Client Landlord Portal Guide
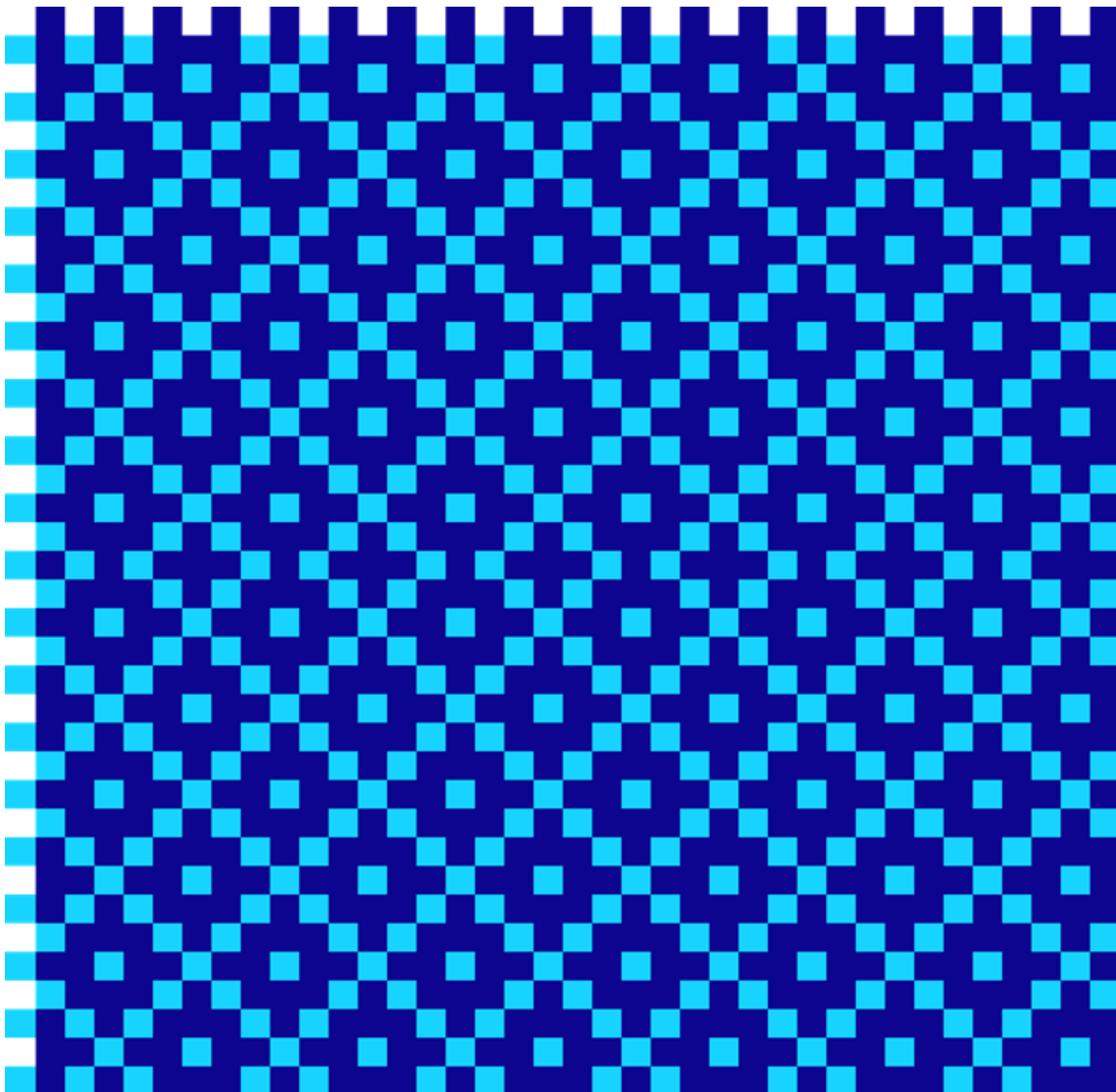
Powered by Featurespace

Version: 1.0

15 May 2024

For the latest technical documentation, see the Documentation Portal.

Thredd 6th Floor, Victoria House, Bloomsbury Square, London, WC1B 4DA

Support Email: occ@thredd.com

Support Phone: +44 (0) 203 740 9682

Copyright

About This Document

This document describes how to use the Client Landlord Portal to:

- Create and manage tenants for Analytics Config Groups (ACGs)
- Take control of a tenant
- Create and manage reports

> **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 as a client landlord.

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
Fraud AMDL Rules Configuration Guide	Explains how to configure the rules used by theThreddFraud Transaction Monitoring System.
Fraud Transaction Monitoring System Access Configuration Guide	Describes how to set up user access and user access role available.
Fraud Transaction Monitoring Portal Guide	Describes how to use the Fraud Transaction Monitoring Portal to review high-risk incidents flagged by the system, configure the behaviour of the system, and view, manage and understand the various reports and metrics available in the portal.

Other Guides

Refer to the table below for other relevant documents.

Document	Description
Payments Dispute Management Guide	Describes how to manage chargebacks and the disputes management process using Thredd.
Smart Client Guide	Describes how to use the Thredd Smart Client to manage your account.

> **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.
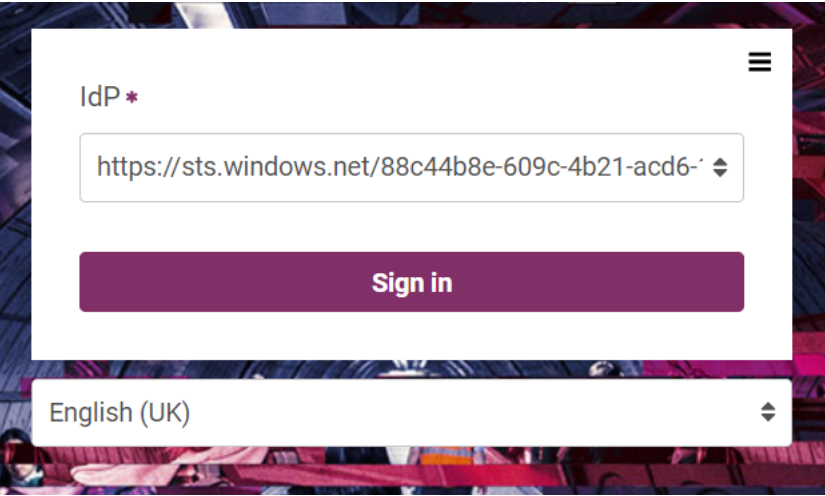

Figure 1: Sign-In Page

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.

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 Client Landlord Dashboard

The Client Landlord Dashboard is the first page you see when you log in. The Dashboard section allows you to view a summary of statistics related to data processing, performance of models and rules, and incident management.
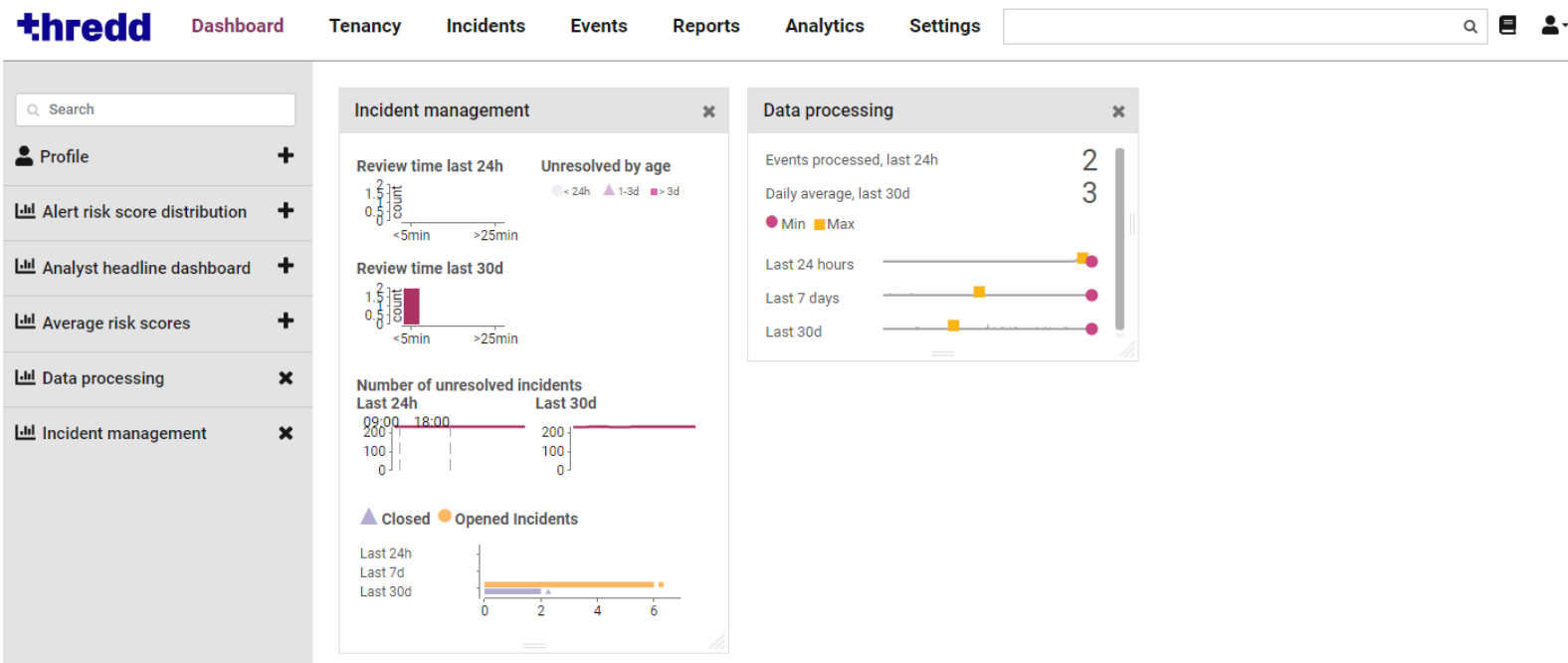

Figure 2: Client Landlord Dashboard

You can customise the dashboard for each user, allowing them to see a personalised layout made up from pre-defined panels and reports. You can also display a summary panel at the top of the dashboard, showing summary metrics.

