Thredd Protect Guide

Version: 2.3
07 June 2023
Publication number: PTG-2.3-6/7/2023

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: +442037409682

Copyright

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

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

About this Document

This guide explains how to use the Thredd Protect portal to help protect your organisation and your cardholders from fraudulent activity. It describes the Thredd Protect user interface and explains how to use the system to monitor transactions, raise cases for investigation, configure rules, collect statistics, and run reports.

Target Audience

This guide is aimed at frequent users of Thredd Protect.

What's Changed?

To find out what's changed since the previous release (the minor upgrade to v5.1.8 in June 2021), 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
Smart Client Guide	How to use Smart Client, which is an administration application that can be used to view and manage cards and transactions in your program.
Cardinal 3D Secure User	Specification and 3D secure configuration rules when using the Cardinal Portal to set up the rules and policies for your program.
Thredd Protect Release Notes	Describes the new features and enhancements to existing features available in the latest Thredd Protect release.

How to Use this Guide

If you are new to Thredd Protect and want to understand how you can use it to guard against fraudulent activity, begin by reading the following topics: Introduction, Overview of Steps in Using Thredd Protect, and Understanding the Thredd Protect Display.

If you are an existing user of Thredd Protect and want to understand what's changed in this release, see the *Thredd Protect Release Notes*.

1 Introduction

This topic introduces Thredd Protect, describes its key features, and explains how you can use it in your card payment programmes to help protect your institution and your cardholders from fraudulent transactions.

Thredd Protect is a bespoke fraud protection programme designed to guard financial institutions and cardholders from fraudulent activity. The system works in near real-time and is based on transactional data checks and calculations to flag suspicious transactions or events.

Simple to setup and manage, Thredd Protect puts you in control of the monitoring, blocking and flagging of live cards, 24 hours a day, 7 days a week. Combined with advice from our team of fraud experts, Thredd helps you to configure and control rules designed to protect your card programme.

1.1 How does Thredd Protect work?

The following diagram illustrates how Thredd Protect works to prevent fraud:

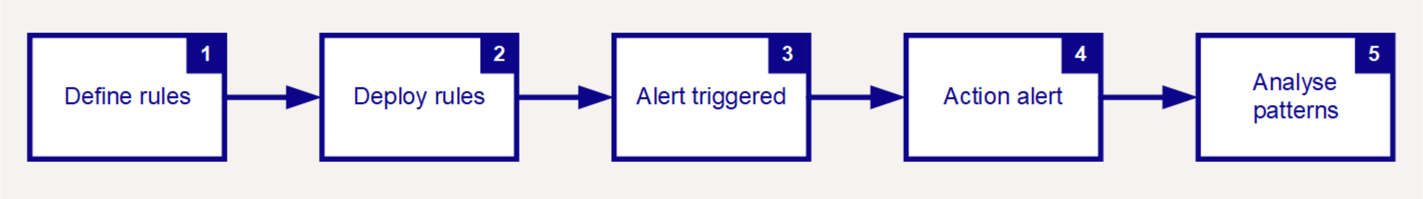


Figure 1: How Thredd Protect prevents fraud

Each step is explained in more detail below:

1. **Define rules**: Thredd works with you to define a bespoke set of rules based on card transactions which can, for example, alert your organisation’s fraud team or block cards, and also define configurations beyond that of default parameters.
2. **Deploy rules**: All authorisation data from the Thredd Apex platform is checked against your organisation’s predefined rules and logic to identify patterns of fraudulent card activity in near real time.
3. **Alert triggered**: Suspicious activity (as per your organisation’s rules) results in an immediate alert with an action, such as block card.
4. **Action alert**: Fraud Analysts/Managers can act manually, or intervention can be automated to block the card.
5. **Analyse patterns**: Thredd Protect helps to analyse fraud patterns over time (for example, the efficiency of rules such as false positives or confirmed fraud prevention) so your organisation can tailor rules as your programme and cardholder behaviour evolves.

2 Overview of Steps in Using Thredd Protect

This topic provides a high-level overview of the steps to help your organisation get up and running with Thredd Protect, with pointers to where to find further information.

Step 1 – Access Thredd Protect

To access Thredd Protect, you use a browser such as Google Chrome or Microsoft Edge. You also require a username and password from Thredd to access the system. For more information, see Accessing Thredd Protect.

Step 2 – Familiarise yourself with the User Interface

Before you begin, learn how to use the Thredd Protect toolbar, menu options and dashboard – see Understanding the Thredd Protect Display.

Thredd Protect provides powerful transaction monitoring functionality, with the ability to flag suspicious events for further investigation. For more information, see Transaction Monitoring .

What you can see and do in Thredd Protect depends on your role and access rights. For more information about user roles and permissions, see User Access Management.

Step 3 – Understand Case Management

Thredd Protect allows you to create cases to track suspicious events and transactions requiring further investigation. For more information about using cases to investigate potential fraud, see Managing Cases for Investigation.

Step 4 – Understand Thredd Protect Rules

Thredd Protect checks all data from the Thredd Apex platform against a set of predefined rules and logic to identify patterns of fraudulent card activity. To view the rules through which transaction verification happens, see Using the Rule Manager.

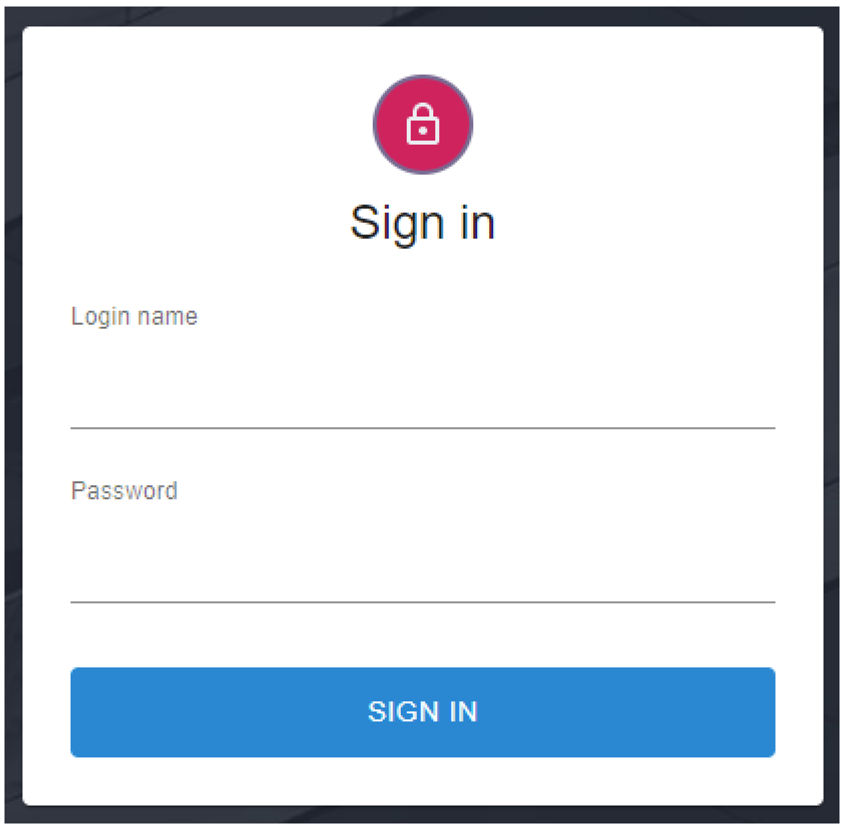
3 Accessing Thredd Protect

This topic explains how to access the Thredd Protect web-based portal.

3.1 Accessing Thredd Protect

Thredd will send you an email containing a link (URL) to Thredd Protect, together with your user login credentials.

Log into Thredd Protect using a web browser. Google Chrome, Microsoft Edge or Safari are recommended.



Sign in

Login name

Password

SIGN IN

Figure 2: Thredd Protect Sign-In Screen

On the **Sign in** page, enter the username and password received from Thredd and click **Sign in**.

Note: Both the username and password are case sensitive. On the first login, you will be asked to change your password.

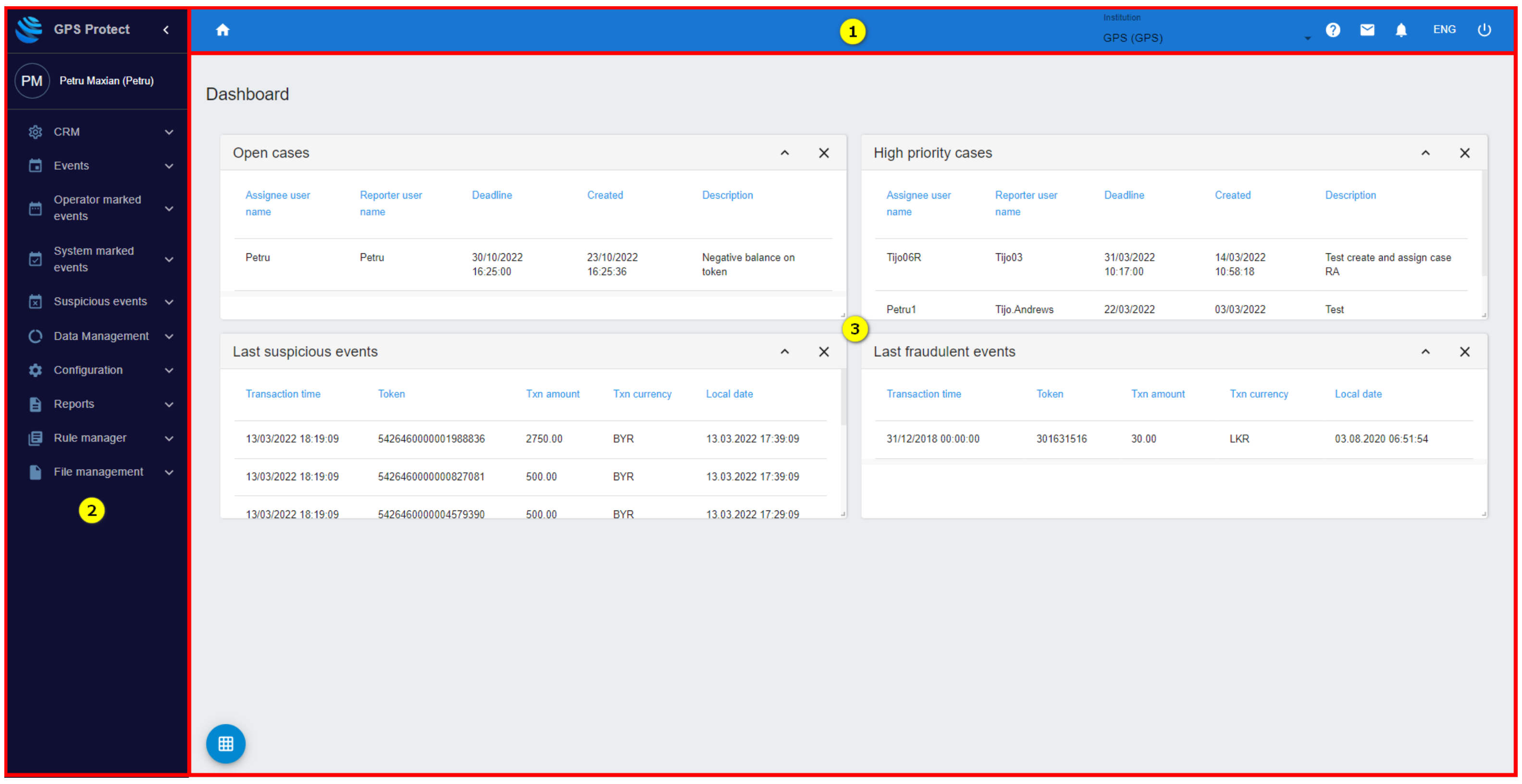
Every Thredd Protect user must have their own credentials; user credential sharing is not permitted. There is no limit on the number of users in your organisation who can access Thredd Protect.

After successful login, the main Thredd Protect screen appears (described in the following section).

4 Understanding the Thredd Protect Display

This topic describes the main Thredd Protect screen and explains how to use the toolbar, menu options and dashboard.

> **Note:** Different levels of user access can be configured on the Thredd Protect portal, depending on role. For example, some users may only be able to view information about transactions while others can view transactions, edit rules and run reports. Therefore, if you cannot see a menu option, this may be because you do not have the appropriate permissions. For more information, see User Access Management.



Open cases

Assignee user name	Reporter user name	Deadline	Created	Description
Petru	Petru	30/10/2022 16:25:00	23/10/2022 16:25:36	Negative balance on token

High priority cases

Assignee user name	Reporter user name	Deadline	Created	Description
Tijo06R	Tijo03	31/03/2022 10:17:00	14/03/2022 10:58:18	Test create and assign case RA
Petru1	Tijo.Andrews	22/03/2022	03/03/2022	Test

Last suspicious events

Transaction time	Token	Txn amount	Txn currency	Local date
13/03/2022 18:19:09	5426460000001988836	2750.00	BYR	13.03.2022 17:39:09
13/03/2022 18:19:09	5426460000000827081	500.00	BYR	13.03.2022 17:39:09
13/03/2022 18:19:09	5426460000004579390	500.00	BYR	13.03.2022 17:29:09

Last fraudulent events

Transaction time	Token	Txn amount	Txn currency	Local date
31/12/2018 00:00:00	301631516	30.00	LKR	03.08.2020 06:51:54

Figure 3: The main Thredd Protect screen

The main interface is divided into three main sections:

Key	Command	Description
1	**Toolbar**	Use the toolbar to navigate quickly to key functions, access help, or sign out. See below for more information.
2	**Menus**	Use the menus to display user profile details, change the appearance of the screen and access key Thredd Protect functions and displays. See below for more information.
3	**Dashboard**	The dashboard displays various widgets (the elements that appear on screen) showing tables, statistical graphs, cases, events etc. You can tailor your dashboard by choosing the widgets you want to display. See below for more information.

4.1 About the Toolbar

The Toolbar contains several icons you can use to access key screens:

Icon	Command	Description
🏠	**Home**	Click **Home** in the top-left of the toolbar to return to the dashboard home screen.
	Institution	Click on the institution name to select the default institution
❓	**Help**	Click **Help** in the top-right of the screen to open the Help interface.

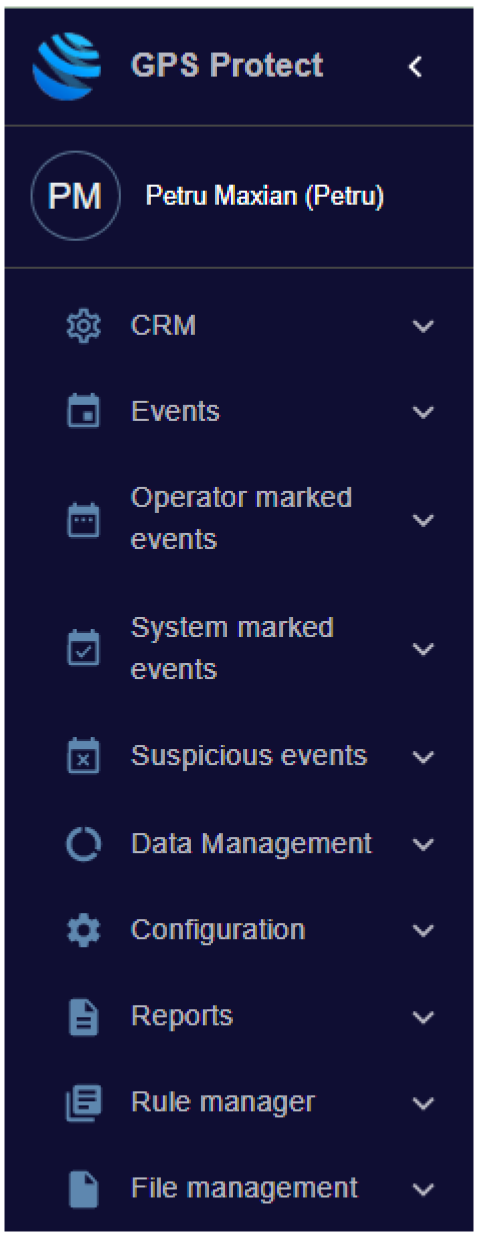
Icon	Command	Description
✉	**Assigned cases**	Click **Assigned cases** to show all the cases currently under investigation.
🔔	**Notifications**	Click **Notifications** to open the **System marked Transactions** screen to see the latest alerts.
ENG	**Language**	Click **Language** to choose from a list of available languages for the interface.
⏻	**Sign Out**	Click **Sign Out** to exit from Thredd Protect.

Tip: Hover your mouse over an icon to view its name.

4.2 About the Menus

The main menu bar on the left-hand-side of the screen enables you to:

- Access your user profile details
- Change the appearance of the display
- Access key Thredd Protect functions and screens



The available menu options are described in more detail below.

4.2.1 About the menu options

On the lower part of the menu bar, you can see all the menu options available to you.

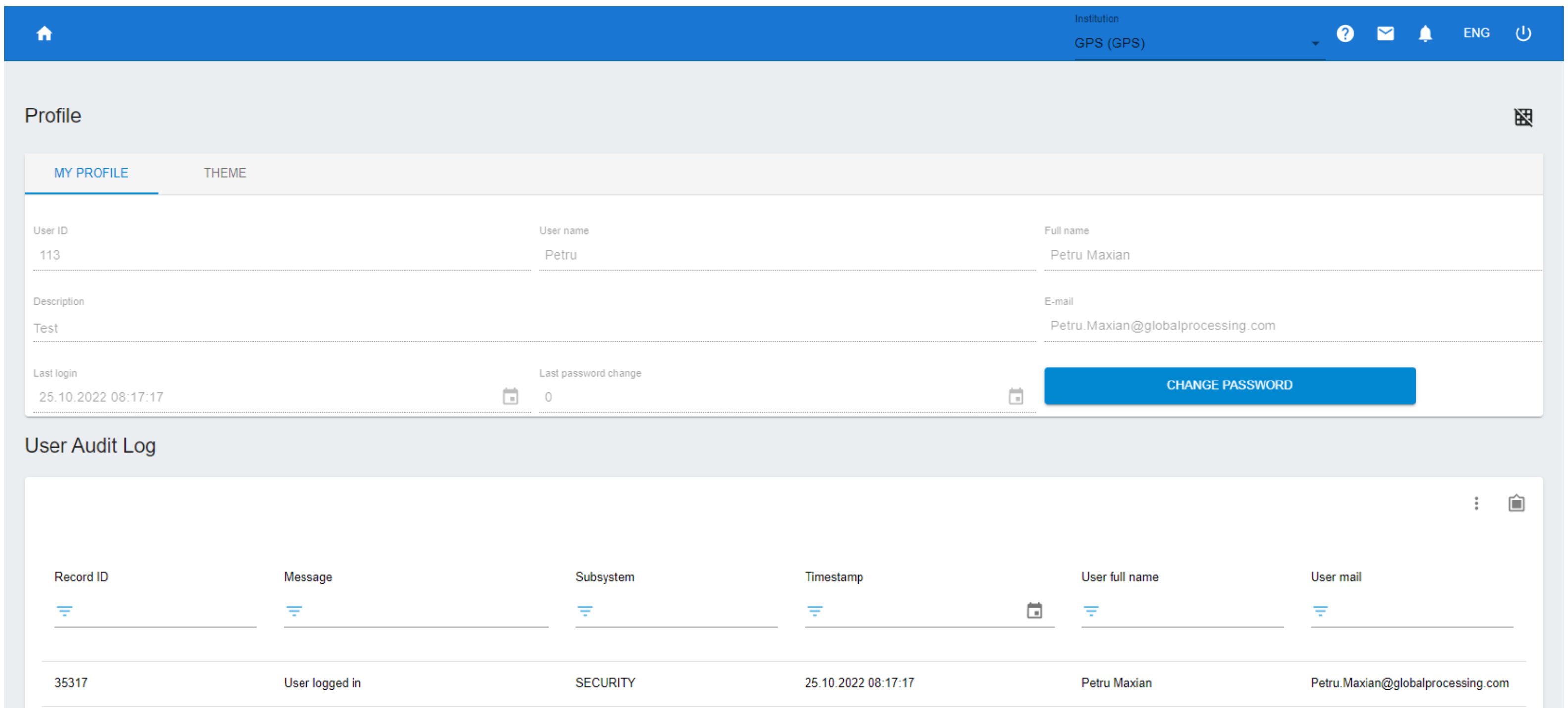
> **Note:** The menu options available to you depend on your role and permissions. If you cannot see a menu option, this may be because you do not have the appropriate permissions. For more information, see User Access Management. If you believe you are missing a menu option or do not have the correct level of access, contact the person responsible for Thredd Protect access within your organisation.

See later in this guide for a detailed description of each of the menu options.

4.2.2 Viewing your User Profile

Your user name and initials are shown in the top of the Menu bar.

To view your user profile details, click on your username. The **Profile** screen appears:



Profile

User ID: 113

User name: Petru

Full name: Petru Maxian

Description: Test

E-mail: Petru.Maxian@globalprocessing.com

Last login: 25.10.2022 08:17:17

Last password change: 0

User Audit Log

Record ID	Message	Subsystem	Timestamp	User full name	User mail
35317	User logged in	SECURITY	25.10.2022 08:17:17	Petru Maxian	Petru.Maxian@globalprocessing.com

Figure 4: The Thredd Protect User Profile screen

This screen has two tabs: **MY PROFILE** (used to view your user details) and **THEME** (used to change the appearance of the screen). These tabs are described below.

MY PROFILE – use this tab to display details related to your profile, such as:

- User ID
- Username
- Full name
- Description (Institution name)
- E-mail (registered email address for the user account)
- Last login (shows the date and time when you last logged into the system)
- Last password change (shows the date and time when you last changed your password)

Also, on the **User Audit Log**, you can see all the logs for any user-related actions such as login times, actions performed while using the system, logout times etc.

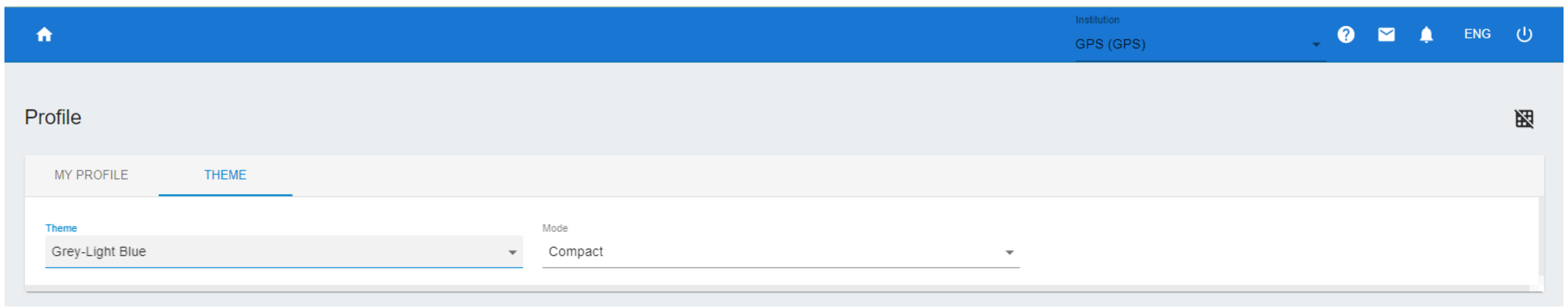
Changing or resetting a password

To change your password, click **Change password**. When prompted, enter your current password, your new password twice, and then click **Save password**.

> **Tip:** If you are not currently logged into your Thredd Protect account and need to reset your password, use the Thredd customer support portal to raise a customer support request, or via email by sending a password reset request to FraudTeam@thredd.com.

4.2.3 Changing the display

Use the **THEME** tab to change the appearance of the screen, as shown below:



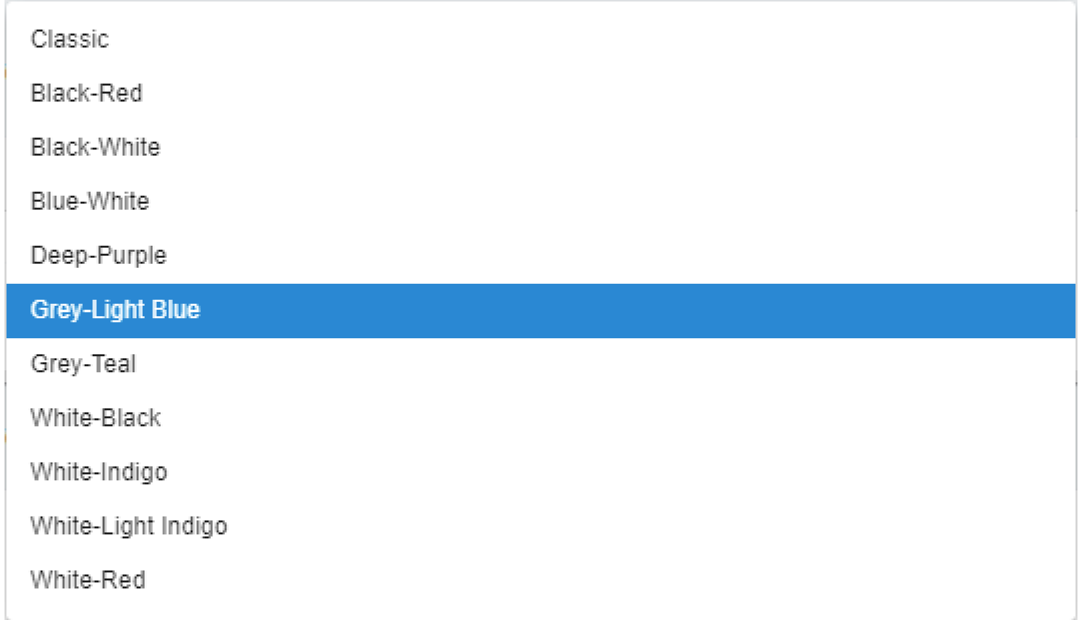
Theme: Grey-Light Blue

Mode: Compact

Figure 5: The Theme tab for changing the appearance of the display

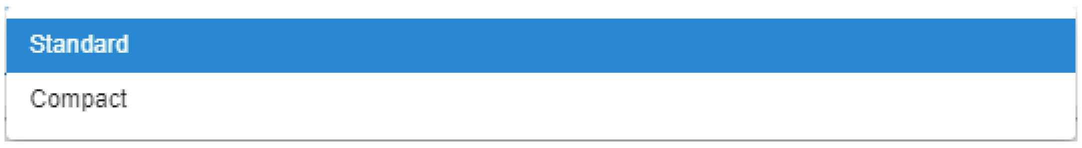
Changing the colour scheme

To change the colour scheme of the display, click on the down arrow ▾ next to **Theme** and choose your preferred option from the dropdown menu:



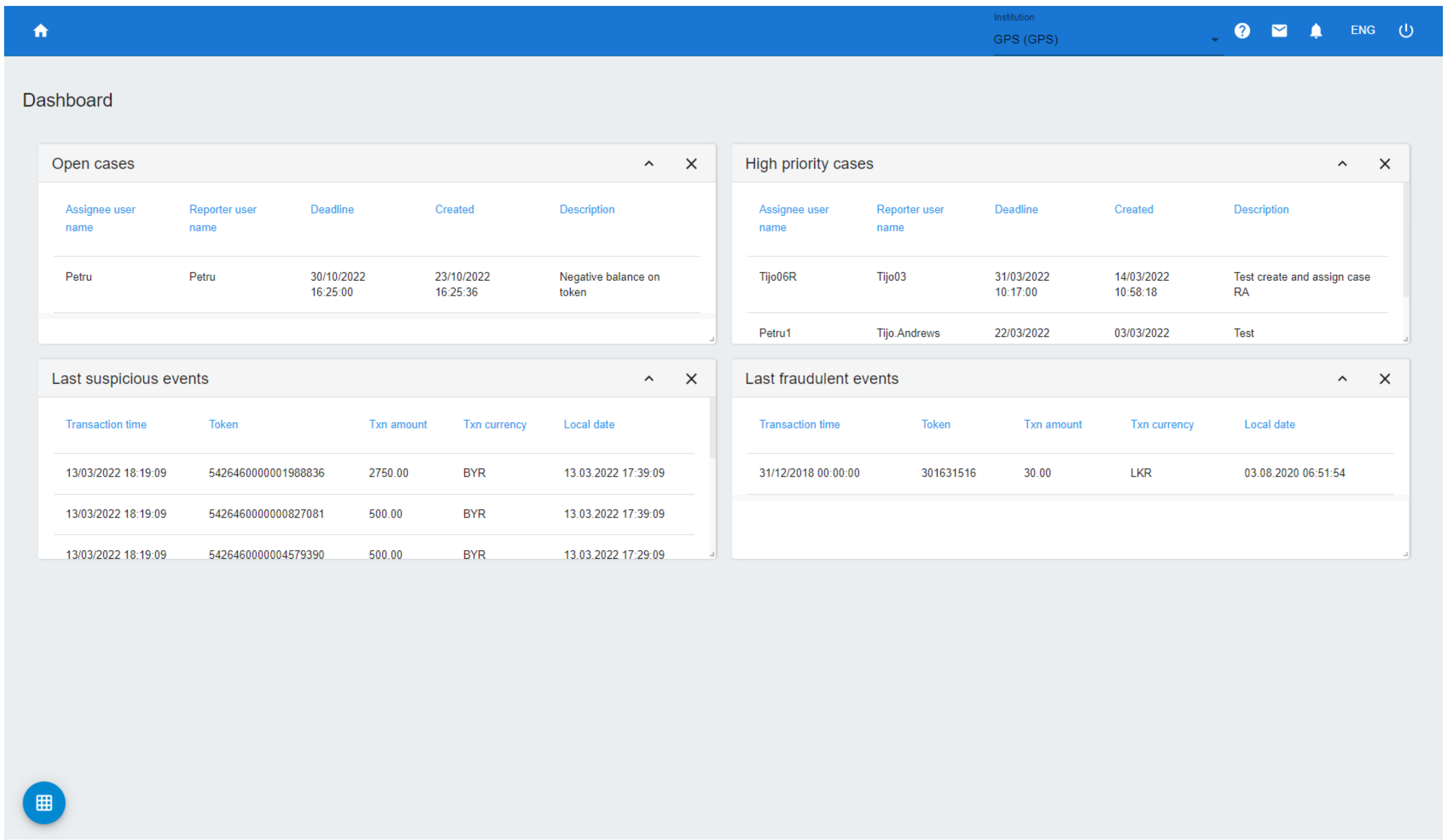
Changing the size and scale

To change the font size/scale/zoom level of the display, click on the down arrow ▾ next to **Mode** and choose the preferred option from the dropdown menu:



4.3 About the Dashboard

The **Dashboard** consists of UI components known as ‘widgets’ which you can choose to display or hide, depending on your requirements. For example, you may want to show the **Open cases** widget to see all open unresolved cases.



