

GPS Protect User Guide

Version: 2.0
30 May 2022

Global Processing Services Ltd.
6th Floor, Victoria House, Bloomsbury Square, London, WC1B 4DA
Support Email: ops24@globalprocessing.com
Support Phone: +442037409682
Documentation queries: docs@globalprocessing.com

Publication number: GPSP-2.0-30.05.2022

Copyright

(c) 2022. Global Processing Services All Rights Reserved.

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

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

To the maximum extent permitted by law, Global Processing Services 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 Global Processing Services Ltd. assumes no responsibility for any errors.

Contents

Contents	3
1. About this Document	6
1.1. Related Documents.....	6
1.2. How to Use this Guide	6
2. Overview of GPS Protect	7
2.1. How does GPS Protect work?.....	7
3. Getting Started with GPS Protect	8
4. Accessing GPS Protect	9
4.1. Accessing GPS Protect	9
5. Understanding the GPS Protect Display	10
5.1. About the Toolbar.....	11
5.2. Using the Menus.....	11
5.2.1. Viewing your User Profile.....	12
5.2.2. Changing the display.....	13
5.2.3. About the menu options.....	13
5.3. About the Dashboard.....	14
5.3.1. Managing widgets.....	14
6. Transaction Monitoring	16
6.1. Using the Transaction Functions.....	16
6.2. About the Contextual Menu.....	17
6.3. Filtering the Data.....	18
6.4. Checking Transaction Details	19
6.5. Understanding the Monitoring Screens.....	20
6.5.1. Viewing all events/transactions.....	20
6.5.2. Viewing system marked events/transactions.....	21
6.5.3. Viewing suspicious events/transactions	21
6.5.4. Viewing operator-marked events/transactions.....	22
7. Managing Cases for Investigation	24
7.1. Opening a Case.....	24

7.2. Managing Cases.....	26
8. Using the Rule Manager	28
8.1. Viewing Rules	28
8.2. Understanding Rule Conditions and Groups	29
8.2.1. About condition groups.....	29
8.3. Configuring Rules	30
8.3.1. Adding a new group of conditions.....	30
8.3.2. Deleting a group and/or condition	31
8.3.3. Updating a rule.....	31
8.4. About Rule Actions.....	31
8.5. Creating a Whitelist for Specific Rules	34
9. Using Datasets.....	36
9.1. Creating a Dataset.....	36
9.2. Updating an Existing Dataset.....	36
10. Configuring Statistical Parameters.....	39
10.1. Displaying Statistical Parameters	39
10.2. Creating Statistical Parameters	39
10.3. Updating Statistical Parameters.....	40
11. Generating Reports.....	42
11.1. Displaying Available Reports	42
11.2. Running a Report.....	42
11.2.1. Saving a Report.....	43
11.2.2. Scheduling a Report	44
12. User Access Management.....	46
12.1. Requesting Changes to User Access.....	46
FAQs and Troubleshooting	48
Setup	48
Monitoring.....	48
Investigating.....	54
Reporting.....	58
Appendix A — Common Codes	61

Message type (MTID).....	61
Processing code (Txn code).....	61
Response status	61
POS (Point of Sale) data code starting with:	62
Example:	63
Card status code.....	63
Document History.....	64
Glossary	65

1. About this Document

This guide explains how to use the GPS Protect portal to help protect your organisation and your cardholders from fraudulent activity. It describes the GPS 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 GPS 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.

1.1. Related Documents

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

Document	Description
<i>Smart Client Guide</i>	How to use Smart Client, which is an administration application that can be used to view and manage cards and transactions in your program.
<i>Cardinal 3D Secure User Guide</i>	Specification and 3D secure configuration rules when using the Cardinal Portal to set up the rules and policies for your program.
<i>GPS Protect Release Notes</i>	Describes the new features and enhancements to existing features available in the latest GPS Protect release.

1.2. How to Use this Guide

If you are new to GPS Protect and want to understand how you can use it to guard against fraudulent activity, begin by reading the following topics: [Overview of GPS Protect](#), [Getting Started with GPS Protect](#), and [Understanding the GPS Protect Display](#).

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

2. Overview of GPS Protect

This topic introduces GPS 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.

GPS 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, GPS 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, GPS helps you to configure and control rules designed to protect your card programme.

2.1. How does GPS Protect work?

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

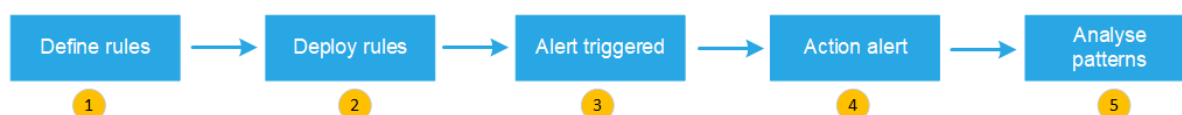


Figure: How GPS Protect prevents fraud

Each step is explained in more detail below:

1. **Define rules** — GPS 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 GPS 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** — GPS 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.

3. Getting Started with GPS Protect

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

Step 1 – Access GPS Protect

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

Step 2 – Familiarise yourself with the User Interface

Before you begin, learn how to use the GPS Protect toolbar, menu options and dashboard — see [Understanding the GPS Protect Display](#).

GPS 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 GPS 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

GPS 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 GPS Protect Rules

GPS Protect checks all data from the GPS 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](#).

4. Accessing GPS Protect

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

4.1. Accessing GPS Protect

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

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

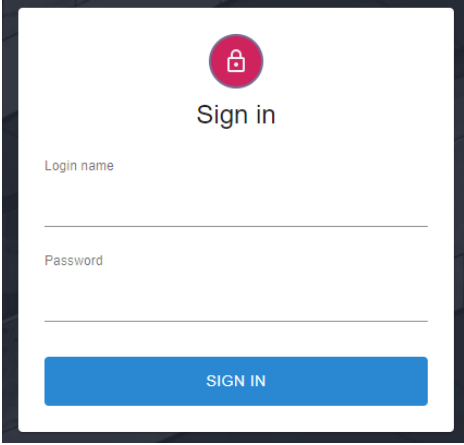


Figure: GPS Protect Sign-In Screen

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

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

Every GPS 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 GPS Protect.

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

5. Understanding the GPS Protect Display

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

Note: Different levels of user access can be configured on the GPS 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](#).

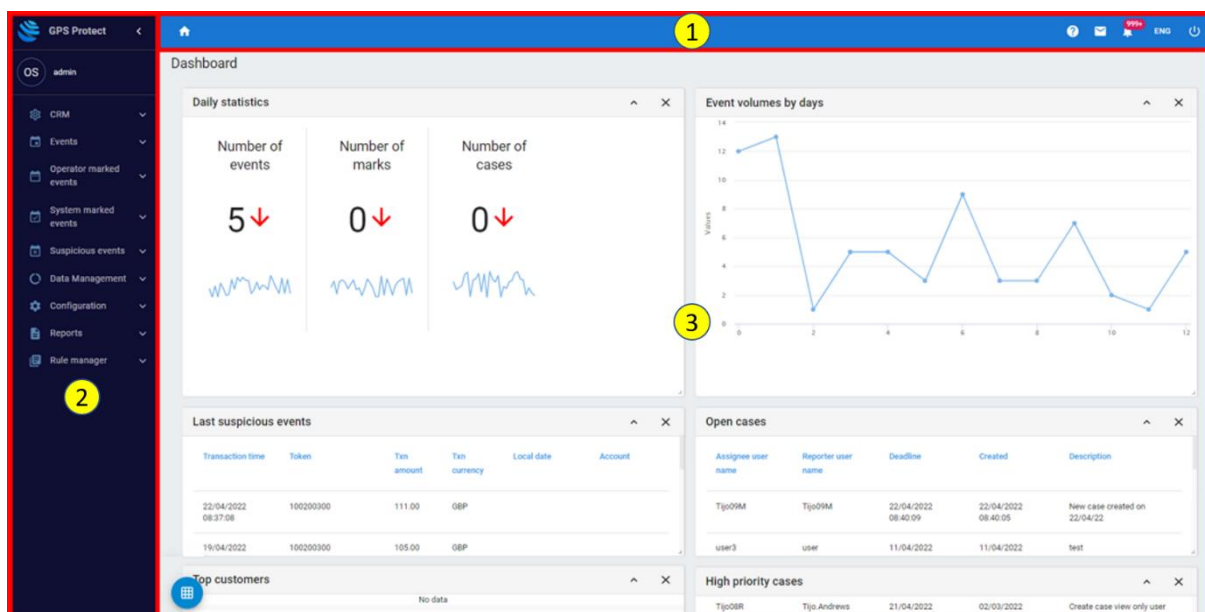


Figure: The main GPS Protect screen






The main interface is divided into three main sections:

- 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 GPS 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.

5.1. About the Toolbar

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

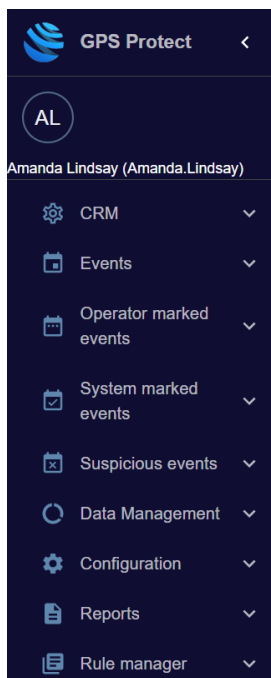
	Home	Click Home in the top-left of the toolbar to return to the dashboard home screen.
	Help	Click Help in the top-right of the screen to open the Help interface.
	Assigned cases	Click Assigned cases to show all the cases currently under investigation.
	Notifications	Click Notifications to open the System 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 GPS Protect.

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

5.2. Using 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 GPS Protect functions and screens



The available menu options are described in more detail below.

5.2.1. 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:

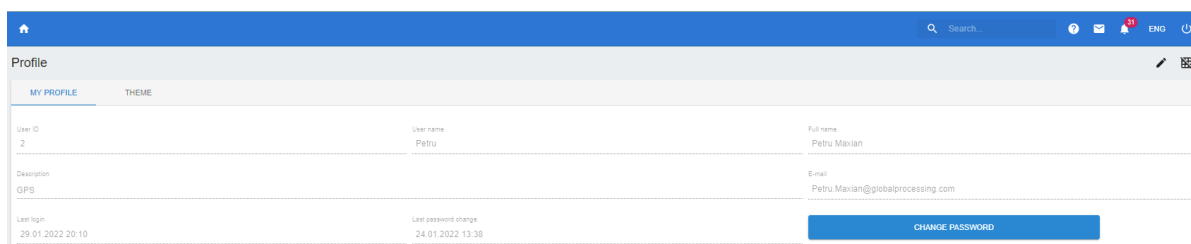


Figure: The GPS Protect User Profile screen

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)

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 GPS Protect account and need to reset your password, contact GPS by raising a [GPS JIRA](#) or via email by sending a password reset request to **FraudTeam@globalprocessing.com**

5.2.2. Changing the display

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

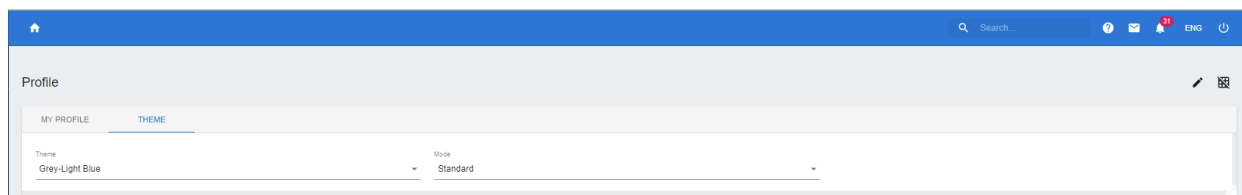


Figure: The Theme tab for changing the appearance of the display

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:



5.2.3. 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 GPS Protect access within your organisation.

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

5.3. 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.

