



Fraud Transaction Monitoring Portal Guide

Powered by Featurespace

Version: 1.2

12 February 2025

Publication number: FTMP-1.2-2/12/2025

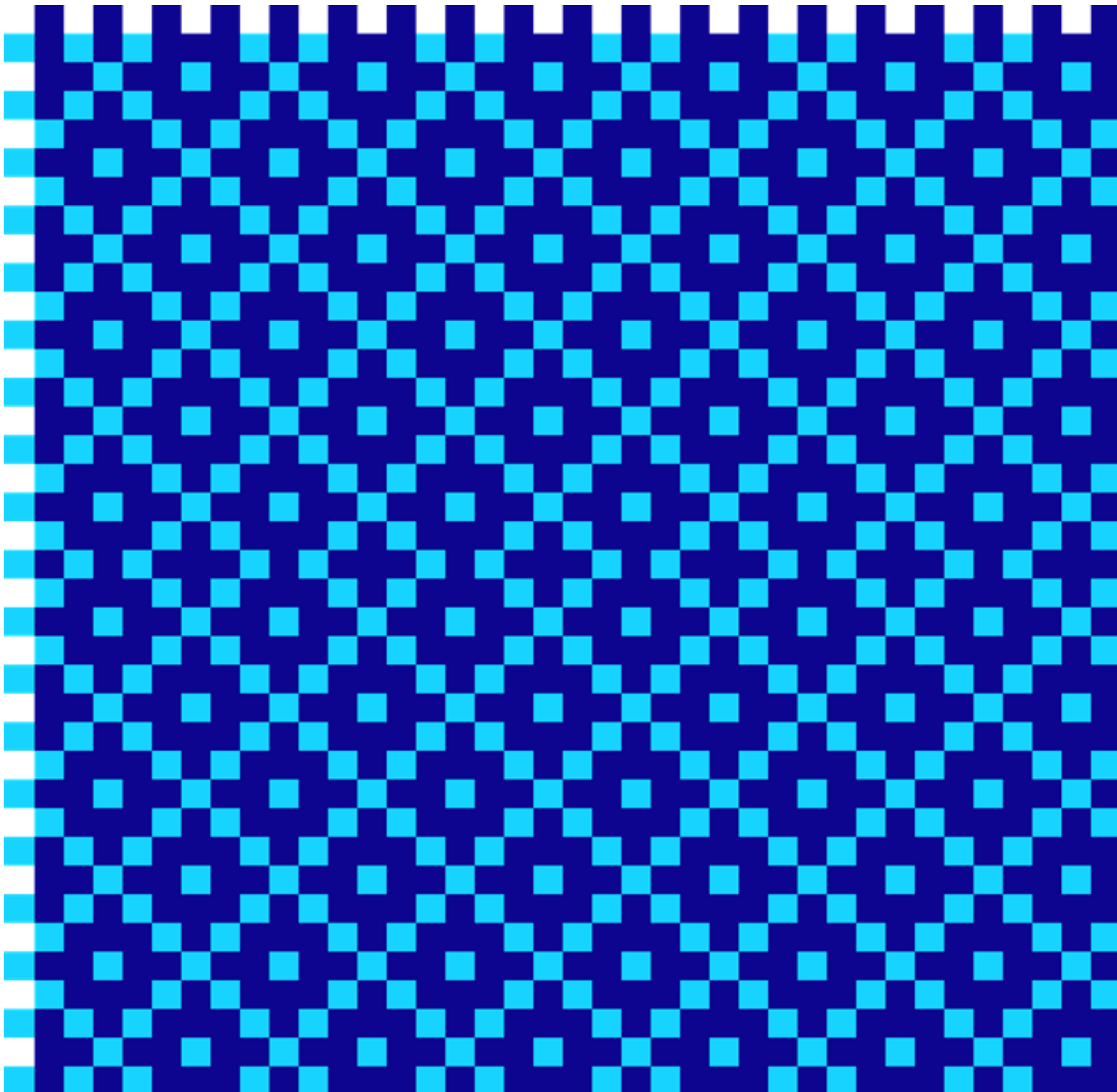
For the latest technical documentation, see the [Documentation Portal](#).

Thredd, Kingsbourne House, 229-231 High Holborn, London, WC1V 7DA

Support Email: occ@thredd.com

Support Phone: +44 (0) 203 740 9682

© Thredd 2025





Copyright

© Thredd 2025

Trade Mark Notice: FEATURESPACE, ARIC, AMDL, OUTSMART RISK, and the FEATURESPACE ORB are registered trademarks and/or images in the UK, US, and EU.

The material contained in this guide is copyrighted and owned by Thredd Ltd together with any other intellectual property in such material.

Except for personal and non-commercial use, no part of this guide may be copied, republished, performed in public, broadcast, uploaded, transmitted, distributed, modified or dealt with in any manner at all, without the prior written permission of Thredd Ltd., and, then, only in such a way that the source and intellectual property rights are acknowledged.

To the maximum extent permitted by law, Thredd Ltd shall not be liable to any person or organisation, in any manner whatsoever from the use, construction or interpretation of, or the reliance upon, all or any of the information or materials contained in this guide.

The information in these materials is subject to change without notice and Thredd Ltd. assumes no responsibility for any errors.



About This Document

This document describes how to use the Fraud Transaction Monitoring Portal to:

- Review high-risk incidents flagged by the Fraud Transaction Monitoring System
- Configure the behaviour of the system
- View, manage and understand the various metrics available in the portal

Note: The Thredd Fraud Transaction Monitoring Portal is based on the Featurespace ARIC Risk Hub product, which has been customised for use by Thredd customers. In this guide, we refer to the Featurespace ARIC Risk Hub User Interface as the Fraud Transaction Monitoring Portal or 'the portal'.

Target Audience

This document is intended for Thredd clients (Program Managers) who are using the Fraud Transaction Monitoring System.

What’s Changed?

If you want to find out what's changed since the previous release, see the [Document History](#) page.

Related Documents

Refer to the table below for other documents which should be used in conjunction with this guide.

Document	Description
<i>Fraud AMDL Rules Configuration Guide</i>	Explains how to configure the rules used by the ThreddFraud Transaction Monitoring System.
<i>Fraud Transaction Monitoring System Access Configuration Guide</i>	Describes how to set up user access and user access role available.

Other Guides

Refer to the table below for other relevant documents.

Document	Description
<i>Payments Dispute Management Guide</i>	Describes how to manage chargebacks and the disputes management process using Thredd.
<i>Smart Client Guide</i>	Describes how to use the legacy Thredd Smart Client to manage your account.
<i>Thredd Portal Guide</i>	Describes how use the Thredd Portal, the new web application for managing your cards and transactions on the Thredd Platform.

Tip: For the latest technical documentation, see the [Documentation Portal](#).



1 Getting Started

This topic describes how to sign in and out of the portal, and covers basic navigation concepts used in the system. You can access the portal from a web browser, using the URL provided by your system administrator. For example:
<https://thredd-prod.aric.featurespace.co.uk/dashboard>

System Requirements

- You should use Google Chrome or Mozilla Firefox to access the portal, as you may not be able to use all of the portal functionality if you try from another browser.
- We recommend a minimum screen resolution of 1440 × 900.
- We recommend that you disable any ad-blocker software and all third-party browser extensions when using the portal, as they may prevent you from accessing certain portal functionality.

Signing In

When accessing the portal for the first time, you are presented with the Sign In page. Click the **Sign In** button to access the portal through SSO.

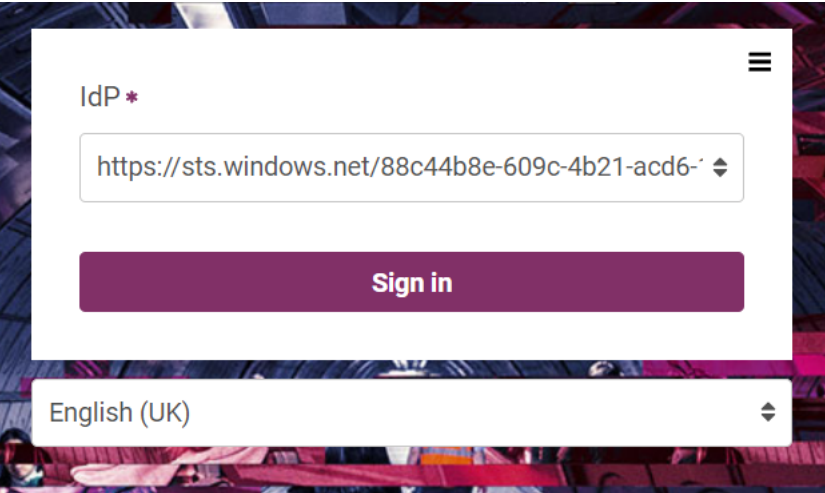


Figure 1: Sign-In Page

The User Menu


At the top right of any page, you can click the icon to access the user menu. From this menu, you can open your user profile page, where you can view and manage details of your portal user account (see [Dashboard](#)). The user menu also allows you to log out of the portal.

To view your user profile page, click the  icon, and then select your username.

For more information about your user profile page, see [Dashboard](#).

Signing Out

You can sign out of the portal from any page. Signing out returns you to the Sign In page.




To sign out, at the top right of the page, click the  icon, and then select **Logout**.

Note: The portal automatically logs you out if your browser is inactive for 30 minutes. A dialogue box appears which gives you the option to extend your session if required (or logout).

The Documentation Sidebar

If you have Documentation permission, you can access the Documentation sidebar from any page. The sidebar provides helpful advice on how to use each section of the portal.



To access the Documentation sidebar, at the top right of the page, click . A sidebar opens on the right. To close the Documentation sidebar, click  again, or click  at the top right of the sidebar.

Messages

The message service appears at the bottom left of every page of the portal and allows users to see messages that have been sent to them by other users. You can send messages to individual or multiple users, either to users in specific teams, or roles.

Create a Message

To create a new message:

1. Click on the **New message** button in the bottom-left corner of the page. The message window displays.

Send new message

Message type

☒ Sidebar (normal)

☐ Banner (important)

Send to

Everyone

Subject

Message subject (optional)

Message *

Message content (max. 4000 characters)

Cancel

Send message

2. Select the message type. Select from either **Sidebar (Normal)** or **Banner (Important)**. Sidebar messages appear at the bottom-left side, while Banner messages display in a banner at the top of every page with an **important message** flag.
3. Select who receives the message. Select from:
 - Everyone (to send a message to all users)
 - Roles (to send messages to users with specific roles)
 - Teams (to send messages to specific teams)
 - Users (to send messages to one or more specified users)

4. Enter a message subject and message content.

Note: The maximum length for your message is 4000 characters.

5. Click the **Send Message** button to send the message.

Receiving and Viewing a Sidebar Message

When messages have been sent as Sidebar messages, to you or several users, you see a notification in the message centre, with the count of messages received.

To open and view a message, click on its subject. After reading the message, click the **Acknowledge** button to confirm the receipt and review of the selected message. The message disappears from your inbox.



Note: If the same message was sent to several users or users with certain roles, the message you acknowledge only disappears from your inbox.

Viewing a Banner Message

When a user has sent a Banner message, the message displays at the top of every page with an **Important message** flag.

To view and dismiss a Banner message:

1. Click on the message subject to view the message, or on the **View full** button.
2. Read the message, then either:
 - Click the **Minimise** button to minimise the message banner. This action keeps the message.
 - or;
 - Click the **Acknowledge** button to confirm receipt and review of the message. The message disappears.

Note: If you have more than one banner message, click the arrow buttons to scroll between messages.



2 Dashboard

The Dashboard is the first page you see when you log in. It provides a quick view of details of your user account and permissions.

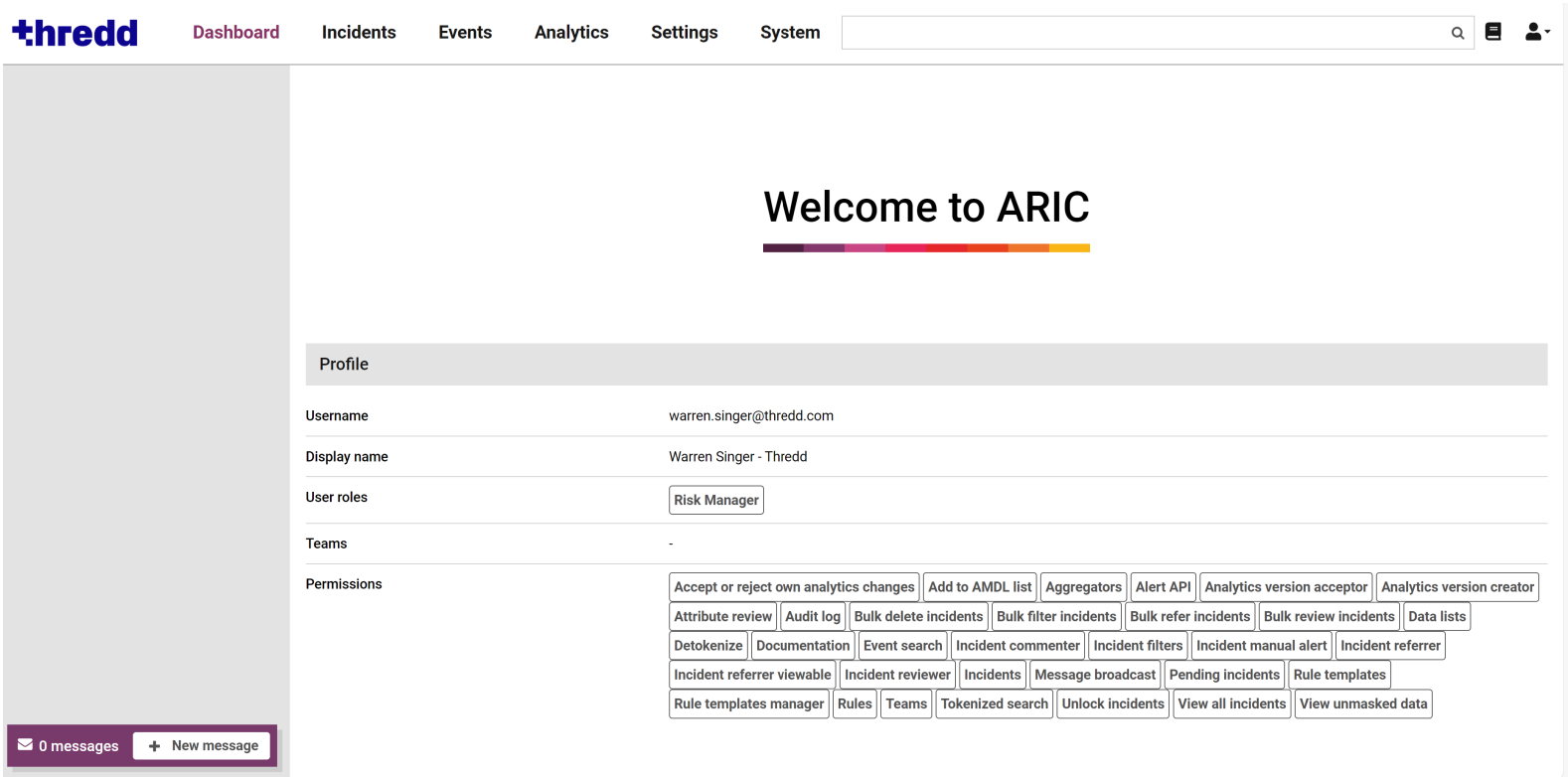


Figure 2: Dashboard

The Profile section shows the following information:

- **Username:** your username (this may not be the name that appears in the portal - see below).
- **Display Name:** when you review incidents, send messages or take other actions, your display name is the name that is shown in the Fraud Transaction Monitoring Portal. If you do not have a display name, your username will be shown instead.
- **User Roles:** the role or roles you have been assigned determine which permissions you have, and therefore which parts of the portal you can see, and the functionality you have access to.
- **Teams:** the teams you are a member of.
- **Permissions:** the permissions you have as a result of the roles you have been assigned.



3 Managing Incidents

You can use the Incidents section of the portal to view and review incidents. Depending on your permissions and your configuration, you can:

- Review individual alerts in an incident as either 'Risk' or 'No Risk'
- Place incidents in a 'Pending' list to await further information
- Add entities or other information to data lists (negative lists, positive lists, watch lists, etc.)

You can also:

- View detailed information about an incident (See [Incident Review Page](#)), including tags and other information added by the portal engine
- View the entity and its activity over time
- View other users' activity related to that entity (e.g. previous incident reviews)

Click the **Incident** button in the portal header to open the Incidents page.

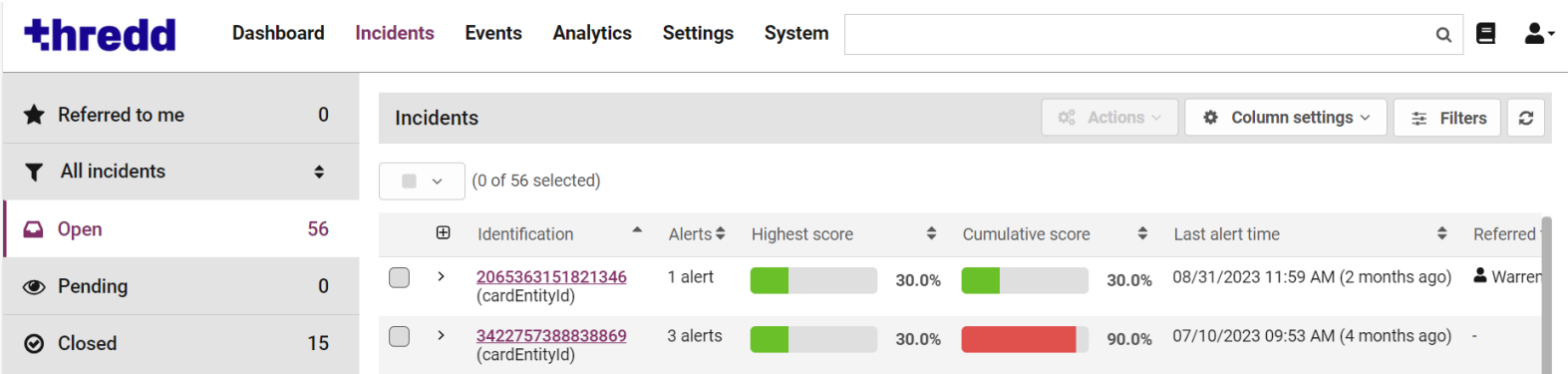


Figure 3: Open Incidents page

Note: Risk score availability is subject to eligibility criteria. If your programme is not eligible for risk scoring, then risk scores displays as greyed out or zero.


The Incidents page consists of a sidebar that contains links to different lists, and a list that displays incidents based on the list selected from the sidebar. The numbers displayed to the right of each list indicate the number of incidents included in each list.

List	Description
Referred to me	Displays unreviewed incidents which have been assigned to you (or your team).
Open	Displays all unreviewed incidents. The Open list displays when you first open the Incidents page.
Pending	Displays incidents which have been specifically sent to this list. This list keeps tab on suspicious entity activity which is not decisively 'Risk' or 'No Risk', or ensures that an incident is not reviewed by other users while you are waiting for additional information.
Closed	Displays details of incidents that have been previously reviewed as 'Risk' or 'No Risk'. You can only manually return entities in the Closed list to the Open list by creating a new alert under the entity. For details on creating an alert, see the Rule Builder section of the Fraud Configuration guide.



Open Incidents Page

The Open Incidents page provides a list of open incidents, and displays by default when clicking the Incidents button. Each incident on this list consists of one or more alerts to review.

Note: To display newly-raised incidents: click .

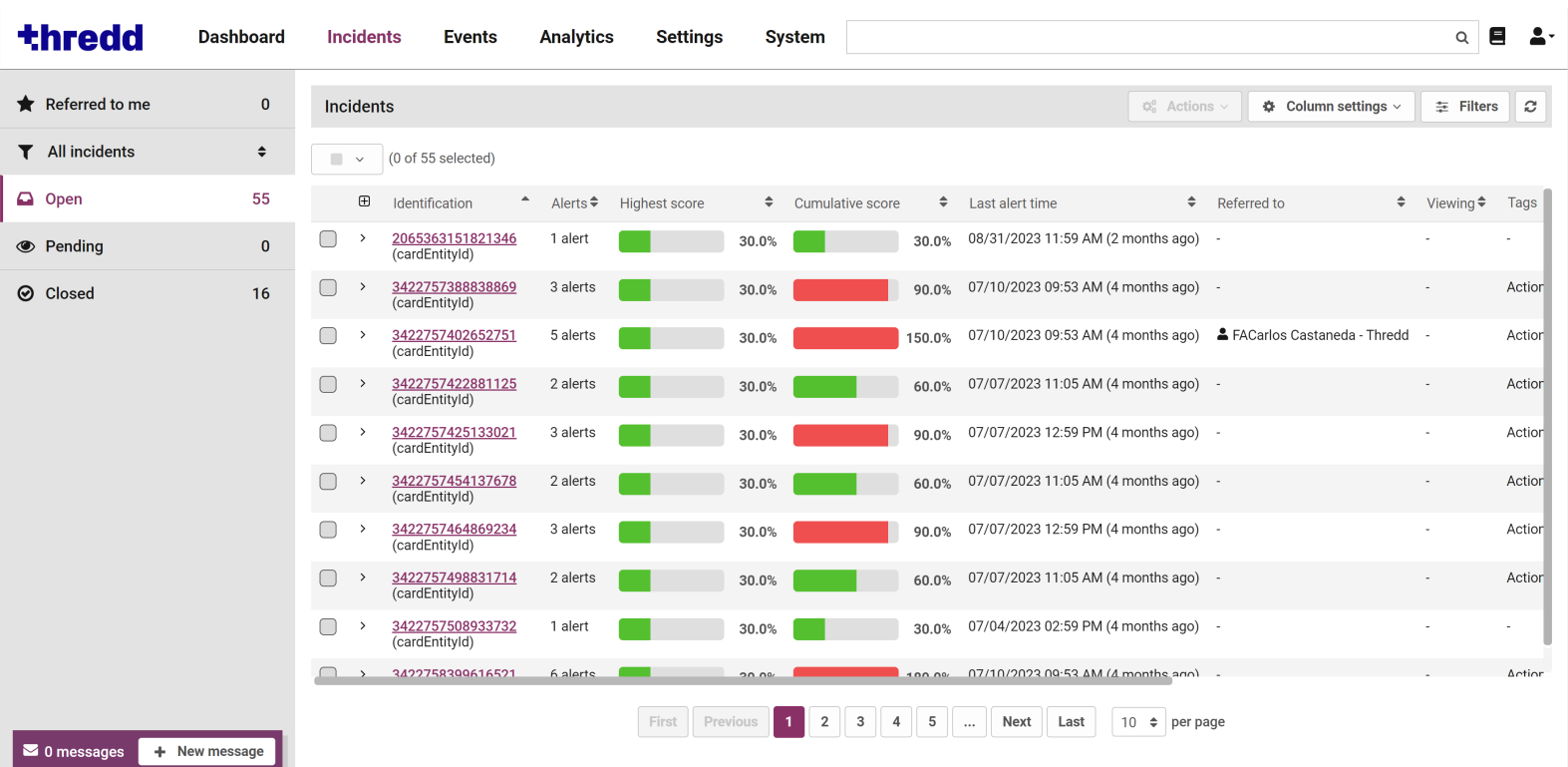


Figure 4: Incidents Page

You can expand an incident and view more details by clicking on the down arrow next to the entity ID.

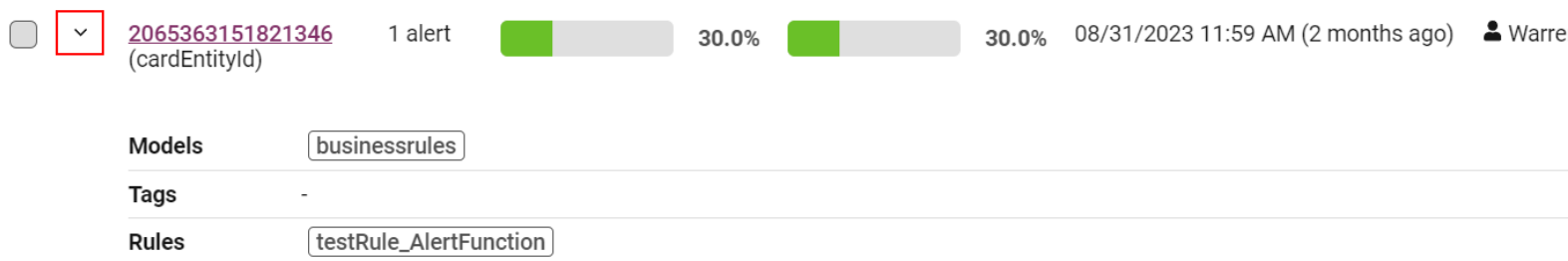



Figure 5: Incident drop-down

Note: To expand all the rows on the page, click the  button in the list header.

