



# **Doc4.0 Manager Manual**

**May 15, 2026**

# CONTENTS

<b>1 Introduction</b>	<b>2</b>
<b>2 Payment Gateway Objects</b>	<b>3</b>
2.1 Infological Model . . . . .	3
2.2 Processing Configuration . . . . .	3
2.3 User Roles . . . . .	4
<b>3 Quick Links</b>	<b>6</b>
<b>4 General Account Information</b>	<b>8</b>
4.1 First Login . . . . .	8
4.2 Login With OTP . . . . .	9
4.3 Left Menu . . . . .	10
4.4 User Profile . . . . .	11
<b>5 Dashboard</b>	<b>15</b>
5.1 Transaction Monitor . . . . .	15
5.2 Analytics . . . . .	16
<b>6 Orders</b>	<b>22</b>
6.1 Orders Search . . . . .	22
6.2 Recurring Payments . . . . .	35
6.3 Ethoca Alerts . . . . .	36
6.4 ChargebackHelp . . . . .	36
<b>7 Reports</b>	<b>37</b>
7.1 Cashflow Report . . . . .	37
7.2 Transaction Report . . . . .	38
7.3 Merchant Cashflow Report . . . . .	39
7.4 Reports Scheduler . . . . .	40
7.5 Performance Report . . . . .	51
7.6 Merchant Daily Performance Report . . . . .	52
7.7 Decline Statistics . . . . .	52
7.8 Fraud/Chargeback Ratio Report . . . . .	53
7.9 Fraud/Chargeback Reasons Report . . . . .	53
7.10 Gate Details Report . . . . .	54
7.11 Processor Detailed Report . . . . .	54
7.12 Close Day Report . . . . .	54
7.13 Statements . . . . .	55
<b>8 Tools</b>	<b>72</b>

8.1	Black, White And Loyalty Lists . . . . .	72
8.2	Monitoring . . . . .	83
8.3	Processing Limits . . . . .	94
8.4	Transaction Marker Notification . . . . .	101
8.5	Transaction Markers . . . . .	103
8.6	Virtual Terminal . . . . .	104
8.7	Batch Operations . . . . .	124
8.8	Integration Panel . . . . .	133
8.9	Fx Rate . . . . .	133
8.10	Analytics Dashboard . . . . .	136
<b>9</b>	<b>Settings</b>	<b>151</b>
9.1	Settings Search . . . . .	151
9.2	Configuration . . . . .	152
9.3	Users . . . . .	403
9.4	Employees . . . . .	435
9.5	Customers Management . . . . .	441
<b>10</b>	<b>Reference</b>	<b>455</b>
10.1	Glossary . . . . .	455
10.2	KPIs Detailed View . . . . .	456
10.3	Transaction Statuses And Types . . . . .	470
10.4	MC/VISA/AmEx Fraud Regulation . . . . .	472
10.5	Construction principles of billing model . . . . .	515
<b>11</b>	<b>Guides</b>	<b>529</b>
11.1	Payment Cashier Configuration . . . . .	529

- *Introduction*
- *Payment Gateway Objects*
  - *Infological Model*
  - *Processing Configuration*
  - *User Roles*
- *Quick Links*

## **INTRODUCTION**

Doc4.0 Payment Gateway (here and hereafter System, Payment Gateway or Doc4.0) provides accepting, processing, storage and transmitting of payment data between members of payment processes. This guide is intended for managers of the Payment Gateway software and hardware complex, which enable effective processing of transactions between:

- merchants (and their facilitators),
- their end customers (referred to as Payers or Receivers),
- acquiring banks or other PSPs (or their facilitators).

Doc4.0 provides a Manager account, which has broad UI and API access to the functionality of the system. This type of account allows to create and configure payment solutions for all merchants according to compliance requirements, limitations and business specifics, assign additional participants to selected merchant projects, and track financial flows of each participant.

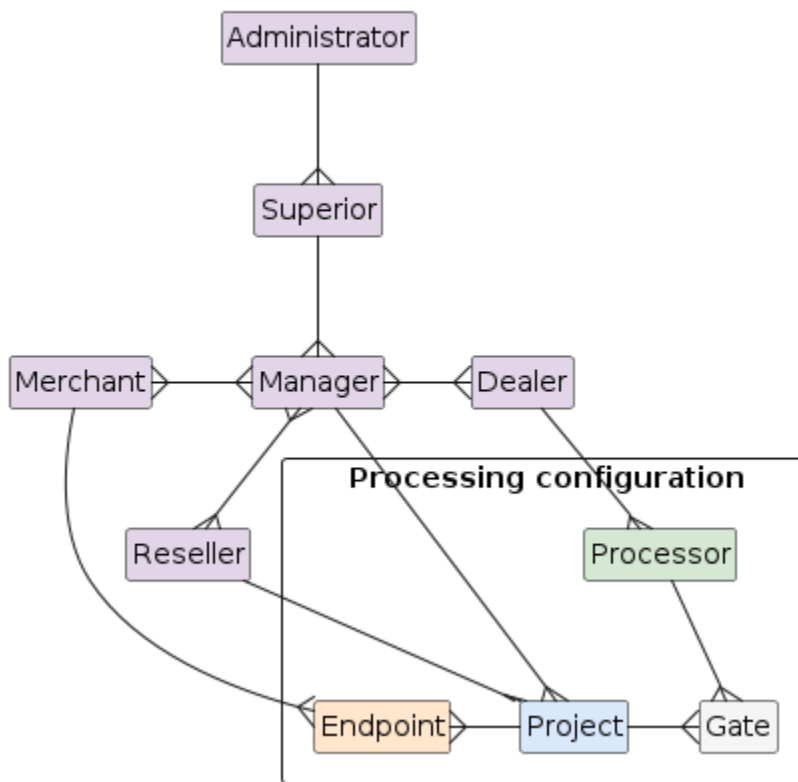
The guide is arranged according to the structure of the Payment Gateway user interface and contains detailed information about each commonly used function.

## PAYMENT GATEWAY OBJECTS

The hierarchy and data scope among users of the System is defined on the Simplified infological model of the System. All user roles and processing entities are described in the sections below.

### 2.1 Infological Model

Simplified Infological Model of the System



### 2.2 Processing Configuration

The system provides a set of integrations, named as “Processors”, with external payment institutions and payment providers. Each processor is a software module that implements

a consistent communication protocol for transferring messages with external systems. To receive, process and transmit payment data, the following entities must be configured.

Object type	Description
Processor	Payment Gateway entity, which encapsulates interconnection with third-party processing system.
Gate	A set of parameters, which identify account registered in a third-party processing system. These parameters can be used to process payment data in an external system using the messaging protocol implemented in the Processor.
Company	System entity which allows to combine several Gates in one entity, which can later be used in many system modules (for example limits, reports, etc.).
Project	System entity which determines the conditions for receiving a payment message from Endpoints and its further routing to the connected Gates.
Endpoint	Uniquely identified terminal, which is assigned to the Merchant and has to be provided in the commands within gateway API.
Endpoint group	A set of Endpoints with different currencies consolidated and available as one logical unit, which is used in gateway API URL address.
Master Endpoint	Additional logical unit which connects multiple Endpoints for Payment Cashier integration.

**Note**

Minimal configuration: 1 Processor, 1 Gate, 1 Project, 1 Endpoint.

The system allows to work with multiple currencies. Currency could be added by request.

## 2.3 User Roles

The Payment Gateway supports a dedicated account access for each user of the system. Discuss the most suitable Payment Gateway accounts model with support manager.

Each root user account can have its own Employees who can get access to the data from the root account, but with certain restrictions. Data scope is defined for all screens and reports of the system. See [Employees](#) for details.

See the list of root user accounts below:

Merchant	Provided to the merchant’s representatives. Merchant accounts can browse their transactions and linked Projects and Endpoints. They can process transactions and manage their own restriction lists.
Manager	Provided to the representatives of PSP or payment institutions. Manager accounts have full access to the configuration of the system.
Superior	Provided to the representatives of multiple Managers. Superior accounts can browse and configure all entities for the linked Managers.

continues on next page

Table 1 - continued from previous page

Reseller	Provided to the agents, which engage merchants for Manager. Reseller accounts can browse multiple linked Projects and Endpoints of Merchants and manage Reseller rate plans. They cannot process any transactions, manage restriction lists, or create new entities. Payment facilitators which represent Merchants can receive Merchant accounts for each represented Merchant, or a single Reseller account connected to Merchant accounts of each represented Merchant.
Dealer	Provided to the agents, which engage processing solutions for Manager. Dealer accounts can browse multiple Gates linked to the Processor and manage Dealer rate plans. They cannot process any transactions, manage restriction lists, or create new entities.

## QUICK LINKS

Most used functionality is gathered for a quick reference:

Account management:

- Discover login and user profile options on [General Account Information](#) page,
- Create and manage dedicated accounts for each member of the team on [Employees](#) screen,

Basic processing configuration setup:

1. Create Merchant account.
2. Create [Gate](#) for selected Processor and set any bank rate plan on it.
3. Create [Project](#) and set any manager rate plan on it, then specify the created Gate in [Routing & Balancing](#) tab.
4. Create [Endpoint](#) to link Merchant to Project, then select Available operations for this Endpoint.
5. Check that everything is connected with test transaction from [Virtual Terminal](#).
6. Clone the Project together with Endpoints and Gates to new currency, if multiple currencies should be supported, and create [Endpoint Group](#) if needed.
7. Provide Endpoint IDs per each currency and/or Endpoint Group for multi-currency integration, Merchant login, Merchant control key (for API integration), password (for UI access) to Merchant representatives.

Merchant integrations and processing assistance:

- Resend [Multiple Callbacks](#) in case of temporary handling issues of transaction results on Merchant server,
- [Capture and Cancel](#) preauthorized transactions and make [Refunds](#) on authorized ones,
- Speed up the merchant integration to Payment Gateway with full request and response logs in [Integration Panel](#),
- Configure follow-up on customers with [E-mail Or SMS Messages](#) after transactions sent from message server,

Monitoring and business analysis:

- Sort and find transactions on [Orders Search](#) screen, see complete information about each transaction on [Orders Details](#) screen,
- Get advanced analytics with [Dashboard](#) and [KPIs](#) or download detailed [Reports](#) with required data in one click using templates,

- Gather data to external systems for further analysis or alerts with [Additional Callbacks](#) for every transaction,
- Resolve ongoing payment issues with [Online Monitor](#) and [Transaction Marker notifications](#),
- Get up-to-date information about [Current Merchant Balances](#) and reflect payouts,

Learn more:

- See all terms definitions in [Glossary](#),
- Discover all supported [Transaction Types And Statuses](#),
- Design an effective payment strategy with [Routing & Balancing](#) in accordance to [Acquirer Restrictions](#) and [Processing Limits](#),
- See options for [Fraud Protection](#) with more than 100 filters,
- Mitigate risks with [Black, White And Loyalty List](#) management,
- Set up Master Endpoints for [Payment Cashier](#) integration,

## GENERAL ACCOUNT INFORMATION

- [First Login](#)
- [Login With OTP](#)
- [Left Menu](#)
- [User Profile](#)
  - [Common](#)
  - [Orders Full View Settings](#)

Manager employees can browse transactions, configure processing solutions and download various reports via Doc4.0 UI. It is available at and at .

### 4.1 First Login

Upon initial access to Doc4.0 UI, after logging in, the manager employee will be asked to create and enter a new password.

**You must change your temporary password**

Password	*	<input type="password"/>
Confirmation	*	<input type="password"/>

The minimum password length must be 8 characters  
Use of lowercase and uppercase letters  
Using at least one special character  
Using at least one digit

The minimum password length must be 8 characters. The password must contain at least one digit, one lowercase and uppercase letters and at least one special character.

#### **Warning**

It is very important that the password does not consist of meaningful linguistic structures. For security reasons it is strongly recommended to use random alphanumeric values and

regularly change the password.

## 4.2 Login With OTP

IF OTP (One Time Password) is enabled, an email will be sent to all users with a one-time link to create a second authentication factor.

An example of this letter:

Dear manageruser10

The account manageruser10 with two-factor authentication support has been created for you.

Below you can find the **one-time link** where you can obtain your temporary password and secret key required in two-factor authentication code calculation.

Enter the secret key or scan the QR code utilizing one of freely available applications which support HOTP (Google Authenticator, Protectimus Smart OTP, Free OTP Authenticator and others). Then use the generated one-time code while you access your account.

[Temporary password and secret key there](#)

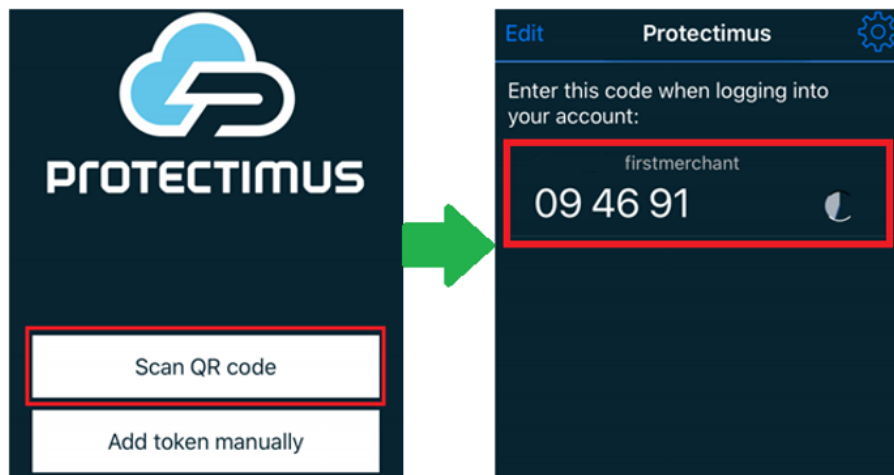
Inside there is a link, by clicking on which the QR code and the secret key will be available:

Two-factor authentication one time link

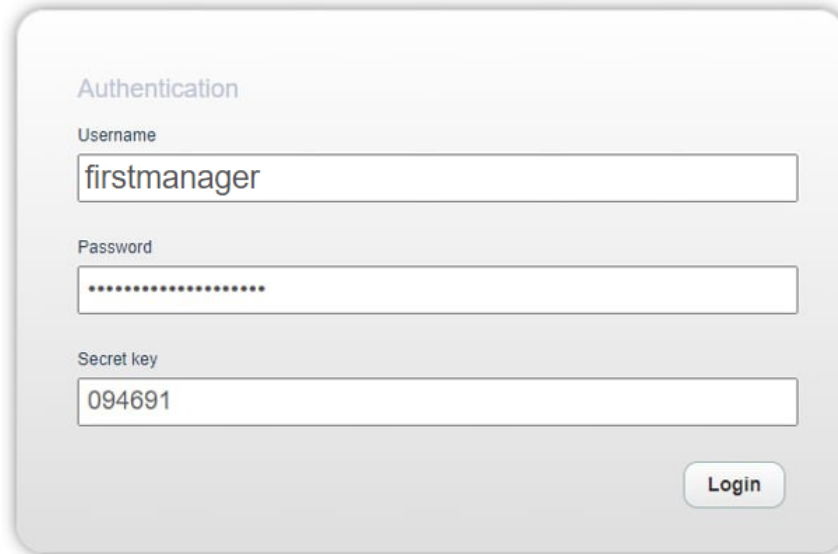


**EMWRY7Z7YCP5WJZKN4WIU43CY7AMUFEJ**

To calculate the second factor, scan the QR code or enter the secret key in any available application that supports HOTP (Google Authenticator, Protectimus Smart OTP, Free OTP Authenticator and others):



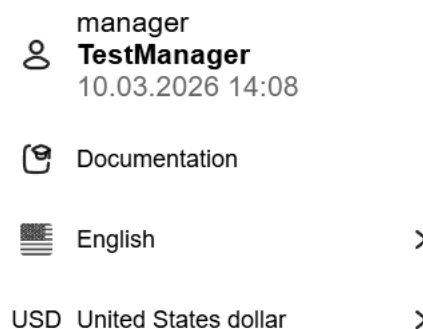
If one-time password authentication is enabled for login, enter this password when logging in. Detailed information on working with OTP is available on the link. When logging into the system, specify a username, password and generated code from the application (each time logging in, new password from application will be required):





The image shows a login form titled "Authentication". It contains three input fields: "Username" with the value "firstmanager", "Password" with masked characters, and "Secret key" with the value "094691". A "Login" button is located at the bottom right of the form.

### 4.3 Left Menu

The menu is always located at the left-down of the screen:



The left menu contains the following items from top to bottom:

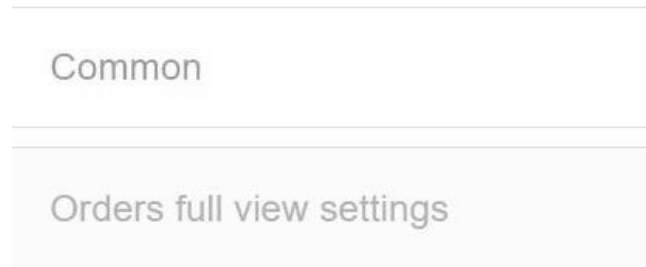
- User profile: **manager** **TestManager** 10.03.2026 14:08
- Documentation:  Documentation
- Language:  English >
- Currency: USD United States dollar >

From up to down, here are located: the account name in Doc4.0 UI and its role in the system, the current date and time in the system time zone, link to the documentation <https://>

[//doc4.codetime.net](http://doc4.codetime.net) with detailed information about Doc4.0 UI and API, menu language and currency calculations.

## 4.4 User Profile

By clicking on Manager name on the top left side of header you will be redirected to user profile where you can setup your profile. From the right side of page you will see to pages Common and Orders full view settings:



### 4.4.1 Common

Your profile manager1 (manager)
Edit profile    Reset password

Name	manager1 manager1
Language	Auto
E-mail	test@testmail.com
Phone	
Default currency	USD
Statement preview limit	5
PGP key	Not specified
CSV delimiter	Detect automatically
Telegram Bot	Register Telegram Bot
Mask request/response logs	Enabled
Enable new menu	Yes
Enable new dashboard	Yes

Common

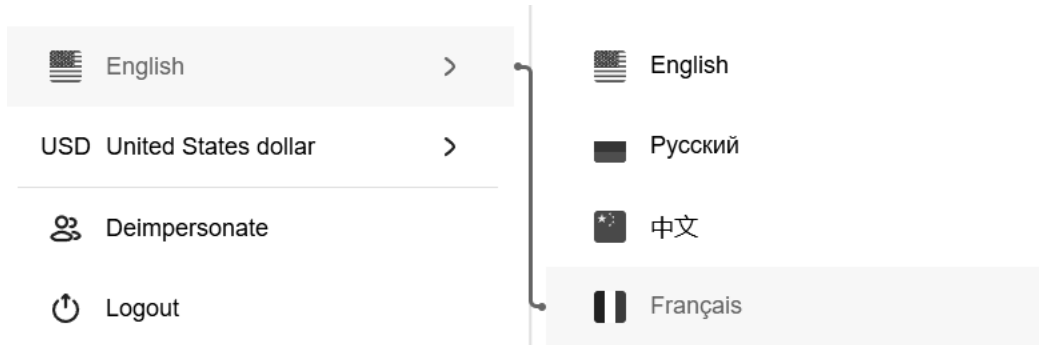
Orders full view settings

Here you can change:

- Name
- Language on which system will be automatically displayed in (possible to change from the drop-down menu at the top of the page any time)
- E-mail address on which all configured notifications will come
- Phone
- Default currency (possible to change from the drop-down menu at the top of the page any time)
- Statement preview limit
- PGP key

- CSV delimiter
- Telegram Bot - from this telegram bot you will receive information about all configured activities
- Mobile application
- Menu view

To change language from the left-bottom menu use the drop-down menu



To change the currency for calculations in transaction monitor and dashboard, use the drop-down menu from header menu. Exchange rate is updated daily.

<input type="text" value=""/>		
United States dollar	USD	1.00
United Arab Emirates dirham	AED	3.67
Argentine peso	ARS	35.38
Australian dollar	AUD	1.38
Bosnia convertible mark	BAM	1.59
Brazilian real	BRL	3.73
Bitcoin	BTC	0.00
Canadian dollar	CAD	1.32
Swiss franc	CHF	1.01
Chilean peso	CLP	684.51
Chinese yuan	CNY	6.96

### **4.4.2 Orders Full View Settings**

In this section it is possible to configure visible fields for detailed view in orders:

## Orders full view settings Manager134492 (manager)

Display seconds in date	No
Display transaction dates	No
Display merchant	No
Display project	No
Display gate	No
Display processor	No
Transaction amount visibility	Never
Transaction information	Decline reason
Order description view	Only description

## Optional fields

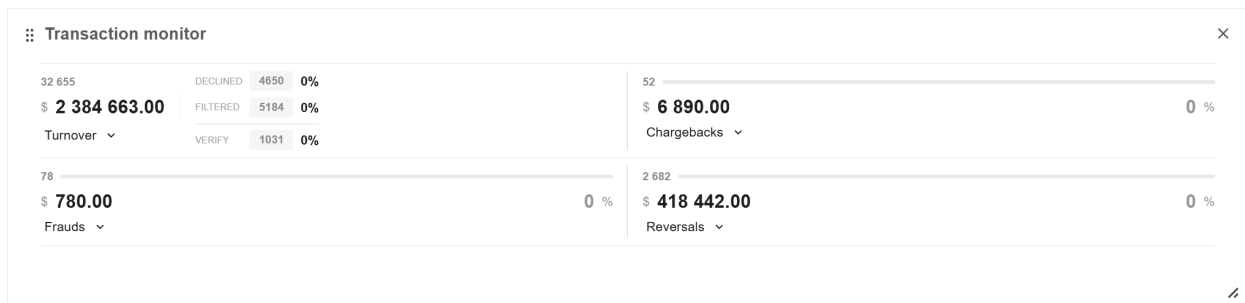
sale	No optional field
account_verification	No optional field
transfer	No optional field
preauth	No optional field
create_card_mapping	No optional field
update_card_mapping	No optional field
inquire_card_mapping	No optional field
delete_card_mapping	No optional field
payout	No optional field
mfo_scoring	No optional field
pan_eligibility	No optional field

## DASHBOARD

- [Transaction Monitor](#)
- [Analytics](#)
  - [Data Scope](#)
  - [Charts bundle](#)
  - [Approval Ratio](#)
  - [Transactions By Country](#)
  - [Transaction Decline Reasons](#)

### 5.1 Transaction Monitor

Transaction monitor is available at the top of the page for general statistics:



This monitor contains the following blocks:

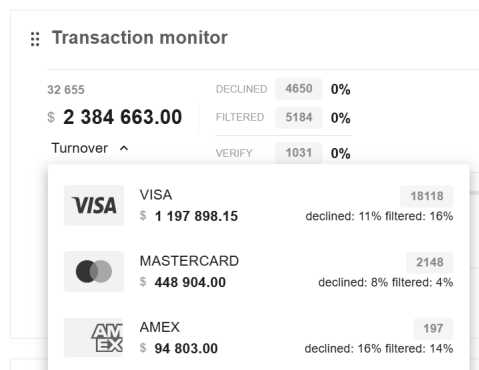
Turnover	The sum of all successful sale, capture, reversal (refund) and transfer operations
----------	--

continues on next page

Table 1 - continued from previous page

Declined, filtered and verify	The number of operations of the aforementioned types with the corresponding status
Chargebacks	The number and amount of successful chargeback and prearbitration operations
Frauds	The number and amount of successful fraud operations
Reversals	The number and amount of successful reversal and void operations

To view the analytics detailed by each payment method, click the pointer on the right side of the relevant block:



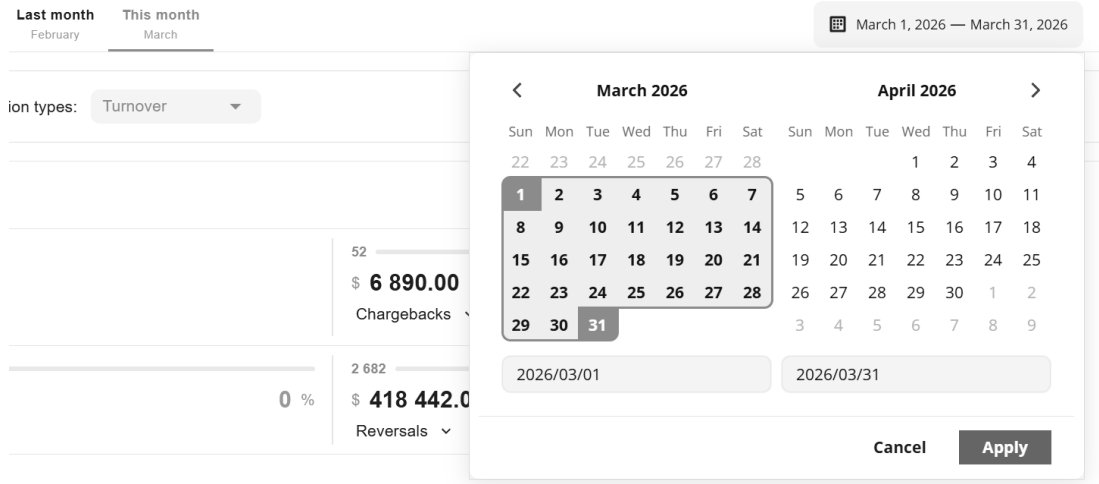
## 5.2 Analytics

### 5.2.1 Data Scope

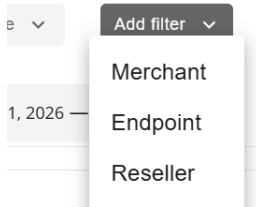
To change the range of statistics, use the switches:

Today	Yesterday	This week	Last week	Last month	This month
Mar 12	Mar 11	Mar 9 - Mar 15	Mar 2 - Mar 8	February	March

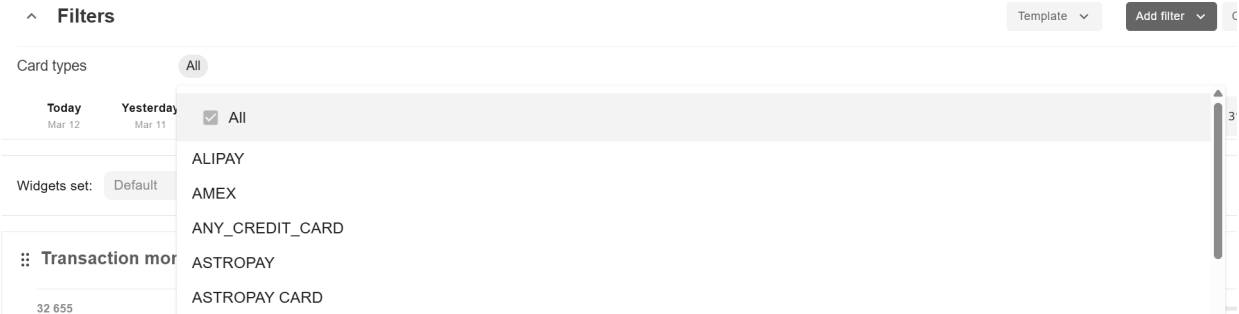
Set the desired date range in the pop-up calendar:



Data for graphs can be sorted using the Add filter button:

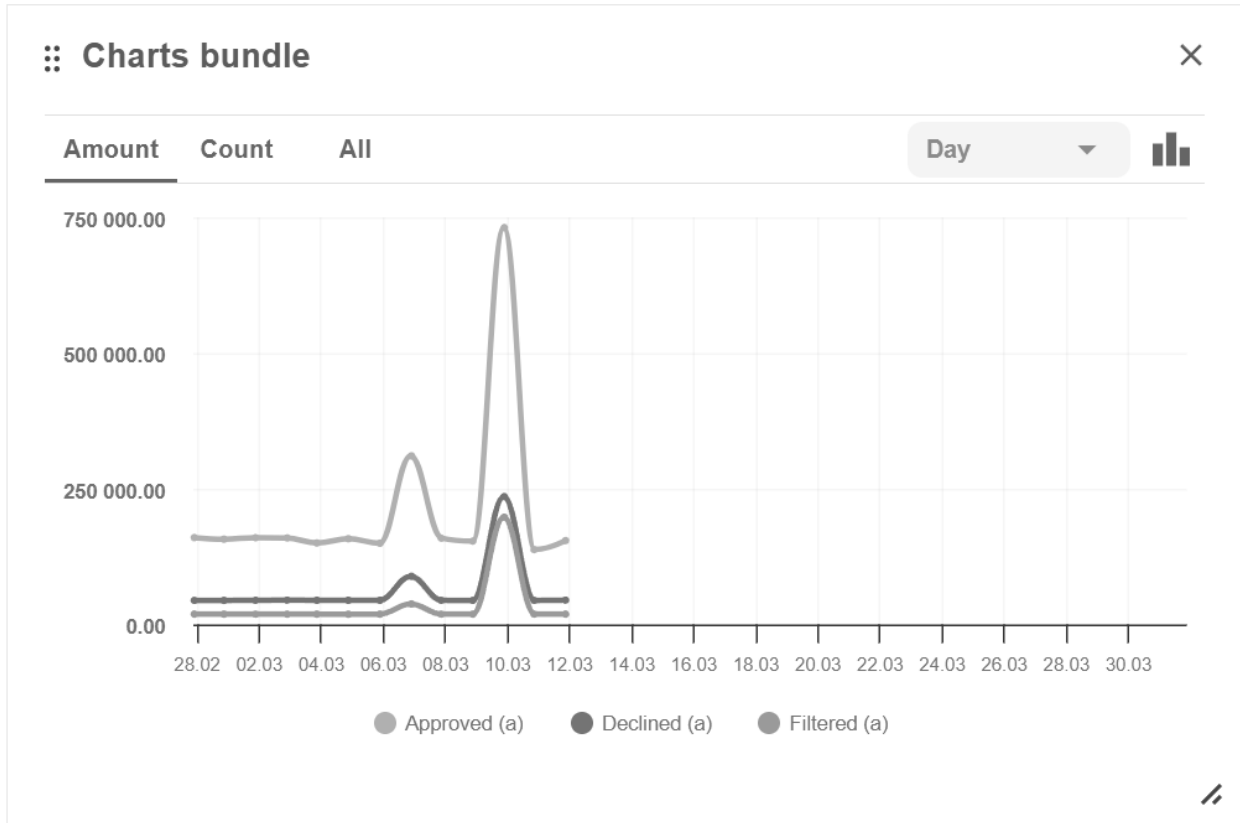



Currencies, payment methods, as well as endpoints, projects and other data can be specified for analysis. Here is the example of the payment method selection to construct the chart:



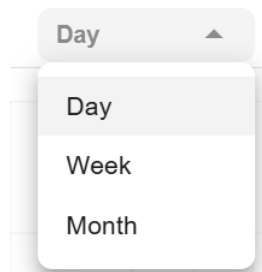
## 5.2.2 Charts bundle

Ratio of successful, rejected and filtered by the system transactions are displayed in the following graph:



The following graphs can be also selected by pressing the  button: the ratio by volume of transactions or by amount of payments, as well as by type of transactions (sale, capture, transfer, etc). Doc4.0 Payment Gateway also displays statistics on negative activity and earnings.

Required time period is set by schedule switch (day, week, month):



Type of chart (amount, count, all) can be changed using the button:

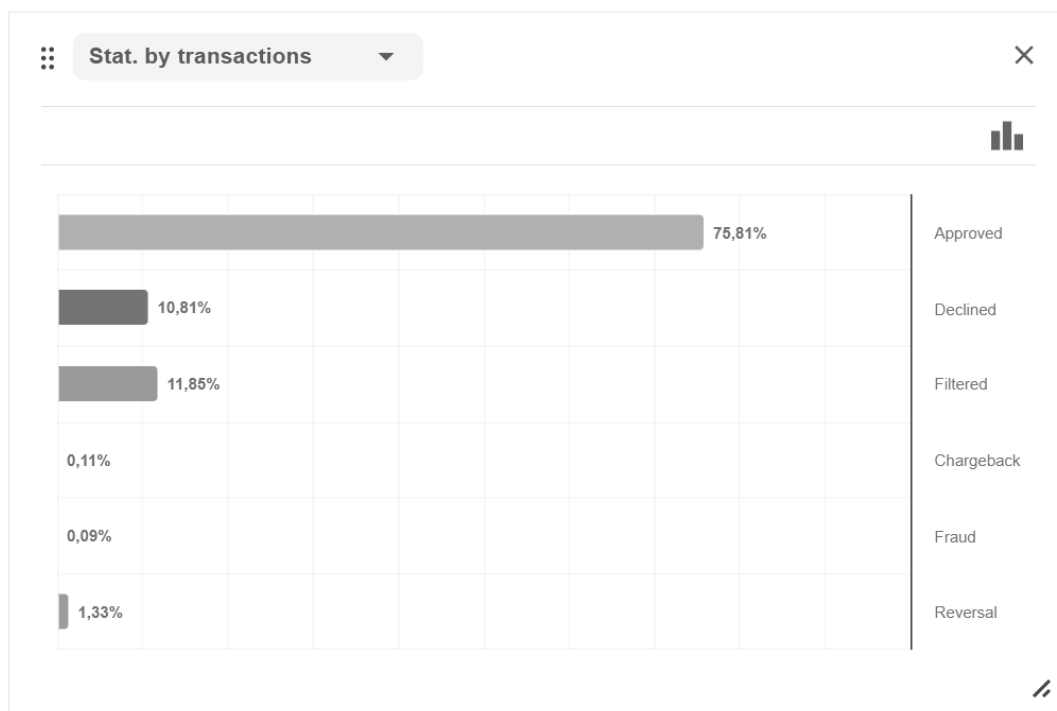


### 5.2.3 Approval Ratio

The graph shows the proportions between successful, declined and filtered transactions for a selected period of time.

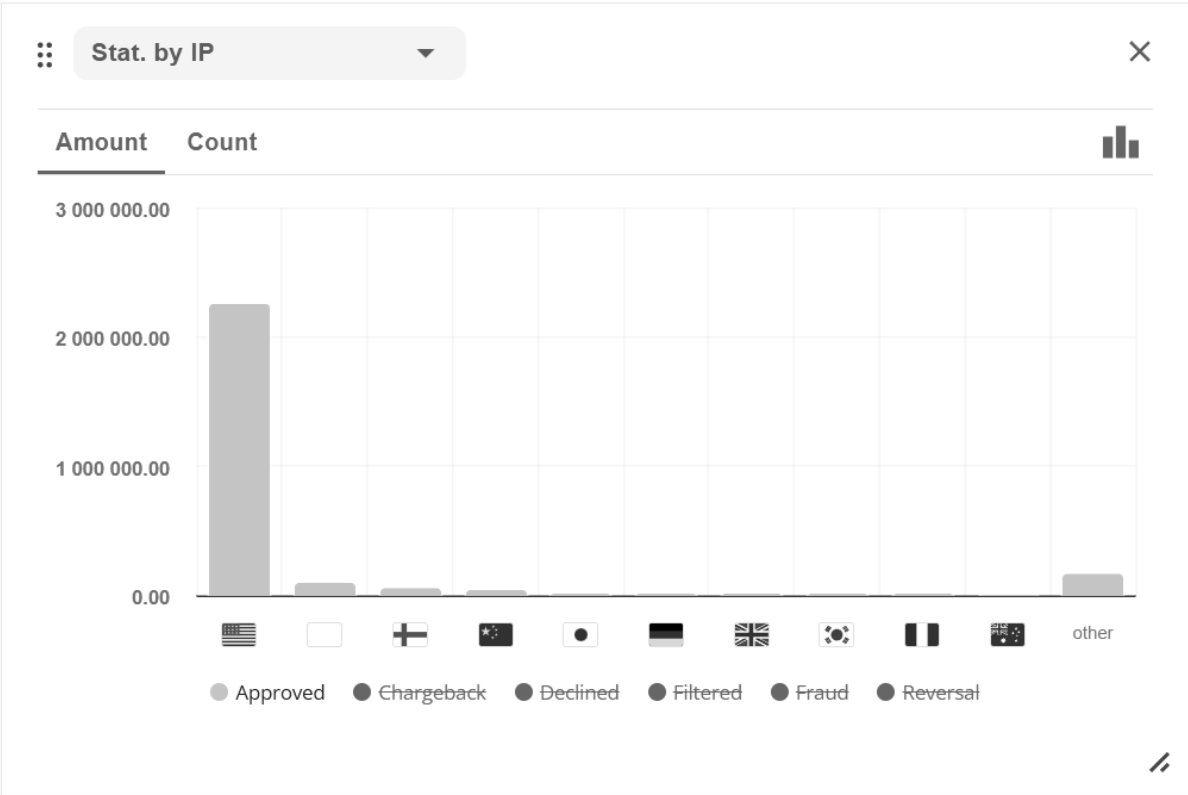
Doc4.0 Payment Gateway also displays statistics per card payment system, per currency, as well as per payment method.

Successful Transaction Analytics for the specified period are displayed as follows:



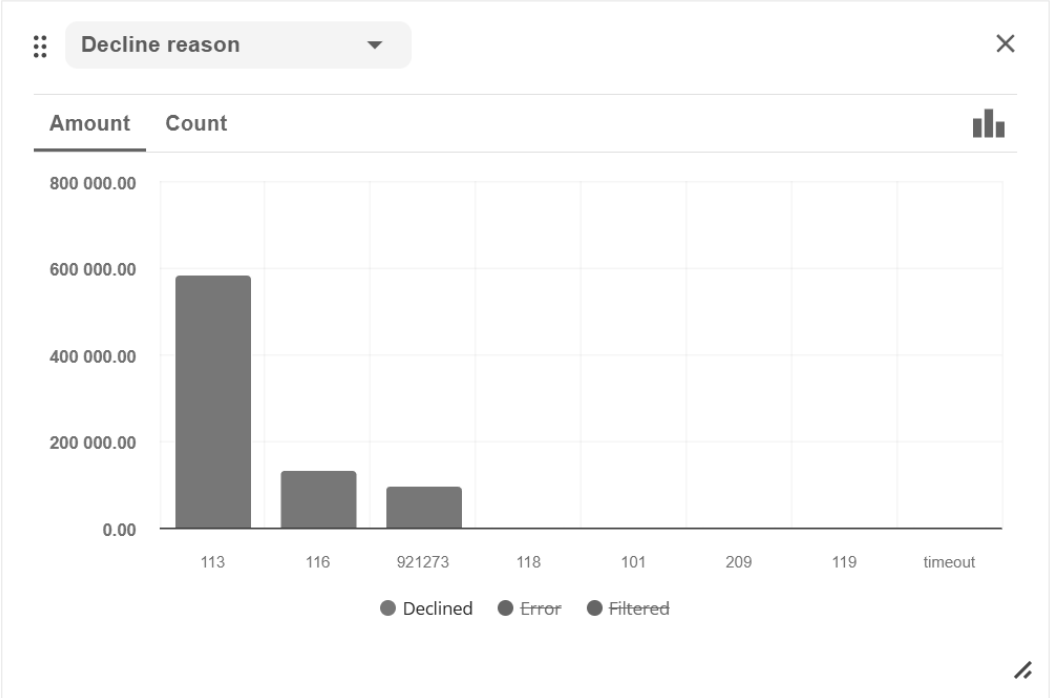
### 5.2.4 Transactions By Country

Overview of analytics by country displays two types of regional statistics: based on customer IP addresses and on card BINs.



### 5.2.5 Transaction Decline Reasons

This statistics screen can be used for a visual assessment of the most frequent decline reasons, as well as chargeback and fraud reasons.



## ORDERS

- *Orders Search*
  - *Find Orders*
  - *Orders View*
  - *Download Of Selected Transactions Report*
  - *Order Details Screen*
  - *Captures And Cancels From Back Office*
  - *Refunds From Back Office*
  - *Callbacks From Back Office*
  - *Change Status From Back Office*
- *Recurring Payments*
- *Ethoca Alerts*
- *ChargebackHelp*

### 6.1 Orders Search

The “Orders search” screen displays information on all transactions processed by Doc4.0. This screen is located in the “Orders” - “Orders search” section. Related transactions are grouped in Orders. Each Order has ID assigned by Doc4.0, ID assigned by Merchant or Connecting Party which represents Merchant and ID assigned by external processor (if transaction was processed in it). For example, sale transaction and subsequent refund on this sale transaction will have the same Order ID in Payment Gateway and will be searchable by both transaction types. Orders can also be accessed from Dashboard via Quick actions.

#### 6.1.1 Find Orders

Basic search is performed by date and exact criteria:

The screenshot shows a search interface with two main sections. The top section is labeled "Date range:" and contains two dropdown menus: "Order status changed" and "This month". To the right of this section is a "Criteria" button with a plus sign. The bottom section is labeled "Exact Criteria:" and contains a text input field with "by 6+4 sec." and a "Search..." button. To the right of this section is a "Search" button with a magnifying glass icon.

Exact criteria can be used to assist in locating a specific transaction:

Main	<ul style="list-style-type: none"> <li>• merchant invoice id</li> <li>• order id in Doc4.0</li> <li>• processor order id</li> <li>• purpose</li> <li>• amount</li> <li>• session token</li> </ul>
Customer	<ul style="list-style-type: none"> <li>• phone</li> <li>• email</li> <li>• IP address</li> <li>• IP address country</li> <li>• billing country</li> </ul>
Source Card	<ul style="list-style-type: none"> <li>• bank name</li> <li>• country</li> <li>• card from order id</li> <li>• BIN</li> <li>• BIN range from order</li> <li>• last 4</li> <li>• 6+4</li> <li>• approval code</li> <li>• ARN</li> <li>• RRN</li> <li>• card holder</li> <li>• card ref id</li> </ul>
Destination Card	<ul style="list-style-type: none"> <li>• bank name</li> <li>• country</li> <li>• card from order id</li> <li>• BIN</li> <li>• BIN range from order</li> <li>• last 4</li> <li>• 6+4</li> <li>• approval code</li> <li>• ARN</li> <li>• RRN</li> <li>• card ref id</li> </ul>
Wire	<ul style="list-style-type: none"> <li>• account number</li> <li>• routing number.</li> </ul>

continues on next page

Table 1 - continued from previous page

Card Present API	<ul style="list-style-type: none"> <li>• reader ID</li> <li>• reader key serial number</li> <li>• reader device serial number</li> </ul>
Mobile API	<ul style="list-style-type: none"> <li>• device serial number</li> <li>• phone serial number</li> <li>• phone IMEI</li> </ul>

The most convenient criteria to find an exact transaction are:

- 6+4 digits, which allows to most accurately search for a specific card;
- approval code and RRN (can be obtained from a bank statement or from a transfer receipt);
- transaction ID.

Additional search criteria are used to help with the selection of relevant orders list.

The following criteria are available:

Card types	allows to view transactions with a specific type of cards and payment methods;
Currency	allows to select one or more currencies;
Transaction types	allows to view only the specified transaction types;
Transaction statuses	allows to view transactions with the specified status;
Order status	when the transaction can't be found, this criterion allows to track the order on all stages of its processing;
Endpoint	allows to view all transactions on selected endpoints;
Project	allows to view all transactions for a specific project or several projects;
Gate	allows you to display all transactions on selected payment gateways
Processor	allows you to display all transactions for a specific processor or multiple processors
Company	allows you to display all transactions for selected companies
Merchant	allows you to display all transactions for a specific Merchant or multiple Merchants
Reseller	allows you to display all transactions for a specific reseller or multiple resellers
Error code	allows to view all transactions with a specific error.

After selecting one or more search criteria, click Search.

### 6.1.2 Orders View

By default, orders in Payment Gateway are displayed as follows:

Date	ID	Merchant	Amount	Tx. Status	Tx. Type	Tx. info	Proc.	Card	Details
Mar 10 06:04	24348964	ATMerch46AWI	53.66 USD	<input checked="" type="checkbox"/>	payout		TST	VISA 474515XXXXX9536	65.153.12.232

Orders can be presented in a brief Brief or Detailed view. This can be switched with the following button:



In detailed form, the orders will be displayed as follows:

Mar 10 06:04	50.33	<input checked="" type="checkbox"/> transfer	auto test order						
24348962			YOUNIQUE MONEY E.D.E. S.A.U.						65.153.12.232
autotestorder			VISA 474515XXXXX4027 TRANSFER HOLDER						
USD			YOUNIQUE MONEY E.D.E. S.A.U.						
			VISA 474515XXXXX9536						



The number of orders displayed on one page can be changed with the buttons in the “Rows” column:



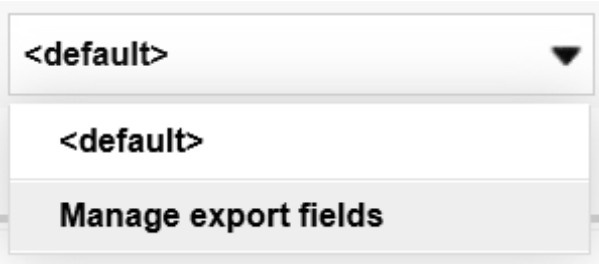
The Date button performs sorting by date. By default the latest transactions will be displayed on top.

### 6.1.3 Download Of Selected Transactions Report

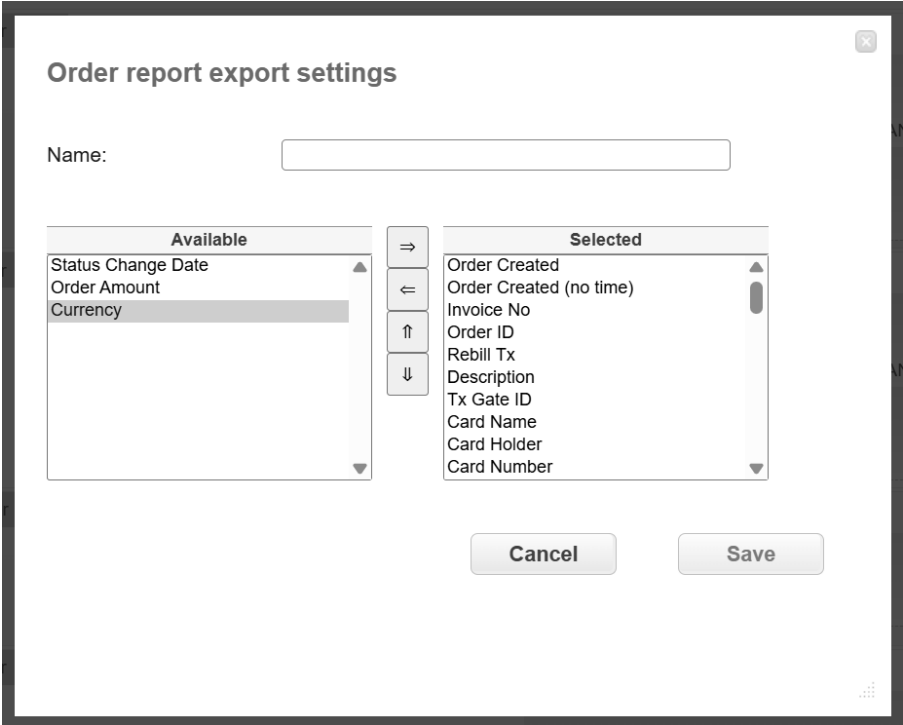
To download the sorted transactions, click one of the following buttons:

-  - download to Excel format
-  - download to CSV format.

An additional menu can be used to manage export fields:








In the pop-up window, select necessary data and save the list:



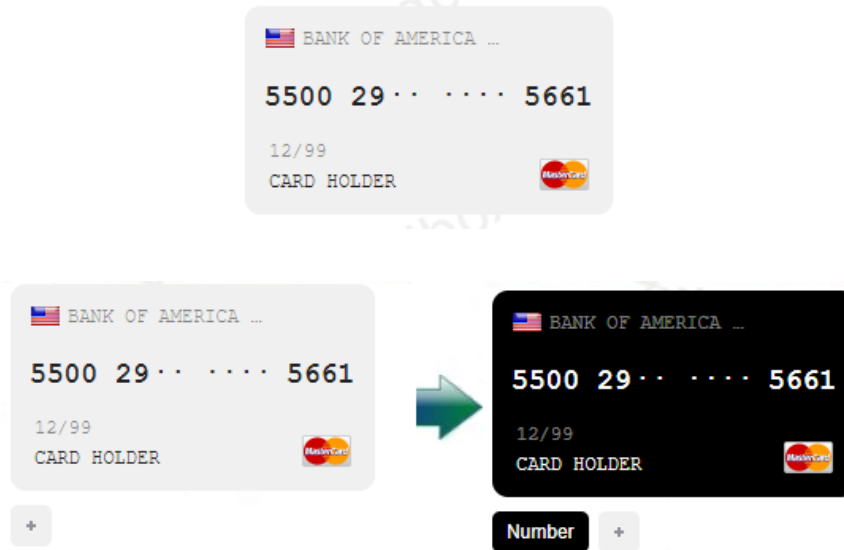
### 6.1.4 Order Details Screen

Order details screen is opened by clicking on the order ID from the search screen. Order details, such as IDs and order creation time, are displayed on the left side of this screen:

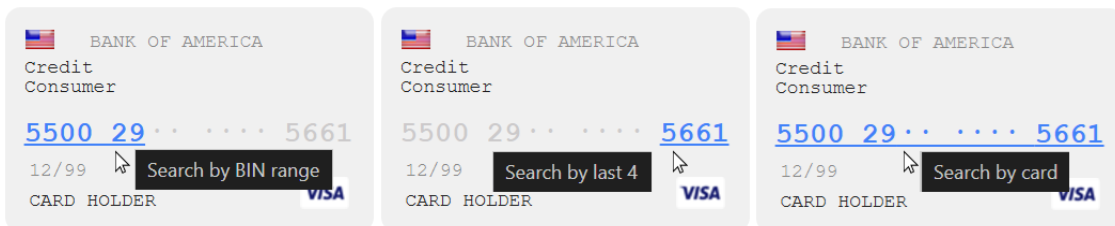
Order details	
Creation time:	11-08-2023 11:53:22.000
Merchant order ID:	34T43R77N
Order ID:	7231988
External Order ID:	PNTEST-7231988
Order description:	RERGTY
Request source:	
Fraud Score:	
Merchant URL:	
Merchant:	TestMerchant 
End Point:	TestEndpoint 
Project:	TestProject 
Gate:	TestGate 
Processor:	tesst processor 

First six and the last four digits of the card number, card expiration date and cardholder name are displayed on the card. There is also information about country, bank, card type and the payment system of the card.

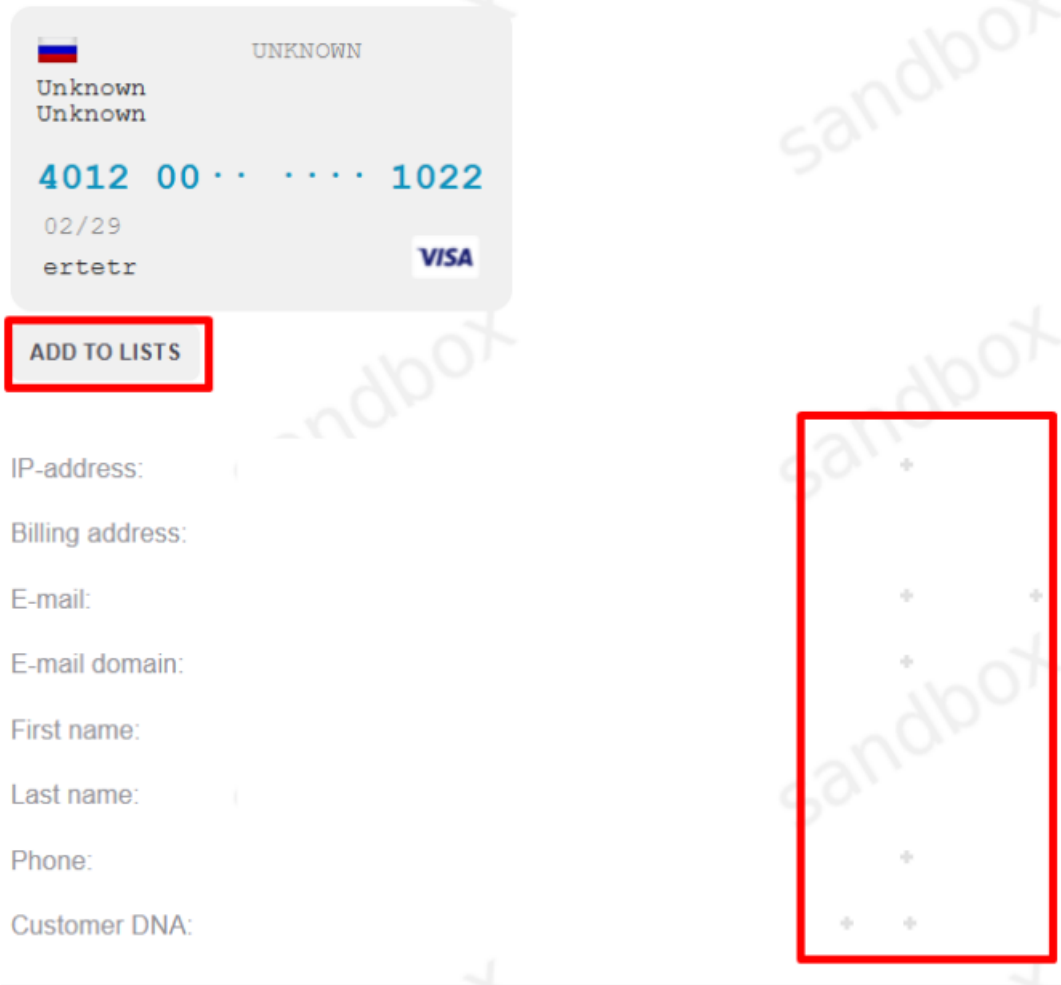
Next to the sender and receiver cards are buttons to add card details to Black, white and loyalty lists.



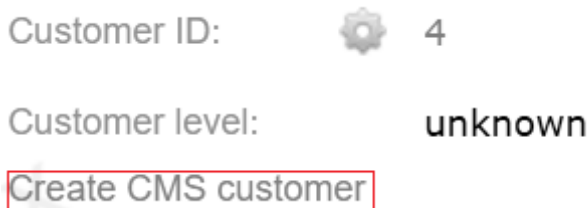
Additional customer data sent by the Merchant or submitted by customer on the form is displayed under the card or other payment method indicator. Clicking on cardholder or customer data parameter (for example, e-mail address) initiates a search for all transactions with a selected parameter.



Click on one of the plus signs near the customer data parameter (highlighted in red on the picture) adds this parameter to black, white or loyalty list. Additional click on this sign removes the parameter from respective list:



If Merchant is added to Customer Management module - new CMS customer can be created manually:



After pressing Create CMS customer - fill in needed fields, assign new "Merchant customer ID" and press Create button. New customer will not be created if "Merchant customer ID" is not unique.

Create customer

---

**Info**

First name \*       Last name \*       Date of birth

---

**Address**

Country       State       City       ZIP code

Address

---

**Contact**

Phone \*       Email \*       Customer IP

---

**Other**

Deposit level       Withdrawal level       Merchant customer ID \*

Language

All transactions within the order are grouped and the commission for each operation is calculated:

Date / Bank / Settle	Transaction	Details		
18-11-2022 16:44	<span style="color: green;">✔</span> sale	Amount: 100.00	Gate: [79523] ZetGate(USD)	External Order ID: [TST] PNTEST-6863381
-		Commission: 3.00	MID: -	External Method: -
-		Hold: 0.00		

This screen has the functionality to leave notes. For example, notes for transaction documents, customer contacts, or any other information related to this order.

**Memos**

This is

Current transaction status can be seen in the upper right part of order screen:

✓ transfer	1 122.00 RUB
Balance:	0.00 RUB
Last change date:	20-09-2018 12:24
3D:	3dFull failed

General information on all transactions associated with provided customer data is displayed in the top panel.

The total amount of all transactions made by the specified cardholder and the number of approved/declined/filtered/etc transactions:

CARD HOLDER	0 fraud
\$ 1 499	0 reversal
12 1 0	0 chargeback
	0 dispute

The total amount of transactions and the number of approved/declined/filtered/etc transactions with the specified E-mail:

john.smith@gmail.com	0 fraud
\$ 842	0 reversal
4 1 0	0 chargeback
	0 dispute

The total amount of transactions and the number of approved/declined/filtered/etc transactions with the specified IP address:

The total amount of transactions and the number of approved/declined/filtered/etc transactions with the specified card number (PAN):

### 6.1.5 Captures And Cancels From Back Office

If Preauth has final successful status, the Merchant can initiate cancel which cancels the deduction and returns locked amount back to customer’s card or the Merchant can initiate capture which deducts the locked amount from customer’s card. To start a cancellation or capturing (deduction) of the transaction, go to the details of the relevant order. On the order

85.26.235.232	0 fraud
\$ 509	0 reversal
7 0 0	0 chargeback
	0 dispute

2200 55XX XXXX 6423	0 fraud
\$ 17	0 reversal
1 0 0	0 chargeback
	0 dispute

details page, click the Cancel order button for cancellation of deducting and Capture order for deducting the locked amount.

Order actions
Cancel order
Capture order

### 6.1.6 Refunds From Back Office

If the order has final successful status, the Manager can return the money to the customer, on their request, for instance. To start a refund (reversal) transaction to the customer card, go to the details of the relevant order. On the order details page, click the Reverse order button.

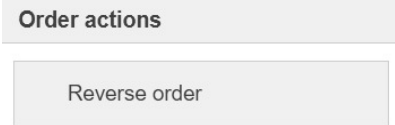
The dialog box will open like presented below:

**Reverse order** ✕

Amount\*:

Comment\*:

In this dialog box specify the amount of reversal. It can be the entire amount of the order, or only a part of it for cases where the Merchant refunds payment for certain goods that are part of one order. In the Comment field a description of this refund can be added.

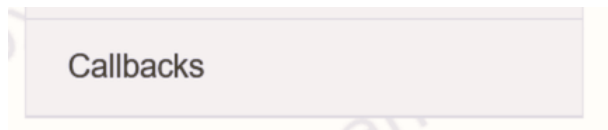


**Warning**

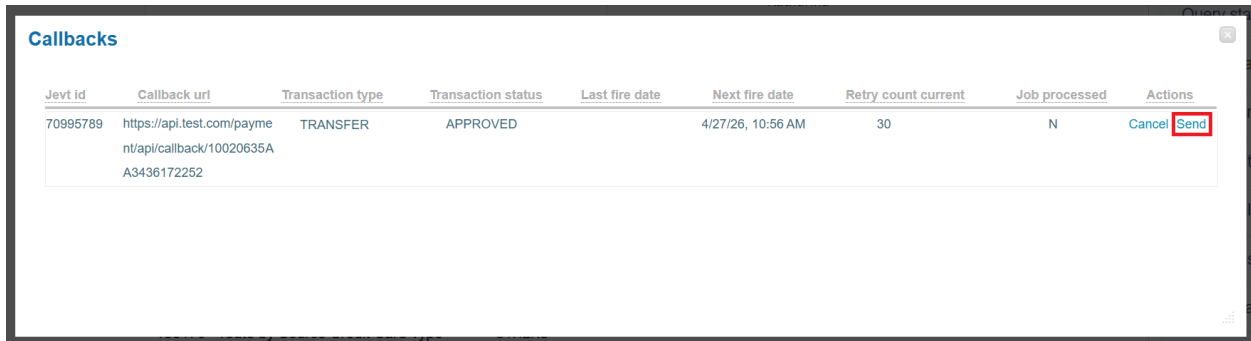
Merchants must be extremely careful when making a refund on the order! Refund requests are immediately sent to the bank and it will not be possible to cancel this transaction from the Doc4.0 system afterwards.

**6.1.7 Callbacks From Back Office**

If the order has final status and had server\_callback\_url in the initial request, the Merchant can re-send the final callback. To send a callback to the Connecting Party, go to the details of the relevant order. On the order details page, click the Callbacks button.



The dialog box will open like presented below:



In this dialog box click Send to sent callback to the Connecting Party.

Callback Fields	Description
Jevt ID	Callback event identifier
Callback URL	Callback receiver URL
Transaction type	Type of the transaction

continues on next page

Table 3 - continued from previous page

Callback Fields	Description
Transaction status	Transaction status
Last fire date	Time of the last callback attempt
Next fire date	Time of the next callback attempt
Retry count current	Remaining automatic retry attempts
Job processed	Callback job processing status

### Callback Sending Logic

Job processed = N	<ul style="list-style-type: none"> <li>• callback sending is active</li> <li>• automatic retries will occur</li> <li>• Cancel button is available</li> </ul>
Job processed = Y	<ul style="list-style-type: none"> <li>• callback sending is stopped</li> <li>• automatic retries will not occur</li> <li>• Cancel button is not available</li> </ul>

When the Send button is pressed, a single manual callback is sent and the Retry count current will decrease by 1. The status will change from: Y → N if the callback attempt fails.

You can stop callbacks by pressing Cancel.

When the Cancel is pressed: The status will change from: N → Y, callback will stop and no further automatic attempts will occur.

#### Note

Cancelling a callback prevents any further automatic retry attempts until the callback is manually triggered again.

### 6.1.8 Change Status From Back Office

If the order has final status, the Manager can change the status from declined to approved (and other way round). To change the order's status, go to the details of the relevant order. On the order details page, click the Change Transaction Status button.



Change transaction status

The dialog box will open like presented below:

In the Amount field the order's amount can be changed. In the Result Status field a order's status (DECLINED/APPROVED) should be chosen. In the External ID field External Order ID can be changed. In the RRN field a retrieval reference number of the transaction can be added.

## 6.2 Recurring Payments

The screen is located in the "Orders" section.

This screen displays recurring payments (for example, subscriptions).

Basic search is performed by date and exact criteria:

The Criteria button contains additional search parameters:

Recurrence status	Allows to select the specified repetition status of the recurring transaction: Failed - unsuccessful attempt; Scheduled - planned attempt; Stopped - currently paused or finished attempt.
-------------------	---

continues on next page

Table 4 - continued from previous page

Recurrence type	Allows to select the specified repetition type of the recurring transaction: Manual - recurring payments are initiated manually; Auto - recurring payments are initiated automatically in accordance with the set schedule; Native- recurring payments use special integration with the acquiring bank.
Endpoint	Allows to select the specific endpoint if there are several endpoints available.
Project	Allows to select the specified project if there are several projects available. Select one or more search criteria and click Search to find the needed transactions.

### 6.3 Ethoca Alerts

This section allows to see alerts from Ethoca which helps in preventing chargebacks:

### 6.4 ChargebackHelp

This section allows to see alerts from Verifi which helps in preventing chargebacks:

REPORTS

## 7.1 Cashflow Report

Calculates transaction turnover: sale, chargeback and amount of funds held. Shows the distribution of turnover, taking into account commissions and approximate profit for the period, as well as broken down by days.

If necessary, you can add additional criteria by clicking the Criteria: endpoints, projects, merchants, gates, processors, etc. The customized search criteria can be saved as a template for later use:

Save as template:

Data is uploaded by pressing the Generate button. An example of the table obtained during unloading is shown in the figure below:

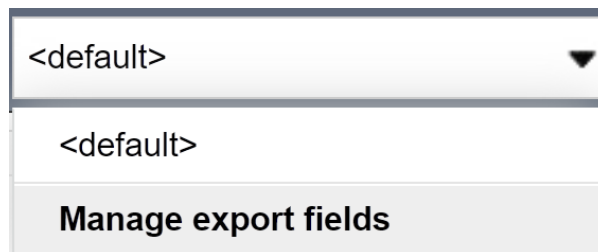
	A	B	C	D	E	F	G	H	I	J	K
1	Sandbox; Date range: 2000-01-01 00:00:00/2999-12-30 23:59:59; Project currency: USD										
2											
3	Merchants: TestMerchant										
4	from 01-Jan-2000 to 31-Dec-2999										
5											
6	Date	Currency	Transaction amount	Transfer amount	Reversal	Cancel	Refund	Fraud	Chargeback	Dispute	Held by reseller
7	12-may-2022	USD	1,00	0,00	0,00	-1,00	0,00	0,00	0,00	0,00	0,00
8	13-may-2022	USD	24,00	0,00	0,00	-2,00	0,00	0,00	0,00	0,00	0,00
9	14-may-2022	USD	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
10	15-may-2022	USD	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
11	16-may-2022	USD	905,20	31,26	0,00	0,00	0,00	0,00	-10,00	0,00	0,00
12	17-may-2022	USD	30,42	0,00	-5,00	0,00	0,00	0,00	0,00	0,00	0,00
13	18-may-2022	USD	210,42	100,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
14	19-may-2022	USD	1210,42	0,00	-100,00	0,00	0,00	0,00	0,00	0,00	-12,10
15	20-may-2022	USD	10000000,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	-10000000,00
16	21-may-2022	USD	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
17	22-may-2022	USD	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
18	23-may-2022	USD	500,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	-5,00
19	24-may-2022	USD	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
20	25-may-2022	USD	15550,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	-4,00

## 7.2 Transaction Report

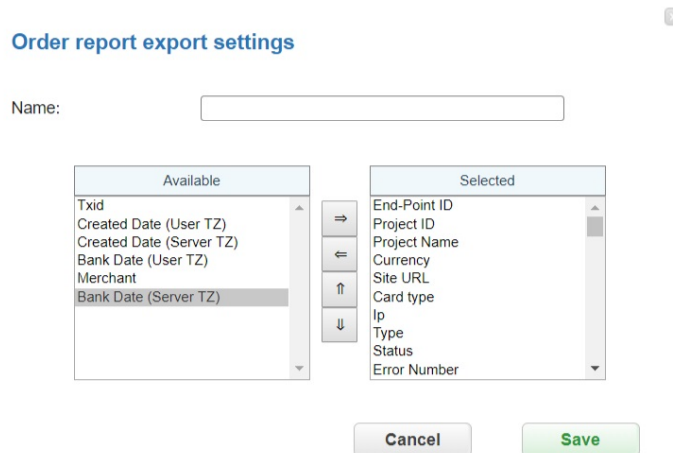
This report contains the list of transactions for the specified time period. To download the necessary data, the following criteria are used: dates, date type, transaction types, change status, card types, transaction id, recurrent filter, time zone, CSV encoding. This report can also be downloaded by API for automated reconciliation or analysis: [Remote transactions report](#)<sup>1</sup>. Additional criteria can be added by pressing the Criteria button: order status, currency, endpoints, projects, etc.

The maximum download period for report is 93 days, if data download for six months or more required, divide the required period into parts.

To change the template, use the template management tool:



Select criteria for this report in the following pop-up window:



After selecting the necessary parameters, enter name for the template and click on Save button. To download the report, click on the CSV button.

Example of the resulting table is shown below:

<sup>1</sup> [https://doc4.codetime.net/integration/common\\_utilities/reports.html#remote-transactions-report](https://doc4.codetime.net/integration/common_utilities/reports.html#remote-transactions-report)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Date range: 2018-09-16 00:00:00/2018-09-22 23:59:59; Dates type: Transaction created dates; Transaction types: [account_verification, arb													
2	Txid	Created Dat	Created Dat	Created D	Mer	End-Poi	Projec	Currency	Card type	Ip	Type	Status	Error	Amount
3	977203	2018-09-17	2018-09-17	17.09.18	ICE	3827	1532	RUB	НСПК МИИ	65.153.12.	sale	approved		10.420
4	977206	2018-09-17	2018-09-17	17.09.18	ICE	3827	1532	RUB	НСПК МИИ	65.153.12.	sale	approved		55123.000
5	977209	2018-09-17	2018-09-17	17.09.18	ICE	3827	1532	RUB	НСПК МИИ	65.153.12.	sale	approved		10500.000
6	977214	2018-09-17	2018-09-17	17.09.18	ICE	3827	1532	RUB	Visa	65.153.12.	sale	approved		10.420
7	977216	2018-09-17	2018-09-17	17.09.18	ICE	3827	1532	RUB	Visa	65.153.12.	sale	approved		1100.000
8	977217	2018-09-17	2018-09-17	17.09.18	ICE	3827	1532	RUB	Visa	85.26.235.	sale	approved		1700.000
9	977218	2018-09-17	2018-09-17	17.09.18	ICE	3827	1532	RUB	Visa	85.26.235.	sale	approved		1700.000
10	977219	2018-09-17	2018-09-17	17.09.18	ICE	3828	1532	RUB	Visa	85.26.235.	transfer	approved		1700.000
11	977202	2018-09-17	2018-09-17	17.09.18	ICE	3827	1532	RUB	НСПК МИИ	65.153.12.	sale	declined	1015	10.420
12	977226	2018-09-17	2018-09-17	17.09.18	ICE	3828	1532	RUB	Visa	85.26.235.	transfer	approved		1700.000
13	977232	2018-09-17	2018-09-17	17.09.18	ICE	3828	1532	RUB	MasterCar	85.26.235.	transfer	approved		13666.000
14	977233	2018-09-17	2018-09-17	17.09.18	ICE	3828	1532	RUB	MasterCar	85.26.235.	transfer	approved		11777.000
15	978194	2018-09-20	2018-09-20	20.09.18	ICE	3828	1532	RUB	НСПК МИИ	85.26.235.	transfer	approved		1122.000

**Note**

The returned report has wellformed CSV format. In accordance with , fields containing line breaks (CRLF, CR, LF), double quotes, and commas are enclosed in double-quotes.

## 7.3 Merchant Cashflow Report

This report calculates transaction turnovers: sale, chargeback, and reversed funds. It shows the distribution of turnover with commissions and the approximate profit for the selected period, as well as day-by-day earnings.

If necessary, you can add additional criteria by clicking the Criteria: endpoints, projects, merchants, gates, processors, etc. The customized search criteria can be saved as a template for later use.

Data can be downloaded by pressing the Generate button.

An example of the resulting report is shown below:

	A	B	C	D	E	F	G	H	I	J	K
1	Sandbox; Date range: 2000-01-01 00:00:00/2999-12-30 23:59:59; Project currency: USD										
2											
3	Merchants: TestMerchant										
4											
5	from 01-Jan-2000 to 31-Dec-2999										
6	Date	Currency	Transaction amount	Transfer amount	Reversal	Cancel	Refund	Fraud	Chargeback	Dispute	Held by reseller
7	12-may-2022	USD	1,00	0,00	0,00	-1,00	0,00	0,00	0,00	0,00	0,00
8	13-may-2022	USD	24,00	0,00	0,00	-2,00	0,00	0,00	0,00	0,00	0,00
9	14-may-2022	USD	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
10	15-may-2022	USD	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
11	16-may-2022	USD	905,20	31,26	0,00	0,00	0,00	0,00	-10,00	0,00	0,00
12	17-may-2022	USD	30,42	0,00	-5,00	0,00	0,00	0,00	0,00	0,00	0,00
13	18-may-2022	USD	210,42	100,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
14	19-may-2022	USD	1210,42	0,00	-100,00	0,00	0,00	0,00	0,00	0,00	-12,10
15	20-may-2022	USD	1000000010,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	-10000000,10
16	21-may-2022	USD	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
17	22-may-2022	USD	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
18	23-may-2022	USD	500,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	-5,00
19	24-may-2022	USD	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
20	25-may-2022	USD	15550,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	-4,00

## 7.4 Reports Scheduler

- [Introduction](#)
- [Configuration](#)
  - [Report Filters](#)
  - [Report Parameters](#)
  - [Report Format](#)
  - [Encode](#)
- [Schedule](#)
  - [Generate The Report](#)
  - [First Report Date](#)
  - [Date Interval](#)
- [Output](#)

### 7.4.1 Introduction

Report Scheduler helps you generate available reports and send them to the email specified in the settings at certain time intervals, depending on the configuration. This functionality can be granted to each Manager individually. Please contact Doc4.0 support team to enable this feature.

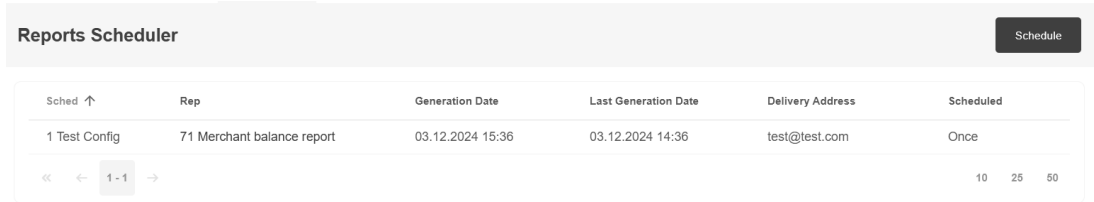
Report Scheduler can be configured via Reports tab.

To set up configuration, follow these steps:

1. Set [Configuration](#) to define report parameters such as report time, report format, and encoding.
2. Set [Schedule](#) to define the timing of report generation and date interval.
3. Set [Output](#) to define the settings for the format of sending the report, specifying the E-mail and the name of the file.

Below is an example of a fully configured report, as well as the report received by email with highlighted steps.

Here is an example of what a configured report looks like on the screen of a report scheduler:

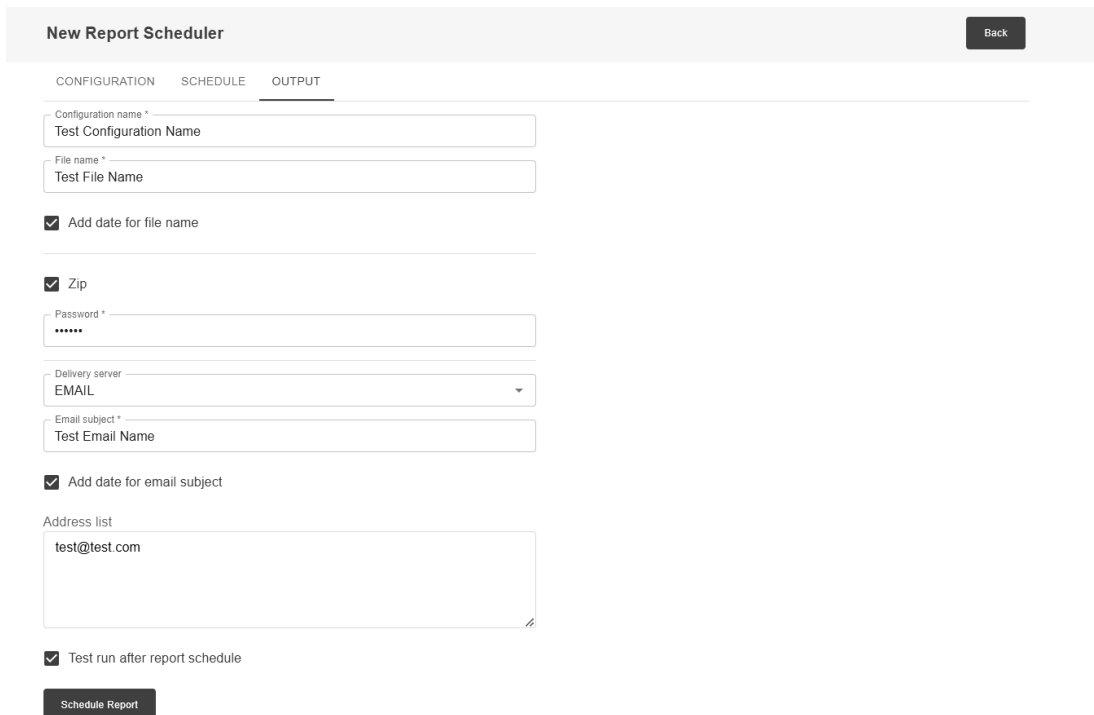


The screenshot shows the 'Reports Scheduler' interface. At the top right is a 'Schedule' button. Below is a table with the following data:

Sched ↑	Rep	Generation Date	Last Generation Date	Delivery Address	Scheduled	
1	Test Config	71 Merchant balance report	03.12.2024 15:36	03.12.2024 14:36	test@test.com	Once

Navigation controls include '<<', '<', '1 - 1', and '>', and a footer with '10 25 50'.

The fully configured setup is shown below:

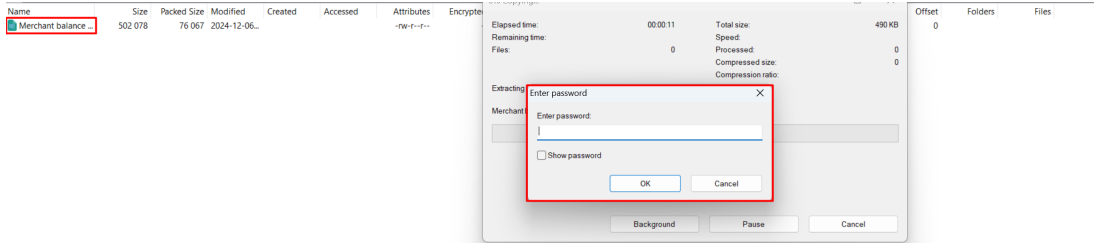


The screenshot shows the 'New Report Scheduler' configuration form. It has a 'Back' button at the top right and three tabs: 'CONFIGURATION', 'SCHEDULE', and 'OUTPUT'. The 'CONFIGURATION' tab is active. The form contains the following fields and options:

- Configuration name \*: Test Configuration Name
- File name \*: Test File Name
- Add date for file name
- Zip
- Password \*: [masked]
- Delivery server: EMAIL (dropdown)
- Email subject \*: Test Email Name
- Add date for email subject
- Address list: test@test.com
- Test run after report schedule

A 'Schedule Report' button is located at the bottom.

An example of the report received by email, with a ZIP password, is shown below:

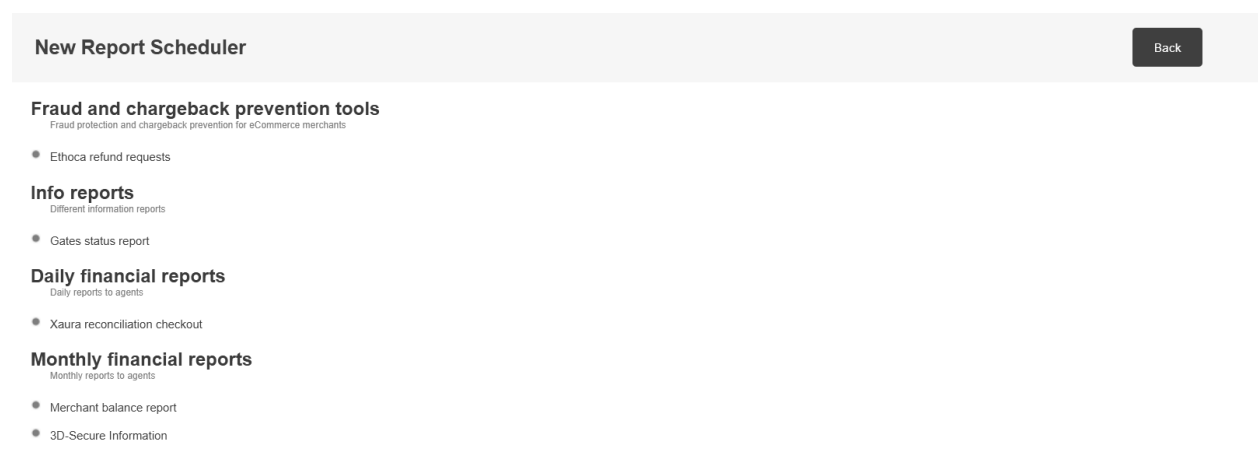


A	B	C	D	E	F	G	H	I	J
1	Merc_id	Merchant name	Id	End_points	Balance_name	Balance total	Balance live	STH	Currency
2	1*	TestMerchant_A	5*	Y*	test	9999999999999999999	9999999999999999999	0.000	USD
3	1*	TestMerchant_A	Total			9999999999999999999	9999999999999999999	0.000	
4	2*	TestMerchant_A	1130*	N*	test	9999999999999999999	9999999999999999999	0.000	AED
5	2*	TestMerchant_A	Total			9999999999999999999	9999999999999999999	0.000	
6	3*	TestMerchant_A	1482*	N*	test	0.000	0.000	0.000	CAD
7	3*	TestMerchant_A	Total			0.000	0.000	0.000	
8	69*	TestMerchant_A	1535*	Y*	test	1782.825	1782.825	0.000	EUR
9	69*	TestMerchant_A	1536*	Y*	test	2309.769	2309.769	0.000	USD
10	69*	TestMerchant_A	Total			4092.594	4092.594	0.000	
11	275*	TestMerchant_A	2481*	N*	statements TestBal	456.000	456.000	0.000	AUD
12	275*	TestMerchant_A	2482*	N*	statements TestBal	3335.000	3335.000	0.000	AED
13	275*	TestMerchant_A	Total			3791.000	3791.000	0.000	
14	425*	TestMerchant_A	1641*	N*	balName	1451.040	1451.040	0.000	USD
15	425*	TestMerchant_A	1642*	N*	test	0.000	0.000	0.000	AUD
16	425*	TestMerchant_A	Total			1451.040	1451.040	0.000	
17	483*	TestMerchant_A	2*	N*	test1*	2808727.390	2808727.390	0.000	RUB
18	483*	TestMerchant_A	Total			2808727.390	2808727.390	0.000	
19	484*	TestMerchant_A	3*	N*	test balance	0.000	0.000	0.000	RUB
20	484*	TestMerchant_A	Total			0.000	0.000	0.000	
21	486*	TestMerchant_B	6*	N*	TestBalRENAMED	281800.000	281800.000	0.000	USD
22	486*	TestMerchant_B	Total			281800.000	281800.000	0.000	
23	487*	TestMerchant_B	8*	N*	testbalance	950980.000	950980.000	0.000	USD
24	487*	TestMerchant_B	Total			950980.000	950980.000	0.000	
25	488*	TestMerchant_B	471*	Y*	test_EDITEDNAME	9999999999999999999	9999999999999999999	0.000	USD
26	488*	TestMerchant_B	472*	N*	test2	0.000	0.000	0.000	USD
27	488*	TestMerchant_B	Total			9999999999999999999	9999999999999999999	0.000	
28	495*	TestMerchant_B	9*	N*	test	1297.260	1297.260	0.000	USD
29	495*	TestMerchant_B	Total			1297.260	1297.260	0.000	
30	497*	TestMerchant_B	2386*	N*	test22	0.000	0.000	0.000	USD
31	497*	TestMerchant_B	Total			0.000	0.000	0.000	
32	519*	TestMerchant_B	1699*	N*	Test balance without ep USD	0.000	0.000	0.000	USD
33	519*	TestMerchant_B	3154*	Y*	test balance with ep USD	0.000	0.000	0.000	USD
34	519*	TestMerchant_B	Total			0.000	0.000	0.000	
35	1077*	TestMerchant_B	10*	N*	BalanceNameQXPNR1*	0.000	0.000	0.000	USD
36	1077*	TestMerchant_B	Total			0.000	0.000	0.000	
37	1078*	TestMerchant_B	11*	N*	BalanceNameRZNPX0*	0.000	0.000	0.000	USD
38	1078*	TestMerchant_B	Total			0.000	0.000	0.000	
39	1079*	TestMerchant_B	12*	N*	BalanceNameHSA13E*	0.000	0.000	0.000	USD
40	1079*	TestMerchant_B	13*	N*	BalanceNameM4EVP*	0.000	0.000	0.000	RUB
41	1079*	TestMerchant_B	Total			0.000	0.000	0.000	
42	1080*	TestMerchant_B	14*	N*	BalanceNameJOSVNG*	0.000	0.000	0.000	USD
43	1080*	TestMerchant_B	15*	N*	BalanceNameRAHAP5*	0.000	0.000	0.000	RUB
44	1080*	TestMerchant_C	Total			0.000	0.000	0.000	
45	1081*	TestMerchant_C	16*	N*	BalanceNameZF9723*	100.000	100.000	0.000	USD
46	1081*	TestMerchant_C	17*	N*	BalanceNameF7AVCC*	0.000	0.000	0.000	RUB
47	1081*	TestMerchant_C	Total			100.000	100.000	0.000	
48	1082*	TestMerchant_C	18*	N*	BalanceName7GL1GX*	100.000	100.000	0.000	USD
49	1082*	TestMerchant_C	19*	N*	BalanceNameCFZB37*	0.000	0.000	0.000	RUB
50	1082*	TestMerchant_C	Total			100.000	100.000	0.000	
51	1084*	TestMerchant_C	20*	N*	BalanceNameM33QX2*	100.000	100.000	0.000	USD
52	1084*	TestMerchant_C	21*	N*	BalanceNameFNCSA*	0.000	0.000	0.000	RUB
53	1084*	TestMerchant_C	Total			100.000	100.000	0.000	
54	1088*	TestMerchant_C	22*	N*	BalanceNameSFU7VD*	100.000	100.000	0.000	USD
55	1088*	TestMerchant_C	23*	N*	BalanceNameZ6LU3L*	0.000	0.000	0.000	RUB
56	1088*	TestMerchant_C	Total			100.000	100.000	0.000	
57	1089*	TestMerchant_C	24*	N*	BalanceNameWZ5T69*	100.000	100.000	0.000	USD
58	1089*	TestMerchant_C	25*	N*	BalanceNameLU2Y9J*	0.000	0.000	0.000	RUB
59	1089*	TestMerchant_C	Total			100.000	100.000	0.000	
60	1090*	TestMerchant_C	26*	N*	BalanceNameAAUSOX*	130.000	130.000	0.000	USD
61	1090*	TestMerchant_C	27*	N*	BalanceNameJVEQKA*	0.000	0.000	0.000	RUB
62	1090*	TestMerchant_C	Total			130.000	130.000	0.000	
63	1091*	TestMerchant_C	28*	N*	BalanceNameJ3J4AY*	130.000	130.000	0.000	USD
64	1091*	TestMerchant_C	29*	N*	BalanceNameA79BPE*	0.000	0.000	0.000	RUB
65	1091*	TestMerchant_C	Total			130.000	130.000	0.000	
66	1092*	TestMerchant_C	30*	N*	BalanceNameMZQFOH*	100.000	100.000	0.000	USD
67	1092*	TestMerchant_C	31*	N*	BalanceNameCR9NSC*	0.000	0.000	0.000	RUB
68	1092*	TestMerchant_C	Total			100.000	100.000	0.000	

**Note**

The report scheduler will work only after all fields in all tabs are filled out.

The available reports to run Report Scheduler can be selected on the New Report Scheduler screen. To increase the number of available reports please contact Doc4.0 support team.



Configuration name - Report configuration name.

Report Name - Report name.

Generation Date - Report generation date.

Last Delivery Date - Date of the last report generation.

Delivery address - Delivery address of the report.

Scheduled - Report schedule.

Reports Scheduler						Schedule
Sched ↑	Rep	Generation Date	Last Generation Date	Delivery Address	Scheduled	
1 Test Config	71 Merchant balance report	03.12.2024 14:36	26.12.2024 09:27	test@test.com	Once	

« ← 1 - 1 → 10 25 50

## 7.4.2 Configuration

### Report Filters

By clicking on Add Criteria the needed filter can be selected. Depending on the report the filters may change.

New Report Scheduler		Back
CONFIGURATION	SCHEDULE	OUTPUT
<b>Report Filters</b>		
Add criteria ▼		
<b>Report parameters</b>		
Report For... CSV ▼	Encode UTF-8 ▼	
Schedule Report		

### Report Parameters

This setting may change depending on the selected report. Available parameters for selection: MM, DD, YYYY, as well as dates to select the report period.

**New Report Scheduler** Back

---

CONFIGURATION
SCHEDULE
OUTPUT

---

**Report parameters**

Start  to End

Report For...  Encode

Schedule Report

## Report Format

Allows to choose the report format. Available parameters for selection:

CSV

**New Report Scheduler** Back

---

CONFIGURATION
SCHEDULE
OUTPUT

---

**Report Filters**

Add criteria

**Report parameters**

Report For...  Encode

Schedule Report

XLS

**New Report Scheduler** Back

---

CONFIGURATION
SCHEDULE
OUTPUT

---

**Report parameters**

Start  to End

Report For...  Encode

**Upload Report Template**

Upload

Schedule Report

PDF

**New Report Scheduler** Back

CONFIGURATION SCHEDULE OUTPUT

**Report parameters**

Start  to End

Report For...  Encode

Upload Report Template

Upload

## Encode

Allows you to choose the Encoding. Available parameters for selection:

UTF-8 and CP1251

**New Report Scheduler** Back

CONFIGURATION SCHEDULE OUTPUT

**Report parameters**

Start  to End

Report For...  Encode

UTF-8  
CP1251

## 7.4.3 Schedule

### Generate The Report

This option allows you to select the appropriate time for sending reports.

Once - By selecting this option, the report will be received once.

Hourly - By selecting this option, the report will be received every N hours.

Daily - By selecting this option, the report will be received every N days.

Weekly - By selecting this option, the report will be received every N weeks. It is possible to select a specific day, multiple days, or all days of the week.

Monthly - By selecting this option, the report will be received every N months.

### New Report Scheduler Back

CONFIGURATION **SCHEDULE** OUTPUT

**Generate the report**

ONCE  
 HOURLY  
 DAILY  
 WEEKLY  
 MONTHLY

every  weeks

**on**

Check All  
 Sunday  
 Monday  
 Tuesday  
 Wednesday  
 Thursday  
 Friday  
 Saturday

**first report date**

Start  to End

Date interval  
FROM\_LAST\_RUN\_DATE

Schedule Report

### First Report Date

An option that allows you to select the dates which will be included in the first report.

**New Report Scheduler** Back

CONFIGURATION SCHEDULE OUTPUT

**Generate the report**

ONCE  
 HOURLY  
 DAILY  
 WEEKLY  
 MONTHLY

every  months

**first report date**

to

Date interval

Schedule Report

### Date Interval

Date interval allows you to set the date filter parameters for the generated report.

FROM\_LAST\_RUN\_DATE - On each subsequent run, the report will contain data based on the date from the last run to the current one.

**New Report Scheduler** Back

CONFIGURATION SCHEDULE OUTPUT

**Generate the report**

ONCE  
 HOURLY  
 DAILY  
 WEEKLY  
 MONTHLY

every  months

**first report date**

to

Date interval

- FROM\_LAST\_RUN\_DATE
- CONFIGURED\_INTERVAL**
- LAST\_N\_DAYS

CONFIGURED\_INTERVAL - On each subsequent run, the report will contain data shifted from the initially set dates schedule.

**New Report Scheduler** Back

CONFIGURATION   SCHEDULE   OUTPUT

**Generate the report**

ONCE  
 HOURLY  
 DAILY  
 WEEKLY  
 MONTHLY

every  months

**first report date**

Start  to End

Date interval  
FROM\_LAST\_RUN\_DATE  
FROM\_LAST\_RUN\_DATE  
CONFIGURED\_INTERVAL  
LAST\_N\_DAYS

LAST\_N\_DAYS - On each subsequent run, the report will contain data for the last N number of days.

**New Report Scheduler**
Back

CONFIGURATION
SCHEDULE
OUTPUT

---

**Generate the report**

ONCE  
 HOURLY  
 DAILY  
 WEEKLY  
 MONTHLY

every  months

**first report date**

to

Date interval

LAST\_N\_DAYS ▲

---

FROM\_LAST\_RUN\_DATE

CONFIGURED\_INTERVAL

LAST\_N\_DAYS

Last N days

### 7.4.4 Output

Configuration Name - The name assigned to the configuration.

File Name - The name displayed in the file received via email.

Add date for file name - Adds the sending date (GMT+3) to the report received via email.

Zip - Sends the report in a ZIP file with the password specified in the Password field.

Delivery Server - Option that defines the server used to send reports. Currently only EMAIL option is available.

Email Subject - The name displayed as the subject of the email.

Add date for email subject - Adds the sending date (GMT+3) to the email subject received via email.

Address list - Email(s) to which the report will be sent. Multiple emails can be specified.

Test run after report schedule - Test run after report schedule.

**New Report Scheduler**
Back

CONFIGURATION
SCHEDULE
OUTPUT

---

Add date for file name

---

Zip

Delivery server
EMAIL
▼

Add date for email subject

Address list

example@email.com,example@email.com,example@email.com,example@email.com,example@email.com,example@email.com

Test run after report schedule

Schedule Report

## 7.5 Performance Report

This report displays the financial flow for the specified period. It also allows to view the number of successful and unsuccessful transactions. Flexible criteria setting allows to get the needed data: date range and type, currencies, card types, grouping of data.

If necessary, you can add additional criteria by clicking the Criteria: endpoints, projects, merchants, gates, processors, etc. The customized search criteria can be saved as a template for later use.

Preview of the report can be viewed by clicking on the Preview button.

The Report can be generated by clicking on the the Generate button.

An example of the resulting report is shown below:

Merchant ID	Merchant	Project ID	Project	Day Number	Day	Sale Amt	Sale Approved Cnt	Sale Declined Cnt	Decline Ratio	Reversal Amt
1456	ICE	1532	Test project Ice			100 108,84	12	1	0,00%	0,00
				260	2018-09-17	100 108,84	12	1	0,00%	0,00
				263	2018-09-20	98 986,84	11	1	0,00%	0,00
TOTAL						1 122,00	1	0	0,00%	0,00
						100108,84	12	1	0,00%	0,00

## 7.6 Merchant Daily Performance Report

This report displays the day-by-day financial flow for a given period.

If necessary, you can add additional criteria by clicking the Criteria: endpoints, projects, merchants, gates, processors, etc. The customized search criteria can be saved as a template for later use.

The report can be downloaded by pressing the Generate button.

An example of the resulting report is shown below:

Merchant ID	Merchant	Day Number	Day	Sale Amt	Sale Approved Cnt	Sale Declined Cnt	Decline Ratio	Reversal Amt	Reversal Cnt	Reversal Ratio	Chb Amt	Chargeback Cnt	Chb Ratio	Fraud Amt	Fraud Cnt	Fraud Ratio	Dispute Amt	Dispute Cnt	Dispute Ratio
		246	2018-09-03	0,00	0	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%
		247	2018-09-04	0,00	0	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%
		248	2018-09-05	0,00	0	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%
		249	2018-09-06	0,00	0	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%
		250	2018-09-07	0,00	0	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%
		251	2018-09-08	0,00	0	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%
		252	2018-09-09	0,00	0	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%
		253	2018-09-10	0,00	0	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%
		254	2018-09-11	0,00	0	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%
		255	2018-09-12	0,00	0	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%
		256	2018-09-13	0,00	0	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%
		257	2018-09-14	0,00	0	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%
		258	2018-09-15	0,00	0	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%
		259	2018-09-16	0,00	0	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%
		260	2018-09-17	98 986,84	11	1	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%
		261	2018-09-18	0,00	0	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%
		262	2018-09-19	0,00	0	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%
		263	2018-09-20	1 122,00	1	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%
		264	2018-09-21	0,00	0	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%
		265	2018-09-22	0,00	0	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%
		266	2018-09-23	0,00	0	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%
		267	2018-09-24	0,00	0	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%
		268	2018-09-25	0,00	0	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%
		269	2018-09-26	0,00	0	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%
		270	2018-09-27	0,00	0	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%
		271	2018-09-28	0,00	0	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%
		272	2018-09-29	0,00	0	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%
		273	2018-09-30	0,00	0	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%
TOTAL				100108,84	12	1	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%	0,00	0	0,00%

## 7.7 Decline Statistics

This report allows to get statistics on rejected transactions, which are divided into the following groups: rejected by the acquiring bank, rejected by internal fraud system and rejected due to an internal error.

If necessary, you can add additional criteria by clicking the Criteria: endpoints, projects, merchants, gates, processors, etc. The customized search criteria can be saved as a template for later use.

Preview of this report can be viewed by clicking on the Preview button.

The Report can be generated by clicking on the the Generate button.

An example of the resulting report is shown below:

Sandbox; Date range: 2023-08-01 00:00:00/2023-08-31 23:59:59; Card types: [ALIPAY, AMEX, ANY\_CREDIT\_CARD, ASTROPAY, ASTROPAY CARD, BITCOIN, CABAL, CASH, CASHU, COMPROCARD,

**Decline Statistics for 01-Aug-2023 - 01-Sep-2023**

**System errors**

()

**Filter declines**

[10165] Manager loyal destination card number check failed (62)	9
[10166] Manager loyal source card number check failed (58)	8
[10159] Customer purpose blacklisted for manager (49)	7
[10160] Destination card number blacklisted for manager (48)	7
[10162] Source card number blacklisted for manager (46)	7
[10161] E-mail domain blacklisted for manager (46)	7
[10158] Customer ip-address blacklisted for manager (46)	7
[10156] Customer e-mail blacklisted for manager (40)	6

## 7.8 Fraud/Chargeback Ratio Report

Calculates the indicators of negative statistics on the MID accounts.

If necessary, you can add additional criteria by clicking the Criteria: endpoints, projects, merchants, gates, processors, etc. The customized search criteria can be saved as a template for later use.

Data can be downloaded by pressing the Generate button.

An example of the resulting report is shown below:

Sandbox; Date range: 2000-01-01 00:00:00/2999-12-31 00:00:00					Chargeback Count			Chargeback Ratio			Chargeback Amount	
Gate ID	Gate Descriptor	Currency	Merchant ID	Merchant	M	V	Total	M	V	Total	M	V
79523	TestGate	USD	770	TestMerchant	0	2	2	0,00%	0,00%	0,00%		645
79558	TestGate1	USD	770	TestMerchant	0	0	0	0,00%	0,00%	0,00%		
79812	TestGate2	USD	770	TestMerchant	0	0	0	0,00%	0,00%	0,00%		
80479	TestGate3	EUR	770	TestMerchant	0	0	0	0,00%	0,00%	0,00%		
80480	TestGate4	EUR	770	TestMerchant	0	0	0	0,00%	0,00%	0,00%		
80481	TestGate5	EUR	770	TestMerchant	0	0	0	0,00%	0,00%	0,00%		
80487	TestGate6	USD	770	TestMerchant	0	0	0	0,00%	0,00%	0,00%		
80669	TestGate7	USD	770	TestMerchant	0	0	0	0,00%	0,00%	0,00%		
81359	TestGate8	USD	770	TestMerchant	0	0	0	0,00%	0,00%	0,00%		
81366	TestGate9	USD	770	TestMerchant	0	0	0	0,00%	0,00%	0,00%		
82307	TestGate10	USD	770	TestMerchant	0	0	0	0,00%	0,00%	0,00%		
167364	TestGate11	USD	770	TestMerchant	0	0	0	0,00%	0,00%	0,00%		

## 7.9 Fraud/Chargeback Reasons Report

Displays a report on the causes of chargebacks for the selected parameters.

If necessary, you can add additional criteria by clicking the Criteria: endpoints, projects, merchants, gates, processors, etc. The customized search criteria can be saved as a template for later use.

Data can be downloaded by pressing the Generate button.

An example of the resulting report is shown below:

	A	B	C	D
1	Sandbox:	Date range: 2000-01-01 00:00:00/2999-12-30 23:59:59; Transaction types: [chargeback, fraud]		
2	<b>Fraud and Chargeback Reasons Report for 01-Jan-2000 - 31-Dec-2999</b>			
3	<b>Transaction Type</b>	<b>Reason Code</b>	<b>Name</b>	<b>Transactions Count</b>
4	chargeback	11.2	Declined Authorization	1
5	<b>TOTAL</b>			<b>1</b>

## 7.10 Gate Details Report

Displays the amount of successful transactions in the context of gates.

If necessary, you can add additional criteria by clicking the Criteria: endpoints, projects, merchants, gates, processors, etc. The customized search criteria can be saved as a template for later use.

Data can be downloaded by pressing the Generate button.

An example of the resulting report is shown below:

Sandbox: Date range: 2023-08-01 00:00:00/2023-08-31 23:59:59										
Gate details report for 01-Aug-2023 - 01-Sep-2023										
Warning: Property for reports.gateDetails.gateId	Gate name	End-Point ID	End-Point name	Project ID	Project name	Merchant ID	Merchant name	Transaction type	Transaction status	Currency
75923	TestGate1	46748	TestEndpoint1	36915	TestProject1	770	TestMerchant	chargeback	approved	USD
79812	TestGate2	39915	TestEndpoint2	36915	TestProject2	770	TestMerchant	sale	approved	USD
79812	TestGate2	39915	TestEndpoint2	36915	TestProject2	770	TestMerchant	transfer	approved	USD
79812	TestGate3	39915	TestEndpoint3	36915	TestProject3	770	TestMerchant	transfer	filtered	USD
<b>Total by USD</b>										

## 7.11 Processor Detailed Report

Displays earnings details grouped by processor.

If necessary, you can add additional criteria by clicking the Criteria: endpoints, projects, merchants, gates, processors, etc. The customized search criteria can be saved as a template for later use.

Data can be downloaded by pressing the Generate button.

An example of the resulting report is shown below:

Sandbox: Date range: 2023-08-01 00:00:00/2023-08-31 23:59:59; Project currency: USD																				
Processors Detailed report																				
	Transaction Amount	Approved Count	Transfer Amount	Approved Transfers Count	Reversal	Reversals Count	Cancel	Cancel Count	Refund	Refunded Count	Fraud	Fraud Count	Chargeback	Chargeback Count	Held by reseller	Held by project	Held by provider	Reseller carryover		
Grand Total:	460,00	4	150,00	1	0,00	0	0,00	0	0,00	0	0,00	0	0,00	0	0,00	0,00	0,00	0,00	12,30	
Reseller earnings:																		0		
Manager earnings:																		0		
Processor	test processor 5																			
Merchant	Merchant ID	Transaction Amount	Approved Count	Transfer Amount	Approved Transfers Count	Reversal	Reversals Count	Cancel	Cancel Count	Refund	Refunded Count	Fraud	Fraud Count	Chargeback	Chargeback Count	Held by reseller	Held by project	Held by provider	Reseller carryover	
TestMerchant	770	,00	0	,00	0	,00	0	,00	0	,00	0	,00	0	,00	0	,00	,00	,00	,00	12,30
Total:		,00	0	,00	0	,00	0	,00	0	,00	0	,00	0	,00	0	,00	,00	,00	,00	12,30
Reseller earnings:																		0		
Manager earnings:																		0		

## 7.12 Close Day Report

Displays the exact time when the close day procedure for settlement was performed on each gate.

If necessary, you can add additional criteria by clicking the Criteria: endpoints, projects, merchants, gates, processors, etc. The customized search criteria can be saved as a template for later use.

