo, Redo & Reset Icons

As the analyst works through the investigation process with the Network Visualization module, it is possible that several UI changes 'down the line', it maybe apparent that some latter changes have in fact made the alert visualization process worse instead of better and so instead of trying having to reset the graph display and start again, the user can simply click the undo/ icon step by step until the desired graph view is reached. Of course the redo function is also available if the user has 'stepped back' too many times.



Figure 163: Undo , Redo and Reset Tabs and Button

(Note : The current step status is indicated in the display).

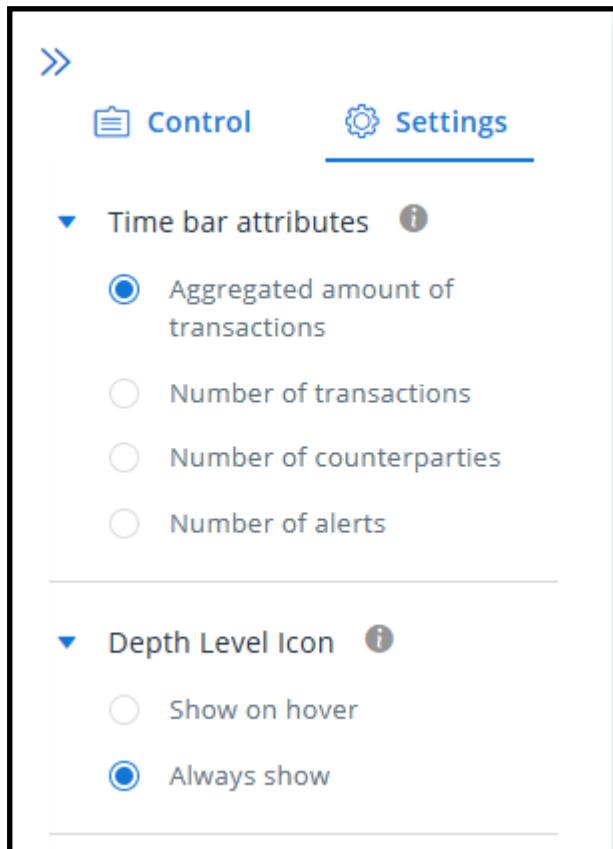
Reset View:

Facilitates returning the graph to its original depth level.

Note: The reset button does not remove any of the source data, it just resets the local graph display.

7.2.3. Settings Tab

An example of the Settings Tab is shown below.



The Settings Tab menu enables the analyst to configure the NV Time bar graph and also set the desired behavior for depth level icon

The Time bar graph is covered in more detail in the Auxiliary NV Functionality Components /Tools section of this chapter section.

7.2.3.1. Auxiliary NV Functionality Components /Tools

The available auxiliary network visualization tools provide a set of screen components and tools to aid and inform the analyst while working with the Network Visualization module.

Each auxiliary component is detailed according to purpose and use.

This includes:

- Key Legend
- Navigation Utility
- Node placement adjustment
- Nodes search utility

- Histogram graph data
- Select node to node direction Flow
- Downloading screen graph segments

Key Legend

The key legend lists and briefly describes elements and icons used throughout an alert NV graph display. The following example figure shows key legend items currently in use.

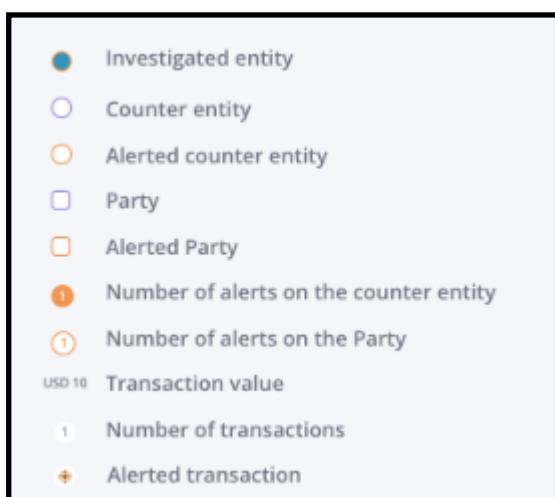


Figure 164: Network Visualization - Key Legends Display

The following table lists and describes key legends

Icon	Key Element	Description
	Investigated Entity	Investigated entity node
	Counter Entity	Counter entity node
	Alerted Counter entity	Counter entity node (alerted)
	Party	Signifies a non alerted party entity as the sender or recipient

Icon	Key Element	Description
	Alerted party	Signifies an alerted party
	Number of alerts on Counter Entity	This tag on the node indicates the number of alerts on the counter entity
\$, Euro	Transaction value	Total transaction amount displayed by currency type
[1]	Number of transactions	Total number of transactions between sender and recipient
	Alerted transaction icon	Signifies transaction is suspected as being a "contributor" to the alert

Note: To maximize the chart canvas area , when not required, you can switch the Legend display off from the filter panel.

7.2.4. Navigation Utility

The Navigation Utility is useful when managing an extensive alert graph. Its main functionality provides:

- Navigation around the graph to locate extended transaction connections
- Selecting the + icon displays functionality tool tip
- Moving the slide bar expand the detail on the screen
- Zoom in and zoom out (via the 'hand' icon toggle)



Figure 165: Screen Navigation Tool

The screen Navigation Tool enables the following functionality:

Call out Tag	Description
1	Depending on which 'compass point selected screen items will be moved (Left, right , up down)
2	Clicking this center point - resets the zoom
3	Selecting the hand icon (instead of the arrow icon) enables you to move the screen by placing it anywhere on the screen and dragging the screen in any direction.
4	Zoom slide, either by moving the slide bar up /down to zoom in or out

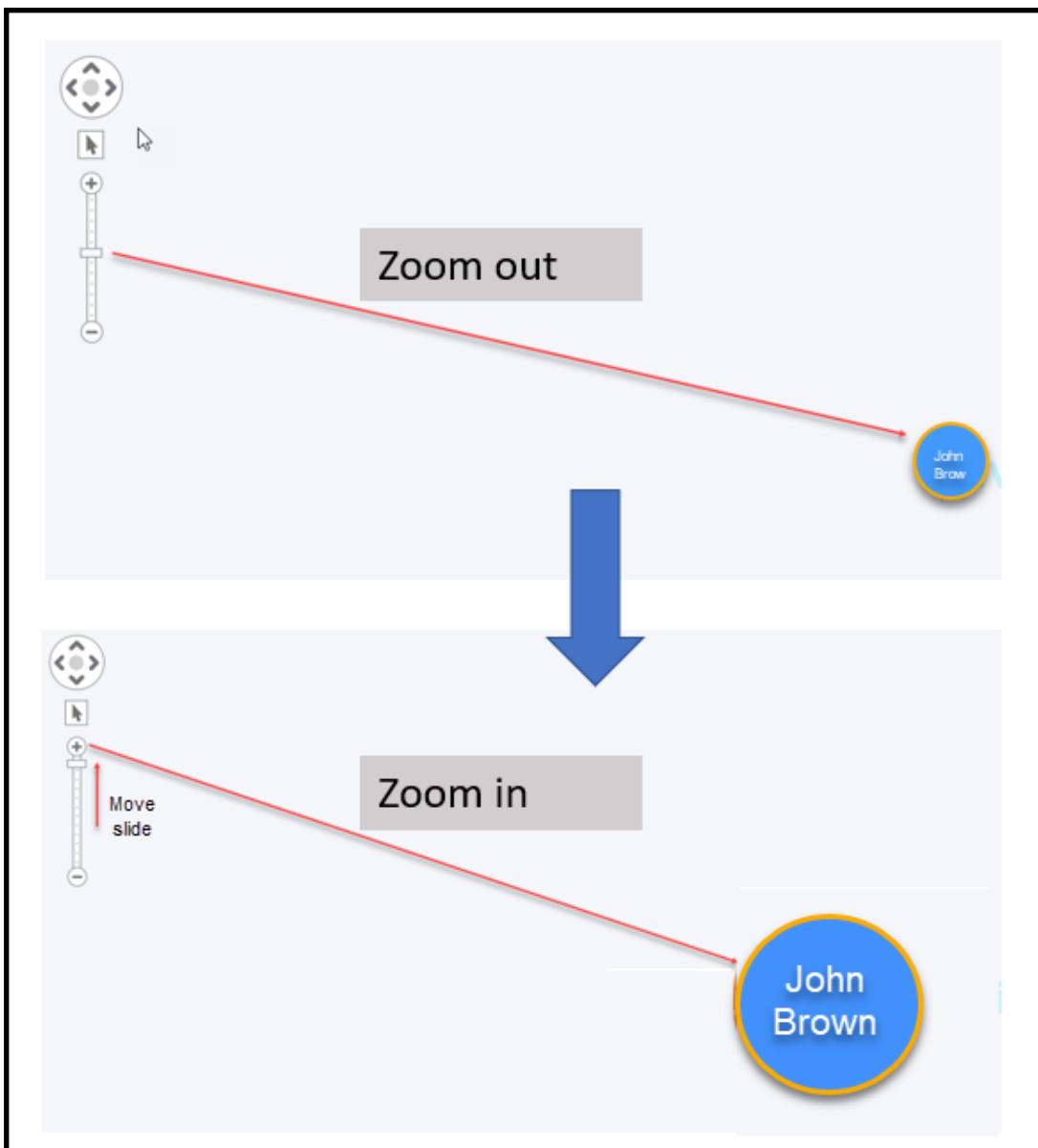


Figure 166: Example of Using the Zoom Slide to Pan out, and Zoom in to Focus on the Item of Interest

7.2.5. Node Placement

7.2.5.1. Drag and Move Nodes Around Screen

If required in high density graphs you can drag and move nodes to a different location ('rubber banding') to help isolate and focus on a particular node and its data.

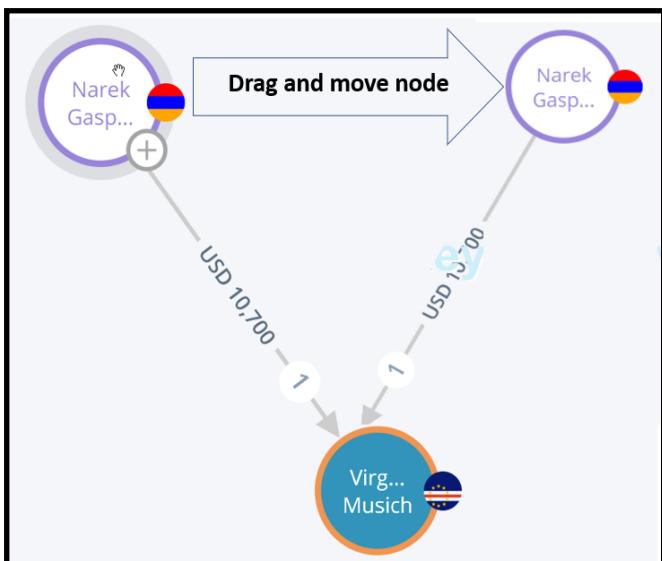


Figure 167: You can Drag and Move Nodes to help Isolate in High Density Graphs

Note: It is also possible to move multiple nodes simultaneously:

» To move multiple nodes:

1. Ctrl click each node entity to select and highlight it.
2. Simply drag one of the selected nodes, to simultaneously move all selected nodes.

7.2.6. Node Search

Alerts that are data intensive and contain many graph node entities, can in some instances cause the analyst to waste valuable time trying to locate a specific entity. To mitigate such scenarios, a node search facility is available.

7.2.6.1. Searching for Graph Nodes

Graph node entities can be searched for by name or Id. The search field shown in the following image is located at the upper edge of the displayed NV graph.

Search by name or Id of the node requires entering target values and pressing either **Enter** or search icon (magnifying glass)

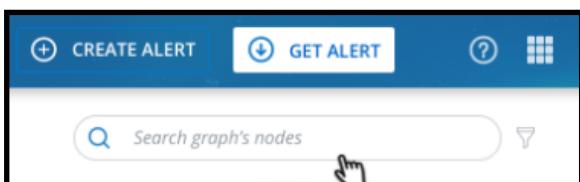


Figure 168: Graph Nodes - Search Field

» To search the alert graph for a specific node:

1. Searching by name or Id requires entering a minimum of 3 chars.

The following image shows a search by name example.

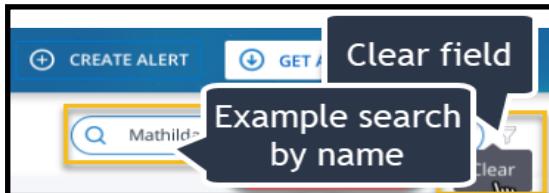


Figure 169: Example Search by Name Entry

Auto complete displays possible matches.

2. Select the best match from the dropdown list.
3. To initialize graph search, either click **Enter** or click the **Magnifying Glass Icon**.

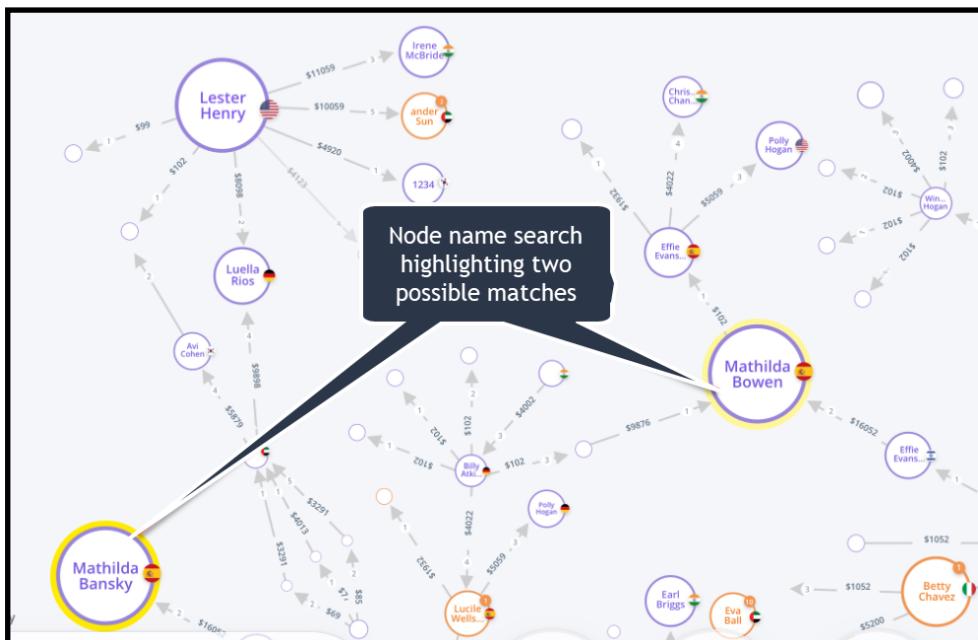


Figure 170: Example Search Results where two Possible Candidates were Located

Time Bar Graph

The purpose of the Time bar graph is to show the key characteristics and trends of the alert under investigation, over an adjustable time period, as a histogram.

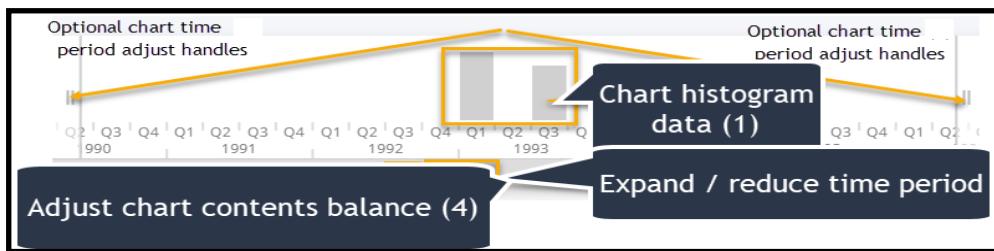


Figure 171: Example - Time Bar Graph

Additional data shown in the Time bar includes::

- Aggregated amount of transactions in the following currencies:
 - USD
 - Euro
 - GBP
- Number of transactions
- Number of counter entities (both Party and Individual accounts)
- Number of alerts

Also the time bar graph can show account alert details either:

- Just when the user hovers over the graph, or
- Always

Timebar Feature - General Information

1. configure and adjust a timeline chart, to display selectable attributes under the main Network Visualization graph.
 - a. First ensure the Control menu is selected .
 - b. Click the *Timeline* check box in the Display on off section to enable the *Timeline* display

The following information will better help you understand the Timeline feature functionality:

- a. Timeline displays are reset when a new filter is selected.
- b. When viewing the displayed entities, adjusting the time period. catchment area outside any of the histogram bars, removes the entity from the viewable main chart.
- c. To move the chart catchment area handles:
 - i. Hover over the handle until the double headed arrow appears.
 - ii. Drag the handle to increase or reduce the time period.

- d. If attribute set, hovering over any of the displayed chart bars displays the value of the selected attribute for that time instance.
 - e. Default currency is displayed as USD - (To change currency value, select from the Timebar attributes.

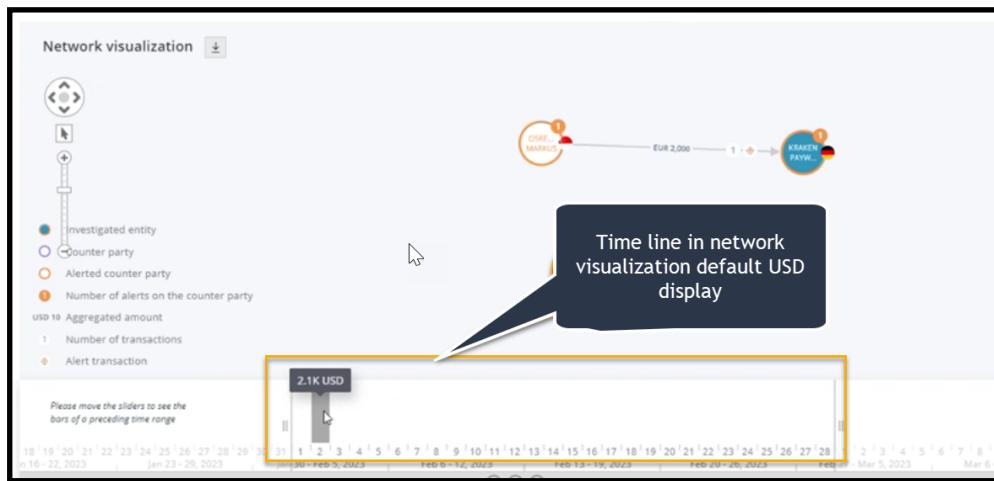


Figure 172: Example Timeline Charts Showing Default Currency as USD

Node Transaction Direction Flow Select

The node direction facility enables the analyst to select whether to view incoming, outgoing or both transaction flows.

The following figure shows an example of selecting the direction flow dropdown menu from the bi directional icon.



Figure 173: Example Transaction Direction Menu Select

7.2.6.2. Downloading screen graph segments

[Download Current / Whole Chart View](#)

To assist you in the investigation process and help you collaborate with fellow analysts, supervisors and other team members, you can download screen shots of current visualization screen views.

The download select icon is located to the left of the upper edge of the graph screen.

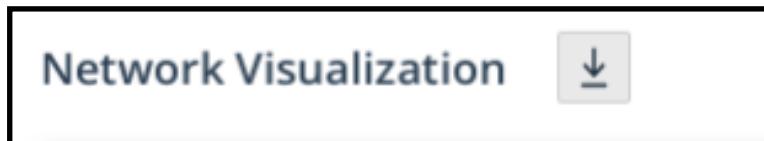


Figure 174: Download Network Visualization Graph Segment or Entire) Graph

» **To download either the current or whole chart view:**

1. Click the download icon (highlighted in the 'Landing Screen' image (7)).
2. Select from the list of download formats as shown below.
3. Select Current or Whole chart view.
4. Click the Download button to download the image file to your local computer.

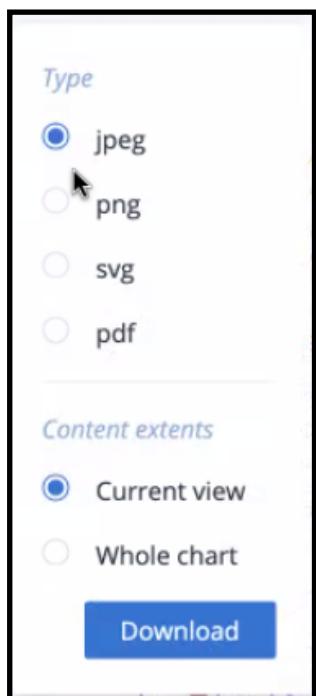


Figure 175: Download Format Options and Content Extent

Note: The downloaded file does not include the legend.

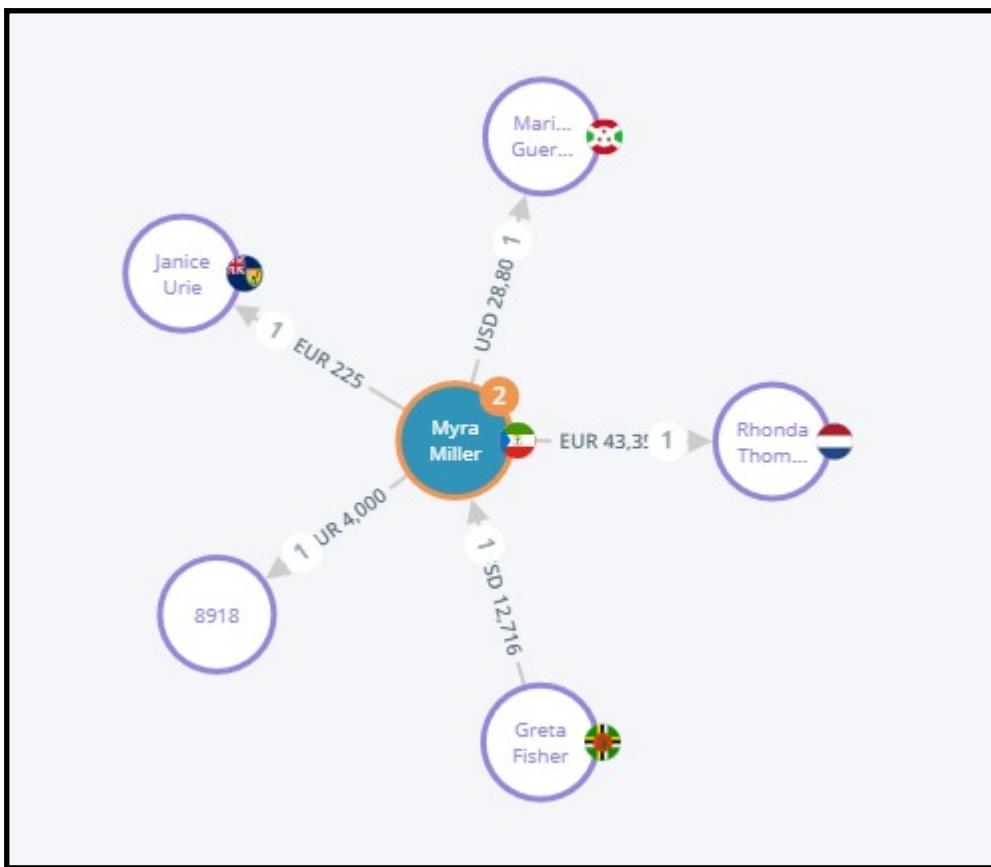


Figure 176: Example of Downloaded jpeg image

7.3. Working with Network Visualization

In the previous chapters we have reviewed the need, purpose and functional layout of the Network Visualization module.

Now let's explore the generic workflow process.

7.3.1. Investigation Strategy with Network Visualization

As will be seen as you begin to develop your Network Visualizations skills, the methodology used to explore the transactions graph differs fundamentally from that used in tabular data investigation.

The methodology in exploring Network Visualization requires you to leverage graph depth expansion (covered in the following chapter on filters), to incrementally reveal more of the transactions network, and the use of the 'click' gesture to localize and expand different areas of the graph to reveal insightful information about the alert under investigation.

7.3.2. Visualization Network - Practical Workflow Suggestions - (High level)

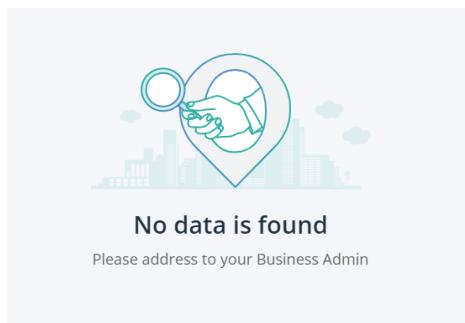
1. In Investigation Center, select the alert to investigate:
 - a. In the Alert details tab examine the transactions table and evidence graphs for initial support activity.
 - b. Check and note details of any related entities activity.
2. From the Alert Details tab:
 - a. Click the Network icon.
 - b. View the Network Visualization landing page with the default settings.
 - c. Locate the Investigated entity node.
 - d. If you know approximately the period of time when the suspicious activity occurred, as a best practice set the time range filter for 4 weeks previous to the occurred on date (to make sure the graph will contain sufficient historical data).
 - e. With initial evidence from Alert Details Tab, make a preliminary investigation of the transactions to and from the investigated entity to try and substantiate the evidence collected from the Alerts Tab.
 - f. Try displaying the alert Id to provide more information.
3. If the transaction trail does not yet reveal any insightful conclusive evidence:
 - a. Try expanding the time period range to see if richer historical data reveals any new evidence.
 - b. Open the Graph depth menu and select level 2.
 - c. Continue to trace the transaction trail on the expanded graph.
 - d. If the graph on the second level is overly dense with data , try filtering out excessive data.
 - e. If necessary, select graph level 3 and repeat the previous investigation strategy.
 - f. If entities have a + icon tag on the border - click it to reveal further related transactions:
 - i. If the newly revealed transaction also has a + icon tag continue to follow this process as far as there is available data.

7.4. Troubleshooting

This chapter includes information on error messages that may be displayed during investigation sessions using the module.

Issue #1

On access a 'No data is found' message is displayed:

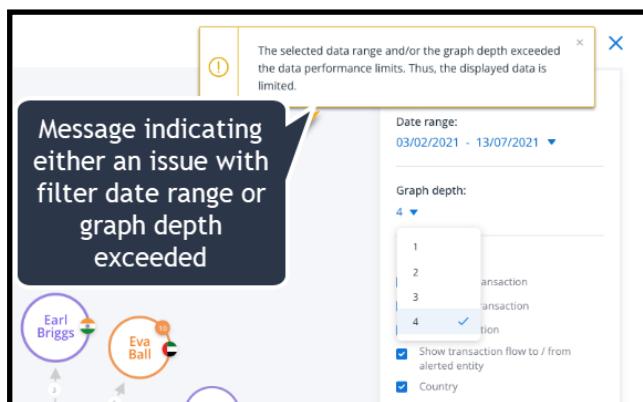


Solution: This may occur with a new system deployment or a temporary technical issue.

To resolve, contact Customer Success or Business Admin.

Issue #2

The following information message may be displayed when using the network visualizations module:



As detailed in the displayed message this can occur when:

1. The selected date range exceeded data performance limits.
or,
2. The selected graph depth level exceeded the amount of graph transactional data available.

Solution:

- In the case of (1) , reselect another date range.
- In the case of (2) , try selecting a lower level of 'graph depth'.

8. Rules Editor - Introduction

Note: If this module is not available as part of your IC deployment, and attempts to access it result in an error message, this may be due to a licensing issue.

This chapter describes in detail the workflow processes to:

- Edit rules parameters
- Test their effectiveness
- Once tested and optimized, apply the modified values to future analyses

Note: In order that the Rules Parameter Editor will function, please note that the contents of the configuration .yaml file detailed in the Decisioning chapter of the Platform User Guide needs to be updated. For more information , refer to the current Platform User Guide.

8.1. Rules Editor Workflow - High Level

Before we deep dive into working with the rules parameter editor, let's take a high level look at the overall process. This will help us get an initial understanding of the workflow process, end to end.

The following high level block diagram shows the three main interconnected stages, and includes the key elements of each stage.

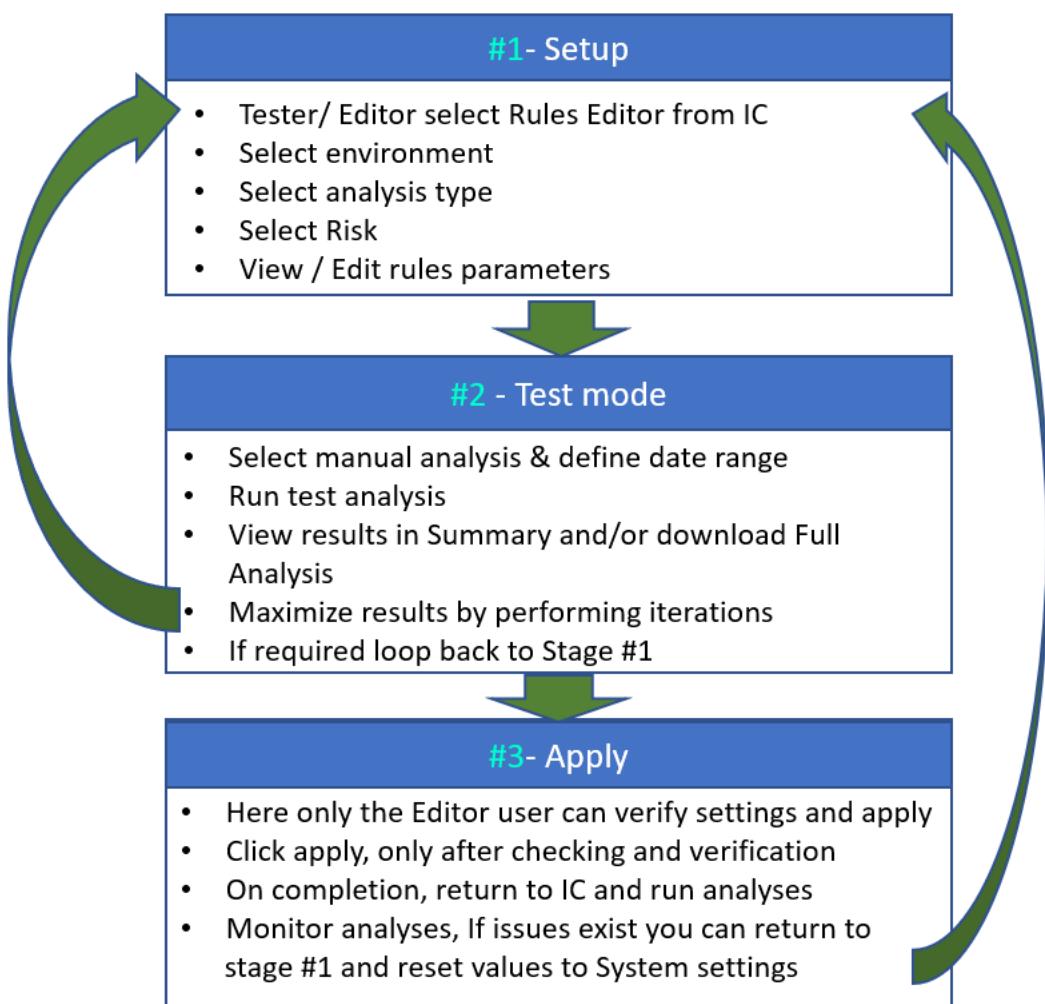


Figure 177: Rules Editor Workflow - High Level

Stage #1-Setup In this stage, you as the user, with either 'Tester' or 'Editor' role can access the Rules Parameter editor from the investigation Center. As shown in the block diagram, the key steps here include, selecting and setting up data related elements including required environment, analysis type, risk, rules and current parameter values.