Managing Incident Columns

You can choose which columns to view in the main Incident List by using the **Column Settings** button at the top right of the dashboard. Depending on how your portal is configured, available columns can include:

- **Identification** – The unique ID of the entity associated with the incident.
- **Alerts** – The number of unreviewed alerts the incident contains.
- **Highest score** – The highest risk score for any of the incident's unreviewed alerts.
- **Cumulative score** – The sum of all risk scores for all the incident's unreviewed alerts.
- **Scam Detect Score** - The scam score for the incident.

Note: Scam Transaction Monitoring is an optional feature which analyses transactions for potential scam events. For information on setting up and using Scam Transaction Monitoring , either speak to your account manager or see the [Scam Transaction Monitoring Guide](#).



- **Last alert time** – The date and time of the most recently triggered alert.
- **Referred to** – The user/team assigned to review the incident (if any).
- **Viewing** – The user currently viewing the incident's review page (if any). If another user is viewing an incident, it is locked. To unlock an incident that another user is reviewing, click **✖**.
- **Tags** – The list of tags output by rules/models for any of the unreviewed alerts that make up the incident.
- **Models** – The models contributing to the incident's risk score.
- **Rules** – A list of Business Rules triggered by any unreviewed alerts.

Note: Any change that you make is specific to you. Logging out of the Fraud Portal automatically saves to your username.

Filtering Incidents

The following section details how to use filter incidents using pre-set filters created in the Settings page.

Pre-set incident filters

Users with pre-set filters assigned to them select different filters from the **All Incidents** drop-down menu in the sidebar on the left-hand side of the page.

Note: For information on creating filters, see [Incident Filters](#).

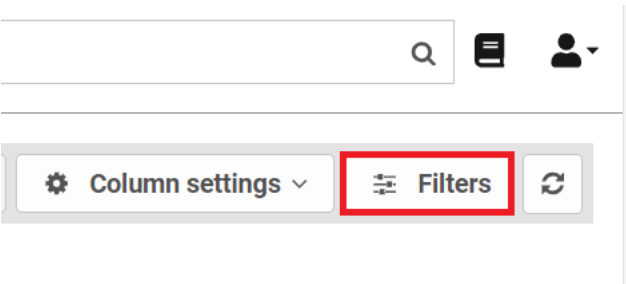
Those without any pre-set filters assigned to them only have the **All Incidents** option available to them.

- To activate a pre-set filter: click **All Incidents** in the sidebar and select a filter in the drop-down menu.
- To deactivate a pre-set filter: select **All Incidents** from the incident filter drop-down menu in the page sidebar.

Using the Filters sidebar

Click **Filters** at the top right of the Incident List page to filter incidents based on:

- **Date range:** show only incidents where the latest alert in that incident was generated between two times.
- **Rules:** show only incidents where the selected rules triggered for at least one alert in the incident. Rule descriptions, if configured, are not visible in this sidebar.
- **Models:** show only incidents where the selected models assigned a risk score to at least one alert in the incident.
- **Filter by highest score:** show only incidents where the riskiest score is between the minimum and maximum score you set using the Filter by highest score.



Any active incident filters apply to all the Incident Lists:

- Open
- Closed
- Pending
- Referred to Me

Bulk Actions

The **Actions** button at the top right-hand side of the Incident List lets you modify or delete multiple incidents. By combining this functionality with filters, you can modify or delete incidents that match your filtering criteria.

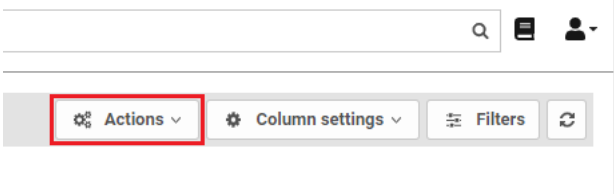


Figure 6: Incident Actions menu

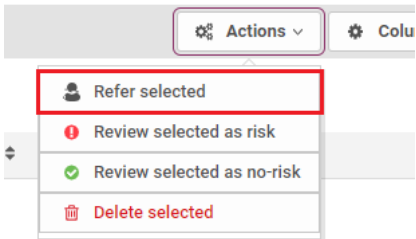
Bulk Incident Referrals

To select multiple incidents for referral in bulk:

1. Tick the incident check boxes on the left, or use the check box at the top of columns, to select one or more incidents to refer (you can select incidents on multiple pages of the same list, but not incidents from multiple lists).

	Identification	Alerts	Highest score
<input checked="" type="checkbox"/>	> 3422757388838869 (cardEntityId)	3 alerts	<div><div></div></div>
<input type="checkbox"/>	> 3422757402652751 (cardEntityId)	5 alerts	<div><div></div></div>
<input checked="" type="checkbox"/>	> 3422757422881125 (cardEntityId)	2 alerts	<div><div></div></div>

2. Click **Actions** and select **Refer Selected** from the menu.



A window will display.

3. Select the team or user to refer these incidents to from the **Refer To** menu.

Refer incidents (2 of 55 selected)

Refer to

jon.bullock@thredd.com

Comment *

Test label for Risk Txns

Use a comment template

Refer 2 incidents

Cancel

4. Add a comment or select a comment template from the menu.

Refer incidents (2 of 55 selected)

Refer to

jon.bullock@thredd.com

Comment *

Test label for Risk Txns

Use a comment template

Refer 2 incidents

Cancel

5. Click **Refer Incidents**. Note that the button will be renamed depending on how many incidents you have selected.



Bulk Incident Reviews

To select multiple incidents for review in bulk:

- 1. Tick the incident checkboxes on the left, or use the checkbox at the top of columns, to select one or more incidents to review. You can select incidents on multiple pages of the same list, but not incidents from multiple lists.

<input type="checkbox"/>	Identification	Alerts	Highest score
<input checked="" type="checkbox"/>	> 3422757388838869 (cardEntityId)	3 alerts	<div><div></div></div>
<input type="checkbox"/>	> 3422757402652751 (cardEntityId)	5 alerts	<div><div></div></div>
<input checked="" type="checkbox"/>	> 3422757422881125 (cardEntityId)	2 alerts	<div><div></div></div>

- 2. Click **Actions**.

⚙️ Actions ▾

⚙️ Column settings ▾

🔍 Filters

🔄

- 3. Either:
 - a. Review all incidents as 'risk':
 - i. Click **Review Selected as Risk**.

⚙️ Actions ▾

👤 Refer selected

⚠️ Review selected as risk

✅ Review selected as no-risk

🗑️ Delete selected

A window will display.

- ii. Assign a risk severity (confirmed or suspected) to all the alerts in the incidents by selecting it from the 'Risk Severity' drop-down list.

Review as risk (2 of 55 selected) ✕

Risk severity *

Confirmed risk

- iii. To explain your decision, select one or more risk reasons from the 'Risk Reasons' menu; these apply to all alerts in the incidents you have selected. You can assign multiple risk reasons to the incident. The assigned risk reasons appear beneath the 'Add a Risk Reason' menu. To remove a risk reason, to the right of its name, click .

Review as risk (2 of 55 selected) ✕

Risk severity *

Confirmed risk

Risk reasons

1 of 6 selected

© Thredd 2025

Fraud Transaction Monitoring Portal Guide

12



iv. Add a comment to the Comment field or select a comment template from the menu.

Comment*

Test label for Risk Txns

Use a comment template

Review 2 incidents

Cancel

- b. Or, to review all incidents as 'no risk':
- i. Click **Review Selected as No-risk**.

⚙️ Actions ▾

Refer selected

Review selected as risk

Review selected as no-risk

Delete selected

- ii. To explain your decision, select one or more risk reasons from the 'No Risk Reasons' menu; these apply to all alerts in the incidents you have selected. You can assign multiple no risk reasons. The assigned no risk reasons appear beneath the 'Add a No Risk Reason' menu. To remove a no risk reason, to the right of its name, click .

Review as no-risk (2 of 55 selected) ✕

No-risk reasons

1 of 3 selected

Comment*

Add a comment

Use a comment template

Review 2 incidents

Cancel

iii. Add a comment to the Comment field or select a comment template from the menu.

Comment*

Test label for Risk Txns

Use a comment template

Review 2 incidents

Cancel

4. Click **Review Incidents**.

Bulk Incident Deletions

To select multiple incidents for deletion in bulk:

1. Tick the incident check boxes on the left, or use the checkbox at the top of columns, to select one or more incidents (you may select incidents on multiple pages of the same list, but not incidents from multiple lists).

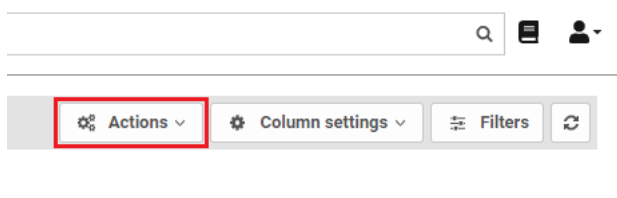
	Identification	Alerts	Highest score
<input checked="" type="checkbox"/>	> 3422757388838869 (cardEntityId)	3 alerts	<div></div>
<input type="checkbox"/>	> 3422757402652751 (cardEntityId)	5 alerts	<div></div>
<input checked="" type="checkbox"/>	> 3422757422881125 (cardEntityId)	2 alerts	<div></div>

2. Click the **Actions** button.

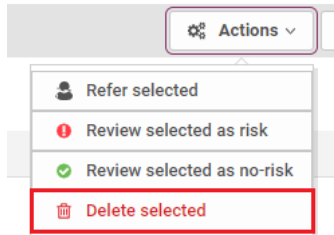
© Thredd 2025

Fraud Transaction Monitoring Portal Guide

13



3. Click the **Delete Selected** button. This cannot be undone and will require you to confirm you want to proceed.



Note: Not all bulk actions will be available to all users as these actions are determined by user role.



4 Incident Review Page

The Incident Review page enables you to view more details and perform actions on an incident.

Depending on your permissions and your configuration, you can use the Incident Review page for different tasks:

- Investigate the details of an incident and classify it as either Risk or No Risk
- Add an incident to the Pending list.
- Add the entity involved (or other data from events in that entity's history) to a list such as a negative list or watch list.
- Refer incidents to a user or team.

The top of the Incident Review page shows details of the entity involved in the incident you are viewing. This includes the entity ID, and entity type (top left). On the right, there is a review timer that shows you how long you have been viewing the incident.

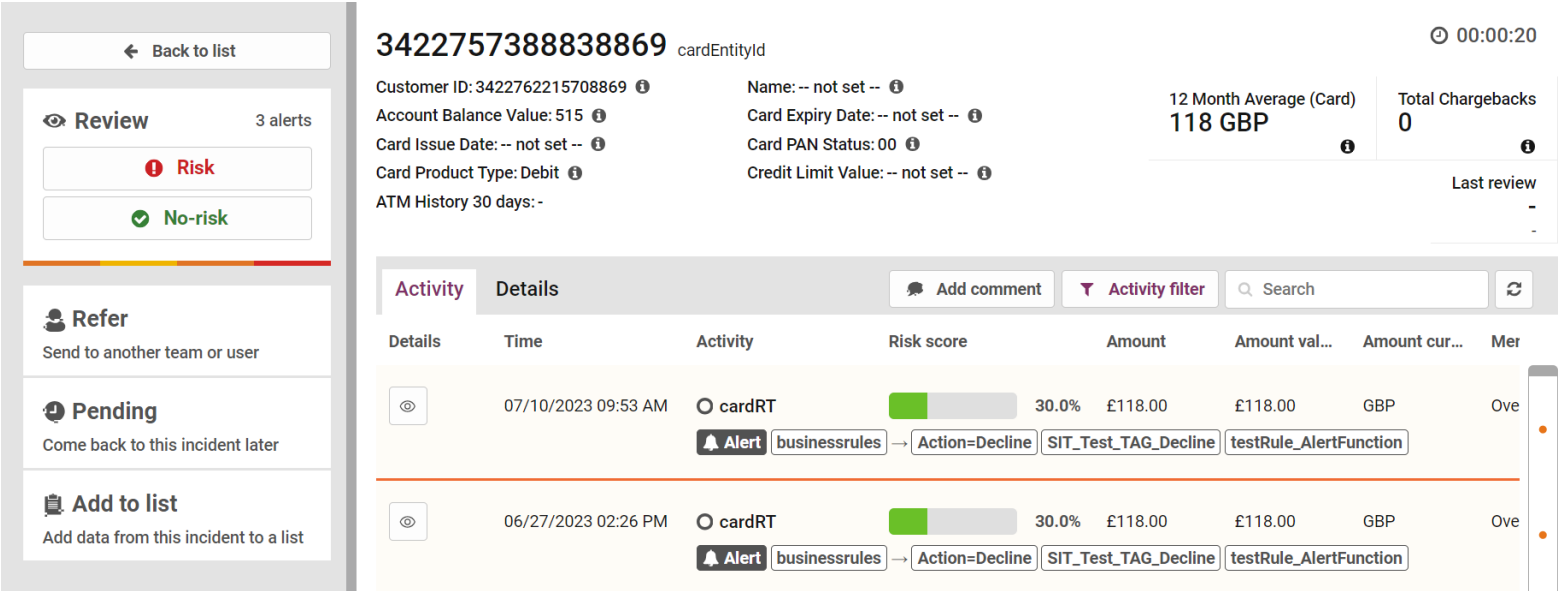


Figure 7: Incidents Review Page

Below the entity ID and type, there are two areas that may display information about the relevant entity: the entity details on the left and the entity headlines on the right. By default, no details are displayed in the entity details area. However, your portal system may be configured to show information drawn from the entity's behavioral profile data, or from other entity data stored by the portal.

2065363151821346 cardEntityId

Customer ID: 1001368468847 ⓘ
Account Balance Value: 5000 ⓘ
Card Issue Date: -- not set -- ⓘ
Card Product Type: Debit ⓘ
ATM History 30 days: -
Name: -- not set -- ⓘ
Card Expiry Date: -- not set -- ⓘ
Card PAN Status: 00 ⓘ
Credit Limit Value: -- not set -- ⓘ

Figure 8: Incident Entity Details

Below the entity details section, the main part of the Incident Review page is split into tabs:

- The Activity tab shows a timeline of the entity's history, including events, alerts and analyst actions (see [Activity Tab](#))
- The Details tab shows a summary of the entity's history (see [Details Tab](#))

Note: Depending on how the portal is configured, some confidential or personal data displayed in the Incident Review page may be hidden or partially hidden.



Activity Tab

The Activity tab shows a timeline of the events generated by the relevant entity. For each event in the timeline, one or more of the following columns are shown:

- Time: the date and time the event took place
- Event: details of the event itself, including the event type
- Risk/Scam score: for events that were scored by a model or rules, the risk (for fraud events) or Scam Transaction Monitoring (for scam events) score for that event

Note: Scam Transaction Monitoring is an optional feature which analyses transactions for potential scam events. For information on setting up and using Scam Transaction Monitoring , either speak to your account manager or see the [Scam Transaction Monitoring Guide](#).

Activity	Details	<div><div>Add comment</div><div>Activity filter</div><div>Search</div><div></div></div>					
Details	Time	Activity	Risk score	Amount	Amount val...	Amount cur...	Mer
	11/09/2023 04:21 PM	Referred to user Warren Singer - Thredd Referred by Warren Singer - Thredd "Please review the transactions by checking with Card holder"					
	08/31/2023 11:59 AM	cardRT	<div><div></div></div> 30.0%	£99.00	£99.00	USD	The
<div>Alert businessrules → testRule_AlertFunction</div>							

Figure 9: Incident Activity Tab

Note: Additional columns containing more information about the events can also be displayed.

By default, the timeline includes events that generated alerts together with all analyst actions (such as reviews and comments). To change which events are included in the timeline, at the top of the timeline, click the **Activity Filter** button(see Filtering the activity timeline).

When an analyst takes action on an incident, it is shown in the activity timeline. The date and time and type of the action are shown, along with the analyst's name and any comment they added. The full comment and other details of the activity can be viewed in the sidebar by clicking the Eye icon to the left of the date.

From the Activity tab, you can:

- Click the Eye icon to view more information about an event select an event in the timeline
- Add a comment to the incident, click (see Adding a comment)
- Click the Refresh button to refresh the incident timeline so that it shows the latest events

Filtering the Activity Timeline

You can use the filter options to select what kind of events are included in the event timeline, such as events that did not generate an alert, alerts that have been reviewed, analyst actions, or specific event types, such as transactions. To filter the activity timeline:

1. Click the Activity Filter button at the top of the activity timeline. The filter panel will open.
2. Use the four buttons on the left of the filter panel to select which statuses of events you want to see. The options available are:
 - Unreviewed alerts
 - Reviewed as risk
 - Reviewed as no-risk
 - Non-alerted

Note: If you do not select any of the available statuses, all event types are included in the timeline.



- 3. Select the types of events that you want to see from the middle panel. Click All to select all event types, or None to clear the selection of all event types. Event types present in the activity timeline of the relevant entity are highlighted in bold.

Note: If you do not select any event types, all event types are included in the timeline.

- 4. Select the types of analyst actions you want to see in the right filter panel, such as Alert review, Add comment, or Refer.

Note: If you do not select any analyst action types, all action types are included in the activity timeline.

- 5. Click the **Activity Filter** button to close the filter panel to save the filter changes.

The changes you make to the filter options are retained when you view another incident. The changes are also retained the next time you log in to the portal.

To export a record of user activity associated with this entity in PDF format, click the **Export Selected Actions (.pdf)** button below the Analyst actions on the left of the filter panel. This will export only the types of analyst action that are currently visible.

Resetting the Activity Filter

To reset the activity filter:

- 1. Click the **Activity Filter** button at the top of the activity timeline.
- 2. Click the **Reset Filter** button at the bottom right of the filter panel.

The timeline return to showing all events that generated alerts and all analyst actions.

Searching the Activity Timeline

Use the search box to search, filter, or highlight the events included in the event timeline. This will search across all columns in the activity timeline.

Activity Types

When the timeline is too large to fit in your browser window, a scrollbar is displayed on the right of the timeline. Dots at regular intervals on the scrollbar represent each activity in the timeline. The dots are colour-coded as shown below:

Dot	Description
	Event that did not generate an alert.
	Unreviewed alert.
	Alert reviewed as 'No Risk'.
	Alert reviewed as 'Risk'.
	Analyst action such as a comment, manual alert creation, or referral.



Details Tab

The Details tab contains detailed information relating to the entity in the current incident.

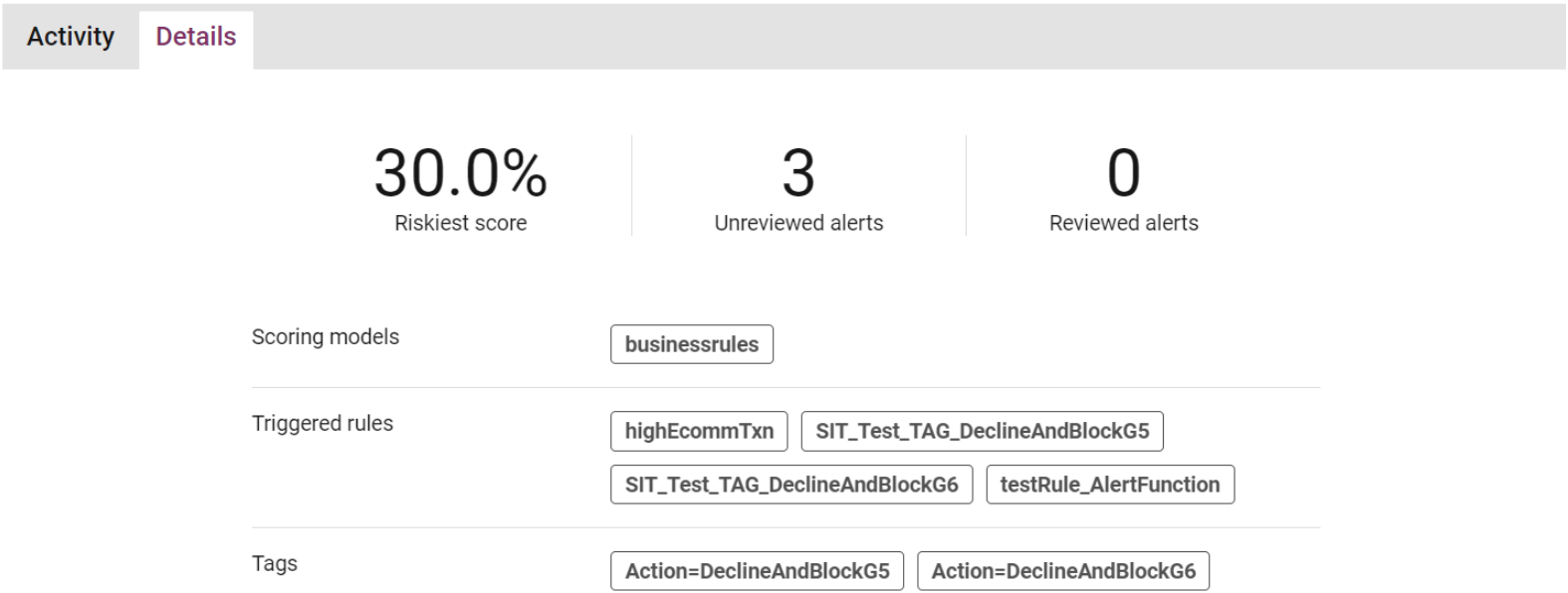


Figure 10: Details Tab

The top panel displays the following information:

- **Riskiest Score:** the highest risk score assigned to an alert generated by this entity.
- **Unreviewed Alerts:** the number of outstanding alerts in this incident.
- **Reviewed Alerts:** the number of alerts for this entity already reviewed in this incident.
- **Scoring Models:** the models which have scored events related to this entity.
- **Triggered Rules:** the rules which have triggered for this entity.
- **Tags:** the tags which have been output by models/rules for this entity.

Events Score Distribution and Event/Alerts Breakdown

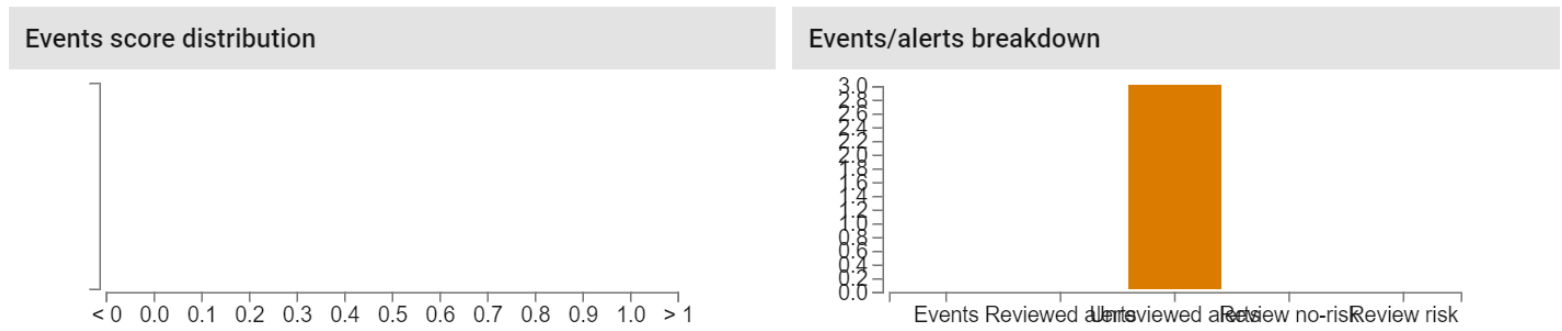


Figure 11: Events score distribution and breakdown section

The Events Score histogram displays the distribution of risk scores for events relating to the current entity.

The Events/Alerts Breakdown histogram displays:

- **All Events:** the total count of events for the current entity.
- **Reviewed Alerts:** the count of alerts which have been previously reviewed.
- **Unreviewed Alerts:** the count of outstanding unreviewed alerts.
- **Review No-risk:** the count of alerts reviewed as 'No risk' for this entity.
- **Review Risk:** the count of alerts reviewed as 'risk' for this entity.



Business Rule Profile

Profile data stored for this entity is displayed in two columns: the left column indicates the name of the variable (i.e. the AMDL state expression). The right column displays the stored data. This data may be one of the following types, as indicated by the icon to the left of the variable name

- Number
- String (this includes timestamp data)
- Boolean (true or false)
- Collection of multiple values

Business rule profile		▲ Collapse all	📄 Copy all
☰ GPShighestload	-- no data --		
☰ GPSSumATMoverseasTxn1d	-- no data --		
☰ GPScountATMoverseasTxn36h	-- no data --		

Figure 12: Business rule profile section



Reviewing Incidents

Incidents can be reviewed based on entity behavior, applying a decision to one or more unreviewed alerts. Incidents are usually reviewed from the 'Open' incident list, but reviewing is also possible for 'Pending' incidents.

Note: Not all users will have the appropriate permissions to review incidents. Users with a read-only role or read-only permissions will see a message in the sidebar stating they do not have permission to action incidents, instead of the review panel.

