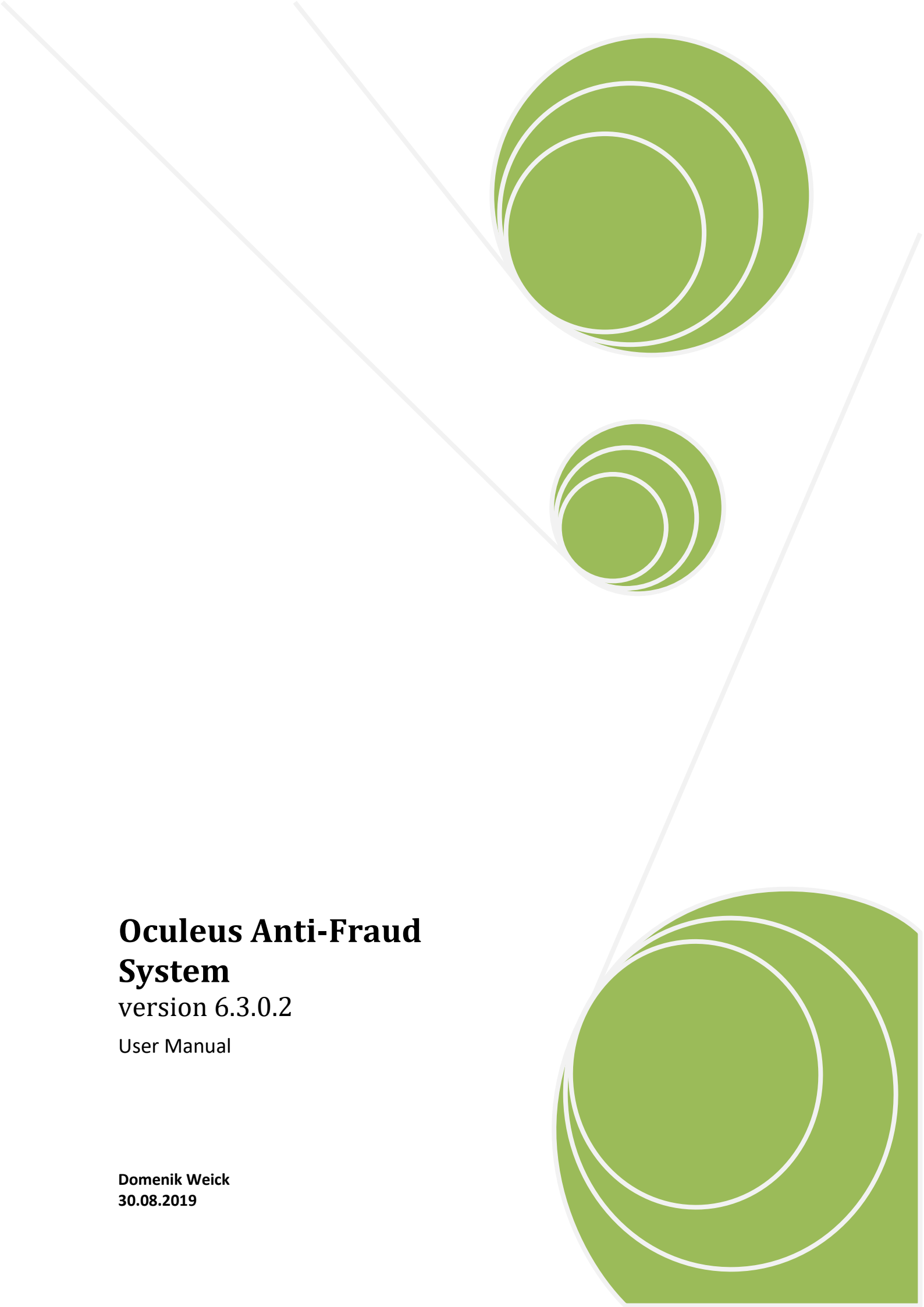




Oculeus Anti-Fraud System

version 6.3.0.2

User Manual

Domenik Weick
30.08.2019

Contents

1 Introduction.....	5
1.1 Summary.....	5
1.2 Objective.....	6
1.3 System Features & Modules.....	6
2 Analytical Dashboard.....	7
2.1 Overview.....	7
2.2 Traffic Distribution Charts	7
2.3 Incident Map	8
How to change the amount of displayed countries:	8
How to change from Origination to Destination:.....	8
How to change from showing only fraudulent traffic to change to total traffic:.....	8
How to see fraudulent calls to a specific Destination/ from a specific Origination:	8
2.4 System Status	9
3 Scenarios	10
3.1 Scenarios	10
How to search for a specific scenario:.....	10
How to filter scenarios based on the used data source:	10
3.2 Scenario Types.....	11
3.2 Scenario Menu.....	12
How to change the scenario view from grid to list:	12
3.3 Monitor Scenario Results	13
How to see the Scenario Overview	13
4 Scenario Setup.....	15
4.1 Step 1 – Configuration.....	15
4.2 Step 2 - Filtering Criteria.....	16
4.2.1 Basic Filter Options.....	16
How to set Basic Filter	17
How to remove Items from Basic Filter.....	17
How to Disable a Basic Filter	17
4.2.2 Advanced Filter Options	17
How to set up an Advanced Filter	18
4.2.3 Filter Lists.....	18
4.2.4 Filtering Formula	18
4.3 Step 3 - Incident Definition.....	20
4.3.1 Overview.....	20

4.3.2 Monitored Traffic Range	20
4.3.3 Incident Types	22
Format of Threshold Lists	22
4.3.4 Incident Thresholds	23
4.3.5 Incident Formula	25
4.3.6 Threshold Scopes	25
4.3.7 Risk Levels	26
4.4 Step 4 – Actions	26
4.4.1 Notifications	26
4.4.2 Blocking Conditions	26
5 Scenario Management	28
5.1 Edit, Duplicate or Delete a Scenario	28
5.2 Add a New Scenario	28
6 Scenario Options	29
6.1 Activities	29
6.1.1 Activity List	29
6.1.2 Incident List	29
6.1.3 Activity Details	30
How to add incident items to the block/ ignore/allow list	31
How to export fraudulent records as .csv file	31
6.2 Call Records	31
6.2.1 Call Records	31
6.2.2 Processed Traffic	31
6.3 Notifications	32
How to open Activity Details from Notifications Menu	32
How to expand notification information	32
7 Fraud Prevention	32
7.1 Blocked Items	32
7.1.1 Automatic Blocking	32
7.1.2 Permanent Blocking	33
7.1.3 Blocking History	33
How to see Activity Details for Blocking History	33
How to see all Blocking Commands created by a specific activity	33
How to exclude all Blocking Commands created by a specific activity	33
How to see Setup of scenario which triggered an automatic blocking	33

How to see all Blocking Commands triggered by a specific scenario.....	33
How to exclude all Blocking Commands created by a specific scenario	33
7.1.4 Active/ Pending/ Expired Items.....	33
How to block Items manually based on external information.....	34
How to release automatic blocked items.....	34
7.2 Ignored Items	35
How to add Items to the ignored Items list.....	35
How to remove Items from the allowed Items list	35
7.3 Allowed Items.....	36
How to add Items to the allowed Items list	36
How to remove Items from the allowed Items list	36
7.4 Filter Lists.....	36
How to create a filter list.....	36
How to update the items within an existing list.....	37
8 Traffic Profiling	37
8.1 Overview.....	37
8.2 Traffic Anomalies.....	37
8.2.1 Overview.....	37
8.2.2 Detected Anomalies Details	39
9 Tools	41
9.1 Traffic Files.....	41
9.1.1 Imported Files.....	41
9.2 Permissions.....	41
9.3 User Logs	41
9.4 Preferences.....	42
9.4.1 Carrier	42
9.4.2 Breakouts.....	42
9.4.3 Routings.....	42
How to add Carrier, Breakouts and Routings.....	42
9.5 Global Configuration	42
How to change user password	42
How to Logout	42
How to disable/enable Auto-Logout	42

1 Introduction

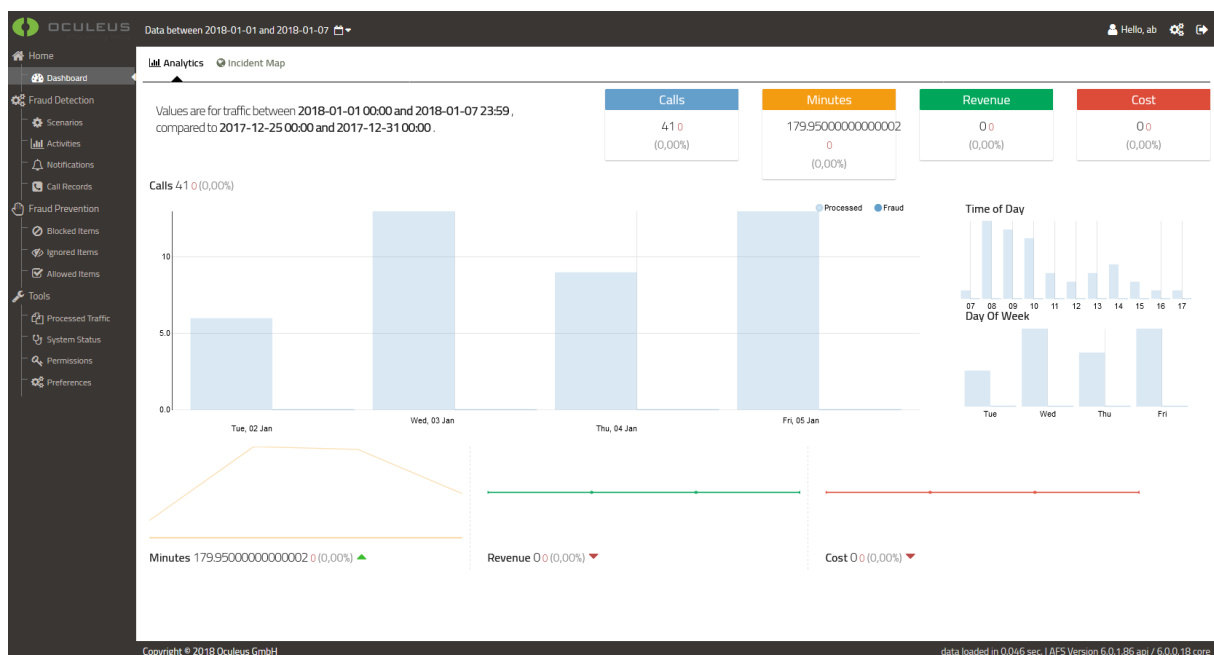
1.1 Summary

Oculus Anti-Fraud System is a highly automated fast and versatile system to identify and fight telecommunication fraud. Within minutes, it is able to identify and fight nearly every type of fraud. Running on Linux, it comes with a state-of-the-art web interface that makes the whole system extremely cost effective.

Fraud detection is increasingly becoming a significant issue with voice operators, where margins are eroded and even the smallest problem can result in dramatic margin loss.

The system has been developed in close cooperation with some of our customers and represents a collection of proven modules of our other systems with the sole purpose to monitor traffic and identify telecom fraud as fast as possible.

The Anti-Fraud System provides traffic profiling functionality to monitor and identify traffic anomalies. Operators can set scenarios to filter unusual fraudulent traffic patterns on specific destinations down to an individual A- or B- number.



The system also generates alerts when the user-set criteria are breached. The notifications can be emailed or reviewed within the program.

The notifications, together with the reports, allow NOC and routing managers to evaluate the potential fraud, check the specific traffic down to the CDR level in order to identify the probable source, and implement changes before traffic volumes increase and significant losses are generated.

The usage of the system is very intuitive, and due to a very small technical footprint required it is possible to set up the system on a Linux platform of any scale starting from Raspberry-PY up to the biggest multi-core servers required for protection of enterprises, telecom carriers, and telecom operators.