> **Note:** This dashboard is not available for tenants.

The panels are populated from your Reports page. By default, there are six panels you can add to the dashboard.

- **Profile** displays the details of your user account, including roles and permissions.
- **Alert Risk Score Distribution** displays the count of alerts over the last 24 hours, and the distribution of risk scores for these alerts.
- **Analyst Headline Dashboard** displays statistics for each analyst, broken down into the total figures for yesterday, and daily averages calculated over the last 7 days and the last 30 days.
- **Average Risk Scores** displays the total number of incidents (per entity), alerts and events for today, the last 7 days, the last 30 days or the last 365 days.
- **Data Processing** displays the total number of events process over for today, the last 7 days, and the last 30 days.
- **Incident Management** displays a number of metrics, such as review time and incidents closed and opened, related to analyst performance over the past 30 days.

Customising Your Dashboard

Your dashboard can be customised to your needs and preferences by changing which dashboard panels are displayed, how large each panel is, and where it is located on your dashboard.

- To add a panel, simply drag and drop the panel of your choice from the sidebar. Or, click on the name of the panel in the sidebar.
- To move a panel to a new location on the dashboard, click anywhere on the panel and drag the panel to a new location.
- To resize panels, click and drag the right-hand side, bottom or bottom-right corner of the panel.

Note: For information on how to create a report that displays on a dashboard, see Manage Reports.

3 Managing Tenancy

> **IMPORTANT:** Do not use the Create or Edit tenant functionality. Creating or editing a tenant is considered a breach of the agreement between you and Thredd.

You can use the Tenancy section of the portal to manage and control your tenants and solutions. From the Tenancy page you can:

- Manage the analytics of your Analytics Configuration Groups (ACG)
- Manage your tenants
- Take direct control of your tenants to manage their events and incidents directly

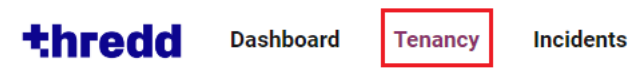Click **Tenancy** in the portal header to open the Tenancy page.

Figure 3: Tenancy option in the Portal header

Tenancy Overview

The Tenancy Overview page gives you an overview of the Analytics Configuration Groups (ACG) and the tenants linked to them. It shows the hierarchy of ACGs, as well as what tenants belong to which ACG and tier.
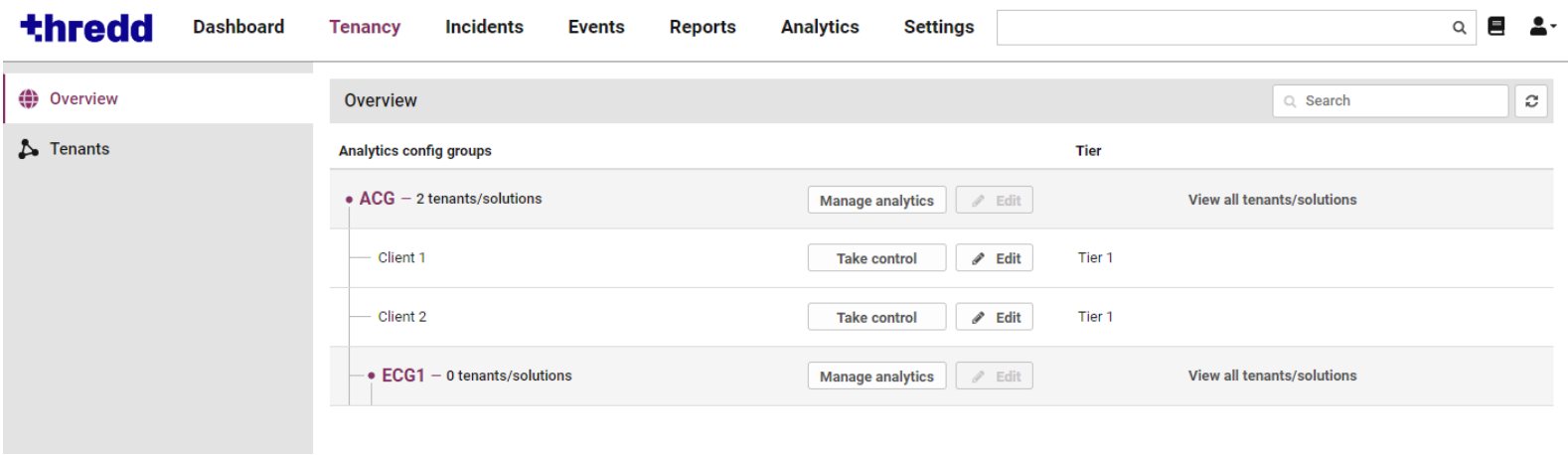
Figure 4: Tenancy Overview Page

You can use the page to select which ACG-level analytics you want to view.

The ACGs you manage are displayed in a tree view, with any child ACGs displayed below their parent. Analytics in a parent ACG are also applied to tenants in the child ACG. The Universal ACG is at the top of the tree. Next to the name of each ACG, you can see the number of tenants in that ACG.

Figure 5: Analytics Configuration Groups (ACG) example

To view a list of all the tenants in an ACG, on the right of the relevant ACG, click **View all Tenants/Solutions**.

Search for a Tenant

You can search for a tenant using the Search field in the top-right of the page.

Manage Analytics

Click **Manage Analytics** to open the Analytics page of the ACG. For more information on managing analytics, see Analytics Configuration.

Take Control of a Tenant
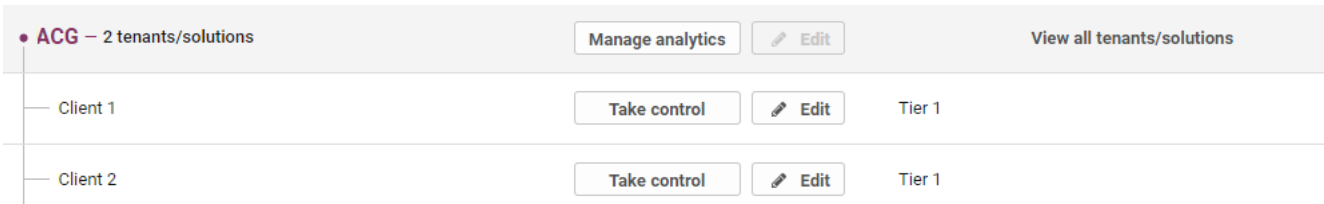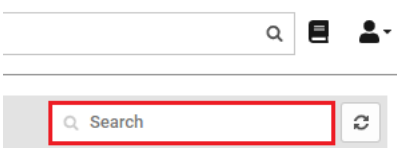
Taking control of a tenant enables you to review incidents specific to that tenant. Depending on your permissions, you can also:

- Add event data to data lists including data lists made at the tenant level (see Adding Items to a Data List)
- Apply tenant-level incident filters to the incident list (see Filtering Incidents)
- Refer incidents to a tenant user or team (see Referring Incidents)
- View a list of incidents that have been referred to you (see Viewing Incident groups)

Click **Take Control** to directly control a tenant. This opens the Fraud Portal for the tenant, with a menu across the top of the page displaying the name of the tenant you're controlling. Click **Release Control** to release control of the tenant you are controlling and return to the Tenancy page.