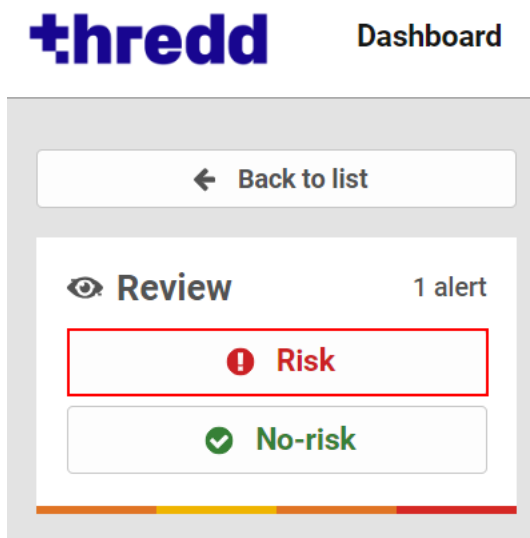
Using the current and past behaviour information presented in the Incident Review page, analysts can assign a decision to the incident, identifying the entity's behaviour as high or low risk.

Reviewing alerts also provides feedback to any Adaptive Behavioral Analytics models, allowing them to learn from user decisions. Review decisions are assigned, and other actions can be taken, using the sidebar that appears to the left of the Incident Review page.

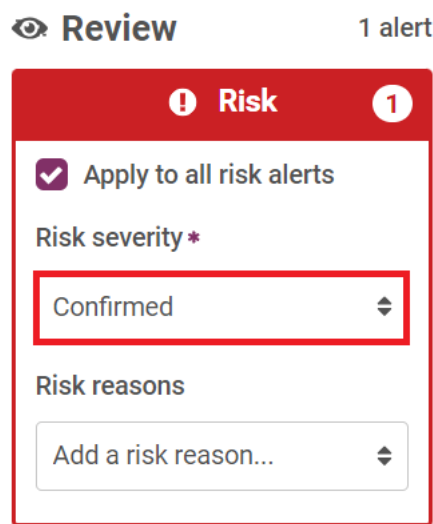
Reviewing All Alerts as Risk

To review all the unreviewed alerts in an incident as 'Risk':

- 1. Click the **Risk** button in the sidebar of the Incident Review page. The Risk review panel appears in the sidebar.



- 2. Either:
 - Assign a risk severity (confirmed or suspected) to all the alerts in the incident by selecting it from the Risk Severity drop-down list.



or

- Assign risk severities to the individual alerts by clearing the 'Apply to all Risk alerts' check box or clicking the button next to



one of the alerts, and then selecting confirmed or suspected from the left drop-down menu beneath each alert.

3. Either:
- Select one or more Risk reasons explaining your decision from the Risk Reasons drop-down list in the sidebar - these will apply to all alerts in the incident.
- The Risk reasons assigned to this incident appear beneath the 'Add a Risk reason' drop-down list. You can remove a Risk reason by clicking the cross to the right of its name.

- or
- Assign Risk reasons to individual alerts by clearing the 'Apply to all Risk alerts' check box or clicking the button next to one of the alerts, and then selecting one or more Risk reasons from the right drop-down list beneath each alert. Risk reasons assigned to an alert appear next to the 'Add a Risk reason' drop-down list. You can remove a Risk reason by clicking the cross to the right of its name.

4. Add a comment about the risk to the Comment field. Alternatively, use the Comment Template drop-down field to select a template to automatically fill the Comment field.

5. Click the **Complete Review** button to complete the review of the incident.



Use a comment template

Complete review

Cancel

The incident is moved to the 'Closed' list until a new alert is triggered for the same entity.

Reviewing All Alerts as No Risk

To review all the unreviewed alerts in an incident as 'Risk':

- Click the **No Risk** button in the sidebar of the Incident Review page. The Risk review panel appears in the sidebar.

thredd

Dashboard

Back to list

Review

1 alert

Risk

No-risk

- Either:
 - Select one or more No Risk reasons explaining your decision from the No Risk Reasons drop-down list in the sidebar. These will apply to all alerts in the incident. You can assign multiple No Risk reasons by repeatedly selecting them from the drop-down - the risk reasons assigned to this incident will appear beneath the 'Add a No Risk reason' drop-down. A risk reason can be removed by clicking the cross to the right of its name.

Review

1 alert

Risk

No-risk

1

Apply to all no-risk alerts

No-risk reasons

Add a no-risk reason...

or

- Assign No Risk reasons by clearing the 'Apply to all No Risk alerts' check box or clicking the button next to one of the alerts, then selecting one or more No Risk reasons from the drop-down menu beneath each alert. If you choose to assign No Risk reasons to individual alerts after assigning one or more No Risk reasons to the whole incident (as in step a), the No Risk reasons you assigned to the whole incident will be assigned to each individual alert. No Risk reasons assigned to an alert will appear next to the 'Add a No Risk reason' drop-down. You can remove a No Risk reason by clicking the cross to the right of its name.

08/31/2023 11:59 AM

cardRT

30.0%

£99.00

£99.00

Alert

businessrules

testRule_AlertFunction

Add a no-risk reason...

© Thredd 2025

Fraud Transaction Monitoring Portal Guide

22



3. Add a comment in the Comment field. Alternatively, use the Comment Template drop-down field to select a template to automatically fill the Comment field.

Comment *

Please review the transactions by checking with Card holder

Use a comment template

Complete review

Cancel

4. Click the **Complete Review** button to complete the review of the incident.

Use a comment template

Complete review

Cancel

The incident is moved to the 'Closed' list until a new alert is triggered for the same entity.

Reviewing an Incident as a Mixture of Risk and No Risk

To review some of the alerts in an incident as 'Risk' and some as 'No Risk':

1. Click on either the **Risk** button (if the majority of the alerts are to be classified as 'Risk', or the **No Risk** button (if the majority of alerts are to be classified as 'No Risk')

Review

1 alert

ⓘ Risk

✓ No-risk

2. Either:
- Click the Risk button next to any alert(s) you want to review as 'Risk',

£99.00

ⓘ

✓

or

- Click the No Risk button next to any alert(s) you want to review as 'No Risk'.

£99.00

ⓘ

✓

Both Risk and No Risk review panels will be displayed in the Incident Review page sidebar, as shown above. The number of alerts to be reviewed as Risk and No Risk will be shown in the appropriate panels, next to the headings.

3. Either:



- Select a risk severity and Risk reasons for all the alerts to be reviewed as 'Risk', as described in Reviewing All Alerts as Risk.
 - or
 - Select risk severities and reasons for each alert individually, as described in Reviewing All Alerts as Risk.
4. Either:
- Select No Risk reasons for all the alerts to be reviewed as 'No Risk', as described in section Reviewing All Alerts as No Risk.
 - or
 - Select No Risk reasons for each alert individually.
5. Add a comment in the Comment field. Alternatively, use the Comment Template drop-down field to select a template to automatically fill the Comment field.

Comment *

Please review the transactions by checking with Card holder

Use a comment template

Complete review

Cancel

6. Click the **Complete Review** button to complete the review of the incident.

Use a comment template

Complete review

Cancel

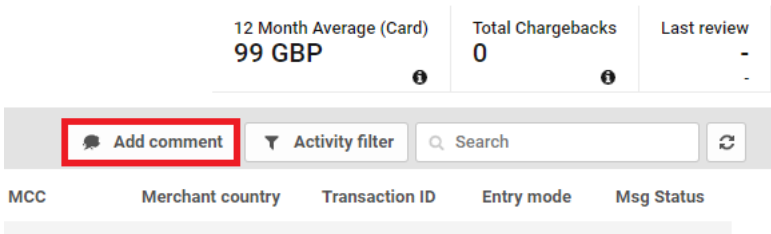


Adding a Comment

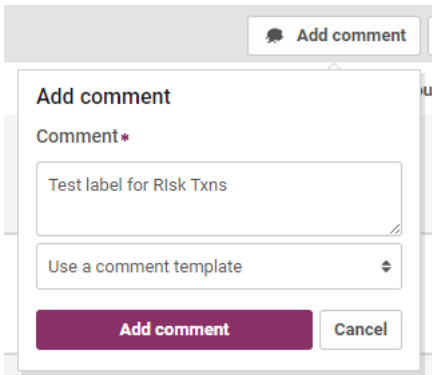
Comments can be added to an entity’s activity timeline, to provide other users with information in the context of the timeline.

To add a comment:

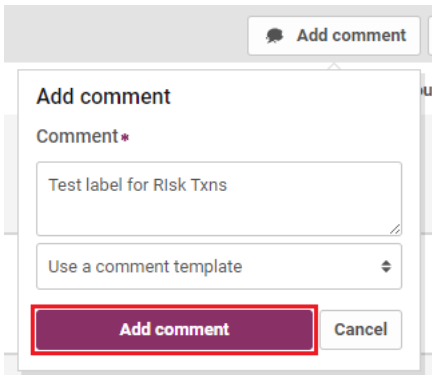
- 1. Click the **Add Comment** button in the gray bar above the activity timeline.



- 2. Add a comment in the Comment field. Alternatively, use the Comment Template drop-down field to select a template to automatically fill the Comment field.



- 3. Click the **Add comment** button to add your comment to the entity's timeline.

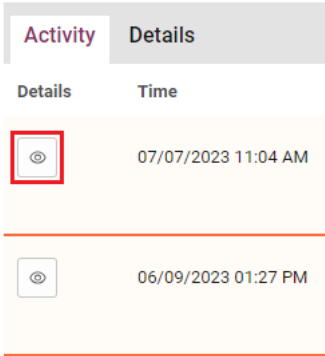




Manually Creating an Alert

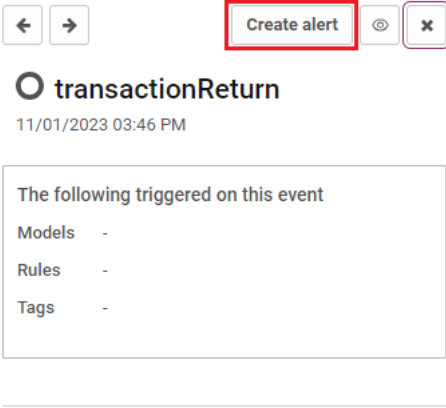
To manually generate an alert on a particular event:

- 1. Click on the Eye icon to the left of that event in the activity timeline, to show the event details sidebar.

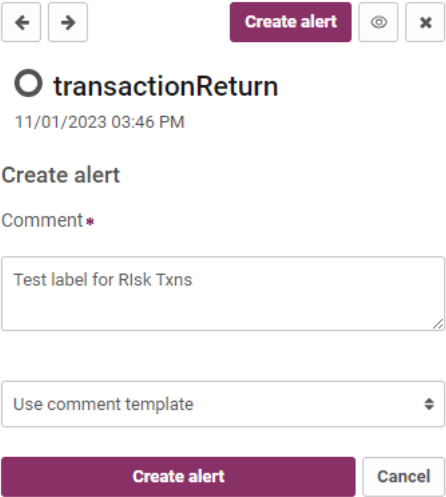


The Event Details Sidebar will open on the right-hand side of the page.

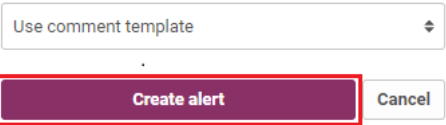
- 2. Click the **Create alert** button in the right-hand sidebar.



- 3. Add a comment in the Comment field. Alternatively, use the Comment Template drop-down field to select a template to automatically fill the Comment field.



- 4. Click the Create Alert button to create the alert.



The event becomes an alert in the activity timeline, and your manual creation of this alert also appears in the timeline as a user action. You or another user can now review this manually created alert.

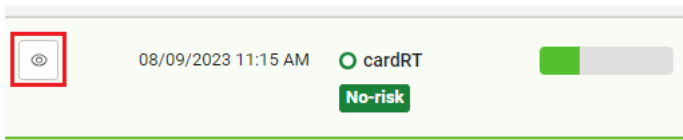


Editing a Review

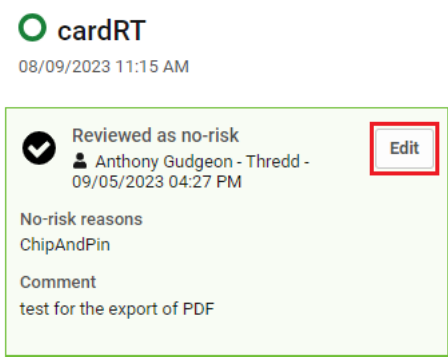
In the event of new information being received, any 'Risk' or 'No Risk' review in an entity's activity timeline can be revised. For example, if an alert previously reviewed as 'No Risk' is discovered to be fraudulent, the decision can be changed. This allows other analysts to see a more accurate picture of the entity's history, and teaches the portal's models to better recognise high-risk events.

To edit a review decision:

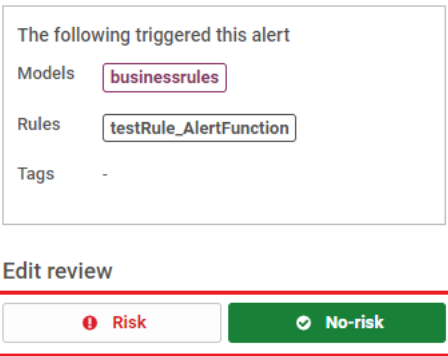
- 1. Click on the original alert review in the entity's activity timeline.



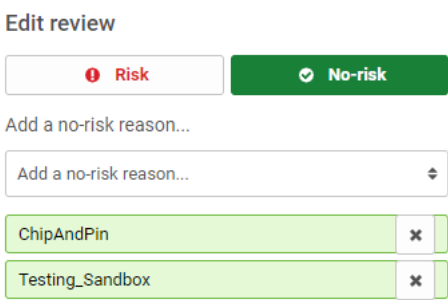
- 2. Click the **Edit** button in the event details sidebar.



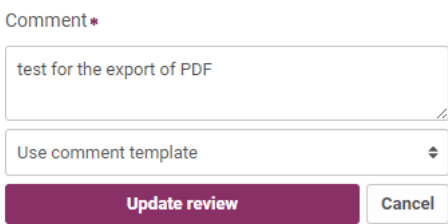
- 3. (Optional) To change a 'No Risk' review to 'Risk', click the Risk button, or to change a 'Risk' risk to 'No Risk', click the No Risk button.



- 4. (Optional) Edit the risk severity (if applicable), risk/no risk reason(s) and comment as required.



- 5. Click the **Update Review** button.





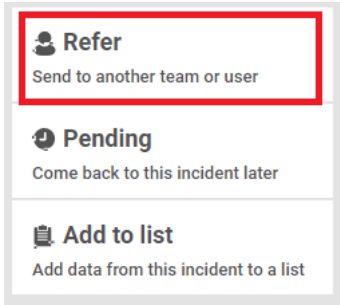
Referring Incidents

You can refer an incident to particular users or user teams for analysis. This allows the reviewing workload to be divided between users, or re-assigned to users with review specialties (For example, a reviewer suspecting an incident results from bot activity could assign it to a user/team who deals with bot detection).

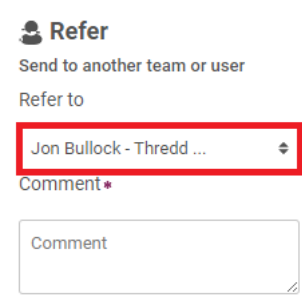
A referred incident displays the referred user or team in the ‘Referred To’ column of the incident list, and the incident will be added to the ‘Referred To Me’ incident list of the corresponding user (or user team members).

To refer an entity/incident:

- 1. Click the **Refer** button in the review actions sidebar.



- 2. Click the **Refer to** drop-down to select the team or user to refer this incident to.



- 3. Add a comment in the Comment field. Alternatively, use the Comment Template drop-down field to select a template to automatically fill the Comment field.

- 4. Click the **Refer Incident** button to refer the incident to your chosen user or team.

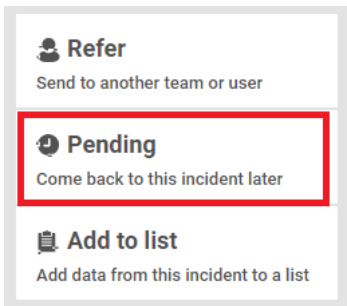


Pending Incidents

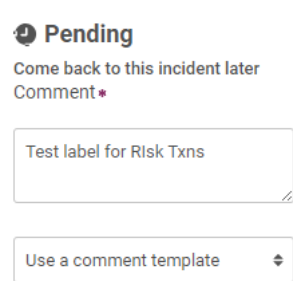
Incidents can be moved to the Pending list, to postpone incident review until further information has been gathered. An incident can be added to the Pending list indefinitely, or for a specified period. Incidents in the Pending list can be reviewed as normal.

To add an incident to the Pending list:

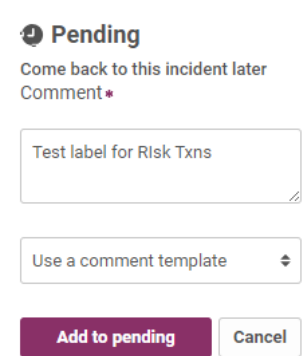
1. Click the **Pending** button in the review sidebar.



2. Add a comment in the Comment field. Alternatively, use the Comment Template drop-down field to select a template to automatically fill the Comment field.

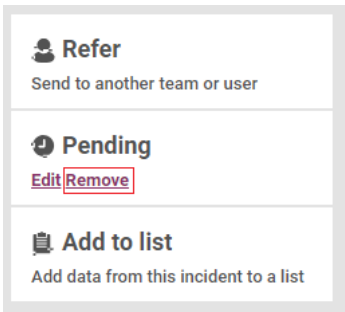


3. Click the **Add to Pending** button.



Removing an Incident from the Pending List


To remove an incident from the Pending list, click the **Remove** button where it is displayed as part of the **Pending** button in the review sidebar.




Editing a Pending Timeout Duration

To edit or remove the timeout duration you set, or to edit the comment you gave for the incident, click on the **Edit** button where it is displayed as part of the **Pending** button in the review sidebar.




 **Refer**

Send to another team or user

 **Pending**

Edit

Remove

 **Add to list**

Add data from this incident to a list

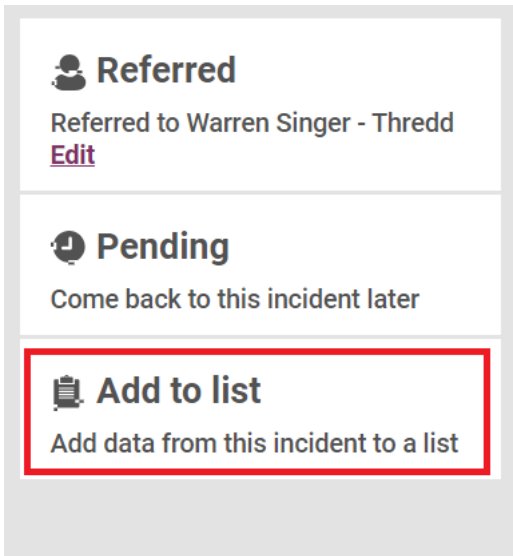


Adding Items to a Data List

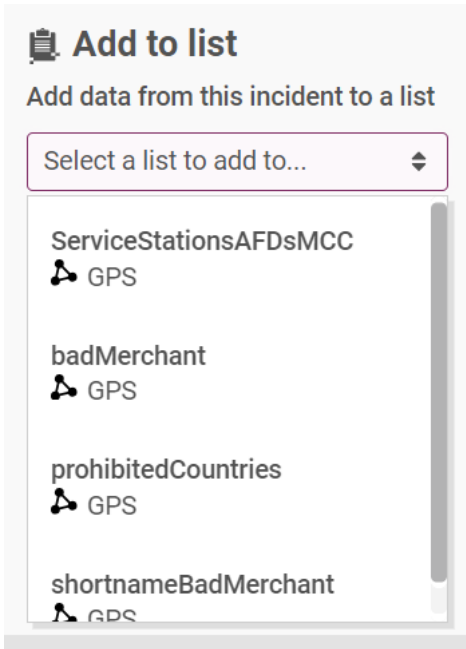
Data from an entity's event history can be added to a data list, using the 'Add to List' button in the review actions sidebar. This allows you to add an entity, IP address, device ID or other information to a list, which rules and other analytics can access. For example, add an IP address to a negative list to enable a rule to trigger an alert if any customer attempts to log in from this address.

To add new items to a data list from the Incident Review page:

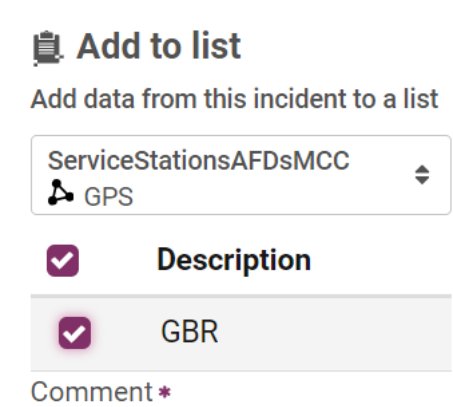
- 1. Click the **Add to List** button in the review actions sidebar.



- 2. From the drop-down list, select the data list you want to add new value(s) to.



The values to be added to the list will be shown beneath the drop-down.



Note: You can remove any values that should not be added to the data list by clicking the at the right-hand side of those values. This will remove those values from the 'Add to Data List' panel.

- 3. Add a comment in the Comment field. Alternatively, use the Comment Template drop-down field to select a template to automatically fill the Comment field.



Comment *

Please review the transactions
by checking with Card holder

Use a comment template

Add to list

Cancel

4. Click the **Add to List** button to save your changes to the data list.

Use a comment template

Add to list

Cancel



5 Viewing Events

The Events page displays a list of all historical events retained by your Fraud Transaction Monitoring System (events are stored for 90 days unless it is an alert, which is stored for a duration in line with our data retention policy). The page also displays the results of searches carried out using the search box in the header bar at the top of all pages of the portal.

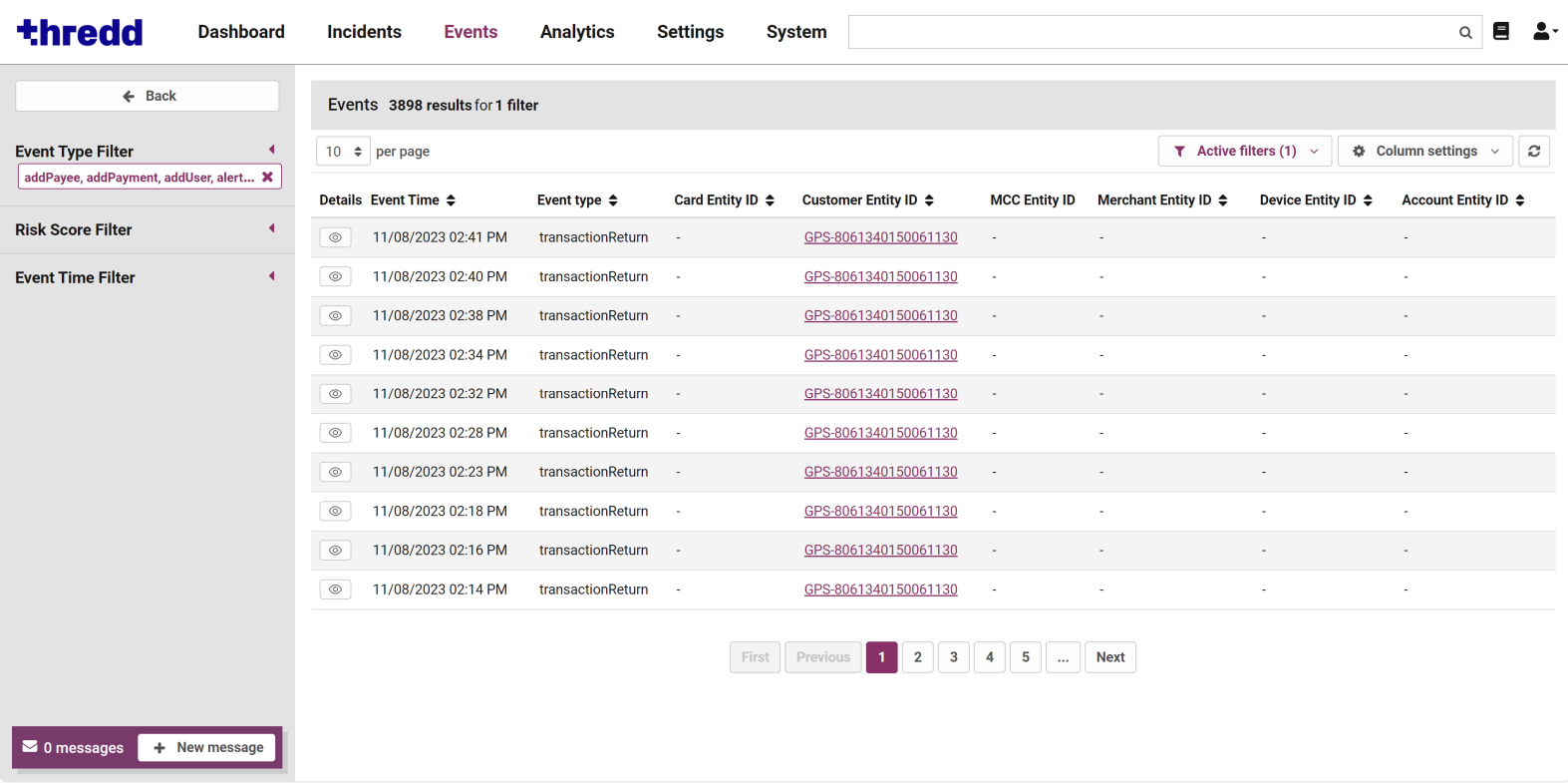


Figure 13: Events page

Note: No events are displayed in the list until you either run an events search or filter the list.