Data can be downloaded by pressing the Generate button.

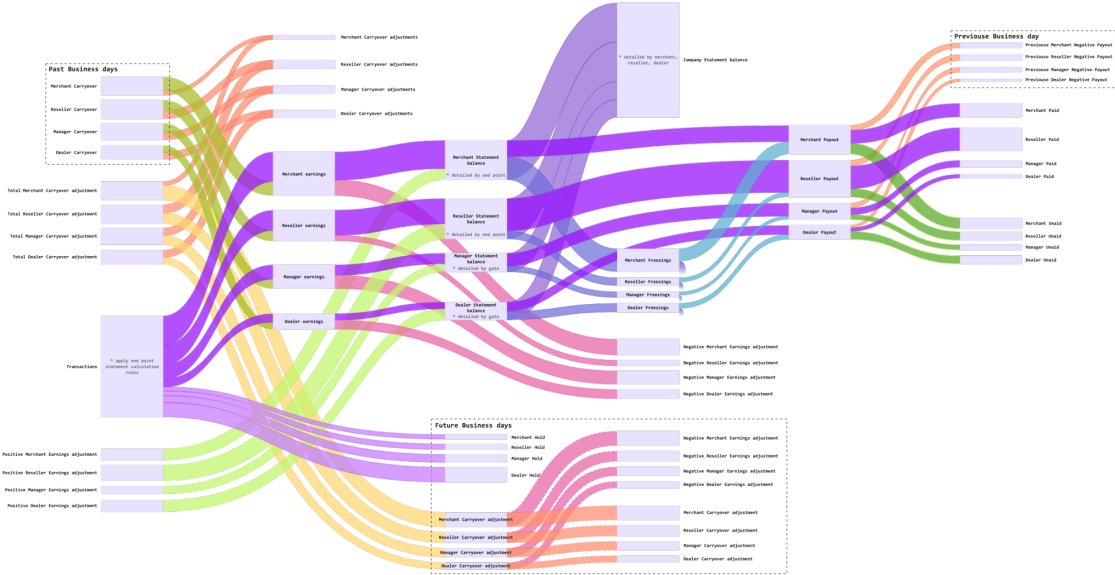
An example of the resulting report is shown below:

Sandbox; Date range: 2023-06-01 00:00:00/2023-08-31 23:59:59			
Close Days Report			
[Warning: Property for 'safeld' not	Gate Name	MID	30.06.2023
79523	TestMerchant		2023-06-30 23:59:00 (close date is Fri Jun 30 09:33:28 MSK 2023)
79524	TestMerchant		2023-07-31 23:59:00 (close date is Sun Jul 31 09:30:00 MSK 2023)

## 7.13 Statements

- [Main Information](#)
- [Statements Calculation Parameters](#)
- [Delay](#)
- [Holding](#)
- [Preliminary Review Of Future Statements](#)
- [Statement Adjustments](#)
- [Earnings Adjustments](#)
- [Carryover Adjustments](#)
- [Statements Calculation Sequence](#)
- [Viewing Statements](#)
- [Freezing Of Payments](#)
- [Making Payments](#)

### 7.13.1 Main Information



Doc4.0 platform contains integrated calculation system to reflect the tariffication between business process partners. Calculation happens on each level, from dealer to merchant. Bank fees are calculated for tariffication and settlement, but statements for settlement with the bank are not provided by the system. Instead, the system calculates statements per Merchant and indicates which exact amount should be received from the bank. Statement is individually generated for each manager or each merchant of this manager. Statement date is called business day. Statement for business day contains all projects for chosen manager. Statements will be calculated for manager if such option is enabled. If statement should be calculated, enable the Default calculate statements flag in manager account details. If this option is not enabled, statements setting in projects of exact manager will be unavailable and statements are not calculated.

**Manager** Cancel Save

Login\*

Password h2mz5O-P Generate new password

Display Name\*

E-mail\*

Control Key E2AA4390-25FA-4780-AFA3-AB959C02A042 Generate New Control Key


Show last gate filter error

Project code

Counterparty MA

Default 'calculate statements'

White label\*

Logo 

API IPs/masks whitelist

Returning customer approve sessions count\*

1

Name\*

Surname\*

Organization

Tags

Login IPs/masks whitelist

Statements can be calculated manually or automatically. Automatic statements calculation starts every 2 hours. Statements menu also has options to create new statement or delete



statement that already exists.

After deleting the statement, all information about paid and frozen amounts is lost forever. Only last business day can be deleted. Deleted statements must be recalculated sequentially from a lesser date to the next. Otherwise, if statements are recalculated by jumping over several dates, then intermediate business periods will be included in one.

## Statements settings

2021-04-12 test manager	Delete statements
2018-04-10 Dummy Manager	Delete statements
2021-04-12 manager1	Delete statements
2018-04-09 Good Idea Technologies	Delete statements

Managers are able to count statements only for themselves and their merchants, superiors are also able to calculate statements for their managers. Positive balances from previous months do not carry over. Negative balances are taken into account in the current period as a balance for the beginning of the period. A separate statement is generated for each currency. If the counterparty has projects in different currencies, then several statements will be generated for each currency.

### 7.13.2 Statements Calculation Parameters

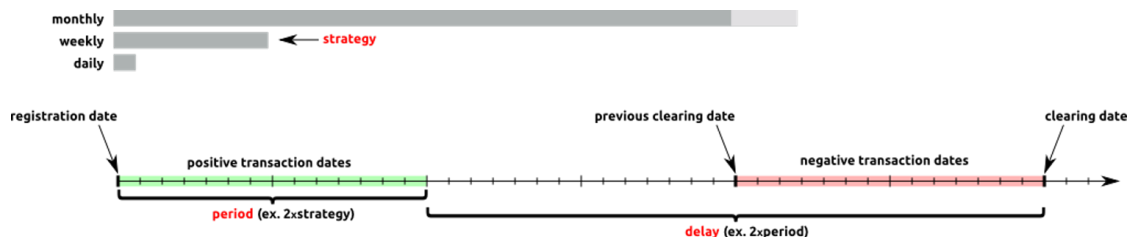
The calculation of statements begins with the definition of a list of transactions, which are included in the specified business period. All transactions are conditionally divided into the following types:

1. Reducing the merchant's balance (chargeback, reversal and etc.)
2. Increasing the merchant's balance (sale, capture and etc.)

The system supports Hold mechanism to determine the list of positive transactions that will be included in statement and Delay mechanism to reduce risks in settlements with counterparties.

### 7.13.3 Delay

Delay — is a mechanism for short-term postponement of payments for positive transaction volumes, which allows to form a safety cushion equal to the average merchant's turnover for the paid period. It allows to minimize the risks of negative activity during the merchant's work.



The payment strategy, its frequency and delay can be configured on endpoint level. The following strategies are supported:

1. daily payments, payment periods and delay are defined in days,
2. weekly payments, payment periods and delays are determined in weeks, statements are generated on Mondays,

3. monthly payments, payment periods and delays are determined in months, statements are generated on the first day of each month.

The start date of payment period, as well as any other derivative dates obtained during the formation of statements, can not be less than the endpoint registration date.

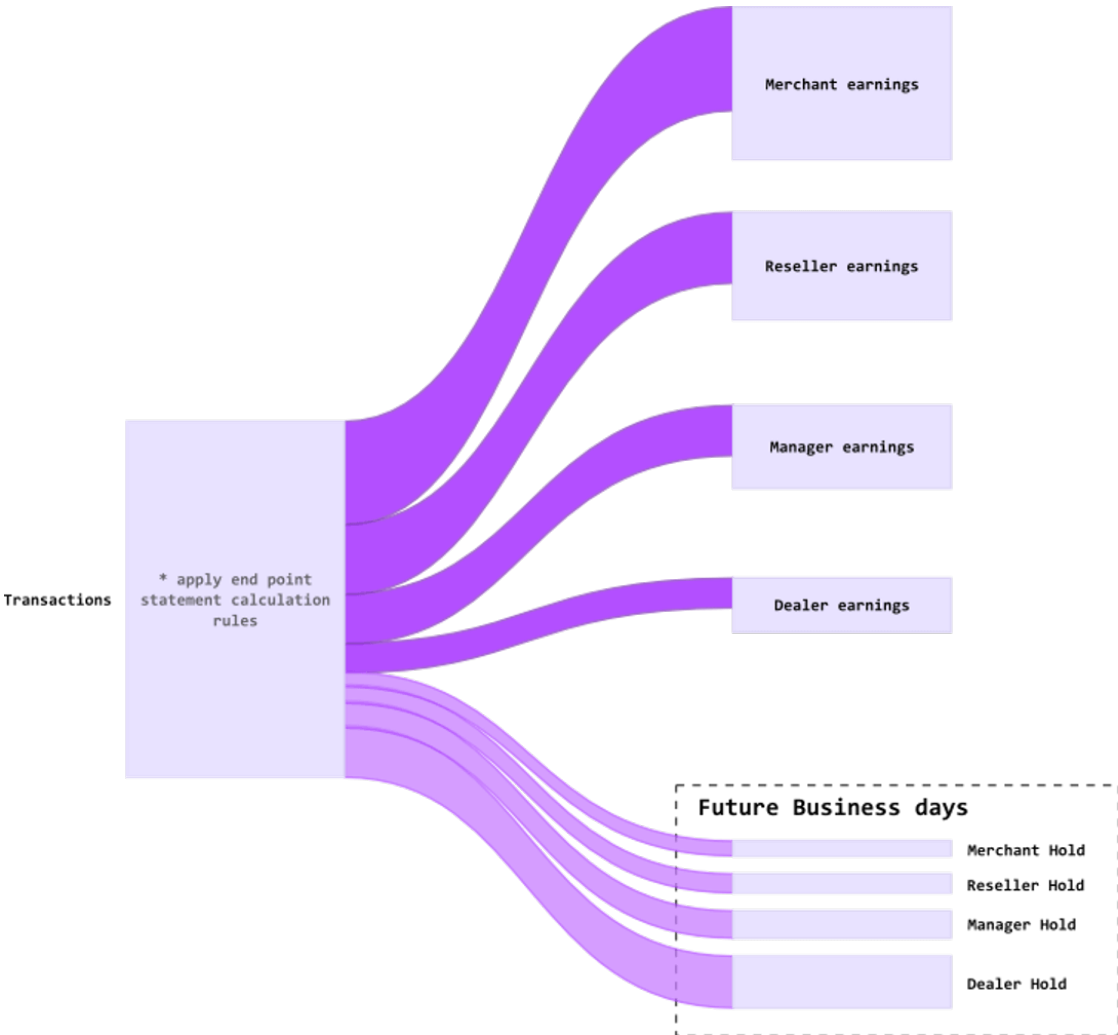
Payment **Period** determines the regularity of business days. For example, if the payment strategy is weekly, and the period is two, then the statements are generated every two weeks. The minimum period is one.

Payment **Delay** determines the number of periods for which the funds received for positive transactions will be delayed before they are paid to the counterparty. For example, if the statements are calculated monthly with a payment period once a month, then, if the delay period is set to one period, the merchant will receive money for positive transactions for the second-to-last month, instead of the last one. The merchant will be able to receive money for the last month only next month. Negative transactions accounted in the statement ignore the delay period to minimize risks.

Statements are calculated using the latest delay parameters configured at the endpoint. This allows to recalculate the statements for the previous business days using the new parameters.

#### **7.13.4 Holding**

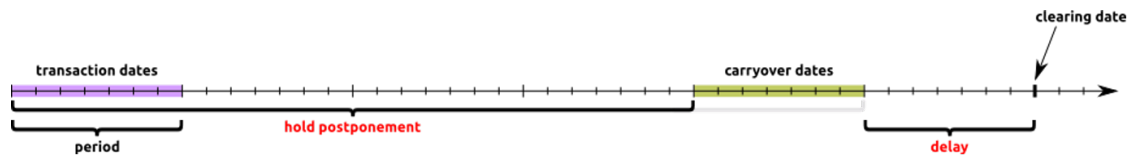
Holding — is a mechanism for medium- and long-term postponement of payments for positive transaction volumes. It allows to form a safety cushion to repay negatives received after the end of the merchant's work.



The amount to be paid for positive transactions that is included to the statement may be partially withheld for periods comparable with dispute flow and fraud claims. Holding mechanisms are used for this purpose. Holding period and amount are specified in the rate plan. The hold period is set in days. The hold value is set in percent. It is not possible to change these values after calculating the rates for the processed transaction. Each transaction has a unique period and a holding percentage calculated on the date of its processing.

Transactions																													
Date / Bank / Settle	Transaction	Details																											
10-03-2026 06:03	<input checked="" type="checkbox"/> sale	Amount: 10.00	Gate: [276022] BalanceByCoefficient...	External Order ID: [TST] PNTEST-24348957																									
-	-	Commission: 0.00	MID:	External Method: -																									
-	-	Hold: 0.00																											
Originator:		RRN: 606914421392	Loyalty message:																										
Auth. code: 321875	Auth. Credit code: 716086	XID:																											
Auth. status: N	ECI:	CAVV:	Loyalty program:	Bonus balance:																									
			Debit ARN: 804086892																										
			Credit ARN: 225540908																										
<table border="1"> <thead> <tr> <th></th> <th></th> <th>Rate</th> <th>Fee</th> <th>Hold</th> <th>Carryover date</th> </tr> </thead> <tbody> <tr> <td>Bank</td> <td>Gate rate: Zero rate by ATManagerLoginYPZVAX &gt; Range 0.000 - ∞</td> <td>0.00</td> <td>0.00</td> <td>0.00</td> <td>08.09.2026</td> </tr> <tr> <td>Manager</td> <td>Project rate: Zero rate by ATManagerLoginYPZVAX &gt; Range 0.000 - ∞</td> <td>0.00</td> <td>0.00</td> <td>0.00</td> <td>08.09.2026</td> </tr> <tr> <td>Provider</td> <td>Project rate: Zero rate by ATManagerLoginYPZVAX &gt; Range 0.000 - ∞</td> <td>0.00</td> <td>0.00</td> <td>0.00</td> <td>08.09.2026</td> </tr> </tbody> </table>								Rate	Fee	Hold	Carryover date	Bank	Gate rate: Zero rate by ATManagerLoginYPZVAX > Range 0.000 - ∞	0.00	0.00	0.00	08.09.2026	Manager	Project rate: Zero rate by ATManagerLoginYPZVAX > Range 0.000 - ∞	0.00	0.00	0.00	08.09.2026	Provider	Project rate: Zero rate by ATManagerLoginYPZVAX > Range 0.000 - ∞	0.00	0.00	0.00	08.09.2026
		Rate	Fee	Hold	Carryover date																								
Bank	Gate rate: Zero rate by ATManagerLoginYPZVAX > Range 0.000 - ∞	0.00	0.00	0.00	08.09.2026																								
Manager	Project rate: Zero rate by ATManagerLoginYPZVAX > Range 0.000 - ∞	0.00	0.00	0.00	08.09.2026																								
Provider	Project rate: Zero rate by ATManagerLoginYPZVAX > Range 0.000 - ∞	0.00	0.00	0.00	08.09.2026																								

When specifying the duration of the delay, please note that the holding period, specified in the rate plan during the carryover payment, does not include the payment delay period, specified in the endpoint settings. This is done in order to avoid holding payments until the main amount is paid, with a large delay in payments and a small delay in the hold. I.e., if the holding period for the transaction is one day for daily payments with a frequency of one day and a delay of three days, the carryover for the transaction will be paid in 4 days from the moment of its processing.



### 7.13.5 Preliminary Review Of Future Statements

It is possible to view statements for future dates before they are generated, in order to be able to predict the necessary amounts to be paid on company accounts. The number of periods for which the preview is available is set in the user profile.

## Your profile TestManager135271 (manager)

---

Name	Erwin Thomas
Language	Auto
E-mail	test@gmail.com
Phone	
Default currency	USD
Statement preview limit	5
PGP key	Not specified
CSV delimiter	Detect automatically
Telegram Bot	<a href="#">Register Telegram Bot</a>
Mask request/response logs	Enabled
Enable new menu	Yes
Enable new dashboard	Yes

The calculation of payment dates when generating the statement and its preview differs from each other. When calculating the preview dates, the delay parameters specified for the endpoint are strictly taken into account. When calculating dates during the scheduled formation of the statement, the start date of the business period is shifted to the end date of the last available business period. This feature is useful when generating statements that include several payment periods and when changing the payment period or delay. If the dates grid, obtained when calculating payment periods, differs from the actual payment dates (for example, when parameters for calculating statements are changed and statements the previous business days are not recalculated) the preview might not be available for a future date or the start dates of the period will be incorrect.

### 7.13.6 Statement Adjustments

Statements can take into account not only the transaction commission. The statement balance can be changed by means of adjustments that can be accrued for any counterparty from the dealer to the merchant. Adjustments can be applied to the statement on a special screen in the menu “Reports” - “Statements” - “Adjustments”.

✕

**Create adjustment**

Adjustment date\*:  17

Merchant\*:  Q

End point:  Q

Reseller:  Q

Manager\*:  Q

Adjustment type\*:  v

Adjustment amount\*:

Currency\*:  v

Deduction type\*:  v

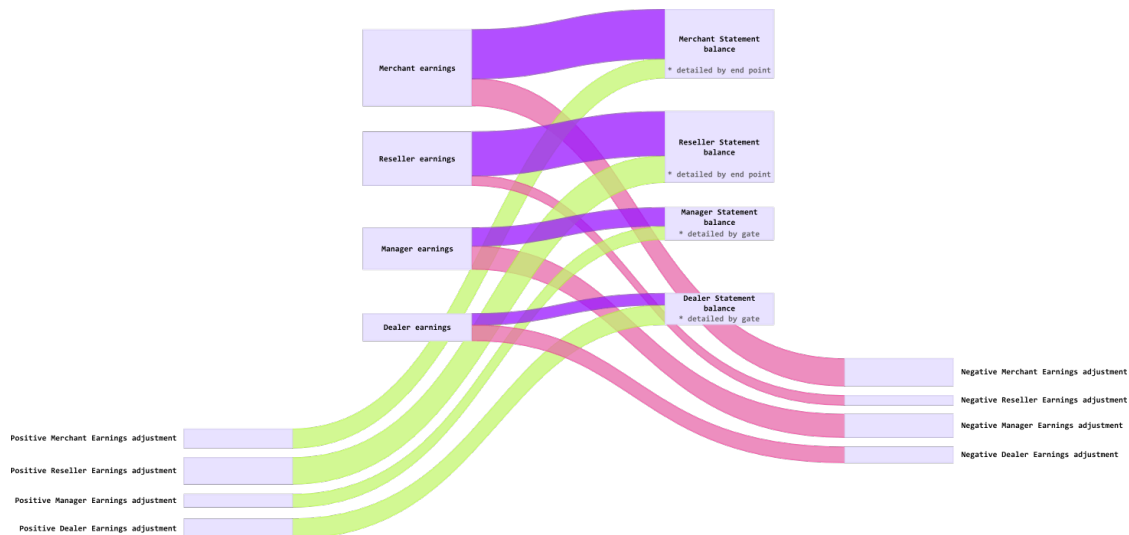
Comment:

Create
Cancel
⋮

There are two types of adjustments:

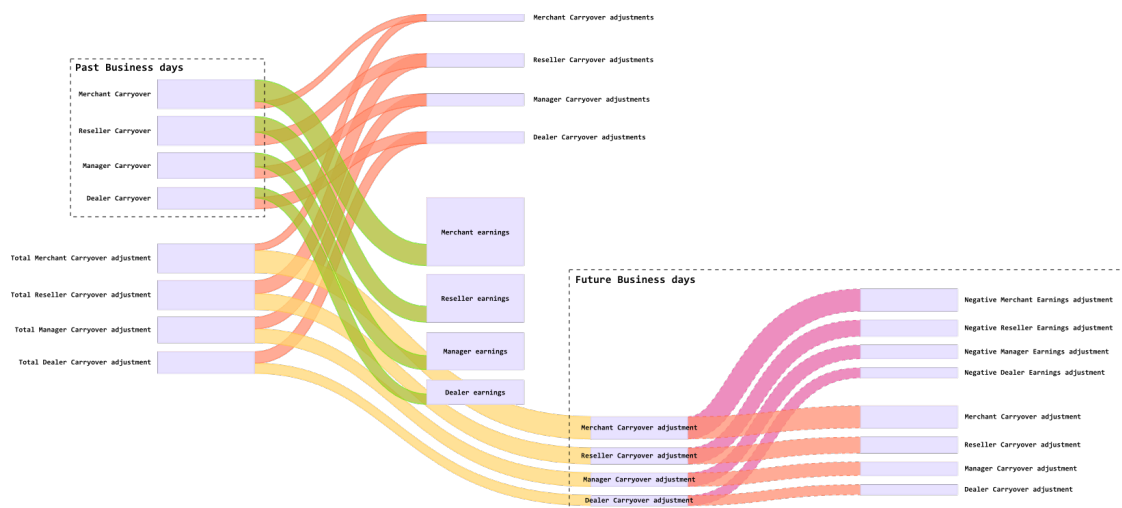
1. earnings adjustment - certainly changes the client’s balance in the current statement by the full amount of the adjustment,
2. carryover adjustment-changes the amount of the paid carryover for the selected number of periods.

### 7.13.7 Earnings Adjustments



The adjustment of earnings can both reduce the statement balance in case of fines, and increase it in case of erroneous billing. The statement takes into account adjustments whose date is less than the date of the statement formation, which were not taken into account in earlier statements. The adjustment can be initiated with the indication of the endpoint. In this case, it will be displayed in the details of the endpoint in the statement, changing its balance. If the endpoint is not specified, the adjustment will be listed in the statement header. Statements for the merchant are generated on behalf of the reseller, if it is available on the project, for the reseller to manage the merchant’s statements. If there is no reseller, statements are generated directly from the manager. Similarly, an adjustment can be made for the merchant. If a reseller is selected when creating an adjustment, an extract will be generated on behalf of the reseller, indicating this adjustment. If the earnings adjustment is included in the statement, then it cannot be changed (except for the comment) or deleted.

### 7.13.8 Carryover Adjustments



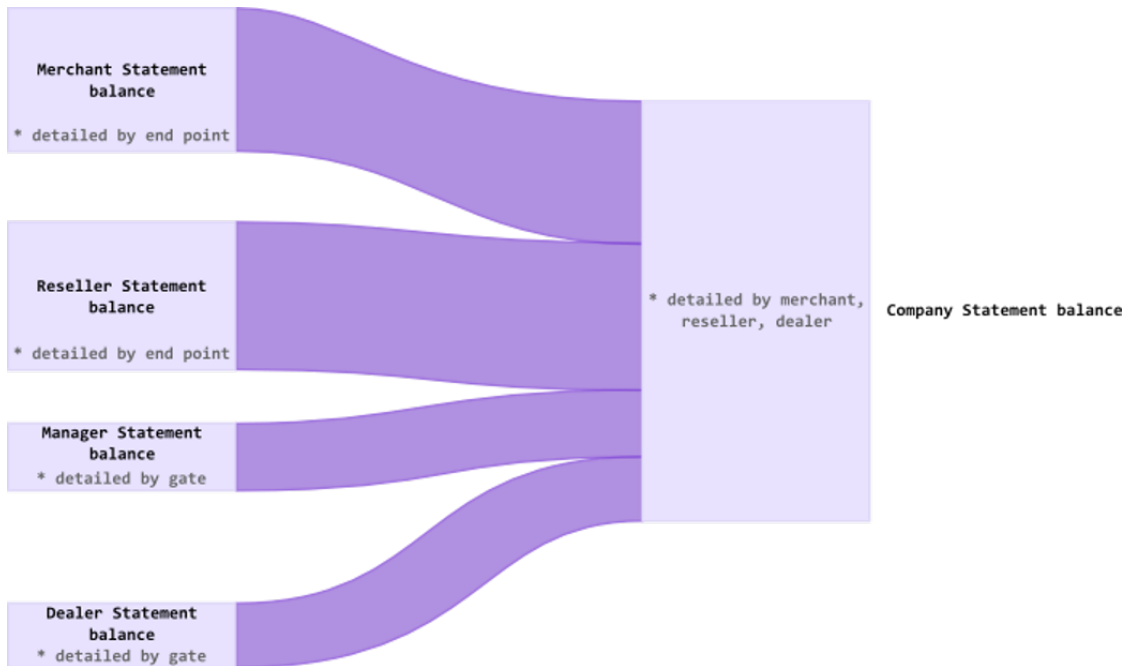
The second type of adjustments can only reduce the statement balance. Carryover adjustments, according to the name, are deducted from the paid hold. If an endpoint is specified when creating an adjustment, the adjustment will be deducted exclusively from the carryover

of this endpoint. If the endpoint is not specified, the adjustment will reduce the entire available carryover of the merchant in exact statement. Unlike earnings adjustments, carryover adjustments can be accounted for in multiple statements. The unaccounted part of the adjustment is transferred to the calculation in the next period. The maximum number of business days in which the adjustment should be taken into account is set by the “Max deduction periods” parameter. If this parameter is zero, the number of business days to be debited is assumed to be equal to infinity. The maximum amount of application of the carryover adjustment in the current billing period is limited to the maximum amount of the carryover, if the current number of statements in which this adjustment was taken into account does not exceed the “Max deduction periods” parameter. If this parameter is exceeded, the unaccounted amount of the adjustment is converted into an earnings adjustment. Creating positive carryover adjustments in the system is prohibited.

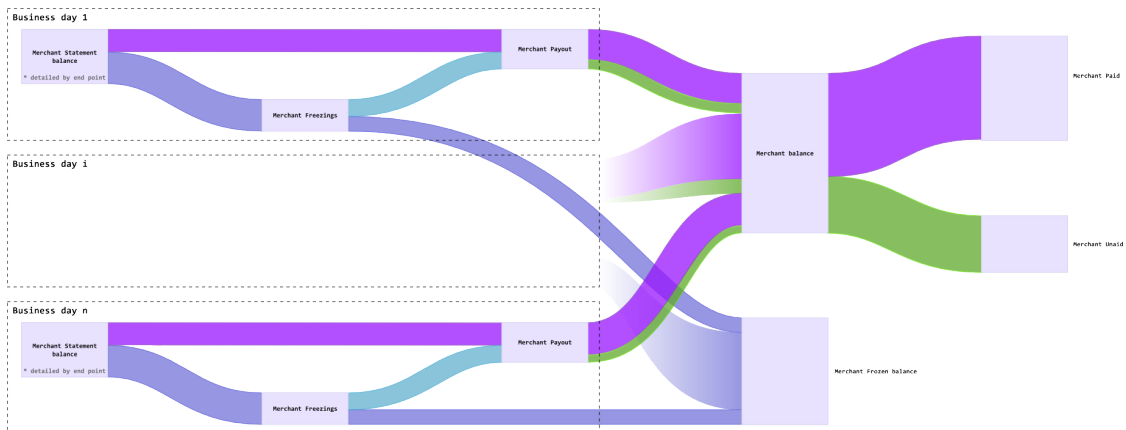
### **7.13.9 Statements Calculation Sequence**

The statements are calculated in the following order:

1. the dealer’s statements are generated. First, the dealer’s statements are detailed by gates. Then the adjustments of the carryover paid to the dealer from the bank are applied. After that, earnings adjustments are calculated. The final balance of the current period is calculated as follows: to the difference between the bank and dealer cold, add the difference between the applied bank and dealer transaction commissions. In the final, the bank carryover is added minus the carryover adjustments and the carryover paid by the dealer is deducted.
2. the manager’s statements are generated, the manager’s statements are detailed by gates; adjustments are applied to the carryover paid to the manager from the dealer or the bank in his absence; earnings adjustments are calculated; the final balance of the current period is calculated as: the difference between the dealer (bank) and the manager’s hold add the difference between the applied dealer (bank) and manager transaction commissions; in the final, the dealer (bank) carryover is added minus the carryover adjustments and the carryover paid by the manager is deducted,
3. reseller statements are generated, reseller statements are detailed by endpoints; adjustments of the carryover paid to the reseller from the manager are applied; earnings adjustments are accrued; the final balance of the current period is calculated as: the differences of the manager’s and reseller’s hold add the difference of the applied manager’s and reseller’s transaction commissions; in the final, the manager’s carryover is added minus the carryover adjustments and the carryover paid by the reseller is deducted,
4. merchant statements are generated, merchant statements are detailed by terminals, indicating the reseller; adjustments are applied to the carryover paid to the merchant from the reseller or manager in his absence; earnings adjustments are accrued; the final balance of the current period is calculated as: the difference between the reseller (manager) and merchant transaction commissions applied; in the final, the reseller (manager) carryover is added minus the carryover adjustments and the amount of the merchant’s transactions excluding the amount of service operations and a Money Transfer type operation,
5. after the formation of statements for all counterparties are combined into statements for companies; statements for companies are detailed by merchant, reseller, dealer and manager, for the possibility of accounting for paid funds on the company’s balance sheet; of all the carryovers and holds, only the bank’s carryover and hold are taken into account in the company’s statements.



The calculated balance of the current period for each type of user is added to its current balance. The balance is maintained individually for each currency. For merchants, the balance is also detailed by the reseller, if available. The company’s balance sheet is not taken into account. The counterparty’s current balance is defined as the sum of the current balance of all its statements, minus paid and frozen funds.



### 7.13.10 Viewing Statements

The statements are viewed in “**Reports**” - “**Statements**”. On this screen, statements can be sorted by currencies, merchants, resellers and dealers, as well as by the payment status (“All”, “Frozen”, “Not paid”) and date range. Using the date range, you can select the date of the statement that you want to upload.

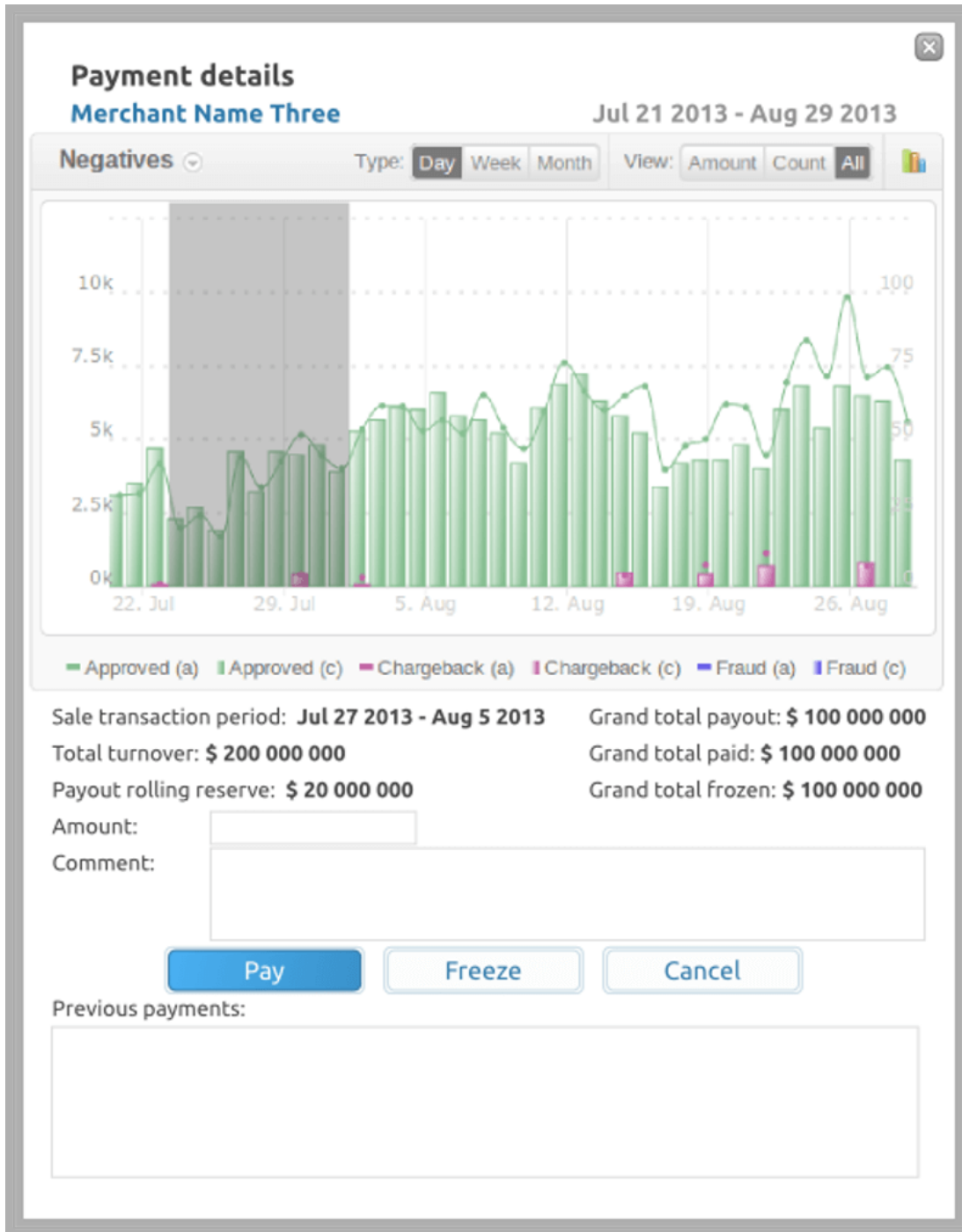


### **7.13.11 Freezing Of Payments**

Frozen payment status in the advanced search can be used to manage statements for which payments have been suspended. The mechanism for freezing payments is used in cases of detecting suspicious activity of the counterparty, or receiving information from the bank about the impossibility of making payments on the current statement for unspecified reasons for an indefinite period, until any disputed issues are resolved. Frozen funds reduce the counterparty's balance for payment. Frozen funds are managed within one business period. The amount of the frozen funds can not exceed the amount of payment of the current statement.

### **7.13.12 Making Payments**

In order to minimize possible losses, relevant information is displayed in the payment window.



After clicking on the amount to be paid, the first graphical component of the analytics panel is displayed, with the following conditions:

1. chart type-negatives,
2. date range: from the beginning of the period of positive transactions included in one of the previous statements to the current date, a total of at least 5 recent periods when paying for the last business day and more when paying for the previous business days
3. axes — sum, quantity,

4. advanced search — for everyone except the merchant: the traffic of all merchants that included in this statement; for the merchant-directly the merchant; all taking into account the currency,
5. the graph shows an interval that displays the period of positive transactions that included in this statement,
6. the following data is displayed for informational purposes. According to the current statement — the period of positive transactions, the amount of transactions of the sale (capture) type, the amount of transactions of the transfer type, the number of transactions of the service type, the held hold. Total — unpaid balance, amount paid, frozen balance. A list of all payouts with a comment is also displayed.

Doc4.0 has several reporting formats for cashflow and performance view, reconciliation and usage in external systems, as well as the ability to flexibly configure data that is displayed in reports. This section covers in detail the functionality of the system for display and download of reports in Excel and CSV format.

Doc4.0 UI allows to generate the following types of reports:

<i>Cashflow Report</i>	Calculates sales, manager turnover, returns, chargebacks, holds. Shows distribution of turnover by tariffs. Shows profit for the period and broken down by days.
<i>Transaction Report</i>	List of transactions for a specific period of time. This type of report is most suitable in cases where it is necessary to reconcile transactions with the bank.
<i>Merchant Cashflow Report</i>	Calculates the turnovers and profits of the merchant date-by-date.
<i>Performance report</i>	Calculates the quantity and total volume of approved and declined transactions, reversals, chargebacks, transactions to which the fraud marker was applied, and the percentage of all unsuccessful financial transactions (declined, reversal, chargeback, fraud) in relation to approved transactions.
<i>Merchant Daily Performance Report</i>	This report allows to generate a summary date-by-date list of transactions with the following types: sale, reversal and chargeback.
<i>Decline Statistics</i>	Displays statistics on rejected transactions, divided into the following groups: rejected by the acquiring banks, rejected by Doc4.0 internal fraud system and rejected due to various errors in processing, should this occur.
<i>Fraud/Chargeback Ratio Report</i>	The chargeback ratio calculates the indicators of negative statistics for the merchant's terminals.
<i>Fraud/Chargeback Reasons Report</i>	Builds a report on merchant chargeback reasons.
<i>Gate Details Report</i>	The report displays detailed information about the amounts of transactions in the context of payment gateways.
<i>Processor Detailed Report</i>	The report displays earnings details grouped by processor.

continues on next page

Table 1 - continued from previous page

---

<i>Close Day Report</i>	The report on closing days displays the exact time when the settlement day was closed at the gateways.
<i>Statements</i>	The integrated system that calculates statements per merchant and indicates which exact amount should be received from the bank for each statement date. Alternative approach to merchant balance calculation.

---

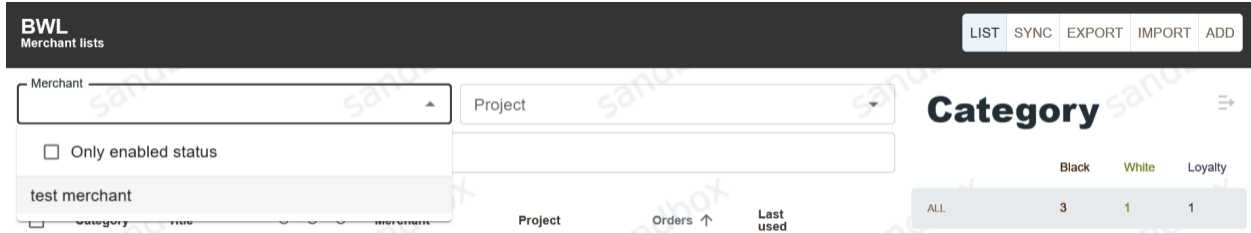
## 8.1 Black, White And Loyalty Lists

- *Overview*
  - *Black Lists*
  - *White Lists*
  - *Loyalty Lists*
- *Adding New Elements To BWL*
- *Importing Lists*
- *Exporting To File*
- *Synchronizing Lists*
  - *Merchant*
  - *Gate*
- *Available Lists For Every Role*
- *Comments*
- *Order Details: Configuring BWL Lists*

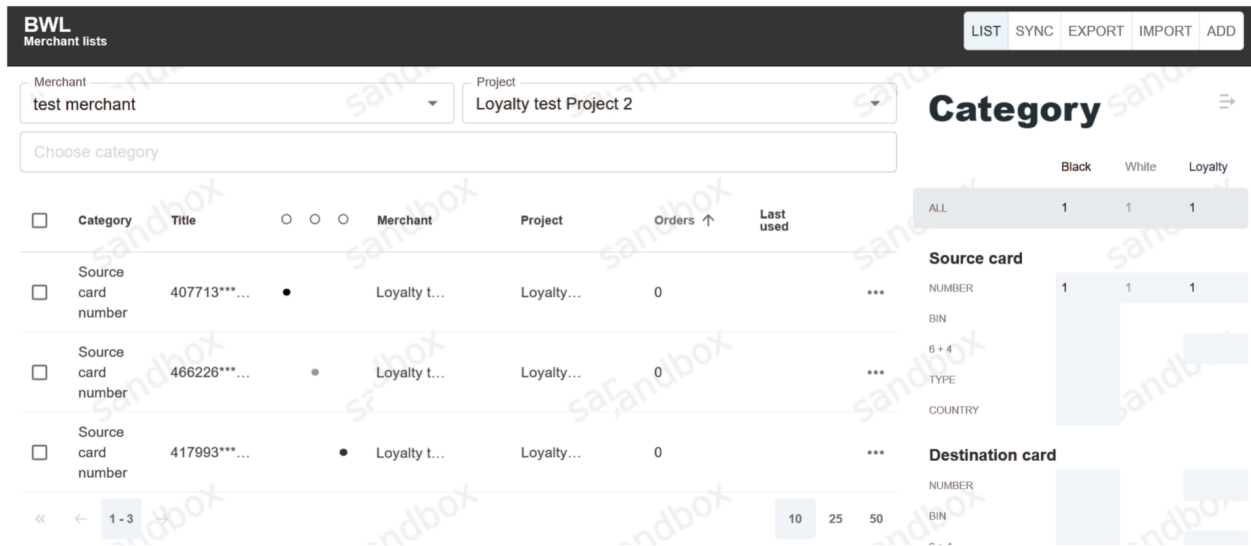
### 8.1.1 Overview

There are 3 types of access control lists, which work as filter checks in Payment Gateway. Lists are being checked while processing the transaction when the respective filter gets applied. BWL screen is designed to manage white, black and loyalty customer lists. This screen is located in "Tools" -> "Black & White lists". It makes the process of putting the transactions' attributes to respective lists faster and easier. It also has quick search which helps to find the exact transaction attribute added previously.

In order to select entries from list, specify manager and merchant/gate/processor for corresponding lists from dropdown menu.



It is possible to show any specific category from a certain list by clicking it in Category list to the right.



**Note**

Lists are being checked while processing the transaction when the respective filter gets applied.

Processor lists will be available for choosing only after you set up gate with this processor in Project Strategy/Balancing Beta. Gate lists are be available after setting up this gate in Project Strategy/Balancing Beta.

**Black Lists**

The first filter checking transaction attributes (email, IP, address, etc) is “Manager/Merchant black list”. It is possible to manage these attributes (excluding BIN) from the Order details screen. The attributes can have the following statuses:

- attribute is in black list
- attribute is not in black list

If any transaction attribute matches attribute in the lists and respective filter is enabled at the Project's level, the transaction status is set to Filtered and the reason for filtering is saved in the transaction data (see [Error Codes in Transaction Filters](#)<sup>2</sup> section in integration documentation).

For blacklisting IP addresses, it is important to note that most customers have dynamic IP which can be possessed by different customers of the same Internet provider. Mobile Internet users change IP address each time a session is created. It is also known that customers using traffic compression services (e.g. Opera Mobile) come via IP address of the proxy server provided by the service, most of which are located in Europe. According to statistics, if IP address is denied for more than 10 hours, the filtering will be in 80% cases false positive. This is why it is not recommended to filter transactions by IP without proper control. It is highly recommended prior to adding IP address into the black list to check with the Internet provider what maximal period of IP address denial can be applied. It is also important to check if the given IP address is in any third-party anti-spam systems.

### White Lists

White list allows to skip additional filter checks for transactions with attributes in this list. The only attributes for whitelisting are: a card number and a customer DNA.

#### Note

If the attribute is found in any white list the third-party fraud control systems' checks are excluded either.

### Loyalty Lists

Loyalty list is designed for merchants who work with the predefined set of customers. Database with customers can be managed on merchant side with PCI DSS certification, or on Doc4.0 side. The system allows to manage the following several types of predefined clients lists such as names, emails, phones and etc.


If any transaction attribute does not match attribute in the lists and respective filter is enabled at the Project's level, the transaction status is set to Filtered and the reason for filtering is saved in the transaction data (see [Error Codes in Transaction Filters](#)<sup>3</sup> section in integration documentation).

One-time box can be checked for automatic removal of customer from loyalty list after their first payment.

<sup>2</sup> [https://doc4.codetime.net/integration/reference/transaction\\_filters.html](https://doc4.codetime.net/integration/reference/transaction_filters.html)

<sup>3</sup> [https://doc4.codetime.net/integration/reference/transaction\\_filters.html](https://doc4.codetime.net/integration/reference/transaction_filters.html)


### 8.1.2 Adding New Elements To BWL

To add new elements, click on the **ADD** button. The type of the added criteria will be automatically identified. Ambiguous criteria type can be manually changed, as presented below. It is also possible to use  button to switch between available options.

### 8.1.3 Importing Lists

In order to add many attributes to one of the lists at once, use **IMPORT** import list feature.

## Import list



[Choose from drive](#) or drag & drop file to this area

test1 <span style="float: right;">x v</span>	tryOEM <span style="float: right;">x v</span>	Source card type <span style="float: right;">v</span>
--	---	---

Fields terminated by <input checked="" type="radio"/> ; <input type="radio"/> ,	Optionally enclosed by <input checked="" type="radio"/> " <input type="radio"/> ""	Lines terminated by <input checked="" type="radio"/> \n <input type="radio"/> \r\n
---	--	--

Black
  White
  Loyal

IMPORT LIST

For example, in order to add card number to list, the following order should be used for every line: (5555514066237247,12,2019) with ',' delimiter between lines. Some lists require a country code. See Alpha-2 Code in Reference section of Integration documentation: [country codes](#)<sup>4</sup>.

### Note

In case of disconnect or other technical problems during the process, contact technical support.

Imported files displayed in a separate table and sorted by ID in the “Last Imported from Files” section.

### Last imported from files

id	Filename	Category	Merchant	Project	Count	Create date
1295	bw-218034025107438474244-list.csv	Source card 6+4	merchant	Project 2	1	23.10.2025 17:46:13

« ← 1-1 → »
10 25 50

<sup>4</sup> [https://doc4.codetime.net/integration/reference/country\\_codes.html](https://doc4.codetime.net/integration/reference/country_codes.html)

### 8.1.4 Exporting To File

In order to export your data into CSV file, use **EXPORT** export to file feature.

## Export list x

x v
manager1

<span style="float: right;">x v</span> <span>test1</span>	<span style="float: right;">x v</span> <span>tryOEM</span>	<span style="float: right;">v</span> <span>Source card number</span>
---	--	--

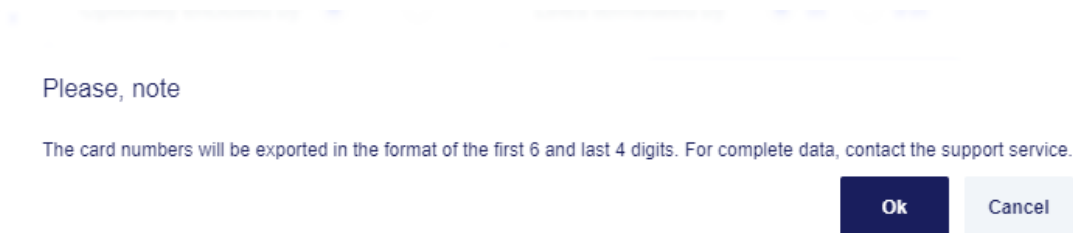
Fields terminated by <input checked="" type="radio"/> ; <input type="radio"/> ,	Optionally enclosed by <input checked="" type="radio"/> " <input type="radio"/> ""	Lines terminated by <input checked="" type="radio"/> \n <input type="radio"/> \r\n
---	--	--

Black  White  Loyal

**EXPORT LIST**

The data will be parsed according to set parameters.

Source card number and Destination card number export will be in 6+4 format. For complete data, please contact the support service.



### 8.1.5 Synchronizing Lists

#### Merchant

To synchronize two merchant lists, administrator can use **SYNC** synchronize list feature. After synchronizing, lists from both merchants will filter transactions as if you joined your two lists.

**Note**

Merchants do not have access to see entries from synchronized lists.

**Sync merchants lists**

Manager  
test menager

Merchants  
test merchant test merchant 2

Categories

Black  White  Loyal Sync list

**Merchant synced lists**

Manager  
test menager

Merchant name

Date range

Category	Merchants	Create date
Source card number	test merchant	23.10.2025 17:53:42

1-1 10 25 50

Synchronization can be cancelled by pressing the X button near the synced lists entry.

**Gate**

To synchronize two gate lists, administrator can use **SYNC** synchronize list feature. After synchronizing, lists from both gates will filter transactions as if you joined your two lists.

**Note**

Merchants do not have access to see entries from synchronized lists.

### Sync gates lists

Manager  
test menager

Gate  
Close day test

Maximum 10 gates

Categories

Black  White  Loyal Sync list

### Gate synced lists

Manager  
test menager

Gate name

Date range

Category	Gates		Create date	
Source card number	Close day test	•	23.10.2025 17:59:58	

<< 1-1 >> 10 25 50

Synchronization can be cancelled by pressing the X button near the synced lists entry.

## 8.1.6 Available Lists For Every Role

### 8.1.7 Comments

When adding new records to the BWL lists, optionally, comments can be attached.

When adding records from order page, automatically comment will be added with transaction id.

In order to display comment, point a cursor on «...» next to record in the list.



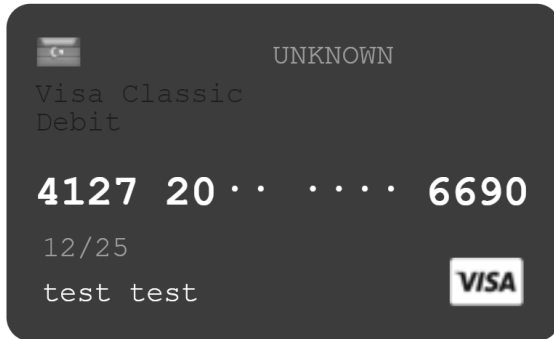
### 8.1.8 Order Details: Configuring BWL Lists

The attributes can also be added and removed from BWL on order details screen, as presented below:

- Select Merchant or Manager to switch between adding BWL list to Merchant or Manager.

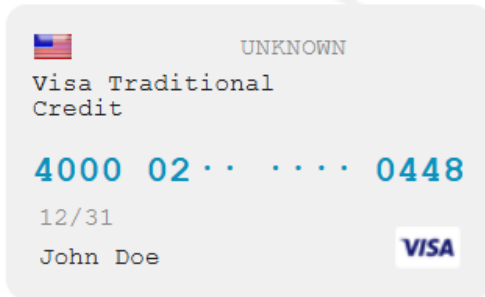
## Customer details

Merchant (0)  Manager (1)




Number

- Press ADD TO LIST and select one of the shown lists:



- Black ▶
- White ▶
- Loyalty ▶

1.1.1.1

Billing address:  100 Main st Seattle 98102 Washington U SA

E-mail: [example@ex.com](mailto:example@ex.com)

E-mail domain: [ex.com](http://ex.com)

First name: John

Last name: Smith

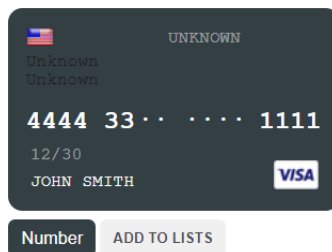
Phone: [12063582043](tel:12063582043)

Purpose: [newpurpose](#)

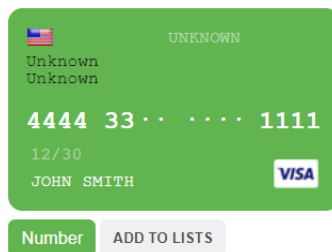
- After selecting any list, select the criterion by which the card will be listed:

Black	▶	Number	+
White	▶	As dest.	+
Loyalty	▶	BIN	+
		BIN as dest	+
		Country	+
		Country as dest	+
		Type	+
		Type as dest	+
		Email + PAN	+
		Phone	+

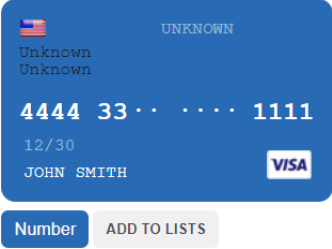
Blacklisted card will be shown in black colour:



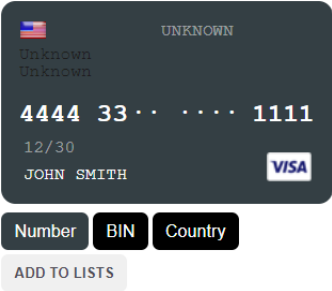
Whitelisted card will be shown in green colour:





Card in loyalty list will be shown in Doc4.0 colour:



- Several criteria can be chosen at the same time:



- Additional criteria can be added via section as shown below:

IP-address:  1.1.1.1  
Billing address:  100 Main st Seattle 98102 Washington U  
SA  
E-mail: example@ex.com  
E-mail domain: ex.com  
First name: John  
Last name: Smith  
Phone: 12063582043  
Purpose: newpurpose



After adding criteria via section described above, parameters will have colours depending on the selected list:



## 8.2 Monitoring

### 8.2.1 Buffer Online Balance Topups

Shows all top ups in the buffer, which will subsequently be added to the balance (e.g. sale).

Buffer Online Balance Topups										EXPORT
Select merchant					Select currency					
BALANCE TOPUP ID	SESSION ID	TRANSACTION AMOUNT	CURRENCY	INSERT TIME STAMP	BANK DATE	TRANSACTION TYPE ID	TRANSACTION TYPE	TRANSACTION STATUS ID	TRANSACTION STATUS	
21636151	338151...	24.72	EUR	02.11.2023 12:36	Nov 2, 2023 12:36:5...	1	sale	1	approved	

It is possible to select Merchant and currency.

Press Export button to export file with all information regarding top-ups.

In order to turn off all reconciliation notifications of specific balance top-up, press button.

## 8.2.2 Buffer Online Balance Holds

Shows all transactions with hold amount. For example while making payout, firstly, amount for payout is getting in buffer on hold (so in case of success, this amount would be transferred to customer account) after the transaction passed amount is released (deducted) from account. In order to hide/show the ignored holds, press "eye" icon.

Buffer Online Balance Holds										EXPORT
Select merchant					Select currency					Ignored:
BALANCE HOLD ID	BALANCE HOLD IDENTIFIER	SESSION ID	TRANSACTION AMOUNT	CURRENCY	INSERT TIME STAMP	BALANCE ID	BALANCE NAME			
100	c601b491-5748-11eb-8f86-10bf48d7f223	6703259	33	USD	15.01.2021 18:46	20	Testbalance1			
99	c2f39de3-5748-11eb-8f86-10bf48d7f223	6703259	33	USD	15.01.2021 18:45	20	Testbalance2			
97	a6137e72-5745-11eb-8f86-10bf48d7f223	6703258	44	USD	15.01.2021 18:23	19	Testbalance3			
96	a3109b50-5745-11eb-8f86-10bf48d7f223	6703258	44	USD	15.01.2021 18:23	19	Testbalance4			
94	37588eba-5745-11eb-8f86-10bf48d7f223	6703257	49.5	USD	15.01.2021 18:20	19	Testbalance5			
90	fb9f7eea-5741-11eb-8f86-10bf48d7f223	6703249	25	USD	15.01.2021 17:57	18	Testbalance6			
89	f89e5b8a-5741-11eb-8f86-10bf48d7f223	6703249	25	USD	15.01.2021 17:57	18	Testbalance7			
88	f59c50bc-5741-11eb-8f86-10bf48d7f223	6703249	25	USD	15.01.2021 17:57	18	Testbalance8			
86	991f2579-573d-11eb-8f86-10bf48d7f223	6703248	33	USD	15.01.2021 17:26	16	Testbalance9			
85	961b304f-573d-11eb-8f86-10bf48d7f223	6703248	33	USD	15.01.2021 17:25	16	Testbalance			

It is possible to select Merchant and currency.

Press Export button to export file with all information regarding holds.

In order to turn off all reconciliation notifications of specific hold balance, press button.


### 8.2.3 Buffer Online Balance Releases

Shows all released amount from hold in the buffer, which will subsequently be deducted from the balance.


Buffer Online Balance Releases										EXPORT
Select merchant					Select currency					
BALANCE RELEASE ID	BALANCE HOLD IDENTIFIER	SESSION ID	TRANSACTION AMOUNT	CURRENCY	INSERT TIME STAMP	TRANSACTION TYPE ID	TRANSACTION TYPE	TRANSA STATUS		
6200236	3cf9d51e-7790-11ed-9b81-ac1f6b763778	270741...	400	EUR	09.12.2022 12:07	11	transfer	2	🔊	
6200338	c46082dc-7794-11ed-9b81-ac1f6b763778	270744...	400	EUR	09.12.2022 12:07	11	transfer	2	🔊	
6197050	0152c874-7632-11ed-9b81-ac1f6b763778	270465...	150	EUR	07.12.2022 16:44	10	payout	2	🔊	
6120930	c3b5cc63-52a6-11ed-9b81-ac1f6b763778	264829...	244.58	EUR	23.10.2022 10:52	10	payout	2	🔊	
6120897	bbae43fc-52a1-11ed-9b81-ac1f6b763778	264827...	100	EUR	23.10.2022 10:38	10	payout	2	🔊	

It is possible to select Merchant and currency.

Press Export button to export file with all information regarding holds.

In order to turn off all reconciliation notifications of specific hold balance, press  button.

### 8.2.4 Merchant Online Balance Reconciliation

This section displays information about all Merchants reconciliations. In order to turn off all reconciliation notifications press  button.

Merchant Online Balance Reconciliation										
TestMerchant					USD					
BALANCE ID	BALANCE NAME	MANAGER ID	MANAGER NAME	MERCHANT ID	MERCHANT NAME	CURRENCY	BALANCE TOTAL CALCULATED	TOTAL	DIFF	
651	Test	70	TestManager	770	TestMerchant	USD	213120	213120	0	🔊

**Note**

Alert will come only if “DIFF” parameter will be more than 1000\$ (equivalent for other currencies)

## 8.2.5 Audit Events

### Overview

The Events monitor is designed to notify about certain events in the system with push or URL notifications.

**Events**

---

URL Notifications

Access to control key

Notification URL

The enabled URL notification sends request to the specified URL. The Connecting Party server is expected to respond with 200 OK HTTP status, otherwise the system will try to send the same notification up to 30 times in 14 days to guarantee it’s delivery.

URL Requirements - HTTPS: 443, 8443

All events, except for “Managers”, are accessible for managers and superiors. “Managers” event is only accessible for superiors.

### Access to control key

“Access to control key” event sends notification to the specified URL about viewing of the merchant control key by any user of the system.

An example of the received data:

```
{access_date: "2021.04.01 23:59:59", user_name: "vp-support", merchant_name: "new merchant name", merchant_id: "1", viewed_data: "merchant_control_key"}
```

Parameter name	Type	Description
access_date	String	Date of access
user_name	String	The name of the user who viewed the control key
merchant_name	String	Merchant’s name
merchant_id	Integer	Merchant’s ID
viewed_data	String	Viewed data

## Access to merchant profile

“Access to merchant profile” event sends notification to the specified URL about visiting of the merchant’s page by any user of the system.

An example of the received data:

```
{access_date: "2021.04.01 23:59:59", user_name: "vp-support", merchant_name: "new merchant name", merchant_id: "1", viewed_data: "merchant_page"}
```

Parameter name	Type	Description
access_date	String	Date of access
user_name	String	The name of the user who viewed the control key
merchant_name	String	Merchant’s name
merchant_id	Integer	Merchant’s ID
viewed_data	String	Viewed data

## End points

“End points” event sends notification to the specified URL about creating a new/changing endpoint status.

An example of the received data:

```
{end_point_id: "1", end_point_name: "new end point name", end_point_status: "Disabled", end_point_rate_plan_id: null, end_point_rate_plan_name: null}
```

Parameter name	Type	Description
end_point_id	Integer	Endpoint’s ID
end_point_name	String	Endpoint’s name
end_point_status	String	Endpoint’s status. Possible values: Enabled, Disabled
end_point_rate_plan_id	String	Endpoint’s rate plan ID
end_point_rate_plan_name	String	Endpoint’s rate plan name

## End points first transaction

“End points first transaction” event sends notification to the specified URL about first endpoint transaction.

An example of the received data:

```
{end_point_id: "1", end_point_name: "new end point name", end_point_status: "Disabled", end_point_first_transaction_date: "2021.04.01 23:59:59"}
```

Parameter name	Type	Description
end_point_id	Integer	Endpoint's ID
end_point_name	String	Endpoint's name
end_point_status	String	Endpoint's status. Possible values: Enabled, Disabled
end_point_first_transaction_date	String	Date of endpoint's first transaction

## Gates

"Gates" event sends notification to the specified URL about the creation of a new/changing gate status.

An example of the received data:

```
{gate_id: "1", gate_name: "new gate name", gate_status: "Disabled", gate_rate_plan_id: "10", gate_rate_plan_name: "new gate rate plan name"}
```

Parameter name	Type	Description
gate_id	Integer	Gate's ID
gate_name	String	Gate's name
gate_status	String	Gate's status. Possible values: Enabled, Disabled
gate_rate_plan_id	String	Gate's rate plan ID
gate_rate_plan_name	String	Gate's rate plan name

## Managers

"Managers" event sends notification to the specified URL about the creation of a new manager.

An example of the received data:

```
{manager_id: "1", manager_name: "new manager name"}
```

Parameter name	Type	Description
manager_id	Integer	Manager's ID
manager_name	String	Manager's name

## Merchant

"Merchants" event sends notification to the specified URL about the creation of a new/changing merchant's status.

An example of the received data:

```
{merchant_id: "1", merchant_name: "new merchant name", merchant_status: "Disabled"}
```

Parameter name	Type	Description
merchant_id	Integer	Merchant's ID
merchant_name	String	Merchant's name
merchant_status	String	Merchant's status. Possible values: Enabled, Disabled

### Merchants first transaction

"Merchants first transaction" event sends notification to the specified URL about the first merchant transaction.

An example of the received data:

```
{merchant_id: "1", merchant_name: "new merchant name", merchant_status: "Disabled", merchant_first_transaction_date: "2021.04.01 23:59:59"}
```

Parameter name	Type	Description
merchant_id	Integer	Merchant's ID
merchant_name	String	Merchant's name
merchant_status	String	Merchant's status. Possible values: Enabled, Disabled
merchant_first_transaction_date	String	Date of merchant's first transaction

### Processing limits

"Processing limits" event sends notification to the specified URL about creating a new/changing configuration/removing a limit.

An example of the received data:

```
{processing_limit_id: "1", processing_limit_action_type: "created"}
```

Parameter name	Type	Description
processing_limit_id	Integer	Processor's limit ID
processing_limit_action_type	String	Type of the processor's limit action. Possible values: Created, Enabled, Disabled, Deleted

## Processor

“Processors” event sends notification to the specified URL about the creation of a new/changing processor status.

An example of the received data:

```
{processor_id: "1", processor_name: "new processor name", processor_status: "Disabled"}
```

Parameter name	Type	Description
processor_id	Integer	Processor's ID
processor_name	String	Processor's name
processor_status	String	Processor's status. Possible values: Enabled, Disabled

## Projects

“Projects” event sends notification to the specified URL about the creation of a new / changing project's status.

An example of the received data:

```
{project_id: "1", project_name: "new project name", project_status: "Disabled",  
project_rate_plan_id: "10", project_rate_plan_name: "new project rate plan name"}
```

Parameter name	Type	Description
project_id	Integer	Project's ID
project_name	String	Project's name
project_status	String	Project's status. Possible values: Enabled, Disabled
project_rate_plan_id	String	Project's rate plan ID
project_rate_plan_name	String	Project's rate plan name

### 8.2.6 Online Monitor

- [Overview](#)
- [Perilous Decline](#)
- [Disabled Scheduled Adjustments](#)
- [Balance Running Out](#)
- [Important Filters](#)

## Overview

The screen is located in “Tools” - “Monitoring” section. This screen displays information about various errors that usually require quick response, as well as the options to subscribe for notifications about any errors via Telegram, Email or Push notification. Phone number and e-mail address are taken from the personal account (Manager or its employee account).

Tasks					
NAME	VALUE	COMMENTS	DATE		
★ Merchant balance reconciliation	1	Merchant balance reconciliation records with diff > 1000\$ - 1	23.10.2025 17:52	🔍	📧
★ Balance running out	18	Current number of merchant account balances with amount ≤ 1000\$ - 18	23.10.2025 18:02	🔍	📧
★ Failed payin session initiators	0	Number of "Failed payin session initiators" for the last 5 minutes - 0	23.10.2025 17:58	🔍	📧
★ Failed PAN eligibility	0	Number of "Failed PAN eligibility" transactions for the last 5 minutes - 0	23.10.2025 17:58	🔍	📧
★ Failed captures	0	Number of "Failed captures" transactions for the last 5 minutes - 0	23.10.2025 18:03	🔍	📧
★ Failed reversals/refunds	0	Number of "Failed reversals/refunds" for the last 5 minutes - 0	23.10.2025 17:58	🔍	📧
★ Perilous declines	0	Number of perilous declines for the last 10 minutes - 0	23.10.2025 17:58	🔍	📧

## Perilous Decline

This section is located in [Overview](#). This section displays triggered perilous declines which were selected by Manager.

To create a list of perilous declines, use [Processor Error Codes screen](#).

If Perilous declines list is empty please contact with support.

★ Perilous declines	0	Number of perilous declines for the last 10 minutes - 0	23.10.2025 18:04	🔍	📧
---------------------	---	---	------------------	---	---

## Disabled Scheduled Adjustments

Disabled scheduled adjustments is necessary to receive notifications when automatic adjustments are disabled due to a negative balance or merchant deactivation.

★ Disabled scheduled adjustments	0		23.10.2025 18:08	🔍	📧
----------------------------------	---	--	------------------	---	---

## Balance Running Out

This alert is used if necessary to receive notification when the Merchant Live balance is equal or under 1000\$.

ID	NAME	ONLINE BALANCE	CURRENCY ID	CURRENCY NAME	BALANCE
193	New test 2	0	1	United States dollar	0

## Important Filters

Notifications can be created for cases in which transactions were filtered due to the one of the following filters:

1. *Source Credit Card Number usage frequency for Email or IP address*
2. *Source Credit Card Number approved transaction interval*
3. *Total Credit Card Number usage frequency for last 24 hours (daily limit)*

Field name	Description
Date	The date when alert has been created.
ID	Alert identification number.
Name	Name of the Merchant.
MerchantID	Merchant identification number.
Error Description	Triggered project filter error description with error code. Example: [1033] Too many approved transactions for the same credit card number.

Field name	Description
Date	The date when alert has been created.
ID	Alert identification number.
Name	Name of the Merchant.
MerchantID	Merchant identification number.
Error Description	Triggered project filter error description with error code. Example: [1033] Too many approved transactions for the same credit card number.

## 8.2.7 Request Group Statistics

Managers are able to monitor requests to Endpoint Groups by getting this statistical table:

## Request group statistics

ID ↑	END POINT GROUP NAME	REQUEST COUNT	ERROR COUNT	HTTP ERROR COUNT	LAST ERROR
1893	TestGroup1	39	0	0	
1962	TestGroup2	3	0	0	
2082	TestGroup4	97	0	0	
2083	TestGroup5	50	0	0	

All parameters of this screen are described below:

Parameter Name	Description
ID	Endpoint group identification number.
END POINT GROUP NAME	The name of the Endpoint group that used as an entry point for incoming Merchant's transactions for multi currency integration. Clicking on the name of the endpoint group redirects user to the Integration Panel <a href="https://gate.doc4.com/paynet-ui/tools/integration-panel">https://gate.doc4.com/paynet-ui/tools/integration-panel</a> with the selected endpoint. Available for Request group statistics.
REQUEST COUNT	Total number of incoming requests.
ERROR COUNT	Total number of errors.
HTTP ERROR COUNT	Total number of http errors only.
LAST ERROR	Field that shows the last error occurred.

### 8.2.8 Request Endpoint Statistics

Managers are able to monitor requests to Endpoints by getting this statistical table:

## Request endpoint statistics

ID ↑	END POINT NAME	REQUEST COUNT	ERROR COUNT	HTTP ERROR COUNT	LAST ERROR
11016	TestEndpoint1	4	0	0	
14012	TestEndpoint2	91	0	0	
14029	TestEndpoint3	19	0	0	
14032	TestEndpoint4	42	0	0	

All parameters of this screen are described below:

Parameter Name	Description
ID	Endpoint identification number.
END POINT NAME	The name of the Endpoint that used as an entry point for incoming Merchant's transactions for single currency integration. Clicking on the name of the endpoint redirects user to the Integration Panel <a href="https://gate.doc4.com/paynet-ui/tools/integration-panel">https://gate.doc4.com/paynet-ui/tools/integration-panel</a> with the selected endpoint. Available for Request endpoint statistics.
REQUEST COUNT	Total number of incoming requests.
ERROR COUNT	Total number of errors.
HTTP ERROR COUNT	Total number of http errors only.
LAST ERROR	Field that shows the last error occurred.

## 8.3 Processing Limits

- [Processing Limits](#)
- [Setting Up A New Limit](#)
  - [Default limits](#)
  - [Limits by country](#)
  - [Alerts for limits](#)

### 8.3.1 Processing Limits

Hard & soft limits and cumulative processing limits can be found at Tools-Processing limits. This screen contains all previously configured default and country limits separated by tabs.

Processing limits
+ Default limit

DEFAULT COUNTRIES

^ Filters
Template ▾
Add filter ▾

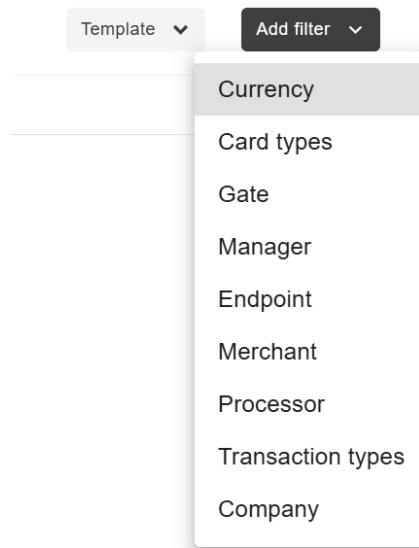
Exact  in All ▾

ID ↑	Rules	Criteria	Current limit value	Action
21	<input checked="" type="checkbox"/> <b>Daily (calendar) without time shift</b> Summarize <b>Transaction amount</b> Up to <b>1 000 000 USD</b> For Suspend Traffic <b>No</b> Name Comment	User defined <b>Total</b> Transaction type <span>sale</span> <span>capture</span>	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">0% <b>1 000 000</b></div> Manager <b>Manager 1</b> ETA limit reached - Expires <b>Feb 18 2026 00:00</b> Forecast <b>0 USD</b>	<span>✎ Edit</span> <span>🗑 Delete</span> <span>🔍 Search</span>
44	<input checked="" type="checkbox"/> <b>Daily (calendar) without time shift</b> Summarize <b>Transaction amount</b> Up to <b>1 900 000 CNY</b> For Suspend Traffic <b>No</b> Name Comment	User defined <b>Total</b> Gate <span>Gate 1</span> Transaction type <span>sale</span>	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">0% <b>1 900 000</b></div> Manager <b>Manager 1</b> ETA limit reached - Expires <b>Feb 18 2026 00:00</b> Forecast <b>0 CNY</b>	<span>✎ Edit</span> <span>🗑 Delete</span> <span>🔍 Search</span>
45	<input checked="" type="checkbox"/> <b>Daily (calendar) without time shift</b> Summarize <b>Transaction amount</b> Up to <b>1 900 000 CNY</b> For Suspend Traffic <b>No</b> Name Comment	User defined <b>Total</b> Gate <span>Gate 2</span> Transaction type <span>sale</span>	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">0% <b>1 900 000</b></div> Manager <b>Manager 1</b> ETA limit reached - Expires <b>Feb 18 2026 00:00</b> Forecast <b>0 CNY</b>	<span>✎ Edit</span> <span>🗑 Delete</span> <span>🔍 Search</span>

Main features:

- Visualization
- Flexible settings
- Multicurrency
- Alerting by e-mail
- Warning limits (several thresholds)
- Stop limit
- Forecast for daily and monthly limits in the context of one period
- Trend for daily limits in the context of several days

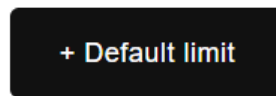
The limit can be found by its ID or name. Multiple limits can be found using search criteria. Search criteria can be saved as a template for future use. The list of created limits can be sorted by their ID. (Last created, First created)



### 8.3.2 Setting Up A New Limit

#### Default limits

Set up a new limit by pressing “+Default limit”:



New limit can be set up with several parameters:

**Processing limits**

Create

Cancel Save

Manager ▼

---

Name

Comment

---

**Mandatory criteria**

User defined

TOTAL 3DS NON 3DS PAYOUT

**Transaction types**

sale capture

+ Add Clear

---

**Additional criteria**

+ Add criteria ^

Please select manager

---

**Period**

MONTHLY WEEKLY DAILY HOURLY

Time shift

NONE ▼

---

**Calculation**

TRANSACTION AMOUNT TRANSACTION COUNT

Currency to sum up ▼

**Consider currencies**

+ Add Clear

Limit value

AMOUNT RANGE

Limit value

---

**Traffic suspension**

Suspend traffic

YES NO

- Manager
- Transaction type
- User defined - can be Total, 3-D Secure, Not 3-D Secure or Payout.
- Additional criteria:
  - Endpoint - after selecting endpoint it's not possible to select Merchant;
  - Merchant - after selecting Merchant it's not possible to select endpoint;
  - Gate - after selecting gate it's not possible to select processor;
  - Processor - after selecting processor it's not possible to select gate;

- Company(group of gates);
- Card types.
- Time period:
- Daily/Weekly/Monthly/Hourly - date-dependent parameter. Monthly – limits refresh on the first day of every month. Weekly - limits refresh every Monday. Daily - limits refresh at every 00:00. Hourly - limits refresh at every hour;
- Time shift. Not supported at the moment, will be added later.
- Calculation:
- Value to summarize - can be set by transaction amount or transaction count;
- Currency to sum up - the currency for limit calculation must be specified;
- Consider currencies (optional field) - transactions in which currencies will be included in limit calculation;
- Suspend traffic - just yes or no. What to do with transactions when limit reached: stop traffic or not;
- Limit value - For Amount enter total transaction amount or transaction count for this limit. Limit doesn't include settled value, if limit should be 15000 for it to be included value must be 15000.01. Range to make the limit amount less transparent.

### Limits by country

Limits by country are available under separate “Countries” tab.

DEFAULT      COUNTRIES

---

Switch to the countries tab and set up a new limit by pressing “+Countries limit”:

+ Countries limit

New limit can be set up with several parameters:

- Manager
- User defined - can be Total, 3-D Secure, Not 3-D Secure.
- Countries
- Additional criteria:
- Gate - after selecting gate it's not possible to select processor;
- Processor - after selecting processor it's not possible to select gate;
- Card types.
- Time period:

**Processing limits**  
Create

Cancel Save

Manager

Name

Comment

**Mandatory criteria**

User defined

TOTAL 3DS NON 3DS

Countries

+Add Clear

**Additional criteria**

+ Add criteria ^  
Please select manager

**Period**

MONTHLY WEEKLY DAILY HOURLY

Time shift  
NONE

**Calculation**

TRANSACTION AMOUNT TRANSACTION COUNT

Currency to sum up

Consider currencies

+Add Clear

**Limit value**

AMOUNT RANGE

Limit value

**Traffic suspension**

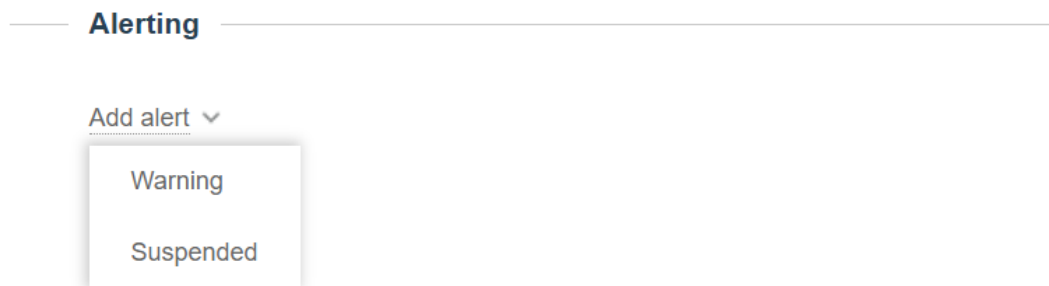
Suspend traffic

YES NO

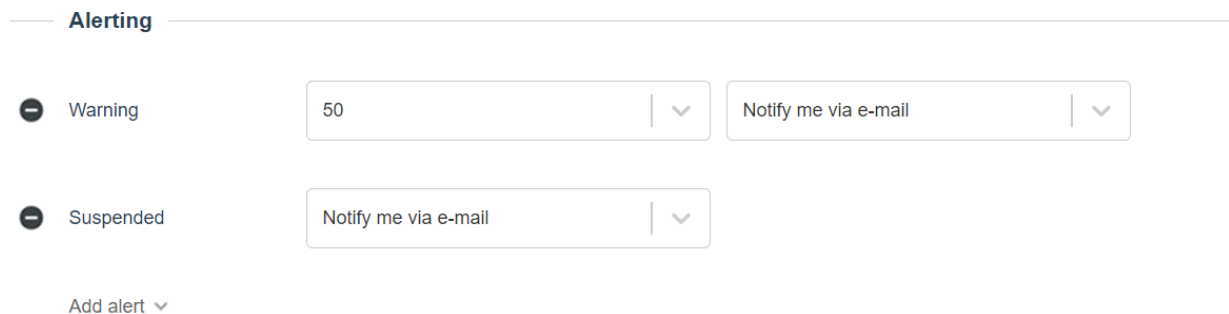
- Daily/Weekly/Monthly/Hourly - date-dependent parameter. Monthly - limits refresh on the first day of every month. Weekly - limits refresh every Monday. Daily - limits refresh at every 00:00. Hourly - limits refresh at every hour;
- Time shift. Not supported at the moment, will be added later.
- Calculation
- Value to summarize - can be set by transaction amount or transaction count;
- Currency to sum up - the currency for limit calculation must be specified;
- Consider currencies (optional field) - transactions in which currencies will be included in limit calculation;
- Suspend traffic - just yes or no. What to do with transactions when limit reached: stop traffic or not;
- Limit value - For Amount enter total transaction amount or transaction count for this limit. Limit doesn't include settled value, if limit should be 15000 for it to be included value must be 15000.01. Range to make the limit amount less transparent

### Alerts for limits

Also, it's possible to set different alerts for limits by pressing Add alert:



- Warnings when limit reaches for example 50%, 75%, 90% or 100% with notification by e-mail to address specified in user account;



- notification by e-mail when traffic is Suspended.

It is possible to add comment for limits by adding text in comment box

**Comment**

Enter your comment

100 characters left

Comment can be found at Tools-Processing limits page

ID ↓	RULES	FILTERS	CURRENT LIMIT VALUE
⋮	<b>Monthly (calendar) without time shift</b> Summarize <b>Transaction amount</b> up to <b>100 000 EUR</b> for Suspend traffic: <b>Yes</b> <span style="border: 1px solid red; padding: 2px;">Comment</span>	Manager Processor Transaction type: <b>sale</b> User defined: <b>Total</b>	<input type="text" value="0%"/> <input type="text" value="100 000"/> ETA limit reached Expires: <b>Jan 1, 2024 12:00:00 AM</b> Forecast: <b>0 EUR</b>

## 8.4 Transaction Marker Notification

- [Overview](#)
- [Configuration](#)

### 8.4.1 Overview

The Transaction marker notification tool is used to notify users about specific issues that might happen to transactions and usually require quick response. Each time the specified transaction marker is triggered, it will send email notification to user’s email address. For example, if notifications for chargebacks are enabled, user will get a new email notification for each chargeback applied to a processed transaction. Email content can be customized.

The main screen displays a list of all notifications, their status, ID, subject, language, merchant name, message type and marker type.

**Transaction marker notification** Create

Last updated by Merchant Language

Status	ID	Last updated by	Subject	Language	Merchant	Message type	Marker type
<input type="checkbox"/>	1	vagaltsov:admin	1	Abkhazian	125209TestMerchant	Email	ABS notification failed
<input type="checkbox"/>	494	AutoQA:admin	ATSubject#0CSB7G4IYK	English	ATMerchYR2Y7	Email (HTML)	chargeback fraud

### 8.4.2 Configuration

To add a new marker, press the Create button in the upper right corner. Notification configuration box will appear with the following parameters:

## New transaction marker notification

 DisabledMerchant Marker type Language 

Message type

 Email Email (HTML)

Subject

Message

CANCEL

SAVE

Parameter	Description
Status	Enabled/Disabled

continues on next page

Table 15 - continued from previous page

Parameter	Description
Marker type:	<ul style="list-style-type: none"> <li>• Chargeback</li> <li>• Chargeback after ethoca reversal</li> <li>• Chargeback after reversal</li> <li>• Duplicated chargeback</li> <li>• Failed cancels</li> <li>• Failed captures</li> <li>• Failed PAN eligibility</li> <li>• Failed payin session initiators</li> <li>• Failed payout session initiators</li> <li>• Failed reversals/refunds</li> <li>• Failed scorings</li> <li>• Fraud</li> <li>• Inconsistent order status</li> <li>• Incorrect decline code</li> <li>• Multiple master approvals</li> <li>• Phone verification</li> <li>• Processor callback notification</li> <li>• Refused payouts</li> <li>• Refused refunds</li> <li>• Retrieval</li> <li>• User defined</li> </ul>
Merchant	To select a merchant, enter the name or ID of the merchant
Subject	All emails for this marker will have this subject
Message type	<ul style="list-style-type: none"> <li>• Email - Email with plain text.</li> <li>• Email (HTML) - Email with HTML support.</li> </ul>
Message	All emails for this marker will have this text message. Transaction Marker Notification supports <a href="#">Message Templates</a> <sup>5</sup> . Additionally \${MARKER_TYPE_NAME} was added.

## 8.5 Transaction Markers

Transaction markers are created to notify users about specific issues that might happen to transactions and usually require quick response or additional business process (for example, manual review or communication with the customer). This screen allows to view all created transaction markers and work with them, by adding comments to markers and set them as “processed” if the issue has been resolved. Notifications about new markers can be sent by e-mail, this functionality is configured on “Transaction Marker Notification” screen. Transaction markers can be sorted with search criteria by marker type and status. The list of markers contains information about each marker type, status and linked order ID:

<sup>5</sup> [https://doc4.codetime.net/integration/common\\_utilities/receipt\\_message.html](https://doc4.codetime.net/integration/common_utilities/receipt_message.html)

## Transaction markers

^ Filters								
Date	ID ↑	Marker type	Status	User name	Processing date	User decision	Order ID	Merchant name
05.02.2025 13:26:38	477414	Failed payin session initiators	Unprocessed		-	-	22910150	vatestmerchant
05.02.2025 16:39:15	477415	Failed payin session initiators	Unprocessed		-	-	22910158	vatestmerchant

## 8.6 Virtual Terminal

- [Overview](#)
- [Asymmetric Cryptography](#)
  - [Generate A Pair Of Public And Private Keys](#)
  - [Import Private Key To Browser Console](#)
  - [Import Private Key To User Interface](#)
- [VT Interface Details](#)
- [Template Management](#)
- [Transaction Specification](#)
  - [Deposit](#)
    - \* [Sale](#)
    - \* [Preauth](#)
  - [C2C \(Card To Card\) Transfer](#)
  - [Withdrawal](#)
    - \* [D2C \(Deposit To Card\) Transfer](#)
    - \* [Payout](#)

### 8.6.1 Overview

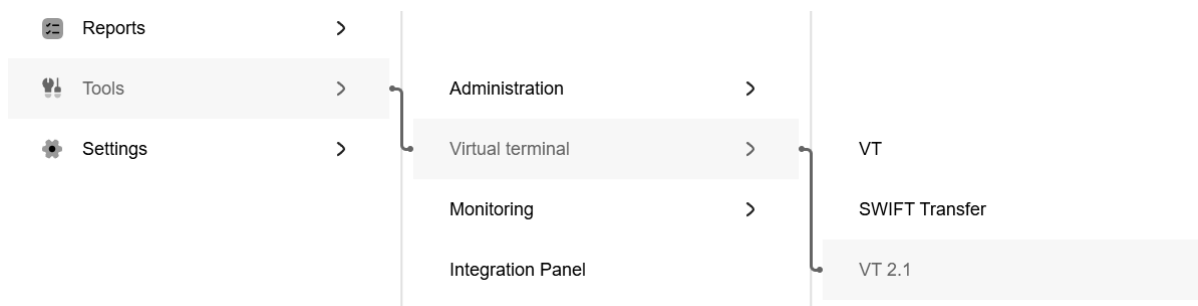
Virtual terminal (VT) is a technological solution that allows to process transactions from Merchant's personal account on User Interface. This feature doesn't require Merchant's API integration to Doc4.0. VT immediately provides a full-featured payment manager's workplace. VT is used for remote processing of transactions without the presence of a customer, for example, if the customer places an order or pays for services while being in another city or country. VT workflow is fully customizable in order to meet the business needs. Flexible templates will help to minimize time of filling all the customer details. The Virtual terminal supports recurring payments (by recurring ID). If the customer provided cardholder data to gate.doc4.com processing system before, and the Merchant registered such payment to get recurring ID, future payments can be made with recurring ID instead of cardholder data. VT also allows to generate a link for the customer to submit cardholder data in the secure environment, and, if needed, pass 3-D Secure validation.

VT provides a secure way of processing MOTO transactions with support of asymmetric cryptography. In order to do so please, [Generate A Pair Of Public And Private Keys](#) and then pass public key to Doc4.0 support and upload the private key in Browser Console ([Import Private Key To Browser Console](#)) or User Interface ([Import Private Key To User Interface](#)).

The available operations for VT are:

- accepting payments from both new and previously registered customers ([Sale](#));
- hold funds from both new and previously registered customers ([Preauth](#));
- transfer of funds from card to card, both for new and previously registered customers ([C2C \(Card To Card\) Transfer](#));
- issuance of funds to the cards of both new and previously registered customers ([D2C \(Deposit To Card\) Transfer](#));
- transfer of funds from one bank account to another ([Payout](#)).

The screen is located in Tools - Virtual terminal (VT).



## 8.6.2 Asymmetric Cryptography

The big advantage of the new Virtual terminal is the use of an asymmetric cryptography system. Asymmetric cryptography, or public-key cryptography, is a cryptographic system that uses pairs of keys: public keys which may be disseminated widely, and private keys which are known only to the owner. The generation of such keys depends on cryptographic algorithms based on mathematical problems to produce one-way functions. Effective security only requires keeping the private key private; the public key can be openly distributed without compromising security.

The Virtual terminal becomes personalized. The user signs transaction request with his private key and the system uses the public key to verify that request is made by the owner of the corresponding private key.

### Generate A Pair Of Public And Private Keys

Virtual terminal requires a pair of public and private keys from user to authorize requests. To generate it, go to <https://www.openssl.org/> ( <https://slproweb.com/products/Win32OpenSSL.html> ), download the latest openssl version and run the following commands:

```
openssl genpkey -algorithm RSA -out private_key_pkcs_8.pem -pkeyopt rsa_keygen_bits:4096
```

```
openssl rsa -pubout -in private_key_pkcs_8.pem -out public_key.pem
```

Please, do not share private key with anyone, it is confidential information for private use only. In contrast, public key must be passed to Doc4.0 for endpoint configuration. Please use different keys for production and testing environments to avoid compromise.

PKCS #8 RSA unencrypted private key in PEM format starts with `-----BEGIN PRIVATE KEY-----` text. This key must be imported to Browser Console or User Interface. See details below.

### Import Private Key To Browser Console

Private key is imported into browser's IndexedDB using a script associated with the currently opened page. This script only uses plain browser APIs (WebCrypt API, IndexedDB API) and does not use any external scripts to avoid the private key being compromised.

Import sequence is:

1. Open <https://gate.doc4.com/paynet-ui/login-step1> page in a browser (Do not login to the system).
2. Open the browser console. In Chrome, it is done with Ctrl+Shift+J. In Safari, it is done with Ctrl+Shift+I, Ctrl+Alt+C. For Mac - Cmd instead of Ctrl.
3. Replace the demo key below with real private key in PEM format (it must have `-----BEGIN PRIVATE KEY-----` prefix in the beginning).

```
var privateKeyPem = `-----BEGIN PRIVATE KEY-----\n
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBCkwwgSjAgEAAoIBAQDJzUVnqQhDWF2H
pxAMcyo7f+ucIEJS3AQHG0ET/dxJ0qssGymIjdzelJ3XI+oTq2y9TTimQjtujoeh
6zl44WrXCbJLcUDWsNjLh7hmBorpu6tJVhw1466CAxkktPJHkMqJYF0efegIf0wU
otTzwY4tGln6iWk0aMJ5ZWhWpZDbgap72vrRXKfCN6/JeTudsOI7PAeZw0me04jZ
8Lova9FVIbVz0JaFGwSUroMvXevIB8r0D57c3VCLTxE3aGNMz+9DLl6Gcm8WZ1US
HmiHybqgvGLyQswBPFcVzFgd7BpgZs+JAzYDh8ZGANvjA5F9u0b6Ynb3Mpm3+9Rl
CtvSxKwpAgMBAAECggEAZ6+hro5KIZggjleHRm5Rz7p9S33DtIE3rJMTT/tKmV+1
9XaLU49YYcDIjMb20V8GawnPRpWXRcnT5J0grXxc0do4kpdRij3ZY63lT/6ilxoX
Uxn8aq/udPy0iYizR5QcjJNHpSgZ9WqCPmQfuJLFw2TYaYh3f6yn54n0Hzj4gd9l
tsol4xeTKQ47c/vUF7kHfD8IYzL8jv3a3++IqzCwJ3jIpTENSBYAgrkbYN9f9GHD
BvX3sz6tgFaYU2R8YbDvA0Yq9tVPwYrPvbhwoht6PsjE/R0UK6yqnKPEADdzWvP8
frXmmtJ35rAymqUWfpqx9RdZ0NMR7J8ut8C5365PJQKBgQD+UidVWut7d9qvhZKq
+T5qtasH5qkD34idFl4Ay8xsSntqTrXr7q1Ff+FQY6R+f/8IzB4ZqgnV58+8AEMc
gJzNmkf9L119SCQDxRV/Tgw2eHrUrI9XS2AI5tmyzaGY1xL4fCQQMvqNAGERT6sS
XJRt8WjuGmE4zeqXNB0XY7u10wKBgQDLIlNks0rPw00lWUbXSHHwdfBzjYU97KVu
Gn0l5fsCmlKanqHUfd/4StnRXpl3l56hig8mYsHV5EcFUEX98PaSbTAY8Lk5y5E9
ye2EN0gl/IyMgHPtT6spFKm7jRmpulqG4FVCGxQl3n6/nSmztA3S1zLZzi0guI0E
oxXCbG796wKBgC8NSg0rr5eHRClnIAyL0nVxqPPsQ+bYi3Dsu3WQPwDmAtFXQKcm
4F3UW/5AgSV6Ttf007jR0cIGglN5BPGYBeqGZ0JGNXd6/PambCU4c+xmKASU07I
nJrnYu2Gx9f8KqFYbl+k3uAJauwF/l0GV1vD5zLuJICa8Enap2s1Y3wTaoGBAKrx
QnLISyIB+XbXtVyrYHdJ2Mp1Ks6cye5pBi9y5RQgqCkEG62FLCh3X0vrTvysNEs+
slccPoBv9UYtuGjmEanRhwenQMiZPaWgu2dJWp8081X9dxEavS/5+oghSpphf3MH
b9gMj5z6qvE3IffFls7iWCGgdquVgt6HG3Wc6J53AoGAc+ZYE8kMj2p9rtu1uJgX
```

(continues on next page)

(continued from previous page)

```

+VMbbdLEUqz3BPC9Tzq+eglULYmwUK1xynKZfkEMcu5PncaBaNLU+GmYKKgw6wZS
soEF1KvbBB4o6nZdlGo0Bir0Q0ijHDWUvtuiaaWAQoQAhQwgqqV2I0C4UfkZ6ORf
A/UW43A9wZq9kaEgb0YW0es=\
-----END PRIVATE KEY-----`;

// Algorithm Object
var algorithmKeyGen = {
  name: "RSASSA-PKCS1-v1_5",
  // RsaHashedKeyGenParams
  modulusLength: 2048,
  publicExponent: new Uint8Array([0x01, 0x00, 0x01]), // Equivalent to 65537
  hash: {
    name: "SHA-256"
  }
};

function parsePem(pemString, type) {
  const expectedPrefix = "-----BEGIN " + type + "-----";
  const expectedPosftix = "-----END " + type + "-----";

  pemString = pemString.trim();
  if (!pemString.startsWith(expectedPrefix)) {
    throw "Expected PEM to start with " + expectedPrefix;
  }
  if (!pemString.endsWith(expectedPosftix)) {
    throw "Expected PEM to end with " + expectedPosftix;
  }
  const base64 = pemString.substring(expectedPrefix.length, pemString.
  ↪length - expectedPosftix.length).trim();
  return Uint8Array.from(atob(base64), c => c.charCodeAt(0))
}

function parsePrivateKeyPem(pem) {
  return parsePem(pem, 'PRIVATE KEY')
}

function storePrivateKey(privateKey) {
  var request = indexedDB.open("keys");

  request.onupgradeneeded = function() {
    // The database did not previously exist, so create object stores and
    ↪indexes.
    var db = request.result;
    var store = db.createObjectStore("privateKeys", {keyPath: "name"});

    // Populate with initial data.
    store.put({name: "first", key: privateKey});
  };

  request.onsuccess = function() {
    db = request.result;
  };
}

```

(continues on next page)

(continued from previous page)

```
}  
var privateKeyArray = parsePrivateKeyPem(privateKeyPem);  
var NON_EXTRACTABLE = false;  
window.crypto.subtle.importKey("pkcs8", privateKeyArray, algorithmKeyGen, NON_  
→EXTRACTABLE, ['sign'])  
.then(function(privateKey) {  
    storePrivateKey(privateKey);  
    privateKeyPem = null;  
    privateKeyArray = null;  
})  
);
```

4. Copy this script content and paste it into browser console.
5. The key has been imported in a non-extractable manner.

### Warning

If private key have been integrated into the browser, but it is impossible to make a transactions, please, clear browser's cache and try again to integrate the private key.

### Note

If the proposed code is not suitable or if more information is required about the **Web Crypto API**, please visit the official site [https://developer.mozilla.org/en-US/docs/Web/API/Web\\_Crypto\\_API](https://developer.mozilla.org/en-US/docs/Web/API/Web_Crypto_API).

## Import Private Key To User Interface

The Virtual terminal has the function of using a private key through the user interface



In order to faster conduct a large number of test transactions, please check the “Save key in the browser” box, and the private key will be automatically saved in the browser.

Add private key



**You can add an RSA private key yourself via the console**

Documentation describing how to create a key pair and add a private key to the Browser

[Go to documentation](#)

**If for some reason you can't add a private key to your browser yourself, you can use our Web interface.**

By using our Web interface, you confirm that you are aware that your private key will not be retrieved or saved by the system. If you have any doubts about the safety of your private key, please add the key to your browser yourself

RSA private key

Save the key to the browser

Cancel

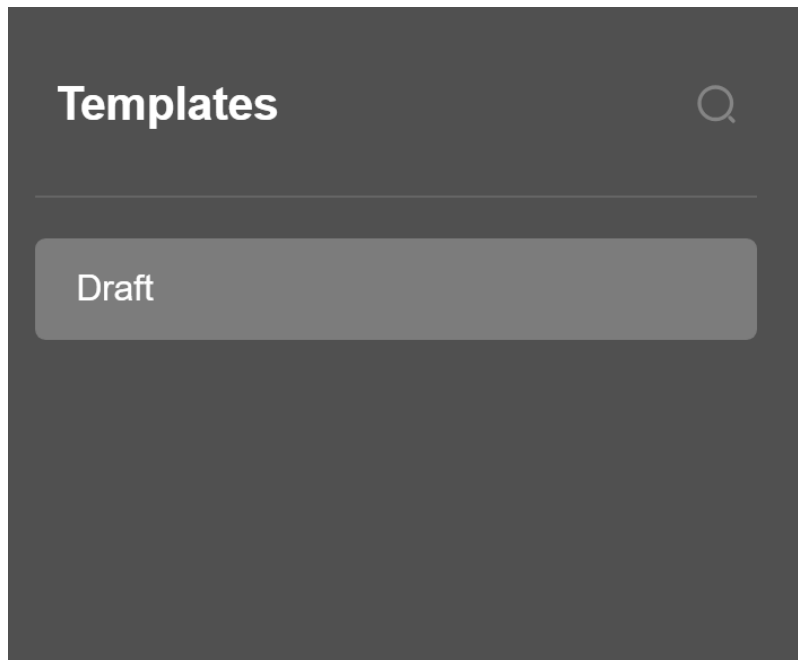
Ok

### 8.6.3 VT Interface Details

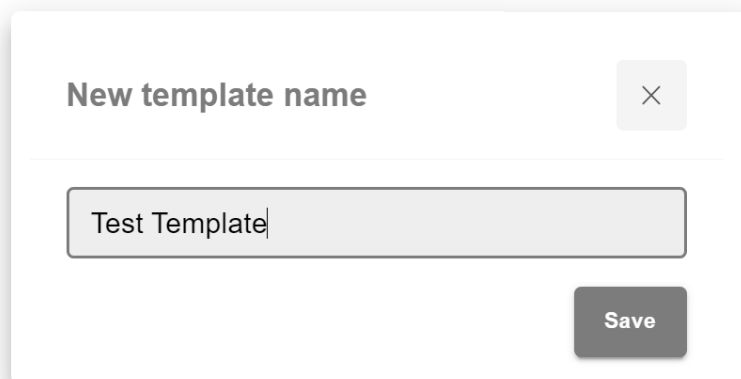
The VT has control buttons, which are described in more details below.

### 8.6.4 Template Management

1) To simplify the work of the Virtual terminal operator, data fields can be saved as a template. Using templates allows to work only with the individual attributes of the client.

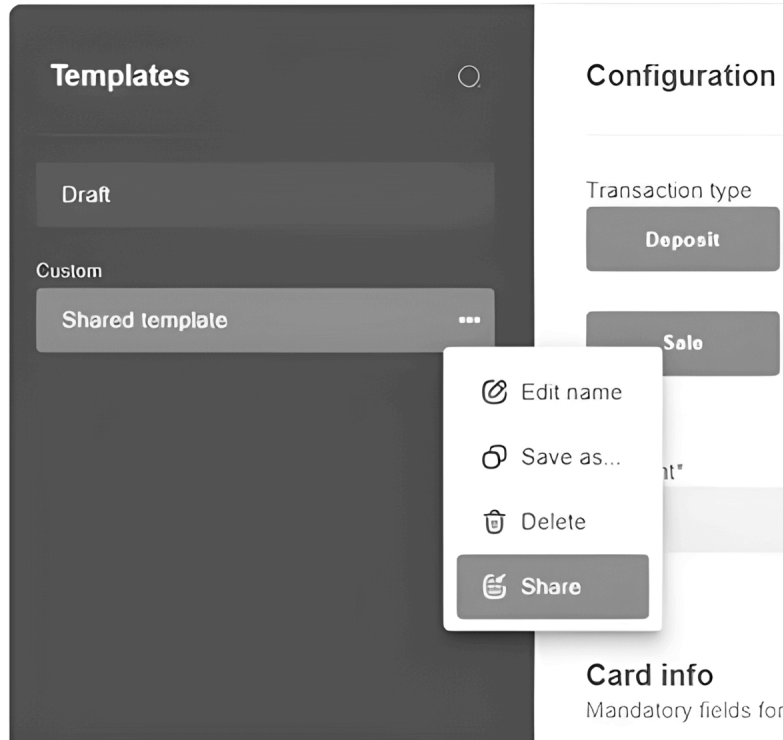


2) After entering data on the right side of the page, it is possible to save this data as a template by clicking 'save as a template' and naming the new template.



3) To edit, clone, delete or share, click three dots near the template name and select the desired parameter. The template can be shared with users at lower levels. This way, a merchant can share the template with their employees.

## Virtual terminal



For all selected users, the created template will become the default upon loading the virtual terminal.

Changes can still be made before conducting a transaction, but only the creator of the template has the authority to modify the template itself. Users with whom the template has been shared are only allowed to make copies.

The number of created templates available for sharing is unlimited. They will all be displayed to users in alphabetical order.

**Share template with...** [X]

my employees

Managers  
 Manager 1 [X]

and with their employees

Merchants  
 Merchant 1 [X] Merchant 2 [X]

and with their employees

Save

## 8.6.5 Transaction Specification

### Deposit

In the deposit section, it is possible to make a Sale and a Preauth transaction, which are described below.

### Sale

Sale is a type of transaction, in which customer receives goods or services from Merchant in exchange for money or other assets.

To initiate transaction, submit the following 3 types of information:

- 1) Transaction data - Endpoint, amount, currency, description, invoice number must be filled directly on VT.
- 2) Card info - Cardholder, Card number, Valid thru:
  - can be filled directly on VT;
  - can be filled automatically together with Personal info, if Recurring ID is provided. If Recurring ID is provided and CVV field is empty, use "Copy link" to provide form to customer for additional confirmation. In case if it will be filled in VT form directly then transaction will be processed directly.
  - can be filled by customer on the form.

3) Personal info - First name, Last name, City, Address, Zip code, Phone, E-mail, Customer IP-address ,Country, etc:

- can be filled directly on VT;
- can be filled automatically together with Card info, if Recurring ID is provided;
- can be filled automatically, if Customer ID is provided.

Process transaction:

- Use "Copy link" button to generate the payment link and send it to the customer. This flow is relevant for transactions which require additional information submitted by customer on the form (cardholder data, 3DS check, etc).
- Use "Process" button if transaction doesn't require any additional information submitted by customer (e.g. noCVV non3D recurring transactions).

The image shows the options available for filling.

Transaction type

Deposit C2C Withdrawal

Sale Preauth

Endpoint\* 1122334 Amount\* 100 Currency\* United States dollar

**Card info**  
Mandatory fields for Process

Cardholder\* Test User Card number\* 444455\*\*\*\*\*7777 Valid thru\* 10/30

CVV\* 123

Last used 1234567 2345678 3456789 6783451 1122334 Recurring ID 1123456

**Order data**

Invoice number\* 1122334 Order description\* Test

Additionally ^

Purpose Test

**Personal info**

First name\* Test Last name\* User City\* NY

Address\* Test Address

Zip code\* 112233 Phone\* 9999999999 E-mail\* test@mail.test

Customer ip-address\* 11.22.33.44 Country\* United States

Additionally ^

Customer user agent Mozilla/5.0 (Windows NT 10.0; W Birthday 1 January 2020 Customer last 4 SSN 1234

Customer deposit level GOLD Customer ID 1122334 Merchant customer ID 12345

State New York Language English Site URL test.test

Customer redirect URL https://test.test/redirect

Copy link Process

## Preauth

Pre authorization is a transaction type in which bank blocks the specified amount in the customer's card account and does not allow the cardholder to use this blocked money.