The following shows an example of a tenant dashboard after taking control of it.
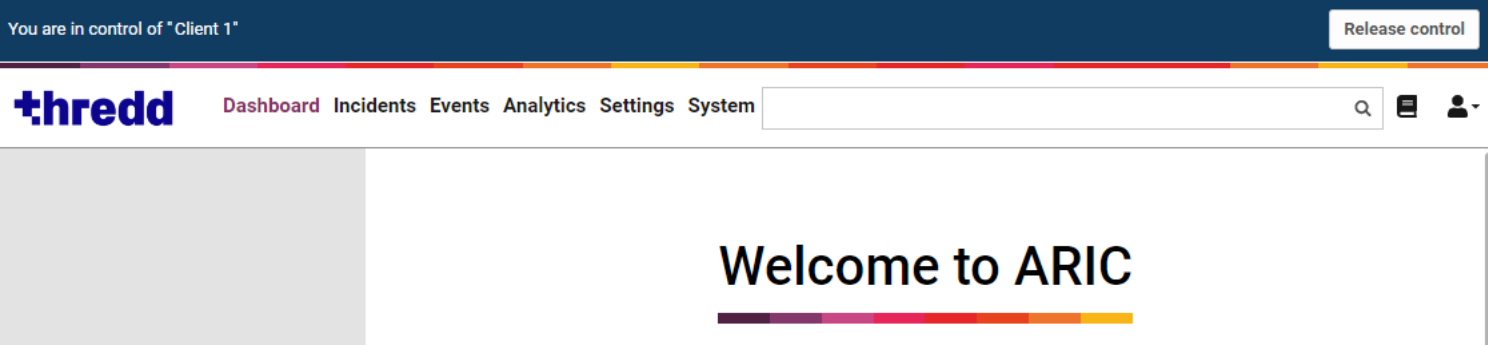
Figure 7: Tenant control page

4 Tenancy List

The Tenancy page lists all the tenants you are assigned to manage. From this page you can take control of a tenant.

> **IMPORTANT:** Do not use the Create or Edit tenant functionality. Creating or editing a tenant is considered a breach of the agreement between you and Thredd.

Figure 8: Tenant List page

Take Control of a Tenant

Taking control of a tenant enables you to view the Tenant UI and manage the tenant users and tenant-level analytics. Click **Take Control** to open the Tenant UI.

You now have control of the tenant, enabling you to use the Portal as a typical user. This includes

- Managing incidents for the tenant
- Viewing events associated with the tenant
- Configuring analytics for the tenant

5 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.
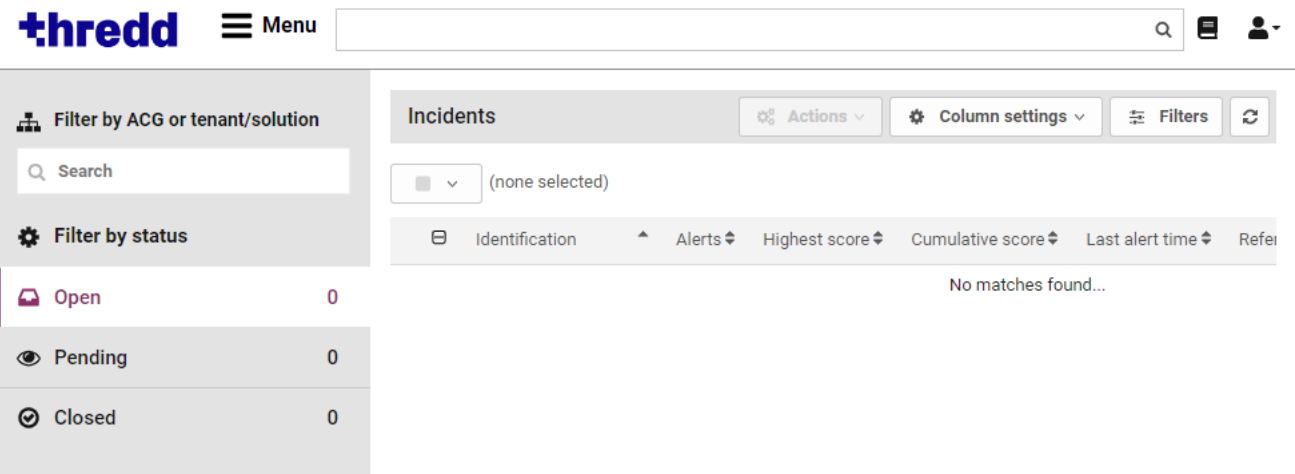
Figure 9: Open Incidents page

> **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
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 ⟳ .
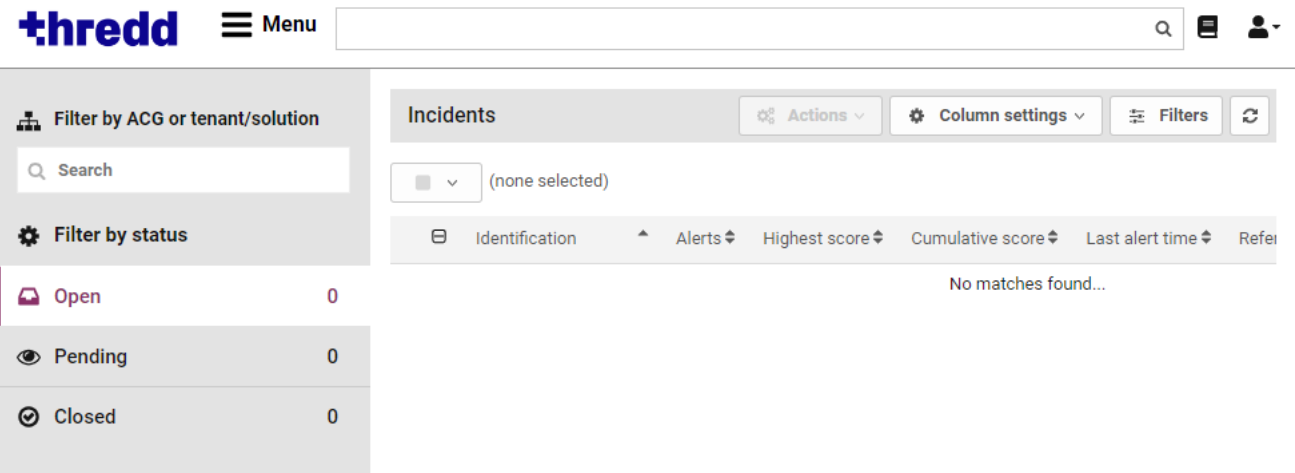
Figure 10: Incidents Page

You can expand an incident and view more details by clicking on the down arrow next to the entity ID.
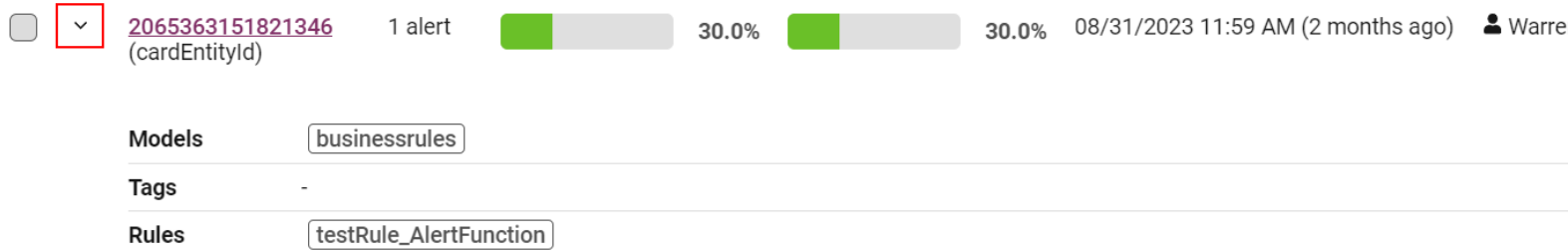
Figure 11: Incident drop-down

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.
- **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.

Filter by ACG or Tenant

Filter by ACG or Tenant enables you to narrow down the incidents listed to those relating to a single tenant or an Analytics Config Group. To apply a filter, click in the Search field and start typing the name of an ACG or enter a tenant ID.
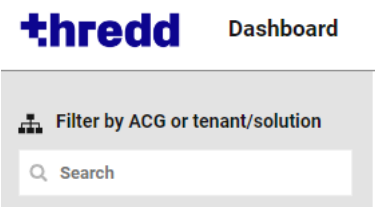
As you start typing, ACGs and tenant IDs which match your search will be suggested. Alternatively, you can click on the box and select an ACG name or tenant ID from the list of suggestions.
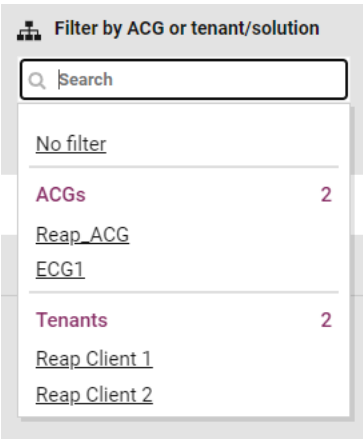
Pre-set incident filters

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:

- **Filter by ACG or tenant**: show only incidents for the ACG or tenant entered into the field.
- **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.
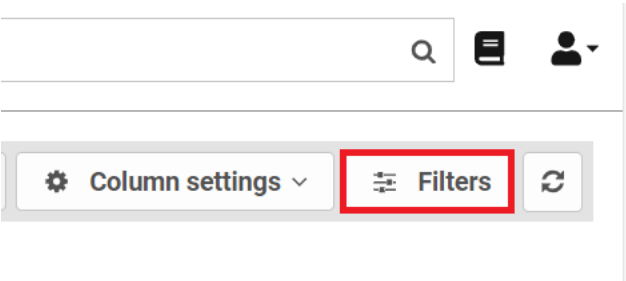
Any active incident filters apply to all the Incident Lists:

- Open
- Closed
- Pending

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.
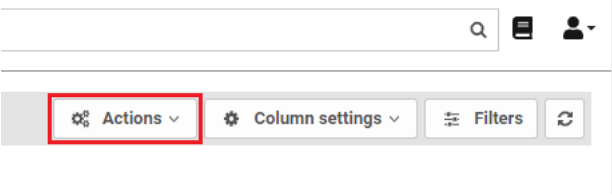
Figure 12: Incident Actions menu

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).