Once rules and values are displayed, you can then proceed to edit the parameter values in preparation for the next stage - Test Mode.

Stage #2 Test Mode. In this stage, before running simulated analysis tests you are initially required to select a date range. Now you can run an analysis simulation based on these settings and parameters. This step can be repeated for as many iterations as required to maximize results and if required you can also return to Stage #1 for further setup . A key point to bear in mind at this stage is that these simulated analysis results are exactly that - simulations. The original parameter values are not changed until you move to the final stage - Apply.

Stage #3 Apply In this final stage, once edited value parameters have been tested and optimized, the final step before applying changes is to check all user analyses configurations

Important Note: It is recommended as a best practice to check all modified analysis rules carefully. Be aware, that when you click apply all modified settings made to any analysis (even provisionally or in a test scenario), will be applied to settings.

Once applied, new parameter values will be implemented when the next new data batch is ingressed.

Now, you have a general overview of how the editor works, we can in the next chapter explore working with the Rules Parameter Editor in detail.

8.2. Icons Used in the Manual

The icons listed and summarized in the following table, are used in the document as an aid in highlighting specific types of information.

Icon	Description
	Good to know
	Best practice suggestion
	Information

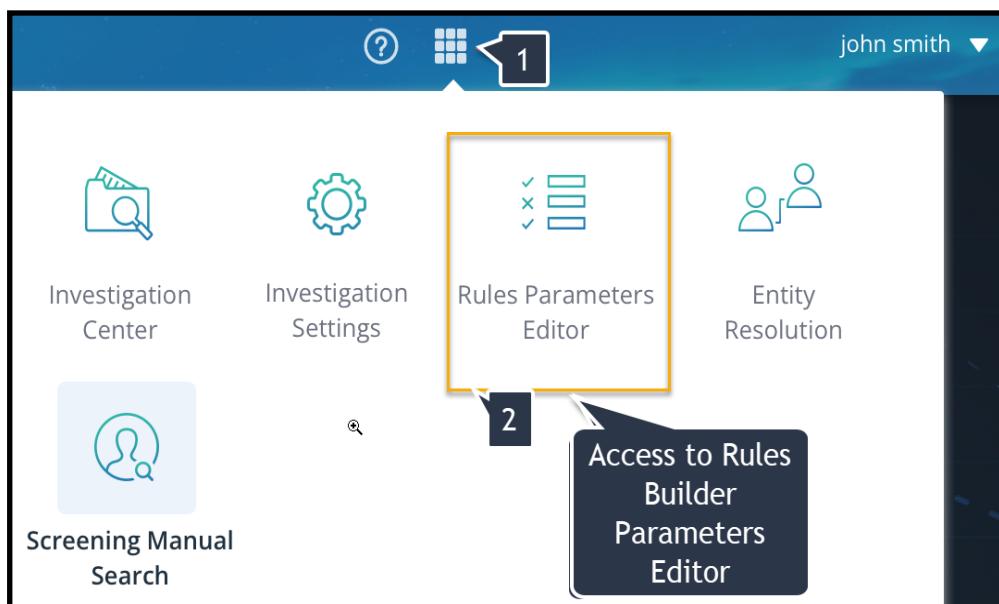
8.3. Editor Access and Initial Orientation

This chapter, includes:

- Accessing the Editor
- Overview of Landing Screen
- Overview Rules View

8.3.1. Access

At login, the user with either Rules-Editor or Rules-Tester role permissions is presented with the following access link, as shown below.



» To access Rules Parameter Editor:

1. Click the matrix icon (1).
2. Select the Editor option (2).

8.3.2. Rules Editor - Landing Page - Overview

Welcome to the Rules Editor. On access, the landing page is displayed as shown in the example image below.

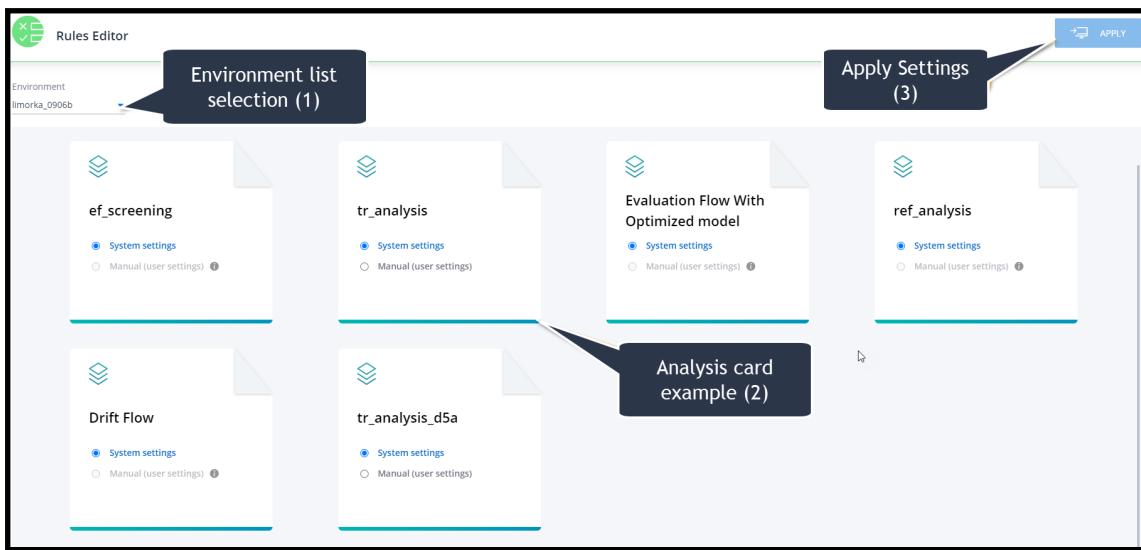


Figure 178: Rules Edit Landing Page Showing Main Features -High Level

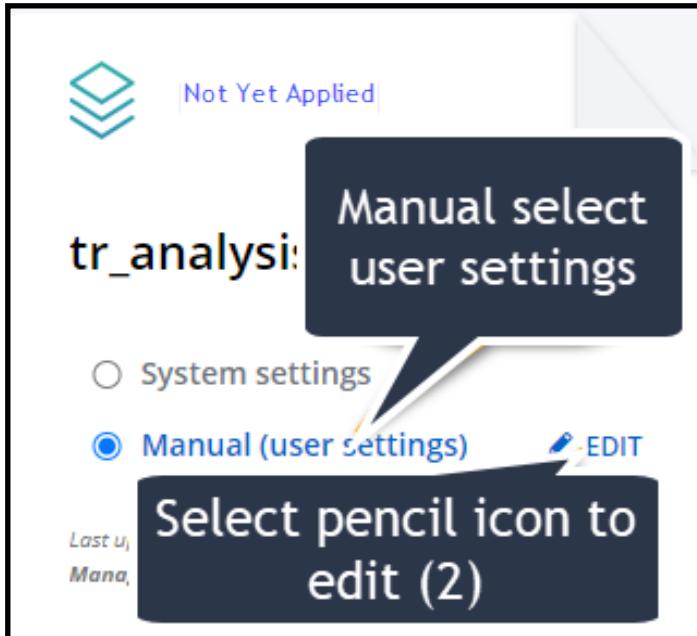
1. With reference to the above image:

- As highlighted in tagged item (1), if your deployment includes more than one environment, you can select alternative environments here.
- All current available analyses are displayed on cards similar to that highlighted in tagged item (2)
- Selecting the system settings radio button (3) mode will use current applied rule parameter values in any test analysis
- Selecting the manual user settings radio button (4) will (If configured and saved) use these parameters values in test analysis
- The Apply button, as highlighted in tagged item (5), is used to update parameters rules values as follows:
 - If the analysis card radio button is set to **System**, then user settings for this analysis will be set to system settings
 - If the analysis card radio button is set to **Manual**, every manual changes made in the edit session and saved, will overwrite previous settings

8.3.2.1. Rules View

 The Rule view screen is where the main editing and analysis evaluation work is done.

1. from the available analyses displayed, select the analysis that contains the rule you wish to evaluate parameter changes and click the EDIT link.



The 'View rule' edit page is displayed as shown in the following example:

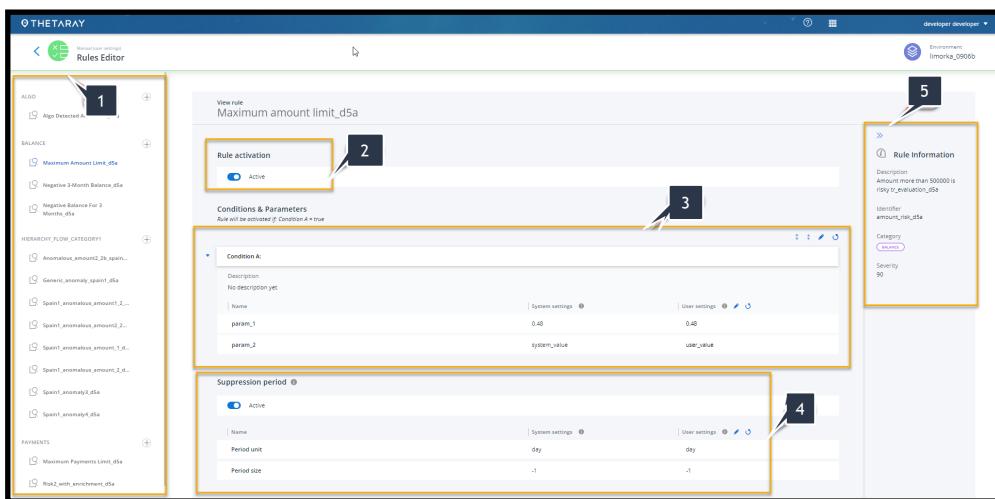


Figure 179: Example View Rule Selected Screen Showing Main Display /Configuration Components

Note: All screens in the Rules Parameter editor are displayed in full web page mode to enable access to related screens

View rule screen

With reference to the above example figure, let's take a look at the '*View rule*' screen, and the part it plays in our Rules Parameters editor.

- The current set rules for this analysis (sorted by category) are listed in the left side panel (1). From this list we select the rule to be edited.
- To the right of this side panel is the rule activation switch (2) , which enables the rule to be active or inactive in the analysis process.
- Below this activate switch, is the parameter value configuration section (3), that contains the rule condition(s) defined logically, and the available rule parameters (that can be modified).
- Under the parameter edit section is the *Suppression period* configuration section.
Rule suppression enables an analysis rule to be made inactive for configurable time periods.

Available configuration settings

- **Inactive:** The rule is not suppressed.
- **Active:** The rule is suppressed according the following settings
 - Period Unit options: Day , Week, Month , default - day
 - Period size options 1 - (any positive integer)
- To the right of the screen is the Rule Information side panel (5) , that contains rule information such as description , identifier, rule category and severity setting.

8.3.2.2. Key takeaway at this stage:

 During the rules value modification and evaluation process, there are **no** changes made to the current values.

In the following chapter, we will deep dive into the process of editing and evaluating changes and results.

8.4. Editing Rules Parameter Values

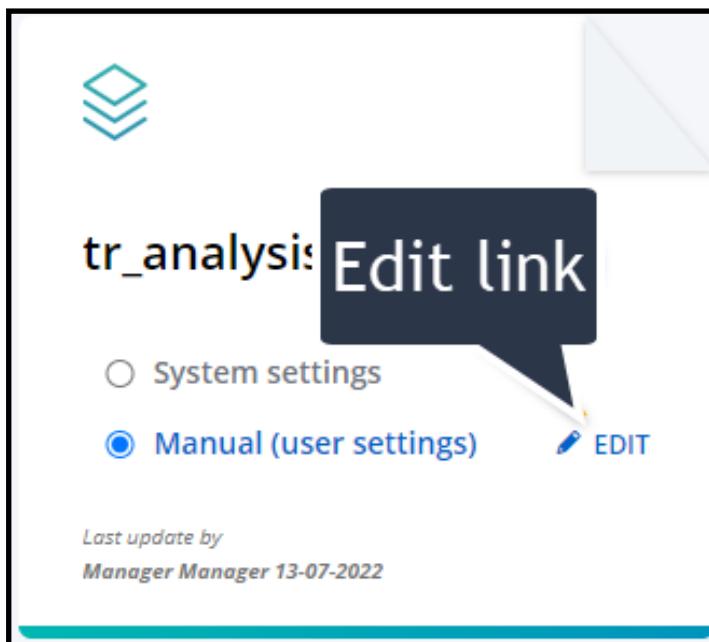
In this chapter, we will take a closer look at the core tasks related to the rules parameter editor by walking through each of the following steps:

- Choosing an example analysis
- Selecting a rule

- Activating / deactivating the rule
- Setting a suppression period
- Editing parameter values
- Rule edit status indication
- Running an evaluation with new parameter values and viewing summary results
- Downloading the results to a CSV file and examining results
- Running different iterations based on different values and comparing results
- Applying new values to overwrite existing values
- Resetting values to the previously set values

8.4.0.1. Step #1 - Choosing an analysis

To start our parameter edit exercise, first we need to select an example analysis from the landing page.



1. click the EDIT link.

The 'View rule' edit page for our selected example analysis is displayed:

8.4.0.2. Selecting a rule

Selecting a rule to edit is simple. Clicking on any listed rule in the *rules side panel* displays the rule for edit.

For the purpose of continuing our deep dive exercise, select the *Negative Balance for 3 months Limit*, rule as displayed below.

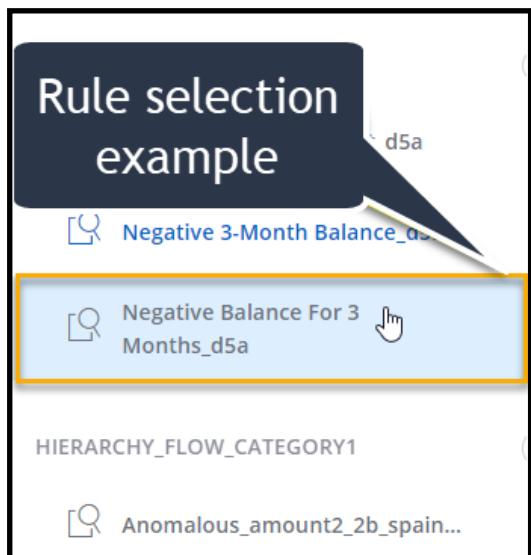


Figure 180: Example Selecting Rule to Edit

The selected Rule is displayed for edit as follows:

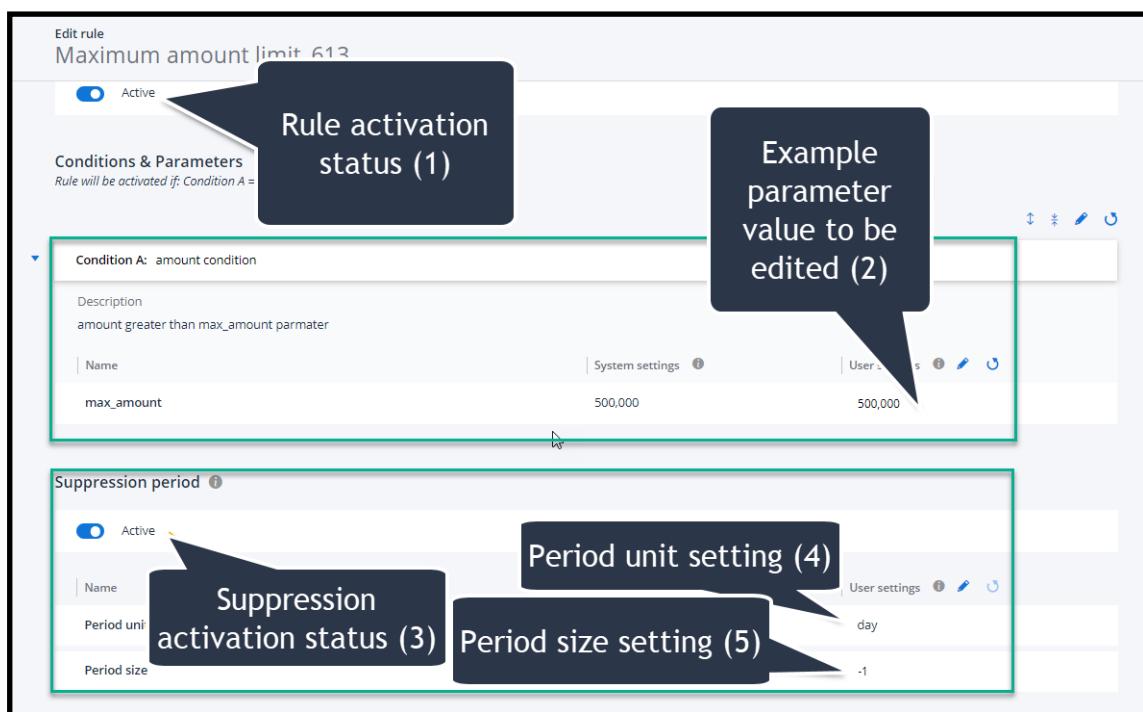


Figure 181: Rule Edit Tasks - Including selecting Activity Status editing Parameters and setting Suppression

8.4.0.3. Activate / deactivate rule

With regard to our example exercise , we can see from the above figure and working top - down, that our fist logical task is whether or not to make our rule

active or inactive (1).

Although either configuration will still allow us to edit the rule parameters, we will in this instance leave the rule in the active state.

8.4.0.4. Editing parameter values

As understood, the process of editing parameter values is to improve on current analysis results.

Edit process:

The edit value process is super simple:

1. Select edit pencil.
2. Modify value.
3. Save.

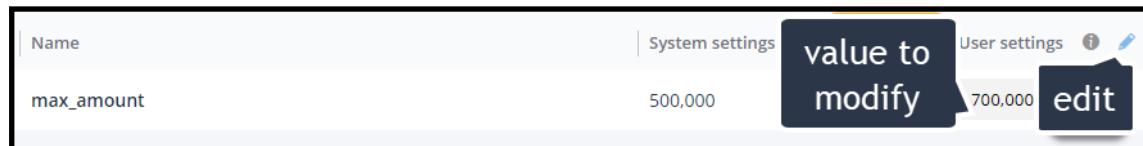


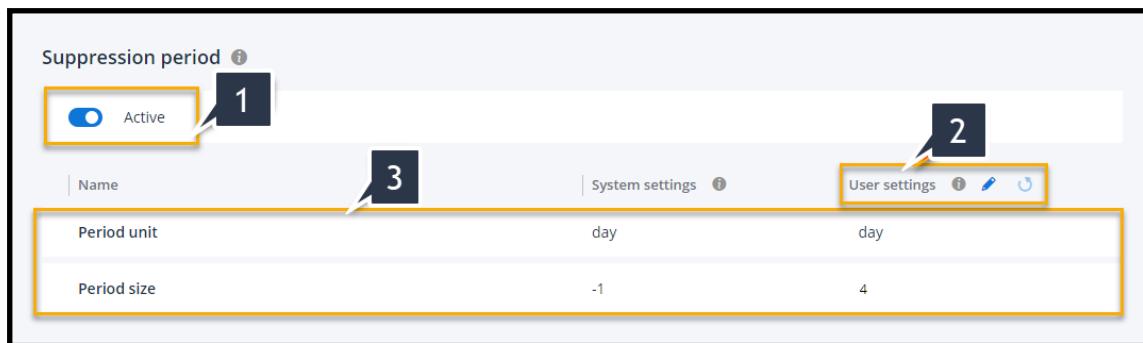
Figure 182: Example Edit Rules Parameter

8.4.0.5. Suppression Period

The suppression period feature enables certain rules to be excluded from analyses for varying time units /periods .

This feature of the Rules Parameter editor is especially useful in managing seasonal transactional spikes in activity. If suppression was not available and activated, the extra transactional 'noise' introduced by the spike would increase demand on resources.

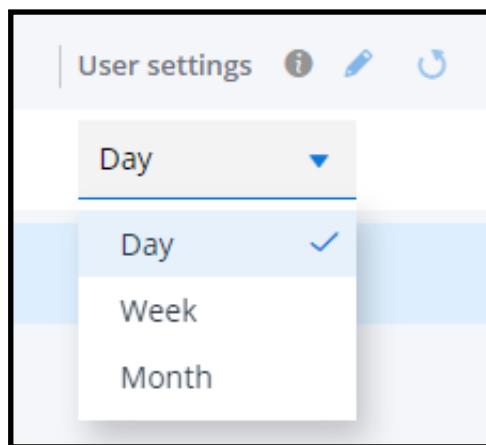
- Referring to the figure below, the activate switch (1) enables rules suppression for the configured time period.
- Editing rules suppression settings is activated by selecting the 'Edit' pencil highlighted in tag (2).
- The list (3)below displays the current set time unit and time period for both system and user settings .



8.4.0.6. Configuring Suppression

» To configure rules suppression for a particular rule:

1. With the rule selected:
 - a. Click the 'Edit' pencil.



- b. Select the unit period from the drop down menu option.
- c. Configure the time period.
- d. Click Save.

8.4.1. Analysis Status indication

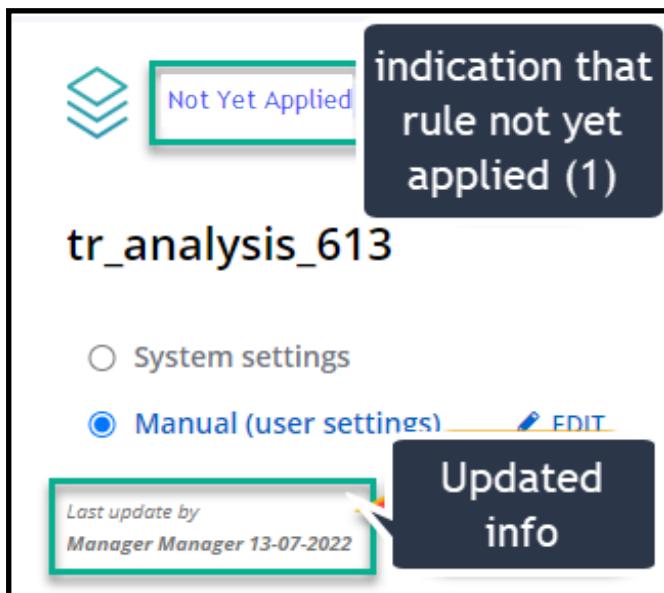
During the edit process the analysis card relating to the particular rules parameter is updated as follows:

- If the rule has or has not yet been applied
- If the rule parameters have been updated , indication is displayed, by whom and when

The following example of a rules analysis card shows:

- The rule has not yet been applied (1).

- The analysis setting were updated by the manager user on the indicated date (2).

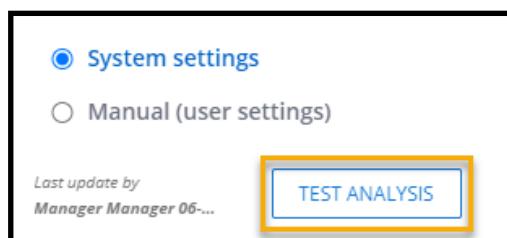


Note: Any modifications done by edit or changing the radio button from system to edit or vice versa, will also be included in the 'Last update by' note, highlighted above.

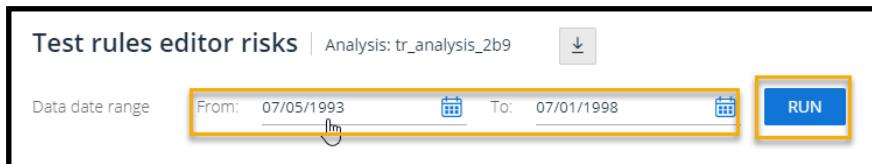
8.4.2. Testing Evaluation Analyses on System and User Set Values

Analyses can be run on both system and user configured values. One prime reason for running an analysis on system settings is to create a baseline for comparison. Whether running a system or user based analysis the process is the same:

1. Choose the radio button for the analysis type
2. Click the Run TEST ANALYSIS button

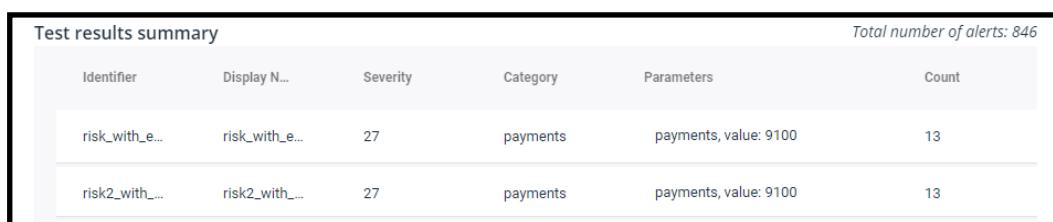


3. From the Test screen view set the time range and click the RUN button.



The screenshot shows a 'Test rules editor risks' interface. At the top, it says 'Analysis: tr_analysis_2b9'. Below that is a 'Data date range' section with 'From: 07/05/1993' and 'To: 07/01/1998'. A blue 'RUN' button is highlighted with a yellow border. The 'RUN' button is located at the bottom right of the date range section.

4. When the analysis has completed a Test Results Summary view table is displayed



Test results summary					Total number of alerts: 846
Identifier	Display N...	Severity	Category	Parameters	Count
risk_with_e...	risk_with_e...	27	payments	payments, value: 9100	13
risk2_with_...	risk2_with_...	27	payments	payments, value: 9100	13

Summary Results - The summary view table contains basic information about the analysis. This information will enable you to assess if the changes made to parameter values has improved results or not. You can then make further adjustments to user values and over a number further iterations, maximize results.

As a best practice, you should compare the summary results of further analysis runs with results returned for the default system values **for the same time period** so as compare results under the same test conditions.

Additionally, be aware that you can manipulate the table column data in a similar manner as with data tables investigations in the thetaray application (AG grid compliant) - for example, sorting column order alphabetically and numerically and also by pivoting column data.

If more of a deep dive into results analysis is required, you can download full results. as explained in the following section.

8.4.3. Download Full Results

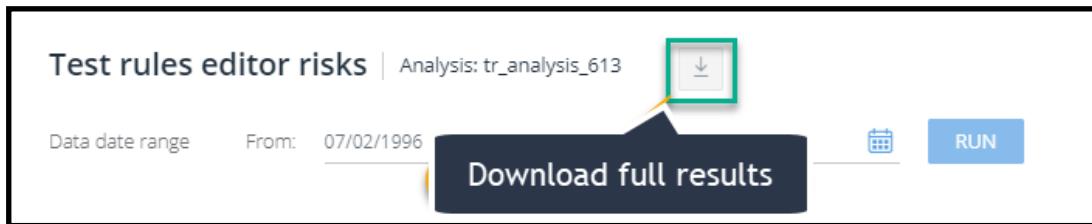
To investigate more information from the Test Analysis, you can download .CSV full results (risks) reports.

The full results download, is a zip file containing two separate files detailing:

- Metadata file - It depicts the analysis rules and their parameters that run under the test as a reference for the user
- Media file - It provides the results of the analysis test, which includes the risk and associated data

➤ **To download Full results (risks) report:**

1. Click the download icon as highlighted in the figure below.



The downloaded zip file has the following example structure:

tr-analysis_2b9-7_5_1993-7_1_1998.zip

An example of the two unzipped .csv files is as follows:



Both files reveal varying information about the evaluation run.

8.4.3.1. Metadata file

The metadata file contains key risk elements of the analysis.

Let's take a closer look at an example metadata .csv file and what it contains.