The **Anti-Fraud System** runs on Linux systems/servers. It does not require any additional cost-intensive third-party database license. The system can be provided to run in-house or hosted. The size and scale of the required hardware depends on traffic volume and commercial setup.

1.2 Objective

This tool allows monitoring specific traffic, such as high-risk destinations, new carriers, or prepaid routings, based on defined patterns and values.

The system also enables dynamic traffic monitoring and analyzes changes in traffic behavior.

The system provides the following functionalities:

- **Dynamic Traffic Profiling** is a self-learning engine that profiles collected traffic for a subsequent prediction of the future traffic profile and analysis of changes in traffic behavior.
- **Fraud Detection** is used for building traffic monitoring rules for fraudulent patterns search and getting notifications whenever applicable. The system also allows users to easily view and analyze filtered traffic of different types for further problem solving.
- **Fraud Traffic Blocking** functionality allows blocking fraudulent traffic automatically in order to prevent significant margin losses.



1.3 System Features & Modules

The **Anti-Fraud System** contains the following modules:

- **Scenario Management:** this module provides functionalities and tools to create and manage different fraud scenarios used in collecting and analyzing traffic.
- **Fraud Reports:** this module provides tools to report on processed traffic, as well as collected traffic based on existing fraud scenarios.
- **Traffic Profiling:** this module allows detecting traffic anomalies based on the traffic profile forecast.
- **Tools & Settings:** this section provides information about tools and administration settings available in the system.

2 Analytical Dashboard

2.1 Overview

The **Dashboard** area provides an overview of the most important information for a defined period. Traffic is summarized on the amount of calls, minutes, revenue und cost. Those values are aggregated as total (processed) and as fraudulent values. The chart information can be changed by clicking on calls, minutes, revenue and cost.



2.2 Traffic Distribution Charts

The **Traffic Distribution Charts** area provides visual representation of traffic distribution over the selected period – three different views of the same data set.

Disable the **Fraud** option to view the **Processed** Traffic chart and vice versa.

The charts on the **Calls**, **Minutes**, **Revenue** and **Cost** tabs of the **Traffic Distribution** view display the corresponding information.

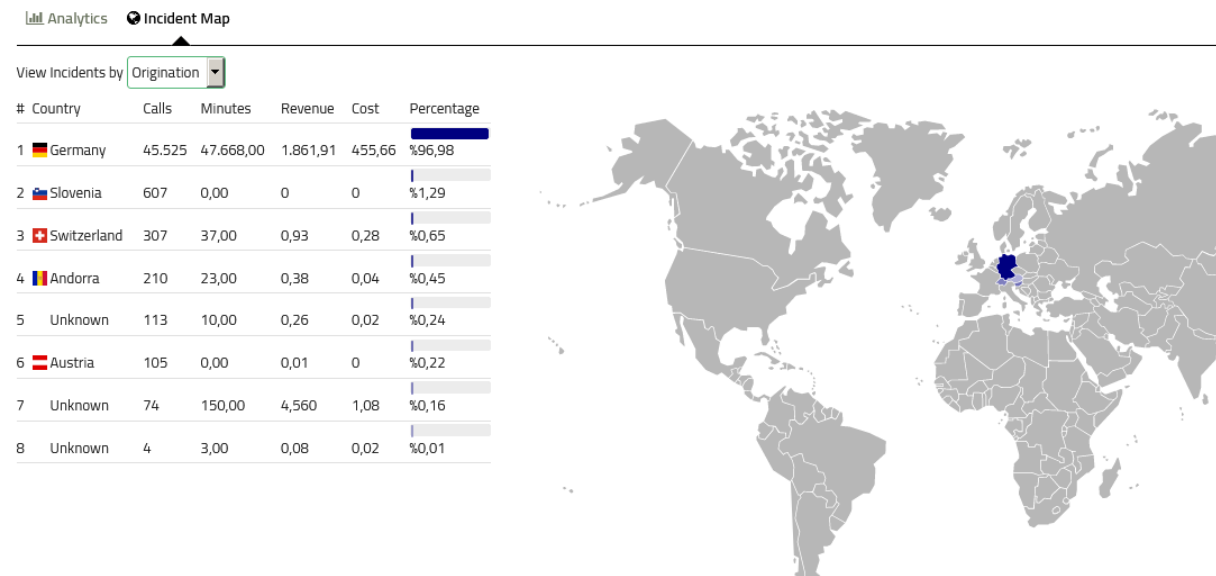
Hover the mouse pointer over the chart to view the processed traffic and fraud values at any moment of the selected period.

The additional **Time of Day** and **Day of Week** bar charts display the traffic distribution aggregated by the hour of day and by the day of week within the selected period, respectively. These aggregated views are useful for monitoring the traffic distribution.

2.3 Incident Map

The **Incident Map** area is a submenu in the dashboard menu.

It provides a visual display of fraud incidents distribution by **Origination** or/and **Destination**.

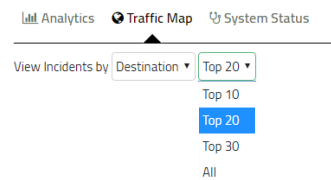


Display of data can be modified, e.g. to show information of total traffic instead of showing only fraudulent traffic, by clicking on the toggle button. ☒ Show fraudulent traffic ☐ Show fraudulent traffic

The amount of shown countries can also be modified from "Top 10" to "Top 20" to "Top 30" or even all.

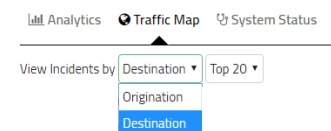
How to change the amount of displayed countries:

1. Click on the current selected amount
2. Select from the top-down menu the preferred amount



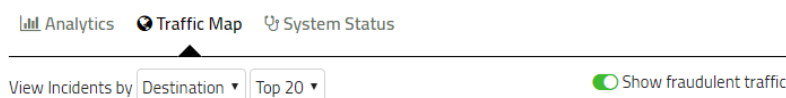
How to change from Origination to Destination:

1. Click on Destination/ Origination
2. Select the preferred choice



How to change from showing only fraudulent traffic to change to total traffic:

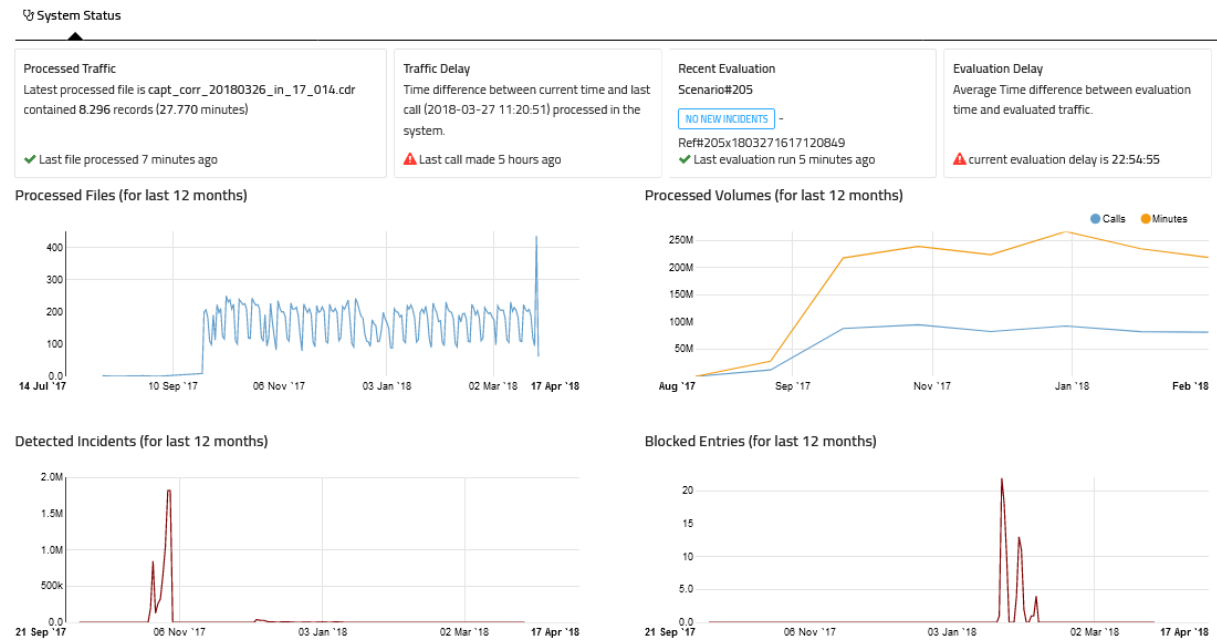
1. Click on the radio-button to change between fraudulent only or all traffic



How to see fraudulent calls to a specific Destination/ from a specific Origination:

1. Open the sub menu Traffic Map
2. Click on the phone button behind the specific Destination
3. To open Calls from a specific Origination change the view of presentation (See How to change from Origination to Destination) and follow the instruction from step 2

2.4 System Status



System Status allows to monitor the traffic behavior of the last 12 months.

It provides:

- The name of **Last File Processed (.CDR)** and the time of its processing by the system.
- Detection of delay between traffic range and its evaluation.
- Time difference between last call and the current time.
- The time of last fraud evaluation check.
- Graphical Overview of Processed Files
- Graphical Overview of Processed Volumes (Calls & Minutes)
- Graphical Overview of Detected Incidents
- Graphical Overview of Blocked Entries

3 Scenarios

3.1 Scenarios

The main objective of the **Fraud Detection** module is to create and manage fraud scenarios.

A **Fraud scenario** is a set of conditions, that are defined to monitor specific traffic patterns. Based on the conditions the system is able to 1) identify fraud, 2) notify via email as soon as fraud is identified and 3) automatically block future traffic.

Scenarios

Find in list [+ New Item](#)

ALL (24) STANDARD (24)

Total items collected: 24

#	Status	Type	Scenario	Range	Description	
1	ENABLED	Standard	#218 - Negative Margin	Periodic Hourly	No Description	... ➤
2	ENABLED	Standard	#206 - Same Duration	Periodic Daily	checking for A-Number range generating calls with same duration	... ➤
3	ENABLED	Standard	#205 - Wangiri - Trap calls	Periodic Hourly	checking for A-Number ranges that generate large failed calls on daily bases	... ➤
4	ENABLED	Standard	#204 - Fair Usage	Periodic Daily traffic compared to Last undefined Hours	checking for A-Number that exceeds 250 minutes daily.	... ➤
5	ENABLED	Standard	#203 - Sequential A and B Numbers	Periodic 6 Hours	checking for calls originated from / terminated to sequential number ranges	... ➤
6	ENABLED	Standard	#202 - Overlapping Calls	Periodic Daily	checking for A-Numbers generating concurrent calls.	... ➤

The system contains a set of preconfigured standard scenarios in order to assist users in creating rules based on their requirements. See the Scenarios Types section for more information.

The **Scenarios** menu displays all scenarios created in the system. Each scenario is automatically assigned to a unique **ID** number in the system.

How to search for a specific scenario:

Use the **Search** option to filter the scenarios list by **Title** or **ID** number.

Find in list

How to filter scenarios based on the used data source:

Use the Upper Ribbon to display either Standard, Dynamic, Live or All Scenarios.

ALL (47) STANDARD (47)

3.2 Scenario Types

The system is able to evaluate three different data sources using the corresponding scenario type:

- Standard CDRs
- Dynamic CDRs
- Live CDRs

Standard scenarios are fully configurable depending on users' input.

Dynamic scenarios use the embedded self-learning traffic prediction engine, to identify fraud by detecting anomalies.

Traffic profiling engine evaluates all traffic and profiles it by using historical data, traffic trends (e.g. normal growth), and seasonality (e.g. time of day, day of week). It also predicts the traffic profile for next period (e.g. for 5 minutes, 15 minutes, and 1 hour). An anomaly is detected when realized/actual traffic does not conform to the predicted traffic. When an anomaly is detected, the system automatically triggers an alert and extracts the abnormal data for further analysis in the system. The analysis is provided by the **Dynamic scenarios**.

