Fraud Access Configuration Guide

Powered by Featurespace

Version: 1.0

25 April 2024

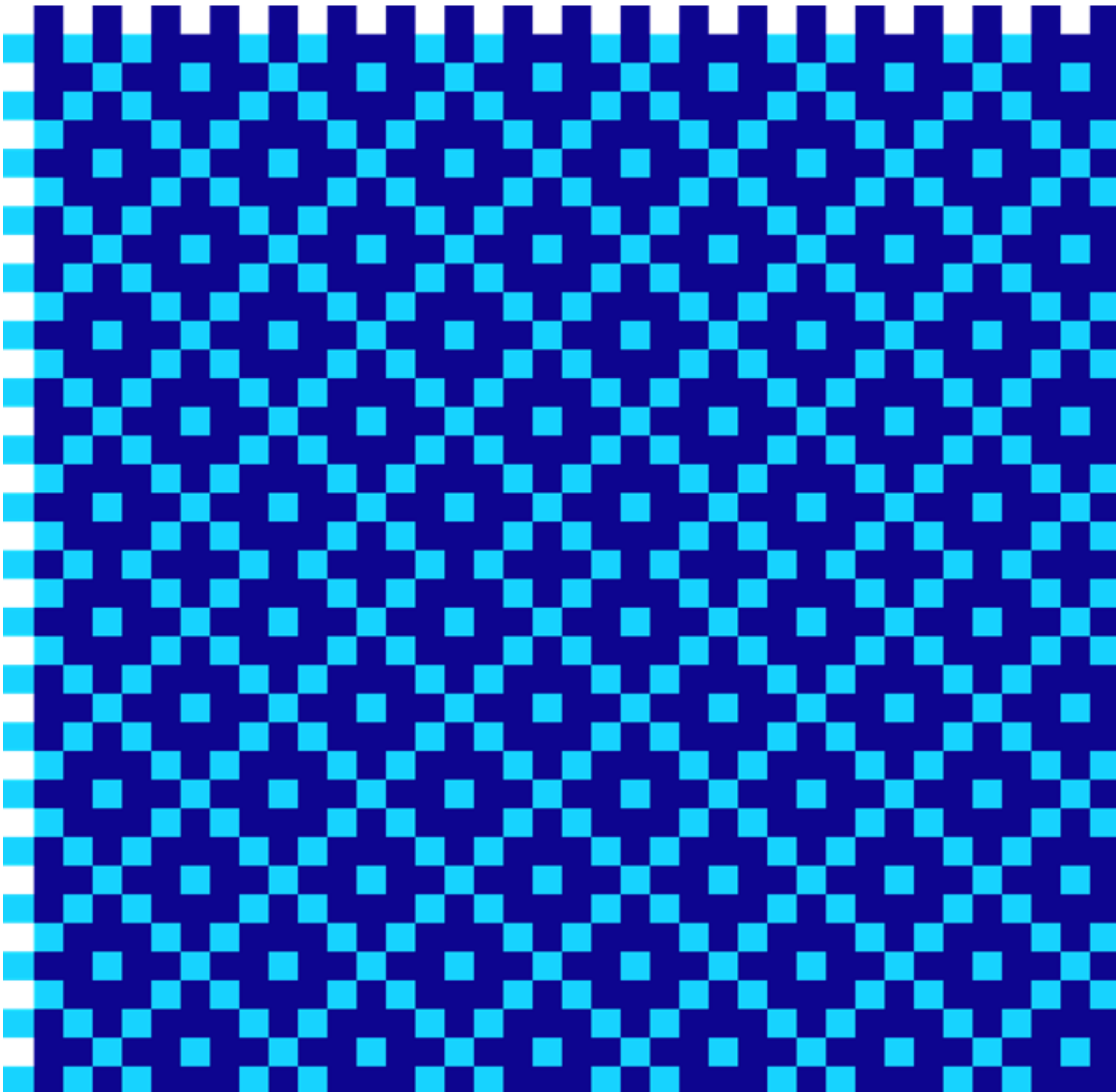
Publication number: FTMP-1.0-4/25/2024

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 the user roles available for access to the Fraud Transaction Monitoring Portal

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

Target Audience

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

What's Changed?

If you want to find out what's changed since the previous release, see the Document History section.