It is important to know that the block remains for a definite period of time depending on whether this is a debit or a credit card (usually the maximum block period is 7 days for debit cards and 28 days for credit cards).

To initiate transaction, submit the following 3 types of information:

- 1) Transaction data - Endpoint, amount, currency, description, invoice number must be filled directly on VT.
- 2) Card info - Cardholder, Card number, Valid thru:
  - can be filled directly on VT;
  - can be filled automatically together with Personal info, if Recurring ID is provided. If Recurring ID is provided and CVV field is empty, use "Copy link" to provide form to customer for additional confirmation. In case if it will be filled in VT form directly then transaction will be processed directly.
  - can be filled by customer on the form.
- 3) Personal info - First name, Last name, City, Address, Zip code, Phone, E-mail, Customer IP-address ,Country, etc:
  - can be filled directly on VT;
  - can be filled automatically together with Card info, if Recurring ID is provided;
  - can be filled automatically, if Customer ID is provided.

Process transaction:

- Use "Copy link" button to generate the payment link and send it to the customer. This flow is relevant for transactions which require additional information submitted by customer on the form (cardholder data, 3DS check, etc).
- Use "Process" button if transaction doesn't require any additional information submitted by customer (e.g. noCVV non3D recurring transactions).

The image shows the options available for filling.

Transaction type

Deposit C2C Withdrawal

Sale Preauth

Endpoint\* 1122334 Amount\* 100 Currency\* United States dollar

**Card info**  
Mandatory fields for Process

Cardholder\* Test User Card number\* 444455\*\*\*\*\*7777 Valid thru\* 10/30

CVV\* 123

Last used 1234567 2345678 3456789 6783451 1122334 Recurring ID 1123456

**Order data**

Invoice number\* 1122334 Order description\* Test

Additionally ^

Purpose Test

**Personal info**

First name\* Test Last name\* User City\* NY

Address\* Test Address

Zip code\* 112233 Phone\* 9999999999 E-mail\* test@mail.test

Customer ip-address\* 11.22.33.44 Country\* United States

Additionally ^

Customer user agent Mozilla/5.0 (Windows NT 10.0; W Birthday 1 January 2020 Customer last 4 SSN 1234

Customer deposit level GOLD Customer ID 1122334 Merchant customer ID 12345

State New York Language English Site URL test.test

Customer redirect URL https://test.test/redirect

Copy link Process

## **C2C (Card To Card) Transfer**

Card-to-card transaction is a direct transfer of funds from card to card (C2C).

Several scenarios are possible:

1) Transfer money from unknown card to registered card.

Receiver data is retrieved using Destination Recurring ID. The receiver Card info (Cardholder, Card number, Valid thru) and Personal info (First name, Last name, City, Address, Zip code, Phone, E-mail, Country and other optional customer data) sections will be filled in automatically. To speed up the filling of recipient fields, use the Last used section next to "Destination recurring ID" field, which contains previously used Recurring IDs. The Merchant creates a special link for the sender with "Copy link" button. The sender receives the link to a form in which he fills his card number, expiration date, holder name and CVV, then passes the 3DS check if needed.

2) Transfer money from registered card to unknown card.

Sender data is retrieved using Recurring ID. The sender Card info (Cardholder, Card number, Valid thru) and Personal info (First name, Last name, City, Address, Zip code, Phone, E-mail, Customer IP-address, Country and other optional customer data) sections will be filled in automatically. CVV is not stored and must be requested from sender. To speed up the filling of sender fields, use the Last used section new to "Recurring ID" field, which contains previously used Recurring IDs. The Merchant creates a special link for the sender with "Copy link". The sender receives the link to a form in which he fills the destination card number, then passes the 3DS check if needed.

3) Transfer money between known or registered cards.

The Merchant fills the cardholder data or use recurring IDs for both sender and receiver of funds directly on VT and initiates transfer processing with "Process" button. In this case the transaction must be processed through the non3D channel, which is not common for C2C transfers.

**Note**

When filling in the Customer ID field, Personal info (First name, Last name, City, Address, Zip code, Phone, E-mail, Country) sections will be filled in automatically.

The image shows the options available for filling.

Missing private key
🔗
🔒
🔄
📄
💾 Save
🔗 Copy link
⚙️ Process

Transaction type

Deposit **C2C** Withdrawal

Endpoint\* 1122334 Amount\* 100 Currency\* United States dollar

**Card info**  
Mandatory fields for Process

Cardholder\* Test User Card number\* 444455\*\*\*\*\*7777 Valid thru\* 10/30

CVV\* 123

Last used 1234567 2345678 3456789 6783451 1122334 Recurring ID 1123456

Destination cardholder\* Test User Destination card number\* 4444 55\*\*\*\*\*77 77 Dest. valid thru 10/30

Destination recurring ID 123456

**Order data**

Invoice number\* 1122334 Order description\* Test

**Personal info**

Customer ip-address\* 11.22.33.44 Customer redirect URL\* https://test.test/redirect

Additionally ^

Sender first name Test Sender last name User Sender middle name Tester

Sender SSN 1122334 Sender birthplace 1 January 2020 Sender birthday 1 January 2020

Sender address Test Address

Sender city NY Sender state New York Sender zip code 112233

Sender citizenship United States Sender country United States Sender phone 9999999999

Sender cell phone 9999999999 Sender e-mail test@mail.test Sender resident YES NO

Sender identity document ID 1122334 Sender identity document series 9999999999 Sender identity document number 1122334

Sender identity document issuer name Test Sender identity document issuer depart... 1122334 Sender identity document issuer date 1 January 2020

Receiver first name Test Receiver last name User Receiver middle name Tester

Receiver birthplace 1 January 2020 Receiver birthday 1 January 2020

Receiver address Test Address

Receiver city NY Receiver zip code 112233 Receiver region Genesee

Receiver area Test Address Receiver citizenship United States Receiver country United States

Receiver phone 9999999999 Receiver e-mail test@mail.test Receiver resident YES NO

Receiver identity document ID 1122334 Receiver identity document series 9999999999 Receiver identity document number 1122334

Receiver identity document issuer name Test Receiver identity document issuer depa... 1122334 Receiver identity document issuer date 1 January 2020

Customer user agent Mozilla/5.0 (Windows NT 10.0; W Customer local time Sun Jan 01 2020 15:00:0 GMT+ Customer screen size 2560x1440

Customer accept language en Customer accept 1122334

🔗 Copy link
⚙️ Process

## Withdrawal

In the withdrawal section, it is possible to make a D2C (Deposit to card) transfer and a Payout, which are described below.

### D2C (Deposit To Card) Transfer

A Deposit-to-Card transaction is a transfer of funds from a bank account to a payment card.

Several scenarios are possible:

1) Transfer money to known card.

The Merchant fills the cardholder data for receiver of funds directly on VT with “Process” button.

2) Transfer money to registered card.

Receiver data is retrieved using Destination Recurring ID. The receiver Card info (Cardholder, Card number, Valid thru) and Personal info (First name, Last name, City, Address, Zip code, Phone, E-mail, Country and other optional customer data) sections will be filled in automatically. To speed up the filling of recipient fields, use the Last used section next to “Destination recurring ID” field, which contains previously used Recurring IDs.

3) Transfer money to unknown card.

The Merchant creates a special link for the recipient of funds with “Copy link” button. The recipient receives the link to a form in which he fills the destination card number.

#### Note

When filling in the Customer ID cell, Personal info (First name, Last name, City, Address, Zip code, Phone, E-mail, Country) sections will be filled in automatically.

The image shows the options available for filling.

Transaction type

Deposit C2C **Withdrawal**

**D2C** Payout

Endpoint\* 1122334 Amount\* 100 Currency\* United States dollar

**Card info**  
Mandatory fields for Process

Destination cardholder Test User Destination card number\* 444455\*\*\*\*\*7777 Dest. valid thru 10/30

Destination recurring ID 1123456

**Order data**

Invoice number\* 1122334 Order description\* Test

**Personal info**

Customer ip-address\* 11.22.33.44 Customer redirect URL https://test.test/redirect

Additionally ^

Receiver first name Test Receiver last name User Receiver middle name Tester

Receiver birthplace 1 January 2020 Receiver birthday 1 January 2020 Receiver city NY

Receiver address Test Address

Receiver zip code 112233 Receiver region Genesee Receiver area Test Address

Receiver citizenship United States Receiver country United States Receiver phone 9999999999

Receiver e-mail test@mail.test Receiver resident YES NO Receiver identity document ID 1122334

Receiver identity document series 9999999999 Receiver identity document number 1122334 Receiver identity document issuer name Test

Receiver identity document issuer depa... Test Receiver identity document issuer date 1 January 2020 Customer user agent Mozilla/5.0 (Windows NT 10.0; W

Customer local time Sun Jan 01 2020 15:00:00 GMT+0 Customer screen size 2560x1440 Customer accept language en

Customer accept 1122334 Customer withdrawal level Customer ID 1122334

Merchant customer ID

Copy link Process

## **Payout**

A Payout transaction is the disbursement of funds to a recipient account number, digital wallet or other type of account. The Merchant fills the payment data for receiver of funds directly on VT and initiates payout with “Process” button.

### **Note**

When filling in the Customer ID field, Personal info (First name, Last name, City, Address, Zip code, Phone, E-mail, Country) sections will be filled in automatically.

The image shows the options available for filling.

Transaction type

Deposit    C2C    **Withdrawal**

D2C    **Payout**

Endpoint\*    Amount\*    Currency\*

1122334    100    United States dollar

**Order data**

Invoice number\*  
1122334

Additionally ^

Order description\*    Merchant data    Bank code  
Test    1122334    1122334

Bank name    Bank branch    Bank province  
Test    Test    Test

Bank area    Bank city  
Test Address    NY

Bank address  
Test Address

Bank zip code    Bank card number    Account name  
1122334    4444 55\*\*\*\*77 77    Test

Account number    Routing number    E-wallet type  
1122334    1122334    Test

E-wallet    Crypto wallet address  
1122334    1122334

**Personal info**

Customer ip-address\*  
11.22.33.44

Additionally ^

Customer user agent    Legal person name    Legal person document number  
Mozilla/5.0 (Windows NT 10.0; W    Test    1122334

Customer redirect URL    Customer withdrawal level    Customer ID  
https://test.test/redirect       1122334

Merchant customer ID    Receiver first name    Receiver last name  
    Test    User

Receiver birthday    Receiver city  
1 January 2020    NY

Receiver address  
Test Address

Receiver zip code    Receiver country    Receiver state  
112233    United States    United States

Receiver phone    Receiver e-mail    Receiver identity document ID  
9999999999    test@mail.test    1122334

Receiver identity document number  
1122334

**Process**

## 8.7 Batch Operations

- *Overview*
- *Gate Operations*
  - *Close Day For Selected Gates*
- *Transaction Operations*
  - *Chargeback*
  - *Reversal*
  - *Fraud*
  - *Capture*
  - *Retry Pending Reversals*
  - *Blacklist*
  - *Commit Reversal*
  - *Add Comment To Transactions*
  - *Add Card Mappings*
  - *Query Status Of Transactions*
  - *Resend Callbacks*
  - *Upload Chargebacks Info*
  - *Sale With Card Reference ID*
  - *Ethoca Alerts Update*
  - *Create Recurring Payments*
  - *Update Recurring Payments*
  - *PIPO Mark Sent*
  - *PIPO Mark Received*
  - *Scoring*
  - *Retrieval*

### 8.7.1 Overview

Batch operations is the set of tools that allows to process multiple operations through the user interface of the system. Below is the list of available batch operations.

### 8.7.2 Gate Operations

#### Close Day For Selected Gates

This batch operation can be useful for closing bank day on a group of gates. Select the gate or processor IDs in order to close bank days on all gates.

**Close day for selected gates**

Close bank day on a group of gates

**Batch settings**

<input type="checkbox"/> Processor:	<input type="text" value="All"/>
<input type="checkbox"/> Gate:	<input type="text" value="All"/>

**Note**

When processor selected, close day will be applied to all gates attached to this processor.

### 8.7.3 Transaction Operations

#### Chargeback

This batch operation can be useful if for some reason reversal was not made to prevent a chargeback and creating chargeback transaction according to specified input is needed. Collect the order IDs, assigned by Doc4.0 system to the CSV file and upload it to make chargebacks for selected transactions. An example of CSV file for upload is available on the same screen.

**Chargeback**

Chargeback transactions in a batch

**Batch settings**

Select batch file (*.CSV): <input type="button" value="Choose File"/> No file chosen	Interpret IDs as: <input type="text" value="internal order IDs"/>	Select processor <input type="text" value="tesst processor"/>	Sample CSV file for this batch: <input type="button" value="Download example"/>
---	--	--	--

#### Reversal

This batch operation can be useful for creating reversal transactions in according to specified input. Collect the order IDs, assigned by Doc4.0 system to the CSV file and upload it to make reversal of selected transactions. An example of CSV file for upload is available on the same screen.

**Reversal**

Make reversal transactions in a batch

**Batch settings**

Select batch file (\*.CSV):  No file chosen

Interpret IDs as:  Select processor

Sample CSV file for this batch:

**Fraud**

If Connecting Party suspects transaction to be fraudulent, then this batch operation can be useful for marking transactions as fraud in according to specified input. Collect the order IDs, assigned by Doc4.0 system to the CSV file and upload it to mark selected transactions as fraud. An example of CSV file for upload is available on the same screen.

**Fraud**

Mark transactions as fraud in a batch

**Batch settings**

Select batch file (\*.CSV):  No file chosen

Interpret IDs as:  Select processor

Sample CSV file for this batch:

**Capture**

This batch operation can be useful for deducting the locked amount from preauth transactions (preauth should be in approved final status) in according to specified input. Collect the order IDs, assigned by Doc4.0 system to the CSV file and upload it to make capture of selected transactions. An example of CSV file for upload is available on the same screen.

**Capture**

Capture transactions in a batch

**Batch settings**

Select batch file (\*.CSV):  No file chosen

Interpret IDs as:  Select processor

Sample CSV file for this batch:

## Retry Pending Reversals

This batch operation re-sends reversal request for pending reversals in according to specified input. Collect the order IDs, assigned by Doc4.0 system to the CSV file and upload it to make reversal of selected transactions. An example of CSV file for upload is available on the same screen.

### Retry Pending Reversals

Retry reversals in a batch

**Batch settings**

Select batch file (*.CSV): <input type="button" value="Choose File"/> No file chosen	Interpret IDs as: <input type="button" value="internal order IDs"/> Select processor	Sample CSV file for this batch: <input type="button" value="Download example"/>	<input type="text" value="tesst.processor"/>
---	---	--	--

## Blacklist

This batch operation, in according to specified input, puts cards in blacklist or external fraud system if such is set up. Collect the order IDs, assigned by Doc4.0 system to the CSV file and upload it to blacklist card of selected transactions. An example of CSV file for upload is available on the same screen.

### Blacklist

Blacklist transactions in a batch

**Batch settings**

Select batch file (*.CSV): <input type="button" value="Choose File"/> No file chosen	Interpret IDs as: <input type="button" value="internal order IDs"/>	Add to external fraud service, not local blacklist: <input checked="" type="checkbox"/>	Sample CSV file for this batch: <input type="button" value="Download example"/>
---	--	--	--

## Commit Reversal

This batch operation can be useful for initiating reversal transactions in according to specified input. Collect the order IDs, assigned by Doc4.0 system to the CSV file and upload it to make reversal of selected transactions. An example of CSV file for upload is available on the same screen.

**Commit reversal**

Commit reversals in a batch

**Batch settings**

Select batch file (\*.CSV):

 No file chosen

Interpret IDs as:

internal order IDs ▾  
 internal order IDs  
 external tx IDs  
 tx RRN

Select processor

Sample CSV file for this batch:

**Add Comment To Transactions**

This batch operation can be useful for adding a or an additional comment to transactions in according to specified input. Collect the order IDs, assigned by Doc4.0 system to the CSV file and upload it to add comment for the selected transactions. An example of CSV file for upload is available on the same screen.

**Add comment to transactions**

Add comments to transactions in a batch

**Batch settings**

Select batch file (\*.CSV):

 No file chosen

Interpret IDs as:

internal order IDs ▾  
 internal order IDs  
 external tx IDs

Select processor

Sample CSV file for this batch:

**Add Card Mappings**

This batch operation can be useful for one or more cardholder identifiers to be mapped (assigning) to card data.

**Add card mappings**

Add card mappings in a batch

**Batch settings**

Select batch file (\*.CSV):

 No file chosen

**Query Status Of Transactions**

This batch operation can be useful for requesting status of transactions (doesn't matter in what status) in according to specified input. Collect the order IDs, assigned by Doc4.0 system to the CSV file and upload it to request status of the selected transactions. An example of CSV file for upload is available on the same screen.

### Query status of transactions

Query transaction statuses in a batch

**Batch settings**

Select batch file (*.CSV): <input type="button" value="Choose File"/> No file chosen	Interpret IDs as: <input type="button" value="internal order IDs"/> Select processor <input type="button" value="internal order IDs"/> <input type="button" value="external tx IDs"/>	Sample CSV file for this batch: <input type="text" value="testprocessor"/> <input type="button" value="Download example"/>
---	--	---

## Resend Callbacks

This batch operation can be useful if information on the final status of transactions is available in Doc4.0 system and for some reason is not available in the Connecting Party system. Collect the order IDs, assigned by Doc4.0 system to the CSV file and upload it to send new callback notifications. An example of CSV file for upload is available on the same screen.

### Resend callbacks

Resend callbacks for transactions

**Batch settings**

Select batch file (*.CSV): <input type="button" value="Choose File"/> No file chosen	Interpret IDs as: <input type="button" value="internal order IDs"/>	Sample CSV file for this batch: <input type="button" value="Download example"/>
---	--	--

## Upload Chargebacks Info

This batch operation can be useful, while chargeback procedure is ongoing, for uploading additional information about chargeback. Collect the order IDs, assigned by Doc4.0 system and enter all information to the CSV file and upload it to add chargebacks information.

### Upload chargebacks info

Upload chargebacks info in a single ZIP archive

**Batch settings**

Select batch file (*.ZIP): <input type="button" value="Choose File"/> No file chosen	Select processor <input type="text" value="testprocessor"/> <input type="button" value=""/>
---	--

## Sale With Card Reference ID

This batch operation can be useful for initiating sale without any card information using only card reference ID. Collect the Endpoint and Card reference IDs, assigned by Doc4.0 system and enter all information to the CSV file and upload it to initiate sale transactions with card reference ID. An example of CSV file for upload is available on the same screen.

**Sale with card reference id**

Make sale with card ref id

**Batch settings**

Select batch file (\*.CSV):

No file chosen

Sample CSV file for this batch:

**Ethoca Alerts Update**

This batch operation can be useful for updating Ethoca statuses. Collect the order IDs, assigned by Doc4.0 system to the CSV file and upload it to send statuses to Ethoca system. An example of CSV file for upload is available on the same screen.

**Ethoca alerts update**

Update Ethoca alerts

**Batch settings**

Select batch file (\*.CSV):

No file chosen

Sample CSV file for this batch:

**Create Recurring Payments**

This batch operation can be useful for initiating recurring payments for transactions that require regular debits with the same data. Collect the order IDs, assigned by Doc4.0 system and enter all information to the CSV file and upload it to create recurring payments. An example of CSV file for upload is available on the same screen.

**Create recurring payments**

Create recurring payments

**Batch settings**

Select batch file (\*.CSV):

No file chosen

End Point :

Sample CSV file for this batch:

## Update Recurring Payments

This batch operation can be useful for updating recurring payments (new customer data and etc.) for transactions that require regular debits with the same data. Collect the recurring order IDs, assigned by Doc4.0 system and enter all information to the CSV file and upload it to update recurring payments information. An example of CSV file for upload is available on the same screen.

### Update recurring payments

Update recurring payments

**Batch settings**

Select batch file (*.CSV): <input type="button" value="Choose File"/> No file chosen	End Point : <input type="text" value="TestEndpoint"/>	Sample CSV file for this batch: <input type="button" value="Download example"/>
---	--	--

## PIPO Mark Sent

This batch operation allows to mark pending bank transfer as sent (but not received yet). This status equals to “processing” for preauth transaction. Collect order IDs, assigned by Doc4.0 system and enter all information to the CSV file and upload it to mark PIPO payments as sent. An example of CSV file for upload is available on the same screen.

### PIPO mark sent

PIPO: mark sent

**Batch settings**

Select batch file (*.CSV): <input type="button" value="Choose File"/> No file chosen	Interpret IDs as: <input type="text" value="Internal order IDs"/>	Sample CSV file for this batch: <input type="button" value="Download example"/>
	Select processor <input type="text" value="testprocessor"/>	

## PIPO Mark Received

This batch allows to mark pending bank transfer as received. This status equals to “approved” for preauth transaction. Collect order IDs, assigned by Doc4.0 system and enter all information to the CSV file and upload it to mark PIPO payments as received. An example of CSV file for upload is available on the same screen.

**PIPO mark received**

PIPO: mark received

**Batch settings**

Select batch file (\*.CSV):  No file chosen

Interpret IDs as:  Select processor

Sample CSV file for this batch:

**Scoring**

This batch allows to get information about card scoring. Collect order IDs and needed card data, assigned by Doc4.0 system and enter all information to the CSV file and upload it to receive card scoring information. An example of CSV file for upload is available on the same screen.

**Scoring**

Scoring

**Batch settings**

Select batch file (\*.CSV):  No file chosen

End Point:

Sample CSV file for this batch:

**Retrieval**

This batch operation can be useful for uploading a copy of the sales ticket to support or identify a potential chargeback. Collect the order IDs, assigned by Doc4.0 system and enter all information to the CSV file and upload it to add retrieval information. An example of CSV file for upload is available on the same screen.

**Retrieval**

Make retrieval transactions in a batch

**Batch settings**

Select batch file (\*.CSV):  No file chosen

Interpret IDs as:  Select processor

Sample CSV file for this batch:

## 8.8 Integration Panel

The screen is located in “Tools” – “Integration Panel” section. The Integration Panel displays requests sent to the system and system responses to these requests, as well as information about possible errors in the requests. This allows to quickly eliminate errors during integration. The panel also helps to view initiating requests for which, as a result of the error, orders were not created.

Request Date	21.10.2025 13:19:06	Request Data
Request URL	/paynet/api/v2/sale/13453	Log time: ***-10-21 13:19:06.*** POST https://sandbox.payneteasys.eu/paynet/api/v2/sale/13453 Remote address: 79.***.***.***
Order Id	3459897	Parameters: 29 address1: *** Main st amount: 10.42 birthday: 19820115 card_printed_name: CARD HOLDER
Endpoint	[E] <a href="#">Vica loyalty test endpoint</a>	Response Data
		21.10.2025 13:19:06 type=async-response &serial-number=00000000-0000-0000-0000-00000524d726 &merchant-order-id=inv2734828 &paynet-order-id=3459897 &end-point-id=13453

The following search criteria are available in Integration Panel:

- by EndPoint ID or EndPoint Group ID, to which the request was sent,
- by order ID, assigned to transaction by Doc4.0 system,
- by serial number of request and response.

Date range can also be specified for the search.

Filters Template ▾

Exact  in Endpoint id ▾ ✕

Date range Today ▾ ✕

## 8.9 Fx Rate

- [Introduction](#)
- [Fx Rate Setup](#)

### 8.9.1 Introduction

Fx Rate is a service that allows to receive exchange rates from various Providers.

### 8.9.2 Fx Rate Setup

The screen is located in “Tools” – “Fx Rate” section.

**There are two sections in Fx Rate:**

- Terminals

- Providers

**Fxrate settings** + Add terminal

TERMINALS PROVIDERS

ID	TERMINAL NAME	PROVIDER NAME	TYPE	CURR. FROM - TO	COEF.	ABS.	DESCRIPTION
1	Test Terminal	First	Buy	USD - EUR	1.1		Description <span style="float: right;">⋮</span>
2	Test Terminal 2	Second	Sell	USD - EUR	1.1		Description <span style="float: right;">⋮</span>

« ← 1 - 2 → 10 25 50

TERMINALS PROVIDERS

ID	NAME	BASE CURRENCY	CURRENCIES	DESCRIPTION
1	First	USD	USD, EUR	description1 <span style="float: right;">Add terminal</span>
2	Second	EUR	USD, EUR	description2 <span style="float: right;">Add terminal</span>
3	Third	RUB	USD, RUB	description3 <span style="float: right;">Add terminal</span>

Terminals section shows all available Terminals and adjust their settings.

Providers section shows all available Providers and allows to add new Terminal to any Provider.

**Note**

To add new Provider, contact the Doc4.0 support service.

To create a new Terminal for Provider, click the “+ Add terminal” button. New window with parameters will appear as shown below:

**Add terminal** [X]

Terminal name  
Test Terminal

Provider name  
First

Type  
BUY

Currency from  
USD

Currency to  
EUR

Coefficient  
1.1

Absolut value

Description  
Description of this terminal

Cancel Create

In opened window it is possible to:

- Name the Terminal
- Select the available Provider from the list
- Choose between two rate types: Buy or Sell
- Choose from which currency to which currency the conversion will be applied
- Add coefficient (additional % modifier to conversion rate)
- Add absolute value (which will be added after every conversion to the resulting amount)
- Add Terminal description

After creating new Terminal it will be possible to see it in “Terminals” section.

It is possible to remove or edit Terminal anytime. It is not possible to edit all fields of the already existing Terminal. To edit Terminal settings, click three dots as shown below:

ID	TERMINAL NAME	PROVIDER NAME	TYPE	CURR. FROM - TO	COEF.	ABS.	DESCRIPTION
1	Test Terminal	First	Buy	USD - EUR	1.1		Description for this terminal

« ← 1-1 → »

50

Edit Remove

These are all fields that can be changed:

### Edit terminal ✕

ID 1	Terminal name Test Terminal
Provider name First	Type BUY
Currency from USD	Currency to EUR
Coefficient 1.1	Absolut value
Description Description for this terminal	

Cancel
Update

## 8.10 Analytics Dashboard

- [Overview](#)
- [General Filters](#)
- [Criteria](#)
- [Dashboard Panels](#)

- *Customer Lifetime Value (Periodic Percent Active Users)*
  - \* *Overview*
  - \* *Filters*
  - \* *Customer Lifetime Value Graph*
    - *Customer Lifetime Value*
    - *Average CLV per month*
    - *Clients count*
    - *Customer Acquisition Cost*
    - *Average Lifetime*
    - *Historical Lifetime*
    - *Predictive Lifetime*
    - *Predictive CLV*
  - \* *Average Order Value Graph*
  - \* *Average Time to Second Order Graph*
  - \* *Average Time to Next Order Graph*
  - \* *Return on Investment Bar Chart*
  - \* *Customer Segmentation CLV Based Segment Chart*
  - \* *Top 10 Table*
- *N-month (Retention Curve)*
  - \* *Overview*
  - \* *Filters*
  - \* *N-month Retention Graph*
    - *Periodic*
    - *Retrospective*
  - \* *Users Waterfall Chart*
  - \* *Quick Ratio Graph*
  - \* *Average Revenue per User Graph*
  - \* *Repeat Customer Rate Graph*
  - \* *Repeat Customers Rate Count-to-Amount Ratio Bar*
  - \* *Top 10 Table*
- *COHORT (For the Period)*
  - \* *Overview*
  - \* *Filters*
  - \* *Cohort Table*
- *Templates*

### **8.10.1 Overview**

### **8.10.2 General Filters**

Starting with - starting date for reports

Show by - period starting from the Starting with date during which the data will be processed

Display currency - currency used in reports

Tx type - transaction type used in reports. For example: sale, transfer, etc.

Status - transaction type used in reports

### **8.10.3 Criteria**

### **8.10.4 Dashboard Panels**

#### **Customer Lifetime Value (Periodic Percent Active Users)**

##### **Overview**

Customer Lifetime Value (CLV) is a per-customer metric that represents the total monetary value generated by a customer over a *selected time period*

##### **Filters**

Grouping type - specifies how metrics are aggregated and displayed in the reports. All calculations are performed independently for each group under the same filters and time range. Possible values: Manager, Merchant, Endpoint

Total cost of marketing campaign - defines the total marketing spend for the selected filters and period

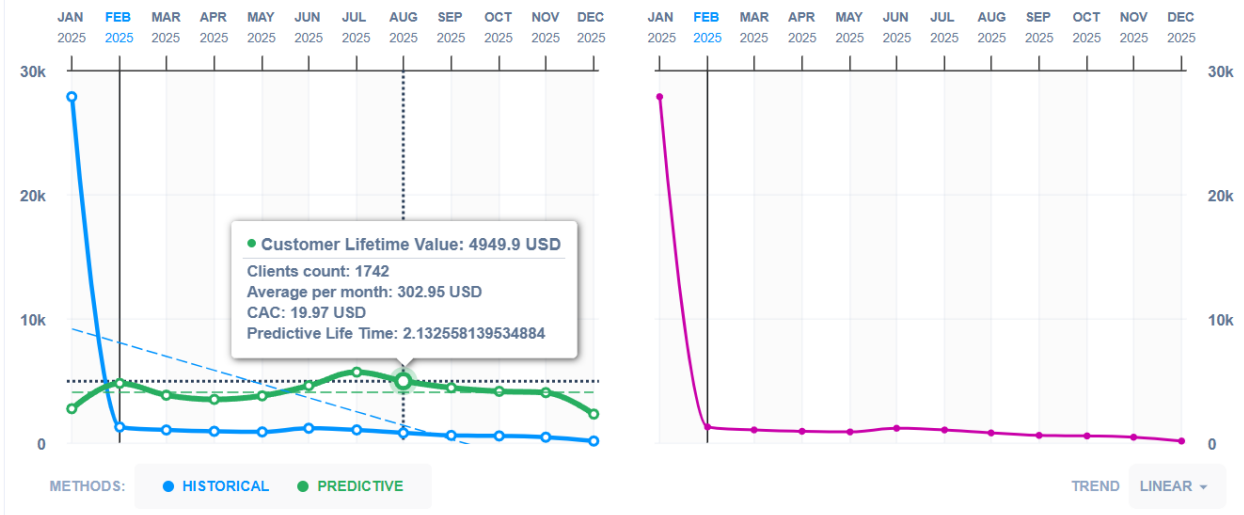
##### **Customer Lifetime Value Graph**

Customer Lifetime Value (CLV) is a per-customer metric that represents the total monetary value generated by a customer over a *selected time period*

### Customer lifetime value ⓘ



### Customer lifetime value ⓘ



## Customer Lifetime Value

Customer Lifetime Value (CLV) is the average total value of transactions generated by a payer over the selected period, expressed in the *selected reporting currency*.

Calculations:

1. For each payer, CLV is calculated as the sum of all *selected transactions*, converted to the *selected in filters currency*:

$$Payer\_CLV = \sum_{i=1}^N (amount_i \cdot convert\_rate)$$

where  $N$  is the number of selected transactions for the payer

2. For each payer determines the month of their first selected transaction

3. Each payer CLV groups by first month of selected transactions
4. For each month  $p$ , the CLV value is the rounded average of  $Payer\_CLV$  across all payers whose first transaction month equals  $p$ :

$$CLV(p) = \text{round}\left(\frac{1}{N_p} \cdot \sum_{i=1}^N Payer\_CLV(p)_i, 4\right)$$

where  $N_p$  is the number of all Payer CLV, where the first month's value is the same as the selected month

### Average CLV per month

Average CLV per Month represents the average transaction value generated per payer per active month within the selected period, expressed in the *selected reporting currency*.

Calculations:

1. For each payer, CLV is calculated as the sum of all *selected transactions*, converted to the *selected in filters currency*:

$$Payer\_CLV = \sum_{i=1}^N amount \cdot convert\_rate$$

where  $N$  is the number of selected transactions for the payer

2. For each payer determines the month of their first and last selected transaction
3. Each payer CLV groups by first month of selected transactions
4. For each month  $p$ , the average CLV per month value calculates as rounded average of  $Payer\_CLV$  across all payers whose first transaction month equals  $p$  divided by the difference between the first and last month:

$$CLV\_per\_month(p) = \text{round}\left(\frac{1}{N_p} \cdot \sum_{i=1}^{N_p} \frac{Payer\_CLV(p)_i}{last\_month_i - first\_month_i + 1}, 4\right)$$

where  $N_p$  is the number of all Payer CLV, where the first month's value is the same as the selected month

### Clients count

Client count is the number of all unique payers for the period defined in *general filters*

### Customer Acquisition Cost

Customer Acquisition Cost (CAC) is the average marketing spend required to acquire one payer within the selected period.

Calculations:

$$CAC = \frac{total\_marketing\_cost}{total\_payers}$$

where  $total\_marketing\_cost$  is the defined in *CLV filters* total cost of marketing campaign, and  $total\_payers$  is the number of all unique payers for the period defined in *general filters*

## Average Lifetime

Average Lifetime represents the average number of months a payer remains active, calculated for payers that match the *selected grouping criteria* (e.g., merchant, manager, or endpoint). A payer is considered active from the month of their first selected transaction through the month of their last selected transaction

Calculations:

1. For each payer determines the month of their first and last selected transaction
2. Each payer groups by first month of selected transactions
3. For a payer  $i$  in cohort month  $p$  (where  $first\_month_i = p$ ), lifetime is calculated as:

$$LT_{p,i} = last\_month_{p,i} - first\_month_{p,i} + 1$$

4. Average Lifetime for specific month ( $p$ ) calculates as rounded average lifetimes across all payers in that cohort:

$$AVG\_LT(p) = \text{round}\left(\frac{1}{N_p} \cdot \sum_{i=1}^{N_p} LT_{p,i}, 4\right)$$

where  $N_p$  is the number of payers whose first month's value is the same as the selected month

## Historical Lifetime

Historical Lifetime is the *Average Lifetime* for all available groups (by grouping type) defined in *CLV filters*

## Predictive Lifetime

Predictive Lifetime estimates the expected number of months a client will remain active based on the observed month-over-month retention rate

Calculations:

1. Total active clients in current and previous months is number of clients which was active in previous month and still active in current month

$$total\_active\_in\_current\_and\_prev\_months(p) = \sum_{i=1}^{N_p} active\_in\_current\_and\_previous\_month_{p,i}$$

where  $N_p$  is the number of clients considered for period  $p$

2. Retention Rate is the share of clients from the previous month who remain active in the current month

$$RR(p) = \begin{cases} \frac{total\_active\_in\_current\_and\_prev\_months_p}{previous\_month\_clients_p}, & previous\_month\_clients_p \neq 0 \\ 0, & previous\_month\_clients_p = 0 \end{cases}$$

where  $previous\_month\_clients_p$  is the total number of active clients in month  $p-1$  for the selected cohort and filters.

Predictive Lifetime for specific period calculates as follows:

$$Predictive\_LT(p) = \begin{cases} \frac{1}{1-RR_p}, & RR_p \neq 1 \\ NULL, & RR_p = 1 \end{cases}$$

### Predictive CLV

Predictive Lifetime estimates the expected average Customer Lifetime Value for a client in period  $p$  based on the *Predictive Lifetime*, *Average Order Value* and average transactions frequency

Calculations:

1. Computes the average number of transactions per period:

$$T = \frac{N_t}{N_p}$$

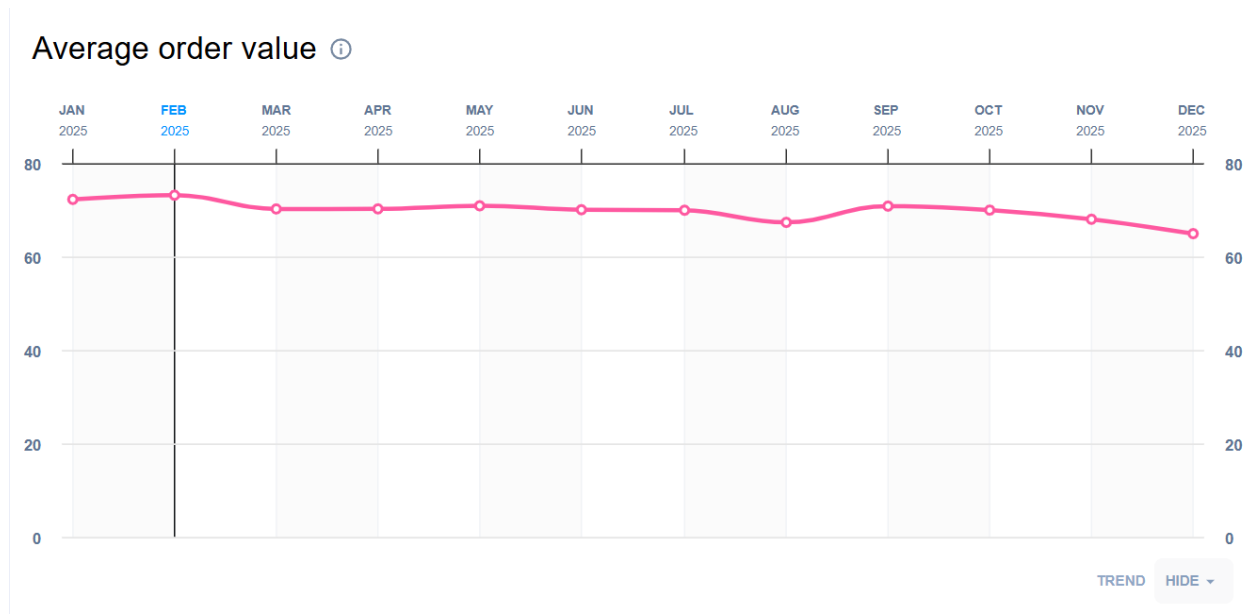
where  $N_t$  is the total number of selected transactions, and  $N_p$  is number of periods

2. For period  $p$ , Predictive CLV is calculated as:

$$Predictive\_CLV(p) = \begin{cases} \frac{T \cdot AOV_p \cdot Predictive\_LT_p}{total\_clients\_in\_previous\_month_p}, & total\_clients\_in\_previous\_month_p \neq 0 \\ 0, & total\_clients\_in\_previous\_month_p = 0 \end{cases}$$

where  $total\_clients\_in\_previous\_month_p$  is number of unique clients in month  $p-1$ ,  $AOV_p$  is *average order value* for specified period

### Average Order Value Graph



Average Order Value (AOV) is the average transaction amount for a specific period, expressed in the *selected reporting currency*.

Calculations:

Average order value for specific period  $p$  calculates as rounded average of all transactions, converted to the *selected in filters currency*, for this period:

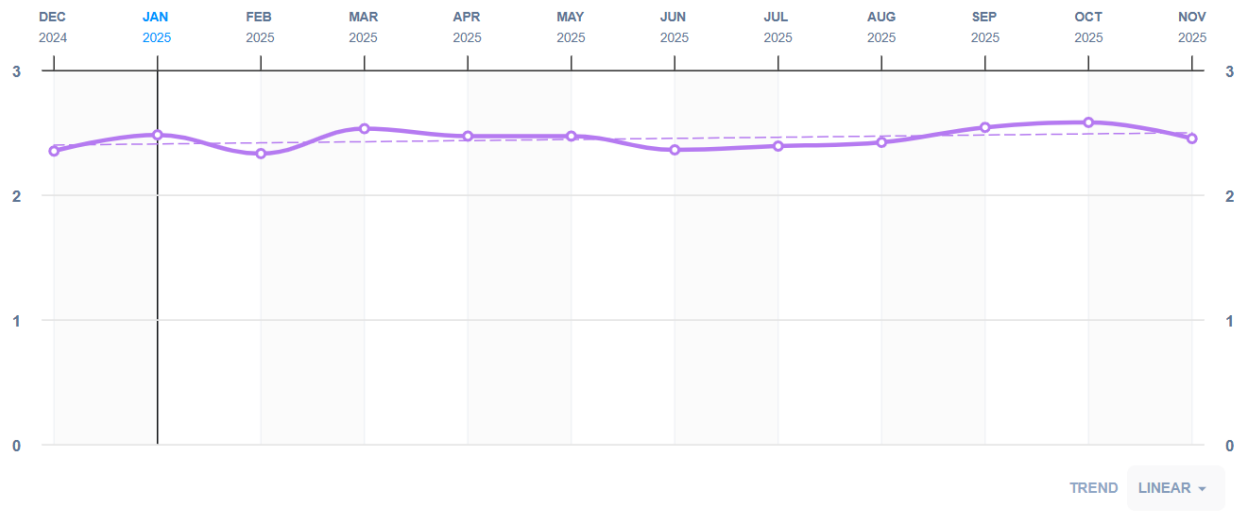
$$AOV(p) = \text{round}\left(\frac{1}{N_p} \cdot \sum_{i=1}^{N_p} amount_i \cdot convert\_rate, 2\right)$$

where  $N_p$  - is the number of all transactions for the period  $p$

### Average Time to Second Order Graph

Average time to second order - average time between first and second orders

Average time to second order ⓘ



Calculations:

Finds out transactions related to each payer (differentiated by card PAN) for the specified period of time:

- 1)  $pan_1 - T_1, T_2, T_3 \dots T_i$
- 2)  $pan_2 - T_1, T_2, T_3 \dots T_i$
- 3) ...

where  $T_1, T_2, T_3 \dots T_i$  - date and time when the payer with  $pan_1$  made payment

For each payer calculates the number of days between first ( $T_1$ ) and second ( $T_2$ ) transactions:

$$date\_diff_i = \text{days}(T_2 - T_1)$$

ATSO for specific period calculates as rounded average of date diff for all payers for this period:

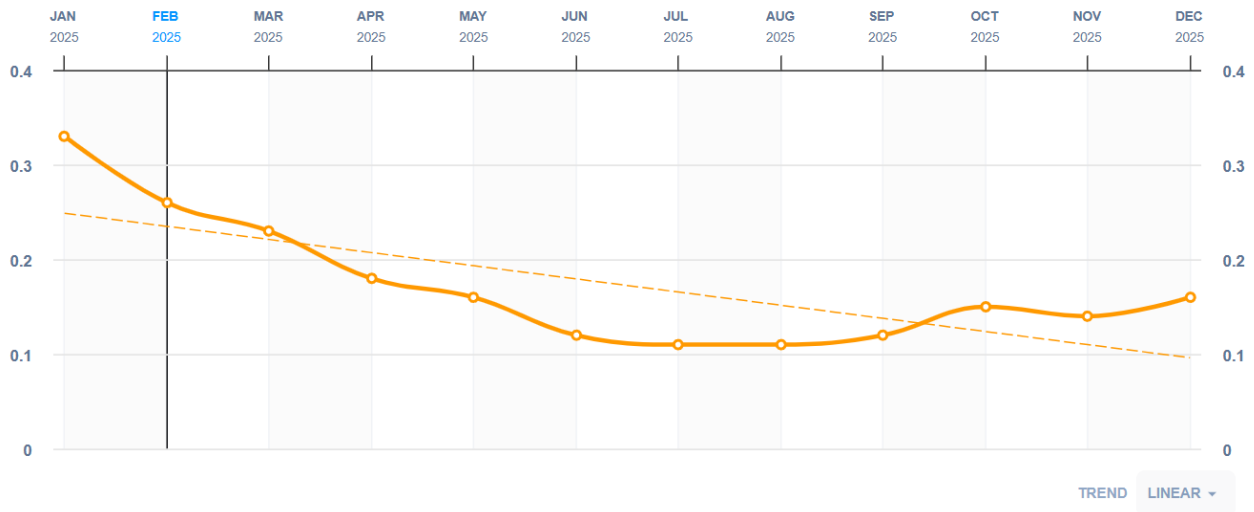
$$ATSO(p) = \text{round}\left(\frac{1}{N_p} \cdot \sum_{i=1}^{N_p} date\_diff_i, 2\right)$$

where  $N_p$  - is the number of all collected date\_diffs for period ( $p$ )

### Average Time to Next Order Graph

Average time to next order - average time between orders

Average time to next order ⓘ



Calculations:

Finds out transactions related to each payer (differentiated by card PAN) for the specified period of time:

- 1)  $pan_1 - T_1, T_2, T_3 \dots T_i$
- 2)  $pan_2 - T_1, T_2, T_3 \dots T_i$
- 3) ...

where  $T_1, T_2, T_3 \dots T_i$  - date and time when the payer with  $pan_1$  made payment

For each  $T_k$  finds a previous transaction made by the same payer and calculates the number of days between them:

$$date\_diff_{pan_i,k} = \text{days}(T_k - T_{k-1})$$

ATNO for specific period calculates as rounded average of all date diffs for all payers for this period:

$$ATNO(p) = \text{round}\left(\frac{1}{N_p} \cdot \sum_{i=1}^{N_p} \frac{1}{N_{pan_i}} \cdot \sum_{k=1}^{N_{pan_i}} date\_diff_{pan_i,k}, 2\right)$$

where  $N_p$  - is the number of all payers for period ( $p$ ), and  $N_{pan_i}$  - is the number of all date diffs for specific payer

**Return on Investment Bar Chart**

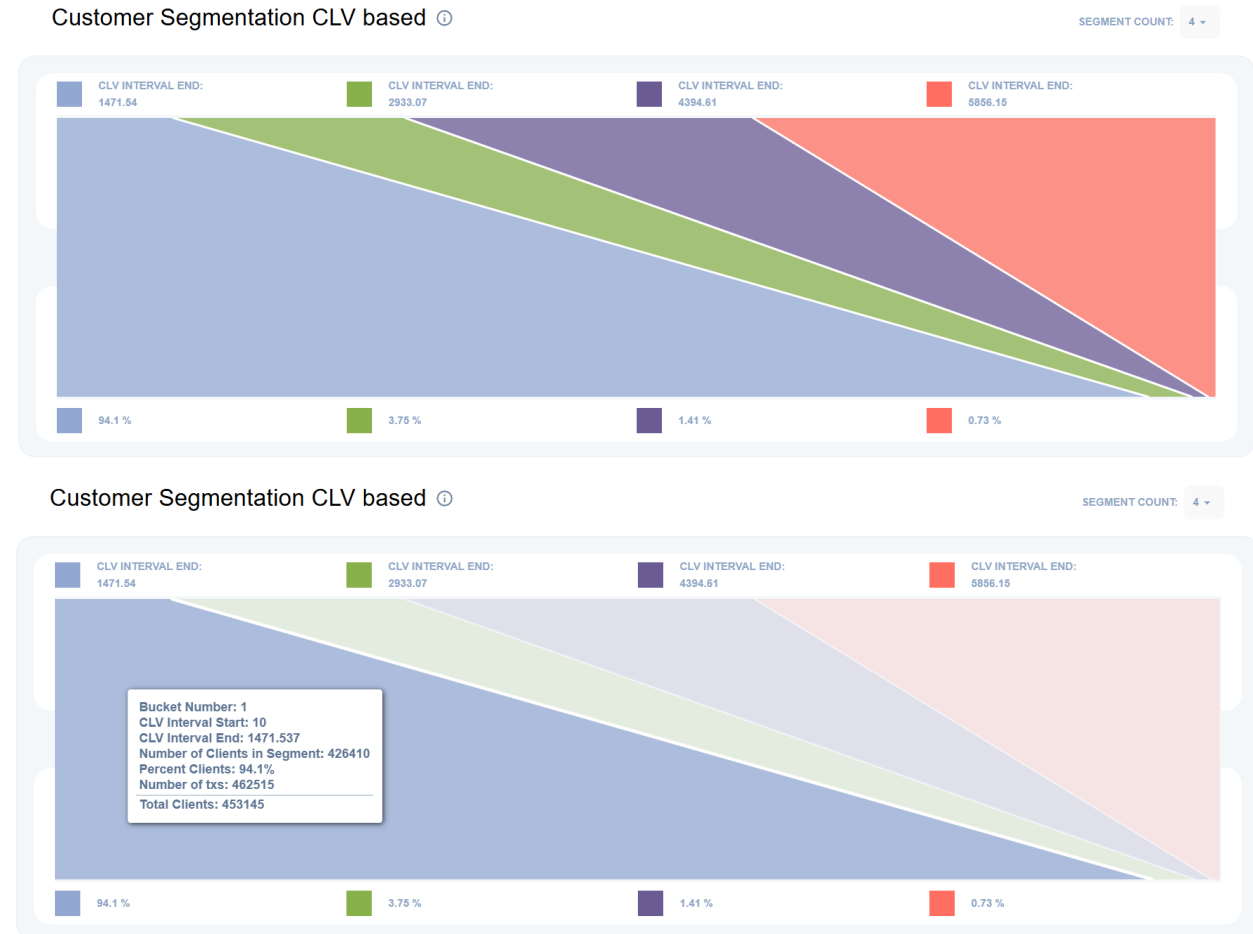
Return on Investment (ROI) expresses the relative return generated per acquired payer, measured against *Customer Acquisition Cost (CAC)*. Values are reported as percentages

Calculations:

For each period  $p$ , ROI is computed from the period CLV value  $CLV_p$  and the corresponding CAC:

$$ROI(p) = \begin{cases} \frac{CLV_p - CAC}{CAC} \cdot 100, & CAC \neq 0 \\ NULL, & CAC = 0 \end{cases}$$

## Customer Segmentation CLV Based Segment Chart



Shows the number of clients in each CLV bucket, providing a distribution of customers by their *Customer Lifetime Value (CLV)*

CLV bucket is a proportional interval of the CLV range used for segmentation. The bucket boundaries are derived from the robust CLV range between the 2nd and 98th percentiles ( $lmin$  and  $lmax$ ) and split into  $bucket\_count$  equal-width intervals (with a minimum bucket width of 1). Each client is assigned to a bucket based on their CLV value

1. For each payer calculates CLV as sum of all selected transactions:

$$Payer\_CLV = \sum_{i=1}^N amount_i \cdot convert\_rate$$

where  $N$  - number of all payer transactions

2. Computes bucket bounds (robust range) from CLV distribution:

$lmin$  = 2nd percentile (0.02 quantile) of all CLV values

$lmax$  = 98th percentile (0.98 quantile) of all CLV values

3. Interval calculates as difference between  $lmax$  and  $lmin$  divided by  $bucket\_count$ . If obtained value less than 1, interval will be 1:

$$interval = \max\left(\frac{lmax - lmin}{bucket\_count}, 1\right)$$

4. For each bucket defines its *interval\_start* and *interval\_end*:

$$interval\_start_i = (i - 1) \cdot interval + lmin$$

$$interval\_end_i = \begin{cases} i \cdot interval + lmin, & i \neq bucket\_count \\ lmax, & i = bucket\_count \end{cases}$$

where *i* - bucket number

5. Each customer is assigned to a corresponding bucket based on their CLV, after which the number of customers in the ranges of each bucket is calculated.
6. Percent clients - is the ratio of customers in the current segment to the total number of customers

$$Percent\_Clients_i = \frac{number\_of\_clients\_in\_segment_i}{total\_clients}$$

where *i* - bucket number

### Top 10 Table

Top 10 entities within the selected grouping type by its *CLV*

Table shows entity's name, *ROI* and CLV growth

$$growth = \left( \frac{CLV_{cur}}{CLV_{prev}} - 1 \right) \cdot 100$$

where *CLV<sub>cur</sub>* - CLV for current month, and *CLV<sub>prev</sub>* - CLV for previous month

### N-month (Retention Curve)

#### Overview

N-month retention shows the percentage of customers who made at least one payment in the N-th calendar month after their first payment month

#### Example

If second-month retention is 50%, it means that 50% of customers whose first payment occurred in the first month made at least one payment in the second month

Active clients — customers from the first payment month who made at least one payment in month *N*. All customers in the first payment month are considered active (by definition)

A customer from the first payment month who made payments in earlier months but did not make a payment in month *N* is a Dormant client

A Dormant client who makes a payment in month *N* is a Reactivated client.

New clients — customers who made at least one payment in month *N* but did not make any payment in the first payment month.

Total clients — the number of unique payers within the period defined in *general filters*.

First month is defined by the Starting with filter in *general filters*.

## Filters

Grouping type - specifies how metrics are aggregated and displayed in the reports. All calculations are performed independently for each group under the same filters and time range. Possible values: Manager, Merchant, Endpoint

Method - method of indicators calculation:

- Periodic - client considered as dormant in the first month if there were no payments.
- Retrospective - client considered as dormant after  $churn_p$  months during which there have been no payments

Churn period - filter of retrospective analysis. The number of months that must pass before a client is considered as Dormant

## N-month Retention Graph

### Periodic

Periodic N-month retention shows the percentage of customers who made at least one payment in the N-th calendar month after their payment in first month

Calculations:

1. Selects all clients who made at least one payment within the chosen reporting period
2. For each client, computes  $min\_period$  — the month of the client's first payment within the selected period. If  $min\_period$  equals the cohort start month, mark the client with the first month purchase flag

$$client\_fpd\_flag_i = \begin{cases} true, & min\_period = cohort\_period\_start \\ false, & min\_period \neq cohort\_period\_start \end{cases}$$

3. Each client who made purchase in specific month  $p$  marks with retention flag for this month
4. For month  $p$ , a client is considered Active if:
  - client has first month purchase flag
  - client has retention flag for month  $p$
  - if current month is not the first month of cohort period ( $p > cohort\_start\_period$ ), client made at least one transaction in previous month  $p - 1$
5. For month  $p$ , a client is considered Reactivated if:
  - client has first month purchase flag
  - client has retention flag
  - if current month is not the first month of cohort period ( $p > cohort\_start\_period$ ), client didn't make transactions in previous month  $p - 1$
6. Retention for period calculates as follows:

$$Ret_p = \frac{active\_clients_p + reactivated\_clients_p}{total\_clients\_in\_the\_first\_month}$$

## Retrospective

Retrospective N-month retention shows the percentage of customers who made at least one payment in the N-th calendar month or in the  $N - th - churn\_period\_window$  month after their payment in first month

Calculations:

1. Selects all clients who made at least one payment within the chosen reporting period
2. For each client, computes  $min\_period$  — the month of the client's first payment within the selected period. If  $min\_period$  equals the cohort start month, mark the client with the first month purchase flag

$$client\_fpd\_flag_i = \begin{cases} true, & min\_period = cohort\_period\_start \\ false, & min\_period \neq cohort\_period\_start \end{cases}$$

3. Each client who made purchase in current  $p$  month or  $p - churn\_period\_window$  months marks with retention flag for this month
4. For month  $p$ , a client is considered Active if:
  - client has first month purchase flag
  - client has retention flag for month  $p$
  - if current month is not the first month of cohort period ( $p > cohort\_start\_period$ ), client made at least one transaction in previous month  $p - 1$
5. For month  $p$ , a client is considered Reactivated if:
  - client has first month purchase flag
  - client has retention flag
  - if current month is not the first month of cohort period ( $p > cohort\_start\_period$ ), client didn't make transactions in previous month  $p - 1$
6. Retention for period calculates as follows:

$$Ret_p = \frac{active\_clients_p + reactivated\_clients_p}{total\_clients\_in\_the\_first\_month}$$

## Users Waterfall Chart

Chart shows number of clients per category in selected month  $p$ : New, Active, Reactivated, Dormant

Percent on chart is share of clients in specific category in selected month relative to the total number of clients for the whole period

## Quick Ratio Graph

Quick Ratio measures growth relative to churn risk. It is defined as the ratio of New and Reactivated clients to Dormant clients for month  $p$ .

Calculations:

$$QR_p = \begin{cases} \frac{new\_clients_p + reactivated\_clients_p}{dormant\_clients_p}, & dormant\_clients_p \neq 0 \\ 0, & dormant\_clients_p = 0 \end{cases}$$

## Average Revenue per User Graph

Average Revenue per User (ARPU) Graph shows average revenue per client by category (New, Active, Reactivated)

Calculations:

For each category  $c$  (New, Active, Reactivated): 1. Counts number of unique clients for specific month  $p$  2. Counts amount of all transactions for specific month  $p$  3. Average Revenue per User for specific month ( $p$ ) for specific category ( $c$ ) calculates as follows:

$$ARPU_{p,c} = \frac{transaction\_amount_{p,c}}{clients\_count_{p,c}}$$

Total amount - amount of all transactions for specific month

### Note

Some clients may not fit into any category. For example New clients from previous month won't be in any category in current month

$$Total\_amount_p \neq amount\_new_p + amount\_active_p + amount\_reactivated_p$$

## Repeat Customer Rate Graph

Repeat customer rate (RCR) - is the share of customers who made two or more transactions during the selected period  $p$ .

Calculations:

1. Counts number of unique customers who made 2 or more transactions for specific period  $p$
2. Counts total number of unique customers for specific period  $p$
3. Repeat customer rate calculates as follows:

$$RCR_p = \frac{repeat\_clients_p}{total\_clients_p}$$

## Repeat Customers Rate Count-to-Amount Ratio Bar

Repeat Customers Rate Count-to-Amount Ratio Bar shows correlation of single-purchase customers and their purchases and multi-purchase customers and their purchases for whole selected period of time

The Count-to-Amount Ratio bar chart compares single-purchase and multi-purchase customers across the entire selected period, showing both:

- the share of customers in each group
- the share of transaction amount generated by each group.

Single-purchase customers - customers with exactly one transaction in the selected period.

Multi-purchase customers - customers with two or more transactions in the selected period.

Calculations:

1. For each group (single- and multi- purchase customers) counts:

- number of unique customers
- total transaction amount

2. Counts total number of customers:

$$total\_number\_of\_customers = number\_of\_single\_purchase\_customers + number\_of\_multi\_purchase\_customers$$

3. Ratio customers count calculates as follows:

$$RCC_{single} = \frac{number\_of\_single\_purchase\_customers}{total\_number\_of\_customers}$$

$$RCC_{multi} = \frac{number\_of\_multi\_purchase\_customers}{total\_number\_of\_customers}$$

4. Ratio spent amount calculates as follows:

$$RSA_{single} = \frac{amount\_of\_single\_purchase\_customers\_transactions}{total\_transaction\_amount}$$

$$RSA_{multi} = \frac{amount\_of\_multi\_purchase\_customers\_transactions}{total\_transaction\_amount}$$

## Top 10 Table

Top 10 entities within the selected grouping type by its *Active percent*

Table shows entity's name, *Active percent* and Active clients growth

$$growth = \left( \frac{Active\_percent_{cur}}{Active\_percent_{prev}} - 1 \right) \cdot 100$$

where *Active\_percent<sub>cur</sub>* - percent of active clients in current month, and *Active\_percent<sub>prev</sub>* - percent of active clients in previous month

## COHORT (For the Period)

### Overview

### Filters

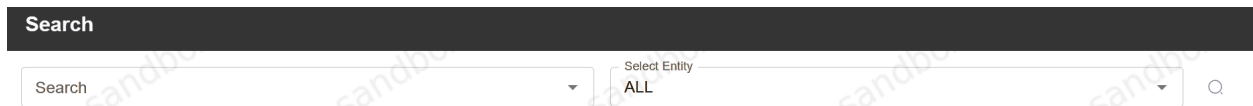
### Cohort Table

## 8.10.5 Templates

## SETTINGS

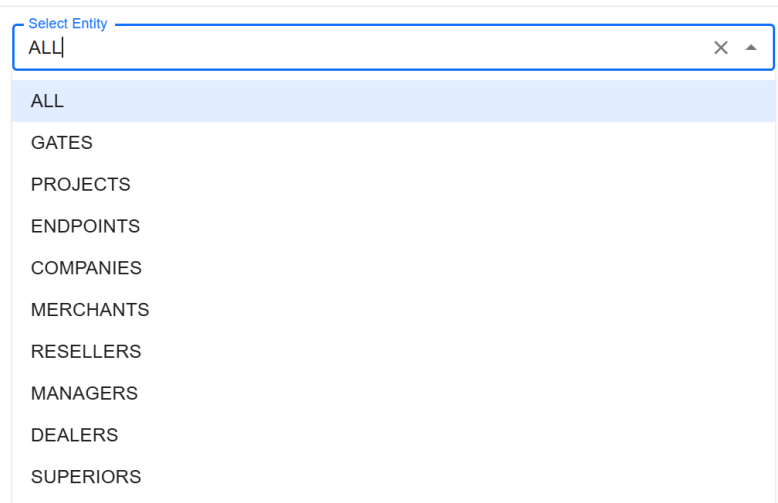
### 9.1 Settings Search

The screen is designed to find projects, endpoints and other entities by their name or ID and is located in “Settings” - “Settings Search” section.



The screenshot shows a dark header bar with the word "Search" in white. Below the header, there is a search input field with the placeholder text "Search" and a dropdown arrow. To the right of the search field is a dropdown menu labeled "Select Entity" with the option "ALL" selected. A magnifying glass icon is positioned to the right of the dropdown menu.

The search range can be specified to endpoints, projects or other entities.



The screenshot shows a dropdown menu titled "Select Entity" with a search input field containing "ALL". The dropdown list is open, showing the following options: ALL, GATES, PROJECTS, ENDPOINTS, COMPANIES, MERCHANTS, RESELLERS, MANAGERS, DEALERS, and SUPERIORS. The "ALL" option is highlighted in blue.

## 9.2 Configuration

### 9.2.1 Endpoint

#### Buy Now Button

- [Buy Now Button Setup](#)
- [Buy Now Button Required Fields](#)
- [Buy Now Button Payment Form Fields](#)

Buy Now Button integration is relevant for Merchants who has limited portfolio of products to sell. It is the easiest way to integrate with Doc4.0. This way of integration doesn't require much technical effort. Buy Now Button integration also allows Merchant (or Connecting Party which represents Merchant) to exclude itself from storing, processing, or transmitting Payer's cardholder data or other sensitive payment details. Such data is submitted by Payer on Doc4.0 hosted customer details form and payment form in PCI DSS certified environment.

#### Buy Now Button Setup

To configure Buy Now Button for Merchant's website follow these instructions:

- Find the relevant Endpoint
- Go to Buy Now Items tab
- Click Add item
- Fill in the required fields.

#### Buy Now Button Required Fields

Parameter Name	Description	Value
Amount	Amount to be charged. The amount has to be specified in the highest units with . delimiter. For instance, 10.5 for USD means 10 US Dollars and 50 Cents.	Necessity: Required Type: Numeric Length: 10
Description	The item's description.	Necessity: Required Type: String Length: 64k
redirect_url	The URL to the page where the Payer will be redirected after transaction is completed.	Necessity: Required Type: String Length: 1024

continues on next page

Table 1 - continued from previous page

Parameter Name	Description	Value
Destination	Destination to where the payment goes. It is useful for Merchants who let their payers to top up their accounts with bank card (Mobile phone accounts, game accounts etc.). Sample values are: +9999999999; mail@example.com etc. This value can be used by the fraud monitoring system.	Necessity: Optional Type: String Length: 128
Payment tool	Payment methods.	Necessity: Optional Type: String Length: 128

### Buy Now Button Payment Form Fields

To configure the fields to be shown on payment form, ask Doc4.0 support manager to:

- Go to API fields on the proper Endpoint.
- Mark each needed API field as Visible and/or Required.
- Save API fields and preview the payment form.

#### Warning

It is strictly advised to create separated Endpoints for Buy Now Button because activating this option might lead to errors with other types of integration. Also:

1. Buttons cannot be removed, only entire Endpoint can be disabled to stop transactions via Buy Now Button.
2. Transaction amount change on payment form will not be supported if any Buy Now Button is configured on this Endpoint.

### Create, Clone, Edit Endpoint

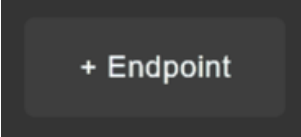
- [Endpoint Creation](#)
- [Endpoint Editing And Cloning](#)

### Endpoint Creation

To create endpoint, go to Settings -> Configuration -> End points and press + End point in the top right corner.

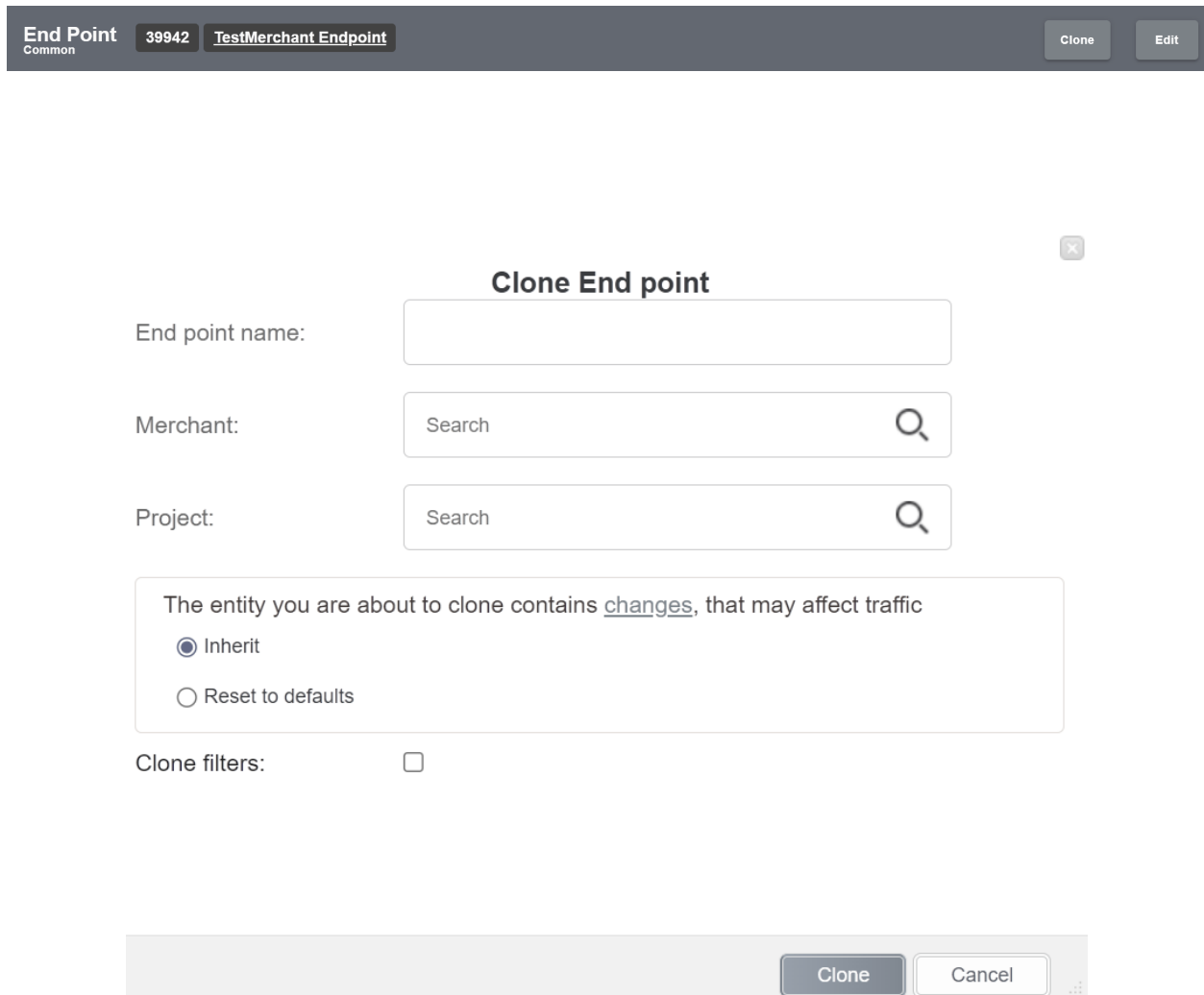
See [Endpoint details](#) table to correctly specify the configuration for new endpoint.

The endpoint inherits its currency from the project it's linked to.



## Endpoint Editing And Cloning

Press Edit button to edit endpoint and Clone button to clone endpoint.



End Point Common 39942 TestMerchant Endpoint Clone Edit

### Clone End point

End point name:

Merchant:

Project:

The entity you are about to clone contains changes, that may affect traffic

Inherit

Reset to defaults

Clone filters:

Clone Cancel

The required parameters for new endpoint are its name, the merchant to whom this endpoint will be linked, and project to which this endpoint will be linked. Endpoint currency will be inherited from linked project.

Other endpoint settings will be inherited automatically. In order to reset parameters to default, select Reset to default.

In order to see which changes for this endpoint will be cloned, press changes button.

✕

### Clone End point

End point name:

Merchant:  🔍

Project:  🔍

The entity you are about to clone contains changes, that may affect traffic

Inherit

Reset to defaults

Endpoint options

Show decline reason

Don't calc. statements

Verification tx type

Clone filters:

Endpoint will show only filters which are enabled on project level, see [Transaction Filters](#)  
 Endpoint filters settings rewrite project filter settings.

To clone filters click Clone filters.

## Callbacks

Additional Callback can be configured at the Endpoint level by using Create Callback utility. To set up new callback, go to the bottom of Endpoint details screen and click the “Add Callback” button. There are several parameters, which can be defined in the configuration window:

- Transaction type.
- URL address - is the fully defined URL with all the parameters Merchant’s target page or script would require. Example: [https://www.merchant.com/sale\\_completed](https://www.merchant.com/sale_completed).
- Comment if it is required.

## Create callback



Transaction type  
All

Url

Comment

+ Parameter

Cancel Create

### Message Templates

Message templates can be used to send SMS or E-mail messages to customer after each successful transaction. Merchant must provide their message server credentials to Doc4.0 support manager in order to send such messages from Merchant address. Templates are created using the Template button. Example of filling the form:

Example of a message template in the form:

Status	ID	Language	Message type
<input type="checkbox"/>	2	Afrikaans	Email (HTML)

« ← 1 - 1 → 10 25 50


**Endpoint** 13453  
Message templates


Status  
 E

Language

Subject template

Message type

 Message sending is enabled.

 Message sending is disabled.

### Account Balance

Each Connecting Party has a merchant user account created in Payment Gateway. If balance display is enabled, Merchant accounts can check current balances via Common tab on Endpoints. Balances also can be requested via API [by Endpoint](#)<sup>6</sup> or [by Merchant](#)<sup>7</sup>. Manager can get balance of any merchant by balance name via API request - [balance by Manager](#)<sup>8</sup> To configure balances, see [Account balances](#).

#### Note

Please contact Doc4.0 support to enable this feature.

An example of endpoint window with current balances is provided below:

Balances	
4 test:	102 097.80 USD
57 test EUR:	6 462.64 EUR
82 Test1:	0.00 AZN
84 check:	0.00 KZT

<sup>6</sup> [https://doc4.codetime.net/integration/API\\_commands/api\\_v2\\_get\\_balance.html](https://doc4.codetime.net/integration/API_commands/api_v2_get_balance.html)

<sup>7</sup> [https://doc4.codetime.net/integration/API\\_commands/api\\_v2\\_get\\_balance\\_merchant.html](https://doc4.codetime.net/integration/API_commands/api_v2_get_balance_merchant.html)

<sup>8</sup> [https://doc4.codetime.net/integration/API\\_commands/api\\_v2\\_get\\_balance\\_manager.html](https://doc4.codetime.net/integration/API_commands/api_v2_get_balance_manager.html)

## Endpoint Details

### Note

Settings specified on Endpoint level override Project level settings.

Parameter Name	Description	Necessity for creation
Status	Shows whether Endpoint is enabled or disabled. Can be changed later.	Required
Project	Shows to which exact project this endpoint is linked. CANNOT be changed later.	Required
Merchant	Shows to which exact merchant this endpoint is linked. CANNOT be changed later.	Required
Description	Shows Endpoint description. Can be changed later.	Optional
Manager rate plan	Allows to set manager rate plan. Can be changed later.	Optional
Reseller rate plan	Allows to set reseller rate plan if reseller is selected. Can be changed later.	Optional
Merchant rate plan	Allows to set additional merchant rate plan. Can be changed later.	Optional
Payment form template	Allows to add payment form which will be displayed after initiating the transaction.	Optional
Wait form template	Allows to add wait form which will be displayed until transaction reaches the final status.	Optional
Finish form template	Allows to add finish form which will be displayed after transaction reaches the final status.	Optional
Tags	Shows the tag of the Endpoint. While searching Endpoints by tag, all Endpoint with the same tag will be shown. Can be changed later.	Optional
Loyalty service	Shows which external loyalty service is selected. Can be changed later.	Optional
Min transaction amount	Possible to set any minimal amount which be passed through the endpoint. Transaction requests with amounts lower than minimum will be rejected. Can be changed later.	Optional

continues on next page

Table 2 - continued from previous page

Parameter Name	Description	Necessity for creation
Max transaction amount	Possible to set any maximum amount which be passed through the endpoint. Transaction requests with amounts higher than maximum will be rejected. Can be changed later.	Optional
Enable auto capture	Enables automatic capture.	Optional
Auto capture period (hours)	Sets the time in hours, after which preauthorized amount will be automatically captured.	Optional
Enable auto return	Enables automatic return.	Optional
Auto return period (minutes)	Sets the time in minutes, after which transaction will be refunded.	Optional
Message server	Allows to select message server.	Optional
Returning customer approve sessions count	Shows after how many transactions with final status approved, customer will be considered as returning for the endpoint.	Optional
Client definition	Shows by which criteria customer will be counted as new or returning for the endpoint.	Optional
Merchant Transfer Inquiry URL	URL of Connecting Party server for Check Transfer stage. Mandatory for <a href="https://doc4.codetime.net/integration/api_use_cases/mobile_device_transfer.html">Mobile Device Transfer</a> <sup>9</sup> .	Optional
Merchant Transfer Notif. URL	URL of Connecting Party server for Transfer Card Mapping stage. Mandatory for <a href="https://doc4.codetime.net/integration/api_use_cases/mobile_device_transfer.html">Mobile Device Transfer</a> <sup>10</sup> .	Optional
Merchant Sale Inquiry URL	URL of Connecting Party server for Check Sale stage. Mandatory for <a href="https://doc4.codetime.net/integration/api_use_cases/mobile_device_sale.html">Mobile Device Sale</a> <sup>11</sup> .	Optional
Merchant Sale Notif. URL	URL of Connecting Party server for Sale Card Mapping stage. Mandatory for <a href="https://doc4.codetime.net/integration/api_use_cases/mobile_device_sale.html">Mobile Device Sale</a> <sup>12</sup> .	Optional
Merchant Verification Inquiry URL	URL of Connecting Party server for Check Verification stage. Mandatory for <a href="https://doc4.codetime.net/integration/api_use_cases/mobile_device_card_verification.html">Mobile Device Verification</a> <sup>13</sup> .	Optional
Merchant Ver. Notif. URL	URL of Connecting Party server for Verification Card Mapping stage. Mandatory for <a href="https://doc4.codetime.net/integration/api_use_cases/mobile_device_card_verification.html">Mobile Device Verification</a> <sup>14</sup> .	Optional

<sup>9</sup> [https://doc4.codetime.net/integration/api\\_use\\_cases/mobile\\_device\\_transfer.html](https://doc4.codetime.net/integration/api_use_cases/mobile_device_transfer.html)

<sup>10</sup> [https://doc4.codetime.net/integration/api\\_use\\_cases/mobile\\_device\\_transfer.html](https://doc4.codetime.net/integration/api_use_cases/mobile_device_transfer.html)

<sup>11</sup> [https://doc4.codetime.net/integration/api\\_use\\_cases/mobile\\_device\\_sale.html](https://doc4.codetime.net/integration/api_use_cases/mobile_device_sale.html)

<sup>12</sup> [https://doc4.codetime.net/integration/api\\_use\\_cases/mobile\\_device\\_sale.html](https://doc4.codetime.net/integration/api_use_cases/mobile_device_sale.html)

<sup>13</sup> [https://doc4.codetime.net/integration/api\\_use\\_cases/mobile\\_device\\_card\\_verification.html](https://doc4.codetime.net/integration/api_use_cases/mobile_device_card_verification.html)

<sup>14</sup> [https://doc4.codetime.net/integration/api\\_use\\_cases/mobile\\_device\\_card\\_verification.html](https://doc4.codetime.net/integration/api_use_cases/mobile_device_card_verification.html)

## Endpoint Overview

Endpoint is uniquely identified terminal in Payment Gateway, which is assigned to the Merchant and has to be provided in the commands within Payment Gateway API. The Endpoint list screen is located at Settings -> Configuration -> End points. This screen contains all Endpoints created for all Merchants in the system.

Status	ID ↑	Name	Description
<input checked="" type="checkbox"/>	13453	test endpoint	
<input checked="" type="checkbox"/>	13461	test endpoint 2	
<input checked="" type="checkbox"/>	13497	master endpoint	test

- Endpoint is enabled.

- Endpoint is disabled.

To monitor the Endpoint activity, Key Performance Indicators (KPI) are used, such as: Merchant earnings, Average order value, and others. The KPI submenu opens by pressing the Detailed button on the Endpoint search screen. See details in [KPIs Detailed View](#).

Click on the Endpoint name to open detailed information about this endpoint.

It is possible to configure custom payment forms on Endpoint or Master Endpoint, see [Forms Customization](#)<sup>15</sup> in integration documentation. Customized forms can be installed on Endpoint details screen.

To view the filters configured on the Endpoint, use the “Fraud protection filters” tab.

To view the necessity of additional fields on payment form, use the “API Fields” tab.

To work with other configuration options, see the information below.

### Note

The Endpoint settings (such as limits, payment forms, client definition, etc) override the Project settings.

## Endpoint Settings

<sup>15</sup> [https://doc4.codetime.net/integration/reference/forms\\_customization.html](https://doc4.codetime.net/integration/reference/forms_customization.html)

<a href="#">Create, Clone, Edit Endpoint Message Templates</a>	This screen shows how to create and edit the endpoint. This screen shows all information about message templates sent to Customers after transactions.
<a href="#">Endpoint Details</a>	Endpoint details screen contains information about configured options on this Endpoint, its ID, limits and linked Project.
<a href="#">Callbacks</a>	This screen shows how to set up callbacks on Endpoint level.
<a href="#">Buy Now Button</a>	This screen shows information and how to set up Buy Now Button.
<a href="#">Endpoint Account Balance</a>	This screen shows all information about Account Balances.

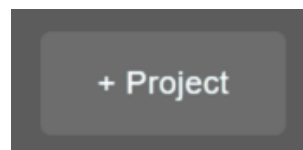
## 9.2.2 Project

### Create, Clone, Edit Project

- [Project Creation](#)
- [Project Editing And Cloning](#)

#### Project Creation

To create Project go to Settings -> Configuration -> Projects and press + Project in the top right corner.



#### Project Editing And Cloning

Press Edit button to edit project and Clone button to clone project.



Select new name and currency.

Project name  
New Test Project

Currency:  
USD

Advanced options

- CLONE GATE     CLONE END POINT    OTHER SETTINGS
- Convert currency settings     Clone project filters
- Convert currency Gate settings     Clone gate filters
- Convert currency Endpoint settings     Clone endpoint filters

The entity you are about to clone contains changes, that may affect traffic

- Inherit
- Reset to defaults

Cancel    Clone

Click on Gate and select which gates to clone together with the project, then select new names for these gates.

Advanced options

- CLONE GATE     CLONE END POINT    OTHER SETTINGS

GATE NAME	NEW GATE NAME
<input checked="" type="checkbox"/> TestGate	New Test Gate
<input checked="" type="checkbox"/> TestGate 2	New Test Gate 2

Cancel    Clone

Click on Endpoint and select which endpoints to clone together with the project, then select new names and which merchant will be assigned for these endpoints.

**Advanced options**

- CLONE GATE   
  CLONE END POINT   
 OTHER SETTINGS

END POINT NAME	NEW END POINT NAME	MERCHANT
<input checked="" type="checkbox"/> TestEndpoint	<input type="text" value="New Endpoint"/>	<input style="border: none; border-bottom: 1px solid #ccc;" type="text" value="Test Merchant"/> ▼
<input checked="" type="checkbox"/> TestEdnpoint 2	<input type="text" value="New Endpoint 2"/>	<input style="border: none; border-bottom: 1px solid #ccc;" type="text" value="Test Merchant"/> ▼
<input checked="" type="checkbox"/> TestEndpoint 3	<input type="text" value="New Endpoint 3"/>	<input style="border: none; border-bottom: 1px solid #ccc;" type="text" value="Test Merchant"/> ▼

Click on Other Settings to select whether to convert currency and copy all available filters on new entities or reset them to default.

**Advanced options**

- CLONE GATE   
  CLONE END POINT   
 OTHER SETTINGS

- Convert currency settings   
  Clone project filters  
 Convert currency Gate settings   
  Clone gate filters  
 Convert currency Endpoint settings   
  Clone endpoint filters

The entity you are about to clone contains changes, that may affect traffic

- Inherit  
 Reset to defaults

To see which changes will be applied to cloned entity, press changes button.

Project options:	Current value:	Default value:
Show decline reason	ALL	Y
Customer definition ID	1	-
Validate tx rates	Y	-
Verification tx type	3	-
Manual transaction review	N	-
Use black lists	Y	N

**Project Details**

Parameter Name	Description	Necessity for creation
Status	Shows whether Project is enabled or disabled. Can be changed later.	Required
Manager	Shows to which exact manager this project is linked. CANNOT be changed later.	Required
Manager rate plan	Allows to set manager rate plan. Can be changed later.	Required
Description	Shows Project description. Can be changed later.	Optional

continues on next page

Table 4 - continued from previous page

Parameter Name	Description	Necessity for creation
Reseller rate plan	Allows to set reseller rate plan if reseller is selected. Can be changed later.	Optional
Payment form template	Allows to add payment form which will be displayed after initiating the transaction.	Optional
Wait form template	Allows to add wait form which will be displayed until transaction reaches the final status.	Optional
Finish form template	Allows to add finish form which will be displayed after transaction reaches the final status.	Optional
Tags	Shows the tag of the Project. While searching Projects by tag, all Project with the same tag will be shown. Can be changed later.	Optional
Loyalty service	Shows which external loyalty service is selected. Can be changed later.	Optional
Min transaction amount	Possible to set any minimal amount which be passed through the project. Can be changed later.	Optional
Max transaction amount	Possible to set any maximum amount which be passed through the project. Can be changed later.	Optional
Enable auto capture	Enables automatic capture.	Optional
Auto capture period (hours)	Sets the time in hours, after which preauthorized amount will be automatically captured.	Optional
Message server	Allows to select message server.	Optional
Returning customer approve sessions count	Shows after how many transactions with final status approved, customer will be considered as returning for the project.	Optional
Client definition	Shows by which criteria customer will be counted as new or returning for the project.	Optional

### Hold Pre-auth until capture settings

This section allows you to configure limits for preauth transactions before capture stage. Once the set limits are reached, subsequent preauth transactions are automatically held in processing status.

## Hold Pre-auth until capture settings

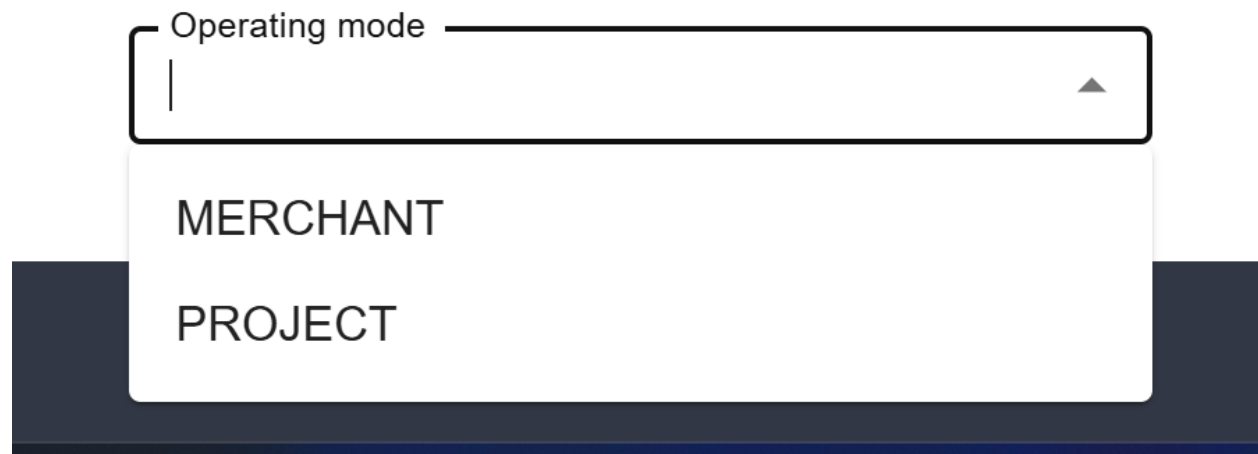
Operating mode ▼

## Operating mode

The Operating mode defines the scope of the limits. You can choose between PROJECT and MERCHANT.

- PROJECT - Limits are calculated across the entire project.
- MERCHANT - Limits are applied individually per merchant.

## Hold Pre-auth until capture settings



The image shows a screenshot of a web interface. At the top, there is a label 'Operating mode' followed by a dropdown menu. The dropdown menu is open, showing two options: 'MERCHANT' and 'PROJECT'. The background of the interface is dark blue.

## Preauth live time, quantity limit, amount

**Preauth live time** - The duration (in hours) after which the blocking period expires. Once this time passes, new pre-auth transactions will resume processing normally.

**Quantity limit** - The maximum number of preauth transactions allowed to pass. Once reached, new transactions will enter processing status until manually declined or the limit resets.

**Amount** - The maximum total volume (sum) of preauth transactions allowed. Any transaction that causes the amount to exceed this value will remain in processing status.

## Hold Pre-auth until capture settings

Operating mode  ✕ ▼

to reset the settings, you need to clear the type selection

Preauth live time

Quantity limit

Amount

### Note

All the transaction that surpassed limit will receive status after limit duration passes.

### Message Templates

Message templates can be used to send SMS or E-mail messages to customer after each successful transaction. Merchant must provide their message server credentials to Doc4.0 support manager in order to send such messages from merchant address. Templates are created using the Template button. After pressing it, a window with new template details will open:

The created template will appear in the list:

**Project** 6571  
 Message templates

Status \* ▼

Merchant \* ▼

Language \* ▼

Subject template \*


Message type \* ▼

Body template \*

Status	ID	Language	Message type
<input checked="" type="checkbox"/>	2	Afrikaans	Email (HTML)

« ← 1-1 →
10 25 50

 Message sending is enabled.

 Message sending is disabled.

### Note

After cloning the project, Message Templates will need to be created manually again for the cloned project.

## Routing & Balancing

- [General Information](#)
- [Routing Types](#)
  - [Source Card](#)

- *Destination Card*
- *Customer*
- *Transaction*
- *Transfer*
- *IP Intelligence*
- *Balancing Types*
  - *Balance By Coefficient*
  - *Balance Equally*
  - *Cascading Chain*
  - *Others*
- *Additional Configurations*
  - *Gate Skips*
  - *Ignore Gates For Direct Processing*
  - *Rates*
  - *Copy, Paste, Cut, Delete*
  - *Import And Export*

### **General Information**






The routing & balancing system allows to distribute traffic between payment gates flexibly depending on the defined criteria and customer's transaction data. Traffic can be routed to a specific group of gates/processors and distributed between them in accordance with the specified balancing. The balancing is configured on the system Project level in the Routing & Balancing tab.

One of routing types must be selected to start the configuration:


## Balancing

for project id: 1209

### SOURCE CARD

-  **Type**  
Visa, Mastercard etc.
-  **BIN**  
190000, 189999 etc.
-  **Bank**  
Sberbank, Tinkoff etc.
-  **Country**  
Russia, USA etc.
-  **Level**  
ATM, CASH BACK etc.

### DESTINATION CARD

-  **Type**  
Visa, Mastercard etc.

New routing block will be created. Each routing block has it's own ID for easier navigation in big projects. The Source Card Type routing type is taken as an example:

## SOURCE\_CARD\_TYPE # 3504

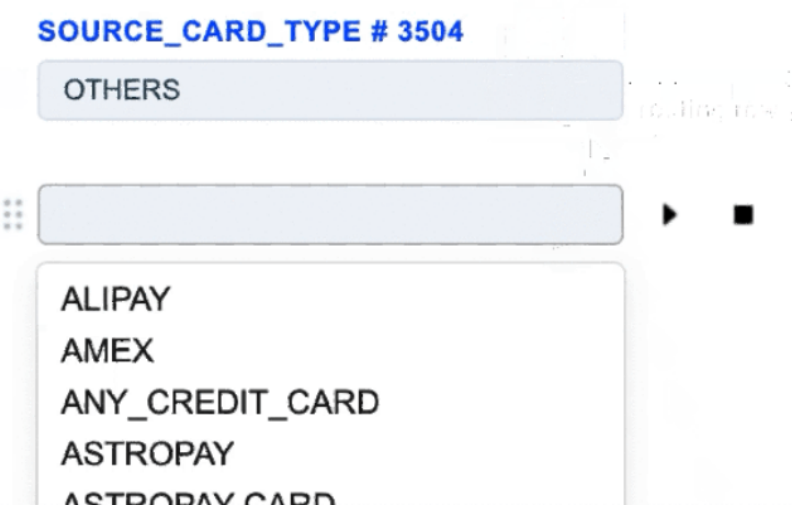
OTHERS

Hover the cursor over the name of this block to select one of the following actions:

**+** - Add routing row - to add options for this block:



Select the card types from the provided list:



**SOURCE\_CARD\_TYPE # 3504**

OTHERS

VISA × MASTERCARD ×

JCB ×

✘ - Delete node - to select another routing or balancing block instead of this one.

Hover the cursor over the any criterion of this block to select one of the following actions:

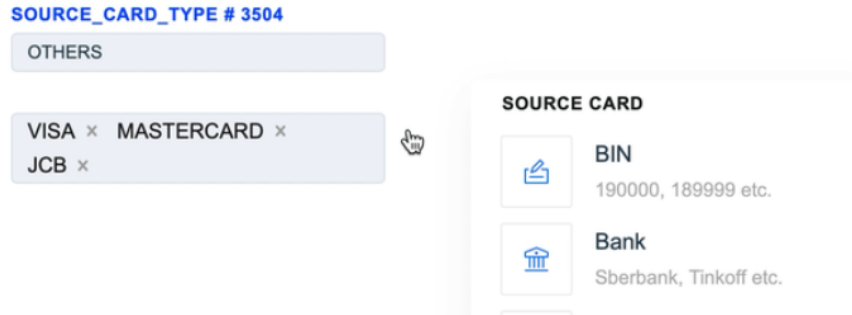
▶ - Continue Routing - to select new routing block and continue the routing strategy.

**SOURCE\_CARD\_TYPE # 3504**

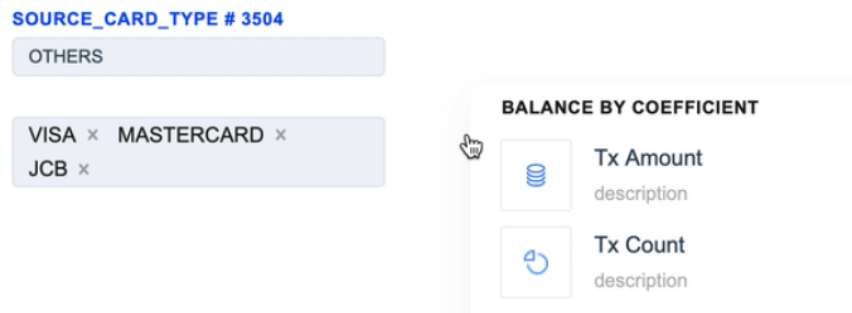
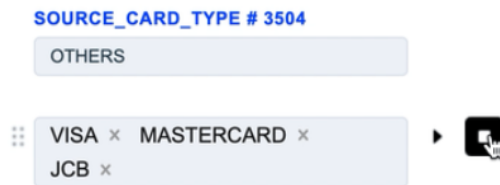
OTHERS

⋮ VISA × MASTERCARD ×  
JCB ×





- - Add balancing - to stop the routing and add the balancing block.



- ⋮ - to enable, disable or delete the routing option.

**SOURCE\_CARD\_TYPE # 3504**

OTHERS

VISA x MASTERCARD x  
JCB x**SOURCE\_CARD\_TYPE # 3504**


OTHERS



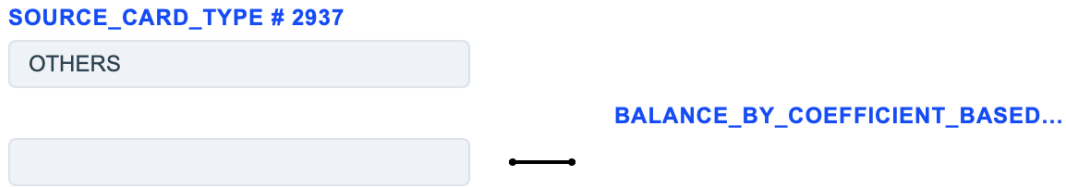
VISA x MASTERCARD x

 On Delete

The default option named OTHERS is always present, it applies for transactions which don't match all other created options.

If the created routing options are enough, click the Add balancing  button to add one of the balancing types with the payment gates.

The Balance by coefficient Based on Tx Amount is taken as an example:



Blocks are connected by arrows to improve the visual presentation. An arrow is directed from a certain routing option to the block created from it. If the transaction parameters match the specified routing option, it is forwarded further along the arrow.

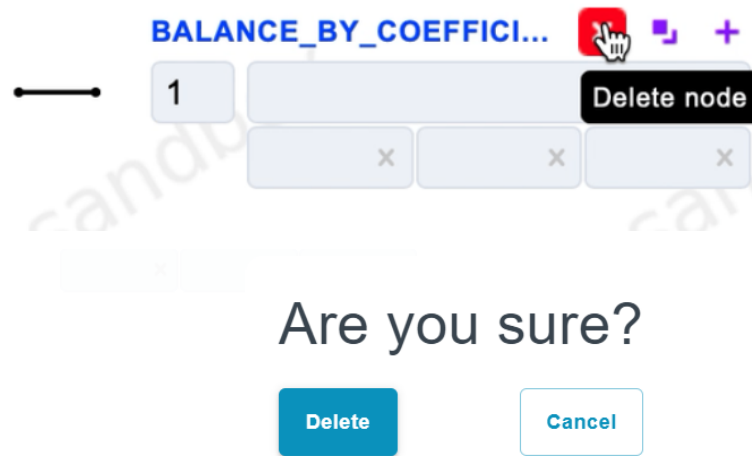
Hover the cursor over the name of this block to select one of the following actions:

**+** - Add balancing row - adds the row with active fields to specify the gate:

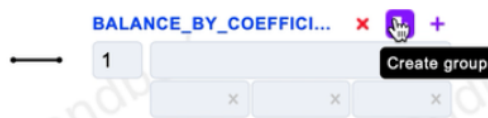


- Payment gate - the longest field is used to select one of the available payment gates.
- Probability percentage - far left field. This percentage determines how likely the transaction is to go to this gate. This field exists only for balancing types with a specified coefficient.
- Three empty fields at the bottom are used to redefine the payment rates.

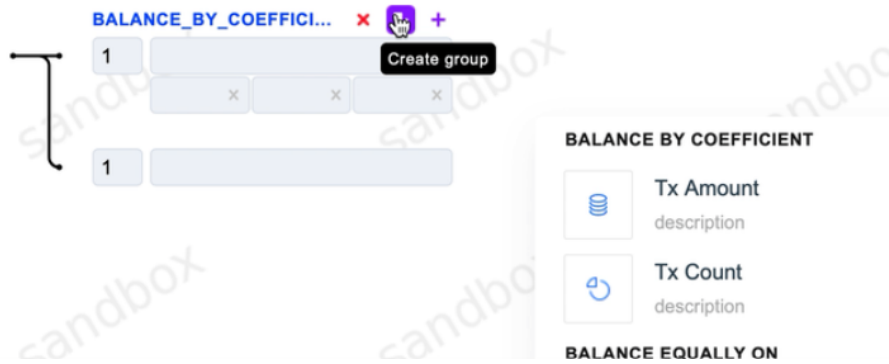
✘ - Delete node - to select another routing or balancing block instead of this one.



📌 - Create group - to create a group of the balancing.



Select a group of the balancing from the provided list:



### BALANCE\_BY\_COEFFICIENT\_BASED...

1

\_\_\_\_\_

\_\_\_\_\_ x \_\_\_\_\_ x \_\_\_\_\_ x

If the transaction meets the created route conditions, it will be forwarded to the balancing block with this payment gate. For more routing criteria, click the Add routing row of the required criterion, then create the subsequent transaction path from it. New block appears to the right of the selected criterion with a new number and routing type name.

The Source Card BIN routing type is taken as an example:

SOURCE\_CARD\_TYPE # 8724

OTHERS

JCB x

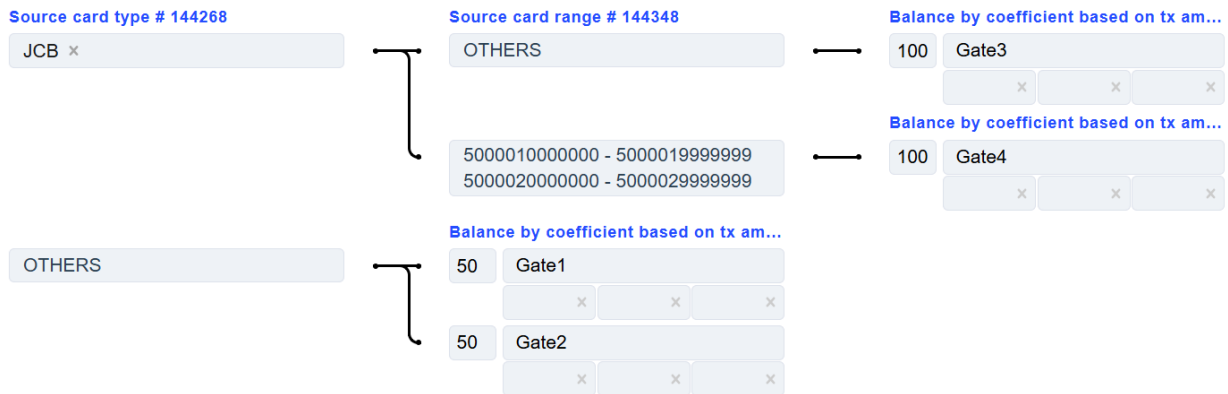
SOURCE\_CARD\_BIN # 8802

OTHERS

500001 x 500002 x



There is already an “OTHERS” default criterion below. As in the first case, click the Add routing row to add the appropriate criterion. Depending on the required routing strategy and the traffic separation level, go on building the routes or finish the route by adding one of the Balancing types and clicking Add balancing row to add the payment gate. The final configuration might look as the following:



**Note**

See the information below to check which types of *routing* and *balancing* are available and which *Additional Configurations* can be applied.

After the Routing & Balancing configuration is set, enable it by going to the “Project” menu, clicking the “Edit” button and selecting the “Use new balancing” check box at the bottom of

the page. To confirm the selection, click “Update”.

Reduce chargeback after reversal

YES NO

Manual transaction review

YES NO

Default Redirect URL

Use new balancing

Average Gross Profit Margin Default Marketing Campaign Returning customer approve sessions count

2

Client definition

by card holder and e-mail

Now, the Routing & Balancing is applied and all the traffic will go through it.

## Routing Types

Several “routing types” are used in the Routing & Balancing to configure the transaction routes more flexibly.

Routing types are filters which allow to specify the traffic separation. Depending on the selected routing type, the transaction flow will be checked in relation to its parameters.

In the Routing & Balancing such routing types are represented as follows:

### Source Card

- 1) The Source Card Type routing type allows to sort transactions by the sender’s card type. Select the appropriate payment methods of the sender and build a further route based on them.

**SOURCE\_CARD\_TYPE # 2524**

OTHERS



ALIPAY

AMEX

ANY\_CREDIT\_CARD

ASTROPAY

ASTROPAY CARD

BITCOIN

CABAL

2) The Card Range routing type allows to sort transactions by the sender's card BIN value. Specify bin and choose the needed BIN range of the sender and build a further route based on it. Several BIN ranges can be found for the specified BIN value. Select the one with lower priority. There is an option to search cards by their BINs. System can search for up to 500 entered card BINs listed one after another and separated by commas. They can be chosen by pressing the "BINs -" button.



Select banks to work with  
Banks available for selection



Buttons: Show all, Only selected (0), Add by BIN IDs, Hide filter ^

BINs - + Add filter [refresh icon]

<input type="checkbox"/>	ID	BIN	COUNTRY CODE	NUMERIC	STATUS	NAME
<input type="checkbox"/>	254909	005037	RUS	643	●	UNKNOWN
<input type="checkbox"/>	458746	011300	PHL	608	●	UNKNOWN
<input type="checkbox"/>	458747	011308	PHL	608	●	UNKNOWN
<input type="checkbox"/>	458748	021502	PRI	630	●	UNKNOWN
<input type="checkbox"/>	316207	042410	USA	840	●	FIFTH THIRD BANK
<input type="checkbox"/>	1	100001	CAN	124	●	CENTRAL SUPPLIES - TDFS
<input type="checkbox"/>	317651	100510	GBR	826	●	UNKNOWN
<input type="checkbox"/>	317652	100515	NOR	578	●	UNKNOWN
<input type="checkbox"/>	309718	101200	GBR	826	●	ASTROPAY CARD
<input type="checkbox"/>	309719	101201	GBR	826	●	ASTROPAY CARD
<input type="checkbox"/>	309720	101202	GBR	826	●	ASTROPAY CARD
<input type="checkbox"/>	309721	101203	GBR	826	●	ASTROPAY CARD
<input type="checkbox"/>	309722	101204	GBR	826	●	ASTROPAY CARD
<input type="checkbox"/>	309723	101205	GBR	826	●	ASTROPAY CARD
<input type="checkbox"/>	309724	101206	GBR	826	●	ASTROPAY CARD
<input type="checkbox"/>	309725	101207	GBR	826	●	ASTROPAY CARD

← BACK

ADD SELECTED

No more than 500

BINs

+

3) The Source Card Bank routing type allows to sort transactions by the sender's Issuer Bank name. Select the needed names of sender's Issuer Banks and build a

further route based on them. There is an option to search Banks by their names. System can search for up to 500 entered Bank names listed one after another and separated by commas. They can be chosen by pressing the “By name -” button.

