Risk Monitoring

Contents

Introduction

In WAY4™, transactions can be monitored online and offline according to specially configured parameters. The WAY4 Real-Time Risk Management module calculates transaction risk levels and then registers suspicious transactions in a special log. With online monitoring, suspicious operations can be declined automatically during authorisation.

This document is intended for issuer and/or acquirer security officers responsible for card transaction monitoring.

While working with this document, it is recommended that users refer to the following reference material from OpenWay's documentation series:

- Documents
- WAY4™ Dictionaries
- WAY4™ Service Packages
- Usage Limiters
- Preferred Counterparties
- Importing Configurations Using the Configuration Inspector Module

The following conventions are used throughout this document:

- Field labels in screen forms are typed in *italics*.
- Button labels used in screen forms are placed in square brackets, such as [Approve].
- Menu selection sequences are shown with the use of arrows, such as Issuing → Contracts Input & Update.
- Key combinations used while working with WAY4 Remote Access are shown in angular brackets such as <Ctrl>+<F3>.
- Warnings of possible erroneous actions are marked with the ⚠ sign.
- Messages marked with the ⓘ sign contain information about important features, additional facilities, or the optimal use of certain functions of the system.

Chapter 1. General Monitoring Principles

Transaction risk rules are specified by usage limiters set up in special Service Packages used to monitor risks (see "Configuring and Using Risk Rules"), called Risk Packages. These Service Packages are additional Service Packages; they are added to Service Packages used to configure Products and register contracts (see the section "Configuring Additional Service Packages" in the document "WAY4™ Service Packages").

Each operation registered in the system is checked against risk rules, which can be specified both on the level of the Service Package used by a group of contracts and individually for a specific contract. This makes risk rule setup in the module more flexible. The module also allows users to use both standard payment system parameters and their own customised parameters to configure risk rules. With the module, users can monitor suspicious transactions according to the transaction activity history of a specific contract (card, device, etc.).

Risk rules specified by usage limiters can have threshold values for the amount and/or number of transactions; if a transaction exceeds the threshold value, it is considered suspicious.

These limiters are analysed during authorisation and in certain cases considered during financial document processing.

Limiters specifying transaction risk rules are analysed offline during financial document processing in the following cases:

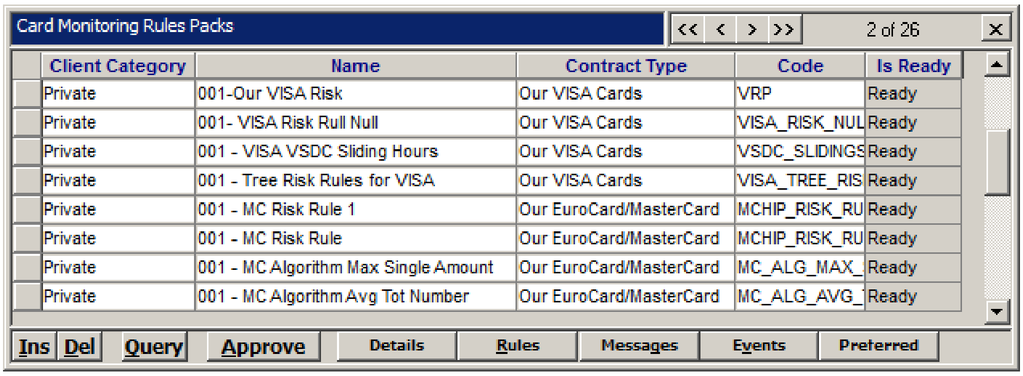
- If the *Fee Algorithm* field of a transaction subtype (see section "Transaction Types and Their Properties" in the Documents Administrator Manual) contains the tag "USAGE_FOR=<code>;", where code = T (Target), S (Source), or B (Both).
- If no authorisation document is found (response code "Chain Not Found") for a financial document processed by the issuer and the transaction type requires authorisation (field *Is Autorized* contains values "Always" or "May be").

ℹ Note that to work with WAY4 Real-Time Risk Management, the RM_USG_CHCK_MODE global parameter must be set to a non-empty value, e.g. "USG". The default parameter value is "CSA", meaning that the module is not used.

Chapter 2. Configuring and Using Risk Rules

Registering Risk Packages

To register Service Packages for risk monitoring, called Risk Packages, select the user menu items "Risk Management Issuing → Configuration → Account Monitoring Rules Packages" and "Risk Management Issuing → Configuration → Card Monitoring Rules Packages" for the issuing module or "Risk Management Acquiring → Configuration → Account Monitoring Rules Packages" and "Risk Management Issuing → Configuration → Device Monitoring Rules Packages" for the acquiring module. These menu items open the "<…> Monitoring Rules Pack" grid form (see Fig. 1) will be displayed.



Client Category	Name	Contract Type	Code	Is Ready
Private	001-Our VISA Risk	Our VISA Cards	VRP	Ready
Private	001- VISA Risk Rull Null	Our VISA Cards	VISA_RISK_NUL	Ready
Private	001 - VISA VSDC Sliding Hours	Our VISA Cards	VSDC_SLIDINGS	Ready
Private	001 - Tree Risk Rules for VISA	Our VISA Cards	VISA_TREE_RIS	Ready
Private	001 - MC Risk Rule 1	Our EuroCard/MasterCard	MCHIP_RISK_RU	Ready
Private	001 - MC Risk Rule	Our EuroCard/MasterCard	MCHIP_RISK_RU	Ready
Private	001 - MC Algorithm Max Single Amount	Our EuroCard/MasterCard	MC_ALG_MAX_	Ready
Private	001 - MC Algorithm Avg Tot Number	Our EuroCard/MasterCard	MC_ALG_AVG_	Ready

Fig. 1. Form for registering Risk Packages

This form is used to register Risk Packages by contract type and client category.

The [Approve] button in the form is used to activate Risk Packages (see the section "Approving Service Packages" in the document "WAY4™ Service Packages").

ⓘ Note that limiters set up for a Risk Package will be used as transaction risk rules starting with the date specified during activation of the main Service Package to which the current Risk Package is added.

The [Details] button is used to display a form with Service Package additional parameters (see the section "Additional Parameters of Service Packages" in the document "WAY4™ Service Packages").

The [Rules] button is used to set up Service Package usage limiters used to specify transaction risk rules (see "Configuring Risk Rules").

The [Messages] button opens the grid form containing messages generated by the system during activation of a Service Package, including all error messages.

The [Events] button is used to set up Events that will open for contracts that have violated a risk rule specified by a limiter (see the document "Events").

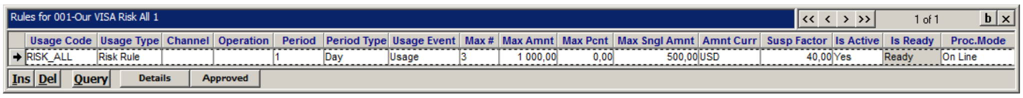
The [Preferred] button is used to set up preferred counterparties (see the document "Preferred Counterparties").

Configuring Risk Rules

Usage limiters are used to create risk rules.

To set up risk rules, click the [Rules] button for the desired Package in the Risk Package grid form (see "Registering ").

This will open the grid form "Rules for <name of Risk Package>" (see Fig. 2) for setting up risk rules.