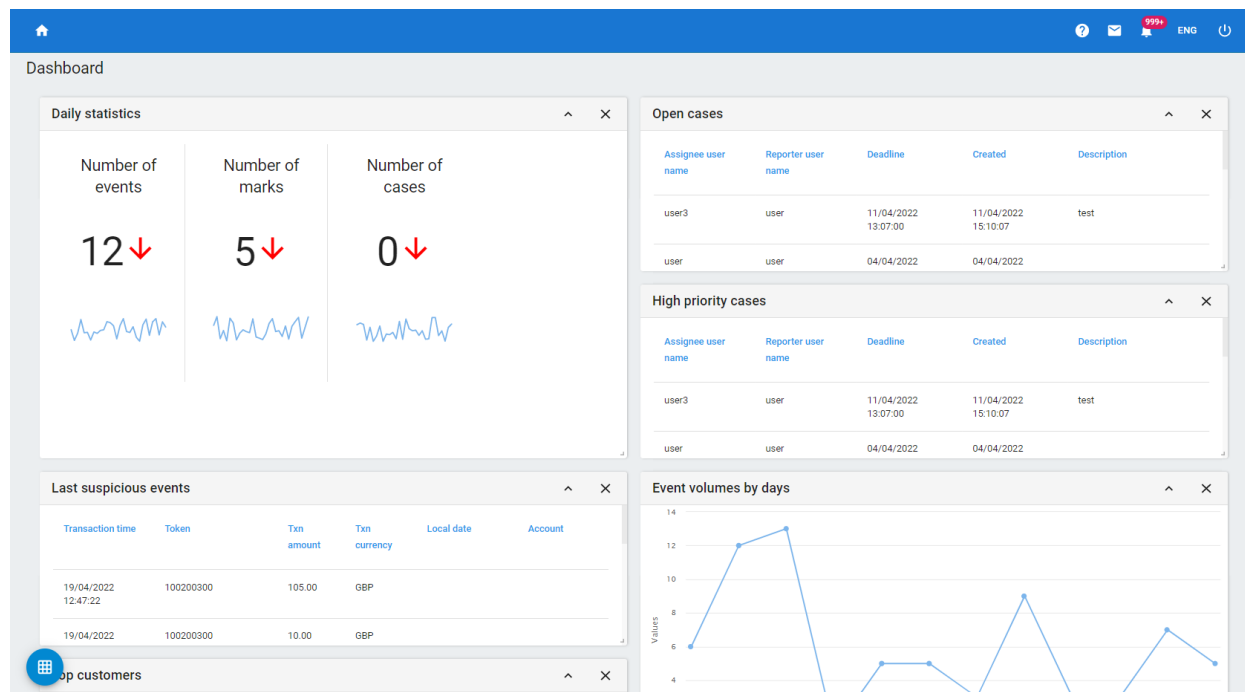

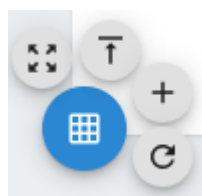


Figure: A typical dashboard display

- **Daily statistics** – shows statistics for the current day, including the number of processed events, the number of events/transactions that generated marks/alarms by the rules, and the number of new open cases.
- **Open cases** – shows all open unresolved cases.
- **High priority cases** – shows high-priority investigation cases assigned to a user.
- **Event volumes by days** – displays a historical graph showing the number of events in the last 30 days.
- **Last suspicious events** – shows a list of the last events marked as suspicious.
- **Top customers** – ignore as not used by GPS.
- **Last fraudulent events** – shows a list of the last events marked as fraudulent.

5.3.1. Managing widgets

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



The following explains the contextual buttons, clockwise:



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:

- ☐ Event volumes by days
- ☒ Top customers
- ☒ Daily statistics
- ☒ High priority cases
- ☒ Open cases
- ☒ Last suspicious events
- ☒ Last fraudulent events



Reset

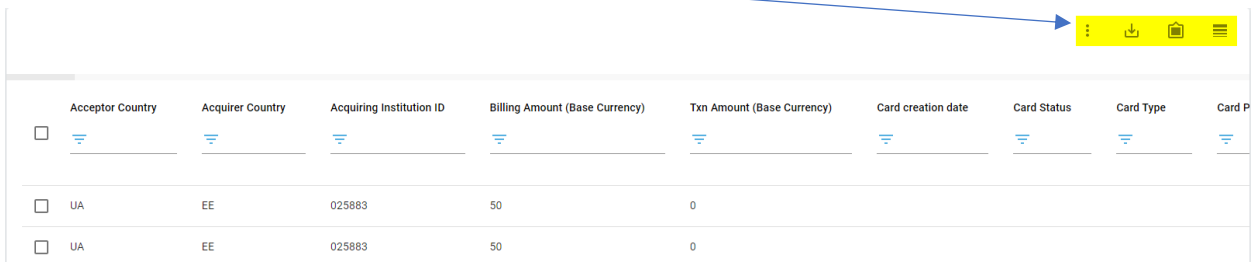
Restore all the widgets to their original/default position and size on the Dashboard.

6. 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.





6.1. Using the Transaction Functions

All transaction monitoring screens have the following common functions in the top right of the display:

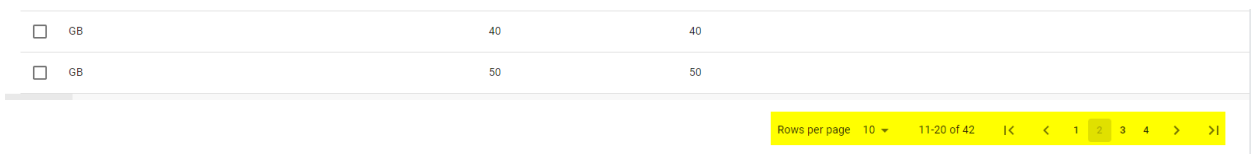


	Acceptor Country	Acquirer Country	Acquiring Institution ID	Billing Amount (Base Currency)	Txn Amount (Base Currency)	Card creation date	Card Status	Card Type	Card P
<input type="checkbox"/>	UA	EE	025883	50	0				
<input type="checkbox"/>	UA	EE	025883	50	0				

Figure: Common functions across the transaction screens

- 
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 table 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.
- 
Show filter Display the filters applied to the screen. You can add or remove filters after this icon is pressed.

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






<input type="checkbox"/>	GB		40	40
<input type="checkbox"/>	GB		50	50

Figure: Page navigation functions across the transaction screens

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


- > Next page** Use to load the next page.

-  **Previous page** Use to load the previous page.
-  **Last page** Use to load the last (final) page.
-  **First page** Use to load the first page.

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.

6.2. About the Contextual Menu

When one or more transactions are selected (by selecting the inline tick box ) , a contextual 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:

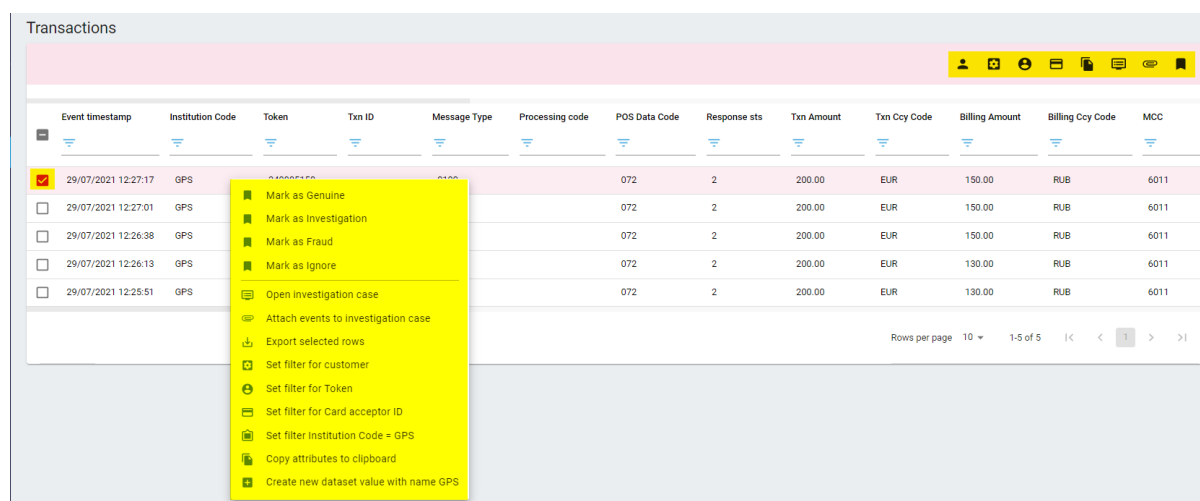















Figure: contextual menu functions in the transaction screens

These functions are explained below:

-  **Mark as Genuine** Assign a *Genuine* status to a transaction.
-  **Mark as Investigation** Assign an *Investigation* status to a transaction.
-  **Mark as Fraud** Assign a *Fraud* status to a transaction.
-  **Mark as Ignore** Assign an *Ignore* 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 for Card acceptor ID
Set a filter for the selected/related Card Acceptor ID number.
- 
Set filter Institution Code
Set a filter for the selected/related institution.
- 
Copy attributes to the clipboard
Copy the selected transaction's attributes/values pairs to the clipboard.
- 
Create new dataset value with name
Add the selected value to an existing dataset.

6.3. Filtering the Data

To retrieve transactional data for you institution, click on  **Show filters**, add the 3-digit **Institution Code** for your institution and click **Apply** to retrieve the filtered data.


In the following examples, transactions are filtered using:

- Merchants for which the Acceptor Country is Ukraine 'UA'
- Acquirer country is Estonia 'EE'
- Acquiring institution ID is 025883
- Billing amount (in the base currency of the card) is 50

☐ AND conditions, OR groups
 ☒ OR conditions, AND groups


Column	Operator	Attribute	✖	+	✖
Institution Code	Equal	GPS	✖	+	✖

 **APPLY**

	Acceptor Country	Acquirer Country	Acquiring Institution ID	Billing Amount (Base Currency)	Txn Amount (Base Currency)	Card creation date	Card Status	Card Type	Card Pr
<input type="checkbox"/>	UA	EE	025883	50	0				
<input type="checkbox"/>	UA	EE	025883	50	0				
<input type="checkbox"/>	MX			0	0				

Rows per page: 10 ▾ 1-3 of 3 |< < 1 > >|

Figure: Filtering data in the transaction screens

Further 'on-the-fly' data filtering is possible for each displayed column/attribute, by inputting a filtering value to the right of the  **Filter list** icon:

⋮ 📄 📁 ☰

☐ AND conditions, OR groups ☒ OR conditions, AND groups

Column
Operator
Attribute

Institution Code
Equal
GPS

🗑️ + 🗑️

+ APPLY

<input type="checkbox"/>	Acceptor Country	Acquirer Country	Acquiring Institution ID	Billing Amount (Base Currency)	Txn Amount (Base Currency)	Card creation date	Card Status	Card Type	Card Pr
<input type="checkbox"/>	UA	EE	025883	50	0				
<input type="checkbox"/>	UA	EE	025883	50	0				

Rows per page 10 ▾ 1-2 of 2 |< < 1 > >|

Figure: on-the-fly filtering in the transaction screens

6.4. 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 GPS by the Merchant/Acquirer via the Schemes such as Transaction Amount or Acceptor Country, as well as some GPS proprietary details like the GPS Product ID of the card on which the transaction was performed.

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

Figure: Transaction details

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

6.5. 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.