Following is the list and brief explanation of the metadata column headers from the download file and also an example file:

- **risk_id:** identity of the risk (alert)
- **risk_display_name:** risk display name
- **risk_description:** a short description of risk
- **risk_severity:** the level of severity (denoted numerically)
- **risk_category:** the category of risk
- **parameters_json:** json file details all the parameters and their values
- **Suppression_period_unit:** Suppression period unit (e.g. - day, week, etc)
- **Suppression_period_size:** Suppression period size (e.g.: any positive integer)

A	B	C	D	E	F	G	
risk_id	risk_display_name	risk_description	risk_severity	risk_category	parameters_json	suppression_period_unit	suppression
risk2_with_enrichment_2b9	risk2_with_enrichment_2b9	risk2_with_enrichment_2b9	27 payments	{'payments':9100}	DAY		
risk_with_enrichment_2b9	risk_with_enrichment_2b9	anomaly tr analysis_2b9	27 payments	{'payments':9100}	Inactive		
payments_risk_2b9	Maximum payments limit_2b9	More then 9000 payments are not allowed for loan tr_6	60 payments	{'max_payments':9000}	Inactive		
algo_risk_2b9	Algo detected anomalies_2b9	The significant presence of Tax Heaven Jurisdictions in	90 algo	{'fusion_threshold': 0.6}	DAY		
3_month_risk_2b9	Negative balance for 3 months_2b9	Negative balance for 3 months tr_analysis_2b9	55 balance	{'zero_param1':0,'zero_param2':0,'zero_min3':0}	Inactive		
min3_risk_2b9	Negative 3-month balance_2b9	Negative 3-month balance tr_analysis_2b9	90 balance	{'max_amount':600000}	WEEK		
amount_risk_2b9	Maximum amount limit_2b9	Amount more than 500000 is risky tr_evaluation_2b9	90 balance	{'max_amount':600000}	DAY		
spain1_anomalous_amount2_2a_2b9	spain1_anomalous_amount2_2a_2b9	Spain Anomalous Amount2 2a tr_analysis_2b9	27 hierarchy_flow_category1	{'payments': 2:9100}	Inactive		
anomalous_amount2_2b_spain1_2b9	anomalous_amount2_2b_spain1_2b9	Spain Anomalous Amount2 2b tr_analysis_2b9	27 hierarchy_flow_category1	{'payments': 2:9100}	Inactive		
spain1_anomalous_amount1_2_2b9	spain1_anomalous_amount1_2_2b9	Spain Anomalous Amount1 2 tr_analysis_2b9	27 hierarchy_flow_category1	{'payments': 2:9100}	Inactive		
spain1_anomalous_amount_1_2b9	spain1_anomalous_amount_1_2b9	Spain Anomalous Amount1 tr_analysis_2b9	27 hierarchy_flow_category1	{'payments': 1:9100}	Inactive		
spain1_anomaly4_2b9	spain1_anomaly4_2b9	Spain anomaly tr_analysis_2b9	27 hierarchy_flow_category1	{'payments':9100}	Inactive		
spain1_anomalous_amount_2_2b9	spain1_anomalous_amount_2_2b9	Spain Anomalous Amount 2 tr_analysis_2b9	27 hierarchy_flow_category1	{'payments_1':9100}	Inactive		
generic_anomaly_spain1_2b9	generic_anomaly_spain1_2b9	Find generic anomalies in Spain Category tr_analysis_2	95 hierarchy_flow_category1	{'fusion_threshold1': 0.1,'min_balance':1}	Inactive		

Figure 183: Example of a Downloaded .csv file - Metadata

8.4.3.2. Media file

The media file contains analysis information about the evaluation.

Let's take a closer look at an example media .csv file and a brief summary of what such a file contains.

- **is_suppressed:** Whether the rule/ risk is subject to suppression or not
- **primary keys:** Identity of the customer entity under investigation
- **occurred_on:** Date on which the risk transaction occurred
- **risk_id:** risk_display_name,risk_severity,risk_category,
- **score:** Score element derived from evaluation algorithm process
- **pattern:** Risk identified and grouped by common characteristics
- **algo information:** (field_value,field_rating,field_rank)(*)

The data contained in the rows indicate the risks that are generated following the analysis, in the set date range

Some key additional elements that are included in the media file that differ from the metadata file as listed below.

Following is an example of a .csv media file. Please note that in this example, the 'primary keys' column (detailed above) is represented by '*account id*'. Be aware that this representation is for example purposes only, the primary key title shown is dynamic and therefore dependent on the actual media content.

8.4.3.3.

A	B	C	D	E	F	G	H	I	J
is_suppressed	account_id	occurred_on	risk_id	risk_display_name	risk_severity	risk_category	score	pattern	account
FALSE	9188	7/28/1993 0:00	generic_anomaly_spain1_2b9	generic_anomaly_spain1_2b9	95	hierarchy_flow_category1	0.6283	min1#min6#min2	
FALSE	9188	7/28/1993 0:00	spain1_anomaly4_2b9	spain1_anomaly4_2b9	27	hierarchy_flow_category1	0.6283	min1#min6#min2	
FALSE	9188	7/28/1993 0:00	algo_risk_2b9	Algo detected anomalies_2b9	90	algo	0.6283	min1#min6#min2	
FALSE	1787	7/5/1993 0:00	generic_anomaly_spain1_2b9	generic_anomaly_spain1_2b9	95	hierarchy_flow_category1	0.7804	min1#payments#mean5	
FALSE	1787	7/5/1993 0:00	spain1_anomaly4_2b9	spain1_anomaly4_2b9	27	hierarchy_flow_category1	0.7804	min1#payments#mean5	
FALSE	1787	7/5/1993 0:00	algo_risk_2b9	Algo detected anomalies_2b9	90	algo	0.7804	min1#payments#mean5	
FALSE	1801	7/11/1993 0:00	generic_anomaly_spain1_2b9	generic_anomaly_spain1_2b9	95	hierarchy_flow_category1	0.772	min1#max5#min5	
FALSE	1801	7/11/1993 0:00	spain1_anomaly4_2b9	spain1_anomaly4_2b9	27	hierarchy_flow_category1	0.772	min1#max5#min5	
FALSE	1801	7/11/1993 0:00	algo_risk_2b9	Algo detected anomalies_2b9	90	algo	0.772	min1#max5#min5	
FALSE	1843	8/3/1993 0:00	generic_anomaly_spain1_2b9	generic_anomaly_spain1_2b9	95	hierarchy_flow_category1	0.5169	min1#has_card#min5	
FALSE	1843	8/3/1993 0:00	spain1_anomaly4_2b9	spain1_anomaly4_2b9	27	hierarchy_flow_category1	0.5169	min1#has_card#min5	
FALSE	11013	9/6/1993 0:00	generic_anomaly_spain1_2b9	generic_anomaly_spain1_2b9	95	hierarchy_flow_category1	0.8167	payments#has_card#mean5	
FALSE	11013	9/6/1993 0:00	spain1_anomaly4_2b9	spain1_anomaly4_2b9	27	hierarchy_flow_category1	0.8167	payments#has_card#mean5	
FALSE	11013	9/6/1993 0:00	algo_risk_2b9	Algo detected anomalies_2b9	90	algo	0.8167	payments#has_card#mean5	
FALSE	5428	9/24/1993 0:00	generic_anomaly_spain1_2b9	generic_anomaly_spain1_2b9	95	hierarchy_flow_category1	0.6977	min1#min2#mean3	
FALSE	5428	9/24/1993 0:00	spain1_anomaly4_2b9	spain1_anomaly4_2b9	27	hierarchy_flow_category1	0.6977	min1#min2#mean3	
FALSE	5428	9/24/1993 0:00	algo_risk_2b9	Algo detected anomalies_2b9	90	algo	0.6977	min1#min2#mean3	
FALSE	11265	9/15/1993 0:00	generic_anomaly_spain1_2b9	generic_anomaly_spain1_2b9	95	hierarchy_flow_category1	0.7404	min1#mean2#mean3	
FALSE	11265	9/15/1993 0:00	algo_risk_2b9	Algo detected anomalies_2b9	90	algo	0.7404	min1#mean2#mean3	
FALSE	11265	9/15/1993 0:00	spain1_anomaly4_2b9	spain1_anomaly4_2b9	27	hierarchy_flow_category1	0.7404	min1#mean2#mean3	
FALSE	8261	9/13/1993 0:00	generic_anomaly_spain1_2b9	generic_anomaly_spain1_2b9	95	hierarchy_flow_category1	0.5679	min5#mean2#mean3	
FALSE	8261	9/13/1993 0:00	spain1_anomaly4_2b9	spain1_anomaly4_2b9	27	hierarchy_flow_category1	0.5679	min5#mean2#mean3	
FALSE	8261	9/13/1993 0:00	generic_anomaly_spain1_2b9	generic_anomaly_spain1_2b9	95	hierarchy_flow_category1	0.5679	min5#mean2#mean3	
FALSE	8261	9/13/1993 0:00	spain1_anomaly4_2b9	spain1_anomaly4_2b9	27	hierarchy_flow_category1	0.5679	min5#mean2#mean3	
FALSE	10973	10/13/1993 0:00	generic_anomaly_spain1_2b9	generic_anomaly_spain1_2b9	95	hierarchy_flow_category1	0.6343	min1#mean5#min2	
FALSE	10973	10/13/1993 0:00	spain1_anomaly4_2b9	spain1_anomaly4_2b9	27	hierarchy_flow_category1	0.6343	min1#mean5#min2	
FALSE	10973	10/13/1993 0:00	algo_risk_2b9	Algo detected anomalies_2b9	90	algo	0.6343	min1#mean5#min2	
FALSE	4894	11/4/1993 0:00	generic_anomaly_spain1_2b9	generic_anomaly_spain1_2b9	95	hierarchy_flow_category1	0.668	min1#min2#min5	
FALSE	4894	11/4/1993 0:00	spain1_anomaly4_2b9	spain1_anomaly4_2b9	27	hierarchy_flow_category1	0.668	min1#min2#min5	
FALSE	4894	11/4/1993 0:00	algo_risk_2b9	Algo detected anomalies_2b9	90	algo	0.668	min1#min2#min5	
FALSE	5270	11/22/1993 0:00	generic_anomaly_spain1_2b9	generic_anomaly_spain1_2b9	95	hierarchy_flow_category1	0.9398	min1#mean3#mean2	
FALSE	5270	11/22/1993 0:00	spain1_anomaly4_2b9	spain1_anomaly4_2b9	27	hierarchy_flow_category1	0.9398	min1#mean3#mean2	
FALSE	5270	11/22/1993 0:00	algo_risk_2b9	Algo detected anomalies_2b9	90	algo	0.9398	min1#mean3#mean2	

Figure 184: Example Section of a Downloaded Analysis Risks .csv file - Media

8.4.3.4. Applying New Parameter values

After the evaluation process is complete and you decide that no further results improvement can be made, the next step is to apply (overwrite) new values to overwrite previously set parameter values and apply the new analysis parameters.

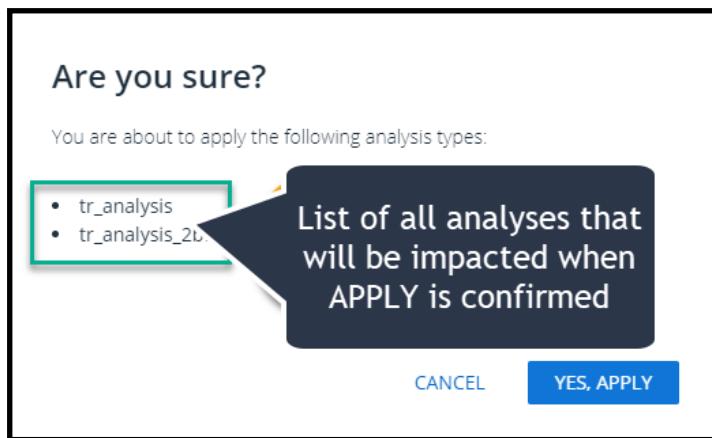
» To apply new values:

1. Return to the Rules Parameter Editor Landing page.

Important note: Don't forget that when you click **Apply** it includes settings of all the analysis under the environment. To reduce the chances of applying unwanted values it is a best practice to check every analysis you have modified and verify settings are accurate.

2. Click the **APPLY** button.

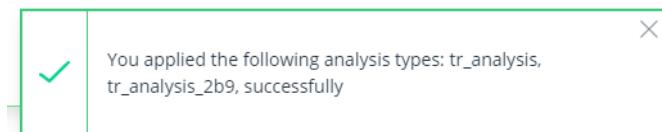
The following verification popup is displayed.



As an aid in remembering which analysis you have modified, the verification popup lists all analysis that will be updated.

3. To confirm action , click **YES APPLY**.

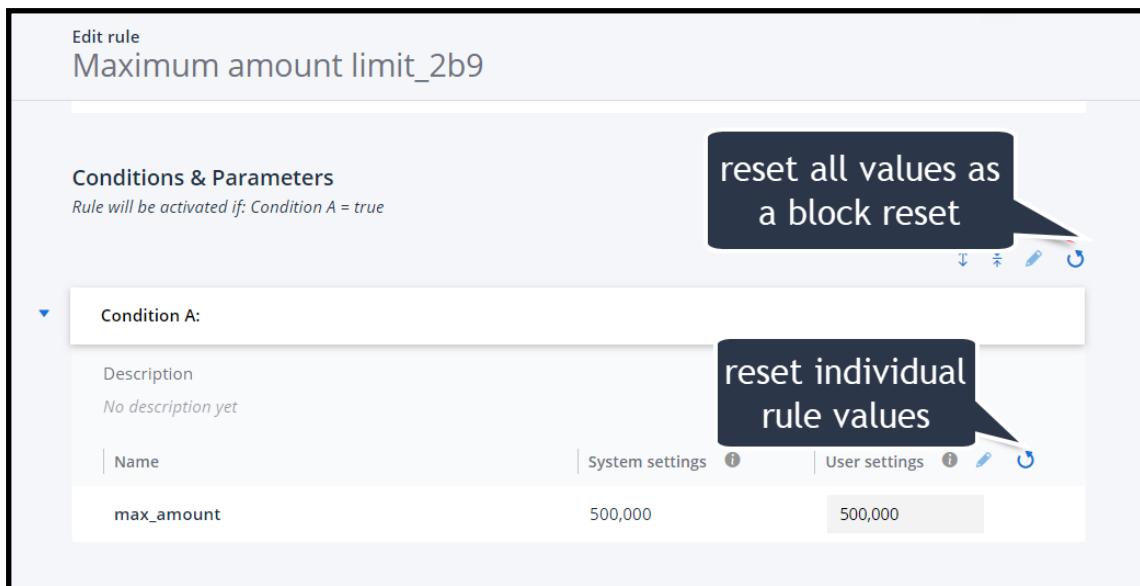
If apply action is successful, the following example message is displayed:



8.4.3.5. Resetting Values to System Settings

So you have applied modified user values and it transpires that there are some settings are not working as expected. This situation can be fixed quickly by resetting the applied user settings and returning them back to the original system setting values.

Reset can be applied to either each rule individually or as a block reset of all user settings.



Conditions & Parameters
Rule will be activated if: Condition A = true

Condition A:

Description
No description yet

Name	System settings	User settings
max_amount	500,000	500,000

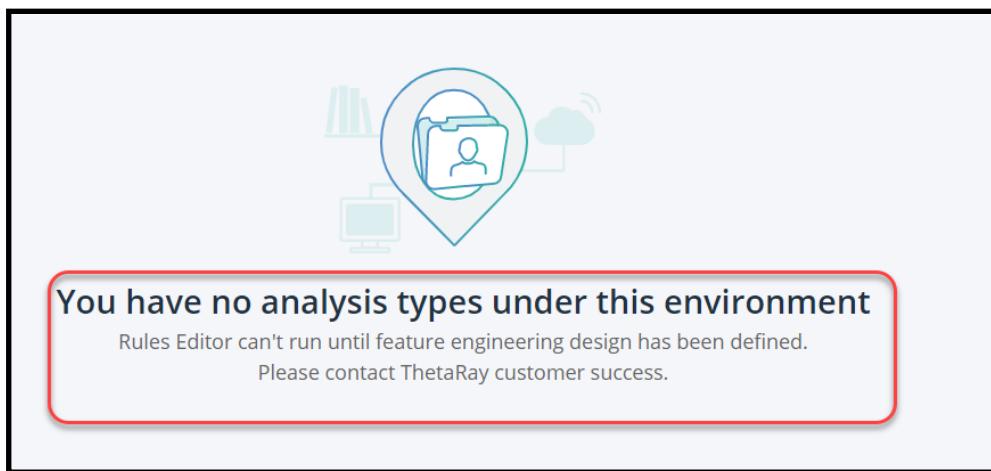
➤ To reset to user settings to default system settings:

1. From the **Rules Edit** panel either select the reset icon  for all rules, or individual rules values.
2. Click **Save**.

Note: After setting rules parameter values back to system settings you should, as a *best practice* run an analysis to verify that analysis results have now returned to their pre-rules parameter edit status.

8.4.4. Rules Parameter Editor -Troubleshooting

Issue When accessing the Rules parameter editor , the following example error message may be displayed when you initially access the module:



You have no analysis types under this environment

Rules Editor can't run until feature engineering design has been defined.
Please contact ThetaRay customer success.

Solution

This message indicates that either:

1. The deployment is new and ThetaRay's customer success have not yet completed the feature engineering design for your environment.
2. There might be some temporary issue that is affecting the display of your system analyses.

Either way, contacting ThetaRay customer success should quickly resolve the issue and enable you to continue your task of editing the rules parameters that control your alert detection process.

8.5. Practical Workflow and Example Scenario

The following suggested workflow is for practical purposes only. It is provided to give you an initial basic grounding when working with the Rules Parameter Editor.

➤ Example workflow routine:

1. Select the analysis that you wish to edit its rules parameter values.
2. From the main edit screen, select the *manual* edit radio button.
3. Run an analysis with the system settings (i.e., no changes to rules values)
4. View the Summary table report:

Note: It is suggested that a screen shot be made of the summary. This can be used as a baseline when initially evaluating changes made to the rules values in the analysis.

5. Return to the same analysis card and from the side panel, select a rule to be edited and tested.
6. Modify the parameters that you wish to evaluate.
7. Save locally and rerun the analysis with modified settings.
8. When the summary results are displayed compare results with the baseline statistics from step 4.
9. For more detailed information you can download a full results report as a .CSV formatted file.
10. Run as many iterations as required to maximize results.

11. Only when satisfied that you have the best results possible, should you apply the new values to the as updated system settings.

8.5.1. ☺ Example Test Scenario

Now that have covered all the functional elements of the **Rules Parameter Editor**, let's take a look at a practical example use case exercise.

Step #1 - To start this test scenario , we will use the 'Maximum payments limit rule' as detailed in the following figure:

View rule
Maximum payments limit_613

Rule activation

Active

Rule is active

Conditions & Parameters

Rule will be activated if: Condition A = true

Condition A: payments condition

Description

payments greater than max_payments parameter

Name System settings User settings

max_payments 9,000 9,000

Suppression period

Inactive

Suppression is inactive

Current settings where user settings are equal to system settings

With reference to the above figure we can see:

1. The selected rule is set to *active*.
2. The max payments *user settings* (max_ payments equal to 9000) are the same as the *system settings*.
3. Suppression is *inactive*.

Step #2 - After running an evaluation test analysis with a date range covering a period of 26 month on system settings, we can now view the following test results summary:

The screenshot shows a 'Test rules editor risks' interface. At the top, there are date range filters ('From: 08/17/1993' and 'To: 10/25/1995') and a 'RUN' button. Below this is a 'Test results summary' table with columns: Identifier, Display Name, Severity, Type, Parameters, and Count. One row is highlighted with a red box: 'payments_risk_613' with 'Display Name: Maximum payments limit_613', 'Severity: 60', 'Type: payments', 'Parameters: max_payments, value: 9000', and 'Count: 2'. A callout box points to this row with the text 'Payments risk rule set to system settings - detected 2 alerts'. The total number of alerts is 477.

In the summary report, we can see that the test results detected 2 alerts.

Step #3 - Once we have a 'baseline' statistic for our scenario, we need to ask the 'What if?' question.

How would lowering the max_payments limit parameter affect the number of detected alerts?

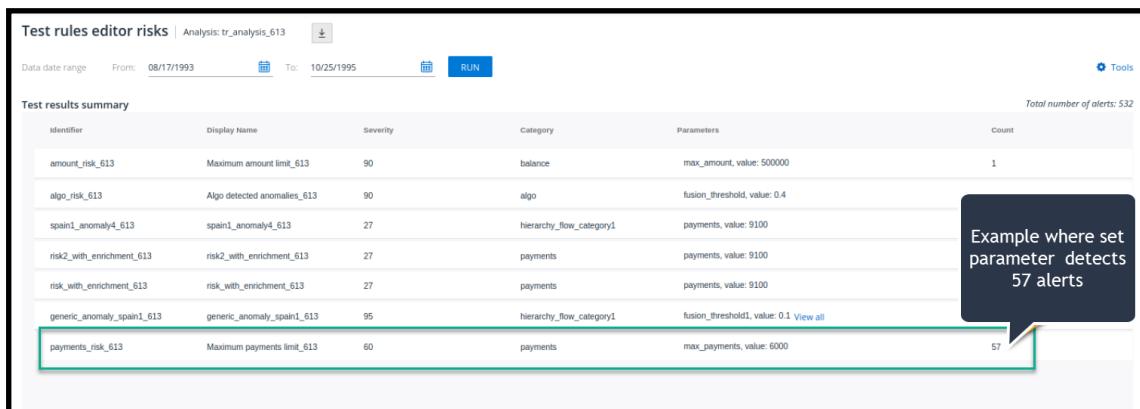
For the purpose of the first test iteration we can try lowering the max_payments value to 6000 and see how the results change.

We return to the rules edit page:

1. Make sure the rule is still activated.
2. Keep the date range as was in the original analysis run.
3. Adjust the max_payments value to 6000,
4. Save the new value as highlighted below.

The screenshot shows the 'View rule' page for 'Maximum payments limit_613'. It includes sections for 'Rule activation' (Active), 'Conditions & Parameters' (Condition A: payments condition), and 'User settings' (max_payments: 6,000). The 'User settings' field is highlighted with a red box.

Step #4 - We now run a new evaluation analysis and as you can see, the amount of alerts has increased to 57!



Test rules editor risks | Analysis: tr_analysis_613

Data date range From: 08/17/1993 To: 10/25/1995 RUN Tools

Total number of alerts: 532

Identifier	Display Name	Severity	Category	Parameters	Count
amount_risk_613	Maximum amount limit_613	90	balance	max_amount, value: 500000	1
algo_risk_613	Algo detected anomalies_613	90	algo	fusion_threshold, value: 0.4	
spain1_anomaly4_613	spain1_anomaly4_613	27	hierarchy_flow_category1	payments, value: 9100	
risk2_with_enrichment_613	risk2_with_enrichment_613	27	payments	payments, value: 9100	
risk_with_enrichment_613	risk_with_enrichment_613	27	payments	payments, value: 9100	
generic_anomaly_spain1_613	generic_anomaly_spain1_613	95	hierarchy_flow_category1	fusion_threshold1, value: 0.1 View all	
payments_risk_613	Maximum payments limit_613	60	payments	max_payments, value: 6000	57

Now, in our test scenario you can see that obviously it is not a simple case of reducing the limit without some sort of trade-off in performance, and therefore more iterations are required to achieve the highest rate of alert detection while gradually increasing the value of max_payments to the highest practical level.

Hopefully, this test scenario should provide you with some practical guidance in using the Rules Parameter Editor.

9. Providing a Recommended Resolution & Closing the Alert

The Task of providing a recommended resolution and closing the alert is split between the Analyst and the Supervisor

9.1. The Analyst Task

In the process of the analyst's tasks, moving towards resolving an alert requires providing a recommended resolution. While selecting a Recommended Resolution, the analyst should create a note that provides a rationale for the judgment call. When the note is applied, a link is created from the alert card that allows the analyst to jump directly to the note in the Note tab.

» **To change a Resolution Code and create a note:**

1. Verify the alert is in the In Review state, (the only state from which the **Resolution Recommended** option can be selected) .
2. In the pop up that is displayed as shown below, select the recommended resolution from the available options.

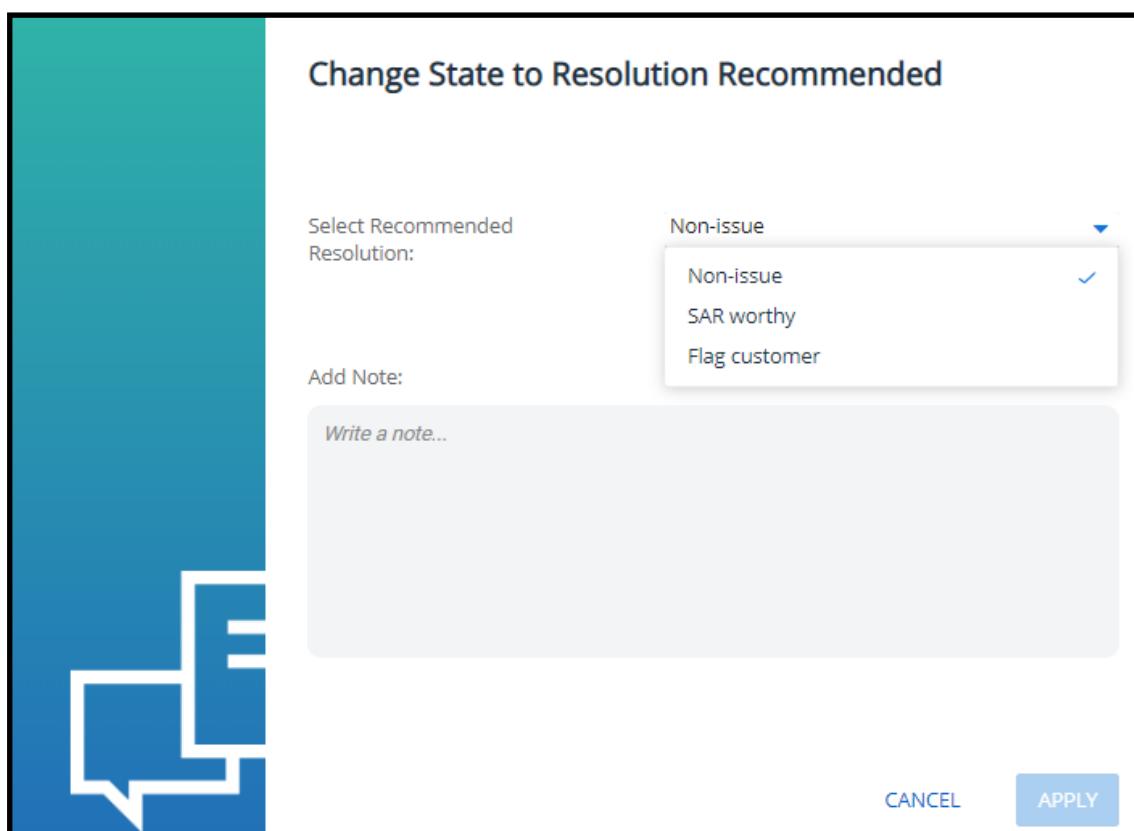


Figure 185: Change State to Resolution Recommended Pop up

3. Write a note explaining the rationale for the suggested resolution recommended and click **Apply**.

A confirmation toaster message is displayed verifying a successful change of state and detailing the system supervisor to whom the alert is now passed.

The Alert Card is now tagged with the selected resolution recommended (Flag Customer in this example), the note text, and a **Go to Note** link as shown below .

The screenshot shows an Alert Card for two alerts. The top alert (AL_00000043) has a note: "Flag Customer By Admin ThetaRay" with the text "Although not at the level of SAR Worthy the collected evidence associated with this Alert suggests the customer is involved with suspicious transactions and therefore should be flagged in the system." Below it is a "Go To Note" link. The bottom alert (AL_00000042) has a "RESOLUTION RECOMMENDED" button labeled "Flag Customer".

Figure 186: Alert Card with Recommended Resolution , Note and Go To Link

Clicking the **Go to Note** link jumps you directly to the Alerts Anomaly Details screen and displays the note you created, as shown **Figure 187:** below.

The screenshot shows the Anomaly Details screen for the flagged alert. It displays various anomaly details and four bar charts. On the right, a note is displayed: "Flag Customer By Admin ThetaRay" with the text "Although not at the level of SAR Worthy the collected evidence associated with this Alert suggests the customer is involved with suspicious transactions and therefore should be flagged in the system." Below it is a "Process" button.

Figure 187: Anomaly Details Screen Showing Created Note

9.2. The Supervisor's Task

The task of the supervisor is to check the analyst's recommended resolution and either to:

- Accept the resolution recommended and close it
- Change it to a different final resolution and close it
- Re-open the alert and re-assign it to a different analyst

10. Browser Support and View Resolution

This section details the browsers supported and the recommended viewing resolution for the current version of Investigation Center.

10.1. Browser Support

Browser	Support Details	Comments/ Issues
Chrome	Full support	Primary browser, no issues. Supported latest version and below, including versions (94.0, 93.0, 92.0 and 91.0)
Internet Explorer	Version - Edge	No issues and supported
Internet Explorer	Starting with IE 11	Not recommended as may exhibit display issues and also its end of life support applies from June 15, 2022
Other Browsers	Not supported	N/A

10.2. View Resolution

A minimum view resolution of 1920 x 1080 should be set to view the display in high definition mode.

11. Customer Screening Module

11.1. Introduction

Customer Screening is the process of monitoring - one time onboarding events (new account being opened for example) or periodic maintenance events that can occur quarterly, semi-annually or annually.

11.2. Overview

The customer screening module is an Investigation Center 'add on' module that provides customers who have deployed the ThetaRay solution, the additional capability of monitoring and resolving alerts that originated as a result of being matched in a customer screening verification process.

11.3. Purpose

The purpose of the supplementary chapter in the Investigation User guide is to provide you, the end user, with detailed information and support regarding how to use your Investigation center, to resolve customer screening alerts.

You will see, as you work through this chapter how the customer screening resolution process differs from the process of resolving alerts sourced from other origins (example: transaction monitoring).

Topics that are common to other alert origins are covered in the parent Investigation Center User guide and for the sake of brevity and documentation efficiency, are not repeated in this chapter.

Main topics covered in this chapter include:

- Alert Lifecycle and Analyst Workflow
- Customer screening alert cards
- Customer screening Risk Details
- Customer screening alerts - resolution process

Let's in the following sections, explore how to resolve the customer screening alerts that populate your Investigation Center case manager.

11.4. Analyst's Screening Alert - Lifecycle and Workflow

The process of resolving screening alerts requires following a specific Alert State Lifecycle analytical flow according to a set default BPMN formatted workflow.

This section of the user guide shows both the lifecycle as an analytical block image and the default workflow as a BPMN diagram.

The following diagrams are applicable to both Transaction and Customer use cases.