Dashboard

Open cases

Assignee user name	Reporter user name	Deadline	Created	Description
Petru	Petru	30/10/2022 16:25:00	23/10/2022 16:25:36	Negative balance on token

High priority cases

Assignee user name	Reporter user name	Deadline	Created	Description
Tijo06R	Tijo03	31/03/2022 10:17:00	14/03/2022 10:58:18	Test create and assign case RA
Petru1	Tijo.Andrews	22/03/2022	03/03/2022	Test

Last suspicious events

Transaction time	Token	Txn amount	Txn currency	Local date
13/03/2022 18:19:09	5426460000001988836	2750.00	BYR	13.03.2022 17:39:09
13/03/2022 18:19:09	5426460000000827081	500.00	BYR	13.03.2022 17:39:09
13/03/2022 18:19:09	5426460000004579390	500.00	BYR	13.03.2022 17:29:09

Last fraudulent events

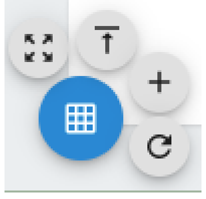
Transaction time	Token	Txn amount	Txn currency	Local date
31/12/2018 00:00:00	301631516	30.00	LKR	03.08.2020 06:51:54

Figure 6: A typical dashboard display

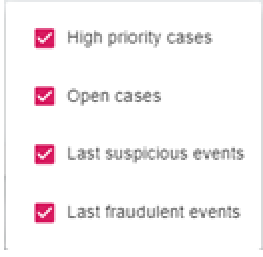
- **Open cases** - shows high-priority investigation cases assigned to a user.
- **High priority cases** - shows all open unresolved cases.
- **Last suspicious events** - shows a list of the last events marked as suspicious.
- **Last fraudulent events** - shows a list of the last events marked as fraudulent.

4.3.1 Managing widgets

You can manage widgets using **Add grid** ▦ in the lower left corner of the **Dashboard** page. When clicked, the following context-sensitive buttons appear:



The following explains the context-sensitive buttons, clockwise:

Icon	Command	Description
⛶	**Edit grid**	Move and resize widgets. Click **Edit grid** to turn it red, indicating widget navigation is on. You can now move widgets to the desired location on the Dashboard and resize them. When done, click the **Edit grid** icon to turn it grey, indicating widget navigation is off and widget cannot be relocated or resized.
⤒	**Expand or collapse all**	Expand or collapse widget. Click the icon to turn it red. In this state, you can collapse all the visible widgets on the Dashboard. Click it again to turn it grey, allowing you to expand all the visible widgets.
+	**Show or hide a grid item**	Display or hide widgets on the Dashboard. Click the icon to show all the widget options that can be displayed. Select the ones you want to display; uncheck the ones you want to hide. For example:  ☑ High priority cases ☑ Open cases ☑ Last suspicious events ☑ Last fraudulent events
↻	**Reset**	Restore all the widgets to their original/default position and size on the Dashboard.

5 Transaction Monitoring

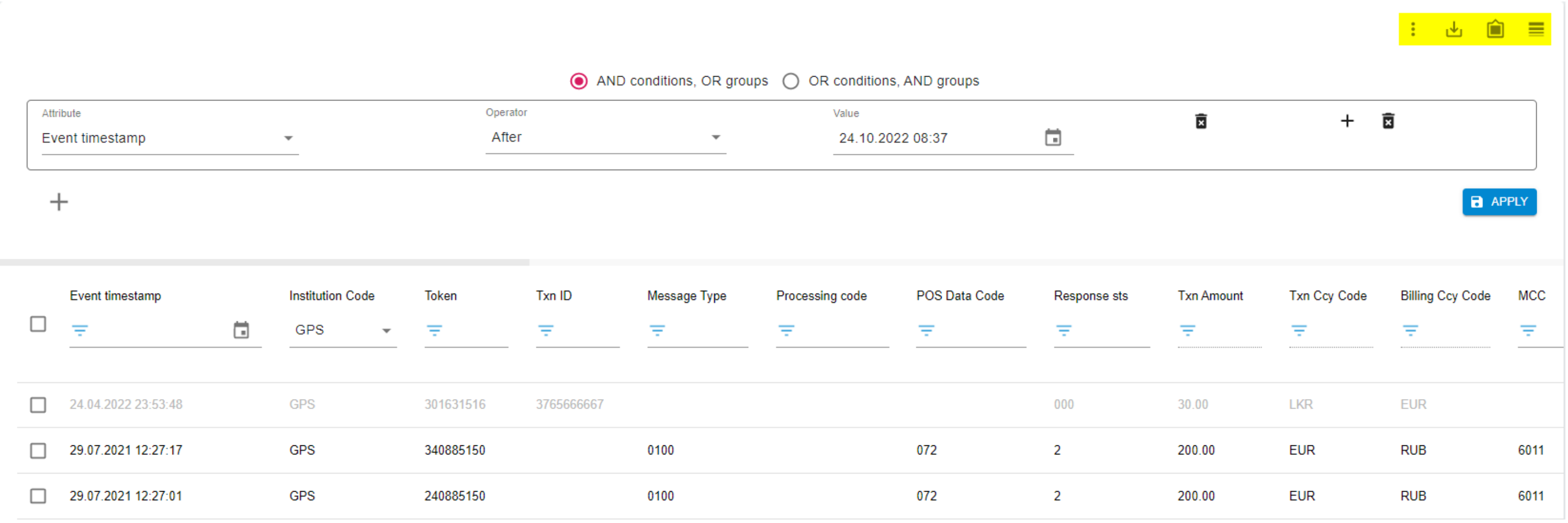
This section introduces the transaction monitoring screens and explains how to use common functions to customise your display, export information, create custom filters, and display the filters applied to the screen.

5.1 Using the Transaction Functions

All transaction monitoring screens have common functions at the top of the display and page navigation functions at the bottom of the display.

5.1.1 Common Functions

The following common functions are in the top right of the display:



● AND conditions, OR groups ○ OR conditions, AND groups

Attribute: Event timestamp

Operator: After

Value: 24.10.2022 08:37

APPLY

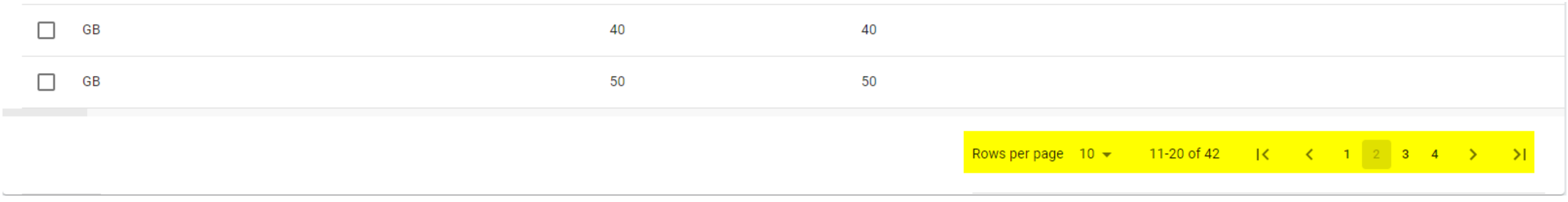
□	Event timestamp	Institution Code	Token	Txn ID	Message Type	Processing code	POS Data Code	Response sts	Txn Amount	Txn Ccy Code	Billing Ccy Code	MCC
		GPS										
□	24.04.2022 23:53:48	GPS	301631516	3765666667				000	30.00	LKR	EUR	
□	29.07.2021 12:27:17	GPS	340885150		0100		072	2	200.00	EUR	RUB	6011
□	29.07.2021 12:27:01	GPS	240885150		0100		072	2	200.00	EUR	RUB	6011

Figure 7: Common functions across the transaction screens. See the following table:

Icon	Command	Description
⋮	**Column customization**	Choose which columns/attributes are displayed on-screen. You can tick or untick the necessary columns/attributes and reorder their appearance by dragging and dropping the columns/attributes into the order you prefer.
⤓	**Export**	Enable the export of all displayed on-screen transactions to either a CSV or an XLSX file.
▣	**Custom filter**	Save and load frequently used search/data filtering options. Once a certain combination of frequently used filters is present on-screen, you can save this using a meaningful name. After, you can click the same icon to load the saved combination of frequently used filters.
≡	**Filter builder**	Display the filters applied to the screen. Using this icon, you can add or remove filters. The default filter for the *Event timestamp* attribute is mandatory and cannot be removed.

5.1.2 Page Navigation Functions

All transaction monitoring screens allow you to set the number of rows per page displayed on-screen:



□	GB	40	40
□	GB	50	50

Rows per page 10 ▾ 11-20 of 42 |< < 1 2 3 4 > >|

Figure 8: Page navigation functions across the transaction screens. See the following table:

You can navigate through the pages either by clicking on the displayed page numbers, or using the page navigation buttons:

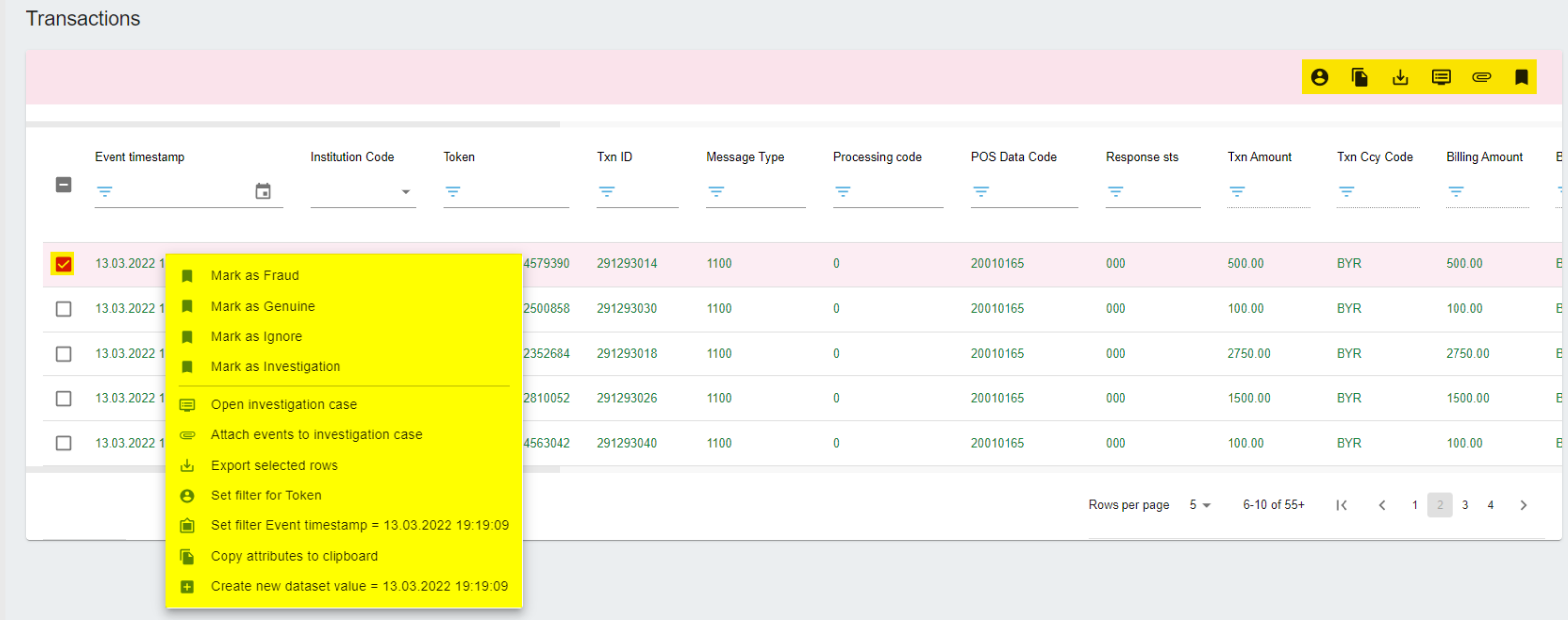
Icon	Command	Description
›	**Next page**	Use to load the next page.
‹	**Previous page**	Use to load the previous page.
>I	**Last page**	Use to load the last (final) page.
I<	**First page**	Use to load the first page.

5.1.3 Sorting data

You can sort information in the columns (for example, under **Token**) by hovering on a column header and using the up and down arrows to sort in ascending or descending order.

5.2 About the Context-sensitive Menu

When one or more transactions are selected (by selecting the inline tick box ☑), a context-sensitive menu with icons appears in the top-right corner of the page. The same options appear in a sub-menu when you right-click on a transaction:



	Event timestamp	Institution Code	Token	Txn ID	Message Type	Processing code	POS Data Code	Response sts	Txn Amount	Txn Ccy Code	Billing Amount	E
☑	13.03.2022 1		4579390	291293014	1100	0	20010165	000	500.00	BYR	500.00	E
□	13.03.2022 1		2500858	291293030	1100	0	20010165	000	100.00	BYR	100.00	E
□	13.03.2022 1		2352684	291293018	1100	0	20010165	000	2750.00	BYR	2750.00	E
□	13.03.2022 1		2810052	291293026	1100	0	20010165	000	1500.00	BYR	1500.00	E
□	13.03.2022 1		4563042	291293040	1100	0	20010165	000	100.00	BYR	100.00	E

Figure 9: Context-sensitive menu functions in the transaction screens. See the following table:

These functions are explained below:

Icon	Command	Description
🔖	**Mark as Fraud**	Assign a *Fraud* status to a transaction.
🔖	**Mark as Genuine**	Assign a *Genuine* status to a transaction.
🔖	**Mark as Ignore**	Assign an *Ignore* status to a transaction.

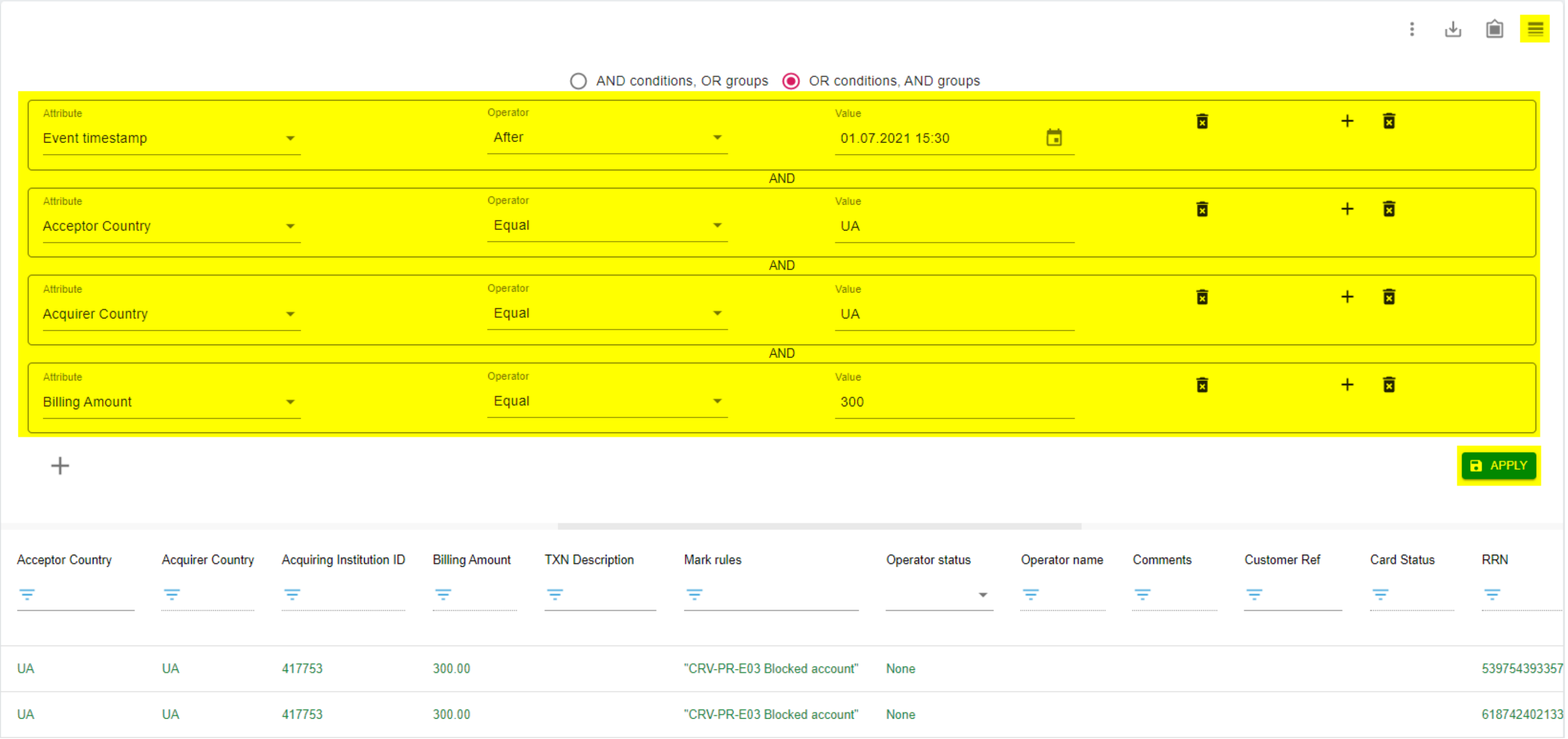
Icon	Command	Description
🔖	**Mark as Investigation**	Assign an *Investigation* status to a transaction.
🖥	**Open investigation case**	Open a case for the selected event.
📎	**Attach events to investigation case**	Attach the selected event to an existing case.
📥	**Export selected rows**	Export the selected event(s) to a CSV/XLSX format report.
👤	**Set filter for Token**	Set a filter for the selected/related Token number.
📋	**Set filter Event timestamp**	Set a filter for the selected/related timestamp.
📄	**Copy attributes to the clipboard**	Copy the selected transaction's attributes/values pairs to the clipboard.
⊞	**Create new dataset value**	Add the selected value to an existing dataset.

5.3 Filtering the Data

To retrieve transactional data for your institution, click on **Filter builder**, select the date from the default filter and click **Apply** to retrieve the filtered data.

In the following examples, transactions are filtered using:

- Event timestamp after 01.07.2021
- Merchants for which the Acceptor Country is Ukraine 'UA'
- Acquirer country is Ukraine 'UA'
- Billing amount (in the base currency of the card) is 300



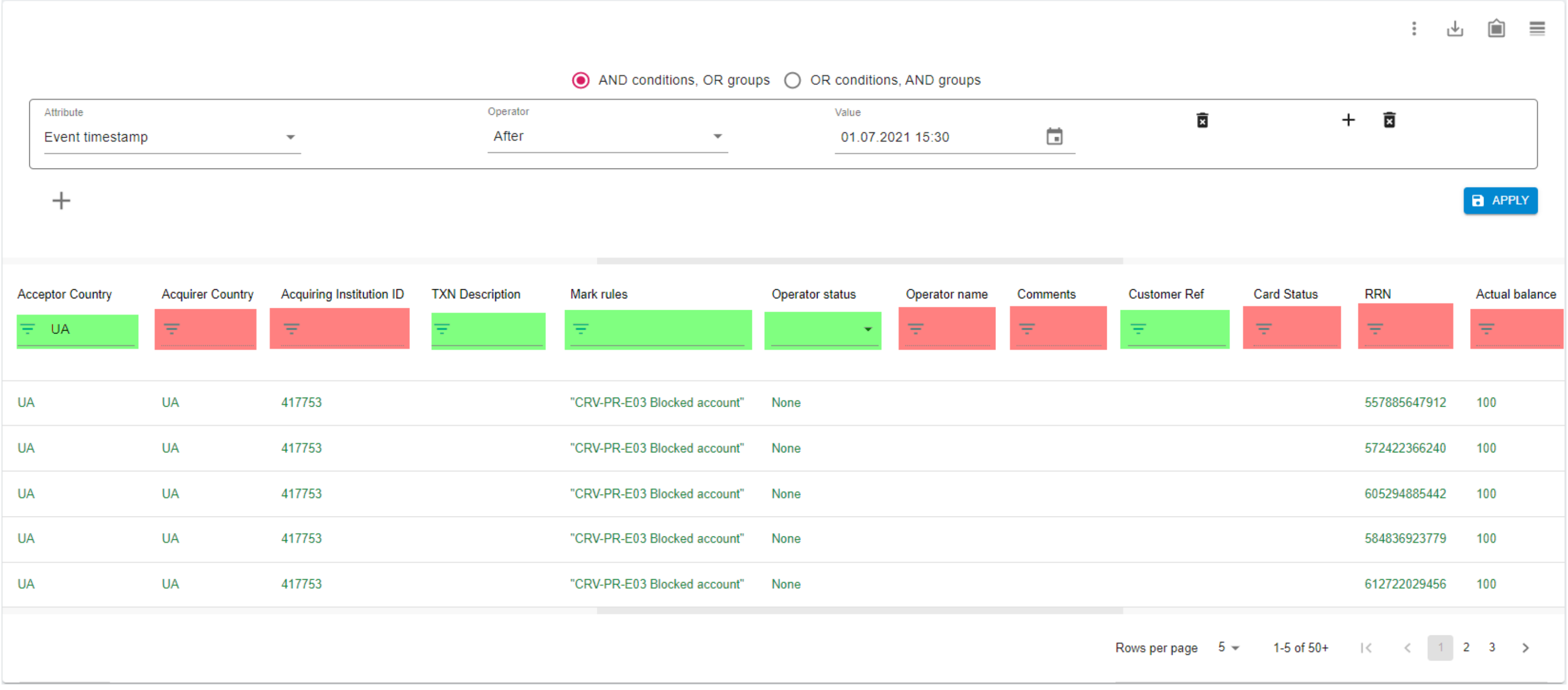
○ AND conditions, OR groups ● OR conditions, AND groups

Attribute	Operator	Value
Event timestamp	After	01.07.2021 15:30
Acceptor Country	Equal	UA
Acquirer Country	Equal	UA
Billing Amount	Equal	300

Acceptor Country	Acquirer Country	Acquiring Institution ID	Billing Amount	TXN Description	Mark rules	Operator status	Operator name	Comments	Customer Ref	Card Status	RRN
UA	UA	417753	300.00		"CRV-PR-E03 Blocked account"	None					539754393357
UA	UA	417753	300.00		"CRV-PR-E03 Blocked account"	None					618742402133

Figure 10: Filtering data in the transaction screens

Further 'on-the-fly' data filtering is possible for some columns/attributes, by inputting a filtering value to the right of the **Filter list** icon (for columns/attributes that display a continuous straight line under the column/attribute header. Note that 'on-the-fly' filtering for columns/attributes that display a dotted line is not available):



● AND conditions, OR groups ○ OR conditions, AND groups

Attribute	Operator	Value
Event timestamp	After	01.07.2021 15:30

Acceptor Country	Acquirer Country	Acquiring Institution ID	TXN Description	Mark rules	Operator status	Operator name	Comments	Customer Ref	Card Status	RRN	Actual balance
🟩 UA	🟥	🟥	🟩	🟩	🟩	🟥	🟥	🟩	🟥	🟥	🟥
UA	UA	417753		"CRV-PR-E03 Blocked account"	None					557885647912	100
UA	UA	417753		"CRV-PR-E03 Blocked account"	None					572422366240	100
UA	UA	417753		"CRV-PR-E03 Blocked account"	None					605294885442	100
UA	UA	417753		"CRV-PR-E03 Blocked account"	None					584836923779	100
UA	UA	417753		"CRV-PR-E03 Blocked account"	None					612722029456	100

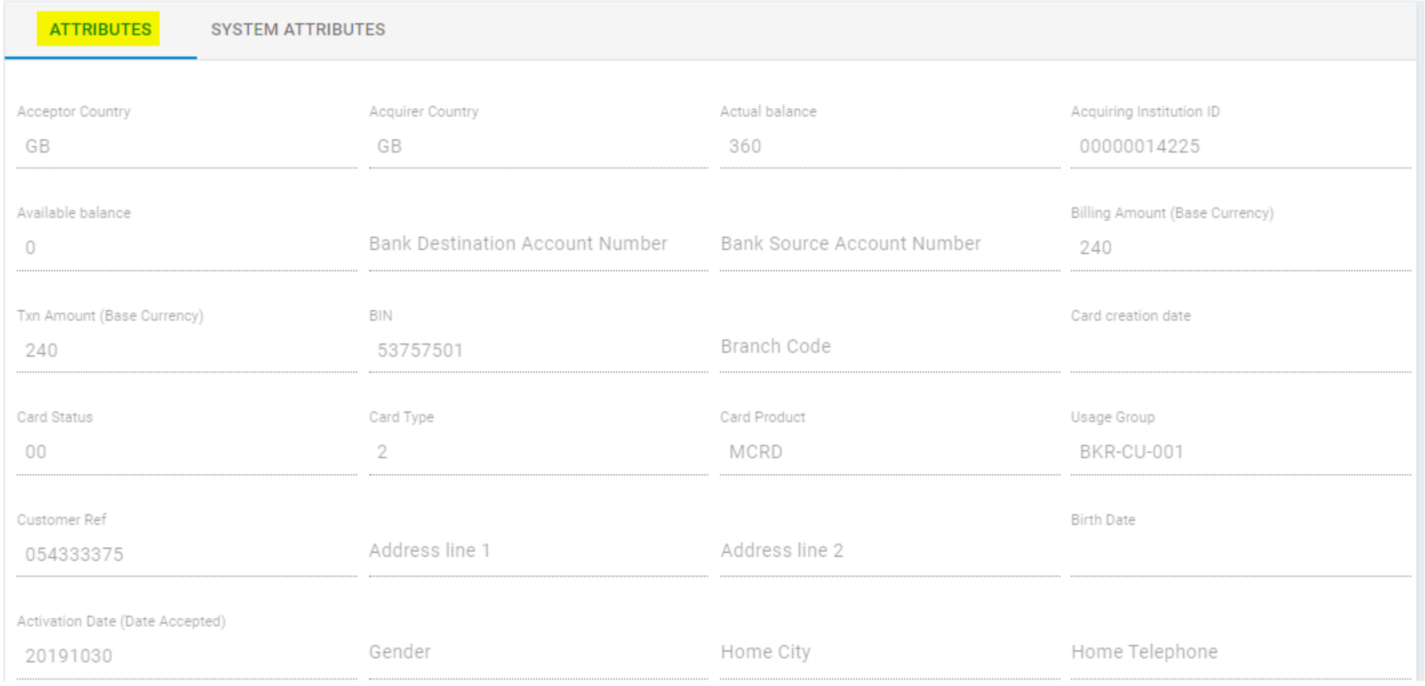
Rows per page 5 1-5 of 50+ 1 2 3

Figure 11: On-the-fly filtering in the transaction screens

5.4 Checking Transaction Details

To check the information available on the system for a particular transaction, click on the transaction to display the details.

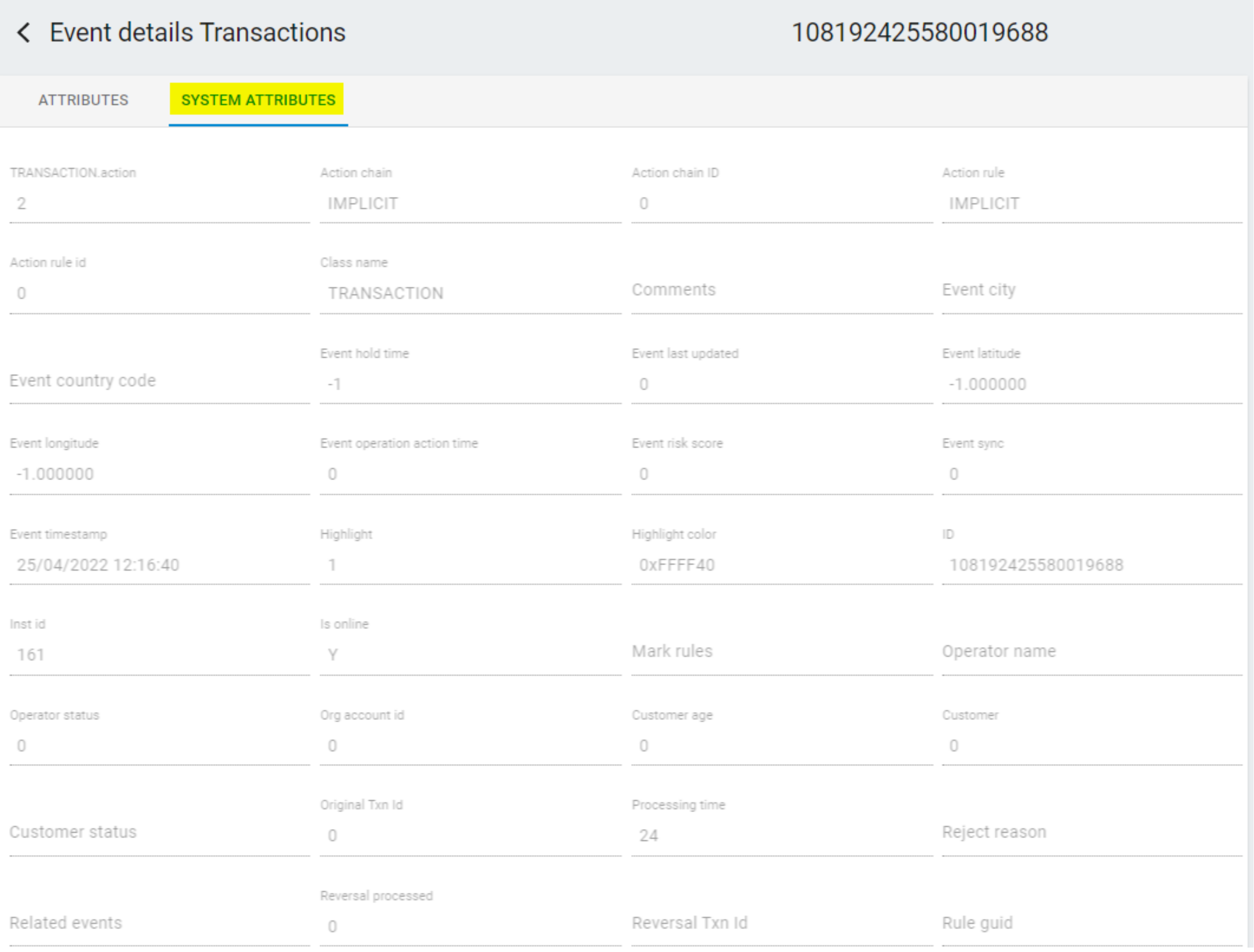
The **ATTRIBUTES** tab shows all the transaction-related details that were sent to Thredd by the Merchant/Acquirer via the Schemes such as Transaction Amount or Acceptor Country, as well as some Thredd proprietary details like the Thredd Product ID of the card on which the transaction was performed.