6.5.1. 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													
<div> <div>OS Petru Masian (Petru)</div> <div>CRM</div> <div>Investigation cases</div> <div>Events</div> <div>Transactions</div> <div>Operator marked events</div> <div>System marked events</div> <div>Suspicious events</div> <div>Data Management</div> </div>													
<div> <div>+</div> <div> <input type="radio"/> AND conditions, OR groups <input checked="" type="radio"/> OR conditions, AND groups </div> <div>APPLY</div> </div>													
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	
<input type="checkbox"/>													
<input type="checkbox"/> 31/01/2020 01:00:00	BKR	263459300	2150330034	0000	22		000	100.00	GBP	100.00	GBP		
<input type="checkbox"/> 31/01/2020 01:00:00	BKR	731687118	2150330035	0000	22		000	100.00	GBP	100.00	GBP		
<input type="checkbox"/> 31/01/2020 01:00:00	BKR	851109839	2150330031	0000	23		000	20.00	GBP	20.00	GBP		
<input type="checkbox"/> 31/01/2020 01:00:00	BKR	731687118	2150330037	0000	23		000	100.00	GBP	100.00	GBP		

Figure: Transactions screen

6.5.2. 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
<input checked="" type="checkbox"/>	02/02/2020 06:06:39	BKR	199885676	4989071072	0100	00	071
<input type="checkbox"/>	02/02/2020 02:22:39	BKR	200201121	4988254895	0100	01	051
<input type="checkbox"/>	02/02/2020 01:54:24	BKR	779495940	4987954477	0100	00	812
<input type="checkbox"/>	02/02/2020 00:51:37	BKR	872074565	4987444554	0100	00	051
<input type="checkbox"/>	02/02/2020 00:51:21	BKR	511763688	4987444044	0100	01	051
<input type="checkbox"/>	01/02/2020 23:26:05	BKR	779496855	4987243148	0100	00	072
<input type="checkbox"/>	01/02/2020 21:22:56	BKR	779496855	4986860876	0100	00	102

Figure: System marked events/System marked Transactions screen

6.5.3. 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 events Transactions							
	Event timestamp	Institution Code	Token	Txn ID	Message Type	Processing code	POS Data Code
<input type="checkbox"/>							
<input type="checkbox"/>	02/02/2020 01:54:24	BKR	779495940	4987954477	0100	00	812
<input type="checkbox"/>	02/02/2020 00:51:37	BKR	872074565	4987444554	0100	00	051
<input type="checkbox"/>	01/02/2020 23:26:05	BKR	779496855	4987243148	0100	00	072
<input type="checkbox"/>	01/02/2020 21:22:56	BKR	779496855	4986860876	0100	00	102
<input type="checkbox"/>	01/02/2020 19:02:25	BKR	872074565	4986069243	0100	00	102
<input type="checkbox"/>	01/02/2020 16:49:52	BKR	196945945	4985216955	0100	00	051
<input type="checkbox"/>	01/02/2020 16:36:20	BKR	196945945	4985105068	0100	00	071
<input type="checkbox"/>	01/02/2020 16:35:42	BKR	196945945	4985101747	0100	00	051
<input type="checkbox"/>	01/02/2020 16:32:15	BKR	196945945	4985083445	0100	00	071
<input type="checkbox"/>	01/02/2020 16:30:32	BKR	196945945	4985073990	0100	00	051

Figure: Suspicious events/Suspicious Transactions screen

Because this screen displays all the alerts automatically triggered by the system, GPS 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.

6.5.4. Viewing operator-marked events/transactions

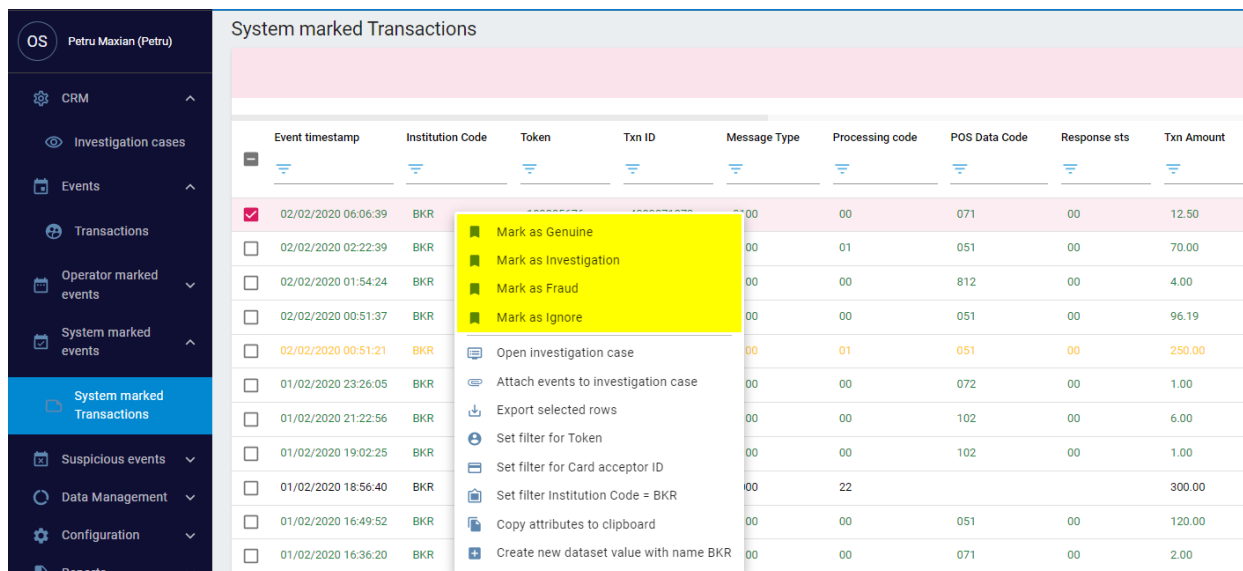
The **Operator marked events/Transactions** screen displays all the transactions that are manually marked and commented on by a user.

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:



Event timestamp	Institution Code	Token	Txn ID	Message Type	Processing code	POS Data Code	Response sts	Txn Amount
02/02/2020 06:06:39	BKR				00	071	00	12.50
02/02/2020 02:22:39	BKR				01	051	00	70.00
02/02/2020 01:54:24	BKR				00	812	00	4.00
02/02/2020 00:51:37	BKR				00	051	00	96.19
02/02/2020 00:51:21	BKR				01	051	00	250.00
01/02/2020 23:26:05	BKR				00	072	00	1.00
01/02/2020 21:22:56	BKR				00	102	00	6.00
01/02/2020 19:02:25	BKR				00	102	00	1.00
01/02/2020 18:56:40	BKR				22			300.00
01/02/2020 16:49:52	BKR				00	051	00	120.00
01/02/2020 16:36:20	BKR				00	071	00	2.00

Figure: Assigning a status to an alert

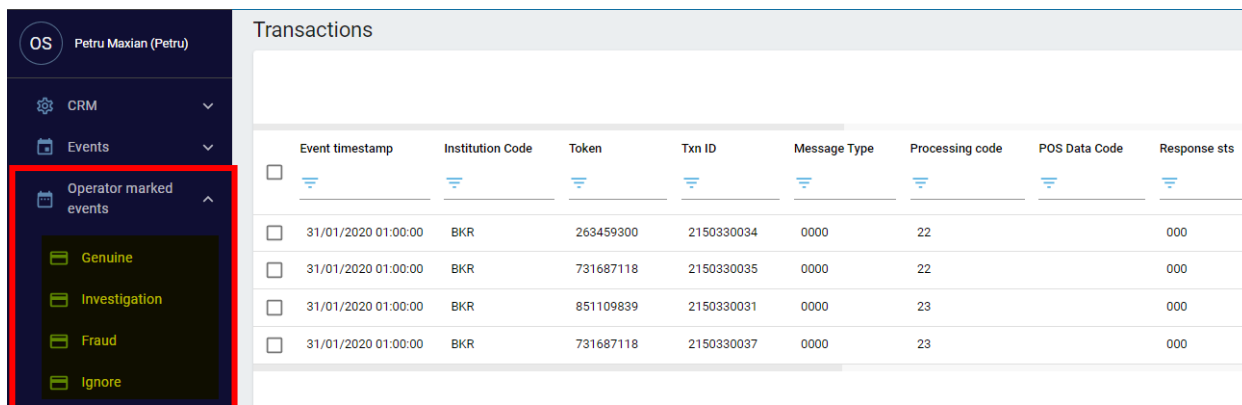
By default, new and unmarked transactions are displayed by the system in **Green**. When a transaction is marked, or its default status is changed, the colour of the event/transaction changes, depending on the newly assigned status.

Transaction colour coding

Status	Colour
Default, new and unmarked	Green
Genuine	Black

Status	Colour
<i>Investigation</i>	Orange
<i>Fraud</i>	Red
<i>Ignore</i>	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 market events)

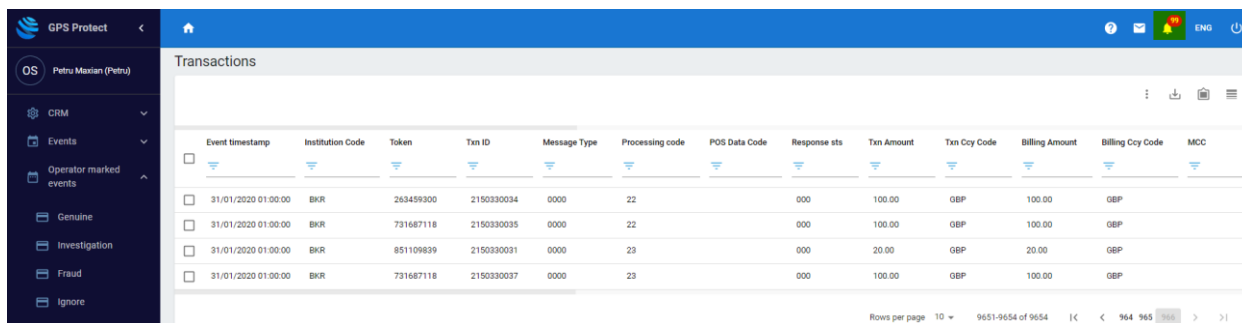


The screenshot shows the GPS Protect interface. On the left, the 'Operator marked events' menu is expanded, showing options: Genuine, Investigation, Fraud, and Ignore. The 'Investigation' option is highlighted. The main area displays a table of transactions with the following columns: Event timestamp, Institution Code, Token, Txn ID, Message Type, Processing code, POS Data Code, and Response sts.

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: 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.



The screenshot shows the GPS Protect interface. On the left, the 'Operator marked events' menu is expanded, showing options: Genuine, Investigation, Fraud, and Ignore. The 'Investigation' option is highlighted. The main area displays a table of transactions with the following columns: 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, and MCC.

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	

At the bottom right, there is a pagination bar showing 'Rows per page 10', '9651-9654 of 9654', and a counter '964 965 966'.

Figure: Alert counter

7. 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.

GPS 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)

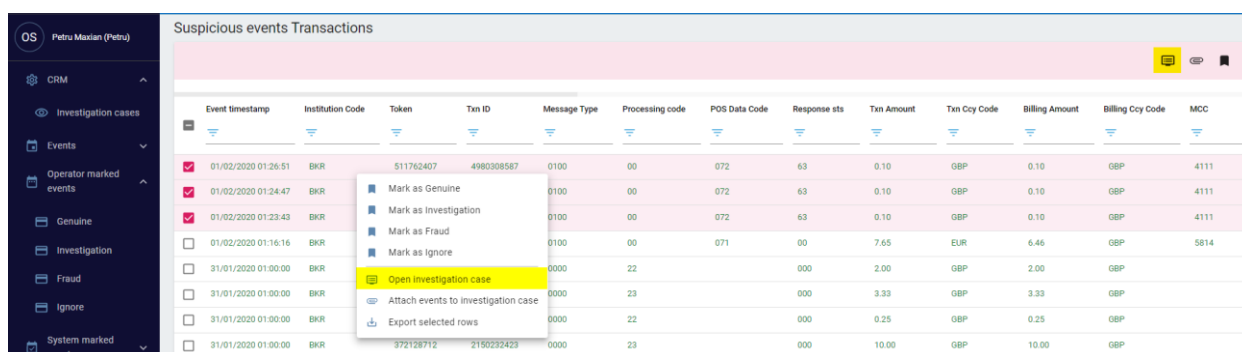
Note: Depending on access rights, some functions are available only to users with the correct permissions (for example, the ability to view all open cases and manage cases). See [User Access Management](#) for further information.