Live scenarios are special type of scenarios that can provide real-time data analysis based on data collected directly from the switches. If supported, call data such as calling/called numbers, can be extracted and evaluated in real time. It allows for faster response time; yet these scenarios have limited evaluation options, compared to **Standard scenarios**.

The system provides users with options to build scenarios based on quality parameters (ASR, ACD, number of calls, or duration) or/and commercial information (revenue, cost, or margin) if the latter is available in CDRs.

3.2 Scenario Menu

Take instant actions on the scenario:

- Edit
- Duplicate
- Enable/Disable
- Delete

Monitoring:

- View scenario
- Scenario Activities

Change displayed Scenario Type:

Search field

Create new a scenario

Configuration Information

Change view

automatic notifications are enabled

automatic blocking is enabled

Scenarios

ALL (22) STANDARD (20) DYNAMIC (2)

Scenario Cards:

- Scenario #218: Negative Margin - Sample**
Range Period: Daily (values reset daily at 10:00).
Description: No Description
- Scenario #208: High Rate Calls - Sample**
Range Period: Daily.
Description: checking for A-Number ranges generating high-rate calls
- Scenario #206: Same Duration - Sample**
Range Period: Daily.
Description: checking for A-Number range generating calls with same duration
- Scenario #205: Wangiri - Trap Calls - Sample**
Range Period: Hourly.
Description: checking for A-Number ranges that generate large failed calls on daily bases
- Scenario #204: Fair Usage - Sample**
Range Period: Daily (values reset daily at 00:00 traffic compared to Last 1 Hours).
Description: checking for A-Number that exceeds 250 minutes daily.
- Scenario #203: Sequential A and B Numbers - Sample**
Range Period: 6 Hours.
Description: checking for calls originated from / terminated to sequential number ranges
- Scenario #202: Overlapping Calls - Sample**
Range Period: Daily.
Description: checking for A-Numbers generating concurrent calls

Scenarios List View:

ALL (24) STANDARD (24)

Total items collected: 24

#	Status	Type	Scenario	Range	Description	
1	ENABLED	Standard	#218 - Negative Margin	Periodic Hourly	No Description	...
2	ENABLED	Standard	#206 - Same Duration	Periodic Daily	checking for A-Number range generating calls with same duration	...
3	ENABLED	Standard	#205 - Wangiri - Trap calls	Periodic Hourly	checking for A-Number ranges that generate large failed calls on daily bases	...
4	ENABLED	Standard	#204 - Fair Usage	Periodic Daily traffic compared to Last undefined Hours	checking for A-Number that exceeds 250 minutes daily.	...
5	ENABLED	Standard	#203 - Sequential A and B Numbers	Periodic 6 Hours	checking for calls originated from / terminated to sequential number ranges	...
6	ENABLED	Standard	#202 - Overlapping Calls	Periodic Daily	checking for A-Numbers generating concurrent calls.	...

How to change the scenario view from grid to list:

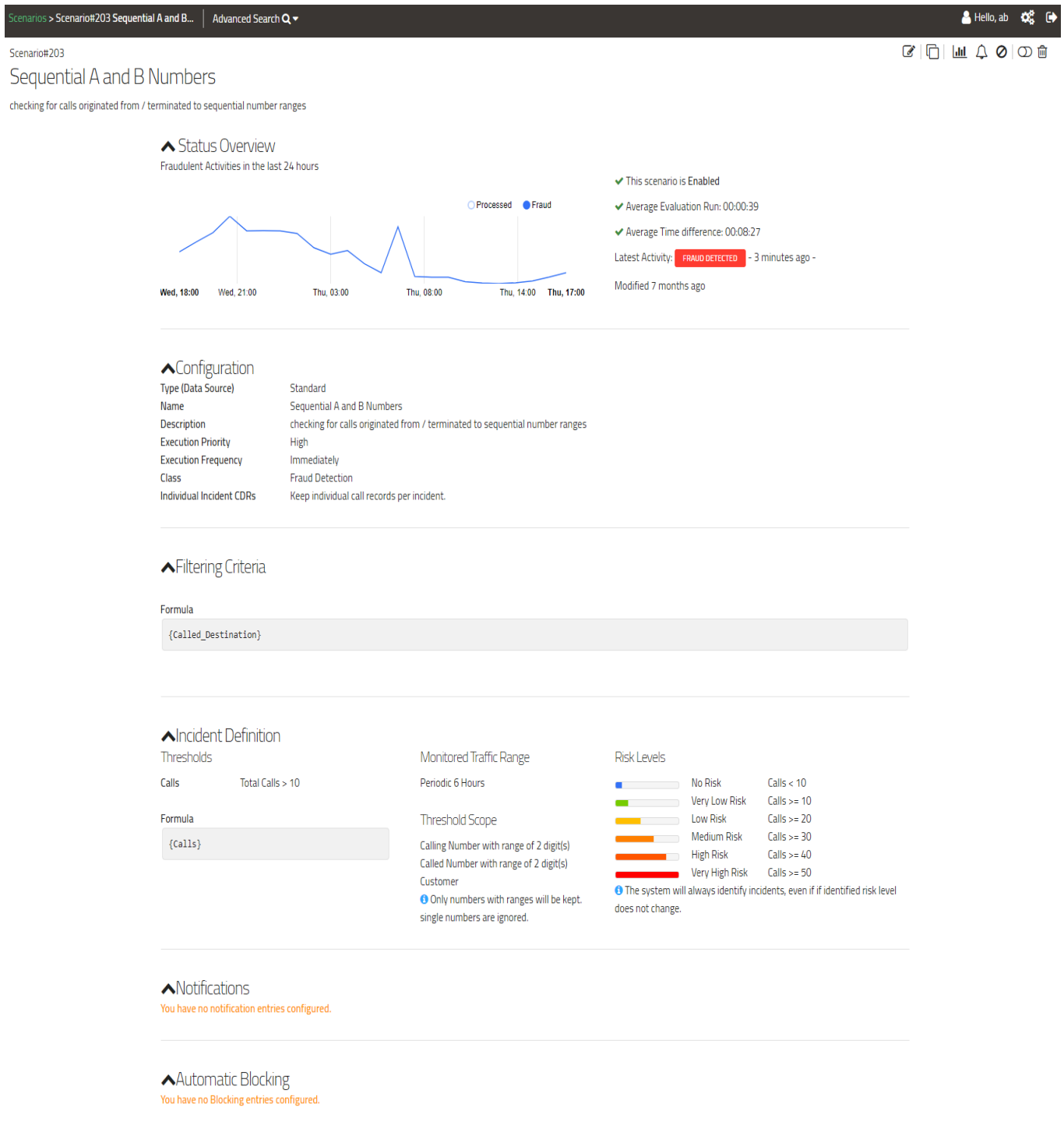
- 1) Open the **Scenarios** menu
- 2) Click on the preferred option in the top right

Actions on this view are:

- add new scenarios
- edit existing scenarios
- duplicate existing scenarios
- enable /disable /delete scenarios
- view scenario details
- view scenario activities
- view scenario notifications
- view items blocked by a scenario
- filter scenarios by specific term
- filter scenarios by used data source (all/standard/ dynamic/live)

3.3 Monitor Scenario Results

The system provides a detailed list of evaluation activities, overview of automated actions (notifications, blockings) per scenario:



The View provides information about the scenario settings as well as a chart displaying the recent activities.

How to see the Scenario Overview

- 1) Open the **Scenarios** menu
- 2) Click on the "list of actions" symbol
- 3) Select **View Scenario**

Actions on the view are shown in the **top right**:

- ➡ Edit /Duplicate Scenarios
- ➡ Enabling/ Disabling Scenarios
- ➡ Delete a Scenario
- ➡ Monitor Scenario Results

The **Scenario View** tab displays the following information:

- Status Overview
- Configuration
- Filtering Criteria
- Incident Threshold
- Threshold Scope
- Monitored Traffic Range
- Risk Levels
- Notification Conditions
- Blocking Conditions

See the **Scenario Setup** section for detailed information.

4 Scenario Setup

To create a standard fraud scenario, the following parameters should be properly defined:

Step 1 - Configuration: the scenario title, category, and a brief description. The scenario description is a readable display of the current scenario setup.

Step 2 - Filtering Criteria: the filtering conditions applied to traffic (e.g. A-/B-number patterns, specific destinations, carriers, or routings). Collected traffic is analyzed and validated.

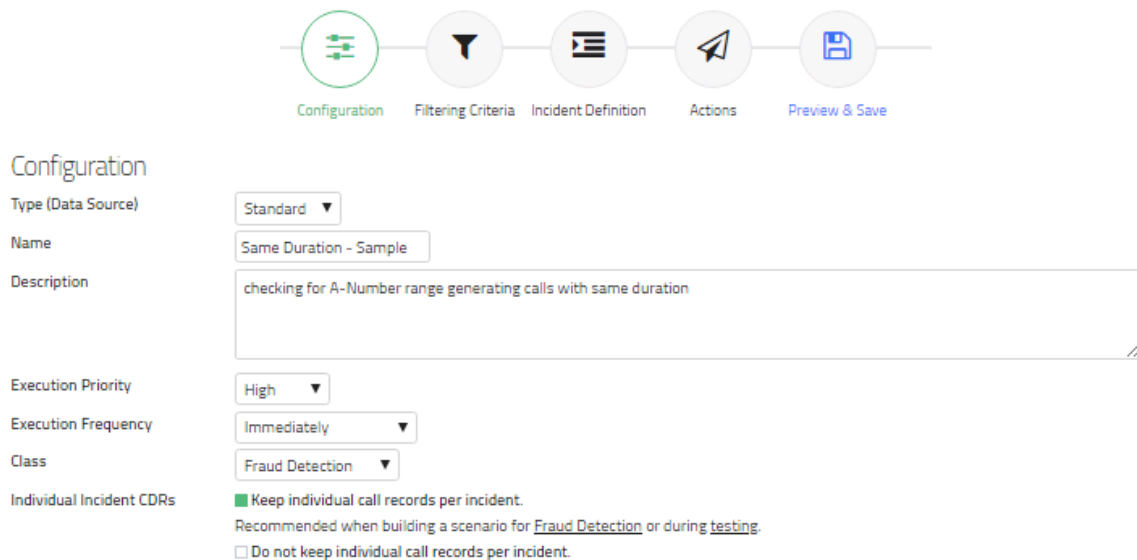
Step 3 - Incident Definition: the thresholds, which identify fraud. The threshold scope elements parameters, e.g. amount of calls per Calling Number, as well as the risk levels.

Step 4 - Actions: Automated actions as email-notifications and blocking based on risk levels.

Step 5 – Preview and Save

4.1 Step 1 – Configuration

The first step focusses on general information and settings of the created scenario.



Configuration

Type (Data Source): Standard

Name: Same Duration - Sample

Description: checking for A-Number range generating calls with same duration

Execution Priority: High

Execution Frequency: Immediately

Class: Fraud Detection

Individual Incident CDRs: ☒ Keep individual call records per incident.
Recommended when building a scenario for Fraud Detection or during testing.
☐ Do not keep individual call records per incident.

Define the general scenario information and settings:

- **Type** (Define on which data source the scenario should apply the configured rules)
- **Name**
- **Description**
- **Execution Priority** (High priority scenarios will be evaluated first)
- **Execution Frequency** (Define whether the scenario should evaluate traffic as soon as it is imported to the system “Immediately”, if it should run on predefined periods “every 15 minutes/ hour/ 6 hours/ 12 hours”, or on predefined times “Daily at 00:00/12:00”, or during weekdays or on weekends)
- **Class/ Purpose (Fraud Detection/ Reporting/ Testing)** This option allows to also setup scenarios which are not intended to detect fraud, therefore the results will not be shown as fraud incidents.
- **Individual Incident CDRs** Define whether the Records which were marked as fraudulent should be saved for specific incidents or not.