Acceptor Country GB	Acquirer Country GB	Actual balance 360	Acquiring Institution ID 00000014225
Available balance 0	Bank Destination Account Number	Bank Source Account Number	Billing Amount (Base Currency) 240
Txn Amount (Base Currency) 240	BIN 53757501	Branch Code	Card creation date
Card Status 00	Card Type 2	Card Product MCRD	Usage Group BKR-CU-001
Customer Ref 054333375	Address line 1	Address line 2	Birth Date
Activation Date (Date Accepted) 20191030	Gender	Home City	Home Telephone

Figure 12: Transaction details

The **SYSTEM ATTRIBUTES** tab shows Thredd Protect proprietary details such as the Action (if any) that was performed by the system on this particular transaction, the Institution ID, the Processing Time the system needed to process the transaction, etc.



Event details Transactions 108192425580019688

ATTRIBUTES | SYSTEM ATTRIBUTES

TRANSACTION.action 2	Action chain IMPLICIT	Action chain ID 0	Action rule IMPLICIT
Action rule id 0	Class name TRANSACTION	Comments	Event city
Event country code	Event hold time -1	Event last updated 0	Event latitude -1.000000
Event longitude -1.000000	Event operation action time 0	Event risk score 0	Event sync 0
Event timestamp 25/04/2022 12:16:40	Highlight 1	Highlight color 0xFFFF40	ID 108192425580019688
Inst id 161	Is online Y	Mark rules	Operator name
Operator status 0	Org account id 0	Customer age 0	Customer 0
Customer status	Original Txn Id 0	Processing time 24	Reject reason
Related events	Reversal processed 0	Reversal Txn Id	Rule guid

Figure 13: System Attributes details

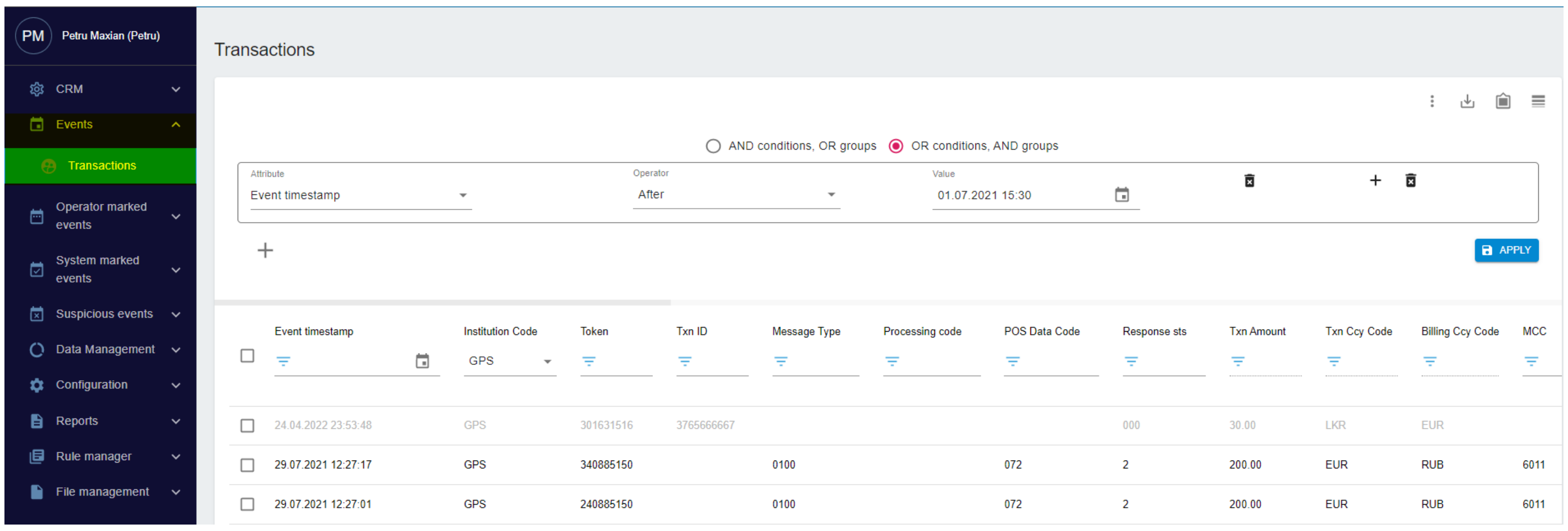
5.5 Understanding the Monitoring Screens

This topic describes the information shown in the Monitoring Transactions screens and explains how to drill down deeper into the transaction details.

Tip: You can sort information in the columns (for example, under **Token**) by hovering on a column header and using the up and down arrows to sort in ascending or descending order.

5.5.1 Viewing all events/transactions

The **Events** > **Transactions** screen displays in near real-time all the transactions performed on your institution's tokens (this includes all events/transactions, not just the ones marked automatically by the rules, or manually by users).



Transactions

○ AND conditions, OR groups ● OR conditions, AND groups

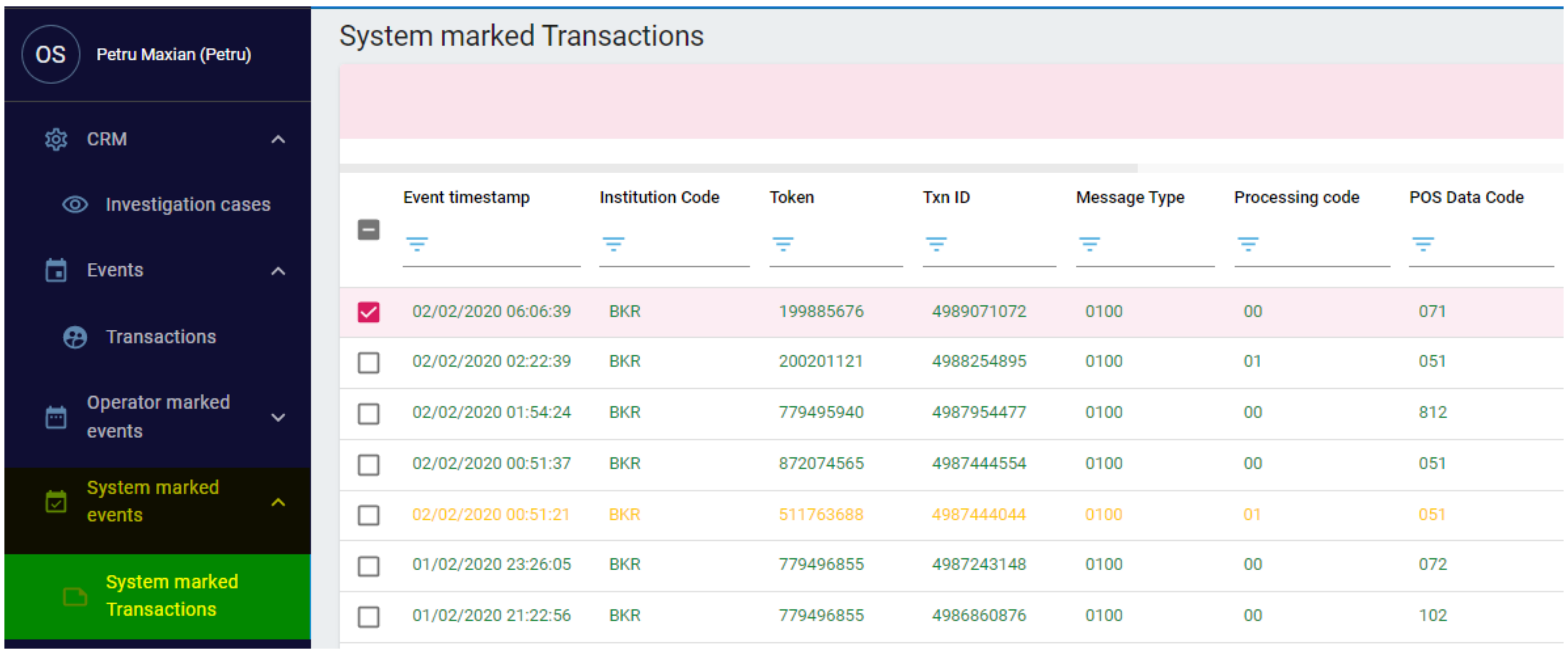
Attribute: Event timestamp
Operator: After
Value: 01.07.2021 15:30

	Event timestamp	Institution Code	Token	Txn ID	Message Type	Processing code	POS Data Code	Response sts	Txn Amount	Txn Ccy Code	Billing Ccy Code	MCC
□		GPS										
□	24.04.2022 23:53:48	GPS	301631516	3765666667				000	30.00	LKR	EUR	
□	29.07.2021 12:27:17	GPS	340885150		0100		072	2	200.00	EUR	RUB	6011
□	29.07.2021 12:27:01	GPS	240885150		0100		072	2	200.00	EUR	RUB	6011

Figure 14: Transactions screen

5.5.2 Viewing system marked events/transactions

The **System marked events** > **System marked Transactions** screen displays all the transactions marked automatically by the system. For example, if an active rule is triggered that has **Action: *Highlight*** enabled, the highlighted event/transaction appears on this screen because the system has marked the transaction automatically.



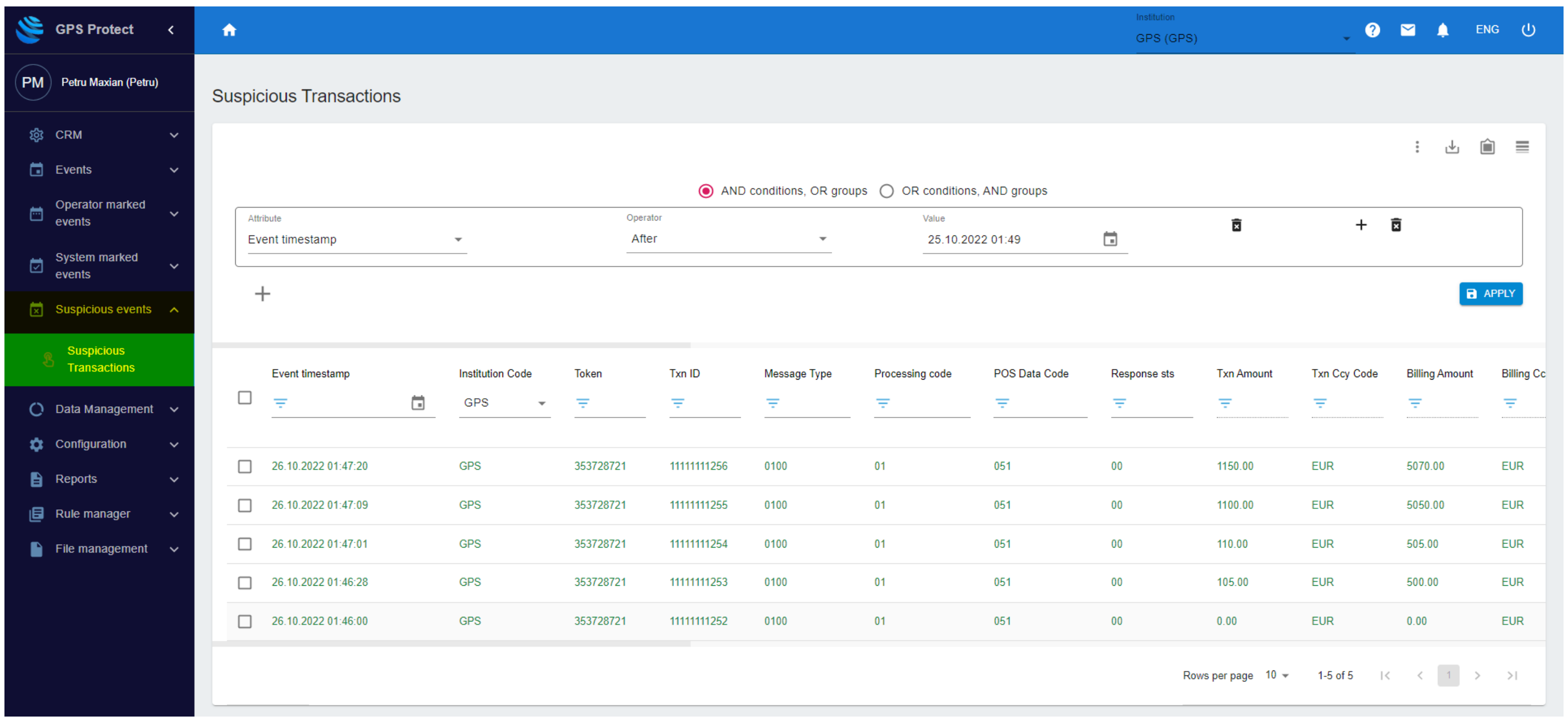
System marked Transactions

	Event timestamp	Institution Code	Token	Txn ID	Message Type	Processing code	POS Data Code
☑	02/02/2020 06:06:39	BKR	199885676	4989071072	0100	00	071
□	02/02/2020 02:22:39	BKR	200201121	4988254895	0100	01	051
□	02/02/2020 01:54:24	BKR	779495940	4987954477	0100	00	812
□	02/02/2020 00:51:37	BKR	872074565	4987444554	0100	00	051
□	02/02/2020 00:51:21	BKR	511763688	4987444044	0100	01	051
□	01/02/2020 23:26:05	BKR	779496855	4987243148	0100	00	072
□	01/02/2020 21:22:56	BKR	779496855	4986860876	0100	00	102

Figure 15: System marked events/System marked Transactions screen

5.5.3 Viewing suspicious events/transactions

The **Suspicious events** > **Suspicious Transactions** screen displays all the transactions that triggered an existing active rule that has ***Action: Marked as suspicious*** enabled.



Suspicious Transactions

● AND conditions, OR groups ○ OR conditions, AND groups

Attribute: Event timestamp
Operator: After
Value: 25.10.2022 01:49

□	Event timestamp	Institution Code	Token	Txn ID	Message Type	Processing code	POS Data Code	Response sts	Txn Amount	Txn Ccy Code	Billing Amount	Billing Cc
		GPS										
□	26.10.2022 01:47:20	GPS	353728721	11111111256	0100	01	051	00	1150.00	EUR	5070.00	EUR
□	26.10.2022 01:47:09	GPS	353728721	11111111255	0100	01	051	00	1100.00	EUR	5050.00	EUR
□	26.10.2022 01:47:01	GPS	353728721	11111111254	0100	01	051	00	110.00	EUR	505.00	EUR
□	26.10.2022 01:46:28	GPS	353728721	11111111253	0100	01	051	00	105.00	EUR	500.00	EUR
□	26.10.2022 01:46:00	GPS	353728721	11111111252	0100	01	051	00	0.00	EUR	0.00	EUR

Rows per page 10 1-5 of 5 1

Figure 16: Suspicious events/Suspicious Transactions screen

Because this screen displays all the alerts automatically triggered by the system, Thredd Protect users responsible for investigating these alerts will likely spend most of their time using this screen.

Once the investigation of a particular alert is complete, you can mark the alert with a predefined status, as described below.

5.5.4 Viewing operator-marked events/transactions

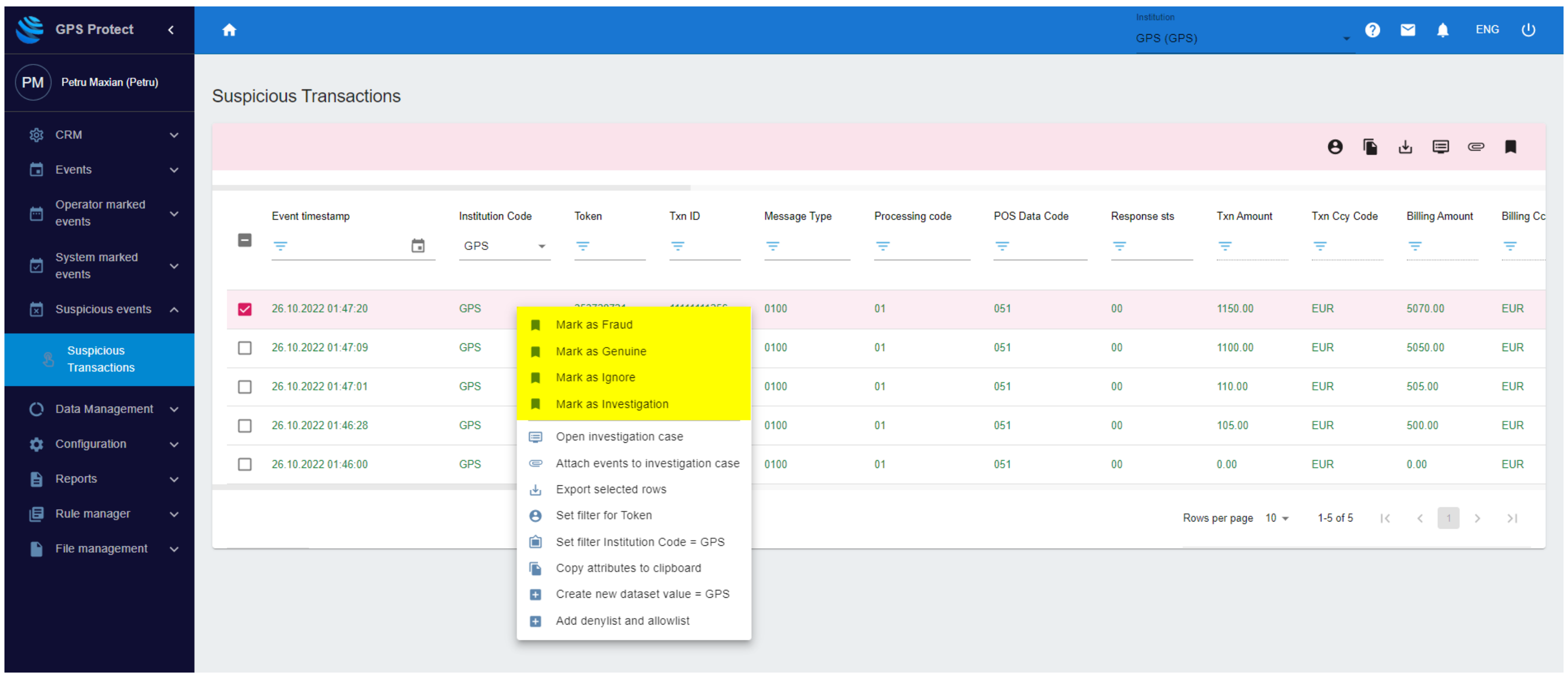
The **Operator marked events/Transactions** screen displays all the transactions that are manually marked and commented on by a user.

Assigning a status to an alert

You can mark a transaction with one of the following statuses:

- **Genuine**
- ***Investigation***
- ***Fraud***
- *Ignore*

To mark a transaction, right-click on the transaction and assign the appropriate status:



Suspicious Transactions

	Event timestamp	Institution Code	Token	Txn ID	Message Type	Processing code	POS Data Code	Response sts	Txn Amount	Txn Ccy Code	Billing Amount	Billing Cc
☑	26.10.2022 01:47:20	GPS			0100	01	051	00	1150.00	EUR	5070.00	EUR
□	26.10.2022 01:47:09	GPS			0100	01	051	00	1100.00	EUR	5050.00	EUR
□	26.10.2022 01:47:01	GPS			0100	01	051	00	110.00	EUR	505.00	EUR
□	26.10.2022 01:46:28	GPS			0100	01	051	00	105.00	EUR	500.00	EUR
□	26.10.2022 01:46:00	GPS			0100	01	051	00	0.00	EUR	0.00	EUR

Rows per page 10 1-5 of 5

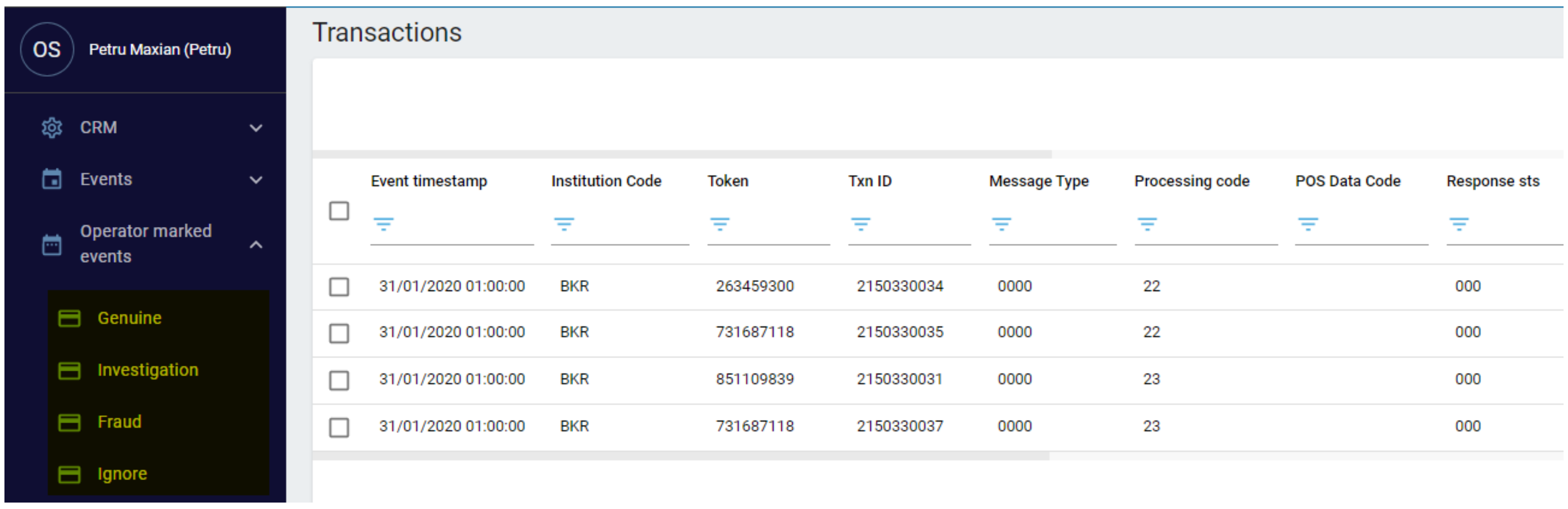
Figure 17: Assigning a status to an alert

By default, new and unmarked transactions are displayed by the system in **Green**. When a transaction is marked, or its default status is changed, the colour of the event/transaction changes, depending on the newly assigned status.

Transaction colour coding

Status	Colour
Default, new and unmarked by users	**Green**
Genuine	Black
Investigation	**Orange**
Fraud	**Red**
Ignore	Grey

When the status changes, the event/transaction is moved from the **Suspicious events** > **Suspicious Transactions** screen, to the appropriate sub-page of the same name as the newly assigned status (under Operator marked events).

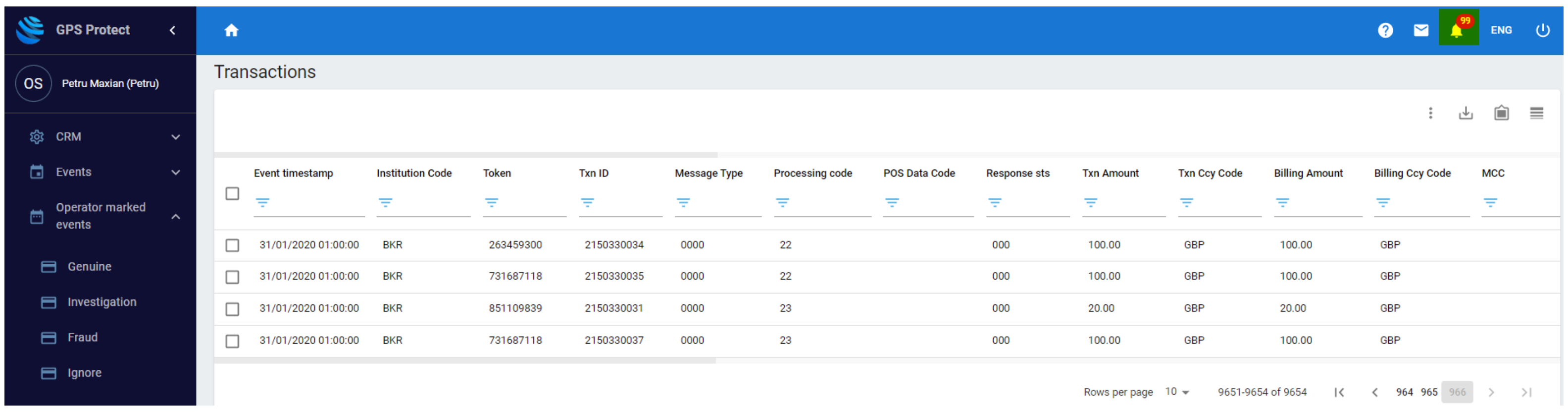


Transactions

□	Event timestamp	Institution Code	Token	Txn ID	Message Type	Processing code	POS Data Code	Response sts
□	31/01/2020 01:00:00	BKR	263459300	2150330034	0000	22		000
□	31/01/2020 01:00:00	BKR	731687118	2150330035	0000	22		000
□	31/01/2020 01:00:00	BKR	851109839	2150330031	0000	23		000
□	31/01/2020 01:00:00	BKR	731687118	2150330037	0000	23		000

Figure 18: Transactions assigned a status

When you assign a new status to an event/transaction, the alert counter displayed in the top-right corner of the screen also decreases, respectively. This is useful in showing how many alerts remain to be worked.



Transactions

□	Event timestamp	Institution Code	Token	Txn ID	Message Type	Processing code	POS Data Code	Response sts	Txn Amount	Txn Ccy Code	Billing Amount	Billing Ccy Code	MCC
□	31/01/2020 01:00:00	BKR	263459300	2150330034	0000	22		000	100.00	GBP	100.00	GBP	
□	31/01/2020 01:00:00	BKR	731687118	2150330035	0000	22		000	100.00	GBP	100.00	GBP	
□	31/01/2020 01:00:00	BKR	851109839	2150330031	0000	23		000	20.00	GBP	20.00	GBP	
□	31/01/2020 01:00:00	BKR	731687118	2150330037	0000	23		000	100.00	GBP	100.00	GBP	

Rows per page 10 9651-9654 of 9654 964 965 966

Figure 19: Alert counter

6 Managing Cases for Investigation

This section explains how to open cases that require further investigation, assign these to a user, and set a deadline for completion.

Thredd Protect allows the creation and investigation of suspicious events/transaction cases. The case functionality is useful for keeping track of and managing fraud by enabling you to review previous cases and the information attached to these.

A case can have one of five possible statuses:

- *New*
- *Assigned*
- *Postponed*
- *Closed*
- *Deleted*

You can open a case if:

- You are unsure if a transaction/set of transactions is fraudulent (and the investigation might require additional actions such as contacting the cardholder)
- Assistance is required from colleagues
- You need to escalate
- Further action is required on an account (for example, closing the account or raising chargebacks)

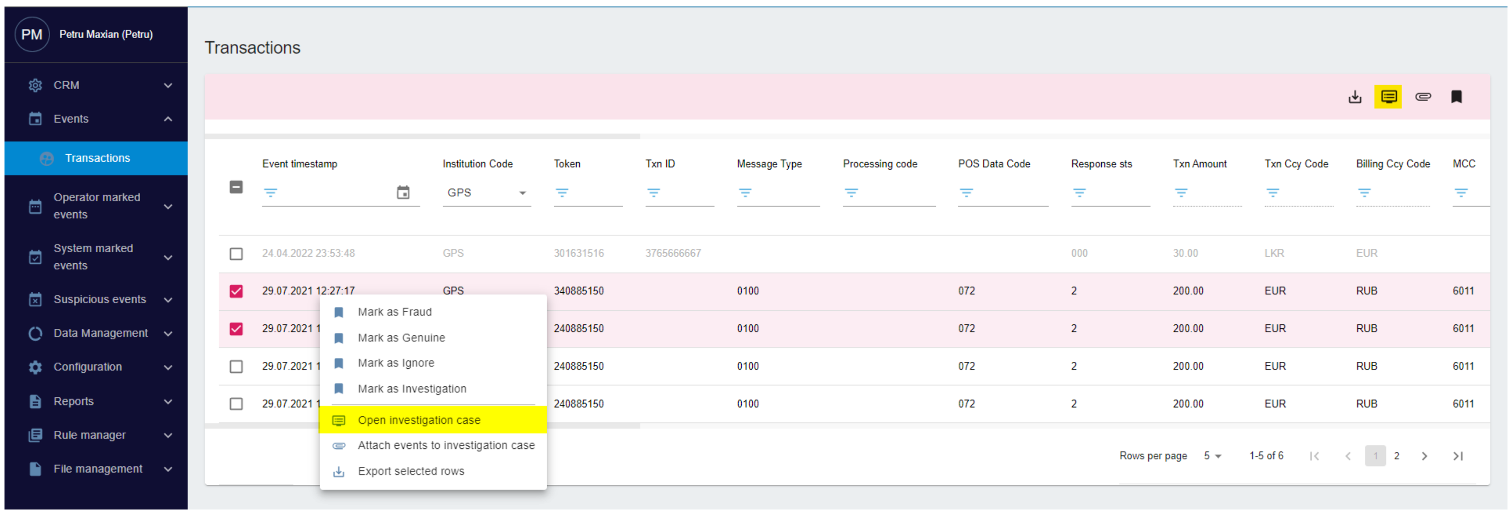
Note: Depending on access rights, some functions are available only to users with the correct permissions (for example, the ability to view all open cases and manage cases). See User Access Management for further information.