Rules for 001-Our VISA Risk All 1

Usage Code	Usage Type	Channel	Operation	Period	Period Type	Usage Event	Max #	Max Amnt	Max Pcnt	Max Sngl Amnt	Amnt Curr	Susp Factor	Is Active	Is Ready	Proc.Mode
RISK_ALL	Risk Rule			1	Day	Usage	3	1 000,00	0,00	500,00	USD	40,00	Yes	Ready	On Line

Fig. 2. Configuring risk rules

When usage limiters are used as risk rules, transactions meeting the usage criteria increase its counter value, and those exceeding the limit are considered suspicious.

For information on usage limiter setup and use, see the document "Usage Limiters".

A limiter type is determined by the *Usage Type* field value. Generally, limiters of any type may be used as risk rules, while limiters of the "Risk rule" type are only used in the risk monitoring module. A limiter is used to limit the number and amount of transactions for a contract. Limits are applied to all transaction types ("Transaction", "Balance Inquiry", etc., see the description of the "Service Class" transaction type classifier in the document "Documents").

Risk rules set by limiters are normally analysed when processing authorisation requests for open contracts only. Limiters with the value "Negative RC" in the *Usage Type* field are an exception. For these limiters all authorisation requests are analysed regardless of a contract's status, including for closed contracts. However, complete analysis of authorisations for a closed contract using this contract's Risk Package is not possible. Therefore, when closing a contract, a Risk Package containing such a limiter should be detached so limiters are not analysed for this contract. If risk rules must be analysed for closed contracts, these limiters should be configured in the Risk Packages of the higher-ranking account contract or the Liability contract of the financial institution.

The value specified in the *Proc.Mode* field determines whether the corresponding criterion (limiter) will be processed at the time of authorisation ("On Line") or if limiter processing will be deferred ("Off Line").

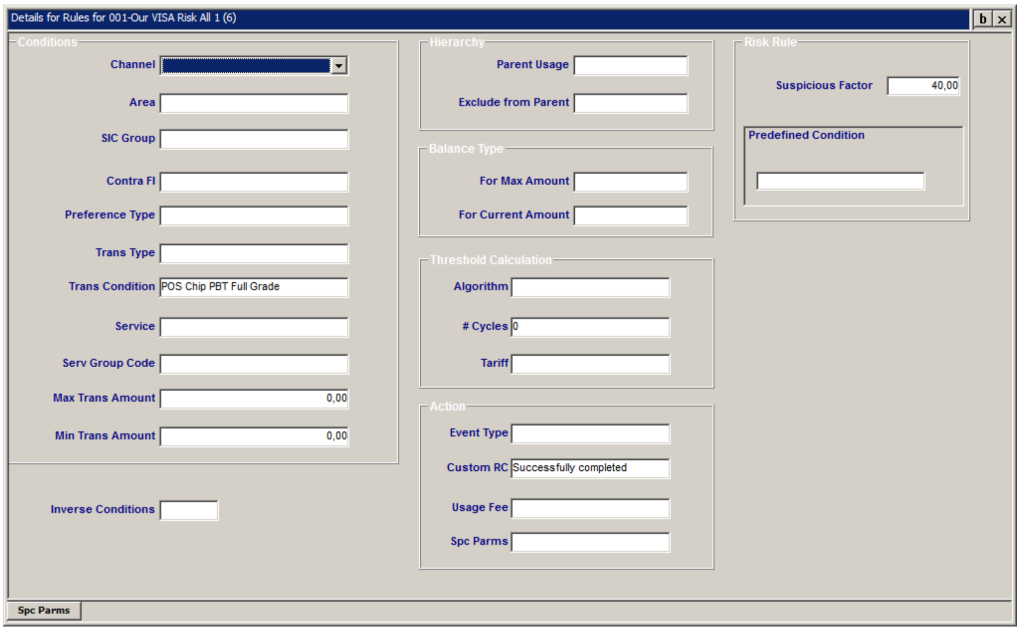
⚠ Note that deferred processing is only possible for limiters that do not cause authorisation to be declined. These limiters may have the "Charge", "Event Only" or "Response" value in the *Usage Event* field, and the *Custom RC* field, available after clicking the [Details] button in the "Rules for <name of Risk Package>" form, must contain the code of a positive response, for example, "Successfully completed".

When a limiter hierarchy is used, the parent and child limiter's *Proc.Mode* field values must match.

For more information about deferred processing of limiters, see the section "Deferred Processing of Limiters".

The [Approved] button opens a form containing records corresponding to all limiter template parameter changes that have ever been approved. Each time a limiter template's changed parameters are approved (this happens when approving the corresponding Service Package) a new record is shown in this form that contains the template parameters and date from which the approved parameters are effective (*Date From*). The previous approved record is "closed" – a value is specified for it in the *Date To* field (expiry date of the template's changed parameters) that is the same as the date the new parameters become effective. This form is used to determine which template parameters were used at a particular point in time.

The [Details] button in the "Rules for <name of Service Package>" grid form is used to open the form for entering additional limiter parameters (see Fig. 3).



Details for Rules for 001-Our VISA Risk All 1 (6)

Trans Condition: POS Chip PBT Full Grade

Max Trans Amount: 0,00

Min Trans Amount: 0,00

Cycles: 0

Custom RC: Successfully completed

Suspicious Factor: 40,00

Fig. 3. Limiter details

Most fields in this form are described in the section "Additional Parameters of Limiters (Details))" section of the "Usage Limiters" document.

The fields of the *Risk Rule* group are only used in the risk monitoring module:

- *Suspicious Factor* – factor used to assess transaction risk degree (see "Analysing Suspicious Transactions"); if the field value is >0, the transaction will be registered in the suspicious transaction log when the limiter is exceeded (see the description of the menu item "by Documents" in the section "Analysing Suspicious Transactions"); the recommended minimum value is "1".
- *Predefined Condition* – code-based conditions (program criteria):
  - "The Same Merchant" – operations with the same bankcard are repeatedly executed in the same merchant's device over a specified period.

    For example, if three operations executed by a cardholder on the same device over 30 minutes are considered suspicious, a rule with the following parameters must be set up:

    - *Period Type* = Sliding Minute

  - *Period* = 30
  - *Max #* = 2
- "Change Country" – the transaction country of operations executed with the same bankcard changes over a specified period.

  For example, a rule with the following parameters may be set up using this condition:

  - *Period Type* = Sliding Hours
  - *Period* = 12
  - *Max #* = 1
- "Amount Fitting" – multiple attempts to execute a transaction with the same card gradually decreasing the transaction amount during a specified time period.

  For example, a rule with the following parameters may be set up using this condition:

  - *Period Type* = Sliding Hours
  - *Period* = 1
  - *Max #* = 2
- "Utilization" – operations decreasing the card's amount available by the specified number of percents of the current amount available.

  For example, a rule with the following parameters may be set up using this condition:

  - *For Max Amount* = Available
  - *Period Type* = Day
  - *Period* = 1
  - *Max Pcnt* = 80
- "Invalid PIN" – multiple incorrect PIN entry attempts.

  For example, a rule with the following parameters may be set up using this condition:

  - *Period Type* = Sliding Days
  - *Period* = 1
  - *Max #* = 2
- "Invalid Expiry Date" – incorrect card expiration date
- "No Such Card" – transaction executed with a card whose number is not in the transaction counterparty database
- "Bad Contract Status" – allows a limiter to activate for all inactive contract statuses (i.e. statuses containing the "Invalid or "Decline" value in the *Is Valid* field of the table "Full → Configuration Setup → Contract Types → Contract Statuses"). Can be used with IF_CS group tags (see the section "Executing Actions Depending on Classifier Values" of the document

"WAY4 Client and Contract Classifiers") to activate a limiter for specific inactive statuses only. This value is used to monitor transactions on blocked cards.