4.2 Step 2 - Filtering Criteria

Filters are used to create a subset of the imported traffic. Some scenarios should only be applied for specific destinations, numbers, customer and supplier or should check for successful calls only. Therefore, the filters are applied to either include or exclude specific traffic. When no filter is selected the system checks the whole imported traffic.

Filtering Criteria

▼ Basic Filter Options

☐ Calling Number (0 item(s) selected)

☐ Origination (0 item(s) selected)

☐ Customer (1 item(s) selected)

☐ Routing (0 item(s) selected)

☐ Called Number (0 item(s) selected)

☐ Destination (0 item(s) selected)

☐ Supplier (1 item(s) selected)

▼ Advanced Filter Options

Use comparison operators , , , , , , to set the filter value.

☒ Duration seconds ☐ Release Cause

☐ Total Revenue

☐ Total Cost

☐ Calling Number Length

☐ Called Number Length

☐ Calling Number NOA

☐ Called Number NOA

☐ Diverted Called Number

▼ Filter Lists

☐ Calling Number List (0 item(s) selected)

☐ Called Number List (0 item(s) selected)

☐ Origination List (0 item(s) selected)

☐ Destination List (0 item(s) selected)

☐ Customer List (0 item(s) selected)

☐ Supplier List (0 item(s) selected)

Formula

Use operators **AND**, **OR** and brackets **(,)** to modify filtering conditions!

4.2.1 Basic Filter Options

Basic Filter Options are filters applied on defined values, e.g. filter on destinations, numbers and carriers.

The system provides several parameters that can be used to formulate the filtering criteria.

Each parameter can be included in or excluded from the filtering condition. For example, the CLI filtering fraud scenario would use a typical filtering rule ***Calling Number Exclude (Unknown, 10000%)***. If the fraud scenario focuses on Non-CLI calls, a typical filtering rule would be ***Calling Number Include (Unknown, 10000%)***.

The same is true for destinations, carriers, and other filtering parameters.

The system provides the following filtering criteria:

- **Numbers: *Calling Number / Called Number***

- Filters can be defined based on A-/B-numbers.
- Filters can contain one or more numbers, as well as number patterns (e.g. 49% for all numbers starting with 0049, 49699203943% to focus on all numbers starting with 49699203943).
- Filters can be applied on numbers (e.g. 49%) or text (i.e. 'Unknown' for Non-CLI calls).

☒ Calling Number (0 item(s) selected)

☒ Origination (0 item(s) selected)

☐ Unknown Origination

- **Destinations***: *Origination(s)/Destination(s)*
- **Carrier***: *Customer (Carrier In) / Supplier (Carrier Out)*
- **Routings***

* Information on available Carriers, Routings and Breakouts are displayed in **7.4 Preferences**.

How to set Basic Filter

- 1) Click on the box in front of a specific Filter ■ Origination
- 2) Define whether to include or exclude specific items
- 3) Click on the **Pencil**  to add an entry
- 4) Start typing the details of the item in the **entry Field** below
- 5) Add the **item** to the filter per right click, or write the complete name and press enter

Note: Information on available Carriers, Routings and Breakouts are displayed in **7.4 Preferences**.

How to remove Items from Basic Filter

To delete specific items:

- 1) Click on the Pencil 
- 2) Click on the **x** to **remove single items**
- 3) Click on the trash  to **remove all items**

■ Calling Number

Include ▼ (2 item(s) selected)  

49177% x
49178% x

How to Disable a Basic Filter

You can disable a filter by unchecking the box in front of the filter. The items of this filter will be saved, but the filter itself is disabled.

4.2.2 Advanced Filter Options

Use available SQL comparison operators to build filtering conditions for the following options:

- **Call Duration**
 - **Successful calls**: calls with duration greater than zero seconds.
 - **Failed / zero duration calls**: calls with duration equal to zero seconds.

Advanced Filter Options

☒ Call Duration	>0 seconds
☐ Release Cause	
☐ Call Revenue	
☐ Call Cost	
☐ Calling Number Length	
☐ Called Number Length	
☐ Calling Number NOA	National ▼
☐ Called Number NOA	National ▼
☐ Diverted Called Number	Yes ▼

Note: Whenever a complex filtering formula is required (e.g. calls between 5 and 15 seconds and calls between 100 and 120 seconds), it is recommended to duplicate a scenario and define separate conditions for short-duration and long duration calls.

- **Release Cause**
 - The **call clearing value** (i.e. the status of the call, and how it was terminated).
 - This is a free text field; users can enter the value directly.
 - The system matches the entered value with the values provided in the CDRs.

- **Call Revenue**
- **Call Cost**
- **Calling Number Length**
- **Called Number Length**
- **Calling Number NOA:** The A-number **NOA (Nature of Address)** is the type of the calling (originating) party number — **National** or **International** number.
- **Called Number NOA:** The B-number **NOA (Nature of Address)** is the type of the called (terminating) party number — **National** or **International** number.
- **Diverted Called Number:** including/excluding (**Yes/No**) B-numbers with forwarding indication.

How to set up an Advanced Filter

- 1) Click on the box in front of a specific filter (e.g. Duration) ■ Duration
- 2) Define via SQL comparison operator which values to focus on
- 3) Define a value for x (and y)

Wanted Command	SQL-Comparison Operator
Equals ...	= x
Greater than ...	> x
Less than ...	< x
Greater than or equal to ...	>= x
Less than or equal to ...	<= x
Not Equal to ...	!= x
Not Less than ...	!< x
Not Greater than ...	!> x
Between 2 Values	Between x and y

4.2.3 Filter Lists

Additionally, to the Basic Filters, the system allows also to create Filter Lists which can be used if many items in the Basic Filter would be selected. Those Filter Lists can be managed in the Main-Menu item "Filter Lists".

The usage of filter lists allows updating scenarios which filter on the same entries with one global change, instead of updating each scenario individually. Those lists also allow including / excluding a huge number of items per scenario.

4.2.4 Filtering Formula

Building complex fraud scenarios requires flexible filtering conditions. Therefore, the system allows users to create filtering formulas.

Formula

```
{Called_Destination} AND ({Carrier_Out} OR {Carrier_In})
```

The filtering formula is only available if filtering criteria are selected. By default, all selected parameters are aggregated (**AND**). This means calls have to fulfill all filter conditions to be forwarded to further fraud evaluation.

Example:

A fraud scenario should monitor any traffic coming from a specific carrier (**Carrier In** = AnnaCom) to a specific supplier (**Carrier Out** = FoxCom) on a set of high-risk destinations (**Destinations** = Cuba and Pakistan):

- **Destination:** Include (Cuba, Pakistan)
- **Customer (Carrier In):** Include AnnaCom
- **Supplier (Carrier Out):** Include FoxCom

By default, these conditions are matched together:

{Called_Destination} and {Carrier_In} and {Carrier_Out}

As a result, all evaluated CDRs have 'Cuba or Pakistan' as **Destinations** and 'AnnaCom' as **Carrier In** and 'FoxCom' as **Carrier Out**.

However, users may need to filter traffic with 'Cuba or Pakistan' as **Destinations** and 'AnnaCom' as **Carrier In** or 'FoxCom' as **Carrier Out**. In this case, the users define the following formula:

{Called_Destination} AND ({Carrier_In}) OR {Carrier_Out}

4.3 Step 3 - Incident Definition

4.3.1 Overview

In the **Incident Definition** users define the conditions, which identify fraud.

As filtering criteria determine a subset of traffic, **Incident Definitions** determine whether the evaluated traffic is actually *fraud* or not.

The screenshot shows the 'Incident Definition' configuration interface. It includes sections for 'Monitored Traffic Range', 'Thresholds', 'Threshold Scope', and 'Risk Levels'.

- Monitored Traffic Range:**
 - Range: Periodic (selected), Daily
 - Use 'top of the hour' range: ☐
 - Use Accumulative values. Reset calculations at: ☐
 - Type: Absolute
- Thresholds:**
 - Frequency: ☐ Calling Number Count: < 0
 - Calls:** ☒ Total Calls: > 99
 - Duration: ☐ Total Duration: < 0 seconds
 - Revenue: ☐ Total Revenue: < 0
 - Cost: ☐ Total Cost: < 0
 - Margin: ☐ Total Margin: < 0
 - ASR: ☐
 - Connections: ☐ Source Connections: < 0
- Threshold Scope:**
 - Calling Number: ☒ with range of 2 digit(s)
 - Called Number: ☐ with range of digit(s)
 - Ignore single numbers: ☐
 - Origination: ☐
 - Destination: ☐
 - Customer: ☐
 - Supplier: ☐
 - Routing: ☐
- Risk Levels:**
 - Records: ☐
 - Threshold: No Risk (Records < 100), Very Low Risk (Records >= 100), Low Risk (Records >= 110), Medium Risk (Records >= 150), High Risk (Records >= 200), Very High Risk (Records >= 250)
 - Identify incidents only when reached risk level changes: ☒
 - Always identify incidents even if reached risk level does not change: ☐

4.3.2 Monitored Traffic Range

The monitored traffic range defines which traffic is included in the evaluation, e.g. "Hourly" -> all CDRs that matched the Filtering Criteria within the last hour are evaluated.

Monitored Traffic Range

Range: Periodic (selected), Hourly

Type: Absolute

The incident evaluation is applied on traffic (CDRs) within the defined period (e.g. hourly, daily, weekly ...).

The system allows creating scenarios with moving ranges (Periodic) and scenarios with fixed ranges.

Fixed Date

Fixed date ranges are used to evaluate:

- (1) Traffic from the past and
- (2) Traffic until a specific date in the future.

Monitored Traffic Range

Range: Fixed Date (selected) between 2018-03-01 00:00 and 2018-03-07 00:00

Periodic

Periodic ranges are used to continuously evaluate the traffic with a fixed period.

The period ranges:

Monitored Traffic Range

Range Periodic Hourly

- **Hourly:** the system identifies the last (maximum) hour in the filtered traffic and calculates the incident definitions based on traffic of 1 hour. The timeframe is between the last hour and 1 hour before.
- **4, 6, 12 Hours:** the system identifies the last (maximum) hour in the filtered traffic and calculates the incident definitions based on traffic of 4, 6, or 12 hours. The timeframe is between the last hour and 4, 6, or 12 hours before.
- **Daily:** the system identifies the last (maximum) hour in the filtered traffic and calculates the incident definitions based on traffic of 24 hours. The timeframe is between the last hour and 24 hours before.
- **Weekly:** the system identifies the last (maximum) day/hour in the filtered traffic and calculates the incident definitions based on traffic of 1 week (from the last identified day/hour). The timeframe is between the last day/hour and 1 week before.
- **Monthly:** the system identifies the last (maximum) day/hour in the filtered traffic and calculates the incident definitions based on traffic of 1 month (from the last identified day/hour). The timeframe is between the last day/hour and 1 month before.

Monitored Traffic Range

Range Periodic Daily

☐ Use 'top of the hour' range

☐ Use Accumulative values. Reset calculations at

'Top of the Hour'

This option allows only considering the calculates range beginning from the start of each hour and ignoring minutes and seconds (HH:00:00).

Use Accumulative values. Reset calculations at

This function enables a calculator, which accumulates the values in the defined period and resets the calculation at a defined date. This option can be used to monitor e.g. fair usage of retail customer.

4.3.3 Incident Types

There are three ways to identify fraud attacks:

1. Values exceed a defined threshold (**Absolute Incidents**)
2. Traffic increases/decreases drastically compared to a previous period (**Comparative Incidents**)
3. Values for predefined items (scope elements) exceed thresholds (**Threshold Lists**)

1. **Absolute Incidents:** the fraud evaluation is based on absolute traffic values, such as total number of calls, duration, or ASR (e.g. 1000 minutes, 52% ASR, etc.).
2. **Comparative Incidents:** the fraud evaluation is based on traffic changes compared to a certain period (e.g. previous hour, day, etc.).
3. **Threshold Lists:** are used to define threshold values per scope element (e.g. Destination Germany-Mobile is less critical than Cuba-Mobile. Therefore, users can define individual incident thresholds: Germany-Mobile > 200.000 calls and Cuba-Mobile > 1.000 calls)

Users can define the following comparison **Period Types**:

- **Fixed Date.**
- **X Last Hours, Days, or Months:** users define the **X** value (e.g. 1 hour, 2 days, etc.).
- **Same Day Last Week:** the current values are compared to the values for the same period of the same day (e.g. Monday) the previous week.