6.1 Opening a Case

A case can be opened from within any of the event/transaction screens.

To open a case:

1. Select the appropriate events or transactions you want to include and click on **Open investigation case** in the right-click menu or the context-sensitive button in the top-right corner of the screen. The **Main details** screen appears.



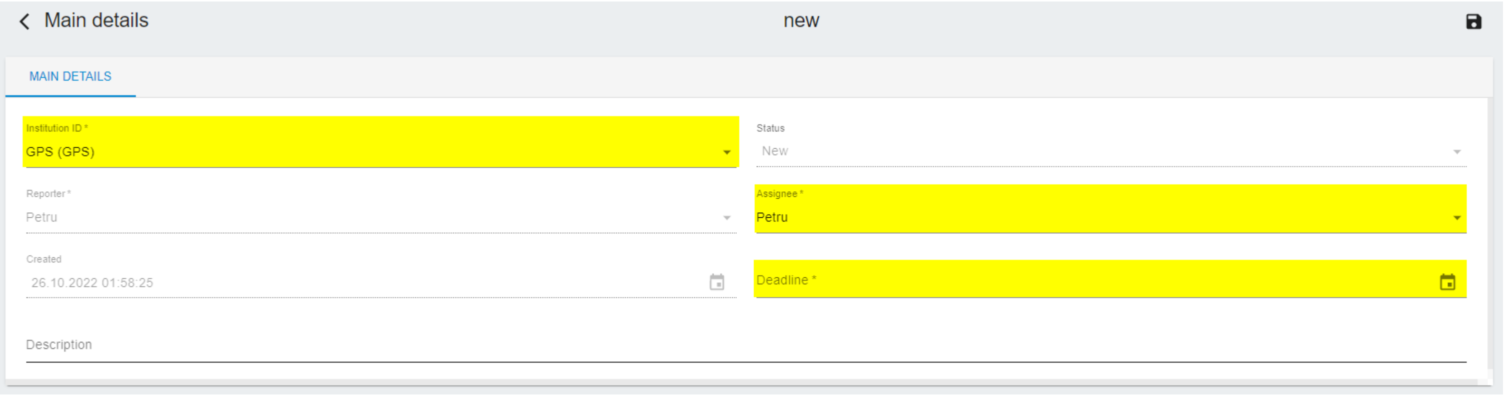
Transactions

☐	Event timestamp	Institution Code	Token	Txn ID	Message Type	Processing code	POS Data Code	Response sts	Txn Amount	Txn Ccy Code	Billing Ccy Code	MCC
		GPS										
☐	24.04.2022 23:53:48	GPS	301631516	3765666667				000	30.00	LKR	EUR	
☑	29.07.2021 12:27:17	GPS	340885150		0100		072	2	200.00	EUR	RUB	6011
☑	29.07.2021 1		240885150		0100		072	2	200.00	EUR	RUB	6011
☐	29.07.2021 1		240885150		0100		072	2	200.00	EUR	RUB	6011
☐	29.07.2021 1		240885150		0100		072	2	200.00	EUR	RUB	6011

Rows per page 5 1-5 of 6 1 2

Figure 20: Opening a case for investigation

2. Complete mandatory fields such as **Institution ID**, **Assignee** and **Deadline**.



Main details

new

MAIN DETAILS

Institution ID *: GPS (GPS)

Status: New

Reporter *: Petru

Assignee *: Petru

Created: 26.10.2022 01:58:25

Deadline *

Description

The following table describes the required fields:

Field name	Description	Field type
Institution ID	The institution the case is opened for	Mandatory
Status	” during the case opening process	Prepopulated
Reporter	The user opening the case	Prepopulated
Assignee	The user the case is assigned to	Mandatory
Created	Prepopulated with the system time when the case is opened	Prepopulated
Deadline	Date when investigation of the case must be completed	Mandatory
Description	Additional comments. **Tip!** Thredd recommends you provide a description of why the case was created	Optional

Once a case deadline is reached, Thredd Protect sends an email notification to the Assignee of the case to remind them that a case remains unresolved.

After completing the opening of the case, all transactions included within the case will have their status set to **Investigation** automatically. If the case status is changed to **Fraud** or **Genuine**, all transactions from the case are automatically marked to match the case status of the parent.

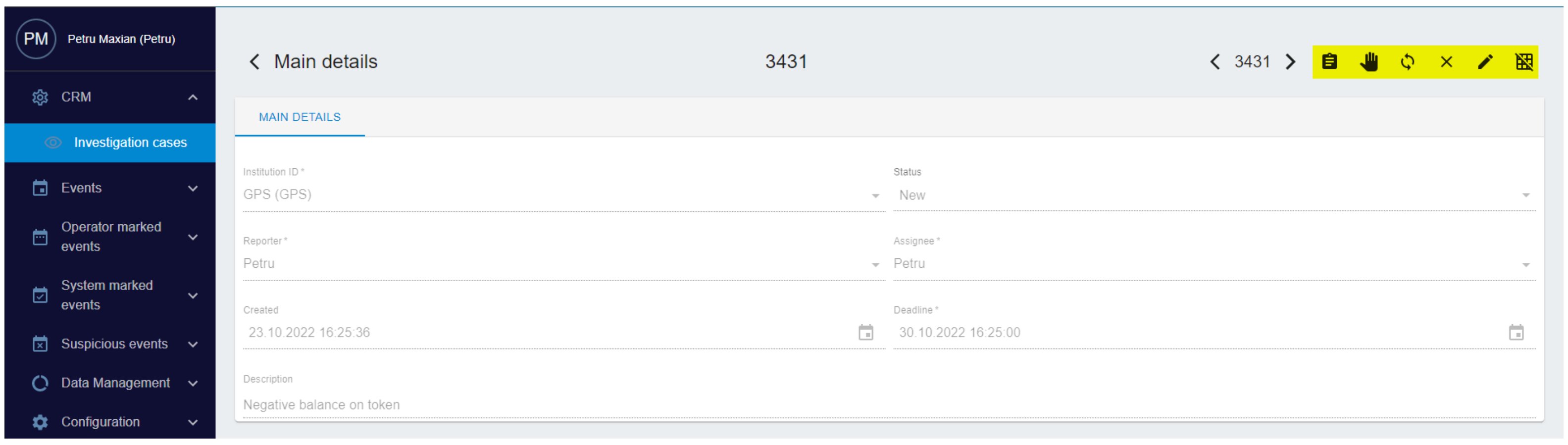
If one or more transactions need to be marked differently from others in a case, you can change their status manually after the case is closed.

6.2 Managing Cases

This section explains how to view and manage the investigation cases you have access to. Using the options available, you can assign a case to a different user, edit the details of a case, or postpone, reopen, close or delete a case. You can also display all the events or transactions related to a case, the audit log, and comments.

To display investigation cases:

1. On the main menu's navigation pane, go to **CRM > Investigation cases**.
2. Select a case record. The **Main details** page appears where you can edit the investigation case using the options displayed in the top-right corner:



Institution ID * GPS (GPS)

Status New

Reporter * Petru

Assignee * Petru

Created 23.10.2022 16:25:36

Deadline * 30.10.2022 16:25:00

Description Negative balance on token

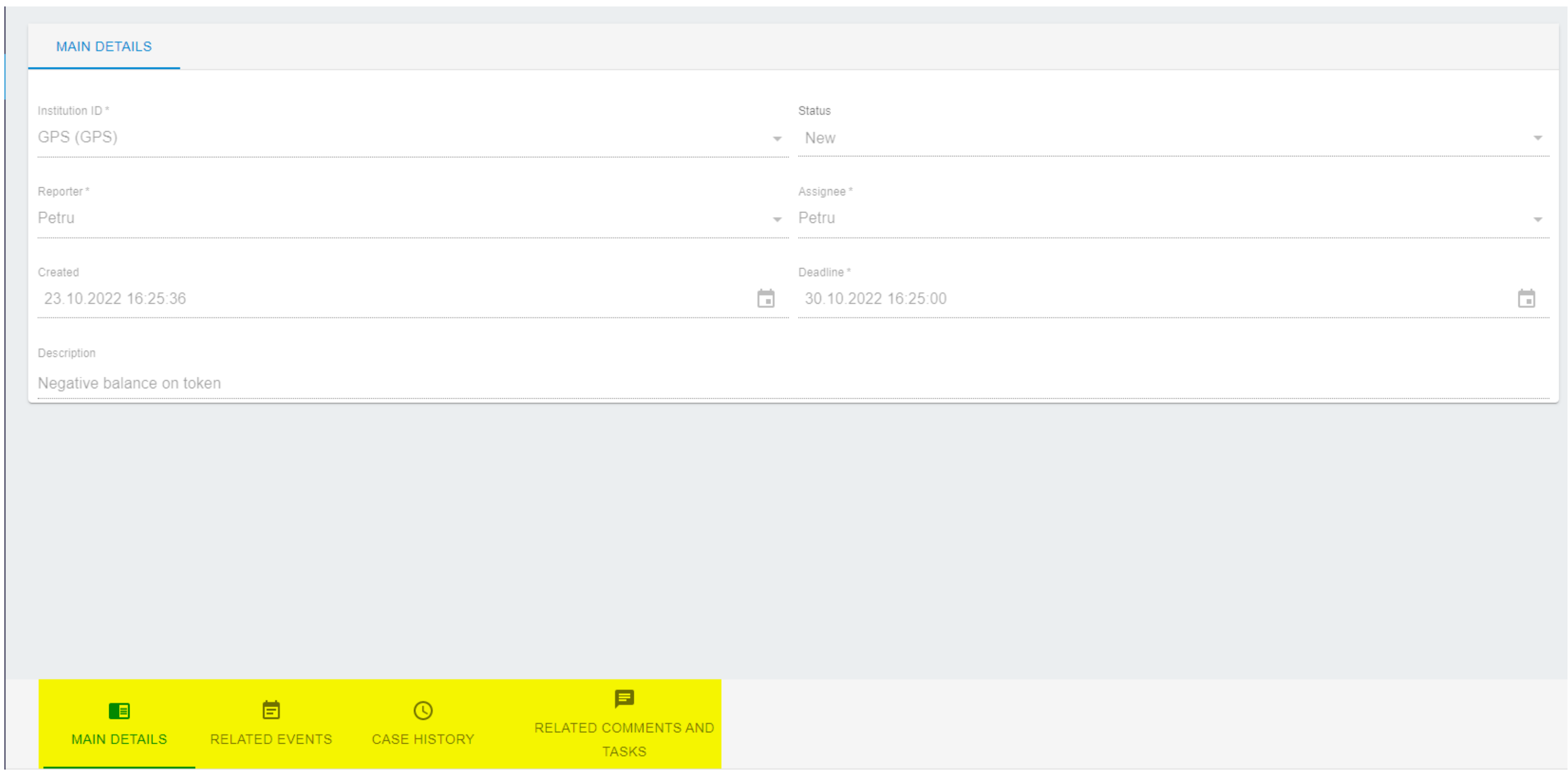
Figure 21: Options available for managing cases. See the following table:

These options are:

Icon	Command	Description
📋	**Assign**	Assign the case to a different user or update the case deadline.
✋	**Postpone**	Postpone investigation of the case.
🔄	**Reopen**	Open a previously closed case.
✕	**Close**	Close a case once a resolution has been reached.
✏	**Edit**	Update case details.
▦	**Edit layout**	Change the layout of case details on-screen.

Tip: Hover your mouse over an icon to view its name.

Use the following additional options at the bottom of the **Main details** page to display events or transactions related to a case, the audit log, and comments:



Institution ID *: GPS (GPS)

Status: New

Reporter *: Petru

Assignee *: Petru

Created: 23.10.2022 16:25:36

Deadline *: 30.10.2022 16:25:00

Description: Negative balance on token

Figure 22: Additional options available for managing cases. See the following table:

Icon	Command	Description
📅	RELATED EVENTS	Display all the events/transactions that are part of the investigation case.
🕒	CASE HISTORY	Display the case history audit log.
💬	RELATED COMMENTS AND TASKS	Display all the comments added during the case investigation process.

7 Using the Rule Manager

This topic describes the use of rules to guard against fraudulent activity.

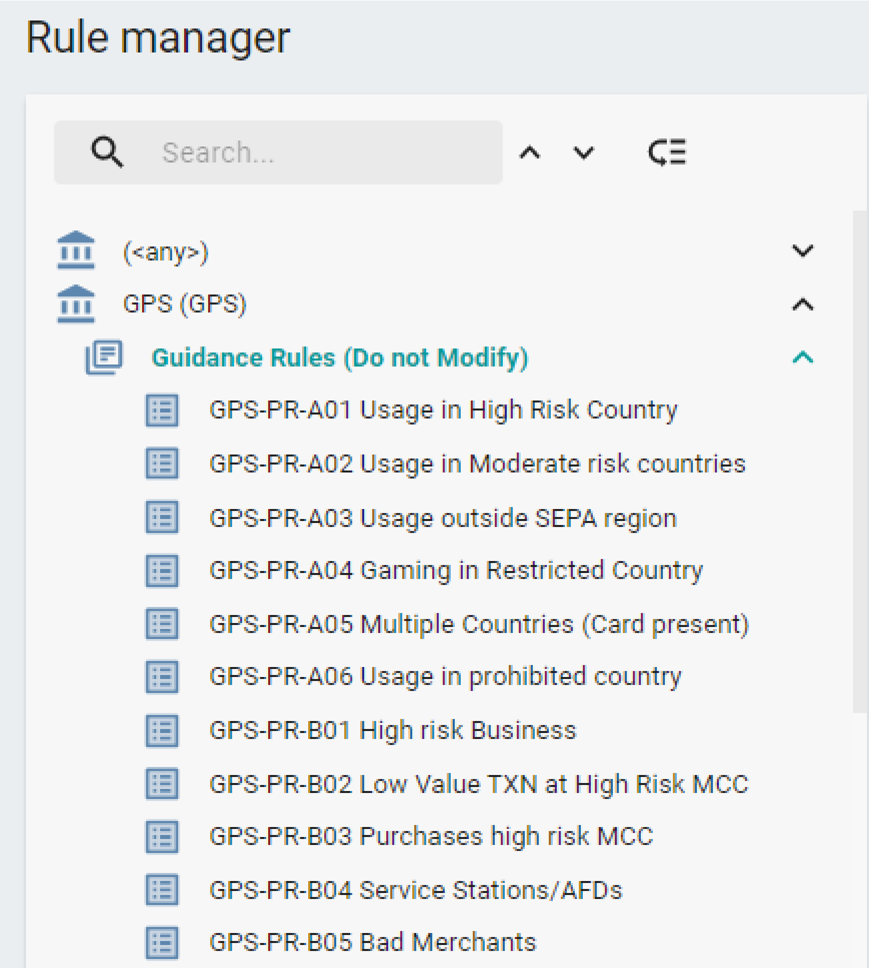
All data from the Thredd Apex platform is checked against a set of predefined rules and logic designed to identify patterns of fraudulent card activity. Any suspicious transactions or events trigger an immediate alert along with an action, such as the blocking of a card.

The rules are the conditions (described as logical expressions) through which transaction verification happens. Rules are tailored to your particular institution.

7.1 Viewing Rules

To see a list of current rules:

1. On the main menu's navigation pane, go to **Rule manager > Rule manager**.



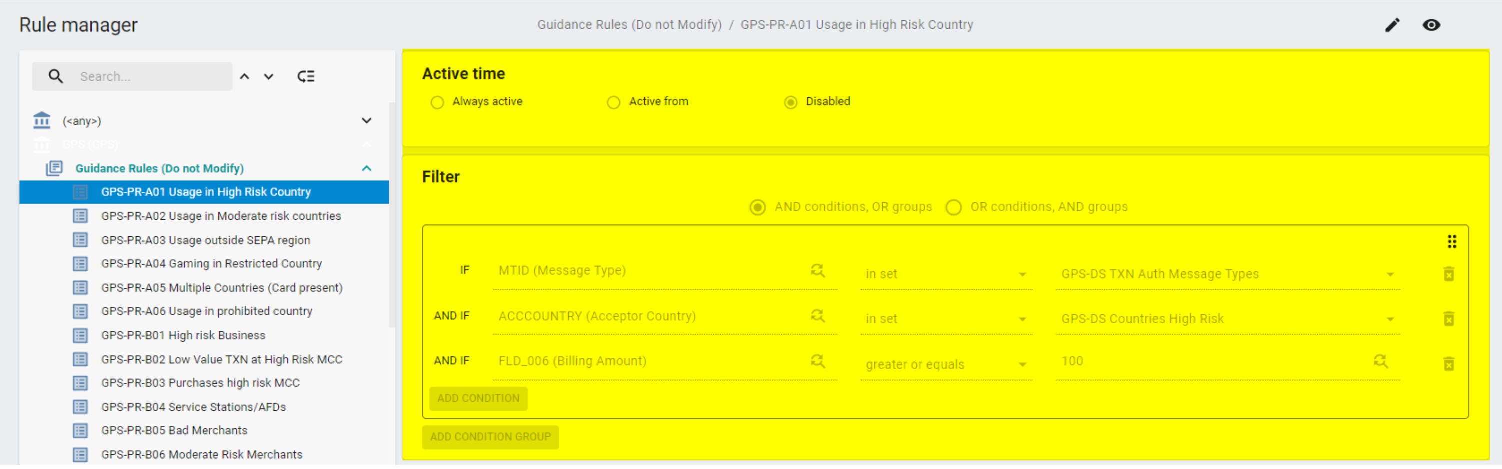
Rule manager

Search...

- (<any>)
- GPS (GPS)
  - Guidance Rules (Do not Modify)
    - GPS-PR-A01 Usage in High Risk Country
    - GPS-PR-A02 Usage in Moderate risk countries
    - GPS-PR-A03 Usage outside SEPA region
    - GPS-PR-A04 Gaming in Restricted Country
    - GPS-PR-A05 Multiple Countries (Card present)
    - GPS-PR-A06 Usage in prohibited country
    - GPS-PR-B01 High risk Business
    - GPS-PR-B02 Low Value TXN at High Risk MCC
    - GPS-PR-B03 Purchases high risk MCC
    - GPS-PR-B04 Service Stations/AFDs
    - GPS-PR-B05 Bad Merchants

Figure 23: Rule Manager

2. Click on a rule to display more information about it in the right-hand pane:



Rule manager

Guidance Rules (Do not Modify) / GPS-PR-A01 Usage in High Risk Country

Search...

- (<any>)
  - Guidance Rules (Do not Modify)
    - GPS-PR-A01 Usage in High Risk Country
    - GPS-PR-A02 Usage in Moderate risk countries
    - GPS-PR-A03 Usage outside SEPA region
    - GPS-PR-A04 Gaming in Restricted Country
    - GPS-PR-A05 Multiple Countries (Card present)
    - GPS-PR-A06 Usage in prohibited country
    - GPS-PR-B01 High risk Business
    - GPS-PR-B02 Low Value TXN at High Risk MCC
    - GPS-PR-B03 Purchases high risk MCC
    - GPS-PR-B04 Service Stations/AFDs
    - GPS-PR-B05 Bad Merchants
    - GPS-PR-B06 Moderate Risk Merchants

Active time

○ Always active ○ Active from ● Disabled

Filter

● AND conditions, OR groups ○ OR conditions, AND groups

IF	MTID (Message Type)	in set	GPS-DS TXN Auth Message Types
AND IF	ACCCOUNTRY (Acceptor Country)	in set	GPS-DS Countries High Risk
AND IF	FLD_006 (Billing Amount)	greater or equals	100

Figure 24: Displaying rule details

7.2 Understanding Rule Conditions and Groups

A rule condition (also called a filter) is a logical expression used by Thredd Protect to determine whether transactions meet the eligibility criteria for triggering an action such as an alert or blocking a card.

You define a rule condition by specifying the left and right part of the expression and a chosen operator in the middle. Typically, the left part of the expression specifies transactional attributes such as Acceptor Country, MCC (Merchant Category Code), etc. The right part usually contains values such as constants or lists of values (known as datasets – see Using Datasets).

The rule condition is evaluated using the chosen operator in the middle of the expression. Depending on what operator is selected, Thredd Protect checks whether the selected attribute on the left of the expression (e.g. Acceptor Country of incoming transactions) "*equals*", "*not equals*", is "*in set*" (is part of a list/a dataset), is "*not in set*" (is not part of a certain list/dataset), etc. as per the right side of the condition.

Example rule condition

To define a condition that filters transactions over 100 in value, specify:

- on the left-hand side, the attribute Billing Amount
- on the right-hand side, the value '100'
- in the middle, the operator "*greater than*"

If Billing amount *greater* than 100

This ensures that only incoming transactions over the value of 100 satisfy the condition.

For information about configuring the action that will result when the conditions of the rule are met, see About Rule Actions.

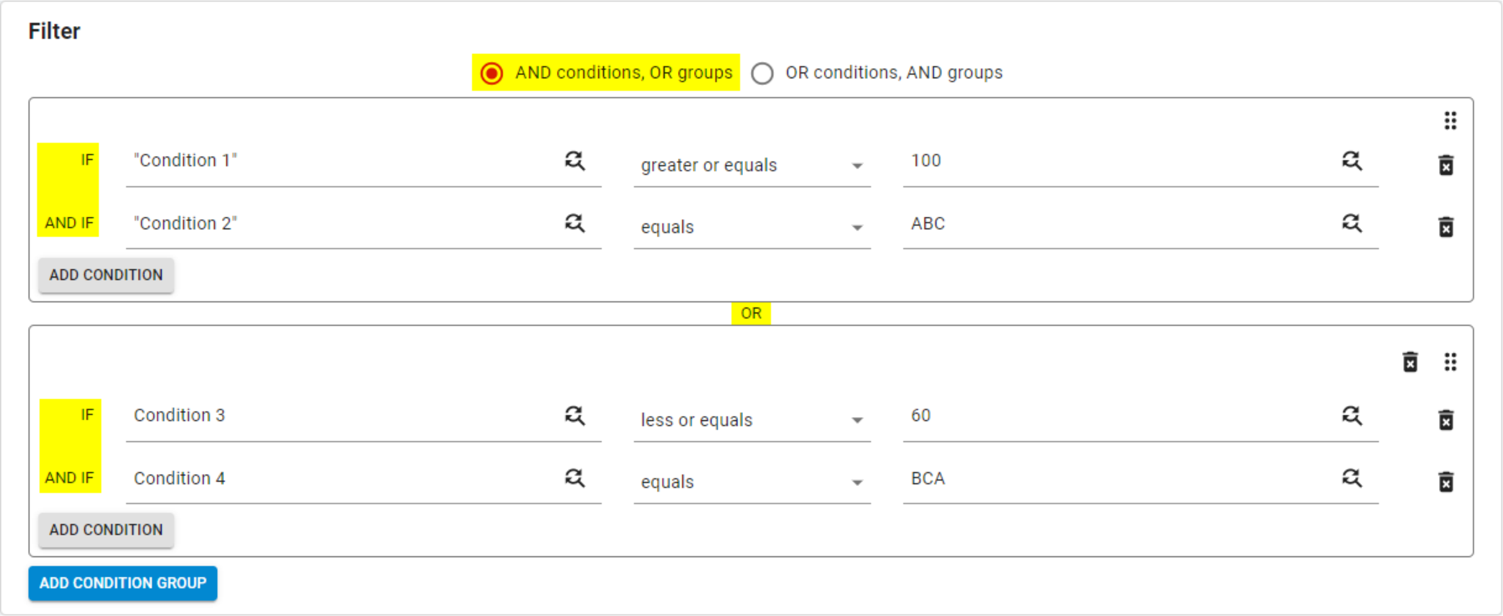
7.2.1 About condition groups

A rule can have one or more conditions. When using multiple conditions, you can form one or multiple *groups of conditions*. For a rule to trigger an action, all the logical expressions/conditions must be satisfied. For example, if a rule has three conditions but only two are satisfied when evaluating an incoming transaction, the rule will not trigger an action.

You can group the conditions associated with rules using *AND* and *OR* operators.

You can choose from two options at the top of the **Filter** pane:

- **AND conditions, OR groups** – between groups of conditions the logical operator *OR* is applied, but the *AND* operator is applied between conditions within each conditions group



Filter

● AND conditions, OR groups ○ OR conditions, AND groups

IF	"Condition 1"	greater or equals	100
AND IF	"Condition 2"	equals	ABC

ADD CONDITION

OR

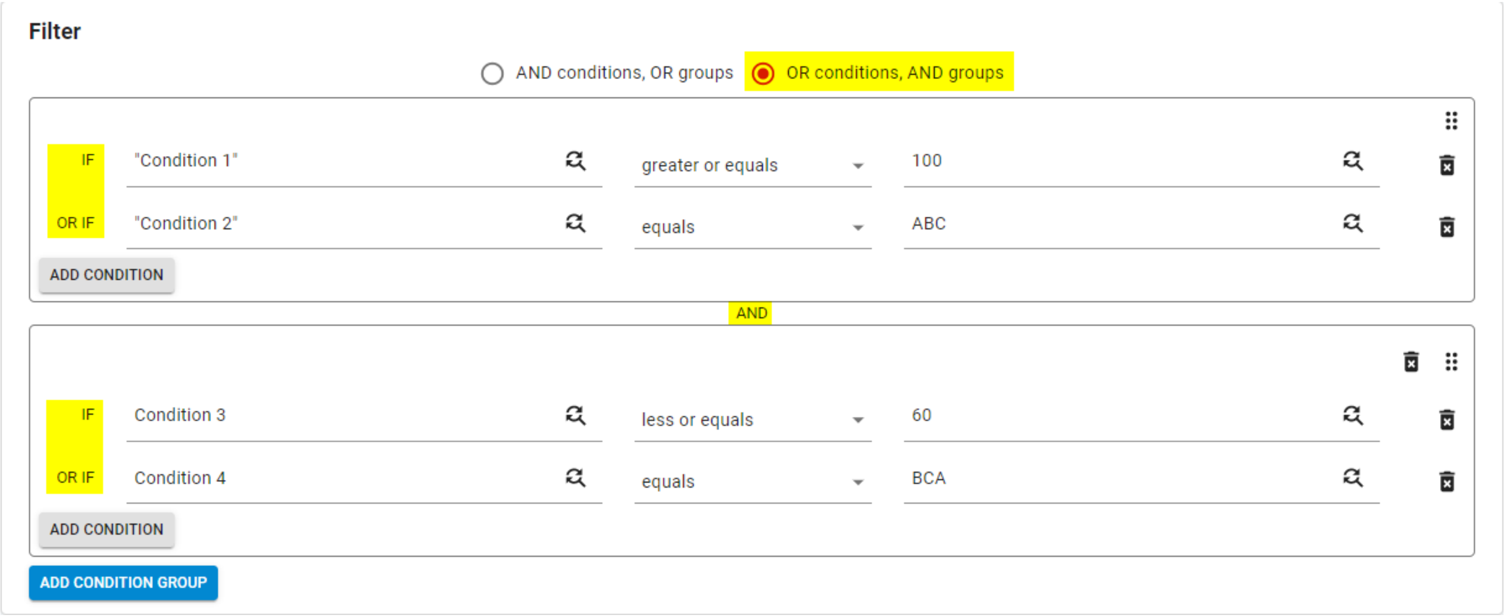
IF	Condition 3	less or equals	60
AND IF	Condition 4	equals	BCA

ADD CONDITION

ADD CONDITION GROUP

Figure 25: Example showing AND conditions, OR groups

- **OR conditions, AND groups** – between groups of conditions the logical operator *AND* is applied, but the *OR* operator is applied between conditions within each condition group



Filter

○ AND conditions, OR groups ● OR conditions, AND groups

IF	"Condition 1"	greater or equals	100
OR IF	"Condition 2"	equals	ABC

ADD CONDITION

AND

IF	Condition 3	less or equals	60
OR IF	Condition 4	equals	BCA

ADD CONDITION

ADD CONDITION GROUP

Figure 26: Example showing OR conditions, AND groups

There are no system limitations to the number of groups you can have within a rule. However, Thredd recommends you check the performance of each rule regularly.

7.3 Configuring Rules

This section explains how to add a new group of conditions, delete a group and/or conditions, and edit rule conditions.

Note: Only managers with the appropriate access rights can modify rules, groups and conditions. See User Access Management for further information.

7.3.1 Adding a new group of conditions

To add a new group of conditions:

1. Click **Add Condition Group**. The new condition group is displayed.
2. To add a condition within the group, click **Add Condition**. By default, a new empty condition is displayed.