11.4.1. Alert State Lifecycle

The following lifecycle diagram displayed below shows the analytical logic path the alert takes from the **New** to the **Closed** state. New alerts are either assigned to the analyst by the team leader/ supervisor or pulled by the analyst from the repository of new alerts. Depending on the level of alert forensic information collected / available, the alert can be take one of the following states:

- **Approved** and then closed
- **Blocked** and then closed
- **On Hold** (till sufficient forensic evidence gathered)

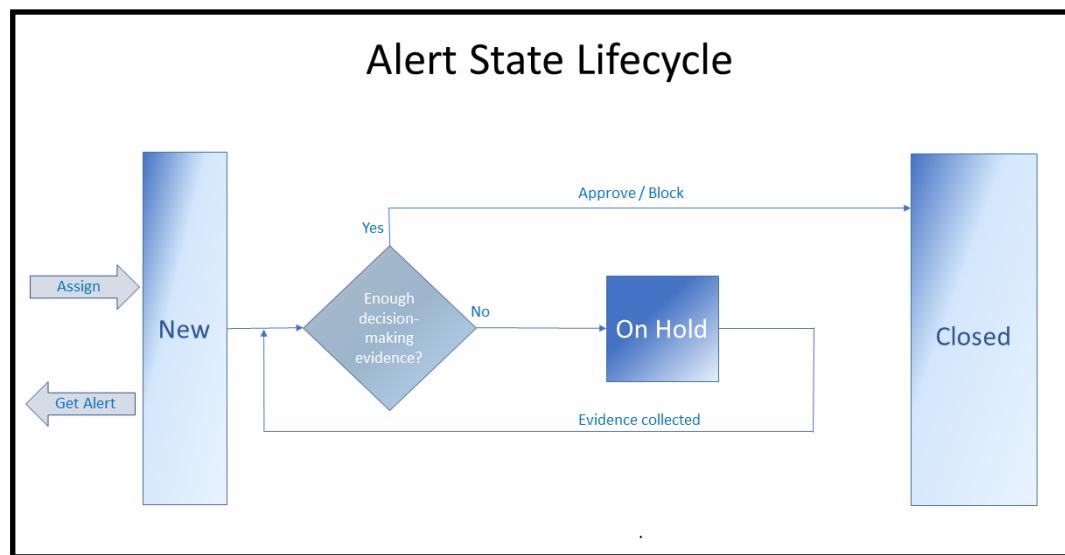


Figure 188: Example - Screening Alert State Lifecycle, as it Pertains to Resolving Screening Alerts

11.4.2. Alert Default Workflow

The screening workflow diagram displayed below shows the default path the new alert takes as it investigated and resolved. The diagram elements displayed include manual and system steps that decide the path the alert takes until resolution.

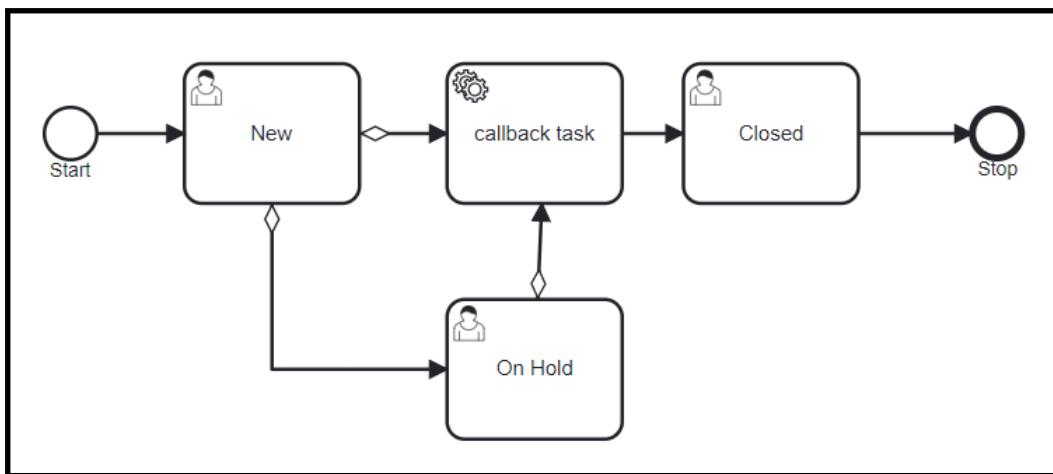


Figure 189: Default Workflow Shown as a collection of BPMN Elements with Process States from Start to End

11.4.3. Whitelisted Call-back Screening Information

Additionally, as part of the screening workflow, call back tasks are used to provide feedback regarding maintenance of a whitelisted list of customers who subsequently do not require investigation in future screening matches.

11.5. Accessing Customer Screening and Overview

Access to Investigation Center (IC) Customer Screening alert module is available to company personnel (for example: analysts or supervisors, with the appropriate access permissions).

➤ To view list of Customer Screening alerts:

1. From Investigation Center login -> filters -> origins, select to view only Customer screening alerts.

Note: If you are experiencing login or access issues, please contact ThetaRay customer support.

11.6. Investigation Center - Customer Screening - Landing Screen

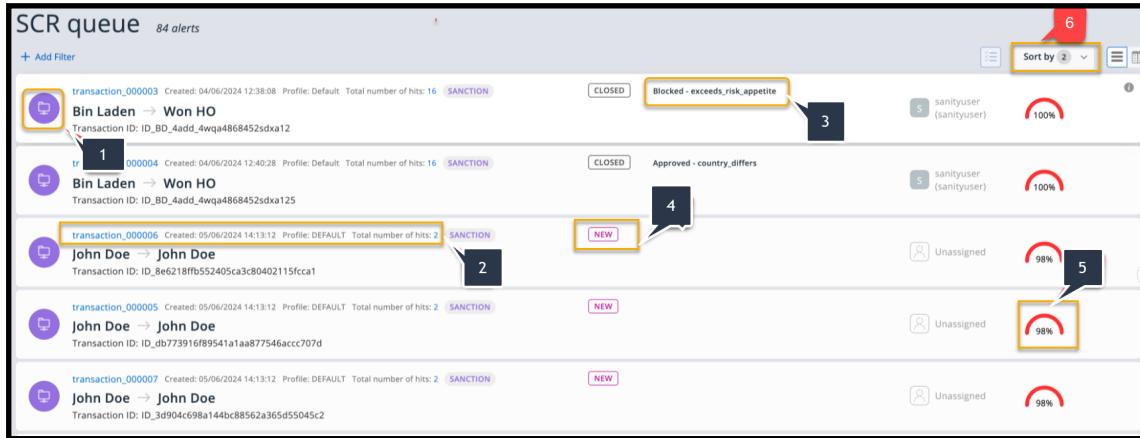


Figure 190: Example of Customer Screening - Landing Screen

Note: If some of the items shown in this example screen are not covered in this topic as they are more generic in nature please refer to the Investigation Center User Guide - Latest version.

11.6.1. Customer Screening Landing Page Main Elements Overview

Refer to the above image as you read the following summary descriptions:

Customer Screening icon (1)

Highlighted here are the alert card attributes that distinguish this alert from other alert types, (example - Customer Screening).

Transactional Data (2)

- Customer id number - unique identity of customer alert
- Created - The date on which the alert was created
- Profile - Either a default value or a custom profile created by Screening admin persona, for example - 'High Risk Customers'
- Total number of hits - Number of accumulated hits (matches) registered against screening lists, used in query

The customer screening icon , which differentiates the Customer Screening card from a Transaction screening card.

Closed Resolution code (3)

With Screening alerts as well as the resolution to close the alert also displayed is the resolution code (eg. Blocked / Approved).

Current Status (4)

- Current status of alert - in general one of the following:
 - NEW
 - STATE_NEW
 - On hold
 - Closed

Note: In certain deployments, custom states can be implemented

Match Score (5)

The matched score is an integral part of the information displayed on the alert card. The match score (a number between 1 and 99), reflects by number weight and graph color intensity , an indication of the degree of certainty to which the displayed match score rating is supported. **Match Score - Breakdown (5a)**

If adjustments are applied to the matching process, the 'Score breakdown' link will appear next to the match score. This feature provides detailed information on how the final match score with adjustments is calculated.

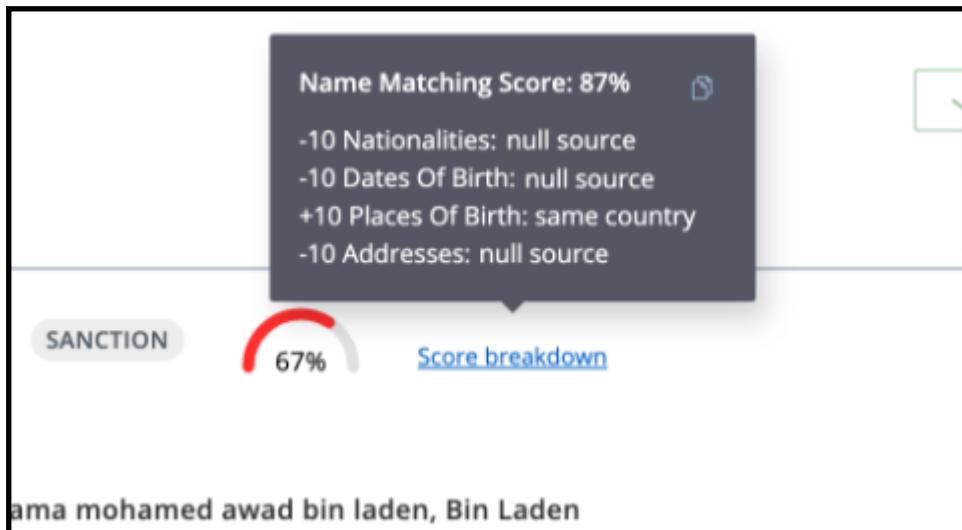
Clicking on a displayed 'Score Breakdown Link', displays the following information:

- Name Matching Score: Displays the name similarity score as a percentage.
- Attribute Adjustments: Lists each attribute that was considered in the matching process, along with the adjustment values applied. These adjustments can be positive or negative and are based on the type of match of secondary attributes.

For example:

- -10 Nationalities: null source: A negative adjustment for missing nationalities.
- -10 Dates Of Birth: null source: A negative adjustment for missing dates of birth.
- +10 Places of Birth: same country: A positive adjustment for a match places of birth in the same country.
- -10 Addresses: null source: A negative adjustment for matching addresses in the same subregion.

A practical example of a breakdown popup is shown below.



Note: Additionally, please notice the "Copy" icon, depicted as two overlapping papers on the upper right area of the popup. Users can utilize this functionality to duplicate score breakdown data for further analysis or sharing purposes.

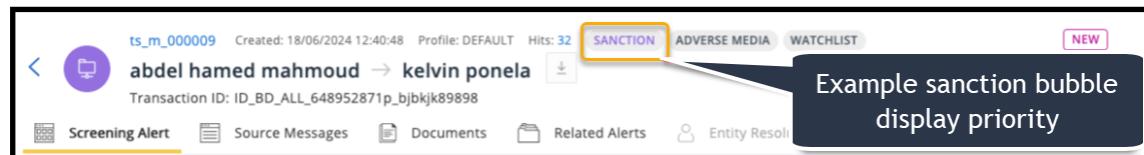
Sort by (6)

The Alerts Screen List 'Sort by' function provides the ability where the user can order the displayed alert cards by a selected parameter. Once the parameter is selected and the order is confirmed, the alerts list is ordered accordingly.

Note: As with filters (6), the 'sort by' function uses a global design which means that some of the parameters not supported in screening, will return an empty state.

11.6.2. Returned Alert Hits Bubble Display Priority

As can be seen in the following screenshot, sanctioned alert hits are given display priority when multiple categories are included in the alert card. This methodology is by and large proven to be more beneficial to analysts in the alert investigation process.



Example, Sanctioned Alert bubble being Prioritized Display before any other bubble categories

11.7. Customer Screening - Managing Alerts

The alerts list includes Customer Screening alerts from the currently selected alert view.

Topics covered in this **Managing Alerts List** section include:

- Screening - relevant filters
- Sorting alerts
- SLAs (If used)
- Viewing alerts in card or tabular format

11.8. Screening - Relevant Filters

The comprehensive list of Investigation Center (IC) filters is detailed in the IC Guide. For convenience Customer Screening related features are shown below in the following figure category and by type:

Table 9: Filters that Apply to Transaction and Customer Screening - by Category and Type

Category	Type
Main General	State
	Resolution Code
	origin
Screening Only	Match Score - High, medium, low
	Source Messages - search by field name then select from displayed matches

11.8.1. Screening Centric Filters

From + Add Filter select -> Origin filter -> select screening.

11.8.2. Filter by Origin Filter

- Transaction Screening

- Customer Screening

Example Filter is shown below:

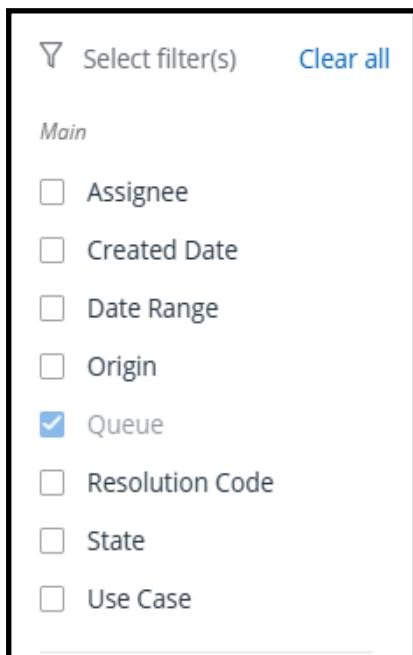


Figure 191: Example of filtering by Screening Attributes



11.8.3. Filter by State

The State filtering option allows the user to filter displayed alerts by state.

» To filter by State:

1. From the Alerts List Filter menu, click the **State** option.
2. Select from either of the two screening alert states:
 - NEW

- STATE_NEW
- ON_HOLD
- CLOSED

11.8.4. Filter by Resolution Code

The Resolution Code filter is an effective way to search for alerts by their closing resolution. (for example approved or blocked)

» To filter by the Resolution code:

1. From the Alerts List Filter menu, click Resolution Code option.
2. Select the requested resolution fields from:
 - **New:** All new alerts start in this state
 - **Blocked:** If one screening event from an Alert is categorised as blocked then the Alert transition to a blocked state
 - **Approved:** If all screening events for an alert are categorised as 'Approved' then the Alert transitions to an 'Approved' state
 - **On Hold:** If one screening event from an Alert is categorised as 'On Hold' then the Alert transition to a on hold state
 - **Closed Approved:** Final state of an Approved alert
 - **Closed Blocked:** Final state of a Blocked alert

Note: To re-open a Blocked or Approved alert requires admin access. This can only be completed manually in this phase.

3. Click APPLY

11.8.5. Sorting Alerts

If required to sort Customer Screening Alert lists, The key method of sorting is by **Match Score**. This can be incremental or decremental.

For more general information on sorting alert lists , please refer to the Investigation Center core user guide.

11.8.6. SLA

Sanction Screening alert SLAs if used, are set by default as follows:

- For an alert assigned to an analyst, the max SLA time period is set for 4 hours after creation.

- For an alert assigned to a supervisor (, the max SLA time period is set by default for 2 hours after escalation

For more general information refer to Investigation Center Core User Guide.

11.8.7. Viewing Alerts in Card or Tabular Format

Screening alerts can be viewed either in a list or tabular format.

For more general information refer to Investigation Center Core User Guide.

11.9. Tab Navigation Bar

The Tab Navigation Bar provides access to the various tabs set for your screening solution IC deployment .

If the deployment is new, only system tabs are displayed by default. These are of the static type and as such are immutable.

The default system tabs for Transaction screening - provided by default are:

- Screening Alert
- Source Messages
- Documents
- Related Alerts
- Entity Resolution (if deployed)
- Notes
- History

An example of the Alerts Tab Navigation Bar with static system tabs is shown in the following figure.

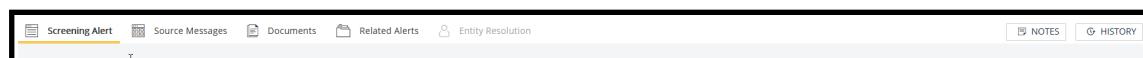


Figure 192: Example navigation Bar for Screening Solution with Default and Optional System Tabs

For more details on working with:

- Documents
- Related Alerts
- Notes (Apart from notes that the analyst can add to any alert resolution case (via auto text templates etc., mandatory notes, created during an investigation (e.g. On Hold Approve, Block etc, are also posted to the Notes tab)

- History

Refer to the Investigation Center User Guide

If your particular deployment requires additional tabs, these can be created as custom tabs and after creation by a Business/ admin user in Investigation *Settings* and added as dynamic tabs to the Tab Navigation bar.

Note: As some of the available modules are optional, if your deployment does not include these, they will appear greyed out on the navigation bar.

11.10. Customer Screening Alerts Tab

From the alerts list, if the alert is not presently assigned to you, you are required to:

1. Click **GET ALERT** to assign the alert to yourself.
2. Make sure the **Screening Alert** tab is selected.

The alert opens, similar to the example shown below.

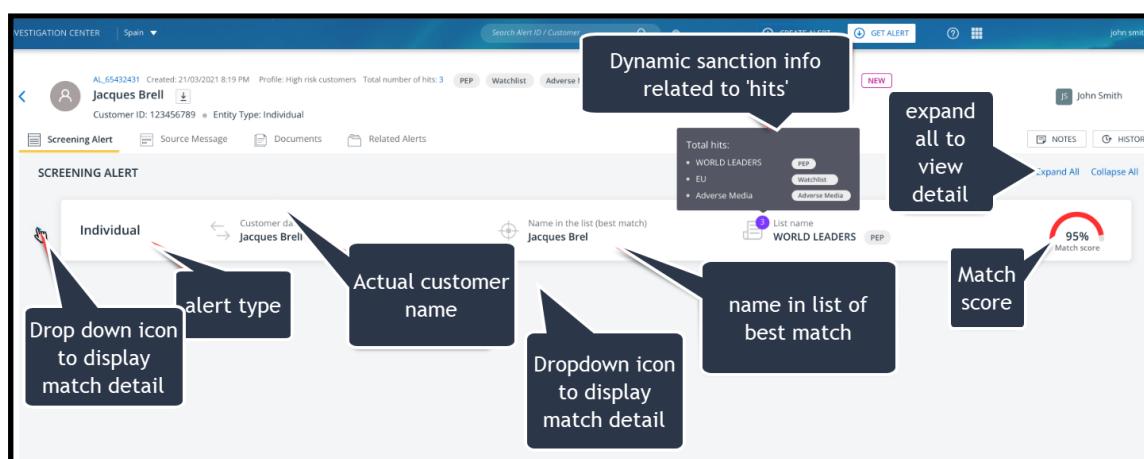


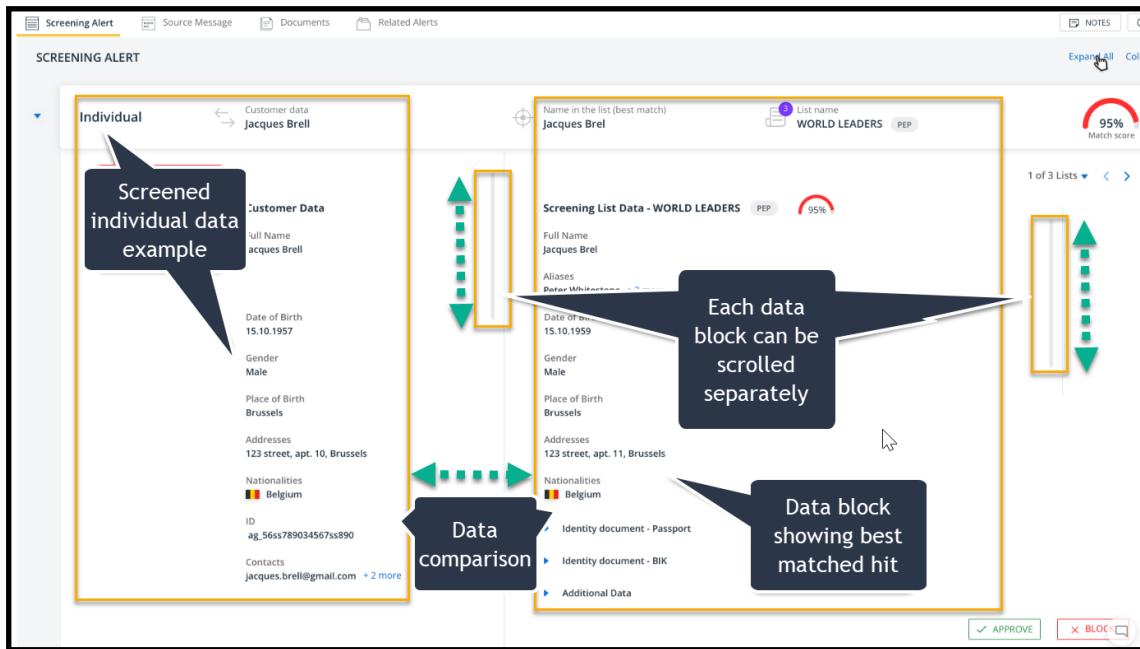
Figure 193: Example Customer Screening Initial Select Card

As **Customer Screening** is based on monitoring the creation and maintenance of accounts the customer sanctions screening model incorporates 4 financial account types related to the creation and maintenance of the account by:

- An individual
- A company
- A merchant (trader)
- An agent (working on behalf of a third party)

To start the resolution process, click the card drop down icon or Expand all link

The expanded view is displayed similar to the figure shown below.



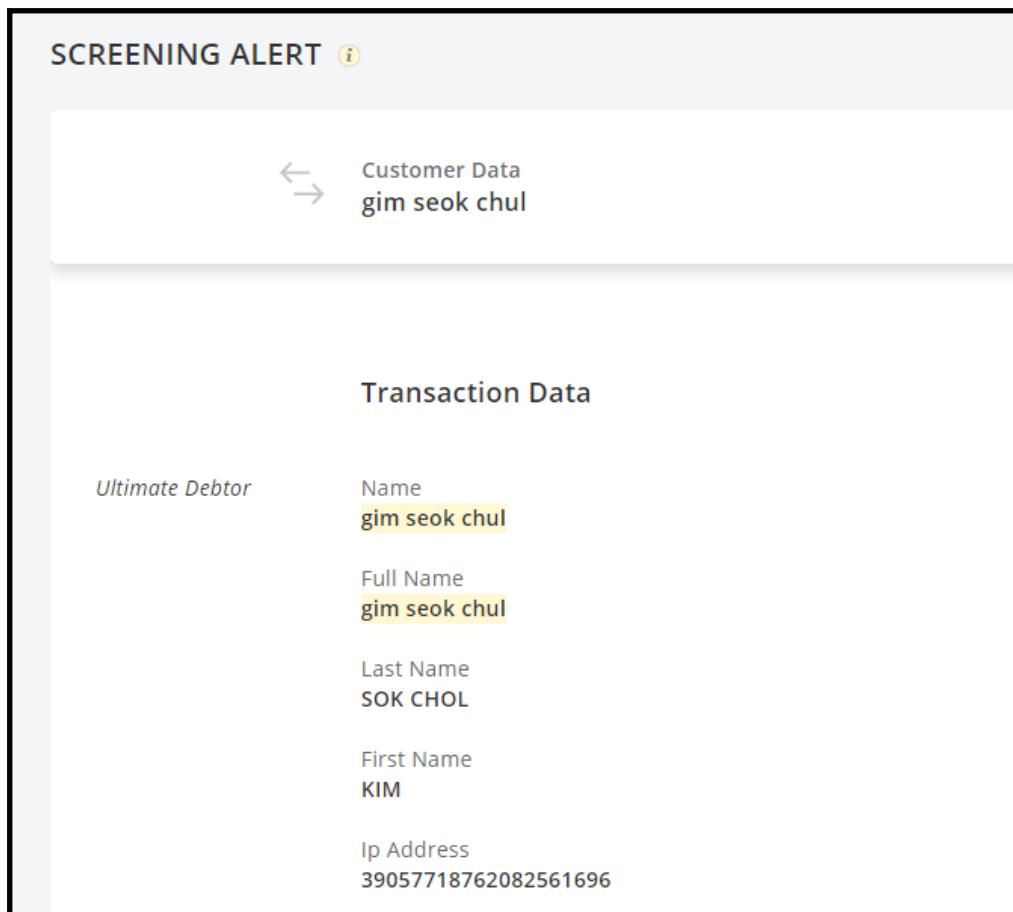
Example of Expanded Alert with Data from both the Customer and Matched hit

11.10.1. Screened Customer Displayed Data Section - More Information

To aid the analyst when viewing the returned results of a screened customer it helps to understand some basic details about the displayed screened customer information displayed on the left side panel:

- The bulk of the information displayed is organized into sections in a structured format and is sourced from the screened entity schema .
- Any information that is not part of the screened entity schema but is available and maybe of aid in the investigation process is supplied under the Additional information section at the end of the customer data block
- To save valuable memory, where data does not exist for certain data categories, the display system dynamically detects this occurrence and automatically blocks the display of unwanted orphaned data headers
- The returned screened 'hit' data returned on the right side panel is not subject to the no data header blocking functionality described in the previous bullet and a no data scenario is denoted by a dash

The following set of images combine to show a practical example of a screened customer data entity with varying Sections of Data Information, as mentioned above.



The screenshot shows a 'SCREENING ALERT' header with a small 'i' icon. Below it, a 'Customer Data' section is shown with a double-headed arrow icon and the name 'gim seok chul'. The main content area is titled 'Transaction Data' and contains the following information:

<i>Ultimate Debtor</i>	Name gim seok chul
	Full Name gim seok chul
	Last Name SOK CHOL
	First Name KIM
	Ip Address 39057718762082561696

Figure 194: Example Customer Data Initial Section Block

11.10.2. Identification Types

Re the identification types that can be returned in a customer screening query, there are two types:

- Individual
- Organization

11.10.2.1. Individual type

Following are a few examples of Individual Identification types

▼ Identification

Identification Type
individual

Identity Documents - Type
Passport

Identity Documents - Number
472310082

Identity Documents - Country
Myanmar

Identity Documents - Description
Test Description

Identity Documents - Dates Of Issue
08/05/2005

Identity Documents - Dates Of Expiry
08/05/2005

Identity Documents - Places Of Issue - City
MM

Identity Documents - Places Of Issue - State
MM

Identity Documents - Places Of Issue - Country
Myanmar

Identity Documents - Places Of Issue - Place Name
MM

Gender
Male

Dates Of Birth
08/05/1955

Places Of Birth - City
MM

Places Of Birth - State
MM

Places Of Birth - Country
Myanmar

Figure 195: Example Core Identification Data Section Block (individual)

Country Of Residence	Myanmar
Screening Entity Type	individual
Id	fake_92652195328932175887
Address	MM

Figure 196: Example Country of Residence Data Block

High Risk Country	Name	gim seek chul
	Full Name	gim seek chul
	Last Name	SOK CHOL
	First Name	KIM
	Ip Address	39057718762082561696
▼ Identification		
	Identification Type	individual
	Identity Documents - Type	Passport
	Identity Documents - Number	472310082
	Identity Documents - Country	Myanmar
	Identity Documents - Description	Test Description
	Identity Documents - Dates Of Issue	08/05/2005
	Identity Documents - Dates Of Expiry	08/05/2005
	Identity Documents - Places Of Issue - City	MM
	Identity Documents - Places Of Issue - State	MM
	Identity Documents - Places Of Issue - Country	Myanmar
	Identity Documents - Places Of Issue - Place Name	MM

Figure 197: Example High Risk Country - Data Block

<i>Previous Instructing Agent</i>	Name
1	ABDUL MANAN
	Screening Entity Type
	individual
	Id
	fake_36712427403373923799
	City
	Quetta
	Iban
	123456789
	Floor
	2
	Region
	Baluchistan Province
	Country
	<input checked="" type="checkbox"/> Pakistan
	Currency
	USD
	Member id
	44551447785
	Postal code
	1234
	Street name
	Kachray Road, Pashtunabad
	Building name
	Quetta
	Building number
	1
	Clearing system id
	45666987745

Figure 198: Example Previous Instructing Agent Data Block

<i>Narrative</i>	Creditor reference fake47991604415899825020
	Remittance info fake82319348815732261548
	Related remittance info fake35980089469666082430
	Sender to receiver info fake70221881656606162358
	Category purpose fake60038023361993733173
	Remittance identification fake67069828598758080633
	Additional remittance information fake58749868560329536938
▼	Creditor reference information
	Creditor reference information type fake88336948959769072363
	Creditor reference information reference fake72410752191711198604
▼	Referred document information
	Referred document information type fake12206965575696655603
	Referred document information line details type fake21929872024080613328
	Referred document information line details number fake31573065405766111701
	Referred document information line details description fake48309468681762202641
▼	Tax remittance
	Tax remittance administration zone fake10008516710091322106

Figure 199: Example Narrative Data Block

Garnishment remittance

Garnishment remittance type
fake44527790756139391999

Garnishment remittance reference number
fake16110505240720322350

Additional Information

Request id
requestIdAuto15042321348487331537

Test
fake_10984732

Test 2
fake_10

Figure 200: Example Garnishment Remittance and Additional Information

11.10.2.2. Organization Type

Organization types differ from Individual types in that they can sometimes represent a more suspicious group of 'bad players' that make up the organization. To aid the analyst in his /her alert resolution task, investigating such organizations, we now, where the customer type is detected as being of the organization type, include the nationality or nationalities of such organizations in the returned results. The following image shows an example of an organization type and the related nationality of the organization.

SCREENING ALERT

Customer Data
Osama bin laden

Full Name
Osama bin laden

Last Name
bin laden

First Name
Osama

Ip Address
string

Identification
Identification Type
organization

Country Of Residence
Afghanistan

partyId
Nationalities
Afghanistan + 1 more

The highlighted fields represent matched names between customer and screening list data. Don't show again

Name in the List (best match)
List Name
High-Risk Country

Screening List Data - OFAC SDN
Debtor Agent
Name
PUBLIC JOINT STOCK COMPANY SBERBANK OF RUSSIA, sberbank of russia

Aliases (12)
SBERBANK ROSSI, sberbank rossi | SBERBANK ROSSI OAO, sberbank rossi | OTKRYTOE AKTSIONERNOE OBSH...