Note: Incident Thresholds of **comparative scenarios** are not written as decimals! **5% = 5**

Format of Threshold Lists

Threshold lists can only be uploaded in csv-format.

The first row always needs to include the header. Correct header names are as follows:

For the Scope Elements: Origination = org

Destination = trm

Customer = cust

Supplier = supp

For the Incident Thresholds: Calls = calls

Duration = duration

Revenue = revenue

Cost = cost

Margin = margin

ASR = asr

The header needs to be created based on the selected fields in the Threshold List configuration (Scope Element; Incident Threshold).

org;cust;calls;minutes

Germany-mobile;Test-Carrier;1000;5000

4.3.4 Incident Thresholds

Incidents can be defined by one or more of the following parameters.

Note: If none of the scope parameters is selected the scenario can't be saved, therefore we added a red frame around this part.

Frequency

The number of unique calls (i.e. CDRs) from a calling number / to a called number is measured as follows:

- **Calling Number Count:** the peak number of unique calling numbers to the same called number made for the defined monitoring period (e.g. 50 calls).
- **Called Number Count:** the peak number of unique called numbers from the same calling number made for the defined monitoring period (e.g. 50 calls).

Thresholds

☒ Frequency

Calling Number Count > 50

Calls

The number of **Calls** (i.e. CDRs) is measured as follows:

- **Total Calls:** the total number of calls, either successful or failed / zero duration, or both, depending on the filtering criteria specified (e.g. 1000 calls).

☒ Calls

☐ Duration

☐ Revenue

☐ Cost

Total Calls	>	50
Total Calls	<	0
Concurrent Calls	<	0
Calls with same duration	<	0
Overlapping Calls	<	0

- **Concurrent Calls:** calls started within the same minute. Normally, the maximum value is 3 calls, whereas automatic dialers are able to produce hundreds calls within a minute.
- **Calls with same duration:** the peak number of calls with the same call duration for the given monitoring period (e.g. > 200 calls/duration). Dialing machines tend to produce numerous calls within the same duration range (i.e. if the dialer is set up to make calls with duration less than a minute, the duration is suspicious as it is around 56 seconds).
- **Overlapping Calls:** or looped calls (loops), are multiple call attempts to the same B-number that overlap one another.

Duration

The call **Duration** value is measured as follows:

- **Total Duration:** the sum of duration values of all filtered calls expressed in seconds or minutes (e.g. 1000 seconds).

☒ Duration

Total Duration > 20 seconds

- **ACD (in seconds):** the calculated **Average Call Duration** value based on the filtered traffic.

☒ Duration

ACD = 10 seconds

Revenue

The traffic **Revenue** value is measured as follows:

- **Total:** the sum of all revenue values of the filtered traffic (e.g. 1000 EUR).
- **Rate per minute:** the revenue per minute value. It is calculated as Total Revenue / Total Duration.

Cost

The traffic **Cost** value is measured as follows:

- **Total:** the sum of all cost values of the filtered traffic (e.g. 1000 EUR).
- **Rate per minute:** the cost per minute value. It is calculated as Total Cost / Total Duration.

Margin

The **Margin** value is measured as follows:

- **Total:** the sum of all margin values of the filtered traffic (e.g. 1000 EUR).
- **Rate per minute:** the margin per minute value. It is calculated as Total Margin / Total Duration.

ASR

ASR (Answer Seizure Ratio) is quality traffic characteristic. It is expressed as the percentage of successful calls with respect to the total calls of the filtered traffic.

The **ASR** value is measured as follows:

- **Supplier ASR:** the ASR value is expressed as a percentage value (e.g. ASR <60%).
- **Customer ASR:** normally, users define the supplier ASR value, but in some cases, depending on the switch settings, there can be a difference between the supplier ASR and the customer ASR.

NOTE:

Unless otherwise specified, the Call Duration filter on the **Filtering Criteria** screen by default is set to consider both successful and failed / zero duration calls. This is a mandatory condition for correct calculation of the **ASR** value.

Connections

- **Source Connections:** define a condition for a number of source (calling) IPs.
- **Termination Connections:** define a condition for a number of terminations (called) IPs.

■ Connections Source Connections ▾ > ▾ 5

4.3.5 Incident Formula

Building complex fraud scenarios requires flexibility in definition of incident parameters. The system allows users to construct logical formulas using the selected parameters.

See the **Filtering Formula** section for more information.

Formula

{Margin} AND {Revenue} AND {Duration}

4.3.6 Threshold Scopes

The Threshold Scope defines on which elements the Incident Thresholds should be accumulated. Therefore, those two settings are highly dependent.

Incident Threshold selected	Threshold Scope selected	Interpretation
Yes	No	ERROR On which element should the system calculate the values?
No	Yes	ERROR What should be checked as fraud?
Yes	Yes	The system will check the Incident threshold PER Threshold Scope

4.3.6.1 Definition of Threshold Scope Elements

- **Calling Number:** incident thresholds are aggregated per calling number. The system can also focus on **ranges only**, where **single numbers will be ignored**, using the **ignore single numbers** function.

Threshold Scope

☒ Calling Number [☒ with range of 2 digit(s)]

☒ Called Number [☒ with range of 2 digit(s)]

☒ Keep ranges only numbers with ranges will be kept. single numbers will be ignored.

- **Called Number:** incident thresholds are aggregated per called number.
- Entering the '1 digit' value means applying the incident definition values to the called number range of 10 numbers (i.e. from 0 to 9), entering '2 digits' — to the range of 100 numbers (i.e. from 00 to 99), etc. The system can also focus on **ranges only**, where **single numbers will be ignored**, using the **Keep ranges only** function.
- **Origination:** incident thresholds are aggregated per origination.
- **Destination:** incident thresholds are aggregated per destination.
- **Customer (Carrier In):** incident thresholds are aggregated per customer.
- **Supplier (Carrier Out):** incident thresholds are aggregated per supplier.
- **Routing:** incident thresholds are aggregated per routing.

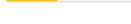
4.3.7 Risk Levels

Risk Levels are used to classify the identified fraud. Therefore, Risk Levels **should not** be smaller than the Incident Threshold, since the classification in risk levels is applied after the Incident Threshold was reached.

Risk Levels are also used to define the automated actions done by the system, e.g. send e-mail notification when specific risk level is reached and block specific items. The system allows setting up multiple actions per scenario, e.g. send e-mail notifications with varying content to different departments at the same risk level, add an additional department when the fraud attack is ongoing and add multiple blocking conditions with varying blocking periods. This way risk levels are a helpful setting to accomplish an escalation plan for fraud attacks.

Risk Levels

Threshold Calls Increasing

	No Risk	Calls < 6
	Very Low Risk	Calls ≥ 6
	Low Risk	Calls ≥ 10
	Medium Risk	Calls ≥ 15
	High Risk	Calls ≥ 20
	Very High Risk	Calls ≥ 50

Risk levels can be applied on **Calls**, **Minutes**, **Revenue**, **Cost**, or **Margin**.

Increasing/ Decreasing: The rise of Risk Levels can be set up to be for increasing or decreasing values.

For example an **decrease of margin** should cause a rise of risk levels, as well as an **increase of costs**.

Note: By default, the risk levels are configured to send alerts as soon as the system evaluated the traffic and the defined risk levels (in combination with the notification-configurations) were reached. The system also allows to **send notifications only if the risk level changes**.

4.4 Step 4 – Actions

4.4.1 Notifications

The system can issue fraud alerts when the incident threshold and a selected risk level is reached.

Yet, there is an internal system condition stating that if the last generated alert is older than 24 hours, then the system generates an alert irrespective of whether the threshold value changes or not. That means that every 24 hours the system generates at least one alert.

4.4.2 Blocking Conditions

The **Blocking Conditions** settings allow users to define a blocking condition and items to be blocked, as well as a blocking period.

^ Blocking Add Entry

Very Low Risk or higher Blocking for the combination values of: Blocking for period of: 6 Hour

 Called Number,  

In the **Automatic Blocking Setup** dialog specify and save the following parameters:

- **Minimum Risk Level:** all items identified at lower risk levels are ignored, but at the selected risk level or higher, those items get automatically blocked.
- **Blocking Period:** as soon as the period ends, the items are automatically released.

- **Blocking Elements:** selected elements get blocked once the minimum risk level is reached.
- **Block as Incoming:** By default, Calling Numbers are blocked as Incoming, which means block the A-Number as A-Number. The blocking can also be modified to block an A-number as Outgoing. The system will block the identified A-Number, whenever this Number appears as B-number. Vice versa for Called Number.
- **Block range of digits:** The AFS can also block number sequences up to 4 digits for one identified Number (e.g. if +1 234 567 89 was identified as fraudulent, the system can block all calls which include the number: +1 234 5xx xx)

New Block Entry

Risk (at what level) Very Low Risk or higher Action Period (for how long) 1 Hour

Action Fields

☒ Calling Number
Block as Incoming ☐ Block range of 1 digit(s)

☒ Called Number
Block as Outgoing ☐ Block range of 1 digit(s)

☐ Origination
☐ Destination
☐ Customer

! When two or more fields are selected, the system will block traffic with the values of combined elements allowing all other combinations.
To block all traffic for a certain field (e.g. Number, or Destination, or Carrier), select that field only.

SAVE

To block all traffic for a certain element (e.g. **Calling Number**, **Destination**, or **Carrier**) select the required parameter only. If two or more elements are selected simultaneously (e.g. **Calling Number and Destination**), the system only blocks traffic for the combined items (e.g. **Calling Number to Destination**), allowing the traffic for other A-numbers and destinations.

Note: Multiple blocking conditions can be created to establish an escalation plan.

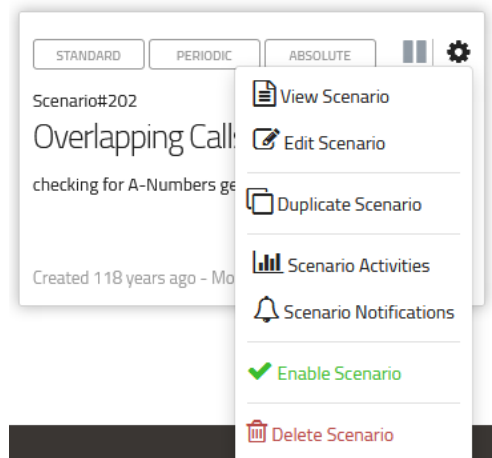
5 Scenario Management

5.1 Edit, Duplicate or Delete a Scenario

To edit an existing scenario, click the **Gearwheel** on the **Scenarios** menu.

The **Edit Scenario** function allows modifying the scenario settings. Make the necessary changes to the scenario and save the new definitions. See below the Add a New Scenario section for detailed information.

Duplicate Scenario allows copying the definitions of an existing scenario to apply slightly different changes without starting from scratch. Users can make necessary modifications to the duplicated scenario and activate the copied scenario.



By default, a duplicated scenario is named as **Original Scenario Title [Copy]** and is not active, even if the original scenario is active.

To delete a scenario, click on the **Delete** button. Before the action is performed, the system displays a **Warning** message. Confirm the message to permanently remove the scenario.

Confirm

Are you sure you want to mark this scenario for deletion?

OK

CANCEL

Note: After confirming the deletion, scenarios will be stored for 24h to undo the deletion. After 24 hours the scenario will be deleted from the system.

5.2 Add a New Scenario

To create a new scenario, click on the **Add New** button in the top-right corner of the **Scenarios** screen.

+ New Item

See the Scenario Setup for detailed configuration options.