Related Documents

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

Document	Description
AMDL Rules Quick Start Guide	Explains how to configure the rules used by theThreddFraud Transaction Monitoring System.
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 User Roles

The following roles are available to users:

Role	Description
Risk Investigator	Allows a user to review and take action on incidents, see entity and event details, and to search and filter events. This role is typically assigned to someone with a job title such as fraud agent, financial crime analyst or AML investigator.
Risk Analyst	Allows a user to manage incidents in the same way as a Risk Investigator, manage analytics in the same way as a Risk Analyst and approve changes to analytics made by a Risk Analyst another Risk Manager or their own changes. **Note:** If you do not want a Risk Manager to have permissions to accept their own changes, please speak to your Account Manager.
Risk Manager	Allows a user to manage incidents in the same way as a Risk Analyst and approve changes to analytics made by a Risk Analyst.
Administrator	Grants a user all the permissions available to other user roles. In addition, this role allows a user to create other users, and manage the roles assigned to other users within your organisation. **Note**: This role is reserved for Thredd use.

Note: Thredd will set up the user roles for your organisation. You will be able to access the Fraud Transaction Monitoring Portal using Single Sign-On (SSO).

1.1 Creating a New User

If you need to create a new user, please raise a Thredd Customer Services Jira and provide details of the username, email address, user role (as above) and user contact mobile phone number.

Note: Thredd will be set up users with Single Sign-On (SSO) and the users will need to authenticate via their mobile device in order to access the Fraud Portal.

1.2 Viewing a User's Permissions

When a user logs in to the Fraud Transaction Monitoring Portal, their User Role and related permissions are displayed on the Portal Dashboard page. See the example below:

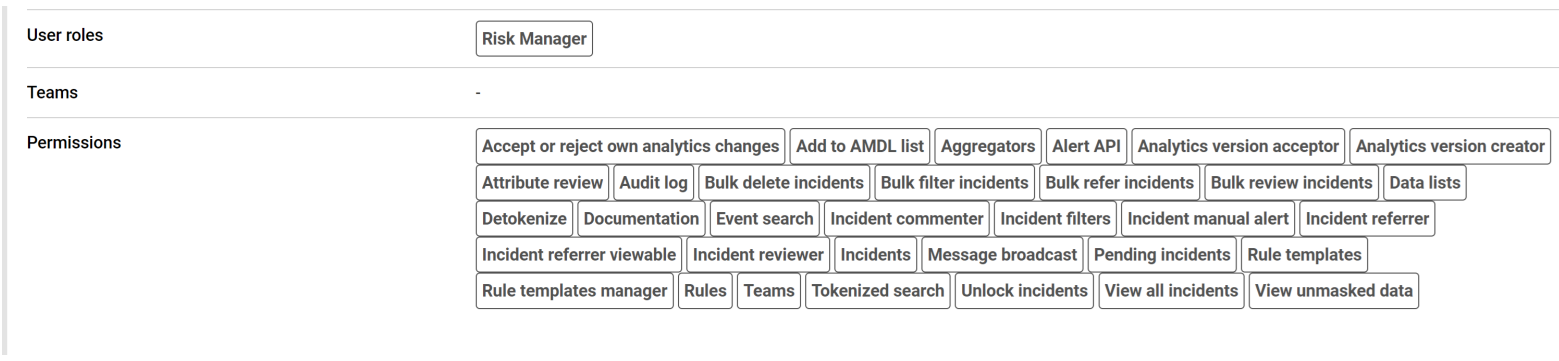


Figure 1: User roles and permissions shown on the Dashboard

1.3 List of User Permissions

The lists of permissions below show which permissions are assigned, by default, to each user role.

In the lists below, permissions that require another permission (referred to as the "parent permission") are indented below their parent permission, with a '∟' to indicate the parent-child relationship.

1.4 Incidents

The table below describes which permissions on the Fraud Transaction Monitoring Portal **Incidents** page are assigned, by default, to each user role.