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.

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

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.

2. Click **Actions**.

3. Either:

    a. Review all incidents as 'risk':

        i. Click **Review Selected as Risk**.

        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.

        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 ⇕

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**.
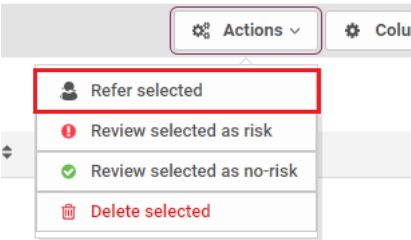
Bulk Incident Deletions

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).

2. Click the **Actions** button.

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.

6 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.

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. **Note:** Put double quotes around values that contain spaces. For example, to search for all events that contain 'John Smith', type "John Smith".
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" **Note:** Put double quotes around search terms that contain spaces.
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.

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.

Filter by Risk Score

To filter the events list by risk score:

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

```
←  Back
Risk Score Filter        ◀
Event Type Filter        ◀
Event Time Filter        ◀
```
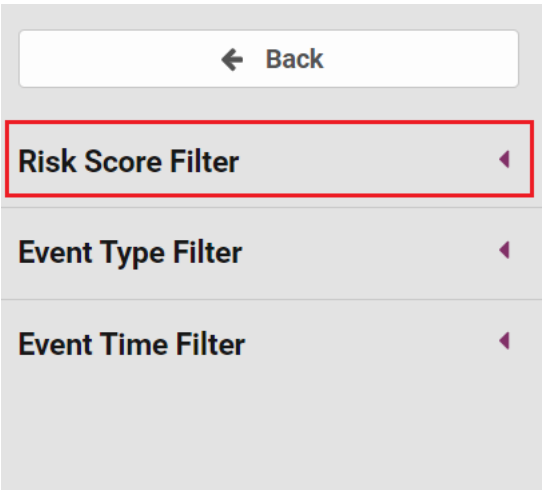
2. If you have risk scores for more than one entity type, select the relevant entity type from the drop-down menu.

```
Event Type Filter        ◀
Risk Score Filter        ▼
Please choose an option...   ⬍
Please choose an option...
accountEntityId
cardEntityId
customerEntityId
deviceEntityId
mccEntityId
merchantEntityId
Event Time Filter        ◀
```
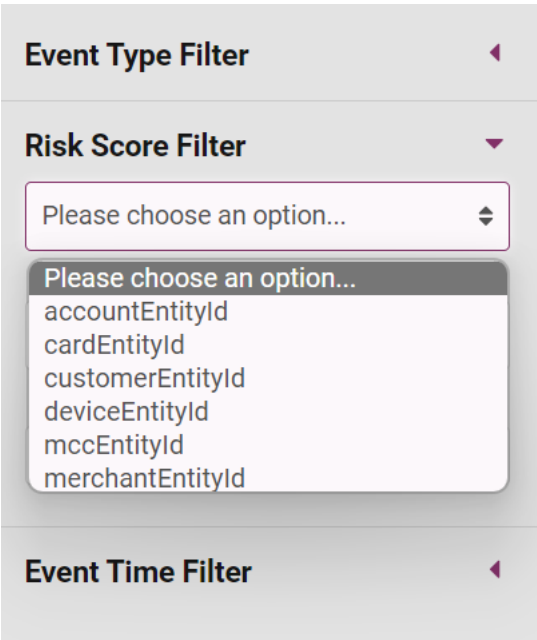
3. Set the range of risk scores for the filter by either dragging the sliders or by manually entering the maximum and minimum values.

```
Risk Score Filter        ▼
Please choose an option...   ⬍
0  ‖————————————‖ 100
   0    50    100
Update filter
```
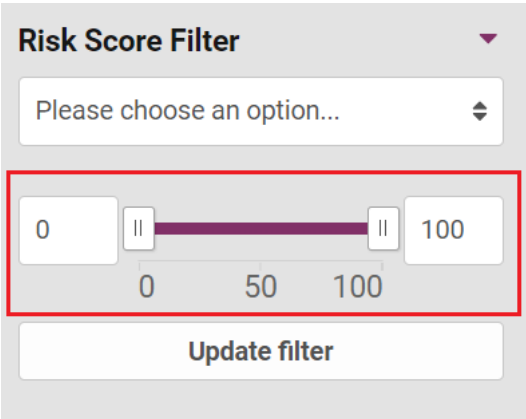
4. Click the **Update Filter** button.

```
Risk Score Filter        ▼
cardEntityId             ⬍
49  ———‖——————‖ 100
   0    50    100
Update filter
```
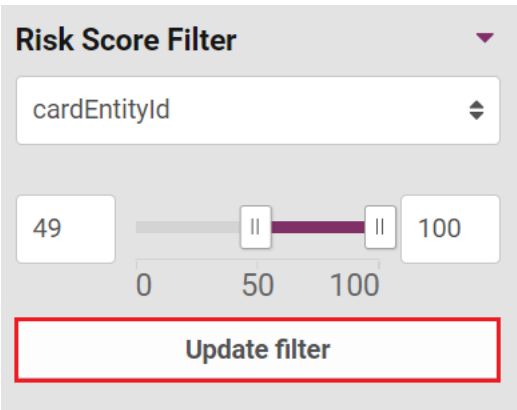
The filter appears at the bottom of the Risk Score Filter section, which you can remove by clicking **X** on the filter.

Filter by Event Type

To filter the events list by event type:

1. In the sidebar, click **Event Type Filter**.
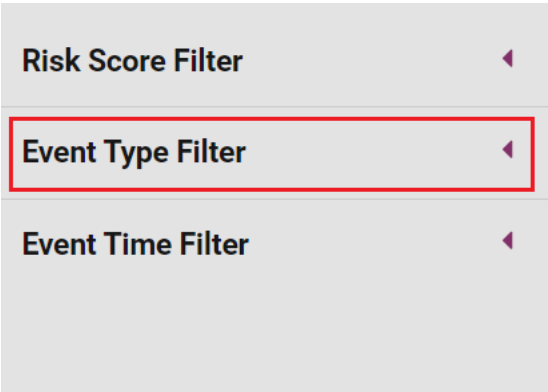
2. (Optional) Use the search box to find the event types you want to show or hide.
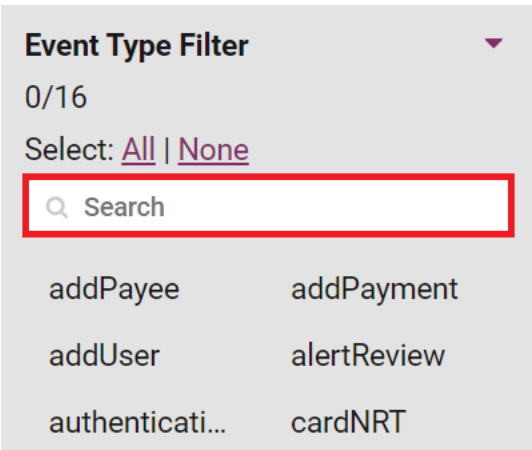
Note: Only cardRT,cardNRT and transactionReturn event types are currently supported.

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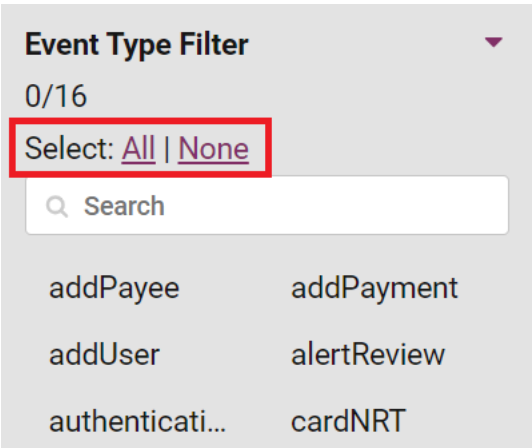
4. Select or deselect the event types that you want to show or hide in the events list.

5. Click **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**.

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

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: ✖   evice Entity ID ⇕ Account Entity ID
49 – 100 (accountEntityI
d)

Using the Event Details Sidebar

To see more details of a specific event, click the row for the event in the list. On the right of the page, the event details sidebar opens.

Figure 16: Event Details sidebar

The event details sidebar in the Events page is similar to the event details sidebar in the Incident page. You can use it to see what models and rules have triggered on the event and what tags have been added. You can also use the sidebar to see detailed information about the event.

To switch between entities: in the **Select entity** field, select the appropriate entity.