7.1. Opening a Case

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

To open a case:

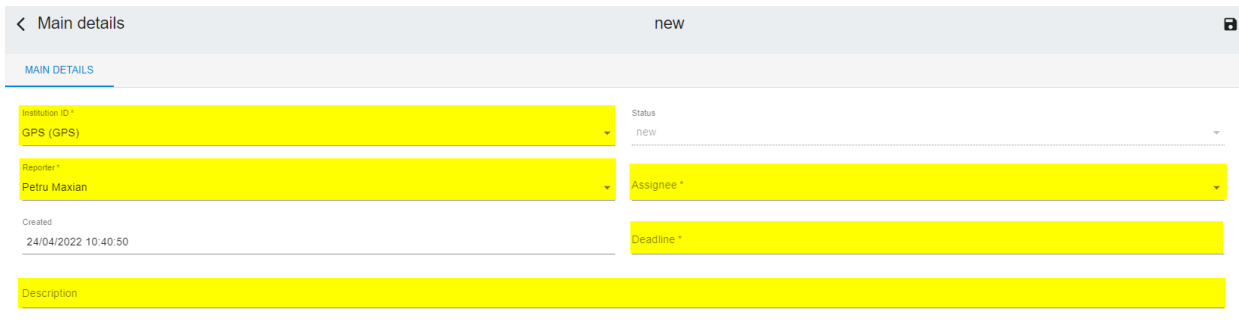
1. Select the appropriate events or transactions you want to include and click on  **Open investigation case** in the right-click menu or the contextual button in the top-right corner of the screen. The **Main details** screen appears.



	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
<input checked="" type="checkbox"/>	01/02/2020 01:26:51	BKR	511762407	4980308587	0100	00	072	63	0.10	GBP	0.10	GBP	4111
<input checked="" type="checkbox"/>	01/02/2020 01:24:47	BKR			0100	00	072	63	0.10	GBP	0.10	GBP	4111
<input checked="" type="checkbox"/>	01/02/2020 01:23:43	BKR			0100	00	072	63	0.10	GBP	0.10	GBP	4111
<input type="checkbox"/>	01/02/2020 01:16:16	BKR			0100	00	071	00	7.65	EUR	6.46	GBP	5814
<input type="checkbox"/>	31/01/2020 01:00:00	BKR			0000	22		000	2.00	GBP	2.00	GBP	
<input type="checkbox"/>	31/01/2020 01:00:00	BKR			0000	23		000	3.33	GBP	3.33	GBP	
<input type="checkbox"/>	31/01/2020 01:00:00	BKR			0000	22		000	0.25	GBP	0.25	GBP	
<input type="checkbox"/>	31/01/2020 01:00:00	BKR			0000	23		000	10.00	GBP	10.00	GBP	

Figure: Opening a case for investigation

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



The following table describes the required fields:

Field name	Description	Field type
Institution ID	The institution the case is opened for	Mandatory
Status	Prepopulated; always "New" during the case opening process	Prepopulated
Reporter	The user opening the case	Mandatory
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! Although not mandatory, GPS recommends you provide a description of why the case was created	Optional

Once a case deadline is reached, GPS 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.

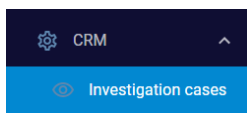
If one or more transactions need to be marked differently from others in a case, you can change their status manually after the case is closed.

7.2. 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:

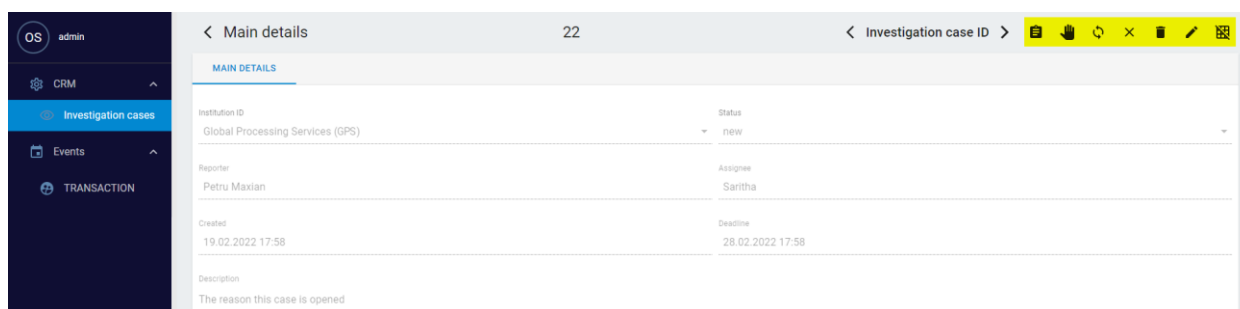









Figure: Options available for managing cases

These options are:

- | | | |
|---|--------------------|--|
|  | 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. |
|  | Delete | Delete a case that was opened by mistake. |
|  | 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:




< Main details
 22
 < Investigation case ID >

MAIN DETAILS

Institution ID	Status
Global Processing Services (GPS)	postponed
Reporter	Assignee
Petru Maxian	Saritha
Created	Deadline
19.02.2022 17:58	28.02.2022 17:58
Description	
The reason this case is opened	

MAIN DETAILS
 RELATED EVENTS
 CASE HISTORY
 RELATED COMMENTS AND TASKS

Figure: Additional options available for managing cases

- 
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.

8. Using the Rule Manager

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

All data from the GPS 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.

8.1. Viewing Rules

To see a list of current rules:

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

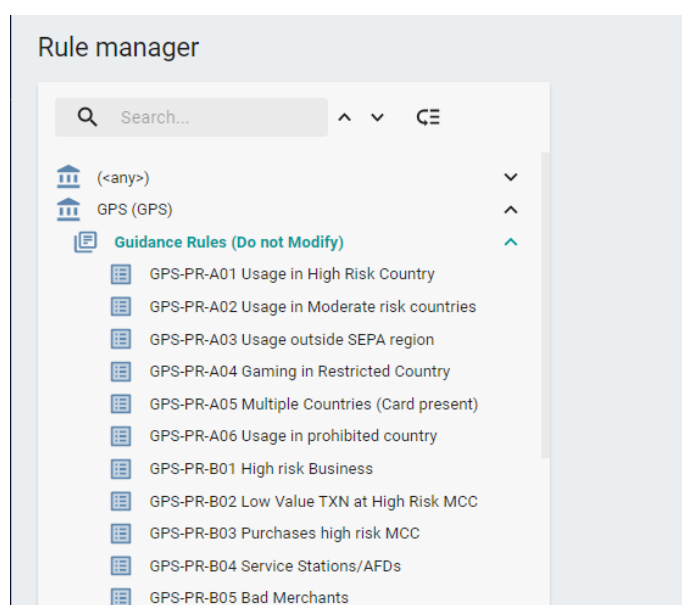


Figure: Rule Manager

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

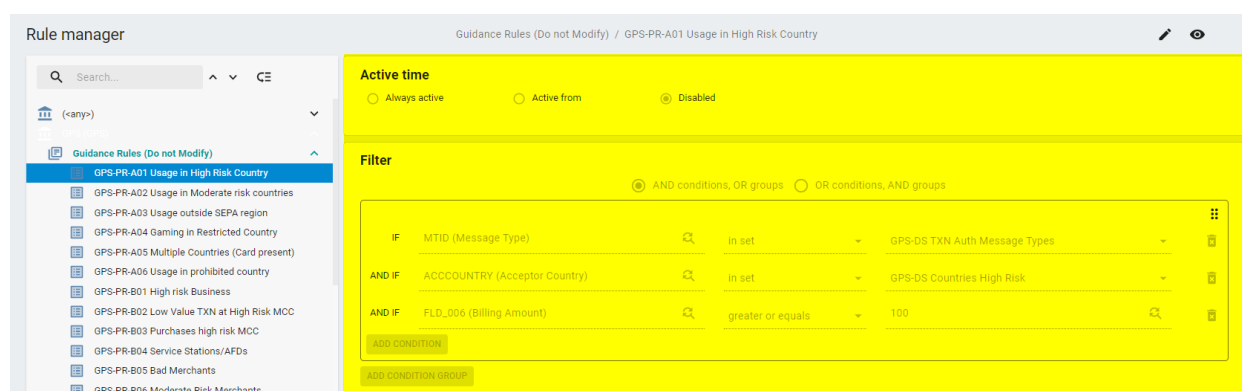


Figure: Displaying rule details

8.2. Understanding Rule Conditions and Groups

A rule condition (also called a filter) is a logical expression used by GPS 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, GPS 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](#).

8.2.1. 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: 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: Example showing OR conditions, AND groups

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

8.3. 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.


8.3.1. 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.





8.3.2. Deleting a group and/or condition

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

8.3.3. 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 GPS side. After the change request is captured on [GPS JIRA](#), GPS checks to ensure the requirements of the change match the actual configuration change before publishing the modifications in the production environment.

8.4. 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

ADD ACTION

Figure: Mark as suspicious rule action

Events marked as suspicious by the GPSProtect 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**

The colour of the event/transaction also changes; for more information, see: [Transaction colour coding](#).

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

Action
?

Action

Highlight

Color

Role

Everyone

ADD ACTION

Figure: 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):

<input type="checkbox"/>	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
<input checked="" type="checkbox"/>	17/03/2022 15:19:37	BKR	100200300	170320231	0100	00	051	101	100.00	GBP	100.00	GBP	5999

<input type="checkbox"/>	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
<input type="checkbox"/>	13/03/2022 19:16:57	CRV	5426460000006109545	291283434	1100	0	20010165	000	500.00	BYR	500.00	BYN	5411

Figure: 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:

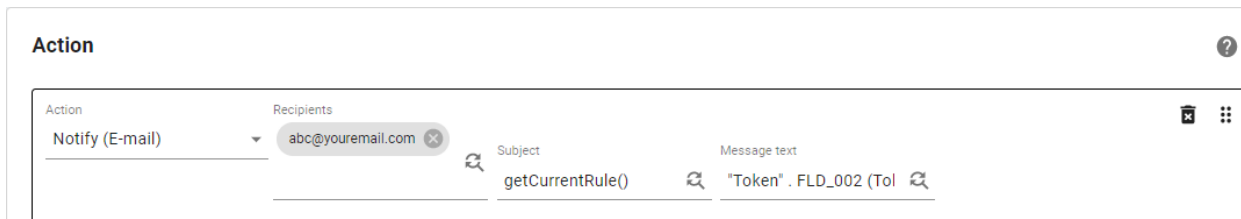





Figure: Configuring a notify action

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

GPS-PR-C03 Large Cash Withdrawal

 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: Example of an email notification from GPS Protect

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

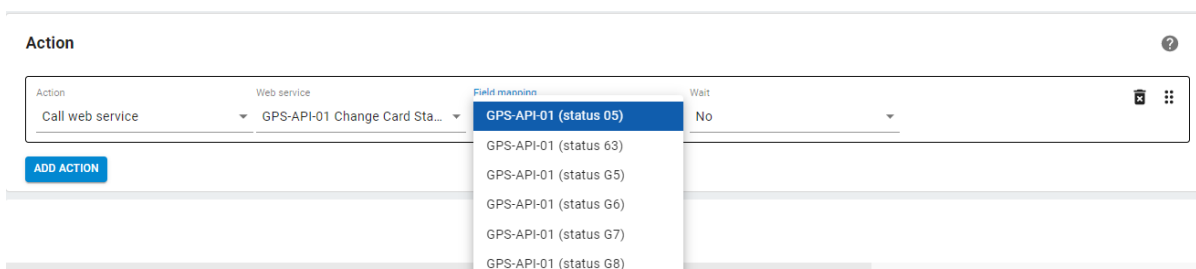
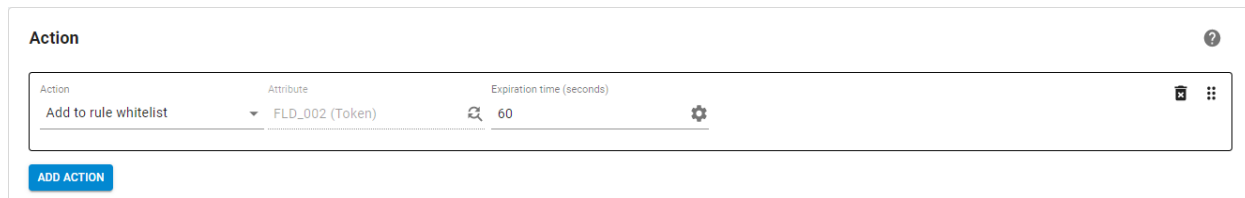