You can configure the columns of the events list, so the columns you see may not be exactly the same as the columns described below. By default, the events list shows:

- **Entity IDs:** The columns on the left show the IDs of the entities involved in the events. There is one column for each entity type in your system.
- **Event Type:** The type of event.
- **Event Time:** The date and time the event occurred.
- **Searchable fields:** By default, all searchable fields are available as columns in this view.
- **Risk scores:** The columns on the right show the overall risk score assigned to this event by analytics assigned to each entity type.

To view the incident page for an entity associated with an event: click the entity ID of the relevant entity.

Searching for Events and Entities

You can use the search box in the header of any page of the portal to search for entities and events. You can search by entity ID, or build searches to find events and entities that match a particular criteria.

To expand the search box: click the search box bar.



Fields

Entity ID
accountAgentFIBranchId
accountAgentId
accountEntityId
accountId
accountNumber
acquirerId
cardEntityId
cardId
cardPAN
companyName
counterpartyId
customerEntityId
customerId

Operators

AND add filter
OR add alternative
NOT exclude

> greater than
< less than
>= greater than or equal
<= less than or equal
* wildcard

Search preview

Enter a search query to see results.

Figure 14: Search Box

The options below the search box are divided into three sections:

- **Fields:** a list of all the searchable fields in your system. You can search for values in any of these fields.
- **Operators:** a list of operators you can use to construct searches and combine criteria.
- **Search preview:** this section displays up to ten entities with events in their histories that match your search. It also shows the number of events that match your search.


Refer to the table below for search options.

Search Option	Description
Search for a value in any searchable fields	Type the value into the search box. For example, to find all events that contain 'John' in any event field, type John. <div>Note: Put double quotes around values that contain spaces. For example, to search for all events that contain 'John Smith', type "John Smith".</div>
Search for a value in a specific field	In the Fields section below the search box, click the name of the field and then enter the value you want to search for. For example: "Customer Name":"John Smith" <div>Note: Put double quotes around search terms that contain spaces.</div>
Search for part of a value	Use the asterisk wildcard (*) to represent any text. For example, to find any event where the 'Customer Name' field begins with 'John', use the following search: "Customer Name":John*
Search in fields that contain dates or date-times	Use yyyy-mm-dd format.
Search for events between two dates	Use the format '[from date TO to date]'. For example, "from 2023-12-01 TO to 2023-12-30".
Search for a number greater than or less than a specified value	Use the operators listed in the Operators section below the search box, such as 'greater than' or 'less than'. You can insert operators by clicking on them, or by entering them manually. For example, to search for events where the value in the 'Amount' field is greater than 150, use the



Search Option	Description
	following search: "Date of birth":[1980-01-01 TO 1989-12-31
Link multiple search terms together	Use 'AND' and 'OR'. You can also use 'NOT' to exclude certain terms. You can type the word 'AND', 'OR', or 'NOT', or click the operators in the 'Operators' section below the search box. For example, to search for 'John Smith' in the 'Customer Name' field, and 1st January 1980 in the 'Date of birth' field, use the following search: "Customer Name": John* AND "Date of birth": 1980-01-01

Viewing Events that Match your search

1. Press Enter on your keyboard or click .

2. In the 'Search Preview' section, click **Events** at the bottom of the section.

Search preview

Entities

accountEntityId

[GPS-1001079878628](#)

cardEntityId

[123456789](#)

[1165363151821340](#)

[7165363151821340](#)

[2065363151821346](#)

[7065363151821340](#)

customerEntityId

[GPS-1001368468847](#)

[GPS-8061340150061130](#)

0 unreviewed alerts

0 unreviewed alerts

0 unreviewed alerts

0 unreviewed alerts

0 unreviewed alerts

0 unreviewed alerts

0 unreviewed alerts

0 unreviewed alerts

0 unreviewed alerts

0 unreviewed alerts

Events

Events


3833 events

The results of your search are displayed in the Events page. A summary of your search query is displayed above the events list.

- To view the incident page of one of the suggested entities: in the 'Search Preview' section, click that entity's ID.
- To clear your search results: on the events page, at the right of the search box, click the **X** button.

Filtering the Events List

As well as searching for events and entities using the search box, you can use the filter options in the sidebar on the left.



Dashboard

Incidents

← Back

Risk Score Filter

Event Type Filter

Event Time Filter

Events

10

Details

E

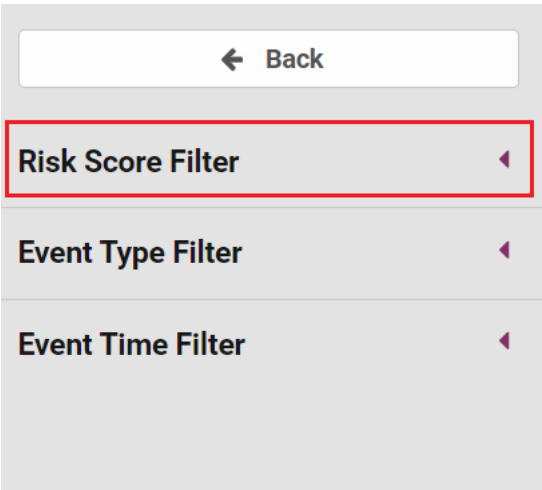


Figure 15: Filter sidebar

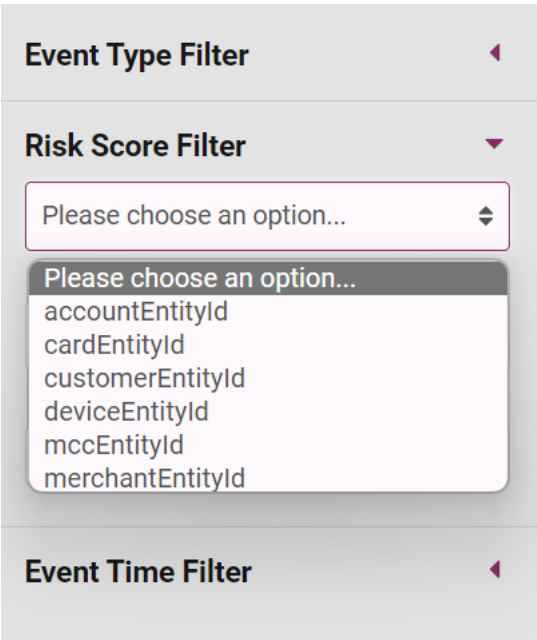
Filter by Risk Score

To filter the events list by risk score:

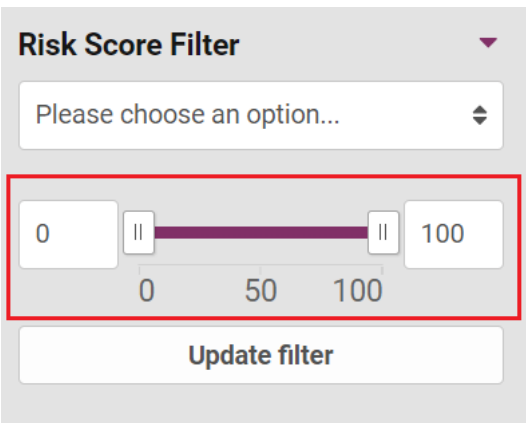
- 1. In the sidebar, click **Risk Score Filter**.



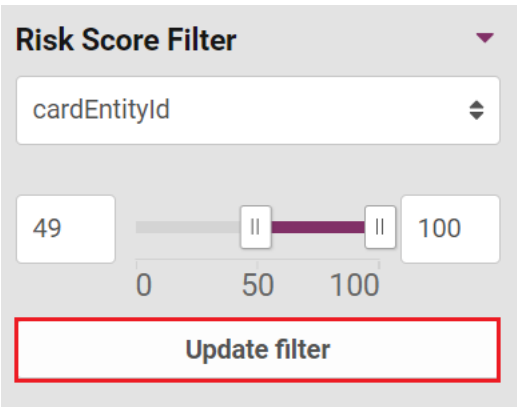
- 2. If you have risk scores for more than one entity type, select the relevant entity type from the drop-down menu.



- 3. Set the range of risk scores for the filter by either dragging the sliders or by manually entering the maximum and minimum values.



- 4. Click the **Update Filter** button.



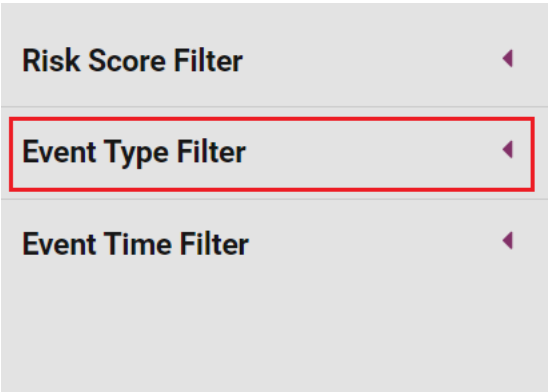


The filter appears at the bottom of the Risk Score Filter section, which you can remove by clicking **X** on the filter.

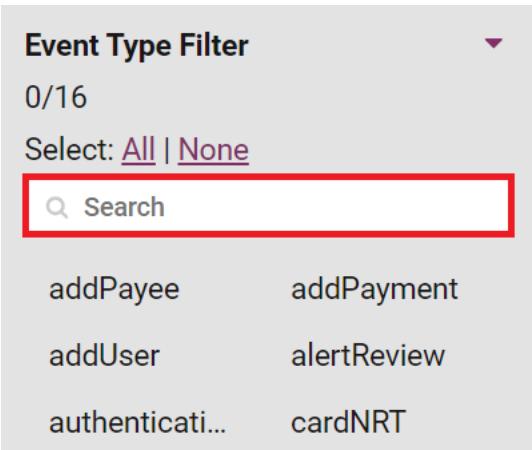
Filter by Event Type

To filter the events list by event type:

- 1. In the sidebar, click **Event Type Filter**.

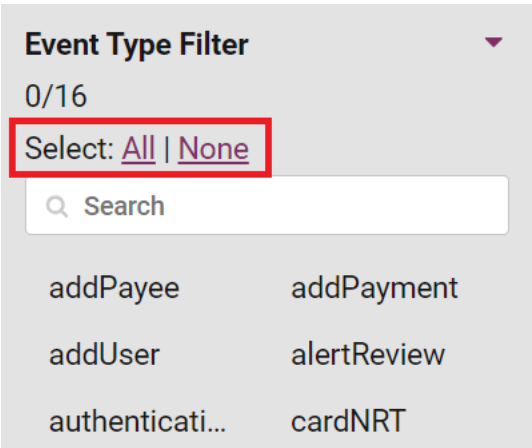


- 2. (Optional) Use the search box to find the event types you want to show or hide.



Note: Only cardRT,cardNRT and transactionReturn event types are currently supported.

- 3. (Optional) use the **All** and **None** options to select or clear the selection of all the event types. Note that when all event types are deselected, all event types are displayed in the events list.



- 4. Select or deselect the event types that you want to show or hide in the events list.



Event Type Filter

2/16

Select: [All](#) | [None](#)

Q Search

addPayee

addPayment

addUser

alertReview

authenticati...

cardNRT

cardRT

cardUpdate

changeLimits

customerAc...

login

monitoringT...

registration

transactionR...

updateCrede...

updateDetails

Update filter

5. Click **Update Filter**.

login

monitoringT...

registration

transactionR...

updateCrede...

updateDetails

Update filter

Filter by Event Time

To filter the events list by the time of the event:

1. In the sidebar, click **Event Time Filter**.

Risk Score Filter

Event Type Filter

Event Time Filter

2. In the 'From' and 'To' boxes, enter start and end dates, or select dates from the drop-down calendars.

Event Time Filter

From

01/11/2023

00:00

To

22/11/2023

23:59

Update filter



3. Click **Update Filter**.

Event Time Filter

From

01/11/2023

00:00

To

22/11/2023

23:59

Update filter

View Active Filters

You can see what filters are currently active by clicking the **Active Filters** button at the top right of the events list.

Active filters (2)

Column settings

Entity ID

Merchant Entity ID

Device Entity ID

Account Entity ID

nd...

As each active filter in the sidebar displays a summary box below it, you can also tell from this which filters are currently active.

Risk Score Filter

49 – 100 (accountEntityId)

Event Type Filter

Event Time Filter

11/01/2023 12:00 AM – 11/21/2023 1...

Although you can apply multiple filters, there can only be one filter for each category (risk score, event type, or event time).

Remove a Filter

To remove a filter, click on the X beside the filter you want to remove.

Risk Score Filter

49 – 100 (accountEntityId)

Alternatively, you can remove a filter by clicking the X beside the filter in the Active Filters drop-down.

Active filters (1)

Column settings

Risk Score Filter:

49 – 100 (accountEntityId)

Device Entity ID

Account Entity ID



The original event data keys (field names) are shown on the left. The corresponding values are shown on the right.

transactionReturn

11/08/2023 02:38 PM

Original event

metadata	
confirmedFraud	false
customerEntityId	GPS-8061340150061130
customerId	8061340150061130
decorationId	
direction	outbound

To return to the simple sidebar view, at the top of the sidebar click the Eye button.

Column Settings

You can use the column settings options to show or hide columns in the events list, add new columns, or sort the events list by up to two columns (a primary column and a secondary column. See [Sorting Events by Columns](#) for more information). Open the Column Settings window by clicking on the **Column Settings** button.

Active filters (0)

Column settings

ity ID Merchant Entity ID Device Entity ID Account Entity ID

To show or hide columns in the events list, use the check boxes on the left of each column name to select which columns are visible in the events list.

Visibility	Sorting	
	pri	sec
<input checked="" type="checkbox"/> Event Time		
<input checked="" type="checkbox"/> Event type		
<input checked="" type="checkbox"/> Card Entity ID		
<input checked="" type="checkbox"/> Customer Entity ID		
<input checked="" type="checkbox"/> MCC Entity ID		
<input checked="" type="checkbox"/> Merchant Entity ID		
<input checked="" type="checkbox"/> Device Entity ID		
<input checked="" type="checkbox"/> Account Entity ID		
+ Add column		

Add Columns to Events List

IMPORTANT: There is potential for issues to arise when adding columns. We advise speaking to your Account Manager before attempting to make any changes.



To add additional columns to the events list:

- 1. Click **Add Column** in the Column Settings drop-down.

Visibility	Sorting	
	pri	sec
<input checked="" type="checkbox"/> Event Time	⬇	⬇
<input checked="" type="checkbox"/> Event type	⬇	⬇
<input checked="" type="checkbox"/> Card Entity ID	⬇	⬇
<input checked="" type="checkbox"/> Customer Entity ID	⬇	⬇
<input checked="" type="checkbox"/> MCC Entity ID	⬇	⬇
<input checked="" type="checkbox"/> Merchant Entity ID	⬇	⬇
<input checked="" type="checkbox"/> Device Entity ID	⬇	⬇
<input checked="" type="checkbox"/> Account Entity ID	⬇	⬇

+ Add column

- 2. Enter a name that displays at the top of the column in the **Name** field.

Name

JSON path *

Create **Cancel**

- 3. Enter the path to the field that you want to display. For example, if the event data field is called 'Fee Value' and is nested in the field 'Fee', enter fee.value.

Name

JSON path *

Create **Cancel**

- 4. Click the **Create** button.

Name

JSON path *

Create **Cancel**



The new field appears in the Events List.

Edit a Column

To edit an added column:

1. Click **Column Settings**.

Active filters (0)

Column settings

ity ID Merchant Entity ID Device Entity ID Account Entity ID

2. Click **Edit** to the right of the column you want to edit.

☒ Account Entity ID

☒ Fee Value

+ Add column

3. Edit the column name or path, and then click **Update**.

Name

Fee Value

JSON path *

fee.value

Update

Delete

Cancel

Delete a Column

Note: There is potential for issues to arise when deleting columns. We advise speaking to your Account Manager before attempting to make any changes.

To delete an added column:

1. Click **Column Settings**.

Active filters (0)

Column settings

ity ID Merchant Entity ID Device Entity ID Account Entity ID

2. Click **Edit** to the right of the column you want to delete.



3. Click **Delete**.

Name

Fee Value

JSON path *

fee.value

Update **Delete** **Cancel**

Sorting Events by Columns

You can sort columns by using the primary (**pri** column) and secondary (**sec** column) attributes. You can only select one primary and one secondary column from all available columns.

Select the primary attribute for a column to sort according to this column. For example, if sorting by Last Alert Time, incidents with the newest alerts (if sorting in descending order) will be shown at the top of the Incident List.

Select the secondary attribute for a column to sort the column as the secondary sort attribute. If two or more items in the list have the same value of the primary sort attribute, they will be sorted according to this column.

To sort the events list by two columns:

1. Click **Column Settings**.

A screenshot of the 'Column settings' menu in the Data Explorer. The menu is open, showing a list of columns: 'Entity ID', 'Merchant Entity ID', 'Device Entity ID', and 'Account Entity ID'. The 'Entity ID' column is highlighted in blue. The 'Column settings' button is circled in red.

2. Use the arrow icons in the **pri** column to select a column for primary sorting and its sort order as ascending or descending.

Visibility

☒ Event Time

☒ Event type

Sorting

pri sec

▲ ▼

▼ ▼

3. Use the arrow icons in the **sec** column to select a column for primary sorting and its sort order as ascending or descending

Visibility

☒ Event Time

☒ Event type

Sorting

pri	sec
▲	▼
▼	▲

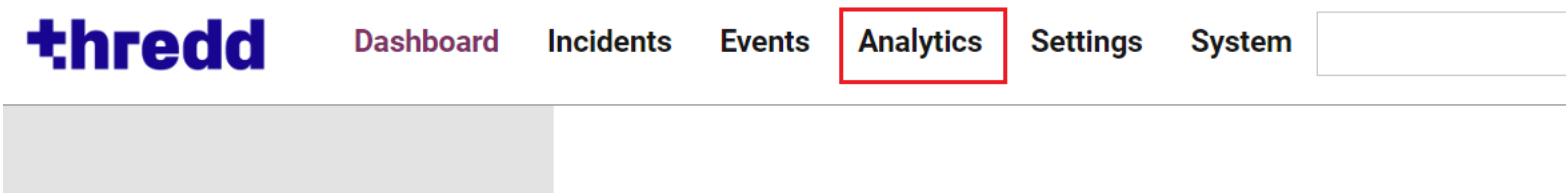
Note: The changes you make to the events list are specific to you.



6 Analytics Configuration

This section of the user guide describes how to create, configure and manage rules, aggregators and other analytics, as well as the process for reviewing and authorizing changes to your portal analytics configuration.

Click **Analytics** to open the Analytics section of the UI.



The portal has a built-in workflow for modifying analytics configuration (risk thresholds, rules, aggregators) and reviewing and approving these changes. Any changes to analytics configuration are made in a staging environment. These changes are not live (and hence do not affect the generation of alerts, the assignment of tags) until they are submitted for review and then approved by a user with the appropriate permissions.

There are two ways to configure the portal's user roles and permissions to ensure a "four eyes" authorization process.

- Risk analyst makes changes and risk manager approves them
- Risk manager makes and approves their own changes

The default approach is to have two different user roles, one with permission to make analytics changes and submit them for review (but not approve or reject those changes), such as a Risk analyst, and one with permission to approve or reject changes (but not submit them for review), such as a Risk manager. This means that a user with one role can make changes in the staging environment but not approve/reject, and a user with the second role can approve changes but not make them.

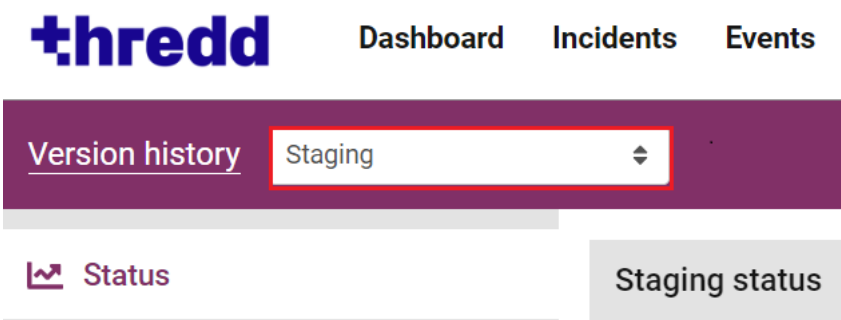
A different approach is to enable users with a specific role (for example, Risk Manager) to make changes, submit them for review, and approve or reject analytics changes, through granting them both the 'Analytics Version Acceptor' and 'Analytics Version Creator' permissions. This enables an individual user to make analytics changes and submit them for review, but not approve or reject an analytics staging version that contains changes they made. This means that a user can approve or reject changes made by other users, but never their own changes, ensuring a "four eyes" authorization process.

There is a third permission, Accept or reject own analytics changes, which enables a user to accept or reject an analytics version that they have made changes to. Whatever the configuration of your other user roles, a user with all three permissions can push changes directly from staging to live without needing another user to review them.



Viewing Analytics Versions

The Analytics section of the UI has a unique feature - the Analytics version bar, which appears at the top of the section, between the portal header and the main page and sidebar. When you first open the Analytics section, you are viewing the staging environment. This is where you can make changes to analytics configuration.

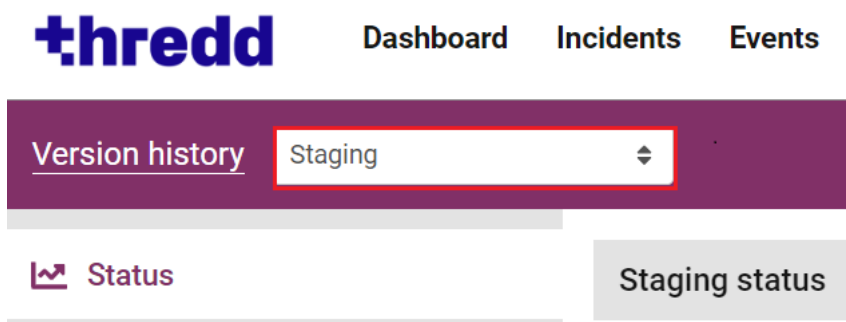


You can navigate the Analytics staging environment (and other analytics versions) in the same way as any other UI section. Links in the sidebar allow you to navigate to the individual pages for viewing the different kind of analytics configurations, and changing the configurations in staging.

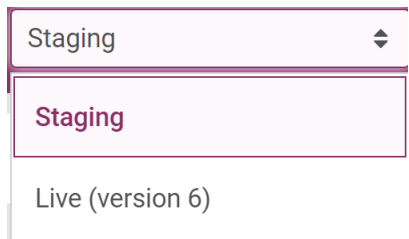
Note: When viewing the live environment, or a historical version, you will not be able to make any changes, only review the configuration of the various analytics.

To view different versions of your analytics configuration:

1. Click the **Version history** field.



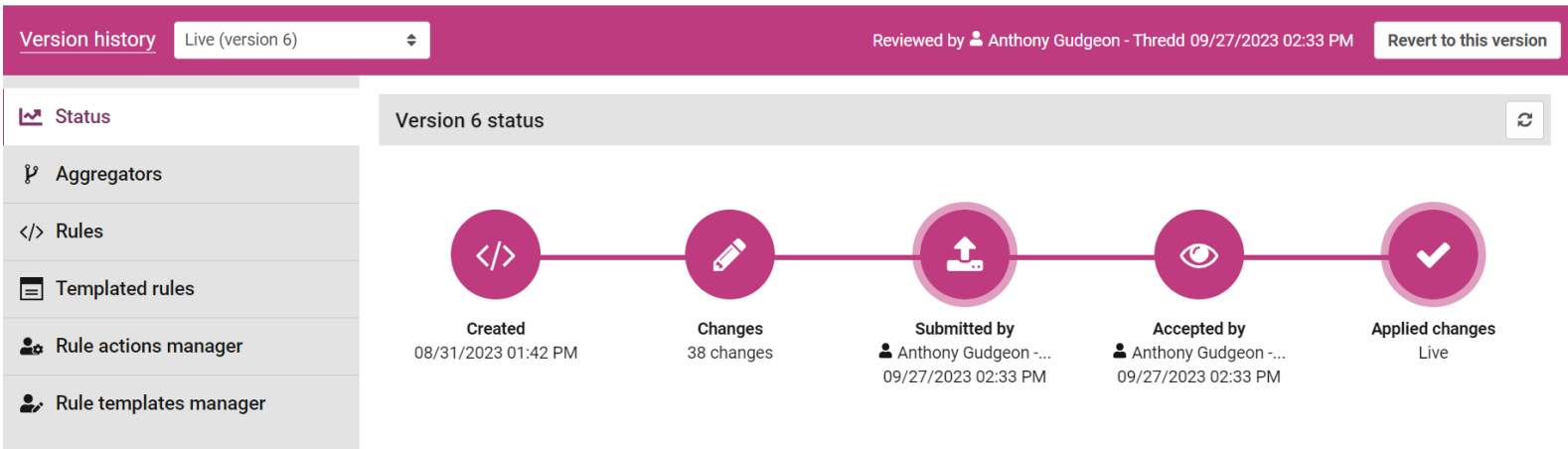
2. Click the version you want to view in the menu.