**SOURCE\_CARD\_BANK # 2532**

OTHERS

GRAND COMMERCIAL BANK x

Select banks to work with  
Banks available for selection



Only selected (0)

<input type="checkbox"/>	ID	NAME	COUNTRY CODE	NUMERIC	STATUS
<input type="checkbox"/>	1	CENTRAL SUPPLIES - TDFS	CAN	124	<span style="color: green;">●</span>
<input type="checkbox"/>	2	UNKNOWN	USA	840	<span style="color: green;">●</span>
<input type="checkbox"/>	3	I&M BANK	KEN	404	<span style="color: green;">●</span>
<input type="checkbox"/>	4	LUXURY JEWELLERY CLASS (LJC) - TDFS	CAN	124	<span style="color: green;">●</span>
<input type="checkbox"/>	5	CASTLE BUILDING CENTRES - TDFS	CAN	124	<span style="color: green;">●</span>
<input type="checkbox"/>	6	BOSE - TDFS	CAN	124	<span style="color: green;">●</span>
<input type="checkbox"/>	7	CHARM DIAMOND CENTRES - TDFS	CAN	124	<span style="color: green;">●</span>
<input type="checkbox"/>	8	CRESCENT GOLD & DIAMONDS - TDFS	CAN	124	<span style="color: green;">●</span>
<input type="checkbox"/>	9	CANTREX - TDFS	CAN	124	<span style="color: green;">●</span>
<input type="checkbox"/>	10	CORBEIL - TDFS	CAN	124	<span style="color: green;">●</span>
<input type="checkbox"/>	11	BEN MOSS JEWELLERS - TDFS	CAN	124	<span style="color: green;">●</span>
<input type="checkbox"/>	12	OUROCARD	BRA	076	<span style="color: green;">●</span>
<input type="checkbox"/>	13	JCB	JPN	392	<span style="color: green;">●</span>
<input type="checkbox"/>	14	DINERS CLUB INTERNATIONAL	GBR	826	<span style="color: green;">●</span>
<input type="checkbox"/>	15	DINERS CLUB INTERNATIONAL	HUN	348	<span style="color: green;">●</span>
<input type="checkbox"/>	16	DINERS CLUB INTERNATIONAL	USA	840	<span style="color: green;">●</span>

← BACK

ADD SELECTED

No more than 500

By name

+

- 4) The Source Card Country routing type allows to sort transactions by the sender's card Country. Select the needed countries of the sender and build a further route based on them.

#### SOURCE\_CARD\_COUNTRY # 2535

- Andorra
- United Arab Emirates
- Afghanistan
- Antigua and Barbuda
- Anguilla
- Albania

- 5) The Source Card Credit Source routing type allows to sort transactions by the sender's card type. Select the needed card types of the sender and build a further route based on them.

**SOURCE\_CARD\_CREDIT\_SOURCE # 9...**

Credit × Prepaid ×  
 Prepaid Reloadable ×  
 Prepaid Non-Reloadable ×  
 Debit × Charge ×  
 Deferred Debit ×  
 Non-Mastercard ×

OTHERS

**Destination Card**

- 1) The Destination Card Type routing type allows to sort transactions by the receiver's card type. Select the needed card types of the receiver and build a further route based on them.

**DESTINATION\_CARD\_TYPE # 2539**

OTHERS

⋮ |

ALIPAY  
 AMEX  
 ANY\_CREDIT\_CARD  
 ASTROPAY  
 ASTROPAY CARD  
 BITCOIN  
 CABAL

- 2) The Card Range routing type allows to sort transactions by the receiver's card BIN value. Specify bin and choose the needed BIN range of the receiver and build a further route based on it. Several BIN ranges can be found for the specified BIN value. Select the one with lower priority. There is an option to search cards by their BINs. System can search for up to 500 entered card BINs listed one after another and separated by commas. They can be chosen by pressing the "BINs -" button.

DESTINATION\_CARD\_RANGE # 79550

OTHERS

52132400000000000000 - 52132477...

55467300000000000000 - 55467399...

42763800100000000000 - 42763802...

Select banks to work with ×  
Banks available for selection

[Show all](#) Only selected (0) [Add by BIN IDs](#) [Hide filter](#) ^

BINs - [+ Add filter](#)

<input type="checkbox"/>	ID	BIN	COUNTRY CODE	NUMERIC	STATUS	NAME
<input type="checkbox"/>	254909	005037	RUS	643	●	UNKNOWN
<input type="checkbox"/>	458746	011300	PHL	608	●	UNKNOWN
<input type="checkbox"/>	458747	011308	PHL	608	●	UNKNOWN
<input type="checkbox"/>	458748	021502	PRI	630	●	UNKNOWN
<input type="checkbox"/>	316207	042410	USA	840	●	FIFTH THIRD BANK
<input type="checkbox"/>	1	100001	CAN	124	●	CENTRAL SUPPLIES - TDFS
<input type="checkbox"/>	317651	100510	GBR	826	●	UNKNOWN
<input type="checkbox"/>	317652	100515	NOR	578	●	UNKNOWN
<input type="checkbox"/>	309718	101200	GBR	826	●	ASTROPAY CARD
<input type="checkbox"/>	309719	101201	GBR	826	●	ASTROPAY CARD
<input type="checkbox"/>	309720	101202	GBR	826	●	ASTROPAY CARD
<input type="checkbox"/>	309721	101203	GBR	826	●	ASTROPAY CARD
<input type="checkbox"/>	309722	101204	GBR	826	●	ASTROPAY CARD
<input type="checkbox"/>	309723	101205	GBR	826	●	ASTROPAY CARD
<input type="checkbox"/>	309724	101206	GBR	826	●	ASTROPAY CARD
<input type="checkbox"/>	309725	101207	GBR	826	●	ASTROPAY CARD

[← BACK](#)

ADD SELECTED

No more than 500

BINs

+

3) The Destination Card Bank routing type allows to sort transactions by the receiver's Issuer Bank name. Select the needed Issuer Bank names of the receiver and build a further route based on them. There is an option to search Banks by their names. System can search for up to 500 entered Bank names listed one after another and separated by commas. They can be chosen by pressing the "By name -" button.

#### DESTINATION\_CARD\_BANK # 2543

OTHERS

GRAND BANK & TRUST OF F... x

Select banks to work with  
Banks available for selection



Show all    Only selected (0)    Hide filter ^

By name -    + Add filter    ↻

<input type="checkbox"/>	ID	NAME	COUNTRY CODE	NUMERIC	STATUS
<input type="checkbox"/>	1	CENTRAL SUPPLIES - TDFS	CAN	124	●
<input type="checkbox"/>	2	UNKNOWN	USA	840	●
<input type="checkbox"/>	3	I&M BANK	KEN	404	●
<input type="checkbox"/>	4	LUXURY JEWELLERY CLASS (LJC) - TDFS	CAN	124	●
<input type="checkbox"/>	5	CASTLE BUILDING CENTRES - TDFS	CAN	124	●
<input type="checkbox"/>	6	BOSE - TDFS	CAN	124	●
<input type="checkbox"/>	7	CHARM DIAMOND CENTRES - TDFS	CAN	124	●
<input type="checkbox"/>	8	CRESCENT GOLD & DIAMONDS - TDFS	CAN	124	●
<input type="checkbox"/>	9	CANTREX - TDFS	CAN	124	●
<input type="checkbox"/>	10	CORBEIL - TDFS	CAN	124	●
<input type="checkbox"/>	11	BEN MOSS JEWELLERS - TDFS	CAN	124	●
<input type="checkbox"/>	12	OIROCARD	BRA	076	●
<input type="checkbox"/>	13	JCB	JPN	392	●
<input type="checkbox"/>	14	DINERS CLUB INTERNATIONAL	GBR	826	●
<input type="checkbox"/>	15	DINERS CLUB INTERNATIONAL	HUN	348	●
<input type="checkbox"/>	16	DINERS CLUB INTERNATIONAL	USA	840	●

← BACK

ADD SELECTED

No more than 500

By name



CANCEL

APPLY

- 4) The Destination Card Country routing type allows to sort transactions by the receiver's card country. Select the required card countries of the receiver and build a further route based on them.

**DESTINATION\_CARD\_COUNTRY # 2545**

OTHERS

⋮

Andorra  
 United Arab Emirates  
 Afghanistan  
 Antigua and Barbuda  
 Anguilla  
 Albania

- 5) The Destination Card Credit Source routing type allows to sort transactions by the receiver's card type. Select the needed card types of the receiver and build a further route based on them.

**DESTINATION\_CARD\_CREDIT\_SOURC...**

Debit × Non-Mastercard ×  
 Prepaid Non-Reloadable ×  
 Credit × Deferred Debit ×  
 Prepaid × Prepaid Reloadable ×  
 Charge ×

OTHERS

**Customer**

- 1) The Customer Account Number Country routing type allows to sort transactions by connecting selected countries to one provider, and the remaining countries connecting to another. This routing type is used for payout transactions. Country and bank are determined by IBAN (International Bank Account Number), which has been generated in accordance with [ISO 13616](https://www.iso.org/standard/81090.html)<sup>16</sup>.

**ACCOUNT\_NUMBER\_COUNTRY # 66011**

Russian Federation x — 1 (TST) Gate#ST6KYJ72#1

Poland x Netherlands x — 1 (TST) Gate#ST6KYJ72#1

- 2) The Customer IP Country routing type allows to sort transactions by the IP address of the customer’s country. Select the countries, the IPs of which will be checked and build a further route based on them.

**CUSTOMER\_IP\_COUNTRY # 2549**

OTHERS

Andorra

United Arab Emirates

Afghanistan

Antigua and Barbuda

Anguilla

Albania

- 3) The Customer IP Range routing type allows to sort transactions which IP address values are within the specified range. Specify the appropriate IP range and build the further route from it. Both IPv4 and IPv6 are accepted.

<sup>16</sup> <https://www.iso.org/standard/81090.html>

**CUSTOMER\_IP\_RANGE # 2551**

OTHERS

127.0.0.1

127.0.0.1

- 4) Customer Billing Country routing type allows to sort transactions by the country from the customer's billing address. Select the needed countries and build a further route based on them.

**CUSTOMER\_BILLING\_COUNTRY # 2553**

OTHERS

⋮

⋮

Andorra

United Arab Emirates

Afghanistan

Antigua and Barbuda

Anguilla

Albania

- 5) Customer Loyalty routing type is divided into endpoint, project, merchant, manager. Each of these levels has a Returning customer approve sessions count field that can be set for Managers by users with Superior role, while for Projects, Endpoints and Merchants - by users with Manager role. This value sets the number of transactions after which the customer will be considered "RETURNING".

By default, the Customer is defined by card. Definition is possible by card number, email, card holder and email, card holder and purpose, card holder and phone. Transaction count begins when definition is modified (each definition type stores its respective transaction count). The client definition is set in respective Client definition field on the Project level or Endpoint level (Endpoint setting overrides Project setting).

Summary:

- RETURNING\_FOR\_MANAGER - approve count on Manager level, Customer definition on Project/Endpoint level.

- RETURNING\_FOR\_MERCHANT - approve count on Merchant level, Customer definition on Project/Endpoint level.
- RETURNING\_FOR\_ENDPOINT - approve count on Endpoint level, Customer definition on Project/Endpoint level.
- RETURNING\_FOR\_PROJECT - approve count on Project level, Customer definition on Project/Endpoint level.

**Customer loyalty # 136629**

OTHERS

NEW\_FOR\_ENDPOINT

NEW\_FOR\_PROJECT

NEW\_FOR\_MERCHANT

NEW\_FOR\_MANAGER

RETURNING\_FOR\_ENDPOINT

RETURNING\_FOR\_PROJECT

RETURNING\_FOR\_MERCHANT

RETURNING\_FOR\_MANAGER

The routing logic is checked sequentially, so the transaction goes through the first route that satisfies the condition.

For example the following route will first check the merchant loyalty and then the manager.

**Customer loyalty # 10645**

RETURNING\_FOR\_MERCHANT

RETURNING\_FOR\_MANAGER

OTHERS

- 6) by Recurring and Non\_recurring routing types allows to sort transactions based on whether transaction type is recurrent or not.

RECURRING\_PAYMENT # 7130

RECURRING

NON\_RECURRING

OTHERS

- 7) by purpose routing type allows to sort transactions based on purpose. It is possible to enter more than one purpose value to each routing row. New values are added using the Add button which is available when editing or creating. Purpose limited to 128 symbols.

View:

Purpose # 10761

OTHERS

Test  
Test 1 

Test 2 

Edit:

**Purpose** ✕

Test 🗑️

Test 1 🗑️

Test 2 🗑️

Add

Cancel Save

- 8) by Phone IMEI (IMEI or International Mobile Equipment Identity) — this is the individual number of the mobile equipment. It is possible to enter more than one purpose value to each routing row. IMEI limited to 32 symbols.

View:

**Customer phone IMEI # 10762**

Test ✎  
Test 1

Test2 ✎

OTHERS

Edit:

## Customer phone IMEI



Test	
Test 1	
Test 2	
Add	
<span>Cancel</span> <span>Save</span>	

**Transaction**

- 1) Transaction Amount routing type allows to sort transactions by their amounts. The number in the square bracket is included in the range and the number in the round bracket is not included in the range. For example, to specify amount from 0 to 100 (including 100), use [0, 100.01). Transactions, which amounts match the specified range, will pass through this routing criterion.

TRANSACTION\_AMOUNT # 29178

OTHERS

[0 100.01)

- 2) Transaction Type routing type allows to sort transactions by their type. Select the needed transaction types and build a further route based on them.

**TRANSACTION\_TYPE # 2559**

OTHERS

account\_verification  
arbitration  
cancel  
capture  
chargeback  
chargeback\_reversal  
create\_card\_mapping  
delete\_card\_mapping  
dispute

3) Amount Multiplicity routing type allows to sort transactions by their amounts matching with specified multipliers. Add amount multiplicity and transaction will route by the highest amount to which it is a multiple. Example: If transaction amount is 1000 and "Amount multiplicity" is settled as 1000 and 500, transaction will route to 1000, and if transaction amount is 1500 it will route to 500, and if transaction amount is 2000 it will route to 1000.

**AMOUNT\_MULTIPLICITY # 79230**

1000

500

OTHERS

4) Transaction Time routing type allows to sort transactions by the time they are created in the system. Timezone GMT+3. This sort type can be used for

processor technical breaks or for any other reason when time is necessary for any route. To set the time, for example, from 22:00 till 06:00, set the time the following way: [22:00:00, 23:59:59], [00:00:00, 06:00:00].

**TRANSACTION\_TIME # 93672**

OTHERS

22:00:00      23:59:59

00:00:00      06:00:00

- 5) Day of week routing type allows to sort transactions by day of the week. Select the needed day of the week and time zone for further route based on them.

**Day of week # 99573**

OTHERS

SUNDAY / GMT\_PLUS\_3 ▶ ■

## Transfer

- 1) Transfer Direction routing type allows to sort transfer transactions by card types or Issuer banks of sender and receiver. Select the needed parameters and build a further route based on them.

## TRANSFER\_DIRECTION # 2561

OTHERS

other directions

any - VISA

any - MASTERCARD

VISA - any

VISA - VISA

VISA - MASTERCARD

MASTERCARD - any

MASTERCARD - VISA

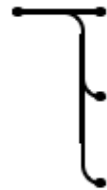
MASTERCARD - MASTERCARD

### IP Intelligence

#### Warning


If Fraud Service - "MaxMind IP check service" is selected on project level, then regardless of whether "fraud filters" or "routing&balancing" are set up - all requests will be send to Max Mind.

- 1) Anonymous vpn routing type allows to check when Payer IP address is considered as anonymous vpn by MaxMind service. YES - if condition is true, NO - if condition is false. Select the needed parameters and build a further route based on them.

**Anonymous vpn # 109474**


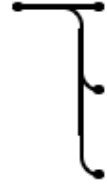
OTHERS	
YES	NO
YES	NO

- 2) Anonymous IP address routing type allows to check when Payer IP address is considered as anonymous by MaxMind service. YES - if condition is true, NO - if condition is false. Select the needed parameters and build a further route based on them.

**Anonymous IP address # 109475**


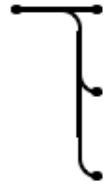
OTHERS	
YES	NO
YES	NO

- 3) Hosting provider routing type allows to check when Payer IP address belongs to a hosting or VPN provider considered by MaxMind service. YES - if condition is true, NO - if condition is false. Select the needed parameters and build a further route based on them.

**Hosting provider # 109476**


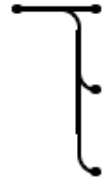
OTHERS	
YES	NO
YES	NO

- 4) Public proxy routing type allows to check when Payer IP address belongs to a public proxy considered by MaxMind service. YES - if condition is true, NO - if condition is false. Select the needed parameters and build a further route based on them.

**Public proxy # 109477**


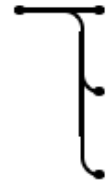
OTHERS	
YES	NO
YES	NO

- 5) Residential proxy routing type allows to check when Payer IP address belongs to a hosting or VPN provider considered by MaxMind service. YES - if condition is true, NO - if condition is false. Select the needed parameters and build a further route based on them.

**Residential proxy # 109478**


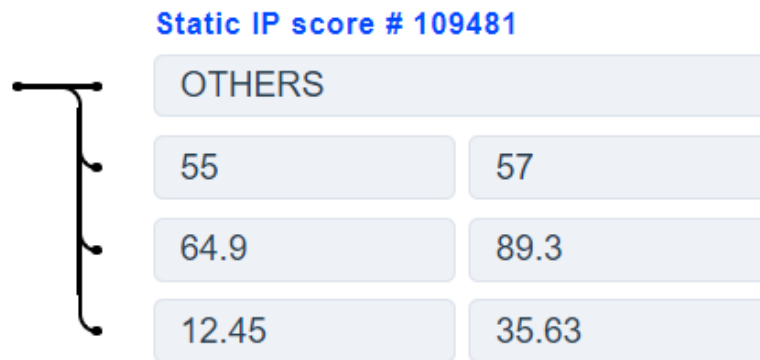
OTHERS	
YES	NO
YES	NO

- 6) Tor exit node routing type allows to check when Payer IP address a Tor exit node considered by MaxMind service. YES - if condition is true, NO - if condition is false. Select the needed parameters and build a further route based on them.

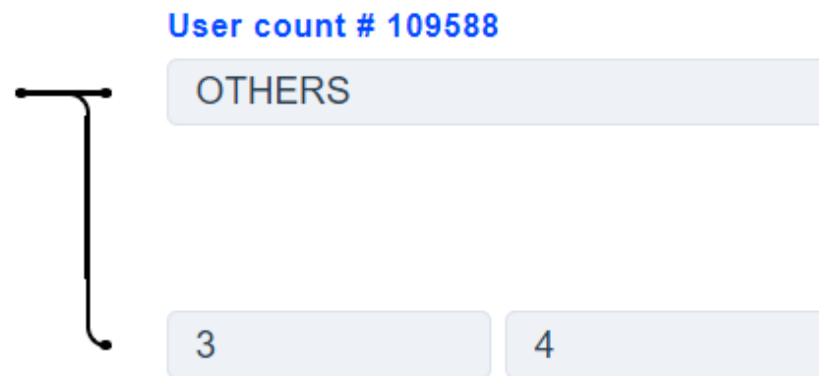
**Tor exit node # 109480**


OTHERS	
YES	NO
YES	NO

- 7) Static IP score routing type allows to check when Payer IP address Static IP score which is considered by MaxMind service is lower or equal to the settled threshold value. Higher values meaning a greater static association. For example, many IP addresses with a user type of cellular have a score under one. Broadband IPs that don't change very often typically have a score above thirty. This indicator can be useful for deciding whether an IP address represents the same user over time. The value ranges from 0 to 99.99. Select the needed parameters and build a further route based on them.



- 8) User count routing type allows to check when Payer IP address user count considered by MaxMind service is higher or equal to the settled threshold value. The estimated number of users sharing the IP/network during the past 24 hours. For IPv4, the count is for the individual IP. For IPv6, the count is for the /64 network. Select the needed parameters and build a further route based on them.



### Balancing Types

Balancing type is a feature which allows to distribute transactions between payment gates in accordance with the configured parameters.

**Note**

The gate can also be specified directly on the endpoint. However, it will still be subject to the routing strategy, but will be selected for all transactions coming from this endpoint on this route.

The following balancing types are presented in the system:

**Balance By Coefficient**

- 1) Balance by coefficient Based on Tx Amount allows to sort transactions by the gates depending on the amount and the specified probability percentage.

**BALANCE\_BY\_COEFFICIENT\_BASED...**

20	Demo_Gate_1	<input type="text"/>	<input type="text"/>	<input type="text"/>
		<input type="text"/>	<input type="text"/>	<input type="text"/>
30	Demo_Gate_2	<input type="text"/>	<input type="text"/>	<input type="text"/>
		<input type="text"/>	<input type="text"/>	<input type="text"/>
50	Demo_Gate_3	<input type="text"/>	<input type="text"/>	<input type="text"/>
		<input type="text"/>	<input type="text"/>	<input type="text"/>

For example, 3 gates have 20%, 30% and 50% coefficients set for them. In this case, 50% of the first several processed transactions will be forwarded to the gate with the probability of 50%, then the traffic will try to reach the distribution of the amount between the gates in accordance with the specified percentages. If the processed amount on a gate exceeds the amounts on the other gates, the transactions will not be forwarded to the gate with the exceeding amount until the amounts on all the gates become equal to the percentages set for the gates.

- 2) Balance by coefficient Based on Tx Count allows to sort transactions by gates depending on their quantity and the specified probability percentage.

**BALANCE\_BY\_COEFFICIENT\_BASED...**

20	Demo_Gate_1	<input type="text"/>	<input type="text"/>	<input type="text"/>
		<input type="text"/>	<input type="text"/>	<input type="text"/>
30	Demo_Gate_2	<input type="text"/>	<input type="text"/>	<input type="text"/>
		<input type="text"/>	<input type="text"/>	<input type="text"/>
50	Demo_Gate_3	<input type="text"/>	<input type="text"/>	<input type="text"/>
		<input type="text"/>	<input type="text"/>	<input type="text"/>

For example, 3 gates have 20%, 30% and 50% coefficients set for them. In this case, 50% of the processed transactions will be forwarded to the gate with the probability of 50%. The transaction amounts are not considered, only their quantity is.

**Balance Equally**

- 1) Balance equally Based on Tx Amount allows to sort transactions by gates depending on the amount with equal probability percentage.

**BALANCE\_BY\_EQUIVALENT\_COEFFI...**

1	Demo_Gate_1	<input type="text"/>	<input type="text"/>	<input type="text"/>
		<input type="text"/>	<input type="text"/>	<input type="text"/>
2	Demo_Gate_2	<input type="text"/>	<input type="text"/>	<input type="text"/>
		<input type="text"/>	<input type="text"/>	<input type="text"/>
3	Demo_Gate_3	<input type="text"/>	<input type="text"/>	<input type="text"/>
		<input type="text"/>	<input type="text"/>	<input type="text"/>
4	Demo_Gate_4	<input type="text"/>	<input type="text"/>	<input type="text"/>
		<input type="text"/>	<input type="text"/>	<input type="text"/>

If there are e.g. 4 gates, “Balance equally on Tx Amount” will set an equal probability percentage of 25% for each gate. The first several transactions can be forwarded to any of them as the percentages are equal, then the traffic will try to reach the equal distribution of the amount between the gates. If the processed amount on a gate exceeds the amounts on the other gates, the transactions will not be forwarded

to the gate with the exceeding amount until the amounts on all the gates become equal.

- 2) Balance equally Based on Tx Count allows to sort transactions by gates depending on the quantity with equal probability percentage.

#### BALANCE\_BY\_EQUIVALENT\_COEFFI...

1	Demo_Gate_1
	<div style="border: 1px solid #ccc; padding: 2px 10px; background-color: #f0f0f0;">x</div> <div style="border: 1px solid #ccc; padding: 2px 10px; background-color: #f0f0f0;">x</div> <div style="border: 1px solid #ccc; padding: 2px 10px; background-color: #f0f0f0;">x</div>
2	Demo_Gate_2
	<div style="border: 1px solid #ccc; padding: 2px 10px; background-color: #f0f0f0;">x</div> <div style="border: 1px solid #ccc; padding: 2px 10px; background-color: #f0f0f0;">x</div> <div style="border: 1px solid #ccc; padding: 2px 10px; background-color: #f0f0f0;">x</div>
3	Demo_Gate_3
	<div style="border: 1px solid #ccc; padding: 2px 10px; background-color: #f0f0f0;">x</div> <div style="border: 1px solid #ccc; padding: 2px 10px; background-color: #f0f0f0;">x</div> <div style="border: 1px solid #ccc; padding: 2px 10px; background-color: #f0f0f0;">x</div>
4	Demo_Gate_4
	<div style="border: 1px solid #ccc; padding: 2px 10px; background-color: #f0f0f0;">x</div> <div style="border: 1px solid #ccc; padding: 2px 10px; background-color: #f0f0f0;">x</div> <div style="border: 1px solid #ccc; padding: 2px 10px; background-color: #f0f0f0;">x</div>

If there are e.g. 4 gates, “Balance equally on Tx Count” will set an equal probability percentage of 25% for each gate. The first several transactions can be forwarded to any of them as the percentages are equal, then the traffic will try to reach the equal distribution between the gates based on the quantity of transactions.

### Cascading Chain

- 1) Chain by Coefficient Based on Tx Count allows to sort transactions by gates using the specified probability percentage and the chain principle. If the incoming transaction is going to be filtered or exceed the limits on some gates, the balancing algorithm excludes these gates and then it forms the chain with the remaining ones according to their coefficients.

**CHAIN\_BY\_COEFFICIENT\_BASED\_ON...**

20	Demo_Gate_1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
30	Demo_Gate_2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
50	Demo_Gate_3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

For example, 3 gates have 20%, 30% and 50% coefficients set for them. In this case, the gate with 50% coefficient has the 50% probability of becoming the first gate in the formed chain. If for some reason the first gate in chain was unable to process the transaction, it goes to the next gate in chain. If the second gate was not able to process the transaction as well, it moves on until one of the subsequent gates in chain processes it. The traffic will try to reach the distribution between the gates according to their coefficients based on the quantity of transactions.

- Chain by Equivalently Based on Tx Count allows to sort transactions by gates using the chain principle and an equal probability percentage. If the incoming transaction is going to be filtered or exceed the limits on some gates, the balancing algorithm excludes these gates and then it forms the chain with the remaining ones based on equal probability percentage.

**CHAIN\_BY\_EQUIVALENT\_COEFFICIE...**

1	Demo_Gate_1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	Demo_Gate_2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	Demo_Gate_3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	Demo_Gate_4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

If there are e.g. 4 gates, "Chain by equivalently on Tx Count" will set an equal

probability percentage of 25% for each gate. In this case, each gate has the 25% probability of becoming the first gate in the formed chain. If for some reason the first gate in chain was unable to process the transaction, it goes to the next gate in chain. If the second gate was not able to process the transaction as well, it moves on until one of the subsequent gates in chain processes it. The traffic will try to reach the equal distribution between the gates based on the quantity of transactions.

- 3) Chain by Sequence allows to sort transactions using the cascading chain principle.

#### CHAIN\_BY\_SEQUENCE # 1667



Transactions will be processed by gates only in a priority order. If for some reason the first gate in the chain was not able to process the transaction, it moves further along the chain until one of the subsequent gates in chain processes it. The gate priority can be changed in “Chain by Sequence” using drag’n’drop.

- 4) Chain by Last Customer Tx Status on Acquirer allows to sort transactions by resulting transaction status and the chain principle.

**CHAIN\_BY\_LAST\_CUSTOMER\_TX\_ST...**

1	Gate#0A561OQA#1			
	x	x	x	
2	Gate#0HESP4TP#0			
	x	x	x	
3	Gate#13JSBAWV#0			
	x	x	x	
4	Gate#4TMA45LU#2			
	x	x	x	

All client transactions (defined by email) are checked within the exact processor (not among all of them) and the next transaction is routed to the gate with last successful transaction of this client. If attempt on this gate was declined, transaction moves further along the chain until one of the subsequent gates in chain processes it.

**Others**

- 1) First in Sequence allows to sort transactions by choosing the first appropriate gate for them.

**FIRST\_IN\_SEQUENCE # 1671**

If the incoming transaction is going to be filtered or exceed the limits on certain gates, the “First in Sequence” algorithm excludes these gates and then it sends the transaction to the highest gate of the remaining ones. The gate priority can be changed by dragging it up and down.

- 2) First in Sequence by Last Customer Tx Status on Acquirer allows to sort transactions by resulting transaction status.

**FIRST\_IN\_SEQUENCE\_BY\_LAST\_CUS...**

All client(by e-mail) transactions for all projects are checked and the next transaction is routed to the gate with processor of the last successful transaction project-wide. If a transaction is in declined status, gate is moved to the bottom of the sequence and receives lowest priority. Also, all gates belonging to the same processor as the gate on which the rejection status occurred receive low priority. Gate with processor with last approved transaction will be first in sequence, a gate with processor with

earlier approves or no approves will be last.

- 3) First in Sequence by Last Customer Tx Status on Gate allows to sort transactions by resulting transaction status.

**FIRST\_IN\_SEQUENCE\_BY\_LAST\_CUS...**

1	Gate#02ORKS9R#2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	Gate#02SJAW4P#0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	Gate#02ZCZZX#1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	Gate#02ZVTXNF#0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

All client(by e-mail) transactions are checked and the next transaction is routed to the gate of the last successful transaction project-wide. If a transaction is in declined status, gate is moved to the bottom of the sequence and receives lowest priority. Unlike First in Sequence by Last Customer Tx Status on Acquirer balancing type, the gates belonging to the same processor as the gate on which the declined status occurred do not lose priority and do not fall at the end of the sequence. Gate with last approved transaction will be first in sequence, a gate with earlier approves or no approves will be last.

## Additional Configurations

### Gate Skips

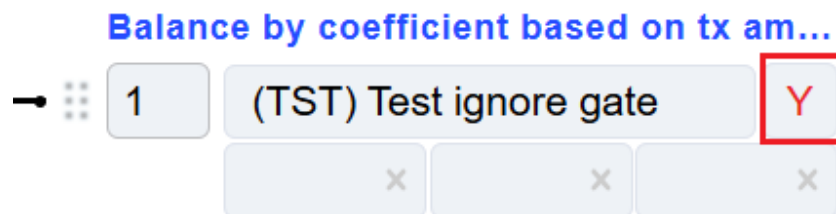
The gates in the balancing block can be skipped for processing of the transaction in the following cases:

- 1.) If *Acquirer restrictions* on gate level is triggered;
- 2.) For Cascading chain options - if the decline message specified in *Chain Strategy Details* or *Chain Strategy Skips* is received, the chain will stop;
- 3.) If the gate is disabled on the gate level;
- 4.) If the gate is disabled in balancing block;
- 5.) If gate is set to be ignored, because it's intended only for direct processing from specific Endpoints (see *Ignore Gates For Direct Processing* below).

## Ignore Gates For Direct Processing

N  Y Ignoring gates - ignores selected gate for whole node.

If it is needed to use gate, but only for the specific Endpoint without any changes in the routing, use Ignoring gates, so that way this gate will be ignored for the rest of the traffic and will only be used with the specific Endpoint.



## Rates

Rates is a system of payment fees for all stakeholders' services.

The system supports such stakeholders as:

Merchant, Reseller, Manager, Dealer, Bank.

In the current model, the fees are incrementally increasing, from the Bank to the Merchant. The following rate plan will count the value of the previous one. Thus, the higher the participant's level is, the greater his total fee is in the system. The Bank and Dealer rate plans can be set on the gate level. Manager, Reseller, and Merchant rate plans can be set on the project level, with the option to override them on the endpoint level. The presence of some participants in the payment rates model is optional.

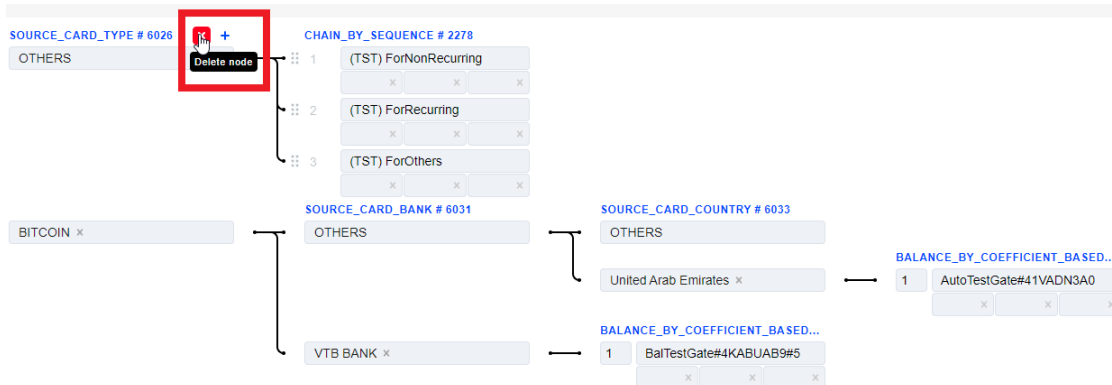
In Routing & Balancing the Rates can be redefined directly on the gates configuration in balancing blocks. These Rates settings override the ones on project or endpoint level.



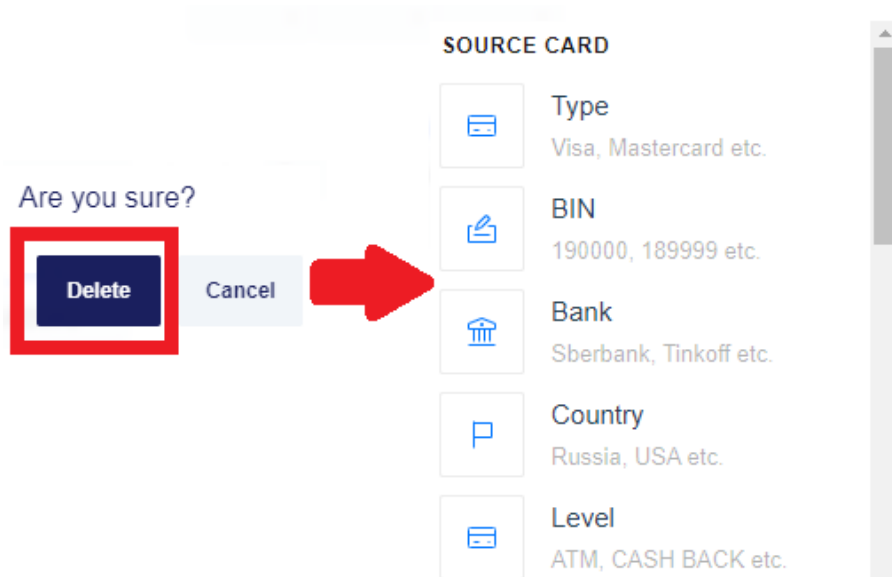
There are 3 active fields below at the gate's name, which are responsible for redefining rate plans for Manager, Reseller and Merchant, from left to right respectively. All rate plans can be selected from the dropdown list of already created ones.

### Copy, Paste, Cut, Delete

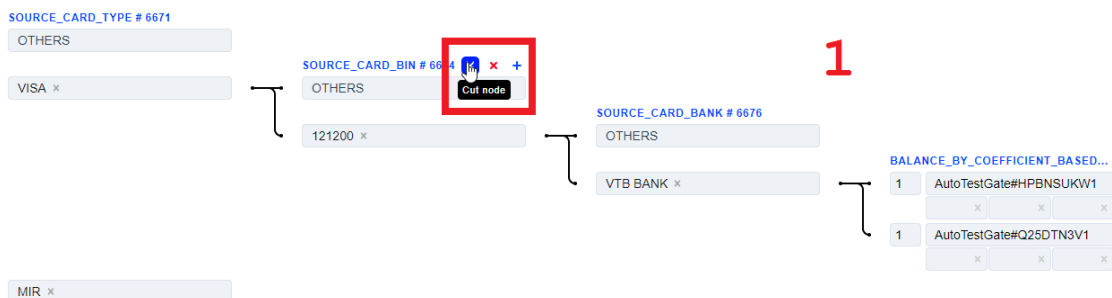
Routing & balancing nodes can be deleted, along with all children:



Each deletion requires confirmation:



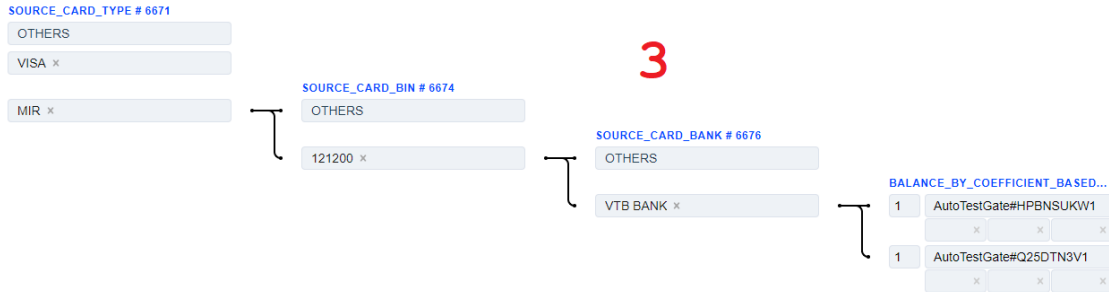
Fragments of balancing tree can also be cut and pasted:



Choose where to paste the cut fragment:



Result:

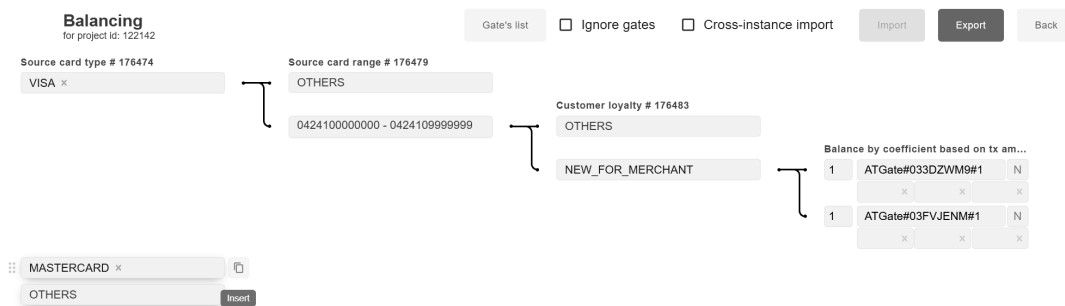


Parts of a balancing tree can be copied in a similar way as well:

Tap on Copy node.



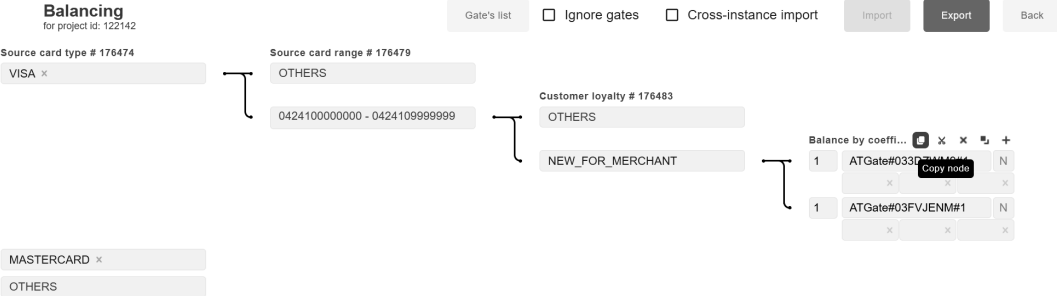
Choose where to paste the copied fragment:



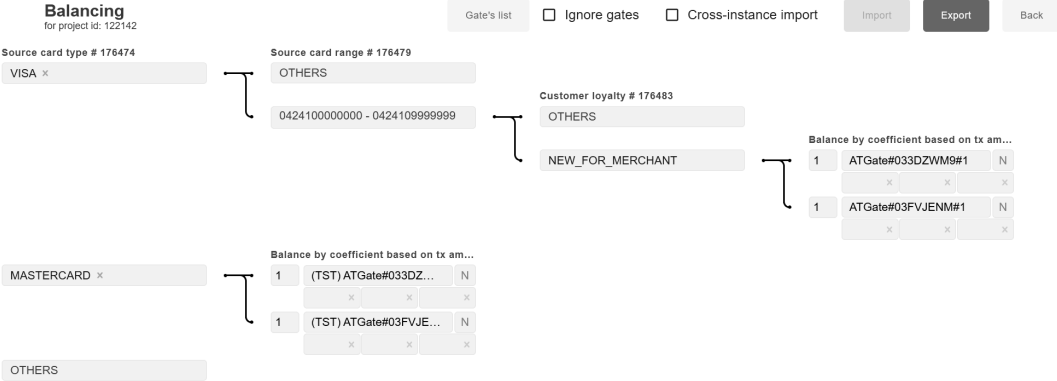
Result:



The same process can be repeated for the last part of the balancing tree:

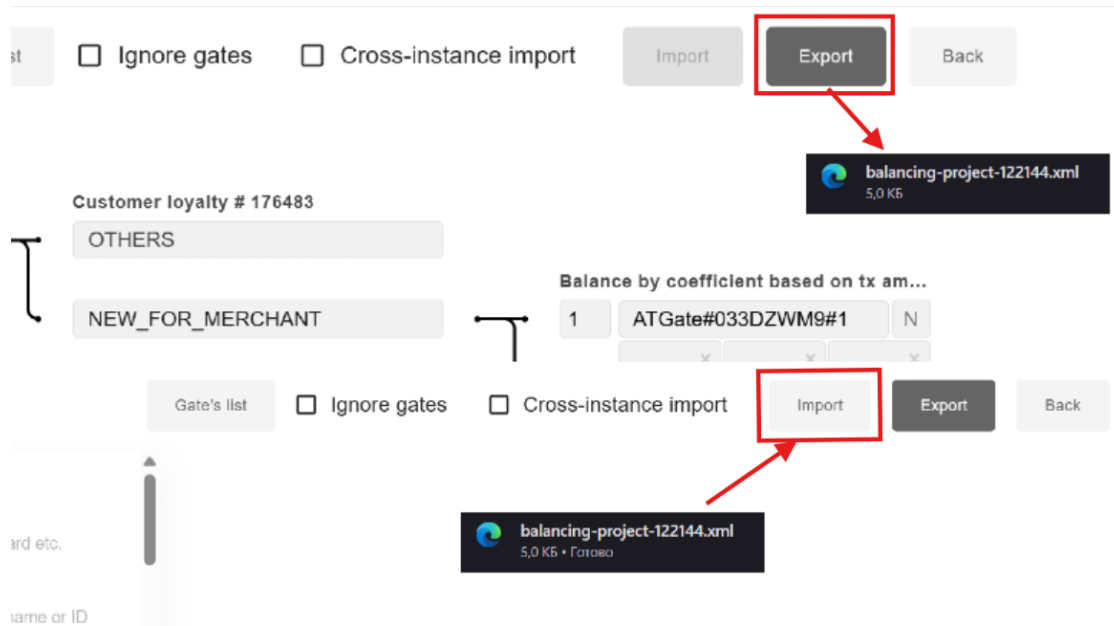


Result:



### Import And Export

You can import and export your balancing tree:



Balancing tree file is generated in xml and has the following structure:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<strategy>
  <projectId>4947</projectId>
  <projectDisplayName>Recur AUD</projectDisplayName>
  <routingNodes>
    <routingNode>
      <id>8572</id>
      <routingId>1</routingId>
      <enabled>true</enabled>
      <routes>
        <route>
          <id>23277</id>
          <enabled>true</enabled>
          <nextRoutingNodeId>8573</nextRoutingNodeId>
          <others>true</others>
          <criteria>
            <criterion>
              <value>OTHERS</value>
            </criterion>
          </criteria>
          <order>0</order>
        </route>
      </routes>
      <root>true</root>
    </routingNode>
    <routingNode>
      <id>8573</id>
      <routingId>2</routingId>
      <enabled>true</enabled>
      <routes>
        <route>
```

(continues on next page)

(continued from previous page)

```

        <id>23279</id>
        <enabled>>true</enabled>
        <nextRoutingNodeId>8574</nextRoutingNodeId>
        <others>>false</others>
        <criteria>
            <criterion>
                <entityId>8104</entityId>
                <entityName>213100</entityName>
            </criterion>
        </criteria>
        <order>0</order>
    </route>
    <route>
        <id>23278</id>
        <enabled>>true</enabled>
        <others>>true</others>
        <criteria>
            <criterion>
                <value>OTHERS</value>
            </criterion>
        </criteria>
        <order>1</order>
    </route>
</routes>
<root>>false</root>
</routingNode>
<routingNode>
    <id>8574</id>
    <routingId>3</routingId>
    <enabled>>true</enabled>
    <routes>
        <route>
            <id>23281</id>
            <enabled>>true</enabled>
            <nextRoutingNodeId>8575</nextRoutingNodeId>
            <others>>false</others>
            <criteria>
                <criterion>
                    <entityId>1825</entityId>
                    <entityName>DEMO BANK</entityName>
                </criterion>
            </criteria>
            <order>0</order>
        </route>
        <route>
            <id>23280</id>
            <enabled>>true</enabled>
            <others>>true</others>
            <criteria>
                <criterion>
                    <value>OTHERS</value>
                </criterion>
            </criteria>
        </route>
    </routes>
</routingNode>

```

(continues on next page)

(continued from previous page)