7.3.2 Deleting a group and/or condition

To delete a new group of conditions:

1. Click **Delete** in the right of the **Filter** pane associated with the appropriate group or condition.

7.3.3 Updating a rule

Changes to existing conditions of rules can be initiated only by managers with the appropriate access rights.

To edit a rule:

1. Click **Edit** in the top right of the screen.
2. Apply your edits and click **Save**.

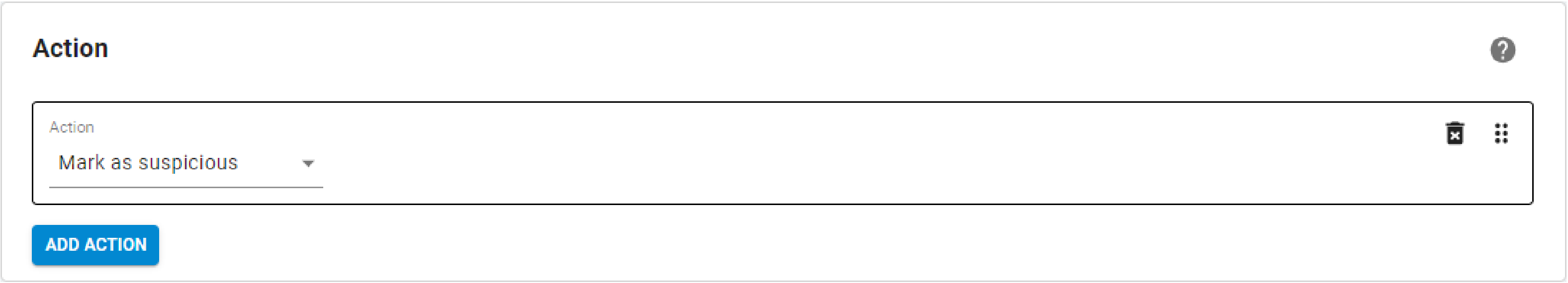
Note: Any changes made to rules appear as change requests on the Thredd side. After the change request is captured on Thredd JIRA, Thredd checks to ensure the requirements of the change match the actual configuration change before publishing the modifications in the production environment.

7.4 About Rule Actions

A rule action is a trigger which is executed immediately after all the conditions of the rule are met. A rule can have a single rule action or multiple rule actions configured. All rule actions are executed in sequential order, as they appear in the **Action** pane. The order can be changed.

The most commonly used rule actions are:

- ***Mark as suspicious:*** This action marks the event as suspicious and displays it on the **Suspicious Transaction Log** screen. This is the default action configured for all rules.



Action

Action: Mark as suspicious

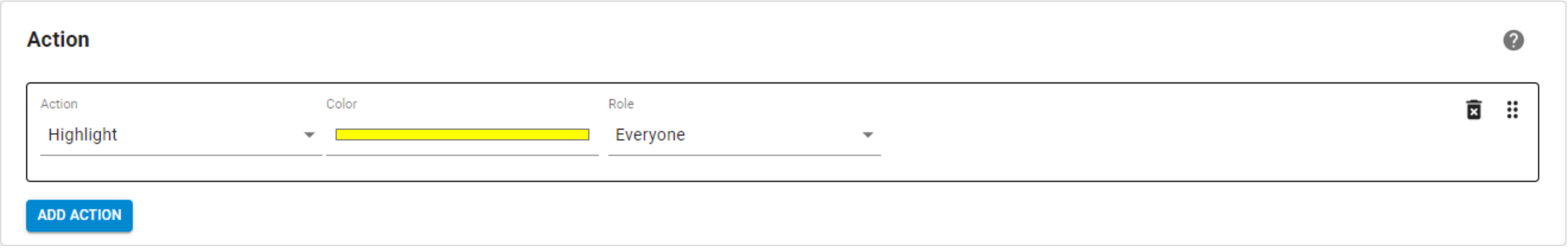
Figure 27: Mark as suspicious rule action

Events marked as suspicious by the Thredd Protect rules are displayed on the **System marked events/System marked Transactions** page in **green**, until the event is reviewed and the status is changed by a user. After a new status is assigned to an event/transaction by a user, the transaction is moved and displayed on the **Operator marked events** pages, depending on the status:

- **Operator marked events** > **Genuine**
- **Operator marked events** > **Investigation**
- **Operator marked events** > **Fraud**
- **Operator marked events** > **Ignore**

  Transaction colour coding.

- **Highlight:** This action highlights an event on the user interface:



Action

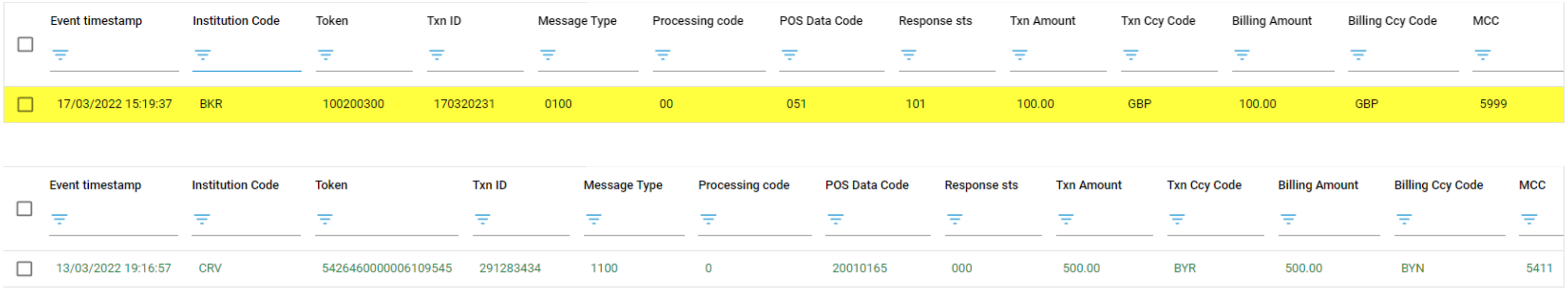
Action: Highlight

Color:

Role: Everyone

Figure 28: Highlight rule action

You can select the colour of the highlighter from a full RGB pallet. The following example shows the difference between a highlighted and a non-highlighted event (the difference between the highlighted action being triggered or not):

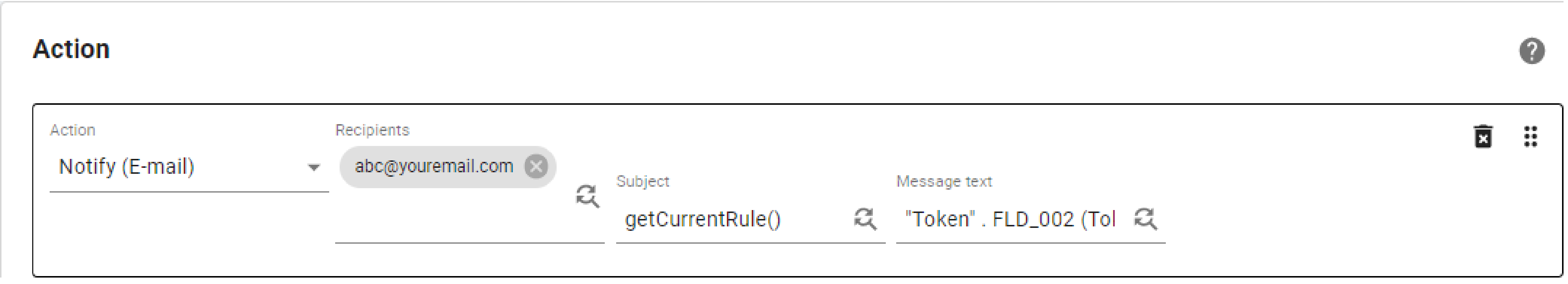


□	Event timestamp	Institution Code	Token	Txn ID	Message Type	Processing code	POS Data Code	Response sts	Txn Amount	Txn Ccy Code	Billing Amount	Billing Ccy Code	MCC
□	17/03/2022 15:19:37	BKR	100200300	170320231	0100	00	051	101	100.00	GBP	100.00	GBP	5999

□	Event timestamp	Institution Code	Token	Txn ID	Message Type	Processing code	POS Data Code	Response sts	Txn Amount	Txn Ccy Code	Billing Amount	Billing Ccy Code	MCC
□	13/03/2022 19:16:57	CRV	5426460000006109545	291283434	1100	0	20010165	000	500.00	BYR	500.00	BYN	5411

Figure 29: Example of a highlighted event

Notify (E-Mail): This action sends an email notification to selected recipients. You can configure the subject of the email and the message text and include any text and/or event attributes as shown below:



Action

Action: Notify (E-mail)

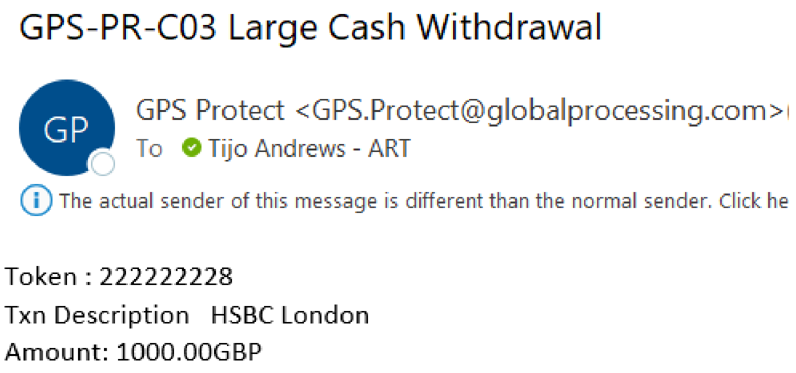
Recipients: abc@youremail.com

Subject: getCurrentRule()

Message text: "Token" . FLD_002 (Tol

Figure 30: Configuring a notify action

Below is an example of an email alert received from Thredd Protect when the *Notify (E-Mail)* action is triggered:



GPS-PR-C03 Large Cash Withdrawal

GP

GPS Protect <GPS.Protect@globalprocessing.com>

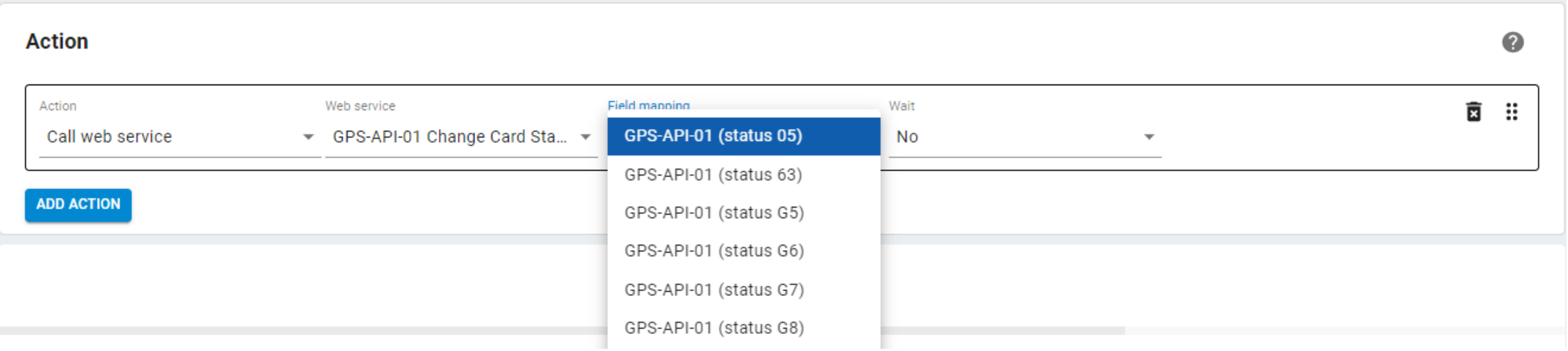
To Tijo Andrews - ART

The actual sender of this message is different than the normal sender. Click he

Token : 222222228
Txn Description HSBC London
Amount: 1000.00GBP

Figure 31: Example of an email notification from Thredd Protect

Call web service: This action blocks a card by changing its status to *05 (Do not honor)*, *63 (Security Violation)* or Thredd specific G5-G8 card statuses. This prevents any further successful transactions on the card.



Action

Action: Call web service

Web service: GPS-API-01 Change Card Sta...

Field mapping: GPS-API-01 (status 05)

Wait: No

Figure 32: Configuring a Call web service action

- ***Add to rule allowlist:*** This action adds an attribute to a rule's allowlist for a specific time period. In the example below, the *Attribute* Token will be allowed (in other words, excluded from the rule triggering) for a period of 60 seconds, as defined in the **Expiration time (seconds)** field.

- ***Add to dataset:*** This action adds an attribute to an existing dataset for a specific time period. In the example below, the **Value** of the attribute "Card Acceptor Terminal ID" will be added to any selected dataset for a period of 60 seconds, as defined in the **Expiration time (seconds)** field.

7.5 Creating an Allowlist for Specific Rules

For each rule, a list of exceptions can be defined for any transaction attributes. Transactions that contain the value defined in the exception list will be ignored by the rule. The allowlist is defined by the transaction attribute value and the **Expiration date and time** of the allowed attribute/record.

To add an attribute to a specific rule's allowlist:

1. Click on + **Add new item** on the **Allowlist** pane. The input form appears. The number of records that can be added to the rule allowlist is unlimited.

   Optionally, to delete a record from the list, select it in the list and click 🗑 **Delete items**.

2. After making your changes, click 💾 **Save**. The allowlist is saved together with the rule. When the selected expiration date and time is reached, the card (or any other selected attribute for allowlisting) is automatically removed from the allowlist.

**While every endeavour will be employed to check the rule operates successfully, Thredd cannot and does not take responsibility for any losses incurred as a result of incorrectly configured rules (rules configured with erroneous parameters) or rules not operating as expected.*

Notes

- In some scenarios, a rule may be triggered although transactions are genuine
- To stop a rule from triggering, you can add a cardholder to the allowlist. The rule will then be ignored
- Only managers with the appropriate access rights can make changes to the rules and allowlists (see User Access Management for all available user access types)
- Over 50 different elements can be allowlisted. The most common ones are: Token, MCC, and Country
- You can only add or modify rules that belong to your institution
- You can make changes to rules under your institution. Thredd will review* the changes before publishing them in the Production environment
- If you’re unsure how to build a rule for a specific scenario, use Thredd customer support portal to raise a customer support request.

8 Using Datasets

This topic describes datasets and explains how to use them in Thredd Protect rules. It describes how to create a new dataset or update the values in an existing dataset.

A dataset is a list/collection of data points or values that Thredd Protect can use to check against the attributes of incoming events/transactions. A data set can be used multiple times in different rules. For example, consider the following scenario:

Use case scenario: dataset of high-risk countries

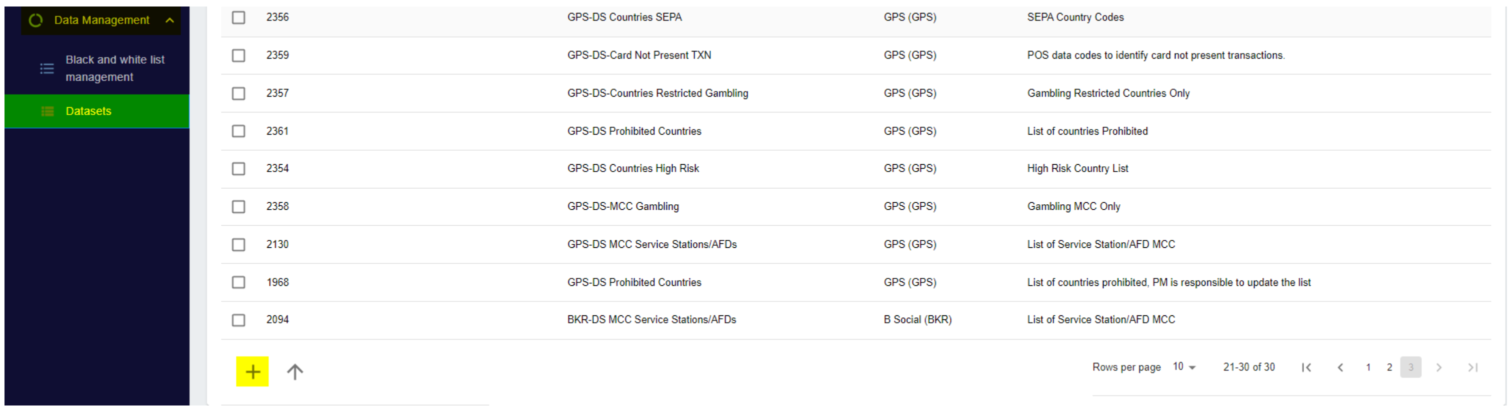
You want to create a rule in Thredd Protect that will check all transactions performed in countries deemed to be high-risk. As part of this, you create a dataset containing a list of ISO-2 values for these high-risk countries and use this dataset in the rule. The system will check the ISO-2 values in the dataset against the attribute *Acceptor Country* for incoming events/transactions.

Tip: For a list of ISO country codes, see: ISO - ISO 3166 – Country Codes.

8.1 Creating a Dataset

To create a new dataset:

1. Go to **Data Management > Datasets** and click on + **Add new item** on the bottom-left of the screen.



□	2356	GPS-DS Countries SEPA	GPS (GPS)	SEPA Country Codes
□	2359	GPS-DS-Card Not Present TXN	GPS (GPS)	POS data codes to identify card not present transactions.
□	2357	GPS-DS-Countries Restricted Gambling	GPS (GPS)	Gambling Restricted Countries Only
□	2361	GPS-DS Prohibited Countries	GPS (GPS)	List of countries Prohibited
□	2354	GPS-DS Countries High Risk	GPS (GPS)	High Risk Country List
□	2358	GPS-DS-MCC Gambling	GPS (GPS)	Gambling MCC Only
□	2130	GPS-DS MCC Service Stations/AFDs	GPS (GPS)	List of Service Station/AFD MCC
□	1968	GPS-DS Prohibited Countries	GPS (GPS)	List of countries prohibited, PM is responsible to update the list
□	2094	BKR-DS MCC Service Stations/AFDs	B Social (BKR)	List of Service Station/AFD MCC

Rows per page 10 21-30 of 30 1 2 3

Figure 33: Creating a dataset

2. In **Dataset details**, enter the **Institution ID**, **Dataset name** and **Dataset description**.

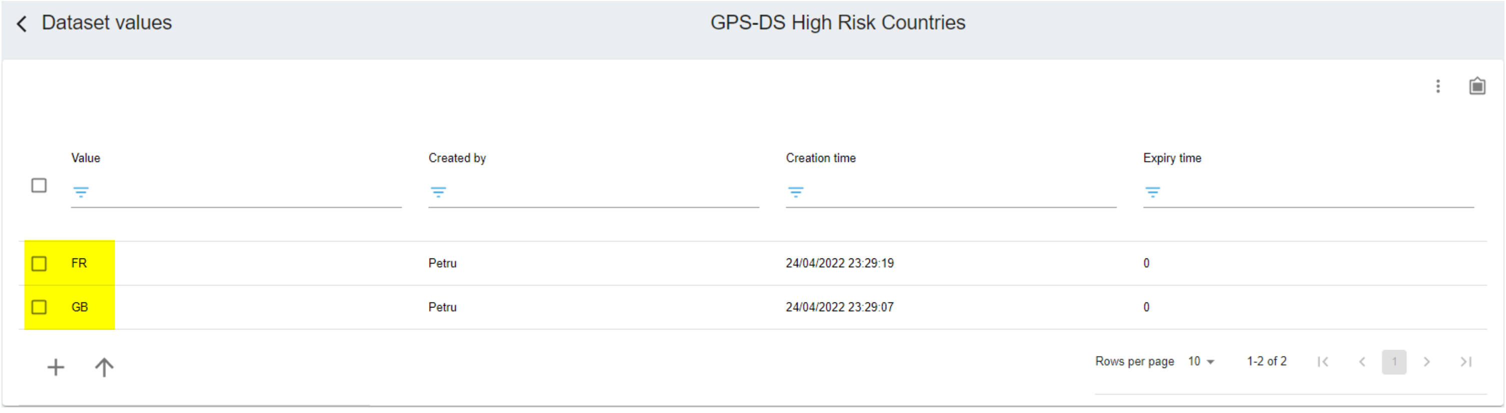
3. To complete the dataset creation process, click **Save** in the top-right corner of the screen.

8.2 Updating an Existing Dataset

This topic explains how to edit and delete values in an existing dataset, including how to import values into a dataset.

To edit an existing dataset:

1. Go to **Data Management > Datasets** and select the dataset you want to edit. The existing values are displayed:



< Dataset values   GPS-DS High Risk Countries

☐	Value	Created by	Creation time	Expiry time
☐	FR	Petru	24/04/2022 23:29:19	0
☐	GB	Petru	24/04/2022 23:29:07	0

Figure 34: Editing an existing dataset

2. To **add values** to a dataset, click on + **Add new item** at the bottom of the pane (dataset values can also be imported by clicking on ↑ **Import**):

3. Input the new **Value** (and, optionally, an **Expiry time** for the new value) and click 💾 **Save** in the top-right corner to complete the process:

4. To **edit** or **delete values** from a dataset, select the values and either right-click and choose an action or click on ⚙ **Edit item** or 🗑 **Delete items**:

Note: You can add new Countries, MCCs, Tokens or other types of data codes so these can be used by the rules you have set up for your institution.

Note: Only managers with the appropriate access rights can make changes to datasets (see User Access Management for all available user access types).

9 Configuring Statistical Parameters

This section explains how to display and configure the statistical parameters used by Thredd Protect.

Thredd Protect helps to analyse fraud patterns over time so that you can tailor rules as your programme and cardholder behaviour evolves. As part of this, Thredd Protect collects statistical data about transactions for specific time periods, as defined by certain parameters. Thredd Protect then uses the values calculated from this data in the logic building of rules.

> **Note:** You can only add or modify statistics belonging to your institution so they can be used by the rules you have set-up. All user types can view statistical parameters but only managers with appropriate access rights can make changes to them (see User Access Management for a list of available user access types).

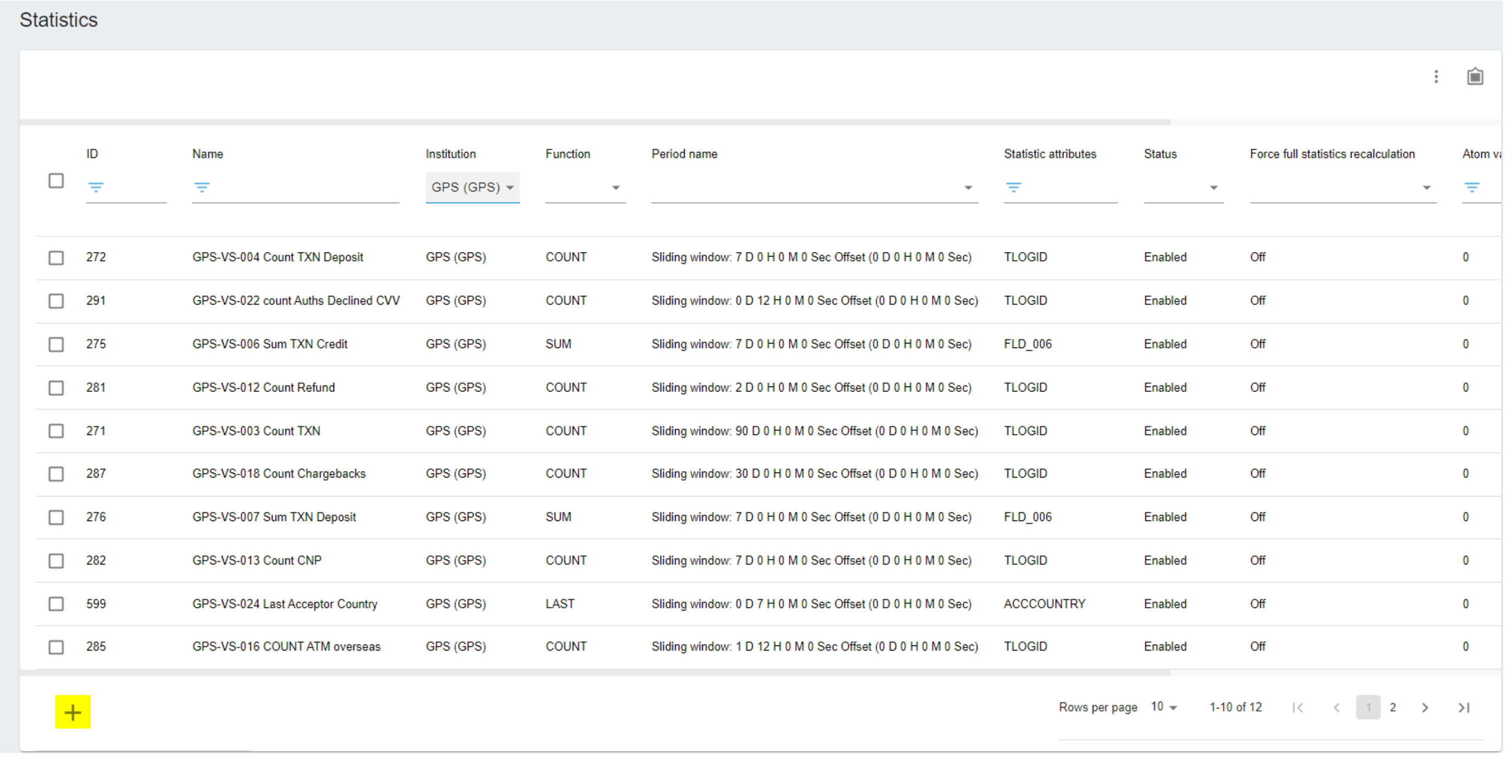
9.1 Displaying Statistical Parameters

To view statistical parameters:

Navigate to **Configuration** > **Statistics manager**. All existing statistical parameters are displayed for the institution(s) you have access to.

9.2 Creating Statistical Parameters

1. To create a new statistical parameter, click + **Add new item** on the bottom-left of the screen.



Statistics

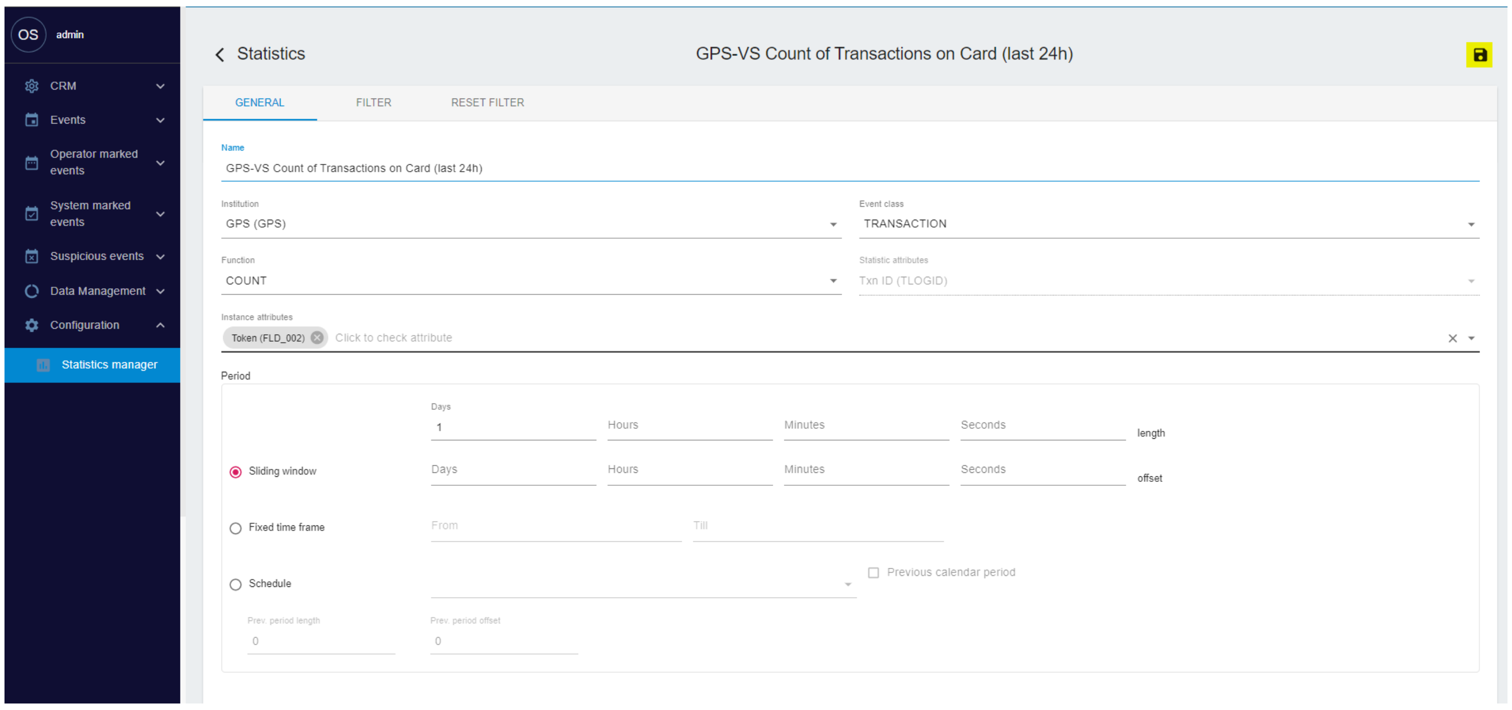
□	ID	Name	Institution	Function	Period name	Statistic attributes	Status	Force full statistics recalculation	Atom va
			GPS (GPS)						
□	272	GPS-VS-004 Count TXN Deposit	GPS (GPS)	COUNT	Sliding window: 7 D 0 H 0 M 0 Sec Offset (0 D 0 H 0 M 0 Sec)	TLOGID	Enabled	Off	0
□	291	GPS-VS-022 count Auths Declined CVV	GPS (GPS)	COUNT	Sliding window: 0 D 12 H 0 M 0 Sec Offset (0 D 0 H 0 M 0 Sec)	TLOGID	Enabled	Off	0
□	275	GPS-VS-006 Sum TXN Credit	GPS (GPS)	SUM	Sliding window: 7 D 0 H 0 M 0 Sec Offset (0 D 0 H 0 M 0 Sec)	FLD_006	Enabled	Off	0
□	281	GPS-VS-012 Count Refund	GPS (GPS)	COUNT	Sliding window: 2 D 0 H 0 M 0 Sec Offset (0 D 0 H 0 M 0 Sec)	TLOGID	Enabled	Off	0
□	271	GPS-VS-003 Count TXN	GPS (GPS)	COUNT	Sliding window: 90 D 0 H 0 M 0 Sec Offset (0 D 0 H 0 M 0 Sec)	TLOGID	Enabled	Off	0
□	287	GPS-VS-018 Count Chargebacks	GPS (GPS)	COUNT	Sliding window: 30 D 0 H 0 M 0 Sec Offset (0 D 0 H 0 M 0 Sec)	TLOGID	Enabled	Off	0
□	276	GPS-VS-007 Sum TXN Deposit	GPS (GPS)	SUM	Sliding window: 7 D 0 H 0 M 0 Sec Offset (0 D 0 H 0 M 0 Sec)	FLD_006	Enabled	Off	0
□	282	GPS-VS-013 Count CNP	GPS (GPS)	COUNT	Sliding window: 7 D 0 H 0 M 0 Sec Offset (0 D 0 H 0 M 0 Sec)	TLOGID	Enabled	Off	0
□	599	GPS-VS-024 Last Acceptor Country	GPS (GPS)	LAST	Sliding window: 0 D 7 H 0 M 0 Sec Offset (0 D 0 H 0 M 0 Sec)	ACCCOUNTRY	Enabled	Off	0
□	285	GPS-VS-016 COUNT ATM overseas	GPS (GPS)	COUNT	Sliding window: 1 D 12 H 0 M 0 Sec Offset (0 D 0 H 0 M 0 Sec)	TLOGID	Enabled	Off	0

Figure 35: Creating a new statistical parameter

2. Enter a **Name** for the parameter.
3. Choose the **Institution** the parameter should be bound to.
4. In **Function**, select the main function of the parameter:
   - **SUM** – sum. For example, Billing Amount on a Card (total spent) for the last X days/weeks.
   - **AVERAGE** – average value. For example, Billing Amount on a Card (average per transaction) for the last *X* days/months etc.
   - **COUNT** – quantity of transactions on a Card (velocity) for the last *X* hour/days etc.
   - **MIN** – minimal value. For example, Billing Amount on a Card (highest ticket) for the last *X* weeks/months etc.
   - **MAX** – maximum value. For example, Billing Amount on a Card (highest ticket) for the last *X* days/months etc.
   - **LAST** – last value. For example, Acceptor Country where a transaction took place
   - **DESCENDING** – descending values.