Note: Analytics configuration can only be edited in the Staging environment.

You cannot make changes when you view the live environment or a historical version, only review the configuration of the various analytics. Click the **Version history** button to see a full list of historical analytics versions.

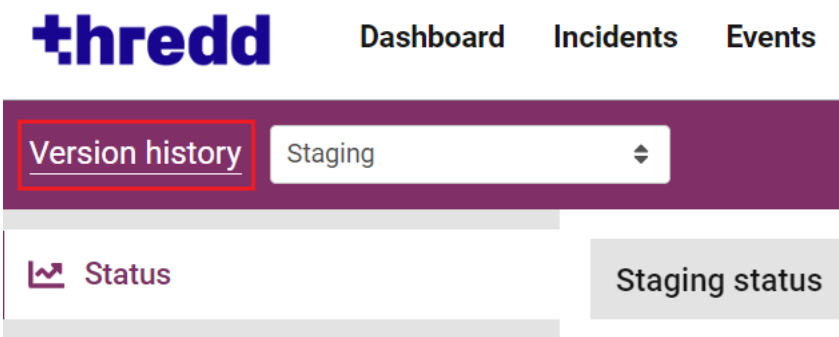
The analytics header bar will change colour to pink when you view the live analytics configuration, and show the date and time the current configuration was reviewed and approved. The username of the reviewer will appear on the right.



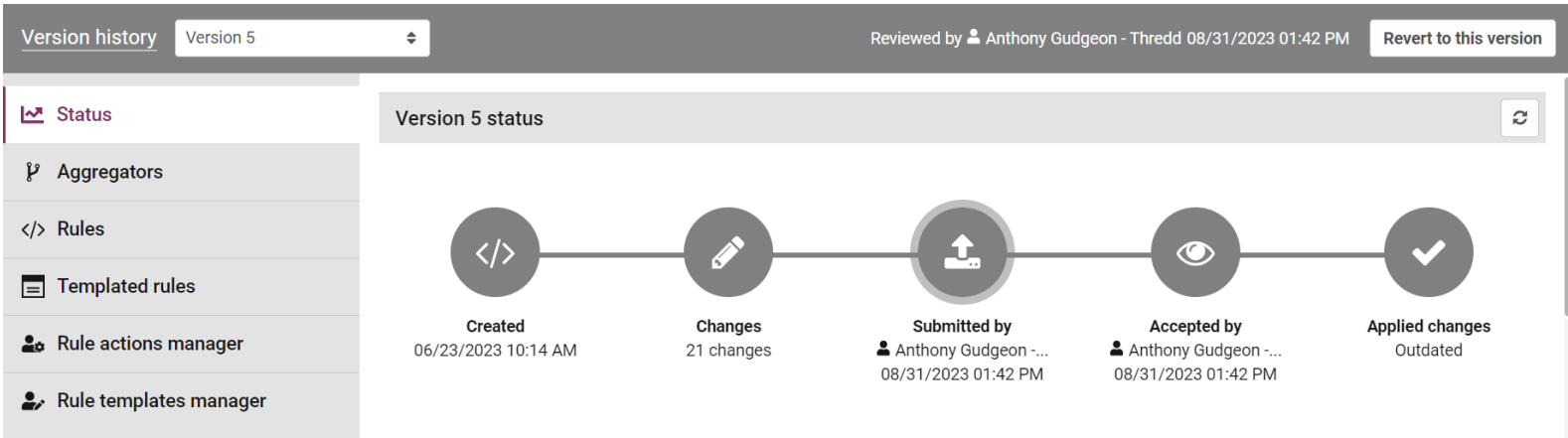


Viewing a historical analytics configuration version

To see a historical analytics configuration version click the **Version History** button.



When viewing a historical version, the analytics header bar will change colour to grey. The user who reviewed the changes will show on the right, with the date and time changes were reviewed.



The version status will be shown in the flow chart. The decision after reviewing changes can be either:

- **Approved:** the changes in this version were approved and promoted to the live environment.
- **Rejected:** the changes in this version were rejected and did not go live.
- **Cancelled:** the user who originally submitted this version for review cancelled the review before it was approved or rejected.

Business Rule Profile

The Business Rule Profile section, below the version status section, contains information on global behavioral profile data (global states) stored for all entities. Global states build up population-level entity profiles over time as more behaviours are captured. The exact definition of what population-level data is stored and displayed is controlled by expressions which are written and managed in the Rules page, in the Analytics section.

Business rule profile		Expand all	Copy all
ACCOUNT	-- no data --		
CARD			
CUSTOMER	-- no data --		
DEVICE	-- no data --		
MCC	-- no data --		
MERCHANT	-- no data --		

Data stored by global states for each entity type is displayed in two columns:

- The left column indicates the variable name
- The right column displays the stored data

CARD	
averageAmount	66.58597

This data may be one of the following types, as indicated by the icon to the left of the variable name:



- String (including time stamp data)
- Integer
- Number
- Boolean
- Collection of multiple values

Note: Collections containing multiple values will by default be displayed in collapsed form.

To expand a collapsed collection and show the individual elements, click the right-facing arrowhead to the left of a collapsed collection's name.

Business rule profile	
ACCOUNT	-- no data --
CARD	
CUSTOMER	-- no data --

To expand all collections shown in the Business Rule Profile, click the **Expand all** button at the top of the Business Rule Profile section.

Expand all

Copy all

--

--

To copy the entire global state profile to the clipboard, click the **Copy all** button at the top of the Business Rule Profile section.

Expand all

Copy all

--

--

To copy an entity type's global state or individual value to the clipboard, including all variables, hover your mouse cursor over an individual entity type or value in this section. Then click on the clipboard and paper icon.

Business rule profile		Expand all	Copy all
ACCOUNT	-- no data --		
CARD			
1 averageAmount	66.58597		

Viewing changes made to an aggregator

To see the changes made to a specific aggregator, feature, rule, model, or Analytical Workflow, click anywhere on the row showing the name of the relevant analytic.

Rules	
Name	Change
> CARD:state.GPSfirsttransactionDate	Added



The differences between the staging configuration and the version you are comparing to display underneath. Elements that are present in the version you are viewing but not in the previous version (i.e. elements that have been added) are highlighted in green; elements that are present in the previous version but not in the version you are viewing (i.e. elements that have been removed) will be highlighted in red.

</> Rules

Name	Change
ACCOUNT:state.accountName	Edited

Change: edited

Version 6 Live

Version 3 Accepted

Directory

accountEntityId/Display States

Enabled

true

Directory

accountEntityId/Display States

Enabled

true

@eventType("updateDetails")
@eventType("cardRT")
state.accountName: event.customerName.fullName

@eventType("updateDetails")
state.accountName: event.customerName.fullName

To view the differences between historical versions, click the **Compare Versions** button.

Configuration difference

Viewing changes from

Version 6

 →

Staging

Compare versions...

A window will display, where you can select the versions to compare.

</> Compare versions

Compare changes from the following versions:

Version 6
Live 09/27/2023 02:33 PM

→

Version 5
Accepted 08/31/2023 01:42 PM

Configuration Difference

The Configuration Difference section at the bottom of the page shows how the analytics configuration in the version you are viewing differs from the previous or another version. For example, on the staging environment, you can see the differences between the staging environment and the live environment. If you view the live environment, you can see the differences between the live environment and the previous analytics configuration version.

Configuration difference

Viewing changes from

Version 6

 →

Staging

Compare versions...

New 1 Edited 0 Removed 0

</> Rules

Name	Change
CARD:state.GPSfirsttransactionDate	Added

Configuration Difference displays a list of the changes, categorized based on the various analytics configuration pages. Each row shows the name of the analytic that was changed, and the type of change:

- Added** - for an aggregator, feature, risk level, model, rule that is present in the configuration version being viewed, but not in the previous version.
- Removed** - for an aggregator, feature, risk level, model, rule that is present in the previous configuration version, but not in the version being viewed.



- **Edited** - for an aggregator, feature, risk level, model, rule that is present in both the configuration version being viewed and in the previous version, but has been edited in one way (e.g. a risk threshold changed, or a rule altered, activated or deactivated).

BIN Attacks

A BIN attack is a type of automated card fraud attack that if successful can affect hundreds or even thousand of cards and customers, and have a potentially catastrophic impact. BIN attacks are ultimately an attack on the card issuer, but can affect merchants and/or card acquirers, as fraud losses can potentially be 'charged-back' by the card issuer.

BIN attacks can occur by:

1. **Targeting a bank's BIN**

The fraudster chooses a financial institution to target, and acquires their Bank Identification Number (BIN). These numbers are public knowledge, so they are very easy to acquire and serve as an ideal starting point for someone attempting to perform a brute-force attack.

2. **Generating possible card numbers with software**

The BIN is only a portion of the full card number, so the fraudster has to generate possible account numbers for the card. While this can be done manually, typically, fraudsters employ software to generate possible card numbers based on the BIN they are targeting. This enables the fraudsters to generate thousands of potential card combinations for the financial institution they are attacking very quickly.

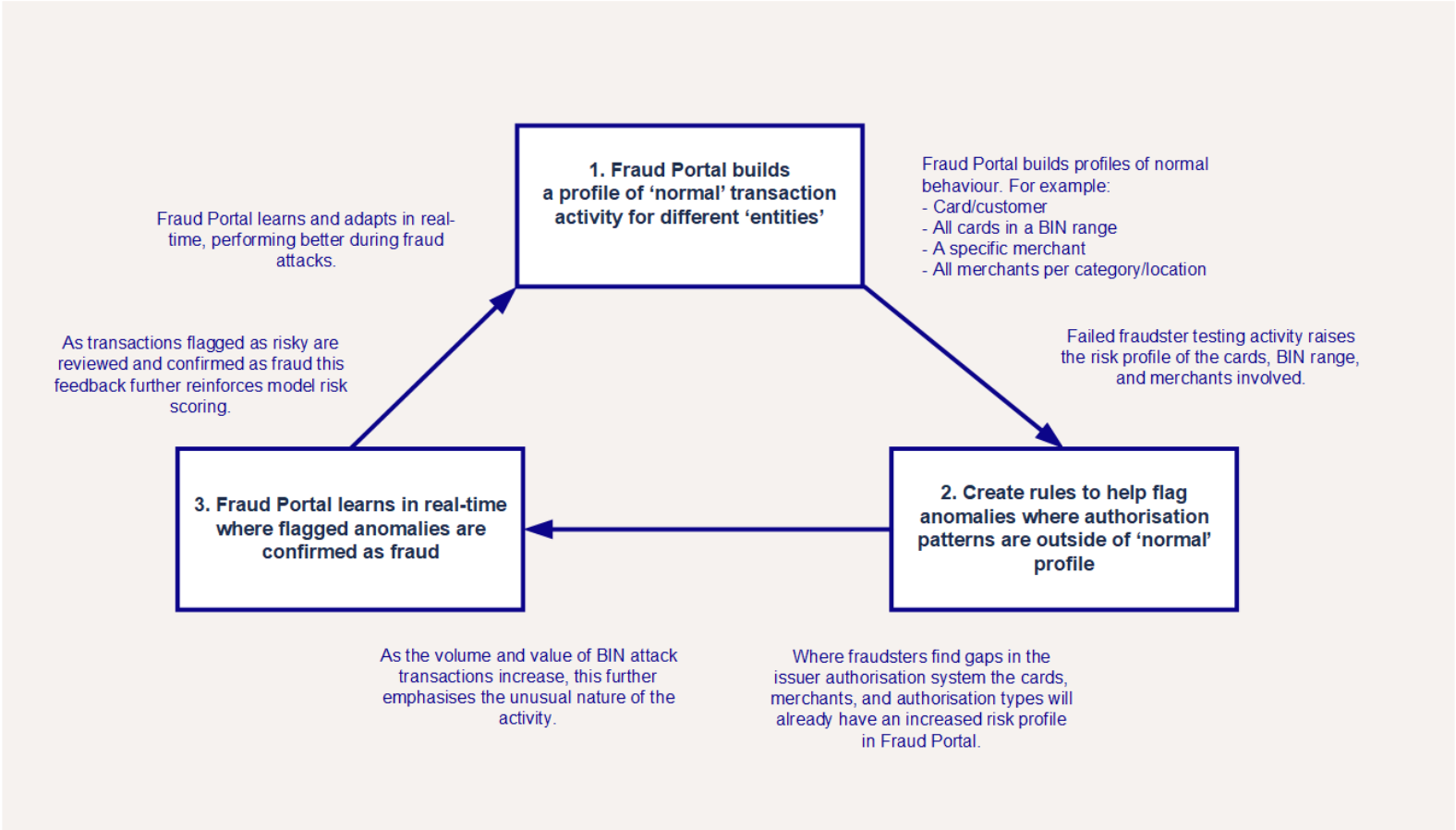
3. **Testing BINs**

When the fraudsters have generated card numbers, they need to test to ensure that the credentials work and they can complete a purchase. Essentially, they are verifying which cards can be used for fraud. The fraudster will perform a series of small transactions with each number until they succeed.

4. **Perform Fraudulent Transactions**

When a card is successfully used to make a fraudulent transaction, the fraudsters store the information so they can make further fraudulent transactions with it. This is so that when they've tested the card works and have the proper credentials, they can begin to commit fraudulent transactions. The fraudster can then continue to commit fraud using the stolen credentials until the card is cancelled or the authentication credentials are changed.

To protect against BIN attacks issuers need to adopt a multi-layered strategy including product design, authorisation system strategies, real-time fraud detection, and tried-and-tested response processes.



The Fraud Transaction Management Portal is well-placed to defend against BIN attacks, helping to overcome weaknesses in issuer or acquirer defences. The Portal uses a unique Adaptive Behavioural Analytics approach that profiles 'normal' behaviour and identifies anomalies, with rules that are able to learn in real-time.



How Thredd can Help Mitigate BIN Attacks

The Adaptive Behavioural Analytics approach flags anomalies where flagged transactions confirmed as fraud provides real-time feedback to the model, which can prevent fraud attacks from scaling. As flagged transactions are confirmed as fraud this provides real-time feedback to the model, which can prevent fraud attacks from scaling.

You can help to prevent BIN attacks by setting up rules in Fraud Portal to capture them. For example, when several low volume authorisations happen for the same value in a very short space of time we recommend setting up stateful rules to manage this. Attacks like card testing and enumeration are different from normal cardholder behaviour, so you can use stateful rules to detect these attacks in real-time. These rules use constantly updating entity profiles to check if a merchant is under attack, returning a BIN attack tag alongside the model score.

For example, if a rule detects 10 declines with a response code of 14 from 10 different cards in 30 seconds, it flags the merchant as under attack and a BIN attack reason code is applied. If the rule doesn't trigger again in 3 hours, then the merchant is no longer considered as under attack. It will be scored normally by the model in either case.

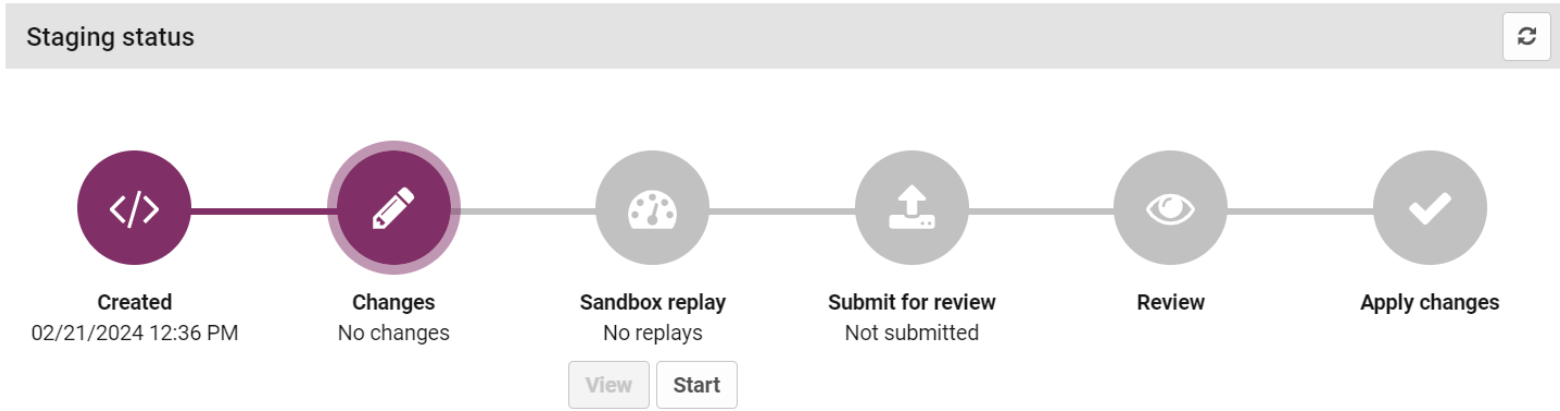
Note: For information on how to build rules that can help prevent BIN attacks, see the [Fraud AMDL Rules Configuration Guide](#).



7 Sandbox Replay

Sandbox Replay allows users to test the effects of changes made to analytics in the staging environment. This feature lets you see how a new analytics configuration would have performed over a selected historical period (for example, over the past 30 days), compared to how the live system performed over the same period. Tests carried out in Sandbox Replay do not affect the live environment.

Note: Users must have the Sandbox Replay permission to use the Sandbox Replay functionality. Contact your Account Manager to purchase the option.



The Sandbox Replay icon displays the running Sandbox Replays for your analytics version. This is usually the staging version, which contains the changes that you might want to test before submitting for approval. Below the Sandbox Replay icon, you can see the status of any replays that have been run or are currently running.

- **No Replays** indicates that no replays have yet been run for this particular analytics version.
- **Pending** indicates that a Sandbox Replay has been configured and created, but is waiting for the relevant service to become available before it can be run. When the service becomes available the status changes to 'Claimed'.
- **Claimed** indicates that a Sandbox Replay has been started, and the relevant service is ready to run it. When the Sandbox Replay is running, the status changes to 'Running'.
- **Running** indicates that a Sandbox Replay is being run, and the percentage completion is shown to indicate the progress of the replay. When the replay is complete, the status changes to 'Completed'.
- **Completed (Up-to-date)** indicates that there is at least one completed Sandbox Replay for the analytics version you are viewing (usually the staging environment). 'Up-to-date' indicates that this completed replay used the up-to-date configuration for this version.
- **Completed (Out of date)** indicates that changes have been made to this analytics version since the replay was run.



Create a Sandbox Replay

When creating a new Sandbox Replay, you need to specify options that determine how the replay is run, the time period it applies to, and other parameters that can have a significant effect on how long the replay takes to run.

Run sandbox replay

Name of replay * is required

Name of replay

Select date range

From

26/02/2024

13:58

To

27/02/2024

13:58

State profile build-up period ?

From

26/02/2024

13:58

To

26/02/2024

16:22

Percentage

10

%

Label waiting period ?

From

27/02/2024

11:34

To

27/02/2024

13:58

Percentage

10

%

Time allocation overview

State profile build-up period: 2 hours

Event processing: 19 hours

Label waiting period: 2 hours

Sandbox replay date range: 1 day

The fields available in the window are detailed in the table below:

Option	Description
Date Range	The date range to consider when running the replay. Events between the start and the end date are processed when running the replay (however, not all events in this period may be processed).
State profile build-up period	A Sandbox Replay starts with no behavioural profile data. Starting with no behavioural data ensures that business rules that make use of behavioural profiles deliver more accurate and less misleading results. The state profile build-up period is a period at the beginning of the replay that allows behavioural profile data to build up for the related entities. No alerts are created during this period as none of the authorisations are assessed for fraud. Authorisations are only assessed after the state profile build-up period and before the label writing period.
Label waiting period	The label waiting period allows for label events such as chargebacks or confirmed fraud reports to be taken into account at the end of the replay time period. Because data might be received some time after the original event, no alerts are created during this period as none of the authorisations are assessed for fraud. Authorisations are only assessed after the state profile build-up period and before the label writing period.
Sampling type	<div>In a production environment, a large number of events is typically ingested and processed by the system over the duration of a Sandbox Replay. Using all of these events when running a replay would result in a very long processing time, so Sandbox Replay uses downsampling to reduce the number of events that must be processed. It does this by randomly selecting a percentage of entities of a given type and processing all events from the selected time range that contain those entities. There are two sampling approaches that you can select:</div> <div><div><div>• Live: A replay that uses live sampling selects entities randomly during the execution of the replay. This means the replay can take longer to execute, but allows you to select what percentage of entities to use, and whether to select in a truly random fashion.</div><div>• Pre Sampled: A pre-sampled replay uses a pre-selected sample of entities (10% of the selected entity type). Because these entities are selected at the time the event is processed, sampling does not have to be carried out as</div></div></div>

© Thredd 2025

Fraud Transaction Monitoring Portal Guide

53

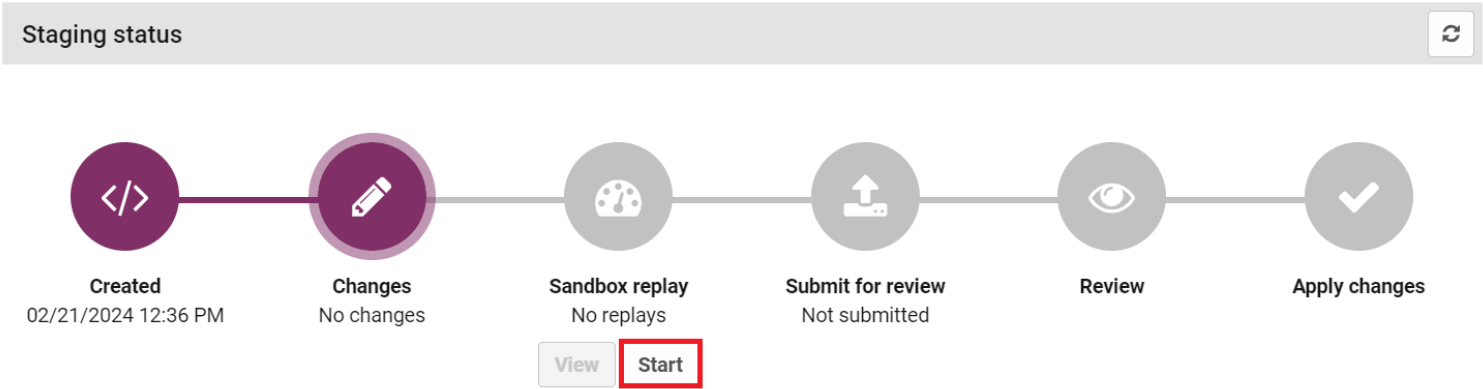


Option	Description
	part of the replay, significantly reducing the time required to execute the replay.
Entity type	(Live sampling only): The entity type to select the sample from.
Risk sampling	(Live sampling only): If you choose to include all events marked as risk in the sample, all entities of the selected type associated with events marked as 'risk' are included in your replay. That includes events labeled as 'risk' by user alert reviews, or by known fraud data such as chargebacks or confirmed fraud reports.
Sampling percentage	(Live sampling only): The percentage of entities that are selected at random to run your changes against. If you choose to include all events marked as 'risk', all entities with an event labeled as 'risk' are included in the sample, combined with randomly-selected entities to make the number up to the selected percentage. The higher the percentage, the longer it can take to run your replay. The time taken to run the replay depends on how many events occurred in this period, and how many analytics changes are being tested.
Random sampling	(Live sampling only): If you choose to randomize your sample, a different random sample of entities are selected each time you run a replay. Otherwise, the same sample of entities are used each time you run a replay over the same time period.

Create a Replay

To create a replay:

- Click **Start** under the Sandbox Replay icon to open the Run Sandbox Replay window.



The Run Sandbox Replay window opens.

- Enter the name of the new replay in the **Name of Replay** field.

Run sandbox replay

Name of replay *

Replay 1

Select date range

From

27/02/2024

14:50

To

28/02/2024

14:50

State profile build-up period

From

27/02/2024

14:50

To

27/02/2024

17:15

Percentage

10

%

- Select a date range for the replay using the From and To date fields. Clicking on the downwards arrow to the right of the box displays a calendar where you can select your start date. You can perform the same action for the end date.



Run sandbox replay

Name of replay *

Replay 1

Select date range

From

27/02/2024

14:50

To

28/02/2024

14:50

State profile build-up period ?

From

27/02/2024

14:50

To

27/02/2024

17:15

Percentage

10

%

4. Define the length of the state profile build-up period at the start of the replay as either:
- a. Enter a percentage of the replay period or leave the length as the default of 10%.
 - b. Select the check-circle beside 'From' and select a specific date and time at which to end the state profile build-up period.