Figure: Configuring a Call web service action

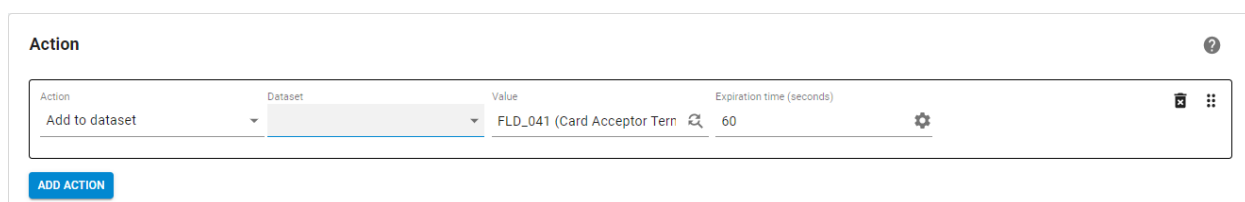
- **Add to rule whitelist:** This action adds an attribute to a rule's whitelist for a specific time period. In the example below, the *Attribute* Token will be whitelisted (in other words, excluded from the rule triggering) for a period of 60 seconds, as defined in the **Expiration time (seconds)**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



The screenshot shows a configuration form titled 'Action'. It has three main fields: 'Action' (set to 'Add to rule whitelist'), 'Attribute' (set to 'FLD_002 (Token)'), and 'Expiration time (seconds)' (set to '60'). There is a settings gear icon on the right. Below the form is a blue 'ADD ACTION' button.

Figure: Configuring an Add to rule whitelist action

- **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.



The screenshot shows a configuration form titled 'Action'. It has four main fields: 'Action' (set to 'Add to dataset'), 'Dataset' (a dropdown menu), 'Value' (set to 'FLD_041 (Card Acceptor Tern)'), and 'Expiration time (seconds)' (set to '60'). There is a settings gear icon on the right. Below the form is a blue 'ADD ACTION' button.

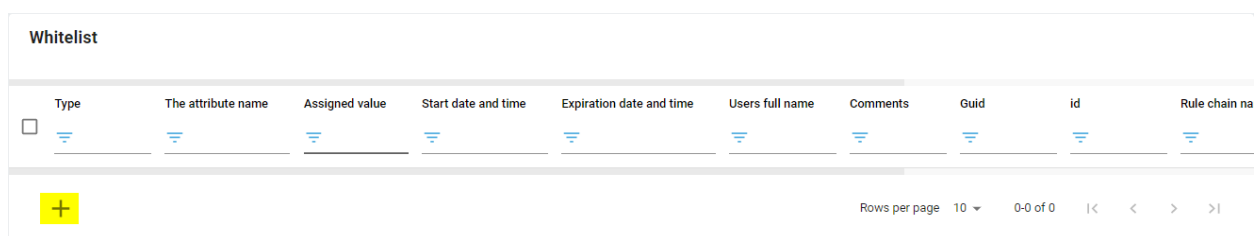
Figure: Configuring an Add to dataset action

8.5. Creating a Whitelist 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 whitelist (also known as an ‘allowed list’) is defined by the transaction attribute value and the **Expiration date and time** of the whitelisted attribute/record.


To add an attribute to a specific rule’s whitelist:

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



The screenshot shows a table titled 'Whitelist'. The table has columns: Type, The attribute name, Assigned value, Start date and time, Expiration date and time, Users full name, Comments, Guid, id, and Rule chain na. There is a checkbox in the first row. Below the table is a yellow button with a plus sign. At the bottom right, it says 'Rows per page 10 0-0 of 0' with navigation arrows.


Figure: Adding an attribute to a rule whitelist

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

Type	The attribute name	Assigned value	Start date and time	Expiration date and time	Users full name	Comments	Guid	id
<input checked="" type="checkbox"/> rules_whitelist	ACCCOUNTRY	UK	18/04/2022 22:11:48	19/04/2022 22:12:25	admin	Test	3935a356-aea4-464d-b7b8-2774cfbd0142	11

Rows per page: 10 0-0 of 0

Figure: Deleting a record from the whitelist

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

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 whitelist. The rule will then be ignored
- Only managers with the appropriate access rights can make changes to the rules and whitelists (see [User Access Management](#) for all available user access types)
- Over 50 different elements can be whitelisted. 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. GPS will review* the changes before publishing them in the Production environment
- If you're unsure how to build a rule for a specific scenario, raise a [GPS JIRA](#) ticket to get support

**While every endeavour will be employed to check the rule operates successfully, GPS 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.*

9. Using Datasets

This topic describes datasets and explains how to use them in GPS 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 GPS 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

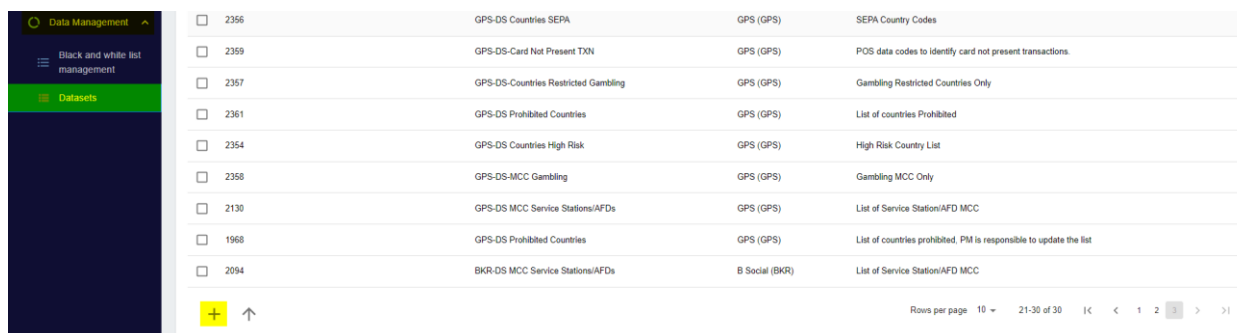
You want to create a rule in GPS Protect that will check all transactions performed in countries deemed to be high-risk. As part of this, you create a dataset containing a list of ISO-2 values for these high-risk countries and use this dataset in the rule. The system will check the ISO-2 values in the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

Tip! For a list of ISO country codes, see: [ISO - ISO 3166 — Country Codes](#).

9.1. Creating a Dataset

To create a new dataset:

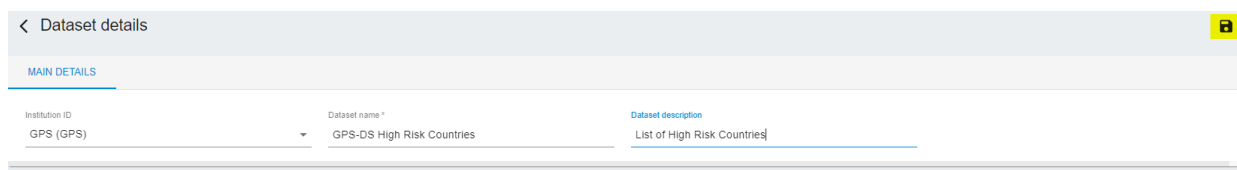
1. Go to **Data Management > Datasets** and click on **+ Add new item** on the bottom-left of the screen.



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

Figure: 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.



< Dataset details

MAIN DETAILS

Institution ID: GPS (GPS)

Dataset name: GPS-DS High Risk Countries

Dataset description: List of High Risk Countries

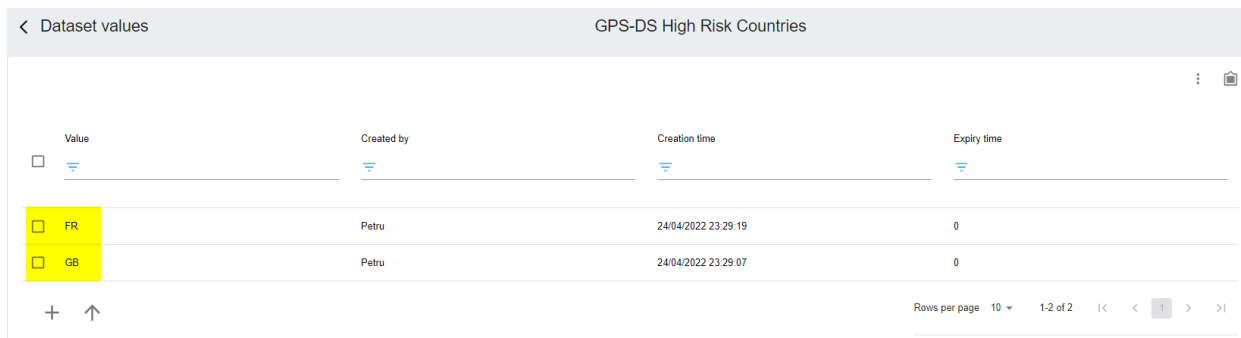
Figure: Dataset details

9.2. 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:

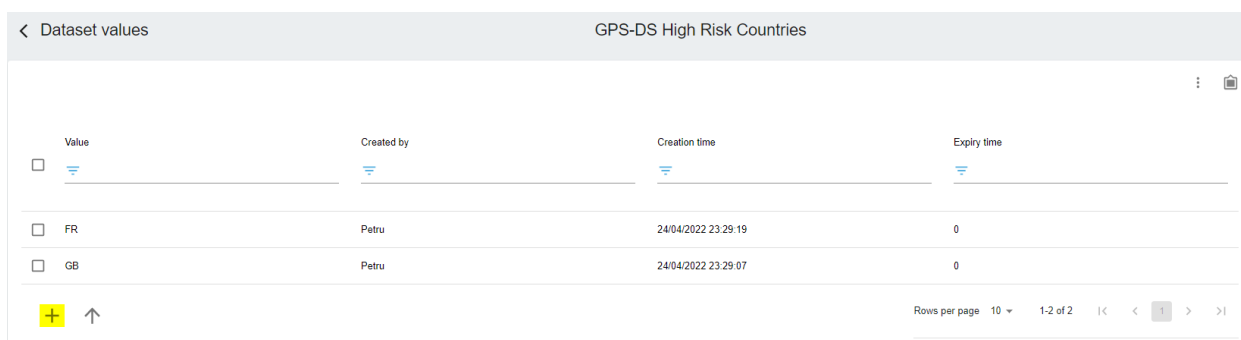
1. Go to **Data Management > Datasets** and select the dataset you want to edit. The existing values are displayed.