Permission	Description	User Roles
Incidents	Access the Incident List. The permission also provides read-only access to the incident detail page. (To review incidents, a user must have the 'Incident reviewer' permission.)	Risk Investigator, Risk Analyst, Risk Manager, Administrator
∟Bulk delete incidents	Delete and incident or delete multiple incidents from the Incident List.	Risk Investigator, Risk Analyst, Risk Manager, Administrator
∟Bulk filter incidents	Filter incidents in the Incident List based on criteria including time, risk score, triggered rules and models.	Risk Investigator, Risk Analyst, Risk Manager, Administrator
∟Bulk refer incidents	Refer multiple incidents simultaneously to a user or team.	Risk Investigator, Risk Analyst, Risk Manager, Administrator
∟Bulk review incidents	Review multiple incidents simultaneously in the Incident List.	Risk Investigator, Risk Analyst, Risk Manager, Administrator
∟Add to AMDL list	Access the 'Add to list' option when reviewing an incident. This is used to add data from the current entity's event history to a data list.	Risk Investigator . Risk Analyst, Risk Manager, Administrator
∟Incident commenter	Add comments to incidents.	Risk Investigator, Risk Analyst, Risk Manager, Administrator
∟Incident manual alert	Create a manual alerts on an incident.	Risk Investigator, Risk Analyst, Risk Manager, Administrator
∟Incident reviewer	Review incidents.	Risk Investigator, Risk Analyst, Risk Manager, System Administrator
∟Incident referrer	Refer incidents to a user or team.	Risk Investigator, Risk Analyst, Risk Manager, Administrator
∟Incident referrer viewable	View incidents that have been referred to other users or teams.	Risk Investigator, Risk Analyst, Risk Manager
∟Unlock incidents	Unlock an incident that is being viewed by another user.	Risk Investigator, Risk Analyst, Risk Manager, Administrator
∟Pending incidents	View the 'Pending' list of incidents and add incidents to this list.	Risk Investigator, Risk Analyst, Risk Manager, Administrator
∟View all incidents	Access the 'All incidents' option in the Incident List filter dropdown menu. Without this permission, a user can only view the Incident List using incident filters.	Risk Investigator, Risk Analyst, Risk Manager, Administrator
∟Attribute review	Assign risk reasons to individual event fields when reviewing an incident.	Risk Investigator, Risk Analyst, Risk Manager, Administrator

1.5 Events

The table below describes which permissions on the Fraud Transaction Monitoring Portal **Events** page are assigned, by default, to each user role.

Permission	Description	User Roles
Event search	Access the search box and the 'Events' section.	Risk Investigator, Risk Analyst, Risk Manager, Administrator

1.6 Analytics

The table below describes which permissions on the Fraud Transaction Monitoring Portal **Analytics** page are assigned, by default, to each user role.

Permission	Description	User Roles
Aggregators	Create and edit aggregators.	Risk Analyst, Risk Manager Administrator
Analytics version acceptor	Approve or reject changes to analytics configuration that have been submitted for review, and to revert to a previous version.	Risk Manager, Administrator
Accept or reject own analytics changes	Approve or reject any changes to analytics configuration, including changes the user has made themselves. This enables a user to push analytics changes directly to live, bypassing the review process.	Risk Manager, Administrator
Analytics version creator	Submit changes to analytics configuration. Once submitted, the changes can be reviewed and accepted or rejected by a user with the 'Analytics version acceptor' permission.	Risk Analyst, Risk Manager Administrator
Rules	Create and manage AMDL Business Rules.	Risk Analyst, Risk Manager, Administrator
Rule templates manager	Manage rule templates and rule actions.	Risk Analyst, Risk Manager, Administrator
Rule templates	Access rule templates.	Risk Analyst, Risk Manager, Administrator
Sandbox replay	Create Sandbox Replays to test new analytics configurations against historical data. **Note:** This add-on feature must be purchased separately.	Risk Analyst, Risk Manager, Administrator

1.7 Settings

The table below describes which permissions on the Fraud Transaction Monitoring Portal **Settings** page are assigned, by default, to each user role.

Permission	Description	User Roles
Data lists Create and manage data lists.	This permission also enables to user to directly add or delete values in data lists, and to import data into data lists from a CSV file.	Risk Analyst, Risk Manager, Administrator
Incident filters	Create and edit incident list filters based on triggered rules, tags, or the team the incident is referred to.	Risk Analyst, Risk Manager, Administrator
Teams	Create and edit teams of users.	Risk Analyst, Risk Manager, Administrator
Users	Manage user accounts and assign roles to users.	Administrator

1.8 System

The table below describes which permissions on the Fraud Transaction Monitoring Portal **System** page are assigned, by default, to each user role.

Permission	Description	User Roles
Audit log	Access the audit log of user interactions with the Fraud Transaction Monitoring Portal.	Risk Manager, Administrator

1.9 Other

The table below describes additional permissions on the Fraud Transaction Monitoring Portal that are assigned, by default, to each user role.

Permission	Description	User Roles
De-tokenize	View the original plain text values of tokenized data.	Risk Investigator, Risk Analyst, Risk Manager, Administrator
Documentation	Access the documentation sidebar.	Risk Investigator, Risk Analyst, Risk Manager, Administrator
Tokenized search	Search tokenized fields using the original non-tokenized value.	Risk Investigator, Risk Analyst, Risk Manager, Administrator
Message broadcast	Send messages to other users.	Risk Investigator, Risk Analyst, Risk Manager, Administrator
View unmasked data	View unmasked data (that would otherwise be masked) in the Fraud Transaction Monitoring Portal.	Risk Investigator, Risk Analyst, Risk Manager, Administrator

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	24/04/2024	Updates to content and graphics to align with taxonomy updates on our Documentation Portal. First version.	WS

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.