6 Scenario Options

6.1 Activities

The system evaluated periodically new traffic for fraud. Activities are detailed evaluation information for each activated scenario.

The status of each activity provides information about the evaluation result.

Status	Interpretation
NO RISK IDENTIFIED	CDRs didn't reach the incident threshold and minimum risk level
NO NEW TRAFFIC	1) CDRs didn't match the filter criteria 2) Scenario is set up to run at specified periods and no new traffic was imported since last evaluation run
FRAUD DETECTED	Incident Threshold and minimum risk level were reached
NO NEW INCIDENTS	Amount of Calls, Minutes, Revenue and Cost didn't change since last fraud detection

6.1.1 Activity List

The Activity List shows 100 items from a selected time range and provides information about the Status, the Traffic Range and the Evaluation Result.

#	Status	Scenario	Traffic Range	Result	Last Update
1	FRAUD DETECTED	Standard - Wangiri - Trap calls	2018-02-14 08:00:00 - 2018-02-14 08:59:59	10 incidents identified (86,267 records checked). (205x1802140915118811)	a year ago
2	FRAUD DETECTED	Standard - Wangiri - Trap calls	2018-02-14 08:00:00 - 2018-02-14 08:52:10	2 incidents identified (48,969 records checked). (205x1802140900088420)	a year ago
3	FRAUD DETECTED	Standard - Wangiri - Trap calls	2018-02-14 08:00:00 - 2018-02-14 08:37:10	1 incidents identified (31,400 records checked). (205x1802140845107040)	a year ago
4	FRAUD DETECTED	Standard - Wangiri - Trap calls	2018-02-14 02:00:00 - 2018-02-14 02:59:59	1 incidents identified (7,584 records checked). (205x1802140830377964)	a year ago
5	FRAUD DETECTED	Standard - Wangiri - Trap calls	2018-02-14 03:00:00 - 2018-02-14 03:59:59	4 incidents identified (7,628 records checked). (205x1802140830377965)	a year ago
6	FRAUD DETECTED	Standard - Wangiri - Trap calls	2018-02-14 04:00:00 - 2018-02-14 04:59:59	1 incidents identified (6,219 records checked). (205x1802140830377964)	a year ago
7	FRAUD DETECTED	Standard - Wangiri - Trap calls	2018-02-14 05:00:00 - 2018-02-14 05:59:59	1 incidents identified (7,720 records checked). (205x1802140830377963)	a year ago
8	FRAUD DETECTED	Standard - Wangiri - Trap calls	2018-02-14 06:00:00 - 2018-02-14 06:59:59	1 incidents identified (16,656 records checked). (205x1802140830377962)	a year ago
9	FRAUD DETECTED	Standard - Wangiri - Trap calls	2018-02-14 07:00:00 - 2018-02-14 07:59:59	5 incidents identified (53,149 records checked). (205x1802140830377961)	a year ago
10	NO RISK IDENTIFIED	Standard - Wangiri - Trap calls	2018-02-14 08:00:00 - 2018-02-14 08:22:07	0 incidents identified (16,576 records checked).	a year ago
11	NO RISK IDENTIFIED	Standard - Wangiri - Trap calls	2018-02-14 07:00:00 - 2018-02-14 07:57:10	0 incidents identified (18,937 records checked).	a year ago

Reference Number: the reference number is a unique number for each activity. The first digits include the scenario ID and the last digits are generated automatically. The reference number is always included in the email notifications.

6.1.2 Incident List

The Incident List shows 100 occurred incidents from a selected time range and provides information about the Risk Level, Incident and Detection Time.

#	Risk Level	Scenario	Src	Dst	Customer	Supplier	Calls	Dur	ACD	ASR	Rev.	Cost	Mrgn.	Last Update
1		TEST - monitor extensions	0040	19	Unknown_Carrier	Unknown_Carrier	6	00:06:44	00:01:07	100,00%	0,00 €	0,00 €	0,00 €	12 days ago

6.1.3 Activity Details

Activity Details can be opened for Activities with the status "Fraud Detected". Those details are split into three sub menu items:

- 1) Incidents
- 2) Call Records
- 3) Processed Traffic

See Fraud Records

Activities: 205x180214091511811 | Advanced Search

Incidents | Call Records | Processed Traffic | **See Evaluated Records**

These are the identified incidents

Overview

Traffic range between 2018-02-14 08:00:00 and 2018-02-14 08:59:59 contained 86,267 (19.29 MB) records that matched the filtering criteria.

Result:
10 incidents [2,105 records, 2.44% of matched records] were identified, as potentially fraudulent.

The system evaluated the traffic at 2018-02-14 09:15:12 (a year ago) and it took 15 seconds to finish.

Risk Overview

Risk Level	Calls	Minutes	Revenue	Cost
Very Low Risk	907	1,043	\$36.40	\$8.83
Low Risk	784	768	\$25.95	\$6.27
Medium Risk				
High Risk	414	170	\$8.12	\$1.40
Very High Risk				

Incident List

Total items collected: 10

#	Risk Level	Src	Dst	CarrierIn	CarrierOut	RoutingType	Calls	Dur	ACD	ASR	Rev.	Cost	Mgn.		
1	Very Low Risk	49823899070	National	497962700608	National	Faxquote Carrier	Wayne Enterprises Carrier	Default Routing	414	02:49:35	00:00:31	77.54%	\$8.12	\$1.40	\$6.72
2	Low Risk	49921162740	National	493578349422	National	Groovestreet Telecom	VoiceCom Kinnamplus	SONUS3	275	03:12:24	00:00:56	74.18%	\$5.34	\$1.25	\$4.09
3	Low Risk	49911660280	National	496966711	National	Groovestreet Telecom	VoiceCom Plusunin	SONUS3	270	03:23:43	00:01:07	67.41%	\$5.68	\$1.47	\$4.21
4	Low Risk	499131860	National	4991318523231	National	Groovestreet Telecom	Ezfel Green-Plus	SONUS3	239	06:11:55	00:02:06	73.64%	\$14.93	\$3.55	\$11.38
5	Low Risk	499119740	National	4998254862	National	Groovestreet Telecom	VoiceCom Kinnamplus	SONUS3	192	05:10:35	00:02:05	77.60%	\$10.78	\$2.75	\$8.03
6	Low Risk	4991118097397	National	495541996390	National	Groovestreet Telecom	VoiceCom Kinnamplus	SONUS3	165	01:11:11	00:00:32	79.39%	\$1.69	\$0.16	\$1.53
7	Low Risk	4991142360	National	491784578494	National	Groovestreet Telecom	VoiceCom Bubba Gump	SONUS3	158	03:40:07	00:01:49	76.58%	\$9.65	\$2.28	\$7.37
8	Low Risk	4991197040	National	49660282245	National	Groovestreet Telecom	Groovestreet Telecom	SONUS3	157	03:50:06	00:01:51	78.98%	\$8.97	\$2.15	\$6.82
9	Low Risk	49911586010	National	496421516	National	Groovestreet Telecom	Groovestreet Telecom	SONUS3	124	02:17:18	00:01:32	71.77%	\$3.44	\$0.94	\$2.50
10	Low Risk	499128921649	National	49922797007	National	Groovestreet Telecom	VoiceCom Kinnamplus	SONUS3	111	01:13:48	00:00:50	78.38%	\$1.87	\$0.55	\$1.32

Mask Numbers

☐ Mask Phone Numbers

Block Permanently
Add to Ignore List
Add to Allowed List

To open the Activity Details, click on the green highlighted **arrow** next to the incident or on the **Reference Number** in the **Activity List**.

6.1.3.1 Incidents per Activity

The sub menu **Incidents** provides detailed information about the evaluation run which identified at least one incident.

Provided Information:

- Which time range was evaluated?
- How many records matched the filtering criteria?
- How many incidents were identified?
- System Performance (How long did the evaluation take?)
- Which risk levels were reached?
- How many Calls, Minutes, Revenue and Cost per risk level
- Detailed information of each incident

The **Incident List** provides detailed information regarding the source, destination, customer, supplier, amount of calls, total duration ...

Items in this list can be **blocked manually**, added to the **allowed items list** (evaluated, but never blocked) or to the **ignored items list** (not evaluated).

0,00 € 0,00 €

☐ Block Permanently

☐ Add to Ignore List

☒ Add to Allowed List

6.1.2.3 Call Records per Activity

Call Records are the records identified as fraudulent (based on the scenario configuration). Therefore, each activity with the status **“fraud detected”** provides the **list of fraudulent calls** in the sub-menu **“Call Records”**.

Incidents **Call Records** Processed Traffic

Q find in list 

These are the records used at the time of detection
Total items collected: 100

☐ Mask Phone Numbers ☐ Automatically Load All Items

#	Src	Dst	Time	Dur	Org	Trm	CarrierIn	CarrierOut	Rev.	Cst.	Margin
1	+9823899***	+97962700***	2018-03-13 23:59:53	00:09:29	National	National	VoiceCom Acme Corporation	Treequote Telecom	\$0.20	\$0.19	\$0.01
2	+9823899***	+97962700***	2018-03-13 23:59:46	00:09:06	National	National	VoiceCom Acme Corporation	Treequote Telecom	\$0.19	\$0.18	\$0.01
3	+9823899***	+97962700***	2018-03-13 23:59:43	00:19:54	National	National	VoiceCom Acme Corporation	Treequote Telecom	\$0.42	\$0.40	\$0.02
4	+9823899***	+97962700***	2018-03-13 23:59:28	00:12:37	National	National	VoiceCom Acme Corporation	Treequote Telecom	\$0.26	\$0.26	\$0.00
5	+9823899***	+97962700***	2018-03-13 23:59:26	00:13:48	National	National	VoiceCom Acme Corporation	Treequote Telecom	\$0.29	\$0.28	\$0.01
6	+9823899***	+97962700***	2018-03-13 23:58:41	00:13:05	National	National	VoiceCom Acme Corporation	Treequote Telecom	\$0.27	\$0.27	\$0.00
7	+9823899***	+97962700***	2018-03-13 23:58:33	00:09:25	National	National	VoiceCom Acme Corporation	Treequote Telecom	\$0.20	\$0.19	\$0.01
8	+9823899***	+97962700***	2018-03-13 23:58:32	00:30:30	National	National	VoiceCom Acme Corporation	Treequote Telecom	\$0.64	\$0.62	\$0.02

Use the **Export** option to download the records as **.csv** file.

6.1.2.4 Processed Traffic per Activity

The sub-menu **“Processed Traffic”** lists all records, which matched the scenarios filtering criteria and therefore got evaluated during the evaluation run of the activity.

How to add incident items to the block/ ignore/allow list

- 1) Open the activity details view (either by clicking on the reference number or from the Activity List)
- 2) Open the sub-menu **“Incidents”**
- 3) Click on the **List of Actions Button**  next to the specific incident
- 4) Select an option: **“Block Permanently”**, **“Add to Ignore List”**, **“Add to Allowed List”**

How to export fraudulent records as .csv file

- 1) Open the activity details view (either by clicking on the reference number or from the Activity List)
- 2) Open the sub-menu **“Call Records”**
- 3) Click on **Export** in the top right

6.2 Call Records

6.2.1 Call Records

Call Records are the **records identified as fraudulent** (based on the scenario configuration).

The **Call Records** menu provides the aggregation of all Call Records for each Activity.