- "Suspicious Contra Party" –the transaction counterparty is suspicious, i.e. has been entered in a stop list (see the section "Merchant Stop List".
- "Under Limit" – financial document for a transaction when there is no authorization document.
- "Check Previous Debit" – makes it possible to monitor that at a specific merchant a credit transaction amount does not exceed the total amount of debit transactions executed with this card for a set period. To implement this condition, two limiters must be configured.

  Rule 1 with parameters:

  - *Usage Type* = Transaction
  - *Predefined Condition* = Check Previous Debit

  Rule 2 with parameters:

  - *Usage Type* = Credit
  - *Predefined Condition* = Check Previous Debit
  - *Parent Usage* = Rule 1
  - *Exclude from parent* = Yes

  As a result, the first limiter will be used to save the history of executing debit transactions at various merchants for a set period. The second limiter will limit credit transactions at a specific merchant for an amount exceeding the amount of debit transactions made at this merchant for a set period.

- "Change Sub Area" – condition for analysing the number of transactions made in areas (groups of countries) that are geographically distant from one another, for example, on different continents.

  This condition assumes the *Area* field in the form with a limiter's additional parameters is used (see Fig. 3). An area including at least one sub area should be specified in this field. In this case, the limiter's counter will activate if after a transaction in a sub area, another transaction is made outside this area within a specified period, or vice versa, after a transaction outside the sub area, a transaction is made in a country belonging to this area. If this field is not filled in, the area "M49: World" with the code "001" from the area dictionary will be used. This area includes all countries registered in WAY4, grouped into five top-level sub areas (Asia, the Americas, Africa, Europe, Oceania). In this case, the limiter's counter will activate when a move is made from one of these sub areas to another. Moves between sub areas in lower levels of the hierarchy, for example, within the area "M49: Americas" are not considered. For more information about area setup, see the section "Country Area Support" of the document "WAY4 Dictionaries™".

  When this condition is used, a rule can be set, for example, using the following values in the limiter's fields:

- *Period Type* = Sliding Hours.
- *Period* = 12.
- *Max #* = 1.

As a result, the limiter will activate if two changes in the sub area in which transactions were made are registered within a 12 hour period.

Features of Average Threshold Value Calculation

If the *Algorithm* field of a limiter (risk rule) is left blank or contains the value "Fixed", the limiter threshold values are specified in fields *Max #*, *Max Amnt*, and *Max Sngl Amnt*.

If threshold values must consider the contract's transaction activity history, special values specified in the *Algorithm* field are used. In this case, threshold values are calculated from the number of cycles to be averaged in the *# Cycles* field; the cycle is defined by limiter parameters *Period Type* and *Period*. For more information about possible *Algorithm* field values, see the section "Threshold Calculation" of the document "Usage Limiters".

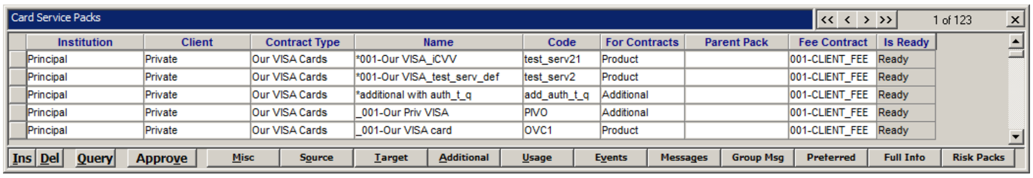
Average threshold value calculation has the following features:

- Average threshold values are calculated at the end of the limiter's effective cycle and the obtained value is used throughout the entire next cycle.
- If the global parameter USG_THRESHOLD_CALC_DELAY (default value "N") is not used:
  - Average threshold values are calculated starting with the second cycle after limiter activation, e.g. from the second day for *Period Type* = "Day" and *Period* = "1" or from the third month for *Period Type* = "Month" and *Period* = "2".
  - During the first cycle after limiter activation, threshold values are the default values specified in the field *Max Sngl Amnt* for the "Average Single" method, field *Max Amnt* for methods "Average Amount" and "Av Total Amount", and field *Max #* for methods "Average Number" and "Av Total Number".
- If the global parameter USG_THRESHOLD_CALC_DELAY = "Y" is used:
  - Average threshold values are calculated with a delay, only after the end of the interval for averaging the number of cycles equal to the value of the #Cycles field.
  - During the first averaging interval, threshold values are those values set by default in the *Max Singl Amnt* field for the "Average Single" method, in the *Max Amnt* field for the "Average Amount" and "Av Total Amount" methods, and in the *Max #* for the "Average Number" and "Av Total Number" methods.

Using Risk Rules

The "<…> Service Packs" form (see Fig. 4) is used to work with Risk Packages. It is opened through the "Risk Management Issuing → Configuration →

Account Service Packs" or "Risk Management Issuing → Configuration → Card Service Packs" user menu items for the issuing module and "Risk Management Acquiring → Configuration → Account Service Packs" and "Risk Management Acquiring → Configuration → Device Service Packs" user menu items for the acquiring module.



Card Service Packs
<< < > >>
1 of 123
Ins Del Query Approve Misc Source Target Additional Usage Events Messages Group Msg Preferred Full Info Risk Packs

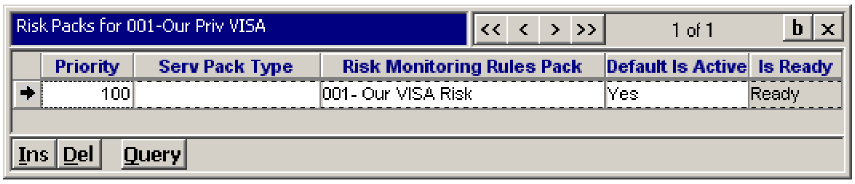
Institution	Client	Contract Type	Name	Code	For Contracts	Parent Pack	Fee Contract	Is Ready
Principal	Private	Our VISA Cards	*001-Our VISA_iCVV	test_serv21	Product		001-CLIENT_FEE	Ready
Principal	Private	Our VISA Cards	*001-Our VISA_test_serv_def	test_serv2	Product		001-CLIENT_FEE	Ready
Principal	Private	Our VISA Cards	*additional with auth_t_q	add_auth_t_q	Additional		001-CLIENT_FEE	Ready
Principal	Private	Our VISA Cards	_001-Our Priv VISA	PIVO	Additional		001-CLIENT_FEE	Ready
Principal	Private	Our VISA Cards	_001-Our VISA card	OVC1	Product		001-CLIENT_FEE	Ready

Fig. 4. Form for working with Risk Packages

The form is mainly used to add Risk Packages to Packages used for Product setup and contract registration. For more details on additional Service Packages, see section "Configuring Additional Service Packages" in the document "WAY4™ Service Packages".

To add a Risk Package, select the necessary main Package with the "Product" value in the *For Contracts* field and click the [Risk Packs] button.

This will open the "Risk Packs for <name of main Service Package>" grid form (see Fig. 5).



Priority	Serv Pack Type	Risk Monitoring Rules Pack	Default Is Active	Is Ready
100		001- Our VISA Risk	Yes	Ready

Fig. 5. Adding Risk Packages

To add a Risk Package, add a row in the table and select the desired Risk Package from the list in the *Risk Monitoring Rules Pack* field. Note that the list only contains Service Packages that have been registered in the risk monitoring module and have the "Risk Rule" value in the *For Contracts* field.