```

        </criteria>
        <order>1</order>
    </route>
</routes>
<root>>false</root>
</routingNode>
<routingNode>
    <id>8575</id>
    <routingId>4</routingId>
    <enabled>>true</enabled>
    <routes>
        <route>
            <id>23282</id>
            <enabled>>true</enabled>
            <balancingNodeId>8750</balancingNodeId>
            <others>>true</others>
            <criteria>
                <criteria>
                    <value>OTHERS</value>
                </criteria>
            </criteria>
            <order>0</order>
        </route>
    </routes>
    <root>>false</root>
</routingNode>
</routingNodes>
<balancingNodes>
    <balancingNode>
        <id>8750</id>
        <enabled>>true</enabled>
        <balancingId>1</balancingId>
        <rows>
            <row>
                <id>0</id>
                <enabled>>false</enabled>
            </row>
        </rows>
    </balancingNode>
</balancingNodes>
</strategy>

```

## Transaction Filters

- [General information](#)
- [Fraud protection filters](#)
- [Technical filters](#)
  - [Detecting and preventing duplicate requests](#)

- *Detecting and preventing duplicate invoices*
- *Detecting and preventing accidental duplicate credit card number usage*
- *Declined transactions frequency by Credit Card number and Invoice*
- *Preventing of repeated withdrawal operations for the same customer*
- *Preventing new transactions with source card which has previous attempt in unknown status*
- *Referral filters*
  - *Blacklist check (BL)*
  - *Predefined loyalty lists check*
  - *Ban untrusted networks*
  - *Credit Card Whitelist check (WL)*
  - *Customer fingerprint*
  - *Check reader entry mode*
  - *IP address Country check*
  - *Issuer Country check*
  - *Billing Country check*
  - *IP address Country blacklist*
  - *Issuer Country blacklist*
  - *Billing Country blacklist*
  - *Issuer Country blacklist by Payment method*
  - *Transaction amount check*
  - *Source Credit Card type check*
  - *Destination Credit Card type check*
- *Consistency filters*
  - *Check customer data*
  - *Customer IP address Country differs from Issuing Country*
  - *Customer name differs from Cardholder name*
  - *Customer IP address differs from IP address used for 3-D Secure validation*
  - *Customer birthday check*
  - *Source Credit Card number expiration date check*
  - *The 6+4 customer cards differs from the 6+4 passed in purpose*
- *Custom business validations*
  - *Transaction amount changing for Purpose*
  - *Authorization reattempts requirements EMEA*
  - *Visa Preauthorized Transaction Decline Response requirements N.A.*

- *MCC 6211 restrictions*
- *MCC 7995 restrictions*
- *CDB processing restrictions*
- *Velocity filters*
  - *Source Credit Card Number decline frequency for last 24 hours (daily decline limit)*
  - *Source Credit Card Number increasing sequence of approved transaction amounts for last 24 hours (daily rising limit)*
  - *Source Credit Card Number usage frequency for last 24 hours (daily limit)*
  - *Source Credit Card Number usage frequency for last 7 days (weekly limit)*
  - *Source Credit Card Number usage frequency for last month (monthly limit)*
  - *Destination Credit Card Number usage frequency for last 24 hours (daily limit)*
  - *Destination Credit Card Number usage frequency for last 7 days (weekly limit)*
  - *Destination Credit Card Number usage frequency for last month (monthly limit)*
  - *Total Credit Card Number usage frequency for last 24 hours (daily limit)*
  - *Total Credit Card Number usage frequency for last 7 days (weekly limit)*
  - *Total Credit Card Number usage frequency for last month (monthly limit)*
  - *Purpose usage frequency for last 24 hours (daily limit)*
  - *Purpose usage frequency for last 7 days (weekly limit)*
  - *Purpose usage frequency for last month (monthly limit)*
  - *Email usage frequency for last 24 hours (daily limit)*
  - *Email usage frequency for last 7 days (weekly limit)*
  - *Email usage frequency for last month (monthly limit)*
  - *IP address usage frequency for last 24 hours (daily limit)*
  - *IP address usage frequency for last 7 days (weekly limit)*
  - *IP address usage frequency for last month (monthly limit)*
  - *Source Credit Card Number usage frequency for Purpose*
  - *Source Credit Card Number usage frequency for Email address*
  - *Source Credit Card Number usage frequency for First and Last name*
  - *Source Credit Card Number usage frequency for Destination Credit Card number*
  - *Source Credit Card Number usage frequency for Email or IP address*
  - *Source Credit Card Number usage frequency*
  - *Customer IP address usage frequency*
  - *Credit Card number already used from another IP address*
  - *Credit Card number already used from another Country*

- *Credit Card number already used with another Email*
- *Credit Card number already used with another Purpose*
- *Credit Card number already used with another Cardholder name*
- *Customer IP address already used by another Cardholder*
- *Customer Email already used by another Cardholder*
- *Source Credit Card Number approved transaction interval*
- *Source Credit Card Number declined transaction interval*
- *Source Credit Card Number Issuer Country change frequency for current Purpose*
- *Reversal frequency*
- *Fingerprint usage frequency for last 24 hours (daily limit)*
- *Fingerprint usage frequency for last 7 days (weekly limit)*
- *Fingerprint usage frequency for last month (monthly limit)*
- *Source Credit Card Number usage frequency for Fingerprint*
- *Source Credit Card number Issuer Country change frequency for current Device Fingerprint*
- *Destination Credit Card Number usage frequency for Device fingerprint*
- *Destination Credit Card number Issuer Country change frequency for current Device fingerprint*
- *Email usage frequency for Device fingerprint*
- *Purpose usage frequency for Device fingerprint*
- *Account Number usage frequency for last 24 hours (daily limit)*
- *Account Number usage frequency for last 7 days (weekly limit)*
- *Account Number usage frequency for last month (monthly limit)*
- *Preventing transaction with the same amount*
- *Issuer country usage frequency*
- *Purpose usage frequency for last year (annual limit)*
- *BIN range usage frequency*
- *Abnormal transaction time*
- *Source Credit Card Number decline frequency for last week (weekly decline limit)*
- *Source Credit Card Number usage frequency per Email address for last 24 hours (daily limit)*
- *Source Credit Card Number usage frequency per Email address for last 7 days (weekly limit)*
- *Source Credit Card Number usage frequency per Email address for last month (monthly limit)*
- *Source Credit Card Number usage frequency for last N days*

- *Destination Credit Card Number usage frequency for last N days*
- *Total Credit Card Number usage frequency for last N days*
- *Purpose usage frequency for last N days*
- *Email usage frequency for last N days*
- *IP address usage frequency for last N days*
- *Fingerprint usage frequency for last N days*
- *Account Number usage frequency for last N days*
- *Source Credit Card Number decline frequency for last month (monthly decline limit)*
- *Destination Credit Card Number decline frequency for last 24 hours (daily decline limit)*
- *Destination Credit Card Number decline frequency for last week (weekly decline limit)*
- *Destination Credit Card Number decline frequency for last month (monthly decline limit)*
- *Total Credit Card Number decline frequency for last 24 hours (daily decline limit)*
- *Total Credit Card Number decline frequency for last week (weekly decline limit)*
- *Total Credit Card Number decline frequency for last month (monthly decline limit)*
- *Customer IP address anonymous VPN*
- *Customer IP address anonymous*
- *Customer IP Hosting Provider*
- *Customer IP Public Proxy*
- *Customer IP Residential Proxy*
- *Customer IP Tor Exit Node*
- *Customer static IP score*
- *Customer IP user count*
- *Customer IP user type*
- *Credit Card Number usage frequency for last N hours*
- *Preventing transaction with the same amount 24 hours*

### General information

Transaction filters in System are intended for rejection of certain transactions on various reasons. For example, there are filters to check fraud transactions, or to check if the issuer-bank or card number is included in the White List, etc.

The Transaction filters are managed on a Project-level of the System. To set filters for the Project navigate to Fraud protection filters in the Project menu.

Project **122142** **ATProject#49WIKZ** To Projects list Export Import

**Technical filters** all  enabled 0 from 6

Status	Filter name	Score	Configure
<input type="checkbox"/>	Detecting and preventing duplicate requests	0 <input type="checkbox"/>	
<input type="checkbox"/>	Detecting and preventing duplicate invoices	0 <input type="checkbox"/>	
<input type="checkbox"/>	Detecting and preventing accidental duplicate credit card number usage	0 <input type="checkbox"/>	
<input type="checkbox"/>	Declined transactions frequency by Credit Card number and Invoice	0 <input type="checkbox"/>	
<input type="checkbox"/>	Preventing of repeated withdrawal operations for the same customer	0 <input type="checkbox"/>	
<input type="checkbox"/>	Preventing new transactions with source card which has previous attempt in unknown status	0 <input type="checkbox"/>	

**Referral filters** all  enabled 1 from 16

Status	Filter name	Score	Configure
<input type="checkbox"/>	Blacklist check (BL)	0 <input type="checkbox"/>	
<input type="checkbox"/>	Predefined loyalty lists check	0 <input type="checkbox"/>	
<input type="checkbox"/>	Ban untrusted networks	0 <input type="checkbox"/>	
<input checked="" type="checkbox"/>	Credit Card Whitelist check (WL)	100 <input checked="" type="checkbox"/>	
<input type="checkbox"/>	Customer fingerprint	0 <input type="checkbox"/>	

Common

Strategy

Routing & Balancing

**Fraud protection filters**

Message templates

The icon to the left from the filter name displays it's status. To turn a filter ON/OFF click on this icon.

Filter's details are available by clicking on the Configure button.

The number (or multiple numbers) in "**Error codes**" is called decline-code, or the code of transaction's rejection reason. This code will be displayed on the Orders screen if the transaction will get the Filtered status.

Some filters have Scoring. Scoring allows more flexible approach in filtering system and fraud control. Each filter's score can be set from 0 to 100. Transaction goes through different filters and each triggered filter adds it's own score to transaction. If transaction reaches 100 score - it gets Filtered; if not - it passes through. Turned OFF filters have 0 score.

Filters are also available on Endpoint-level of the System. Filter settings on Endpoint-level override Project-level settings.

Some Filter parameters can be added only from the Order information screen.

## Fraud protection filters

Rule name	Rule description
Technical filters	Technical filters compare two or more merchant requests to detect and prevent duplicate invoice payments. All filters in this category could be applied to requests in a short period of time since the moment of the transaction received by our system.
Referral filters	Referral checks allow to establish block and trust lists of both good and bad transaction attributes, affecting the risk score based on a known trend on many different customer attributes.
Velocity filters	Velocity checks allow merchants to set velocity thresholds on various customer attributes, controlling how often a customer can attempt transactions. These checks are intended to identify high-speed fraud attacks. Velocity Rules are calculated at the merchant account level. If a merchant has several merchant accounts under their company account, velocity counts do not aggregate across the entire company if not specified additionally. For example: A single credit card is used for 2 transactions in merchant account A and 3 transactions in Merchant Account B. The Velocity Rule counts 2 in Account A and 3 in Account B. An abandonment of the shopper after redirecting to a payment method or 3-D Secure is counted as an attempt and adds to the count for velocity rules as declined transaction. But not all of these abandoned attempts can be found in the payment list, it depends on the exact integration with PSP.
Consistency filters	Consistency checks compare two or more transaction attributes with each other.
Custom business validations	Additional validations and risk profiles defined by the manager.

### Technical filters

#### Detecting and preventing duplicate requests

Merchant request with the same request parameters will be filtered out

Score: No

Enabled by default: N

#### Parameters

Name	Description	Value
Checking interval in seconds	max interval in seconds to check duplicate request	Type: int Default: 15

continues on next page

Table 6 - continued from previous page

Name	Description	Value
Skip declined transactions	Y - to skip sessions in Filtered or Declined status, N - otherwise	Type: Enum Default: No

**Error codes**

#	Code	Name
10001	1007	Duplicate request

**Detecting and preventing duplicate invoices**

Merchant request with the same client order ID will be filtered out

Score: No

Enabled by default: N

**Parameters**

Name	Description	Value
Checking interval in seconds	max interval in seconds to check duplicate invoices, set to 0 for infinity	Type: int Default: 30
Skip error transactions	Y - to skip sessions in Error, Failed, Limited or Rejected status, N - otherwise	Type: Enum Default: Yes
Skip unapproved transactions	Y - to skip to skip sessions in Filtered, Declined or Cancelled status, N - otherwise	Type: Enum Default: Yes

**Error codes**

#	Code	Name
10048	1058	Duplicate invoice

### Detecting and preventing accidental duplicate credit card number usage

Customer request for the current merchant with the same credit card number will be filtered out

Score: No

Enabled by default: N

#### Parameters

Name	Description	Value
Checking interval in seconds	max interval in seconds to check duplicate credit card number usage, values more then 60 seconds are ignored	Type: int Default: 30
Skip declined transactions	Y - to skip sessions in Filtered or Declined status, N - otherwise	Type: Enum Default: Yes

#### Error codes

#	Code	Name
10087	1097	Duplicate credit card

### Declined transactions frequency by Credit Card number and Invoice

This check fires when the number of declined transactions associated with exact Credit Card number and Invoice number exceeds the configured thresholds. The time threshold is a moving window calculated backwards from the moment of the transaction, all transactions dates are truncated to minutes during window calculation. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 declines in 60 minutes, it fires on the 11th decline in 60 minutes. Counts transactions for Account verification, Sale, Preauth or Transfer transactions in the Filtered or Declined status. The limit is calculated for the current End point if parameter "for all merchant projects" set to N, or for all Merchant Projects if parameter set to Y.

Score: No

Enabled by default: N

#### Parameters

Name	Description	Value
checking interval in minutes	time frame to calculate declines count in minutes, values more then 24 hours are ignored	Type: int Default: 30
For all Merchant projects	Y - to check transactions for all projects of the current Merchant, otherwise check transactions for current end point only	Type: Enum Default: No
Maximum declines count	maximum number of declined or filtered transactions allowed	Type: int Default: 2

**Error codes**

#	Code	Name
10009	1013	Too many declines for the same credit card number and invoice

**Preventing of repeated withdrawal operations for the same customer**

This check fires when there is more than one transaction for one customer in a non-final status at any time. The risk fires on the second transaction if the first transaction is still in a non-final status. The filter works only for projects added to the CMS. Counts reverse transactions, payouts or transfers.

Score: Yes

Enabled by default: N

**Parameters**

Name	Description	Value
For all merchant projects	Yes: for all merchant projects No: for current project only	Type: Enum Default: Yes
Skip reversals	Yes: reversal transactions are not taken into account No: reversal transactions are taken into account	Type: Enum Default: Yes

**Error codes**

#	Code	Name
10205	1215	Repeated withdrawal request

### Preventing new transactions with source card which has previous attempt in unknown status

This check fires when customer tries to perform new card transaction while last transaction with the same source card still has non-final unknown status for past N minutes (max 1 hour). Counts Sale, Preauth or Transfer transactions in unknown status.

Score: No

Enabled by default: N

#### Parameters

Name	Description	Value
Checking interval in minutes	Max interval in minutes to check existing unknown operation	Type: Int Default: 60
For all merchant projects	Y - to check transactions for all projects of the current merchant N - check transactions for current end point only	Type: Enum Default: No

### Error codes

#	Code	Name
10259	1269	Customer card has previous transactions in unknown status

### Referral filters

When transaction is filtered by merchant blacklist, the API response message will have the following structure: "Transaction declined - please contact support with the following code: {error code}:{error #}" This message is relevant only for merchant black lists and can be displayed to the customer instead of actual filtering reason.

### Blacklist check (BL)

Allows blacklisting of specified clients based on various criteria such as email, IP address, etc

Score: No

Enabled by default: Y

#### Parameters

Name	Description	Value
For all merchant projects	Y - to check blacklists for all projects of the current merchant, otherwise check blacklists for current project only	Type: Enum Default: Yes

### Error codes

#	Code	Name
10137	1147	Billing country blacklisted for merchant
10138	1148	IP-address country blacklisted for merchant
10139	1149	Customer e-mail blacklisted for merchant
10140	1150	Customer fingerprint blacklisted for merchant
10141	1151	Customer ip-address blacklisted for merchant
10142	1152	Customer purpose blacklisted for merchant
10143	1153	Destination card bin blacklisted for merchant
10144	1154	Destination card country blacklisted for merchant
10145	1155	Destination card number blacklisted for merchant
10146	1156	Destination card type blacklisted for merchant
10147	1157	E-mail domain blacklisted for merchant
10148	1158	Source card bin blacklisted for merchant
10149	1159	Source card country blacklisted for merchant
10150	1160	Source card number blacklisted for merchant
10151	1161	Source card type blacklisted for merchant
10156	1166	Customer e-mail blacklisted for manager
10157	1167	Customer fingerprint blacklisted for manager
10158	1168	Customer ip-address blacklisted for manager
10159	1169	Customer purpose blacklisted for manager
10160	1170	Destination card number blacklisted for manager
10161	1171	E-mail domain blacklisted for manager
10162	1172	Source card number blacklisted for manager
10169	1179	Customer e-mail + source card number blacklisted for merchant
10194	1204	Source card mask blacklisted for merchant
10195	1205	Destination card mask blacklisted for merchant
10196	1206	Source card mask blacklisted for manager
10197	1207	Destination card mask blacklisted for manager

### Predefined loyalty lists check

Allows processing for trusted customers only. Different merchants have different definitions of a trusted customer, this filter allows processing for customers with emails, source/destination card or purpose in corresponding loyalty lists only. Transactions for customers that are not listed in any loyalty list will be filtered out. Filter will be applied for chosen countries only, for all other countries check will be ignored.

Score: Yes

Enabled by default: N

### Parameters

Name	Description	Value
BIN country identifier	*	Type: List Default: *
For all merchant projects	Y - to check customer email in email anti-blacklists for all projects of the current merchant, otherwise check in email list for current project only	Type: Enum Default: Yes
Ignore check for account type	*	Type: String Default: *
Ignore check for bank id list	*	Type: String Default: *
IP country identifier	apply filter for selected countries only, country defined by customer IP	Type: List Default: *

### Error codes

#	Code	Name
10152	1162	Merchant loyal customer e-mail check failed
10153	1163	Merchant loyal customer purpose check failed
10154	1164	Merchant loyal destination card number check failed
10155	1165	Merchant loyal source card number check failed
10163	1173	Manager loyal customer e-mail check failed
10164	1174	Manager loyal customer purpose check failed
10165	1175	Manager loyal destination card number check failed
10166	1176	Manager loyal source card number check failed
10168	1178	Merchant loyal customer e-mail + source card number end check failed
10183	1193	Merchant loyal customer e-mail + source card number check failed
10184	1194	Merchant loyal customer phone + source card number check failed
10185	1195	Merchant loyal customer purpose + source card number check failed
10186	1196	Merchant loyal customer fingerprint + source card number check failed
10193	1203	Transaction declined - please contact support with the following code: 1203:10193
10260	1270	Manager loyal destination card mask check failed
10261	1271	Merchant loyal source card mask check failed
10262	1272	Merchant loyal destination card mask check failed
10263	1273	Manager loyal source card mask check failed

### Ban untrusted networks

Allows to make block lists based on the specific IP address ranges of the customer. Merchants are able to submit IP address ranges in either IPv4 or IPv6 format via CSV upload.

Score: No

Enabled by default: N

### Parameters

Name	Description	Value
Customer ip ranges	file format example: 192.168.0.0, 192.168.255.255 fd00:0000:0000:0000:0000:0000:0000:0000, fdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff	Type: File

### Error codes

#	Code	Name
10034	1044	Untrusted network

### Credit Card Whitelist check (WL)

Allows ignoring all other fraud filters for selected credit cards. Sometimes customer's behavior can lead to the unfortunate situation where a shopper is completely unable to process transactions. You can whitelist a customer's credit card so they can successfully process their transaction. White list will be applied only before total transactions amount for the last month for this credit card will not reach the limit specified by filter parameters. White list could be specified for: the exact source card number by manager and merchant, the exact destination card number by merchant or the whole source card number issuer BIN range.

Score: N/A

Enabled by default: Y

### Parameters

Name	Description	Value
For all merchant projects	current total transactions amount for the last month for this credit card value would be calculated, - Y: for all projects, - 3D: for 3D gates only, - Non3D: for non 3D gates only, - N: for current project only of the current merchant and converted to current project currency to compare with "up to amount" value	Type: Enum Default: Yes
Subtract Cancel transactions	*	Type: Enum Default: Yes
Up to amount	maximum total transactions amount for the last month for this credit card to allow credit card to be whitelisted, if this limit reached - whitelist will be ignored	Type: Decimal Default: 99999999

**Customer fingerprint**

Score: Yes

Enabled by default: N

**Parameters**

Name	Value
Add to black list threshold	Type: Decimal Default: 10.0
Block transaction threshold	Type: Decimal Default: 3.5

**Error codes**

#	Code	Name
10035	1045	Fraud suspicious activity
10039	1049	Fraud suspicious activity

**Check reader entry mode**

If reader entry mode not in allowed list and this list is configured - filter declines transaction

Score: No

Enabled by default: N

**Error codes**

#	Code	Name
10088	1098	Incorrect reader entry mode

**IP address Country check**

This referral list allows the merchant to process transactions only for selected countries based on country of the customer IP address. Requests from IP addresses listed in "Merchant API IP address" are ignoring this check.

Score: No

Enabled by default: N

**Parameters**

Name	Description	Value
Country identifier	comma separated country identifiers list	Type: List

**Error codes**

#	Code	Name
10014	1024	Country not in trust list

**Issuer Country check**

This referral list allows the merchant to process transactions only for selected countries based on issuing country of the card. Requests from IP addresses listed in “Merchant API IP address” are ignoring this check. Check applied for both Source and Destination card numbers.

Score: No

Enabled by default: N

**Parameters**

Name	Description	Value
Country identifier	comma separated country identifiers list	Type: List

**Error codes**

#	Code	Name
10015	1025	Issuer country not in trust list

**Billing Country check**

This referral list allows the merchant to process transactions only for selected countries based on billing country of the customer. Requests from IP addresses listed in “Merchant API IP address” are ignoring this check.

Score: No

Enabled by default: N

**Parameters**

Name	Description	Value
Country identifier	comma separated country identifiers list	Type: List

**Error codes**

#	Code	Name
10112	1122	Billing country not in trust list

### IP address Country blacklist

This referral list allows the merchant to make block lists based on country of the customer IP address. Requests from IP addresses listed in “Merchant API IP address” are ignoring this check.

Score: No

Enabled by default: N

#### Parameters

Name	Description	Value
Country identifier	comma separated country identifiers list	Type: List

#### Error codes

#	Code	Name
10028	1038	Country in blacklist

### Issuer Country blacklist

This referral list allows the merchant to make block lists based on issuing country of the card. Requests from IP addresses listed in “Merchant API IP address” are ignoring this check. Check applied for both Source and Destination card numbers.

Score: No

Enabled by default: N

#### Parameters

Name	Description	Value
Country identifier	comma separated country identifiers list	Type: List

#### Error codes

#	Code	Name
10027	1037	Issuer country in blacklist

### Billing Country blacklist

This referral list allows the merchant to make block lists based on billing country of the customer. Requests from IP addresses listed in “Merchant API IP address” are ignoring this check.

Score: No

Enabled by default: N

#### Parameters

Name	Description	Value
Country identifier	comma separated country identifiers list	Type: List

#### Error codes

#	Code	Name
10113	1123	Billing country in blacklist

### Issuer Country blacklist by Payment method

This referral list allows the merchant to make block lists based on issuing country of the card for selected payment method. Requests from IP addresses listed in “Merchant API IP address” are ignoring this check. Check applied for both Source and Destination card numbers.

Score: N/A

Enabled by default: N

#### Parameters

Name	Value
	Type: List Default: -

#### Error codes

#	Code	Name
10123	1133	Issuer country in blacklist for selected payment method

### Transaction amount check

This check can be used to apply higher risk scores to transactions based on the transaction amount.

Score: Yes

Enabled by default: N

**Parameters**

Name	Value
Transaction amount	Type: Decimal Default: 0.0

**Error codes**

#	Code	Name
10032	1042	Incorrect transaction amount

**Source Credit Card type check**

This referral list allows the merchant to process transactions only for selected Source Credit Card types. Counts Sale and Transfer transactions.

Score: No

Enabled by default: N

**Parameters**

Name	Description	Value
forbidden card level types	comma separated card level type list. Typical card types: PREPAID, REWARDS, VIRTUAL, CASH, ATM, STANDARD, CLASSIC, GOLD, SIGNATURE, PLATINUM, ELECTRON, CORPORATE, BUSINESS, WORLD, DEBIT and variations like GOLD REWARDS, WORLD CORPORATE, etc.	Type: String Default: PREPAID, REWARD, CORPORATE, BUSINESS

**Error codes**

#	Code	Name
10127	1137	Unsupported product type

**Destination Credit Card type check**

This referral list allows the merchant to process transactions only for selected Destination Credit Card types. Counts Sale and Transfer transactions.

Score: No

Enabled by default: N

**Parameters**

Name	Description	Value
forbidden card level types	comma separated card level type list. Typical card types: PREPAID, REWARDS, VIRTUAL, CASH, ATM, STANDARD, CLASSIC, GOLD, SIGNATURE, PLATINUM, ELECTRON, CORPORATE, BUSINESS, WORLD, DEBIT and variations like GOLD REWARDS, WORLD CORPORATE, etc.	Type: String Default: PREPAID, REWARD, CORPORATE, BUSINESS

### Error codes

#	Code	Name
10129	1139	Unsupported destination product type

### Consistency filters

#### Check customer data

If one of the stop words contains in cardholder name or firstname/last name OR if cardholder name or firstname/lastname match the specified regexp OR if customer data failed basic validation rules (in case the validation flag is turned on) - filter declines transaction.

Score: Yes

Enabled by default: N

#### Parameters

Name	Value
Apply basic validation rules	Type: Enum Default: Y
Check if customer first name and last name are equal	Type: Enum Default: N
Check if customer first name contains last name	Type: Enum Default: N
Check if customer last name contains first name	Type: Enum Default: N
Deny regexp	Type: String Default: *
Min customer first name length	Type: Int Default: 0

continues on next page

Table 48 – continued from previous page

Name	Value
Min customer last name length	Type: Int Default: 0
Stop word list	Type: String Default: *

### Customer IP address Country differs from Issuing Country

This risk check is triggered when a transaction has the customer IP country different from the issuing country of the card. Requests from IP addresses listed in “Merchant API IP address” are ignoring this check. If parameter “apply for countries” is empty, filter will require strict customer country to issuer country matching for all the countries, otherwise this check will force country matching for listed countries only. For example if you setup “apply for countries” to US - check will be triggered for following country combinations US-anyNonUS or anyNonUS-US, but for combinations anyNonUS-anyNonUS and US-US the check will not fire. For card2card transactions issuer country of the source card should be equal to issuer country of the destination card, i.e. this check will be triggered for any cross-border transaction.

Score: Yes

Enabled by default: N

#### Parameters

Name	Description	Value
apply for countries	if current parameters are not empty, check will be applied for listed countries only	Type: List Default: 0
ignore undefined countries	ignore check if country of the customer or issuer could not be defined	Type: Enum Default: Y
skip country identifier	ignore check for specific customer country, for example check could be skipped if customer uses mobile network with Opera browser proxy to process the transaction	Type: List Default: 0

#### Error codes

#	Code	Name
10013	1023	Country of the customer does not correspond to the country of the issuer

### Customer name differs from Cardholder name

This check fires when the provided customer name does not match cardholder name.

Score: Yes

Enabled by default: N

### Parameters

Name	Description	Value
greatest levenshtein distance	greatest levenshtein distance to consider customer and cardholder names equal	Type: Int Default: 3

### Error codes

#	Code	Name
10114	1124	Customer name does not correspond to the cardholder name

### Customer IP address differs from IP address used for 3-D Secure validation

This check fires when the provided Customer IP address does not match IP address used for 3-D Secure validation. Sometimes fraudsters are changing the destination of the payment converting sale operations (revocable operation) to card2card transfers to their own cards (irrevocable operation). To exclude the automation of such fraud cases this filter could be used. Some providers are using dynamic IP addresses for their clients and during transaction processing customer IP address might be changed slightly. To avoid false positives in such cases IP address change in /24 subnet is allowed.

Score: Yes

Enabled by default: N

### Error codes

#	Code	Name
10070	1080	Customer IP address have been changed during transaction processing

### Customer birthday check

This check fires when the provided customer birthday is in incorrect format or customer is too young or too old to perform requested operation.

Score: Yes

Enabled by default: N

### Parameters

Name	Description	Value
date format	input format for customers birthday, following macros are allowed - %Y Year, numeric, four digits - %m Month, numeric (00..12) - %d Day of the month, numeric (00..31)	Type: String Default: %Y%m%d
maximum age	maximum client age to process the transaction	Type: Int Default: 100
minimum age	minimum client age to process the transaction	Type: Int Default: 16

### Error codes

#	Code	Name
10086	1096	Invalid customer birthday

### Source Credit Card number expiration date check

This check fires when the provided Source Credit Card expiration date will expire soon. The time threshold is a moving window calculated backwards from the moment of the transaction. Usually card expires in the last day of the expiration month printed on card. Check could be used to avoid acceptance of the Credit Card for future preauthorized payments if it expires before the the last recurring payment planned.

Score: Yes

Enabled by default: N

### Parameters

Name	Description	Value
minimum days before card expiration	minimum days before card expiration date	Type: Int Default: 0

### Error codes

#	Code	Name
10126	1136	Card expires too soon

### The 6+4 customer cards differs from the 6+4 passed in purpose

This check fires when the provided Customer 6+4 card does not match 6+4 passed in purpose. Counts Sale and Preauth transactions in any status.

Score: Yes

Enabled by default: N

**Error codes**

#	Code	Name
10249	1259	Customer card 6+4 does not match the purpose

**Custom business validations****Transaction amount changing for Purpose**

This check fires when the Transaction amount changing associated with exact Purpose exceeds the configured thresholds. The time threshold is a moving window calculated backwards from the moment of the transaction. So, if you set a quantity threshold of 10 transactions in 30 days, only 10 transactions with amount fitting parameter regexp below will be allowed, starting from 11th transactions its amount should fit regexp after parameter value. Counts Account verification, Sale, Preauth or Transfer transactions in Approved status.

Score: No

Enabled by default: N

**Parameters**

Name	Description	Value
for all merchant projects	Y - to check transactions for all projects of the current merchant, otherwise check transactions for current project only	Type: Enum Default: N
lookup period in days	lookup period to analyse transaction amount velocity in days	Type: int Default: 30
quantity threshold	since specified threshold all transaction amounts should fit "regexp after" parameter value	Type: int Default: 99999
regexp after	regular expression value to fit all transaction amounts, starting from "quantity threshold" parameter value	Type: String Default: ^(2[5-9][0-9] [3-9][0-9]{2}) [1-9][0-9]{3,10})([0-9]{0,3})?\$\$
regexp below	if transaction amount fits this parameter value, "quantity threshold" current value increased by one	Type: String Default: ^([0-9]{1,2} 1[0-9]{2} 2[0-4][0-9])([0-9]{0,3})?\$\$

**Error codes**

#	Code	Name
10080	1090	Invalid transaction amount

### Authorization reattempts requirements EMEA

This check fires for all purchase transactions. Merchants that receive a decline response for a transaction will only be allowed to resubmit it for authorization up to fifteen times within 30 calendar days from the date of the original decline response if the response code is one of the following:

- Response Code 100-Decline (general, no comments)
- Response Code 101-Decline, expired card
- Response Code 102-Decline, suspected fraud
- Response Code 104-Decline, restricted card
- Response Code 106-Decline, allowable PIN tries exceeded
- Response Code 107-Decline, refer to card issuer
- Response Code 108-Decline, refer to card issuer's special conditions
- Response Code 109-Decline, invalid merchant
- Response Code 110-Decline, invalid amount
- Response Code 112-Decline, PIN data required
- Response Code 114-Decline, no account of type requested
- Response Code 115-Decline, requested function not supported
- Response Code 116-Decline, not sufficient funds
- Response Code 117-Decline, incorrect PIN
- Response Code 120-Decline, transaction not permitted to terminal
- Response Code 121-Decline, exceeds withdrawal amount limit
- Response Code 122-Decline, security violation
- Response Code 123-Decline, exceeds withdrawal frequency limit
- Response Code 124-Decline, violation of law
- Response Code 160-Decline, additional customer authentication required
- Response Code 197-Decline, call AmEx
- Response Code 198-Decline, call Card Processing Centre
- Response Code 903-Status message: re-enter transaction
- Response Code 904-Decline reason message: format error
- Response Code 907-Decline reason message: card issuer or switch inoperative
- Response Code 909-Decline reason message: system malfunction
- Response Code 913-Decline reason message: duplicate transmission
- Response Code 914-Decline reason message: not able to trace back to original transaction
- Response Code 921-Decline reason message: security software/hardware error - no action

- Response Code 950-Denial reason message: violation of business arrangement

International card systems Rules to prohibit acquirers and their recurring services merchants from resubmitting a declined transaction for authorization if it receives a response:

- Response Code 111-Denial, invalid card number
- Response Code 180-Denial, by cardholders wish
- Response Code 200-Pick-up (general, no comments)
- Response Code 207-Pick-up, special conditions
- Response Code 208-Pick-up, lost card
- Response Code 209-Pick-up, stolen card
- Response Code 908-Denial reason message: transaction destination cannot be found for routing

Visa only:

- Response Code 119-Denial, transaction not permitted to cardholder
- Response Code 902-Denial reason message: invalid transaction

Mastercard only:

- Response Code 201-Pick-up, expired card
- Response Code 202-Pick-up, suspected fraud
- Response Code 203-Pick-up, card acceptor contact card acquirer
- Response Code 204-Pick-up, restricted card
- Response Code 205-Pick-up, card acceptor call acquirer's security department
- Response Code 206-Pick-up, allowable PIN tries exceeded
- Response Code 210-Pick-up, suspected counterfeit card

The time threshold is a moving window calculated backwards from the moment of the transaction. Counts Account verification, Sale, Preauth transactions in Declined status for listed decline reasons. Correct decline reasons should be supported by a connected PSP. Limits are calculated separately for each merchant id, PAN and transaction amount.

Score: No

Enabled by default: N

### Error codes

#	Code	Name
10182	1192	Payment system authorisation reattempts limit reached

### Visa Preauthorized Transaction Decline Response requirements N.A.

This check fires for recurring transactions only. Merchants that receive a decline response for a preauthorized transaction will only be allowed to resubmit it for authorization up to four times within 16 calendar days from the date of the original decline response if the response code is one of the following:

- Response Code 05 - Authorization Declined
- Response Code 51 - Insufficient Funds
- Response Code 61 - Exceeds Approval Amount Limit
- Response Code 65 - Exceeds Withdrawal Frequency Limit

If an approval response is not received within this time frame, merchants must not resubmit the transaction or their acquirers may be subject to non-compliance actions, as outlined in the Visa Rules, and may be subject to chargebacks. Visa Rules to prohibit acquirers and their recurring services merchants from resubmitting a declined transaction for authorization if it receives a pickup response:

- Response Code 04 - Pick Up Card
- Response Code 07 - Pick Up Card, Special
- Response Code 33 - Expired Card, Capture
- Response Code 34 - Suspected Fraud, Retain Card
- Response Code 35 - Card Acceptor, Contact Acquirer, Retain Card
- Response Code 36 - Restricted Card, Retain Card
- Response Code 37 - Contact Acquirer Security Department, Retain Card
- Response Code 41 - Lost Card
- Response Code 43 - Stolen Card
- Response Code 67 - Capture Card

or a decline response of

- Response Code 14 - Invalid Account Number (No Such Number)
- Response Code 54 - Expired Card
- Response Code 57 - Transaction Not Permitted

The time threshold is a moving window calculated backwards from the moment of the transaction. Counts Account verification, Sale, Preauth or Transfer transactions in Declined status for listed decline reasons. Correct decline reasons should be supported by a connected PSP. Limits are calculated separately for each gate descriptor.

Score: No

Enabled by default: N

**Parameters**

Name	Description	Value
apply restriction types	CANCEL (only cancel decline reasons), PICKUP (only pickup decline reasons), DELAY (only time frame delays)	Type: String Default: CANCEL,PICKUP,DELAY

continues on next page

Table 62 – continued from previous page

Name	Description	Value
ignore period in months	if this parameter value greater zero, only one declined transaction allowed during the specified period, independently from its decline code	Type: Int Default: 0

**Error codes**

#	Code	Name
10090	1100	Visa rules violation for preauthorized transaction(DELAY)
10135	1145	PSP rules violation for no CVV transaction (CANCEL)
10136	1146	PSP rules violation for no CVV transaction (PICKUP)

**MCC 6211 restrictions**

## Security Brokers/Dealers

- [5] American Samoa
- [7] Angola
- [9] Antarctica
- [19] Bangladesh
- [22] Belgium
- [24] Benin
- [26] Bhutan
- [28] Bosnia and Herzegovina
- [30] Bouvet Island
- [32] British Indian Ocean Territory
- [34] Bulgaria
- [35] Burkina Faso
- [36] Burundi
- [39] Canada
- [40] Cabo Verde
- [43] Chad
- [45] China
- [46] Christmas Island
- [47] Cocos (Keeling) Islands
- [49] Comoros
- [50] Congo
- [54] Cote d'Ivoire
- [60] Djibouti
- [61] Dominica
- [66] Equatorial Guinea
- [67] Eritrea
- [69] Ethiopia
- [70] Falkland Islands (Malvinas)

[78] Gabon  
[79] Gambia  
[85] Greenland  
[86] Grenada  
[87] Guadeloupe  
[91] Guinea  
[92] Guinea-Bissau  
[94] Haiti  
[95] Heard Island and McDonald Islands  
[96] Holy See (Vatican City State)  
[107] Israel  
[110] Japan  
[115] Kosovo  
[116] Kiribati  
[121] Lao People's Democratic Republic  
[125] Liberia  
[131] North Macedonia  
[132] Madagascar  
[133] Malawi  
[136] Mali  
[139] Martinique  
[140] Mauritania  
[144] Micronesia, Federated States of  
[147] Mongolia  
[151] Mozambique  
[152] Myanmar  
[154] Nauru  
[155] Nepal  
[157] Netherlands Antilles  
[158] New Caledonia  
[161] Niger  
[163] Niue  
[164] Norfolk Island  
[165] Northern Mariana Islands  
[169] Palau  
[170] Palestine, State of  
[176] Pitcairn  
[179] Puerto Rico  
[181] Reunion  
[184] Rwanda  
[185] Saint Barthelemy  
[186] Saint Helena, Ascension and Tristan da Cunha  
[189] Saint Martin (French part)  
[190] Saint Pierre and Miquelon  
[194] Sao Tome and Principe  
[196] Senegal  
[203] Solomon Islands

[206] South Georgia and the South Sandwich Islands  
 [210] Suriname  
 [211] Svalbard and Jan Mayen  
 [217] Tajikistan  
 [220] Timor-Leste  
 [221] Togo  
 [222] Tokelau  
 [223] Tonga  
 [228] Turks and Caicos Islands  
 [229] Tuvalu  
 [238] Vanuatu  
 [240] Viet Nam  
 [243] Wallis and Futuna  
 [244] Western Sahara  
 [246] Zambia  
 [247] Zimbabwe  
 [254] Bonaire, Sint Eustatius and Saba

Score: No

Enabled by default: N

### Parameters

Name	Description	Value
allow Australia	allows Australia processing	Type: Enum Default: N
allow France	allows France processing	Type: Enum Default: N
allow Jamaica	allows Jamaica processing	Type: Enum Default: N
allow MasterCard for NA	allows MasterCard processing for North America	Type: Enum Default: N
allow Netherlands	allows Netherlands processing	Type: Enum Default: N
allow Uganda	allows Uganda processing	Type: Enum Default: N

### Error codes

#	Code	Name
10099	1109	MCC 6211 rules violation

### MCC 7995 restrictions

#### Betting/Casino Gambling

- [5] American Samoa
- [7] Angola
- [8] Anguilla
- [9] Antarctica
- [15] Austria
- [19] Bangladesh
- [22] Belgium
- [24] Benin
- [26] Bhutan
- [28] Bosnia and Herzegovina
- [29] Botswana
- [30] Bouvet Island
- [32] British Indian Ocean Territory
- [33] Brunei Darussalam
- [34] Bulgaria
- [35] Burkina Faso
- [36] Burundi
- [40] Cabo Verde
- [42] Central African Republic
- [43] Chad
- [46] Christmas Island
- [47] Cocos (Keeling) Islands
- [49] Comoros
- [50] Congo
- [54] Cote d'Ivoire
- [55] Croatia
- [56] Cuba
- [57] Cyprus
- [58] Czech Republic
- [59] Denmark
- [60] Djibouti
- [61] Dominica
- [62] Dominican Republic
- [66] Equatorial Guinea
- [67] Eritrea
- [68] Estonia
- [69] Ethiopia
- [70] Falkland Islands (Malvinas)
- [72] Fiji

[73] Finland  
[74] France  
[78] Gabon  
[79] Gambia  
[82] Ghana  
[84] Greece  
[85] Greenland  
[86] Grenada  
[87] Guadeloupe  
[91] Guinea  
[92] Guinea-Bissau  
[94] Haiti  
[95] Heard Island and McDonald Islands  
[96] Holy See (Vatican City State)  
[98] Hong Kong  
[99] Hungary  
[103] Iran, Islamic Republic of  
[104] Iraq  
[105] Ireland  
[107] Israel  
[108] Italy  
[109] Jamaica  
[111] Jersey  
[115] Kosovo  
[116] Kiribati  
[117] Korea, Democratic People's Republic of  
[118] Korea, Republic of  
[121] Lao People's Democratic Republic  
[122] Latvia  
[123] Lebanon  
[125] Liberia  
[126] Libya  
[128] Lithuania  
[129] Luxembourg  
[131] North Macedonia  
[132] Madagascar  
[133] Malawi  
[136] Mali  
[137] Malta  
[139] Martinique  
[140] Mauritania  
[144] Micronesia, Federated States of  
[147] Mongolia  
[149] Montserrat  
[151] Mozambique  
[152] Myanmar  
[154] Nauru

[155] Nepal  
[156] Netherlands  
[157] Netherlands Antilles  
[158] New Caledonia  
[161] Niger  
[163] Niue  
[164] Norfolk Island  
[165] Northern Mariana Islands  
[166] Norway  
[169] Palau  
[170] Palestine, State of  
[175] Philippines  
[176] Pitcairn  
[177] Poland  
[178] Portugal  
[179] Puerto Rico  
[181] Reunion  
[184] Rwanda  
[185] Saint Barthelemy  
[186] Saint Helena, Ascension and Tristan da Cunha  
[188] Saint Lucia  
[189] Saint Martin (French part)  
[190] Saint Pierre and Miquelon  
[194] Sao Tome and Principe  
[196] Senegal  
[200] Singapore  
[201] Slovakia  
[202] Slovenia  
[203] Solomon Islands  
[204] Somalia  
[206] South Georgia and the South Sandwich Islands  
[207] Spain  
[209] Sudan  
[210] Suriname  
[211] Svalbard and Jan Mayen  
[212] Eswatini  
[213] Sweden  
[214] Switzerland  
[215] Syrian Arab Republic  
[217] Tajikistan  
[220] Timor-Leste  
[221] Togo  
[222] Tokelau  
[223] Tonga  
[226] Turkey  
[228] Turks and Caicos Islands  
[229] Tuvalu

[230] Uganda  
 [234] United States  
 [238] Vanuatu  
 [239] Venezuela, Bolivarian Republic of  
 [240] Viet Nam  
 [242] Virgin Islands, U.S.  
 [243] Wallis and Futuna  
 [244] Western Sahara  
 [245] Yemen  
 [246] Zambia  
 [247] Zimbabwe  
 [253] Curaçao  
 [254] Bonaire, Sint Eustatius and Saba  
 [255] South Sudan

Score: No

Enabled by default: N

#### Parameters

Name	Description	Value
allow Germany	allows Germany processing	Type: Enum Default: N
allow UK	allows United Kingdom processing	Type: Enum Default: N

#### Error codes

#	Code	Name
10124	1134	MCC 7995 rules violation

#### CDB processing restrictions

Deny all countries except USA and EU countries. Also deny the following EU countries: Austria, Belgium, Denmark, Malta, Portugal, Romania, Slovakia, Estonia, Latvia; and the following US states: Alabama, Georgia, Missouri, South Dakota, Nebraska, California, North Carolina, Florida.

Score: No

Enabled by default: N

#### Parameters

Name	Value
check credit card BIN country	Type: Enum Default: Y
check customer billing address country	Type: Enum Default: Y
check customer IP country	Type: Enum Default: Y

### Error codes

#	Code	Name
10167	1177	CDB processing restrictions violation.

### Velocity filters

#### Source Credit Card Number decline frequency for last 24 hours (daily decline limit)

This check fires when the number or amount of declined transactions associated with exact Source credit card number exceeds the configured thresholds. The time threshold is a 24 hours window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 24 hours. Counts Account verification, Sale, Preauth or Transfer transactions in the Declined status.

Score: Yes

Enabled by default: N

#### Parameters

Name	Description	Value
amount limit	maximum total transactions amount for the last 24 hours for this credit card used as Source card	Type: Decimal Default: 999999999
For all merchant projects	current total transactions amount or count for the last 24 hours for this credit card value would be calculated: - Y: for all projects - 3DS: for 3DS gates only - Non-3DS: for non-3DS gates only - N: for current project only of the current merchant and converted to current project currency to compare with amount or quantity limit values	Type: Enum Default: Y

continues on next page

Table 70 - continued from previous page

Name	Description	Value
quantity limit	maximum total transactions count for the last 24 hours for this credit card used as Source card	Type: Int Default: 99999
Use calendar days	"Y" For calculation using calendar days instead of calculation from moment when filter was enabled "N" for calculation from moment when filter was enabled	Type: Enum Default: N

**Error codes**

#	Code	Name
10083	1093	Daily decline amount limit exceeded for sender
10084	1094	Daily decline quantity limit exceeded for sender

**Source Credit Card Number increasing sequence of approved transaction amounts for last 24 hours (daily rising limit)**

This check fires when the number of approved transactions with increasing amount associated with exact Source credit card number exceeds the configured thresholds. The time threshold is a 24 hours window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 increasing transactions, it fires on the 11th increasing transaction in 24 hours. Counts Sale, Preauth or Transfer transactions in the Approved status. This check only cross-checks transactions within the same merchant account in the same project.

Score: Yes

Enabled by default: N

**Parameters**

Name	Description	Value
quantity limit	maximum transactions count with increasing amount for the last 24 hours for this credit card number	Type: Int Default: 99999

**Error codes**

#	Code	Name
10022	1032	Too many transactions with increasing amounts for sender

### Source Credit Card Number usage frequency for last 24 hours (daily limit)

This check fires when the number or amount of transactions associated with exact Source credit card number exceeds the configured thresholds. The time threshold is a 24 hours window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 24 hours. Counts Sale, Preauth or Transfer transactions in the approved status.

Score: Yes

Enabled by default: N

#### Parameters

Name	Description	Value
amount limit	maximum total transactions amount for the last 24 hours for this credit card used as Source card	Type: Decimal Default: 999999999
for all merchant projects	current total transactions amount or count for the last 24 hours for this credit card value would be calculated: - Y: for all projects - 3DS: for 3DS gates only - Non-3DS: for non-3DS gates only - N: for current project only of the current merchant and converted to current project currency to compare with amount or quantity limit values	Type: Enum Default: Y
quantity limit	maximum total transactions count for the last 24 hours for this credit card used as Source card	Type: Int Default: 99999
skip payouts	allows to process Payout transactions even when the count or amount exceeds the thresholds	Type: Enum Default: N
subtract Cancel transactions	subtracts Cancelled transactions from the calculated count and amount thresholds	Type: Enum Default: N
use calendar day	"Y" For calculation using calendar days instead of calculation from moment when filter was enabled "N" for calculation from moment when filter was enabled	Type: Enum Default: N

#### Error codes

#	Code	Name
10016	1026	Daily amount limit exceeded for sender
10017	1027	Daily quantity limit exceeded for sender

### Source Credit Card Number usage frequency for last 7 days (weekly limit)

This check fires when the number or amount of transactions associated with exact Source credit card number exceeds the configured thresholds. The time threshold is a 7 days window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 168 hours. Counts Sale, Preauth or Transfer transactions in the approved status.

Score: Yes

Enabled by default: N

#### Parameters

Name	Description	Value
amount limit	maximum total transactions amount for the last 7 days for this credit card used as Source card	Type: Decimal Default: 999999999
calendar week starts from Sunday	“Y”: calendar week starts from Sunday “N”: calendar week starts from Monday	Type: Enum Default: N
for all merchant projects	current total transactions amount or count for the last 7 days for this credit card value would be calculated: - Y: for all projects - 3DS: for 3DS gates only - Non-3DS: for non-3DS gates only - N: for current project only of the current merchant and converted to current project currency to compare with amount or quantity limit values	Type: Enum Default: Y
quantity limit	maximum total transactions count for the last 7 days for this credit card used as Source card	Type: Int Default: 99999
skip payouts	allows to process Payout transactions even when the count or amount exceeds the thresholds	Type: Enum Default: N
subtract Cancel transactions	subtracts Cancelled transactions from the calculated count and amount thresholds	Type: Enum Default: N
use calendar week	“Y” For calculation using calendar weeks instead of calculation from moment when filter was enabled “N” for calculation from moment when filter was enabled	Type: Enum Default: N

#### Error codes

#	Code	Name
10018	1028	Weekly amount limit exceeded for sender

continues on next page

Table 77 - continued from previous page

#	Code	Name
10019	1029	Weekly quantity limit exceeded for sender

### Source Credit Card Number usage frequency for last month (monthly limit)

This check fires when the number or amount of transactions associated with exact Source credit card number exceeds the configured thresholds. The time threshold is a one month window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in one month. Month calculation based on calendar i.e. 28th, 29th, 30th and 31st of March would be bumped to 28th of February during window calculation. Counts Sale, Preauth or Transfer transactions in the approved status.

Score: Yes

Enabled by default: N

#### Parameters

Name	Description	Value
amount limit	maximum total transactions amount for the last one month for this credit card used as Source card	Type: Decimal Default: 999999999
for all merchant projects	current total transactions amount or count for the last one month for this credit card value would be calculated: - Y: for all projects - 3DS: for 3DS gates only - Non-3DS: for non-3DS gates only - N: for current project only of the current merchant and converted to current project currency to compare with amount or quantity limit values	Type: Enum Default: Y
quantity limit	maximum total transactions count for the last one month for this credit card used as Source card	Type: Int Default: 99999
skip payouts	allows to process Payout transactions even when the count or amount exceeds the thresholds	Type: Enum Default: N
subtract Cancel transactions	subtracts Cancelled transactions from the calculated count and amount thresholds	Type: Enum Default: N
use calendar month	“Y” For calculation using calendar months instead of calculation from moment when filter was enabled “N” for calculation from moment when filter was enabled	Type: Enum Default: N

#### Error codes

#	Code	Name
10020	1030	Monthly amount limit exceeded for sender
10021	1031	Monthly quantity limit exceeded for sender

### Destination Credit Card Number usage frequency for last 24 hours (daily limit)

This check fires when the number or amount of transactions associated with exact Destination credit card number exceeds the configured thresholds. The time threshold is a 24 hours window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 24 hours. Counts Transfer transactions only in the approved status.

Score: Yes

Enabled by default: N

#### Parameters

Name	Description	Value
amount limit	maximum total transactions amount for the last 24 hours for this credit card used as Destination card	Type: Decimal Default: 999999999
for all merchant projects	current total transactions amount or count for the last 24 hours for this credit card value would be calculated: - Y: for all projects - 3DS: for 3DS gates only - Non-3DS: for non-3DS gates only - N: for current project only of the current merchant and converted to current project currency to compare with amount or quantity limit values	Type: Enum Default: Y
quantity limit	maximum total transactions count for the last 24 hours for this credit card used as Destination card	Type: Int Default: 99999
use calendar day	"Y" For calculation using calendar days instead of calculation from moment when filter was enabled "N" for calculation from moment when filter was enabled	Type: Enum Default: N

#### Error codes

#	Code	Name
10049	1059	Daily amount limit exceeded for recipient
10050	1060	Daily quantity limit exceeded for recipient

### Destination Credit Card Number usage frequency for last 7 days (weekly limit)

This check fires when the number or amount of transactions associated with exact Destination credit card number exceeds the configured thresholds. The time threshold is a 7 days window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 168 hours. Counts Transfer transactions only in the approved status.

Score: Yes

Enabled by default: N

#### Parameters

Name	Description	Value
amount limit	maximum total transactions amount for the last 7 days for this credit card used as Destination card	Type: Decimal Default: 99999999
calendar week starts from Sunday	"Y": calendar week starts from Sunday "N": calendar week starts from Monday	Type: Enum Default: N
for all merchant projects	current total transactions amount or count for the last 7 days for this credit card value would be calculated: - Y: for all projects - 3DS: for 3DS gates only - Non-3DS: for non-3DS gates only - N: for current project only of the current merchant and converted to current project currency to compare with amount or quantity limit values	Type: Enum Default: Y
quantity limit	maximum total transactions count for the last 7 days for this credit card used as Destination card	Type: Int Default: 99999
use calendar week	"Y" For calculation using calendar weeks instead of calculation from moment when filter was enabled "N" for calculation from moment when filter was enabled	Type: Enum Default: N

#### Error codes

#	Code	Name
10051	1061	Weekly amount limit exceeded for recipient
10052	1062	Weekly quantity limit exceeded for recipient

### Destination Credit Card Number usage frequency for last month (monthly limit)

This check fires when the number or amount of transactions associated with exact Destination credit card number exceeds the configured thresholds. The time threshold is a one month window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in one month. Month calculation based on calendar i.e. 28th, 29th, 30th and 31st of March would be bumped to 28th of February during window calculation. Counts Transfer transactions only in the approved status.

Score: Yes

Enabled by default: N

#### Parameters

Name	Description	Value
amount limit	maximum total transactions amount for the last one month for this credit card used as Destination card	Type: Decimal Default: 999999999
check preauth transactions	"Y" Prohibit preauth transactions when the quantity limit is reached, it is necessary to enable the filter and set the correct values of the limit on all projects where this functionality requires	Type: Enum Default: N
for all merchant projects	current total transactions amount or count for the last one month for this credit card value would be calculated: - Y: for all projects - 3DS: for 3DS gates only - Non-3DS: for non-3DS gates only - N: for current project only of the current merchant and converted to current project currency to compare with amount or quantity limit values	Type: Enum Default: Y
quantity limit	maximum total transactions count for the last one month for this credit card used as Destination card	Type: Int Default: 99999
Use calendar month	"Y" For calculation using calendar months instead of calculation from moment when filter was enabled "N" for calculation from moment when filter was enabled	Type: Enum Default: N

#### Error codes

#	Code	Name
10053	1063	Monthly amount limit exceeded for recipient

continues on next page

Table 85 – continued from previous page

#	Code	Name
10054	1064	Monthly quantity limit exceeded for recipient

### Total Credit Card Number usage frequency for last 24 hours (daily limit)

This check fires when the number or amount of transactions associated with exact credit card number used as Source or Destination exceeds the configured thresholds. The time threshold is a 24 hours window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 24 hours. Counts Sale, Preauth or Transfer transactions in the approved status

Score: Yes

Enabled by default: N

#### Parameters

Name	Description	Value
amount limit	maximum total transactions amount for the last 24 hours for this credit card used as Source or Destination	Type: Decimal Default: 999999999
for all merchant projects	current total transactions amount or count for the last 24 hours for this credit card value would be calculated: - Y: for all projects - 3DS: for 3DS gates only - Non-3DS: for non-3DS gates only - N: for current project only of the current merchant and converted to current project currency to compare with amount or quantity limit values	Type: Enum Default: Y
quantity limit	maximum total transactions count for the last 24 hours for this credit card used as Source or Destination	Type: Int Default: 99999
subtract Cancel transactions	subtracts Cancelled transactions from the calculated count and amount thresholds	Type: Enum Default: N
use calendar day	“Y” For calculation using calendar days instead of calculation from moment when filter was enabled “N” for calculation from moment when filter was enabled	Type: Enum Default: N

#### Error codes

#	Code	Name
10055	1065	Daily total amount limit exceeded for sender
10056	1066	Daily total quantity limit exceeded for sender
10057	1067	Daily total amount limit exceeded for recipient

continues on next page

Table 87 - continued from previous page

#	Code	Name
10058	1068	Daily total quantity limit exceeded for recipient

### Total Credit Card Number usage frequency for last 7 days (weekly limit)

This check fires when the number or amount of transactions associated with exact credit card number used as Source or Destination exceeds the configured thresholds. The time threshold is a 7 days window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 168 hours. Counts Sale, Preauth or Transfer transactions in the approved status

Score: Yes

Enabled by default: N

#### Parameters

Name	Description	Value
amount limit	maximum total transactions amount for the last 7 days for this credit card used as Source or Destination	Type: Decimal Default: 999999999
calendar week starts from Sunday	"Y": calendar week starts from Sunday, "N": calendar week starts from Monday	Type: Enum Default: N
for all merchant projects	current total transactions amount or count for the last 7 days for this credit card value would be calculated: - Y: for all projects - 3DS: for 3DS gates only - Non-3DS: for non-3DS gates only - N: for current project only of the current merchant and converted to current project currency to compare with amount or quantity limit values	Type: Enum Default: Y
quantity limit	maximum total transactions count for the last 7 days for this credit card used as Source or Destination	Type: Int Default: 99999
subtract Cancel transactions	subtracts Cancelled transactions from the calculated count and amount thresholds	Type: Enum Default: N
use calendar week	"Y" For calculation using calendar weeks instead of calculation from moment when filter was enabled "N" for calculation from moment when filter was enabled	Type: Enum Default: N

#### Error codes

#	Code	Name
10059	1069	Weekly total amount limit exceeded for sender
10060	1070	Weekly total quantity limit exceeded for sender
10061	1071	Weekly total amount limit exceeded for recipient
10062	1072	Weekly total quantity limit exceeded for recipient

### Total Credit Card Number usage frequency for last month (monthly limit)

This check fires when the number or amount of transactions associated with exact credit card number used as Source or Destination exceeds the configured thresholds. The time threshold is a one month window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in one month. Month calculation based on calendar i.e. 28th, 29th, 30th and 31st of March would be bumped to 28th of February during window calculation. Counts Sale, Preauth or Transfer transactions in the approved status.

Score: Yes

Enabled by default: N

#### Parameters

Name	Description	Value
amount limit	maximum total transactions amount for the last one month for this credit card used as Source or Destination	Type: Decimal Default: 999999999
for all merchant projects	current total transactions amount or count for the last one month for this credit card value would be calculated: - Y: for all projects - 3DS: for 3DS gates only - Non-3DS: for non-3DS gates only - N: for current project only of the current merchant and converted to current project currency to compare with amount or quantity limit values	Type: Enum Default: Y
quantity limit	maximum total transactions count for the last one month for this credit card used as Source or Destination	Type: Int Default: 99999
subtract Cancel transactions	subtracts Cancelled transactions from the calculated count and amount thresholds	Type: Enum Default: N
use calendar month	“Y” For calculation using calendar months instead of calculation from moment when filter was enabled “N” for calculation from moment when filter was enabled	Type: Enum Default: N

#### Error codes

#	Code	Name
10063	1073	Monthly total amount limit exceeded for sender
10064	1074	Monthly total quantity limit exceeded for sender
10065	1075	Monthly total amount limit exceeded for recipient
10066	1076	Monthly total quantity limit exceeded for recipient

### Purpose usage frequency for last 24 hours (daily limit)

This check fires when the number or amount of transactions associated with exact Purpose exceeds the configured thresholds. The time threshold is a 24 hours window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 24 hours. Counts Sale, Preauth or Transfer transactions in the approved status.

Score: Yes

Enabled by default: N

#### Parameters

Name	Description	Value
amount limit	maximum total transactions amount for the last 24 hours for this Purpose	Type: Decimal Default: 999999999
for all merchant projects	current total transactions amount or count for the last 24 hours for this credit card value would be calculated: - Y: for all projects - 3DS: for 3DS gates only - Non-3DS: for non-3DS gates only - N: for current project only of the current merchant and converted to current project currency to compare with amount or quantity limit values	Type: Enum Default: Y
quantity limit	maximum total transactions count for the last 24 hours for this Purpose	Type: Int Default: 99999
subtract Cancel transactions	subtracts Cancelled transactions from the calculated count and amount thresholds	Type: Enum Default: N
use calendar days	"Y" For calculation using calendar days instead of calculation from moment when filter was enabled "N" for calculation from moment when filter was enabled	Type: Enum Default: N

#### Error codes

#	Code	Name
10040	1050	Daily amount limit exceeded for purpose

continues on next page

Table 93 - continued from previous page

#	Code	Name
10041	1051	Daily quantity limit exceeded for purpose

### Purpose usage frequency for last 7 days (weekly limit)

This check fires when the number or amount of transactions associated with exact Purpose exceeds the configured thresholds. The time threshold is a 7 days window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 168 hours. Counts Sale, Preauth or Transfer transactions in the approved status.

Score: Yes

Enabled by default: N

### Parameters

Name	Description	Value
amount limit	maximum total transactions amount for the last 7 days for this Purpose	Type: Decimal Default: 999999999
calendar week starts from Sunday	“Y”: calendar week starts from Sunday, “N”: calendar week starts from Monday	Type: Enum Default: N
for all merchant projects	current total transactions amount or count for the last 7 days for this credit card value would be calculated: - Y: for all projects - 3DS: for 3DS gates only - Non-3DS: for non-3DS gates only - N: for current project only of the current merchant and converted to current project currency to compare with amount or quantity limit values	Type: Enum Default: Y
quantity limit	maximum total transactions count for the last 7 days for this Purpose	Type: Int Default: 99999
Subtract Cancel transactions	subtracts Cancelled transactions from the calculated count and amount thresholds	Type: Enum Default: Y
Use calendar days	“Y” For calculation using calendar days instead of calculation from moment when filter was enabled “N” for calculation from moment when filter was enabled	Type: Enum Default: N

### Error codes

#	Code	Name
10042	1052	Weekly amount limit exceeded for purpose
10043	1053	Weekly quantity limit exceeded for purpose

### Purpose usage frequency for last month (monthly limit)

This check fires when the number or amount of transactions associated with exact Purpose exceeds the configured thresholds. The time threshold is a one month window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in one month. Month calculation based on calendar i.e. 28th, 29th, 30th and 31st of March would be bumped to 28th of February during window calculation. Counts Sale, Preauth or Transfer transactions in the approved status.

Score: Yes

Enabled by default: N

### Parameters

Name	Description	Value
amount limit	maximum total transactions amount for the last one month for this Purpose	Type: Decimal Default: 999999999
for all merchant projects	current total transactions amount or count for the last one month for this credit card value would be calculated: - Y: for all projects - 3DS: for 3DS gates only - Non-3DS: for non-3DS gates only - N: for current project only of the current merchant and converted to current project currency to compare with amount or quantity limit values	Type: Enum Default: Y
quantity limit	maximum total transactions count for the last one month for this Purpose	Type: Int Default: 99999
subtract Cancel transactions	subtracts Cancelled transactions from the calculated count and amount thresholds	Type: Enum Default: N
use calendar days	"Y" For calculation using calendar days instead of calculation from moment when filter was enabled "N" for calculation from moment when filter was enabled	Type: Enum Default: N

### Error codes

#	Code	Name
10044	1054	Monthly amount limit exceeded for purpose

continues on next page

Table 97 - continued from previous page

#	Code	Name
10045	1055	Monthly quantity limit exceeded for purpose

### Email usage frequency for last 24 hours (daily limit)

This check fires when the number or amount of transactions associated with exact Email address exceeds the configured thresholds. The time threshold is a 24 hours window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 24 hours. Counts Sale, Preauth or Transfer transactions in the approved status.

Score: Yes

Enabled by default: N

### Parameters

Name	Description	Value
amount limit	maximum total transactions amount for the last 24 hours for this Email address	Type: Decimal Default: 999999999
for all merchant projects	current total transactions amount or count for the last 24 hours for this credit card value would be calculated: - Y: for all projects - 3DS: for 3DS gates only - Non-3DS: for non-3DS gates only - N: for current project only of the current merchant and converted to current project currency to compare with amount or quantity limit values	Type: Enum Default: Y
quantity limit	maximum total transactions count for the last 24 hours for this Email address	Type: Int Default: 99999
subtract Cancel transactions	subtracts Cancelled transactions from the calculated count and amount thresholds	Type: Enum Default: N
use calendar days	"Y" For calculation using calendar days instead of calculation from moment when filter was enabled "N" for calculation from moment when filter was enabled	Type: Enum Default: N

### Error codes

#	Code	Name
10073	1083	Daily amount limit exceeded for email address
10074	1084	Daily quantity limit exceeded for email address

### Email usage frequency for last 7 days (weekly limit)

This check fires when the number or amount of transactions associated with exact Email address exceeds the configured thresholds. The time threshold is a 7 days window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 168 hours. Counts Sale, Preauth or Transfer transactions in the approved status.

Score: Yes

Enabled by default: N

#### Parameters

Name	Description	Value
amount limit	maximum total transactions amount for the last 7 days for this Email address	Type: Decimal Default: 999999999
calendar week starts from Sunday	"Y": calendar week starts from Sunday "N": calendar week starts from Monday	Type: Enum Default: N
for all merchant projects	current total transactions amount or count for the last 7 days for this credit card value would be calculated: - Y: for all projects - 3DS: for 3DS gates only - Non-3DS: for non-3DS gates only - N: for current project only of the current merchant and converted to current project currency to compare with amount or quantity limit values	Type: Enum Default: Y
quantity limit	maximum total transactions count for the last 7 days for this Email address	Type: Int Default: 99999
subtract Cancel transactions	subtracts Cancelled transactions from the calculated count and amount thresholds	Type: Enum Default: N
use calendar days	"Y" For calculation using calendar days instead of calculation from moment when filter was enabled "N" for calculation from moment when filter was enabled	Type: Enum Default: N

#### Error codes

#	Code	Name
10075	1085	Weekly amount limit exceeded for email address
10076	1086	Weekly quantity limit exceeded for email address

### Email usage frequency for last month (monthly limit)

This check fires when the number or amount of transactions associated with exact Email address exceeds the configured thresholds. The time threshold is a one month window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in one month. Month calculation based on calendar i.e. 28th, 29th, 30th and 31st of March would be bumped to 28th of February during window calculation. Counts Sale, Preauth or Transfer transactions in the approved status.

Score: Yes

Enabled by default: N

#### Parameters

Name	Description	Value
amount limit	maximum total transactions amount for the last one month for this Email address	Type: Decimal Default: 999999999
for all merchant projects	current total transactions amount or count for the last one month for this credit card value would be calculated: - Y: for all projects - 3DS: for 3DS gates only - Non-3DS: for non-3DS gates only - N: for current project only of the current merchant and converted to current project currency to compare with amount or quantity limit values	Type: Enum Default: Y
quantity limit	maximum total transactions count for the last one month for this Email address	Type: Int Default: 99999
Subtract Cancel transactions	subtracts Cancelled transactions from the calculated count and amount thresholds	Type: Enum Default: N
Use calendar days	"Y" For calculation using calendar days instead of calculation from moment when filter was enabled "N" for calculation from moment when filter was enabled	Type: Enum Default: N

#### Error codes

#	Code	Name
10077	1087	Monthly amount limit exceeded for email address
10078	1088	Monthly quantity limit exceeded for email address

**IP address usage frequency for last 24 hours (daily limit)**

This check fires when the number or amount of transactions associated with exact customer IP address exceeds the configured thresholds. The time threshold is a 24 hours window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 24 hours. Counts Sale, Preauth or Transfer transactions in the approved status.

Score: Yes

Enabled by default: N

**Parameters**

Name	Description	Value
amount limit	maximum total transactions amount for the last 24 hours for this IP address	Type: Decimal Default: 999999999
for all merchant projects	current total transactions amount or count for the last 24 hours for this credit card value would be calculated: - Y: for all projects - 3DS: for 3DS gates only - Non-3DS: for non-3DS gates only - N: for current project only of the current merchant and converted to current project currency to compare with amount or quantity limit values	Type: Enum Default: Y
quantity limit	maximum total transactions count for the last 24 hours for this IP address	Type: Int Default: 99999
subtract Cancel transactions	subtracts Cancelled transactions from the calculated count and amount thresholds	Type: Enum Default: N
use calendar days	"Y" For calculation using calendar days instead of calculation from moment when filter was enabled "N" for calculation from moment when filter was enabled	Type: Enum Default: N

**Error codes**

#	Code	Name
10100	1110	Daily amount limit exceeded for IP address
10101	1111	Daily quantity limit exceeded for IP address

**IP address usage frequency for last 7 days (weekly limit)**

This check fires when the number or amount of transactions associated with exact customer IP address exceeds the configured thresholds. The time threshold is a 7 days window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 168 hours. Counts Sale, Preauth or Transfer transactions in the approved status.

Score: Yes

Enabled by default: N

**Parameters**

Name	Description	Value
amount limit	maximum total transactions amount for the last 7 days for this IP address	Type: Decimal Default: 999999999
calendar week starts from Sunday	“Y”: calendar week starts from Sunday “N”: calendar week starts from Monday	Type: Enum Default: N
for all merchant projects	current total transactions amount or count for the last 7 days for this credit card value would be calculated: - Y: for all projects - 3DS: for 3DS gates only - Non-3DS: for non-3DS gates only - N: for current project only of the current merchant and converted to current project currency to compare with amount or quantity limit values	Type: Enum Default: Y
quantity limit	maximum total transactions count for the last 7 days for this IP address	Type: Int Default: 99999
subtract Cancel transactions	subtracts Cancelled transactions from the calculated count and amount thresholds	Type: Enum Default: N
use calendar days	“Y” For calculation using calendar days instead of calculation from moment when filter was enabled “N” for calculation from moment when filter was enabled	Type: Enum Default: N

**Error codes**

#	Code	Name
10102	1112	Weekly amount limit exceeded for IP address
10103	1113	Weekly quantity limit exceeded for IP address

**IP address usage frequency for last month (monthly limit)**

This check fires when the number or amount of transactions associated with exact customer IP address exceeds the configured thresholds. The time threshold is a one month window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in one month. Month calculation based on calendar i.e. 28th, 29th, 30th and 31st of March would be bumped to 28th of February during window calculation. Counts Sale, Preauth or Transfer transactions in the approved status.

Score: Yes

Enabled by default: N

**Parameters**

Name	Description	Value
amount limit	maximum total transactions amount for the last one month for this IP address	Type: Decimal Default: 999999999
for all merchant projects	current total transactions amount or count for the last one month for this credit card value would be calculated: - Y: for all projects - 3DS: for 3DS gates only - Non-3DS: for non-3DS gates only - N: for current project only of the current merchant and converted to current project currency to compare with amount or quantity limit values	Type: Enum Default: Y
quantity limit	maximum total transactions count for the last one month for this IP address	Type: Int Default: 99999
Subtract Cancel transactions	subtracts Cancelled transactions from the calculated count and amount thresholds	Type: Enum Default: N
Use calendar days	"Y" For calculation using calendar days instead of calculation from moment when filter was enabled "N" for calculation from moment when filter was enabled	Type: Enum Default: N

**Error codes**

#	Code	Name
10104	1114	Monthly amount limit exceeded for IP address
10105	1115	Monthly quantity limit exceeded for IP address

### Source Credit Card Number usage frequency for Purpose

This check fires when the number of Source Credit Cards associated with exact Purpose exceeds the configured thresholds. The time threshold is a moving window calculated backwards from the moment of the transaction. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 Credit Cards in 6 hours, it fires on the 11th unique Credit Card in 6 hours. Counts unique Source Credit Card numbers for Account verification, Sale, Preauth or Transfer transactions in any status for the current Merchant.

Score: Yes

Enabled by default: N

#### Parameters

Name	Description	Value
checking interval in hours	time frame to calculate unique credit card numbers count	Type: Int Default: 12
maximum card number count	maximum number of unique credit cards	Type: Int Default: 5

#### Error codes

#	Code	Name
10071	1081	Too many credit cards used for the same account

### Source Credit Card Number usage frequency for Email address

This check fires when the number of Source Credit Cards associated with exact Email address exceeds the configured thresholds. The time threshold is a moving window calculated backwards from the moment of the transaction. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 Credit Cards in 6 hours, it fires on the 11th unique Credit Card in 6 hours. Counts unique Source Credit Card numbers for Account verification, Sale, Preauth or Transfer transactions in any status for the current Merchant.

Score: Yes

Enabled by default: N

#### Parameters

Name	Description	Value
checking interval in hours	time frame to calculate unique credit card numbers count	Type: Int Default: 12
maximum card number count	maximum number of unique credit cards	Type: Int Default: 5

### Error codes

#	Code	Name
10091	1101	Too many credit cards used for the same Email address

### Source Credit Card Number usage frequency for First and Last name

This check fires when the number of Source Credit Cards associated with exact Customer First and Last names exceeds the configured thresholds. The time threshold is a moving window calculated backwards from the moment of the transaction. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 Credit Cards in 6 hours, it fires on the 11th unique Credit Card in 6 hours. Counts unique Source Credit Card numbers for Sale or Preauth transactions in any status for the current Merchant.

Score: Yes

Enabled by default: N

### Parameters

Name	Description	Value
checking interval in hours	time frame to calculate unique credit card numbers count	Type: Int Default: 12
maximum card number count	maximum number of unique credit cards	Type: Int Default: 5

### Error codes

#	Code	Name
10092	1102	Too many credit cards used for the same customer

### Source Credit Card Number usage frequency for Destination Credit Card number

This check fires when the number of Source Credit Cards associated with exact Destination Credit Card number exceeds the configured thresholds. The time threshold is a moving window calculated backwards from the moment of the transaction. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 Credit Cards in 6 hours, it fires on the 11th unique Credit Card in 6 hours. Counts unique Source Credit Card numbers for Transfer transactions in any status for the current Merchant.

Score: Yes

Enabled by default: N

#### Parameters

Name	Description	Value
checking interval in hours	time frame to calculate unique credit card numbers count	Type: Decimal Default: 12.000
maximum card number count	maximum number of unique credit cards	Type: Int Default: 5

#### Error codes

#	Code	Name
10093	1103	Too many source cards used for the same destination card

### Source Credit Card Number usage frequency for Email or IP address

This check fires when the number of Source Credit Cards associated with exact Email or IP address exceeds the configured thresholds. The time threshold is a moving window calculated backwards from the moment of the transaction. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 Credit Cards in 6 hours, it fires on the 11th unique Credit Card in 6 hours. Counts unique Source Credit Card numbers for Sale, Preauth or Transfer transactions in Approved status for the current Merchant.

Score: Yes

Enabled by default: N

#### Parameters

Name	Description	Value
checking interval in hours	time frame to calculate unique credit card numbers count	Type: Int Default: 24
maximum card number count	maximum number of unique credit cards	Type: Int Default: 4

### Error codes

#	Code	Name
10026	1036	Too many source cards used for the same email or IP address

### Source Credit Card Number usage frequency

This check fires when the number of requests associated with exact Source Credit Card exceeds the configured thresholds. The time threshold is a moving window calculated backwards from the moment of the transaction. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 requests in 6 hours, it fires on the 11th request in 6 hours. Counts requests count for Account verification, Sale, Preauth or Transfer transactions in the Approved or Declined status for the current Merchant.

Score: Yes

Enabled by default: N

### Parameters

Name	Description	Value
checking interval in hours	time frame to calculate requests count	Type: Int Default: 24
maximum number of requests	maximum number of requests allowed	Type: Int Default: 5

### Error codes

#	Code	Name
10072	1082	Too many requests for the same credit card

### Customer IP address usage frequency

This check fires when the number of requests associated with exact Customer IP address exceeds the configured thresholds. Such Customer IP address is automatically added to the IP blacklist of merchant and manager. The time threshold is a moving window calculated backwards from the moment of the transaction. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 requests in 60 minutes, it fires on the 11th request in 60 minutes. Counts requests count for Account verification, Sale, Preauth or Transfer transactions in the Approved or Declined status for the current Merchant. Local IP addresses are ignored. Requests from IP address listed in "Merchant API IP address" list are ignored, i.e. if merchant initiates the request from IP address X.X.X.X and knowingly sets customer\_ip\_address to Y.Y.Y.Y for each transaction, but address X.X.X.X classified as "API IP address" for this merchant, this check will be ignored.

Score: Yes

Enabled by default: N

#### Parameters

Name	Description	Value
checking interval in minutes	time frame to calculate requests count	Type: Int Default: 10
maximum number of requests	maximum number of requests allowed	Type: Int Default: 5

### Error codes

#	Code	Name
10115	1125	Too many requests from the same IP address

### Credit Card number already used from another IP address

This check fires when the Credit Card number has already been successfully used from a different IP address. The time threshold is a moving window calculated backwards from the moment of the transaction. This check only cross-checks transactions within the same merchant account. Analyses Sale, Preauth or Transfer transactions in the Approved status. Requests from IP addresses listed in "Merchant API IP address" are ignoring this check.

Score: Yes

Enabled by default: N

**Parameters**

Name	Description	Value
checking interval in minutes	time frame to analyse approved transactions in minutes, set to 0 for infinity (not recommended)	Type: Int Default: 30

**Error codes**

#	Code	Name
10008	1006	Too many IP addresses for the same credit card number

**Credit Card number already used from another Country**

This check fires when the Credit Card number has already been successfully used from another Country. IP address is used to calculate customers country code. This check only cross-checks transactions within the same merchant account. Analyses Sale, Preauth or Transfer transactions in the Approved status. Requests from IP addresses listed in “Merchant API IP address” are ignoring this check.

Score: Yes

Enabled by default: N

**Error codes**

#	Code	Name
10079	1089	Too many countries for the same credit card number

**Credit Card number already used with another Email**

This check fires when the Credit Card number has already been successfully used with a different Email address. The time threshold is a moving window calculated backwards from the moment of the transaction. This check only cross-checks transactions within the same merchant account. Analyses Sale, Preauth or Transfer transactions in the Approved status. Requests from IP addresses listed in “Merchant API IP address” are ignoring this check.

Score: Yes

Enabled by default: N

**Parameters**

Name	Description	Value
checking interval in minutes	time frame to analyse approved transactions in minutes, set to 0 for infinity (not recommended)	Type: Int Default: 30

### Error codes

#	Code	Name
10007	1005	Too many Emails for the same credit card number

### Credit Card number already used with another Purpose

This check fires when the Credit Card number has already been successfully used with a different Purpose. The time threshold is a moving window calculated backwards from the moment of the transaction. This check only cross-checks transactions within the same merchant account. Analyses Account verification, Sale, Preauth or Transfer transactions in the Approved status. Requests from IP addresses listed in “Merchant API IP address” are ignoring this check.

Score: Yes

Enabled by default: N

### Parameters

Name	Description	Value
checking interval in minutes	time frame to analyse approved transactions in minutes, set to 0 for infinity (not recommended)	Type: Int Default: 30

### Error codes

#	Code	Name
10081	1091	Too many purposes for the same credit card number

### Credit Card number already used with another Cardholder name

This check fires when the Credit Card number has already been successfully used with another Cardholder name. Distances between current Cardholder name and existing ones are calculated using Levenshtein algorithm. This check only cross-checks transactions within the same merchant account. Analyses Sale, Preauth or Transfer transactions in the Approved status.

Score: Yes

Enabled by default: N

**Parameters**

Name	Description	Value
checking interval in hours	time frame to analyse approved transactions in hours	Type: Int Default: 30
greatest levenshtein distance	greatest levenshtein distance to consider both cardholder names equal	Type: Int Default: 3

**Error codes**

#	Code	Name
10089	1099	Too many cardholder names for the same credit card number

**Customer IP address already used by another Cardholder**

This check fires when the Customer IP address has already been successfully used by a customer with a different Cardholder name. The time threshold is a moving window calculated backwards from the moment of the transaction. This check only cross-checks transactions within the same merchant account. Analyses Sale, Preauth or Transfer transactions in the Approved status.

Score: Yes

Enabled by default: N

**Parameters**

Name	Description	Value
checking interval in minutes	time frame to analyse approved transactions in minutes	Type: Int Default: 30

**Error codes**

#	Code	Name
10006	1004	Too many card holders from the same IP address

### Customer Email already used by another Cardholder

This check fires when the Customer Email has already been successfully used by a customer with a different Cardholder name. The time threshold is a moving window calculated backwards from the moment of the transaction. This check only cross-checks transactions within the same merchant account. Analyses Sale, Preauth or Transfer transactions in the Approved status.

Score: Yes

Enabled by default: N

#### Parameters

Name	Description	Value
checking interval in minutes	time frame to analyse approved transactions in minutes	Type: Int Default: 30

#### Error codes

#	Code	Name
10005	1003	Too many card holders for the same Email

### Source Credit Card Number approved transaction interval

This check fires when the interval for the last approved transaction associated with exact Source credit card number lesser the configured thresholds. The time threshold is time window calculated backwards from the moment of the transaction. The risk fires on the transaction below the set threshold. So, if you set a threshold of 10 minutes and the last approved transaction time is 10:00:00, it fires untill 10:10:01. Counts Sale, Preauth or Transfer transactions in the Approved status.

Score: Yes

Enabled by default: N

#### Parameters

Name	Description	Value
checking interval in minutes	time frame to analyse approved transactions in minutes	Type: Int Default: 30

continues on next page

Table 137 - continued from previous page

Name	Description	Value
for all merchant projects	Y - to check transactions for all projects of the current merchant, otherwise check transactions for current project only	Type: Enum Default: N

**Error codes**

#	Code	Name
10023	1033	Too many approved transactions for the same credit card number

**Source Credit Card Number declined transaction interval**

This check fires when the interval for the last declined transaction associated with exact Source credit card number lesser the configured thresholds. The time threshold is time window calculated backwards from the moment of the transaction. The risk fires on the transaction below the set threshold. So, if you set a threshold of 10 minutes and the last declined transaction time is 10:00:00, it fires until 10:10:01. Counts Account verification, Sale, Preauth or Transfer transactions in the Declined and Filtered status.

Score: Yes

Enabled by default: N

**Parameters**

Name	Description	Value
checking interval in minutes	time frame to analyse approved transactions in minutes	Type: Int Default: 30
for all merchant projects	Y - to check transactions for all projects of the current merchant, otherwise check transactions for current project only	Type: Enum Default: N

**Error codes**

#	Code	Name
10085	1095	Too many declined transactions for the same credit card number

### Source Credit Card Number Issuer Country change frequency for current Purpose

This check fires when the number of Countries, calculated for Source Credit Card number issuer, associated with exact Purpose exceeds the configured thresholds. The time threshold is a moving window calculated backwards from the moment of the transaction. The risk fires on the transaction after the set threshold. So, if you set a threshold of 2 Countries in 24 hours, it fires on the 3rd unique Country in 24 hours for the same Purpose. Counts unique Source Credit Card number issuer Countries for Sale, Preauth or Transfer transactions in Approved status for the current Merchant. Requests from IP addresses listed in "Merchant API IP address" are ignoring this check.

Score: Yes

Enabled by default: N

#### Parameters

Name	Description	Value
checking interval in hours	time frame to calculate countries count	Type: Int Default: 24
ignore BINs	requests for listed BINs are ignoring this check	Type: String Default: N/A
maximum countries count	maximum number of countries per one purpose allowed	Type: Int Default: 5

#### Error codes

#	Code	Name
10122	1132	Too many countries per account

### Reversal frequency

This check fires when the number or ratio of reversal transactions calculated for the whole merchant or for the exact merchant project exceeds the configured thresholds. Ratio is calculated for the full lifetime, absolute number could be limited for the whole lifetime or on daily basis from 00:00:00 till 23:59:59. The risk fires on the transaction after the set threshold. So, if you set a threshold of 5 reversals, it fires on the 6th one. Ratio calculation is based on transitions count, i.e. total reversal transactions count divided by total sale transactions count. Counts Sale and Capture transactions in Approved status and Reversal and Void transactions.

Score: No

Enabled by default: N

### Parameters

Name	Description	Value
absolute number	maximum allowable number of reversal transactions	Type: Int Default: 99999
daily absolute number	maximum allowable number of reversal transactions per day	Type: Int Default: 9999
for all merchant projects	Y - to check transactions for all projects of the current merchant, otherwise check transactions for current project only	Type: Enum Default: N
percentage ratio	maximum allowable ratio of reversal transactions calculated by transaction count in percent (from 0 to 100)	Type: Decimal Default: 101.000

### Error codes

#	Code	Name
10036	1046	Too high reversal ratio
10037	1047	Too many reversals
10038	1048	Too many reversals today

### Fingerprint usage frequency for last 24 hours (daily limit)

This check fires when the number or amount of transactions associated with exact Fingerprint exceeds the configured thresholds. The time threshold is a 24 hours window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 24 hours. Counts Sale, Preauth or Transfer transactions in the approved status.

Score: Yes

Enabled by default: N

### Parameters

Name	Description	Value
amount limit	maximum total transactions amount for the last 24 hours for this Fingerprint	Type: Decimal Default: 999999999
for all merchant projects	Y - to check transactions for all projects of the current merchant, otherwise check transactions for current project only	Type: Enum Default: Y

continues on next page

Table 145 - continued from previous page

Name	Description	Value
quantity limit	maximum total transactions count for the last 24 hours for this Fingerprint	Type: Int Default: 99999
subtract Cancel transactions	subtracts Cancelled transactions from the calculated count and amount thresholds	Type: Enum Default: N
use calendar days	"Y" For calculation using calendar days instead of calculation from moment when filter was enabled "N" for calculation from moment when filter was enabled	Type: Enum Default: N

**Error codes**

#	Code	Name
10170	1180	Daily amount limit exceeded for fingerprint
10171	1181	Daily quantity limit exceeded for fingerprint

**Fingerprint usage frequency for last 7 days (weekly limit)**

This check fires when the number or amount of transactions associated with exact Fingerprint exceeds the configured thresholds. The time threshold is a 7 days window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 168 hours. Counts Sale, Preauth or Transfer transactions in the approved status.

Score: Yes

Enabled by default: N

**Parameters**

Name	Description	Value
amount limit	maximum total transactions amount for the last 7 days for this Fingerprint	Type: Decimal Default: 99999999
calendar week starts from Sunday	"Y": calendar week starts from Sunday "N": calendar week starts from Monday	Type: Enum Default: N
for all merchant projects	Y - to check transactions for all projects of the current merchant, otherwise check transactions for current project only	Type: Enum Default: Y
quantity limit	maximum total transactions count for the last 7 days for this credit Fingerprint	Type: Int Default: 99999

continues on next page

Table 147 - continued from previous page

Name	Description	Value
subtract Cancel transactions	subtracts Cancelled transactions from the calculated count and amount thresholds	Type: Enum Default: N
use calendar days	“Y” For calculation using calendar days instead of calculation from moment when filter was enabled “N” for calculation from moment when filter was enabled	Type: Enum Default: N

**Error codes**

#	Code	Name
10172	1182	Weekly amount limit exceeded for fingerprint
10173	1183	Weekly quantity limit exceeded for fingerprint

**Fingerprint usage frequency for last month (monthly limit)**

This check fires when the number or amount of transactions associated with exact Fingerprint exceeds the configured thresholds. The time threshold is a one month window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in one month. Month calculation based on calendar i.e. 28th, 29th, 30th and 31st of March would be bumped to 28th of February during window calculation. Counts Sale, Preauth or Transfer transactions in the approved status.

Score: Yes

Enabled by default: N

**Parameters**

Name	Description	Value
amount limit	maximum total transactions amount for the last one month for this Fingerprint	Type: Decimal Default: 999999999
for all merchant projects	Y - to check transactions for all projects of the current merchant, otherwise check transactions for current project only	Type: Enum Default: Y
quantity limit	maximum total transactions count for the last one month for this credit Fingerprint	Type: Int Default: 99999
subtract Cancel transactions	subtracts Cancelled transactions from the calculated count and amount thresholds	Type: Enum Default: N

continues on next page

Table 149 - continued from previous page

Name	Description	Value
use calendar days	“Y” For calculation using calendar days instead of calculation from moment when filter was enabled “N” for calculation from moment when filter was enabled	Type: Enum Default: N

**Error codes**

#	Code	Name
10174	1184	Monthly amount limit exceeded for fingerprint
10175	1185	Monthly quantity limit exceeded for fingerprint

**Source Credit Card Number usage frequency for Fingerprint**

This check fires when the number of Source Credit Cards associated with exact Fingerprint exceeds the configured thresholds. The time threshold is a moving window calculated backwards from the moment of the transaction. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 Credit Cards in 6 hours, it fires on the 11th unique Credit Card in 6 hours. Counts unique Source Credit Card numbers for Account verification, Sale, Preauth or Transfer transactions in any status for the current Merchant.

Score: Yes

Enabled by default: N

**Parameters**

Name	Description	Value
checking interval in hours	time frame to calculate unique card number count	Type: Int Default: 12
maximum card count	maximum number of unique card numbers	Type: Int Default: 5

**Error codes**

#	Code	Name
10176	1186	Too many source credit cards used for the same fingerprint

### Source Credit Card number Issuer Country change frequency for current Device Fingerprint

This check fires when the number of Countries, calculated for Source Credit Card number issuer, associated with exact Fingerprint exceeds the configured thresholds. The time threshold is a moving window calculated backwards from the moment of the transaction. The risk fires on the transaction after the set threshold. So, if you set a threshold of 2 Countries in 24 hours, it fires on the 3rd unique Country in 24 hours for the same Purpose. Counts unique Source Credit Card number issuer Countries for Sale, Preauth or Transfer transactions in Approved status for the current Merchant. Requests from IP addresses listed in "Merchant API IP address" are ignoring this check.

Score: Yes

Enabled by default: N

#### Parameters

Name	Description	Value
checking interval in hours	time frame to calculate unique card number count	Type: Int Default: 24
maximum countries count	maximum number of countries for one fingerprint	Type: Int Default: 5

#### Error codes

#	Code	Name
10177	1187	Too many countries for the same fingerprint

### Destination Credit Card Number usage frequency for Device fingerprint

This check fires when the number of Destination Credit Cards associated with exact Device Fingerprint exceeds the configured thresholds. The time threshold is a moving window calculated backwards from the moment of the transaction. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 Credit Cards in 6 hours, it fires on the 11th unique Credit Card in 6 hours. Counts unique Destination Credit Card numbers for Transfer transactions in any status for the current Merchant.

Score: Yes

Enabled by default: N

#### Parameters

Name	Description	Value
checking interval in hours	time frame to calculate unique destination credit card numbers count	Type: Int Default: 12
maximum card count	maximum number of unique destination credit cards	Type: Int Default: 5

### Error codes

#	Code	Name
10178	1188	Too many destination credit cards used for the same fingerprint

### Destination Credit Card number Issuer Country change frequency for current Device fingerprint

This check fires when the number of Countries, calculated for Destination Credit Card number issuer, associated with exact Device Fingerprint exceeds the configured thresholds. The time threshold is a moving window calculated backwards from the moment of the transaction. The risk fires on the transaction after the set threshold. So, if you set a threshold of 2 Countries in 24 hours, it fires on the 3rd unique Country in 24 hours for the same Fingerprint. Counts unique Destination Credit Card number issuer Countries for Sale, Preauth or Transfer transactions in Approved status for the current Merchant. Requests from IP addresses listed in "Merchant API IP address" are ignoring this check.

Score: Yes

Enabled by default: N

### Parameters

Name	Description	Value
checking interval in hours	time frame to calculate unique card number count	Type: Int Default: 24
maximum countries count	maximum number of destination countries for one fingerprint	Type: Int Default: 5

### Error codes

#	Code	Name
10179	1189	Too many destination credit cards countries used for the same fingerprint

### Email usage frequency for Device fingerprint

This check fires when the number of email addresses associated with exact Device Fingerprint exceeds the configured thresholds. The time threshold is a moving window calculated backwards from the moment of the transaction. The risk fires on the transaction after the set threshold. So, if you set a threshold of 2 email addresses in 24 hours, it fires on the 3rd unique email address in 24 hours for the same Fingerprint. Counts unique email addresses for all types of transactions for the current Merchant.

Score: Yes

Enabled by default: N

#### Parameters

Name	Description	Value
checking interval in hours	time frame to calculate unique emails count	Type: Int Default: 24
maximum emails count	maximum number of emails for one fingerprint	Type: Int Default: 5

### Error codes

#	Code	Name
10180	1190	Too many emails used for the same fingerprint

### Purpose usage frequency for Device fingerprint

This check fires when the number of Purpose associated with exact Device Fingerprint exceeds the configured thresholds. The time threshold is a moving window calculated backwards from the moment of the transaction. The risk fires on the transaction after the set threshold. So, if you set a threshold of 2 Purpose in 24 hours, it fires on the 3rd unique Purpose in 24 hours for the same Fingerprint. Counts unique Purposes for all types of transactions for the current Merchant.

Score: Yes

Enabled by default: N

#### Parameters

Name	Description	Value
checking interval in hours	time frame to calculate unique purposes count	Type: Int Default: 24
maximum purposes count	maximum number of purposes for one fingerprint	Type: Int Default: 5

### Error codes

#	Code	Name
10181	1191	Too many purposes used for the same fingerprint

### Account Number usage frequency for last 24 hours (daily limit)

This check fires when the number or amount of transactions associated with exact Account number exceeds the configured thresholds. The time threshold is a 24 hours window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 24 hours. Counts Sale, Preauth, Payout or Transfer transactions in the approved status.

Score: No

Enabled by default: N

### Parameters

Name	Description	Value
amount limit	maximum total transactions amount for the last 24 hours for this account number	Type: Decimal Default: 999999999
for all merchant projects	current total transactions amount or count for the last 24 hours for this credit card value would be calculated - Y: for all projects - 3D: for 3D gates only - Non3D: for non 3D gates only - N: for current project only of the current merchant and converted to current project currency to compare with amount or quantity limit values	Type: Enum Default: Y
quantity limit	maximum total transactions count for the last 24 hours for this account number	Type: Int Default: 99999999

continues on next page

Table 163 - continued from previous page

Name	Description	Value
skip payouts	ignore payouts	Type: Enum Default: N
subtract Cancel transactions	ignore cancel transactions for two-stage payments	Type: Enum Default: N
use calendar day	"Y" For calculation using calendar days instead of calculation from moment when filter was enabled "N" for calculation from moment when filter was enabled	Type: Enum Default: N

**Error codes**

#	Code	Name
10187	1197	Daily amount limit exceeded for account number address
10188	1198	Daily quantity limit exceeded for account number address

**Account Number usage frequency for last 7 days (weekly limit)**

This check fires when the number or amount of transactions associated with exact Account number exceeds the configured thresholds. The time threshold is a 7 days window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 168 hours. Counts Sale, Preauth, Payout or Transfer transactions in the approved status.

Score: No

Enabled by default: N

**Parameters**

Name	Description	Value
amount limit	maximum total transactions amount for the last 7 days for this account number	Type: Decimal Default: 999999999
calendar week starts from Sunday	"Y": calendar week starts from Sunday, "N": calendar week starts from Monday	Type: Enum Default: N

continues on next page

Table 165 - continued from previous page

Name	Description	Value
for all merchant projects	current total transactions amount or count for the last 7 days for this credit card value would be calculated - Y: for all projects - 3D: for 3D gates only - Non3D: for non 3D gates only - N: for current project only of the current merchant and converted to current project currency to compare with amount or quantity limit values	Type: Enum Default: Y
quantity limit	maximum total transactions count for the last 7 days for this account number calculated	Type: Int Default: 99999999
skip payouts	ignore payouts	Type: Enum Default: N
subtract Cancel transactions	ignore cancel transactions for two-stage payments	Type: Enum Default: N