The list of models, rules and tags displayed in the event details sidebar is updated to show items relating to analytics associated with the selected entity.

To see detailed information about an event, click the Eye button at the top of the sidebar.

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
☑ Event Time	⇕	⇕
☑ Event type	⇕	⇕
☑ Card Entity ID	⇕	⇕
☑ Customer Entity ID	⇕	⇕
☑ MCC Entity ID		
☑ Merchant Entity ID	⇕	⇕
☑ Device Entity ID	⇕	⇕
☑ 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
☑ Event Time	⇕	⇕
☑ Event type	⇕	⇕
☑ Card Entity ID	⇕	⇕
☑ Customer Entity ID	⇕	⇕
☑ MCC Entity ID		
☑ Merchant Entity ID	⇕	⇕
☑ Device Entity ID	⇕	⇕
☑ Account Entity ID	⇕	⇕

+ Add column

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

Name

Fee Value

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

Fee Value

JSON path *

fee.value

Create   Cancel

4. Click the **Create** button.

Name

Fee Value

JSON path *

fee.value

Create   Cancel

The new field appears in the Events List.

Edit a Column

To edit an added column:

1. Click **Column Settings**.

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

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**.

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

3. Click **Delete**.

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**.

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

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

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

7 Reports

The Reports section of the Fraud Portal enables you to view and create reports that can be used to monitor and visualise overall trends and analytics performance, as well as monitor and compare analyst performance over time.

Click **Reports** in the UI header to open the Reports page.
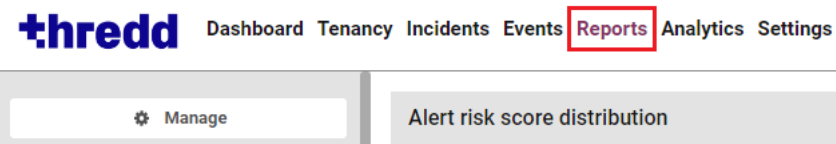
Figure 17: Reports in the Portal header

All the reports and dashboard panels that are visible to you are listed in the Reports sidebar. Each report or panel has an icon next to it, which indicates what kind of report it is.
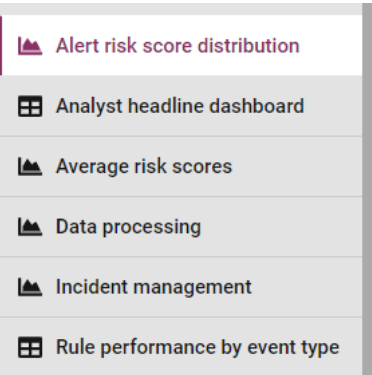
Figure 18: Reports sidebar

By default, the following reports are available:

- Alert Risk Score Distribution shows the count of alerts over the last 24 hours, and the distribution of risk scores for these alerts.
- Analyst headline dashboard shows a number of statistics for each analyst, broken down into the total figures for yesterday, and daily averages calculated over the last 7 days and the last 30 days
- Average Risk Scores shows the total number of incidents (per entity), alerts and events for today, the last 7 days, the last 30 days or the last 365 days.
- Data Processing shows the total amount of events processed over the last 24 hours, the last 7 days and the last 30 days
- Incident management shows visual indicators of a number of metrics related to analyst performance over the past 30 days.
- Rule performance by event type shows the volume of alerts raised by each rule/model and the false positive ratio for each event type.

Custom reports are shown in their own sections of the reports sidebar, headed Line Charts for line charts, Overview for overview panels, and Tables for tables.
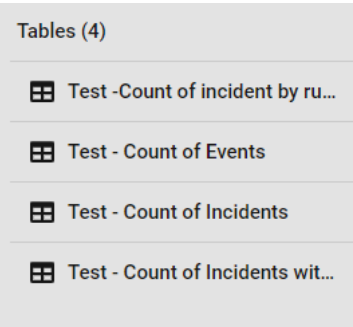
Figure 19: Example Custom Reports Sidebar

From this page, you can:

- To view a report, click the name of the report in the sidebar. The report will display in the main pane.

- To search for a specific report or reports, enter your search term in the Search field at the top of the reports sidebar. Any reports with names that contain your search term are displayed in the sidebar.

- To export report data in Comma-Separated Values (CSV) format, for further processing and analytics, click **Export Data (CSV)** at the top-right of the report.

Manage Reports

The Manage Reports screen consists of two sections: Reports (pre-generated) at the top, and the Custom Reports at the bottom of the page. Click **Manage** in the top-left corner of the Reports page to open Manage Reports.

Pre-Generated Reports

Pre-generated reports can be set to one of four visibility levels, which control what landlord users can see in the reports sidebar:

- **Hidden**: The report is not visible to any users.
- **Visible to User**: The report is visible to one specific user.
- **Visible to Role**: The report is visible to all users with a specific user role.
- **Public**: The report is visible to all users.

The visibility level of each report is displayed in the Visibility column of the Reports list.

To change the visibility level of pre-generated reports:

1. Select the check boxes for the report or reports you want to change the visibility of.

2. Click **Update Reports**.

   The Edit Reports window displays.

3. Select a new visibility level from the **Visibility Level** field.

   Note: If you select the Visible to Role or Visible to User options, a Role and User field displays respectively. Select a role or user for the reports to be visible from the field.

4. Click **Submit**.

Custom Reports

The bottom of the Manage Reports page shows a list of Custom Reports. Customised reports are created by users using a pre-set list of attributes. Custom reports can be set to one of three visibility levels, which control which users can see that report in the reports sidebar:

- **Private**: The report is visible only to the user who created it.
- **Visible to Role**: The report is visible to all users with a specific user role.
- **Public**: The report is visible to all users.

Line Charts

Line chart reports display the values over time of one (or more) reporting attributes.
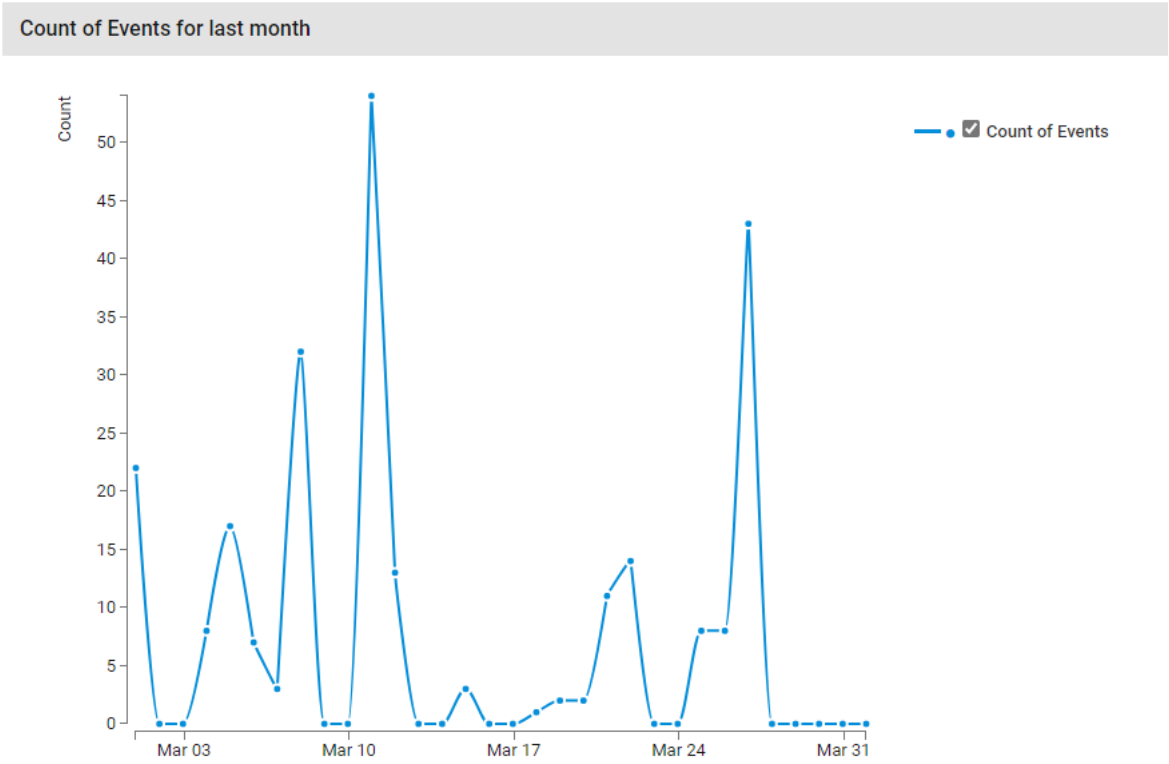
Where a report attribute contains multiple grouped counts (For example, Count of Events or Grouped by Event Type), each grouping will be displayed as a separate line. In addition, a 'total' line will be displayed which displays the total of all sub-groups contained in the attribute.