- **SAMEVAL** – identical value.
- **DISTINCT** – distinct value.

5. Select the **Statistic** and **Instance attributes**.
6. Select the **Period** of time the parameter will use in its calculations.



Statistics — GPS-VS Count of Transactions on Card (last 24h)

Name: GPS-VS Count of Transactions on Card (last 24h)

Institution: GPS (GPS)

Event class: TRANSACTION

Function: COUNT

Statistic attributes: Txn ID (TLOGID)

Instance attributes: Token (FLD_002) Click to check attribute

Period

Days: 1 Hours Minutes Seconds length

● Sliding window Days Hours Minutes Seconds offset

○ Fixed time frame From Till

○ Schedule □ Previous calendar period

Prev. period length: 0 Prev. period offset: 0

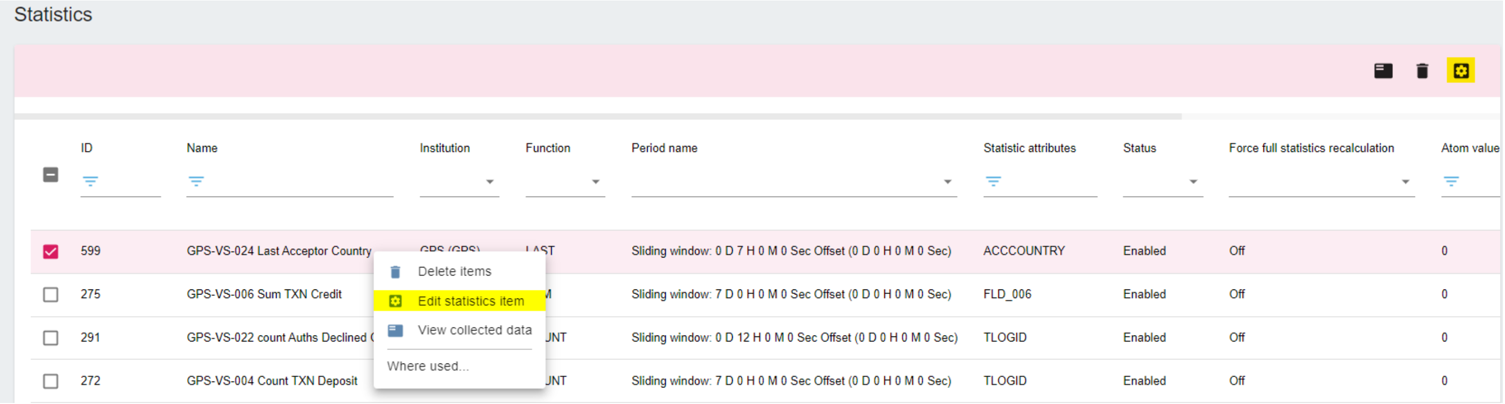
Figure 36: Configuring a statistical parameter

7. To complete parameter creation, click **Save** (top-right corner).

9.3 Updating Statistical Parameters

This section explains how to edit and delete statistical parameters.

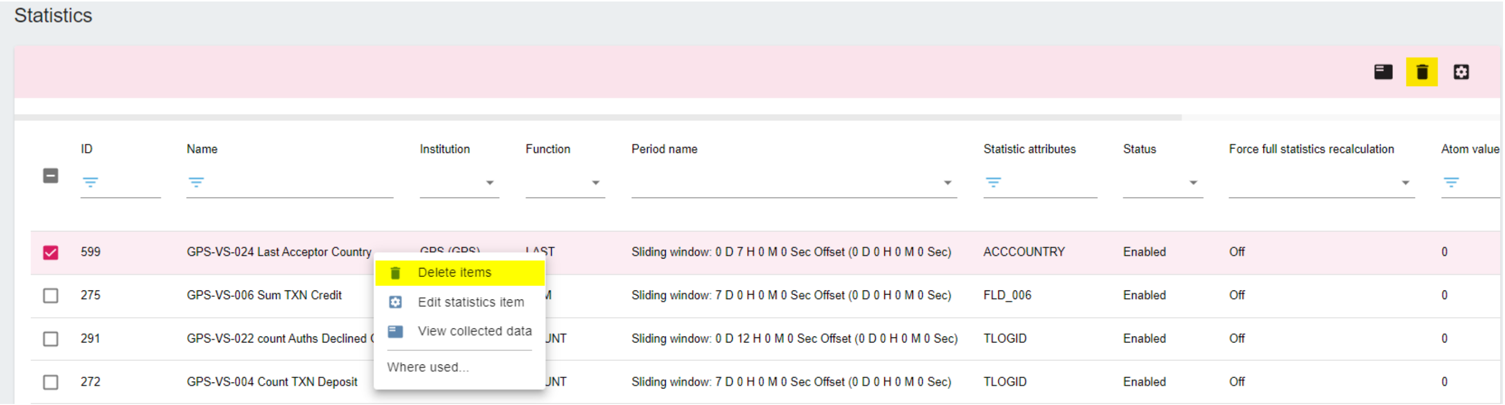
1. To **edit** a statistical parameter, select it and either right-click and choose the option or click **Edit statistics item**:



	ID	Name	Institution	Function	Period name	Statistic attributes	Status	Force full statistics recalculation	Atom value
☑	599	GPS-VS-024 Last Acceptor Country	GPS (GPS)	LAST	Sliding window: 0 D 7 H 0 M 0 Sec Offset (0 D 0 H 0 M 0 Sec)	ACCCOUNTRY	Enabled	Off	0
□	275	GPS-VS-006 Sum TXN Credit		M	Sliding window: 7 D 0 H 0 M 0 Sec Offset (0 D 0 H 0 M 0 Sec)	FLD_006	Enabled	Off	0
□	291	GPS-VS-022 count Auths Declined (		UNT	Sliding window: 0 D 12 H 0 M 0 Sec Offset (0 D 0 H 0 M 0 Sec)	TLOGID	Enabled	Off	0
□	272	GPS-VS-004 Count TXN Deposit		UNT	Sliding window: 7 D 0 H 0 M 0 Sec Offset (0 D 0 H 0 M 0 Sec)	TLOGID	Enabled	Off	0

Figure 37: Editing a statistical parameter

2. To **delete** a statistical parameter, select it and either right-click and choose the option or click 🗑 **Delete items**:



Statistics

☐	ID	Name	Institution	Function	Period name	Statistic attributes	Status	Force full statistics recalculation	Atom value
☑	599	GPS-VS-024 Last Acceptor Country	GPS (GPS)	LAST	Sliding window: 0 D 7 H 0 M 0 Sec Offset (0 D 0 H 0 M 0 Sec)	ACCCOUNTRY	Enabled	Off	0
☐	275	GPS-VS-006 Sum TXN Credit		M	Sliding window: 7 D 0 H 0 M 0 Sec Offset (0 D 0 H 0 M 0 Sec)	FLD_006	Enabled	Off	0
☐	291	GPS-VS-022 count Auths Declined (		UNT	Sliding window: 0 D 12 H 0 M 0 Sec Offset (0 D 0 H 0 M 0 Sec)	TLOGID	Enabled	Off	0
☐	272	GPS-VS-004 Count TXN Deposit		UNT	Sliding window: 7 D 0 H 0 M 0 Sec Offset (0 D 0 H 0 M 0 Sec)	TLOGID	Enabled	Off	0

Figure 38: Deleting a statistical parameter

10 Generating Reports

This section provides details about the reports available in Thredd Protect and explains how to generate a report and view its results.

Note: Only managers with the appropriate access rights can view and generate reports (see User Access Management for more information).

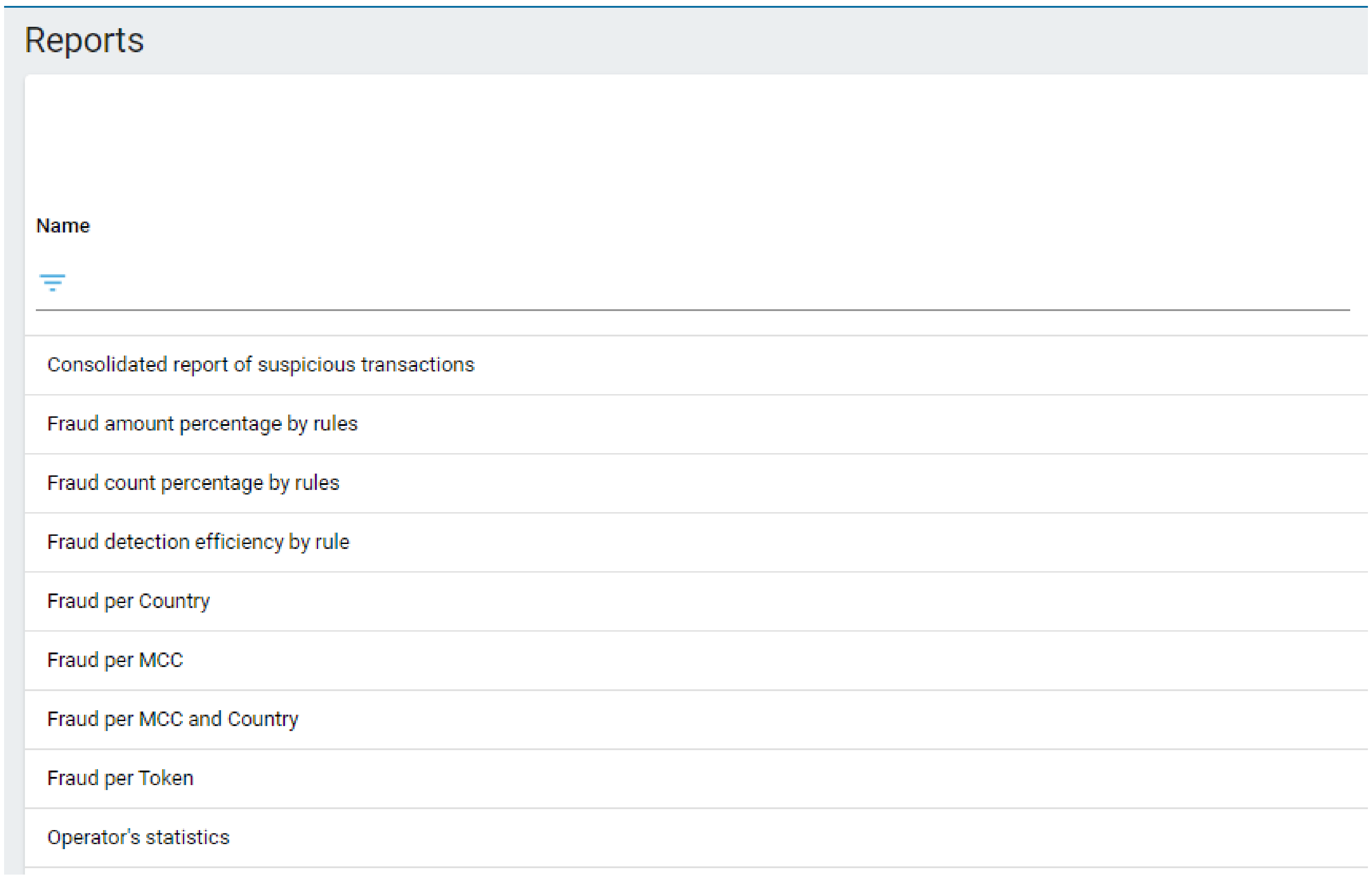
Assigning a status to an alert.

10.1 Displaying Available Reports

To see a list of the reports available in Thredd Protect:

1. On the main menu, go to **Reports** > **Reports list**.

   The 🗎 **Reports** screen appears showing a list of available reports.



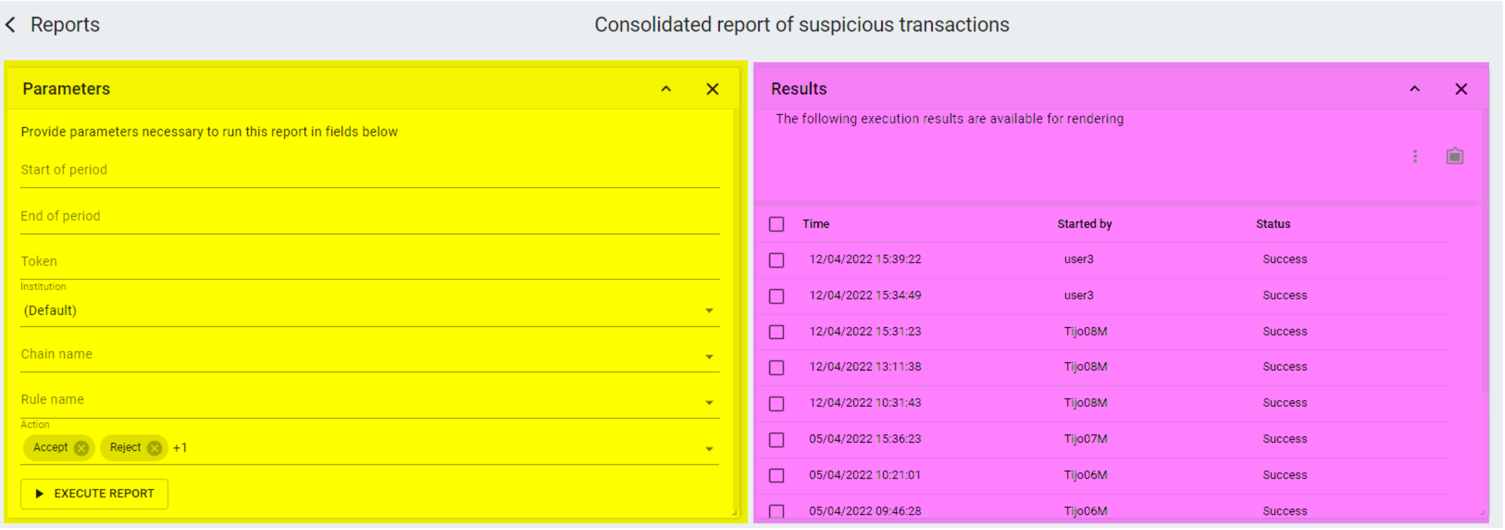
Reports

Name
Consolidated report of suspicious transactions
Fraud amount percentage by rules
Fraud count percentage by rules
Fraud detection efficiency by rule
Fraud per Country
Fraud per MCC
Fraud per MCC and Country
Fraud per Token
Operator's statistics

Figure 39: List of available reports

10.2 Running a Report

1. Click on a report to display information about its parameters and execution results. For example, the **Consolidated report of suspicious transactions**:



Consolidated report of suspicious transactions

Provide parameters necessary to run this report in fields below

Institution: (Default)

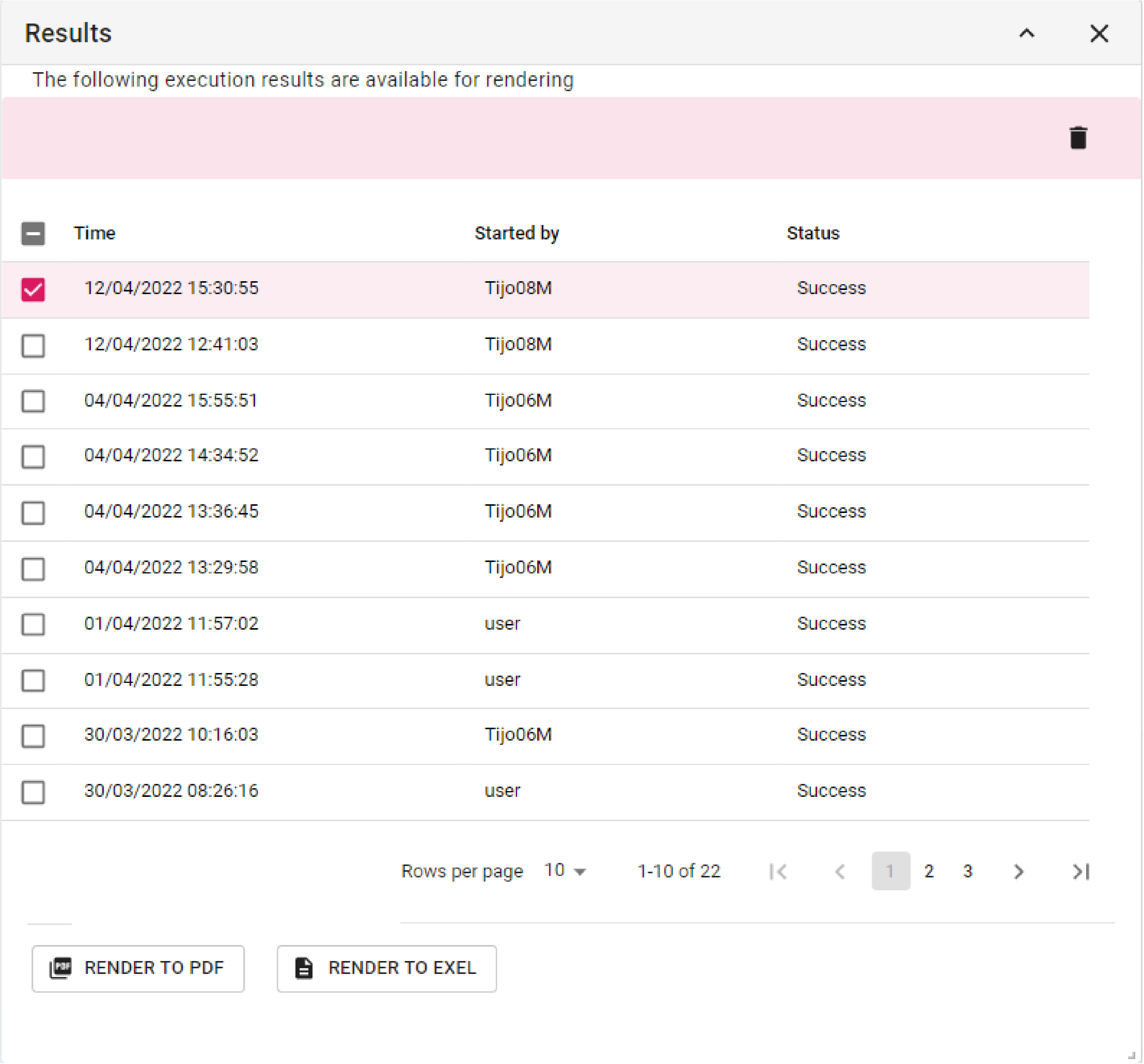
Action: Accept Reject +1

The following execution results are available for rendering

□	Time	Started by	Status
□	12/04/2022 15:39:22	user3	Success
□	12/04/2022 15:34:49	user3	Success
□	12/04/2022 15:31:23	Tijo08M	Success
□	12/04/2022 13:11:38	Tijo08M	Success
□	12/04/2022 10:31:43	Tijo08M	Success
□	05/04/2022 15:36:23	Tijo07M	Success
□	05/04/2022 10:21:01	Tijo06M	Success
□	05/04/2022 09:46:28	Tijo06M	Success

Figure 40: Report parameters and results

2. In **Parameters**, specify any required fields and filters, such as the reporting period (maximum 90 days between "Start of period" and “End of period”). Note that the report parameters change depending on the report you selected.
3. To execute the report, click on **Execute Report** on the bottom-left. The report runs and the results appear in the **Results** pane on the right-hand side.


Results

The following execution results are available for rendering

☐	Time	Started by	Status
☑	12/04/2022 15:30:55	Tijo08M	Success
☐	12/04/2022 12:41:03	Tijo08M	Success
☐	04/04/2022 15:55:51	Tijo06M	Success
☐	04/04/2022 14:34:52	Tijo06M	Success
☐	04/04/2022 13:36:45	Tijo06M	Success
☐	04/04/2022 13:29:58	Tijo06M	Success
☐	01/04/2022 11:57:02	user	Success
☐	01/04/2022 11:55:28	user	Success
☐	30/03/2022 10:16:03	Tijo06M	Success
☐	30/03/2022 08:26:16	user	Success

Rows per page 10 1-10 of 22

Figure 41: Report results

Note: Reports that contains a large amount of data may take a long time to generate.

10.2.1 Saving a Report

You can save the results of a report locally in either *Adobe PDF* or *Microsoft Excel* file format.

1. To save a report, select the report in the *Results* pane and click on **Render to PDF** or **Render to EXCEL** depending on the format you want.

The system saves the report to your local drive where you can open it.

10.2.2 Scheduling a Report

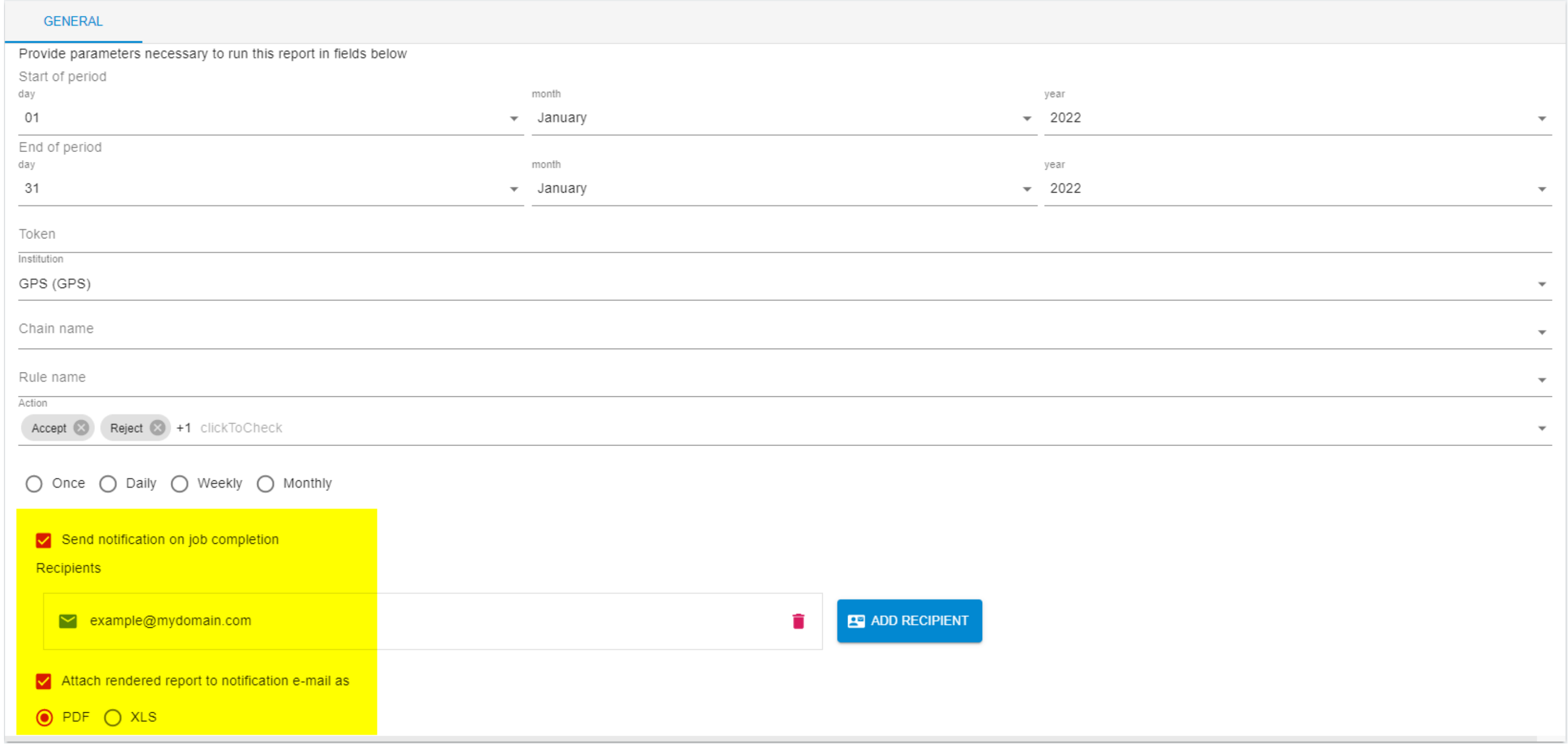
Reports can be generated on a scheduled basis. For example, you might choose to schedule the *Consolidated report of suspicious transactions* to run on the first day of every month, and send an email notification to a group of recipients.

To schedule a report:

1. In the **Schedule** pane, click on + **Add new item**.
2. In the **General** tab, specify the report execution frequency. Choose from **Once**, **Daily**, **Weekly** or **Monthly**.

3. To receive an email notification about successfully completed scheduled report generations, select **Send notification on job completion**, and provide one or more email addresses. To specify that the report should be sent as an attachment, select **Attach rendered report to notification e-mail as**, and specify either **PDF** or **XLS** format.

Note: there is a 25Mb file size limit, in line with many email systems.



Provide parameters necessary to run this report in fields below

Start of period

day	month	year
01	January	2022

End of period

day	month	year
31	January	2022

Token

Institution: GPS (GPS)

Chain name

Rule name

Action: Accept ⊗ Reject ⊗ +1 clickToCheck

○ Once ○ Daily ○ Weekly ○ Monthly

☑ Send notification on job completion

Recipients

example@mydomain.com

☑ Attach rendered report to notification e-mail as

● PDF ○ XLS

Figure 42: Send a notification

GPS.Protect@globalprocessing.com to the registered email address(es). Ensure you add this email address to your email system’s ‘allowed list’ so that notifications do not end up in your Spam folder.

11 User Access Management

This topic describes user access to Thredd Protect and how to raise a request for access or to change permissions.

Different levels of user access can be configured on the Thredd Protect portal, depending on role. For example, some users may only be able to view information about transactions and rules while others can view transactions, edit rules and run reports.

In Thredd Protect, there are three *Default User Access Types* based on role:

- Manager
- Analyst
- View Only

The following table shows the *Default User Access Types* with additional access permissions highlighted in blue:

Thredd Protect Default User Access Types		
View Only	**Risk Analyst**	**Manager**
Report Manager	**Report Manager**	**Report Manager**
-	-	+ Report Manager
-	-	+ Report Scheduler
Transactions	**Transactions**	**Transactions**
View all Transactions	View all Transactions	View all Transactions
View all Suspicious Transactions	View all Suspicious Transactions	View all Suspicious Transactions
View all Operator Marked Events	View all Operator Marked Events	View all Operator Marked Events
View all System Marked Events	View all System Marked Events	View all System Marked Events
Export Data to CSV	Export Data to CSV	Export Data to CSV
-	+ Review/Mark Transactions	Review/Mark Transactions
File Management	**File Management**	**File Management**
Access to all files	Access to all files	Access to all files
Denylist and allowlist management	**Denylist and allowlist management**	**Denylist and allowlist management**
-	View all records	View all records
-		+ Add/Delete/Edit Records
Rules	**Rules**	**Rules**
View Rules	View Rules	View Rules
-	-	+ Edit Rules
-	-	+ Edit Datasets

Thredd Protect Default User Access Types		
-	-	+ Edit Statistical Parameters
Cases	**Cases**	**Cases**
-	+ Open/Manage Cases	Open/Manage Cases

11.1 Requesting Changes to User Access

Thredd Protect user management is carried out by Thredd. To create a new user or request a change to permissions, the person responsible for user access permissions in your organisation needs to use the Thredd customer support portal to raise a customer support request.