Run sandbox replay

Name of replay *

Replay 1

Select date range

From

27/02/2024

14:50

To

28/02/2024

14:50

State profile build-up period ?

From

27/02/2024

14:50

To

27/02/2024

17:15

Percentage

10

%

5. Define a label waiting period at the end of the replay as either:
- a. Enter a percentage of the replay period or leave the length as the default of 10%; or
 - b. Select the check-circle beside 'From' and select a specific date and time at which to end the label waiting period.

Label waiting period ?

From

28/02/2024

12:27

To

28/02/2024

14:50

Percentage

10

%

Time allocation overview

State profile build-up period: 2 hours

Event processing: 19 hours

Label waiting period: 2 hours

Sandbox replay date range: 1 day

The time allocation overview below these sections indicates:

- The total date range of the replay.
 - The length of the state profile build-up and label waiting periods.
 - The length of the period between these in which analytics results are quantified and compared.
6. Select the entity type the replay runs for from the drop-down menu.

Entity type *

accountEntityId
cardEntityId
customerEntityId
deviceEntityId
mccEntityId
merchantEntityId

Sampling ?

Configuration ?

7. Select the sampling type as either:
- a. Default (live, randomized sampling with a 10% sample size, including all events labeled as 'risk'.); or
 - b. Custom. Selecting this option displays the Sampling Type Live and Pre-sampled fields



Entity type *

accountEntityId

Sampling ?

☒ Default (live; 10%; include all events labeled risk, randomized sampling)

☐ Custom

Note: We highly recommend using the Default option. The custom option can include accessing hundreds of thousands of authorisations which can lead to a long assessment.

8. If you selected live sampling, set the parameters that determine how entities are sampled:
- a. Select the 'Risk sampling' check box to include all events labelled as 'risk' in the sampling (this is the default), or clear the check box to sample entities randomly across the whole population.

Sampling ?

☐ Default (live; 10%; include all events labeled risk, randomized sampling)

☒ Custom

Sampling type ?

☒ Live

☐ Pre-sampled

Risk sampling ?

☒ Include all events labeled as risk in the sampling (recommended)

Sampling percentage

10

Random sampling ?

☒ Randomize the downsampling

- b. Select a sampling percentage (the percentage of entities that are selected).

Sampling ?

☐ Default (live; 10%; include all events labeled risk, randomized sampling)

☒ Custom

Sampling type ?

☒ Live

☐ Pre-sampled

Risk sampling ?

☒ Include all events labeled as risk in the sampling (recommended)

Sampling percentage

10

Random sampling ?

☒ Randomize the downsampling

- c. Select the 'Random Sampling' check box if you want a new random sample of entities to be selected each time you run the replay (this is the default).

Sampling ?

☐ Default (live; 10%; include all events labeled risk, randomized sampling)

☒ Custom

Sampling type ?

☒ Live

☐ Pre-sampled

Risk sampling ?

☒ Include all events labeled as risk in the sampling (recommended)

Sampling percentage

10

Random sampling ?

☒ Randomize the downsampling

9. Enable or clear the Configuration checkbox to include all or specific analytics from staging.

Configuration ?

☒ Include all features, rules (not including templated rules), and third-party models, as well as aggregators that use these as inputs, from staging and live (recommended)



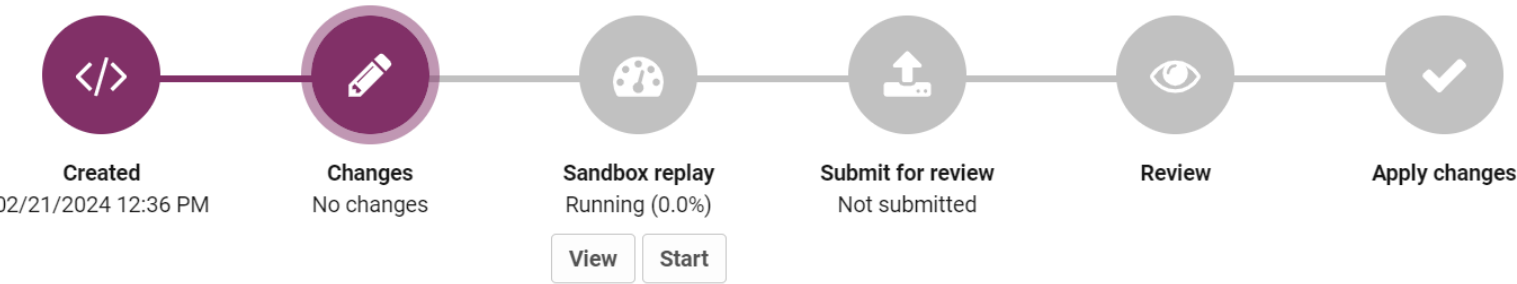
You can use the tabs and check boxes to manually select the analytics you want to include.

10. Click **Run Sandbox Replay**.

past, it will not keep any profiles from this time or

Run sandbox replay

The Sandbox Replay status changes to 'Pending'. The Sandbox Replay window, and the Sandbox Replay icon in the analytics configuration workflow, shows the progress of your replay.



View Sandbox Replay Results

When the replay has finished, click View below the Sandbox Replay icon on the Analytics Status page to see your results. The most recent replay appears first. To see the results of older replays, select the replay you are interested in from the "Select Replay" drop-down at the top of the results window.

Sandbox replay

Select replay *

Replay 1 (02/29/2024 09:50 AM)

Operation ID

65e053659d3ec043e14b94e5

Replay status

✔ Completed

Configuration status

✔ Up-to-date with staging configuration

The 'Results' tab displays the count of alerts that would have triggered in both the Live and Staging (Replay) environment with your new configuration, as well as:

- **True Positives:** Alerts that were reviewed as risk or events that were automatically flagged as high risk (e.g. confirmed fraud).
- **False Positives:** Alerts generated by genuine transaction.
- **Missed:** Events labeled as 'risk' that did not generate alerts (also known as a false negatives).



Results		Configuration		
Results		Full results: Export CSV		
Name	Count of alerts	True positives	False positives	Missed
Live	1	0	0	0
Replay	1	0	0	0

You can export results as a CSV file by clicking **Export CSV**. This file includes a detailed summary of every incident generated by the live analytics configuration during the time window selected, and incidents that would have been generated by the staging configuration. These include entity details, risk scores, and a list of rules that (would have) triggered and tags that have been assigned.

Results		Configuration		
Results		Full results: Export CSV		
Name	Count of alerts	True positives	False positives	Missed
Live	1	0	0	0
Replay	1	0	0	0

If results are not conclusive, or you want to run the replay again with new configuration, the replay can be deleted by clicking **Delete Replay**.

[Refresh](#)

[Delete replay](#)

Results		Configuration		
Results		Full results: Export CSV		
Name	Count of alerts	True positives	False positives	Missed



8 Reports

The Reports page provides a reporting capability that works across solutions and tenants. Using a powerful and fast backend database with report visualization capabilities, Reports enables customers to manage operations, analytics, and solution-specific needs all in one place.

The Fraud Transaction Monitoring Portal provides customers with out-of-the-box reporting for operations, analytics, and solutions that can be used by any customer and financial crime team.

For each report, users will be able to apply further filters and adapt the data in charts through a range of UI-based tooling. Filters include time range, value, volume, tenant, status, rules, and model. These data manipulation tools can be applied through the filter section in the UI or by engaging with specific elements within the charts themselves.

Click Apply to save any changes to the filters.

Time Filter

TIME RANGE

2024-09-26T08:46:48 s col < 2024-10-26T08:46:48

TIME GRAIN

Day

Filter

ALERT SOURCE

Type or Select [Alert Source]

INVESTIGATOR

Type or Select [Investigator]

SOLUTION/TENANT

Type or Select [Solution/Tenant]

REVIEW STATUS

Type or Select [Review Status]

EVENT TYPE

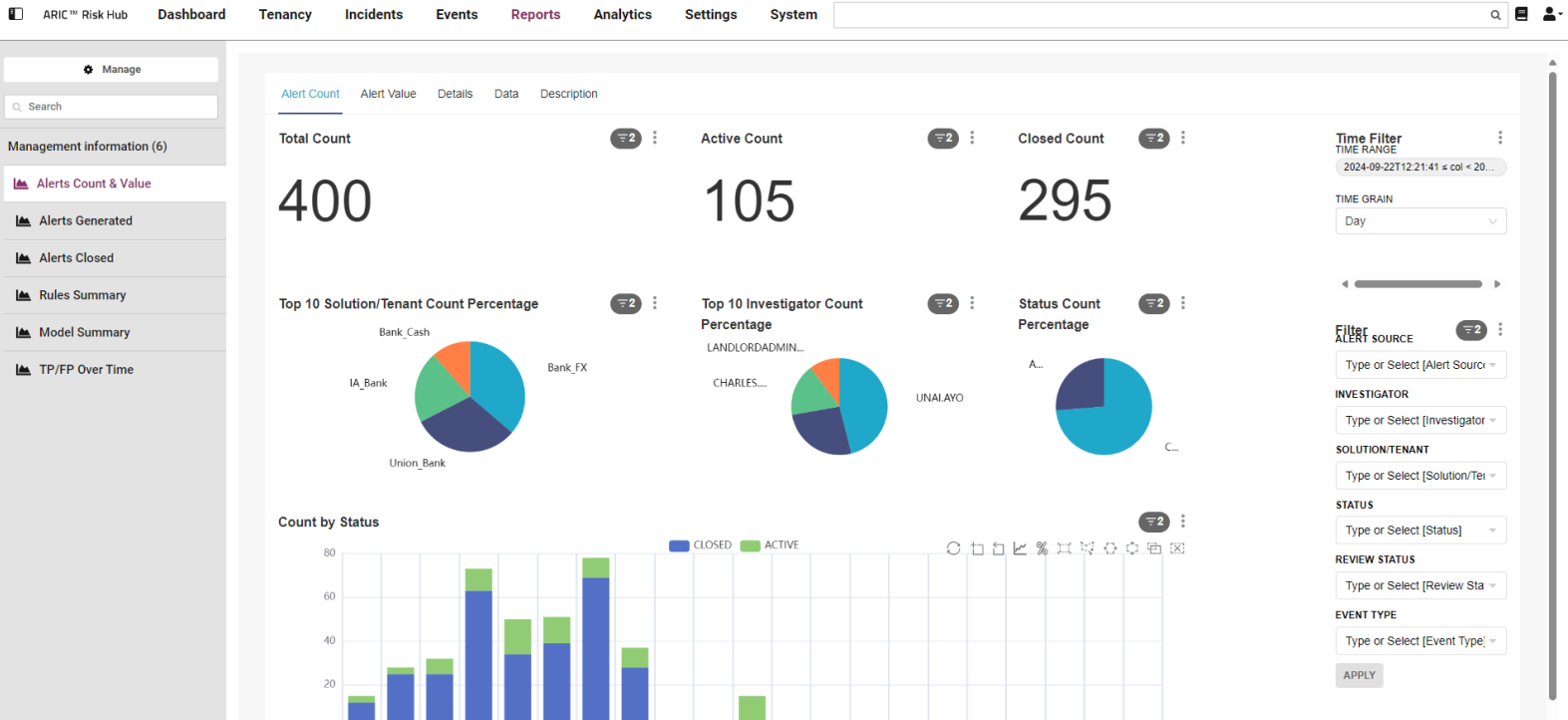
Type or Select [Event Type]

STATUS

Type or Select [Status]

APPLY

Note: For customers with multiple tenants, reports can be broken down per tenant or across multiple tenants depending on each user’s privileges. For example, a tenant level user will only have access to reports for their tenant while a landlord user will have greater access to data across tenants. This access is aligned with the permissions associated with each user role.



There are six reports that are available out-of-the-box.

Report	Description
Alerts Count and Value	Provides an overview of the open and closed alerts in the date range selected.



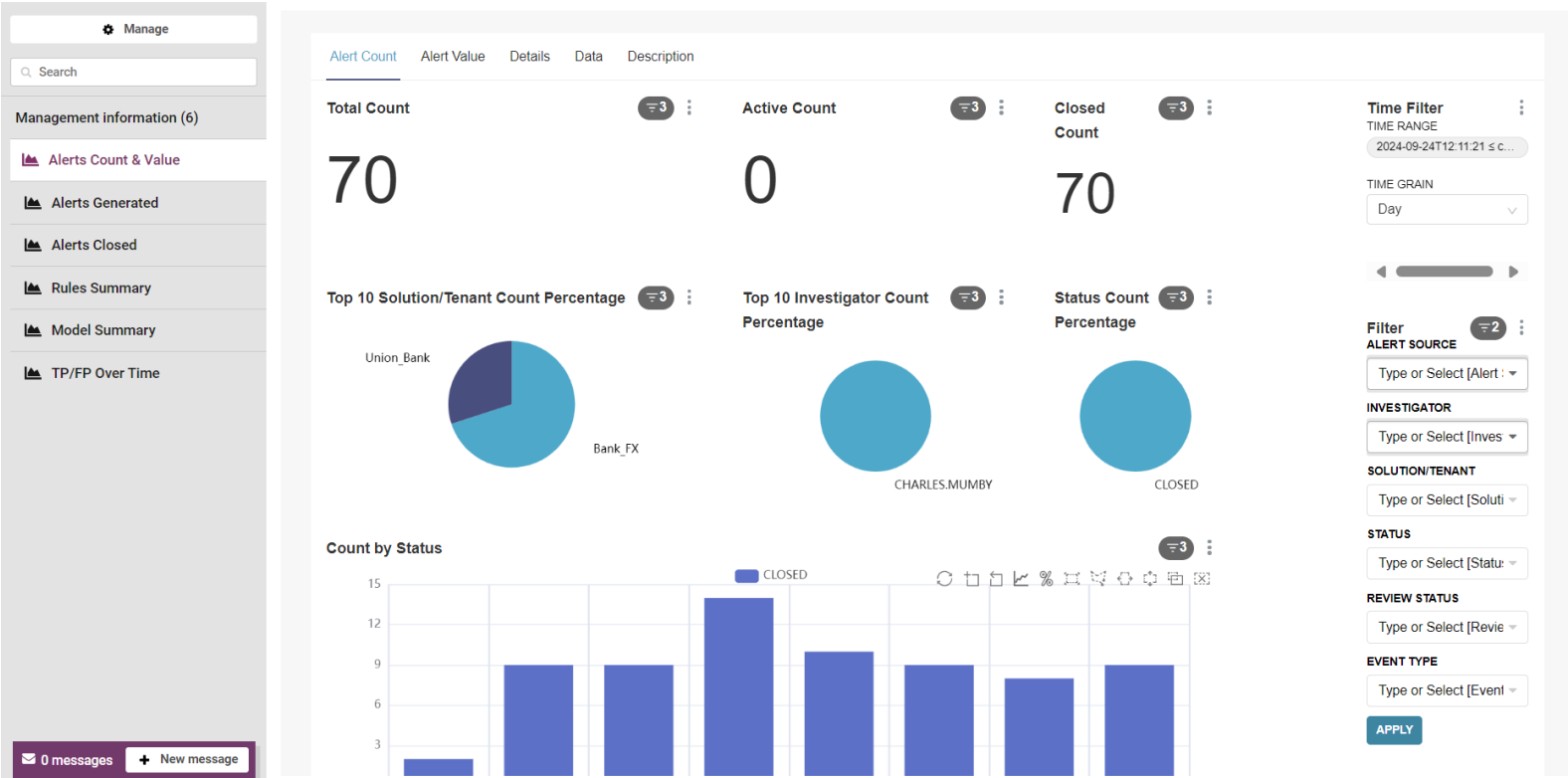
Report	Description
Alerts Generated	Provides information about the total number of alerts generated in Fraud Transaction Monitoring Portal in a configurable time window.
Alerts Closed	Provides an overview of Closed alerts in the time range selected.
Rules Summary	Provides the number of rules triggered over time, grouped by rule.
Model Summary	Provides an overview of model performance across a specified time range.
TP/FP Over Time	Provides an overview of the analytics reports, showing values, volumes and rates through time, across all analytics measurements.

Note: All reports can be configured to suit your needs. If you need to revert back to the base report, contact Thredd.



Alerts Count and Value Report

The Alerts Count & Value report provides an overview of the open and closed alerts in the date range selected. This enables a manager or supervisor to quickly assess how many alerts have been generated, actioned, and what alerts still require review. The data available in this report can be narrowed down to the individual investigator level, which helps determine how the workload is spread. This report also enables an accurate count of the alerts generated and can show trends over time, allowing better projections in the future.



The Alerts Count and Value Report consists of multiple tabs that display a range of information on alerts.

Alert Count Tab

The Alert Count tab displays reports for the amount of alerts in the date range selected. The following table describes each of the reports available.

Report	Description
Total Count	Displays the total number of alerts generated by Fraud Transaction Monitoring Portal during the time interval defined in the filters, regardless of status and how they were generated.
Active Count	Displays the total number of active alerts generated by Fraud Transaction Monitoring Portal during the time interval defined in the filters.
Closed Count	Displays the number of closed alerts out of the alerts generated in a specific time range, regardless of when these alerts were closed.
Top 10 Solution/Tenant Count Percentage	Displays the top ten Solutions or Tenants contributing the largest percentages of total alerts. Hover over each slice to see the exact percentage the Tenant/Solution contributed.
Top 10 Investigator Count Percentage	Displays key investigators and their workloads, which can be used to ensure that team workloads are balanced. The Top 10 Investigator Count Percentage displays team members associated with the highest volume of closed alerts, including all closed alerts (unless changed in the filters.)
Status Count Percentage	Displays the percentage of alerts segmented by the values in the STATUS filter.



Report	Description
	For example, which alerts are ACTIVE or CLOSED in the time range specified in the filter. This helps to understand the ratio of alerts with different statuses in their Solutions.
Count by Status	Displays the volume of alerts that were active and the volume of alerts that were closed during the time interval defined in the filters.

Alert Value Tab

The Alert value tab shows the same information as the Alert Count tab but for the financial value of the alerts.

The following table describes each of the reports available.

Report	Description
Total Value	Displays the financial value associated with the total number of alerts generated by Fraud Transaction Monitoring Portal during the time interval defined in the filters, regardless of status and how they were generated. The currency used is defined in each tenant.
Active Value	Displays the total number of active alerts generated by Fraud Transaction Monitoring Portal during the time interval defined in the filters, with details about the financial value associated with these alerts.
Closed Value	Displays the number of closed alerts out of the alerts generated in a specific time range, regardless of when these alerts were closed. The Closed Value report also provides details about the financial value associated with these alerts
Top 10 Solution/Tenant Value Percentage	Displays key investigators and their workloads to ensure that team workloads are balanced. The Top 10 Investigator Count Percentage shows team members associated with the highest financial value of closed alerts, including all closed alerts (unless changed in the filters.)
Top 10 Investigator Value Percentage	Displays which team members closed the highest financial value of alerts. This includes all alerts unless changed in the filters. This chart has details on the financial value associated with these alerts.
Status Value Percentage	Displays the percentage of alerts segmented by the values in the STATUS filter. For example, which alerts are ACTIVE or CLOSED in the time range specified in the filter. This helps you understand the ratio of alerts with different statuses in their Solutions. This chart has details on the financial value associated with these alerts.
Value by Status	Displays the financial value associated to the alerts that were active and the financial value associated to the alerts that were closed during the time interval defined in the filters.

Details Tab

The Details tab provides a high-level breakdown of the data used to generate the visualizations displayed in the Alert Count and Alert Value tabs. The Details tab summarises the raw data into groups and provides the next level of data granularity.



Data Tab

The Data tab displays the raw data that is summarised in the Details tab and visualised in the Alert Count and Alert Values tabs.

Description Tab

Provides a high-level description of the charts and reports.



Alerts Generated Report

The Alerts Generated report provides information about the total number of alerts generated in Fraud Transaction Monitoring Portal in a configurable time window. Using this report, you can assess how many alerts have been created and alerts that are still active. These reports use the alert generated date to plot the data on a timeline. You can change the data displayed using the filters to focus on a specific period of time, such as daily, weekly, monthly or quarterly. These reports can also help you understand what type of alerts are most common and what is causing them.



The Alerts Generated Report consists multiple tabs that display a range of information on alerts.

Generated By Event Type and Review Status Tab

The Generated By Event Type and Review Status Tab displays information on the total number of alerts generated, the types of event generated, and the review status of events generated.

The following table describes each of the reports available.

Report	Description
Generated Date Cumulative Count	Displays the total number of alerts generated in Fraud Transaction Monitoring Portal and a graph with the cumulative count of alerts generated by Fraud Transaction Monitoring Portal over time.
Generated By Event Type	Displays alerts by event type over time. This helps you to understand which event types cause the most alerts. Organisations can use this data to investigate their processes and understand why one event type might be causing more alerts than others.
Generated By Review Status	Displays alerts by review status during the time interval defined in the filters. This gives a snapshot view of how well the rules and models in =Fraud Transaction Monitoring Portal are performing compared to the assessments made by investigators. The report can be helpful when reviewing false positive rates and identifying potential improvements to risk scoring.

Generated by Alert Source & Investigator Tab

The Generated by Alert Source & Investigator Tab displays information on alerts generated by assigned investigators and alert source.



The following table describes each of the reports available.

Report	Description
Generated By Assigned Investigator (Top 50)	<div>Displays the top 50 investigators that closed these alerts generated by Fraud Transaction Monitoring Portal during the time range. This covers alerts generated by Fraud Transaction Monitoring Portal and alerts closed by that investigator. The legend for this chart shows the investigator user names next to a colour block. A block that does not have a name shows alerts that have not been closed.</div> <div>Note: If you require more granularity, use the Data tab or export the content of the page to .csv to analyse the data outside of Fraud Transaction Monitoring Portal.</div>
Generated By Alert Source	Displays the volume of alerts automatically generated by Fraud Transaction Monitoring Portal models and rules, or manually by the investigator.

Generated by Status & Solution/Tenant Tab

The Generated by Status & Solution/Tenant Tab displays information on alerts generated by solution/tenants, and alerts generated by status.



The following table describes each of the reports available.

Report	Description
Generated By Solution/Tenant (Top 50)	Displays which Solutions or Tenants generated the most alerts (top 50). This report is useful multi-tenancy or multi-solution deployments.
Generated By Status	<div>Displays the breakdown of the total number of alerts still active or already closed. This chart aggregates all the values from the chart and displays the total across all Tenants and Solutions. By default, all alerts are included in this chart. Use the STATUS option in the Filter menu to specify if you want to see OPEN alerts or CLOSED alerts.</div> <div>When OPEN or CLOSED is applied in the filter, the chart segments the data on REVIEW STATUS.</div>



Data Tab

The raw data summarised in the Details tab and visualised in the Alert Generated tabs.

Description Tab

Provides a high-level description of the charts and reports.



Alerts Closed

The Alerts Closed reports provide an overview of the alerts closed within the time range selected. This enables a Manager/Supervisor to quickly assess how many alerts have been actioned and closed.

This group of reports is similar to the Alerts Generated reports, but focuses on closed alerts. This report provides an overview of the alerts closed within the time range you selected in the Filter pane. This allows you to quickly assess how many alerts have been actioned and closed. These reports use the alert closed date to plot the data on a timeline.

The time and date associated with the Alerts Closed report are when the alerts were closed. and are not originally generated like in the Alert Count or Alert Generated reports.

Closed by Event Type & Review Status Tab

The Closed by Event Type & Review Status Tab displays information on the total number of alerts closed, the type of event closed and the review status of closed alerts.



The following table describes each of the reports available.

Report	Description
Close Date Cumulative Count	Displays the total number of alerts closed in Fraud Transaction Monitoring Portal and a graph with the cumulative count of alerts closed over time.
Closed by Event Type	Displays alerts that have been closed by event type over time. This helps you to understand which event types cause the most alerts.
Closed by Review Status	<p>Displays over time all closed alerts within the time period selected in the Filter pane and segments them according to whether they were reviewed as RISK, RISK-SUSPECTED, NO-RISK, or DISCOUNT.</p> <p>This gives a snapshot view of how well the rules and models in Fraud Transaction Monitoring Portal are performing in comparison to the assessments made by human investigators, and can be helpful when reviewing false positive rates and identifying potential improvements to risk scoring.</p>

Closed by Alert Source & Investigator Tab

The Closed by Alert Source & Investigator Tab displays information on alerts closed by an assigned investigator and alerts closed by their alert source.