Line visibility can be toggled on or off by selecting or clearing the boxes in the key to the right of the chart. Individual sub-group lines cannot be individually toggled in this way.
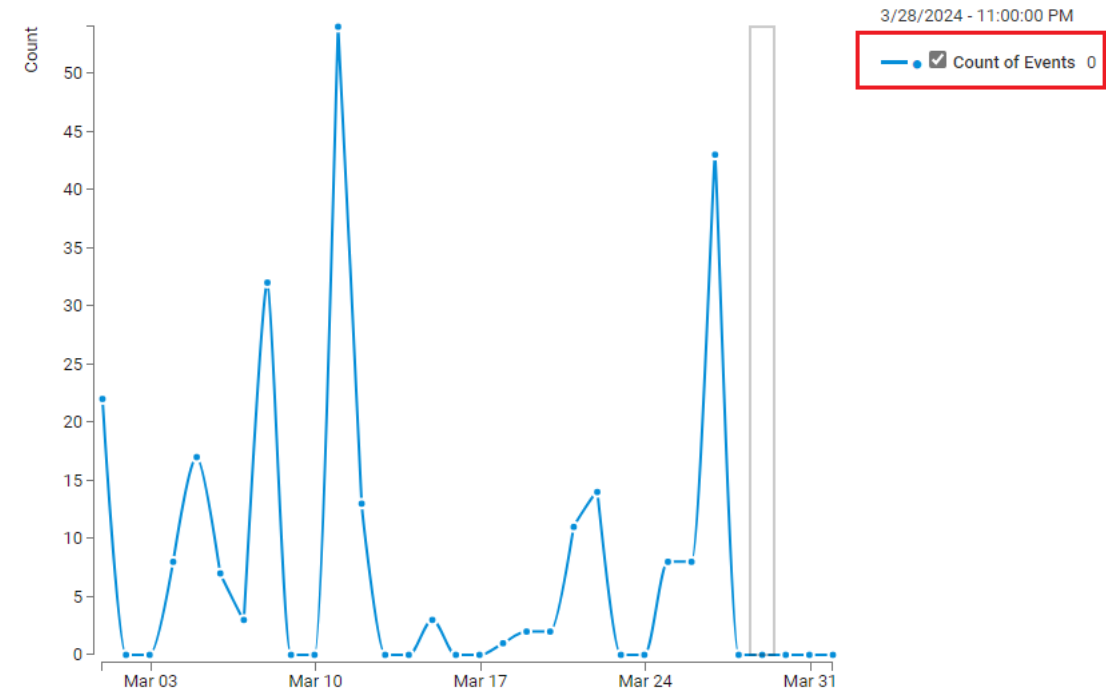
Details of the data contained at any data point can be displayed by placing the mouse cursor over the point. A tooltip box will appear. This displays the y-axis value of the data point, the x-axis date stamp, and which attribute line (or lines) intersect with the data point.

All data displayed on a custom line chart can be downloaded in CSV format. Click **Export Data (CSV)** to export the report.

Create Line Chart Report

To create a line chart report:

1. Click **Create Custom Report**.

The Create Report page displays.

2. Select Line Chart from the **Report Type** field.

3. Enter a name for the report in the Report field.

4. (Optional) Enter a description for the report in the Description field.

5. Select the attributes you want to include in the report from the Attributes field. You can select up to 6 attributes from this list.

6. Select the visibility level for the report from the Visibility Level field.

7. Select the date range the report will pull data from the Date Range field. If you select the Custom option, use the Start and End fields to set the range.

8. Click **Create** to create the report.

Tables

Table reports display the total values of one reporting attribute during the configured time period.

Test - Count of Events - Count of Events (17/3/2024 12:00 AM - 16/4/2024 12:00 PM)	
	⬇ Export data (CSV)
Date range	**Count of Events**
17/3/2024 12:00 AM - 14/4/2024 12:59 AM	143
14/4/2024 1:00 AM - 16/4/2024 11:59 AM	2

Where a report attribute contains multiple grouped counts (For example, Count of Events, Grouped by Event Type), each grouping will be displayed as a separate column or row in the table.

For single-level grouped attributes (For example, Count of Incidents, Grouped By Triggered Rules), the sub-groups (For example, for each triggered rule) will be displayed in separate columns.

For two-level grouped attributes (For example, Count of Incidents, Grouped By Event Types, Triggered Rules), the first grouping (For example, Event Types) will be displayed as separate rows, and the second grouping (For example, Triggered Rules) will be displayed as separate columns. All data displayed in a custom table can be downloaded in CSV format. Click **Export Data (CSV)** to export the report.

Create a Table Report

To create a table report:

1. Click **Create Custom Report**.

Custom reports					
10 ⬍ per page			➕ Create custom report	🔍 Search	↻
Dashboard ⬍	**Name** ⬍	**Type** ⬍	**Visibility** ⬍		
⊗	Test -Count of incident by rule rule triggers	Table	Public	✏ Edit	🗑 Delete

2. Select Table from the **Report Type** field.

3. Enter a name for the report in the Report field.

Name ★

Count of Incidents for last week

4. Enter a description for the report in the Description field.

5. Select an attribute you want to include in the table from the Attributes field.

Attribute ★

Please choose an option...

Count of Distinct Entities Grouped by Rule Review Status
Count of Distinct Entities in Events
Count of Events
Count of Events Grouped by Event Types
Count of Incidents
Count of Incidents Grouped by Event Types Triggered Models
Count of Incidents Grouped by Event Types Triggered Rules
Count of Incidents Grouped by Triggered Models
Count of Incidents Grouped by Triggered Rules
Count of Incidents with Triggered Rules
Count of Reviews Grouped by Model Review Status
Count of Reviews Grouped by Review Status
Count of Reviews Grouped by Rule Review Status

6. Select the visibility level for the report from the Visibility Level field.

Visibility level *

Private	⇕

7. Select the date range the report will pull data from the Date Range field. If you select the Custom option, use the Start and End fields to set the range.

Date range *

Last 7 days	⇕

8. Click **Create** to create the report.

Cancel   Create

Overviews

An overview is a report that can be viewed in a user's dashboard.

Create Overview Panel

To create a custom overview panel:

1. Click **Create Custom Report**.

Custom reports

10 ⇕ per page		+ Create custom report	🔍 Search	⟳

Dashboard ⇕	Name ⇕	Type ⇕	Visibility ⇕		
❌	Test -Count of incident by rule rule triggers	Table	Public	✏️ Edit	🗑 Delete

2. Select Overview from the **Report Type** field.

Report type *

Overview	⇕

3. Enter a name for the report in the **Name** field.

Name *

Count of Incidents for last week

4. (Optional) Enter a description for the report in the **Description** field.

5. Select an attribute you want to include in the summary panel from the Attributes field. You can select up to three attributes from this list.

Attributes *

1 of 13 selected	⇕

🔍 Search

☐ Select all

☐ Count of Distinct Entities in Events
☐ Count of Events
☐ Count of Events Grouped by Event Types
☑ Count of Incidents
☐ Count of Incidents Grouped by Event Types Triggered Models

> **Note:** An overview panel will not show attributes broken down into specific categories. For example, selecting 'Count of Events, Grouped by Event Types' will show the same information as selecting 'Count of Events' (the total number of events processed by the portal in the selected time range).

6. Select the visibility level for the report from the **Visibility Level** field.

    Visibility level •
    [Private ⬍]

7. Select the date range the report will pull data from the **Date Range** field. If you select the Custom option, use the Start and End fields to set the range.

    Date range •
    [Last 7 days ⬍]

8. Click **Create** to create the report.

    [Cancel] [Create]

8 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.
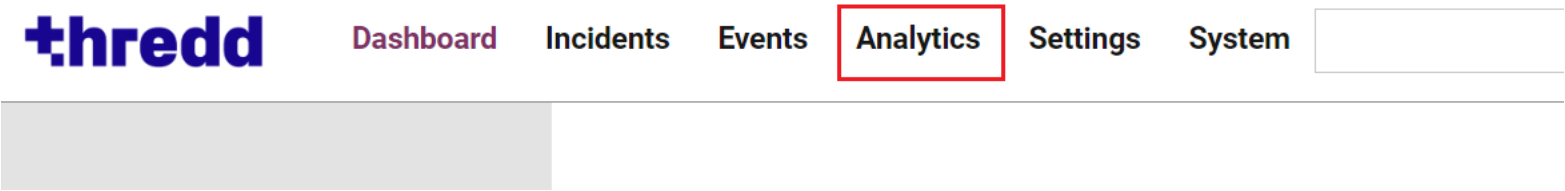
The portal has a built-in workflow for modifying analytics configuration (risk thresholds, rules, aggregators) and reviewing and approving these changes. Any changes to analytics configuration are made in a staging environment. These changes are not live (and hence do not affect the generation of alerts, 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.

Changing Analytics Config Group

The Overview field displays the current ACG you're viewing the analytics for. Use this page to manage the analytics for the ACG.
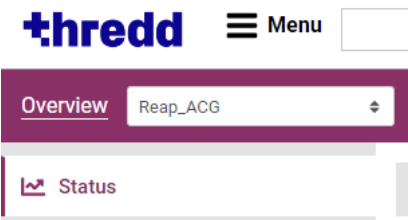
You can switch between the different ACGs you have permissions to use by clicking the field and selecting the ACG you want to view.