In the *Default Is Active* field, select whether this Package will be added to the main Package by default (value "Yes") or by an Event (value "No").

The [Events] button in the "Service Packs" form is used to register Events that activate/deactivate Service Packages (on using Events this way, see the section "Activating Additional Service Packages" in the document "Events").

ⓘ When approving changes in a Service Package, the correspondence of the mail and additional Service Package client category and contract type is not checked. Therefore, for risk monitoring it is possible to configure one Service Package for all contract (card) types.

ⓘ Note that since risks are monitored by usage limiters, transaction risk analysis may use both rules set up for a specific contract and any higher-ranking contracts. In this case, the *Usage Scenario* field of the contracts must contain the value "Main and Own".

ⓘ It is possible to configure general risk rules for all contracts of a financial institution. To do so, the rules must be configured for the financial institution's liability contract (see the section "Configuring Institution Specifications" of the "Financial Institutions" document).

Merchant Stop List

The user menu item "Risk Management Issuing → Configuration → Merchant Stop List" is used to add to merchant stop lists according to risk monitoring results.

For more information about working with stop lists, see the section "Merchant Stop List" in the document "WAY4™ Stop Lists".

Importing Configurations

It is possible to import Risk Packages configured by the WAY4 vendor.

To do so, use the menu items "Risk Management → Configuration → Import → Configuration File Import" and "Risk Management → Configuration → Import → Copy Configuration Import Screen".

For more information about importing Risk Packages, see the document "Importing Configurations Using the Configuration Inspector Module."

Chapter 3. Analysing Suspicious Transactions

To monitor and analyse suspicious transactions, use the following menu group items: "Risk Management Issuing → Monitoring" and "Risk Management Acquiring → Monitoring".

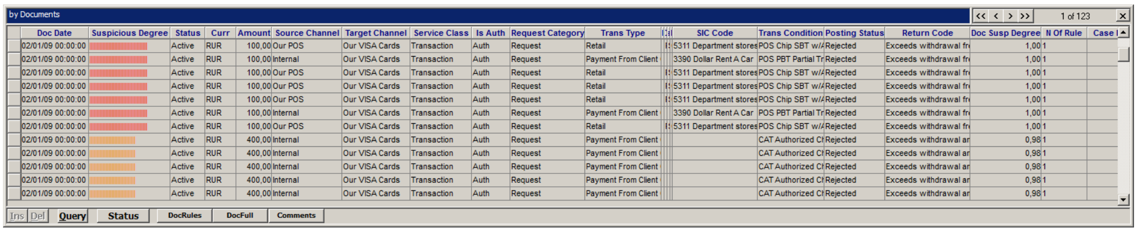
- by Documents – list of documents for transactions found to be suspicious.
- by Contract – list of contracts participating in suspicious transactions.
- by Rule – list of broken risk rules.

When selecting the specified menu items, define the monitoring period in a special window.

Note that the type of data shown in monitoring forms – issuing or acquiring – is determined by the value of the local constant "Product Category" (PCAT). For information about local constants, see the section "Initialising Local Constants" of the document "DB Manager User Management".

Analysing Transactions

The "by Documents" (see Fig. 6) grid form contains a list of documents for transactions found to be suspicious due to broken rules (limits) with a Suspicious Factor > 0 (see the section "Configuring Risk Rules").



by Documents

Doc Date	Suspicious Degree	Status	Curr	Amount	Source Channel	Target Channel	Service Class	Is Auth	Request Category	Trans Type	I	SIC Code	Trans Condition	Posting Status	Return Code	Doc Susp Degree	N Of Rule	Case I
02/01/09 00:00:00	🟥	Active	RUR	100,00	Our POS	Our VISA Cards	Transaction	Auth	Request	Retail	I	5311 Department stores	POS Chip SBT w/A	Rejected	Exceeds withdrawal fr	1,00	1	
02/01/09 00:00:00	🟥	Active	RUR	100,00	Internal	Our VISA Cards	Transaction	Auth	Request	Payment From Client		3390 Dollar Rent A Car	POS PBT Partial Tr	Rejected	Exceeds withdrawal fr	1,00	1	
02/01/09 00:00:00	🟥	Active	RUR	100,00	Our POS	Our VISA Cards	Transaction	Auth	Request	Retail	I	5311 Department stores	POS Chip SBT w/A	Rejected	Exceeds withdrawal fr	1,00	1	
02/01/09 00:00:00	🟥	Active	RUR	100,00	Our POS	Our VISA Cards	Transaction	Auth	Request	Retail	I	5311 Department stores	POS Chip SBT w/A	Rejected	Exceeds withdrawal fr	1,00	1	
02/01/09 00:00:00	🟥	Active	RUR	100,00	Our POS	Our VISA Cards	Transaction	Auth	Request	Retail	I	5311 Department stores	POS Chip SBT w/A	Rejected	Exceeds withdrawal fr	1,00	1	
02/01/09 00:00:00	🟥	Active	RUR	100,00	Internal	Our VISA Cards	Transaction	Auth	Request	Payment From Client		3390 Dollar Rent A Car	POS PBT Partial Tr	Rejected	Exceeds withdrawal fr	1,00	1	
02/01/09 00:00:00	🟥	Active	RUR	100,00	Our POS	Our VISA Cards	Transaction	Auth	Request	Retail	I	5311 Department stores	POS Chip SBT w/A	Rejected	Exceeds withdrawal fr	1,00	1	
02/01/09 00:00:00	🟧	Active	RUR	400,00	Internal	Our VISA Cards	Transaction	Auth	Request	Payment From Client			CAT Authorized Cl	Rejected	Exceeds withdrawal an	0,98	1	
02/01/09 00:00:00	🟧	Active	RUR	400,00	Internal	Our VISA Cards	Transaction	Auth	Request	Payment From Client			CAT Authorized Cl	Rejected	Exceeds withdrawal an	0,98	1	
02/01/09 00:00:00	🟧	Active	RUR	400,00	Internal	Our VISA Cards	Transaction	Auth	Request	Payment From Client			CAT Authorized Cl	Rejected	Exceeds withdrawal an	0,98	1	
02/01/09 00:00:00	🟧	Active	RUR	400,00	Internal	Our VISA Cards	Transaction	Auth	Request	Payment From Client			CAT Authorized Cl	Rejected	Exceeds withdrawal an	0,98	1	
02/01/09 00:00:00	🟧	Active	RUR	400,00	Internal	Our VISA Cards	Transaction	Auth	Request	Payment From Client			CAT Authorized Cl	Rejected	Exceeds withdrawal an	0,98	1	

Fig. 6. Suspicious transaction log

The form contains the transaction date, amount, currency, and other transaction parameters of each document.

The "by Documents" form also contains the field *N Of Rule* showing how many risk rules were broken and fields showing the transaction risk degree:

- *Suspicious Degree* – degree of suspiciousness as a graphic; the field uses a bar whose length and colour indicates the total transaction risk level: blank – very low, blue – low, green – average, orange – high, and red – very high
- *Doc Susp Degree* – degree of suspiciousness represented in numbers

The transaction risk degree depends on two factors:

- Importance of the violated rule or set of violated rules (see the description of the Suspicious Factor parameter in the section "Configuring Risk Rules").
- Degree by which the threshold set by the rule is exceeded.

  ⓘ Note that if a transaction amount limit is used, when the limit is significantly exceeded, the transaction will be considered suspicious event if the violated rule is not important.