For a user creation request, the person responsible for user access permissions in your organisation needs to provide the following information to Thredd:

- First name
- Surname
- Email address
- Required Access Type: Manager / Risk Analyst / View only

Note: An institution can have a maximum of two Managers and an unlimited number of Analysts and View Only access type accounts.

Appendix A – Common Codes

This section describes codes commonly used in the Thredd Protect system.

Tip: For a full list of all codes, see the Smart Client Guide.

Message type (MTID)

- 0100 = Authorisation
- 1240 = Presentment

Processing code (Txn code)

Status	Description
00	Debits (goods and services)
01	Debits (for ATM withdrawals or for cash disbursements)
02	Adjustment credits
09	Debits (goods with cash back)
11	Visa quasi-cash (POS) transactions
12	Cash disbursement
16	Payment Out
17	Debits (for cash advance)
18	Unique Transaction (requiers unique MCC)
19	Adjustment debits (goods and services with cash back)
20	Credits for refund
21	Credits (for deposit
22	Credits - Card load
23	Credits - Card unload
28	Credits (for Payment Transaction)
59	Blocked Amount Posting
90	PIN Unblock Transactions
30	Balance Enquiry

Status	Description
92	PIN Change Transactions

Response status

Status	Description
00	All good (Transaction was accepted)
01	Txn declined
03	Invalid merchant
04	Capture card
05	Do not honour
06	Unspecified Error
08	Honour with identification
10	Partial Approval
12	Invalid transaction
13	Invalid amount
14	Invalid card number (no such number)
15	Unable to route at IEM
17	Customer Cancellation
30	Format error
32	Completed Partially
33	Restricted card
37	Card acceptor call acquirer security
38	Allowable PIN tries exceeded
41	Lost card (Capture)
43	Stolen card (Capture)
51	Insufficient funds

Status	Description
54	Expired card
55	Incorrect PIN
57	Transaction not permitted to cardholder
61	Exceeds withdrawal amount limit
62	Restricted card
63	Security violation
64	Original amount incorrect
65	Exceeds withdrawal frequency limit
66	Card acceptor call acquirer's
67	Card to be picked up at ATM
68	Response to contact issuer
71	PIN not changed
75	Allowable number of PIN tries exceeded
76	Wrong PIN, allowable number of PIN tried exceeded
77	Issuer does not participate in the service
78	Unacceptable PIN- Transaction declined
80	Network error
81	Foreign network failure
82	Timeout at IEM
83	Card destroyed
85	Pin Unblock request
85	PIN validation not possible
87	Purchase Amount Only. No Cash Back Amount
88	Cryptographic failure
89	Authentication failure

Status	Description
91	Issuer or switch is inoperative
92	Unable to route at AEM
94	Duplicate Transmission
95	Reconcile error
96	System malfunction
98	Refund given to Customer
99	Card Voided
N7	Incorrect CVV (VISA Only)
P5	PIN Change/Unblock request declined
P6	Unsafe PIN

POS (Point of Sale) data code starting with

Status	Description
00	Unknown
01	Manual entry
02	Magstripe
03	Barcode reader
04	Optical Character Reader (OCR)
05	Chip Transaction
06	Chip PayPass Mapping Service application
07	Contactless
80	Magstripe
81	Ecommerce
90	Magstripe
91	Contactless magnetic stripe

Status	Description
92	Contactless input
95	Visa only

These can have subfields:

0 = Unspecified or unknown

1 = Terminal has PIN entry capability

2 = Terminal does not have PIN entry capability

8 = Terminal has PIN entry capability but PIN pad is not currently operative

Example:

- 050(0) = PAN auto-entry via integrated circuit card (ICC)- Unspecified or unknown
- 051(0) = PAN auto-entry via integrated circuit card (ICC) - Terminal has PIN entry capability
- 052(0) = PAN auto-entry via integrated circuit card (ICC)-Terminal does not have PIN entry capability

Card status code

Status	Description
05	Do not honour
14	Invalid Card Number
41	Lost card
43	Stolen card
54	Expired card
62	Restricted card
63	Security Violation
70	Cardholder to contact issuer
83	Card Destroyed
99	Card Voided

FAQs and Troubleshooting

This section provides answers to frequently asked questions and common troubleshooting issues.

Setup

Cannot log into Thredd Protect

- Check your credentials are correct. Both the username and password are case sensitive.
- If you forget your username or password, contact Thredd by raising a Thredd JIRA to request your username or a password reset.

> **Note:** After 3 failed login attempts, your account will be locked for 15 minutes after which you can try again. If you are unable to log in, contact Thredd to unlock your account and send you a password reminder.

How do I reset my password?

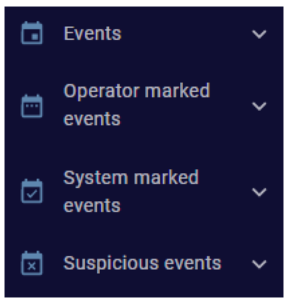
Changing or resetting a password.

Thredd JIRA or via email by sending a password reset request to FraudTeam@thredd.com.

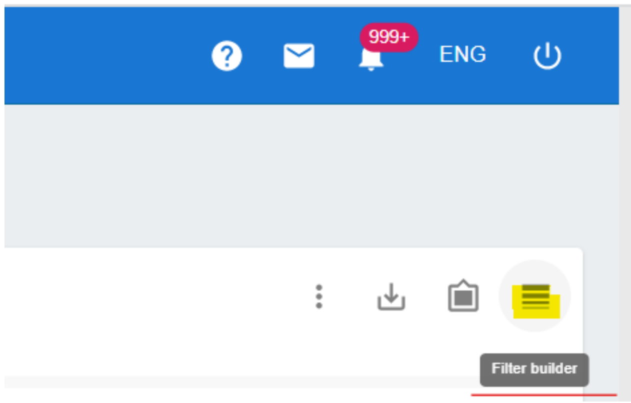
Monitoring

How do I filter data on transactional pages?

On any transactional page/sub-page (*Events*, *Operator marked events*, *System marked events* or *Suspicious events*):

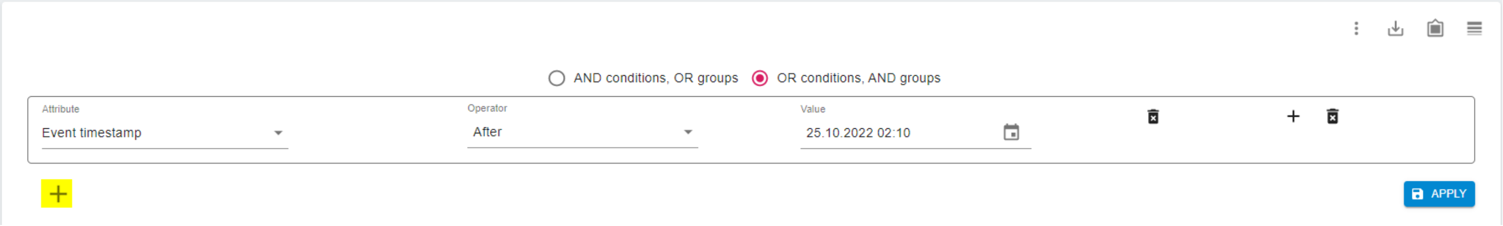


1. Click on ☰ *Filter builder* in the top-right of the page:



The filter area appears. The following filter appears with the default filter *Event timestamp* attribute (this filter is always present and cannot be removed).

2. Click + **Add new item** to add an additional filter if needed.

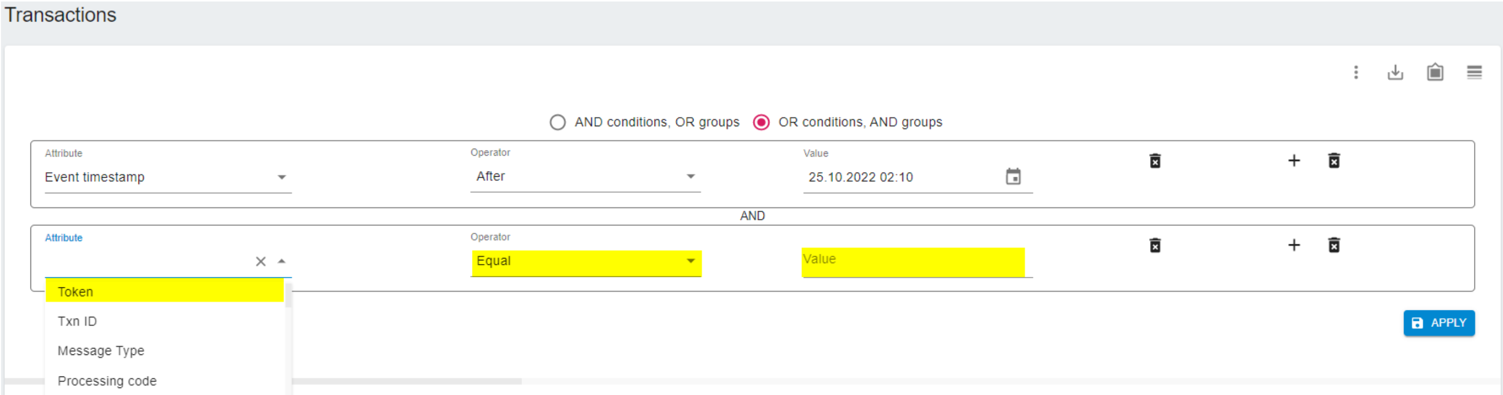


○ AND conditions, OR groups ● OR conditions, AND groups

Attribute: Event timestamp
Operator: After
Value: 25.10.2022 02:10

The default options appear.

3. From the dropdown, select the filtering “*Attribute”* (for example, Token), choose an operator (for example, Equals), provide the actual value of the attribute (for example, the token number) and click on **APPLY** to filter the data.



Transactions

○ AND conditions, OR groups ● OR conditions, AND groups

Attribute	Operator	Value
Event timestamp	After	25.10.2022 02:10

AND

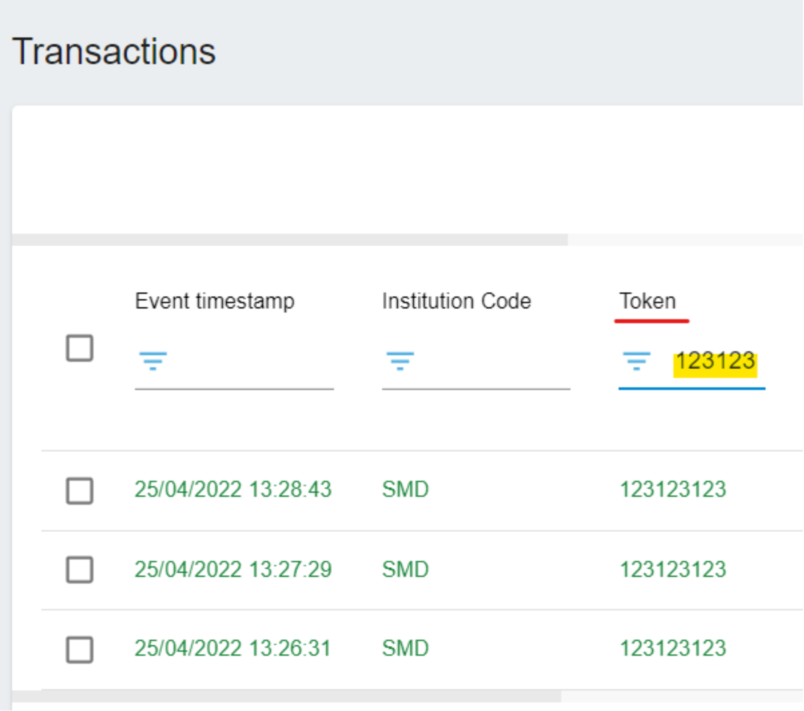
Attribute	Operator	Value
	Equal	Value

Token
Txn ID
Message Type
Processing code

APPLY

How can I quickly filter transactional data?

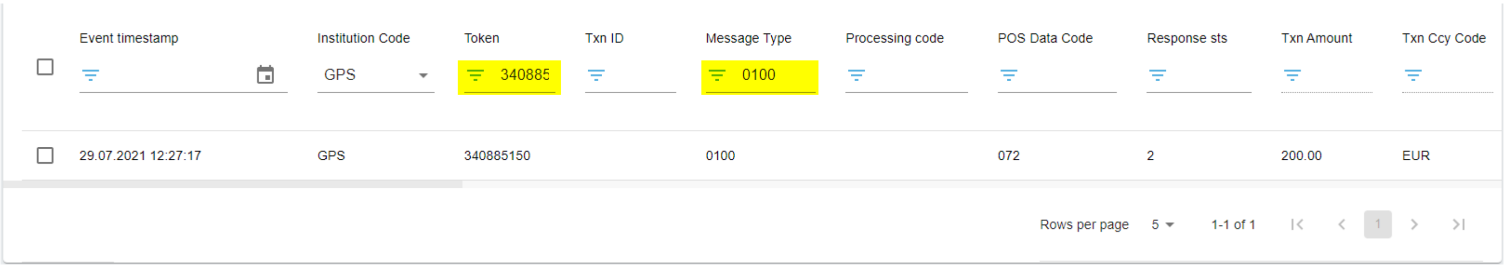
1. On any transactional page, at the top of each column, type or copy/paste the values you want to filter on. For example, to filter and display only transactions for a particular token, input its value to the right of :



Transactions

☐	Event timestamp	Institution Code	Token
			123123
☐	25/04/2022 13:28:43	SMD	123123123
☐	25/04/2022 13:27:29	SMD	123123123
☐	25/04/2022 13:26:31	SMD	123123123

2. Multiple quick filter options can be used simultaneously by inputting values to the right of in the columns that display a continuous line (for example, Token = 340885150 AND Message Type = 0100):

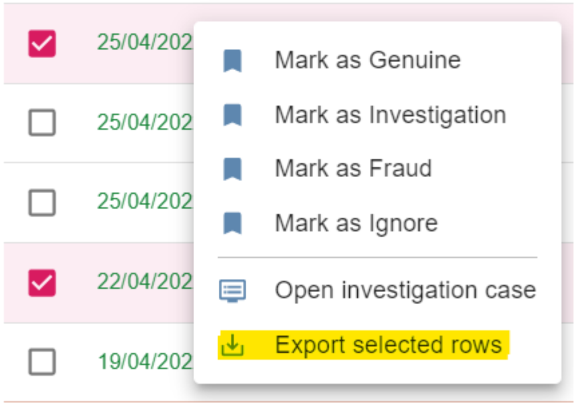


☐	Event timestamp	Institution Code	Token	Txn ID	Message Type	Processing code	POS Data Code	Response sts	Txn Amount	Txn Ccy Code
		GPS	340885		0100					
☐	29.07.2021 12:27:17	GPS	340885150		0100		072	2	200.00	EUR

Rows per page 5 1-1 of 1

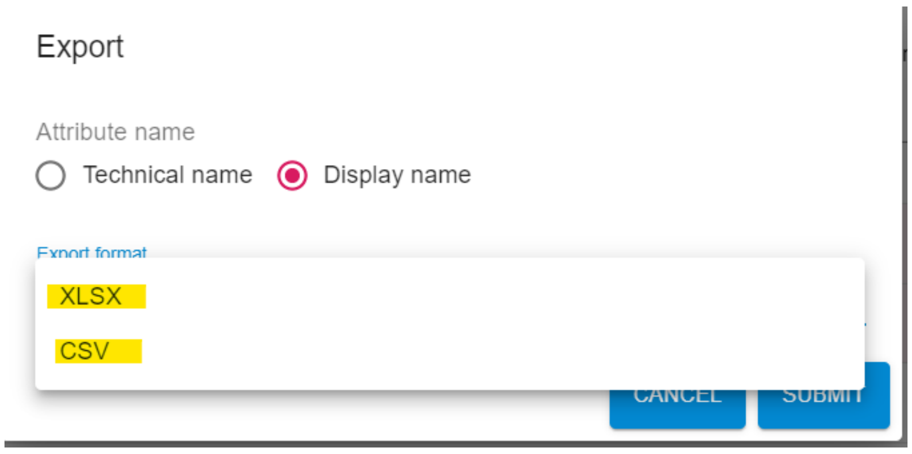
How do I export transactional data?

1. To export a *selection of transactions*, select your transactions then right-click and select **Export selected rows** or click **Export selected rows** in the top-right corner:



A window appears in which you can select the **Export format** such as XLSX or CSV.

2. Click **SUBMIT** to save the file on your local computer.

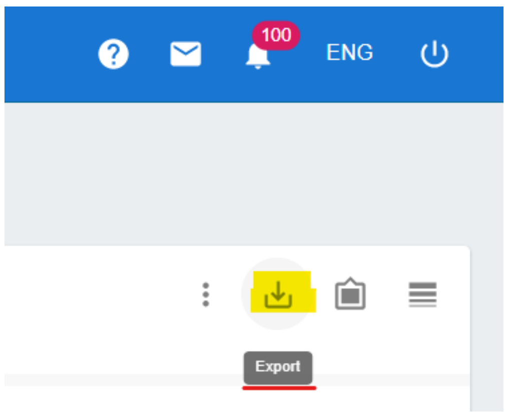


Export

Attribute name
○ Technical name ● Display name

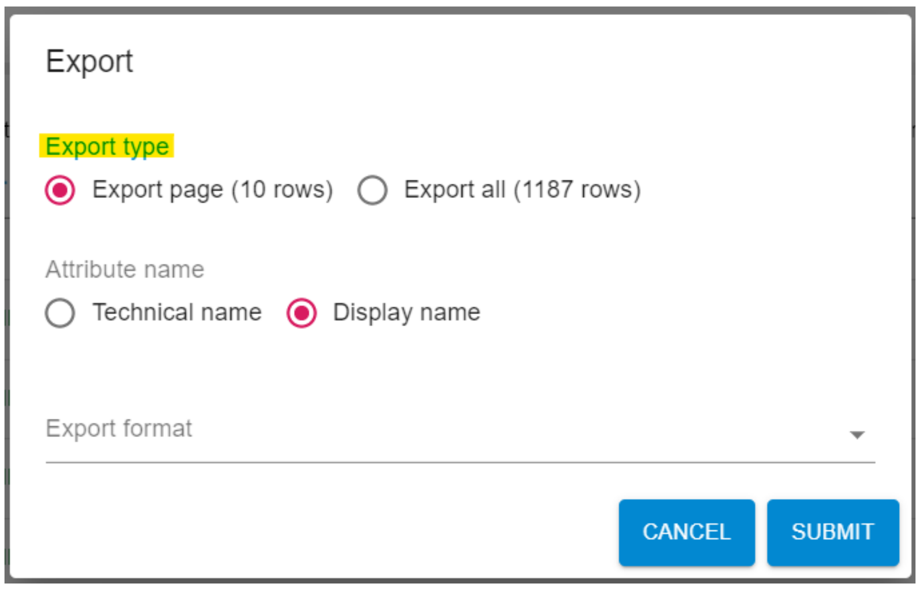
Export format
XLSX
CSV

3. To export *all transactions on a page* (no specific transactions are selected), click ⤓ **Export** in the top-right corner:



A window appears in which you can select the **Export format** such XLSX or CSV.

4. Click **SUBMIT** to save the file on your local computer.



Export

Export type
● Export page (10 rows) ○ Export all (1187 rows)

Attribute name
○ Technical name ● Display name

Export format

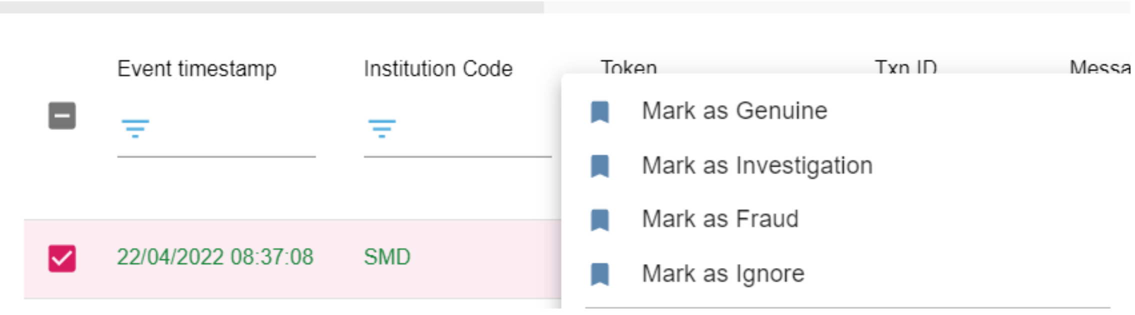
How do I mark transactions after investigating them?

There are two methods which are described below.

Note: With both methods, multiple transactions can be selected simultaneously so that you can bulk mark multiple transactions with the same status.

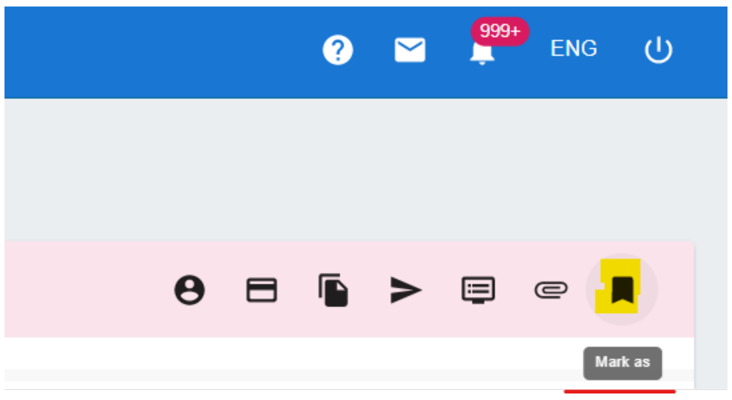
Method 1

After finalising the investigation, select the checkbox next to the transaction, then right-click and assign a status:



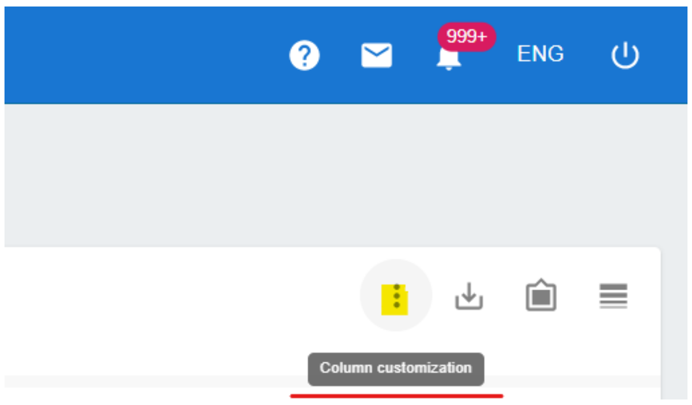
Method 2

After finalising the investigation, select the checkbox next to the transaction, then click 🔖 **Mark as** and select the option to assign a status:

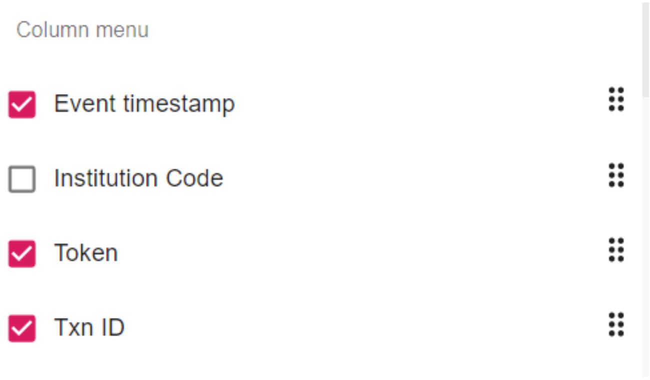


How do I customise the displayed data on transactional pages?

1. To display specific columns on-screen, hide columns or reorder columns so they better reflect how you use the data, on any transactional page/sub-page (*Events*, *Operator marked events*, *System marked events* or *Suspicious events*) click ⋮ **Column customization** on the top right:



2. After the list of displayed columns appears, select or deselect a column to add or remove it from the screen. To reorder columns, drag and drop them up and down:



Column menu

☑ Event timestamp

☐ Institution Code

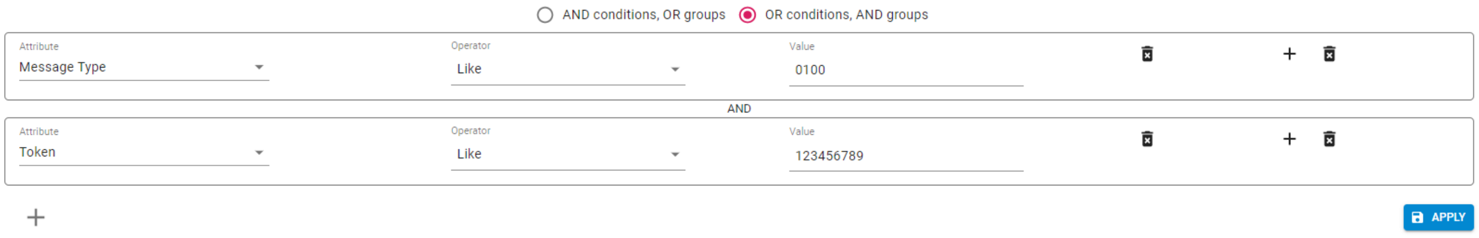
☑ Token

☑ Txn ID

How do I save and use frequently-used filters on transactional pages?

1. Make sure all frequently used filters/conditions are configured and contain the desired values.

   In the example below, two filters/conditions are defined:



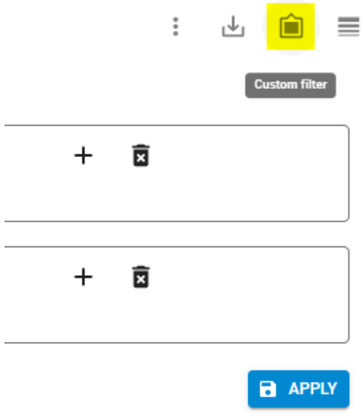
○ AND conditions, OR groups ● OR conditions, AND groups

Attribute: Message Type | Operator: Like | Value: 0100

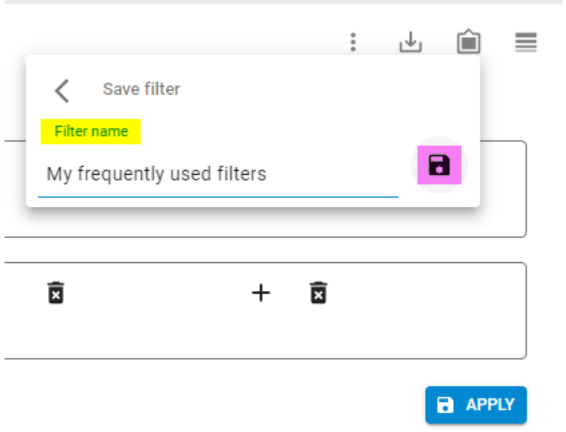
AND

Attribute: Token | Operator: Like | Value: 123456789

2. To save these for later use, click Custom filter in the top-right corner:



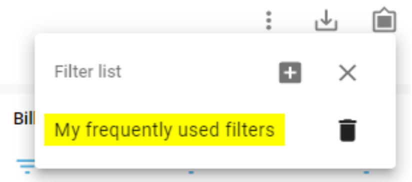
3. A pop-up appears. Click Save.



Save filter

Filter name: My frequently used filters

To use a saved filter, on the transactional page click Custom filter in the top-right corner, and select your filter:



Filter list

My frequently used filters

All the conditions/groups will be automatically populated and can be used to filter the data on the selected page.

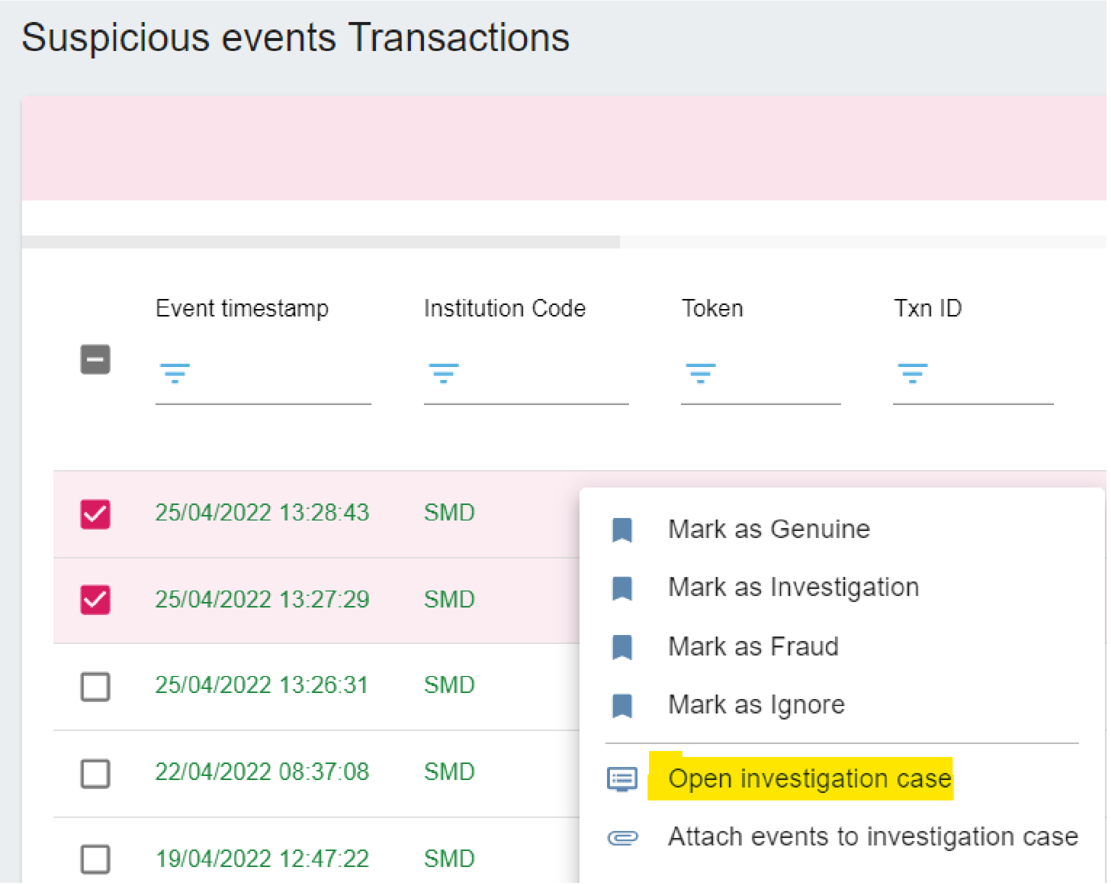
Investigating

How do I open an investigation case?