Addresses
Moscow, 19 ul. Vavilova, 117312, Russia + 3 more

Country
Date of Birth
Place of Birth
Nationalities

100%
Match score

1 of 16 Lists

Figure 201: Example - Organization Type with Nationality also Displayed

11.10.3. Screening - Dynamic Matched Fields Highlighting

In screening queries, to help support the analyst to quickly identify returned hit name field matching, when a screening hit is registered, if either a direct match is made to the customer, transaction or beneficiary name or an alias name, both the right panel (static screened entity data name and the returned 'hit' data name are automatically and dynamically highlighted.

This feature works with all screening event type names including Originator, Beneficiary, alias name etc..

The figure below shows an example where the transaction Beneficiary is matched.

The highlighted fields represent matched names between customer and screening list data. Don't show again

Customer Data: abu bakr al-baghdadi

Entity type: Beneficiary

Beneficiary Name: qasem soleimani

Beneficiary Address: —

Beneficiary Counter: —

Screening List Data - EU: SANCTION

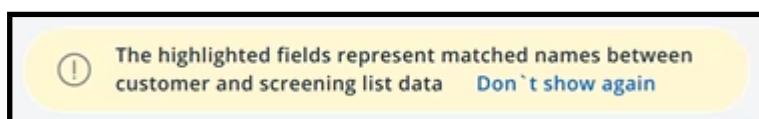
Aliases (21): Qasem Soleimani | Qasim, Soleimani | Qasim Soleimani + 18 more

Match score: 100%

Figure 202: Example Matched Names Highlighting in a Screening Request Alert Hit Return Display

The functionality of this feature is also displayed on the SCREENING ALERT displayed screen. If this feature display info text is no longer required the signed in user can remove it by clicking the 'Don't show again' link as shown below.

If required to view the feature information again after it has been removed simply mouse over the information icon that remains after text removal, for the displayed text to be re - displayed.



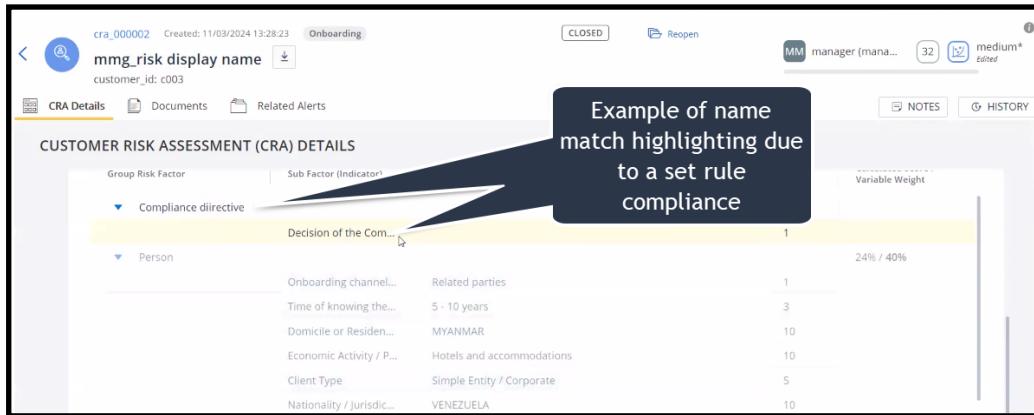
Additional feature information

- If, on scrolling down the displayed data other name fields are also matched say for example, the Originator Name, the match is switched to dynamically display this further match
- This feature applies to both Transaction and Customer screening
- Matched name highlighting is carried out automatically so there is no need to switch the feature function on

11.10.4. Name Match Highlighting in CRA Deployments

Additionally, name matching also works with Customer Risk Assessment alerts if the CRA product is included in the ThetaRay deployment.

Example name matching due to a set CRA rule compliance and alert creation event is triggered.



The screenshot shows a ThetaRay interface for a Customer Risk Assessment (CRA) alert. The alert is titled 'cra_000002' and was created on 11/03/2024 at 13:28:23. It is marked as 'Onboarding' and 'CLOSED'. The alert is for a 'mmg_risk display name' customer with ID 'c003'. A callout box highlights 'Example of name match highlighting due to a set rule compliance' pointing to the 'Decision of the Com...' section. The 'CRA Details' tab is selected, showing 'CRA Details' and 'Documents' sections. The 'CRA Details' section includes a table with columns for 'Group Risk Factor', 'Sub Factor (Indicator)', 'Decision of the Com...', and 'Variable Weight'. The table data includes:

Group Risk Factor	Sub Factor (Indicator)	Decision of the Com...	Variable Weight
Compliance directive		1	24% / 40%
Person		10	
Onboarding channel...	Related parties	1	
Time of knowing the...	5 - 10 years	3	
Domicile or Residen...	MYANMAR	10	
Economic Activity / P...	Hotels and accommodations	10	
Client Type	Simple Entity / Corporate	5	
Nationality / Jurisdic...	VENEZUELA	10	

11.10.5. Additional Information on PEP Data

In Customer Screening alert resolution, if the entity under investigation, is a PEP (Politically exposed person) data returned as **Adverse Media** can indeed provide critical evidence to the analyst that can have a direct influence on the alert resolution.

All information available about the PEP is obviously important but related information on the PEP's associates can also provide a deeper insight into the dubious activities of the PEP under investigation.

Data about associates of the PEP can include:

- Full Name
- Type of relationship

Relationship to PEP can for example be:

- Child
- Spouse

- Sibling
- Business partner

To view information about the matched associate the analyst should click the Close associate link (if provided).

The image below shows an example of Associates data available in customer screening.

The screenshot shows a user interface for customer screening. On the left, there are sections for 'Place of Birth' (Brussels), 'Addresses' (123 street, apt. 11, Brussels), and 'Nationalities' (Belgium). A dark callout box labeled 'Listed associates and relationships' points to a table on the right. The table has two columns: 'Person' and 'Relationship'. The data is as follows:

Person	Relationship
Gordon Brell	Child
Rena Brell	Child
Helen Clayton	Spouse
Belle Reed	Spouse
Oscar Brell	Sibling
Sophia Scott	Business partner
Rosetta Brell	Mother

Figure 203: Example of Available Customer Screening Associates Data

The figure below shows in detail particulars of an associate.

The screenshot shows a detailed view of an associate. A table is displayed with columns for 'Person' (Richard John Cripwell), 'Relationship' (Archie Cripwell is a son of Richard John Cripwell), 'Start Date' (not specified), and 'End Date' (not specified). A 'Associates' section is expanded, showing the same data. A 'Additional Information' section is also present.

Figure 204: Details of a PEP Associate

11.10.6. World Check Screening legal Notice Disclaimer

As a compliance requirement from the **Refinitiv** screening 3rd party provider, the following legal disclaimer is displayed if a customer screening match hit is made using this particular service provider. Analysts, requiring more information about Refinitiv can simply click on the notice to access the Refinitiv website.

An example customer screening alert that was matched by the Refinitiv service is shown below.

Screening Entity Type
Individual

▼ Identity document - Registration Number

Number
110647997

▼ Additional Data

The contents of this record are private and confidential and should not be disclosed to third parties unless: (i) the terms of your contract with us or our partner company allow you to do so; (ii) the record subject requests any data that you may hold on them, and such request is in accordance with the data protection laws of your jurisdiction; (iii) you must consider and abide by your obligations in relation to the data privacy rights of individuals and must notify them of your intention to search against World-Check and provide information contained in the World-Check privacy statement: <https://www.refinitiv.com/en/products/world-check-kyb-screening/privacy>; (iv) you shall not rely upon the content of this report without making independent checks to verify the information contained therein. In the event of a discrepancy a necessary brief note should be read by you in the context of the fuller data available in the external sources to which this report refers. The accuracy of the information found in the underlying sources must be verified with the record subject before any action is taken. If you are in any doubt as to the sources are broken, if this record contains a negative allegation, it should be assumed that such allegation is made by the subject. You should not draw any negative inferences about individuals or entities merely because they are identified in this record, nor because they are shown as "Reported being linked to" others listed in the database. The nature of linking varies considerably. Many persons are included solely because they hold or have held prominent political positions or are connected to such individuals.

Legal Note
The contents of this record are private...

World check
disclaimer
notification
Click to access
Refinitive
website for more
details

11.11. Alert Resolution Process

In general, resolving a customer screening alert includes the following steps:

1. Investigating each screening account type using the following guidelines:
 - a. Viewing and comparing known customer data with data retrieved with matched hits.
 - b. Check details retrieved on other hits by navigating thru the hits.

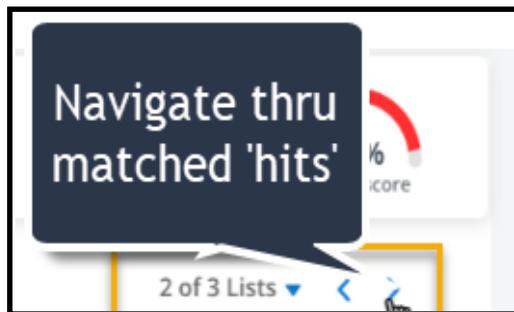


Figure 205: Navigate from Hit to Hit to Examine More Data

- c. You can also sort the order of matches scores in ascending or descending order

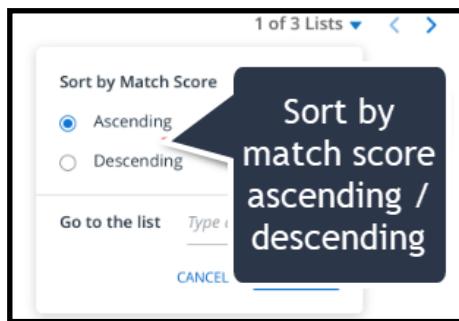


Figure 206: Sort by Matched Score

- d. Examining evidence such as any available gathered forensic documents , notes both current or historical any adverse media data , PEP data etc.



Figure 207: Example of 'Hit' with Adverse Media Picture

- e. Under the messages tab checking for messages that provide evidence of suspicious activity by the party under scrutiny.
- f. Checking under the **Related Alerts** tab for associated alerts that contain relevant related information.

Note: For more general information on handling forensic documents, refer to the Alert details tab section of the core Investigation Center document

- g. If necessary changing the alert status to temporarily 'on hold' while evidence is gathered

When all forensic evidence has been gathered, an '**approve**' or '**block**' decision is required for each screening account type.



Figure 208: Resolution Requires an Approve or Block Decision

11.11.1. Closing Resolution State - Resolution Rule

The closing resolution defines whether the customer screening alert is approved or blocked. The process requires the investigator to:

- Complete a mandatory note providing reason for resolution
- The final alert screening resolution is governed by the following rule:
- "Only if all screening account types are 'signed off' as *Approved* is the transaction closed as approved. If any of the events are blocked, then the transaction is closed as *Blocked*."

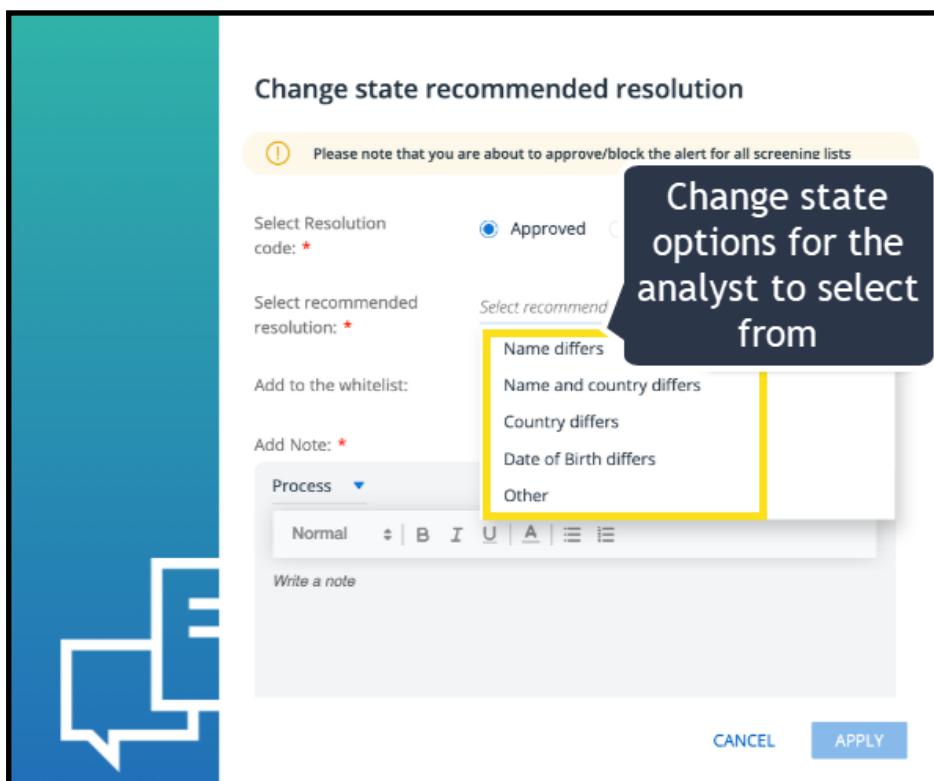


Figure 209: Example of Change State Pop-up Requiring the user to Select reason for Transaction Approval

Approve:

If the selected status is to approve the customer, selecting this option displays the following example pop-up.

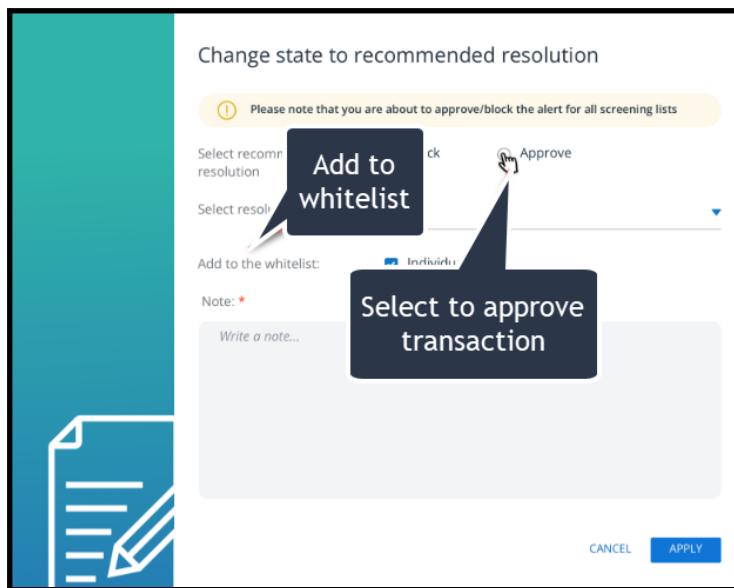


Figure 210: Example 'Approve' Popup with Information Requirements

- **Preset resolution codes:** -Select from list (Mandatory)
- **Add to whitelist:** (Optional)
- **Requirement for detailed approve reason** (Mandatory)

Block:

If the selected status change is to block the event, selecting this option displays the following example pop-up.

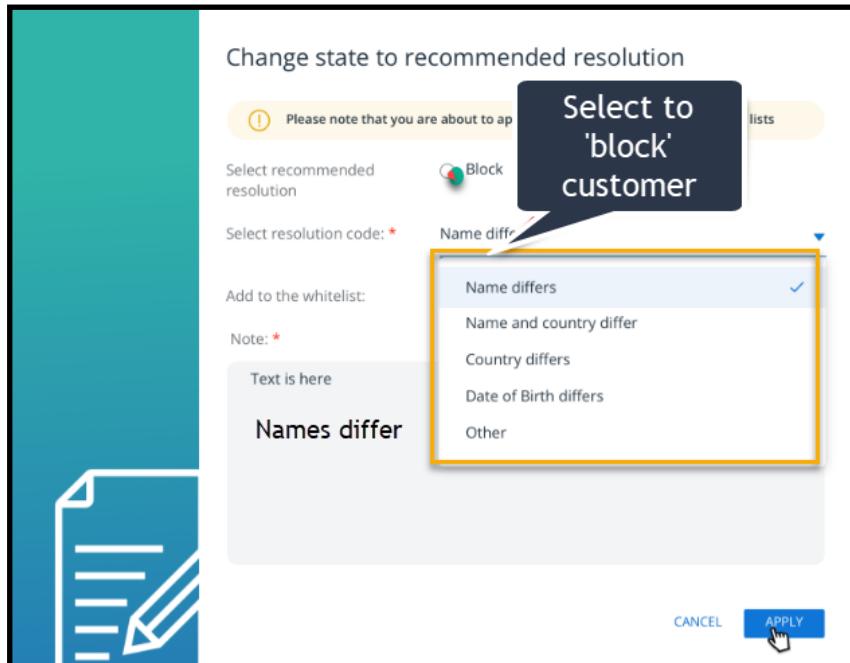


Figure 211: Example Resolution Select Options + Mandatory Note with Rationale for 'Block' Resolution

If the selected status is to temporarily put the alert resolution 'on hold' (say, while waiting for more forensic evidence, there is a requirement to provide a reason for the delay.

Note: The on hold status selection is only temporary, and when all the forensic evidence is gathered and examined, the final closed status must be selected.

11.11.2. Additional Info Availability - Post Resolution Stage

If post resolution analysis info is required, the following images provide the analyst or Supervisor with example system information that can be obtained.

Note: Please note that the information supplied in this sub section also applies to Transaction Screening alerts.

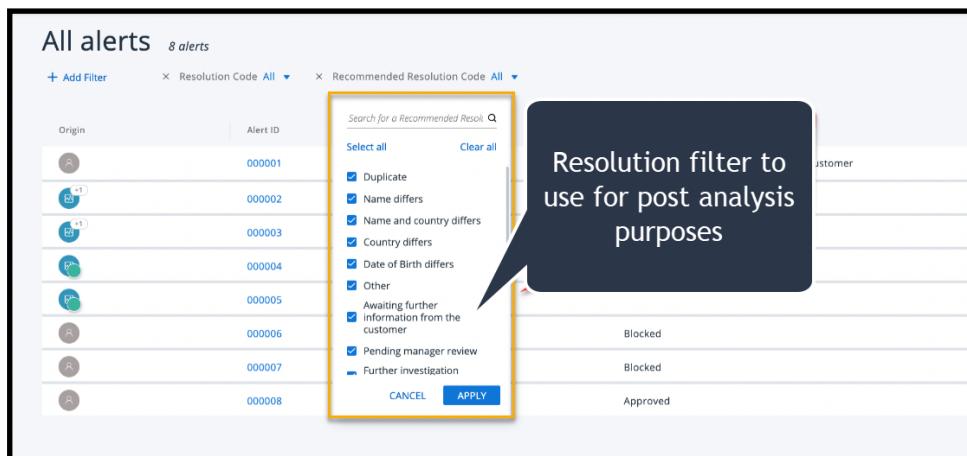


Figure 212: Example Image Showing Filter to view Post Resolution Results

Example post resolution data displayed on screening alert cards

Alert ID	Created	Profile	Hits	Status	Resolution	Comments	Progress
cs_000001	23/08/24	DEFAULT	5	On Hold	Awaiting further information from the customer...	sanityuser (sanityuser sanit...)	100%
tm_000002	23/08/24	anomaly1 (tm_000002)	1	Resolved	Reopen	sanityuser (sanityuser sanit...)	90% (High)
tm_000003	23/08/24	anomaly1 (tm_000003)	1	Request_Further_Information	Under_Review	manager (manager mana...)	90% (High)
tm_000004	23/08/24	test (tm_000004)	1	Under_Review	Under_Review	sanityuser (sanityuser sanit...)	77% (High)
tm_000005	27/08/24	katya1 (tm_000005)	1	Under_Review	Under_Review	manager (manager mana...)	89% (High)
cs_000006	28/08/24	muhamed	6	Pending_manager_review	Pending_manager_review	manager (manager mana...)	100%
cs_000007	28/08/24	ali	2	Blocked - Other	Blocked - Other	manager (manager mana...)	100%
cs_000008	28/08/24	putin	2	Closed	Approved - Name differs	manager (manager mana...)	100%

Figure 213: Example Display of Closed Screening Alerts with Resolution Data Displayed

11.12. Source Messages - Customer Screening

The Source Messages tab contains a list of Customer Screening messages that are associated with each screening alert selected in the Alerts List for further investigation.

These messages provide the analyst with an additional source of forensic evidence when completing the task of investigating alert event types and making an informed decision on the closing resolution (approve or block).

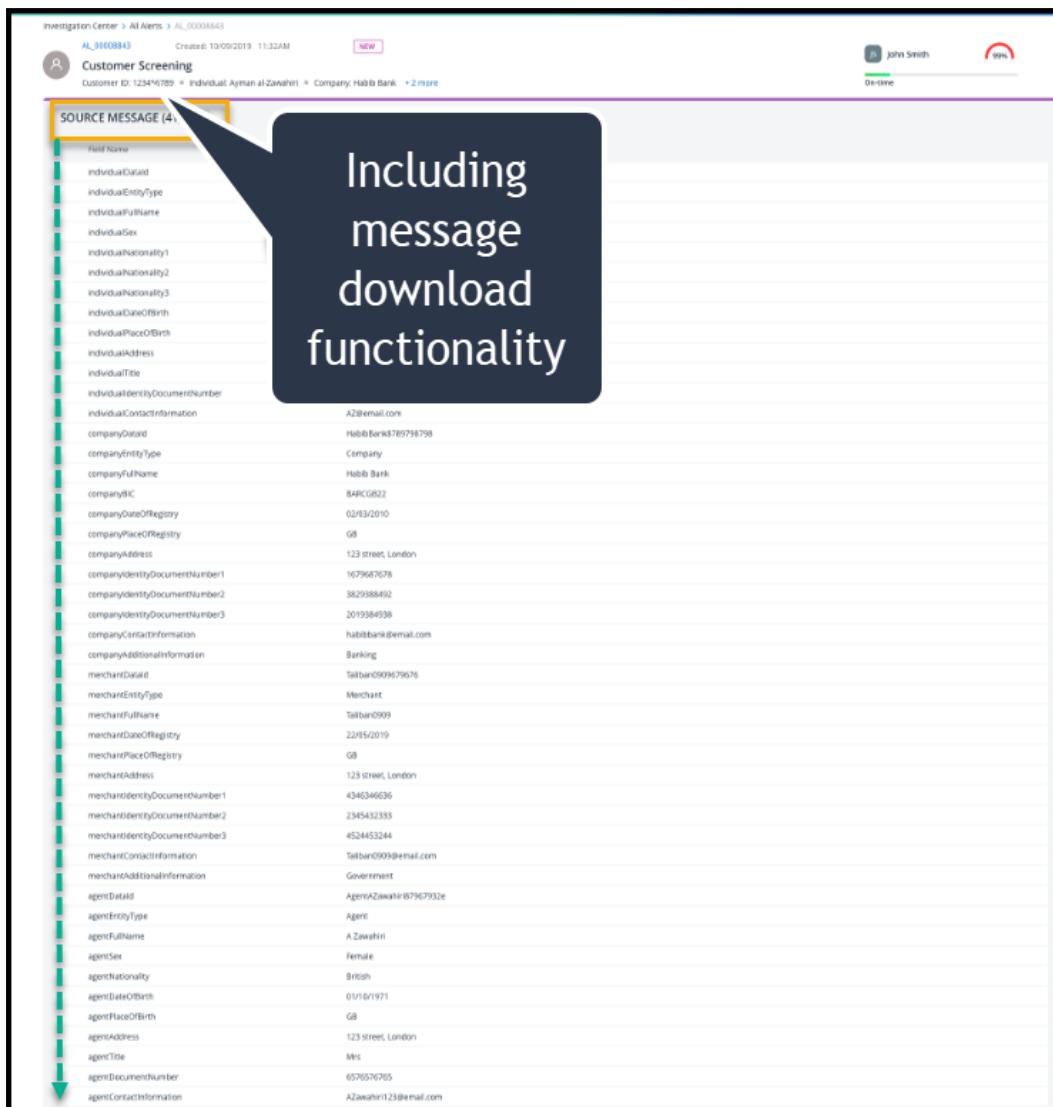
» To select the Source Messages Tab:

1. From the Navigation bar, click the Source messages Tab as shown in the following figure.



Figure 214: Source Messages Select Tab in Navigation Bar

The messages tab opens and displays a list of source messages similar to that shown in the following example figure.



Including message download functionality

Investigation Center > All Alerts > AL_00000000000000000000000000000000

AL_00000000000000000000000000000000 Created: 10/09/2019 11:32AM NEW

Customer Screening

Customer ID: 123456789 - Individual: Ayman al Zawahiri - Company: Habib Bank +2 more

John Smith 99%

On-line

SOURCE MESSAGE (4)

Field Name	Value
individualCountry	
individualEntityType	
individualFullName	
individualSex	
individualNationality1	British
individualNationality2	Pakistani
individualNationality3	French
individualDateOfBirth	15/05/1976
individualPlaceOfBirth	
individualAddress	
individualTitle	
individualIdentityDocumentNumber	
individualContactInformation	
companyCountry	
companyEntityType	
companyFullName	
companyNIC	
companyDateOfRegistry	02/03/2010
companyPlaceOfRegistry	GB
companyAddress	123 street, London
companyIdentityDocumentNumber1	1679667078
companyIdentityDocumentNumber2	3829384892
companyIdentityDocumentNumber3	2019384938
companyContactInformation	habibbank@email.com
companyAdditionalInformation	Banking
merchantCountry	United Kingdom
merchantEntityType	Merchant
merchantFullName	Taliban0909
merchantDateOfRegistry	22/05/2019
merchantPlaceOfRegistry	GB
merchantAddress	123 street, London
merchantIdentityDocumentNumber1	4346346636
merchantIdentityDocumentNumber2	2345432353
merchantIdentityDocumentNumber3	4524453244
merchantContactInformation	Taliban0909@email.com
merchantAdditionalInformation	Government
agentCountry	United Kingdom
agentEntityType	Agent
agentFullName	A.Zawahiri
agentSex	Female
agentNationality	British
agentDateOfBirth	01/01/1971
agentPlaceOfBirth	GB
agentAddress	123 street, London
agentTitle	Mrs
agentDocumentNumber	6576576705
agentContactInformation	A.Zawahiri123@email.com

Figure 215: Example Customer Screening Messages

From the above listing, some example messages are shown below :

individualNationality1	British
individualNationality2	Pakistani
individualNationality3	French
individualDateOfBirth	15/05/1976

As can be seen in the above example messages the list contains useful information about the alert and related events such as , for example account holder name and nationality.

A download icon is also included. This enables you as an example, to download the list, copy to a third party text editor, highlight specific message rows and then upload the edited copy to the *Documents Tab* as additional forensic evidence.

11.13. Customer Manual Screening

11.13.1. Overview

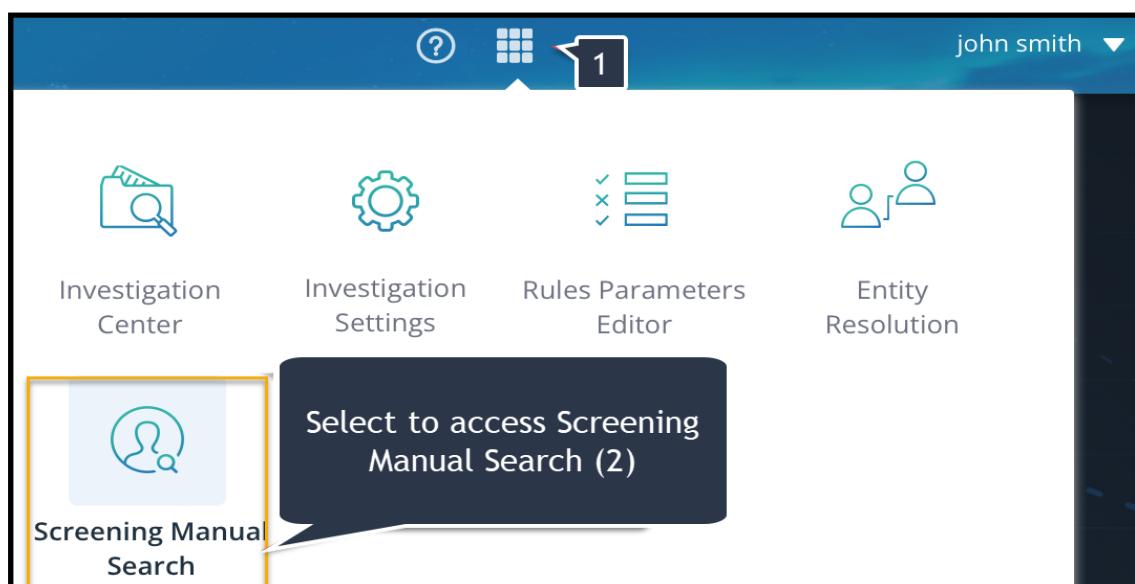
Customer manual screening enables analysts to carry out screening of target entities on an ad-hoc basis. The feature further enhances the scope and effectiveness of the alert resolution process that analysts are tasked with.

Similar to ThetaRay's standard automated customer screening, many of the key system components are also used in customer manual screening. The user for example, can select to make manual screening searches by setting a match score percentage parameter and screening against various available list categories and target customer entity types.

Note: Customer Manual Screening access is dependent on the user being allocated the appropriate role permission

11.13.2. Customer Manual Screening

1. From the IC Landing page - > Select matrix icon



2. From Module select pop-up select - Screening Manual Search (2)

The Screening Manual Search Landing screen is displayed as shown below.