The transaction risk degree is calculated as follows:

- The value of the "Risk Factor" variable is calculated according to one of the following formulas:
  - ♦ Risk Factor = Current Amount/Limit Amount
  - ♦ Risk Factor = Current Number/Limit Number

  where Current Amount/Number is the current value, and Limit Amount/Number is the threshold value
- The transaction risk factor is calculated:

  Rule Suspicious Factor = 1 – (1/Risk Factor)/Suspicious Factor,

  where Suspicious Factor is the limiter parameter
- If several rules are broken, the total risk degree is calculated:

  Total Suspicious Factor = 1 – (1 – Rule Suspicious Factor_1)(1 – Rule Suspicious Factor_2)…(1 – Rule Suspicious Factor_N),

  where Rule Suspicious Factor_K is the transaction risk factor according to the Kth limit.

Note that for visualisation, the length of the graphic (bar) indicating transaction risk is determined according to a special formula:

$$51 - 50\sqrt[4]{1 - Total\ Suspicious\ Factor}$$

where:

51 is the maximum length of the graphic indicator in vertical strokes.

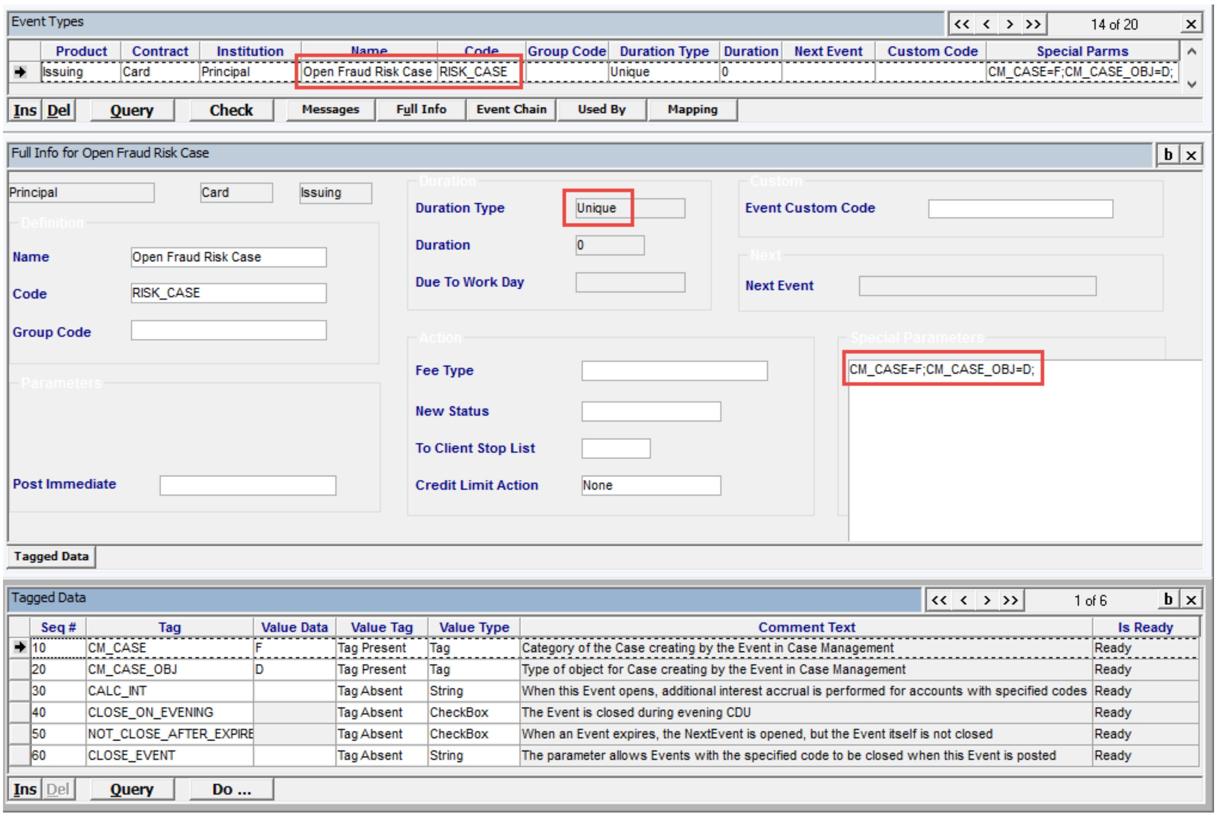
This formula ensures that if a set threshold is insignificantly exceeded, the indicator’s sensitivity is higher than for when a threshold is significantly exceeded. In other words, the change in the indicator will be significantly greater when a threshold goes from being exceeded by a factor of 2 to being exceeded by a factor of 4 then when a threshold that was exceeded by a factor of 20 is exceeded by a factor of 40.

The [Status] button allows document status to be changed according to risk monitoring. A change in document status may be accompanied by comments. The [Comments] button is used to access all comments for the document. The following statuses are supported:

- "Active" – the documents has not been processed.
- "Closed – Genuine" – the transaction is not fraudulent.
- "Closed – Fraud" – the transaction is fraudulent.

ⓘ Note that the [Status] button in the "by Documents" form will be available only when the following three conditions are met:

1. An Event type whose parameters are shown in Fig. 7 using an issuing module card contract as an example is registered for the Product category and card contract.



Event Types
<< < > >>
14 of 20
Ins Del Query Check Messages Full Info Event Chain Used By Mapping

Product	Contract	Institution	Name	Code	Group Code	Duration Type	Duration	Next Event	Custom Code	Special Parms
Issuing	Card	Principal	Open Fraud Risk Case	RISK_CASE		Unique	0			CM_CASE=F;CM_CASE_OBJ=D;

Full Info for Open Fraud Risk Case

Principal Card Issuing

Definition

Name: Open Fraud Risk Case

Code: RISK_CASE

Group Code:

Parameters

Post Immediate:

Duration

Duration Type: Unique

Duration: 0

Due To Work Day:

Action

Fee Type:

New Status:

To Client Stop List:

Credit Limit Action: None

Custom

Event Custom Code:

Next

Next Event:

Special Parameters

CM_CASE=F;CM_CASE_OBJ=D;

Seq #	Tag	Value Data	Value Tag	Value Type	Comment Text	Is Ready
10	CM_CASE	F	Tag Present	Tag	Category of the Case creating by the Event in Case Management	Ready
20	CM_CASE_OBJ	D	Tag Present	Tag	Type of object for Case creating by the Event in Case Management	Ready
30	CALC_INT		Tag Absent	String	When this Event opens, additional interest accrual is performed for accounts with specified codes	Ready
40	CLOSE_ON_EVENING		Tag Absent	CheckBox	The Event is closed during evening CDU	Ready
50	NOT_CLOSE_AFTER_EXPIRE		Tag Absent	CheckBox	When an Event expires, the NextEvent is opened, but the Event itself is not closed	Ready
60	CLOSE_EVENT		Tag Absent	String	The parameter allows Events with the specified code to be closed when this Event is posted	Ready

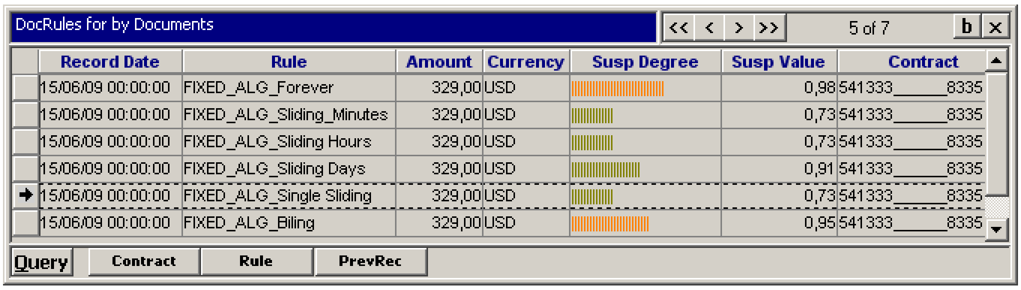
Fig. 7. "Open Fraud Risk Case" Event type parameters

2. This Event type is specified in the *Event Type* field of additional parameters for the limiter used to set up the rule (see Fig. 3 in the section "Configuring Risk Rules").
3. Preconfiguration has been performed by running the menu item "Risk Management Acquiring → Configuration → Set Workflow Configuration".