use calendar week	"Y" For calculation using calendar week instead of calculation from moment when filter was enabled "N" for calculation from moment when filter was enabled	Type: Enum Default: N

### Error codes

#	Code	Name
10189	1199	Weekly amount limit exceeded for account number address
10190	1200	Weekly quantity limit exceeded for account number address

### Account Number usage frequency for last month (monthly limit)

This check fires when the number or amount of transactions associated with exact Account number exceeds the configured thresholds. The time threshold is a one month window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in one month. Month calculation based on calendar i.e. 28th, 29th, 30th and 31st of March would be bumped to 28th of February during window calculation. Counts Sale, Preauth, Payout or Transfer transactions in the approved status.

Score: No

Enabled by default: N

### Parameters

Name	Description	Value
amount limit	maximum total transactions amount for the last one month for this account number	Type: Decimal Default: 999999999
for all merchant projects	current total transactions amount or count for the last one month for this credit card value would be calculated - Y: for all projects - 3D: for 3D gates only - Non3D: for non 3D gates only - N: for current project only of the current merchant and converted to current project currency to compare with amount or quantity limit values	Type: Enum Default: Y
quantity limit	maximum total transactions count for the last one month for this account number	Type: Int Default: 999999999
skip payouts	ignore payouts	Type: Enum Default: N
subtract Cancel transactions	ignore cancel transactions for two-stage payments	Type: Enum Default: N
use calendar month	“Y” For calculation using calendar month instead of calculation from moment when filter was enabled “N” for calculation from moment when filter was enabled	Type: Enum Default: N

### Error codes

#	Code	Name
10191	1201	Monthly amount limit exceeded for account number address
10192	1202	Monthly quantity limit exceeded for account number address

### Preventing transaction with the same amount

This check fires when more than one transaction is made with same amount in a time threshold (in seconds). The maximum time threshold is a 300 seconds window, calculated backwards from the moment of the first transaction. The risk fires on the second transaction with the same amount during set time threshold. Counts Sale, Preauth, Payouts or Transfer transactions.

Score: Yes

Enabled by default: N

### Parameters

Name	Description	Value
checking interval in seconds	max interval in seconds to check requests with the same amount, values more then 300 seconds or less 10 seconds are ignored	Type: int Default: 60
skip declined transactions	Y - to skip sessions in Filtered or Declined status, N - otherwise	Type: Enum Default: N

### Error codes

#	Code	Name
10198	1208	Such transaction amount has already been processed in the set threshold of time

### Issuer country usage frequency

This check fires when the number of transactions associated with the same card issuer country exceeds the configured thresholds. The maximum time threshold is a 300 seconds window, calculated backwards from the moment of the first transaction. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 300 seconds. Counts Sale, Preauth, Payouts or Transfer transactions.

Score: Yes

Enabled by default: N

### Parameters

Name	Description	Value
Checking interval in seconds	max interval in seconds to check transactions associated with the same card issuer country, values more then 300 seconds or less 10 seconds are ignored	Type: int Default: 60
Quantity limit	pick a value for the number of transactions over which the filter will be fired	Type: int Default: 10
Skip country identifier	choose the countries where the filter will be applied	Type: List Default: *

continues on next page

Table 171 - continued from previous page

Name	Description	Value
Skip declined transactions	Y - to skip sessions in Filtered or Declined status, N - otherwise	Type: Enum Default: N

**Error codes**

#	Code	Name
10199	1209	Exceeding the limit of cards issued in the same country

**Purpose usage frequency for last year (annual limit)**

This check fires when the number or amount of transactions associated with exact Purpose exceeds the configured thresholds. The time threshold is a one year window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 100 transactions, it fires on the 101th transaction in one year. Calculation of the year can be started from the beginning of the calendar year or from the filter activation truncated to the month and -12 months. I.e. if you activated the filter on May 15, 2021, the filter will consider transactions from May 2020. Counts Sale, Preauth or Transfer transactions in the approved status.

Score: Yes

Enabled by default: N

**Parameters**

Name	Description	Value
amount limit	maximum total transactions amount for the last year for this Purpose	Type: int Default: 999999999
for all merchant projects	current total transactions amount or count for the last year for this Purpose value would be calculated. - Y: for all projects. - 3D: for 3D gates only. - Non3D: for non 3D gates only. N: for current project only of the current merchant and converted to current project currency to compare with amount or quantity limit values	Type: Enum Default: Y
quantity limit	maximum total transactions count for the last year for this Purpose	Type: int Default: 99999

continues on next page

Table 173 - continued from previous page

Name	Description	Value
subtract Cancel transactions	*	Type: Enum Default: N
use calendar year	*	Type: Enum Default: N

### Error codes

#	Code	Name
10200	1210	Annual amount limit exceeded for purpose
10201	1211	Annual quantity limit exceeded for purpose

### BIN range usage frequency

This check fires when the number of transactions associated with the specific card BIN range exceeds the configured thresholds. The maximum time threshold is a 300 seconds window, calculated backwards from the moment of the first transaction. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 300 seconds. Counts Sale, Preauth, Payouts or Transfer transactions.

Score: Yes

Enabled by default: N

### Parameters

Name	Description	Value
BIN range exceptions	card BIN range list for which checks will not be performed	Type: * Default: *
checking interval in seconds	max interval in seconds to check transactions associated with the same card issuer country, values more then 300 seconds or less 10 seconds are ignored	Type: int Default: 60
quantity limit	pick a value for the number of transactions over which the filter will be fired	Type: int Default: 10
skip declined transactions	Y - to skip sessions in Filtered or Declined status, N - otherwise	Type: Enum Default: N

**Error codes**

#	Code	Name
10202	1212	Exceeding the limit of cards associated with the same card BIN range

**Abnormal transaction time**

This check fires when transactions are received outside the set time period. So, if you set the time period from 10:00 to 20:00, it fires on any transaction from 0:00 to 9:59 and from 20:00 to 0:00. The time is set in the GMT+3 time zone. Counts Sale, Preauth, Payouts or Transfer transactions.

Score: Yes

Enabled by default: N

**Parameters**

Name	Value
Time period from	Type: String Default: 10:00
Time period to	Type: String Default: 19:00
Time zone	Type: Int Default: 3

**Error codes**

#	Code	Name
10203	1213	Transaction in abnormal time
10204	1214	Customer data validation failed (first name, last name, cardholder, email, phone)

**Source Credit Card Number decline frequency for last week (weekly decline limit)**

This check fires when the number or amount of declined transactions associated with exact Source credit card number exceeds the configured thresholds. The time threshold is a 7 days window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 168 hours. Counts Account verification, Sale, Preauth or Transfer transactions in the Declined status.

Score: Yes

Enabled by default: N

### Parameters

Name	Description	Value
amount limit	maximum total transactions amount for the last 7 days for this credit card used as Source card	Type: Decimal Default: 999999999
calendar week starts from Sunday	"Y": calendar week starts from Sunday "N": calendar week starts from Monday	Type: Enum Default: N
for all merchant projects	current total transactions amount or count for the last 7 days for this credit card would be calculated - Y: for all projects - 3D: for 3D gates only - Non3D: for non 3D gates only - N: for current project only of the current merchant and converted to current project currency to compare with amount limit values	Type: Enum Default: N
quantity limit	maximum total transactions count for the last 7 days for this credit card used as Source card	Type: Int Default: 99999
use calendar week	"Y" For calculation using calendar week instead of calculation from moment when filter was enabled "N" for calculation from moment when filter was enabled	Type: Enum Default: N

### Error codes

#	Code	Name
10206	1216	Weekly decline amount limit exceeded for sender
10207	1217	Weekly decline quantity limit exceeded for sender

### Source Credit Card Number usage frequency per Email address for last 24 hours (daily limit)

This check fires when the number of Source Credit Cards associated with exact Email address exceeds the configured thresholds. The time threshold is a moving window calculated backwards from the moment of the transaction. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 Credit Cards, it fires on the 11th unique Credit Card in 24 hours. Counts unique Source Credit Card numbers for Sale or Preauth transactions in any status for the current Merchant.

Score: Yes

Enabled by default: N

### Parameters

Name	Description	Value
approved only	counts unique Source Credit Card numbers for Sale or Preauth transactions in approved status	Type: Enum Default: N
maximum card number count	maximum total card number count for the last 24 hours for this Email address	Type: Int Default: 99999
use calendar day	“Y” For calculation using calendar days instead of calculation from moment when filter was enabled “N” for calculation from moment when filter was enabled	Type: Enum Default: N

### Error codes

#	Code	Name
10208	1218	Daily card number count limit exceeded for email address

### Source Credit Card Number usage frequency per Email address for last 7 days (weekly limit)

This check fires when the number of Source Credit Cards associated with exact Email address exceeds the configured thresholds. The time threshold is a moving window calculated backwards from the moment of the transaction. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 Credit Cards, it fires on the 11th unique Credit Card in 7 days. Counts unique Source Credit Card numbers for Sale or Preauth transactions in any status for the current Merchant.

Score: Yes

Enabled by default: N

### Parameters

Name	Description	Value
approved only	counts unique Source Credit Card numbers for Sale or Preauth transactions in approved status	Type: Enum Default: N
calendar week starts from Sunday	“Y”: calendar week starts from Sunday, “N”: calendar week starts from Monday	Type: Enum Default: N
maximum card number count	maximum total card number count for the last 7 days for this Email address	Type: Int Default: 99999
use calendar week	“Y” For calculation using calendar week instead of calculation from moment when filter was enabled “N” for calculation from moment when filter was enabled	Type: Enum Default: N

### Error codes

#	Code	Name
10209	1219	Weekly card number count limit exceeded for email address

### Source Credit Card Number usage frequency per Email address for last month (monthly limit)

This check fires when the number of Source Credit Cards associated with exact Email address exceeds the configured thresholds. The time threshold is a moving window calculated backwards from the moment of the transaction. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 Credit Cards, it fires on the 11th unique Credit Card in 1 month. Counts unique Source Credit Card numbers for Sale or Preauth transactions in any status for the current Merchant.

Score: Yes

Enabled by default: N

#### Parameters

Name	Description	Value
approved only	counts unique Source Credit Card numbers for Sale or Preauth transactions in approved status	Type: Enum Default: N
maximum card number count	maximum total card number count for the last month for this Email address	Type: Int Default: 99999
use calendar month	"Y" For calculation using calendar month instead of calculation from moment when filter was enabled "N" for calculation from moment when filter was enabled	Type: Enum Default: N

#### Error codes

#	Code	Name
10210	1220	Monthly card number count limit exceeded for email address

### Source Credit Card Number usage frequency for last N days

This check fires when the number or amount of transactions associated with exact Source credit card number exceeds the configured thresholds. The time threshold is a N days window calculated backwards from the moment of the transaction. The N parameter (date period) can be set from 1 to 30. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in N days. Counts Sale, Preauth or Transfer transactions in the approved status.

Score: Yes

Enabled by default: N

#### Parameters

Name	Description	Value
amount limit	maximum total transactions amount for the last N days for this credit card used as Source card	Type: Decimal Default: 999999999
for all merchant projects	current total transactions amount or count for the last N days for this credit card value would be calculated - Y: for all projects - 3D: for 3D gates only - Non3D: for non 3D gates only - N: for current project only of the current merchant and converted to current project currency to compare with amount limit values	Type: Enum Default: N
for last N days	date period can be set from 1 to 30 days	Type: Int Default: 1
quantity limit	maximum total transactions count for the last N days for this credit card used as Source card	Type: Int Default: 99999
subtract Cancel transactions	ignore cancel transactions for two-stage payments	Type: Enum Default: N

### Error codes

#	Code	Name
10211	1221	Specified period amount limit exceeded for sender
10212	1222	Specified period quantity limit exceeded for sender

### Destination Credit Card Number usage frequency for last N days

This check fires when the number or amount of transactions associated with exact Destination credit card number exceeds the configured thresholds. The time threshold is a N days window calculated backwards from the moment of the transaction. The N parameter (date period) can be set from 1 to 30. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in N days. Counts Transfer transactions in the approved status.

Score: Yes

Enabled by default: N

### Parameters

Name	Description	Value
amount limit	maximum total transactions amount for the last N days for this credit card used as Destination card	Type: Decimal Default: 999999999
for all merchant projects	current total transactions amount or count for the last N days for this Destination card value would be calculated - Y: for all projects - 3D: for 3D gates only - Non3D: for non 3D gates only - N: for current project only of the current merchant and converted to current project currency to compare with amount limit values	Type: Enum Default: N
for last N days	date period can be set from 1 to 30 days	Type: Int Default: 1
quantity limit	maximum total transactions count for the last N days for this credit card used as Destination card	Type: Int Default: 99999
subtract Cancel transactions	ignore cancel transactions for two-stage payments	Type: Enum Default: N

### Error codes

#	Code	Name
10213	1223	Specified period amount limit exceeded for recipient
10214	1224	Specified period quantity limit exceeded for recipient

### Total Credit Card Number usage frequency for last N days

This check fires when the number or amount of transactions associated with exact credit card number used as Source or Destination exceeds the configured thresholds. The time threshold is a N days window calculated backwards from the moment of the transaction. The N parameter (date period) can be set from 1 to 30. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in N days. Counts Sale, Preauth or Transfer transactions in the approved status.

Score: Yes

Enabled by default: N

### Parameters

Name	Description	Value
amount limit	maximum total transactions amount for the last N days for this credit card used as Source or Destination card	Type: Decimal Default: 999999999
for all merchant projects	current total transactions amount or count for the last N days for this credit card value would be calculated - Y: for all projects - 3D: for 3D gates only - Non3D: for non 3D gates only - N: for current project only of the current merchant and converted to current project currency to compare with amount limit values	Type: Enum Default: N
for last N days	date period can be set from 1 to 30 days	Type: Int Default: 1
quantity limit	maximum total transactions count for the last N days for this credit card used as Source or Destination card	Type: Int Default: 99999
subtract Cancel transactions	ignore cancel transactions for two-stage payments	Type: Enum Default: N

### Error codes

#	Code	Name
10215	1225	Specified period total amount limit exceeded for sender
10216	1226	Specified period total quantity limit exceeded for sender
10217	1227	Specified period total amount limit exceeded for recipient
10218	1228	Specified period total quantity limit exceeded for recipient

### Purpose usage frequency for last N days

This check fires when the number or amount of transactions associated with exact Purpose exceeds the configured thresholds. The time threshold is a N days window calculated backwards from the moment of the transaction. The N parameter (date period) can be set from 1 to 30. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in N days. Counts Sale, Preauth or Transfer transactions in the approved status.

Score: Yes

Enabled by default: N

### Parameters

Name	Description	Value
amount limit	maximum total transactions amount for the last N days for this Purpose	Type: Decimal Default: 999999999
for all merchant projects	current total transactions amount or count for the last N days for this Purpose would be calculated - Y: for all projects - 3D: for 3D gates only - Non3D: for non 3D gates only - N: for current project only of the current merchant and converted to current project currency to compare with amount limit values	Type: Enum Default: N
for last N days	date period can be set from 1 to 30 days	Type: Int Default: 1
quantity limit	maximum total transactions count for the last N days for this Purpose	Type: Int Default: 99999
subtract Cancel transactions	ignore cancel transactions for two-stage payments	Type: Enum Default: N

### Error codes

#	Code	Name
10219	1229	Specified period amount limit exceeded for purpose
10220	1230	Specified period quantity limit exceeded for purpose

### Email usage frequency for last N days

This check fires when the number or amount of transactions associated with exact Email exceeds the configured thresholds. The time threshold is a N days window calculated backwards from the moment of the transaction. The N parameter (date period) can be set from 1 to 30. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in N days. Counts Sale, Preauth or Transfer transactions in the approved status.

Score: Yes

Enabled by default: N

### Parameters

Name	Description	Value
amount limit	maximum total transactions amount for the last N days for this Email	Type: Decimal Default: 999999999
for all merchant projects	current total transactions amount or count for the last N days for this Email would be calculated - Y: for all projects - 3D: for 3D gates only - Non3D: for non 3D gates only - N: for current project only of the current merchant and converted to current project currency to compare with amount limit values	Type: Enum Default: N
for last N days	date period can be set from 1 to 30 days	Type: Int Default: 1
quantity limit	maximum total transactions count for the last N days for this Email	Type: Int Default: 99999
subtract Cancel transactions	ignore cancel transactions for two-stage payments	Type: Enum Default: N

### Error codes

#	Code	Name
10221	1231	Specified period amount limit exceeded for email address
10222	1232	Specified period quantity limit exceeded for email address

### IP address usage frequency for last N days

This check fires when the number or amount of transactions associated with exact IP address exceeds the configured thresholds. The time threshold is a N days window calculated backwards from the moment of the transaction. The N parameter (date period) can be set from 1 to 30. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in N days. Counts Sale, Preauth or Transfer transactions in the approved status.

Score: Yes

Enabled by default: N

### Parameters

Name	Description	Value
amount limit	maximum total transactions amount for the last N days for this IP address	Type: Decimal Default: 999999999

continues on next page

Table 197 - continued from previous page

Name	Description	Value
for all merchant projects	current total transactions amount or count for the last N days for this IP address would be calculated - Y: for all projects - 3D: for 3D gates only - Non3D: for non 3D gates only - N: for current project only of the current merchant and converted to current project currency to compare with amount limit values	Type: Enum Default: N
for last N days	date period can be set from 1 to 30 days	Type: Int Default: 1
quantity limit	maximum total transactions count for the last N days for this IP address	Type: Int Default: 99999
subtract Cancel transactions	ignore cancel transactions for two-stage payments	Type: Enum Default: N

**Error codes**

#	Code	Name
10223	1233	Specified period amount limit exceeded for IP address
10224	1234	Specified period quantity limit exceeded for IP address

**Fingerprint usage frequency for last N days**

This check fires when the number or amount of transactions associated with exact Fingerprint exceeds the configured thresholds. The time threshold is a N days window calculated backwards from the moment of the transaction. The N parameter (date period) can be set from 1 to 30. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in N days. Counts Sale, Preauth or Transfer transactions in the approved status.

Score: Yes

Enabled by default: N

**Parameters**

Name	Description	Value
amount limit	maximum total transactions amount for the last N days for this Fingerprint	Type: Decimal Default: 999999999

continues on next page

Table 199 - continued from previous page

Name	Description	Value
for all merchant projects	current total transactions amount or count for the last N days for this Fingerprint would be calculated - Y: for all projects - 3D: for 3D gates only - Non3D: for non 3D gates only - N: for current project only of the current merchant and converted to current project currency to compare with amount limit values	Type: Enum Default: N
for last N days	date period can be set from 1 to 30 days	Type: Int Default: 1
quantity limit	maximum total transactions count for the last N days for this Fingerprint	Type: Int Default: 99999
subtract Cancel transactions	ignore cancel transactions for two-stage payments	Type: Enum Default: N

**Error codes**

#	Code	Name
10225	1235	Specified period amount limit exceeded for fingerprint
10226	1236	Specified period quantity limit exceeded for fingerprint

**Account Number usage frequency for last N days**

This check fires when the number or amount of transactions associated with exact Account Number exceeds the configured thresholds. The time threshold is a N days window calculated backwards from the moment of the transaction. The N parameter (date period) can be set from 1 to 30. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in N days. Counts Sale, Preauth, Payout or Transfer transactions in the approved status.

Score: Yes

Enabled by default: N

**Parameters**

Name	Description	Value
amount limit	maximum total transactions amount for the last N days for this Account Number	Type: Decimal Default: 999999999

continues on next page

Table 201 - continued from previous page

Name	Description	Value
for all merchant projects	current total transactions amount or count for the last N days for this Account Number would be calculated Y: for all projects - 3D: for 3D gates only - Non3D: for non 3D gates only - N: for current project only of the current merchant and converted to current project currency to compare with amount limit values	Type: Enum Default: N
for last N days	date period can be set from 1 to 30 days	Type: Int Default: 1
quantity limit	maximum total transactions count for the last N days for this Account Number	Type: Int Default: 99999
subtract Cancel transactions	ignore cancel transactions for two-stage payments	Type: Enum Default: N

**Error codes**

#	Code	Name
10227	1237	Specified period amount limit exceeded for account number
10228	1238	Specified period quantity limit exceeded for account number

**Source Credit Card Number decline frequency for last month (monthly decline limit)**

This check fires when the number or amount of declined transactions associated with exact Source credit card number exceeds the configured thresholds. The time threshold is a one month window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in one month. Month calculation based on calendar i.e. 28th, 29th, 30th and 31st of March would be bumped to 28th of February during window calculation. Counts Account verification, Sale, Preauth or Transfer transactions in the Declined status.

Score: Yes

Enabled by default: N

**Parameters**

Name	Description	Value
amount limit	maximum total transactions amount for the last month for this credit card used as Source card	Type: Decimal Default: 999999999

continues on next page

Table 203 - continued from previous page

Name	Description	Value
for all merchant projects	current total transactions amount or count for the last month for this credit card would be calculated - Y: for all projects - 3D: for 3D gates only - Non3D: for non 3D gates only - N: for current project only of the current merchant and converted to current project currency to compare with amount limit values	Type: Enum Default: N
quantity limit	maximum total transactions count for the last month for this credit card used as Source card	Type: Int Default: 99999
use calendar month	"Y" For calculation using calendar month instead of calculation from moment when filter was enabled "N" for calculation from moment when filter was enabled	Type: Enum Default: N

**Error codes**

#	Code	Name
10229	1239	Monthly decline amount limit exceeded for sender
10230	1240	Monthly decline quantity limit exceeded for sender

**Destination Credit Card Number decline frequency for last 24 hours (daily decline limit)**

This check fires when the number or amount of declined transactions associated with exact Destination credit card number exceeds the configured thresholds. The time threshold is a 24 hours window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 24 hours. Counts Transfer transactions in the Declined status.

Score: Yes

Enabled by default: N

**Parameters**

Name	Description	Value
amount limit	maximum total transactions amount for the last 24 hours for this credit card used as Destination card	Type: Decimal Default: 999999999

continues on next page

Table 205 - continued from previous page

Name	Description	Value
for all merchant projects	current total transactions amount or count for the last day for this credit card would be calculated - Y: for all projects - 3D: for 3D gates only - Non3D: for non 3D gates only - N: for current project only of the current merchant and converted to current project currency to compare with amount limit values	Type: Enum Default: N
quantity limit	maximum total transactions count for the last day for this credit card used as Destination card	Type: Int Default: 99999
use calendar day	"Y" For calculation using calendar day instead of calculation from moment when filter was enabled "N" for calculation from moment when filter was enabled	Type: Enum Default: N

**Error codes**

#	Code	Name
10231	1241	Daily decline amount limit exceeded for recipient
10232	1242	Daily decline quantity limit exceeded for recipient

**Destination Credit Card Number decline frequency for last week (weekly decline limit)**

This check fires when the number or amount of declined transactions associated with exact Destination credit card number exceeds the configured thresholds. The time threshold is a 7 days window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 168 hours. Counts Transfer transactions in the Declined status.

Score: Yes

Enabled by default: N

**Parameters**

Name	Description	Value
amount limit	maximum total transactions amount for the last week for this credit card used as Destination card	Type: Decimal Default: 999999999
calendar week starts from Sunday	"Y": calendar week starts from Sunday "N": calendar week starts from Monday	Type: Enum Default: N

continues on next page

Table 207 - continued from previous page

Name	Description	Value
for all merchant projects	current total transactions amount or count for the last week for this credit card would be calculated - Y: for all projects - 3D: for 3D gates only - Non3D: for non 3D gates only - N: for current project only of the current merchant and converted to current project currency to compare with amount limit values	Type: Enum Default: N
quantity limit	maximum total transactions count for the last week for this credit card used as Destination card	Type: Int Default: 99999
use calendar week	"Y" For calculation using calendar week instead of calculation from moment when filter was enabled "N" for calculation from moment when filter was enabled	Type: Enum Default: N

### Error codes

#	Code	Name
10233	1243	Weekly decline amount limit exceeded for recipient
10234	1244	Weekly decline quantity limit exceeded for recipient

### Destination Credit Card Number decline frequency for last month (monthly decline limit)

This check fires when the number or amount of declined transactions associated with exact Destination credit card number exceeds the configured thresholds. The time threshold is a one month window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in one month. Month calculation based on calendar i.e. 28th, 29th, 30th and 31st of March would be bumped to 28th of February during window calculation. Counts Transfer transactions in the Declined status.

Score: Yes

Enabled by default: N

### Parameters

Name	Description	Value
amount limit	maximum total transactions amount for the last month for this credit card used as Destination card	Type: Decimal Default: 999999999

continues on next page

Table 209 - continued from previous page

Name	Description	Value
for all merchant projects	current total transactions amount or count for the last month for this credit card would be calculated - Y: for all projects - 3D: for 3D gates only - Non3D: for non 3D gates only - N: for current project only of the current merchant and converted to current project currency to compare with amount limit values	Type: Enum Default: N
quantity limit	maximum total transactions count for the last month for this credit card used as Destination card	Type: Int Default: 99999
use calendar month	"Y" For calculation using calendar month instead of calculation from moment when filter was enabled "N" for calculation from moment when filter was enabled	Type: Enum Default: N

**Error codes**

#	Code	Name
10235	1245	Monthly decline amount limit exceeded for recipient
10236	1246	Monthly decline quantity limit exceeded for recipient

**Total Credit Card Number decline frequency for last 24 hours (daily decline limit)**

This check fires when the number or amount of declined transactions associated with exact Source or Destination credit card number exceeds the configured thresholds. The time threshold is a 24 hours window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 24 hours. Counts Account verification, Sale, Preauth or Transfer transactions in the Declined status.

Score: Yes

Enabled by default: N

**Parameters**

Name	Description	Value
amount limit	maximum total transactions amount for the last 24 hours for this credit card	Type: Decimal Default: 999999999

continues on next page

Table 211 - continued from previous page

Name	Description	Value
for all merchant projects	current total transactions amount or count for the last day for this credit card would be calculated - Y: for all projects - 3D: for 3D gates only - Non3D: for non 3D gates only - N: for current project only of the current merchant and converted to current project currency to compare with amount limit values	Type: Enum Default: N
quantity limit	maximum total transactions count for the last day for this credit card	Type: Int Default: 99999
use calendar day	"Y" For calculation using calendar day instead of calculation from moment when filter was enabled "N" for calculation from moment when filter was enabled	Type: Enum Default: N

**Error codes**

#	Code	Name
10237	1247	Daily decline total amount limit exceeded for sender
10238	1248	Daily decline total quantity limit exceeded for sender
10239	1249	Daily decline total amount limit exceeded for recipient
10240	1250	Daily decline total quantity limit exceeded for recipient

**Total Credit Card Number decline frequency for last week (weekly decline limit)**

This check fires when the number or amount of declined transactions associated with exact Source or Destination credit card number exceeds the configured thresholds. The time threshold is a 7 days window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 168 hours. Counts Account verification, Sale, Preauth or Transfer transactions in the Declined status.

Score: Yes

Enabled by default: N

**Parameters**

Name	Description	Value
amount limit	maximum total transactions amount for the last week for this credit card	Type: Decimal Default: 999999999
calendar week starts from Sunday	"Y": calendar week starts from Sunday "N": calendar week starts from Monday	Type: Enum Default: N

continues on next page

Table 213 - continued from previous page

Name	Description	Value
for all merchant projects	current total transactions amount or count for the last week for this credit card would be calculated - Y: for all projects - 3D: for 3D gates only - Non3D: for non 3D gates only - N: for current project only of the current merchant and converted to current project currency to compare with amount limit values	Type: Enum Default: N
quantity limit	maximum total transactions count for the last week for this credit card	Type: Int Default: 99999
use calendar week	"Y" For calculation using calendar week instead of calculation from moment when filter was enabled "N" for calculation from moment when filter was enabled	Type: Enum Default: N

**Error codes**

#	Code	Name
10241	1251	Weekly decline total amount limit exceeded for sender
10242	1252	Weekly decline total quantity limit exceeded for sender
10243	1253	Weekly decline total amount limit exceeded for recipient
10244	1254	Weekly decline total quantity limit exceeded for recipient

**Total Credit Card Number decline frequency for last month (monthly decline limit)**

This check fires when the number or amount of declined transactions associated with exact Source or Destination credit card number exceeds the configured thresholds. The time threshold is a one month window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in one month. Month calculation based on calendar i.e. 28th, 29th, 30th and 31st of March would be bumped to 28th of February during window calculation. Counts Account verification, Sale, Preauth or Transfer transactions in the Declined status.

Score: Yes

Enabled by default: N

**Parameters**

Name	Description	Value
amount limit	maximum total transactions amount for the last month for this credit card	Type: Decimal Default: 999999999

continues on next page

Table 215 - continued from previous page

Name	Description	Value
for all merchant projects	current total transactions amount or count for the last month for this credit card would be calculated - Y: for all projects - 3D: for 3D gates only - Non3D: for non 3D gates only - N: for current project only of the current merchant and converted to current project currency to compare with amount limit values	Type: Enum Default: N
quantity limit	maximum total transactions count for the last month for this credit card	Type: Int Default: 99999
use calendar month	"Y" For calculation using calendar month instead of calculation from moment when filter was enabled "N" for calculation from moment when filter was enabled	Type: Enum Default: N

**Error codes**

#	Code	Name
10245	1255	Monthly decline total amount limit exceeded for sender
10246	1256	Monthly decline total quantity limit exceeded for sender
10247	1257	Monthly decline total amount limit exceeded for recipient
10248	1258	Monthly decline total quantity limit exceeded for recipient

**Customer IP address anonymous VPN**

This check fires when customer IP address is considered as anonymous VPN by MaxMind service. Counts Sale, Preauth or Transfer transactions.

Score: Yes

Enabled by default: N

**Parameters**

Name	Description	Value
filter parameter value	Y - to filter if condition is true, N - to filter if condition is false	Type: Enum Default: Y

**Error codes**

#	Code	Name
10250	1260	Customer IP address is anonymous VPN

### Customer IP address anonymous

This check fires when customer IP address is considered as anonymous by MaxMind service. Counts Sale, Preauth or Transfer transactions.

Score: Yes

Enabled by default: N

#### Parameters

Name	Description	Value
filter parameter value	Y - to filter if condition is true, N - to filter if condition is false	Type: Enum Default: Y

#### Error codes

#	Code	Name
10251	1261	Customer IP address is anonymous

### Customer IP Hosting Provider

This check fires when customer IP address belongs to a hosting or VPN provider considered by MaxMind service. Counts Sale, Preauth or Transfer transactions.

Score: Yes

Enabled by default: N

#### Parameters

Name	Description	Value
filter parameter value	Y - to filter if condition is true, N - to filter if condition is false	Type: Enum Default: Y

#### Error codes

#	Code	Name
10252	1262	Customer ip address is hosting provider

### Customer IP Public Proxy

This check fires when customer IP address belongs to a public proxy considered by MaxMind service. Counts Sale, Preauth or Transfer transactions.

Score: Yes

Enabled by default: N

#### Parameters

Name	Description	Value
filter parameter value	Y - to filter if condition is true, N - to filter if condition is false	Type: Enum Default: Y

**Error codes**

#	Code	Name
10253	1263	Customer IP address is public proxy

**Customer IP Residential Proxy**

This check fires when customer IP address belongs to a hosting or VPN provider considered by MaxMind service. Counts Sale, Preauth or Transfer transactions.

Score: Yes

Enabled by default: N

**Parameters**

Name	Description	Value
filter parameter value	Y - to filter if condition is true, N - to filter if condition is false	Type: Enum Default: Y

**Error codes**

#	Code	Name
10254	1264	Customer IP address is residential proxy

**Customer IP Tor Exit Node**

This check fires when customer IP address is a Tor exit node considered by MaxMind service. Counts Sale, Preauth or Transfer transactions.

Score: Yes

Enabled by default: N

**Parameters**

Name	Description	Value
filter parameter value	Y - to filter if condition is true, N - to filter if condition is false	Type: Enum Default: Y

**Error codes**

#	Code	Name
10255	1265	Customer IP address is tor exit node

### Customer static IP score

This check fires when customer IP address static IP score which is considered by MaxMind service is lower or equal to the settled threshold value. Higher values meaning a greater static association. For example, many IP addresses with a user type of cellular have a score under one. Broadband IPs that don't change very often typically have a score above thirty. This indicator can be useful for deciding whether an IP address represents the same user over time. The value ranges from 0 to 99.99. Counts Sale, Preauth or Transfer transactions.

Score: Yes

Enabled by default: N

#### Parameters

Name	Description	Value
filter threshold value	Lower or equal values will be filtered out	Type: Decimal Default: 20.000

### Error codes

#	Code	Name
10256	1266	Customer IP address static IP score is less or equal to configured threshold

### Customer IP user count

This check fires when customer IP address user count considered by MaxMind service is higher or equal to the settled threshold value. The estimated number of users sharing the IP/network during the past 24 hours. For IPv4, the count is for the individual IP. For IPv6, the count is for the /64 network. Counts Sale, Preauth or Transfer transactions.

Score: Yes

Enabled by default: N

#### Parameters

Name	Description	Value
filter threshold value	Higher or equal values will be filtered out	Type: Int Default: 3

### Error codes

#	Code	Name
10257	1267	Customer IP address user count is higher or equal to configured threshold

### Customer IP user type

This check fires when customer IP address user type considered by MaxMind service is in blocked user types list. Possible values: business, cafe, cellular, college, consumer\_privacy\_network, content\_delivery\_network, government, hosting, library, military, residential, router, school, search\_engine\_spider, traveler. Counts Sale, Preauth or Transfer transactions.

Score: Yes

Enabled by default: N

#### Parameters

Name	Description	Value
blocked user types	Blocked user types will be filtered out, split values with comma	Type: String Default: None

### Error codes

#	Code	Name
10258	1268	Customer IP address user type is in blocked user types list

### Credit Card Number usage frequency for last N hours

This check fires when the number of transactions associated with exact credit card number exceeds the configured thresholds. The time threshold is a N hours window calculated backwards from the moment of the transaction. The N parameter (date period) can be set from 1 to 24. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in N hours. This filter takes into account full hours. Counts Sale, Preauth or Transfer transactions in the approved status. Source and destination cards are considered separately.

Score: Yes

Enabled by default: N

#### Parameters

Name	Description	Value
for last N hours	time frame to calculate unique credit card count	Type: Int Default: 24
maximum transactions count	maximum number of transactions for one credit card number	Type: Int Default: 2
skip declined transactions	“Y” to skip sessions in Declined status, “N” for otherwise	Type: Enum Default: N

### Error codes

#	Code	Name
10269	1280	Specified period quantity limit exceeded

### Preventing transaction with the same amount 24 hours

This check fires when the number of transactions with the same amount associated with exact credit card number exceeds the configured thresholds. The time threshold is a 24 hours window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 24 hours. Also you can set the value of the amount starting from which transactions will be taken into account by the filter. Counts Sale, Preauth or Transfer transactions in the approved status. Source and destination cards are considered separately.

Score: Yes

Enabled by default: N

### Parameters

Name	Description	Value
maximum transactions count	maximum number of transactions with the same amount	Type: Int Default: 2
min amount to filter	value of the transaction amount starting from which transaction will be taken into account by the filter	Type: Float Default: 0.000
skip declined transactions	“Y” to skip sessions in Declined status, “N” for otherwise	Type: Enum Default: N


### Error codes


#	Code	Name
10270	1281	Limit transactions with the same amount for exact card exceeded

### Project Overview

Project is a Payment Gateway entity which determines the conditions for receiving a payment message and its further routing to the connected Processor. The Project list screen is located at Settings -> Configuration -> Projects. This screen contains all Projects created for all Merchants in the system.



 - Project is enabled.

 - Project is disabled.

To monitor the Project activity, Key Performance Indicators (KPI) are used, such as: Merchant earnings, Average order value, and others. The KPI submenu opens by pressing the Detailed button on the Project search screen. See details in [KPIs Detailed View](#).

Click on the Project name to open detailed information about this project.

To work with other configuration options, see the information below.

### Project Settings

<a href="#">Create, Clone, Edit Project Message Templates</a>	This screen shows how to create and edit the project. Shows all information about message templates sent to Customers after transactions.
<a href="#">Project Details</a>	Project details screen contains information about configured options on this Project, its ID and limits.

continues on next page

Table 239 – continued from previous page

<a href="#">Routing &amp; Balancing</a>	The routing & balancing system allows to distribute traffic between payment gates flexibly depending on the defined criteria and customer’s transaction data.
<a href="#">Fraud protection filters</a>	All information about filters.

## 9.2.3 Gate

### Acquirer restrictions

- [Gate level](#)
- [Processor level](#)

### Gate level

This functionality allows to set internal filters and prevent non-successful processing of transactions on gates which have specific limitations. To switch these limitations on, go to the required gate and click on the “Acquirer restrictions” tab.

### Warning

If the restriction on the gate is triggered, this gate is removed from balancing block in processing strategy for the current transaction.

Information and reason codes about gates which were excluded from balancing due to triggered restrictions is displayed in transaction details on UI:

Balancing logs		
●	4087 Demo_Gate_2	15004 0.000 of 200.000

API response text for these restrictions can be found on Internal Errors page in Integration section.

There are such restrictions as:

Restriction Name	Comment	UI code
Whitelist check (WL)	Allows ignoring all other Acquirer restrictions for selected Source credit card numbers and Device fingerprints. Sometimes customer's behavior can lead to the unfortunate situation where a shopper is completely unable to process transactions. You can whitelist a customer's data so they can successfully process their transaction. White list could be specified for the exact Source card number by manager and the exact Device fingerprint by manager.	
Predefined loyalty lists check	Allows processing for trusted customers only. Different acquirers have different definitions of a trusted customer, this filter allows processing for customers with emails, source/destination card or purpose in corresponding loyalty lists only. Transactions for customers that are not listed in any loyalty list will be filtered out.	15034 15035 15036 15037
Automatic loyalty lists check	This filter allows to specify a set of gates (group name) and create subsets of gates (financial instruments) within this set scope to allow processing of transactions with card numbers only on linked subsets of gates. Each card number which is processed by one of the gates within the set (group name) for the first time is linked to the subset (financial instrument) of the gate used for processing. All new transactions with the same card number will be allowed to process only on gates with the linked financial instrument and filtered on all other gates with different financial instruments within the same group name set. If the group name or financial instrument is not indicated on the gate, this filter will not be applied (even if it's enabled).	15110

continues on next page

Table 240 - continued from previous page

Restriction Name	Comment	UI code
Automatic customer email loyalty lists check	This filter allows to specify a set of gates (group name) and create subsets of gates (financial instruments) within this set scope to allow processing of transactions with e-mail only on linked subsets of gates. Each e-mail which is processed by one of the gates within the set (group name) for the first time is linked to the subset (financial instrument) of the gate used for processing. All new transactions with the same e-mail will be allowed to process only on gates with the linked financial instrument and filtered on all other gates with different financial instruments within the same group name set. If the group name or financial instrument is not indicated on the gate, this filter will not be applied (even if it's enabled).	15110
Destination Credit Card type check	This referral list allows to block transactions processing for selected Destination Credit Card types (Business, Corporate, etc.)	15170
Source Credit Card type check	This referral list allows to block transactions processing for selected Source Credit Card types (Business, Corporate, etc.)	15171
Check client approve count for merchant	This check fires when the number of transactions associated with exact client for that merchant does not reach the configured thresholds. The client can be identified by card or email address. Counts Sale, Preauth or Transfer transactions in the approved status.	15172
Check client approve count for manager	This check fires when the number of transactions associated with exact client for that manager does not reach the configured thresholds. The client can be identified by card or email address. Counts Sale, Preauth or Transfer transactions in the approved status.	15173

continues on next page

Table 240 - continued from previous page

Restriction Name	Comment	UI code
Check client approve date for manager	This check fires if the client's date since their first approved transaction is below the required number of days. The client will be identified by client definition set on endpoint/project level where endpoint overrides project setting. Counts Preauth, Sale, Transfer, Payout transactions in the approved status.	15176
Source Credit Card Number usage frequency for last 24 hours (daily limit)	This check fires when the number or amount of transactions associated with exact Source credit card number exceeds the configured thresholds. The time threshold is a 24 hours window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 24 hours. Counts Sale, Preauth or Transfer transactions in the approved status.	15004 15005
Source Credit Card Number usage frequency for last 7 days (weekly limit)	This check fires when the number or amount of transactions associated with exact Source credit card number exceeds the configured thresholds. The time threshold is a 7 days window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 168 hours. Counts Sale, Preauth or Transfer transactions in the approved status.	15002 15003

continues on next page

Table 240 - continued from previous page

Restriction Name	Comment	UI code
Source Credit Card Number usage frequency for last month (monthly limit)	This check fires when the number or amount of transactions associated with exact Source credit card number exceeds the configured thresholds. The time threshold is a one month window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in one month. Month calculation based on calendar i.e. 28th, 29th, 30th and 31st of March would be bumped to 28th of February during window calculation. Counts Sale, Preauth or Transfer transactions in the approved status.	15000 15001
Source Credit Card Number usage frequency for last 3 months	This check fires when the number or amount of transactions associated with exact Source credit card number exceeds the configured thresholds. The time threshold is a window of last 3 calendar months, starting from current month. For window calculation all transaction dates are truncated to months. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 3 months. Counts Sale, Preauth or Transfer transactions in the approved status.	15075 15076

continues on next page

Table 240 - continued from previous page

Restriction Name	Comment	UI code
Source Credit Card Number usage frequency for last 6 months	This check fires when the number or amount of transactions associated with exact Source credit card number exceeds the configured thresholds. The time threshold is a window of last 6 calendar months, starting from current month. For window calculation all transaction dates are truncated to months. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 6 months. Counts Sale, Preauth or Transfer transactions in the approved status.	15077 15078
Source Credit Card Number usage frequency for last 12 months	This check fires when the number or amount of transactions associated with exact Source credit card number exceeds the configured thresholds. The time threshold is a window of last 12 calendar months, starting from current month. For window calculation all transaction dates are truncated to months. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 12 months. Counts Sale, Preauth or Transfer transactions in the approved status.	15079 15080
Purpose usage frequency for last 24 hours (daily limit)	This check fires when the number or amount of transactions associated with exact Purpose exceeds the configured thresholds. The time threshold is a 24 hours window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 24 hours. Counts Sale, Preauth or Transfer transactions in the approved status.	15016 15017

continues on next page

Table 240 - continued from previous page

Restriction Name	Comment	UI code
Purpose usage frequency for last 7 days (weekly limit)	This check fires when the number or amount of transactions associated with exact Purpose exceeds the configured thresholds. The time threshold is a 7 days window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 168 hours. Counts Sale, Preauth or Transfer transactions in the approved status.	15014 15015
Purpose usage frequency for last month (monthly limit)	This check fires when the number or amount of transactions associated with exact Purpose exceeds the configured thresholds. The time threshold is a one month window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in one month. Month calculation based on calendar i.e. 28th, 29th, 30th and 31st of March would be bumped to 28th of February during window calculation. Counts Sale, Preauth or Transfer transactions in the approved status.	15012 15013
Email usage frequency for last 24 hours (daily limit)	This check fires when the number or amount of transactions associated with exact Email address exceeds the configured thresholds. The time threshold is a 24 hours window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 24 hours. Counts Sale, Preauth or Transfer transactions in the approved status.	15010 15011

continues on next page

Table 240 - continued from previous page

Restriction Name	Comment	UI code
Email usage frequency for last 7 days (weekly limit)	This check fires when the number or amount of transactions associated with exact Email address exceeds the configured thresholds. The time threshold is a 7 days window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 168 hours. Counts Sale, Preauth or Transfer transactions in the approved status.	15008 15009
Email usage frequency for last month (monthly limit)	This check fires when the number or amount of transactions associated with exact Email address exceeds the configured thresholds. The time threshold is a one month window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in one month. Month calculation based on calendar i.e. 28th, 29th, 30th and 31st of March would be bumped to 28th of February during window calculation. Counts Sale, Preauth or Transfer transactions in the approved status.	15006 15007

continues on next page

Table 240 - continued from previous page

Restriction Name	Comment	UI code
Visa Preauthorized Transaction Decline Response requirements	<p>This check fires for recurring transactions only. Merchants that receive a decline response for a preauthorized transaction will only be allowed to resubmit it for authorization up to four times within 13 calendar days from the date of the original decline response for the same acquirer if the response code is one of the following:</p> <ul style="list-style-type: none"> <li>• Response Code 05 - Authorization Declined</li> <li>• Response Code 51 - Insufficient Funds</li> <li>• Response Code 61 - Exceeds Approval Amount Limit</li> <li>• Response Code 65 - Exceeds Withdrawal Frequency Limit</li> </ul> <p>If an approval response is not received within this time frame, merchants must not resubmit the transaction or their acquirers may be subject to non-compliance actions, as outlined in the Visa Rules, and may be subject to chargebacks. Visa Rules to prohibit acquirers and their recurring services merchants from resubmitting a declined transaction for authorization if it receives a pickup response:</p> <ul style="list-style-type: none"> <li>• Response Code 04 - Pick Up Card</li> <li>• Response Code 07 - Pick Up Card, Special</li> <li>• Response Code 33 - Expired Card, Capture</li> <li>• Response Code 34 - Suspected Fraud, Retain Card</li> <li>• Response Code 35 - Card Acceptor, Contact Acquirer, Retain Card</li> <li>• Response Code 36 - Restricted Card, Retain Card</li> <li>• Response Code 37 - Contact Acquirer Security Department, Retain Card</li> <li>• Response Code 41 - Lost Card</li> <li>• Response Code 43 - Stolen Card</li> <li>• Response Code 67 - Capture Card</li> </ul>	15023 - CANCEL 15024 - CANCEL 15025 - PICKUP 15026 - DELAY

or a decline response of

- Response Code 14 - Invalid Account Number (No Such Number)

Table 240 - continued from previous page

Restriction Name	Comment	UI code
Entire Email usage frequency for last 24 hours (entire daily limit)	This check fires when the number or amount of transactions associated with exact Email address exceeds the configured thresholds. The time threshold is a 24 hours window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 24 hours. Counts Sale, Preauth or Transfer transactions in any status.	15042
		15043
Entire Email usage frequency for last 7 days (entire weekly limit)	This check fires when the number or amount of transactions associated with exact Email address exceeds the configured thresholds. The time threshold is a 7 days window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 168 hours. Counts Sale, Preauth or Transfer transactions in any status.	15044
		15045
Entire Email usage frequency for last month (entire monthly limit)	This check fires when the number or amount of transactions associated with exact Email address exceeds the configured thresholds. The time threshold is a one month window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in one month. Month calculation based on calendar i.e. 28th, 29th, 30th and 31st of March would be bumped to 28th of February during window calculation. Counts Sale, Preauth or Transfer transactions in any status.	15046
		15047

continues on next page

Table 240 - continued from previous page

Restriction Name	Comment	UI code
Entire Purpose usage frequency for last 24 hours (entire daily limit)	This check fires when the number or amount of transactions associated with exact Purpose exceeds the configured thresholds. The time threshold is a 24 hours window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 24 hours. Counts Sale, Preauth or Transfer transactions in any status.	15048
		15049
Entire Purpose usage frequency for last 7 days (entire weekly limit)	This check fires when the number or amount of transactions associated with exact Purpose exceeds the configured thresholds. The time threshold is a 7 days window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 168 hours. Counts Sale, Preauth or Transfer transactions in any status.	15050
		15051
Entire Purpose usage frequency for last month (entire monthly limit)	This check fires when the number or amount of transactions associated with exact Purpose exceeds the configured thresholds. The time threshold is a one month window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in one month. Month calculation based on calendar i.e. 28th, 29th, 30th and 31st of March would be bumped to 28th of February during window calculation. Counts Sale, Preauth or Transfer transactions in any status.	15052
		15053

continues on next page

Table 240 - continued from previous page

Restriction Name	Comment	UI code
Entire Source Credit Card Number usage frequency for last 24 hours (entire daily limit)	This check fires when the number or amount of transactions associated with exact Source credit card number exceeds the configured thresholds. The time threshold is a 24 hours window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 24 hours. Counts Sale, Preauth or Transfer transactions in any status.	15054
		15055
Entire Source Credit Card Number usage frequency for last 7 days (entire weekly limit)	This check fires when the number or amount of transactions associated with exact Source credit card number exceeds the configured thresholds. The time threshold is a 7 days window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 168 hours. Counts Sale, Preauth or Transfer transactions in any status.	15056
		15057
Entire Source Credit Card Number usage frequency for last month (entire monthly limit)	This check fires when the number or amount of transactions associated with exact Source credit card number exceeds the configured thresholds. The time threshold is a one month window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in one month. Month calculation based on calendar i.e. 28th, 29th, 30th and 31st of March would be bumped to 28th of February during window calculation. Counts Sale, Preauth or Transfer transactions in any status.	15058
		15059

continues on next page

Table 240 - continued from previous page

Restriction Name	Comment	UI code
Entire Source Credit Card Number usage frequency for last 3 months (entire 3 months limit)	This check fires when the number or amount of transactions associated with exact Source credit card number exceeds the configured thresholds. The time threshold is a window of last 3 calendar months, starting from current month. For window calculation all transaction dates are truncated to months. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 3 months. Counts Sale, Preauth or Transfer transactions in any status.	15081 15082
Entire Source Credit Card Number usage frequency for last 6 months (entire 6 months limit)	This check fires when the number or amount of transactions associated with exact Source credit card number exceeds the configured thresholds. The time threshold is a window of last 6 calendar months, starting from current month. For window calculation all transaction dates are truncated to months. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 6 months. Counts Sale, Preauth or Transfer transactions in any status.	15083 15084
Entire Source Credit Card Number usage frequency for last 12 months (entire 12 months limit)	This check fires when the number or amount of transactions associated with exact Source credit card number exceeds the configured thresholds. The time threshold is a window of last 12 calendar months, starting from current month. For window calculation all transaction dates are truncated to months. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 12 months. Counts Sale, Preauth or Transfer transactions in any status.	15085 15086

continues on next page

Table 240 - continued from previous page

Restriction Name	Comment	UI code
Source Credit Card Number usage frequency for Destination Credit Card Number	This check fires when the number of Source Credit Cards associated with exact Destination Credit Card number exceeds the configured thresholds. The time threshold is a moving window calculated backwards from the moment of the transaction. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 Credit Cards in 6 hours, it fires on the 11th unique Credit Card in 6 hours. Counts unique Source Credit Card numbers for Transfer transactions in approved or declined status for the current Gate.	15072
Declined Email usage frequency for last 24 hours (decline daily limit)	This check fires when the number or amount of transactions associated with exact Email address exceeds the configured thresholds. The time threshold is a 24 hours window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 24 hours. Counts Sale, Preauth or Transfer transactions in declined status.	15066
Declined Email usage frequency for last 7 days (decline weekly limit)	This check fires when the number or amount of transactions associated with exact Email address exceeds the configured thresholds. The time threshold is a 7 days window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 168 hours. Counts Sale, Preauth or Transfer transactions in declined status.	15068

continues on next page

Table 240 - continued from previous page

Restriction Name	Comment	UI code
Declined Email usage frequency for last month (decline monthly limit)	This check fires when the number or amount of transactions associated with exact Email address exceeds the configured thresholds. The time threshold is a one month window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in one month. Month calculation based on calendar i.e. 28th, 29th, 30th and 31st of March would be bumped to 28th of February during window calculation. Counts Sale, Preauth or Transfer transactions in declined status.	15070
Source Credit Card Number declined transactions count per period	This check fires when the number or amount of transactions associated with exact Account number exceeds the configured thresholds. The time threshold is a one month window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in one month. Month calculation based on calendar i.e. 28th, 29th, 30th and 31st of March would be bumped to 28th of February during window calculation. Counts Sale, Preauth, Payout or Transfer transactions in the approved status.	15125 15126

continues on next page

Table 240 - continued from previous page

Restriction Name	Comment	UI code
Source Credit Card Number decline frequency for last 24 hours (daily decline limit)	This check fires when the number or amount of declined transactions associated with exact Source credit card number exceeds the configured thresholds. The time threshold is a 24 hours window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 24 hours. Counts Account verification, Sale, Preauth or Transfer transactions in the Declined or Filtered status.	
Source Credit Card Number decline frequency for last week (weekly decline limit)	This check fires when the number or amount of declined transactions associated with exact Source credit card number exceeds the configured thresholds. The time threshold is a 7 days window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 7 days. Counts Account verification, Sale, Preauth or Transfer transactions in the Declined status.	15128 15129

continues on next page

Table 240 - continued from previous page

Restriction Name	Comment	UI code
Source Credit Card Number decline frequency for last month (monthly decline limit)	This check fires when the number or amount of declined transactions associated with exact Source credit card number exceeds the configured thresholds. The time threshold is a one month window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in one month. Month calculation based on calendar i.e. 28th, 29th, 30th and 31st of March would be bumped to 28th of February during window calculation. Counts Account verification, Sale, Preauth or Transfer transactions in the Declined status.	15130 15131
Destination Credit Card Number decline frequency for last 24 hours (daily decline limit)	This check fires when the number or amount of declined transactions associated with exact Destination credit card number exceeds the configured thresholds. The time threshold is a 24 hours window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 24 hours. Counts Transfer transactions in the Declined status.	15132 15133

continues on next page

Table 240 - continued from previous page

Restriction Name	Comment	UI code
Destination Credit Card Number decline frequency for last week (weekly decline limit)	This check fires when the number or amount of declined transactions associated with exact Destination credit card number exceeds the configured thresholds. The time threshold is a 7 days window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 168 hours. Counts Transfer transactions in the Declined status.	15134
		15135
Destination Credit Card Number decline frequency for last month (monthly decline limit)	This check fires when the number or amount of declined transactions associated with exact Destination credit card number exceeds the configured thresholds. The time threshold is a one month window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in one month. Month calculation based on calendar i.e. 28th, 29th, 30th and 31st of March would be bumped to 28th of February during window calculation. Counts Transfer transactions in the Declined status.	15136
		15137

continues on next page

Table 240 - continued from previous page

Restriction Name	Comment	UI code
Total Credit Card Number decline frequency for last 24 hours (daily decline limit)	This check fires when the number or amount of declined transactions associated with exact Source or Destination credit card number exceeds the configured thresholds. The time threshold is a 24 hours window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 24 hours. Counts Account verification, Sale, Preauth or Transfer transactions in the Declined status.	15138
		15139
		15140
		15141
Total Credit Card Number decline frequency for last week (weekly decline limit)	This check fires when the number or amount of declined transactions associated with exact Source or Destination credit card number exceeds the configured thresholds. The time threshold is a 7 days window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 168 hours. Counts Account verification, Sale, Preauth or Transfer transactions in the Declined status.	15142
		15143
		15144
		15145

continues on next page

Table 240 - continued from previous page

Restriction Name	Comment	UI code
Total Credit Card Number decline frequency for last month (monthly decline limit)	This check fires when the number or amount of declined transactions associated with exact Source or Destination credit card number exceeds the configured thresholds. The time threshold is a one month window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in one month. Month calculation based on calendar i.e. 28th, 29th, 30th and 31st of March would be bumped to 28th of February during window calculation. Counts Account verification, Sale, Preauth or Transfer transactions in the Declined status.	15146 15147 15148 15149
Source Credit Card Number usage frequency for last N days	This check fires when the number or amount of transactions associated with exact Source credit card number exceeds the configured thresholds. The time threshold is a N days window calculated backwards from the moment of the transaction. The N parameter (date period) can be set from 1 to 30. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in N days. Counts Sale, Preauth or Transfer transactions in the approved status.	15150 15151

continues on next page

Table 240 - continued from previous page

Restriction Name	Comment	UI code
Destination Credit Card Number usage frequency for last N days	This check fires when the number or amount of transactions associated with exact Destination credit card number exceeds the configured thresholds. The time threshold is a N days window calculated backwards from the moment of the transaction. The N parameter (date period) can be set from 1 to 30. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in N days. Counts Transfer transactions in the approved status.	15152
		15153
Total Credit Card Number usage frequency for last N days	This check fires when the number or amount of transactions associated with exact Source or Destination credit card number exceeds the configured thresholds. The time threshold is a N days window calculated backwards from the moment of the transaction. The N parameter (date period) can be set from 1 to 30. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in N days. Counts Sale, Preauth or Transfer transactions in the approved status.	15154
		15155
		15156
		15157
Purpose usage frequency for last N days	This check fires when the number or amount of transactions associated with exact Purpose exceeds the configured thresholds. The time threshold is a N days window calculated backwards from the moment of the transaction. The N parameter (date period) can be set from 1 to 30. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in N days. Counts Sale, Preauth or Transfer transactions in the approved status.	15158
		15159

continues on next page

Table 240 - continued from previous page

Restriction Name	Comment	UI code
Email usage frequency for last N days	This check fires when the number or amount of transactions associated with exact Email address exceeds the configured thresholds. The time threshold is a N days window calculated backwards from the moment of the transaction. The N parameter (date period) can be set from 1 to 30. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in N days. Counts Sale, Preauth or Transfer transactions in the approved status.	15160 15161
IP address usage frequency for last N days	This check fires when the number or amount of transactions associated with exact IP address exceeds the configured thresholds. The time threshold is a N days window calculated backwards from the moment of the transaction. The N parameter (date period) can be set from 1 to 30. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in N days. Counts Sale, Preauth or Transfer transactions in the approved status.	15162 15163
Fingerprint usage frequency for last N days	This check fires when the number or amount of transactions associated with exact Fingerprint exceeds the configured thresholds. The time threshold is a N days window calculated backwards from the moment of the transaction. The N parameter (date period) can be set from 1 to 30. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in N days. Counts Sale, Preauth or Transfer transactions in the approved status.	15164 15165

continues on next page

Table 240 - continued from previous page

Restriction Name	Comment	UI code
Account Number usage frequency for last N days	This check fires when the number or amount of transactions associated with exact Account Number exceeds the configured thresholds. The time threshold is a N days window calculated backwards from the moment of the transaction. The N parameter (date period) can be set from 1 to 30. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in N days. Counts Sale, Preauth or Transfer transactions in the approved status.	15166 15167
BIN range usage frequency	This check fires when the number of transactions associated with the specific card BIN range exceeds the configured thresholds, also can specify a list of card BIN range exceptions for which checks will not be performed. The maximum time threshold is a 300 seconds window, calculated backwards from the moment of the first transaction. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 300 seconds. Counts Sale, Preauth, Payouts or Transfer transactions.	15119
Issuer country usage frequency	This check fires when the number of transactions associated with the same card issuer country exceeds the configured thresholds. The maximum time threshold is a 300 seconds window, calculated backwards from the moment of the first transaction. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 300 seconds. Counts Sale, Preauth, Payouts or Transfer transactions.	15114

continues on next page

Table 240 - continued from previous page

Restriction Name	Comment	UI code
Preventing transaction with the same amount	This check fires when more than one transaction is made with same amount in a time threshold (in seconds). The maximum time threshold is a 300 seconds window, calculated backwards from the moment of the first transaction. The risk fires on the second transaction with the same amount during set time threshold. Counts Sale, Preauth, Payouts or Transfer transactions.	15113
Customer IP address Country differs from Issuing Country	This risk check fires when the customer IP country different from the issuing country of the card. Requests from IP addresses listed in "Merchant API IP address" are ignoring this check. If parameter "apply for countries" is empty, filter will require strict customer country to issuer country matching for all the countries, otherwise this check will force country matching for listed countries only. For example if you setup "apply for countries" to US - check will be triggered for following country combinations US-anyNonUS or anyNonUS-US, but for combinations anyNonUS-anyNonUS and US-US the check will not fire. For card2card transactions issuer country of the source card should be equal to issuer country of the destination card, i.e. this check will be triggered for any cross-border transaction.	15116

continues on next page

Table 240 - continued from previous page

Restriction Name	Comment	UI code
Purpose usage frequency for last year (annual limit)	This check fires when the number or amount of transactions associated with exact Purpose exceeds the configured thresholds. The time threshold is a one year window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 100 transactions, it fires on the 101th transaction in one year. Calculation of the year can be started from the beginning of the calendar year or from the filter activation truncated to the month and -12 months. I.e. if you activated the filter on May 15, 2021, the filter will consider transactions from May 2020. Counts Sale, Preauth or Transfer transactions in the approved status.	15117 15118
Transaction number per period	This check fires when the number of transactions exceeds the configured thresholds. The maximum time threshold is a 600 seconds window, calculated backwards from the moment of the first transaction. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction during 600 seconds. Counts Sale, Preauth, Payouts or Transfer transactions.	15115
Minimum time between transactions in the acquirer	This check fires when more than one transaction is made with same card in the same financial instrument in a time threshold (in minutes). The maximum time threshold is a 120 minutes window, calculated backwards from the moment of the first transaction. The filter takes into consideration only approved transactions. The risk fires on the second transaction with the same card during set time threshold. Counts Sale and Transfer transactions.	15120

continues on next page

Table 240 - continued from previous page

Restriction Name	Comment	UI code
Account Number usage frequency for last 24 hours (daily limit)	This check fires when the number or amount of transactions associated with exact Account number exceeds the configured thresholds. The time threshold is a 24 hours window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 24 hours. Counts Sale, Preauth, Payout or Transfer transactions in the approved status.	15121 15122
Account Number usage frequency for last 7 days (weekly limit)	This check fires when the number or amount of transactions associated with exact Account number exceeds the configured thresholds. The time threshold is a 7 days window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 168 hours. Counts Sale, Preauth, Payout or Transfer transactions in the approved status.	15123 15124

continues on next page

Table 240 - continued from previous page

Restriction Name	Comment	UI code
Account Number usage frequency for last month (monthly limit)	This check fires when the number or amount of transactions associated with exact Account number exceeds the configured thresholds. The time threshold is a one month window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in one month. Month calculation based on calendar i.e. 28th, 29th, 30th and 31st of March would be bumped to 28th of February during window calculation. Counts Sale, Preauth, Payout or Transfer transactions in the approved status.	15125 15126

Below is the example of configuration for “Email usage frequency for last month (monthly limit)” restriction. To switch this restriction on, click on the toggle button near it’s name:

Email usage frequency for last month (monthly limit) disabled  enabled

This check fires when the number or amount of transactions associated with exact Email address exceeds the configured thresholds. The time threshold is a one month window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in one month. Month calculation based on calendar i.e. 28th, 29th, 30th and 31st of March would be bumped to 28th of February during window calculation. Counts Sale, Preauth or Transfer transactions in the approved status.

**Parameters**

Name	Description	Value
amount limit	maximum total transactions amount for the last one month for this e-mail address	999999999.000
for all gates with the same descriptor	current total transactions amount or count for the last one month for this e-mail address value would be calculated - Y: for all gates with the same descriptor - N: for current gate only and converted to current gate currency to compare with amount or quantity limit values	No
quantity limit	maximum total transactions count for the last one month for this e-mail address	99999
use calendar month		No

**Error codes**

#	Code	Description
15006		E-mail approved monthly amount limit reached
15007		E-mail approved monthly quantity limit reached

Common

Acquirer restrictions

Properties

3DS Properties

Chain strategy details

Chain strategy skips

Settlement settings

Gate logs

Import PIN Online Key

Import terminal authentication key

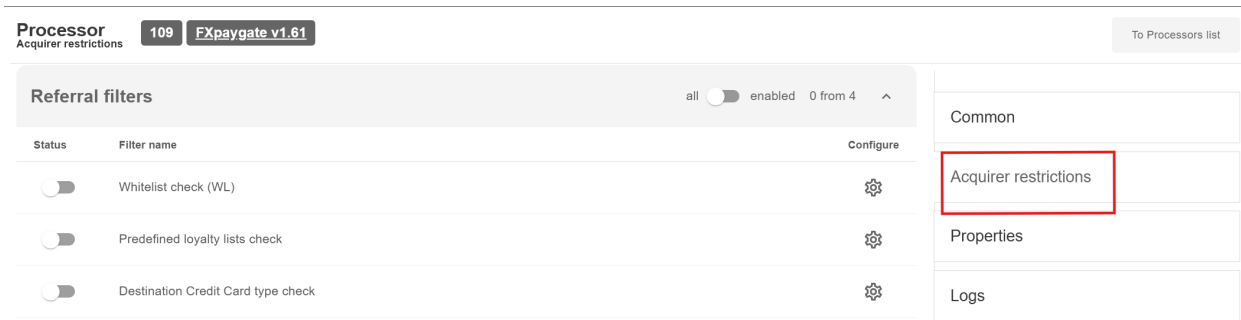
This restriction supports the following settings:

- 1) The Amount limit maximum total transactions amount for the last one month for this e-mail address. Value: total amount value.
- 2) For all gates with the same descriptor - current total transactions amount or count for the last one month for this e-mail address value would be calculated and converted to current gate currency to compare with amount or quantity limit. Specify the value “Y” (Yes) instead of “N” (No) to enable. Values: Y: for all gates with the same descriptor, N: for current gate only.
- 3) The quantity limit parameter specifies the transactions quantity limits. Value: total quantity value.
- 4) Use calendar month : Value: Y/N.

The choice of “Country Identifier” will be available in the “Deny” restriction configurations. Each country is assigned its own numerical identifier. The required country can be chosen from the list.

### Processor level

This functionality allows to prevent non-successful processing of transactions on all gates of the same processor which have specific limitations. To switch them on, go to the required processor and click on the “Acquirer restrictions” tab. Tab will be available only for manager account and linked superiors.



There are such restrictions as:

Restriction Name	Comment	UI code and reason
Whitelist check (WL)	Allows ignoring all other Acquirer restrictions for selected Source credit card numbers and Device fingerprints. Sometimes customer's behavior can lead to the unfortunate situation where a shopper is completely unable to process transactions. You can whitelist a customer's data so they can successfully process their transaction. White list could be specified for: the exact Source card number by manager, the exact Device fingerprint by manager	
Predefined loyalty lists check	Allows processing for trusted customers only. Different acquirers have different definitions of a trusted customer, this filter allows processing for customers with emails, source/destination card or purpose in corresponding loyalty lists only. Transactions for customers that are not listed in any loyalty list will be filtered out..	18042 - Processor loyal source card number check failed  18043 - Processor loyal destination card number check failed
Destination Credit Card type check	This referral list allows to block transactions processing for selected Destination Credit Card types (Business, Corporate, etc).	18112 - Processor unsupported destination product type
Source Credit Card type check	This referral list allows to block transactions processing for selected Source Credit Card types (Business, Corporate, etc).	18113 - Processor unsupported product type
Check client approve count for merchant	This check fires when the number of transactions associated with exact client for that merchant does not reach the configured thresholds. The client can be identified by card or email address. Counts Sale, Preauth or Transfer transactions in the approved status.	18116 - Processor required number of approvals for merchant has not achieved

continues on next page

Table 241 - continued from previous page

Restriction Name	Comment	UI code and reason
Check client approve count for manager	This check fires when the number of transactions associated with exact client for that manager does not reach the configured thresholds. The client can be identified by card or email address. Counts Sale, Preauth or Transfer transactions in the approved status.	18117 Processor required number of approvals for manager has not achieved
Source Credit Card Number usage frequency for last 24 hours (daily limit)	This check fires when the number or amount of transactions associated with exact Source credit card number exceeds the configured thresholds. The time threshold is a 24 hours window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 24 hours. Counts Sale, Preauth or Transfer transactions in the approved status. Timeframe can be set to calendar day instead of 24 hours window.	18004 - Approved hourly amount limit reached  18005 - Approved hourly quantity limit reached
Source Credit Card Number usage frequency for last 7 days (weekly limit)	This check fires when the number or amount of transactions associated with exact Source credit card number exceeds the configured thresholds. The time threshold is a 7 days window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 168 hours. Counts Sale, Preauth or Transfer transactions in the approved status.	18002 - Approved weekly amount limit reached  18003 - Approved weekly quantity limit reached

continues on next page

Table 241 - continued from previous page

Restriction Name	Comment	UI code and reason
Source Credit Card Number usage frequency for last month (monthly limit)	This check fires when the number or amount of transactions associated with exact Source credit card number exceeds the configured thresholds. The time threshold is a one month window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in one month. Month calculation based on calendar i.e. 28th, 29th, 30th and 31st of March would be bumped to 28th of February during window calculation. Counts Sale, Preauth or Transfer transactions in the approved status.	18000 - Approved monthly amount limit reached  18001 - Approved monthly quantity limit reached
Source Credit Card Number decline frequency for last 7 days (decline weekly limit)	This check fires when the number of declined transactions associated with exact Source credit card number exceeds the configured thresholds. The time threshold is a 7 days window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 168 hours. Counts Sale, Preauth or Transfer transactions in declined status.	18058 - Weekly decline quantity limit exceeded for the same credit card number on processor  18059 - Weekly decline amount limit exceeded for the same credit card number on processor

continues on next page

Table 241 - continued from previous page

Restriction Name	Comment	UI code and reason
Source Credit Card Number decline frequency for last month (decline monthly limit)	This check fires when the number of declined transactions associated with exact Source credit card number exceeds the configured thresholds. The time threshold is a 7 days window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in one month. Month calculation based on calendar i.e. 28th, 29th, 30th and 31st of March would be bumped to 28th of February during window calculation. Counts Sale, Preauth or Transfer transactions in the approved status.	18060 - Monthly decline quantity limit exceeded for the same credit card number on processor  18061 - Monthly decline amount limit exceeded for the same credit card number on processor
Destination Credit Card Number usage frequency for last 24 hours (daily limit)	This check fires when the number or amount of transactions associated with exact Destination credit card number exceeds the configured thresholds. The time threshold is a 24 hours window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 24 hours. Counts Transfer transactions only in the approved status.	18032 - Destination approved hourly amount limit reached  18033 - Destination approved hourly quantity limit reached
Destination Credit Card Number usage frequency for last 7 days (weekly limit)	This check fires when the number or amount of transactions associated with exact Destination credit card number exceeds the configured thresholds. The time threshold is a 7 days window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 168 hours. Counts Transfer transactions only in the approved status.	18030 - Destination approved weekly amount limit reached  18031 - Destination approved weekly quantity limit reached

continues on next page

Table 241 - continued from previous page

Restriction Name	Comment	UI code and reason
Destination Credit Card Number usage frequency for last month (monthly limit)	This check fires when the number or amount of transactions associated with exact Destination credit card number exceeds the configured thresholds. The time threshold is a one month window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in one month. Month calculation based on calendar i.e. 28th, 29th, 30th and 31st of March would be bumped to 28th of February during window calculation. Counts Transfer transactions only in the approved status.	18028 - Destination approved monthly amount limit reached  18029 - Destination approved monthly quantity limit reached
Total Credit Card Number usage frequency for last 24 hours (daily limit)	This check fires when the number or amount of transactions associated with exact credit card number used as Source or Destination exceeds the configured thresholds. The time threshold is a 24 hours window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 24 hours. Counts Sale, Preauth or Transfer transactions in the approved status.	18038 - Total approved hourly amount limit reached  18039 - Total approved hourly quantity limit reached

continues on next page

Table 241 - continued from previous page

Restriction Name	Comment	UI code and reason
Total Credit Card Number usage frequency for last 7 days (weekly limit)	This check fires when the number or amount of transactions associated with exact credit card number used as Source or Destination exceeds the configured thresholds. The time threshold is a 7 days window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 168 hours. Counts Sale, Preauth or Transfer transactions in the approved status.	18036 - Total approved weekly amount limit reached  18037 - Total approved weekly quantity limit reached
Total Credit Card Number usage frequency for last month (monthly limit)	This check fires when the number or amount of transactions associated with exact credit card number used as Source or Destination exceeds the configured thresholds. The time threshold is a one month window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in one month. Month calculation based on calendar i.e. 28th, 29th, 30th and 31st of March would be bumped to 28th of February during window calculation. Counts Sale, Preauth or Transfer transactions in the approved status.	18034 - Total approved monthly amount limit reached  18035 - Total approved monthly quantity limit reached

continues on next page

Table 241 - continued from previous page

Restriction Name	Comment	UI code and reason
Email usage frequency for last 24 hours (daily limit)	This check fires when the number or amount of transactions associated with exact Email address exceeds the configured thresholds. The time threshold is a 24 hours window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 24 hours. Counts Sale, Preauth or Transfer transactions in the approved status.	18010 - E-mail approved hourly amount limit reached  18011 - E-mail approved hourly quantity limit reached
Email usage frequency for last 7 days (weekly limit)	This check fires when the number or amount of transactions associated with exact Email address exceeds the configured thresholds. The time threshold is a 7 days window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 168 hours. Counts Sale, Preauth or Transfer transactions in the approved status.	18008 - E-mail approved weekly amount limit reached  18009 - E-mail approved weekly quantity limit reached
Email usage frequency for last month (monthly limit)	This check fires when the number or amount of transactions associated with exact Email address exceeds the configured thresholds. The time threshold is a one month window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in one month. Month calculation based on calendar i.e. 28th, 29th, 30th and 31st of March would be bumped to 28th of February during window calculation. Counts Sale, Preauth or Transfer transactions in the approved status.	18006 - E-mail approved monthly amount limit reached  18007 - E-mail approved monthly quantity limit reached

continues on next page

Table 241 - continued from previous page

Restriction Name	Comment	UI code and reason
Email usage lifetime	Allows to limit the number and amount of transactions available to an individual customer and set a limit on the processor for the ALL time of existence. Customer is determined by E-Mail. This check fires when the number or amount of transactions associated with exact Email address exceeds the configured thresholds. The time period is lifetime. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction. Counts Sale, Preauth or Transfer transactions in the approved status.	18048 - E-mail approved lifetime amount limit reached  18049 - E-mail approved lifetime quantity limit reached
Customer IP usage frequency for last 24 hours (daily limit)	This check fires when the number or amount of transactions associated with exact Customer IP address exceeds the configured thresholds. The time threshold is a 24 hours window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 24 hours. Counts Sale, Preauth or Transfer transactions in the approved status.	18022 - Customer IP approved hourly amount limit reached  18023 - Customer IP approved hourly quantity limit reached
Customer IP usage frequency for last 7 days (weekly limit)	This check fires when the number or amount of transactions associated with exact Customer IP address exceeds the configured thresholds. The time threshold is a 7 days window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 168 hours. Counts Sale, Preauth or Transfer transactions in the approved status.	18020 - Customer IP approved weekly amount limit reached  18021 - Customer IP approved weekly quantity limit reached

continues on next page

Table 241 - continued from previous page

Restriction Name	Comment	UI code and reason
Customer IP usage frequency for last month (monthly limit)	This check fires when the number or amount of transactions associated with exact Customer IP address exceeds the configured thresholds. The time threshold is a one month window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in one month. Month calculation based on calendar i.e. 28th, 29th, 30th and 31st of March would be bumped to 28th of February during window calculation. Counts Sale, Preauth or Transfer transactions in the approved status.	18018 - Customer IP approved monthly amount limit reached  18019 - Customer IP approved monthly quantity limit reached
Purpose usage frequency for last 24 hours (daily limit)	This check fires when the number or amount of transactions associated with exact Purpose exceeds the configured thresholds. The time threshold is a 24 hours window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 24 hours. Counts Sale, Preauth or Transfer transactions in the approved status.	18016 - Purpose approved hourly amount limit reached  18017 - Purpose approved hourly quantity limit reached
Purpose usage frequency for last 7 days (weekly limit)	This check fires when the number or amount of transactions associated with exact Purpose exceeds the configured thresholds. The time threshold is a 7 days window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 168 hours. Counts Sale, Preauth or Transfer transactions in the approved status.	18014 - Purpose approved weekly amount limit reached  18015 - Purpose approved weekly quantity limit reached

continues on next page

Table 241 - continued from previous page

Restriction Name	Comment	UI code and reason
Purpose usage frequency for last month (monthly limit)	This check fires when the number or amount of transactions associated with exact Purpose exceeds the configured thresholds. The time threshold is a one month window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in one month. Month calculation based on calendar i.e. 28th, 29th, 30th and 31st of March would be bumped to 28th of February during window calculation. Counts Sale, Preauth or Transfer transactions in the approved status.	18012 - Purpose approved monthly amount limit reached  18013 - Purpose approved monthly quantity limit reached
BIN range usage frequency	This check fires when the number of transactions associated with the specific card BIN range exceeds the configured thresholds, also can specify a list of card BIN range exceptions for which checks will not be performed. The maximum time threshold is a 300 seconds window, calculated backwards from the moment of the first transaction. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 300 seconds. Counts Sale, Preauth, Payouts or Transfer transactions.	18056 - Transaction quantity limit exceeds by BIN range on processor
Issuer country usage frequency	This check fires when the number of transactions associated with the same card issuer country exceeds the configured thresholds. The maximum time threshold is a 300 seconds window, calculated backwards from the moment of the first transaction. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 300 seconds. Counts Sale, Preauth, Payouts or Transfer transactions.	18053 - Transactions quantity limit exceeds by country on processor

continues on next page

Table 241 - continued from previous page

Restriction Name	Comment	UI code and reason
Preventing transaction with the same amount	This check fires when more than one transaction is made with same amount in a time threshold (in seconds). The maximum time threshold is a 300 seconds window, calculated backwards from the moment of the first transaction. The risk fires on the second transaction with the same amount during set time threshold. Counts Sale, Preauth, Payouts or Transfer transactions.	18052 - Same amount request on processor
Transaction number per period	This check fires when the number of transactions exceeds the configured thresholds. The maximum time threshold is a 600 seconds window, calculated backwards from the moment of the first transaction. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction during 600 seconds. Counts Sale, Preauth, Payouts or Transfer transactions.	18057 - Detected transaction in the set threshold of time
Account Number usage frequency for last 24 hours (daily limit)	This check fires when the number or amount of transactions associated with exact Account number exceeds the configured thresholds. The time threshold is a 24 hours window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 24 hours. Counts Sale, Preauth, Payout or Transfer transactions in the approved status.	15121 15122

continues on next page

Table 241 - continued from previous page

Restriction Name	Comment	UI code and reason
Account Number usage frequency for last 7 days (weekly limit)	This check fires when the number or amount of transactions associated with exact Account number exceeds the configured thresholds. The time threshold is a 7 days window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 168 hours. Counts Sale, Preauth, Payout or Transfer transactions in the approved status.	15123 15124
Account Number usage frequency for last month (monthly limit)	This check fires when the number or amount of transactions associated with exact Account number exceeds the configured thresholds. The time threshold is a one month window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in one month. Month calculation based on calendar i.e. 28th, 29th, 30th and 31st of March would be bumped to 28th of February during window calculation. Counts Sale, Preauth, Payout or Transfer transactions in the approved status.	15125 15126

continues on next page

Table 241 - continued from previous page

Restriction Name	Comment	UI code and reason
Destination Credit Card Number decline frequency for last 24 hours (daily decline limit)	This check fires when the number or amount of declined transactions associated with exact Destination credit card number exceeds the configured thresholds. The time threshold is a 24 hours window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 24 hours. Counts Transfer transactions in the Declined status.	18068 - Daily decline amount limit exceeded for the recipient on processor  18069 - Daily decline quantity limit exceeded for the recipient on processor
Destination Credit Card Number decline frequency for last week (weekly decline limit)	This check fires when the number or amount of declined transactions associated with exact Destination credit card number exceeds the configured thresholds. The time threshold is a 7 days window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 168 hours. Counts Transfer transactions in the Declined status.	18070 - Weekly decline amount limit exceeded for the recipient on processor  18071 - Weekly decline quantity limit exceeded for the recipient on processor

continues on next page

Table 241 - continued from previous page

Restriction Name	Comment	UI code and reason
Destination Credit Card Number decline frequency for last month (monthly decline limit)	This check fires when the number or amount of declined transactions associated with exact Destination credit card number exceeds the configured thresholds. The time threshold is a one month window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in one month. Month calculation based on calendar i.e. 28th, 29th, 30th and 31st of March would be bumped to 28th of February during window calculation. Counts Transfer transactions in the Declined status.	18072 - Monthly decline amount limit exceeded for the recipient on processor  18073 - Monthly decline quantity limit exceeded for the recipient on processor
Total Credit Card Number decline frequency for last 24 hours (daily decline limit)	This check fires when the number or amount of declined transactions associated with exact Source or Destination credit card number exceeds the configured thresholds. The time threshold is a 24 hours window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 24 hours. Counts Account verification, Sale, Preauth or Transfer transactions in the Declined status.	18074 - Daily decline total amount limit exceeded for the sender on processor  18075 - Daily decline total quantity limit exceeded for the sender on processor  18076 - Daily decline total amount limit exceeded for the recipient on processor  18077 - Daily decline total quantity limit exceeded for the recipient on processor

continues on next page

Table 241 - continued from previous page

Restriction Name	Comment	UI code and reason
Total Credit Card Number decline frequency for last week (weekly decline limit)	This check fires when the number or amount of declined transactions associated with exact Source or Destination credit card number exceeds the configured thresholds. The time threshold is a 7 days window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 168 hours. Counts Account verification, Sale, Preauth or Transfer transactions in the Declined status.	<p>18078 - Weekly decline total amount limit exceeded for the sender on processor</p> <p>18079 - Weekly decline total quantity limit exceeded for the sender on processor</p> <p>18080 - Weekly decline total amount limit exceeded for the recipient on processor</p> <p>18081 - Weekly decline total quantity limit exceeded for the recipient on processor</p>

continues on next page

Table 241 - continued from previous page

Restriction Name	Comment	UI code and reason
Total Credit Card Number decline frequency for last month (monthly decline limit)	This check fires when the number or amount of declined transactions associated with exact Source or Destination credit card number exceeds the configured thresholds. The time threshold is a one month window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in one month. Month calculation based on calendar i.e. 28th, 29th, 30th and 31st of March would be bumped to 28th of February during window calculation. Counts Account verification, Sale, Preauth or Transfer transactions in the Declined status.	18082 - Monthly decline total amount limit exceeded for the sender on processor
		18083 - Monthly decline total quantity limit exceeded for the sender on processor
		18084 - Monthly decline total amount limit exceeded for the recipient on processor
Source Credit Card Number usage frequency for last N days	This check fires when the number or amount of transactions associated with exact Source credit card number exceeds the configured thresholds. The time threshold is a N days window calculated backwards from the moment of the transaction. The N parameter (date period) can be set from 1 to 30. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in N days. Counts Sale, Preauth or Transfer transactions in the approved status.	18085 - Monthly decline total quantity limit exceeded for the recipient on processor
		18086 - Approved specified period amount limit reached  18087 - Approved specified period quantity limit reached

continues on next page

Table 241 - continued from previous page

Restriction Name	Comment	UI code and reason
Destination Credit Card Number usage frequency for last N days	This check fires when the number or amount of transactions associated with exact Destination credit card number exceeds the configured thresholds. The time threshold is a N days window calculated backwards from the moment of the transaction. The N parameter (date period) can be set from 1 to 30. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in N days. Counts Transfer transactions in the approved status.	18088 - Approved specified period amount limit reached,  18089 - Approved specified period quantity limit reached
Total Credit Card Number usage frequency for last N days	This check fires when the number or amount of transactions associated with exact Source or Destination credit card number exceeds the configured thresholds. The time threshold is a N days window calculated backwards from the moment of the transaction. The N parameter (date period) can be set from 1 to 30. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in N days. Counts Sale, Preauth or Transfer transactions in the approved status.	18090 - Total specified period amount limit reached  18091 - Total specified period quantity limit reached  18092 - Total specified period amount limit reached for recipient  18093 - Total specified period quantity limit reached for recipient

continues on next page

Table 241 - continued from previous page

Restriction Name	Comment	UI code and reason
Purpose usage frequency for last N days	This check fires when the number or amount of transactions associated with exact Purpose exceeds the configured thresholds. The time threshold is a N days window calculated backwards from the moment of the transaction. The N parameter (date period) can be set from 1 to 30. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in N days. Counts Sale, Preauth or Transfer transactions in the approved status.	18094 - Purpose approved specified period amount limit reached  18095 - Purpose approved specified period quantity limit reached
Email usage frequency for last N days	This check fires when the number or amount of transactions associated with exact Email address exceeds the configured thresholds. The time threshold is a N days window calculated backwards from the moment of the transaction. The N parameter (date period) can be set from 1 to 30. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in N days. Counts Sale, Preauth or Transfer transactions in the approved status.	18096 - E-mail approved specified period amount limit reached  18097 - E-mail approved specified period quantity limit reached
IP address usage frequency for last N days	This check fires when the number or amount of transactions associated with exact IP address exceeds the configured thresholds. The time threshold is a N days window calculated backwards from the moment of the transaction. The N parameter (date period) can be set from 1 to 30. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in N days. Counts Sale, Preauth or Transfer transactions in the approved status.	18098 - IP address approved specified period amount limit reached  18099 - IP address approved specified period quantity limit reached

continues on next page

Table 241 - continued from previous page

Restriction Name	Comment	UI code and reason
Fingerprint usage frequency for last N days	This check fires when the number or amount of transactions associated with exact Fingerprint exceeds the configured thresholds. The time threshold is a N days window calculated backwards from the moment of the transaction. The N parameter (date period) can be set from 1 to 30. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in N days. Counts Sale, Preauth or Transfer transactions in the approved status.	18100 - Fingerprint approved specified period amount limit reached, 18101 - Fingerprint approved specified period quantity limit reached
Account Number usage frequency for last N days	This check fires when the number or amount of transactions associated with exact Account Number exceeds the configured thresholds. The time threshold is a N days window calculated backwards from the moment of the transaction. The N parameter (date period) can be set from 1 to 30. For window calculation all transaction dates are truncated to days. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in N days. Counts Sale, Preauth or Transfer transactions in the approved status.	18102 - Specified period amount limit exceeded for account number on processor 18103 - Specified period quantity limit exceeded for account number on processor
Customer name differs from Cardholder name	This check fires when the provided customer name does not match cardholder name.	18120 - Customer name does not correspond to the cardholder name

continues on next page

Table 241 - continued from previous page

Restriction Name	Comment	UI code and reason