Call Records Processed Traffic

Standard Q find in list 

Total items collected: 100

☐ Mask Phone Numbers

#	Src	Dst	Time	Dur	Org	Trm	CarrierIn	CarrierOut	Rev.	Cst.	Margin
1	8613467745123	386492900456	2018-02-14 08:13:01	00:00:07	China Mobile	Slovenia Mobile IPKO	Ezfel Bioholding	Ezfel Data	\$0.12	\$0.02	\$0.10
2	8613467745123	386492900456	2018-02-14 08:12:42	00:00:04	China Mobile	Slovenia Mobile IPKO	Ezfel Bioholding	Ezfel Data	\$0.07	\$0.01	\$0.06
3	8613467745123	386491119456	2018-02-14 08:11:56	00:00:10	China Mobile	Slovenia Mobile IPKO	VoiceCom Soyilent Corp	Ezfel Data	\$0.17	\$0.04	\$0.13
4	971561052123	919847559456	2018-02-14 08:11:40	00:03:57	United Arab Emirates Mobile	India Mobile Others	VoiceCom Soyilent Corp	VoiceCom Acme Corporation	\$0.15	\$0.05	\$0.10
5	8613467745123	386491119456	2018-02-14 08:11:31	00:00:09	China Mobile	Slovenia Mobile IPKO	Ezfel Bioholding	Ezfel Data	\$0.15	\$0.04	\$0.11
6	8613467745123	386491119456	2018-02-14 08:10:47	00:00:00	China Mobile	Slovenia Mobile IPKO	VoiceCom Soyilent Corp	Ezfel Data	\$0.00	\$0.00	\$0.00

Use the **Export** option to save the grid data as a **.csv** file.

6.2.2 Processed Traffic

The sub-menu **“Processed Traffic”** lists all records, which matched the scenarios filtering criteria and therefore got evaluated.

6.3 Notifications

The system can send automated email notifications regarding fraud activities. Those notifications are set up in the scenario configuration. This menu lists all notifications sent by the system. The option “Always identify incidents even if reached risk level does not change” in the scenario configuration (Step 3) enables notifications regarding incidents, which were already identified and alerts notifications were already sent **BUT** they are also sent even if the risk level does not change. Instead they are sent if one of the following parameters changed since last evaluation: Amount of calls, minutes, revenue or cost.

Notifications List

Total items collected: 22

Search within list:

1 Low Risk Fraud Alert - [Wangiri - Trap calls] - Ref# 205x1802121130452072
Ref# 205x1802121130452072 fraud@example.com 2018-02-12 11:31:31 (a year ago)

Show/Hide Notification Body

Dear Partner, The following potentially problematic traffic has been detected with the following condition(s): Total Calls > 100 These conditions are applied on the combination of the following scope element(s): Origination, Calling Number Here is more details: Detection : 2018-02-12:11:31: Traffic : between 2018-02-12 09:00 and 2018-02-12 09:59: Majority of Traffic is ranked with Risk Level#2 (of 5 risk levels) with total volume of 218 calls and total duration 415.12. Below is 2 records that are ranked with highest Risk Level reached (Risk Level#2)

Records#2/2:

Calling Number: 499118826 - National

Calls: 218
ACD: 362.79
Records#2/2:

Calling Number: 4991223800 - National

Calls: 119
ACD: 112.52

**** This alert was generated by * AnnaCon * Scenario#205 [Wangiri - Trap calls] * Ref# 205x1802121130452072 **** Best Regards

***** Attachments *****

activity_details_205x1802121130452072.csv: contains activity details based on selected notification elements

2 High Risk Fraud Alert - [Wangiri - Trap calls] - Ref# 205x1802121130452071
Ref# 205x1802121130452071 fraud@example.com 2018-02-12 11:31:05 (a year ago)

3 Very High Risk Fraud Alert - [Wangiri - Trap calls] - Ref# 205x1802121115595670
Ref# 205x1802121115595670 fraud@example.com 2018-02-12 11:16:14 (a year ago)

Those notifications are sent to defined e-Mail addresses and can also be viewed in the Notifications List in the Web Interface.

The **Notification Details** screen includes the **Reference** area with the **Scenario** title and the activity **Reference Number**.

How to open Activity Details from Notifications Menu

- 1) Open the Notifications menu
- 2) Click on the Reference Number to get forwarded to the **Activity Details**

How to expand notification information

- 1) Open the Notifications menu
- 2) click on its **Show** button

7 Fraud Prevention

7.1 Blocked Items

The **Blocked Items** menu provides the list of all items blocked automatically by scenarios and manually by user.

7.1.1 Automatic Blocking

The Automatic Blocking Screen provides a list of all Items blocked by the system. Items are blocked automatically for a **Blocking Period** defined in the scenario **Automatic Blocking Setup** dialog. See the Blocking Conditions section for more information.

7.1.2 Permanent Blocking

Users can also add items manually. Such items are blocked for the **Blocked Period** defined in the **Manual Blocking Entry** dialog.

In the **Blocked Items Menu**, they are listed in the **Permanent Blocking Screen**.

7.1.3 Blocking History

All blocking commands forwarded to the switch(es) are stored in the Blocking history tab.

How to see Activity Details for Blocking History

- 1) Open the Blocked Items menu
- 2) Click on Blocking History in the sub-menu
- 3) Mouse over the Activity Reference Number
- 4) Click on 

How to see all Blocking Commands created by a specific activity

- 1) Open the Blocked Items menu
- 2) Click on Blocking History in the sub-menu
- 3) Mouse over Activity Reference Number in the shown list
- 4) Click on the filter icon 

How to exclude all Blocking Commands created by a specific activity

- 1) Open the Blocked Items menu
- 2) Click on Blocking History in the sub-menu
- 3) Mouse over Activity Reference Number in the shown list
- 4) Click on the filter-out icon 

How to see Setup of scenario which triggered an automatic blocking

- 1) Open the Blocked Items menu
- 2) Click on Blocking History in the sub-menu
- 3) Mouse over the Scenario Name
- 4) Click on 

How to see all Blocking Commands triggered by a specific scenario

See "How to see all Blocking Commands created by a specific activity" **mouse over scenario** instead of Activity Reference Number.

How to exclude all Blocking Commands created by a specific scenario

See "How to exclude all Blocking Commands created by a specific activity" **mouse over scenario** instead of Activity Reference Number.

7.1.4 Active/ Pending/ Expired Items

The system provides also the status of blocking. Therefore, select in the sub-menu which items to be displayed.

Status of Blocking	Interpretation
Active	The blocking is still effective on the switch
Pending	
Expired	Blocking is already released

How to block Items manually based on external information

- 1) Select **Blocked Items** in the menu
- 2) Click on **Permanent Blocking**
- 3) click on the **New Item** button in the top-right corner

 + New Item

The **Manual Blocking Entry** window opens.

- 4) Enter a **Calling Number** and/or a **Called Number**, select the necessary criteria (**Origination**, **Destination**, **Customer**, and/or **Supplier**); define the **Blocked Period**, and add **Comments**.
- 5) **Save** entry

Block Item

Calling Number add number or prefix	Called Number add number or prefix
Origination add breakout	Destination add breakout
Customer add carrier	
Valid To  click to select a date	
Notes 	

 SAVE

How to release automatic blocked items

- 1) Select **Blocked Items** in the menu
- 2) Click on **Automatic Blocking**
- 3) Click on the lock icon to release specific items manually

7.2 Ignored Items

Ignored Items will **not be evaluated** by the system. They are removed from the raw CDRs as the system imports traffic.

The **Ignored Items** screen provides the overview of all items temporarily ***excluded from fraud evaluation*** for the **Exclusion Period** defined in the **New Excluded Entry** dialog. When this period expires, the item is released from the exclusions list automatically.

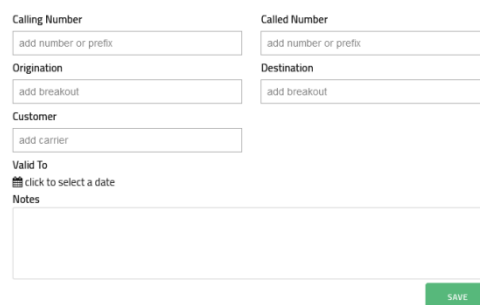
How to add Items to the ignored Items list

- 1) Select **Ignored Items** in the menu
- 2) Click on the **New Item** button in the top-right corner

A green rectangular button with a white plus icon and the text "New Item".

The **Ignored Item** window opens.

- 3) Enter a **Calling Number** and/or a **Called Number**, select the necessary criteria (**Origination**, **Destination**, **Customer**, and/or **Supplier**); define the **Period of ignoring**, and add **Comments**.
- 4) **Save** entry

A screenshot of the "New Excluded Entry" dialog. It contains two columns of input fields. The left column has "Calling Number" (with a subtext "add number or prefix"), "Origination" (with a subtext "add breakout"), "Customer" (with a subtext "add carrier"), "Valid To" (with a subtext "click to select a date"), and "Notes" (a large text area). The right column has "Called Number" (with a subtext "add number or prefix") and "Destination" (with a subtext "add breakout"). A green "SAVE" button is at the bottom right.

How to remove Items from the allowed Items list

- 1) Select **Allowed Items** in the Navigation bar
- 2) Click on the **Action Button** to the right of the entry 
- 3) Select **Expire Now**

7.3 Allowed Items

Allowed Items will also be **evaluated** for fraud and included in E-Mail Notifications, but they are **permanently ignored from blocking** (e.g. number of hospitals, legitimate call centers...).

✓ Allowed Items find in list + New Item

ALL (100) PENDING ITEMS (0) ACTIVE ITEMS (100) EXPIRED ITEMS (0)

Total items collected: 100

#	Status	Condition	Effective Time	Notes	Last Modified
1	ACTIVE	traffic from 49176 to all numbers from all customers to all suppliers	1899-12-29 23:00:00 - 2038-01-19 02:14:07		2 months ago
2	ACTIVE	traffic from 49176 to all numbers from all customers to all suppliers	1899-12-29 23:00:00 - 2038-01-19 02:14:07		2 months ago
3	ACTIVE	traffic from 49176 to all numbers from all customers to all suppliers	1899-12-29 23:00:00 - 2038-01-19 02:14:07		2 months ago
4	ACTIVE	traffic from 49176 to all numbers from all customers to all suppliers	1899-12-29 23:00:00 - 2038-01-19 02:14:07		2 months ago
5	ACTIVE	traffic from 49176 to all numbers from all customers to all suppliers	1899-12-29 23:00:00 - 2038-01-19 02:14:07		2 months ago

Allowed Items are used to exclude specific items from blocking files provided to the routing proxy /switch. Therefore, the allowed items condition needs to match the blocking parameters (e.g. **Blocking on Destination** -> Allowed Item: **Destination** or **Blocking on A-Number** -> Allowed Item: **specific A-Numbers**).

Note: The above-mentioned functionality is fully supported in combination with the Routing Proxy. Please contact Oculeus, to further evaluate this functionality in conjunction with other switch integrations/setups.

How to add Items to the allowed Items list

- 1) Select **Allowed Items** in the menu
- 2) Click on the **New Item** button in the top-right corner

+ New Item

The **New Allowed Entry** window opens.

- 3) Enter a **Calling Number** and/or a **Called Number**, select the necessary criteria (**Origination**, **Destination**, **Customer**); define the **Period of allowing**, and add **Comments**.
- 4) **Save** entry

Calling Number add number or prefix	Called Number add number or prefix
Origination add breakout	Destination add breakout
Customer add carrier	
Valid To click to select a date	
Notes	

SAVE

How to remove Items from the allowed Items list

- 1) Select **Allowed Items** in the menu
- 2) Click on the **Action Button** to the right of the entry
- 3) Select **Expire Now**

7.4 Filter Lists

Filter Lists are used for the scenarios, which filter on a huge amount of entries in the Basic Filter. Those lists can be managed within this section. Import entities by editing/ creating a filter list. The drag and drop field is used to import the items. Once the filter list is modified the changes are applied on each scenario which is using the corresponding list.

This way allows to easily modify scenarios with huge amount of entities to focus on.