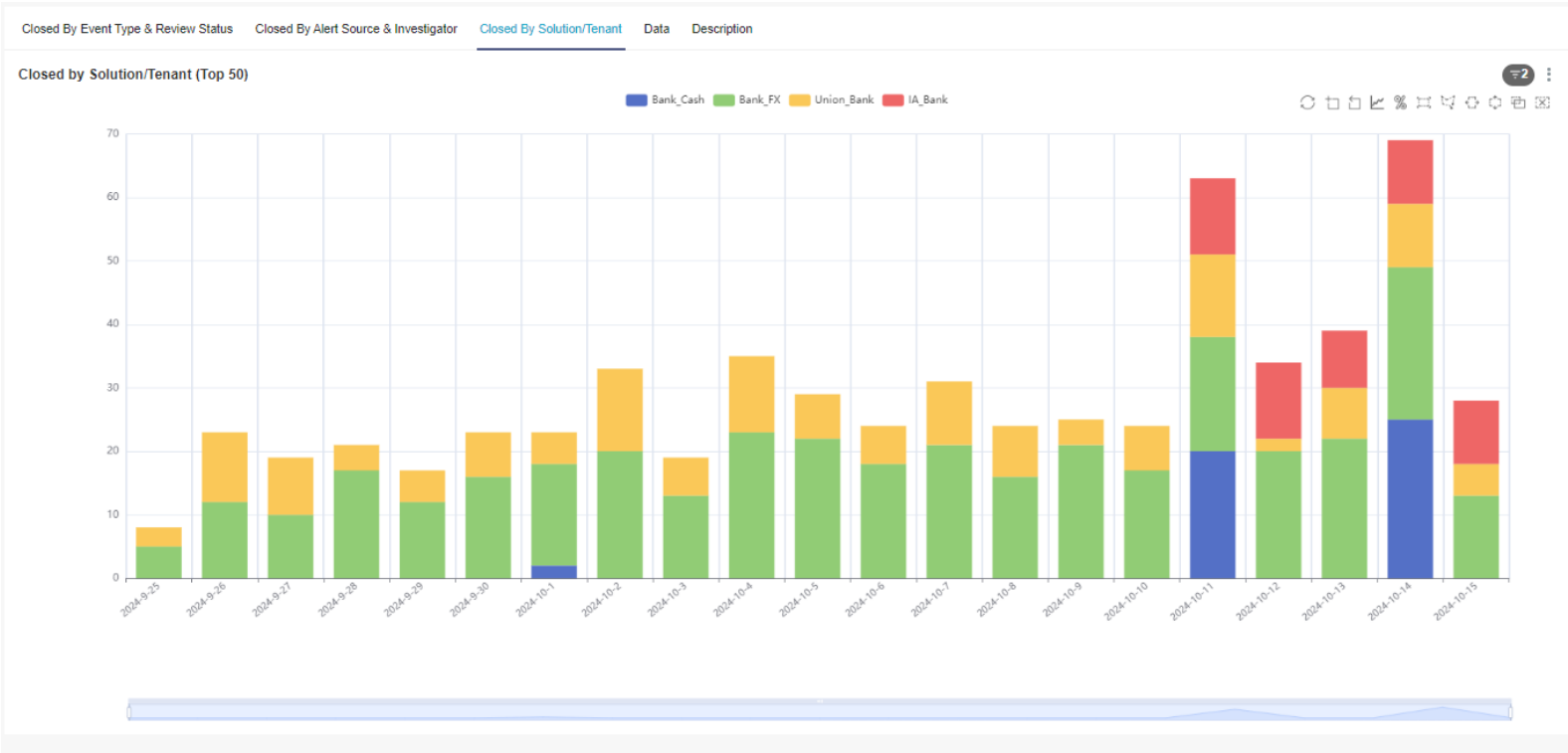


The following table describes each of the reports available.

Report	Description
Closed by Assigned Investigator (Top 50)	<div>Displays all the alerts closed over time within the time range specified in the filters on the Closed By Alert Source & Investigator tab. The data is ranked by investigator, in order of the number of alerts each investigator has closed in the specified time range.</div> <div>This report allows you to track investigator performance and compare real world close rates to projections, which can help with resource management.</div> <div>Note: If you require more granularity, use the Data tab or export the content of the page to .csv to analyse the data outside of Fraud Transaction Monitoring Portal.</div>
Closed by Alert Source	<div>Displays the volume of closed alerts automatically generated by Fraud Transaction Monitoring Portal models and rules, or manually by the investigator.</div>

Closed by Solution/Tenant Tab

The Closed by Solution/Tenant Tab display information on alerts closed by tenants or solutions.



The following table describes each of the reports available.



Report	Description
Closed by Solution/Tenant (Top 50)	<p>Displays the top 50 tenants or Solutions in terms of the number of alerts each tenant or Solution has closed.</p> <p>If you require more granularity, use the Data tab or export the content of the page to .csv to analyse the data outside of Fraud Transaction Monitoring Portal.</p>

Data Tab

The raw data summarised in the Details tab and visualised in the Alert Closed tabs.

Description Tab

Provides a high-level description of the charts and reports.



Rules Summary

The Rules Summary report shows the number of rules triggered over time, grouped by rule. You can specify the number of rules that are triggered in a specified range, grouped by rule. This enables you to see the volume of rules that have been triggered by events that came into the system.



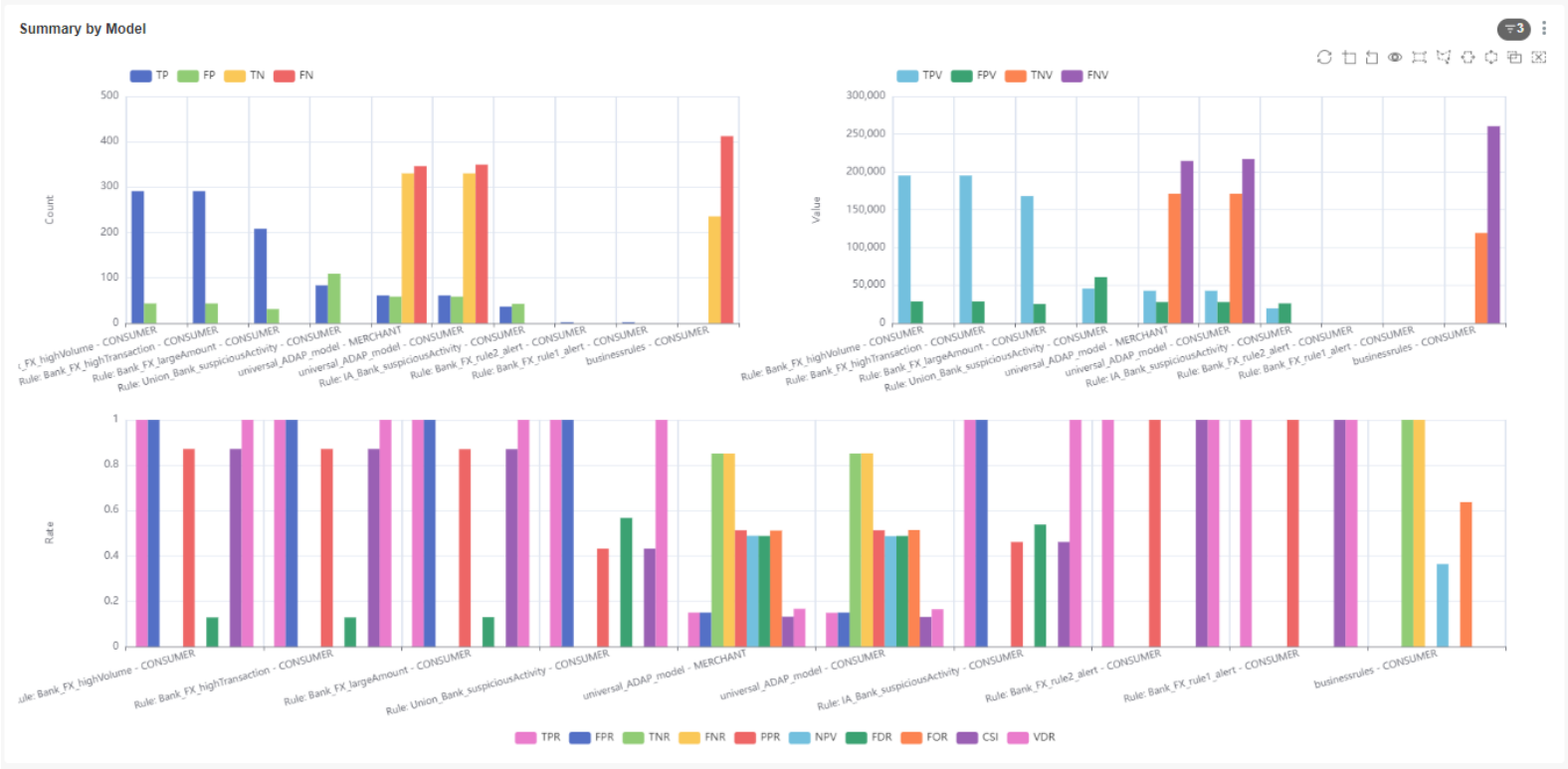
The following table describes each of the reports available.

Report	Description
Triggered rules over time	<p>Displays the number of times each rule triggered over time. For example:</p> <ul style="list-style-type: none">You have three rules - A, B, and C.A, B, and C trigger on the same alert.Event triggers three different rules - One for rule A, one for B and one for C.
Triggered rules over time grouped by event	<p>Displays the number of times a group of rules are triggered together. In this chart, an alert where rules A, B and C triggered at the same time would be counted once. An alert where only rules A and B triggered would be another category, and an alert where rule B triggered on its own would be a third category.</p> <p>For example, the following chart extract shows the same data as the 'Triggered rules over time' chart, but grouped by event rather than rule. In this case, the event triggered the same two rules, but Fraud Transaction Monitoring Portal treats the two alerts as a single data point because they were triggered by the same event.</p>



Model Summary

The Model Summary report provides an overview of model performance across a specified time range. This report enables you to understand how the analytics might change when thresholds are different.



This report shows metrics such as financial value, volumes (counts), and true and false positive rates at a given risk threshold for each rule and model, as follows:

- **TPR (True Positive Rate):** Events where the score the model generated is higher than the threshold filter or the business rule has generated an alert. The event is also confirmed as fraud (reviewed as RISK by the analyst or using an external fraud label).
- **FPR (False Positive Rate):** Events where the score the model generated is higher than the threshold filter or the business rule has generated an alert, and is reviewed as NO-RISK by the analyst or not decisioned by the analyst. By default, reports assume all events are genuine. This metric is only available for machine learning models, and should be ignored for rules.
- **TNR (True Negative Rate):** Events where the score the model generated is lower than the threshold filter and reviewed as NO-RISK by the analyst or still not decisioned by the analyst. By default, reports assume all events are genuine. This metric is only available for machine learning models, and should be ignored for rules.
- **FNR (False Negative Rate):** Events where the score the model generated is lower than the threshold filter and the event is confirmed as fraud (reviewed as RISK by the analyst or using an external fraud label). This metric is only available for machine learning models, and should be ignored for rules.
- **PPR (Positive Predictive Rate):** Proportion of events identified as fraud/crime by the model that were actually fraud or crime.
- **NPV (Negative Predictive Value):** Proportion of events identified as genuine activity by the model that were actually genuine. This metric is only available for machine learning models, and should be ignored for rules.
- **FDR (False Discovery Rate):** Proportion of events identified as fraud/crime by the model that were incorrectly classified (actually genuine).
- **FOR (False Omission Rate):** Proportion of events identified as genuine by the model that were incorrectly classified (actually fraud/crime). This metric is only available for machine learning models, and should be ignored for rules.
- **CSI (Critical Success Index):** Number of events correctly identified as fraud/crime as a fraction of the number of events classified as fraud/crime plus the number of missed cases of fraud/crime. This metric is only available for machine learning models, and should be ignored for rules.
- **VDR (Value Detection Rate):** Proportion of fraud/crime correctly identified by the model by transaction value. This metric is only available for machine learning models, and should be ignored for rules.
- **TP (True Positive) count and value:** Count and value of fraud/crime correctly identified as fraud/crime (the score the model generated was higher than the threshold defined in the filter or the rule alerted).
- **FP (False Positive) count and value:** Count and value of genuine events incorrectly identified as fraud/crime (the score the model generated was higher than the threshold defined in the filter or the rule alerted).



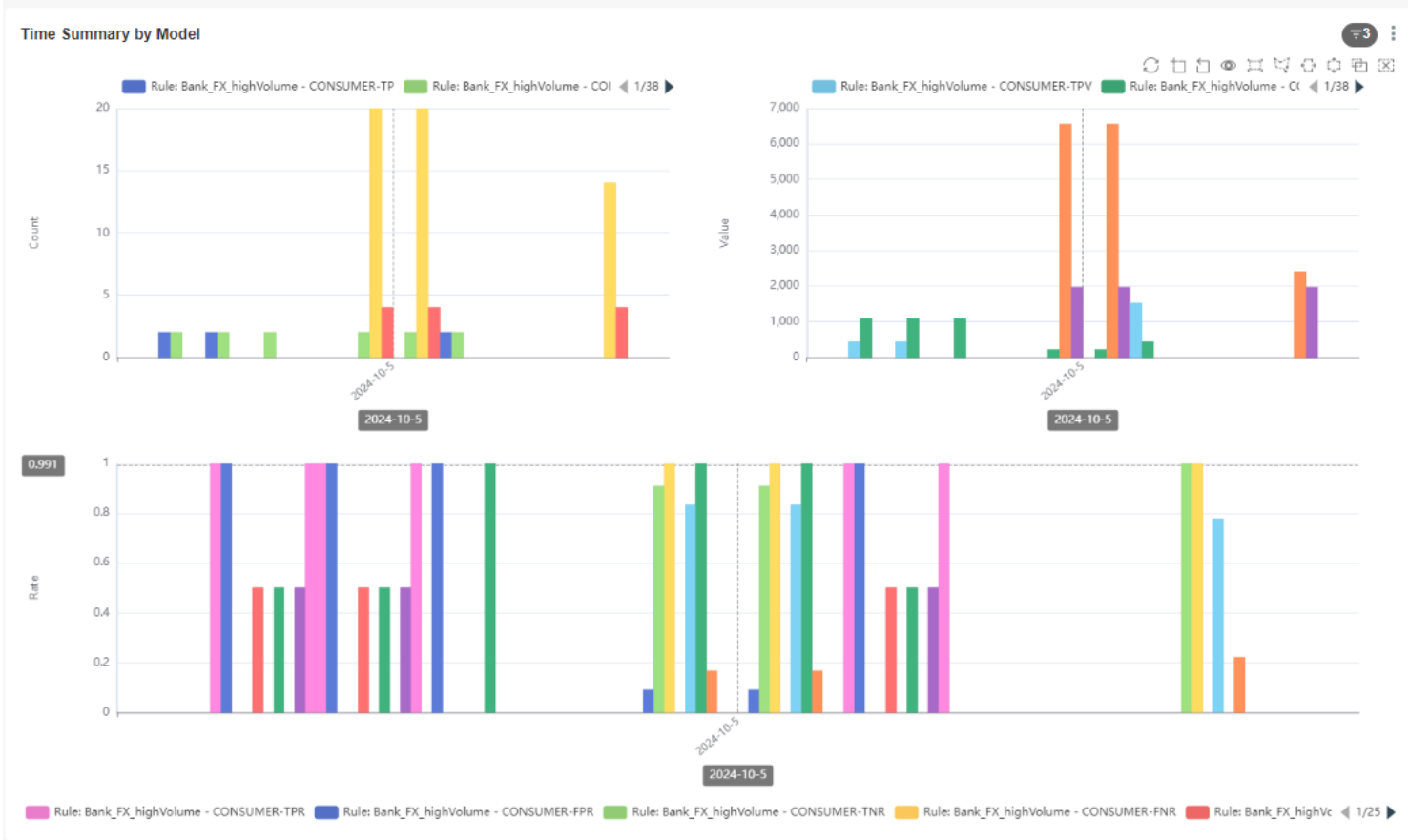
- **TN (True Negative) count and value:** Count and value of genuine events correctly identified as genuine (the score the model generated was lower than the threshold defined in the filter). This metric is only available for machine learning models, and should be ignored for rules.
- **FN (False Negative) count and value:** Count and value of fraud/crime incorrectly identified as genuine (the score the model generated was lower than the threshold defined in the filter). This metric is only available for machine learning models, and should be ignored for rules.

Note: To use this report, you must select a rule or model using the Model filter. If your model outputs a score, set the threshold appropriately. The report shows the different analytics metrics, based on the assumption that any event that scored above the threshold you set generated an alert.



TP/FP Over Time

The Time Summary by Model report provides an overview of the analytics reports, showing values, volumes and rates through time, across all analytics measurements.



It is broken down as follows:

- **TPR (True Positive Rate):** Events where the score the model generated is higher than the threshold filter or the business rule has generated an alert. The event is also confirmed as fraud (reviewed as RISK by the analyst or using an external fraud label).
- **FPR (False Positive Rate):** Events where the score the model generated is higher than the threshold filter or the business rule has generated an alert, and is reviewed as NO-RISK by the analyst or not decisioned by the analyst. By default, reports assume all events are genuine. This metric is only available for machine learning models, and should be ignored for rules.
- **TNR (True Negative Rate):** Events where the score the model generated is lower than the threshold filter and reviewed as NO-RISK by the analyst or still not decisioned by the analyst. By default, reports assume all events are genuine. This metric is only available for machine learning models, and should be ignored for rules.
- **FNR (False Negative Rate):** Events where the score the model generated is lower than the threshold filter and the event is confirmed as fraud (reviewed as RISK by the analyst or using an external fraud label). This metric is only available for machine learning models, and should be ignored for rules.
- **PPR (Positive Predictive Rate):** Proportion of events identified as fraud/crime by the model that were actually fraud or crime.
- **NPV (Negative Predictive Value):** Proportion of events identified as genuine activity by the model that were actually genuine. This metric is only available for machine learning models, and should be ignored for rules.
- **FDR (False Discovery Rate):** Proportion of events identified as fraud/crime by the model that were incorrectly classified (actually genuine).
- **FOR (False Omission Rate):** Proportion of events identified as genuine by the model that were incorrectly classified (actually fraud/crime). This metric is only available for machine learning models, and should be ignored for rules.
- **CSI (Critical Success Index):** Number of events correctly identified as fraud/crime as a fraction of the number of events classified as fraud/crime plus the number of missed cases of fraud/crime. This metric is only available for machine learning models, and should be ignored for rules.
- **VDR (Value Detection Rate):** Proportion of fraud/crime correctly identified by the model by transaction value. This metric is only available for machine learning models, and should be ignored for rules.
- **TP (True Positive) count and value:** Count and value of fraud/crime correctly identified as fraud/crime (the score the model generated was higher than the threshold defined in the filter or the rule alerted).
- **FP (False Positive) count and value:** Count and value of genuine events incorrectly identified as fraud/crime (the score the model generated was higher than the threshold defined in the filter or the rule alerted).



- **TN (True Negative) count and value:** Count and value of genuine events correctly identified as genuine (the score the model generated was lower than the threshold defined in the filter). This metric is only available for machine learning models, and should be ignored for rules.
- **FN (False Negative) count and value:** Count and value of fraud/crime incorrectly identified as genuine (the score the model generated was lower than the threshold defined in the filter). This metric is only available for machine learning models, and should be ignored for rules.

Note: To use this report, you must select a rule or model using the Model filter. If your model outputs a score, set the threshold appropriately. The report shows the different analytics metrics, based on the assumption that any event that scored above the threshold you set generated an alert.



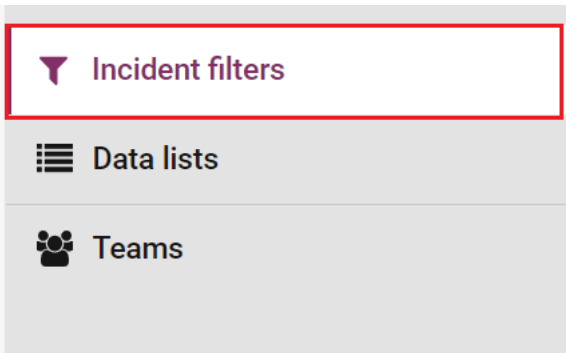
9 Settings

The Settings section of the Portal enables you to configure the appearance and features of the portal. You can also use this section to manage incident filters, data lists, and teams.

Incident Filters

The Incident Filters page allows you to view a list of incident filters that are currently available. You can configure a filter for incidents here, which appear in the Incidents section sidebar.

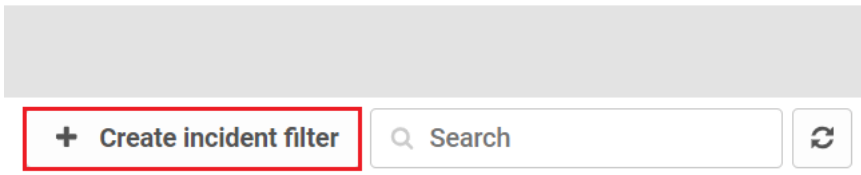
To access the Incident Filters page and view a list of incident filters that are currently available in the sidebar on the left, click the Incident Filters option in the sidebar.



Create an Incident Filter

To create a new filter:

1. Click the **Create Incident Filter** button.



The Create incident filter page opens.

2. Enter the name of the incident filter in the Name field.

Name *

Filter A

3. Enter the mode of the incident filter in the Mode field. Select from:
 - **By Type** enables you to create a filter that only shows incidents related to a specified entity type.
 - **Identifier** enables you to create a filter than only shows incidents related to a specified entity.
 - **Unrestricted** is the default option, and enables you to create a filter that shows incidents related to any entity.

Mode *

Unrestricted

Filter by an entity or entity type

☒ Include only unreviewed alerts

4. (Optional) Set whether the filter should include only unreviewed alerts by selecting the Include only unreviewed alerts check box. If this check box remains selected, the filter displays incidents that contain one or more unreviewed alerts that match the specified filter conditions.



Mode *

Unrestricted

Filter by an entity or entity type

☒ Include only unreviewed alerts

5. If you selected the **By Type** mode, select an entity type from the Entity type drop-down field.

☒ Include only unreviewed alerts

Entity type *

accountEntityId

6. If you selected the **Identifier** mode, select an entity identifier from the Entity identifier field.

☒ Include only unreviewed alerts

Entity identifier *

Entity identifier

7. Set the time period for the filter. Select from:

- All incidents
- Filter by time

Time period

Time period

☒ All incidents ☐ Filter by time

If you want the filter to only include incidents that occurred in a specified time frame, select the **Filter by time** option, followed by one of the following options:

- **Exclude latest incidents** lets you enter an exclusion period in days, hours or minutes. Any incidents that occurred within this period are excluded. For example, if you set the exclusion period to 1 day, any incidents that occurred in the last 24 hours are excluded.
- **Exclude oldest incidents** lets you enter an inclusion period in days, hours or minutes. Only incidents that occurred within this period are displayed. For example, if you set the inclusion period to 1 day, only incidents that occurred in the last 24 hours are included by the filter
- **Exclude oldest and latest incidents** lets you enter an inclusion and exclusion period in days, hours or minutes. The exclusion period defines an interval up to the current time. The inclusion period defines an interval up to the beginning of the exclusion period. Incidents are only included if they occurred in the inclusion period. For example, if you set the inclusion period to 2 days and the exclusion period to 3 days, only incidents that occurred between 3 and 5 days ago are displayed.

8. (Optional) Select the rules you want to include in the filter from the Rules section. The filter shows incidents containing one or more alerts that the selected rules have triggered on (or that match tag or team conditions that you have also added to the filter). If no rules are selected, the filter applies any conditions based on rules.

You can select a rule to be included by clicking the check box to the left of the rule name.



Rules

10 per page

Name

☒

 ATMReversal7

☐

 blockedAccount15

9. (Optional) Select the tags you want to include in the filter from the Tags section. The filter shows incidents containing one or more alerts that have a selected tag added to them (or that match rule or team conditions that you have also added to the filter). If no tags are selected, the filter will not apply any conditions based on tags.
- You can select a tag to be included by clicking the check box to the left of the tag name.

Tags

10 per page

Name

☒

 Action=Decline

☐

 Action=DeclineAndBlockG5

10. (Optional) Select incident filters you want to exclude from the filter from the Excluded incident filters section. Any incidents that match an excluded incident filter are displayed in this incident filter, even though they otherwise match the specified filter conditions.
- You can select an incident filter to be excluded by clicking the check box to the left of the incident filter name.

Excluded incident filters

10 per page

☒

 Incident filter

☒

 Filter A

11. (Optional) Select the teams you want to include in the filter from the Teams section. The filter will only show incidents containing one or more alerted events that have been referred to one of the selected teams (or that match rule or tag conditions that you have also added to the filter). If no teams are selected, the filter will not apply any conditions base on teams.
- You can select a team to be included by clicking the check box to the left of the team name.

Teams

10 per page

☒

 Name

☒

 Team A

12. Click **Create** at the top of the page.



Q

Create

Cancel

Edit an Incident Filter

To edit an existing filter, click **Edit** to the right of the filter in the Incident Filters list. You can configure and change any of the options described above.

Incident filters

10 per page

+ Create incident filter

Q Search

Name

Mode

Mode filter

Filter A

Unrestricted

-

Edit

Delete

Delete an Incident Filter

To delete an incident filter, click **Delete** to the right of that filter in the Incident Filters list. You can confirm or cancel the deletion.