You can use several methods to create an investigation case:

Method 1

On any transactional page/sub-page (*Events*, *Operator marked events*, *System marked events* or *Suspicious events*) select the transaction(s) that should be part of the case, then right-click and select ▤ **Open investigation case** from the context menu:

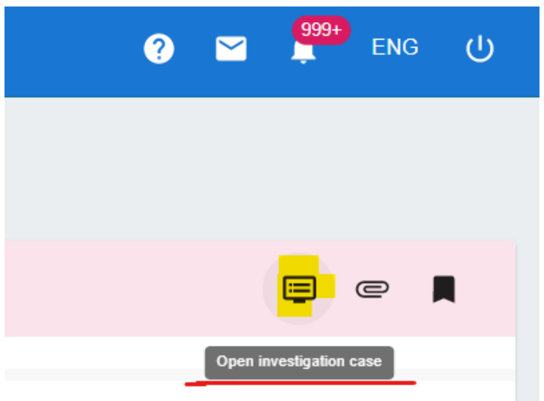


Suspicious events Transactions

☐	Event timestamp	Institution Code	Token	Txn ID
☑	25/04/2022 13:28:43	SMD		
☑	25/04/2022 13:27:29	SMD		
☐	25/04/2022 13:26:31	SMD		
☐	22/04/2022 08:37:08	SMD		
☐	19/04/2022 12:47:22	SMD		

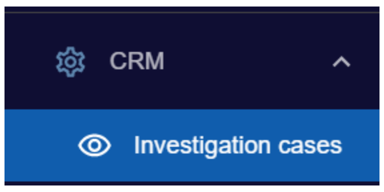
Method 2

After selecting transactions, click ▤ **Open investigation case** in the top-right corner:



Method 3

Navigate to **CRM > Investigation cases** and click + **Add new item** to create a new case.



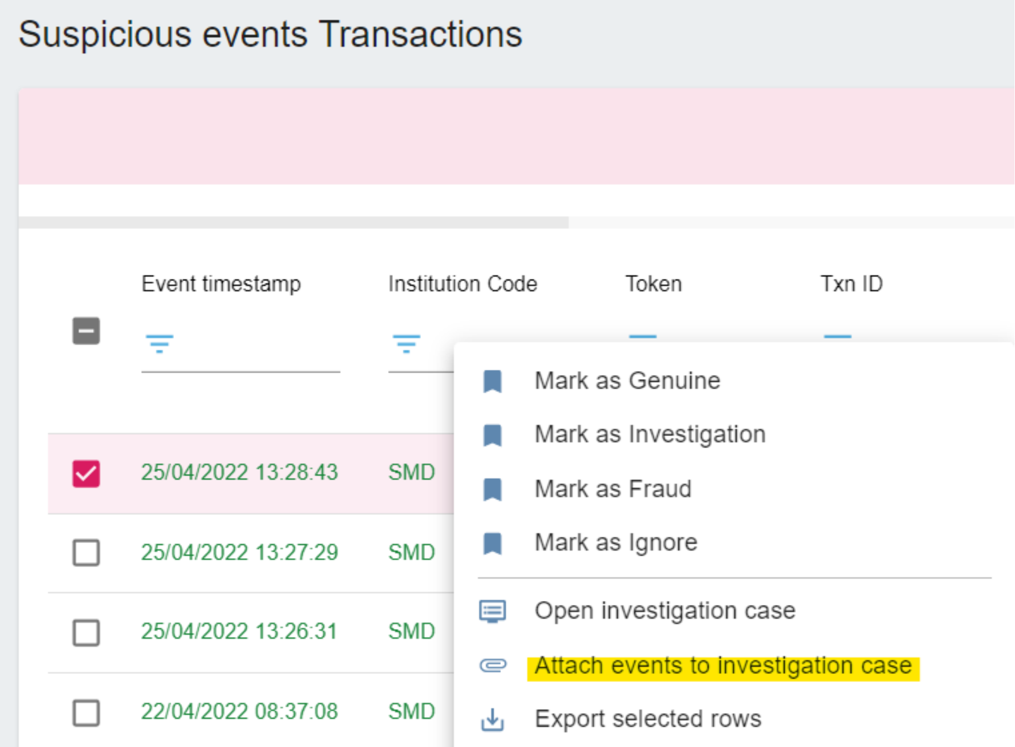
Transactions can be added later to an existing case, as described in the following topic.

How do I add transactions to an existing case?

You can use two methods to add transactions to an existing investigation case.

Method 1

1. Select the transaction(s) you want to add to an existing case, then right-click and select 📎 **Attach events to investigation case** from the context menu:

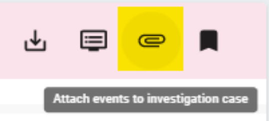


Suspicious events Transactions

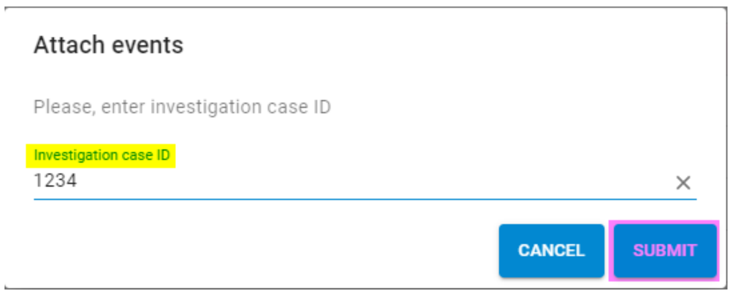
	Event timestamp	Institution Code	Token	Txn ID
☑	25/04/2022 13:28:43	SMD		
□	25/04/2022 13:27:29	SMD		
□	25/04/2022 13:26:31	SMD		
□	22/04/2022 08:37:08	SMD		

Method 2

1. After selecting transactions, click 📎 **Attach events to investigation case** in the top-right corner:



Regardless of the method used, you will be prompted to provide the *Investigation case ID* for the case the transactions are to be added to. Click **SUBMIT** to commit the addition:



Attach events

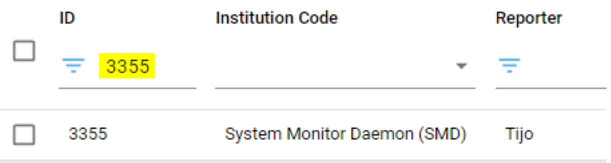
Please, enter investigation case ID

Investigation case ID: 1234

How do I find specific investigation **cases?**

1. On the **CRM > Investigation case** page, at the top of each column, type or copy/paste the values you want to find.

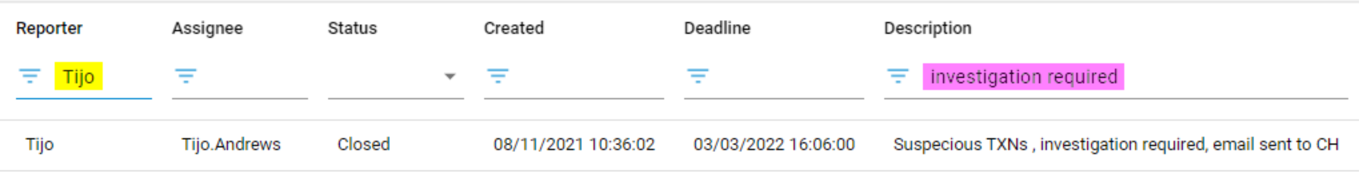
   For example, if you know the Case ID you are looking for, input its value to the right of ≡ :



□	ID	Institution Code	Reporter
	3355		
□	3355	System Monitor Daemon (SMD)	Tijo

Multiple quick filter options can be used simultaneously by inputting the appropriate values to the right of ≡ in the corresponding columns.

For example, if you do not know the Case ID number but you remember you opened the case (you were the reporter) and you mentioned in the description that further investigation is required (for example, *Case ID* = 3355 AND *Description* = %investigation required%):

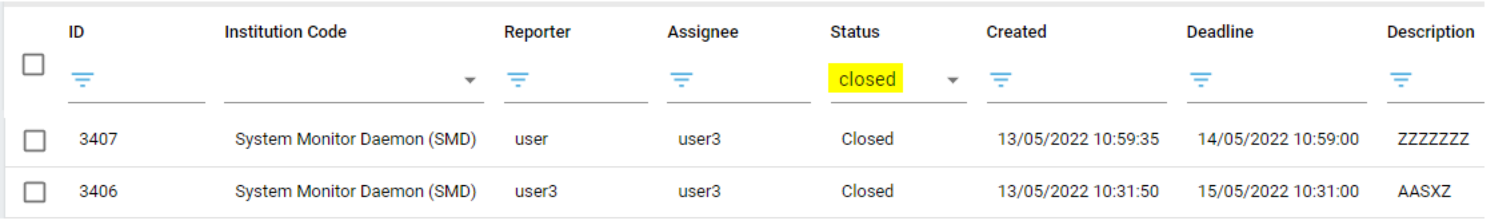


Reporter	Assignee	Status	Created	Deadline	Description
Tijo					investigation required
Tijo	Tijo.Andrews	Closed	08/11/2021 10:36:02	03/03/2022 16:06:00	Suspecious TXNs , investigation required, email sent to CH

How do I export cases?

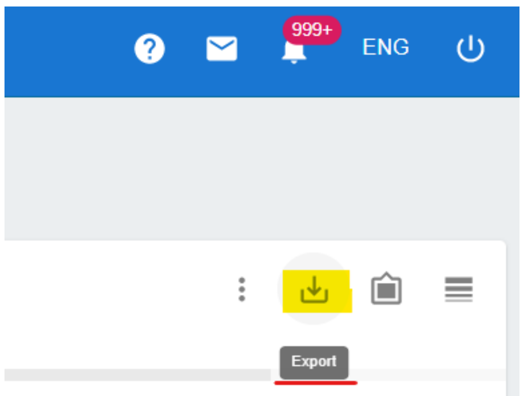
1. Using the **CRM > Investigation case** page, you can export all cases (the default) or select particular cases to export.

   For example, to export only closed cases, you can apply a filter or a quick filter *Status* = closed.

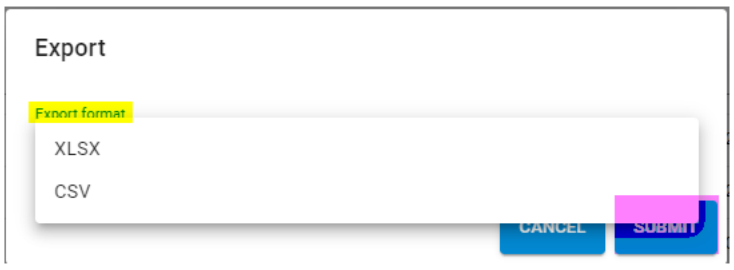


☐	ID	Institution Code	Reporter	Assignee	Status	Created	Deadline	Description
					closed			
☐	3407	System Monitor Daemon (SMD)	user	user3	Closed	13/05/2022 10:59:35	14/05/2022 10:59:00	ZZZZZZZ
☐	3406	System Monitor Daemon (SMD)	user3	user3	Closed	13/05/2022 10:31:50	15/05/2022 10:31:00	AASXZ

2. After the cases that meet your requirements appear, click **Export** in the top-right corner:



3. A pop-up appears. Select the Export format (**XLSX** or **CSV**) and click **SUBMIT**:

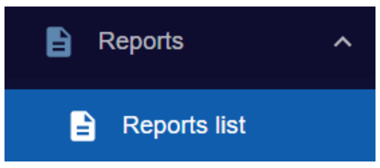


The selected file format containing all the cases is exported and saved to your workstation/local drive.

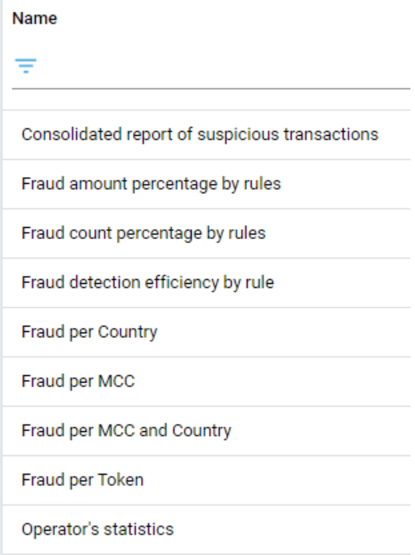
Reporting

How do I generate reports?

1. Navigate to **Reports > Reports list** (note that only users with *Manager* access can generate reports):

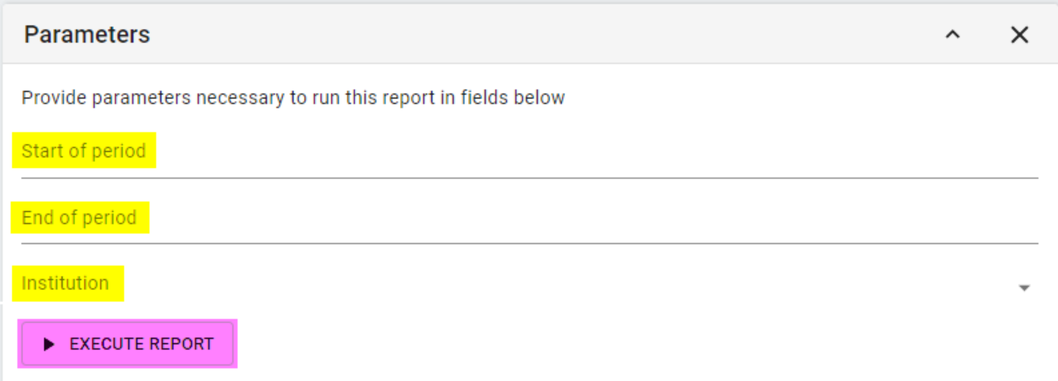


2. Select a report from the list:



Name
Consolidated report of suspicious transactions
Fraud amount percentage by rules
Fraud count percentage by rules
Fraud detection efficiency by rule
Fraud per Country
Fraud per MCC
Fraud per MCC and Country
Fraud per Token
Operator's statistics

3. Input all the requested parameters (*Start of period*, *End of period*, *Institution* etc.) and click **EXECUTE REPORT**:



Parameters

Provide parameters necessary to run this report in fields below

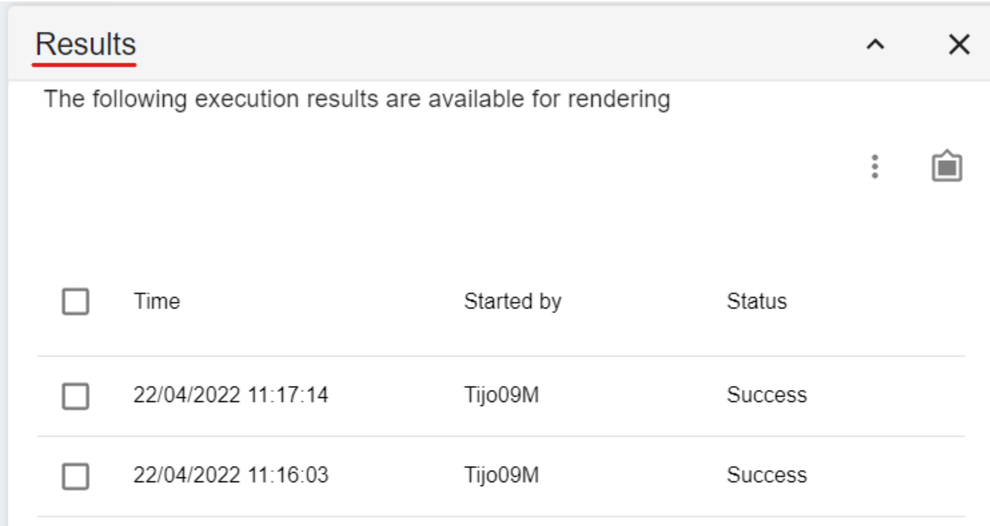
Start of period

End of period

Institution

After the report is generated, you can view it on the **Results** pane.

> **Tip:** If the report takes time to generate, try refreshing your browser page.

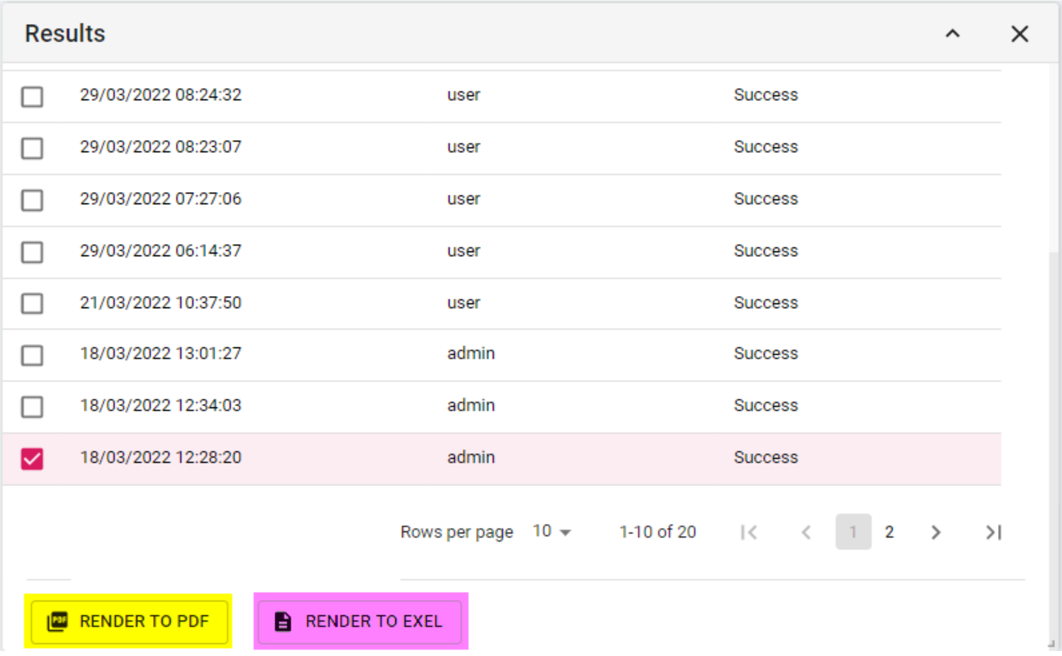


Results

The following execution results are available for rendering

□	Time	Started by	Status
□	22/04/2022 11:17:14	Tijo09M	Success
□	22/04/2022 11:16:03	Tijo09M	Success

4. Choose the generated report by selecting the checkbox next to it and, depending on the exported format, click either **RENDER TO PDF** or **RENDER TO EXCEL**:



□	29/03/2022 08:24:32	user	Success
□	29/03/2022 08:23:07	user	Success
□	29/03/2022 07:27:06	user	Success
□	29/03/2022 06:14:37	user	Success
□	21/03/2022 10:37:50	user	Success
□	18/03/2022 13:01:27	admin	Success
□	18/03/2022 12:34:03	admin	Success
☑	18/03/2022 12:28:20	admin	Success

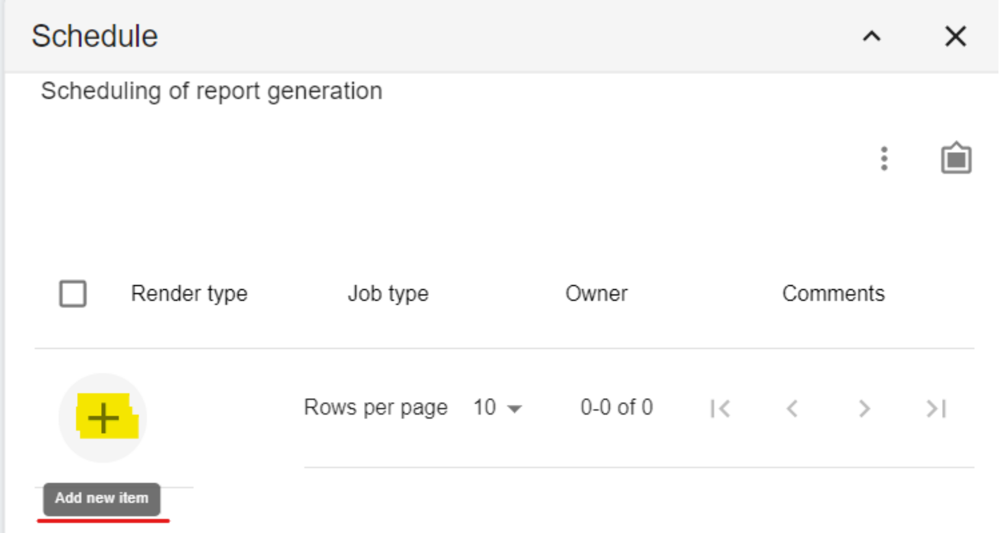
Rows per page 10 1-10 of 20 1 2

The selected file format containing the report is exported and saved to your workstation/local drive.

How do I generate reports on a scheduled basis?

Reports can be generated automatically by the system with a predefined frequency.

1. Navigate to **Reports > Reports list** (note that only users with *Manager* access can generate reports) and click on a report.
2. On the **Schedule** pane, click + **Add new item**:

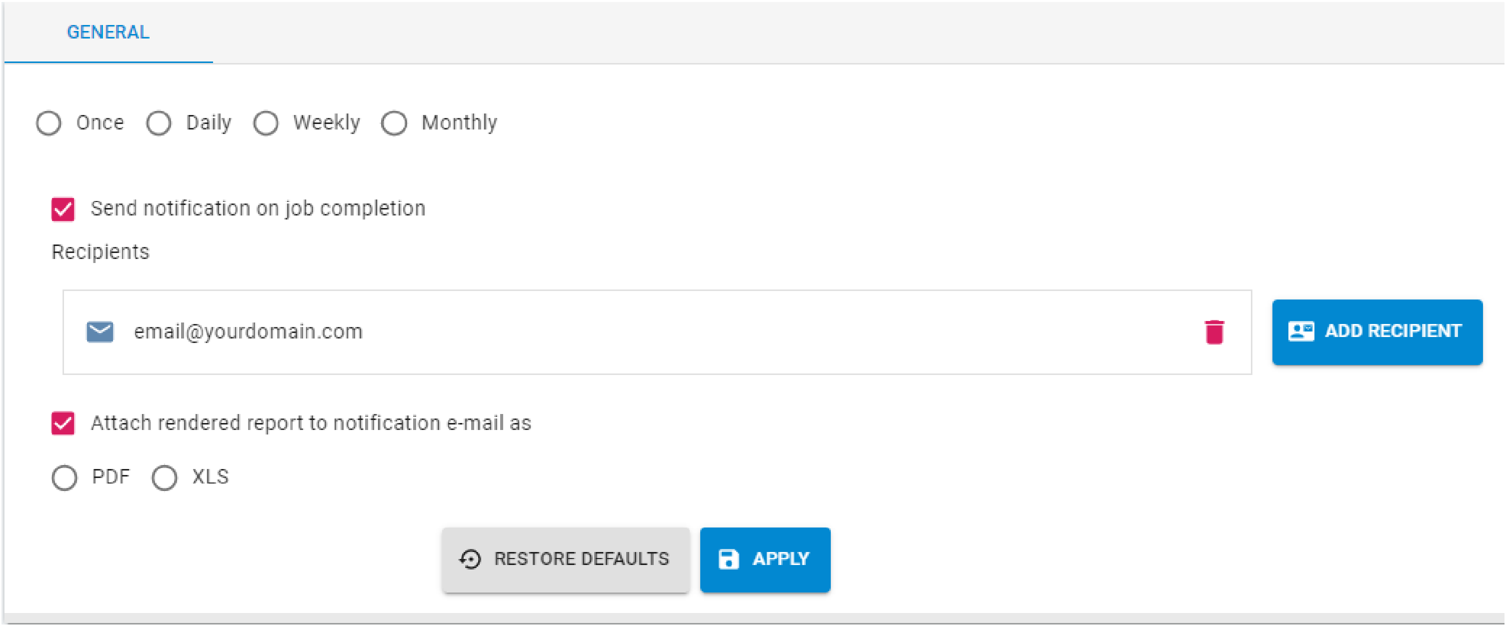


Scheduling of report generation

□	Render type	Job type	Owner	Comments

Rows per page 10 0-0 of 0

3. In the window that appears, input the requested information:



○ Once ○ Daily ○ Weekly ○ Monthly

☑ Send notification on job completion

Recipients

email@yourdomain.com

☑ Attach rendered report to notification e-mail as

○ PDF ○ XLS

- Choose the frequency: **Once**, **Daily**, **Weekly**, or **Monthly**
- **Send notification on job completion** (if selected, an email confirmation is sent to the provided recipient(s) to notify them the report has been generated as scheduled)

- **Recipients**: input the email address(es) of the recipient(s)
- **Attach rendered report to notification e-mail as** (if selected, the report is attached to the email sent to the recipient(s))

4. Click **APPLY** to save the scheduled report generation job.

Glossary

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

A

Acquirer

The merchant acquirer or bank that offers the merchant a trading account, to enable the merchant to take payments in store or online from cardholders.

Authorisation

Stage where a merchant requests approval for a card payment by sending a request to the card issuer to check that the card is valid, and that the requested authorisation amount is available on the card. At this stage the funds are not deducted from the card.

C

Card Scheme

Card network, such as MasterCard or Visa, responsible for managing transactions over the network and for arbitration of any disputes.

F

Filter

See Rule condition

I

Issuer

The card issuer, typically a financial organisation authorised to issue cards. The issuer has a direct relationship with the relevant card scheme.

M

MCC

Merchant Category Code

Merchant

The shop or store providing a product or service that the cardholder is purchasing. A merchant must have a merchant account, provided by their acquirer, in order to trade. Physical stores use a terminal or card reader to request authorisation for transactions. Online sites provide an online shopping basket and use a payment service provider to process their payments.

P

Program Manager

A Thredd customer who manages a card program. The program manager can create branded cards, load funds and provide other card or banking services to their end customers.

R

Rule

Conditions (described as logical expressions) through which transaction verification happens. Rules are tailored to your institution.

Rule condition

A rule condition (also called a filter) is a logical expression used by Thredd Protect to determine whether transactions meet the eligibility criteria for triggering an action such as an alert.

S

sFTP

Secure File Transfer Protocol. File Transfer Protocol FTP) is a popular unencrypted method of transferring files between two remote systems. SFTP (SSH File Transfer Protocol, or Secure File Transfer Protocol) is a separate protocol packaged with SSH that works in a similar way but over a secure connection.

Smart Client

Smart Client is Thredd's user interface for managing your account on the Thredd Apex system. It is also called Smart Processor Thredd. 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.

SSL Certification

An SSL certificate displays important information for verifying the owner of a website and encrypting web traffic with SSL/TLS, including the public key, the issuer of the certificate, and the associated subdomains.

Stand In Processing (STIP)

The card network (Visa and Mastercard) may perform approve or decline a transaction authorisation request on behalf of the card issuer. Depending on your Thredd mode, Thredd may also provide STIP on your behalf, where your systems are unavailable.

T

Thredd Apex platform

A comprehensive, robust and reliable solution for card payment processing which is integrated within the global payment network.

Thredd Protect

A bespoke fraud protection programme designed to guard financial institutions and cardholders from fraudulent activity.

Token

Tokenisation is a security technology which replaces the sensitive 16-digit permanent account number (PAN) that is typically embossed on a physical card with a unique payment token (a digital PAN or DPAN) that can be used in payments and prevents the need to expose or store actual card details.

W

Widgets

UI components that appear on screen showing tables, statistical graphs, cases, events etc. You can tailor your dashboard by choosing the widgets you want to display.

Document History

This section provides details of what has changed since the previous document release.

Version	Date	Description	Revised by
2.3	07/06/2023	Updated Operations email address to be occ@thredd.com	MW
	15/05/2023	Updated the Fraud Team email address in FAQs and Troubleshooting and Understanding the Thredd Protect Display.	MW
	27/04/2023	Guide rebrand to new company name and brand identity.	JB
2.2	21/12/2022	Updating the numbering in the Table of Contents	MW
	01/12/2022	Updated the Copyright Statement.	MW
2.1	01/11/2022 11/11/2022	New guide layout and HTML version now available. Updates to screenshots for latest release, Updates to table layouts in Appendix A.	PC, PM, AL & WS
2.0	30/05/2022	Major upgrade to v6.0.8 for a new Web interface	PM & AL
1.6	15/06/2021	Sub-chapter on Rule Actions added. Other minor updates throughout the text	PM
1.5	11/05/2020	Major upgrade to v5.1.7 with a redesigned interface	PM
1.4	04/04/2019	Updates to the server IP address and other minor updates/revisions	PM
1.3	01/02/2019	Wording changes	PM
1.2	27/09/2018	Re-wording, additional diagrams and explanation of terms	PM

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: +442037409682

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.