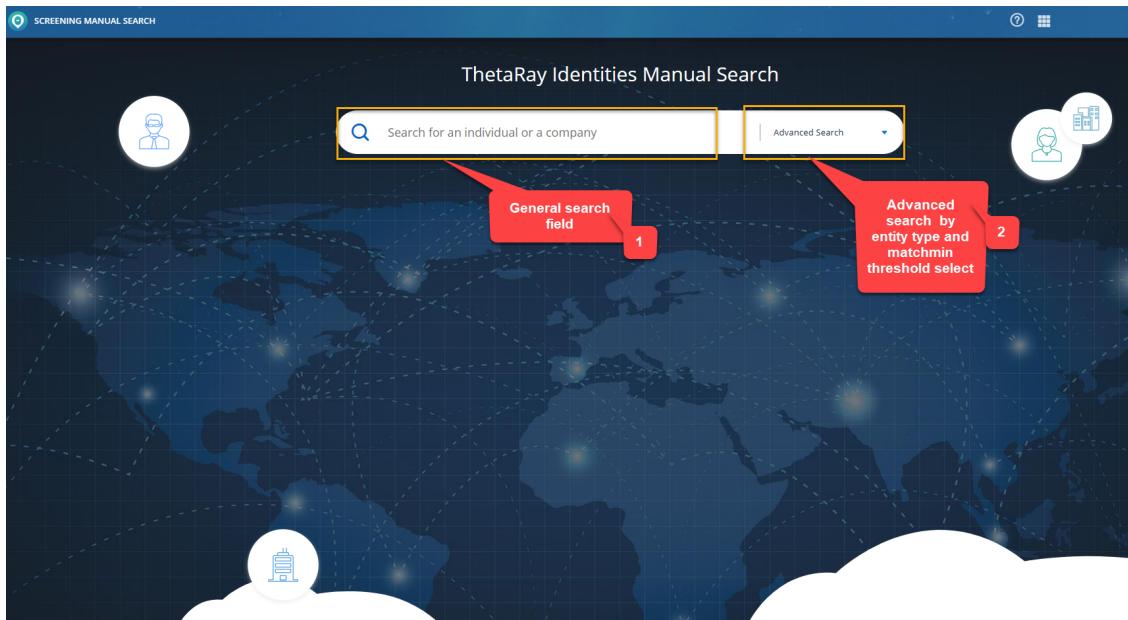


Figure 216: Screening manual Search Landing Screen

The Landing Screen provides two methods of manually searching for a customer entity:

1. **General Search Field** - enables the analyst to make search based simply on an individual name or company name
2. **Advanced Search** - enables a search to be made based on the info entered in (1) plus additional attributes, (entity type, threshold level and profile)
3. To display the **Advanced Search Menu** , click the 'down arrow' (3).

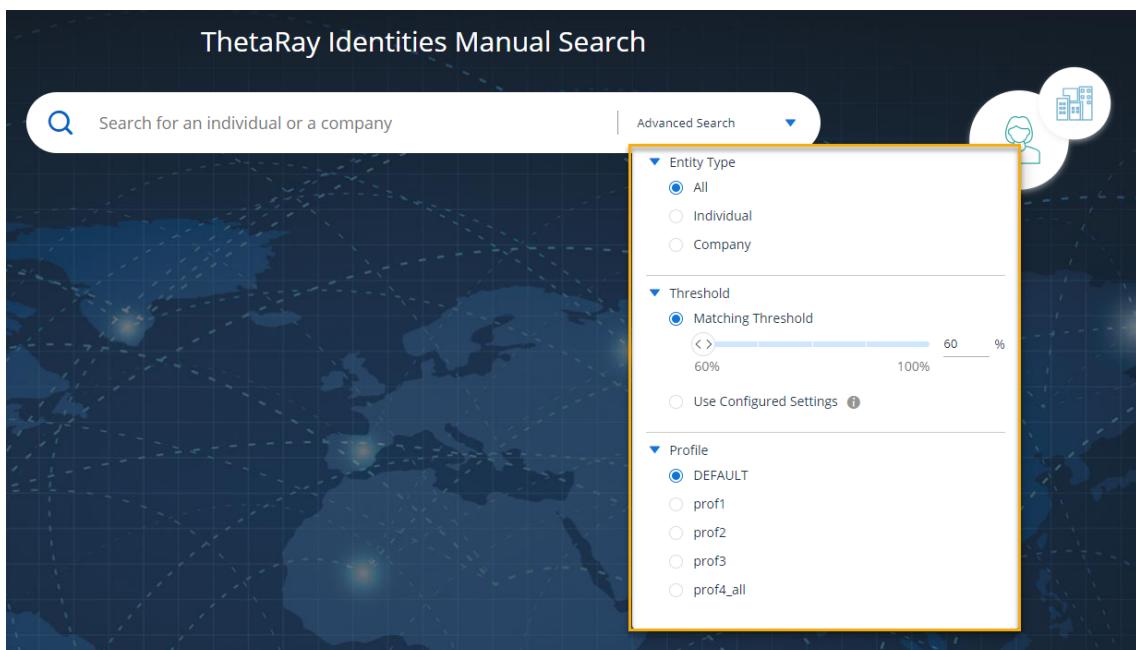


Figure 217: Advanced Search Options

11.13.2.1. Advanced Search Options

- **Entity Types** - Customer entity type parameters are aligned with standard 'automated' customer screening options.
- **Matching Thresholds** - As can be seen threshold filter settings can be set between 60 and 100%. (default 60%). In addition to a customizable threshold, an option to screen with the configured thresholds is available. Configured thresholds are set by the Screening Settings File and are utilized when screening via API.
- **Profile** - this option will be available in case the screening solution utilizes multiple profiles. The profile options will be available for selection, and only one profile can be used at a time. The results will be displayed according to the lists configured within the selected profile.

Search Results

If there are no search results, the following message is displayed.

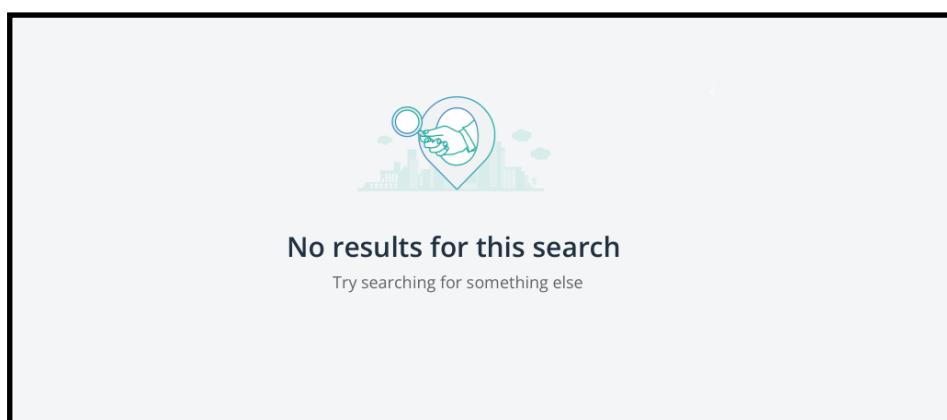


Figure 218: Displayed Message when Search does not Return any Results

List Name	List Description	Configured Threshold
EU	EU Financial Sanctions Files (FSF)	80%
UK	UK OFSI Consolidated List of Asset Free...	80%
UN	UN Security Council Consolidated Sanct...	80%
OFAC SDN	US OFAC Specially Designated National...	80%
OFAC CONS...	US OFAC Consolidated (non-SDN) List	80%

Figure 219: Example of Screened Lists

The screenshot shows the ThetaRay Identities Manual Search interface. The search bar contains 'muhammar gaddafi'. The results list three entries, each with a 'SANCTION' tag and an 85% match score. The interface includes a 'Filter by' section with 'SANCTION' selected, a 'Threshold 60%' button, and a 'Screened Lists' button. Navigation controls at the top right show '1 of 75 pages' with arrows for 'next' and 'previous'.

Figure 220: Manual Screening -Example Results Page

The screenshot shows the ThetaRay Results Display Screen. The search bar contains 'MARIAN'. The results list three entries: 'MARIAN' (Sanction, 95% match score), 'Karen Mok' (Politician, 83% match score), and 'Hana Marvanová' (Politician, 81% match score). The interface includes a 'Local Filter' button (3), a 'Threshold 80%' button, and a 'Number of pages returned' indicator (1). Navigation controls at the top right show '1 of 25 pages' with arrows for 'next' and 'previous'. A red callout (4) points to the 'Expand collapse all entities' button.

Figure 221: Example - Results Display Screen

To better understand the results screen let's take a closer look at the above figure.

- To aid clarity, the results screen displays only the first 3 entities returned from the 'hits' search results (1)
- The total number of pages are displayed with next > and previous , navigation between pages (1)
- Screened Lists - the screening lists used for the search can be viewed by hovering on "Screened Lists" as shown above. The lists displayed will be congruent with the profile selected. The Screened Lists will include the list names, descriptions and the specific threshold configured for each list. Please note that the thresholds listed here will be relevant for the search only if "Use Configured Settings" option is selected in the advanced settings.
- The item marked 'local' filter (3) enables the analyst to further analyze returned results by filtering by dynamic sanctioned groups such as, Sanction, Politician, Close Associate, Diplomat and a % static threshold filter.
 - To display the threshold filter (3), click the highlighted percentage link in the row of Filter by tabs.

Note: Clicking the 'Filter by' tags or moving the 'Matching threshold' level slide , dynamically applies the filter to the entities data displayed

Filter Note: In this feature, there are actually two threshold filters:

1. The initial 'hits' threshold filter as described above, filters against screening lists hits.
2. A local filter that enables the analyst to further filter against entities returned in the lists hits. If selecting the "Use Configured Settings" option, then the threshold displayed in this filter will be the minimum threshold from the configured lists.

To display the details of the entity hit either click the 'Expand' arrow as highlighted in (2) to expand the individual entity (2) or click the 'Expand All" to expand all the displayed entities.

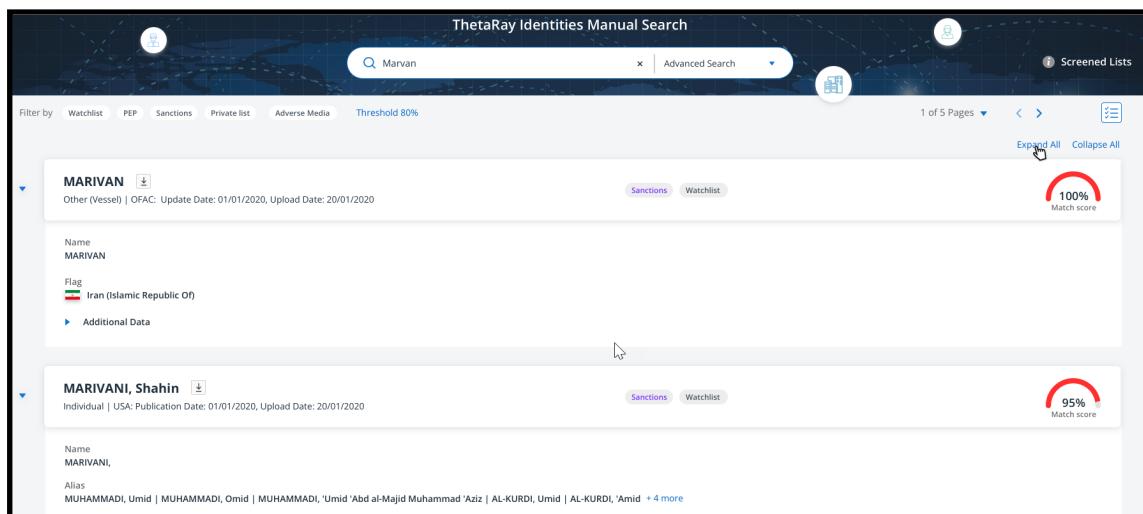
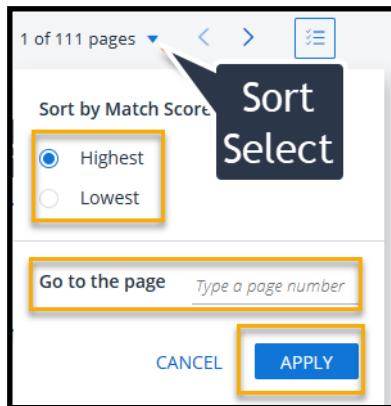


Figure 222: Example of the Expanding and Individual Entity

Sorting by highest to lowest match or lowest to highest.

1. Click the down arrow in the pages range display as shown below.



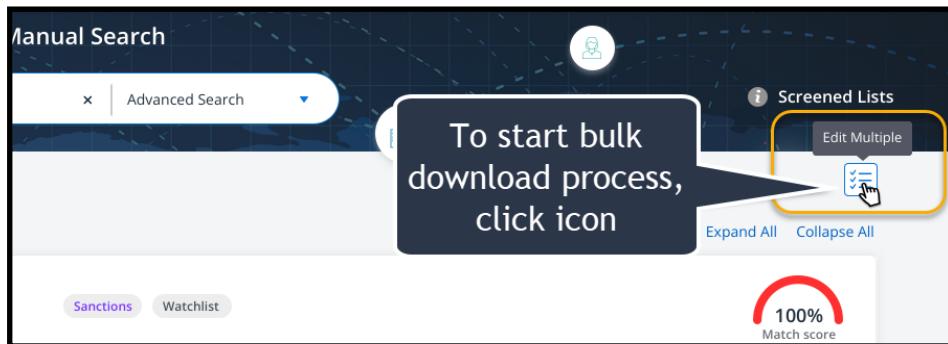
2. Either click on the radio button to select option or type the page number.
3. Click **APPLY** to display by selected option.

Download Search Results

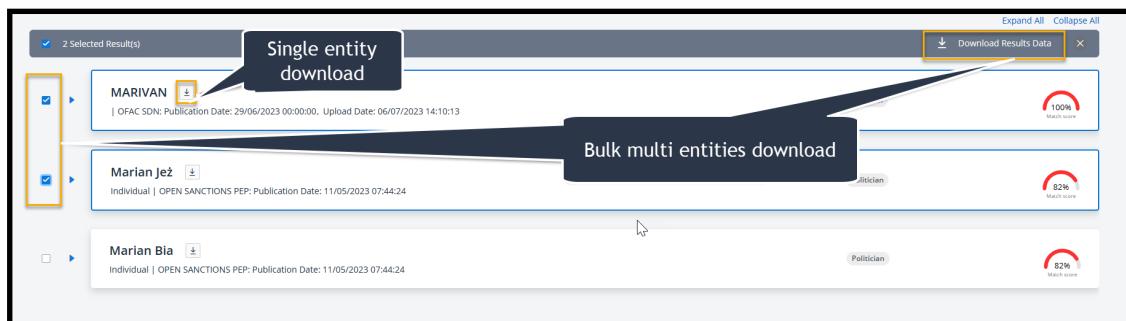
Download data is either on an individual basis or as bulk down to download multiple entities.

Downloads are made to the local machine in .csv format.

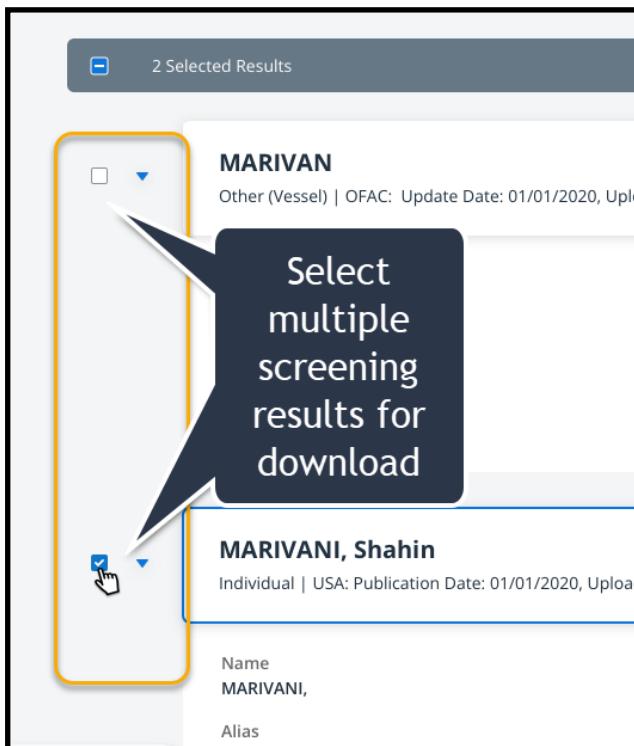
To select the bulk download option click the icon as shown below.



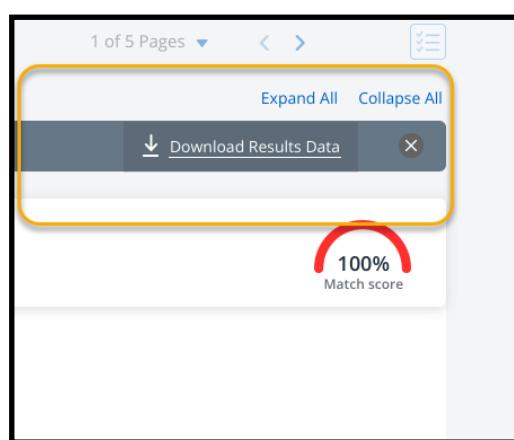
The bulk multi entity select option is displayed as shown below.



1. To download an individual entity, select the download icon as displayed above
2. To initiate bulk download, click the Edit Bulk Download icon and check the box next to each entity you wish to include in the bulk download as indicated below



3. Check the and click the **Download Results Data** button.



The download is completed, and a .csv Excel file is created in your local directory.

12. Adverse Media Screening Module

The adverse media optional screening module, provides the analyst with additional media related data, derived during the customer screening process. The available data for example could include information such as adverse media reports about the entity under investigation, whether it is an individual or a company.

This extra forensic evidence would be of value to the analyst in the task of reaching an appropriate alert resolution.

The remainder of this module description shows examples of adverse media information related to an individual or his / her related company.

12.1. Adverse Media

As part of customer screening investigation, adverse media is an optional service to Customer Screening clients. When included in the Customer Screening service, the individual or company under investigation undergoes an additional layer of screening. If such information is discovered it is added to the available forensic evidence as follows:

In the Investigation tabs bar, an additional tab is added as shown in the following example.

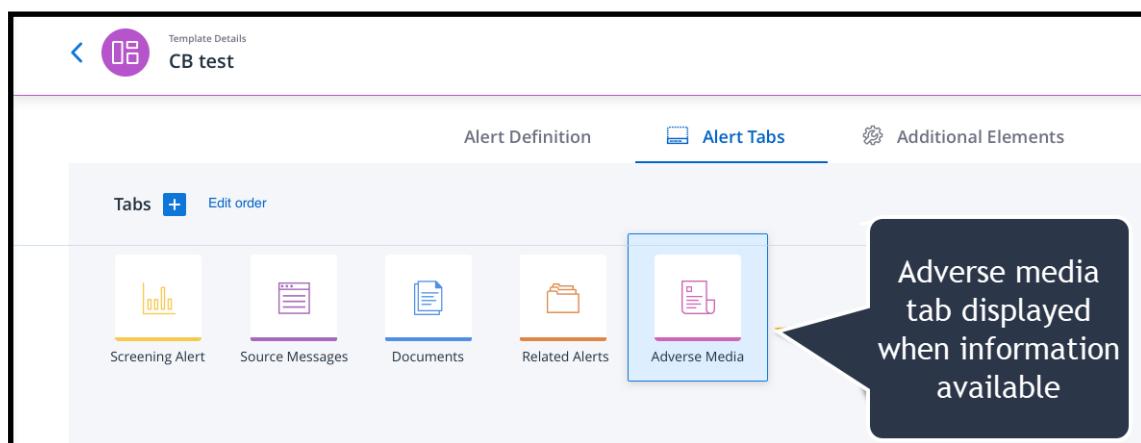


Figure 223: Example of Adverse Media Tab Displayed with Other General Tabs When Media Discovered

Figure 224: Example Adverse Media Data Related to an Individual, the Subject of an Alert

Figure 225: Example Adverse Media Data Related to a Company, the Subject of an Alert

12.2. Screening - Adverse Media (List Support)

Business Fields for each Dataset List:

Expected field name	Screena Field Name	Screening Field Type	Screening Model
Left Panel			

Expected field name	Screena Field Name	Screening Field Type	Screening Model
Image	targetData → medias → value images will be in type field PNG and JPG	List<IcMedias> medias	IcMedias: { String type; String value; }
Name	targetData → names → fullName	IcMatchName name;	fullName
Business registration number	targetData → identityDocuments → get "number" field by "type": "Registration Number", e.g. {String type : "Registration Number", String number: "1027700132195"}	List<IcMatchIdentityDocument> identityDocuments;	IcMatchIdentityDocument: { String type; String country; String description; String number; IcMatchDate dateOfIssue; IcMatchDate dateOfExpiry; }
Address	targetData → addresses	List<IcMatchAddress> addresses	IcMatchAddress: { String streetNumber; String streetName; String street; String poBox; String zipCode; String city; String state; String country; }

Expected field name	Screena Field Name	Screening Field Type	Screening Model
Country	targetData → addresses → country	List<IcMatchAddress> addresses	IcMatchAddress: { String streetNumber; String streetName; String street; String poBox; String zipCode; String city; String state; String country; }
Country of Incorporation	placesOfRegistry	List<IcMatchPlace> placesOfRegistry;	IcMatchPlace: { String city; String state; String country; }
Website	targetData → contactInformation → get value by "type": "Internet Site",	List<IcContactInformation> contactInformation;	IcContactInformation: { String type; String value; }
Category	targetData → categories	List<String> categories	
Description	targetData → additionalInformations → get Value by "type": "Note",	List<IcAdditionalInformation> additionalInformations	IcAdditionalInformation: { String type; String value; }

Expected field name	Screena Field Name	Screening Field Type	Screening Model
Related individuals	targetData → links	List<IcLink> links;	IcLink: { List<String> categories; List<String> subcategories: String status, List<IcPeriodsOfLink> periodsOfLink, List<IcLinkInformation> linkInformations, List<IcLinked> linked }, IcPeriodsOfLink: { String started; String ended; }, IcLinkInformation: { String type; String value; }, IcLinked: { String caption; }

Right panel (List of objects)

Title	targetData → sources → title	List<IcSource> sources;	IcSource: { String title String summary ????
Summary	targetData → sources → summary		String dateOfPublication String path
Capture Date			
Date of			

Expected field name	Screena Field Name	Screening Field Type	Screening Model
Publication URL	targetData-> sources ->??? targetData → sources → path		}

Individual Fields for each DatasetList:

Expected field name	Screena Field Name	Screening Field Type	Screening Model
Left Panel			
Image	targetData → medias → value images will be in type field PNG and JPG	List<IcMedias> medias	IcMedias: { String type; String value; }
First Name	targetData → names → givenName	IcMatchName name;	IcMatchName: { String fullName; String givenName;
Middle Name	targetData → names → fatherName (motherName) ??		String surname; String fatherName; String motherName; }
Last Name	targetData → names → surname		
Gender	targetData → sex	String gender;	

Expected field name	Screena Field Name	Screening Field Type	Screening Model
Birth Information	targetData → datesOfBirth	List<IcMatchDate> datesOfBirth;	IcMatchDate: { String date; }
Nationality	targetData → nationalities	List<IcMatchCountry> nationalities	IcMatchCountry: { String country; }
Address	targetData → addresses	List<IcMatchAddress> addresses	IcMatchAddress: { String streetNumber; String streetName; String street; String poBox; String zipCode; String city; String state; String country; }
Category	targetData → categories	List<String> categories	List<String> categories
Right panel (List of objects)			
		List<IcSource> sources;	

13. Transaction Screening Module

13.1. Introduction

Transaction Sanction screening is a process of verifying transactions made between a sender and a beneficiary (or beneficiaries). If either the sender or beneficiary is matched in the verification process the transaction is blocked in transit, and an alert is created requiring further investigation.

13.2. Overview

The transaction screening module is an Investigation Center 'add on' module that provides customers who have deployed the ThetaRay solution, the additional capability of reviewing and resolving matched transactional alerts

13.3. Purpose

The purpose of this Investigation Center chapter is to provide you, the end user, with detailed information and support regarding how to use your Investigation center, to resolve transaction screening alerts.

You will see, as you work through this chapter how the transaction screening resolution process differs from the process of resolving alerts sourced from other origins (example: transaction monitoring).

13.4. Contents

The guide also covers topics such as viewing new alert listings, examining related event types and forensic evidence messages and subsequently the process of closing the alert with a status of approved or blocked.

Topics that are common to other alert origins /sources are covered in the parent Investigation Center User guide and for the sake of brevity and documentation efficiency, are not repeated in this chapter.

Topics covered in this chapter include:

- Alert Lifecycle and Analyst Workflow
- Customer screening alert cards
- Customer screening Risk Details
- Customer screening alerts - resolution process

Let's in the following sections, explore how to resolve the transaction screening alerts that populate your Investigation Center case manager.

13.5. Analyst's Screening Alert - Lifecycle and Workflow

The process of resolving screening alerts requires following a specific Alert State Lifecycle analytical flow according to a set default BPMN formatted workflow. This section of the user guide shows both the lifecycle as an analytical block image and the default workflow as a BPMN diagram. The following diagrams are applicable to both Transaction and Customer use cases.

13.5.1. Alert State Lifecycle

The following lifecycle diagram displayed below shows the analytical logic path the alert takes from the **New** to the **Closed** state. New alerts are either assigned to the analyst by the team leader/ supervisor or pulled by the analyst from the repository of new alerts. Depending on the level of alert forensic information collected / available, the alert can be take one of the following states:

- **Approved** and then closed
- **Blocked** and then closed
- **On Hold** (till sufficient forensic evidence gathered)

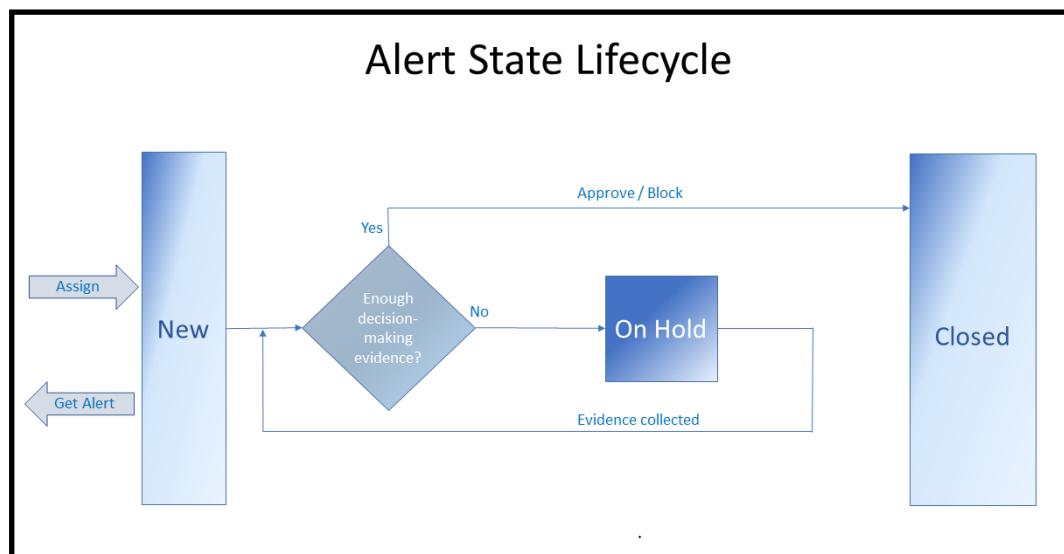


Figure 226: Example - Screening Alert State Lifecycle, as it Pertains to Resolving Screening Alerts

13.5.2. Alert Default Workflow

The screening workflow diagram displayed below shows the default path the new alert takes as it investigated and resolved. The diagram elements displayed include manual and system steps that decide the path the alert takes until resolution.

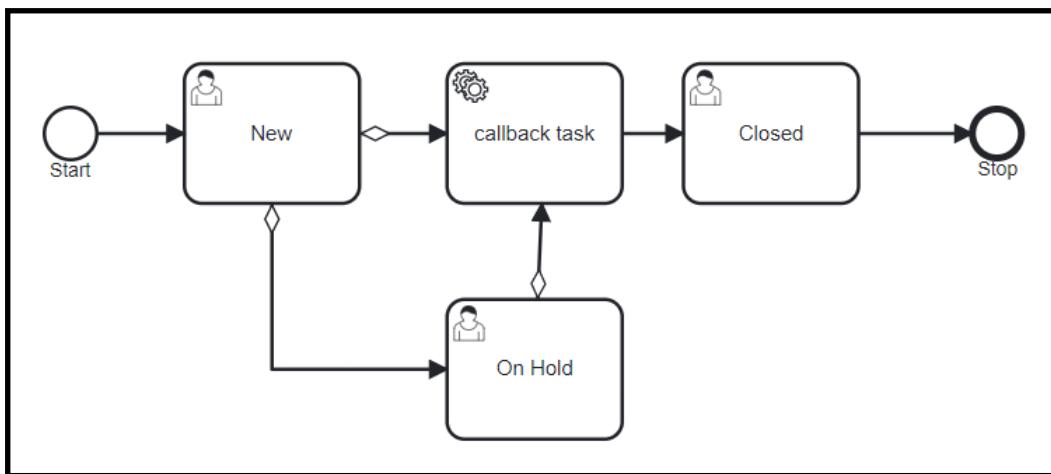


Figure 227: Default Workflow Shown as a collection of BPMN Elements with Process States from Start to End

13.5.3. Whitelisted Call-back Screening Information

Additionally, as part of the screening workflow, call back tasks are used to provide feedback regarding maintenance of a whitelisted list of customers who subsequently do not require investigation in future screening matches.

13.6. Accessing IC Transaction Screening Module

Access to Investigation Center (IC) Transaction screening alerts module is available to company personnel (for example: analyst or supervisor, with the appropriate access permissions).

➤ To view list of Transaction Screening alerts:

1. From Investigation Center login -> filters -> origins, select to view only Transaction screening alerts.

Note: If you are experiencing login or access issues, please contact ThetaRay customer support.

13.7. Investigation Center - Transaction Screening - Landing Screen

High level overview of the elements displayed on the Transaction Screening alerts list landing page:



Note: If some of the tagged items are not covered in detail in this screening add-on supplementary chapter, for more information please refer to the Investigation Center User Guide - Latest version.

Transaction Screening Icon (1)

Icon that indicates type of screening alert.

Screening alert card attributes (2)

Alert card key attributes:

- Alert unique id number- An identity number that uniquely identifies the alert
- Created - The date on which the alert was identified and created
- Total number of 'hits' - The total number of matched from the various lists queried

Summary of alert specific details (3)

The information shown on the card varies depending on the usecase

Alert status (4)

Possible Alert States:

- NEW
- STATE_NEW
- On_HOLD
- CLOSED

Match Score (5)

The matched score is an integral part of the information displayed on the alert card. The match score (a number between 1 and 99), reflects by number weight and graph color intensity , an indication of the degree of certainty to which the displayed match score rating is supported. **Match Score - Breakdown (5a)**

If adjustments are applied to the matching process, the 'Score breakdown' link will appear next to the match score. This feature provides detailed information on how the final match score with adjustments is calculated.