Incident filters

10 per page

+ Create incident filter

Q Search

Name

Mode

Mode filter

Filter A

Unrestricted

-

Edit

Delete



Data Lists

Data lists enable you to create lists of entities or other data, such as account IDs, email addresses, or IP addresses. This can be useful for creating negative lists or positive lists. Data lists can also be used to create more complex tables of information, to allow rules to look up information in a dynamic, multi-column table that can be updated manually or programmatically.

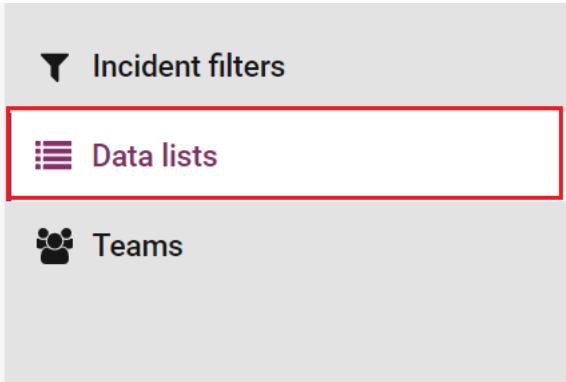
Users can manually create lists, import existing lists, or add event or entity data to lists from the Incident Review page.

A data list is organised as a table containing one or more columns. Each item in the data list forms a row in the table. Each item has an identifier, which must be unique (in a list of entities, this could be the entity ID). Each item can also have one or more properties, which form the other columns in the table. These properties are optional; only the identifier is required.

Data lists can be used by rules, where rule items can be added to data lists using AMDL expressions. The following are a couple of examples:

- A rule might use a data list to check if an event originates from a suspect IP address
- A rule might add a customer to a data list whose account has been suspended due to suspected fraud to a list of potentially compromised accounts

Open the Data Lists page by clicking the Data Lists option in the sidebar.



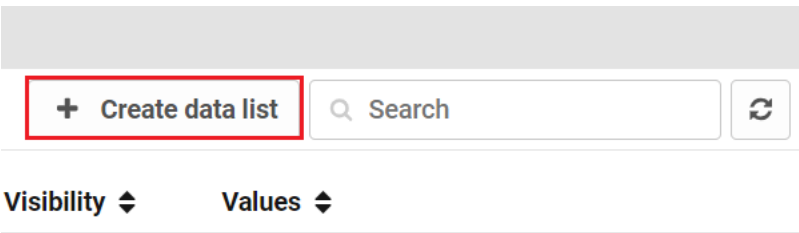
The following data list items appear:

Column	Description
Name	The name of the list.
Context	The portal the data list belongs to.
Full name	The full name of this list to be used in Business Rules. If you want to refer to a public data list in a rule that belongs to a different portal from the list, you must use the reference given in the Full name column.
Visibility	Whether this list is private or public. Public data lists can be viewed by all users, and Private data lists can only be referred to by portal-level rules defined in the same portal as the list.
Values	The number of entries in the list.

Create a Data List

To create a new, blank data list:

1. Click the **Create data list** button.





2. Enter the name of your new data list. This can only contain letters, numbers and underscores, and must start with a letter in the **List Name** field.

List name * is required

List name

Can contain upper- and lowercase letters, numbers and underscores. Must start with a letter.

Incident data

☐ Data can be added to this list from the incident review page

Add to list

Add data from this incident to a list

3. (Optional) To enable users to add items to the list when reviewing an incident, select the check box **Data can be added to this list from the Incident Review page**. See [Add Values to a Data List](#).

List name * is required

List name

Can contain upper- and lowercase letters, numbers and underscores. Must start with a letter.

Incident data

☐ Data can be added to this list from the incident review page

Add to list

Add data from this incident to a list

To define which event data fields can be added to the data list, either select a path from the Property paths drop-down field, or enter the name of the path.

4. Click the **Add Item** button to add this event data field to the list of properties.

☒ Data can be added to this list from the incident review page

Add to list

Add data from this incident to a list

Property paths

VIPIndicator

Add item

Note: If the field(s) defined for this list appears in multiple events in the history of the entity in question, each unique value in any event generated by that entity will be displayed for the analyst to add to the data list. Some fields, such as entity ID, will only ever have one value; some, such as device ID, might have a limited list of unique values for each customer; others might only appear in one event type which occurs infrequently, or even only once (e.g. a customer registration date). These fields are often suitable for addition to a data list using the Add to List button. However, some fields (e.g. event date/time, transaction value) will have a unique value for a large proportion of events generated by that entity, and so are not suitable for adding to data lists in this way.

5. Click the **Create** button to save the data list.



Create

Cancel

Edit a Data List

To change the properties of an existing data list, click **Edit** on the appropriate row of the list of data lists.

Values

0 values

Edit

Delete

For more information, see [Editing Data Lists](#).

Delete a Data List

To delete a data list: click **Delete** on the appropriate row of the list of data lists. You can confirm or cancel the deletion.

Values

0 values

Edit

Delete

View and Filtering Data Lists

To view the items in a data list, click the name of the relevant list on the Data Lists page. This opens the List items page, as shown in the image below. You can also use the List Items page to edit and filter the list.

Data lists > "pliproductids"

Edit data list

List items

List items

Download CSV

Batch tasks

Add items manually

Identifier

Search

10 per page

Identifier	Last updated at	Created at	
> 1431013159551703	11/13/2023 08:33 AM	11/13/2023 08:33 AM	<div> Edit</div> <div> Delete</div>
> 1431013170424633	11/13/2023 08:33 AM	11/13/2023 08:33 AM	<div> Edit</div> <div> Delete</div>

For each item in the data list, the List items page shows the following columns:

- **Identifier:** The unique identifier for the item.
- **Last updated at:** The date and time the item was most recently updated.
- **Created at:** The date and time the item was added to the list.

You can sort the items by any of these three columns.

If the data list has multiple columns, the page also displays any additional columns. You can click the expand icon on the left of a row to see the username of the person who last updated the item and any comment they added when they made the update.



Filtering a data list by data column

You can filter the List items page to show only the items that contain a specified value in either the unique identifier column or any additional data column. To filter the list by these columns:

1. Click the **Filter** field and select the data you want to filter from the menu.

▼

Identifier

⌵

🔍

Search

↺

2. Enter a value in the **Search** field. When you finish typing, the list is filtered to show only those items where the selected column matches this value. Note that the filter is case sensitive.

▼

Identifier

⌵

🔍

Search

↺

To remove the filter, on the right of the Search field, click **Close**.

Filtering a data list by time

You can filter the List items page by item update time or creation time, as displayed in the Last updated at and Created at columns. For example, you can filter the page to show only the items that were recently updated or only the items that were added in a date range.

To filter the list by time:

1. Click **Filters**.
2. Use the options in the Filters sidebar to filter by one of the following criteria:
 - Update Time: By setting a date/time range, you can choose to show only items that were last updated between two times.
 - Created Time: By setting a date/time range, you can choose to show only items that were added between two times.

Add Values to Data Lists

To manually add values to a data list:

1. Click on the Data List you want to add values to from the Data Lists page.

Data lists

10 ⌵ per page

+

Create data list

🔍

lista

✕

↺

Name ⌵Context ⌵Full name ^Visibility ⌵Values ⌵

ListA

📍

GPS

lists.ListA

private

0 values

✎

Edit

🗑

Delete

First

Previous

1

Next

Last

2. Click the **Add items manually** button.



[Data lists](#) > "ListA"

Edit data list

List items

Download CSV

Batch tasks

+ Add items manually

Identifier

The Add Item window displays.

3. Enter the unique identifier for the data list item in the Identifier field. This cannot be the same as an existing identifier in the list.

Add item

Identifier *

Item Identifier

Note: The portal has no way to check whether the identifier is of the correct type. For example, there is no way to reject the addition of an IP address as the identifier to a list in which all the other identifiers are entity IDs. Therefore, you should take care when manually adding items to lists, to ensure that the correct identifier is used, and the list items can be utilised in rules.

4. (Optional) If the data list contains properties (i.e. other columns) already, specify a value for one or more of these in the Properties section by entering the value in the field next to the property name.

Properties

Property A

1

x

+ Add property

5. (Optional) Add a new property to this item by clicking the **Add Property** button. Enter the name of the new property (the column header) in the Key field, and the value for the new item in the Value field. You can remove any new properties by clicking the Remove button.

Properties

+ Add property

Comment * is required

Comment

Because all properties are optional, no other items in the list will have a value for this property unless you edit those items subsequently.

6. Enter a comment in the Comment field.

Properties

+ Add property

Comment * is required

Comment

7. Click **Add Item** to add the new item to the data list.



Add item

Batch Import

Instead of manually adding values to a data list, you can import a Comma Separated Values (CSV) file. The CSV file must be arranged in one or more columns, and the first row must be a header row. One of the columns acts as the unique identifier for each row with the heading labelled `_id`. This method can be used to add values to an empty data list, or to an existing data list that already contains values.

Note: If you need to import a data list with more than 100,000 entries, contact your Operations Manager.

To add items to a data list using the batch import method:

- 1. Create a blank data list (See [Create a Data List](#)).
- 2. Open the newly created data list from the Data Lists page.

Data lists

10 per page

+ Create data list

lista

Name	Context	Full name	Visibility	Values	
ListA	GPS	lists.ListA	private	0 values	<div>EditDelete</div>

First

Previous

1

Next

Last

- 3. Click **Batch Tasks** and select the Batch Import option.

Edit data listList items

Download CSV

Batch tasks

+ Add

10 per page

Identifier

Batch import

Batch delete

No matches

A window will display.

- 4. Click **Choose File**.



Batch import items

List items to import * is required

Choose a file

Comment *

Comment

Import items

5. Navigate to the csv file you want to import and click **Open**.

Name	Date modified	Type	Size
Yesterday			
data-list-export-pliproductids	30/11/2023 15:53	Microsoft Excel Com...	

File name: data-list-export-pliproductids

Custom files

Open

Cancel

The number of new items that will be imported will be shown, as well as the number and list of new headers (i.e. data list columns) that will be created.

6. Enter a comment in the Comment field.

✔ 7143 new values will be imported

⚠ 1 new header will be imported:

Comment *

Comment for the import

7. Click **Import Items**.

Import items

Note: When using the batch import method to update a data list, any columns and values for identifiers present in both the existing data list and the CSV file will be overwritten with the columns and values for those identifiers from the CSV file. This is the case even if the existing data list contains columns and values that are not present in the CSV file.

Editing Data Lists

To edit a Data List, go to the page for that list. On this page, you can view and edit individual items in the list, or add new items.



- To view the details of an individual item in a data list, click anywhere on the row showing the name of the item. This will display details of the individual item, including the comment added by the user who last added or updated this item, whether from the 'List Items' page, or the Incident Review page.
- To delete a value (row) from a data list, on the right of the relevant value, click the **Delete** button, and then click 'Confirm Delete'.
- To add to an existing data list using the batch import method, follow the steps in the section on [Batch Import](#).

Edit an Item in the Data List

To edit an item in a data list:

1. Click the **Edit** button to the right of the item you want to edit in the item list.

10 per page

Identifier

Last updated at

Created at

1

> Identifier1

12/01/2023 01:52 PM

12/01/2023 01:52 PM

1

Edit

Delete

The Edit Item window opens.

2. (Optional) If the data list contains properties, specify or edit the value for one or more of these in the 'Properties' section. You can do this by entering the value or editing the existing value in the field next to the property name. Note that the data list containing properties can include other columns.

Properties

1

1

+ Add property

3. (Optional) Add a new property to this item by clicking the **Add Property** button. Enter the name of the new property (the column header) in the Key field, and the value for the new item in the **Value** field. You can remove any new properties by clicking the **Remove** button.

Properties are invalid – empty key(s)

1

1

Key

Value

+ Add property

4. Enter a comment in the Comment field.

Comment*

A comment in the comment field.

5. Click the **Edit Item** button to save your changes.

Edit item

Delete Multiple Items from a Data List

Instead of manually deleting values from a data list, you can delete items using a Comma Separated Values (CSV) file. The batch delete functionality removes any items from the data list that have a unique identifier matching one in the `_id` column of the data list.

To delete multiple items from a data list:



1. Open the data list where you want to delete items from the Data List page.

Data lists

10 per page

+ Create data list

lista

✕

↺

Name	Context	Full name	Visibility	Values	
ListA	GPS	lists.ListA	private	0 values	<div>Edit</div> <div>Delete</div>

First

Previous

1

Next

Last

2. Click **Batch Tasks** and select the Batch Delete option.

Download CSV

Batch tasks

+ Add items ma

10 per page

Batch import

Batch delete

Identifier

Last

ted at

3. Click **Choose File**.

Batch delete items

Upload file containing list items for deletion* is required

Choose a file

Deleting lots of records may take a long time.

Delete items

4. Navigate to the csv file and click **Open**.

Yesterday

data-list-export-pliproductids

30/11/2023 15:53

Microsoft Excel Com...

File name: data-list-export-pliproductids

Custom files

Open

Cancel

5. Select the **Confirm deletion** check box.

☒ Confirm deletion of 7143 records*

Deleting lots of records may take a long time.

Delete items

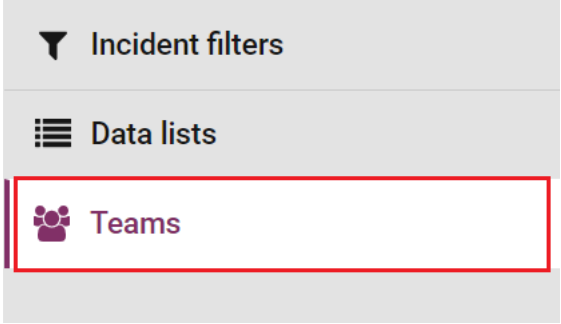
6. Click **Delete Items**.

Delete items



Teams

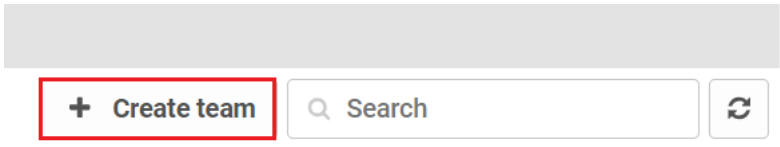
Teams are groups of users that exist in the portal. You can refer Incidents to all the members of a team (see Referring Incidents), assign an incident filter to a team (see Incident Filters), and send a broadcast message to all members of a team (see Message Service). Click the Teams option in the Settings sidebar to access the list of teams, create new teams, and add and remove users from teams.



Create Teams

To create a new team:

1. Click the **Create team** button.



The Create Team page opens.

2. Enter the name of the new team in the **Name** field.

Name *

Name

3. Select the users that will be part of this team.

<div><div></div><div></div></div>	Name	Display name
<div><input type="checkbox"/></div>	facarlos.castaneda@thredd.com	FACarlos Castaneda - Thredd
<div><input checked="" type="checkbox"/></div>	jon.bullock@thredd.com	Jon Bullock - Thredd

4. Click **Create** to save the new team.

Create

Cancel

Change Users on a Team

To change which users are members of an existing team:



1. Click **Edit** to the right of the team's name in the team list.

Name ^	Users ⇅	
Team A	1 user	<div><div> Edit</div><div> Delete</div></div>

2. Select or clear the check boxes next to the names of the users you want to add or remove from the team.

<div><div> v</div></div>	Name	Display name
<input type="checkbox"/>	facarlos.castaneda@thredd.com	FACarlos Castaneda - Thredd
<input checked="" type="checkbox"/>	jon.bullock@thredd.com	Jon Bullock - Thredd

3. Click **Update** to save the changes to the team.

Update

Delete

Cancel

Delete a Team

To delete a team: click **Delete** to the right of that team's name in the Teams list. You can confirm or cancel the deletion.

Users ⇅	
0 users	<div><div> Edit</div><div> Delete</div></div>

Note: You can only delete teams that have no members, so to delete a team which has users in it, remove those users from the team first.



10 Audit Log

This area provides a full audit log of user activity on the portal.

This item list shows each user interaction with the portal. Like other item lists, the list can be sorted or searched. The columns of the list provide a timestamp, username, HTTP method used, IP address and the URL accessed.


You can do the following with the list data:


- You can view the JSON-formatted content submitted to the portal server by clicking anywhere on the appropriate row of the list.

▼ 01/11/2024 03:28 PM jon.bullock@thredd.com POST 165.85.138.15, 172.25.96.171 /api/value_lists/Name/items/query?tenantIdentifier=GPS

Request

```
{
  "currentPage": 0,
  "orderBy": "ITEM_KEY",
  "orderReverse": false,
  "perPage": 10
}
```

- You can expand all rows by clicking on the icon on the top left corner of the table.
- Use the  Copy to clipboard button on the right-hand side of each row to copy the log data to the clipboard.

The report is a point-in-time snapshot. To see more recent activity, click the  button in the top right corner of the page.



11 FAQs

Q. How do I see incidents that need reviewing?

When you first go to the Incidents page, it shows a list of all incidents visible to you that haven't yet been reviewed. You can choose to view only certain incidents, using filters. For more information, see [Managing Incidents](#).

Q. How do I make a decision on an incident or alert?

The Incidents page allows you to review information on an incident, and review alerts as 'risk' or 'no-risk', discount alerts, or put the incident aside to work on later. For more information, see [Managing Incidents](#).

Q. How do I see more information on an incident or alert?

The Incident Review page contains detailed information on:

- The event that triggered an alert
- The entity that event happened to
- Related user activity, including how previous alerts for the same entity were reviewed
- Notes and comments from analysts who reviewed previous alerts

For more information, see [Incident Review Page](#).

Q. How do I search for a particular entity or event?

The search box in the UI header allows you to search for entities or events by ID or by fields within the event data, and then you can view and filter those results in the Events section of the UI. For more information, see [Viewing Events](#).

Q. How do I refer or escalate an incident to someone else?

You can do this from the Incident Review page. For more information, see [Incident Review Page](#).



Glossary

This page provides a list of glossary terms used in this guide.

A

Aggregator

An aggregator is a type of analytic that can combine and use the outputs of multiple rules and models to generate alerts.

Alert

The Fraud Transaction Monitoring System can flag up high-risk events for alert reviews. A flagged event is said to have generated an alert. The system's analytics rules, models and aggregators) can all generate alerts.

Alert Review

This is where analysts review alerts generated by the Thredd Fraud Transaction Monitoring System. They can classify alerts as 'Risk' or 'No Risk', refer them to other users, or put them aside for further monitoring or to await additional information.

AMDL

AMDL (ARIC Modelling Data Language) is a language for specifying rules and logic within the Fraud Transaction Monitoring System. It is a declarative language for specifying state updates and executions on each event that passes through the system. An example of an event is an account registration or a transaction. Every event contains a reference (for example, an ID field) to one or more entities of different types, such as a merchant and a consumer. You can use AMDL to create Business Rules for the detection of fraud.

B

BIN Attack

An act of guessing an accurate combination of a debit or credit card number, Card Verification Value (CVV), and expiry date using brute-force computing. When this has been completed and the fraudster acquires the right information, they use the card to commit fraudulent transactions.

C

Chargeback

Where a cardholder disputes a transaction on their account and is unable to resolve directly with the merchant, they can raise a chargeback with their card issuer. The chargeback must be for a legitimate reason, such as goods and services not received, faulty goods, or a fraudulent transaction. For more information, see the Payments Dispute Management Guide.

E

Entity

Events happen to entities. An entity represents a unique individual or object, and every event is associated with at least one entity. For example, if a customer makes a card transaction, that event can be associated with the customer entity, the card entity, or both.

Entity ID

Each entity is identified by a unique entity ID in the event data for example, a 16-digit token.

Entity State

Every entity has a state - a combination of information about the entity that the system has accumulated over time. This is also called a behavioral profile. Every event processed by the system has the potential to update an entity's state, adding more information or updating information that the system can use to build a behavioral profile of a customer or card for example.

Event

The Fraud Transaction Monitoring System recognizes potential fraud and financial crime by monitoring events. An event could be a customer transaction, a new customer application, or a merchant attempting to process a payment - these are all examples of event types. Each event is associated with one or more entities and one or more solutions.

I

Incident

In the Fraud Transaction Monitoring System, alerts are grouped into incidents. Each incident contains all the unreviewed alerts related to a particular entity.



Issuer (BIN sponsor)

The card issuer, typically a financial organisation authorised to issue cards. The issuer has a direct relationship with the relevant card scheme (payment network). For more information, see the Key Concepts Guide.

L

Label Events

Label events are types of event that contain ground truth information. They are used to label other events as 'risk' (i.e. confirmed fraud, financial crime, etc.) or 'no risk' (i.e. genuine). Alert reviews are one common form of label event, but your portal may also use other kinds of label event, such as chargebacks or manual fraud reports. Labels are used by Adaptive Behavioral Analytics models to learn to better identify high-risk events. They are also used to quantify and report on the performance of models.

M

Mastercard Fraud and Loss Database

A Mastercard repository of fraud transactions submitted by issuers. It is used for reporting, monitoring, and combating card fraud. Previously known as: System to Avoid Fraud Effectively (SAFE).

MasterCom API

MasterCom API offers Mastercard customers the ability to create and manage dispute claims in MasterCom. MasterCom is a system for dispute management. All activities for any given dispute can be tracked within a single claim using Mastercom, including Retrieval Request and Fulfilment, First Chargeback, Second Presentment, Fraud reporting, Case Filing, and Fee Collection requests. All activities for any given dispute throughout its lifecycle can be tracked within a single claim.

Model

A model in the Thredd Fraud Transaction Monitoring System is a predictive model that processes events and generates a risk score for certain event types, for example, authorisations.

P

PAN

The Primary Account Number (PAN) is the card identifier found on payment cards, such as credit/debit/prepaid cards, as well as stored-value cards, gift cards and other similar cards. The card's 16-digit PAN is typically embossed on a physical card. For more information, see the Key Concepts Guide.

R

Real time/near-real time events

Every event is processed by analytics in the Featurespace fraud monitoring system engine. This processing happens in strict chronological order, so that no event is ever processed out of sequence. This is asynchronous processing, and happens to all events. However, some events, such as authorisations, require a real-time response (within a few hundredths of a second). These must be processed in a way that prioritizes low latency (such as a fast response), rather than chronological order. This kind of event is called a real-time event, and is processed by the portal synchronous response generator (as well as the portal Engine). Events that do not require a real-time response (asynchronous events), are only processed by the engine, for example, chargebacks, address or phone number updates

Rule

A rule defines some simple logic - rules take in information from events, entity states, and other data, and output a simple true/false response. Rules are written in the business logic definition language, AMDL.

Rule Set

Each Analytical Workflow is divided into a series of Rule Sets. Each Rule Set contains a number of expressions written in AMDL, and one or more Scorecards which contain conditions that determine what effects the Workflow triggers (e.g. generating an alert, adding a tag, outputting a risk score). Each Rule Set may also have a condition that determines whether or not that Rule Set is executed for an event.

S

Single Sign-On (SSO)

An identification method that enables users to log in to multiple applications and websites with one set of credentials.



Smart Client

Smart Client is Thredd's legacy desktop application for managing your account on the Thredd Platform.

Solution

Multiple product Solutions may be configured in your portal deployment. Each Solution provides a combination of UI configurations, data enrichment and analytics for detecting a specific type of risk. For example, you may have a Solution for application fraud and another for inbound/outbound payments, subject to your programs set up with Thredd and Featurespace. The same event may trigger separate alerts in different Solutions.

Solution ID

Each Solution is uniquely identified by a Solution ID in the event data.

Solution UI

The fraud system user interface that users access when they open the relevant Solution. The Solution UI is mainly used for reviewing incidents that are specific to that Solution, and can be customized for detecting the relevant type of financial risk.

State

Every entity has a state - a combination of information about the entity that the systems has accumulated over time. This is also called a behavioral profile. Every event processed by the system has the potential to update an entity's state, adding more information or updating information that the system can use to build a behavioral profile of a customer or card for example.

T

Tag

Rules, aggregators and models can add tags to alerts, to give analysts more information or to automate a response in a downstream system, such as declining a transaction.

Thredd Portal

Thredd Portal is Thredd's new web application for managing your cards and transactions on the Thredd Platform.

Token

Displays the unique token linked to the card PAN on which the transaction was made.



Document History

Version	Date	Description	Revised by
1.2	11/02/2025	Added references to Thredd Portal, our new web application for managing your cards and transactions.	JB
	29/01/2025	New BIN Attacks section added.	JB
	25/11/2024	New Reports section added.	JB
	27/06/2024	Updated the company address .	PC
1.1	24/04/2024	Updates to content and graphics to align with taxonomy updates on our Documentation Portal. New Sandbox Replay section added.	JB
1.0	01/12/2023	First version	JB



Contact Us

Please contact us if you have queries relating to this document. Our contact details are provided below.

Thredd UK Ltd.

Company registration number 09926803

Support Email: occ@thredd.com

Telephone: +44 (0) 203 740 9682

Our Head Office

Kingsbourne House
229-231 High Holborn
London
WC1V 7DA

Technical Publications

If you want to contact our technical publications team directly, for queries or feedback related to this guide, you can email us at:
docs@thredd.com.