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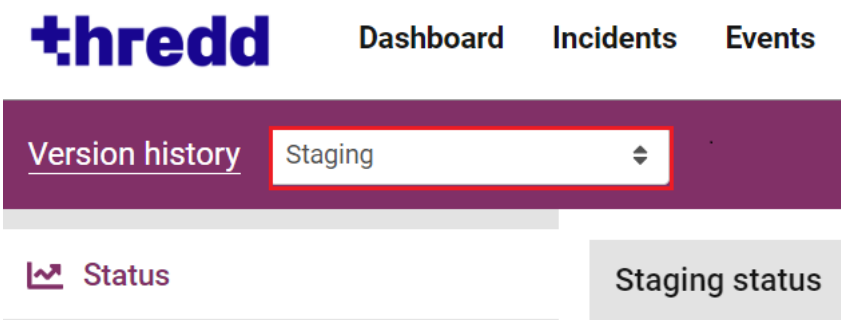
You can navigate the Analytics staging environment (and other analytics versions) in the same way as any other UI section. Links in the sidebar allow you to navigate to the individual pages for viewing the different kind of analytics configurations, and changing the configurations in staging.

> **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.
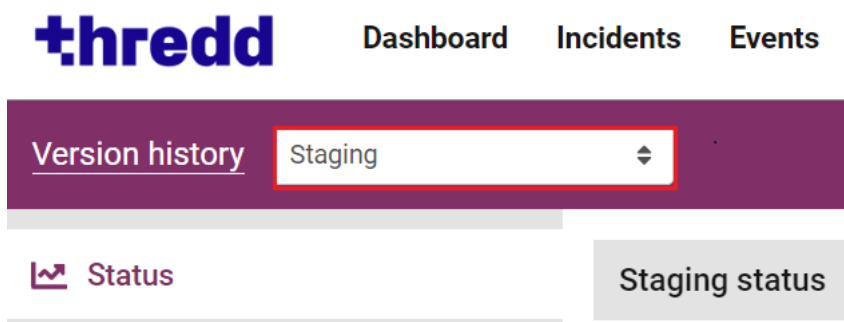
2. Click the version you want to view in the menu.
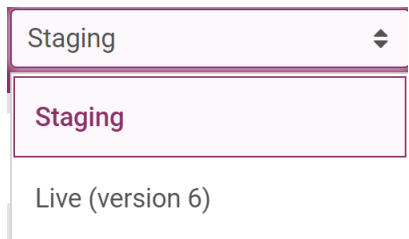
> **Note:** Analytics configuration can only be edited in the Staging environment.

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.
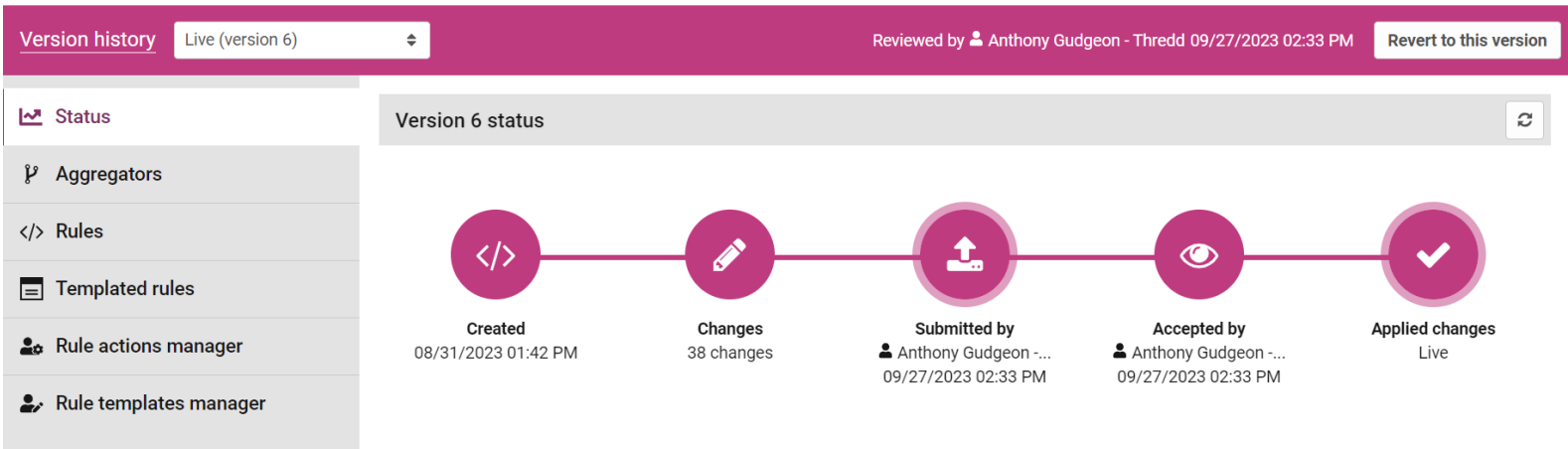
Viewing a historical analytics configuration version

To see a historical analytics configuration version click the **Version History** button.
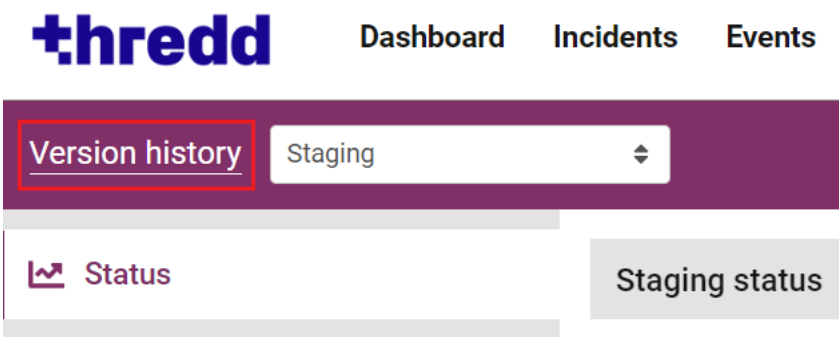
When viewing a historical version, the analytics header bar will change colour to grey. The user who reviewed the changes will show on the right, with the date and time changes were reviewed.
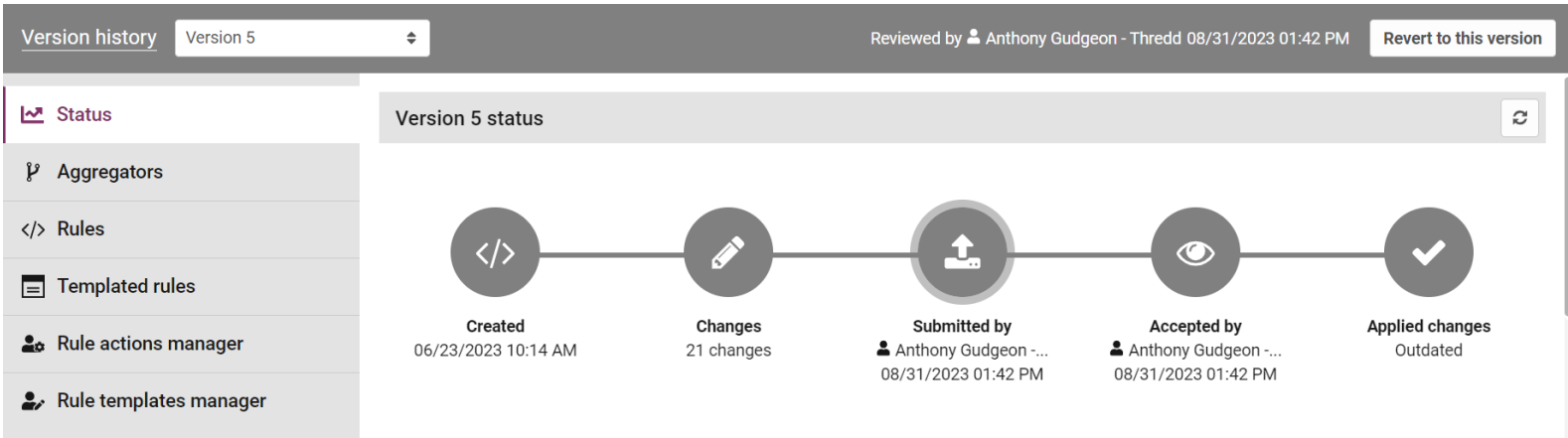
The version status will be shown in the flow chart. The decision after reviewing changes can be either:

- **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.

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

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.

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

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

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.

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.

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.

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

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

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 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).