Customer billing address Country differs from Issuing Country	This risk check is triggered when a transaction has the customer billing address country different from the issuing country of the card. If parameter "apply for countries" is empty, filter will require strict customer country to issuer country matching for all the countries, otherwise this check will force country matching for listed countries only. For example if you setup "apply for countries" to US - check will be triggered for following country combinations US-anyNonUS or anyNonUS-US, but for combinations anyNonUS-anyNonUS and US-US the check will not fire. For card2card transactions issuer country of the source card should be equal to issuer country of the destination card, i.e. this check will be triggered for any cross-border transaction.	18121 - Customer billing address Country does not correspond to the Issuing Country
Processor lockout by specified declines	The filter allows locking out a Processor for Lockout period of time based on the defined Limit of declined transactions with the specific Analyzed decline codes occurred for the Analyzed period of time. Once the filter is activated one can track the filter lockout activities in the Processor Logs screen. When the filter is disabled it resets current status of the Processor to unblocked despite the Lockout period remaining time. Processor logs screen is enabled by request.	19100 - Processor lockout, decline time limit reached

continues on next page

Table 241 - continued from previous page

Restriction Name	Comment	UI code and reason
Declined Email usage frequency for last 24 hours (decline daily limit)	This check fires when the number or amount of transactions associated with exact Email address exceeds the configured thresholds. The time threshold is a 24 hours window calculated backwards from the moment of the transaction. For window calculation all transaction dates are truncated to hours. The risk fires on the transaction after the set threshold. So, if you set a threshold of 10 transactions, it fires on the 11th transaction in 24 hours. Counts Sale, Preauth or Transfer transactions in declined status.	19101 - E-mail decline hourly amount limit reached
		19102 - E-mail decline hourly quantity limit reached

## Chain Strategy Details

Chain strategy details allows to select which Declines (negative processing results) will continue or stop the chain.

If the configured routing has such balancing types as: Chain by Sequence, Chain by Equivalently on Tx Count, Chain by Coefficient on Tx Count, it's possible to go to the "Chain Strategy Details" tab on the gate level and select the criteria to continue or stop the chain.

The number and name of the gate is at the top of the page. The active line "Continue the chain" is located below and the choice of criteria is to the right of it. "Independently of the decline reason" is selected by default.

Two active columns - "Unavailable" and "Available" - are located below. The reasons for decline are located in the "Unavailable" field. The chain can continue:

- Independently of the decline reason - the chain will continue regardless of the received decline codes.
- Only for the selected decline reasons - the chain will continue only for the specified decline reasons. Select the reasons from the "Unavailable" column with the check boxes next to them, and add them to the "Available" column by clicking the "Add" button. Remove

the unwanted reasons by selecting them with the check boxes and clicking the “Remove” button. Confirm the parameters with the “Save” button.

- For any decline reason except the selected ones - the chain will continue for all reasons, EXCEPT for the specified ones. Select the reasons from the “Unavailable” column with the check boxes next to them, and add them to the “Available” column by clicking the “Add” button. Remove the unwanted reasons by selecting them with the check boxes and clicking the “Remove” button. Confirm the parameters with the “Save” button.

## Chain Strategy Skips

Chain strategy skips allows to skip a gate per PAN for a transaction if one of selected errors codes occur. After transaction is declined for a specific PAN on one gate, this gate will be skipped from cascading on next transactions with the same PAN for the specified time period (set in minutes).

The screenshot displays the configuration for a gate named "CP replica". The "Chain strategy skips" parameter is set to 2. The "Decline reason specified by" dropdown is set to "error code". Below this is a search bar. The main area is divided into "Available" and "Added" sections. The "Available" section lists error codes 000 through 007. The "Added" section lists error codes 002 and 004, each with a duration of 30 minutes. On the right, there is a sidebar with navigation links: Common, Acquirer restrictions, Properties, Chain strategy details, and Chain strategy skips.

This functionality is supported for the following options:

- Chain by Sequence
- Chain by Last Customer tx Status on Acquirer
- Chain by Coefficient Based on tx Count
- Chain by Equivalent Coefficient Based on tx Count
- First in Sequence
- First in Sequence by Last Customer tx Status on Acquirer
- First in Sequence by Last Customer tx Status on Gate

## Close day

- [Overview](#)
- [Manual day closure](#)
- [Automatic day closure](#)
- [Automatic scheduled day closure](#)
- [Allow closing day via API](#)

- [Gate Lock Release Tool](#)

## Overview

For some processors, funds are transferred to the bank account only after the Close Day procedure, which initiates bank clearing.

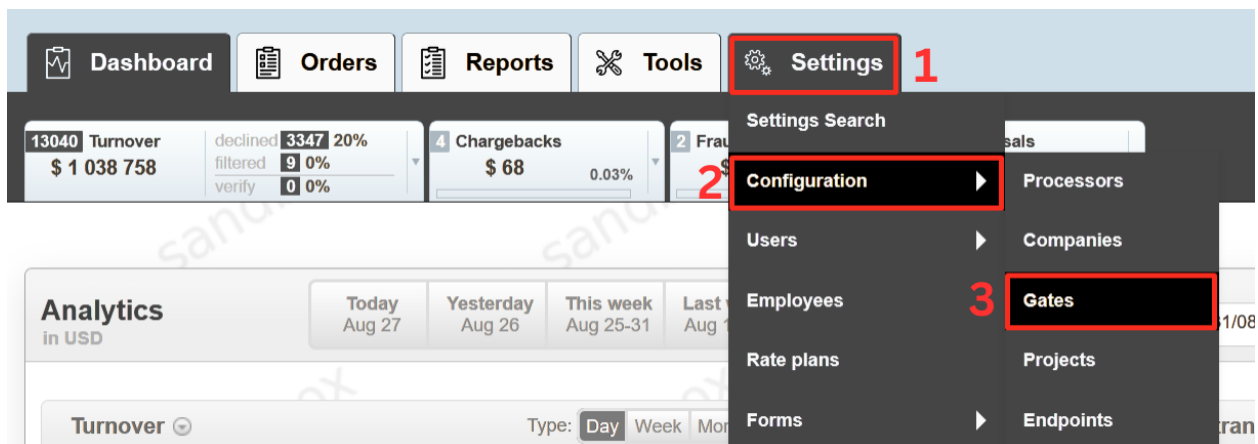
Close Day procedure can be initiated via API, manually with “Close Day” button on the Gate level, or automatically each day at pre-set or system selected time. If for any reason it is not possible to make “Close Day” using via API, then it is necessary to perform “Close Day” procedure manually on the Gate level.

### Warning

During the Close Day procedure the following gate will be blocked and transactions will not go through it.

## Manual day closure

In order to perform Close Day procedure, go to Settings -> Configuration -> Gates:



**Gates** Create

^ **Filters** Template ▾ Add filter ▾

Exact  1 in All ▾

On/Off	ID ↑	Display name	Description
<input type="checkbox"/>	9865	Close day test <span style="color: red; font-weight: bold;">← 2</span>	test

« ← 1 - 1 → 10 25 50

On the gate details page, click the Close day button and confirm this action on the pop-up window. The window “Close day for ‘gate name’” will appear on the page. Wait for the operation to complete:

Gate  
Common
9865
Close day test

Status:	Enabled
3D:	Yes
Description:	test
MID:	-
Tags:	-
Processor:	-
Manager:	-
Bank rate plan:	-
Dealer:	-
Dealer rate plan:	-
Currency:	EUR
Descriptor:	test
Project:	-
Company:	-
Loyalty Service:	-
Close day time:	-
Use external form:	-
Filter by blacklist:	-
API descriptor:	-
Min transaction amount:	-
Max transaction amount:	-
Method:	-
Last day closing date:	-
Day closing maximum delay (days):	-
Automatic selection of day closure:	No
Allow day closing via API:	No
Method 2:	-
Financial instrument:	-

### Are you sure?

2

Ok

Cancel

Close day for undefined
3
x

---

Name: Starting ...

Created time:	Estimated/elapsed time:	Steps processed:
Aug 27, 2025, 8:31:17 PM		

#### Bank Closed Days

Close Day

1

After the successful day closure, the gate details page will display the day closing date and the amount of transactions from the last to the current day closing date:

Gate  
Common
9865
Close day test

Status:	Enabled
3D:	Yes
Description:	test
MID:	-
Tags:	-
Processor:	Test processor
Manager:	Vica Loyalty test menager
Bank rate plan:	Zero rate by Vica_Loyalty_test_menager x1
Dealer:	-
Dealer rate plan:	-
Currency:	EUR
Descriptor:	test
Project:	Vica Loyalty test Project 3
Company:	-
Loyalty Service:	-
Close day time:	-
Use external form:	No
Filter by blacklist:	Yes
API descriptor:	-
Min transaction amount:	-
Max transaction amount:	-
Method:	-
Last day closing date:	27.08.2025 20:31:26
Day closing maximum delay (days):	-
Automatic selection of day closure:	Yes
Allow day closing via API:	No
Method 2:	-
Financial instrument:	-

**Bank Closed Days**

Close Day

Date	Bank response	Transactions amount
27.08.2025 20:31:26	OK	0

### Automatic day closure

In order to perform Close Day automatically, go to Settings -> Configuration -> Gates:

The screenshot shows the Doc4.0 Manager interface. At the top, there is a navigation bar with tabs for Dashboard, Orders, Reports, Tools, and Settings. The Settings tab is highlighted with a red box and a red number '1'. Below the navigation bar, there are several analytics cards. The first card shows '13040 Turnover' with a value of '\$ 1 038 758'. The second card shows 'declined 3347 20%' and 'filtered 9 0%'. The third card shows '4 Chargebacks' with a value of '\$ 68' and '0.03%'. The fourth card shows '2 Fraud' with a value of '\$ 108'. Below the analytics cards, there is an 'Analytics in USD' section with a 'Turnover' chart. The chart shows data for 'Today Aug 27', 'Yesterday Aug 26', 'This week Aug 25-31', and 'Last Aug 24'. The chart type is set to 'Day'. A settings menu is open, showing 'Settings Search' and a list of options: Configuration (2), Users, Employees, Rate plans, Forms, Processors, Companies, Gates (3), Projects, and Endpoints. The 'Configuration' option is highlighted with a red box and a red number '2', and the 'Gates' option is highlighted with a red box and a red number '3'.

The screenshot shows the 'Gates' configuration page. At the top right, there is a 'Create' button. Below the header, there is a 'Filters' section with a 'Template' dropdown and an 'Add filter' button. The 'Exact' filter is selected, and the 'close day' filter is highlighted with a red box and a red number '1'. Below the filters, there is a table with the following columns: On/Off, ID ↑, Display name, and Description. The table contains one row with the following data: On/Off (toggle switch), ID (9865), Display name (Close day test), and Description (test). The 'Close day test' display name is highlighted with a red box and a red number '2'. At the bottom of the table, there is a pagination control showing '1 - 1' and a '10 25 50' dropdown.

On the gate details page, click the Edit button, mark Automatic closing of the day and click Save. The optimal Close Day time is selected by the system automatically (UTC+3):

Gate Common 9865 Cancel Save

Loyalty Service

Close day automatically

Use external form

Filter by blacklist

API descriptor

Min transaction amount

Max transaction amount

Method

Day closing maximum delay (days)  
0

Automatic selection of day closure **1**

Allow day closing via API

Method 2

Financial instrument

Import PIN Online Key

Import terminal authentication key

IP configurator

Activate

After each successful day closure, the gate details page will display the day closing date and the amount of transactions from the last to the current day closing date:

Gate  
Common
9865
Close day test

Status:	Enabled
3D:	Yes
Description:	test
MID:	-
Tags:	-
Processor:	Test processor
Manager:	Vica Loyalty test menager
Bank rate plan:	Zero rate by Vica_Loyalty_test_manager x1
Dealer:	-
Dealer rate plan:	-
Currency:	EUR
Descriptor:	test
Project:	Vica Loyalty test Project 3
Company:	-
Loyalty Service:	-
Close day time:	-
Use external form:	No
Filter by blacklist:	Yes
API descriptor:	-
Min transaction amount:	-
Max transaction amount:	-
Method:	-
Last day closing date:	27.08.2025 20:31:26
Day closing maximum delay (days):	-
Automatic selection of day closure:	Yes
Allow day closing via API:	No
Method 2:	-
Financial instrument:	-

**Bank Closed Days**

Close Day

Date	Bank response	Transactions amount
27.08.2025 20:31:26	OK	0

### Automatic scheduled day closure

In order to perform Close Day automatically at pre-set time, go to Settings -> Configuration -> Gates:

The screenshot shows the Doc4.0 Manager interface. At the top, there is a navigation bar with tabs for Dashboard, Orders, Reports, Tools, and Settings. The Settings tab is highlighted with a red box and a '1'. Below the navigation bar, there are several widgets: Turnover (\$1,038,758), Chargebacks (\$68), and Fraud. The Analytics section shows Turnover in USD for Today, Yesterday, This week, and Last week. The Settings menu is open, showing Configuration, Users, Employees, Rate plans, and Forms. The Configuration menu is highlighted with a red box and a '2', and the Gates option is highlighted with a red box and a '3'. The Gates page shows a table with columns On/Off, ID, Display name, and Description. The Close day test row is highlighted with a red box and a '2', and the close day filter is highlighted with a red box and a '1'.

On the gate details page, click the Edit button and mark Close day automatically. After that Close day time row. Select the preferred close day time and then click Save. Please note, that Automatic closing of the day checkbox must be turned off, otherwise the gate closing time will be selected automatically by the system:

Gate Common 9865 Cancel 4 Save

Loyalty Service

Close day automatically **1**

Close day time 03:00 PM **2**

Use external form

Filter by blacklist

API descriptor

Min transaction amount

Max transaction amount

Method

Day closing maximum delay (days)

Automatic selection of day closure **3**

Allow day closing via API

Method 2

Financial instrument

Import PIN Online Key

Import terminal authentication key

IP configurator

Activat

After each successful day closure, the gate details page will display the day closing date and the amount of transactions from the last to the current day closing date:

Gate  
Common
9865
Close day test

Status:	Enabled
3D:	Yes
Description:	test
MID:	-
Tags:	-
Processor:	<a href="#">Test processor</a>
Manager:	<a href="#">Vica Loyalty test menager</a>
Bank rate plan:	Zero rate by Vica_Loyalty_test_menager x1
Dealer:	-
Dealer rate plan:	-
Currency:	EUR
Descriptor:	test
Project:	<a href="#">Vica Loyalty test Project 3</a>
Company:	-
Loyalty Service:	-
<b>Close day time:</b>	15:00
Use external form:	No
Filter by blacklist:	Yes
API descriptor:	-
Min transaction amount:	-
Max transaction amount:	-
Method:	-
<b>Last day closing date:</b>	27.08.2025 20:31:26
Day closing maximum delay (days):	-
Automatic selection of day closure:	Yes
Allow day closing via API:	No
Method 2:	-
Financial instrument:	-

### Bank Closed Days

Close Day

Date	Bank response	Transactions amount
27.08.2025 20:31:26	<div style="background-color: #444; color: white; padding: 2px 10px; border: 1px solid #ccc;">OK</div>	0

### Allow closing day via API

In order to allow this procedure via API, go to Settings -> Configuration -> Gates:

The screenshot shows the Doc4.0 Manager interface. At the top, there is a navigation bar with tabs for Dashboard, Orders, Reports, Tools, and Settings. The Settings tab is highlighted with a red box and a '1'. Below the navigation bar, there are several widgets: Turnover (\$1,038,758), Chargebacks (\$68), and Fraud. The Analytics section shows Turnover in USD for Today, Yesterday, This week, and Last week. The Settings menu is open, showing Configuration, Users, Employees, Rate plans, and Forms. Configuration is highlighted with a red box and a '2'. The Configuration menu is open, showing Processors, Companies, Gates, Projects, and Endpoints. Gates is highlighted with a red box and a '3'. The Gates page is shown, with a 'close day' filter highlighted with a red box and a '1'. The table of gates has a 'Close day test' gate highlighted with a red box and a '2'.

On/Off	ID ↑	Display name	Description
<input type="checkbox"/>	9865	Close day test	test

On the gate details page, click the Edit button, mark Allow closing day via API. The number of days after which the Close Day will be triggered automatically can be set in the Day closing maximum delay (days) (3 days is automatically set) then click Save:

Gate Common 9865 Cancel Save

Loyalty Service

Close day automatically

Use external form

Filter by blacklist

API descriptor

Min transaction amount

Max transaction amount

Method

Day closing maximum delay (days)  
2

Automatic selection of day closure

Allow day closing via API

Method 2

Financial instrument

Import PIN Online Key

Import terminal authentication key

IP configurator

### Gate Lock Release Tool

If during the gate closure via API one or more Gates remained blocked (in the body of the response with status: finished for Gate - isDayClosing : true), then removal of the lock can be done manually. In order to make this procedure go to Settings -> Configuration -> Gates:

Dashboard Orders Reports Tools **Settings** 1

13040 Turnover \$ 1 038 758 declined 3347 20% filtered 9 0% verify 0 0%

4 Chargebacks \$ 68 0.03%

2 Fraud

Settings Search

**Configuration** 2

Processors

Users Companies

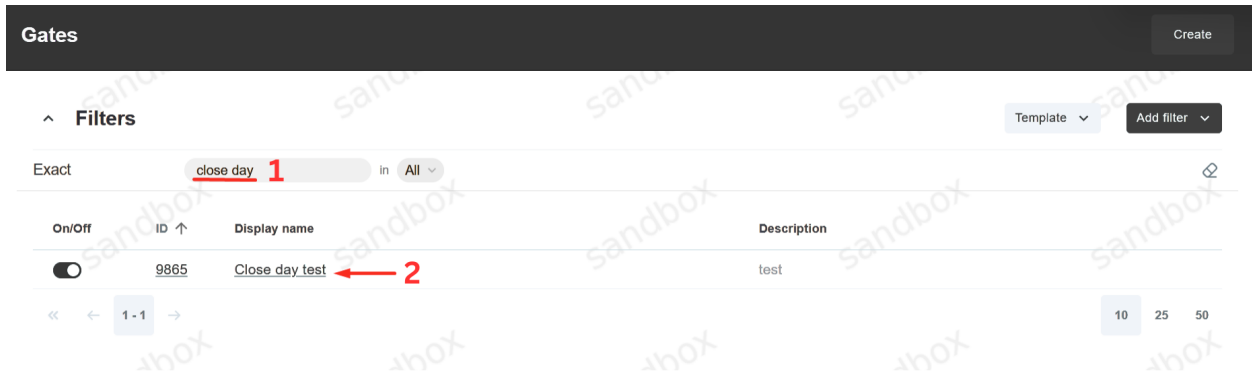
Employees **Gates** 3

Rate plans Projects

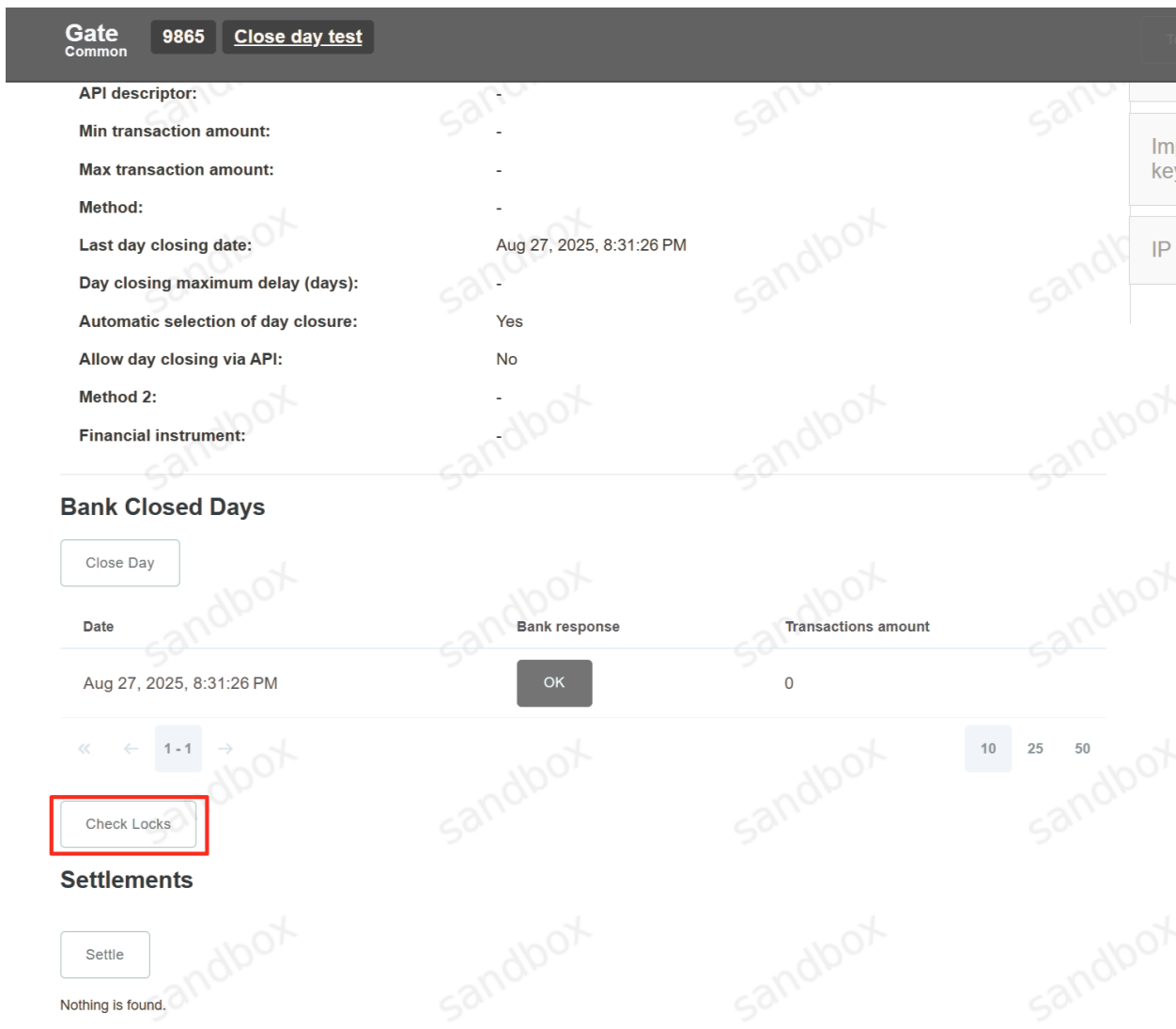
Forms Endpoints

Analytics in USD Today Aug 27 Yesterday Aug 26 This week Aug 25-31 Last Aug

Turnover Type: Day Week Mon



On the Gate details page tap on Locks:



The current Gate lock information is displayed in the “Current locks” menu:

- Lock session ID - ID of the lock session.
- Start day closing date - the start date of the Close Day.
- Bank terminal lock status- blocking the Endpoint for performing transactions (Blocked/Free).
- Initial gate job status - the status of the initialization Gate.
- Close day job status - the status of the closing Gate.
- Is day closing - the Gate is in the closing stage which means that is it locked or not (Y/N). Y - the Gate is blocked, N - not blocked.

The following unlock commands are available:

- CLEAR\_TRANSACTION\_LOCK - reset the session that caused the lock.
- CLEAR\_INIT\_ATTEMPT- reset the status of the initialization Gate.
- CLEAR\_CLOSING\_DAY\_ATTEMPTS - reset the status of the closing Gate.
- CLEAR\_CLOSING\_DAY\_FLAG - reset the assignment of the closing Gate, remove the lock.

Mark the applicable menu checkbox and click the Update button.

After the unlock, re-open the Gate Lock Release Tool and check that the status of the lock parameter has changed in the “Current locks” menu. For example, if the Gate was blocked, then after removing the lock, the parameter equals to Is day closing = N.

### Close days locks ×

---

Current locks

Lock	Value
Lock session ID	
Start closing date	
Terminal lock status	
Init job status	
Close day job status	Y
<u>Is day closing</u>	<u>N</u>

Clear locks

Clear transaction lock

Clear init attempt

Clear close day attempts

**1**  Clear close day flag

---

Cancel
**2** Update

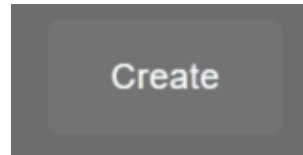
## Create, Clone, Edit Gate

- [Gate Creation](#)
- [Gate Editing And Cloning](#)

## Gate Creation

To create gate, go to Settings -> Configuration -> Gates and press + New Gate in the top right corner.

See [Gate details](#) table to correctly specify the configuration for new gate.



### Gate Editing And Cloning

Press Edit button to edit the gate or Clone button to clone it.



### Clone Gate ✕

---

Clone filters

Convert currency Gate settings

The entity you are about to clone contains changes, that may affect traffic

Inherit

Reset to defaults

---

Auto-name

---

Gates are cloned for the same processor. The required parameters for new gate are its name and currency.

Other gate settings will be inherited automatically. In order to reset parameters to default, select Reset to default.

In order to see which changes for new gate will be cloned, press changes button.

For cloning/creating several gates at once, click Add button. It is also possible to auto-name new gates by clicking Auto-name.

Gate options:	Current value:	Default value:
Gate date auto closed	Y	N
Gate auto close time	03:00	-
Method	-	-
Auto start day closing	Y	N
Method 2	-	-
Financial instrument	-	-

To clone acquirer restrictions to new gate, click Clone filters.

To convert all settings with amount into new currency, click Convert currency Gate settings

## Gate Details

Parameter Name	Description	Necessity for creation
Status	Shows whether gate is enabled or disabled. Can be changed later.	Required
3D	Possible to enable if 3DS flow is expected on this gate. Can be changed later.	Optional
Description	Shows gate description. Can be changed later.	Optional
MID	Shows Merchant identification number. Can be changed later.	Optional
Tags	Shows the tags for this gate. While searching gates by tag, all gates with the same tag will be shown. Can be changed later.	Optional
Processor	Shows to which exact processor this gate is linked. CANNOT be changed later.	Required
Manager	Shows to which exact manager this gate is linked. CANNOT be changed later.	Required

continues on next page

Table 242 - continued from previous page

Parameter Name	Description	Necessity for creation
Bank rate plan	Shows which rate plan for acquirer bank is currently specified on the gate. Can be changed later.	Required
Dealer	Shows which Dealer is specified on this gate. It is only possible to choose Dealers that are linked to the Processor. CANNOT be changed later.	Required for Processors with Dealers
Dealer rate plan	Shows which rate plan for Dealer is currently on the gate. Can be changed later.	Required for Processors with Dealers
Company	Shows company to which this gate is related to. Can be changed later.	Optional
Loyalty service	Shows which external loyalty service is selected. Can be changed later.	Optional
Close day automatically	Provides the option to setup time for automatic close day procedure. Can be changed later.	Optional
Use external form	Enable if it is expected to use external form logic (redirect to processor). Can be changed later.	Optional
Filter by blacklist	Enable if filtering by blacklist is required. Can be changed later.	Optional
API descriptor	Gate descriptor which if set up will be sent in callbacks and status responses to Merchant. Can be changed later.	Optional
Min transaction amount	Minimum amount per transaction which is allowed through the gate. Can be changed later.	Optional
Max transaction amount	Maximum amount per transaction which is allowed through the gate. Can be changed later.	Optional
Method	Additional parameter to group gates by specific marker, if needed. This field is present in transaction report. Can be changed later.	Optional
Last day closing date	Shows when the last close day procedure was initiated.	
Day closing maximum delay (days)	Select for how many days it is acceptable to delay the close day procedure. Can be changed later.	Optional
Automatic selection of day closure	If this parameter is enabled, the system will automatically select the close day procedure time. Can be changed later.	Optional
Allow day closing via API	If this parameter is enabled, it will be possible to make "Close day" requests via API. Can be changed later.	Optional

continues on next page

Table 242 - continued from previous page

Parameter Name	Description	Necessity for creation
Method 2	Additional parameter to group gates by specific marker, if needed. This field is present in transaction report. Can be changed later.	Optional
Financial instrument	For internal use. Can be changed later.	Optional

## Batch Operations for Gates

- [Overview](#)
- [Process Batch Operations for Gates in User Interface](#)
  - [Enable/Disable Gates](#)
  - [Min/Max Transaction Amount](#)
  - [Acquirer Restrictions](#)
  - [Task Execution and Monitoring](#)

### Overview

Batch Operations feature allows simultaneous management of multiple payment gates without the need to edit each gate individually.

The functionality is designed to simplify administrative tasks related to gate configuration, particularly for cases where acquirer limits or filters must be updated across many gates at once. This functionality is available in the “Gates” section of the user interface. It is available for Manager and Superior roles by default, and can be added for Employees by request.

Available Actions:

Action	Description
Enable/Disable Gates	Turns the selected gates ON or OFF.
Min/Max Amount	Sets the minimum and maximum transaction amount for selected gates.
Acquirer Restrictions	Allows enabling and configuring Referral and Velocity filters.

### Process Batch Operations for Gates in User Interface

1. Go to Settings -> Configuration -> Gates.
2. Use **Advanced Search** to filter gates according to specific criteria.

3. Select gates using checkboxes located in the left column of the gate list. Select all gates on the page or all filtered gates (up to 20,000).
4. Once gates are selected, use the Actions button in the upper-right corner to open the list of available batch operations.

**Filters**

Exact  in All ▾

	On/Off	ID ↑	Display name
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<a href="#">131</a>	<a href="#">test gate 1</a>
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<a href="#">165</a>	<a href="#">test gate 2</a>
<input type="checkbox"/>	<input type="checkbox"/>	<a href="#">166</a>	<a href="#">test gate 3</a>
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<a href="#">167</a>	<a href="#">test gate 4</a>

**Note**

Only one batch operation can run at a time. Attempts to start a new one will show the relevant warning message.

**Enable/Disable Gates**

This operation changes the activation status of multiple gates simultaneously.

Steps:

1. Select required gates.
2. Choose Actions -> Enable/Disable.
3. In the modal window, select the desired action (Enable or Disable).

4. Click Apply.

**Enable / Disable**
✕

Set status for all selected gates

ENABLE

DISABLE

<input checked="" type="checkbox"/>	ID	Name
<input checked="" type="checkbox"/>	131	<a href="#">test gate 1</a>
<input checked="" type="checkbox"/>	167	<a href="#">test gate 2</a>

<<
<

1 - 2

>
>>

10

25

50

Cancel

Apply

### Min/Max Transaction Amount

Used to define minimum and maximum allowed transaction amounts for selected gates. If the selected gates have different currencies, the system converts the values automatically based on the current internal exchange rate.

Steps:

1. Select gates.
2. Choose Actions -> Min/Max Amount.
3. In the modal window specify:
  - Currency — selected from the list (only one currency can be applied);
  - Min Transaction Amount;
  - Max Transaction Amount.
4. Ensure that the minimum value is not greater than the maximum value.
5. Click Apply.

**Min/max**
×

Currency ▼

Min

Max

<input checked="" type="checkbox"/>	ID	Name
<input checked="" type="checkbox"/>	131	test gate 1
<input checked="" type="checkbox"/>	165	test gate 2

«
←

1 - 2

→
»

10

25

50

Cancel

Apply

### Warning

If the MIN or MAX value is already set at the gate level, then when applying the batch, incorrect values (for example, if MIN is greater than MAX) may be displayed as successfully applied, but will not actually be written to the gate. The display of notifications will be improved in the future.

## Acquirer Restrictions

This function allows applying **Referral** and **Velocity** filters to a group of gates, and configuring their specific parameters.

Steps:

1. Select gates.
2. Choose Actions -> Acquirer Restrictions.
3. In the modal window, check selected gates and click Next.
4. At the **Filters** tab, select one or more filters from the available list (Referral and Velocity).
5. In the right tab **Configurations**, specify filter settings:
  - Enable/Disable switch;
  - Choose currency;
  - Amount and quantity limits. If the selected gates have different currencies, the system converts the values automatically based on the current internal exchange rate;
  - Additional options (for example: *for all gates with the same descriptor*).
6. Hover over the i icon near each filter or parameter to view a tooltip description.

7. Click Apply to execute the operation.

**Acquirer restrictions** ✕

1 Selected gates — 2 Filters — 3 Configurations

<input checked="" type="checkbox"/>	ID	Name
<input checked="" type="checkbox"/>	131	test gate 1
<input checked="" type="checkbox"/>	165	test gate 2

« ‹ 1 - 2 › » 10 25 50

**Acquirer restrictions** ✕

Selected gates — 2 Filters — 3 Configurations

Search

- Referral Filters
- Whitelist check (WL)
- Predefined loyalty lists check
- Autom 

Allows processing for trusted customers only. Different acquirers have different definitions of a trusted customer, this filter allows processing for customers with emails, source/destination card or purpose in corresponding loyalty lists only. Transactions for customers that are not listed in any loyalty list will be filtered out.
- Destination Credit Card type check

### Acquirer restrictions



Selected gates     
  Filters     
  3 Configurations

Currency\*

#### Velocity Filters

Collapse / Expand

Source Credit Card Number usage frequency for last 24 hours (daily limit) (i) (trash) ^

---

(i) amount limit

(i) for all gates with the same descriptor 
 YES  NO

(i) quantity limit

(i) use calendar day 
 YES  NO

Email usage frequency for last 7 days (weekly limit) (i) (trash) ^

---

(i) use calendar week 
 YES  NO

(i) amount limit

(i) calendar week starts from Sunday 
 YES  NO

(i) for all gates with the same descriptor 
 YES  NO

(i) quantity limit

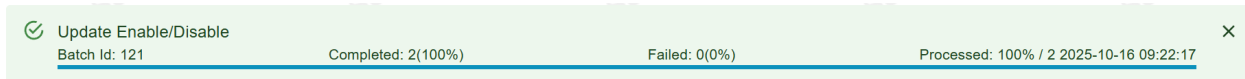
    
      

### Task Execution and Monitoring

Each batch operation is added to the execution queue and processed asynchronously by the backend system.

#### User Interface Behavior:

- While the batch task is running, an informational panel is displayed above the gate list showing:
  - Total number of gates in process
  - Current progress (percentage)
  - Count and percentage of successfully updated gates
  - Count and percentage of failed updates
- When the task completes:
  - A download link for a CSV file with failed gate updates and error codes appears.
  - The temporary CSV file is deleted after it's downloaded.
  - The user can close the panel with the Close (X) button.





## Gate Overview

Gate is a set of parameters, which identify account registered in a third-party processing system. These parameters can be used to process payment data in an external system using the messaging protocol implemented in the Processor. The Gate list screen is located at Settings -> Configuration -> Gates. This screen contains all Gates created for Manager in the system.

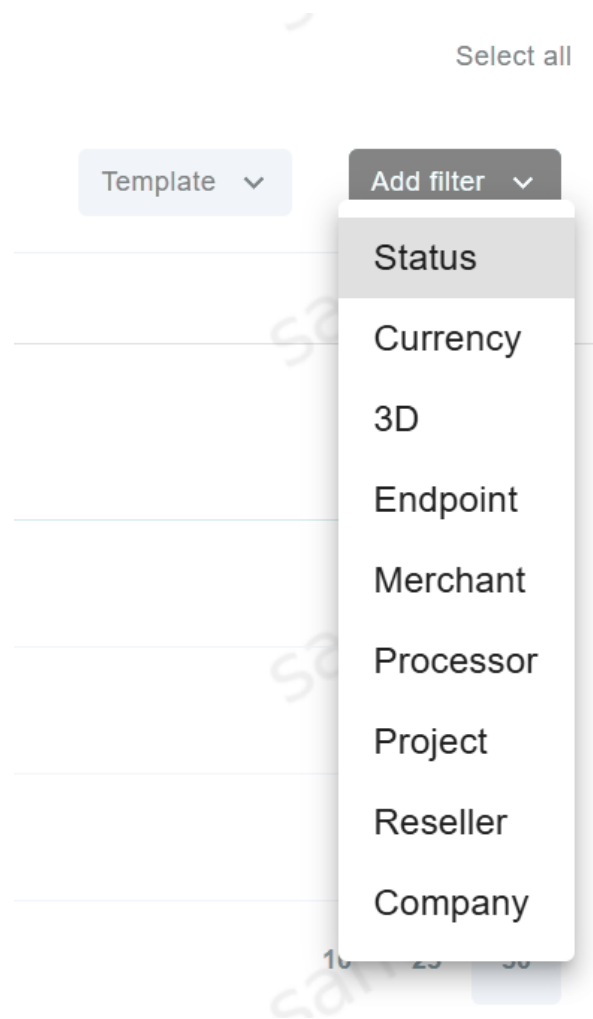
The screenshot shows the 'Gates' configuration screen. At the top, there is a header with 'Gates' on the left and 'Operations with the selected' followed by 'Actions' and 'Create' buttons on the right. Below the header, there is a 'Filters' section with a search bar and a dropdown menu set to 'All'. The main content is a table with the following columns: 'On/Off', 'ID', 'Display name', and 'Description'. The table contains two rows of data:

On/Off	ID	Display name	Description
<input type="checkbox"/>	9804	test_gate	test
<input type="checkbox"/>	9815	test_gate 222	test

 - Gate is enabled.

 - Gate is disabled.

To add new search filters, click the Add filter button. Gates search can be filtered by: Status, Currency, 3D, Endpoint, Merchant, Processor, Project, Reseller and Company.



To monitor the Gate activity, Key Performance Indicators (KPI) are used, such as: Manager earnings, Average order value, and others. The KPI submenu opens by pressing the Detailed button on the Gate search screen. See details in [KPIs Detailed View](#).

Click on the Gate name to open detailed information about this gate.

The Gate can only be added to the Project with same currency.

To work with other configuration options, see the information below.

#### Note

It is important to note that the Gate settings (such as limits, rates, client definition, etc)

override the Processor settings.

## Gate Settings

<a href="#">Create, Clone, Edit Gate</a> <a href="#">Gate Details</a>	This screen shows how to create and edit the gate. This screen shows all parameters and details about the gate.
<a href="#">Acquirer Restrictions</a>	Configurable sets of rules which allow to restrict the traffic by certain criteria (Gate and Processor levels).
<a href="#">Chain Strategy Details</a>	All information about additional cascading chains setup.
<a href="#">Chain Strategy Skips</a>	All information about additional cascading chains setup.
<a href="#">Close Day</a>	Shows information about close day procedure.
<a href="#">Batch Operations for Gates</a>	This screen shows how to make batch operations with gates.

## 9.2.4 Processor

### Processor error codes

Processor error codes provides the ability for managers to designate a selected error as a *Perilous decline*. If one of the chosen as perilous decline codes is received from the processor:

1. The corresponding notification will appear on [monitoring process](#) screen.
2. The corresponding marker will be attached to transaction and will be displayed on [Order Details](#) screen.

Processors **1 test\_processor** To Processors list

Processor error codes

Select manager

ID	Code	Message	Critical decline
20002	000	Approved	<input type="checkbox"/>
20003	001	Approved, honour with identification	<input type="checkbox"/>
20004	002	Approved for partial amount	<input type="checkbox"/>
20005	003	Approved for VIP	<input type="checkbox"/>

Common  
Acquirer restrictions  
Properties  
Logs

### Processor Details

Parameter Name	Description
Status	Shows whether processor is enabled or disabled.
Created	Shows the exact date and time of processor creation.

continues on next page

Table 245 - continued from previous page

Parameter Name	Description
Description	Shows processor description. Possible to edit after creating the processor. Please contact support team in order to change description.
Tags	Shows the tag of the processor. While searching processor by tag, all processors with the same tag will be shown. Possible to edit after creating the processor. Please contact support team in order to change tag.
Spring bean id	Shows under which Spring bean id the processor is. Represents processor logic for internal use by Payment Gateway support team.
Processor Group Id	Shows under which group id the processor is for internal use by Payment Gateway support team.
Type	General processing logic (e.g. CC)
Default card type	Shows default card type on the processor.
Code	Short code for processor. Possible to edit after creating the processor. Please contact support team in order to change code.
Dealer	Shows which Dealer is connected to the processor. Not possible to add Dealer after creating the processor.
Filter by blacklist	Allowing blacklist filter on processor level.
Transaction Types	Sale, Sale 3D, Reversal, Auth, Auth 3D, Capture, Cancel, Refund, Void, Chargeback, Chargeback Reversal, Prearbitration, Arbitration, Retrieval, Fraud, Pan Eligibility, Payout Cancel, CUP Payout. If transaction type has marker YES that means that processor can process these transaction types, if it has marker NO that means that processor cannot process them. If some type of transaction should be added or activated please contact support team.
MPI	Shows if MPI is on processor's side or not.
Close Day	Shows if close day function is available on processor.

## Processor Overview

Processor is a Payment Gateway internal entity, which encapsulates interconnection with third-party processing system (e.g. Acquirer). The Processor list screen is located at Settings -> Configuration -> Processors. This screen contains all Processors created in the system.



## Processor Settings

[Processor Error Codes](#)  
[Processor Details](#)

This screen shows how to use processor error codes.  
 This screen shows all parameters and details about the processor.

## 9.2.5 Master Endpoints

- [Master Endpoint Overview](#)
- [Master Endpoint Configuration](#)
- [Payment Cashier Forms](#)

### Master Endpoint Overview

Master Endpoint is an entity which allows to set up Parallel form, also known as [Payment Cashier](#)<sup>17</sup>. Payment Cashier hosted on Payment Gateway side can display multiple payment methods for the Payer to choose from. Master Endpoint screen allows Merchants to configure such form and select which payment methods in which order will be available to each Payer according to Payer's country.

Each specific payment method is configured on a separate Endpoint, and these specifically configured Endpoints are connected to Master Endpoint. Such Endpoints, connected to Master Endpoint, are called Auxiliary Endpoints. The Master Endpoint currency is inherited from the Project it's linked to, but Auxiliary Endpoints don't have to be in the same currency as Master Endpoint.

### Master Endpoint Configuration

In order to create Master Endpoint, go to "Settings" -> "Configuration" -> "Master endpoints" and click the "+Master Endpoint" button.

ID ↑	Name	Description
13497	master_endpoint	test

<sup>17</sup> [https://doc4.codetime.net/integration/api\\_use\\_cases/payment\\_cashier.html](https://doc4.codetime.net/integration/api_use_cases/payment_cashier.html)

After selecting Master Endpoint this screen will appear:

Auxiliary Endpoint name	Tab name	Method ref. name	Tx type	Country list	Default tab
<input type="checkbox"/> test en	Card	CREDIT_CARD	sale	-	✓
<input type="checkbox"/> test en	Withdrawal	WITHDRAWAL	sale	-	-

Click on the To details button to view Master Endpoint itself (filters, payment form, name and etc).

Click on the Edit button to configure:

- available payment methods and their order on the form (delete, move and etc.),
- initiated transaction type for each payment method (sale or preauth with capture),
- the list of countries for each payment method to be displayed.

To hide or show payment method use on/off button. Turning off payment method will turn it off only for current master endpoint.

For more information see [Payment Cashier Configuration](#).

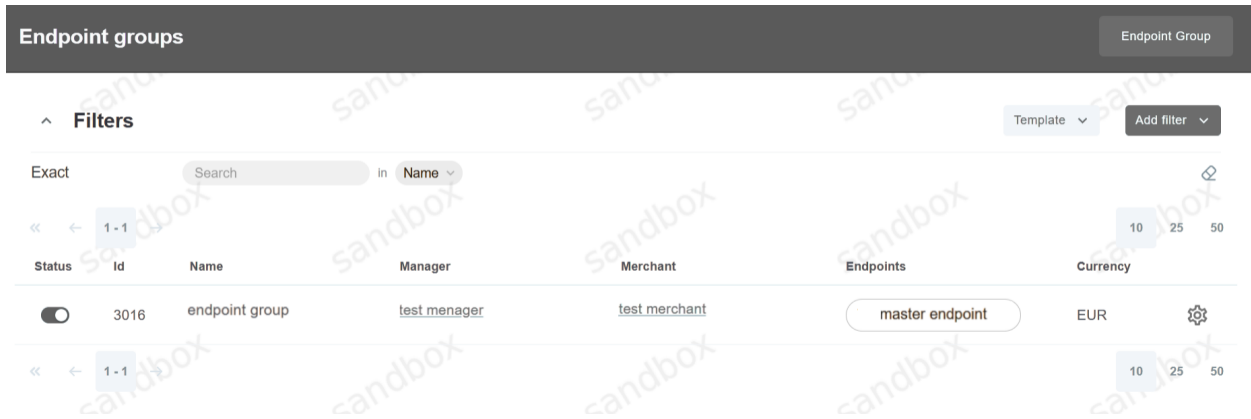
## Payment Cashier Forms

It is possible to configure custom payment forms for Master Endpoint and each connected Auxiliary Endpoint. For configuration please see [Forms Customization](#)<sup>18</sup> in integration documentation. Provide the customized forms to Doc4.0 support manager for installation.

### 9.2.6 Endpoint Groups

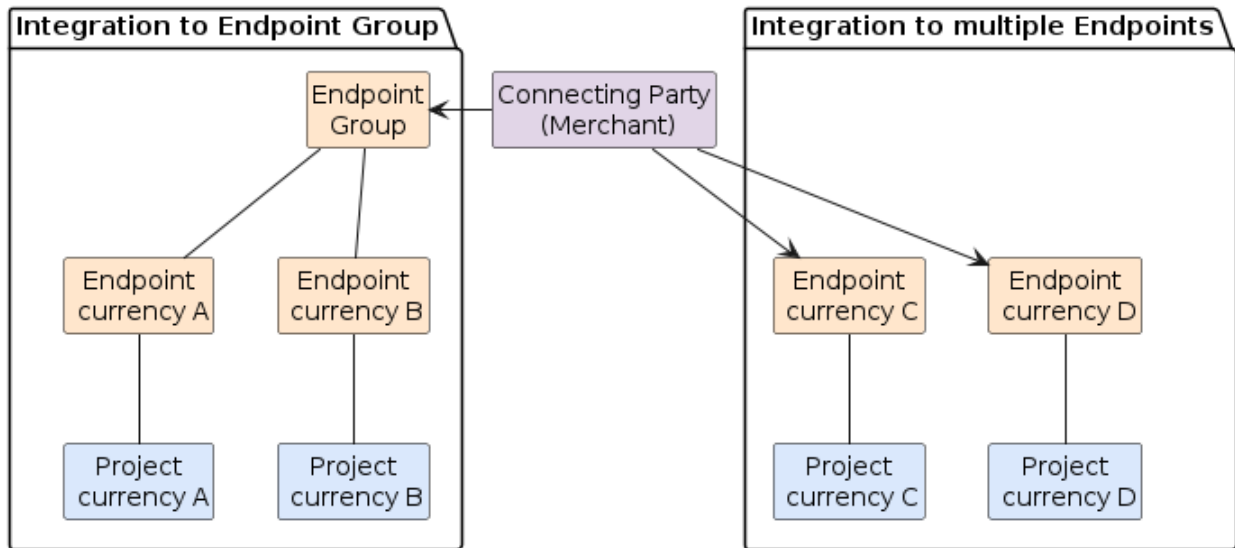
Endpoint group is an entity that combines several Endpoints and Master Endpoints in different currencies. The Endpoint Group simplifies the integration of a Connecting Party business to Doc4.0 Payment Gateway when working with various currencies. This screen allows to view configured Endpoint Groups.

<sup>18</sup> [https://doc4.codetime.net/integration/reference/forms\\_customization.html](https://doc4.codetime.net/integration/reference/forms_customization.html)



Here is shown the structure and logic of Endpoint Group:

**Options for multi-currency processing integration**



**9.2.7 Companies**

System entity which allows to combine several Gates in one entity, which can later be used in many system modules (for example limits, reports, etc.), which will simplify the work flow. Projects, Endpoints and Merchants will be added automatically, but only for information purposes. The Company list screen is located at Settings -> Configuration -> Companies.

**Companies** + Company

Filters Template Add filter

Exact Search in All

Status	ID ↑	Name
<input type="checkbox"/>	72	test company

« ← 1-1 → 10 25 50

**Warning**

Company cannot be used for routing

Select a Company in Company field on any entity in order to add it to list.  
Press + Company to create new Company.

**Company**  
Create Company Cancel Create

Company name \*  
test company

Status  
Enabled

Tags

After creating Company, all entities connected to it can be viewed in created Company screen.

Company 72 test company
To Companies list
Edit

**Status:** Enabled

**Tags:** -

**Manager:** Loyalty test manager

---

**Linked Gates**

ID	Display name
9815	test gate 222
9804	test gate

« ← 1 - 2 → » 5

---

**Linked Projects**

ID	Display name
6571	test Project
6575	test Project 2

« ← 1 - 2 → » 5

---

**Linked Endpoints**

ID	Display name
13497	test master endpoint
13461	loyalty test endpoint 2

## 9.3 Users

### 9.3.1 Merchants

- [Creating Merchant](#)
- [Merchant details](#)
  - [Linked Endpoints](#)
- [Account balance](#)
  - [Introduction](#)
  - [Account configuration](#)
    - \* [Application Rate Direction](#)
    - \* [Application Impact on Balance](#)
    - \* [Rate Types](#)
    - \* [Date Bumping Functions](#)

- [Add account configuration](#)
- [Balances](#)
  - \* [Add balance](#)
  - \* [Types](#)
    - [Balance Total](#)
    - [Balance Live](#)
    - [Short-Term Holds](#)
    - [Rolling Reserve](#)
  - \* [Endpoint Setting](#)
  - \* [Multiple Balances In One Currency](#)
- [Account configuration override](#)
  - \* [Creation Date Changing](#)
  - \* [Export Balance Transactions](#)
  - \* [Balance Reconciliation](#)
- [Adjustments](#)
  - \* [Manual Adjustment](#)
  - \* [Adjustment API](#)
  - \* [Export Adjustments](#)
  - \* [Scheduled Adjustment](#)

## Creating Merchant

To see and search all Merchants, go to Settings -> Users -> Merchants, then in order to create new Merchant press to + New Merchant button:

The screenshot shows the 'Merchants' management page. At the top right, there are buttons for 'Brief', 'Full', 'Setting view', and 'New Merchant' (highlighted with a red box). Below this is a 'Filters' section with a 'Template' dropdown and an 'Add filter' button. A search bar is present with the text 'Exact' and 'in All'. Below the search bar is a table with the following columns: Status, ID ↑, Name, E-Mail, Login, and an unlabeled column. The table contains one row with the following data: Status (toggle off), ID (4763), Name (Loyalty test merchant), E-Mail (test.test@gmail.com), Login (loyalty\_test\_merchant), and the unlabeled column (loyalty\_test\_merchant). At the bottom of the table, there are pagination controls showing '1 - 1' and a dropdown for page size with options '10', '25', and '50'.

Below are all the fields available for filling in:

Field name	Description	Necessity
Login	Login which is required while logging in the system. <b>Cannot be changed after creation.</b>	Required
Password	Password for login. In order to change it, contact support.	Required
Display Name	Merchant name which will be displayed.	Required
E-mail	Contact E-mail which will be added to this Merchant account.	Required
Control Key	Secret key which will be used for signing requests.	Required
Payment group	Currently not in use. "Common" is a default value. <b>Cannot be changed after creation.</b>	Required
Name	Shows Merchant's contact person name. This name will be displayed only in merchant details.	Required
Surname	Shows Merchant's contact person surname. This name will be displayed only in merchant details.	Required
Business type	Will show which business type Merchant has.	Optional
Returning customer approve sessions count	Shows after how many approved transactions, Payer will be considered as Returning for Merchant.	Optional
Registration country	Shows Merchant country.	Optional
Merchant site URL	Merchant site URL can now be set on Merchant details screen and included in E-mail notifications (MERCHANT_SITE_URL macro).	Optional
Organization	Shows Merchant's organization name.	Optional
Tags	Shows tags by which Merchant can be found later in system.	Optional
API descriptor	Manager can set API descriptor parameter in the Merchant profile. This value will be returned instead of gate values specified in <a href="#">Gate Details</a> .	Optional

### Merchant details

The screen allows to view all details of created merchant, change settings, configure merchant balance and view linked endpoints.

### Linked Endpoints

This section by default display enabled linked endpoints to merchant. By selecting Show disabled endpoints the sheet will be replaced and will display disabled linked endpoints.

## Linked Endpoints

Show disabled endpoints

ID	Display name
13497	test master endpoint
13461	loyalty test endpoint 2
13453	loyalty test endpoint

« ← 1 - 3 → 5

## Account balance

### Introduction

Manager can configure and view multiple balances for each Merchant account and [request balances by API with manager access](#)<sup>19</sup>. These balances calculate the total accumulated funds from transactions associated with Merchant. Balances calculation supports configured rate plans, including STH - Short-Term Hold and RR - Rolling Reserve.

Manager can add adjustments to Merchant balances on UI or with [adjustment API](#)<sup>20</sup> to reflect non-transactional changes in Merchant balance. See [Get Balance Adjustments](#)<sup>21</sup>.

By default Merchants can't see their balances on UI or [request balances by API with merchant access](#)<sup>22</sup>, but this functionality can be granted to each Merchant individually.

Merchant balances can be configured via Accounts tab on Merchant details screen.

To set up calculation of balances, follow these steps:

1. Set [Account configuration](#) to define how and which transactions and rates should affect [balances](#).
2. Set [Balances](#) for required [currencies](#) and [endpoints](#).
3. Set [Account configuration override](#) for specific [Balances](#) (if needed).

First balance is funded by sale transactions and defunded by payout transactions and is set up for USD currency, also Merchant rates applied for sale transactions. Second balance has override for sale transactions which will deduct balance with amount calculated from manager rate plan.

Below is the example of fully configured balance with highlighted steps.

<sup>19</sup> [https://doc4.codetime.net/integration/API\\_commands/api\\_v2\\_get\\_balance\\_manager.html](https://doc4.codetime.net/integration/API_commands/api_v2_get_balance_manager.html)

<sup>20</sup> [https://doc4.codetime.net/integration/API\\_commands/api\\_v2\\_get\\_balance\\_merchant.html](https://doc4.codetime.net/integration/API_commands/api_v2_get_balance_merchant.html)

<sup>21</sup> [https://doc4.codetime.net/integration/API\\_commands/accounts\\_adjustments.html](https://doc4.codetime.net/integration/API_commands/accounts_adjustments.html)

<sup>22</sup> [https://doc4.codetime.net/integration/API\\_commands/api\\_v2\\_get\\_balance\\_merchant.html](https://doc4.codetime.net/integration/API_commands/api_v2_get_balance_merchant.html)

Configuration

+ Add

ID	Transaction type	Apply rate	Apply direction	Date bump	Gate	Endpoint	Manager name
379	sale	NOTHING	ADD	ASAP			
384	sale	MANAGER	ADD	ASAP_pl...	-	-	
385	fraud	ACQUIRER	ADD	DAY+1	-	-	
386	transfer	DEALER	DEDUCT	BDAY+1			
387	void	RESELLER	ADD	BDAY+10	-	-	

ACCOUNT BALANCES	PROCESSOR BALANCES	VIRTUAL CARD BALANCES	GATE GROUP BALANCES
------------------	--------------------	-----------------------	---------------------

Account balances

+ Add

	Def	ID	Balance name	End points	Created date	Reseller name	Manager name	Balance total	Ba Liv	
				194	New test 3	No	27.08.2025 21:48:28	test manager	0	0
				193	New test 2	No	27.08.2025 21:48:17	test manager	0	0
				190	New test	Yes	20.08.2025 13:29:56	test manager	0	0

Configuration override for New test 2 balance

Remove all

+ Add

ID	Transaction type	Apply rate	Apply direction	Date bump	Gate	Endpoint	Manager name
388	sale	MERCHANT	DEDUCT	DAY+1	-	-	
389	capture	MERCHANT	DEDUCT	DAY+1	-	-	

## Account configuration

Merchant's accounts can be configured via Accounts tab. See example of accounts window below:

Merchant Accounts 4763 test merchant

### Configuration + Add

ID	Transaction type	Apply rate	Apply direction	Date bump	Gate	Endpoint	Manager name
379	sale	NOTHING	ADD	ASAP			
384	sale	MANAGER	ADD	ASAP_pl...			
385	fraud	ACQUIRER	ADD	DAY+1			
386	transfer	DEALER	DEDUCT	BDAY+1			
387	void	RESELLER	ADD	BDAY+10			

ACCOUNT BALANCES
PROCESSOR BALANCES
VIRTUAL CARD BALANCES
GATE GROUP BALANCES

### Account balances + Add

## Application Rate Direction

Transactions with rate only can select both ADD and DEDUCT. For each transactions apply rate can be specified differently. For example, if it is needed to deduct a commission for a Payout transaction in addition to deducting the amount of the Payout itself then need to choose DEDUCT in the Apply direction configuration.

## Application Impact on Balance

Different types of transactions count differently when calculating balances. List of application impact on balance is shown in the table below:

Transaction type	Impact on balance
sale	Add
capture	Add
dispute	Add
chargeback_reversal	Add
arbitration	Add
payout_cancel	Add
chargeback	Deduct

continues on next page

Table 248 - continued from previous page

Transaction type	Impact on balance
prearbitration	Deduct
reversal	Deduct
payout	Deduct
transfer (deposit2card)	Deduct
preauth	Rate only
cancel	Rate only
fraud	Rate only
retrieval	Rate only
pan_eligibility	Rate only
create_card_mapping	Rate only
update_card_mapping	Rate only
inquire_card_mapping	Rate only
delete_card_mapping	Rate only
mfo_scoring	Rate only
account_verification	Rate only
void	Rate only

### Rate Types

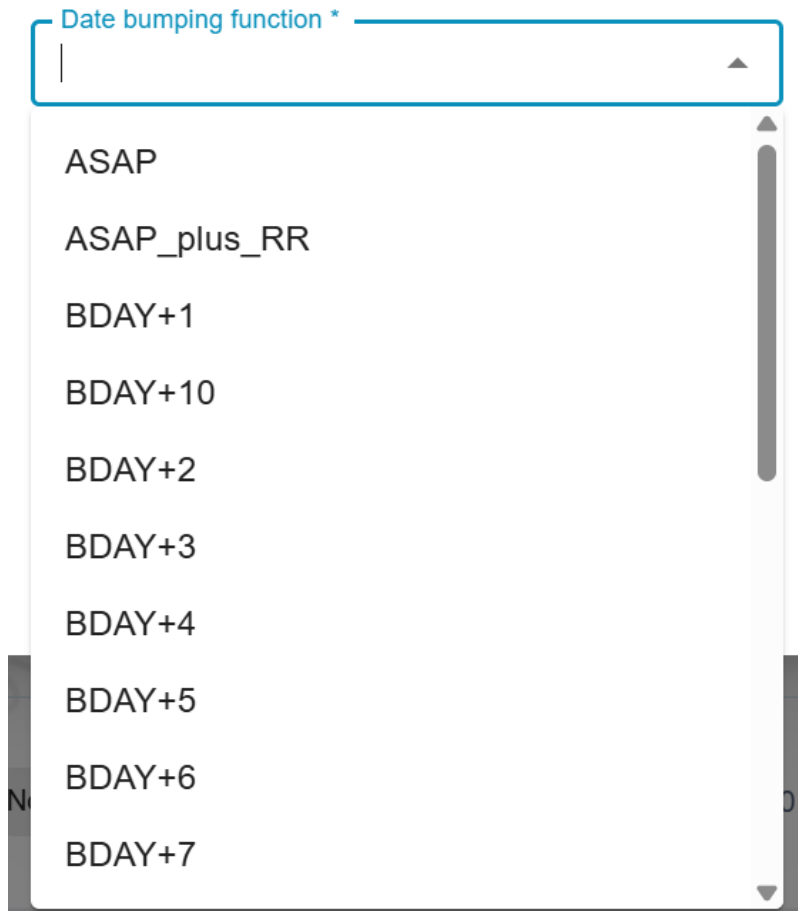
For each type of transaction, Manager can separately apply the rate (commission). Possible rate types are:

- Nothing
- Merchant
- Reseller
- Manager
- Dealer
- Acquirer

### Date Bumping Functions

Date bumping functions allows to choose when the funds will be credited to the account. Possible values are:

- ASAP - crediting funds without delay. Doesn't include STH and Rolling Reserve.
- ASAP\_plus\_RR - crediting funds ASAP and counts Rolling reserve. Doesn't include STH.
- DAY + n - crediting funds from STH after the specified number of days + Rolling Reserve.
- BDAY + n - crediting funds from STH after the specified number of business days + Rolling Reserve.



### Add account configuration

To create new account balance, add account configuration and balance:

1. To add new account configuration press +Add button in configuration field and set up the transaction type and rates, which will add or deduct funds from balance by settings described in [Accounts Configuration](#). Optionally, gate and endpoint can be selected - if they are left empty, balance configuration will work for all gates and endpoints of selected Merchant.

Add configuration



Transaction type \*

Apply rate type \*

Application rate direction \*

Date bumping function \*

Gate

Endpoint

Manager name \*

Cancel

Add

**Balances**

**Add balance**

2. To add new account balance press +Add button in account balances field and set up balance and manager name and currency. Detailed setting of account balance is described below in this section.

Add account balance



Balance name \*

Manager name \*

Reseller name

Currency \*

Endpoints

Cancel Add

Types

There are four types of funds for each balance:

Balance Total

Balance Total - amount of funds calculated based on configuration, including STH and RR.

Account balances + Add

End points	Created date	Reseller name	Manager name	Balance total	Balance Live	STH	Rolling Reserve	Currency	Max Rolling Reserve
No	27.08.2025 21:48:28		test menager	1222	1222	0	0	EUR	-

Balance Live

Balance Live - amount of funds calculated based on configuration, excluding STH and RR.

Account balances

+ Add

End points	Created date	Reseller name	Manager name	Balance total	Balance Live	STH	Rolling Reserve	Currency	Max Rolling Reserve
No	27.08.2025 21:48:28		test menager	1222	1222	0	0	EUR	-

**Example**

Balance Live = Balance Total - STH - RR.

**Short-Term Holds**

Short-Term Holds - amount of funds calculated based on the Date bumping function.

Account balances

+ Add

End points	Created date	Reseller name	Manager name	Balance total	Balance Live	STH	Rolling Reserve	Currency	Max Rolling Reserve
No	27.08.2025 21:48:28		test menager	1222	1222	0	0	EUR	-

**Example**

Transactions passed today from 11:01 to 11:59 will be credited at 12:01 on the day on which they should be credited according to the parameter DAY + n or BDAY + n.

**Rolling Reserve**

Rolling Reserve (Long-Term Holds or Holds from Rate Plan) - amount of funds calculated based on the rate plan hold. Max Rolling Reserve - a limit on the amount of Rolling Reserve.

Account balances + Add

Created date	Reseller name	Manager name	Balance total	Balance Live	STH	Rolling Reserve	Currency	Max Rolling Reserve
17.10.2024 11:38:49		TestManager	1009321	1004701	0	4620	USD	- ←

Max Rolling Reserve can be changed in the Change Max Rolling Reserve window that appears. To set or edit the Max Rolling Reserve, click on the value -.

**Change max rolling reserve** ✕

Cancel

Update

**Warning**

Rolling reserve will be credited to balance on Transaction Date + Period from Rate Plan + 1 day. When the Max Rolling Reserve limit is reached, the total amount of hold funds will not increase and the Rolling Reserve calculated from next transactions will be added to balance live instead. Also, If the Max Rolling Reserve is set later and is less than the current accumulated Rolling Reserve, then the Rolling Reserve calculated from next transactions will be added to the balance live.

**Endpoint Setting**

There is possibility to selecting one or more endpoints for each balance, according to which balance will be calculated.

Endpoint can be added when creating a balance:

**Add account balance** ×

---

▼

▼










▼

▼

---

Or it can be specified for an existing balance by clicking on one of the area highlighted in the picture:

**Account balances** + Add

Def	ID	Balance name	End points	Created date	Reseller name	Manager name	Balance total	Ba Liv
   <input type="radio"/>	194	New test 3	No	27.08.2025 21:48:28		test menager	0	0
   <input type="radio"/>	193	New test 2	No	27.08.2025 21:48:17		test menager	0	0
   <input type="radio"/>	190	New test	Yes	20.08.2025 13:29:56		test menager	0	0

This picture also displays the difference between the balances configured with and without the specified Endpoint.

### Multiple Balances In One Currency

There can be several balances configured for the same currency.

In this case, only one of the balances can be without the specified Endpoints. When creating all subsequent balances, it is mandatory to specify the Endpoint. The calculation is made for each balance separately: the balance without the specified Endpoints is counted only for those Endpoints for which a separate balance has not been created.

## Edit account balance



Balance name \*













Manager name \*

Endpoints

### Account configuration override

There is possibility to change configuration for every balance (not for all Merchant's balances). For this case need to press Configuration button as in the picture below:

**Account balances** + Add

	Def	ID	Balance name	End points	Created date	Reseller name	Manager name	Balance total	Ba Liv
   		194	New test 3	No	27.08.2025 21:48:28		test menager	0	0
   		193	New test 2	No	27.08.2025 21:48:17		test menager	0	0
   		190	New test	Yes	20.08.2025 13:29:56		test menager	0	0

And after this press the Add button:

**Account balances** + Add

Def	ID	Balance name	End points	Created date	Reseller name	Manager name	Balance total	Ba Liv
⋮ ⚙️ ⚙️ ○	194	New test 3	No	27.08.2025 21:48:28		test menager	1222	12
⋮ ⚙️ ⚙️ ○	193	New test 2	No	27.08.2025 21:48:17		test menager	0	0
⋮ ⚙️ ⚙️ ○	190	New test	Yes	20.08.2025 13:29:56		test menager	0	0

**Configuration override for New test 3 balance** Remove all + Add

ID	Transaction type	Apply rate	Apply direction	Date bump	Gate	Endpoint	Manager name
Nothing is found.							

In this window can be changed the balance settings as well as in the Configuration

### Warning

If at least one operation type is overrode, balance will count by overrode configuration and only for overrode operations. If there is no overrode for operation types, than balance will counts by main configuration.

Example: For balance 191 Sale and Payout operations are overrode, that means for this balance main configuration doesn't affect.

**Configuration**
+ Add

ID	Transaction type	Apply rate	Apply direction	Date bump	Gate	End point	Manager name	
458	sale	MANAGER	ADD	ASAP_plus_RR			BalanceTestManager	
2152	capture	NOTHING	DEDUCT	ASAP			BalanceTestManager	
2154	fraud	ACQUIRER	ADD	DAY+1	MerchantByByrka14 3DS	MerchantByByrka14 IN	BalanceTestManager	
2153	transfer	DEALER	DEDUCT	BDAY+1			BalanceTestManager	
2155	void	RESELLER	ADD	BDAY+10	MerchantByByrka14 Non3D	MerchantByByrka14 OUT	BalanceTestManager	

Account balances
Processor balances
Virtual card balances
Gate group balances

**Account balances**
+ Add

ID	End Points	Balance name	Created date	Reseller name	Manager name	Balance total	Balance Live	STH	Rolling Reserve	Currency	Def	
183	No	saa	2022-04-12 15:18:35		BalanceTestManager	113.1	113.1	0	0	USD	<input type="radio"/>	
1989	No	DocumentationBalance	2023-06-09 10:40:16		BalanceTestManager	0	0	0	0	EUR	<input type="radio"/>	
1990	Yes	TestBalance2	2023-06-09 10:50:06		BalanceTestManager	0	0	0	0	USD	<input type="radio"/>	

Configuration override for TestBalance2 balance
Remove all
+ Add

ID	Transaction type	Apply rate	Apply direction	Date bump	Gate	End point	Manager name	
2156	sale	MERCHANT	DEDUCT	DAY+1			BalanceTestManager	
2157	capture	MERCHANT	DEDUCT	DAY+1			BalanceTestManager	






To remove configuration override press Remove all button and confirm the deletion.

### Creation Date Changing

To change balance created date press Change created date button:


Account balances + Add

Def	ID	Balance name	End points	Created date	Reseller name	Manager name	Balance total	Ba Liv
	194	New test 3	No	27.08.2025 21:48:28		<a href="#">test menager</a>	1222	12
		New test 2	No	27.08.2025 21:48:17		<a href="#">test menager</a>	0	0
		New test	Yes	20.08.2025 13:29:56		<a href="#">test menager</a>	0	0

-  Edit
-  Reconciliation balance
-  Change created date
-  Export transaction (csv)
-  Remove

Select date of creation and press Update button:

### Change created date ×

2025-08-27 21:48:28 

CancelUpdate

After changing the creation date, use [reconciliation](#) to recalculate the balance.

### Export Balance Transactions

To use Balance reconciliation press on Reconciliation balance button:

**Account balances** + Add

Def	ID	Balance name	End points	Created date	Reseller name	Manager name	Balance total	Ba Liv
	194	New test 3	No	27.08.2025 21:48:28		test menager	1222	12
		New test 2	No	27.08.2025 21:48:17		test menager	0	0
		New test	Yes	20.08.2025 13:29:56		test menager	0	0

**Adjustments for New test 3 balance** Export + Add

COMMON SCHEDULED Full adjustment amount: 1 222

ID ↑	Adjustment date	Adjustment amount	Application date	External ID	External source	External info
243	27.08.2025 22:11	1 222	27.08.2025 22:13		Bank	

Navigation: << 1-1 >> Page: 10 25 50

To export balance transactions press on Export Transactions button and select transactions' period:

Account balances

+ Add

Def	ID	Balance name	End points	Created date	Reseller name	Manager name	Balance total	Ba Liv
	194	New test 3	No	27.08.2025 21:48:28		test manager	1222	12
		New test 2	No	27.08.2025 21:48:17		test manager	0	0
		New test	Yes	20.08.2025 13:29:56		test manager	0	0

- Edit
- Reconciliation balance
- Change created date
- Export transaction (csv)
- Remove

Period

×

Start  to End

The maximum period is 31 days

**Note**

The maximum period is 31 days.

**Note**

The date is counted as [day\_From, day\_To), so the last day will not be included in the interval.

CSV file contains the following fields:

Bank Date	Session Id	Transaction Type	Transaction Status	Live Balance Change	Rolling Reserve Amount	Rolling Reserve Date	Short-Term Hold Date	Short-Term Hold Date
07.04.2022 13:40	6823963	sale	approved	0.000	0.000	08.04.2022 0:00	10.420	08.04.2022 13:40
07.04.2022 13:45	6823967	sale	approved	0.000	0.000	08.04.2022 0:00	200.000	08.04.2022 13:45
07.04.2022 14:44	6823970	sale	approved	0.000	0.000	08.04.2022 0:00	300.000	08.04.2022 14:44
07.04.2022 15:30	6823977	sale	approved	0.000	0.000	08.04.2022 0:00	300.000	08.04.2022 15:30
11.04.2022 11:10	6823999	sale	approved	0.000	0.000	12.04.2022 0:00	700.000	12.04.2022 11:10
07.04.2022 15:19	6823975	payout	approved	-100.000	0.000		0.000	
07.04.2022 15:28	6823976	payout	approved	-100.000	0.000		0.000	
07.04.2022 16:41	6823978	payout	approved	-100.000	0.000		0.000	
08.04.2022 15:17	6823995	payout	approved	-100.000	0.000		0.000	
08.04.2022 15:18	6823996	payout	approved	-100.000	0.000		0.000	

**Warning**

“Reserve date” and “STH date” fields are the date and time when amount will affect the balance. The STH date in report doesn’t count hourly period described in balance types.

**Balance Reconciliation**

Reconciliation allows to recalculate balance after changes.

To reconcile balance press 3 dots near balance then Reconciliation Balance button and after Reconcile button:

Account balances

+ Add

Def	ID	Balance name	End points	Created date	Reseller name	Manager name	Balance total	Ba Liv
	194	New test 3	No	27.08.2025 21:48:28		test manager	1222	12
		New test 2	No	27.08.2025 21:48:17		test manager	0	0
		New test	Yes	20.08.2025 13:29:56		test manager	0	0

- Edit
- Reconciliation balance
- Change created date
- Export transaction (csv)
- Remove

Adjustments for New test 3 balance

Export

+ Add

COMMON SCHEDULED

Full adjustment amount: 1 222

ID ↑	Adjustment date	Adjustment amount	Application date	External ID	External source	External info
243	27.08.2025 22:11	1 222	27.08.2025 22:13		Bank	

1 - 1

10 25 50

**Note**

Only Total and Live balances are reconciled. RR and STH can not be reconciled; their amount will be credited to live balance according to the configuration at the time the transaction was created.

Move Rolling Reserve allows to manually transfer the Rolling Reserve to the active balance, before the release date of the holding. To move Rolling Reserve press 3 dots near balance then Move Rolling Reserve button:

The screenshot displays the 'Account Balances' section of the application. At the top, there are four tabs: 'ACCOUNT BALANCES', 'PROCESSOR BALANCES', 'VIRTUAL CARD BALANCES', and 'GATE GROUP BALANCES'. Below the tabs, the 'Account Balances' title is shown next to a '+ Add' button. A table lists account balances with the following columns: DEF, BALANCE NAME, END POINTS, CREATED DATE, RESELLER NAME, MANAGER NAME, and BALANCE TOTAL. A row for 'Test' is selected, showing 'Yes' for END POINTS, '20.12.2023 09:04:21' for CREATED DATE, 'Test Manager' for MANAGER NAME, and '21590' for BALANCE TOTAL. A context menu is open over the 'Test' row, listing actions: Edit, Move rolling reserve (highlighted), Reconciliation balance, Change created date, and Export transaction (csv).

DEF	BALANCE NAME	END POINTS	CREATED DATE	RESELLER NAME	MANAGER NAME	BALANCE TOTAL
	Test	Yes	20.12.2023 09:04:21		Test Manager	21590

**Adjustments**

Adjustments allows to change balances amount without making any transactions.

List of adjustments and full adjustment amount can be viewed by clicking on Adjustments button:

**Adjustments for New test 3 balance** Export + Add

COMMON SCHEDULED Full adjustment amount: **1 222**

ID ↑	Adjustment date	Adjustment amount	Application date	External ID	External source	External info
243	27.08.2025 22:11	1 222	27.08.2025 22:13		Bank	

« ← 1 - 1 → 10 25 50

For the convenience of users, adjustments can be sorted by ID using the button below:

**Adjustments for New test 3 balance** Export + Add

COMMON SCHEDULED Full adjustment amount: **1 222**

**ID ↓** Adjustment date Adjustment amount Application date External ID External source External info

243	27.08.2025 22:11	1 222	27.08.2025 22:13		Bank	
-----	------------------	-------	------------------	--	------	--

« ← 1 - 1 → 10 25 50

### Manual Adjustment

Adjustment amount and external source of the adjustment are mandatory. Adjustments for balance can be made via Add+ button:

**Adjustments for New test 3 balance** Export **+ Add**

COMMON SCHEDULED Full adjustment amount: **1 222**

ID ↓ Adjustment date Adjustment amount Application date External ID External source External info

243	27.08.2025 22:11	1 222	27.08.2025 22:13		Bank	
-----	------------------	-------	------------------	--	------	--

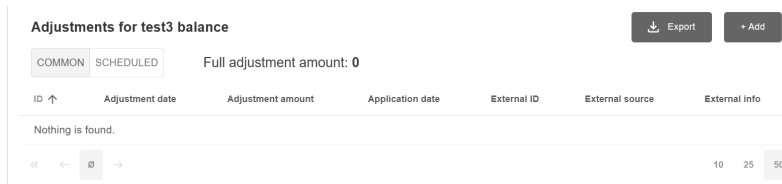
« ← 1 - 1 → 10 25 50

When adding adjustment, next fields can be specified:

- Adjustment amount
- External ID
- External source
- External info

### Note

Adjustment amount and External source are mandatory fields:



## Adjustment API

In addition to manual adjustments, it is possible to make adjustments via API.

To do this, a tsv has to be created, zipped and sent via the API. API command with examples is specified in the [integration documentation](#)<sup>23</sup>.

## Export Adjustments

To export all adjustments for specific balance press the Export button, specify period of time and after that press Export button. The csv file of adjustments will download automatically.

### Note

The maximum period is 31 days

Downloaded file contains next fields:

- Create Date
- Adjustment Amount
- Adjustment Application Date
- External Adjustment Unique Id
- External Source Name

<sup>23</sup> [https://doc4.codetime.net/integration/API\\_commands/accounts\\_adjustments.html](https://doc4.codetime.net/integration/API_commands/accounts_adjustments.html)

- External Adjustment Info

The first line of the file contains the period and the sum of all adjustments.

	A	B	C	D	E	F
1	Full Adjustment Amount from 2023-06-09 to 2023-06-09: 110.000					
2	Create Date	Adjustment Amount	Adjustment Application Date	External Adjustment Unique Id	External Source Name	External Adjustment Info
3	09-06-23 12:15	55	09-06-23 12:15		merchant info	
4	09-06-23 12:28	55	09-06-23 12:28		merchant test	

## Scheduled Adjustment

This functionality helps to configure a monthly/weekly fee, which can be set up on the appointed dates every month/week. Scheduled for balance adjustments can be made via Add+ button :

Adjustments for te22 balance + Add

COMMON SCHEDULED

STATUS	ID	PERIOD	DATE	NEXT SCHEDULE DATE	LAST RUN DATE	AMOUNT	AUTOMATIC
Nothing is found.							

« ← ∅ → 10 25 50

When adding adjustment, next fields can be specified:

- Date of first adjustment
- Date of last adjustment
- Amount
- Currency
- Automatically stop creating adjustments when a merchant is disabled
- Automatically stop making adjustments when balance goes negative or zero
- I am aware that the creation of such an adjustment can significantly affect the balance of the merchant, and lead to its uncontrolled change in the long term, which can cause financial losses due to the possibility of unlimited withdrawal of funds due to an uncontrolled increase of the merchant balance. **This checkbox is mandatory**

## Create adjustment

For te22



WEEKLY

MONTHLY

Date of first adjustment \*

Date of last adjustment \*

Amount \*

Currency \* 

- Automatically stop creating adjustments when a merchant is **disabled**
- Automatically stop making adjustments when balance **goes negative or zero**



I am aware that the creation of such an adjustment can significantly affect the balance of the merchant, and lead to its uncontrolled

- change in the long term, which can cause financial losses due to the possibility of unlimited withdrawal of funds due to an uncontrolled increase of the merchant balance.

Cancel



Create

Status indicates whether the adjustment is active or not. It can also be turned on or off by clicking on it:

STATUS	ID	PERIOD	DATE	NEXT SCHEDULE DATE	LAST RUN DATE	AMOUNT	AUTOMATIC		
<input checked="" type="checkbox"/>	1	Weekly	22.12.2024 - 31.05.2099	22.12.2024	-	55 AED	-	-	 



<< < 1-1 > >> 10 25 50

ID is unique identifier of the scheduled adjustment:

STATUS	ID	PERIOD	DATE	NEXT SCHEDULE DATE	LAST RUN DATE	AMOUNT	AUTOMATIC		
<input checked="" type="checkbox"/>	1	Weekly	22.12.2024 - 31.05.2099	22.12.2024	-	55 AED	-	-	 

<< < 1-1 > >> 10 25 50

Period shows which schedule is selected for the following adjustment:

STATUS	ID	PERIOD	DATE	NEXT SCHEDULE DATE	LAST RUN DATE	AMOUNT	AUTOMATIC		
<input checked="" type="checkbox"/>	1	Weekly	22.12.2024 - 31.05.2099	22.12.2024	-	55 AED	-	-	 

<< < 1-1 > >> 10 25 50

Date shows time interval from first adjustment to the last adjustment:

STATUS	ID	PERIOD	DATE	NEXT SCHEDULE DATE	LAST RUN DATE	AMOUNT	AUTOMATIC			
<input checked="" type="checkbox"/>	1	Weekly	22.12.2024 - 31.05.2099	22.12.2024	-	55 AED	-	-		

<< < 1-1 > >> 10 25 50

Next schedule date shows when is the next scheduled adjustment:

STATUS	ID	PERIOD	DATE	NEXT SCHEDULE DATE	LAST RUN DATE	AMOUNT	AUTOMATIC			
<input checked="" type="checkbox"/>	1	Weekly	22.12.2024 - 31.05.2099	22.12.2024	-	55 AED	-	-		

<< < 1-1 > >> 10 25 50

Last run date shows when was the last scheduled adjustment:

STATUS	ID	PERIOD	DATE	NEXT SCHEDULE DATE	LAST RUN DATE	AMOUNT	AUTOMATIC		
<input checked="" type="checkbox"/>	1	Weekly	22.12.2024 - 31.05.2099	22.12.2024	-	55 AED	-	-	

<< < 1-1 > >> 10 25 50

Amount shows the adjustment amount:

STATUS	ID	PERIOD	DATE	NEXT SCHEDULE DATE	LAST RUN DATE	AMOUNT	AUTOMATIC		
<input checked="" type="checkbox"/>	1	Weekly	22.12.2024 - 31.05.2099	22.12.2024	-	55 AED	-	-	

<< < 1-1 > >> 10 25 50

Automatic shows in which conditions scheduled adjustment will be stopped:

STATUS	ID	PERIOD	DATE	NEXT SCHEDULE DATE	LAST RUN DATE	AMOUNT	AUTOMATIC
<input checked="" type="checkbox"/>	2	Weekly	22.12.2024 - 31.05.2099	22.12.2024	-	55 AED	<div style="border: 1px solid black; padding: 2px;">                     Stop when disabled                      Stop when balance goes negative or zero                 </div>



<< < 1-1 > >>
 10 25 50

Edit can be used to edit scheduled adjustment:

STATUS	ID	PERIOD	DATE	NEXT SCHEDULE DATE	LAST RUN DATE	AMOUNT	AUTOMATIC
<input checked="" type="checkbox"/>	1	Weekly	22.12.2024 - 31.05.2099	22.12.2024	-	55 AED	- -

<< < 1-1 > >>
 10 25 50

Delete can be used to delete scheduled adjustment:

STATUS	ID	PERIOD	DATE	NEXT SCHEDULE DATE	LAST RUN DATE	AMOUNT	AUTOMATIC		
<input type="checkbox"/>	1	Weekly	22.12.2024 - 31.05.2099	22.12.2024	-	55 AED	-	-	 

« < 1-1 > »

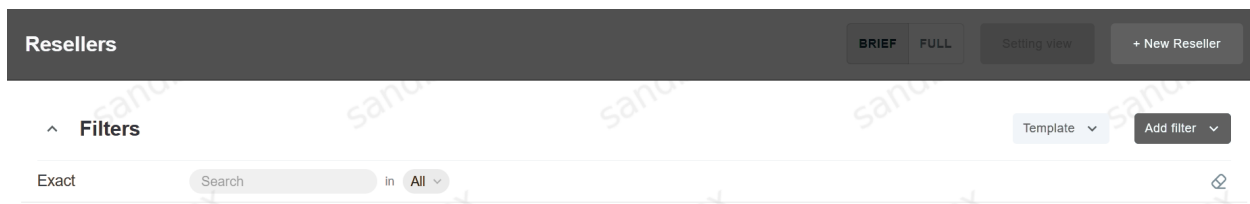
10 25 50

## 9.3.2 Resellers

- [Creating Reseller](#)

### Creating Reseller

To see and search all Resellers, go to Settings -> Users -> Resellers, then in order to create new Reseller press to + New Reseller button:



Below are all the fields available for filling in:

Field name	Description	Necessity
Login	Login which is required while logging in the system. Cannot be changed after creation.	Required
Password	Password for login. In order to change it, contact support.	Required
Display Name	Reseller name which will be displayed. Can be changed after creation.	Required
E-mail	Contact E-mail which will be added to this Reseller account. Can be changed after creation.	Required
Control Key	Secret key which will be used for signing requests. Can be changed after creation.	Required
Payment group	Currently not in use. "Common" is a default value. Cannot be changed after creation.	Required
Name	Shows Reseller's contact person name. This name will be displayed only in Reseller details. Can be changed after creation.	Required
Surname	Shows Reseller's contact person surname. This name will be displayed only in Reseller details. Can be changed after creation.	Required
Logo	The logo of Reseller. Can be changed after creation.	Optional
Organization	Shows Reseller's organization name. Can be changed after creation.	Optional

continues on next page

Table 249 - continued from previous page

Field name	Description	Necessity
Tags	Shows tags by which Reseller can be found later in system. Can be changed after creation.	Optional

The Users screen is located at Settings -> Users. This screen allows to view, configure and create user accounts in the system. Each user account can have multiple linked employees.

<a href="#">Merchants</a>	This screen allows to create, configure and see all Merchant accounts created in system.
<a href="#">Resellers</a>	This screen allows to create, configure and see all Reseller accounts created in system.

## 9.4 Employees

- [Create Employee Account](#)
- [User Privileges](#)
  - [Merchant](#)
  - [Reseller](#)
  - [Manager](#)
  - [Dealer](#)
  - [Superior](#)

### 9.4.1 Create Employee Account

Creating new accounts to access the system is available in “Settings” - “Employees”.

The Employees tab contains a list of all employees accounts, established in the system for the all users connected to manager.

New employee account can be created with the Add User button. The following form must be filled:

**Create User** Cancel Create

Login\*

Password F\*8V7geK [Generate new password](#)

Display Name\*

E-mail\*

Principal role\*

Status  
Enabled

Name \*

Surname \*

Organization

Login IPs/masks whitelist

Scope username should be clicked in order to open the drop-down menu and select main account of the manager or other user, which needs a new employee account:

Scope username\*

Manager134494Test

Next, select one of available employee roles in the system:

MANAGER-FINANCE  
MANAGER-LIMITED-VIEW  
MANAGER-LOYALTY  
MANAGER-LOYALTY-EXTENDED  
MANAGER-NO-FINANCE  
MANAGER-NO-SETTINGS  
MANAGER-PHONE  
MANAGER-RECONCILIATION  
MANAGER-RESTRICTED  
MANAGER-SPECIFIC  
MANAGER-SUPPORT  
MANAGER-TRANSACTION  
MANAGER-VIEW

After the personal account is created, an employee can immediately log in. Login and password are generated at the stage of creating a personal account (do not forget to save the password beforehand). If the password was not saved, it can be reset on employee details screen.

Password

When employee logs in to the account for the first time, the system asks to change the temporary password to a permanent one:

### You must change your temporary password

Password \*

Confirmation \*

The minimum password length must be 8 characters  
Use of lowercase and uppercase letters  
Using at least one special character  
Using at least one digit

## 9.4.2 User Privileges

Here are all available roles for Merchant, Reseller, Manager, Dealer and Superior.

### Merchant

Main Merchant account has access only to his traffic and not able to see other Merchants.

Employee type	Description
merchant-support	This employee is the same as Merchant account, but not able to create Merchant employees. Can reverse orders from orders page
merchant-support-readonly	This employee is limited version of merchant-support, no access to the configuration change. Can reverse orders from orders page
merchant-risk	This employee has access to transaction details and actions with them, view and operate with BWL lists and BWL options from order details page, Reports and Batch operations. Can reverse orders from orders page
merchant-risk-readonly	This employee has access to transaction details, view and operate with BWL lists and BWL options from order details page, has no access to Reports and Batch operations
merchant-finance	This employee has access to view some entities in the system, Dashboard and transaction details
merchant-finance-readonly	This employee can see only transaction details, Batch operations and Reports
merchant-vt-only	This employee has access only to Virtual terminal
merchant-vt-transaction	This employee has access only to Virtual terminal and transaction details
merchant-desc	This employee can see only Dashboard and transaction details
merchant-loyalty	This employee can see only BWL lists and transaction details
merchant-client-support	This employee can see only transaction details
merchant-transaction	This employee is almost identical to merchant-client-support
merchant-analyst	This employee is almost identical to merchant-transaction with access to Dashboard, can't view Projects

### Reseller

Main Reseller account has only access to see the traffic for the Projects linked to this Reseller.

Employee type	Description
reseller-support	This employee is the same as Reseller account, but not able to create Reseller employees

continues on next page

Table 252 - continued from previous page

Employee type	Description
reseller-finance	This employee is the same as reseller-support, but not able to deal with rate plans
reseller-no-finance	This employee is the same as reseller-support, can create employees, but no access to banking information at all
reseller-desc	This employee is the same as reseller-support, has access to some actions with transactions and transaction markers, but no access to Integration panel
reseller-client-support	This employee is the same as reseller-support, can see uploaded documents on Order details page, but no access to the Dashboard and Adjustments

Ask the Doc4.0 support manager to find the most suitable roles for specific cases or get a complete list of the roles functionality.

### Manager

Main Manager account logically is same as Superior account, but doesn't have access to other Managers.

Employee type	Description
manager-support	This employee is the same as Manager account, but not able to create Manager employees. Can reverse orders from orders page
manager-no-settings	Limited version of manager-support, without access to the configuration at all. Can reverse orders from orders page
manager-no-finance	This employee has access to the configuration, BWL lists, but without financial reports and actions that could be done with transactions
manager-limited-support	Extended version of manager-no-finance, because it has access to the processing limits page, to the rate plans and can work with BWL lists. Also can manage employees
manager-view	This employee is the same as Manager account, but not able to edit anything
manager-limited-view	Limited version of manager-no-settings, without access to the processors on Order details page, but with access to Gates. Can reverse orders from orders page
manager-finance	Limited version of manager-support, but cannot edit Merchant details and with very limited Tools page. Can reverse orders from orders page
manager-restricted	Limited version of manager-support, the minimum of entities
manager-transaction	This employee has access only to view transaction details

continues on next page

Table 253 - continued from previous page

Employee type	Description
manager-transaction-readonly	Same as manager-transaction, but cannot download transaction reports from Orders page, decrypt customer data and see total turnover amount
manager-banking	This employee has access only to view transaction details, Dashboard and Transaction report
manager-report	This employee has access to view transaction details, Dashboard and Transaction report, BWL lists and Batch operations
manager-loyalty	This employee has access only to BWL lists (not from Order details page)
manager-loyalty-extended	This employee has access to view transaction details and to BWL lists
manager-sales	This employee has access to Dashboard, to view transaction details and all entities without Edit option
manager-reconciliation	This employee has no access to Batch operations, has access to Transaction reports, to view transaction details and all entities without Edit option

### Dealer

Main Dealer account has only access to see the traffic for Gates and Processors linked to this Dealer.

Employee type	Description
dealer-support	This employee is the same as Dealer account, but not able to create Dealer employees
dealer-finance	This employee is a limited version of dealer-support with very few differences
dealer-finance-limited	This employee is a limited version of dealer-finance without access to a customer personal info (billing address, email and phone number) and transaction reports through the orders page
dealer-limited	This employee is a limited version of dealer-finance without access to a customer personal info (billing address, email and phone number) and gates

### Superior

Main superior account is able to see and manage all Manager accounts that belong to current account, as well as all Merchant accounts that belong to the following Managers.

Employee type	Description
superior-support	This employee is the same as Superior account, but not able to create Superior employees. Can reverse orders from orders page

continues on next page

Table 255 - continued from previous page

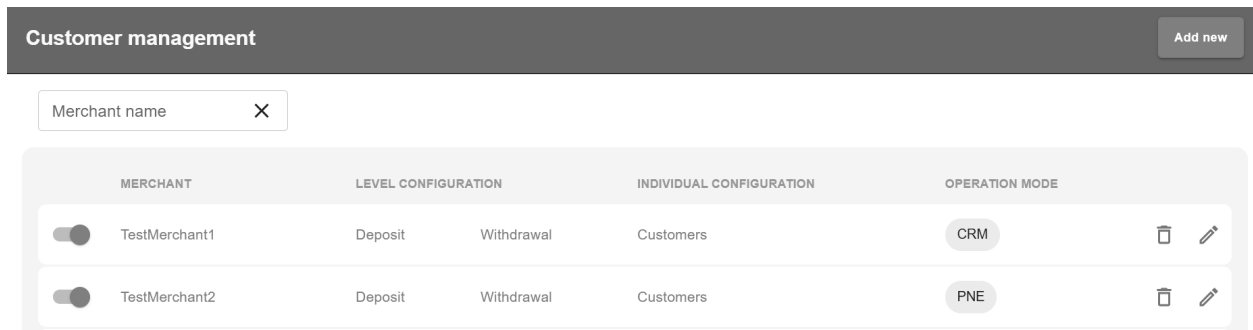
Employee type	Description
superior-limited-support	Limited version of superior-support, there is no access to reconciliation and balance pages, no Integration panel and Processing limits page. Can reverse orders from orders page
superior-client-support	This employee is able to see only transactions
superior-transaction	More extended type than superior-client-support, this employee is also able to download transaction report and view the details of some entities in the system (without Edit option)
superior-desc	More extended type than superior-transaction, this employee also has access to the Dashboard, actions which could be done with Orders, but doesn't have access to entities from Order details page. Can reverse orders from orders page
superior-finance	This employee differs from Superior role by the following: no access to the Dashboard and configuration. Can reverse orders from orders page and has access to Adjustments
superior-no-finance	This employee has access to the configuration, BWL lists, but without financial reports and actions that could be done with transactions
superior-restricted	This employee has access to the configuration, BWL lists, processing limits page, rate plans. Also can manage employees
superior-risk	This employee doesn't have access to the configuration, but has access to Dashboard, Order details and actions, Reports, Statements, BWL option. Can reverse orders from orders page
superior-sales	This employee has access to transactions and Virtual terminal
superior-view	The same as Superior account, but without Edit option
superior-vt-transaction	This employee has access to transactions, Virtual terminal and can view some entities

## 9.5 Customers Management





- [Introduction](#)
- [Adding New Merchant To Customer Management](#)
  - [CRM](#)
  - [Payment Gateway](#)
- [Level Configuration](#)
  - [Customer level configuration](#)
  - [Filters](#)
- [Customers](#)
  - [Common Settings](#)
  - [Individual Payment Settings](#)

### 9.5.1 Introduction

Customer Management - is a module which allows to set custom payment flow. It is located at Settings -> Customers management. This screen contains the list of all Merchants in the system that are connected to Customers Management.



The screenshot displays the 'Customer management' interface. At the top, there is a dark header bar with the title 'Customer management' on the left and an 'Add new' button on the right. Below the header is a search bar labeled 'Merchant name' with a clear 'X' button. The main content area features a table with the following columns: 'MERCHANT', 'LEVEL CONFIGURATION', 'INDIVIDUAL CONFIGURATION', and 'OPERATION MODE'. Two merchant entries are listed:

MERCHANT	LEVEL CONFIGURATION	INDIVIDUAL CONFIGURATION	OPERATION MODE
<input checked="" type="checkbox"/> TestMerchant1	Deposit    Withdrawal	Customers	CRM  
<input checked="" type="checkbox"/> TestMerchant2	Deposit    Withdrawal	Customers	PNE  

On this screen it is possible to make a search by Merchants or to add new Merchant(Configuration) into the Customer Management module by pressing Add new button on the right top corner of the screen.

### 9.5.2 Adding New Merchant To Customer Management

After pressing Add new button, this screen will popup:

### Add new merchant ✕

Merchant ▼

Operation mode

CRM (API) PNE (GATE)

Customer is determined by merchant customer id, not configured levels are created if customer level parameter is present in API calls.

Default behavior

PROJECT  UNKNOWN LEVEL

In case not configured customer level is present in API calls, project+endpoint settings are used.

Reset individual payment settings when customer level changed

Automatically add all merchant projects to Unknown level

Cancel ADD

First select the Merchant in Merchant field which will be connected to Customer Management system.

Then select one of the operation mode - CRM(API) or Payment Gateway.

- CRM(API) - allows to determine Customer by merchant customer id. Not configured levels are created if customer level parameter is present in API calls.
- Payment Gateway - allows to determine Customer by internal customer id.

In default behavior select either Project or Unknown Level.

- Project - In case if not configured customer level is present in API calls, Project and Endpoint settings (Client definition) will be used.
- Unknown Level - In case if not configured customer level is present in API calls, Unknown level settings will be used.

**Warning**

Any misconfiguration may lead to payment processing stop.

After selecting Operation mode and Default behaviour, (by choice) select one of the choices or both:

- Reset individual payment settings when customer level changed.
- Automatically add all merchant projects to Unknown level

After adding Merchant to Customer Management it is possible to edit or delete configuration.

**CRM**

CRM (API) - allows to determine Customer by merchant customer id.

Parameters used in CRM configuration:

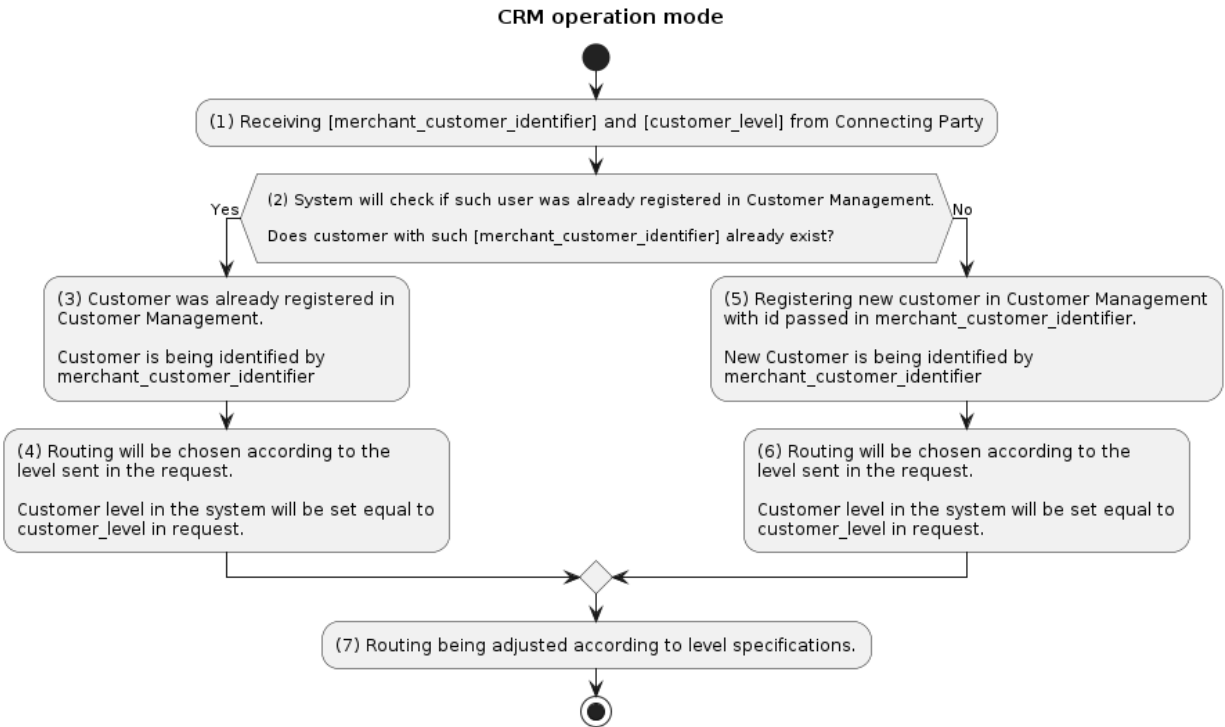
- merchant\_customer\_identifier
- customer\_level

**Warning**

customer\_id should not be included in the request.

(3), (5) merchant\_customer\_identifier should not be passed with empty value. If merchant\_customer\_identifier is sent with an empty value, the customer will be created in Customer Management and can only be identified using the Client Definition configured at the Project or Endpoint level.

(4), (6) In case of customer\_level being sent empty, customer will be granted an empty level or Unknown level, if Unknown level Default Behaviour was configured.

**Warning**

Parameters being sent improperly could lead to transactions being incorrectly routed or not being processed entirely.

**Payment Gateway**

PNE (GATE) - allows to determine Customer by internal customer id.

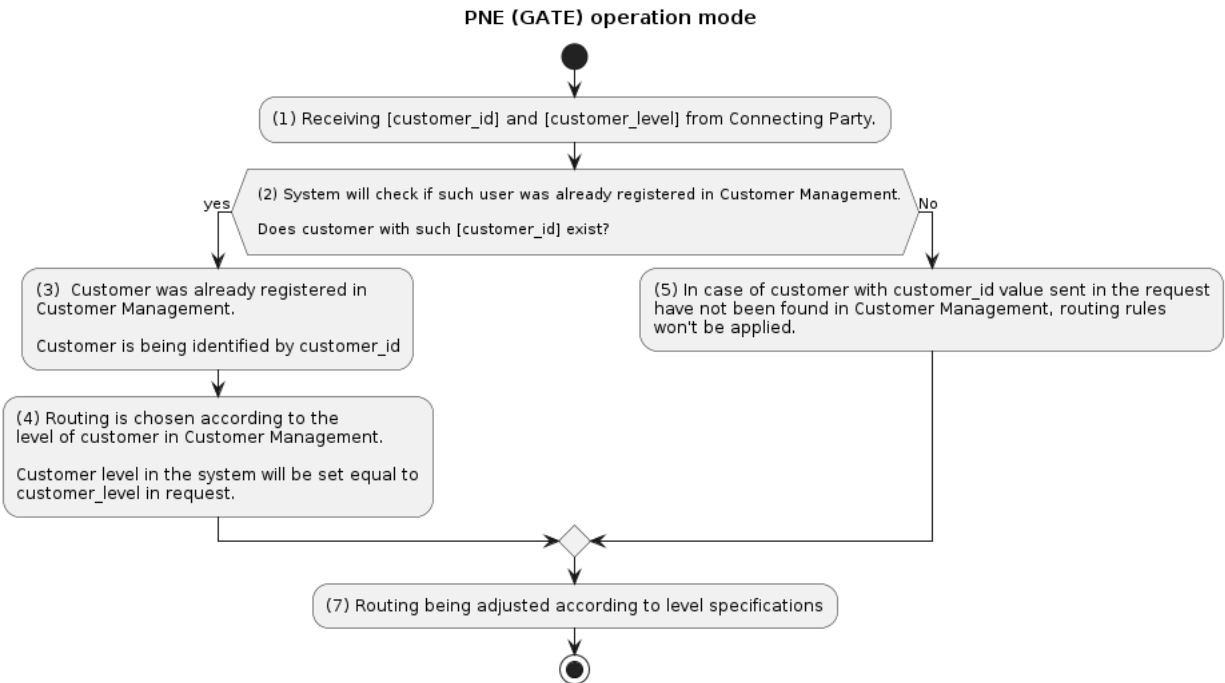
Parameters used in PNE configuration:

- customer\_id
- customer\_level

**Warning**

merchant\_customer\_identifier should not be included in the request.

(3), (5) In case of customer\_id being sent empty, Client Definition set on Project or Endpoint level being checked and if no customer found, new customer with new customer\_id will be created.



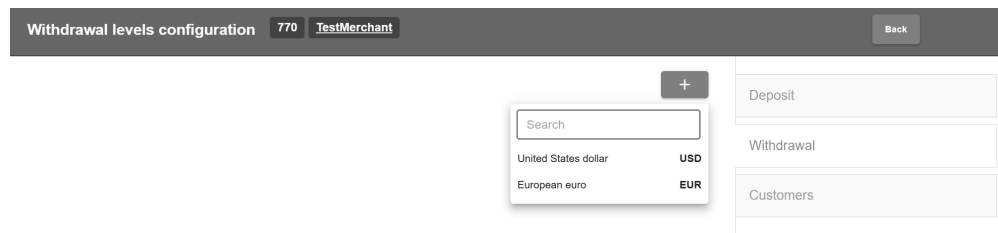
(4), (6) In case of customer\_level being sent empty, routing will be set according to Unknown level or Project default behavior that was configured.

### Warning

Parameters being sent improperly could lead to transactions being incorrectly routed or not being processed entirely.

### 9.5.3 Level Configuration

Level configuration can be done for Deposits and Withdrawals. In order to add configurations press + button and select the currency.



**Note**

The currency may vary based on the currencies in which the Merchant's Projects are available.

LEVEL NAME	PROJECTS	CREATED	MODIFIED
unknown	TestProject	Dec 9, 2024 12:07:55 PM	Dec 11, 2024 3:24:32 PM

unknown is a default level that will be created automatically.

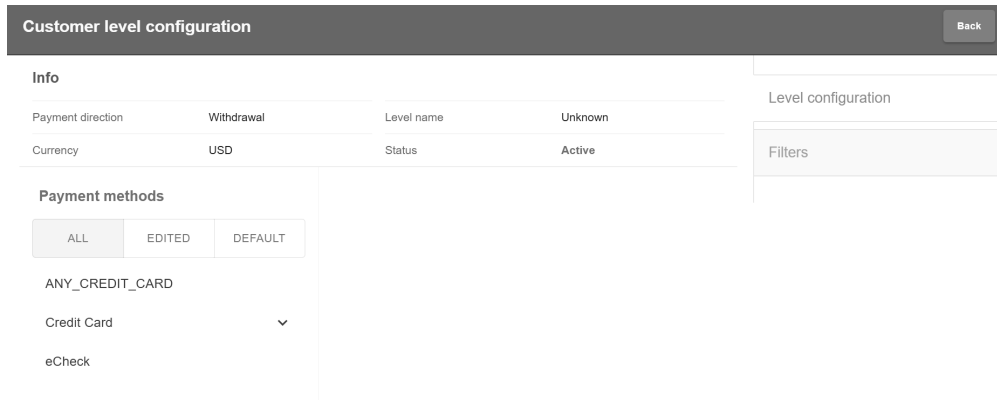
On the screen shown above, all levels will be displayed with the next information:

- Level name
- Projects - all Merchant's projects that are connected to Customer Management.
- Created and Modified - which will show the time - configuration was created or modified.

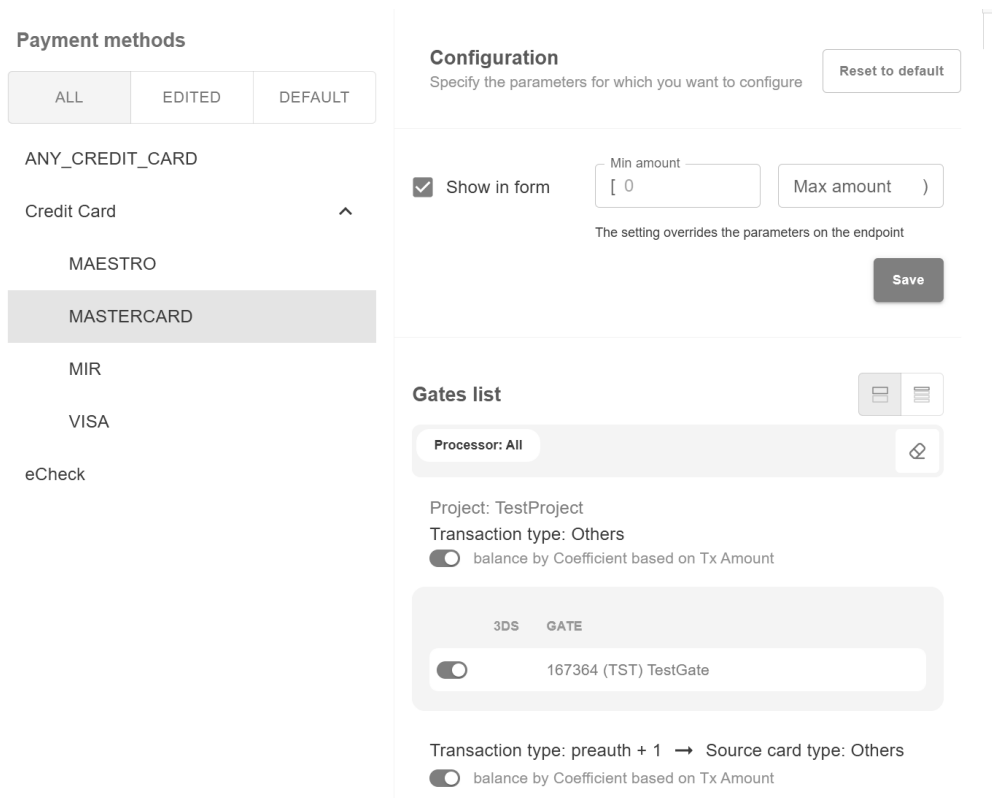
Press edit button to change level name or add/remove projects from level or Delete "currency" in order to delete the whole configuration for the currency.

### Customer level configuration

Press on Level Name to access Customer level configuration. In opened window select Level configuration to setup custom payment flow for Customer level or Filters to add additional checks for level.



This screen will display information about level such as - Payment direction - Deposit or Withdrawal, Currency, Level name, Status - which shows the status of level (active/disabled).



In Payment methods section all available methods for Payment Cashier will be displayed. By pressing on any of the methods Configuration window will popup.

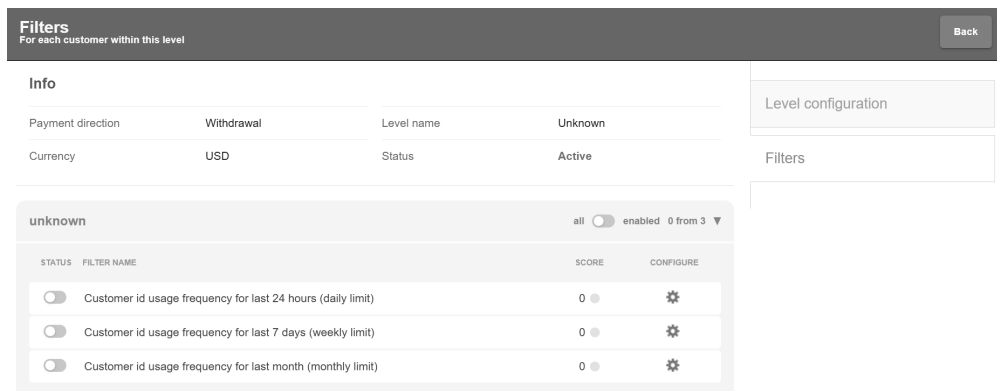
In Configuration section press Reset to default to restore all setup to default;  
 Check or uncheck the Show in form box to show/hide selected payment method from the Payment Cashier Form;  
 Set min/max amount which will set or override these parameters on Endpoint level.  
 Press Save button for the configuration to be applied.

In Gate list select which Routing route or gate will be available for selected level.

After all configurations - changed payment methods will be moved to Edited tab. All unchanged methods will be shown in Default tab.

### Filters

Transaction filters in System are intended for rejection of certain transactions on various reasons.



There are three level filters:

- Customer id usage frequency for last 24 hours (daily limit)
- Customer id usage frequency for last 7 days (weekly limit)
- Customer id usage frequency for last month (monthly limit)

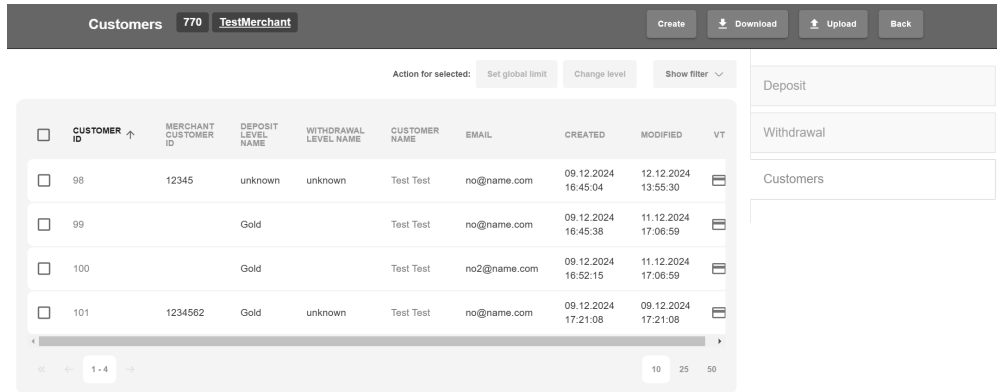
Name	Description	Value
amount limit	maximum total transactions amount for the last 24 hours (week, month) for exact Customer id	99999
calendar week starts from Sunday	“Yes”: calendar week starts from Sunday, “No”: calendar week starts from Monday	Yes/No
for all merchant currencies in CMS	current total transactions amount or count for the last 24 hours (week, month) for this customer id would be calculated “Yes”: for all merchant levels in all currencies in payment direction (Deposit or Withdrawal) and converted to the currency of the current level for comparison with the amount limit “No”: for current level only	
quantity limit	maximum total transactions count for the last 24 hours (week, month) for exact Customer id	99999
subtract Cancel transactions		
use calendar day		

### Error codes

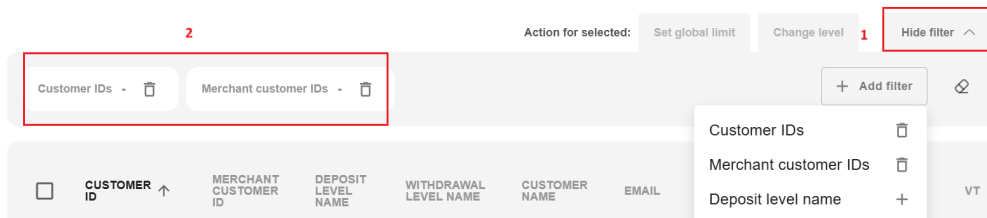
#	Code	Name
19000		Daily amount limit exceeded for customer id
19001		Daily quantity limit exceeded for customer id
19002		Weekly amount limit exceeded for customer id
19003		Weekly quantity limit exceeded for customer id
19004		Monthly amount limit exceeded for customer id
19005		Monthly quantity limit exceeded for customer id

### 9.5.4 Customers

Individual configuration can be done for Customers. Depending on the parameter that were sent (customer\_id, customer\_level, merchant\_customer\_identifier), customer can be created automatically or manually through Customers screen. Press on Customers in order to access the Customers screen.



All customers with brief information will be displayed on this screen.



As shown on the image above, press 1 - Show filter to open additional criterion for search. In popp up screen select next criterion: (Payment Gateway's) Customer IDs, Merchant Customer IDs, Deposit level name, Withdrawal level name, Email or Date range (creation dates).

It is possible to add,change or delete information from the 2 bar or through filter section.

Select group of customers or all of them to Set global limit or Change level - for all selected customers.

Press Create to create new customer.

Create customer
Back Create

---

**Info**

First name \*  Last name \*  Date of birth

---

**Address**

Country  State  City  ZIP code

Address

---

**Contact**

Phone \*  Email \*  Customer IP

---

**Other**

Deposit level  Withdrawal level  Merchant customer ID \*

Language

Press Download to download list of all customers with their details.

Press Upload to upload the list of the customers with their details using the options, shown below:

**Batch operation**
✕

---

Select batch file

↑ Upload CSV

File not loaded

gen mock

Sample CSV file for this batch

↓ Download template

---

Cancel

Process

Upload CSV - for uploading the list of customers;  
 Download template - for downloading an example file;  
 gen mock - for generating customers with fake data.

## Common Settings

By pressing on any customer's ID next window will pop-up:

Customer #98

Edit info
Virtual terminal
All orders
Back

<p><b>Info</b></p> <table style="width: 100%; border-collapse: collapse;"> <tr><td style="width: 50%;">First name</td><td>Test</td></tr> <tr><td>Last name</td><td>Test</td></tr> <tr><td>Date of birth</td><td>17.07.1996</td></tr> </table> <p><b>Address</b></p> <table style="width: 100%; border-collapse: collapse;"> <tr><td>Country</td><td>-</td></tr> <tr><td>State</td><td>-</td></tr> <tr><td>City</td><td>City</td></tr> <tr><td>ZIP code</td><td>12345</td></tr> <tr><td>Address</td><td>TESST</td></tr> </table> <p><b>Contact</b></p> <table style="width: 100%; border-collapse: collapse;"> <tr><td>Phone</td><td>+99400000000</td></tr> <tr><td>Email</td><td>no@name.com</td></tr> </table>	First name	Test	Last name	Test	Date of birth	17.07.1996	Country	-	State	-	City	City	ZIP code	12345	Address	TESST	Phone	+99400000000	Email	no@name.com	<p><b>Individual level settings</b></p> <table style="width: 100%; border-collapse: collapse;"> <tr><td>Deposit level</td><td>unknown</td></tr> <tr><td>Withdrawal level</td><td>unknown</td></tr> </table> <p><b>Other</b></p> <table style="width: 100%; border-collapse: collapse;"> <tr><td>Customer IP</td><td>-</td></tr> <tr><td>Customer DNA</td><td>-</td></tr> <tr><td>Language</td><td>-</td></tr> <tr><td>SSN last 4</td><td>-</td></tr> <tr><td>Customer ID</td><td>98</td></tr> <tr><td>Merchant customer ID</td><td>12345</td></tr> <tr><td>Created</td><td>09.12.2024 16:45:04</td></tr> <tr><td>Modified</td><td>12.12.2024 13:55:30</td></tr> </table>	Deposit level	unknown	Withdrawal level	unknown	Customer IP	-	Customer DNA	-	Language	-	SSN last 4	-	Customer ID	98	Merchant customer ID	12345	Created	09.12.2024 16:45:04	Modified	12.12.2024 13:55:30	<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">Common settings</div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">Individual payment settings</div> <div style="border: 1px solid #ccc; padding: 5px;">Payment details</div>
First name	Test																																									
Last name	Test																																									
Date of birth	17.07.1996																																									
Country	-																																									
State	-																																									
City	City																																									
ZIP code	12345																																									
Address	TESST																																									
Phone	+99400000000																																									
Email	no@name.com																																									
Deposit level	unknown																																									
Withdrawal level	unknown																																									
Customer IP	-																																									
Customer DNA	-																																									
Language	-																																									
SSN last 4	-																																									
Customer ID	98																																									
Merchant customer ID	12345																																									
Created	09.12.2024 16:45:04																																									
Modified	12.12.2024 13:55:30																																									

In Common settings all customer information will be shown. Press Edit info to change customer information except Customer ID and Merchant customer ID. The Virtual terminal button will allow to open the virtual terminal with all customer information directly from this screen. All orders will show all orders associated with customer.

## Individual Payment Settings

Individual payment settings allows to setup Cashier Payment Form for each customer separately. First choose level and currency for the setup. Then select Use as global limit for customer if min/max amount for currency should be applied for all available solutions . Select Payment methods and apply setup if needed. By pressing Virtual terminal button Virtual terminal with all customer information will be opened.

## REFERENCE

### 10.1 Glossary

For the purposes of this guide, the following terms and their definitions are used:

Doc4.0 Hardware and Software System (Doc4.0 Payment Gateway)	An information system designed for automated and secure processing of payment transactions and their storage.
Doc4.0 Payment Management System (Doc4.0 UI)	Payment management user interface and analytical platform of Doc4.0 Payment Gateway.
Merchant	The company that provides services, works or sales of goods through the E-commerce, mobile commerce or mPOS channels.
Manager	An organization that provides services for processing transactions of Processor Merchants using the Doc4.0 Payment Gateway and accounting for transactions in the Doc4.0 UI.
Processor	The entity of the system, which is a technical integration with a specific acquiring bank or other payment service provider for processing transactions.
Account	Identification data in the Doc4.0 UI, which allows the user to interact with the system on their own behalf.
Transaction	An agreement to carry out a financial operation between a customer and the merchant to pay for services, work or goods, to return funds for previously paid services, works or goods, to transfer money from card to card, or to hold funds for future payment.
Antifraud filter	Technical transaction analysis algorithm for identifying suspicious and fraudulent transactions, based on the experience of Doc4.0 employees and international fraud monitoring practices.
BIN	Bank identification number, first 6 digits of card number.

## 10.2 KPIs Detailed View

- [Overview](#)
- [KPIs](#)
  - [Gross Traffic](#)
  - [Earnings](#)
  - [Carryover](#)
  - [The Dates Of The First And Last Transactions](#)
  - [Average Transaction Amount](#)
  - [Order Number Per Client Per Month](#)
  - [The Returning Clients Conversion](#)
  - [Transactions By Country By Client's IP Address](#)
  - [Transactions By Country By BIN](#)
  - [Average Earnings Per Transaction](#)
  - [3DS/non-3DS Ratio](#)
  - [3DS/non-3DS Ratio For Declined Transactions](#)
  - [3DS/non-3DS Ratio For Approved Transactions](#)

### 10.2.1 Overview

Key Performance Indicators, or KPI, is an analysis module which helps the user to quickly visualize the detailed business related information for each main system entity such as Endpoint, User, Project, Gate and etc..

The screenshot displays the 'End Points' KPIs Detailed View interface. At the top, there is a search bar with a 'Templates search' dropdown and a 'Search criteria' button. Below the search bar, there are controls for rows (10, 15, 20) and a date range selector (Today, Yesterday, This month, Last month). The main table lists endpoints with columns for On/off, ID, Display name, Decline Ratio (with a dropdown arrow), Negative Ratio, Gross traffic, Average tx. amount, and Current. A dropdown menu is open, showing various KPI categories like Gross traffic, Merchant earnings, Reseller earnings, Manager earnings, Dealer earnings, Bank earnings, Current Carryover, First tx. date, Last tx. date, Average tx. amount, Order count per Client, Primary IP country, Primary BIN country, Client conversion, Merchant CPO, Reseller CPO, Manager CPO, Dealer CPO, Bank CPO, 3D Ratio, 3D decline ratio, and 3D approve ratio. The interface also includes a '+ End Point' button and an 'Apply' button at the bottom of the dropdown menu.

On/off	ID	Display name	Decline Ratio	Negative Ratio	Gross traffic	Average tx. amount	Current
🔦	38	Saturn's green bear ...			226 524.01	100.14	
🔦	29	Earth's red dog twenty			222 359.08	99.67	
🔦	30	Earth's orange goat ...			147 252.03	100.38	
🔦	47	Sun's white elephan...			243 885.53	100.16	
🔦	66	Mars's pink tiger twe...			153 445.29	102.16	

To view the details of the relevant element, open the respective element common screen and pick the KPIs in the dropdown Details menu. The order of KPI shown on the details view corresponds to the order in which KPIs are picked in the dropdown. The first chosen KPI is placed on the left, then goes the second etc. The user can pick up to 5 KPIs.

The search criteria (point 1 on the screenshot) only affect the list of elements shown and not the calculated value of the KPI.

The KPI value could be calculated within a time period (the control elements 2` on the picture above). The time period is ignored when the meaning of the KPI contradicts the selected date range or in case the KPI is beside the purpose.

Each KPI could be used for sorting to provide the most valuable data. The user can apply the sorting by clicking the name of KPI(the control element 3 on the picture above). Please keep in mind that if KPI is selected for sorting and then removed, the sorting will still be applied.

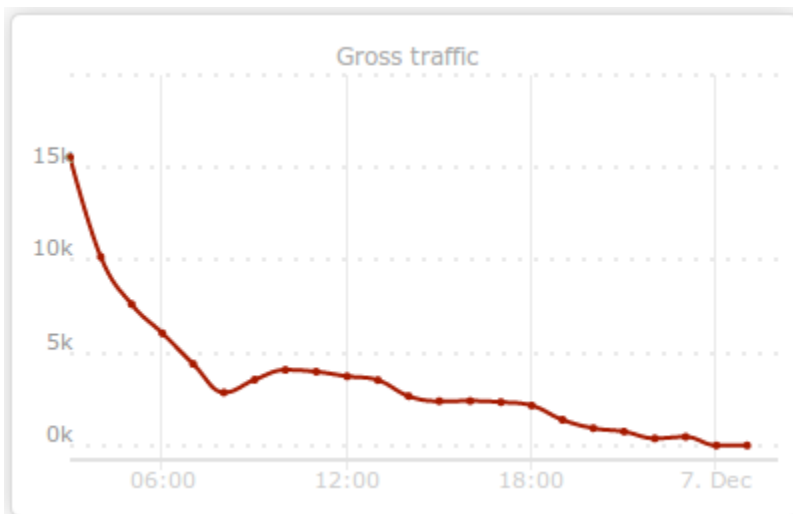
## 10.2.2 KPIs

### Gross Traffic

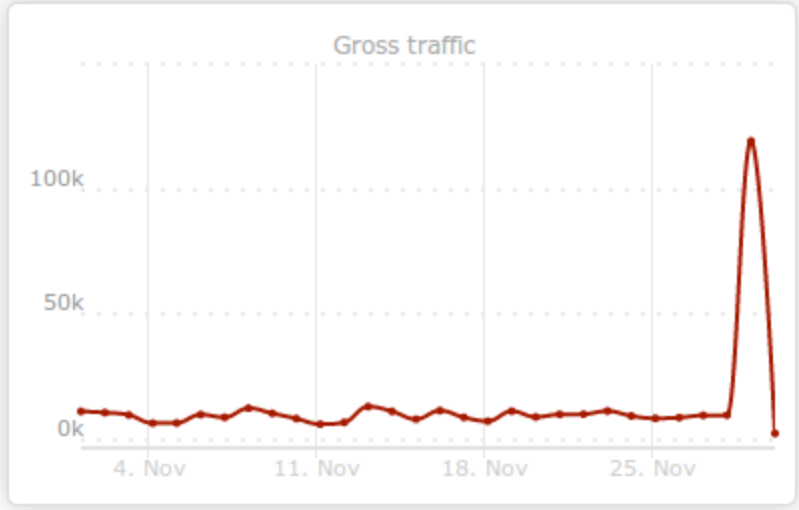
Shows: The total sum of the approved transactions of the types: sale, capture, dispute, transfer approved.

Update frequency: virtually real-time (no more than 10 seconds delay).

Graph: the total sum per hour if selected date range is Today or Yesterday; the total sum per day if selected date range is This Month or previous Month.



Gross traffic per hour for December 7th.



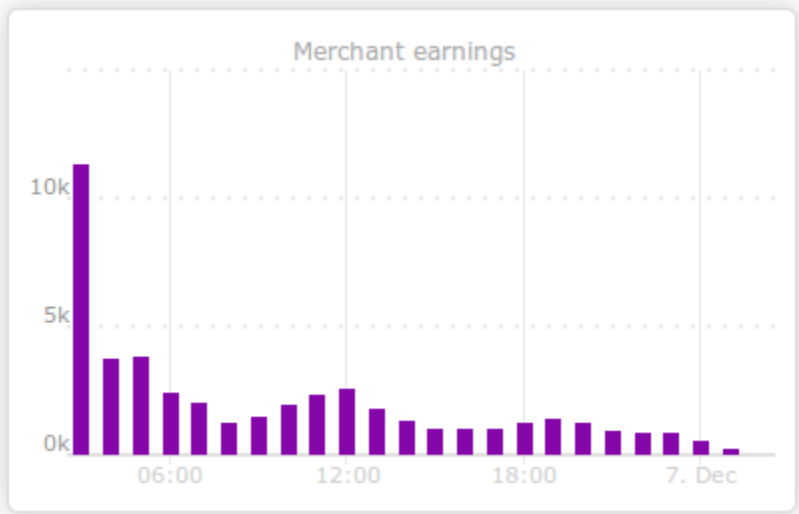
Gross traffic per day for November.

**Earnings**

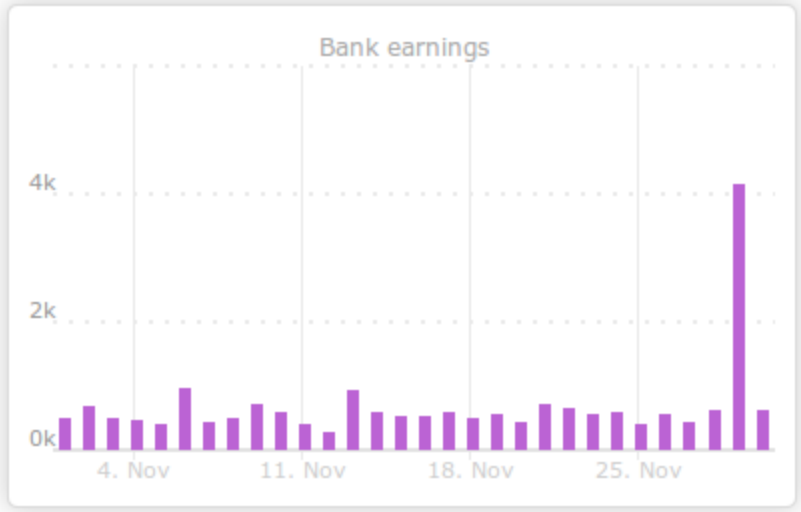
Shows: earnings for the Bank, Dealer, Manager, Reseller or Merchant without holds for any type of transaction in any status

Update frequency: virtually real-time (no more than 10 seconds delay)

Graph: the earnings per hour if selected date range is Today or Yesterday; the earnings per day if selected date range is This Month or previous Month.



Merchant's earnings per hour for December 7th.



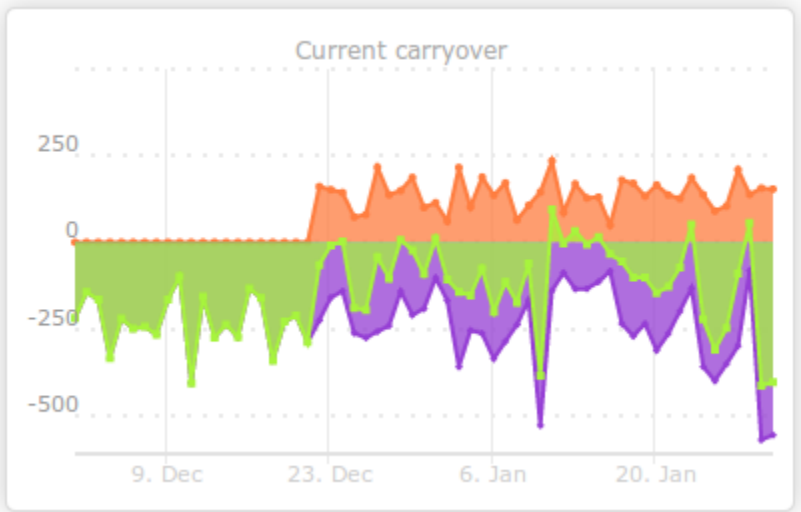
Bank’s earnings per day for November.

**Carryover**

Shows: The value of the Carryover for the current date disregarding the selected date range. Each type of user can see respective value of the Carryover. The only exception is a Superior who can see the Carryover for the Manager.

Update frequency: daily at 00:00

Graph: shows the carryover value starting from the selected date plus 2 months; it shows both total carryover due by the user (positive) and the carryover due to the user(negative). It also shows the carryover balance which is a sum of the two above values.



The carryover for the Manager begins from the December 1st. As you can see there’s no carryover from the Bank to the Manager by December 21st and the Merchant’s carryover due is there and thus the carryover balance is negative. Starting from December 22nd the Bank

begins paying the carryover to the Manager but they can not cover the Merchant's carryover. This view allows you to forecast the future carryover dues.

### The Dates Of The First And Last Transactions

Shows: The date of the first and last processed transaction regardless of the date range chosen. It allows quickly finding inactive instances of the infologic model elements.

Update frequency: virtually real-time (no more than 10 seconds delay)

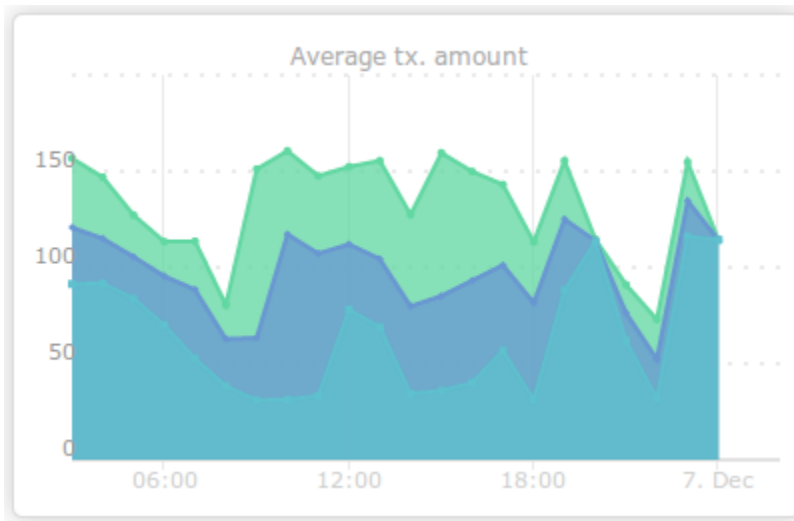
Graph: N/A

### Average Transaction Amount

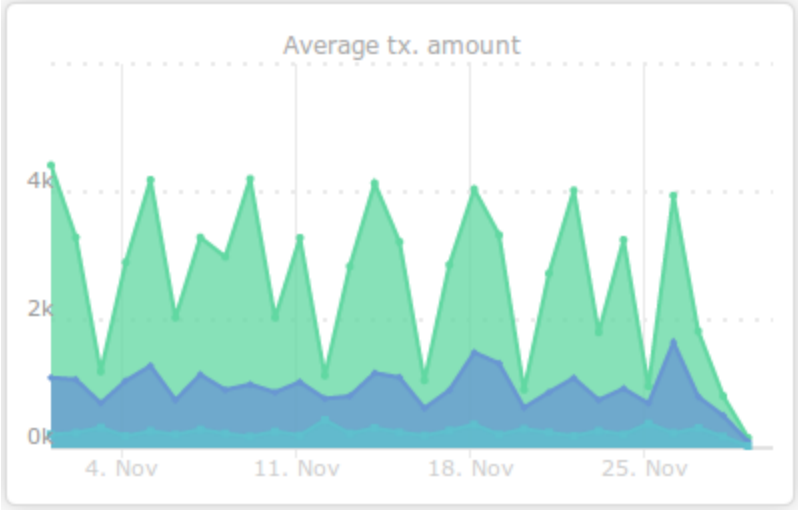
Shows: The average transaction amount: sale, capture, dispute, transfer in approved status. It allows to detect abnormalities when merchant changes the source of incoming payment traffic or the products sold.

Update frequency: virtually real-time (no more than 10 seconds delay)

Graph: Minimal, maximal and average transaction amount per hour if selected date range is Today or Yesterday; the Minimal, maximal and average transaction amount per day if selected date range is This Month or previous Month.



Minimal, maximal and average transaction amount per hour for December 7th



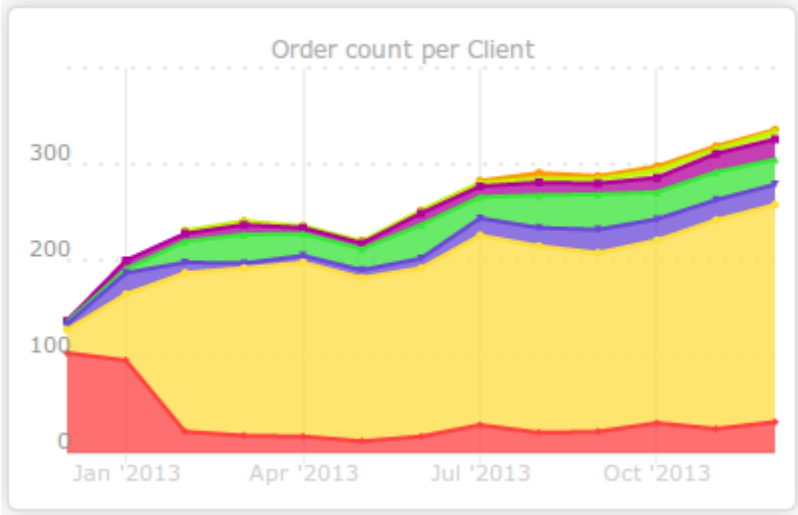
Minimal, maximal and average transaction amount per day for November

**Order Number Per Client Per Month**

Shows: The average number of the transaction of any type and in any status for the month which falls into the selected date range. The KPI is only calculated for Endpoints and Projects. The definition of the customer is set up at the Project level, one card means one customer by default. The customer at the Endpoint differs from the customer at the Project to have an option to examine various sources of the payment traffic

Update frequency: virtually real-time (no more than 10 seconds delay)

Graph: the number of orders made by a customer per month ending by the chosen date and starting from the date of 12 months earlier.



The number of orders made by a customer per month. Various numbers of orders are marked by different colors . The customers who made 5-6, 7-10 and more than 10 orders are united

into one group.

### The Returning Clients Conversion

Shows: The ratio of the repeated transactions made by a particular customer to the total number of transactions made by the customer for the month that fall into selected date range. The transaction is considered repeated for the chosen month if the customer has made a transaction at any time before. The KPI is only calculated for Endpoints and Projects. The definition of the customer is set up at the Project level, one card means one customer by default. The customer at the Endpoint differs from the customer at the Project to have an option to examine various sources of the payment traffic

Update frequency: virtually real-time (no more than 10 seconds delay)

Graph: The ratio of the repeated transactions made by a particular customer to the total number of transactions made by the customer per month ending by the chosen date and starting from the date of 12 months earlier.



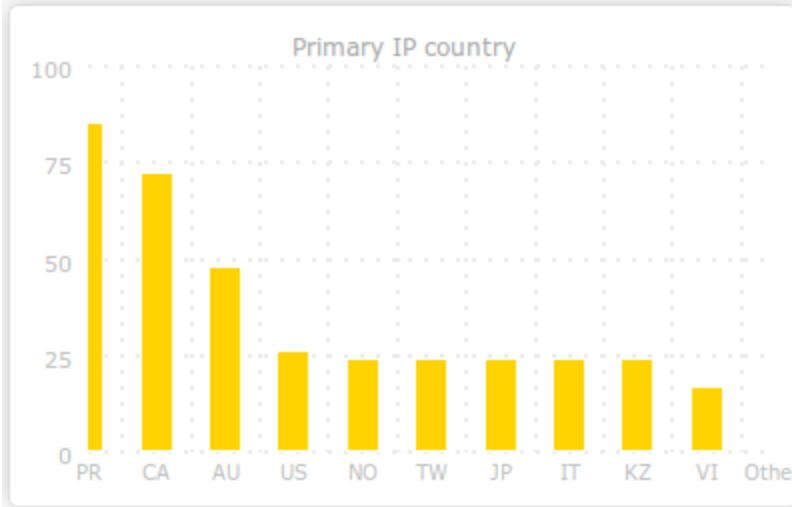
The ratio of the repeated transactions made by a particular customer to the total number of transactions made by the customer per month for the past year.

### Transactions By Country By Client's IP Address

Shows: The country is determined by the IP address of the customer. The transactions of any type in any status are taken into consideration. The parameter does not depend on the date range and is calculated for the lifetime.

Update frequency: daily at 00:45

Graph: The number of transactions of any type in any status per country which is derived from the customer's IP address for the given date range, refreshed every 10 seconds



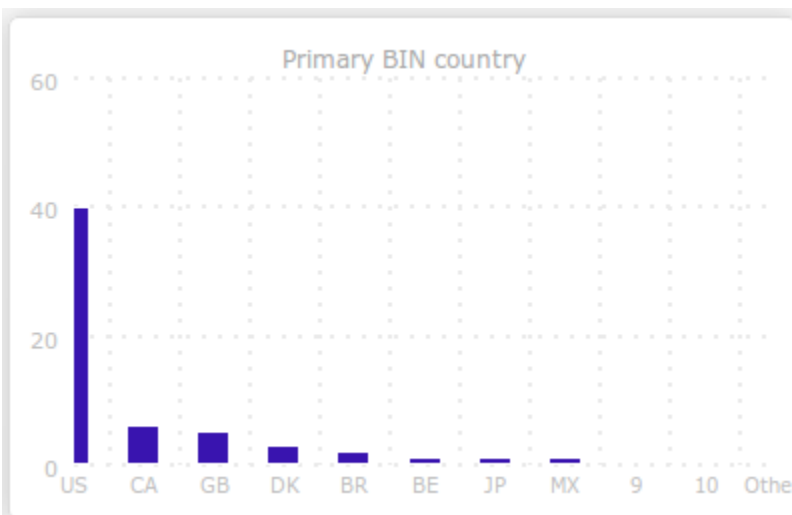
The number of transactions for top 10 countries which are derived from the customer's IP address

### Transactions By Country By BIN

Shows: The country is derived from the customer's card BIN. The transactions of any type in any status are taken into consideration. The parameter does not depend on the date range and is calculated for the lifetime.

Update frequency: daily at 00:45

Graph: The number of transactions of any type in any status per country which is derived from the customer's card BIN for the given date range, refreshed every 10 seconds



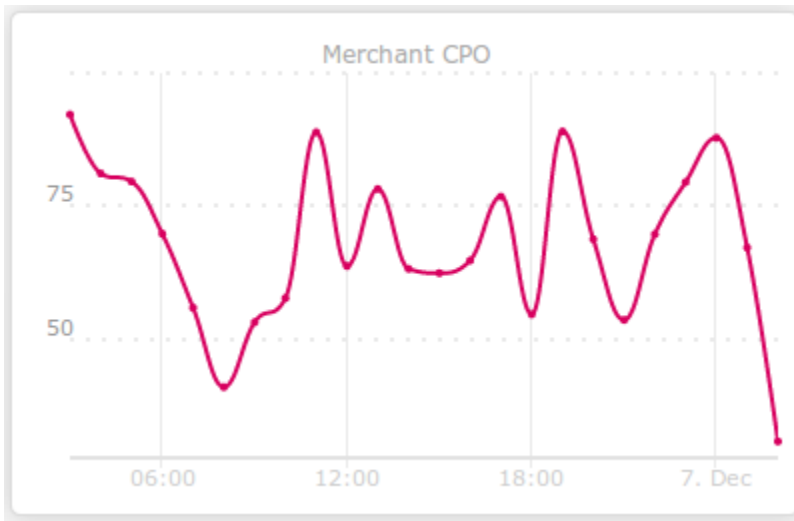
The number of transactions for top 10 countries which are derived from the customer's card BIN.

### Average Earnings Per Transaction

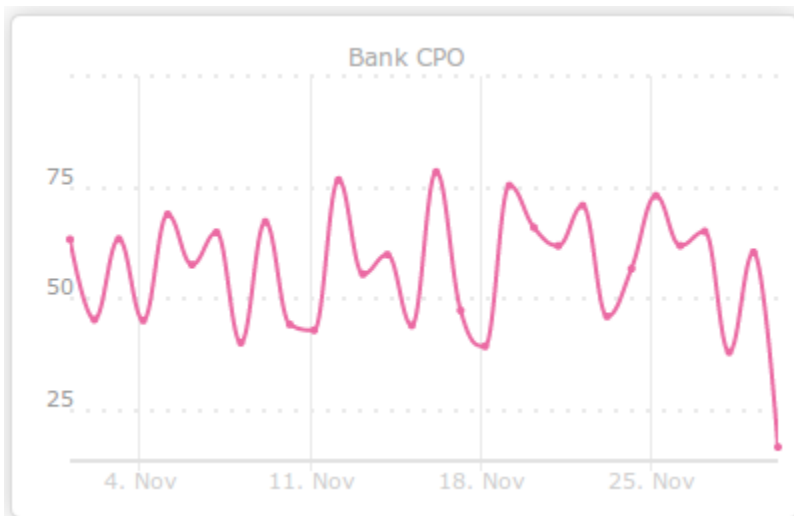
Shows: Average earnings per transaction for Bank, Dealer, Manager, Reseller or Merchant without holds for any type of transaction in any status.

Update frequency: virtually real-time (no more than 10 seconds delay)

Graph: Average earnings per transaction per hour if selected date range is Today or Yesterday; the Average earnings per transaction per day if selected date range is This Month or Previous Month.



The Merchant's average earnings per transaction per hour for December 7th.



The Bank's average earnings per transaction per month for November.

**3DS/non-3DS Ratio**

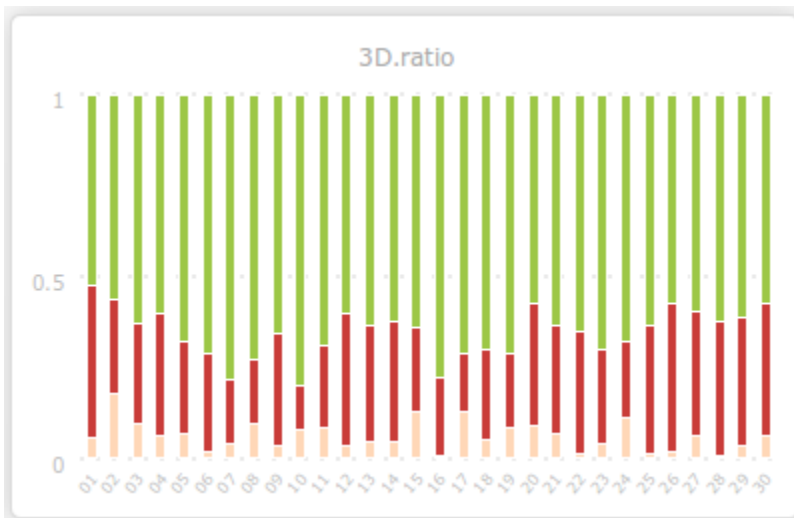
Shows: The ratio of the number of 3DS/non-3DS sale, preauth, transfer transactions in approved, filtered and declined statuses to the total number of such transactions for the given date range.

Update frequency: virtually real-time (no more than 10 seconds delay)

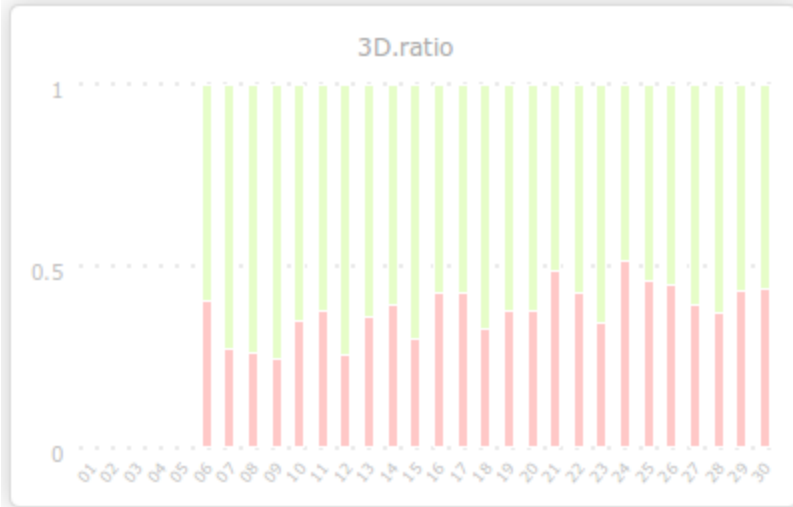
Graph: The ratio of the number of 3DS/non-3DS sale, preauth, transfer transactions in approved, filtered and declined statuses to the total number of such transactions for the given date range per day starting from the month's first date to the end date of the given date range.

Legend:

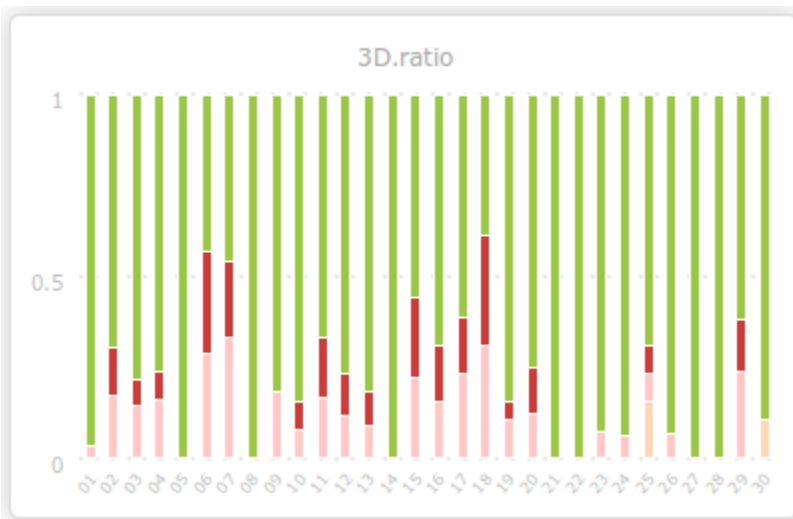
- - 3D Gate filtered
- - non3D Gate filtered
- - 3D Gate declined
- - non3D Gate declined
- - 3D Gate approved
- - non3D Gate approved



The ratio of the number of transactions in different statuses for 3DS Gate for November.



The ratio of the number of transactions in different statuses for non-3DS Gate for November.



The ratio of the number of transactions in different statuses for November.

### 3DS/non-3DS Ratio For Declined Transactions

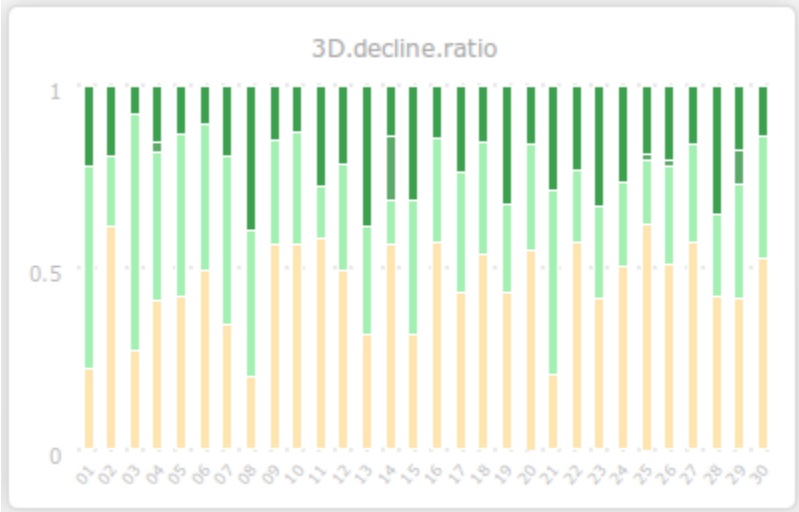
Shows: The ratio of the number of 3DS transactions in declined status processed by the 3DS Gate, for Enrolled cards which have MPI status Y or A to the total number of transactions of the types sale, preauth or transfer for the given period

Update frequency: virtually real-time (no more than 10 seconds delay)

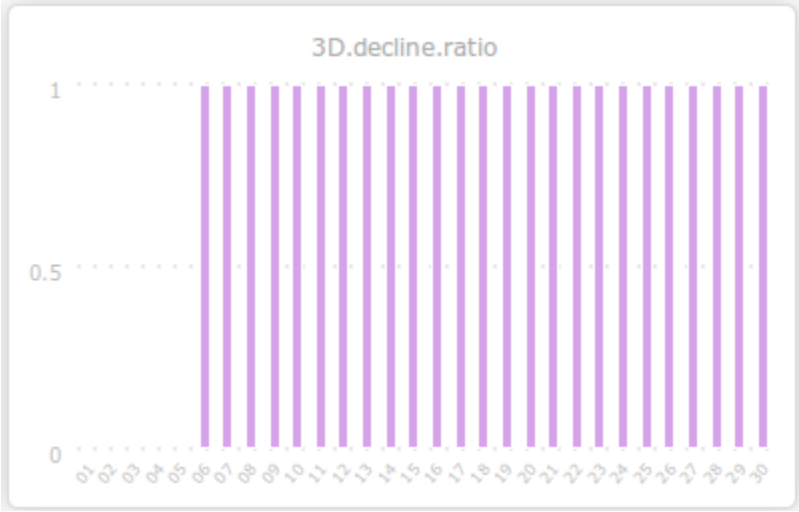
Graph: The ratio of the number of 3DS/non-3DS transactions in declined status per day for the given date range starting from the month's first date to the end date of the given date range.

Legend:

- 3D Gate, enrolled cards, MPI status "Y"
- 3D Gate, enrolled cards, MPI status "A"
- 3D Gate, enrolled cards, MPI status "U"
- 3D Gate, enrolled cards, MPI status ""
- 3D Gate, enrolled cards, MPI status "N"
- 3D Gate, cards not enrolled
- non3D Gate



The ratio of the number of transactions in declined status for 3DS Gate for November.



The ratio of the number of transactions in declined status for non-3DS Gate for November.



The ratio of the number of transactions in declined status for mixed traffic for November

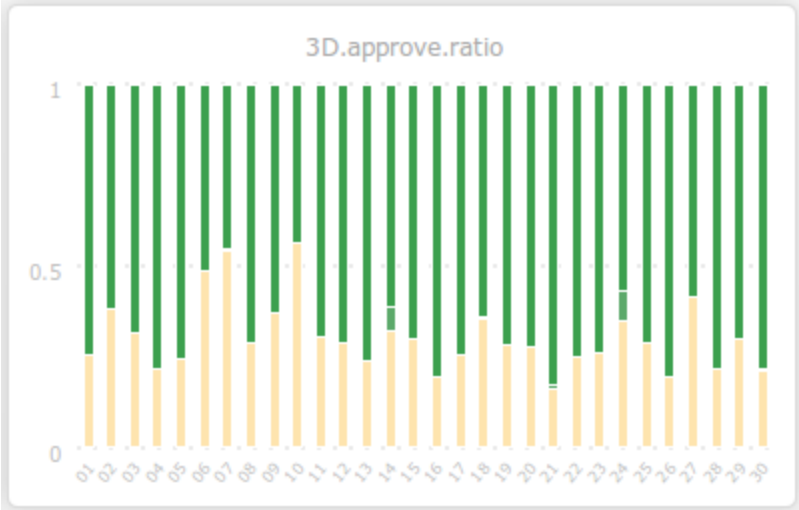
### 3DS/non-3DS Ratio For Approved Transactions

Shows: The ratio of the number of 3DS transactions in approved status processed by the 3DS Gate, for Enrolled cards which have MPI status Y or A to the total number of transactions of the types sale, preauth or transfer for the given period

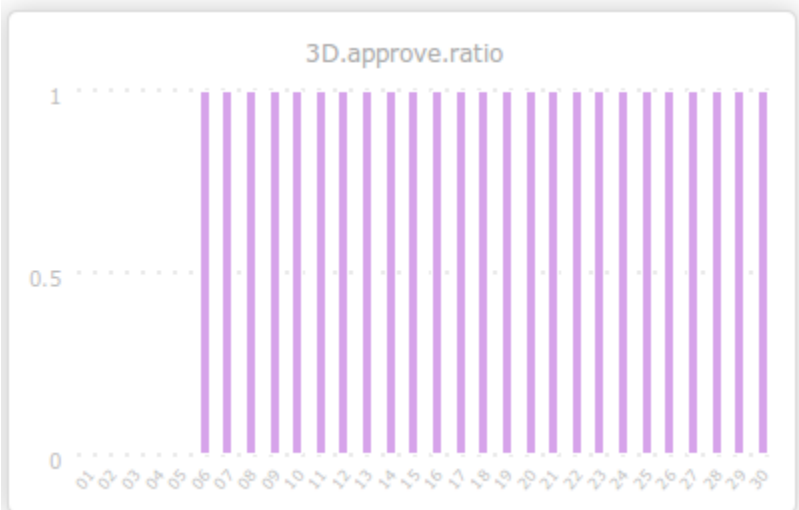
Update frequency: virtually real-time (no more than 10 seconds delay)

Graph: The ratio of the number of 3DS/non-3DS transactions in approved status per day for the given date range starting from the month's first date to the end date of the given date range.

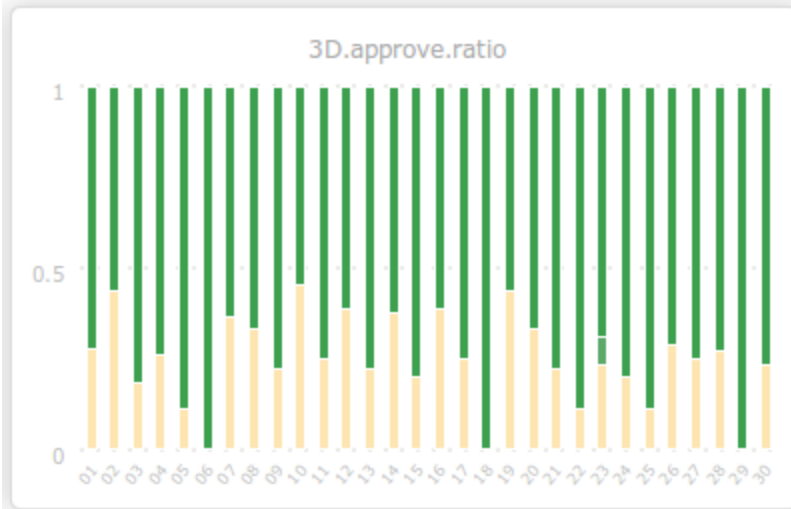
- - 3D Gate, enrolled cards, MPI status "Y"
- - 3D Gate, enrolled cards, MPI status "A"
- - 3D Gate, enrolled cards, MPI status "U"
- - 3D Gate, enrolled cards, MPI status ""
- - 3D Gate, enrolled cards, MPI status "N"
- - 3D Gate, cards not enrolled
- - non3D Gate



The ratio of the number of transactions in approved status for 3DS Gate for November.



The ratio of the number of transactions in approved status for non-3DS Gate for November.



The ratio of the number of transactions in approved status for mixed traffic for November

**Warning**

The MPI status and Enrollment status could be only determined if Doc4.0 MPI plugin is being used or the Processor properly returns the data after 3DS verification.

### 10.3 Transaction Statuses And Types

- [Transaction Types](#)
- [Transaction Statuses](#)

#### 10.3.1 Transaction Types

Doc4.0 processing platform divides all transactions into several types, depending on the purpose of each transaction. Each transaction has a specific status.

sale	Acceptance of payment for provided goods or services in a single operation;
preauth	Blocking of a fixed amount of money on the card for the subsequent withdrawal (financial pledge). The cardholder will not be able to use the held funds, however, this money will not be withdrawn from the bank account until a subsequent request (capture) is received from the merchant. After a certain period of time, if a follow-up request is not received from the merchant, the holding of this funds amount is cancelled and it will become available for use again.








continues on next page

Table 2 - continued from previous page

capture	Withdrawal of the previously held by “preauth” transaction funds from the cardholder bank account.
cancel	Cancellation of fund holding by “preauth” transaction.
reversal	a refund operation for previously approved transaction (“sale” or “preauth” followed by “capture”). For example, a cancellation of an order by the customer, or a partial return of goods to the store.
transfer	Peer-to-peer (p2p) transfer transaction between 2 cards. This transaction can be split into 2 steps in some cases - card2account and deposit2card.
chargeback	Forced refund operation initiated by the cardholder, or the issuing bank, in case of fraud.
fraud	Special marker for fraudulent transactions.