How to create a filter list

- 1) Click on Filter List
- 2) Click on **New Item**
- 3) Add Items by clicking in **Edit**
- 4) Click on **Save**

Filter List Details

Name: Fraud Numbers

Description: this is a test filter list

Status: Enabled

Type: Standard

Field: Numbers

Filter items: 0 item(s) currently in the list. [Edit]

SAVE

How to update the items within an existing list

- 1) Disable the Filter List
- 2) Click on the “Reset Item” button
- 3) Click on “Edit”
- 4) Upload the new Filter List
- 5) Save and Enable the List

Filter List Format

Filter Lists need to be uploaded in CSV format (.csv)

The structure and content are always the same:

item_value;item_comment

where item_value is either the exact number, the carrier defined in the system or the breakout defined in the system. Every Filter list can only include one type of information (number/carrier/breakout). To review the exact names configured in the system open the “Review” in the top right menu.

item_comment is an extra field where comments can be added, those need to be in proper ASCII hyphens ‘comment ‘.

NOTE:

- Empty lines cause the system to stop the import from this line
- Numbers need to be entered without leading zeros and/or tech-prefixes

8 Traffic Profiling

8.1 Overview

Traffic Profiling is a self-learning engine that profiles collected traffic for a subsequent prediction of the traffic profile and analysis of changes in traffic behavior.

Traffic profiling engine evaluates all traffic and profiles it by using historical data, traffic trends (e.g. normal growth), and seasonality (e.g. time of day, day of week). It also predicts the traffic profile for next period (e.g. for 5, 15, and 1 hour). An anomaly is detected when actual traffic does not conform to the predicted traffic. When an anomaly is detected, the system automatically triggers an alert and extracts the abnormal data for further analysis in the system. The analysis is provided by **dynamic** and **live scenarios**.

The **dynamic scenarios** use the embedded traffic-profiling engine to identify fraud by detecting anomalies. The **live scenarios** are special type of scenarios that can provide real-time data analysis based on data collected directly from the switches.

8.2 Traffic Anomalies

8.2.1 Overview

The system monitors four target parameters for each destination and each carrier. They are as follows:

Quantitative characteristics:

- ***Calls***
- ***Minutes***

Qualitative characteristics:

- ***ASR*** (the ***Answer Seizure Ratio*** is a percent ratio of successfully answered (with non-zero duration) calls to the total number of call hunts).
- ***ACD*** (the ***Average Call Duration*** is an average duration of a call).

Each working parameter is monitored separately, as oftentimes a single parameter may stay unaffected by a potential problem. However, if the monitoring system detects anomalies of all parameters, the probability of accurate failure detection rises above 90%.

A problem with a carrier or a destination does not necessarily affect the overall performance, so it is crucial to monitor each carrier and each destination individually.

The **Traffic Anomalies** screen provides the overview of all detected anomalies in the system.

Traffic Anomalies

find in list

Total items collected: 100

#	Name	Type	Criterina	Last Update	Details
1	Singapore Mobile	Destinations	ASR	2018-04-17 18:10:00	>
2	MATRIX	Suppliers	Calls	2018-04-17 18:10:00	>
3	KATO2 IN	Customers	ASR	2018-04-17 18:10:00	>
4	BELTELECOM	Suppliers	ASR	2018-04-17 18:10:00	>
5	DEE TELECOM NON CLI	Suppliers	ACD	2018-04-17 18:10:00	>
6	Pakistan Mobile Moblink	Destinations	Minutes	2018-04-17 18:10:00	>
7	GLOBAL CARRIER	Suppliers	Minutes	2018-04-17 18:10:00	>
8	Bangladesh Mobile	Destinations	Calls	2018-04-17 18:10:00	>
9	PLDT_HK	Customers	Calls	2018-04-17 18:10:00	>

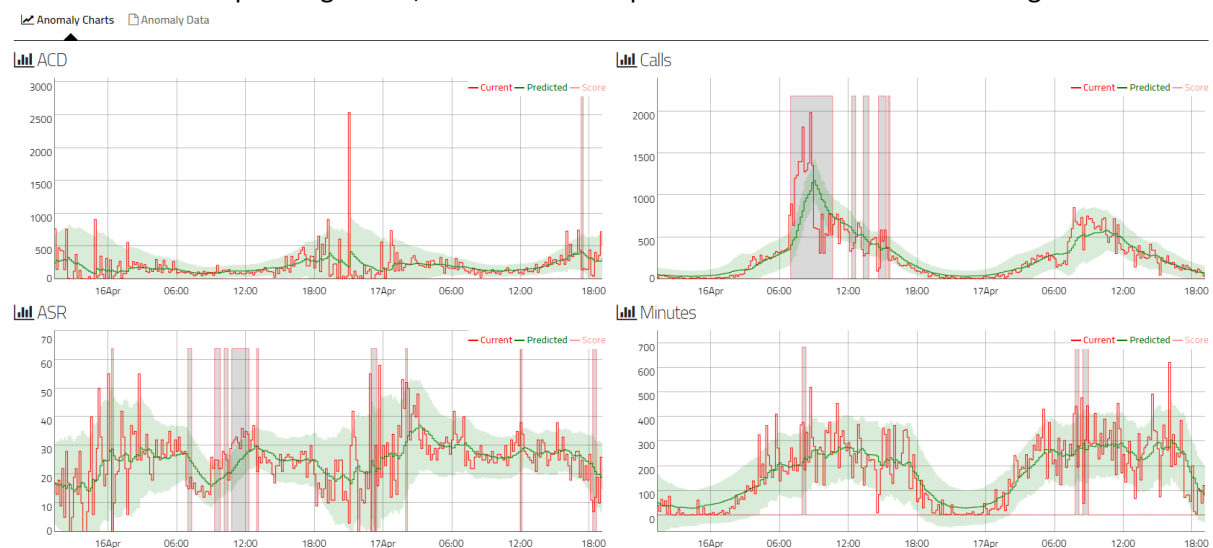
The grid contains the following information:

- **ID**
- **Name**
- **Anomaly Type**: the traffic type — **Customers, Suppliers, or Destinations** — on which the anomalies were detected.
- **Criteria**
- **Last Update**
- **Details**: see below the Detected Anomalies Details section.

8.2.2 Detected Anomalies Details

8.2.2.1 Charts

To view the traffic profiling charts, use the **Details** option in the **Detected Anomalies** grid.



There are four charts based on the anomaly's detection criteria:

- **Minutes**
- **Calls**
- **ACD**
- **ASR**

There are two curves of different colours and the green area in the chart.

The **Current** parameter values are plotted in **red**.

The **green curve** represents the values dynamics, **Predicted** by the Holt-Winters forecasting algorithm.

The Holt-Winters forecasting algorithm is a short-term forecasting mechanism: it only predicts time series values one-time step into the future. For predictions, the method also considers the current value of an observed parameter, allowing the system to flexibly adapt to its changes throughout the day. Once a sudden change in traffic behaviour is detected, the system triggers an alert. Then the difference between the observed value and the predicted one fades away, and the anomaly

(aberration) disappears. In fact, the forecast method means monitoring dynamic changes of the values rather than current values of the parameters.

The **light green area** defines the **confidence band width**, which limits the oscillations of the red (**Current**) curve.

If the red curve exceeds the confidence band (light green area) over a certain time interval an anomaly (aberration) occurrence is registered followed by the system alert (the **Alerted** intervals).

The band width is not constant. It is a dynamic forecast and automatically calculated, depending on the possible spread of values over a particular time of day.

The smallest time interval in the chart is equal to 10 minutes.

Read the chart legend and hover the mouse pointer over the chart to view the **Current**, **Predicted**, and **Alerted** values at any selected time.

NOTE:

It should be mentioned that while traffic volume is measured in minutes, the ACD values – in seconds and the ASR values – in percentage terms.

8.2.2.2 Anomaly Data

The **Anomaly Data** grid displays the chart numerical values – a result of fraud evaluation provided by last measurement.

Detected At	Current Value	Predicted Value	Anomaly Score
2018-04-16 16:00:00 (10 months ago)	234.0	316.5 (73.93%)	0.0
2018-04-16 15:50:00 (10 months ago)	276.0	330.14 (83.60%)	0.0
2018-04-16 15:40:00 (10 months ago)	223.0	350.84 (63.56%)	0.0
2018-04-16 15:30:00 (10 months ago)	227.0	373.22 (60.82%)	2182.4
2018-04-16 15:20:00 (10 months ago)	368.0	381.78 (96.39%)	0.0
2018-04-16 15:10:00 (10 months ago)	586.0	367.2 (159.59%)	2182.4
2018-04-16 15:00:00 (10 months ago)	452.0	365.61 (123.63%)	2182.4
2018-04-16 14:50:00 (10 months ago)	585.0	348.98 (167.63%)	2182.4
2018-04-16 14:40:00 (10 months ago)	132.0	380.55 (34.69%)	2182.4
2018-04-16 14:30:00 (10 months ago)	95.0	419.57 (22.64%)	0.0
2018-04-16 14:20:00 (10 months ago)	498.0	418.04 (119.13%)	0.0
2018-04-16 14:10:00 (10 months ago)	480.0	418.54 (114.68%)	0.0
2018-04-16 14:00:00 (10 months ago)	469.0	420.26 (111.60%)	0.0

The grid contains the following data:

- **Detected at**
- **Current Value**
- **Predicted Value**
- **Anomaly Score**: the red-coloured records.

9 Tools

9.1 Traffic Files

9.1.1 Imported Files

The **Imported Traffic** screen displays the raw traffic data provided to the **Anti-Fraud System** for further analysis in the system.

Processed Traffic

Imported Files

ALL (100)

STANDARD (100)

DYNAMIC (0)

LIVE (0)

Q find in list

Total items collected: 100

#	Type	Status	File Name	Records	Successful Records	Unsuccessful Records	Minutes	Last Updated
1	STANDARD	PENDING	capt_corr_20180327_in_13_010.cdr	30.000	0 (0,00%)	0 (0,00%)	0	a few seconds ago
2	STANDARD	PENDING	capt_corr_20180327_in_13_009.cdr	30.000	0 (0,00%)	0 (0,00%)	0	a few seconds ago

It also provides information on the Status of Process (Pending/ Processed) as well as the amount of calls, minutes, successful and unsuccessful calls per file.

Processed Traffic

Imported Files

Q find in list

Total items collected: 100

#	Src	Dst	Time	Dur	Org	Tirm	CarrierIn	CarrierOut	Trunkin	Trunkout	Rev.	Cst.	Margin
1	 4982	 4982	2018-03-27	00:00:00	National	National	M X	_RETAIL_AUG/	-SBC-HKW-to-DTAG	_RETAIL_AUG/	0,00 €	0,00 €	0,00 €

9.2 Permissions

The Permissions Menu allows to create/ edit Access Permissions (See How-To Manual: Manage Access Roles) and to create/ edit Users (See How-To Manual: Manage Users)

9.3 User Logs

In this menu items all user-actions within the AFS are tracked, e.g. view details of a specific incident, enabling/disabling scenarios. Successful and unsuccessful login attempts will also be saved to identify access violations and to track which account might be endangered.

9.4 Preferences

The Preferences Menu provides information about **carrier**, **breakouts** and **routings** defined in the system

9.4.1 Carrier

All carrier (CarrierIn (Customer)/ CarrierOut (Supplier)) defined in the settings are listed with their *Carrier ID* in alphabetical order.

9.4.2 Breakouts

All Destinations defined in the system settings are listed with their *Destination ID* in alphabetical order.

9.4.3 Routings

All Routings defined in the system settings are listed with their *Route ID* in alphabetical order.

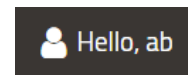
How to add Carrier, Breakouts and Routings

Those settings cannot be managed within the interface, please contact fds_support@oculeus.com if the data needs to get updated.

9.5 Global Configuration

How to change user password

- 1) Click on the username displayed on top right
- 2) Select "Password"
- 3) Enter current password and new password
- 4) Click on "Change Password"



Note: If the AFS receives data from Captura, passwords need to get changed in Captura.

How to Logout

- 1) Click on the Logout Button in the menu
- 2) Click in the top-menu on the Logout Button



How to disable/enable Auto-Logout

By default the system will always logout after 15minutes of inactivity

To disable/enable the function **click** on the toggle button in the menu called "**Auto-Logout**".