9 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.
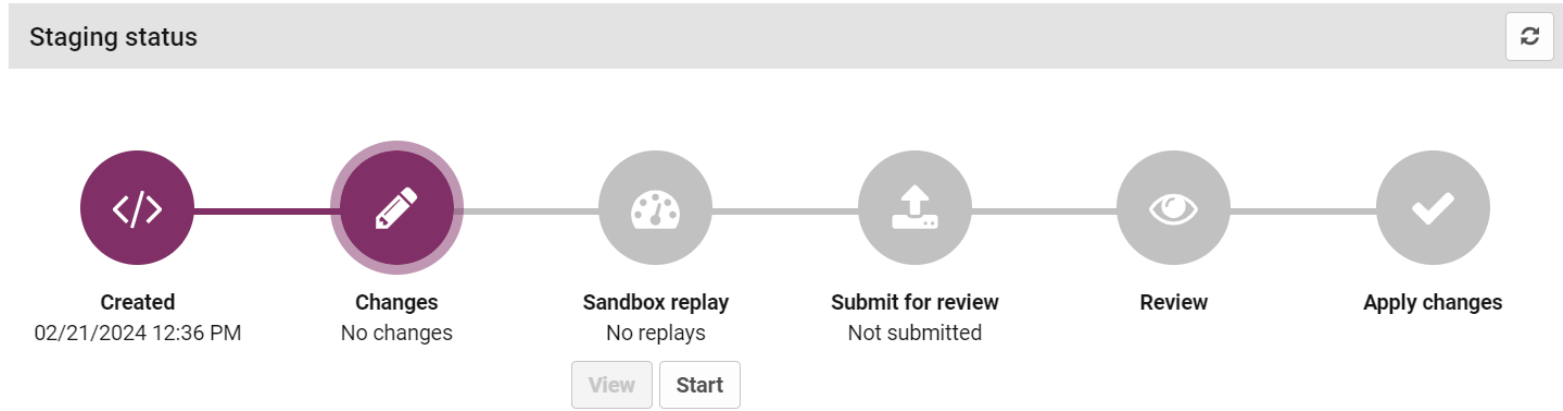
The Sandbox Replay icon displays the running Sandbox Replays for your analytics version. This is usually the staging version, which contains the changes that you might want to test before submitting for approval. Below the Sandbox Replay icon, you can see the status of any replays that have been run 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.

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	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: • 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. • 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

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:

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

Staging status

Created
02/21/2024 12:36 PM

Changes
No changes

Sandbox replay
No replays

View   Start

Submit for review
Not submitted

Review

Apply changes
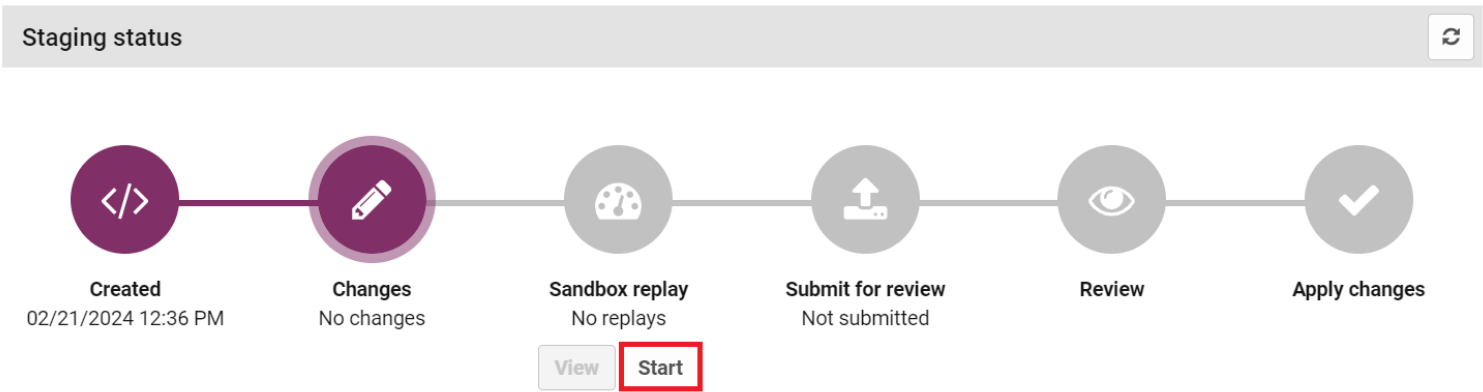
The Run Sandbox Replay window opens.

2. 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   To
27/02/2024   14:50   28/02/2024   14:50

State profile build-up period ❓   From   To   ✓ Percentage
27/02/2024   14:50   27/02/2024   17:15   10 %

3. 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 *	Select entity type to base downsampling by for replay ⇕
	accountEntityId
	cardEntityId
Sampling ❓	customerEntityId
	deviceEntityId
	mccEntityId
Configuration ❓	merchantEntityId

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**.

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.
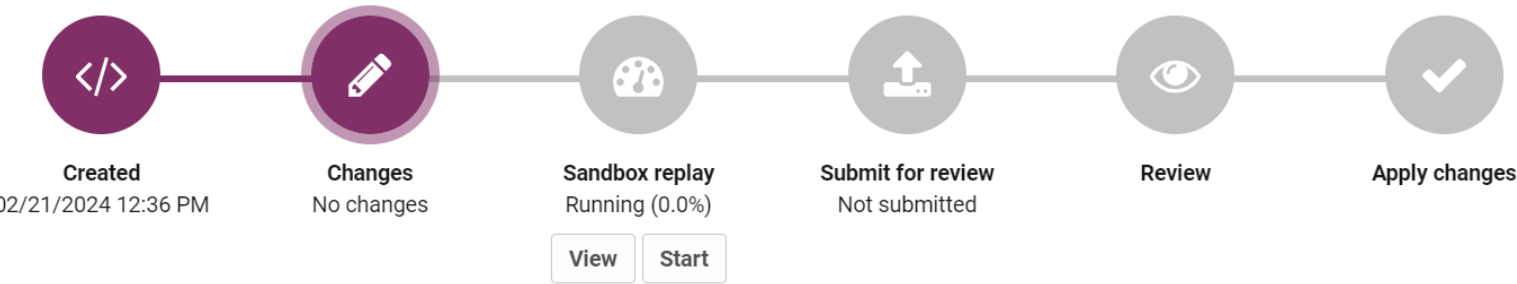
View Sandbox Replay Results

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.

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

10 Settings

The Settings page enables you to create and manage data lists. Data lists are lists of items that can be used by rules, allowing you to create negative and positive lists containing large numbers of values.

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. Each item can also have one or more properties, which form the other columns in the table.

Each data list has a visibility level: public, private or overridable.

- Public data lists can be viewed by tenant users that belong to the same ACG as the list, or that belong to any ACG that is a child of the list's ACG. Rules defined at the tenant level for tenants belonging to these ACGs can also refer to public lists.

- Private data lists can only be referred to by rules that belong to the same ACG as the list, and cannot be viewed by tenant users or referred to by tenant-level rules.

- Overridable data lists enable tenant users that belong to the same ACG as the list (or that belong to any ACG that is a child of the list's ACG) to add elements to a duplicated version of the list, so the original list remains visible only to landlord users. Tenant users can only view the list of overrides they have made to the list, not the items on the original list. Rules defined at the tenant level for tenants belonging to these ACGs can update a duplicated version of the list, but this does not alter the original list.

Lists can be created manually, an existing list can be imported, or analysts can add event or entity data to lists from the Incident Review screen.

Create 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.

3. Select the ACG the data list will be associated with from the Analytical Config Group field.

4. Select the visibility of the data list using the radio boxes. Select from:

   - **Public** data lists can be viewed by tenant users that belong to the same ACG as the list, or that belong to any ACG that is a child of the list's ACG. Rules defined against tenants belonging to these ACGs can also refer to public lists.

   - **Private** data lists can only be referred to by rules that belong to the same ACG as the list, and cannot be viewed by tenant users or referred to by tenant-level rules.

   - **Overridable** data lists enable tenant users that belong to the same ACG as the list (or that belong to any ACG that is a child of the list's ACG) to add elements to a duplicated version of the list.

5. (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.

   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.

6. 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.

7. Click **Create** 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.

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	✎ Edit	🗑 Delete
> 1431013170424633	11/13/2023 08:33 AM	11/13/2023 08:33 AM	✎ Edit	🗑 Delete

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	✖

➕ 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	✏ Edit	🗑 Delete

[First] [Previous] [**1**] [Next] [Last]

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

| **Edit data list** | **List items** |

[⤓ Download CSV] [**Batch tasks**] [+ Ad...]

[10 ⇕] per page

⊟ **Identifier** ▲

🗐 **Batch import**
🗑 **Batch delete**

No matches

A window will display.

4. Click **Choose File**.

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

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.

7. Click **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.

   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.

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.

4. Enter a comment in the Comment field.

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

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.

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

3. Click **Choose File**.

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

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

6. Click **Delete Items**.

11 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.

12 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 Monioring 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.

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 know 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 user interface for managing your account on the Thredd system. Smart Client is installed as a desktop application and requires a VPN connection to Thredd systems in order to be able to access your account. For more information, see the Smart Client Guide.

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.

Token

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

Document History

Version	Date	Description	Revised by
1.0	15/05/2024	First version	JB

Contact Us

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

Thredd Ltd.

Support Email: occ@thredd.com

Support Phone: +44 (0) 203 740 9682

Our Head Office

6th Floor,

Victoria House,

Bloomsbury Square,

London,

WC1B 4DA

Telephone: +44 (0)330 088 8761

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.