⚠ Note that it is recommended to set up functionality for changing document status only for risk rules that are mandatory for analysis by risk managers. WAY4 expects a risk manager to confirm or reject fraud for each document for which status change functionality is available. This is because when this setting is used, a large number of unprocessed documents (with the "Active" status) may negatively affect performance of the authorisation subsystem.

To access full document information, use the [DocFull] button. It opens the form containing all the parameters of a document for a suspicious transaction.

To analyse broken rules, use the [DocRules] button to open the "DocRules for Suspicious Documents" form (see Fig. 8). It contains the list of rules broken by the transaction.



	Record Date	Rule	Amount	Currency	Susp Degree	Susp Value	Contract
	15/06/09 00:00:00	FIXED_ALG_Forever	329,00	USD		0,98	541333______8335
	15/06/09 00:00:00	FIXED_ALG_Sliding_Minutes	329,00	USD		0,73	541333______8335
	15/06/09 00:00:00	FIXED_ALG_Sliding Hours	329,00	USD		0,73	541333______8335
	15/06/09 00:00:00	FIXED_ALG_Sliding Days	329,00	USD		0,91	541333______8335
➔	15/06/09 00:00:00	FIXED_ALG_Single Sliding	329,00	USD		0,73	541333______8335
	15/06/09 00:00:00	FIXED_ALG_Biling	329,00	USD		0,95	541333______8335

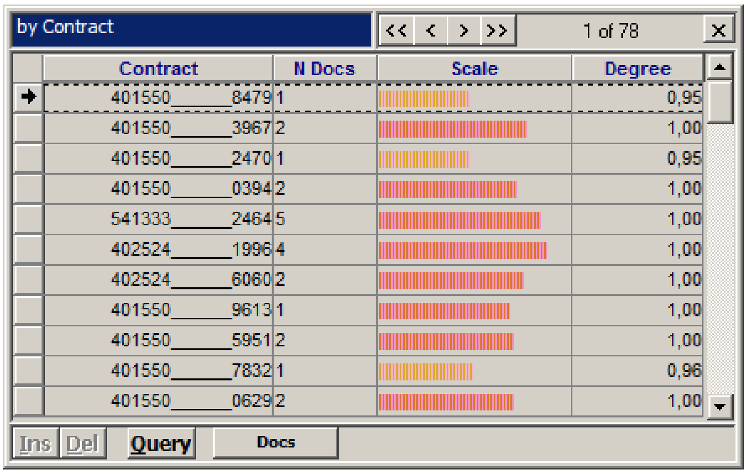
Fig. 8. List of broken rules

For each broken rule, users can:

- Get information on the contract containing the broken rule using the [Contract] button.
- Get information on the broken rule's parameters using the [Rule] button.
- Get information on the previous documents that along with the current document resulted in the rule violation using the [PrevRec] button; if the rule was violated by a single (current) document, only this document will be shown in the list.

Analysing Contracts

The grid form "by Contract" (see Fig. 9) contains a list of contracts that participated in suspicious transactions.

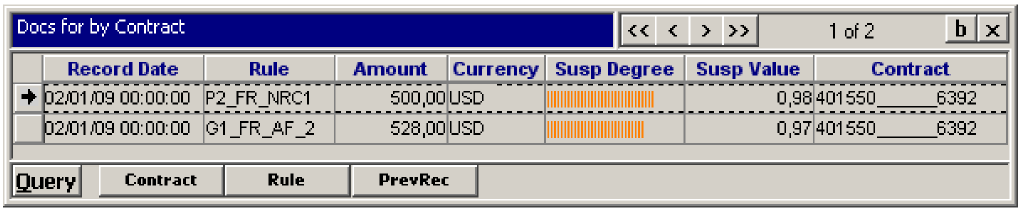


Contract	N Docs	Scale	Degree
401550______8479	1		0,95
401550______3967	2		1,00
401550______2470	1		0,95
401550______0394	2		1,00
541333______2464	5		1,00
402524______1996	4		1,00
402524______6060	2		1,00
401550______9613	1		1,00
401550______5951	2		1,00
401550______7832	1		0,96
401550______0629	2		1,00

Fig. 9. List of contracts participating in suspicious transactions

In the *Scale* and *Degree* fields, a graphic and numeric value, respectively, are shown as suspicion indicators for the contract for a specified period.

For each contract, by clicking [Docs] it is possible to obtain information on documents for transactions found to be suspicious (see Fig. 10).

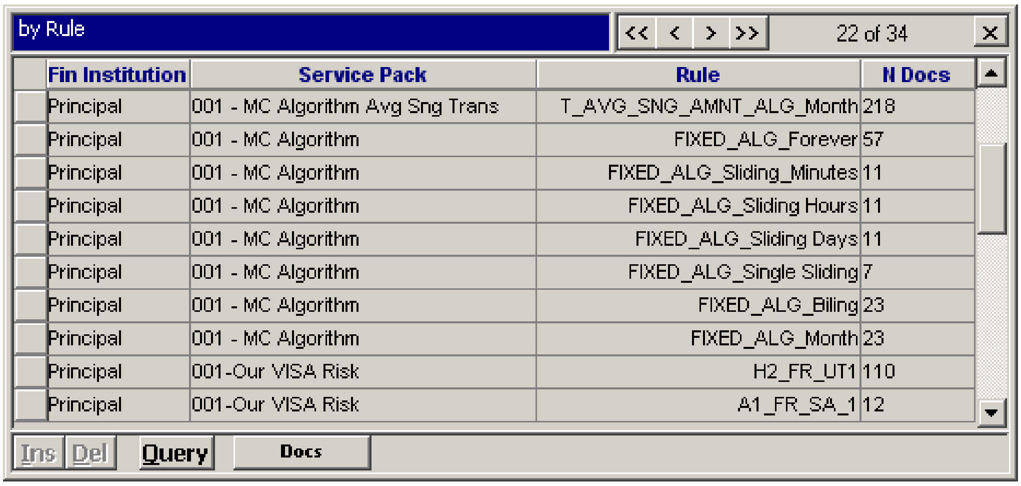


Record Date	Rule	Amount	Currency	Susp Degree	Susp Value	Contract
02/01/09 00:00:00	P2_FR_NRC1	500,00	USD		0,98	401550______6392
02/01/09 00:00:00	G1_FR_AF_2	528,00	USD		0,97	401550______6392

Fig. 10. List of documents for a contract's suspicious transactions

Analysing Broken Rules

The grid form "by Rule" (see Fig. 11) contains a list of broken risk rules.