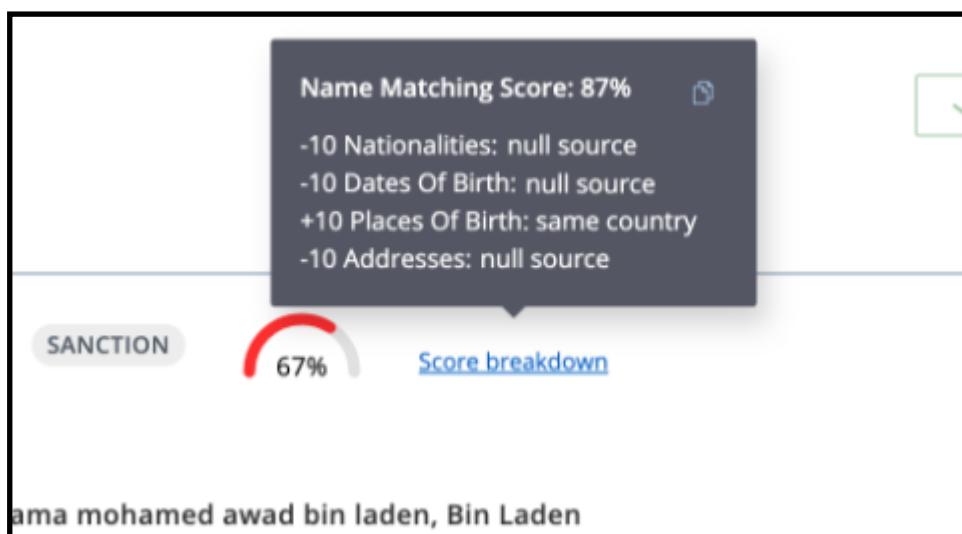
Clicking on a displayed 'Score Breakdown Link', displays the following information:

- Name Matching Score: Displays the name similarity score as a percentage.
- Attribute Adjustments: Lists each attribute that was considered in the matching process, along with the adjustment values applied. These adjustments can be positive or negative and are based on the type of match of secondary attributes.

For example:

- -10 Nationalities: null source: A negative adjustment for missing nationalities.
- -10 Dates Of Birth: null source: A negative adjustment for missing dates of birth.
- +10 Places of Birth: same country: A positive adjustment for a match places of birth in the same country.
- -10 Addresses: null source: A negative adjustment for matching addresses in the same subregion.

A practical example of a breakdown popup is shown below.



Note: Additionally, please notice the "Copy" icon, depicted as two overlapping papers on the upper right area of the popup. Users can utilize this functionality to duplicate score breakdown data for further analysis or sharing purposes.

Sort by(6)

The Alerts Screen List 'Sort by' function provides the ability where the user can order the displayed alert cards by decending or descending order. Once the option is selected and confirmed, the alerts list is ordered accordingly.

Note: As with filters, the 'sort by' function uses a global design which means that some of the parameters not supported in screening, will return an empty state.

13.8. Tab Navigation Bar

The Tab Navigation Bar provides access to the various tabs set for your screening solution IC deployment.

If the deployment is new, only system tabs are displayed by default. These are of the static type and as such are immutable.

The default system tabs for Transaction screening - provided by default are:

- Screening Alert
- Source Messages
- Documents
- Related Alerts
- Entity Resolution (if deployed)
- Notes
- History

An example of the Alerts Tab Navigation Bar with static system tabs is shown in the following figure.



Figure 228: Example navigation Bar for Screening Solution with Default and Optional System Tabs

For more details on working with:

- Documents
- Related Alerts
- Notes (Apart from notes that the analyst can add to any alert resolution case (via auto text templates etc., mandatory notes, created during an investigation (e.g. On Hold Approve, Block etc, are also posted to the Notes tab)
- History

Refer to the Investigation Center User Guide

If your particular deployment requires additional tabs, these can be created as custom tabs and after creation by a Business/ admin user in *Investigation Settings* and added as dynamic tabs to the Tab Navigation bar.

Note: As some of the available modules are optional, if your deployment does not include these, they will appear greyed out on the navigation bar.

13.9. Transaction Screening Alerts Risk Tab

In transaction screening deployments, the Screening Alerts tab provides the analyst/supervisor with the core functionality to manage the alert investigation and its closing resolution.

13.9.1. Alert States

The alert process flow includes one of the following three states:

- New
- On Hold
- Closing Resolution

13.9.1.1. New State

Every new screening alert that populates the Investigation Center automatically is assigned the New State.

To start the investigation / resolution process a system analyst / supervisor is required to click the Get alert link to assign the alert to him/her self.

13.9.1.2. On Hold State

In the alert investigation process, if there is a delay in any of the investigation tracks, the investigation user can evoke the 'On Hold' state to the alert. The various reasons for assigning the On Hold state are as follows::

- Awaiting further information from a customer
- Awaiting further information from a banking partner
- Pending manager review
- Further investigation required
- Other

Additionally when assigning the alert to the 'On Hold' state a mandatory description is required.

13.9.1.3. Closing Resolution State - Resolution Rule

The closing resolution defines whether the transaction is approved or blocked. The process requires the investigator to:

'sign off' on each of the transactions event types.

The final alert screening resolution is governed by the following rule:

"Only if all events are 'signed off' as *Approved* is the transaction closed as approved. If any of the events are blocked, then the transaction is closed as *Blocked*."

Note: When an alert resolution is finally made the alert cannot be closed until a mandatory reason for closure is provided. For more information refer to [Transaction Screening Alerts Risk Tab](#)

In general a maximum of seven events can exist, but this number can vary depending on the transaction and on the specific use case being deployed.

The seven basic events are as follows:

Transaction Screening – Originator Name

- Transaction Screening – Beneficiary Name
- Transaction Screening – Originator Bank
- Transaction Screening – Beneficiary Bank
- Transaction Screening – Agent
- Transaction Screening – Merchant
- Transaction Screening – Transaction Reference

13.9.2. Working with the Screening Alert Resolution Process

When the alert ID is selected from the Alert List the Alert Tab is opened displaying the events related to the transaction and a copy of the associated alert card as shown in the following example figure:

The screenshot shows the Transaction Screening Alert Tab with the following annotations:

- Alert attribute (2)**: Points to the list of alerts on the left, including "transaction-sc-mp_000030" and "transaction-sc-mp_000031".
- Alert specific details (3)**: Points to the details of the selected alert "transaction-sc-mp_000030", which includes "Created: 07/07/2023 16:02:13" and "Total number of hits: 2".
- Sort by ascending or descending match scores (6)**: Points to the sorting dropdown and the list of alerts.
- Alert status (4)**: Points to the status section showing "Unassigned" and a "Matched score (5)" of 100%.
- Matched score (5)**: Points to the percentage value in the status section.

Figure 229: Example Transaction Screening Alert Tab Showing Events Related to Transaction, and Card Details

13.9.2.1. Investigation and Resolution Process - High Level

To better understand how to work with the Screening Alert's tab, let's use the following example to show the overall work process the investigator would typically undertake.

From the Screening alert tab each event has a dedicated cursor arrow that when clicked, reveals drill down information about each event.

1. For example, clicking the arrow next to the Originator event in our example, displays the following detail as shown in the following figure.

The screenshot shows the 'transaction-sc-mp_000032' alert tab. It displays 'Customer Data' and 'Transaction Data' on the left, and a 'Matched List Data - USA' section on the right. A callout box highlights the 'Alert data summarized in alert card is displayed in the 'hit' data block'. Another callout box points to the 'Data block showing details of best matched 'hit''. A third callout box points to the 'Navigation between matched results' section. A fourth callout box points to the 'Expand or collapse viewable fields' section. A fifth callout box points to the 'This data block is scrollable for comparison with hit data' section. A sixth callout box points to the 'This data block is scrollable for comparison with TX data' section. A seventh callout box points to the 'Expand All / Collapse All' button. A eighth callout box points to the '100% Match score' indicator.

Figure 230: Alert Details Dropdown showing ,Transaction Data and Matched Hit lists Data Options

To help understand how the dropdown detail information is used in alert approval or block, let's zoom in on the Screening List details shown below.

- As can be seen, the Screening List that matched our transaction 'Bad actor' in any of the events is displayed (1).
- In section (2) other forensic detail about the transaction is displayed including:
 - Originator match name
 - Originator aliases (if detected)
 - Date of Birth
 - Nationality
 - Place of birth
 - Match Score (3)

- Gender (4)

13.9.2.2. Identification Types

Re the identification types that can be returned in a transaction screening query, there are two types:

- Individual
- Organization

Individual type

Following are a few examples of Individual Identification types

▼ Identification

Identification Type
individual

Identity Documents - Type
Passport

Identity Documents - Number
472310082

Identity Documents - Country
 Myanmar

Identity Documents - Description
Test Description

Identity Documents - Dates Of Issue
08/05/2005

Identity Documents - Dates Of Expiry
08/05/2005

Identity Documents - Places Of Issue - City
MM

Identity Documents - Places Of Issue - State
MM

Identity Documents - Places Of Issue - Country
 Myanmar

Identity Documents - Places Of Issue - Place Name
MM

Gender
Male

Dates Of Birth
08/05/1955

Places Of Birth - City
MM

Places Of Birth - State
MM

Places Of Birth - Country
 Myanmar

Figure 231: Example Core Identification Data Section Block (individual)

Country Of Residence	
Myanmar	
Screening Entity Type	
individual	
Id	
fake_92652195328932175887	
Address	
MM	

Figure 232: Example Country of Residence Data Block

High Risk Country	Name
	gim seek chul
	Full Name
	gim seek chul
	Last Name
	SOK CHOL
	First Name
	KIM
	Ip Address
	39057718762082561696
	▼ Identification
	Identification Type
	individual
	Identity Documents - Type
	Passport
	Identity Documents - Number
	472310082
	Identity Documents - Country
	Myanmar
	Identity Documents - Description
	Test Description
	Identity Documents - Dates Of Issue
	08/05/2005
	Identity Documents - Dates Of Expiry
	08/05/2005
	Identity Documents - Places Of Issue - City
	MM
	Identity Documents - Places Of Issue - State
	MM
	Identity Documents - Places Of Issue - Country
	Myanmar
	Identity Documents - Places Of Issue - Place Name
	MM

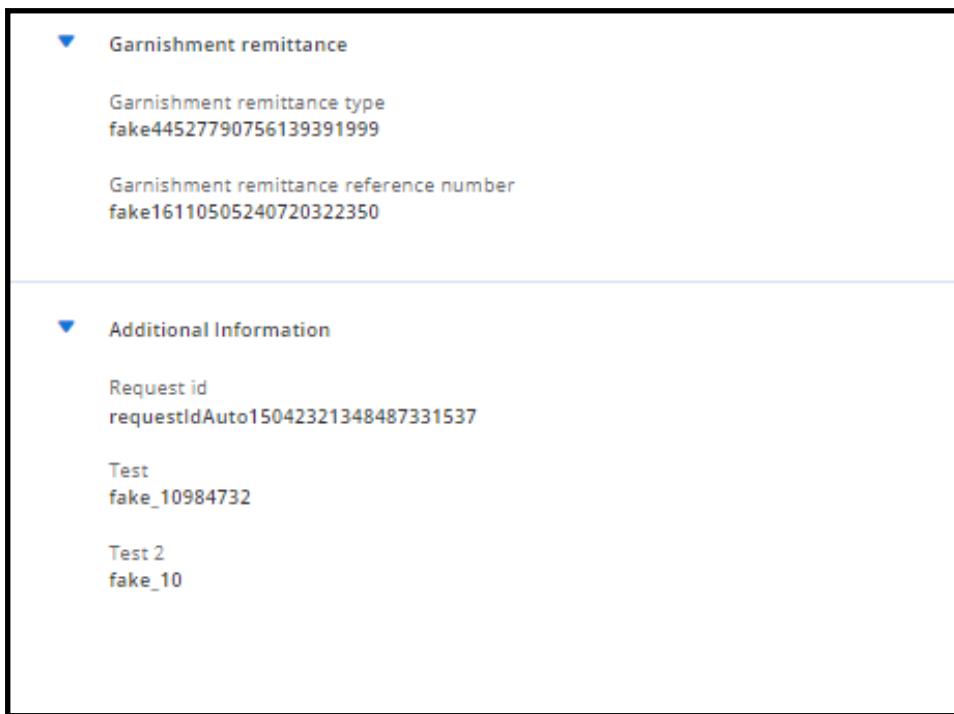
Figure 233: Example High Risk Country - Data Block

<i>Previous Instructing Agent</i>	Name
1	ABDUL MANAN
	Screening Entity Type
	individual
	Id
	fake_36712427403373923799
	City
	Quetta
	Iban
	123456789
	Floor
	2
	Region
	Baluchistan Province
	Country
	<input checked="" type="checkbox"/> Pakistan
	Currency
	USD
	Member id
	44551447785
	Postal code
	1234
	Street name
	Kachray Road, Pashtunabad
	Building name
	Quetta
	Building number
	1
	Clearing system id
	45666987745

Figure 234: Example Previous Instructing Agent Data Block

<i>Narrative</i>	Creditor reference fake47991604415899825020
Remittance info	fake82319348815732261548
Related remittance info	fake35980089469666082430
Sender to receiver info	fake70221881656606162358
Category purpose	fake60038023361993733173
Remittance identification	fake67069828598758080633
Additional remittance information	fake58749868560329536938
▼ Creditor reference information	
Creditor reference information type	fake88336948959769072363
Creditor reference information reference	fake72410752191711198604
▼ Referred document information	
Referred document information type	fake12206965575696655603
Referred document information line details type	fake21929872024080613328
Referred document information line details number	fake31573065405766111701
Referred document information line details description	fake48309468681762202641
▼ Tax remittance	
Tax remittance administration zone	fake10008516710091322106

Figure 235: Example Narrative Data Block



Garnishment remittance

Garnishment remittance type
fake44527790756139391999

Garnishment remittance reference number
fake16110505240720322350

Additional Information

Request id
requestIdAuto15042321348487331537

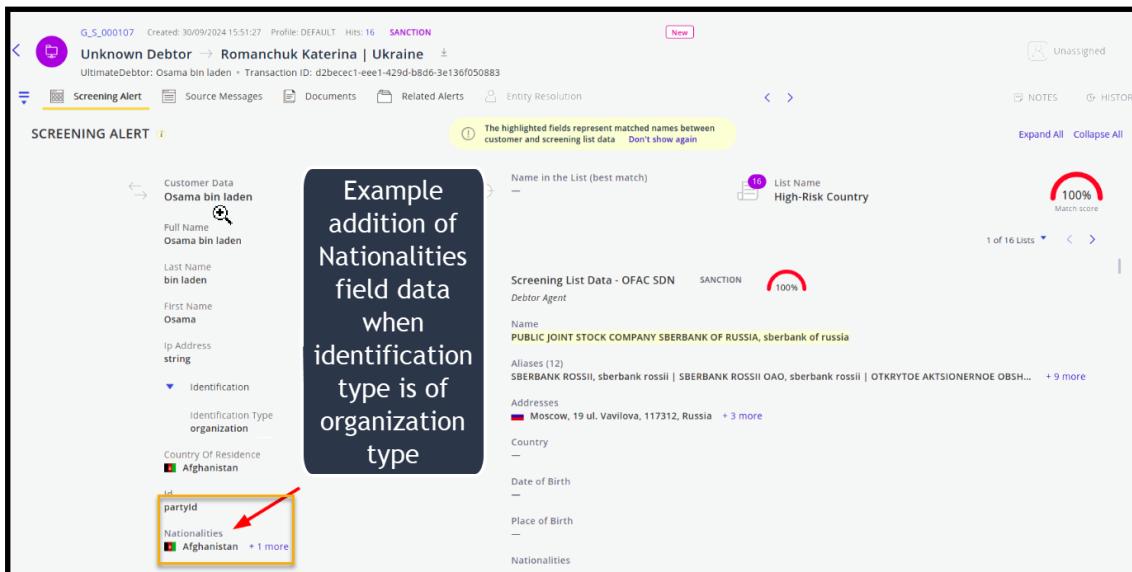
Test
fake_10984732

Test 2
fake_10

Figure 236: Example Garnishment Remittance and Additional Information

Organization Type

Organization types differ from Individual types in that they can sometimes represent a more suspicious group of 'bad players' that make up the organization. To aid the analyst in his /her alert resolution task, investigating such organizations, we now, where the customer type is detected as being of the organization type, include the nationality or nationalities of such organizations in the returned results. The following image shows an example of an organization type and the related nationality of the organization.



SCREENING ALERT

Customer Data
Osama bin laden

Full Name
Osama bin laden

Last Name
bin laden

First Name
Osama

Ip Address
string

Identification
Identification Type
organization

Country Of Residence
Afghanistan

partyId

Nationalities
Afghanistan + 1 more

Example addition of Nationalities field data when identification type is of organization type

Name in the List (best match)

List Name
High-Risk Country

Screening List Data - OFAC SDN SANCTION

Debtor Agent

Name
PUBLIC JOINT STOCK COMPANY SBERBANK OF RUSSIA, sberbank of russia

Aliases (12)
SBERBANK ROSSI, sberbank rossi | SBERBANK ROSSI OAO, sberbank rossi | OTKRYTOE AKTSIONERNOE OBSH...

Addresses
Moscow, 19 ul. Vavilova, 117312, Russia + 3 more

Country

Date of Birth

Place of Birth

Nationalities

Figure 237: Example - Organization Type with Nationality also Displayed

13.9.2.3. Event Sort by Function

- Event Sort by - enables listed alert screening events to be ordered by the default listing or by match score - descending order of priority.

13.9.2.4. Investigating Further Evidence

Before a decision is made on the event resolution the analyst should navigate to, and investigate the content of the other system tabs listed in the Navigation tab. This will provide a broader and clearer picture of the transactional risk.

For example the Source Messages tab contains all the raw data messages that are associated with the transaction and the documents or notes tab may contain further forensic evidence to substantiate the approve or block decision.

These other system tabs are listed and described in the Tab Navigation topic.

13.9.3. Alert Resolution Process

In general, resolving a customer screening alert includes the following steps:

1. Investigating each screening account type using the following guidelines:
 - a. Viewing and comparing known customer data with data retrieved with matched hits.
 - b. Check details retrieved on other hits by navigating thru the hits.

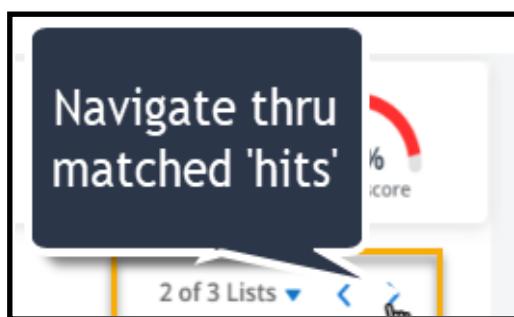


Figure 238: Navigate from Hit to Hit to Examine More Data

- c. You can also sort the order of matches scores in ascending or descending order

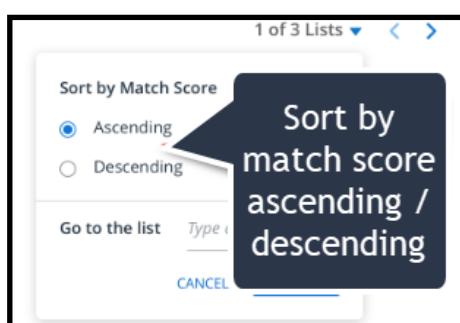


Figure 239: Sort by Matched Score

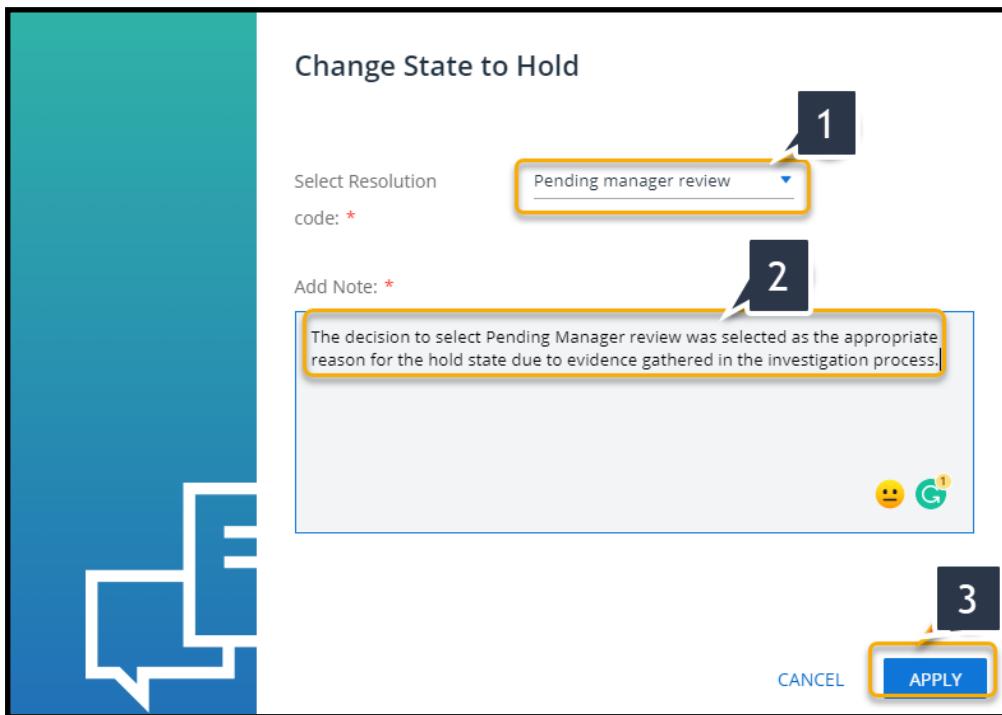


Figure 240: Example of Reason and Description for changing state to "On Hold"

2. Click APPLY (3).

Note: When the required information is received, clicking either the approve or block link for the alert removes the 'On Hold' state and closes just that particular event.

13.9.4. Event and Alert Closure Resolution

After the event Investigation process is complete, it is required to define if the event is approved or blocked

1. When all forensic evidence has been gathered, an '**approve**' or '**block**' decision is required for each screening account type.

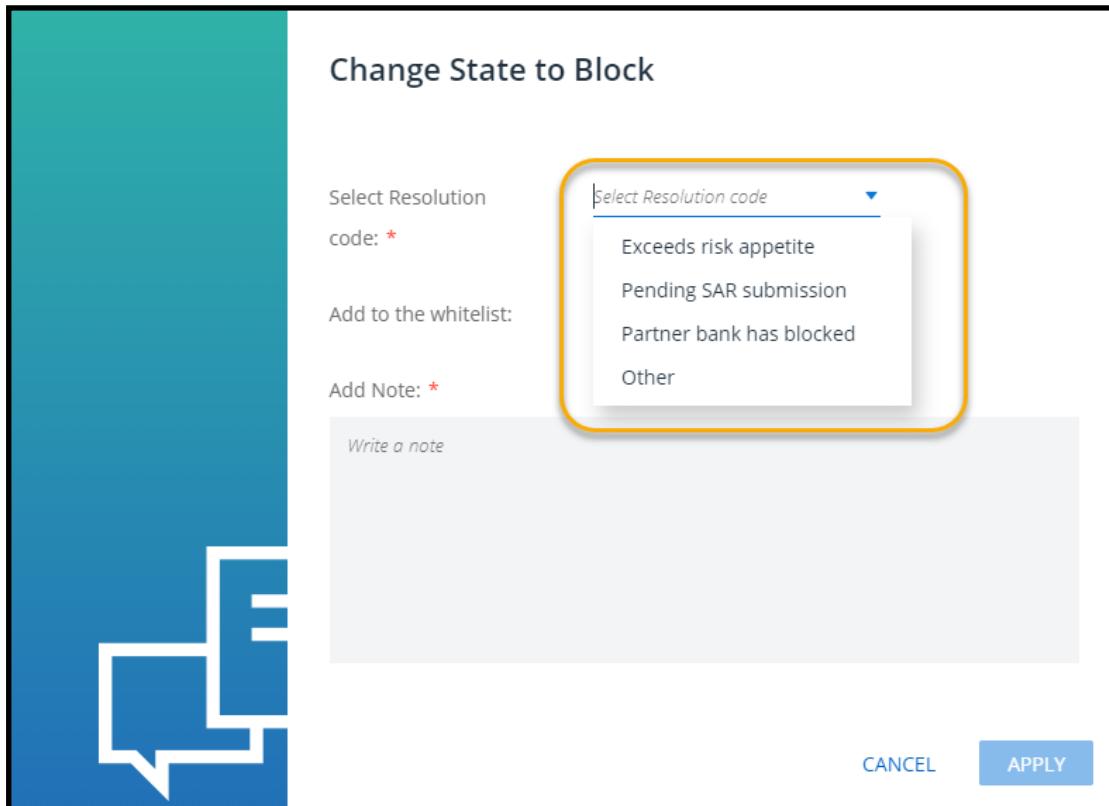


Figure 241: Approve or Block Required for each , Matched Event

13.9.4.1. Requirement to Provide a Reason for Selected Resolution

Regardless of whether or not an alert is finally approved or blocked, a mandatory reason for the selected resolution must be provided as part of the alert closure procedure. For more information on the event resolution process refer to the rule covering alert final resolution detailed in the section [Transaction Screening Alerts Risk Tab](#)

The following figures show examples of resolutions, both approved and blocked, including preset reasons and examples of 'free' text descriptions.



Change State to Block

Select Resolution code: *

Add to the whitelist:

Add Note: *

Resolution code:

- Exceeds risk appetite
- Pending SAR submission
- Partner bank has blocked
- Other

Write a note

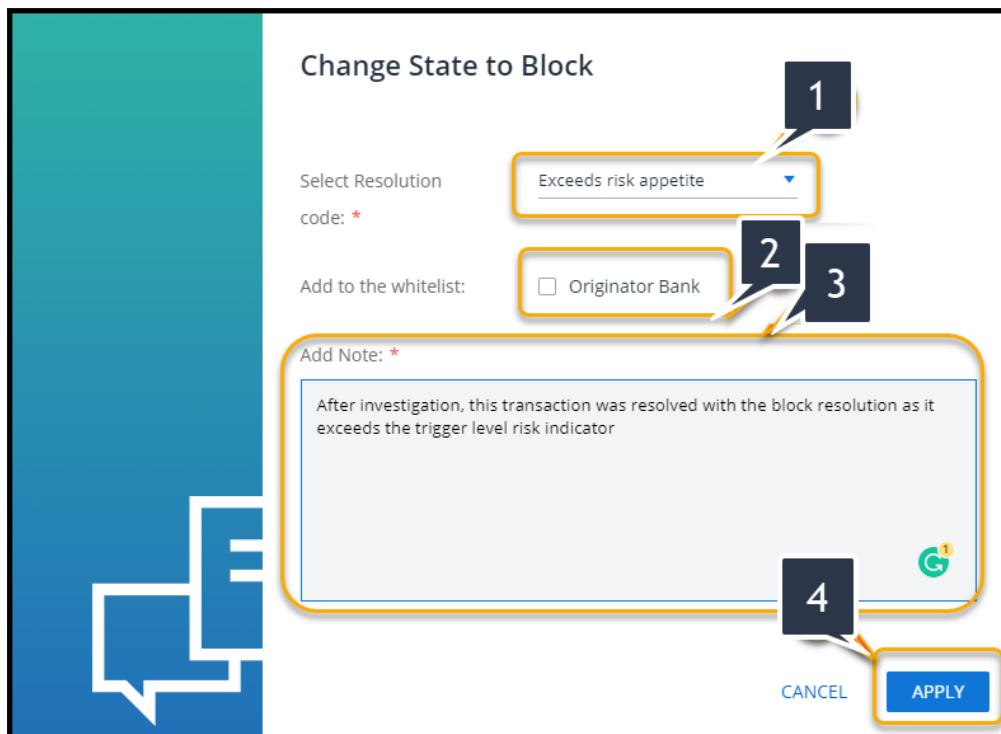
CANCEL APPLY

Figure 242: Example of Block Resolution State and Possible Resolution Codes

Once change state to block is selected you are required to:

- Provide a Resolution (1).
- Select whether to add the transaction bank to the whitelist or not (2).
- Provide a description (free text) supporting the resolution (3).
- Click APPLY (4).