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: Editing an existing dataset

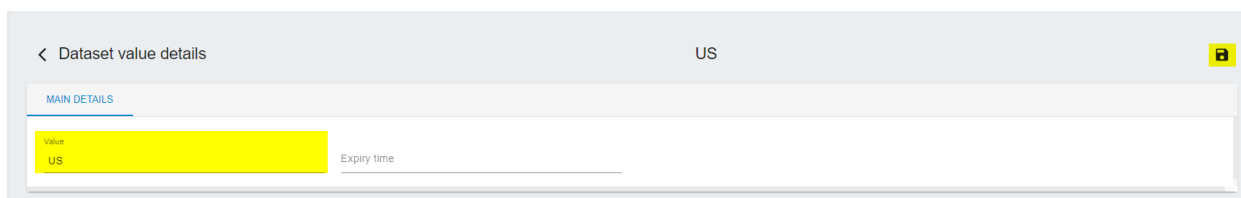
2. To **add values** to a dataset, click on **+ Add new item** at the bottom of the pane (dataset values can also be imported by clicking on **↑ Import**):



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: Adding values to a dataset

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:





Value	Expiry time
US	

Figure: Save changes to a dataset



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**:

< Dataset values GPS-DS High Risk Countries

Value	Created by	Creation time	Expiry time
<input type="checkbox"/> FR	Petru	24/04/2022 23:29:19	0
<input type="checkbox"/> GB	Petru	24/04/2022 23:29:07	0
<input checked="" type="checkbox"/> US	Petru	25/04/2022 00:14:17	0

+ ↑

 Edit item
 Delete items

Rows per page 10 1-3 of 3 |< < 1 > >|

Figure: Editing or deleting values in a dataset

Notes:

- 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
- Only managers with the appropriate access rights can make changes to datasets (see [User Access Management](#) for all available user access types)

10. Configuring Statistical Parameters

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

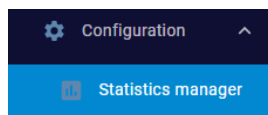
GPS Protect helps to analyse fraud patterns over time so that you can tailor rules as your programme and cardholder behaviour evolves. As part of this, GPS Protect collects statistical data about transactions for specific time periods, as defined by certain parameters. GPS Protect then uses the values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

10.1. 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.



10.2. Creating Statistical Parameters

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

<input type="checkbox"/>	Event class	Name	Institution	Function	Period name	Statistic attributes	Enabled	Atom value
<input type="checkbox"/>	TRANSACTION	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	1	
<input type="checkbox"/>	TRANSACTION	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	1	
<input type="checkbox"/>	TRANSACTION	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	1	
<input type="checkbox"/>	TRANSACTION	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	1	
<input type="checkbox"/>	TRANSACTION	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	1	
<input type="checkbox"/>	TRANSACTION	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	1	
<input type="checkbox"/>	TRANSACTION	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	1	
<input type="checkbox"/>	TRANSACTION	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	1	
<input type="checkbox"/>	TRANSACTION	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	1	
<input type="checkbox"/>	TRANSACTION	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	1	

+ Add new item

Rows per page 10 ▾ 1-10 of 12 |< < 1 2 > >|

Figure: Creating a new statistical parameter

- Enter a **Name** for the parameter.
- Choose the **Institution** the parameter should be bound to.
- 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.

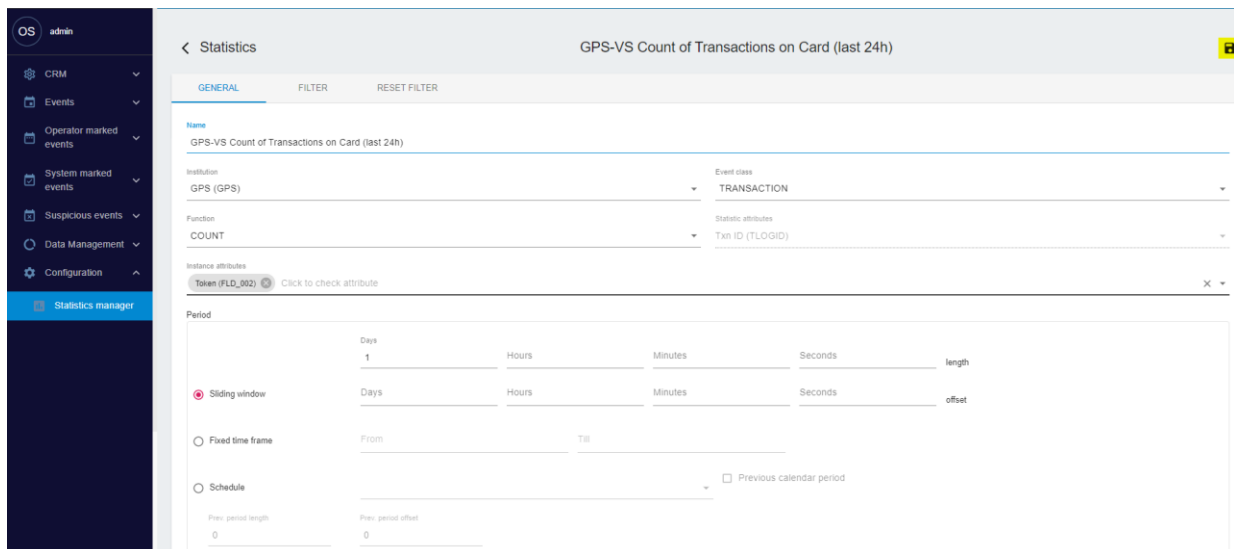




Figure: Configuring a statistical parameter

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

10.3. Updating Statistical Parameters


This section explains how to edit and delete statistical parameters.

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

Statistics

Event class	Name	Institution	Function	Period name	Statistic attributes	Enabled	Atom value
<input checked="" type="checkbox"/> TRANSACTION	Delete items	Deposit	GPS (GPS)	COUNT	Sliding window: 7 D 0 H 0 M 0 Sec Offset (0 D 0 H 0 M 0 Sec)	TLOGID	1
<input type="checkbox"/> TRANSACTION	Edit statistics item	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	1
<input type="checkbox"/> TRANSACTION	View collected data	redit	GPS (GPS)	SUM	Sliding window: 7 D 0 H 0 M 0 Sec Offset (0 D 0 H 0 M 0 Sec)	FLD_006	1
<input type="checkbox"/> TRANSACTION	Where used...	nd	GPS (GPS)	COUNT	Sliding window: 2 D 0 H 0 M 0 Sec Offset (0 D 0 H 0 M 0 Sec)	TLOGID	1

Figure: Editing a statistical parameter

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

Statistics

Event class	Name	Institution	Function	Period name	Statistic attributes	Enabled	Atom value
<input checked="" type="checkbox"/> TRANSACTION	Delete items	Deposit	GPS (GPS)	COUNT	Sliding window: 7 D 0 H 0 M 0 Sec Offset (0 D 0 H 0 M 0 Sec)	TLOGID	1
<input type="checkbox"/> TRANSACTION	Edit statistics item	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	1
<input type="checkbox"/> TRANSACTION	View collected data	redit	GPS (GPS)	SUM	Sliding window: 7 D 0 H 0 M 0 Sec Offset (0 D 0 H 0 M 0 Sec)	FLD_006	1
<input type="checkbox"/> TRANSACTION	Where used...	s	GPS (GPS)	COUNT	Sliding window: 2 D 0 H 0 M 0 Sec Offset (0 D 0 H 0 M 0 Sec)	TLOGID	1
<input type="checkbox"/> TRANSACTION	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	1

Figure: Deleting a statistical parameter

11. Generating Reports

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

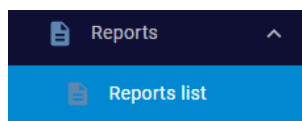
Note: Only managers with the appropriate access rights can view and generate reports (see [User Access Management](#) for more information).


Before you begin, ensure all events are marked as Genuine, Fraud, Investigation or Ignore, otherwise GPS Protect will not have the information required to produce meaningful data. For more information, see [Assigning a status to an alert](#).

11.1. Displaying Available Reports

To see a list of the reports available in GPS 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: List of available reports

11.2. 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**:

< Reports Consolidated report of suspicious transactions

Parameters

Provide parameters necessary to run this report in fields below

Start of period

End of period

Token

Institution
(Default)

Chain name

Rule name

Action
Accept Reject +1

▶ EXECUTE REPORT

Results

The following execution results are available for rendering

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

Figure: Report parameters and results

- In **Parameters**, specify any required fields and filters, such as the reporting period. Note that the report parameters change depending on the report you selected.
- 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

<input type="checkbox"/>	Time	Started by	Status
<input checked="" type="checkbox"/>	12/04/2022 15:30:55	Tijo08M	Success
<input type="checkbox"/>	12/04/2022 12:41:03	Tijo08M	Success
<input type="checkbox"/>	04/04/2022 15:55:51	Tijo06M	Success
<input type="checkbox"/>	04/04/2022 14:34:52	Tijo06M	Success
<input type="checkbox"/>	04/04/2022 13:36:45	Tijo06M	Success
<input type="checkbox"/>	04/04/2022 13:29:58	Tijo06M	Success
<input type="checkbox"/>	01/04/2022 11:57:02	user	Success
<input type="checkbox"/>	01/04/2022 11:55:28	user	Success
<input type="checkbox"/>	30/03/2022 10:16:03	Tijo06M	Success
<input type="checkbox"/>	30/03/2022 08:26:16	user	Success

Rows per page 10 1-10 of 22 |< < 1 2 3 > >|

Figure: Report results

Note: Generating reports containing large amounts of data may take time.

11.2.1.Saving a Report

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

- 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.

11.2.2.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:**

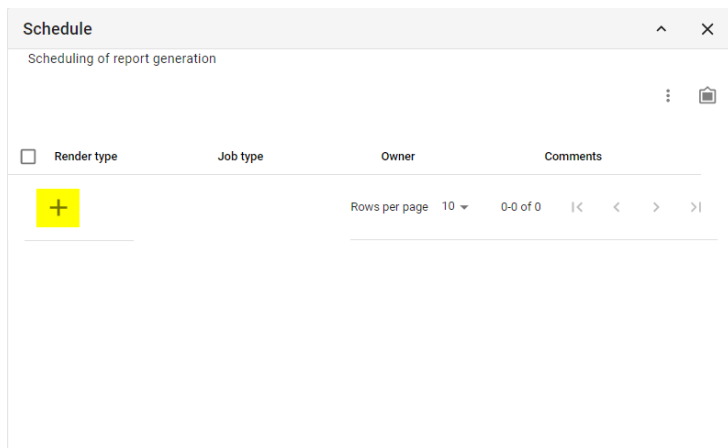


Figure: Schedule pane

2. In the **General** tab, specify the report execution frequency. Choose from **Once**, **Daily**, **Weekly** or **Monthly**:

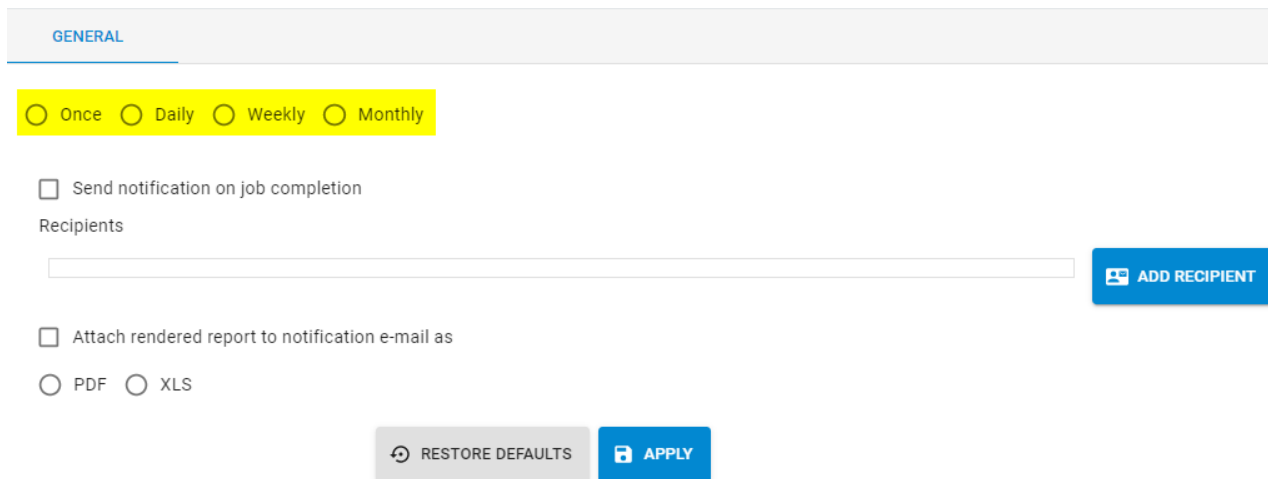


Figure: Scheduling a report

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.