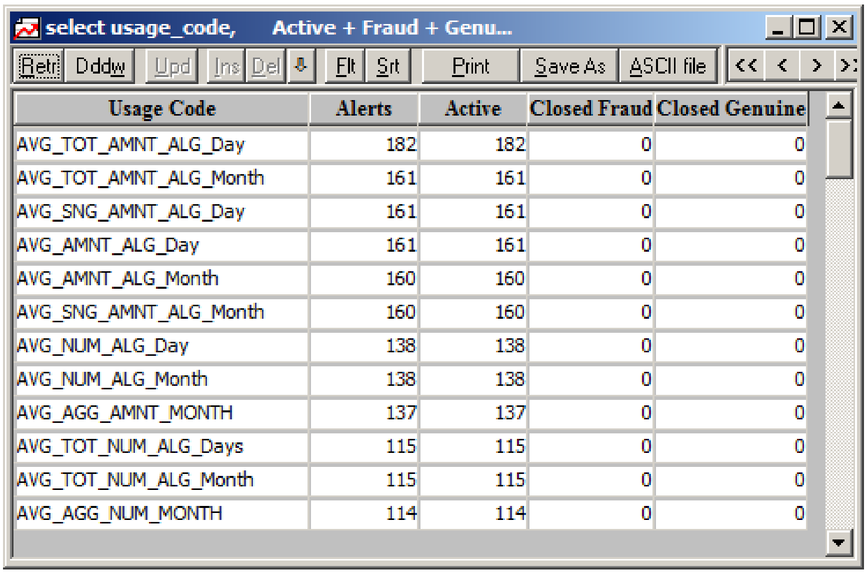
Fin Institution	Service Pack	Rule	N Docs
Principal	001 - MC Algorithm Avg Sng Trans	T_AVG_SNG_AMNT_ALG_Month	218
Principal	001 - MC Algorithm	FIXED_ALG_Forever	57
Principal	001 - MC Algorithm	FIXED_ALG_Sliding_Minutes	11
Principal	001 - MC Algorithm	FIXED_ALG_Sliding Hours	11
Principal	001 - MC Algorithm	FIXED_ALG_Sliding Days	11
Principal	001 - MC Algorithm	FIXED_ALG_Single Sliding	7
Principal	001 - MC Algorithm	FIXED_ALG_Biling	23
Principal	001 - MC Algorithm	FIXED_ALG_Month	23
Principal	001-Our VISA Risk	H2_FR_UT1	110
Principal	001-Our VISA Risk	A1_FR_SA_1	12

Fig. 11. List of broken risk rules

Clicking the [Docs] button for each of the rules shows information on documents for transactions which caused the rule to be broken. The form opened by clicking this button is similar to the "by Documents" form (see Fig. 6).

Risk Rule Activation Statistics

To obtain statistic information about the number of activated risk rules and the results of processing suspicious transaction documents, use the report opened by the menu item "OpenWay → Risk Management → Monitoring → Rule Efficiency Report" (see Fig. 12).



Usage Code	Alerts	Active	Closed Fraud	Closed Genuine
AVG_TOT_AMNT_ALG_Day	182	182	0	0
AVG_TOT_AMNT_ALG_Month	161	161	0	0
AVG_SNG_AMNT_ALG_Day	161	161	0	0
AVG_AMNT_ALG_Day	161	161	0	0
AVG_AMNT_ALG_Month	160	160	0	0
AVG_SNG_AMNT_ALG_Month	160	160	0	0
AVG_NUM_ALG_Day	138	138	0	0
AVG_NUM_ALG_Month	138	138	0	0
AVG_AGG_AMNT_MONTH	137	137	0	0
AVG_TOT_NUM_ALG_Days	115	115	0	0
AVG_TOT_NUM_ALG_Month	115	115	0	0
AVG_AGG_NUM_MONTH	114	114	0	0

Fig. 12. Rule activation statistics

For the period selected when starting the report, for each rule report columns show the total number of suspicious transactions (Alerts), the number of fraudulent transactions (Fraud), the number of transactions that were not fraudulent (Genuine) and the number of transactions that have not yet been processed (Active).

ⓘ Note that statistics are gathered for transactions for which the risk manager confirmed or rejected fraud. This decision is made using functionality for changing a document's status (see the section "Analysing Transactions").

Expert Tools

The menu folder Risk Management Issuing → Expert Tools is used to analyse merchants that are counterparties in risk monitoring card transactions.

The menu item Risk Management Issuing → Expert Tools → Merchant Stop List Analyse opens a merchant stop list form similar to that described in the section "Merchant Stop List" with the difference that it is possible to analyse whether documents for suspicious transactions correspond to a record in a merchant stop list. To determine whether there are suspicious transactions belonging to a merchant selected in the stop list, click the [Analyse] button and specify the required time period. To access information about card contracts that were parties to the transaction with the selected merchant, click the [Cards] button.

The Risk Management Issuing → Expert Tools → Coincide Merchants menu folder makes it possible to identify merchants at which bankcard data may have been copied.

This functionality may be implemented as follows:

- According to cardholders' statements or information from other sources, cards whose data was copied are identified.
- Using the "Mark Card for Analyse" form (Risk Management Issuing → Expert Tools → Coincide Merchants → Mark Card for Analyse) the cards identified are marked for analysis.
- The process of searching for merchants "Risk Management Issuing → Expert Tools → Coincide Merchants → Find Coincide Merchants" is started.
- Using the "Suspicious Merchants" form (Risk Management Issuing → Expert Tools → Coincide Merchants → Suspicious Merchants), merchants common to the marked cards are analysed.

This form makes it possible to see lists of all documents and all cards serviced at the selected merchant for the specified period.

Identified merchants may be, for example, entered in a merchant stop list (see "Merchant Stop List").

For cards whose data was copied, an Event may be opened; for example, to change status and/or send messages to cardholders.

Deferred Processing of Limiters

Starting from WAY4 version 03.38.30, to decrease the load in online processing of transaction messages in WAY4, deferred, offline processing is supported for limiters used, for example, as risk rules or for charging fees such as balance inquiry fees.

When configuring limiters that can be processed offline, the "Off Line" value must be specified in the *Proc.Mode* field.

Deferred processing of limiters works according to the following rules:

- When processing contract usage limiters (see the section "Principles of Usage Limiter Operation" of the document "Usage Limiters") a set of documents for which limiter processing must be deferred is created from documents being processed.
- The "Offline Usage Limiters Processing" process is used for deferred processing of limiters. This process can be started with the menu item "Risk Management → Monitoring → Offline Processing → Run Offline Processing - Single pass".
- To start periodic execution of the process for deferred processing of limiters in the issuing module, the menu item "Risk Management Issuing → Monitoring → Offline Processing → Start Processing Scheduler" is used; and in the acquiring module the menu item "Risk Management Acquiring → Monitoring → Offline Processing → Start Processing Scheduler". To stop periodic execution of the process in the issuing module, the menu item "Risk Management Issuing → Monitoring → Offline Processing → Stop Processing Scheduler" is used and in the acquiring module, the menu item

"Risk Management Acquiring → Monitoring → Offline Processing → Stop Processing Scheduler".

- For the process "Offline Usage Limiters Processing" to be periodically started, the frequency with which the process is to be started must be specified. The interval of time between starts of the process is set (in seconds) in the *Period* field of the "Process Parameters" form (Full → Configuration Setup → Main Tables → Process Parameters). Parallel execution of the process can also be configured in this table, when necessary (see the document "Running WAY4™ Processes in Parallel").