retrieval	Request of additional documents for disputed or suspicious payment. Documents can be requested from the merchant or from their agent (service provider).
account verification	Validation of Payer’s card account information.
payout	Transfer of funds from Connecting Party banking account to customer (receiver) banking account or digital wallet.

### 10.3.2 Transaction Statuses

All transactions are marked according to their statuses:

	Approved transaction	The transaction was processed by the acquirer successfully (payment was made as part of the transaction), final status.
	Declined transaction	For any technical reason the acquirer cannot process the transaction. For example, this may be caused by insufficient funds on the customer card or account, final status.
	Filtered transaction	The transaction was filtered by Doc4.0 Payment Gateway and was not processed, final status.
	Error	Processing of transaction failed. A second attempt can be made to process the transaction. If the error occurs again, contact the Doc4.0 support service, final status.
	Unknown	Payment Gateway failed to get final transaction status. Contact the Doc4.0 support service to clarify the transaction status, non final status
	Failed	System’s internal status. It means there are no available settings to route transaction in the system due to filter restrictions, final status.
	Processing	Transaction is being processed, should continue polling. If transaction status haven’t been changed for one hour something went wrong, please stop polling and inform your payment gateway manager, non final status.

**Note**

after reconciliation transaction status could be changed even if transaction is in final status

## 10.4 MC/VISA/AmEx Fraud Regulation

- *Definitions*
- *Doc4.0 Flags and EFT possible Penalties*
- *Fraud programs description*
  - *MasterCard Excessive Chargeback Program*
    - \* *ECP Definitions*
  - *MasterCard Global Merchant Audit Program*
  - *Visa Merchant Chargeback Activity Monitoring*
  - *Visa Global Merchant Chargeback Monitoring Program Overview*
  - *Visa High Risk Chargeback Monitoring Program*
  - *Visa's Global Merchant Fraud Performance Program*
  - *Visa's Regional Merchant Fraud Performance Program*
  - *American Express Chargeback Programs*
- *Visa US Rules*
  - *Merchant Chargeback Monitoring Program - U.S. Region*
  - *Merchant Chargeback Monitoring Program Fees - U.S. Region*
  - *High-Brand Risk Chargeback Monitoring Program Fees - U.S. Region*
- *Acquirer Penalties*
  - *Acquirer Global Merchant Chargeback Monitoring Program*
  - *Acquirer Chargeback Monitoring Program - U.S. Region*
  - *Acquirer Fraud Monitoring Program*
  - *Acquirer Fraud Performance Monitoring Program Penalty Schedule - AP Region and CEMEA Region*
  - *Acquirer Fraud Monitoring Program Fines - U.S. Region*
  - *Risk Identification Service Online Conditions and Fees - U.S. Region*
- *Fraud reasons*
- *Chargeback reasons*
- *Retrieval Request Reasons*

### 10.4.1 Definitions

Country ID	Country
CTR	MasterCard's or Visa's Chargeback-to-Transaction Ratio
FSDVR	MasterCard's Fraud-to-Sales Dollar Volume Ratio
FSR	Visa's Fraud-to-Sales Ratio
GMAP	MasterCard's Global Merchant Audit Program
CMM	MasterCard's Chargeback-Monitored Merchant
ECM	MasterCard's Excessive Chargeback Merchant
MCMP	Visa's Merchant Chargeback Activity Monitoring
HRCMP	Visa's High Risk Chargeback Monitoring Program
GMCMP	Visa's Global Merchant Chargeback Monitoring Program
GMFPP	Visa's Global Merchant Fraud Performance Program
RMFPP	Visa's Regional Merchant Fraud Performance Program
International transaction	Transactions where the card was issued in the different country then the merchant is located
Regional transaction	Transactions where the card was issued in the same region as the merchant is located

### 10.4.2 Doc4.0 Flags and EFT possible Penalties

EFT	PNE Flag	Conditions	Penalties
MasterCard	CMM	<ul style="list-style-type: none"> <li>CTR 1.00%</li> <li>Chargebacks Count 100</li> </ul>	<ul style="list-style-type: none"> <li>Period calendar month</li> <li>Report Submission Fee USD 50</li> <li>Late Report Submission Fee USD 5,000 per month</li> <li>Chargeback Fee USD 0</li> </ul>

continues on next page

Table 5 - continued from previous page

EFT	PNE Flag	Conditions	Penalties
MasterCard	ECM	<ul style="list-style-type: none"> <li>• CTR 1.50%</li> <li>• Chargebacks Count 100</li> </ul>	<ul style="list-style-type: none"> <li>• Period two consecutive calendar months</li> <li>• Report Submission Fee USD 100</li> <li>• Late Report Submission Fee from USD 500 to USD 1,000 per day</li> <li>• Chargeback Fee USD 25 for Chargebacks exceeded 1.5%</li> <li>• Period first through sixth month</li> <li>• Report Submission Fee USD 100</li> <li>• Late Report Submission Fee from USD 500 to USD 1,000 per day</li> <li>• Chargeback Fee USD 25 for Chargebacks exceeded 1.5%</li> <li>• Period seventh through twelfth month</li> <li>• Report Submission Fee USD 100</li> <li>• Late Report Submission Fee from USD 500 to USD 1,000 per day</li> <li>• Chargeback Fee USD 25 for Chargebacks exceeded 1.5%</li> <li>• USD 50,000 per month after 12 months</li> </ul>
MasterCard	GMAP Step 1	<ul style="list-style-type: none"> <li>• FSDVR 3.00 - 4.99%</li> <li>• Frauds Count 3</li> <li>• Frauds Amount USD 3,000</li> </ul>	<ul style="list-style-type: none"> <li>• Period calendar month</li> <li>• Chargeback any fraud transaction NO</li> </ul>
MasterCard	GMAP Step 2	<ul style="list-style-type: none"> <li>• FSDVR 5.00 - 7.99%</li> <li>• Frauds Count 4</li> <li>• Frauds Amount USD 4,000</li> </ul>	<ul style="list-style-type: none"> <li>• Period calendar month</li> <li>• Chargeback any fraud transaction NO</li> </ul>

continues on next page

Table 5 - continued from previous page

EFT	PNE Flag	Conditions	Penalties
MasterCard	GMAP Step 3	<ul style="list-style-type: none"> <li>• FSDVR 8.00%</li> <li>• Frauds Count 5</li> <li>• Frauds Amount USD 5,000</li> </ul>	<ul style="list-style-type: none"> <li>• Period calendar month</li> <li>• Chargeback any fraud transaction YES</li> <li>• MasterCard, at its sole discretion, may extend the chargeback liability period to 12 months</li> </ul>
Visa	MCMP	<ul style="list-style-type: none"> <li>• CTR 3.00%</li> <li>• International (or Regional) Chargebacks Count 100</li> </ul>	<ul style="list-style-type: none"> <li>• Period any month</li> <li>• Chargeback Fee USD 0</li> </ul>
Visa	GMCMP	<ul style="list-style-type: none"> <li>• CTR 2.00%</li> <li>• International (or Regional) Chargebacks Count 200</li> <li>• International (or Regional) Transaction Count 200</li> </ul>	<ul style="list-style-type: none"> <li>• Period months 1-3</li> <li>• Chargeback Fee USD 0</li> <li>• Period months 4-9</li> <li>• Chargeback Fee USD 100 - USD 200</li> <li>• Period beyond month 9</li> <li>• Chargeback Fee USD 100 - USD 200</li> <li>• Penalty USD 25,000</li> </ul>
Visa	HRCMP Step 1	<ul style="list-style-type: none"> <li>• CTR 2.00%</li> </ul>	<ul style="list-style-type: none"> <li>• Period months 1-3</li> <li>• Chargeback Fee USD 100</li> <li>• Period months 4-6</li> <li>• Chargeback Fee USD 150</li> <li>• Period month 7 and subsequent months</li> <li>• Chargeback Fee USD 150</li> <li>• Penalty disqualify</li> </ul>
Visa	HRCMP Step 2	<ul style="list-style-type: none"> <li>• CTR 4.00%</li> <li>• International (or Regional) Chargebacks Count 3000</li> <li>• Merchant is assessed US \$1 million or more in GMCMP fees</li> </ul>	<ul style="list-style-type: none"> <li>• Period any month</li> <li>• Penalty disqualify</li> </ul>

continues on next page

Table 5 - continued from previous page

EFT	PNE Flag	Conditions	Penalties
Visa	GMFPP Step 1	<ul style="list-style-type: none"> <li>• FSR 2.50%</li> <li>• International Fraud Transaction count 25</li> <li>• International Fraud Transactions amount USD 25,000</li> </ul>	<ul style="list-style-type: none"> <li>• Period month 1-3</li> <li>• Period month 3 and above</li> <li>• Penalty USD 5,000 + USD 5,000 for every next month</li> <li>• Chargeback any fraud transaction YES</li> </ul>
Visa	GMFPP Step 2	<ul style="list-style-type: none"> <li>• FSR 2.50%</li> <li>• International Fraud Transactions amount USD 250,000</li> </ul>	<ul style="list-style-type: none"> <li>• Period month 1 and above</li> <li>• Penalty USD 5,000 + USD 5,000 for every next month</li> <li>• Chargeback any fraud transaction YES</li> </ul>
Visa	RMFPP Step 1	<ul style="list-style-type: none"> <li>• FSR 7.50%</li> <li>• Regional Fraud Transaction count 15</li> <li>• Regional Fraud Transactions amount USD 15,000</li> </ul>	<ul style="list-style-type: none"> <li>• Period month 1-3</li> <li>• Period month 3 and above</li> <li>• Chargeback any fraud transaction YES</li> </ul>
Visa	RMFPP Step 2	<ul style="list-style-type: none"> <li>• FSR 20.00%</li> <li>• Regional Fraud Transaction count 20</li> <li>• Regional Fraud Transactions amount USD 40,000</li> </ul>	<ul style="list-style-type: none"> <li>• Period month 1 and above</li> <li>• Chargeback any fraud transaction YES</li> </ul>
AmEx	AECP	<ul style="list-style-type: none"> <li>• CTR 3.00%</li> </ul>	<ul style="list-style-type: none"> <li>• Period 3 months and above</li> <li>• USD 5 per Disputed Charge if the Merchant is in the Immediate Chargeback Program</li> <li>• USD 15 per Disputed Charge if the Merchant is not in the Immediate Chargeback Program</li> </ul>

### 10.4.3 Fraud programs description

#### MasterCard Excessive Chargeback Program

MasterCard designed the Excessive Chargeback Program (ECP) to encourage each Acquirer to closely monitor, on an ongoing basis, its chargeback performance at the Merchant level and to determine promptly when a MasterCard Merchant has exceeded or is likely to exceed monthly chargeback thresholds.

See [ECP Manual](#)<sup>24</sup>

### **ECP Definitions**

#### MasterCard's Chargeback-to-Transaction Ratio (CTR)

The CTR is the number of MasterCard chargebacks received by the Acquirer for a Merchant in a calendar month divided by the number of the Merchant's MasterCard sales Transactions in the preceding month acquired by that Acquirer. (A CTR of 1% equals 100 basis points, and a CTR of 1.5% equals 150 basis points.)

#### MasterCard's Chargeback-Monitored Merchant (CMM)

A CMM is a Merchant that has a CTR in excess of 100 basis points and at least 100 chargebacks in a calendar month.

#### MasterCard's Excessive Chargeback Merchant (ECM)

A Merchant is an ECM if in each of two consecutive calendar months (the "trigger months"), the Merchant has a minimum CTR of 150 basis points and at least 100 chargebacks in each month. This designation is maintained until the ECM's CTR is below 150 basis points for two consecutive months.

#### Tier 1 ECM

A Merchant is a Tier 1 ECM during the first through sixth month (whether consecutive or non-consecutive) that the Merchant is identified as an ECM.

#### Tier 2 ECM

A Merchant is a Tier 2 ECM during the seventh through twelfth month (whether consecutive or non-consecutive) that the Merchant is identified as an ECM.

### **MasterCard Global Merchant Audit Program**

The Global Merchant Audit Program (GMAP) uses a rolling six months of data to identify MasterCard Merchant locations that, in any calendar month, meet the following criteria set.

See

#### Tier 1 - Informational Fraud Alert

- Three fraudulent Transactions
- At least USD 3,000 in fraudulent Transactions
- A fraud-to-sales dollar volume ratio minimum of 3% and not exceeding 4.99%

#### Tier 2 - Suggested Training Fraud Alert

<sup>24</sup> <https://www.mastercard.us/en-us/business/overview/support/rules.html>

- Four fraudulent Transactions
- At least USD 4,000 in fraudulent Transactions
- A fraud-to-sales dollar volume ratio minimum of 5% and not exceeding 7.99%

#### Tier 3 - High Fraud Alert

- Five fraudulent Transactions
- At least USD 5,000 in fraudulent Transactions
- A fraud-to-sales dollar volume ratio minimum of 8%

MasterCard, at its sole discretion, may extend the chargeback liability period to 12 months. MasterCard reserves the right to list the Acquirer ID, Acquirer name, Merchant name, Merchant location, and chargeback liability period of any Tier 3 Merchant in a Global Security Bulletin. When MasterCard lists the Acquirer and Merchant information in a Global Security Bulletin, Issuer chargeback rights will apply. Each Issuer then has a right to use message reason code 4849 - Questionable Merchant Activity to charge back to the Acquirer some fraudulent Transactions.

#### MasterCard's Fraud-to-Sales Dollar Volume Ratio (FSDVR)

The FSDVR is the amount of MasterCard frauds received by the Acquirer for a Merchant in a calendar month divided by the amount of the Merchant's MasterCard sales Transactions in the same month acquired by that Acquirer.

### **Visa Merchant Chargeback Activity Monitoring**

#### Visa's Chargeback-to-Transaction Ratio (CTR)

The CTR is the number of Visa chargebacks received by the Acquirer for a Merchant in a calendar month divided by the number of the Merchant's Visa sales Transactions in the same month acquired by that Acquirer. Disputes related to Chargeback Reason Code 93, "Merchant Fraud Performance Program", are excluded from program monitoring.

An Acquirer must monitor the Chargeback-to-Transaction volume ratio of its Merchants and identify any Merchant that:

- Receives more than 100 Chargebacks per month
- Exceeds a Chargeback-to-Transaction volume ratio of 3%

### **Visa Global Merchant Chargeback Monitoring Program Overview**

Visa monitors Merchant Outlets and Acquirers that generate an excessive level of international Chargebacks through the Global Merchant Chargeback Monitoring Program, as noted below and as specified in the Visa Global Merchant Chargeback Monitoring Program (GMCMP) Program Guide. Disputes related to Chargeback Reason Code 93, "Merchant Fraud Performance Program," are excluded from program monitoring.

A Merchant Outlet is identified in the Global Merchant Chargeback Monitoring Program if it meets or exceeds all of the following monthly performance activity levels:

- 200 international Chargebacks

- 200 International Transactions
- 2% ratio of international Chargebacks to International Transactions

Visa may modify or create new monthly performance levels to respond to different Chargeback and fraud trends that emerge.

**Global Merchant Chargeback Monitoring Program Handling Fees**

Visa assesses an Acquirer a Chargeback handling fee of US \$100 for each international Chargeback received for each identified Merchant Outlet once the Merchant has been placed in the Global Merchant Chargeback Monitoring Program. Visa collects the Chargeback handling fee from the Acquirer and disburses US \$70 to the Issuer that initiated the Chargeback through the Visa Integrated Billing Statement. Visa retains the balance as an administration fee. If the Acquirer and Merchant have not implemented procedures to reduce Chargebacks, Visa may assess the Acquirer an increased Chargeback handling fee not exceeding US \$200 for each international Chargeback received for its Merchant. Visa may, at its discretion, assess the Acquirer Chargeback handling fees for Trailing Chargeback Activity that occurs up to 4 months after Merchant termination, regardless of sales volume.

**Global Merchant Chargeback Monitoring Program Penalties**

Visa assesses Global Merchant Chargeback Monitoring Program penalties to the Acquirer, as described in the following tables.

Penalties for Global Merchant Chargeback Monitoring Program - Merchant-Level Thresholds	
Merchant Outlet meets or exceeds the Chargeback activity thresholds, as specified in Global Merchant Chargeback Monitoring Program Overview, in months 1-3 (month 1 = initial notification)	<ul style="list-style-type: none"> <li>• Workout Period <sup>1</sup></li> <li>• No fee</li> </ul>
Merchant Outlet meets or exceeds the Chargeback activity thresholds, as specified in Global Merchant Chargeback Monitoring Program Overview, in months 4-9	<ul style="list-style-type: none"> <li>• US \$100 per international Chargeback for every month the Merchant meets or exceeds the program thresholds <sup>1</sup></li> <li>• If the Acquirer and Merchant have not implemented procedures to reduce Chargebacks, Visa may assess the Acquirer a fee of US \$200 for each international Chargeback received for its Merchant <sup>2</sup></li> </ul>
Merchant Outlet meets or exceeds the Chargeback activity thresholds, as specified in Global Merchant Chargeback Monitoring Program Overview, beyond month 9	<ul style="list-style-type: none"> <li>• US \$100 per international Chargeback for every month the Merchant meets or exceeds the program thresholds <sup>1</sup></li> <li>• If the Acquirer and Merchant have not implemented procedures to reduce Chargebacks, Visa may assess the Acquirer a fee of US \$200 for each international Chargeback received for its Merchant <sup>2</sup></li> <li>• Acquirer is eligible for US \$25,000 review fee</li> <li>• Visa may initiate Merchant disqualification processes against a Merchant Outlet and/or its principals</li> </ul>

<sup>1</sup> The Workout Period is not applicable for Acquirer-level thresholds, High-Risk Merchants, or High-Brand Risk Merchants, as specified in High-Brand Risk Merchant Category Codes

<sup>2</sup> Visa allocates US \$70 of each fee to the Issuer via a Funds Disbursement

**Visa High Risk Chargeback Monitoring Program**

A Merchant required to use one of the following Merchant Category Codes is considered high-brand risk:

- 5962, “Direct Marketing-Travel-Related Arrangement Services”
- 5966, “Direct Marketing-Outbound Telemarketing Merchants”
- 5967, “Direct Marketing-Inbound Telemarketing Merchants”
- 7995, “Betting, including Lottery Tickets, Casino Gaming Chips, Off-Track Betting, and Wagers at Race Tracks”
- 5912, “Drug Stores, Pharmacies”
- 5122, “Drugs, Drug Proprietaries, Druggist Sundries”
- 5993, “Cigar Stores and Stands”, for Merchants that sell cigarettes in a Card-Absent Environment

Global Merchant Chargeback Monitoring Program - High-Brand Risk Merchants - Penalties  
 The following table specifies the penalties per international Chargeback for Acquirers of High-Brand Risk Merchants placed in the Global Merchant Chargeback Monitoring Program.

Merchant meets or exceeds the specified Chargeback ratio <sup>1</sup>	<ul style="list-style-type: none"> <li>• Months 1-3</li> <li>• US \$100 per Chargeback per month for each identified Merchant Outlet <sup>2</sup></li> </ul>
Merchant meets or exceeds the specified Chargeback ratio <sup>1</sup>	<ul style="list-style-type: none"> <li>• Months 4-6</li> <li>• US \$150 per Chargeback per month for each identified Merchant Outlet <sup>2</sup></li> </ul>
Merchant meets or exceeds the specified Chargeback ratio <sup>1</sup>	<ul style="list-style-type: none"> <li>• Month 7 and subsequent months</li> <li>• US \$150 per Chargeback per month for each identified Merchant Outlet <sup>2</sup> and Visa may disqualify the Merchant from participation in the Visa Program</li> </ul>
<p>Visa may disqualify the Merchant from participation in the Visa Program if merchant meets or exceeds the specified Chargeback ratio <sup>1</sup> without an effective Chargeback reduction plan, and 2 of the following levels of Chargeback activity are reached:</p>	<ul style="list-style-type: none"> <li>• Merchant’s Chargeback ratio is 2 or more times the specified Chargeback ratio (Single month)</li> <li>• Merchant is assessed fees for 3,000 or more Chargebacks (Single month)</li> <li>• Merchant is assessed US \$1 million or more in Global Merchant Chargeback Monitoring Program fees (When reached)</li> </ul>

<sup>1</sup> The Chargeback ratio threshold is 2%

<sup>2</sup> If the Acquirer and Merchant have not implemented procedures to reduce Chargebacks, Visa may assess the Acquirer a fee of US \$200 for each international Chargeback received for its Merchant

Acquirer does not identify a High-Brand Risk Merchant with the correct Merchant Category Code, as specified in “High-Brand Risk Merchant Category Codes”

- When violation occurs
- US \$25,000 per Merchant per month

### **Visa’s Global Merchant Fraud Performance Program**

Applies if a merchant is located in one region and a card is issued in another region.

### **Visa’s Regional Merchant Fraud Performance Program**

Applies to transactions where the card was issued in the same region as the merchant is located.

Visa’s Fraud-to-Sales Ratio (FSR)

The FSR is the number of Visa frauds received by the Acquirer for a Merchant in a calendar month divided by the number of the Merchant’s Visa sales Transactions in the same month acquired by that Acquirer.

### **American Express Chargeback Programs**

See [American Express Merchant Reference Guide - U.S.](#)<sup>25</sup>

Some chargebacks arise because merchants are placed in one of AmEx’s chargeback programs. The company may place you in any of these programs either upon signing your contract or at any time during the term of the agreement. These programs are:

#### **Immediate Chargeback Program**

This program allows AmEx to process a chargeback at any time a cardholder disputes a transaction, for any reason other than actual or alleged fraud and without having to first send you an inquiry. You may be placed in this program for one of the following three reasons:

- You choose to enroll in this program to avoid receiving inquiries or disputes.
- AmEx places you in this program if you meet the company’s criteria for disproportionate inquiries and chargebacks.
- Your industry has historically had high rates of customer disputes (not necessarily resulting in chargebacks).

#### **Partial Immediate Chargeback Program**

Your enrollment in this program allows AmEx to process chargebacks below a predetermined amount, without having to first send you an inquiry at any time a cardholder disputes a transaction for any reason other than actual or alleged fraud. All disputes for charges that are

---

<sup>25</sup> [https://www.americanexpress.com/content/dam/amex/us/merchant/new-merchant-regulations/Reference-Guide\\_EN\\_US.pdf](https://www.americanexpress.com/content/dam/amex/us/merchant/new-merchant-regulations/Reference-Guide_EN_US.pdf)

above that predetermined amount will be processed under the standard policy. You may be placed in this program for one of these three reasons:

- You choose to enroll in this program to avoid receiving inquiries for charges below a specific dollar amount.
- Your AmEx agreement stipulates participation in this program.
- Your industry has historically generated high rates of customer disputes.

#### Fraud Full Recourse Program

This program allows AmEx to issue chargebacks without first sending you an inquiry at any time it receives a cardholder dispute that is based on actual or alleged fraud. You may be placed in this program for one or more of the following reasons:

- You are classified as a high-risk merchant.
- AmEx receives a disproportionately high number of inquiries and chargebacks relative either to your prior history or to industry standards.
- Your merchant account has been cancelled for being fictitious, prohibited or otherwise in violation of the agreement.

Be advised that the above list of reasons, for which you may be placed in one of AmEx's chargeback programs, is not exhaustive. At its sole discretion, the company may place you in any one of them at any time.

#### Excessive dispute fee

If, in any three (3) months, the monthly ratio of Disputed Charges to gross Charges (less Credits) at an Establishment exceeds three percent, and thereafter in any month when the Establishment again exceeds this ratio, we may charge the Merchant a fee for each Disputed Charge in excess of this ratio.

- \$5 per Disputed Charge if the Merchant is in the Immediate Chargeback Program or
- \$15 per Disputed Charge if the Merchant is not in the Immediate Chargeback Program

### **10.4.4 Visa US Rules**

#### **Merchant Chargeback Monitoring Program - U.S. Region**

Visa monitors the total volume of U.S. Domestic and International Interchange and Chargebacks for a single Merchant Outlet and identifies U.S. Merchants that experience all of the following activity levels during any month:

- 100 or more interchange transactions
- 100 or more Chargebacks
- A 1% or higher ratio of overall Chargeback-to-Interchange volume

For the purposes of the U.S. Merchant Chargeback Monitoring Programs, if an Acquirer submits Interchange for a single Merchant Outlet under multiple names, Visa:

- Groups the Merchant activity
- Notifies the respective Acquirer of the Interchange grouping

**Merchant Chargeback Monitoring Program Fees - U.S. Region**

Visa assesses Merchant Chargeback Monitoring Program fees to a U.S. Acquirer, as described in the table below.

Merchant Chargeback Monitoring Program Fees - U.S. Region	
U.S. Merchant Outlet meets or exceeds the Chargeback activity thresholds specified in “Merchant Chargeback Monitoring Program - US Region”	<ul style="list-style-type: none"> <li>• Initial Notification - month 0</li> <li>• No fee</li> </ul>
U.S. Merchant Outlet continues to meet or exceed the Chargeback activity thresholds for the month following initial Notification	<ul style="list-style-type: none"> <li>• Notification - month 1</li> <li>• US \$5,000 for failure to return completed documentation within 10 calendar days of the Notification letter date</li> <li>• US \$1,000 per day until completed documentation is received</li> </ul>
U.S. Merchant Outlet continues to meet or exceed the Chargeback activity thresholds for the second month	<ul style="list-style-type: none"> <li>• Notification - month 2</li> <li>• US \$10,000 for failure to respond with an acceptable Chargeback reduction plan within 10 calendar days of the Notification letter date</li> <li>• US \$1,000 per day until acceptable Chargeback reduction plan is received</li> </ul>
U.S. Merchant Outlet continues to meet or exceed the Chargeback activity thresholds for months 3, 4, and 5	<ul style="list-style-type: none"> <li>• US \$50 per Chargeback for every month the Merchant continues to meet or exceed the Chargeback thresholds <sup>1</sup></li> </ul>
U.S. Merchant Outlet continues to meet or exceed the Chargeback activity thresholds for months 6 and 7	<ul style="list-style-type: none"> <li>• US \$100 per Chargeback for every month the Merchant continues to meet or exceed the Chargeback thresholds <sup>2</sup></li> </ul>
U.S. Merchant Outlet continues to meet or exceed the Chargeback activity thresholds for months 8 and 9	<ul style="list-style-type: none"> <li>• US \$25,000 review fee</li> <li>• US \$100 per Chargeback for every month the Merchant continues to meet or exceed the Chargeback thresholds <sup>2</sup></li> </ul>
U.S. Merchant Outlet continues to meet or exceed the Chargeback activity thresholds beyond month 9	<ul style="list-style-type: none"> <li>• US \$100 per Chargeback for every month the Merchant continues to meet or exceed the Chargeback thresholds <sup>2</sup></li> <li>• Merchant and its principals eligible for disqualification proceedings, as specified in “Critical Chargeback Levels - U.S. Region”</li> </ul>

<sup>1</sup> Visa allocates US \$40 of each fee to the Issuer via a Funds Disbursement

<sup>2</sup> Visa allocates US \$90 of each fee to the Issuer via a Funds Disbursement

## High-Brand Risk Chargeback Monitoring Program Fees - U.S. Region

<p>Visa assesses High-Brand Risk Chargeback Monitoring Program fees to a U.S. Acquirer, from the date of Notification, as described in the following table</p>	
<p>During months 1-3, the Merchant meets or exceeds the Chargeback activity thresholds specified in “High-Brand Risk Chargeback Monitoring Program - U.S. Region”</p>	<ul style="list-style-type: none"> <li>• US \$ 5,000 review fee month</li> <li>• US 100 per Chargeback in months 1-3 <sup>1</sup></li> </ul>
<p>During months 4-6, the Merchant meets or exceeds the applicable Chargeback ratios specified in <sup>1</sup> above</p>	<ul style="list-style-type: none"> <li>• US \$ 150 per Chargeback in months 4-6 <sup>2</sup></li> <li>• US \$ 25,000 review fee in month 6</li> </ul>
<p>After 6 months in which the Merchant has met or exceeded the Chargeback thresholds specified in “High-Brand Risk Chargeback Monitoring Program - U.S. Region”</p>	<ul style="list-style-type: none"> <li>• Visa may disqualify the Merchant from participation in the Visa Program</li> </ul>

<sup>1</sup> Visa allocates US \$90 of each fee to the Issuer via a Funds Disbursement

<sup>2</sup> Visa allocates US \$135 of each fee to the Issuer via a Funds Disbursement

### Merchant Disqualification - U.S. Region

Visa may disqualify a U.S. Merchant specified in “High-Brand Risk Merchant Category Codes” from participating in the Visa Program if the Merchant:

- Meets or exceeds a critical level of Chargeback activity, as determined by Visa
- Acts with the intent to circumvent Visa programs
- Causes harm to the Visa system
- The Acquirer must pay a US \$5,000 non-refundable fee and include it with the appeal letter

## 10.4.5 Acquirer Penalties

### Acquirer Global Merchant Chargeback Monitoring Program

An Acquirer is identified in the Global Merchant Chargeback Monitoring Program if it meets or exceeds all of the following monthly performance activity levels:

- 500 international Chargebacks
- 500 International Transactions
- 1.5% ratio of international Chargebacks to International Transactions
- One or more Merchants in the program during the reporting month

Penalties for Global Merchant Chargeback Monitoring Program - Acquirer-Level Thresholds

Acquirer meets or exceeds the Chargeback activity thresholds as specified in Global Merchant Chargeback Monitoring Program Overview	<ul style="list-style-type: none"> <li>• US \$25,000 for every month the Acquirer meets or exceeds the program thresholds</li> </ul>
Acquirer meets or exceeds the Chargeback activity thresholds, as specified in Global Merchant Chargeback Monitoring Program Overview, more than 3 times in a rolling 12-month period	<ul style="list-style-type: none"> <li>• US \$50,000 for every month the Acquirer meets or exceeds the program thresholds</li> </ul>
Acquirer meets or exceeds the Chargeback activity thresholds, as specified in Global Merchant Chargeback Monitoring Program Overview, more than 6 times in a rolling 12-month period	<ul style="list-style-type: none"> <li>• US \$100,000 for each subsequent month the threshold is met or exceeded</li> <li>• Acquirer is eligible for the imposition of Risk Reduction Procedures as specified in Member Risk Reduction Requirements</li> <li>• Visa may apply additional fines for repetitive or willful violations, as specified in Repetitive Violations and Willful Violations</li> </ul>

**Acquirer Chargeback Monitoring Program - U.S. Region**

Visa monitors the total volume of U.S. Domestic and International Interchange and Chargebacks for any U.S. Acquirer that experiences all the following activity levels during any month:

- 500 or more interchange transactions
- 500 or more Chargebacks
- A 1% or higher ratio of overall Chargeback-to-Interchange volume

Visa assesses High-Brand Risk Chargeback Monitoring Program fees to a U.S. Acquirer, from the date of Notification, as described in the following table

<p><b>Acquirer does not</b></p> <ul style="list-style-type: none"> <li>• Identify a High-Brand Risk Merchant with the correct Merchant Category Code</li> <li>• Register a High-Brand Risk Merchant</li> </ul>	<ul style="list-style-type: none"> <li>• US \$25,000 per Merchant per month</li> <li>• US \$100,000 after 3 violations in calendar year and/or prohibition against signing High-Brand Risk Merchants <sup>1</sup></li> </ul>
<p>Acquirer knowingly signs a disqualified Merchant or any of the disqualified Merchant’s principals</p>	<ul style="list-style-type: none"> <li>• US \$250,000 per month until the Acquirer terminates the Merchant Agreement <sup>1</sup></li> </ul>

<sup>1</sup> Visa may impose conditions on Acquirers for violations of the U.S. Regional Operating Regulations, up to and including termination of the Acquirer program

Visa assesses Acquirer Chargeback Monitoring Program fees to a U.S. Acquirer, as described in the following table.

Acquirer Chargeback Monitoring Program Fees - U.S. Region	
Acquirer knowingly attempts to circumvent the provisions of "Acquirer Chargeback Monitoring Program - U.S. Region"	<ul style="list-style-type: none"> <li>• US \$25,000 assessed 60 calendar days after Notification to the Acquirer</li> </ul>
Acquirer meets or exceeds the Chargeback activity thresholds specified in "Acquirer Chargeback Monitoring Program - U.S. Region"	<ul style="list-style-type: none"> <li>• US \$25,000</li> </ul>
Acquirer meets or exceeds the Chargeback activity thresholds more than 3 times in a rolling 12-month period	<ul style="list-style-type: none"> <li>• US \$100,000 for each subsequent month that either threshold is exceeded</li> </ul>
Acquirer has had 3 or more Merchants in the Merchant Chargeback Monitoring Programs for 6 consecutive months	<ul style="list-style-type: none"> <li>• Daily review fee of at least US \$2,500, with a one-week minimum fee of US \$17,500, assessed while a review of the Acquirer's and/or Merchants' Visa Card-related processing activities is being conducted, as specified in "Acquirer Processing Activity Review - U.S. Region"</li> </ul>
Acquirer fails to take action on recommendations resulting from a review of the Acquirer's and/or Merchants' Visa Card-related processing activities	<ul style="list-style-type: none"> <li>• US \$75,000 minimum</li> </ul>

### Acquirer Fraud Monitoring Program

Visa monitors an Acquirer to determine disproportionate fraud-to-sales ratios.

An Acquirer exceeding 3 times the worldwide or regional fraud-to-sales ratio for more than one quarter will be considered non-compliant and may be subject, but not limited, to the following fines and penalties:

- Monetary fines specified in the applicable Visa Regional Operating Regulations
- Temporary suspension of contracting with new Merchants
- Termination of membership

### Acquirer Fraud Performance Monitoring Program Penalty Schedule - AP Region and CEMEA Region

First violation	<ul style="list-style-type: none"> <li>• US \$25,000</li> </ul>
Second consecutive violation	<ul style="list-style-type: none"> <li>• US \$50,000</li> </ul>
3 or more consecutive violations	<ul style="list-style-type: none"> <li>• US \$100,000 for every subsequent violation per quarter OR Visa may revoke or suspend the Acquirer's license</li> </ul>

**Acquirer Fraud Monitoring Program Fines - U.S. Region**

First month	• US \$25,000
Second month	• US \$50,000
Third month	• US \$75,000
Fourth and subsequent months	• US \$100,000

**Risk Identification Service Online Conditions and Fees - U.S. Region**

Visa may:

- Impose conditions on a U.S. Acquirer if any of its Merchants are designated as an Identified Merchant by RIS Online
- Assess a daily review fee of at least US \$2,500, with a one-week minimum fee of US \$17,500, if an onsite review is required

If Visa determines that a U.S. Acquirer or its Merchant changed, modified, or altered Merchant data in any way to avoid detection by Risk Identification Service (RIS) Online, Visa may assess a US \$25,000 fee to the Acquirer for each occurrence identified.

Visa assesses the following fines, as specified in the table below, to a U.S. Acquirer after the 3-month Workout Period, as described in “Excessive Fraud Activity Notification - U.S. Region.”

Fine Period - month 1 <sup>1</sup> Acquirer receives Excessive Fraud Activity Notification <sup>2</sup>	• US \$10,000
Fine Period - month 2 or 3. Acquirer receives Excessive Fraud Activity Notification <sup>2</sup>	• US \$25,000
Fine Period - month 4. Acquirer receives Excessive Fraud Activity Notification <sup>2</sup>	• US \$50,000
Fine Period - month 5. Acquirer receives Excessive Fraud Activity Notification <sup>2</sup>	• US \$75,000
Fine Period - month 6. Acquirer receives Excessive Fraud Activity Notification <sup>2</sup>	• US \$50,000
Fine Period - beyond month 6. Acquirer receives subsequent Excessive Fraud Activity Notification(s) <sup>2</sup>	• US \$100,000 per month * Merchant and its principal(s) eligible for disqualification proceedings, as specified in “Critical Chargeback Levels - U.S. Region”

<sup>1</sup> The Risk Identification Service Online remediation process, including Notification requirements, is described in “Excessive Fraud Activity Notification - U.S. Region.”

<sup>2</sup> An Identified Merchant must remain below RIS Online Notification thresholds that incur a fine for at least 3 consecutive months for the Acquirer to exit the fine period specified in this table.

### 10.4.6 Fraud reasons

Code	Reason	Description
00	Lost Fraud	A fraudulent transaction that occurs with the use of a lost credit or debit card (or other device accessing a credit or debit card account for example convenience and balance transfer checks) without the actual implied or apparent authority of the cardholder.
01	Stolen Fraud	A fraudulent transaction that occurs with the use of a stolen credit or debit card (or other device accessing a credit or debit card account for example convenience and balance transfer checks) without the actual implied or apparent authority of the cardholder.
02	Never Received Issue	The interception and use of a credit or debit card (or other device accessing credit or debit card account for example convenience and balance transfer checks) before receipt by the cardholder by a person without the actual implied or apparent authority of the cardholder.
03	Fraudulent Application	A fraudulent transaction that occurs with the use of a credit or debit card that was obtained with an application using a false name or other false identification information.
04	Counterfeit Card Fraud	The use of altered or illegally reproduced credit or debit card (or other physical device accessing a credit or debit card account for example convenience and balance transfer checks) including the replication or alteration of the magnetic stripe or embossing.
05	Account Takeover Fraud	An existing credit or debit account is used without the actual implied or apparent authority of the cardholder by a person who gains access to and use of the account through an unauthorized means such as a change of address or request for re-issuance of credit or debit cards (or other device for accessing a credit or debit account for example convenience and balance transfer checks) but not lost or stolen cards.
06	Card Not Present Fraud	A fraudulent transaction that occurs with the use of credit or debit account information including pseudo-account information without the physical card or other device being involved via the phone mail Internet or other electronic means without the actual implied or apparent authority of the cardholder.
07	Multiple Imprint Fraud	A fraudulent transaction that occurs with a credit or debit card where the merchant having completed a legitimate face-to-face transaction deposits one or more additional transactions without the actual implied or apparent authority of the cardholder. For example the merchant makes several imprints of a card on paper formsets or produces terminal receipts upon receiving additional online or offline card-read authorization approvals.

continues on next page

Table 10 - continued from previous page

Code	Reason	Description
51	Bust-out Collusive Merchant	A collusive cardholder engaging in transactions with a collusive merchant as defined in the Cardholder-Merchant Collusion Program.

### 10.4.7 Chargeback reasons

Code	Reason	Description
30	Services Not Provided or Merchandise Not Received	<p>Merchant was unable or unwilling to provide services or Cardholder or authorized person did not receive the merchandise at the agreed-upon location or by the agreed-upon date.</p> <p>Required documents: Documentation to prove that Cardholder received services or proof that merchandise or ticket was received by Cardholder or authorized person on agreed-upon date or at agreed-upon location.</p> <p>Time frame: 120 days from the Transaction Processing Date or the date that the Cardholder expected to receive the service.</p>
41	Cancelled Recurring Transaction	<p>The Merchant continued to charge a Cardholder for a Recurring Transaction despite notification of cancellation.</p> <p>Required documents: Documentation to prove that service was not cancelled 15 calendar days prior to the Transaction Processing Date and documentation showing portion or amount of services or merchandise used.</p> <p>Time frame: 120 days from the Transaction Processing Date.</p>
4801	Requested Transaction Data Not Received	<p>Retrieval Request was not fulfilled.</p> <p>Required documents: Copy of Transaction Receipt.</p> <p>Time frame: 60 days from Retrieval request date.</p>

continues on next page

Table 11 - continued from previous page

Code	Reason	Description
4802	Requested/Required Information Illegible or Missing	<p>The Received a Transaction Receipt and the Account Number or amount is illegible.</p> <p>Required documents: Copy of Transaction Receipt.</p> <p>Time frame: 120 days from the Transaction Processing Date.</p>
4807	Warning Bulletin File	<p>The card was listed on electronic Warning Bulletin File however the Merchant completed the transaction.</p> <p>Required documents: None.</p> <p>Time frame: 45 days from the Transaction Processing Date.</p>
4808	Requested/Required Authorization Not Obtained	<p>The transaction amount exceeded the floor limit established by MasterCard but the Authorisation was not obtained or was declined.</p> <p>Required documents: None.</p> <p>Time frame: 45 days from the Transaction Processing Date.</p>
4812	Account Number Not on File	<p>Transaction did not receive Authorization and was processed using an Account Number that does not match any on the Issuer.</p> <p>Required documents: None.</p> <p>Time frame: 45 days from the Transaction Processing Date.</p>

continues on next page

Table 11 - continued from previous page

Code	Reason	Description
4831	Transaction Amount Differs	<p>The cardholder states that he or she was billed an incorrect amount.</p> <p>Required documents: Copy of the transaction receipt and proof to support that the cardholder is responsible for the disputed amount.</p> <p>Time frame: 120 days from the Transaction Processing Date.</p>
4834	Duplicate Processing	<p>The same transaction was processed more than once.</p> <p>Required documents: Copies of two different transaction receipts.</p> <p>Time frame: 120 days from the Transaction Processing Date.</p>
4835	Card Not Valid or Expired	<p>A Merchant completed the Transaction with a Card that expired prior to the Transaction Date and the Merchant did not obtained Authorization.</p> <p>Required documents: None.</p> <p>Time frame: 120 days from the Transaction Processing Date.</p>
4837	No Cardholder Authorization	<p>A Merchant did not obtained an Imprint and a signature (or a PIN) in a Card-Present Environment and the Merchant completed the Transaction without the Card holder's permission or a Transaction was processed with a Fictitious Account Number or no valid Card was outstanding bearing the Account Number or the Transaction Receipt.</p> <p>Required documents: Evidence of both: an Imprint, a signature or PIN.</p> <p>Time frame: 120 days from the Transaction Processing Date.</p>

continues on next page

Table 11 - continued from previous page

Code	Reason	Description
4840	Fraudulent Processing of Transactions	<p>Multiple Transactions occurred on a single Card at the same Merchant Outlet without the Cardholder's permission.</p> <p>Required documents: All transaction receipts and merchant explanation.</p> <p>Time frame: 120 days from the Transaction Processing Date.</p>
4841	Cancelled Recurring Transaction	<p>The card acceptor continued to bill a cardholder for a recurring transaction after receiving notification of cancellation from the cardholder or issuer or the issuer listed the cardholder.</p> <p>Required documents: None.</p> <p>Time frame: 120 days from the Transaction Processing Date.</p>
4842	Late Presentment	<p>Transaction was not processed within the required time limits.</p> <p>Required documents: None.</p> <p>Time frame: 120 days from the Transaction Processing Date.</p>
4846	Correct Transaction Currency Code Not Provided	<p>The acquirer did not transmit the correct transaction currency code. The transaction occurred in a dual currency environment and a transaction currency is not specified on the transaction receipt. A cardholder was not given the opportunity to choose the desired currency in which the transaction was completed or did not agree to the currency of transaction.</p> <p>Required documents: Documentation proving the correct currency was provided or specified.</p> <p>Time frame: 120 days from the Transaction Processing Date.</p>

continues on next page

Table 11 - continued from previous page

Code	Reason	Description
4847	Requested/Required Authorization Not Obtained and Fraudulent Transaction	<p>The transaction amount exceeded the floor limit established by MasterCard but the Authorisation was not obtained or was declined and the transaction is fraudulent.</p> <p>Required documents: None.</p> <p>Time frame: 120 days from the Transaction Processing Date.</p>
4849	Questionable Merchant Activity	<p>Issuers can use this chargeback only if the acquirer processed a transaction for a card acceptor that later was listed in a MasterCard Global Security Bulletin for violating MasterCard rules.</p> <p>Required documents: None.</p> <p>Time frame: 120 calendar days from the Global Security Bulletin publication date.</p>
4850	Credit Posted as a Purchase	<p>Cardholder account has been inaccurately posted with a debit instead of a credit as a result of an incorrect transaction code or keying error.</p> <p>Required documents: The acquirer must provide a copy of the TID as proof of the retail sale instead of a credit.</p> <p>Time frame: 120 days from the Transaction Processing Date.</p>
4853	Cardholder Dispute	<p>Cardholder returned (or attempted to return) goods or services to a card acceptor because it was not as described.</p> <p>Required documents: Copy of the TID or invoice (if applicable). Card acceptor.</p> <p>Time frame: 120 calendar days from the Transaction Processing Date or the date of receipt of goods and services if delayed delivery.</p>

continues on next page

Table 11 - continued from previous page

Code	Reason	Description
4855	Nonreceipt of Merchandise	<p>Cardholder or his or her authorized representative did not receive goods that were to be shipped or delivered.</p> <p>Required documents: Proof that the cardholder or person that the cardholder authorized received the merchandise.</p> <p>Time frame: 120-calendar day time frame is calculated from either the Transaction processing Date of the presented transaction or the latest anticipated delivery date.</p>
4857	Card-Activated Telephone Transaction	<p>The issuer.</p> <p>Required documents: Additional or corrected information to resolve billing discrepancy.</p> <p>Time frame: 120 days from the Transaction Processing Date.</p>
4859	Services Not Rendered	<p>The card acceptor is unwilling or unable to render services. The cardholder paid for services or goods by other means. The cardholder received none or only a part of an ATM cash disbursement. The cardholder did not receive airline transportation.</p> <p>Required documents: Proof that the services were rendered or that the card acceptor is able to render them. Appropriate card acceptor explanation. Documentation that verifies the disbursement of funds.</p> <p>Time frame: 120 days from the Transaction Processing Date.</p>

continues on next page

Table 11 - continued from previous page

Code	Reason	Description
4860	Credit Not Processed	<p>Card acceptor has not posted a credit to his or her account or that the card acceptor posted a credit and reduced the amount of the credit due without proper disclosure.</p> <p>Required documents: Card acceptor rebuttal (for example, the card acceptor rebuttal states that the merchandise was never returned or that the cancellation was not accepted) or proper disclosure given at the point of int.</p> <p>Time frame: 120 days from the Transaction Processing Date.</p>
4862	Counterfeit Transaction Magnetic Stripe POS Fraud	<p>Fraudulent transaction and that the cardholder or a person authorized by him or her was in possession of all cards issued with the account on the transaction date.</p> <p>Required documents: Evidence of both: an Imprint, a signature or PIN.</p> <p>Time frame: 120 days from the Transaction Processing Date.</p>
4863	Cardholder Does Not Recognize	<p>The Cardholder does not recognize the Transaction.</p> <p>Required documents: Copy of Transaction Receipt.</p> <p>Time frame: 120 days from the Transaction Processing Date.</p>
4870	Chip Liability Shift	<p>A counterfeit card-present transaction was processed to chip card on non-EMV terminal and both the issuer and the acquirer are located in a country or region that has adopted a chip liability shift program.</p> <p>Required documents: None.</p> <p>Time frame: 120 days from the Transaction Processing Date.</p>

continues on next page

Table 11 - continued from previous page

Code	Reason	Description
4871	Chip/PIN Liability Shift	<p>A fraudulent transaction resulted from the use of a hybrid PIN-preferring card at a magnetic stripe-reading-only terminal (whether PIN-capable or not) or at a chip-capable terminal not equipped with a PIN pad capable (at a minimum) of checking the PIN offline and both the issuer and the acquirer are located in a country or region that has adopted a chip liability shift program.</p> <p>Required documents: None.</p> <p>Time frame: 120 days from the Transaction Processing Date.</p>
4899	Domestic Chargeback Dispute (Europe Region Only)	<p>Issuers only may use message reason code 4899 in the case of a centrally acquired domestic transaction or a domestic transaction processed through Banknet or EPS-Net where a chargeback is available according to the applicable domestic rule but cannot be processed under a different message reason code.</p> <p>Required documents: With accordance with domestic rule.</p> <p>Time frame: With accordance with domestic rule.</p>
53	Not as Described or Defective Merchandise	<p>The Cardholder received damaged or defective merchandise or the merchandise or service did not match what was described on the Transaction Receipt or other documentation presented at the time of purchase.</p> <p>Required documents: Documents to prove that the service or merchandise was correctly described and was not defective. Proof that the service was not cancelled and was used by the cardholder or proof that the merchandise.</p> <p>Time frame: 120 days from the Transaction Processing Date.</p>

continues on next page

Table 11 - continued from previous page

Code	Reason	Description
57	Fraudulent Multiple Transactions	<p>Multiple Transactions occurred on a single Card at the same Merchant Outlet without the Cardholder's permission.</p> <p>Required documents: Evidence that fraudulent multiple Transactions did not occur. Evidence that Transactions represent valid delayed or amended charges for T&amp;E Transaction.</p> <p>Time frame: 120 days from the Transaction Processing Date.</p>
60	Illegible fulfillment	<p>The Received a Transaction Receipt and the Account Number or amount is illegible.</p> <p>Required documents: Legible copy of the Transaction Receipt.</p> <p>Time frame: 120 days from the Transaction Processing Date.</p>
62	Counterfeit Transaction	<p>A Counterfeit Card was used for a Magnetic stripe or Chip-initiated transaction that received Authorization but the Authorization Request did not include the required data or contained altered data. A counterfeit card-present transaction was processed to chip card on non-EMV terminal and both the issuer and the acquirer are located in a country or region that has adopted a chip liability shift program.</p> <p>Required documents: None.</p> <p>Time frame: 120 days from the Transaction Processing Date.</p>
70	Card Recovery Bulletin or Exception file	<p>A Merchant did not check the Card Recovery Bulletin or Exception File for a Transaction with an amount that was below the Floor Limit.</p> <p>Required documents: None.</p> <p>Time frame: 75 days from the Transaction Processing Date.</p>

continues on next page

Table 11 - continued from previous page

Code	Reason	Description
71	Declined Authorization	<p>A Merchant completed the Transaction after an Authorization Request received a Decline Response.</p> <p>Required documents: None.</p> <p>Time frame: 75 days from the Transaction Processing Date.</p>
72	No Authorization	<p>Authorization was required for the Transaction but the Merchant did not obtain Authorization.</p> <p>Required documents: None.</p> <p>Time frame: 75 days from the Transaction Processing Date.</p>
73	Expired Card	<p>A Merchant completed the Transaction with a Card that expired prior to the Transaction Date and the Merchant did not obtained Authorization.</p> <p>Required documents: Documentation to prove the card was not expired on the Transaction Date.</p> <p>Time frame: 75 days from the Transaction Processing Date.</p>
74	Late Presentment	<p>Transaction was not processed within the required time limits and the account was not in good standing on the Chargeback. Processing Date or the Transaction was processed more than 180 calendar days from the Transaction Date.</p> <p>Required documents: None.</p> <p>Time frame: 120 days from the Transaction Processing Date.</p>

continues on next page

Table 11 - continued from previous page

Code	Reason	Description
75	Transaction not Recognized	<p>The Cardholder does not recognize the Transaction.</p> <p>Required documents: Copy of Transaction Receipt.</p> <p>Time frame: 120 days from the Transaction Processing Date.</p>
76	Incorrect currency or Transaction Code or Domestic Transaction processing violation	<p>Transaction was processed with an incorrect Transaction code or an incorrect currency code or the Merchant did not deposit a Transaction Receipt in the country where the Transaction occurred or the Cardholder was not advised that Dynamic Currency Conversion would occur or was refused the choice of paying in the Merchant.</p> <p>Required documents: Transaction Receipt or other record that proves that the Transaction was correct.</p> <p>Time frame: 120 days from the Transaction Processing Date.</p>
77	Non-matching Account Number	<p>Transaction did not receive Authorization and was processed using an Account Number that does not match any on the Issuer.</p> <p>Required documents: None.</p> <p>Time frame: 120 days from the Transaction Processing Date.</p>
78	Service Code Violation	<p>Authorization was not obtained for a Magnetic-Stripe read Transaction on a Visa Electron Card or on a Visa Card in a registered mandatory positive Authorization account range.</p> <p>Required documents: None.</p> <p>Time frame: 75 days from the Transaction Processing Date.</p>

continues on next page

Table 11 - continued from previous page

Code	Reason	Description
80	Incorrect Transaction Amount or Account Number	<p>Transaction amount is incorrect or an addition or transposition error was made when calculating the Transaction amount or Merchant altered the Transaction amount after the Transaction was completed without the consent of the Cardholder or a Transaction was processed using an incorrect Account Number.</p> <p>Required documents: Transaction Receipt or other record to prove that Transaction Amount and Account number was correct.</p> <p>Time frame: 120 days from the Transaction Processing Date.</p>
81	Fraud - Card-Present Environment	<p>A Merchant did not obtain an Imprint and a signature (or a PIN) in a Card-Present Environment and the Merchant completed the Transaction without the Cardholder's permission or a Transaction was processed with a Fictitious Account Number or no valid Card was outstanding bearing the Account Number or the Transaction Receipt. A fraudulent card-present transaction was processed to a lost/stolen chip card on a non-EMV terminal and both the issuer and the acquirer are located in a country or region that has adopted a chip liability shift program.</p> <p>Required documents: Transaction Receipt or other record to prove separate Transactions were processed and a proof that the transactions were not for the same service or merchandise.</p> <p>Time frame: 120 days from the Transaction Processing Date.</p>

continues on next page

Table 11 - continued from previous page

Code	Reason	Description
82	Duplicate Processing	<p>A single Transaction was processed more than once.</p> <p>Required documents: Evidence of Imprint and signature or PIN. Compelling evidence that the cardholder participated in the Transaction.</p> <p>Time frame: 120 days from the Transaction Processing Date.</p>
83	Fraud - Card-Absent Environment	<p>A Mail/Phone Order Recurring or Electronic Commerce Transaction was processed without the Cardholder's permission or a Fictitious Account Number was used or no valid Card was outstanding bearing the Account number on the Transaction Receipt.</p> <p>Required documents: Proof that the service was not cancelled and was used by the cardholder or proof that the merchandise was not returned. Proof that cancellation policy was correctly described.</p> <p>Time frame: 120 days from the Credit Transaction Processing Date.</p>
85	Credit Not Processed	<p>A Merchant did not process a Credit Transaction Receipt as required.</p> <p>Required documents: Documents (other than Transaction Receipt) to prove that Merchant did not receive payment by other means for the same merchandise or service.</p> <p>Time frame: 120 days from the Transaction Processing Date.</p>
86	Paid by Other Means	<p>Merchandise or service was received but paid by other means.</p> <p>Required documents: None.</p> <p>Time frame: 120 days from the Transaction Processing Date.</p>

continues on next page

Table 11 - continued from previous page

Code	Reason	Description
90	Non-Receipt of Cash or Load Transaction Value at ATM or Load Device	<p>Cardholder did not receive or received only a portion of cash or Load Transaction value.</p> <p>Required documents: Evidence of both: an Imprint, a signature or PIN.</p> <p>Time frame: 120 days from the Transaction Processing Date.</p>
93	Merchant Fraud Performance Program	<p>Visa notified that the Transaction is identified by the Merchant Fraud Performance Program.</p> <p>Required documents: None.</p> <p>Time frame: 120 days from the Transaction Processing Date.</p>
96	Transaction Exceeds Limited Amount	<p>An Unattended Acceptance Terminal that performs Cardholder-Activated Transaction Type A or Cardholder-Activated Transaction Type B exceeded the allowed amount.</p> <p>Required documents: None.</p> <p>Time frame: 120 days from the Transaction Processing Date.</p>
28	Request for Copy Bearing Signature	The cardholder's bank requests a copy of the transaction receipt from the merchant for fraud analysis.
33	Fraud Analysis Request	The cardholder's bank requests a copy of the receipt from the merchant for fraud analysis.
79	Requested Transaction Information Not Received	This chargeback occurs when a merchant does not respond to a retrieval request within the specified time frame or does not provide a legible response.
5621	Sales Draft Chargeback	Sales Draft Chargeback.
10	Fraud	Fraud.
10.1	EMV Liability Shift Counterfeit Fraud	EMV Liability Shift Counterfeit Fraud.
10.2	EMV Liability Shift Non-Counterfeit Fraud	EMV Liability Shift Non-Counterfeit Fraud.
10.3	Other Fraud-Card Present Environment	Other Fraud-Card Present Environment.
10.4	Other Fraud-Card Absent Environment	Other Fraud-Card Absent Environment.

continues on next page

Table 11 - continued from previous page

Code	Reason	Description
10.5	Visa Fraud Monitoring Program	Visa Fraud Monitoring Program.
11.1	Card Recovery Bulletin	Card Recovery Bulletin.
11.2	Declined Authorization	Declined Authorization.
11.3	No Authorization	No Authorization.
12.1	Late Presentment	Late Presentment.
12.2	Incorrect Transaction Code	Incorrect Transaction Code.
12.3	Incorrect Currency	Incorrect Currency.
12.4	Incorrect Account Number	Incorrect Account Number.
12.5	Incorrect Amount	Incorrect Amount.
12.6	Duplicate Processing/Paid by Other Means	Duplicate Processing/Paid by Other Means.
12.7	Invalid Data	Invalid Data.
13	Consumer Dispute	Consumer Dispute.
13.1	Merchandise / Services Not Received	Merchandise / Services Not Received.
13.2	Cancelled Recurring	Cancelled Recurring.
13.3	Not as Described or Defective Merchandise/Services	Not as Described or Defective Merchandise/Services.
13.4	Counterfeit Merchandise	Counterfeit Merchandise.
13.5	Misrepresentation	Misrepresentation.
13.6	Credit Not Processed	Credit Not Processed.
13.7	Cancelled Merchandise/Services	Cancelled Merchandise/Services.
13.8	Original Credit Transaction Not Accepted	Original Credit Transaction Not Accepted.
13.9	Non-Receipt of Cash or Load Transaction Value	Non-Receipt of Cash or Load Transaction Value.
501	Non-JCB Card	This chargeback occurs when a valid authorization was not obtained from the Issuing bank and the card information embossed on or encoded in the magnetic stripe of the card does not conform to JCB's card specification. This chargeback may be reversed by supplying proof that a valid authorization was obtained at the time of the sale along with a signed swiped or imprinted sales draft that conforms to JCB specifications or evidence that a credit was issued.
502	Card-Member Dispute	This chargeback occurs when a cardholder disputes goods received or services rendered. This chargeback may be reversed by supplying a written rebuttal which provides proof that the goods/services described on the sales receipt or invoice were suitable there was proper disclosure at the time of purchase or evidence that a credit was issued.

continues on next page

Table 11 - continued from previous page

Code	Reason	Description
503	Expired JCB Card	This chargeback occurs when the card used in a transaction expired before the transaction date and the sale is processed without a valid authorization. This chargeback may be reversed by supplying proof that a valid authorization was obtained at the time of the sale along with a signed swiped or imprinted sales draft that provides a valid expiration date for the card at the time of the sale or evidence that a credit was issued.
507	Incorrect Transaction Amount	This chargeback occurs when the incorrect transaction amount is entered for a sale. This chargeback may be reversed by supplying proof that the transaction amount is correct and/or a legible copy of the signed swiped or imprinted sales draft or evidence that a credit was issued.
510	Mis-Post	This chargeback occurs when a credit transaction incorrectly posts as a debit or a debit posts as a credit to the cardholder's account.
512	Duplicate Processing	This chargeback occurs when a cardholder states that they were charged twice for the same transaction. This chargeback may be reversed by supplying two separate signed sales drafts for each transaction or evidence that a credit has been issued.
513	Credit Not Received	This chargeback occurs when a customer indicates they have not received a credit to their account. This chargeback may be reversed by supplying proof that the credit has been issued to this account or a signed sales receipt stating your refund policy at the time of purchase or evidence that a credit has been issued.
516	Non-Receipt of Requested Item	This chargeback occurs when a customer claims they did not receive merchandise which was to be delivered or goods were paid for by other means. This chargeback may be reversed by supplying proof of delivery signed by the cardholder a signed swiped draft proving the cardholder picked up the merchandise or evidence that a credit has been issued.

continues on next page

Table 11 - continued from previous page

Code	Reason	Description
517	Requested Copy Illegible	This chargeback occurs when the Issuer of an account requests a copy of a transaction receipt on behalf of the cardholder and a legible copy of the draft requested was not received. This chargeback may be reversed by supplying a legible copy of the signed swiped or imprinted draft that was requested or evidence that a credit has been issued.
521	Transaction Exceeds Floor limit	This chargeback occurs when a transaction exceeds the relevant floor limit that applies without a valid authorization at the time of the sale or the transaction amount that exceeds the relevant floor limit is greater than the authorized amount. This chargeback may be reversed by supplying proof of a valid authorization for the transaction or any amount that is greater than your assigned floor limit or evidence that a credit has been issued.
522	Authorization Declined	This chargeback occurs when a transaction for an account was processed after receiving a decline response. This chargeback may be reversed by supplying proof that a valid authorization was given for the transaction or evidence that a credit was issued.
523	Incorrect Card Number	This chargeback occurs when an account number is provided to the Issuer for a transaction and it does not match any account number in the bank's master file. This chargeback may be reversed by supplying an imprinted or swiped sales draft which has the same account number as the one that is being disputed.
524	Addition Error	This chargeback occurs when a cardholder's copy of the sales draft or other transaction record shows an error in addition which causes the total amount to be incorrect. This chargeback may be reversed by providing proof that the transaction amount is correct and/or a legible copy of the signed swiped or imprinted sales draft or evidence that a credit has been issued.
525	Altered Amount	This chargeback occurs when a customer claims that the incorrect amount was billed to their account. This chargeback may be reversed by supplying proof that the transaction was processed correctly or evidence that a credit has been issued.

continues on next page

Table 11 - continued from previous page

Code	Reason	Description
526	No Signature	This chargeback occurs when a cardholder claims they did not participate in or authorize a transaction to take place. This chargeback may be reversed by supplying a signed swiped or imprinted sales draft proof of delivery signed by the cardholder or evidence that a credit has been issued.
527	No Imprint	This chargeback occurs when a cardholder claims they did not participate in or authorize a transaction to take place. This chargeback may be reversed by supplying a signed swiped or imprinted sales draft or evidence that a credit has been issued.
534	Unauthorized Multiple Transactions	This chargeback occurs when two or more transactions take place at one location and the cardholder claims they only authorized or participated in one. This chargeback may be reversed by supplying a signed swiped or imprinted sales draft for all transactions with the cardholder or evidence that a credit has been issued.
536	Late Submission	This chargeback occurs when more than 45 days have elapsed between the transaction date and the settlement of the sale. This chargeback may be reversed by supplying a signed swiped or imprinted sales draft and the corresponding batch header ticket or evidence that a credit has been issued.
537	No Show Dispute	This chargeback occurs when a cardholder claims they made a hotel or car rental reservation but one of the following occurred.
538	Advance Deposit	This chargeback occurs when a cardholder claims that they participated in a transaction for an advance deposit to secure a hotel reservation but one of the following occurred.
541	Illegible Item	This chargeback occurs when the Issuer of an account requests a copy of a transaction receipt on behalf of the cardholder and a legible copy of the draft requested was not received. This chargeback may be reversed by supplying a legible copy of the signed swiped or imprinted sales draft that was requested or evidence that a credit has been issued.
544	Cancelled Recurring Transaction	This chargeback occurs when a cardholder claims that the authority to process recurring transactions was cancelled prior to the transaction date. This chargeback may be reversed by supplying proof that the cardholder authorized the transaction or evidence that a credit has been issued.

continues on next page

Table 11 - continued from previous page

Code	Reason	Description
546	Unauthorized Purchase	This chargeback occurs when a cardholder claims that they did not participate in or authorize a transaction to take place. This chargeback may be reversed by supplying a signed swiped or imprinted sales draft proof of delivery signed by the cardholder or evidence that a credit has been issued.
547	JCB Card on Stop List	This chargeback occurs when the JCB card presented for payment was listed on a Stop List that was effective at the time of sale. This chargeback may be reversed by providing proof that the card was not listed on the Stop List at the time of sale or evidence that a credit has been issued.
554	Non-Receipt of Merchandise/Cash at ATM	This chargeback occurs when a) the cardholder does not receive merchandise at the agreed location or b) the cardholder participated in an ATM transaction but the requested amount of cash was not dispensed to the cardholder. This chargeback may be reversed by supplying proof of delivery showing the cardholder received the merchandise or received the requested amount in the case of an ATM transaction or evidence that a credit has been issued.
580	Non-Receipt of T&E Documentation	This chargeback occurs when an Issuer did not receive the requested copy of the sales draft within the allowed time frame. This chargeback may be reversed by supplying proof that the requested copy was provided within the allowed time frame or evidence that a credit has been issued.
581	Split Sale	This chargeback occurs when a transaction requiring an authorization decision was split into two or more card sales to avoid authorization and had the whole sale been submitted for authorization it would have been declined. This chargeback may be reversed by supplying proof that the transaction is not a split sale or that a valid authorization was obtained for the whole amount or evidence that a credit has been issued.
582	Domestic Transaction	This chargeback occurs when the domestic transaction processed was settled through the International Interchange. This chargeback may be reversed by supplying documentation or information that you feel will assist in reversing the chargeback or evidence that a credit has been issued.

continues on next page

Table 11 - continued from previous page

Code	Reason	Description
583	Paid By Other Means	This chargeback occurs when a cardholder paid for a transaction by an alternate method. This chargeback may be reversed by supplying a signed swiped or imprinted sales draft or evidence that a credit has been issued.
A01	Charge Amount Exceeds Authorization Amount	No additional information.
A02	No Valid Authorization	No additional information.
A08	Authorization Approval Expired	No additional information.
C02	Credit Not Processed	No additional information.
C04	Goods/Services Returned or Refused	No additional information.
C05	Goods/Services Canceled	No additional information.
C08	Goods/Services Not Received or Only Partially Received	No additional information.
C14	Paid by Other Means	No additional information.
C18	No Show or CARDeposit Canceled	No additional information.
C28	Canceled Recurring Billing	No additional information.
C31	Goods/Services Not As Described	No additional information.
C32	Goods/Services Damaged or Defective	No additional information.
F10	Missing Imprint	No additional information.
F14	Missing Signature	No additional information.
F24	No Card Member Authorization	No additional information.
F29	Card Not Present	No additional information.
F30	EMV Counterfeit	No additional information.
F31	EMV Lost/Stolen/Non - Received	No additional information.
FR2	Fraud Full Recourse Program	No additional information.
FR4	Immediate Chargeback Program	No additional information.
FR6	Partial Immediate Chargeback Program	No additional information.
M01	Chargeback Authorization	No additional information.
M10	Vehicle Rental - Capital Damages	No additional information.
M49	Vehicle Rental - Theft or Loss of Use	No additional information.
P01	Unassigned Card Number	No additional information.
P03	Credit Processed as Charge	No additional information.
P04	Charge Processed as Credit	No additional information.
P05	Incorrect Charge Amount	No additional information.
P07	Late Submission	No additional information.
P08	Duplicate Charge	No additional information.
P22	Non-Matching Card Number	No additional information.
P23	Currency Discrepancy	No additional information.
R03	Insufficient Reply	No additional information.
R13	No Reply	No additional information.

continues on next page

Table 11 - continued from previous page

Code	Reason	Description
6321	No authorize or participate	A chargeback initiated when the cardholder claims they were in possession of a valid card on the date of transaction or she did not authorize or participate in the transaction processed by the merchant.
6323	Transaction Information Document (TID)	Represents a situation where the cardholder is requesting Transaction Information Document (TID) from the merchant needed for his personal records expense reporting etc.
6341	Fraud investigation by the bank or issuer	A dispute that is initiated due to a fraud investigation by the bank or issuer.
G001	Recall/Customer Dispute	Recall/Customer Dispute.

### 10.4.8 Retrieval Request Reasons

Code	Description
3	Credit Not Received for Tickets/Vouchers
4	Request Reshipment of Tickets Not Received
7	Billing was to be in Installments - Credit Due
9	Customer Requests Return Instructions/Pickup
10	Partial Credit Received - Remaining Credit Due
11	Customers Requests Waiving Cancellation Fee - Credit Due
12	Charged Billed Twice in Error
15	Requests Credit for Exchange Fee
16	Requests Credit for Damaged Merchandise
18	Requests Credit for Overcharge
20	Claims Cancelled Service - Requests Credit and Discontinue Future Billings
21	Claims Cancelled Service - Issue Credit or Provide Cancellation Policy and Discontinue Billing
22	Claims Cancelled Membership - Requests Credit and Discontinue Future Billings
24	Damaged Merchandise, Requests Return
27	Order Canceled - Issue Credit or Provide Cancellation Policy/Proof of Delivery
28	Membership Cancelled in Writing - Issue Credit/supply signed Cancellation Policy & discontinue
29	Membership Expired - Issue Credit or supply signed contract with renewal policy/expiration date
30	Defective Merchandise - Credit Requested
31	Deposit on Vehicle not Purchased, Issue Credit or provide Signed Agreement
33	Cardholder Does has No Knowledge of Charges, Provide support and itemization or Issue Credit
40	Service / Membership Cancelled - Credit Requested or Proof of Usage
41	Unable to contact/cancel - Discontinue Charges
42	Customer Claims Alternate Bill Arrangement - Requests Credit and Discontinue Future Billings
43	Request to Cancel Service - Contact Customer Directly
44	Requests Cancellation of Service - Provide Cancellation instructions/authorization
45	Requests Replacement for Damaged Merchandise

continues on next page

Table 12 - continued from previous page

Code	Description
48	Requests Replacement for Damaged Merchandise
49	Deposit on Vehicle not Leased - Issue Credit or Provide signed Agreement
59	Requests Repair of Damaged Merchandise
60	Requests Repair of Defective Merchandise
61	Credit should have been Charge - Bill Customer
62	Charge should have been Credit - Issue Full Credit
63	Dissatisfied w/ Good/Service - Credit Requested
70	Dissatisfied w/ Repair Work on Vehicle - Credit Requested
71	Requests Credit for Personal Property Damage (Moving services) - Credit Requested
72	Cardholder has no Knowledge of Billing and it has Wrong Signature
73	Reservation not Guaranteed, was to be Cancelled - Credit Requested
76	Cancelled Service - Issue credit or provide copy of agreement and Discontinue Future Billings
77	Request to Return Merchandise - Provide Return Instructions
78	Invalid Plastic Number, Provide Valid Number to avoid Chargeback
79	Invalid Plastic Number, Provide Valid Number to avoid Chargeback
80	Cancelled Time Share - Credit Requested or provide copy of signed agreement
82	Customer has No Knowledge of Credit to their Account
83	Referenced Customer Deceased
86	Discontinue billings to this Inactive Account
87	Issue Credit and Discontinue Billing to Inactive Acct
89	Alternative Billing Arrangements - Credit Requested or provide supporting documentation
90	Membership/Service Paid in Full - Credit Requested and Discontinue Future Billings
91	Cancellation Made within Allowable Time - Credit Requested
93	Cardholder Does Not Recognize Charges
94	Cardholder Does Not Recognize Charges
95	Cancelled Service - Credit Requested or provide signed proof serviced were rendered
97	Customer Requests Credit for Unauthorized Charges
99	Class/Course Cancelled - Credit Requested
107	Facility No Longer Open - Credit Requested and Discontinue Future Billings
110	Calls associated with charges Connected to Wrong Number
117	Call associated with charges was Cut-off
119	Cardholder has No Knowledge of CARDeposit Billing - Requests Credit
120	Requests Credit for Overcharge for Vehicle Rental
121	Requests Credit for Rental Vehicle did not perform properly
122	Cardholder has No Knowledge of Vehicle Rental - Issue Credit
123	Cardholder has No Knowledge of Vehicle Rental - Issue Credit
124	Customer Requests support for Charges
125	Cardholder has No Knowledge of Vehicle Rental - Issue Credit
127	Cardholder Does Not Recognize Charges, Provide Documentation or Issue Credit
128	Cardholder Claims they did Not Authorize Charges, Provide Documentation or Issue Credit
129	Cardholder Does Not Recognize Charges, Provide Documentation or Issue Credit
130	Requests Credit for Deposit not Deducted from Rental Billing
131	Charge was to be Billed Directly to Insurance company
132	Customer Billed Twice from separate business addresses

continues on next page

Table 12 - continued from previous page

Code	Description
133	Billed Twice for same Purchase
134	Customer Claims Portion of Charge was a Deposit
136	Customer Claims Charge was for Deposit
141	Customer Claims Charge was Deposit on Vehicle Returned
143	Customer Claims Flowers ordered Not Received
146	Disputed Merchandise Returned but 2nd charge processed instead of credit
147	Customer Claims Billing Paid by Insurance Company
150	Returned Damaged Merchandise - Provide Documentation or Issue Credit
151	Returned Damaged Merchandise and Requests Replacement or Credit
152	Received & Returned Incorrect Merchandise, Provide Documentation or Issue Credit
153	Received & Returned Incorrect Merchandise and Requests Replacement or Credit
154	Cancelled Order - Provide Documentation or Issue Credit
155	Merchandise not Received - Provide Documentation or Issue Credit
156	Merchandise not Received - Issue Credit and Rebill Upon Delivery
157	Returned Merchandise but not sent Replacement- Provide Documentation or Issue Credit
158	Merchandise Returned, Provide Documentation or Issue Credit
159	Customer Requests signed support and itemization for Charges
160	Tickets/Vouchers not Ordered - Provide Documentation or Issue Credit
161	Tickets/Vouchers Returned - Provide Documentation or Issue Credit
162	Tickets/Vouchers Returned - Provide Documentation or Issue Credit
163	Tickets/Vouchers Not Received - Provide Documentation or Issue Credit
164	Tickets/Vouchers unused and Lost or Stolen - Provide Documentation or Issue Credit
165	Tickets/Vouchers Lost or Stolen - Provide Documentation or Issue Credit
166	Requests Credit for Payment made directly to establishment,
167	Reservation Confirmed on Incorrect Date - Provide Documentation or Issue Credit
168	Reservation Confirmed in Incorrect Location - Provide Documentation or Issue Credit
169	Incorrect Conversion Rate Used - Provide Documentation or Issue Credit
170	Cancelled Reservation - Provide Documentation or Issue Credit
171	Assured Reservation Not Honored - Provide Documentation or Issue Credit
173	Requests Credit for Duplicate Billing
174	Customer Requests signed support and itemization for Charges
175	Customer Requests Credit for a Charge
176	Cardholder Does Not Recognize the referenced Charges
177	Cardholder Claims Charge Unauthorized
178	No Merchandise Ordered or Delivered - Provide Documentation or Issue Credit
179	Cardholder Does Not Recognize Charge for Reservation
180	Cardholder Does Not Recognize Charge for stay at Establishment.
181	No Knowledge of Referenced No Show Charge
182	Cardholder Question Charges for Damages at Establishment
183	Cardholder Does Not Recognize Charges from Establishment
184	Charges identified as Cash Advances - cannot be billed through AmEx
185	Purchased but refused Delivery - Provide Documentation or Issue Credit
186	Incorrect Merchandise - Issue Credit and provider Return Instructions
187	Requests Replacement for Incorrect Merchandise
188	Cardholder has no Knowledge of Charge, Requests Credit
189	No Subscription Issues Received - Provide Documentation or Issue Credit

continues on next page

Table 12 - continued from previous page

Code	Description
190	No Subscription Issues Received - Request to begin Delivery
191	Merchandise not Ordered or Received - Provide Documentation or Issue Credit
192	Customer Requests signed support and itemization for Charges
193	Charges Incurred at establishment are Fraudulent
194	Charges Incurred at establishment are Fraudulent - Full Magnetic Stripe data not received
195	Customer Doesn't Recognize charge and Requests signed support and itemization for Charges
196	Cardholder Does Not Recognize Charges, Provide Documentation or Issue Credit
197	Subscription Cancelled yet Billed - Provide Documentation or Issue Credit
198	Subscription Never Ordered - Provide Documentation or Issue Credit
199	Cardholder charged for both stay and no-show - Requests Credit for No-show
200	Sent Claim Report and Request signed support and itemization for Charges
608	Customer not disputing but requests signed support and itemization of charges
610	Charge was to be to Third Party - Provide Documentation or Issue Credit
620	Customer was under billed
656	No Knowledge of Referenced No-Show/Assured Reservation Charge
657	Requests Credit for Overcharge
658	Claims Received Multiple Billings in Error
671	Billing was to be Complimentary Stay
672	Customer Doesn't Recognize delayed charges - Provide Documentation or Issue Credit
673	Billed Assured Reservation and Actual Stay - Credit Due for Assured Reservation
674	Invalid or Incorrect Acct Number - Customer Doesn't Recognize Charge
675	CARDeposit Billing was to be Applied to the Stay - Provide Documentation or Issue Credit
676	Cancelled CARDeposit Reservation - Provide Documentation or Issue Credit
678	Second Request for Credit on Billing
679	Billed Twice for CARDeposit
680	Customer Claims Overcharge - Provide Documentation or Issue Credit
681	Guaranteed Reservation Cancelled within Guidelines - Provide Documentation or Issue Credit
682	Cancellation of Membership - Provide Documentation or Issue Credit
683	Charge Belongs to another Person due to AmEx cards being switched
684	Charge was Paid in Cash - Provide Documentation or Issue Credit
685	Customer Requests Copy of Signed Receipt
687	Does Not Recognize Charge, Provide Documentation or Issue Credit
688	Charge was to be Paid by Customer's Company - Credit and Rebill Correct Party
689	Reservation Made and paid by Third Party - Provide Documentation or Issue Credit
690	Not Disputing Charges but requesting support and itemization
691	Not Disputing Charges but requesting signed support and itemization
692	Customer should have been billed for only one night - Provide Documentation or Issue Credit
693	Customer Questions charge for Damages - Provide Documentation or Issue Credit
694	Dissatisfactory Accommodations, Requests Credit
695	Payment made directly to Establishment - Provide Documentation or Issue Credit
696	Car Rental Cancelled - Provide Documentation or Issue Credit
697	Claims Billed Twice for same Rental Vehicle - Provide Documentation or Issue Credit
698	Customer Requests support for Rental Charges

continues on next page

Table 12 – continued from previous page

Code	Description
699	Customer should have been billed for only one night – Provide Documentation or Issue Credit
700	Service Cancelled – Provide Documentation or Issue Credit
701	Customer Requests Cancellation of Service- Discontinue Future Billings
702	Customer Received Duplicate Credits
703	Repair/Replacement was to be covered under warranty – Provide Documentation or Issue Credit
704	Event Cancelled – Credit due for Tickets not used
705	Tickets Cancelled – Provide Documentation or Issue Credit
706	Customer Refused Delivery – Provide Documentation or Issue Credit
707	Call Associated with Bill had poor transmission quality
708	Call Associated with Bill was not completed/connected
712	Services Not Rendered
713	Duplicate Billing – Provide Documentation or Issue Credit
722	Customer Does Not Recognize Charge for Stay – Provide Documentation or Issue Credit
723	Payment made directly to Establishment – Provide Documentation or Issue Credit
730	Issue Credit for Charge and Discontinue all Future Billings
792	Customer has no Knowledge of charge – Credit and Discontinue Future Billings
800	Customer No Longer Disputes Charge (Positive Signal)
R040	Service/Membership Cancelled – Issue Credit and Discontinue Future Billings
R041	Customer Unable to contact and Cancel Service – Discontinue Future Billings
R042	Customer made Alternate Billing Arrangements – Provide Documentation or Issue Credit
R043	Customer Requests Cancellation of Service – Contact Customer Directly
R044	Customer Requests Cancellation Instructions/Authorization- Contact Directly
RM05	Cardholder does not agree to amount billed
RM21	Cardholder does not recognize
RM23	Cardholder Requests Copy
RM41	Require for Legal/Fraud Analysis
RM42	Required for chargeback
S06	Automatic Closure of Inquiry
V28	Cardholder Requests Copy w/ Signature
V29	Charge detail or rental agreement request
V30	Cardholder requests copy
V31	Required for chargeback
V32	Original lost in transit
V33	Required for legal/fraud analysis
V34	Repeat request for copy
V35	Written cardholder demand
V36	Legal process specifies original
V37	Previous copy illegible
V38	Required for paper/handwriting analysis
V39	Repeat request for original
V40	Required for arbitration
V78	Cardholder requests copy with signature
V79	Charge detail or rental agreement request
V80	Cardholder requests copy
V81	Required for chargeback
V82	Original lost in transit

continues on next page

Table 12 – continued from previous page

Code	Description
V83	Required for legal/fraud analysis
V84	Repeat request for copy
V85	Written cardholder demand
V86	Legal process specifies original
V87	Previous copy illegible
V88	Required for paper/handwriting analysis
V89	Repeat request for original
V90	Required for arbitration
6305	Cardholder does not agree with billed amount
6321	Cardholder does not recognize transaction
6322	Transaction Certificate (ICC Transaction)
6323	Transaction Information Document (TID) needed for cardholder's personal records expense reporting
6341	Fraud investigation
6342	Potential chargeback or compliance documentation
6343	Real-time Substantiation Audit Request (IIAS)

## 10.5 Construction principles of billing model

- *Overview*
- *Rates definition*
- *Commission accounting*
- *The hold and its carryover*
- *Rates validation*
- *Event model*
  - *Standard transaction types*
  - *Standard transaction statuses*
- *Rates table configuration*
- *Complex rates*

### 10.5.1 Overview

Starting from release 3.23.01 the revenue is distributed among all participants in hierarchical manner. It allows calculations to be more precise, to manage the hold payout parameters and to tune the rates model depending on the payment flow.

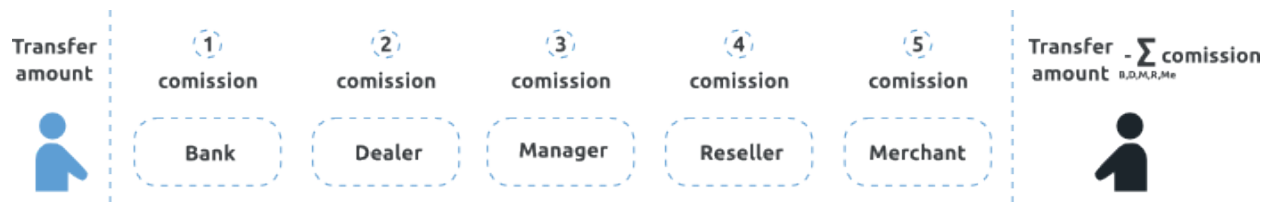
This kind of model allows to redefine the rates as well as the hold amount and its payout date.

The order of revenue distribution for the sale transactions



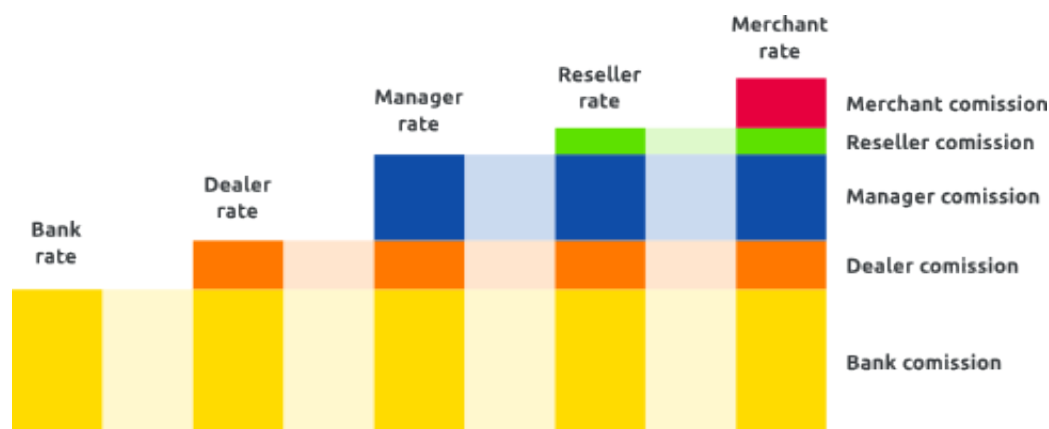
When an SMS or DMS transaction is processed all the participants withdraw their fee from the sale amount according to the rates defined. The rates applied from Bank to Merchant. Each participant in the flow can see only the rates defined for him without knowing the rates of preceding participants of the payment flow. For sale transactions the last participant is the Reseller and his rate will be the final one.

The order of revenue distribution for the transfer transactions



When the transfer transaction is being processed the rate calculation is the same, except for the additional participant - the money receiver. The last participant in this flow is the Merchant, and the receiver sees his rate as final

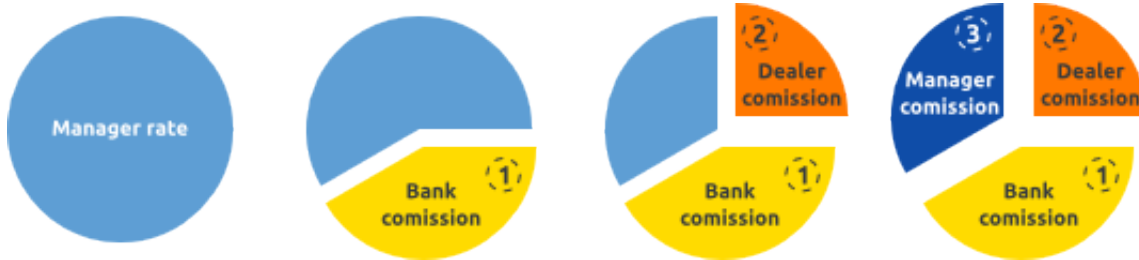
### 10.5.2 Rates definition



The rates are applied in increasing manner, each successive rates plan will adopt the preceding rate. Thus, the higher the user level the higher his rate is. The Bank's and Dealer's rates are defined at Gate level, for the others - Managers, Resellers and Merchants - at the

Project level. These rates can be overridden at the Endpoint level. There can be some missing participants in this flow.

### 10.5.3 Commission accounting



The first element on the diagram is the total commission accounted for the transaction. For the sake of simplicity we will examine sale transaction on the Project without Reseller. Thus the Merchant was deducted the commission defined in Manager's rate plan. In this case the commission calculation goes through the priority flow Bank → Dealer → Manager. That means that the Bank is the first to get its share according to the Bank's rate, then the Dealer's commission will be deducted and the Manager takes the rest.

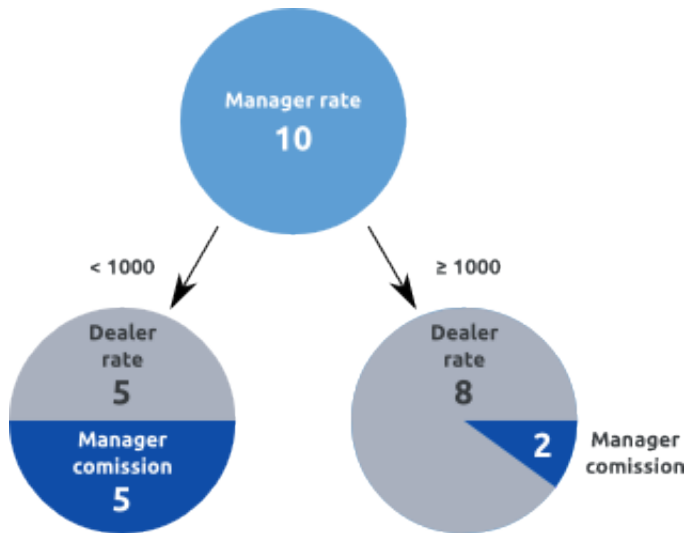
There is a probability that the commission would not match the expected one.

#### Example 1:

Let's see how the calculation of the commission would change depending on the ranges applied.

- The Dealer's rate plan is denied as follows: if the transaction amount is between 0 and 1000 USD, the Dealer's rate is 5 USD, if greater than 1000 USD - 8 USD;
- The Manager's rate is fixed: 10 USD;

Let's assume that the Manager didn't notice the ranges defined by the Dealer and expects the commission of 5 USD



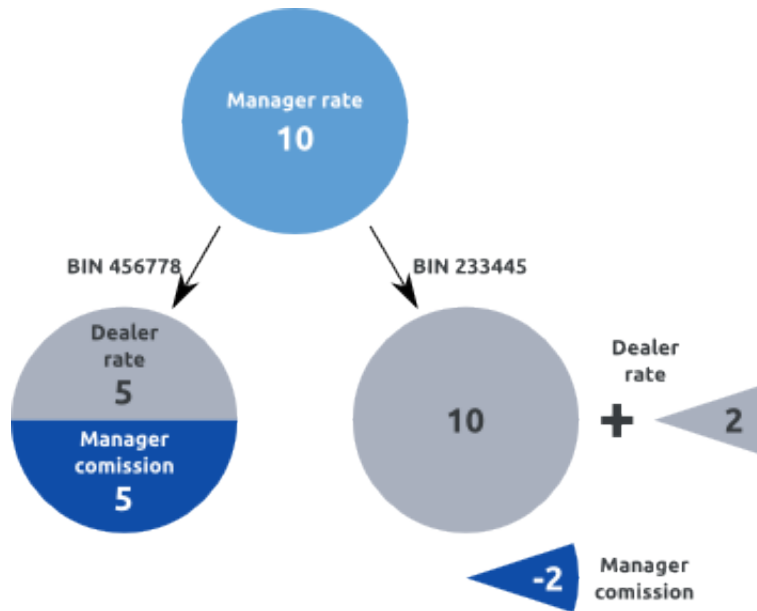
As you can see on the picture the Dealer's commission is calculated before Manager's and the actual Manager's commission will be lower the expected - 2 USD.

*Example 2:*

You should be much more careful with the rates defined for BIN, country or bank Let's assume that the Dealer's and Manager's ranges are the same.

- Dealer's rate: for all the transactions 5 USD, except for BIN 233445 which has the rate of 12 USD;
- Manager's rate: let's assume that the Manager's didn't take into account the Dealer's rate for the BIN and defined the fix rate of 10 USD.

Let's examine the transaction with the BIN 456778. The total commission will be distributed in the following way: 5 USD for the Dealer, 5 USD for the Manager; The transaction with the BIN 233445 makes 12 USD for the Dealer and the Manager's commission will be negative: -2 USD, because the total commission in the Manager's rate plan is 10 USD.

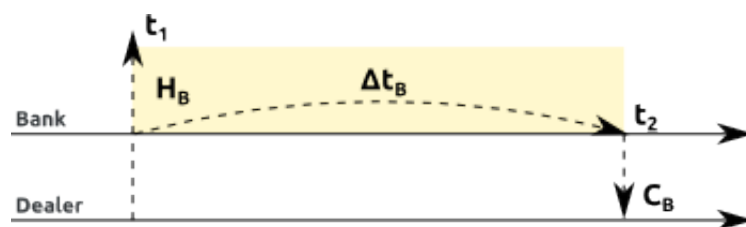


### 10.5.4 The hold and its carryover

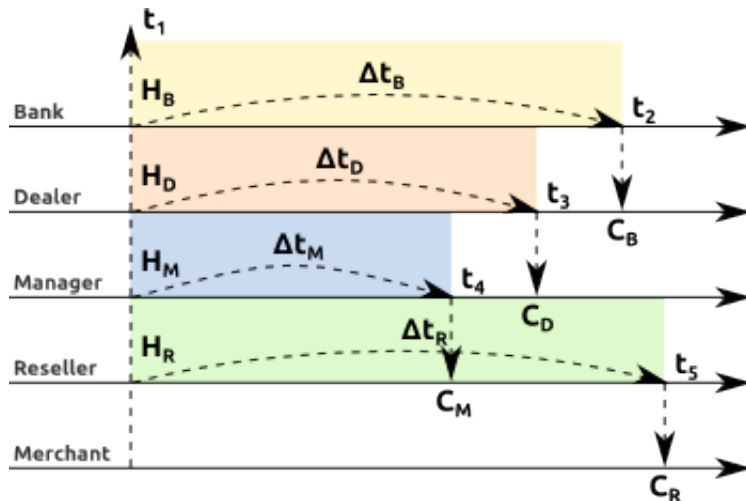
In order to insure the risks carried by the Merchant it is possible to define the hold for particular Merchants. The payout management system provides the accounting of frozen holds and the amount of holds that are due to be paid back to the Merchant. The hold covers the risks related to chargebacks initiated by unhappy customers in case the contract with the Merchant was canceled. The carryover operation is accomplished during no more than 182 calendar days. The payment period as well as the hold percentage is defined in the rates.

The algorithm of the hold calculation and carryover

Every participant of the payment flow, except for the Merchant, can define his own the hold percentage and the hold period. The hold percentage and hold period do not depend on each other.



According to the figure, for the transaction  $t_1$  the Bank withdraws from the value of  $H_B$  from the total commission, for the period of  $\Delta t_B$ , defined in the Bank's rate. Thus the Bank holds the amount of  $H_B$  for the period  $[t_1, t_2]$  on its account to cover the risks of chargeback and fraud operations. After  $\Delta t_B$  period has expired, in case there were no negative transactions the Bank pays out the hold back to the Dealer. This process  $C_B$  is known as carryover. The same flow is applied to any participant of the payment flow.



The total earnings of any participant is: commission + hold of the participant - hold of preceding participant.

- For the Bank: in the moment  $t_1$  for the period  $\Delta t_B$  the earnings will be topped up by the amount of the hold  $H_B$ , in the moment  $t_2$  will be deducted the same amount;
- For the Dealer: in the moment  $t_1$  for the period  $\Delta t_D$  the earnings will be topped up by the amount of the hold  $H_D$ , in the moment  $t_3$  will be deducted the same amount, in the moment  $t_2$  the Dealer's earnings are topped up by the amount of the carryover  $C_B$  paid back by the Bank
- For the Manager: in the moment  $t_1$  for the period  $\Delta t_M$  the earnings will be topped up by the amount of the hold  $H_M$ , in the moment  $t_4$  will be deducted the same amount, in the moment  $t_3$  the Manager's earnings are topped up by the amount of the carryover  $C_D$  paid back by the Dealer
- For the Reseller: in the moment  $t_1$  for the period  $\Delta t_R$  the earnings will be topped up by the amount of the hold  $H_R$ , in the moment  $t_5$  will be deducted the same amount, in the moment  $t_4$  the Reseller's earnings are topped up by the amount of the carryover  $C_M$  paid back by the Manager
- For the Merchant: the Merchant cannot define the hold values, in the moment  $t_1$  for the period  $\Delta t_R$  the earnings will be deducted the amount of the hold  $H_R$ , in the moment  $t_5$  will be topped up by the same amount

If you define the hold parameters in the correct way the hold percentage of the payment flow participant is not less than the hold percentage of the preceding participant. Otherwise it leads to financial risks. The same is true for the hold period parameter.

### 10.5.5 Rates validation

Starting from the release 3.23.0 you can define negative rates. It is not possible to validate the rate plans at the time of creation and the validation is carried out at the time of transaction processing. If the negative rates were defined deliberately you should turn off the validation in the Project settings. This will switch off the validation for all the rates defined for the Project.

### 10.5.6 Event model

Doc4.0 uses event model to apply the rates. The Processors generate various events. The rates are applied to those events according to the rate plans. Doc4.0 associate the event with the transaction in the system whether it's sale transaction or an external fraud system call. The transaction is the minimal unit of tariffing. The transaction has type and status.

#### Standard transaction types

Transaction	Description
sale	withdraws the amount from the client's account
preauth	holds the amount on the client's account but doesn't withdraw
capture	captures the amount from the client's account, can be only issued after the respective preauth
cancel	cancels the preauth transaction, if it has not been captured by capture operation
reversal	returns the amount back to the client's account
chargeback	the request to charge back the amount initiated by the cardholders via the issuing bank
dispute	to contest the chargeback operation, confirms the double withdrawal
fraud	the operation marks the transaction as fraudulent
refund	the operation to debit the client's account directly
transfer	the money transfer operation, transfer the money between the cards or from the Merchant's account

#### Standard transaction statuses

Transaction	Description
approved	the transaction is approved by the Bank or PSP
decline	the transaction is declined by the Bank or PSP
filtered	the transaction is filtered out by the system before it reached the Bank or PSP

The current model allows the following combinations of types and statuses:

- APPROVED: all transaction types ;
- DECLINED: sale, preauth, transfer;
- FILTERED: sale, preauth, transfer, reversal;

To apply the rates to an event you should define the following parameters:

- Minimum (min)
- Percentage (rate)
- Fixed(absolute) rate (abs)

- Hold percentage (hold)
- Hold period
- User defined function

The rate is calculated in the following way:

- the maximum of the defined minimum and percentage multiplied by the transaction amount is first calculated:  $\text{greatest}(\text{min}, \text{amount} \times \text{rate})$
- to the calculated value the fixed rate is added:  $\text{greatest}(\text{min}, \text{amount} \times \text{rate}) + \text{abs}$
- the hold is being withdrawn:  $\text{greatest}(\text{min}, \text{amount} \times \text{rate}) + \text{abs} + \text{hold}$
- the User defined function gets applied. The function can redefine the calculation
- the transaction amount is deducted by the calculated amount

When you define rates for the BIN, bank or country you should set the following parameters:

- Minimum (min)
- Percentage (rate)
- Fixed(absolute) rate (abs)
- User defined function

You are not allowed to redefine the hold parameters. For the redefined events the following priority search will be applied: first the BIN redefined rate is being found, if it's not found, the system looks for bank redefined rate, if it's not found the country redefined rate is being searched. If none are redefined the default rate is applied.

### **10.5.7 Rates table configuration**

To get the better flexibility to define the rates you can use rate table definition user interface. For the types of transactions that initiate the orders, except for the transfer, the single level range rates table is supported. The range can be defined for: transaction amount, total amount and total number of the transactions processed by the Gate for the current month.

For the transactions that do not initiate orders you can define the following ranges: the ratio of the current number of transactions of this type to the total number of the transactions for the current or past month.

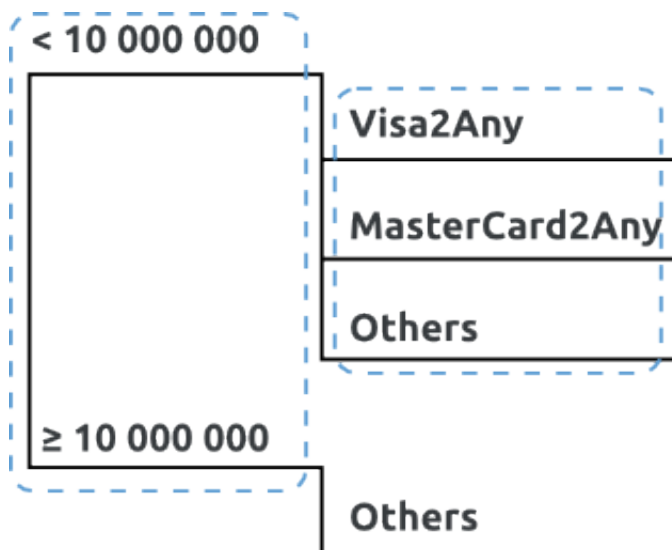
For transfer transactions you can define two levels of ranges in the rates table. The first level ranges are the same as for the transaction that initiate orders. The second level is the transfer direction. The transfer directions are defined at the Doc4.0 instance level. The standard directions are: from Visa card to any other card, from MasterCard card to any other card, the transfer within the bank and a lot of others. To select the desired directions, please, create an enhancement request.



The calculation of the aggregated amounts (total amount, total number and ratio) is accomplished by default at the Gate level. In order to insure the rates transparency you should select the calculation of the aggregated amounts at the Endpoint or Project level.

Let's examine the rates table configuration for the transfer transactions

Let's assume that the Gate supports transfers for various types of cards. The rate of the transfer depends on the total amount of the transactions processed by the Gate. The limit is set to 10 000 000. You can define different rates depending on the transfer direction. If the total amount is less than 10 000 000 the rates for the following directions are applied: Visa2Any, MasterCard2Any, Any2Any, otherwise the common rate is set. In this case we have the following hierarchy:



Let's examine the flow of a transaction made with the card 4444 5555 6666 1111. Since the first level ranges are defined for the total transactions amount first the total amount of the transactions processed by the Gate is examined at the time of transaction processing. Assume that the total amount is 5 000 000, that means the flow goes via the upper branch. Next, the range for the card type is defined, the card being processed is Visa. For Visa cards there's a

transfer direction Visa2Any. It means the system will pick the rate in the table: < 10 000 000, Visa2Any.

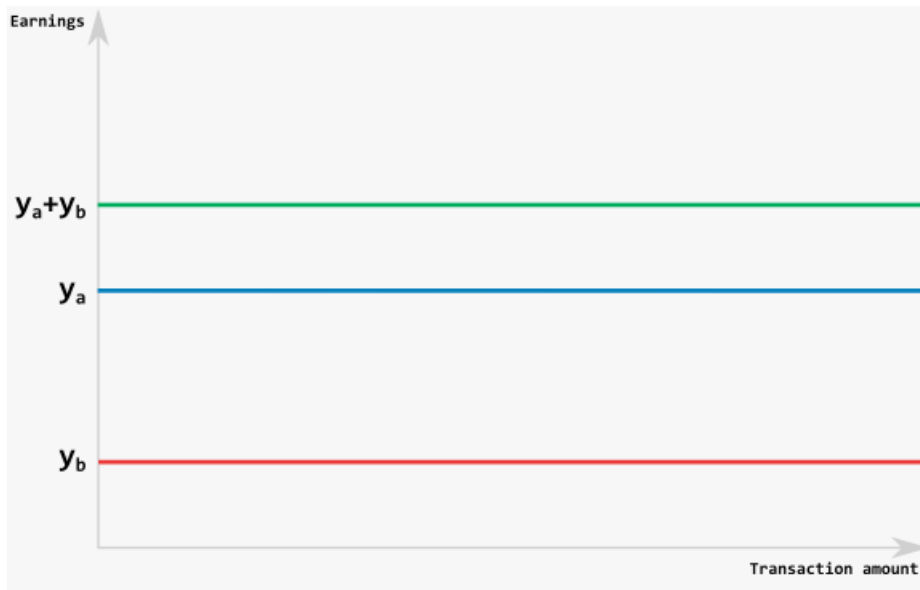


It might happen the the card will fall into several directions at the same time. In this case the direction is selected in the following priority: the transfer within a bank, then the direction where both sender and receiver are defined (e.g. Visa2Visa), then the direction where only the sender is defined (e.g. Visa2Any), the direction where only the receiver is defined(e.g. Any2Visa), default direction.

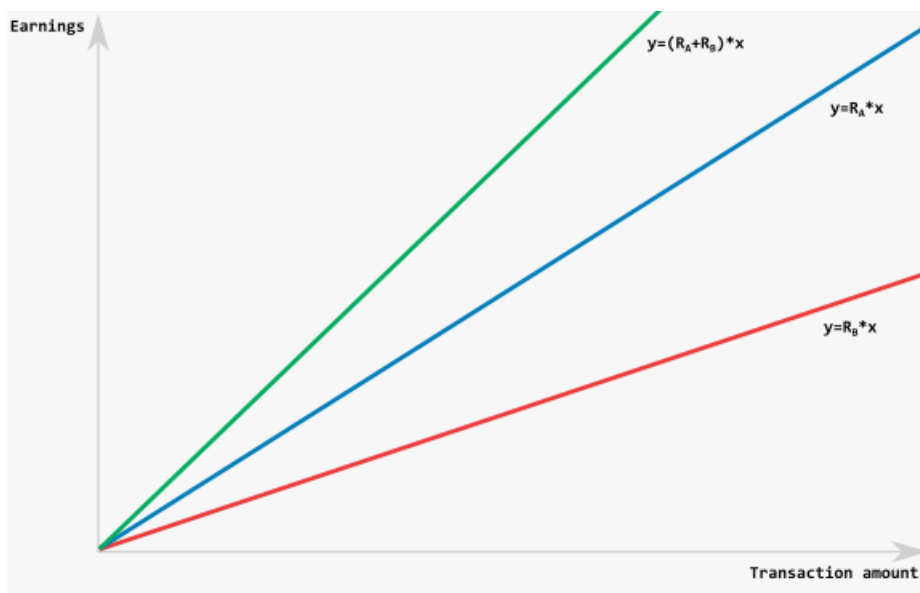
You are allowed to define the ranges for directions as the first level of hierarchy. In this case when you define the rates table, the amount and number of the transactions will be calculated for all directions separately.

### **10.5.8 Complex rates**

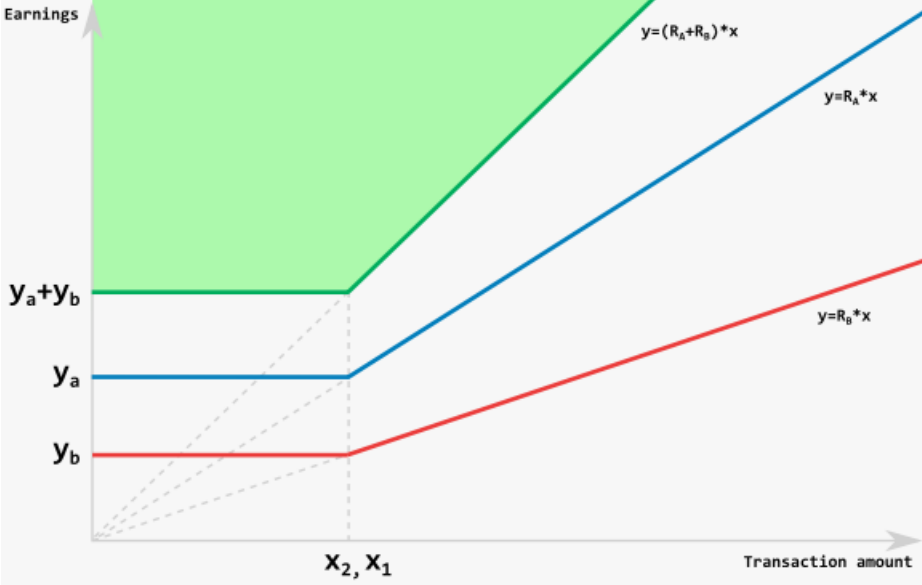
To define the rate plan correctly you have to understand how you can make it for different participants of the payment flow. Let's first examine simple cases. Let's say the commission of the participants A and B is defined solely by the minimal value and doesn't depend on transaction amount. The participant A expects the earnings  $y_a$ , the participant B -  $y_b$ . In such a case you have to define the rate plan with the minimal rate of  $y_a+y_b$ .



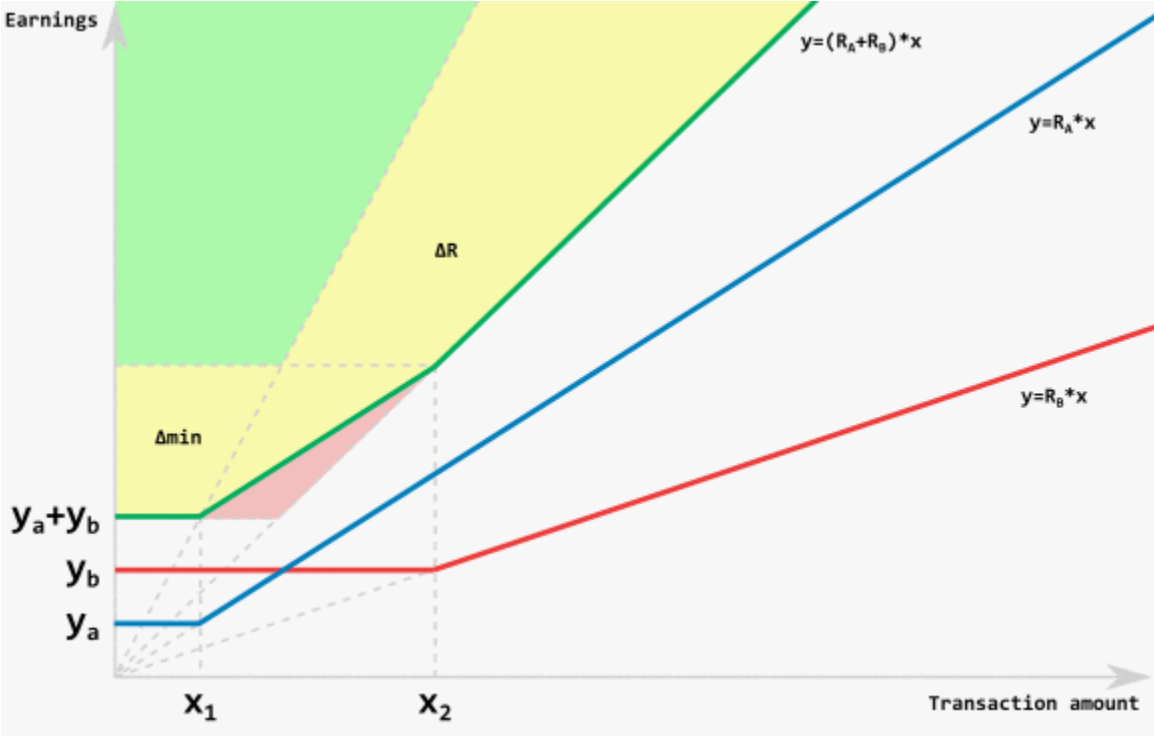
The same logic is applied for the rates with defined percentage rate only. Let's assume the commission of the participants A and B is only defined as a percentage of the transaction amount. The participant A expects the commission  $R_a$ , the participant B -  $R_b$ . In such a case you have to define the rate plan with the commission set to  $R_a + R_b$ .

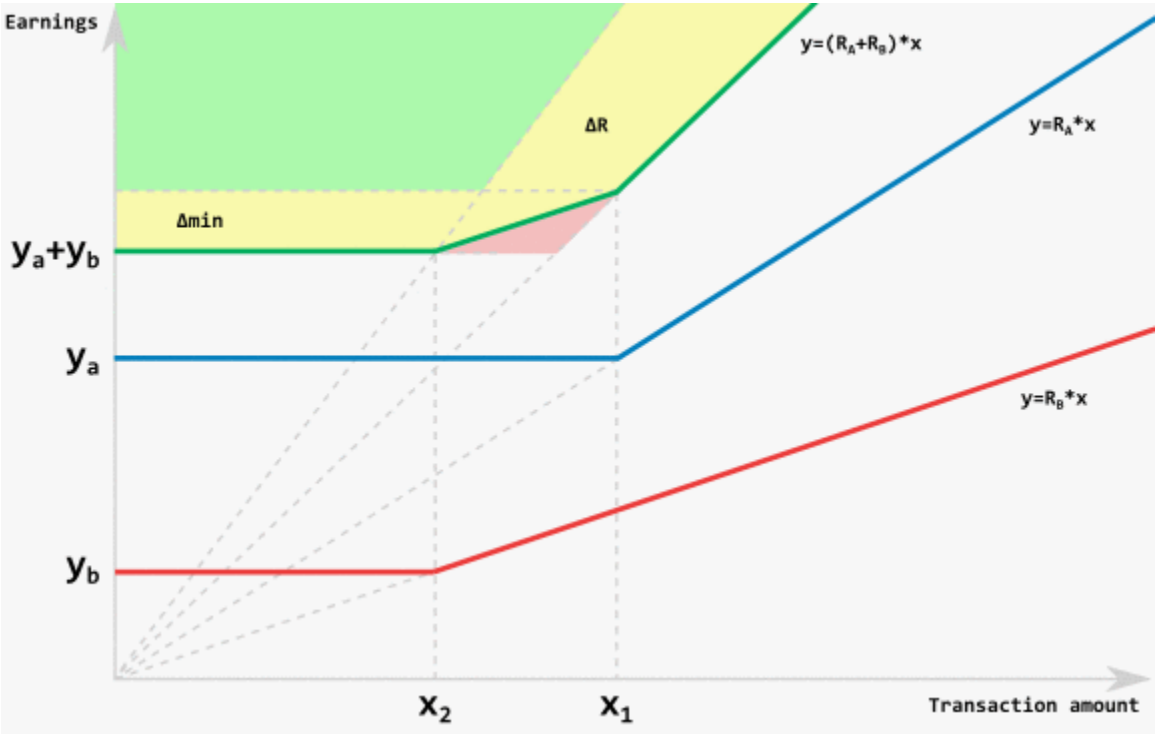
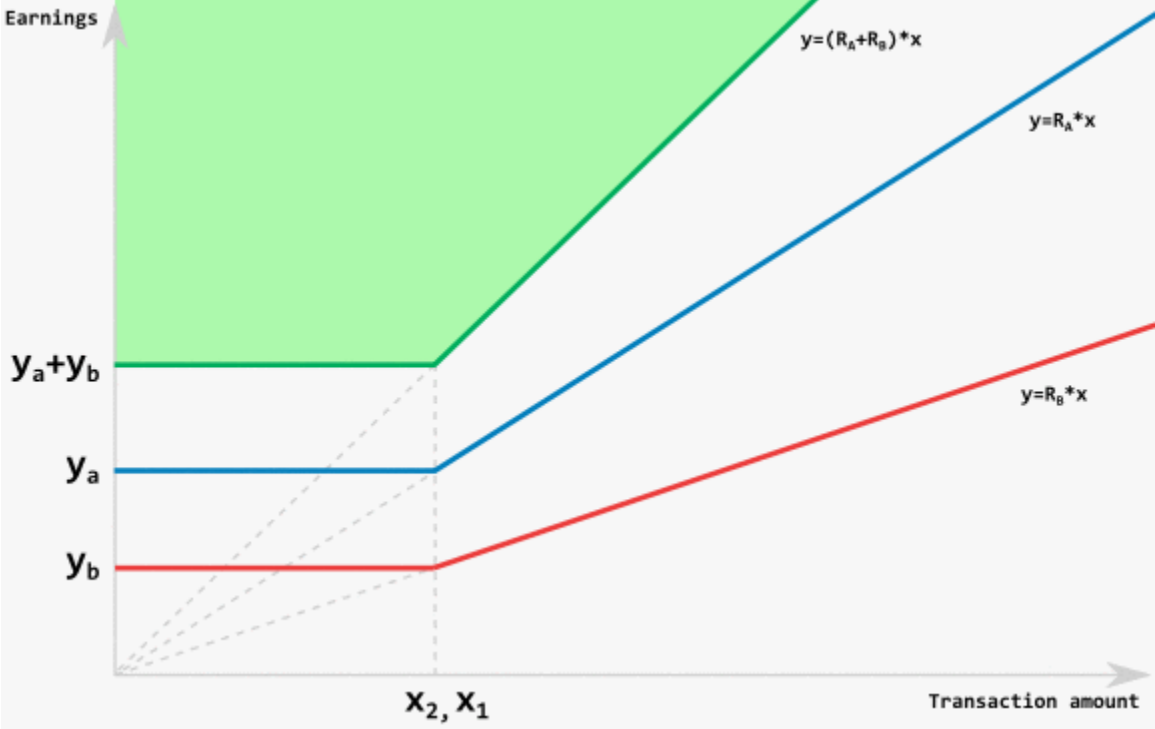


Let's examine a more complex case. Assume that both participants expect the commission as a minimal value for transactions less than certain amount and the percentage of the transaction otherwise. The threshold to switch from the minimal rate to percentage rate for the participant A is  $x_1$ , for the participant B -  $x_2$ . If this threshold is the same for both participants ( $x_1 = x_2$ ), then the applied rate will be the sum of the minimal rates below the threshold and the sum of the percentage amounts above it.



If the parameters are different the rate is calculated in a more complex way. Let's visualize the possible cases.





On the figure the minimal possible rate is marked green. In the range  $(x_1, x_2)$  the rate is defined by another formula than just the sum of two minimal rates and the sum of the percentage rates. It's not possible to correctly define such a rate in a precise manner. You have to add the two ranges:  $x_1, x_2$ . In  $(0, x_2]$  the rate is defined as a sum of minimal commissions. In  $[x_1, x_2]$  the rate is defined as a percentage rate of the participant A (or the

participant B if his threshold triggers first) and the absolute value of the participant B's commission which is equal to the minimal commission of the participant B (or A vice versa). In  $[x_2, +\infty)$  the rate is defined as the sum of the percentage rates of the both participants.

In order to avoid too complex rates tables you have to adjust the minimal rate value as well as the percentage. If you increase the minimal rate in the range  $\Delta_{min}$  you have to increase the percentage rate  $\Delta R$  as well. If you adjust the minimal rate value by more than  $\Delta_{min}$  amount you should not adjust the percentage rates. The adjustment bounds are marked with dotted line.

If you ignore these adjustments for the transactions amounts that fall into  $(x_1, x_2)$ , the commission for the participant B will be lowered (assume that B is lower in the payment flow hierarchy).

## **11.1 Payment Cashier Configuration**

- [Introduction](#)
- [Parallel Form Master Endpoint Settings](#)
- [Payment Page Display Logic](#)

### **11.1.1 Introduction**

Payment Cashier integration requires a configured Master Endpoint to display Cashier Form (also called Parallel Form) and configured Auxiliary Endpoints for each payment method to be displayed on the Parallel Form. The Manager can configure on Master Endpoint which transaction type (sale, preauth) will be initiated for each payment method and for which list of countries this payment method will be displayed. There can be several payment methods, such as Credit Card, Bank Transfer, etc. on the same Parallel Form available for the Payer to choose from.

### **11.1.2 Parallel Form Master Endpoint Settings**

There is an instruction for Project configuration to use Parallel Form:

1. To configure Parallel Form that includes payment methods in different currencies, at least one Project for each currency should be created. For example, if payments in USD, EUR and JPY are to be processed, 3 different Projects must be created accordingly.
2. After Projects were created, all required Endpoints for provided payment methods have to be created and connected to appropriate Projects. All these Endpoints will be auxiliary to Master Endpoint and called Auxiliary Endpoints.
3. To create Master Endpoint, go to (Settings -> Configuration -> Master Endpoints -> + Master Endpoint).
4. Auxiliary Endpoints, which represent payment methods, must be connected to the Master Endpoint to be displayed on the Parallel Form. This can be done in Master Endpoint settings. To add new Auxiliary Endpoint, press the Add button. The form with three following fields

should be filled: “Endpoint”, “Payment method” and “Payment method reference name”. In the “Endpoint” field one of the available Endpoints should be chosen. The “Payment method” field defines the name of the payment method shown on the relevant Parallel Form tab. “Payment method reference name” field defines the internal reference name of this payment method, which can be used for customization of this payment method display style in Parallel Form template.

5. After the Auxiliary Endpoint is added, the Manager may also select which transaction type will be initiated (sale, preauth) and set the list of countries where this payment method will be available. To select the list of countries, press the three-points button that stays opposite of the Auxiliary Endpoint field.

6. To change the default Parallel Form template, go to the Master Endpoint (Master endpoint details screen -> Common -> Edit -> Payment form template). To change the default payment form template for particular payment method, go to the respective Auxiliary Endpoint details screen and set the corresponding Payment form template. Such form template returning algorithm is used for all kinds of form templates: payment, waiting and finish templates. See Payment Page Display Logic in the next section for details.

**Note**

It is also possible to set the payment form template in the Project settings (Project details screen -> Common -> Edit -> Payment form template). When the request is sent to Master Endpoint without a specified Parallel Form template, Master Endpoint inherit Parallel Form template from the Project settings. This option is not recommended, because usually both Master Endpoint and Auxiliary Endpoints are connected to the same Project and this way all Endpoints will inherit the same form template.

Below is an example of configured Master Endpoint with multiple available payment methods represented by Auxiliary Endpoints connected to it:

The screenshot shows a configuration page for a Master endpoint. At the top, it displays 'Master endpoint 13497 master endpoint' and navigation buttons: 'To Master-endpoints list', 'To details', and 'Edit'. Below this is a table with the following columns: Auxiliary Endpoint name, Tab name, Method ref. name, Tx type, Country list, and Default tab.

Auxiliary Endpoint name	Tab name	Method ref. name	Tx type	Country list	Default tab
<input type="checkbox"/> test en	Card	CREDIT_CARD	sale	-	✓
<input type="checkbox"/> test en	Withdrawal	WITHDRAWAL	sale	-	-

To the right of the table is a 'Common' tab, which is currently selected.

Below is an example of a successful transaction via the Master Endpoint. When Payer opened the Parallel Form, master transaction initiated an auxiliary transaction for the payment method selected on the form. Once the auxiliary transaction received final successful status, it triggered final successful status on the master transaction:

The screenshot displays the Doc4.0 Manager interface with the following sections:

- Order details:**
  - Creation time: 17-11-2023 10:56:22.000
  - Merchant order ID: 123
  - Order ID: 1912963
  - External Order ID:
  - Order description: 123
  - Request source:
  - Fraud Score:
  - Merchant URL:
  - Merchant: Demo merchant A
  - End Point: Demo Master EUR
  - Project: Demo Ams EUR
- Customer details:**
  - Payment System:
  - IP-address: 85.132.52.250
  - Billing address: Rus\*\*\*ZE
  - E-mail: j\*\*\*x@gmail.com
  - E-mail domain: gmail.com
  - First name: Demo
  - Last name: test
  - Phone: +7\*\*\*54826
  - Customer DNA: 01D642EB5AD36EF057C3DCA0D97F65...
  - Customer ID: 4
  - Customer level: unknown
  - Create CMS customer (requests for personal data will be logged)
- Transactions:**

Date / Bank / Settle	Transaction	Details
-	sale	Amount: - Gate: [-] External Order ID: [-]
-		Commission: - MID: - External Method: -
-		Hold: -
- Auxiliary orders:**

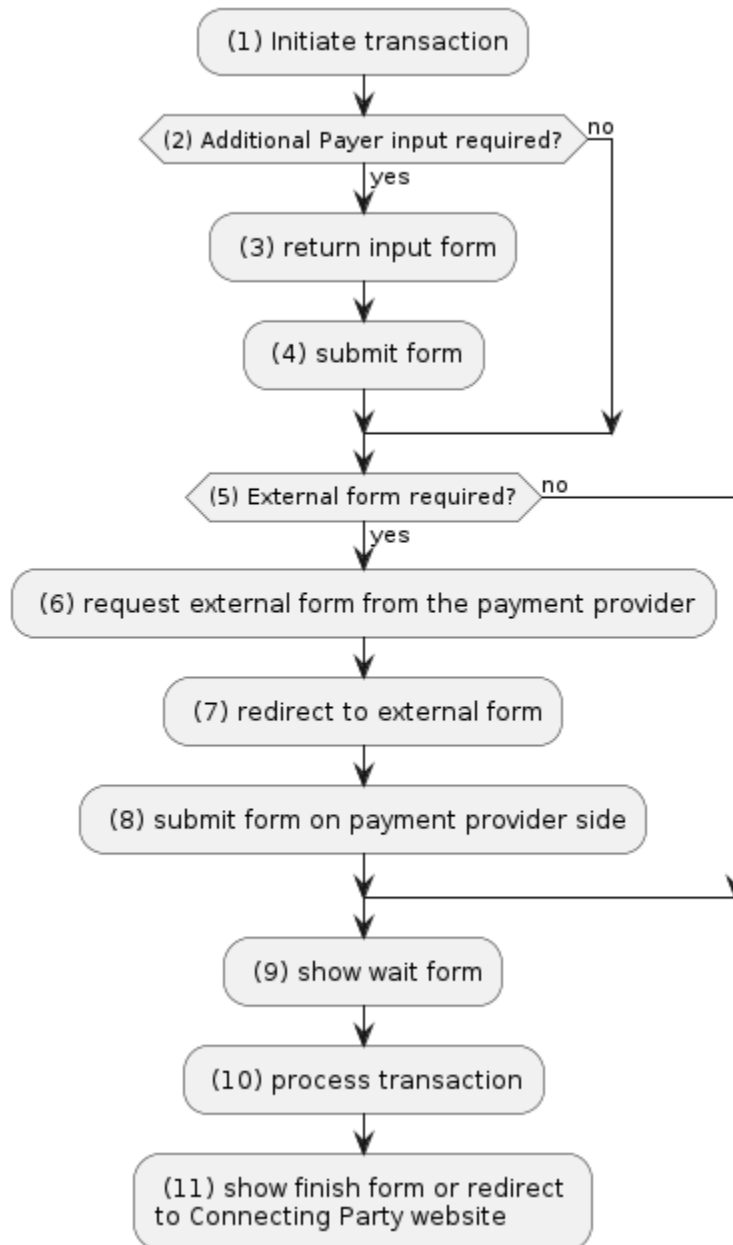
Date	Bank	Transaction ID	Amount	Status	Method
2023-11-17 10:56:56	VISA	1912964	55.00 EUR	✓	preauth

### 11.1.3 Payment Page Display Logic

Payment Cashier transactions can be initiated with API requests or via Virtual Terminal on UI. When Connecting Party (merchant or payment facilitator which represents merchant) sends a request to Master Endpoint, the Doc4.0 system returns Parallel Form URL, HTML content of which is defined on the Master Endpoint level. When payment method is selected on Parallel Form, Doc4.0 system returns HTML content of this payment method form template specified on the respective Auxiliary Endpoint level (or displays external payment form instead).

Each payment method has its own payment page display logic. Payment Cashier might have multiple transactions initiated within the same payment session, because it can have multiple payment methods available for the Payer. When Payer selects payment tab appropriate auxiliary transaction is initiated.

(1) Transactions can be initiated with API requests, batch upload or via Virtual terminal on UI. Each payment method has its own payment page display logic.



**Note**

Payment Cashier might have multiple transactions initiated within the same payment session, because it can have multiple payment methods available for the Payer. When Payer selects payment tab, respective auxiliary transaction is initiated.

(3) For credit card payment method form is displayed on Payment Gateway side and can be customized. See Payment Page Customization. Some other payment methods may have additional forms on Payment Gateway side. Contact support for details.

(7) Some payment methods require the Payer to be redirected to their own form. That form is not hosted by Payment Gateway and can't be customized.

(9) Until transaction reaches final status, Payment Gateway displays Wait Form for the Payer.

(11) After the transaction reaches the final status, Payment Gateway displays Finish Form for the Payer or Redirect to Connecting Party website.

**Note**

For all templates and macros for customization see [Forms Customization](#)<sup>26</sup>

---

<sup>26</sup> [https://doc4.codetime.net/integration/reference/forms\\_customization.html](https://doc4.codetime.net/integration/reference/forms_customization.html)