The following figure shows the Change State to Block form and example completion



1

2

3

4

Cancel Apply

Change State to Block

Select Resolution code: *

Exceeds risk appetite

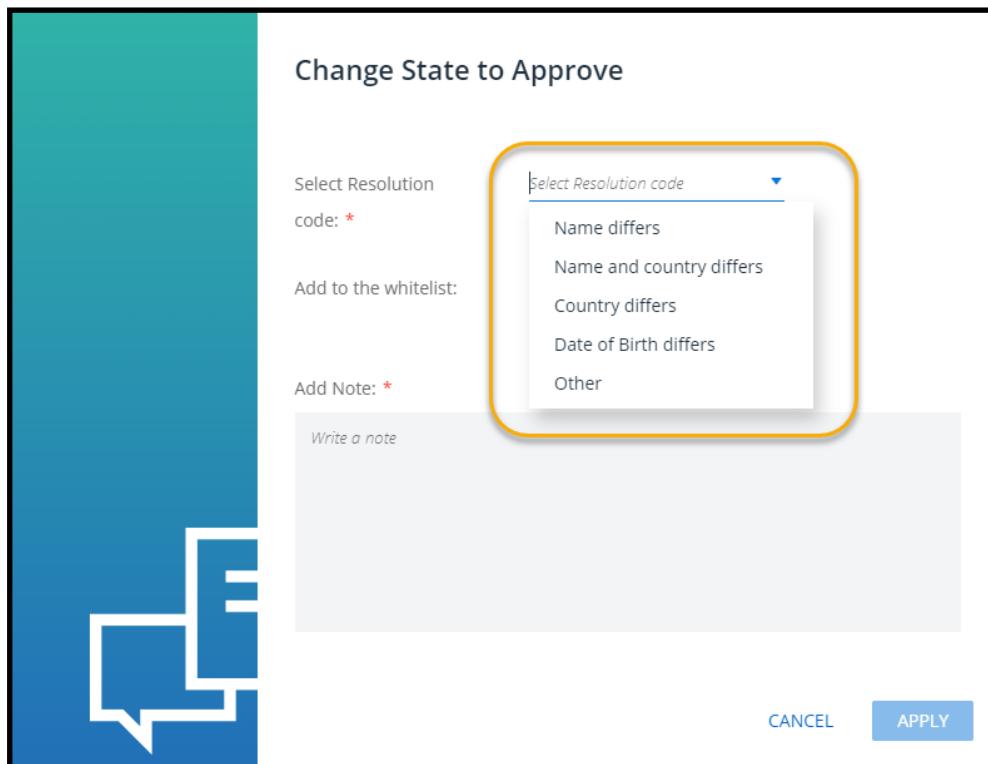
Add to the whitelist:

Originator Bank

Add Note: *

After investigation, this transaction was resolved with the block resolution as it exceeds the trigger level risk indicator

Figure 243: Example -Block resolution , Add Bank to Whitelist, Description and APPLY Confirmation



Cancel Apply

Change State to Approve

Select Resolution code: *

Select Resolution code

- Name differs
- Name and country differs
- Country differs
- Date of Birth differs
- Other

Add Note: *

Write a note

Figure 244: Example of Approve Resolution State and Possible Resolution Codes

If change state to approve is selected:

- Provide a Resolution (1).

- Select whether to add the transaction bank and /or the Transaction Reference to the whitelist or not (2).
- Provide a description (free text) supporting the resolution (3).
- Click APPLY (4).

The following figure shows the Change State to Approve Resolution

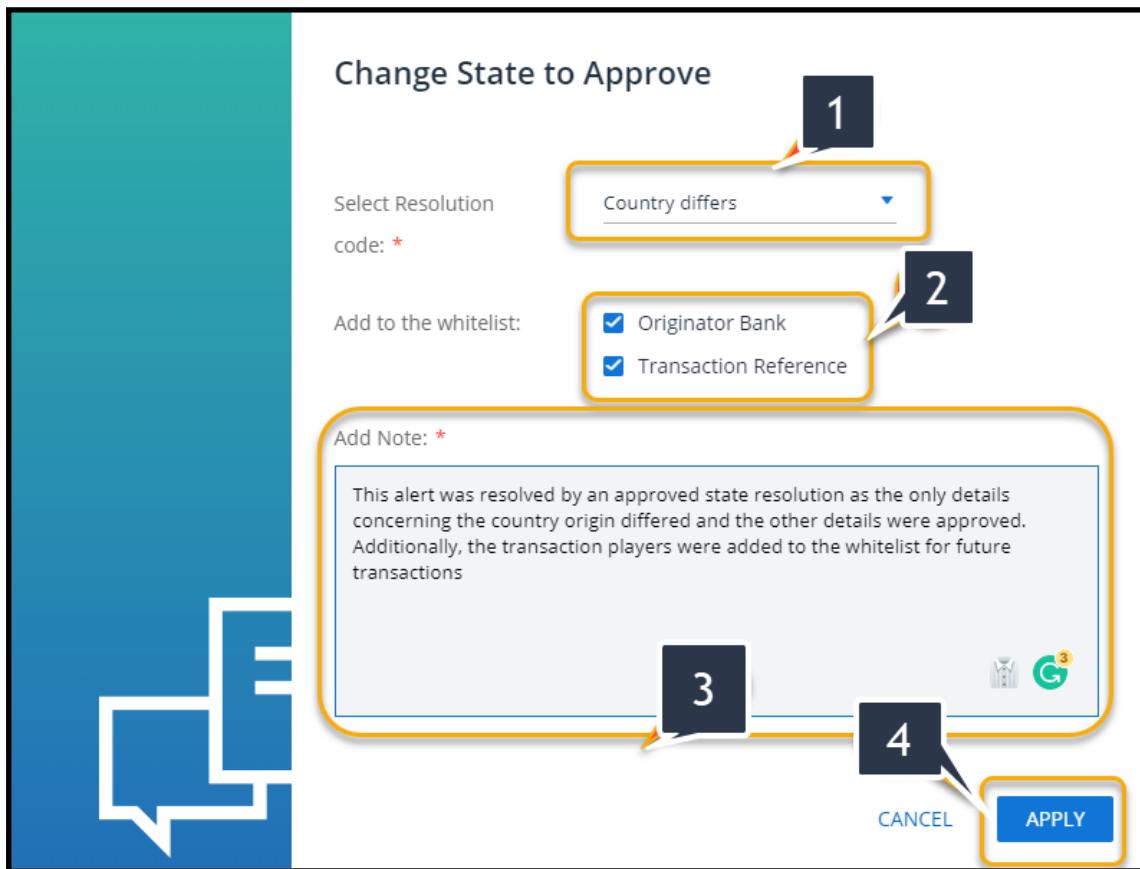


Figure 245: Example Alert Approved with Reason (1), Whitelisting (2), Description text (3) and APPLY(4)

13.9.4.2. Transaction Screening - Additional UI Information

Note: If the event is approved it is displayed bordered in green as shown in the following figure.



Figure 246: Example of Event Approved (Green Border)

Note: If any event is blocked it is displayed bordered in red as shown in the following figure.



Figure 247: Example of Event Blocked (Red Border)

Closed message is shown in the following figure.



13.10. Source Messages Tab - Transaction Screening

The Source Messages tab contains a list of Transaction Screening messages that are associated with each screening alert selected in the Alerts List for further investigation.

These messages provide the analyst with an additional source of forensic evidence when completing the task of investigating alert event types and making an informed decision on the closing resolution (approve or block).

» To select the Source Messages Tab:

1. From the Navigation bar, click the Source messages Tab as shown in the following figure.

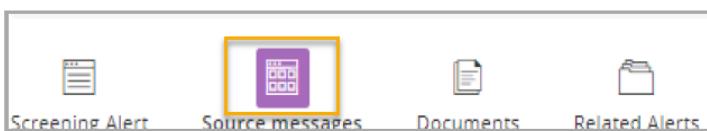
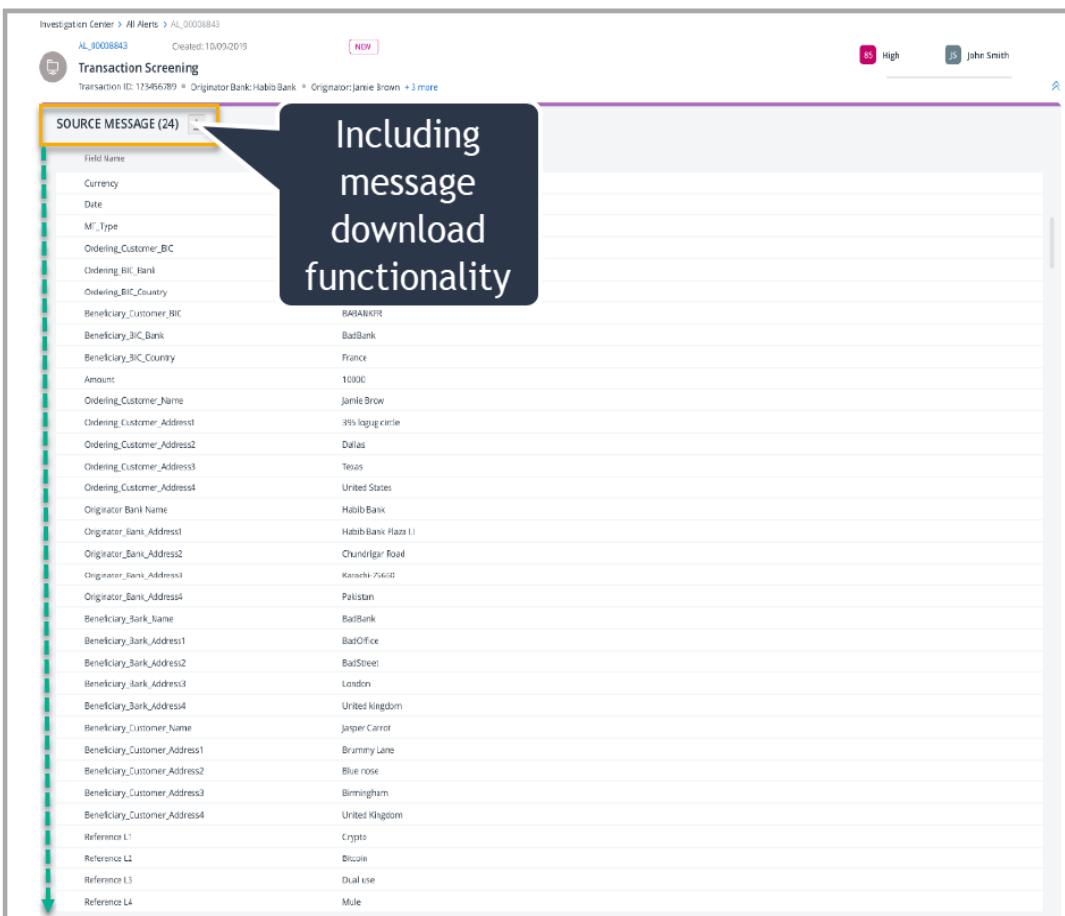


Figure 248: Source Messages Select Tab in Navigation Bar

The messages tab opens and displays a list of source messages similar to that shown in the following example figure.



The screenshot shows a table titled 'SOURCE MESSAGE (24)' with two columns: 'Field Name' and 'Transaction Data'. The table lists various transaction details. A callout box with a dark blue background and white text is overlaid on the table, containing the text 'Including message download functionality'. The table has a light gray background with alternating row colors. The 'Field Name' column includes fields like 'Field Name', 'Currency', 'Date', 'Mf_Type', 'Ordering_Customer_BIC', 'Ordering_BIC_Bank', 'Ordering_BIC_Country', 'Beneficiary_Customer_BIC', 'Beneficiary_BIC_Bank', 'Beneficiary_BIC_Country', 'Amount', 'Ordering_Customer_Name', 'Ordering_Customer_Address1', 'Ordering_Customer_Address2', 'Ordering_Customer_Address3', 'Ordering_Customer_Address4', 'Originator Bank Name', 'Originator_Bank_Address1', 'Originator_Bank_Address2', 'Originator_Bank_Address3', 'Originator_Bank_Address4', 'Beneficiary_Bank_Name', 'Beneficiary_Bank_Address1', 'Beneficiary_Bank_Address2', 'Beneficiary_Bank_Address3', 'Beneficiary_Bank_Address4', 'Beneficiary_Customer_Name', 'Beneficiary_Customer_Address1', 'Beneficiary_Customer_Address2', 'Beneficiary_Customer_Address3', 'Beneficiary_Customer_Address4', 'Reference_L1', 'Reference_L2', 'Reference_L3', 'Reference_L4'. The 'Transaction Data' column contains values such as 'B444NFR', 'B444NFR', 'France', '10000', 'Jamie Brown', '395 Jagger Circle', 'Dallas', 'Texas', 'United States', 'Halib Bank', 'Halib Bank Plaza 11', 'Chundrigar Road', 'Karnihi 75610', 'Pakistan', 'B40Office', 'B40Street', 'London', 'United Kingdom', 'Jasper Carrot', 'Brammy Lane', 'Blue nose', 'Birmingham', 'United Kingdom', 'Crypto', 'Bitcoin', 'Dual use', 'Mule'.

Figure 249: Example list of Source Messages in the Source Messages Tab

As can be seen in the above example a copy of the alert card containing alert details is included above the listed messages as well as the total number of associated messages for this particular alert.

The *Field* column holds a list of useful transaction related data such as currency, date, amount etc. and the *Transaction Data* column holds the corresponding value.

A download icon is also included. This enables you as an example, to download the list, copy to a third party text editor, highlight specific message rows and then upload the edited copy to the *Documents Tab* as additional forensic evidence.

14. Customer Risk Assessment (CRA) User Guide

14.1. CRA Introduction

CRA or Customer Risk Assessment, is a Thetaray product that provides financial institutions with a dedicated case manager containing CRA type alerts requiring investigation. These alerts are triggered and created by available risk data about a particular individual or company entity.

This initial phase #1 of the CRA offering, includes the following features:

- Core IC module supporting alert investigation and resolution
- CRA data reporting including automatic report generation after each CRA run or On - demand reports generation and download.

14.2. Purpose and Scope

The content of this document describes how to work with the Customer Risk Assessment (CRA) alert resolution product. Although the CRA is a dedicated separate product, some of the common Investigation Center Case manager information is equally relevant to the other available IC modules (e.g. Transaction Monitoring, Transaction Screening and Customer Screening), to avoid unnecessary content duplication, this common information is described and included in the core chapters of the Investigation Center(IC) User Guide. So if you have any issues locating IC descriptions or simply want to know more about alert management, please refer to the Standard Investigation Center User Guide Contents. For more comprehensive theoretical information about the CRA product, please refer to the ***CRA Overview*** document.

Note: It is of course the prime intention of the ***Product Documentation Department*** to maintain as comprehensive as possible IC User Guide, so to that end we earnestly welcome your feedback on the provided content.

14.3. Customer Risk Assessment (CRA)- Reports

This CRA Reports sub module chapter, supports ThetaRay's CRA customers with managing gathered related detailed reports information available as part of the Customer Risk Assessment deployment.

Topics covered include:

- CRA overview
- Accessing CRA Reports module

- Automated reports and on-demand reports
- Filtering and Selecting Reports per Parameters & Downloading
- Selecting and viewing individual report details
- Data display sorting
- Downloading (all) very high severity reports

14.3.1. CRA Reports- Access, and General Functionality

Access to the Reports module is via the module icon as indicated in the following figure.

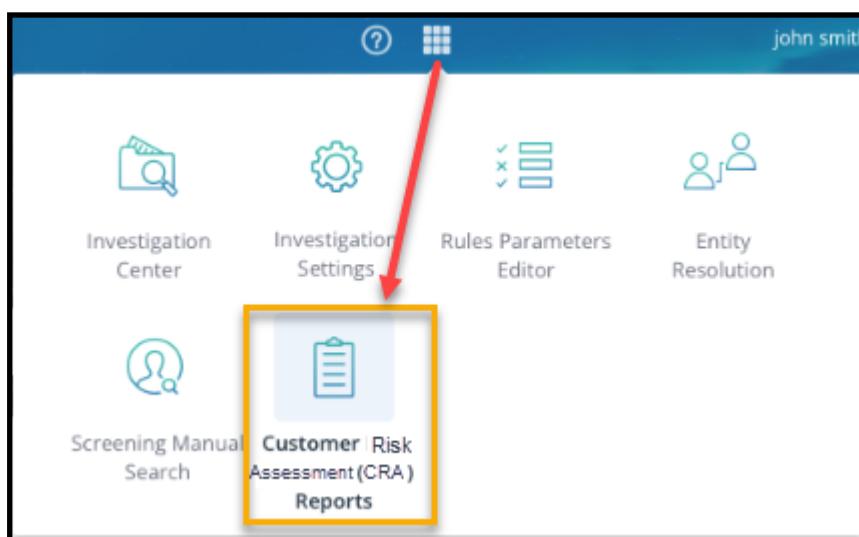


Figure 250: Customer Risk Assessment (CRA) Reports Module Selection

Selecting the highlighted CRA Reports icon option, displays an landing screen similar to the figure shown below.

14.3.1.1. Functionality Overview

On Access, two report tabs are available:

- **On Demand Reports** - For users requiring access to real-time reports, this tab presents an initial view of reports generated within the last 24 hours for all customers.
- **Download Automatic Reports** - Serving as a repository for automatic reports generated at the end of each risk assessment run.

Note: Reports display all details from the risk assessment run, including KYC data, risk indicators, weights and scores. Reports can be downloaded either in CSV or Excel format.

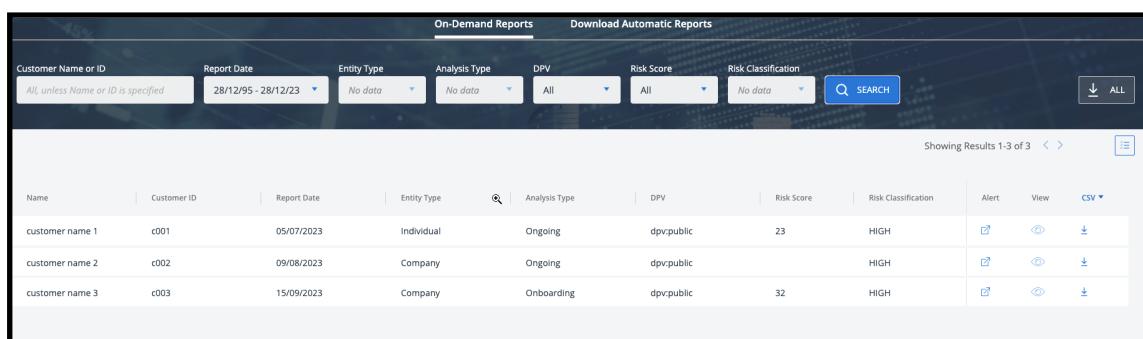
The following chapter provides more detail about report types and the CRA investigation procedure

14.3.2. Report Types

As mentioned in the previous chapter in the Reports module there are two report types available.

14.3.2.1. On Demand Reports

This default screen automatically shows on demand reports screen containing user reports from the last 24 hours. Dropdown filters at the top of the page allow for refined searches, which generate less results and so are easier to navigate.



The screenshot shows the 'On-Demand Reports' screen. At the top, there are dropdown filters for 'Customer Name or ID' (set to 'All, unless Name or ID is specified'), 'Report Date' (set to '28/12/95 - 28/12/23'), 'Entity Type' (set to 'No data'), 'Analysis Type' (set to 'No data'), 'DPV' (set to 'All'), 'Risk Score' (set to 'All'), 'Risk Classification' (set to 'No data'), and a 'SEARCH' button. To the right of the search button is a download icon labeled 'ALL'. Below the filters, a message says 'Showing Results 1-3 of 3'. A table follows, with columns: Name, Customer ID, Report Date, Entity Type, Analysis Type, DPV, Risk Score, Risk Classification, Alert, View, and CSV. The table contains three rows of data:

Name	Customer ID	Report Date	Entity Type	Analysis Type	DPV	Risk Score	Risk Classification	Alert	View	CSV
customer name 1	c001	05/07/2023	Individual	Ongoing	dpv:public	23	HIGH			
customer name 2	c002	09/08/2023	Company	Ongoing	dpv:public		HIGH			
customer name 3	c003	15/09/2023	Company	Onboarding	dpv:public	32	HIGH			

Figure 251: Example CRA On - Demand Landing Screen

14.3.2.2. Automated Reports

These are generated automatically and users can retrieve them via the minio link that they receive when the batch onboarding, ongoing runs are complete.

Although similar to the on- demand reports screen the main difference is due to the fact that automated reports are system created the only filter that can logically be applied is the time period filter (from - to) that enables the analyst to select a specific time period from which to query reports data.

Reclassification reports can also be excluded from automated reports generation, as indicated by the available 'Exclude Reclassification Report' check box as shown in the figure below.

Name	Report Date	Analyzed Customer Count	Reclassification Report	Size	CSV
CDD_risk_rating_report_tr_cdd_ef_2023_12_28_13...	28/12/2023	3	All	1.2 KB	

Figure 252: Example - Automated Reports Display Screen

14.3.3. CRA Reports Screen- Overview

With reference to the following Reports Screen diagram, let's briefly review the workflow procedures to select report types, filter by parameter, search, download, and display results.

As the 'On Demand Reports' tab is selected by default at module select, we will initially focus the description of the workflow from this tab selected and then afterwards describe differences when working with the *Download Automatic Reports* tab option.

Selecting CRA reports from the module select matrix icon after sign in, displays a reports screen similar to the following figure.

Name	Customer ID	Report Date	Entity Type	Analysis Type	DPV	Risk Score	Risk Classification
customer name 1	c001	05/07/2023	Individual	Ongoing	dpv/public	23	HIGH
customer name 2	c002	09/08/2023	Company	Ongoing	dpv/public		HIGH
customer name 3	c003	15/09/2023	Company	Onboarding	dpv/public	32	HIGH

1. Report type options - *On Demand Reports* and *Download Automatic Reports*.
2. Filters - filter results by parameter settings.
3. Search - initiates search query and displays results in a tabular format.
4. Search reports results display example.
5. Actions Panel - provides the analyst with additional reports investigation functionality.
6. ALL - Icon that provides a quick shortcut option to download all filtered reports.

14.3.4. Selecting Filters

Filtering parameters from the *Filter Bar* enables the analyst to fine tune and focus CRA investigation results.

Filters description include :

- Customer name or ID
- Report Date Period
- Classification Type
- Analysis Type
- Per DPV
- Risk Score
- Risk Classification

Figure 253: CRA Alerts - Filter Bar Options

Customer Name or ID

Customer by Name	Description	Example
First Name , last Name or Full Name	Report returns on customer entities being reviewed either on boarding or On going	

Report Date Period

The Report Date Period filter enables the analyst to select a specific date range period to be used in the search query results. Available date ranges are listed in the following table

By Report Date	Description	Examples
Last 24 hours	previous 24 hour period	
Last 7 days	previous 7 day period	
Last 30 days	Previous 30 day period	
Custom setting	Select the Custom From and to Date	From 24/11 23 to 30/11/23

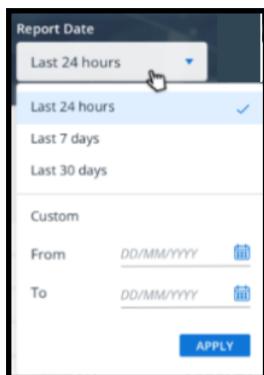


Figure 254: Example Report Date Period Select

Classification Type

The classification type filter enables the analyst user to refine the displayed report results by displaying reports for either an individual customer, an organization or both, for the selected time period, as shown in the following table example.

Classification Type	Description	Example
Individual and or organization	Classification of customer being reviewed	Jon Brown, Ajax Finance co.

Analysis Type

The *Analysis Type* filter enables the analyst user to refine reports results to display either the Onboarding entities, the ongoing entities or both types, as described in the following table example.

Analysis Type	Description	Example
On boarding	New entity undergoing CRA for the first time	James Brown
Ongoing	Existing Entity undergoing follow up CRA testing	Financial services
All	Both of the above types	James Brown, Financial services

DPV

The DPV filter enables the analyst to fine tune reports results to display reports by DPV region, country or district as shown the following table example.

By DPV	Description	Example
Name of DPV	Country or region - IC investigation domain	Spain, UK

Risk Score

The Risk score filter enables the analyst to fine tune reports results by Risk Score value. The Risk score is an numerical indicator (1 - 100) that is system generated, and in many cases , the value can be an extra indicator of the entity's risk likelihood especially with very high levels.

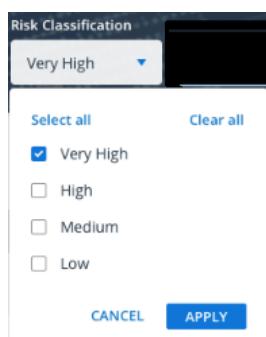
By Risk Score	Description	Example
Evaluated risk score	An integer value between 1 and 100 indicating relative computed risk value	95

Risk Classification

Risk classification is a system calculated severity level that grades the entity under investigation by levels as follows :

- Low
- Medium
- High
- Very High

By Risk Classification	Description	Example
Very High	Automated risk classification of risk (High



14.3.5. Selecting to View Alerts Detail from Reports Module

» To display results of filtered Parameters:

1. Click the Search button (3)

As shown in the example below, available reports that comply with the selected filters are displayed



The screenshot shows a table with columns: Name, Customer ID, Report Date, Entity Type, Analysis Type, DPV, Risk Score, and Risk Classification. There are three rows of data: customer name 1 (c001, 05/07/2023, Individual, Ongoing, dpv:public, 23, HIGH), customer name 2 (c002, 09/08/2023, Company, Ongoing, dpv:public, HIGH), and customer name 3 (c003, 15/09/2023, Company, dpv:public, 32, HIGH). A red box labeled 'Reports Table listing (1)' points to the table. To the right is an 'Actions panel (2)' containing four icons: a magnifying glass for Alert, a blue eye for View, a download arrow for CSV, and a download arrow for ALL.

Name	Customer ID	Report Date	Entity Type	Analysis Type	DPV	Risk Score	Risk Classification
customer name 1	c001	05/07/2023	Individual	Ongoing	dpv:public	23	HIGH
customer name 2	c002	09/08/2023	Company	Ongoing	dpv:public		HIGH
customer name 3	c003	15/09/2023	Company		dpv:public	32	HIGH

Lets take a closer look at the on - demand report results display.

As can be seen the displayed reports data table (1) displays found CRA content such as Name , Id , Report Date, Entity type, DPV , calculated score and Risk calculation.

The actions panel(2) is a core useful utility that allows the investigating analyst to:

- a. Jump directly to the IC case manager and open the CRA alert. From here the alert can be investigated and subsequently resolved. 
- b. Open the alert details page locally to facilitate quick view of the key alert evidences. 
- c. Select to download a copy of the selected report to the analyst's local machine. 
- d. If required and as a quick shortcut all reports results can be downloaded by the conveniently sited "All" download button, as shown above in the tagged element (6). 

From the above utilities available in the Actions panel we will continue the CRA investigation by selecting to view the Alert details locally as described in (b).

2. Clicking the *Alert Details* view icon, displays the alert details panel as shown in the following example.

The screenshot shows the 'Customer Due Diligence Details' page for alert ID OP_65432433. The page is titled 'Customer Due Diligence Details' and includes sections for 'Customer Due Diligence Details', 'KYC Data', 'Risk Classification Results', and a table of risk factors. The 'KYC Data' and 'Risk Classification Results' sections are highlighted with yellow boxes.

Group Risk Factor	Sub Factor (Indicator)	Client Data	Risk Level	Calculated Score / Variable Weight
Person			Current	

With reference to the above alert detail page the evidence data that is displayed is presented in three information blocks:

- General entity information such as full name, date alert created, available documentation evidence, related alerts, plus notes and history related to the alert entity
- Know your customer (KYC) - containing key customer information, such as Id, country of origin, PEP status and other standard KYC data
- Risk Classification results - information such as score, alert severity, group risk factor, sub factor indicator and any other relevant data that confirms and indicates the risk probability factor

14.3.6. Selecting Download Format & Downloading Reports

Reports Downloading

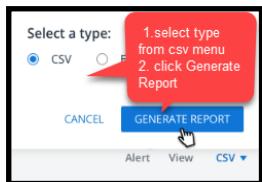
Downloading reports either on a 1 by 1 basis or using the downloading all function is a relatively straight forward process.

The two stages are:

- Select the download format.
- Download the individual report, or download all reports.

» To select the download format:

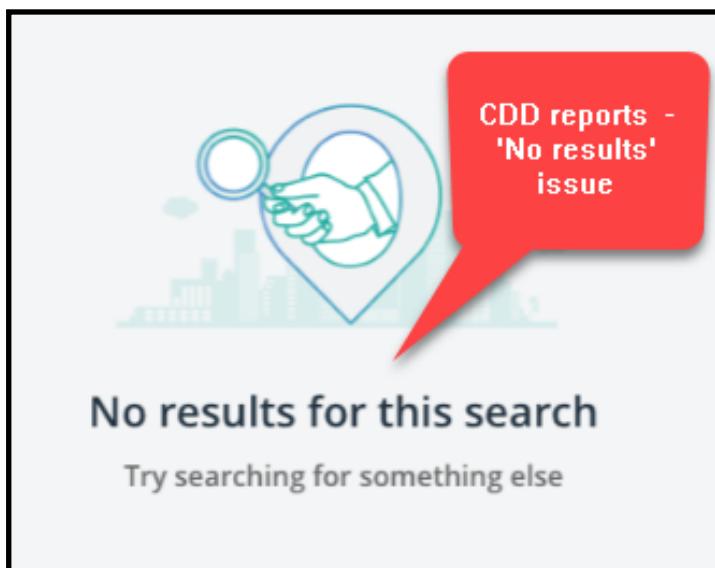
- Next to the download icon for the selected row, click the menu arrow.
- Select csv or Excel type.
- Click Generate Report



The CRA report is downloaded to the local machine.

14.3.7. Troubleshooting CRA Reports

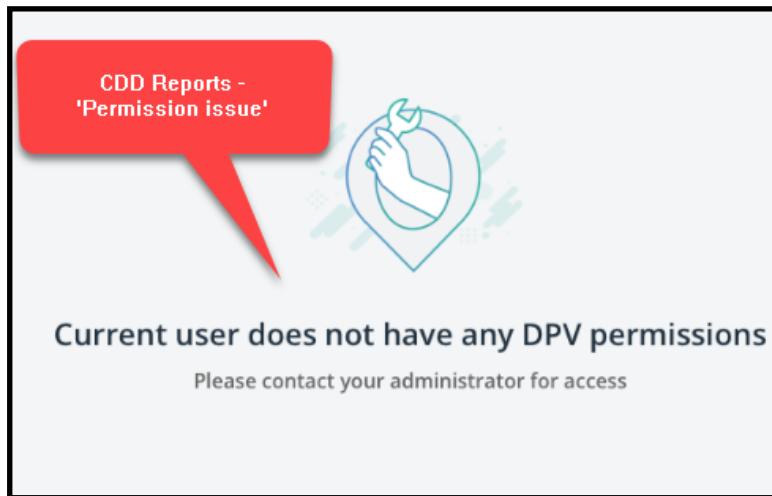
Scenario #1 - When selecting filter parameters and there is no data available the following is 'no results' popup is displayed.



Resolution: Try changing the search parameters.

Scenario #2

The following popup is displayed if there is a user permission issue.
information



Resolution: Try contacting your Admin user to check permissions.