  ⓘ Note that the list of processes that can be selected in the "Process Parameters" form only contains those processes with information in the process log; i.e. processes that have already been executed in WAY4. Therefore, to be able to select the process "Offline Usage Limiters Processing" from the list of processes to set its parameters, it must be executed with the menu item "Risk Management → Monitoring → Offline Processing → Run Offline Processing - Single pass".

  If errors occurred when processing a set of documents, the process is stopped and can be restarted after the errors have been eliminated. The list of document sets whose processing was interrupted is available for the issuing module in the form "Risk Management Issuing → Monitoring → Offline Processing → Troubleshooting → Crude Offline Batchs" and for the acquiring module in the form "Risk Management Acquiring → Monitoring → Offline Processing → Troubleshooting → Crude Offline Batchs". This form contains the "Unprocessed Docs" row corresponding to a document set waiting for processing, and the "Docs to Processing" rows corresponding to document sets whose processing was interrupted. The [ProcessLog] button makes it possible to get information on the results of process execution and errors that occurred during execution. Limiter processing can be restarted for a selected document set by clicking the [StartProc] button.

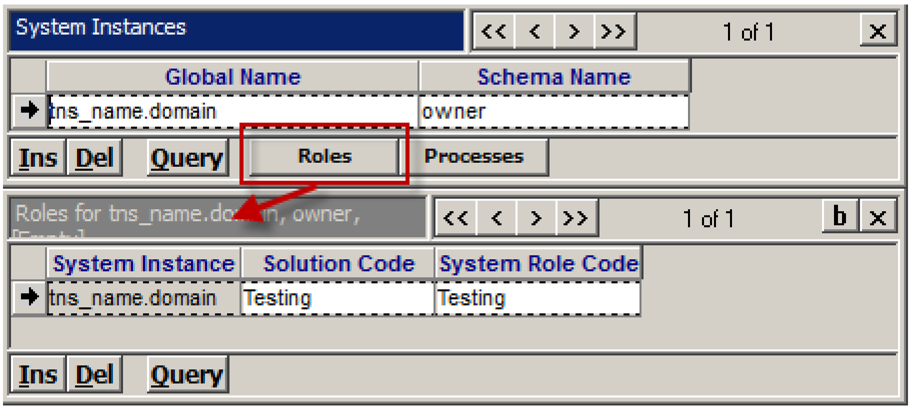
Chapter 4. Testing Limiter Settings

To test risk monitoring limiter settings in WAY4 a procedure is provided for recalculating the contents of limiter counters.

The recalculation procedure involves checking the execution of limiters of all documents from the date specified by the user.

⚠Note that limiters may only be recalculated on a test system. If recalculation is run on a production system, the process will be terminated with an error message.

To run the recalculation procedure on a test system, open the form "Testing - Usage Recalculation → System Instances" (see Fig. 13) and ensure there is a test system record.


System Instances
<< < > >>
1 of 1
Ins Del Query Roles Processes
Roles for tns_name.domain, owner,
<< < > >>
1 of 1
Ins Del Query

Global Name	Schema Name
tns_name.domain	owner

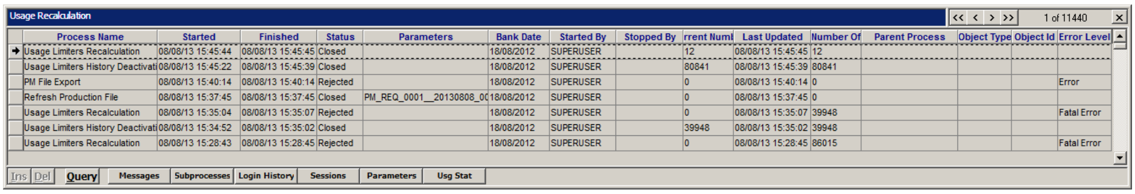
System Instance	Solution Code	System Role Code
tns_name.domain	Testing	Testing

Fig. 13. Test system registration

If this record is absent, register a test system, specifying the global name and schema name; and in the "Roles" child form add a record, specifying the "Testing" value in the *Solution Code* and *System Role Code* fields.

After starting the recalculation procedure ("Testing - Usage Recalculation → Usage Recalculation") a form will be displayed to enter the date from which recalculation should be executed.

At the end of the procedure the "Usage Recalculation" form will be displayed (see Fig. 14).


Usage Recalculation
<< < > >>
1 of 11440
Ins Del Query Messages Subprocesses Login History Sessions Parameters Usg Stat

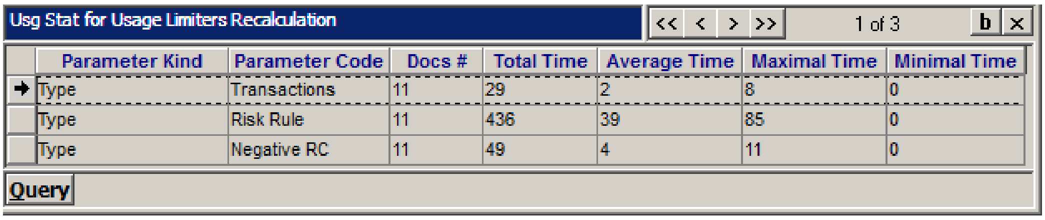
Process Name	Started	Finished	Status	Parameters	Bank Date	Started By	Stopped By	rrent Numl	Last Updated	Number Of	Parent Process	Object Type	Object Id	Error Level
Usage Limiters Recalculation	08/08/13 15:45:44	08/08/13 15:45:45	Closed		18/08/2012	SUPERUSER		12	08/08/13 15:45:45	12				
Usage Limiters History Deactivati	08/08/13 15:45:22	08/08/13 15:45:39	Closed		18/08/2012	SUPERUSER		80841	08/08/13 15:45:39	80841				
PM File Export	08/08/13 15:40:14	08/08/13 15:40:14	Rejected		18/08/2012	SUPERUSER		0	08/08/13 15:40:14	0				Error
Refresh Production File	08/08/13 15:37:45	08/08/13 15:37:45	Closed	PM_REQ_0001__20130808_0(	18/08/2012	SUPERUSER		0	08/08/13 15:37:45	0				
Usage Limiters Recalculation	08/08/13 15:35:04	08/08/13 15:35:07	Rejected		18/08/2012	SUPERUSER		0	08/08/13 15:35:07	39948				Fatal Error
Usage Limiters History Deactivati	08/08/13 15:34:52	08/08/13 15:35:02	Closed		18/08/2012	SUPERUSER		39948	08/08/13 15:35:02	39948				
Usage Limiters Recalculation	08/08/13 15:28:43	08/08/13 15:28:45	Rejected		18/08/2012	SUPERUSER		0	08/08/13 15:28:45	86015				Fatal Error

Fig. 14. Form with a record on execution of the limiter recalculation procedure

The last record in this form corresponds to the limiter recalculation procedure.

To obtain statistic information on recalculation results, click the [Usg Stat] button.

This command will open the "Usg Stat for Usage Limiters Recalculation" form (see Fig. 15).



Parameter Kind	Parameter Code	Docs #	Total Time	Average Time	Maximal Time	Minimal Time
Type	Transactions	11	29	2	8	0
Type	Risk Rule	11	436	39	85	0
Type	Negative RC	11	49	4	11	0

Fig. 15. Limiter recalculation results

This form contains information about the number of processed documents "Docs #), total processing time (Total Time) and the average, maximum and minimum time for processing one document.

According to the results for time spent processing limiters, the user can evaluate efficiency of settings and correct them, if required.

Recalculation results may be further analysed in monitoring forms (see the section "Analysing Suspicious Transactions".