GENERAL

☐ Once ☐ Daily ☐ Weekly ☐ Monthly

☒ Send notification on job completion

Recipients

☒ example@mydomain.com 

☒ Attach rendered report to notification e-mail as

☒ PDF ☐ XLS




 RESTORE DEFAULTS  APPLY  ADD RECIPIENT

Figure: Send a notification

After the report is generated, a notification is sent from 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.

12. User Access Management

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

Different levels of user access can be configured on the GPS 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 GPS 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 green:

GPS 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 Transaction		View all Transaction		View all Transaction
View all Suspicious Transaction		View all Suspicious Transaction		View all Suspicious Transaction
-	+	Review/Mark Transaction		Review/Mark Transaction
Export data to CSV		Export data to CSV		Export data to CSV
Rules		Rules		Rules
View rules		View rules		View rules
-		-	+	Edit Rules
-		-	+	Edit Datasets
-		-	+	Edit Statistical Parameters
Cases		Cases		Cases
-	+	Open/Manage Cases		Open/Manage Cases

Figure: User Access Types

12.1. Requesting Changes to User Access

GPS Protect user management is carried out by GPS. To create a new user or request a change to permissions, the person responsible for user access permissions in your organisation needs to raise a [GPS JIRA](#).

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

- 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.

FAQs and Troubleshooting

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

Setup

Cannot log into GPS Protect

- Check your credentials are correct. Both the username and password are case sensitive.
- If you forget your username or password, contact GPS by raising a [GPS 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 GPS to unlock your account and send you a password reminder.

How do I reset my password?

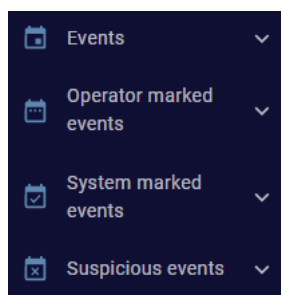
If you are logged into GPS Protect, you can change your current password using the Change Password function — for more information, see [Changing or resetting a password](#).


If you are not logged into your GPS Protect account and need to reset your password, contact GPS by raising a [GPS JIRA](#) or via email by sending a password reset request to **FraudTeam@globalprocessing.com**

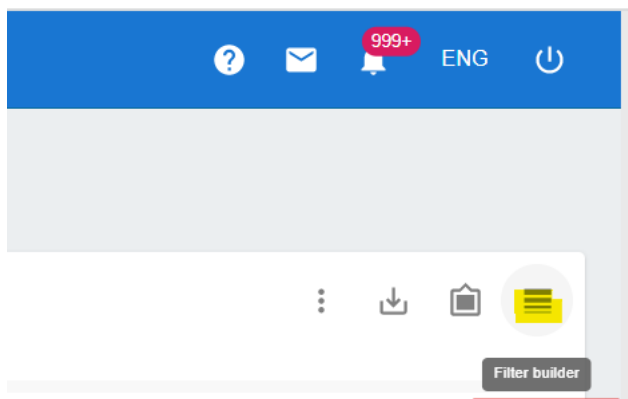
Monitoring

How do I filter data on transactional pages?

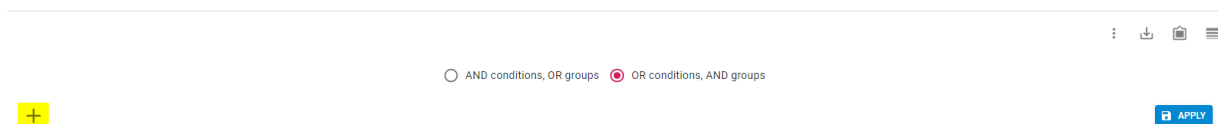
On any transactional page/sub-page (*Events, Operator marked events, System marked events or Suspicious events*):



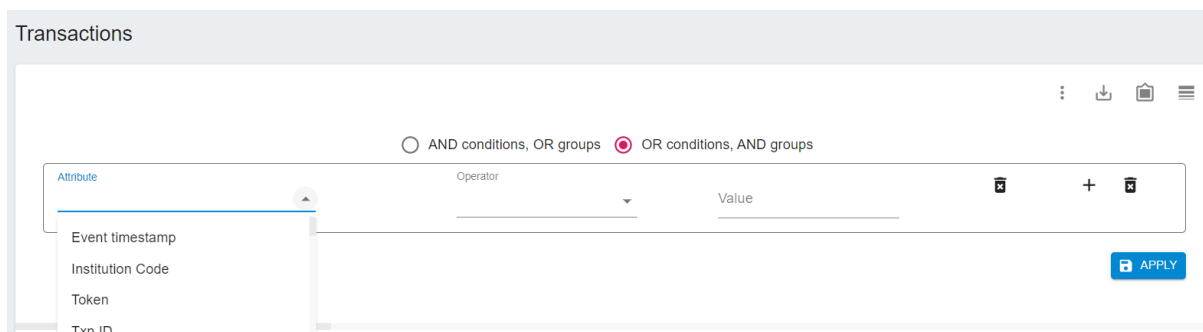
Click on  *Filter builder* in the top-right of the page:



The filter area appears. Click **+ Add new item** to add a filter.



The default options appear. 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.




How can I quickly filter transactional data?

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 **Token**:


Transactions

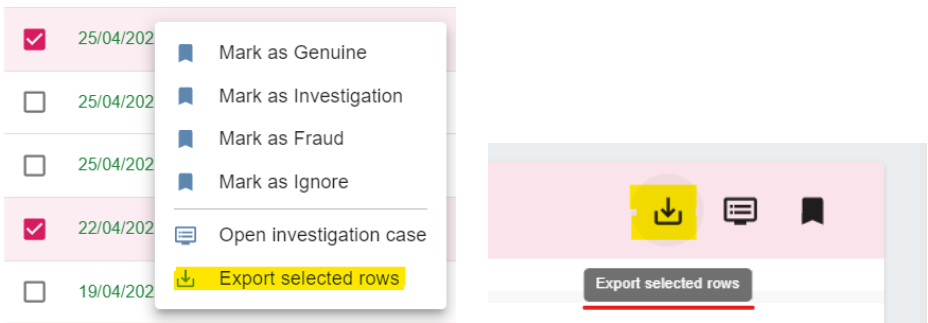
	Event timestamp	Institution Code	Token
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="123123"/>
<input type="checkbox"/>	25/04/2022 13:28:43	SMD	123123123
<input type="checkbox"/>	25/04/2022 13:27:29	SMD	123123123
<input type="checkbox"/>	25/04/2022 13:26:31	SMD	123123123

Multiple quick filter options can be used simultaneously by inputting values to the right of  in the corresponding columns (for example, *Token* = 301631516 AND *Billing Amount* = 20):

Token	Txn ID	Message Type	Processing code	POS Data Code	Response sts	Txn Amount	Txn Ccy Code	Billing Amount
<input type="text" value="3016315"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="20"/>
301631516	3765658653					30.00	LKR	20.00
301631516	3765658655					30.00	LKR	20.00

How do I export transactional data?

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.

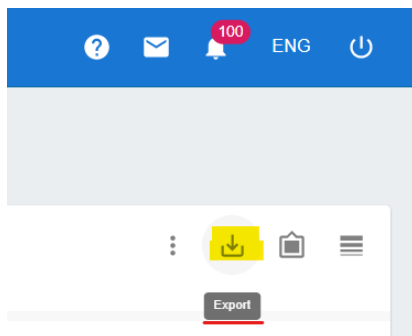
Click **SUBMIT** to save the file on your local computer.

Export

Attribute name
☐ Technical name ☒ Display name

Export format
☒ XLSX
☐ CSV

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.

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

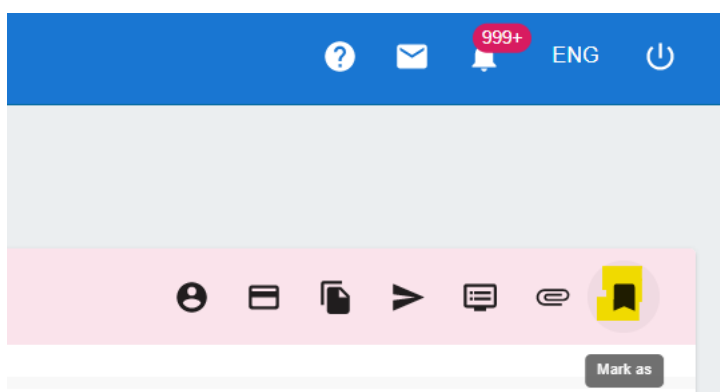
After finalising the investigation, select the checkbox next to the transaction, then right-click and assign a status:

Event timestamp	Institution Code	Token	Txn ID	Messa
<input checked="" type="checkbox"/>	22/04/2022 08:37:08	SMD		

☐ Mark as Genuine
☐ Mark as Investigation
☐ Mark as Fraud
☐ Mark as Ignore

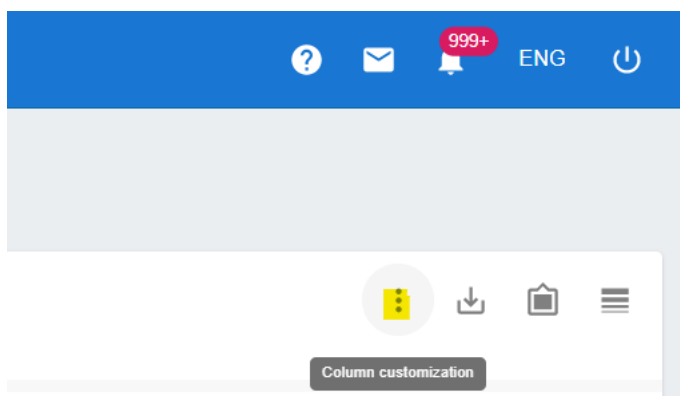
Method 2

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?

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:



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?

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	Operator	Value			
Message Type	Like	0100		+	
AND					
Token	Like	123456789		+	

APPLY



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

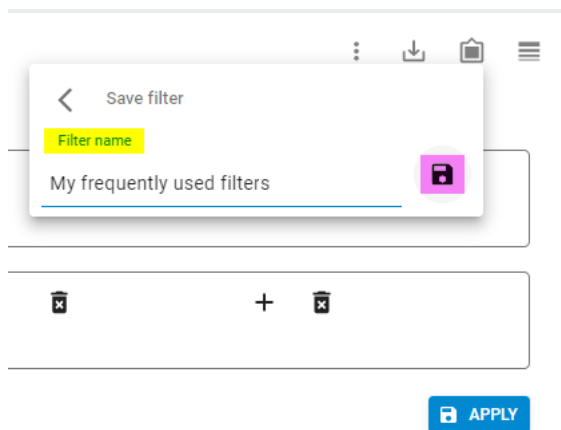


Custom filter

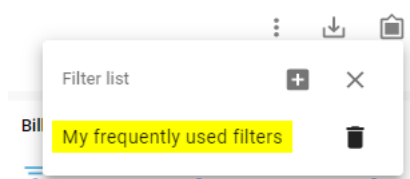
+	x
+	x

APPLY

A pop-up appears. Click  **Add filter**, give the new filter a name and press  **Save**.



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




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:

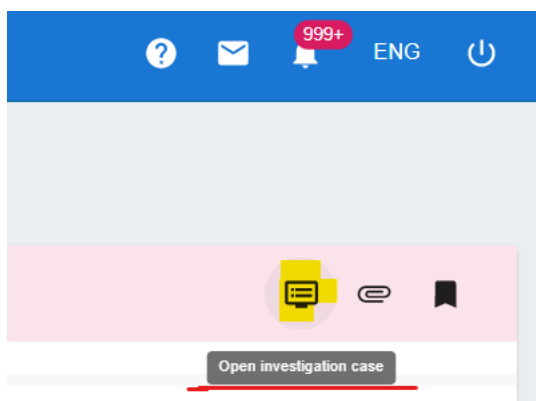
Suspicious events Transactions

	Event timestamp	Institution Code	Token	Txn ID
<input checked="" type="checkbox"/>	25/04/2022 13:28:43	SMD		
<input checked="" type="checkbox"/>	25/04/2022 13:27:29	SMD		
<input type="checkbox"/>	25/04/2022 13:26:31	SMD		
<input type="checkbox"/>	22/04/2022 08:37:08	SMD		
<input type="checkbox"/>	19/04/2022 12:47:22	SMD		

☐ Mark as Genuine
☐ Mark as Investigation
☐ Mark as Fraud
☐ Mark as Ignore
☒ Open investigation case
☐ Attach events to investigation case

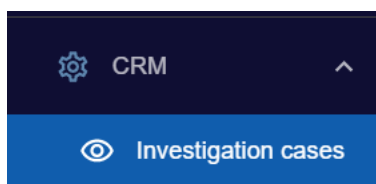
Method 2

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.




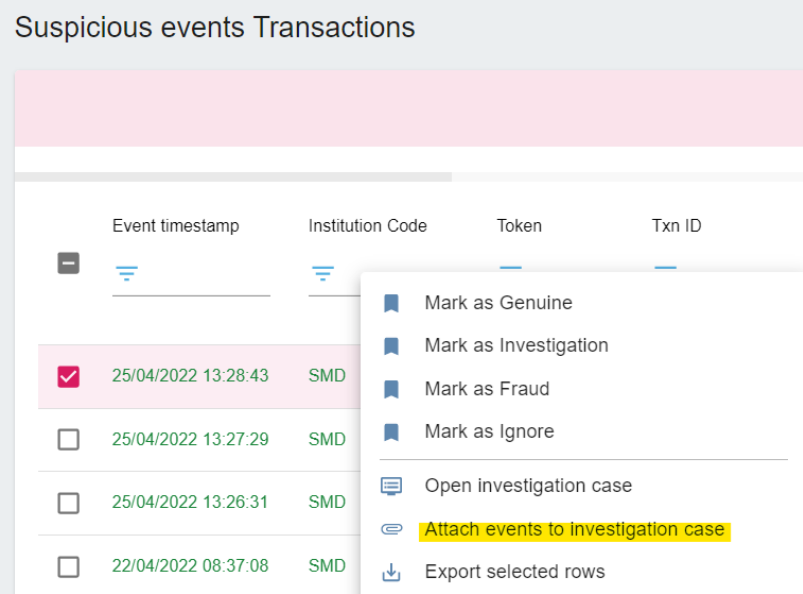
Transactions can be added later to an existing case, as described in the following topic.

How do I add transactions to an existing case?

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

Method 1

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:




The screenshot shows a table titled "Suspicious events Transactions" with columns: Event timestamp, Institution Code, Token, and Txn ID. A context menu is open over the first row, showing options: Mark as Genuine, Mark as Investigation, Mark as Fraud, Mark as Ignore, Open investigation case, **Attach events to investigation case** (highlighted), and Export selected rows.

	Event timestamp	Institution Code	Token	Txn ID
<input checked="" type="checkbox"/>	25/04/2022 13:28:43	SMD		
<input type="checkbox"/>	25/04/2022 13:27:29	SMD		
<input type="checkbox"/>	25/04/2022 13:26:31	SMD		
<input type="checkbox"/>	22/04/2022 08:37:08	SMD		

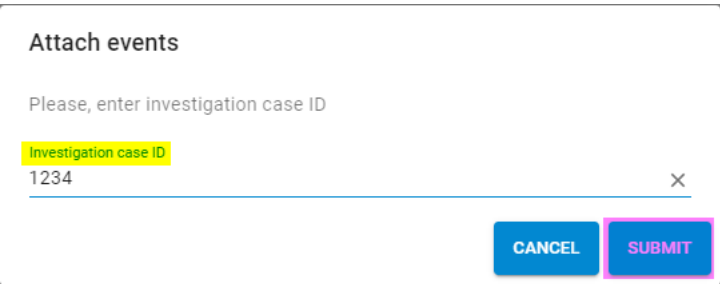
Method 2

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



The screenshot shows the top-right corner of the table with a toolbar containing icons for download, list, **Attach events to investigation case** (highlighted), and bookmark.


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:







The screenshot shows a dialog box titled "Attach events" with the text "Please, enter investigation case ID". Below this is a text input field with the value "1234" and a close button (X). At the bottom are two buttons: "CANCEL" and "SUBMIT".

How do I find specific investigation cases?







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
<input type="checkbox"/>  3355		
<input type="checkbox"/> 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	Suspicious TXNs , investigation required, email sent to CH

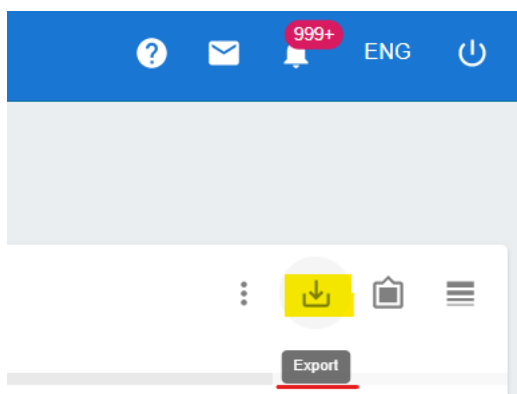
How do I export cases?

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
<input type="checkbox"/> 				 closed			
<input type="checkbox"/> 3407	System Monitor Daemon (SMD)	user	user3	Closed	13/05/2022 10:59:35	14/05/2022 10:59:00	ZZZZZZ
<input type="checkbox"/> 3406	System Monitor Daemon (SMD)	user3	user3	Closed	13/05/2022 10:31:50	15/05/2022 10:31:00	AASXZ

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



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

Export

Export format

XLSX
CSV

CANCEL

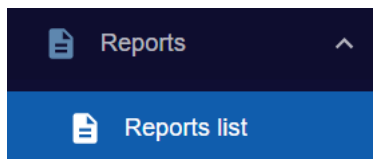
SUBMIT

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

Reporting

How do I generate reports?

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



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

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

▶ EXECUTE REPORT

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

⋮
📎

<input type="checkbox"/>	Time	Started by	Status
<input type="checkbox"/>	22/04/2022 11:17:14	Tijo09M	Success
<input type="checkbox"/>	22/04/2022 11:16:03	Tijo09M	Success

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**:

Results
^
×

<input type="checkbox"/>	29/03/2022 08:24:32	user	Success
<input type="checkbox"/>	29/03/2022 08:23:07	user	Success
<input type="checkbox"/>	29/03/2022 07:27:06	user	Success
<input type="checkbox"/>	29/03/2022 06:14:37	user	Success
<input type="checkbox"/>	21/03/2022 10:37:50	user	Success
<input type="checkbox"/>	18/03/2022 13:01:27	admin	Success
<input type="checkbox"/>	18/03/2022 12:34:03	admin	Success
<input checked="" type="checkbox"/>	18/03/2022 12:28:20	admin	Success

Rows per page 10 ▾
 1-10 of 20
 |<
 <
 1
 2
 >
 >|

📄 RENDER TO PDF

📄 RENDER TO EXEL

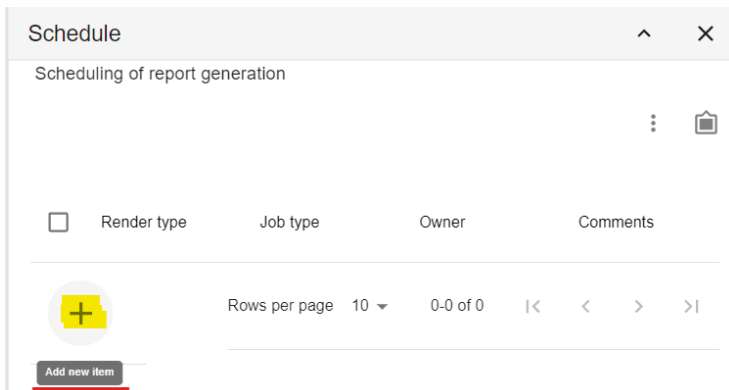
The selected file format containing the report is exported and saved to your workstation/local drive.

How do I generate reports on a scheduled basis?

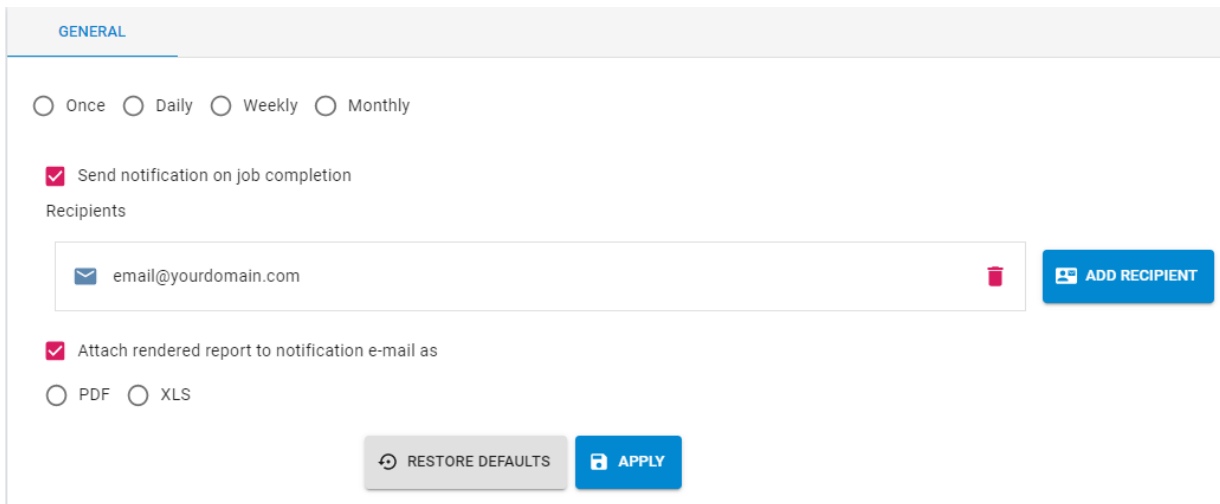
Reports can be generated automatically by the system with a predefined frequency.

Navigate to **Reports > Reports list** (note that only users with *Manager* access can generate reports) and click on a report.

On the **Schedule** pane, click **+ Add new item**:



In the window that appears, input the requested information:



- 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))

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

Appendix A — Common Codes

This section describes codes commonly used in the GPS 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)

- 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 (requires 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
- 92 = PIN Change Transactions

Response status

- 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
- 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
- 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:

- 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
- 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

- 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

Document History

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

Version	Date	Revised by	Description
2.0	30/05/2022	PetruM & AmandaL	Major upgrade to v6.0.8 for a new Web interface
1.6	15/06/2021	PetruM	Sub-chapter on Rule Actions added. Other minor updates throughout the text
1.5	11/05/2020	PetruM	Major upgrade to v5.1.7 with a redesigned interface
1.4	04/04/2019	PetruM	Updates to the server IP address and other minor updates/revisions
1.3	01/02/2019	PetruM	Wording changes
1.2	27/09/2018	PetruM	Re-wording, additional diagrams and explanation of terms

Glossary

This section explains the terms used in this guide.

Filter	See <i>Rule condition</i>
GPS Apex platform	A comprehensive, robust and reliable solution for card payment processing which is integrated within the global payment network
GPS Protect	A bespoke fraud protection programme designed to guard financial institutions and cardholders from fraudulent activity
MCC	Merchant Category Code
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 GPS Protect to determine whether transactions meet the eligibility criteria for triggering an action such as an alert
Smart Client	The user interface for managing your account on the GPS Apex platform
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
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

Tip! A full GPS glossary of terms can be found on the *Developer Portal*: [Glossary \(globalprocessing.com\)](https://globalprocessing.com/glossary)