SMS Firewall

Functionality overview

Document type: Functionality overview

Date of issue: 10/03/2025

SMS Firewall version: 1.5.0

Alarislabs Pte Ltd reserves the right to change any information contained in this document without prior notice.

COPYRIGHT INFORMATION

This document details the business tasks handled by SMS Firewall and provides an overview of its functionality.

Table of contents

Glossary
Business tasks solved by SMS Firewall
Integration of SMS Firewall into the carrier network
System interfaces
- Overview
- Sign-in form
- Global rules
- URL scanner
- Text normalization
  - Normalization settings
  - Mimicry dictionary
- Traffic analysis
  - Lists of conditions
  - Tags
  - Speed limits
  - Logical rules
  - Watchdog
- Traffic monitoring
  - Alerts
  - Analytics
- Traffic simulation
- Flash call detection
  - Flash call detection tab
  - CDR files tab
- Users and Roles
  - Users
  - Roles
- MCCMNC reference book
- History log
- Settings
  - System settings
  - Your account
  - Backups
    - Backup settings
    - Scheduled backups

Glossary

SIM gateway, SIM gate - gateway that employs a set of SIM cards for generating and sending messages. It is often used to terminate messages locally in case there is no direct connection to a telecom carrier.

Fraud - in the context of this document, deception used to gain a dishonest advantage that employs telecommunication technologies.

Global title (GT) - the switch address used for routing in the SCCP protocol. It corresponds to mobile network operator (MNO) equipment ID on the sender carrier's network.

Recipient - the message recipient number.

Sender ID - message sender ID. The ID can be either alphabetic (GOOGLE) or numeric (900). A sender ID can be a local number (+79217771122).

TEXT - message content.

Sending MNO - mobile network operator on the sending side of the traffic.

Receiving MNO - mobile network operator on the receiving side of the traffic.

Business tasks solved by SMS Firewall

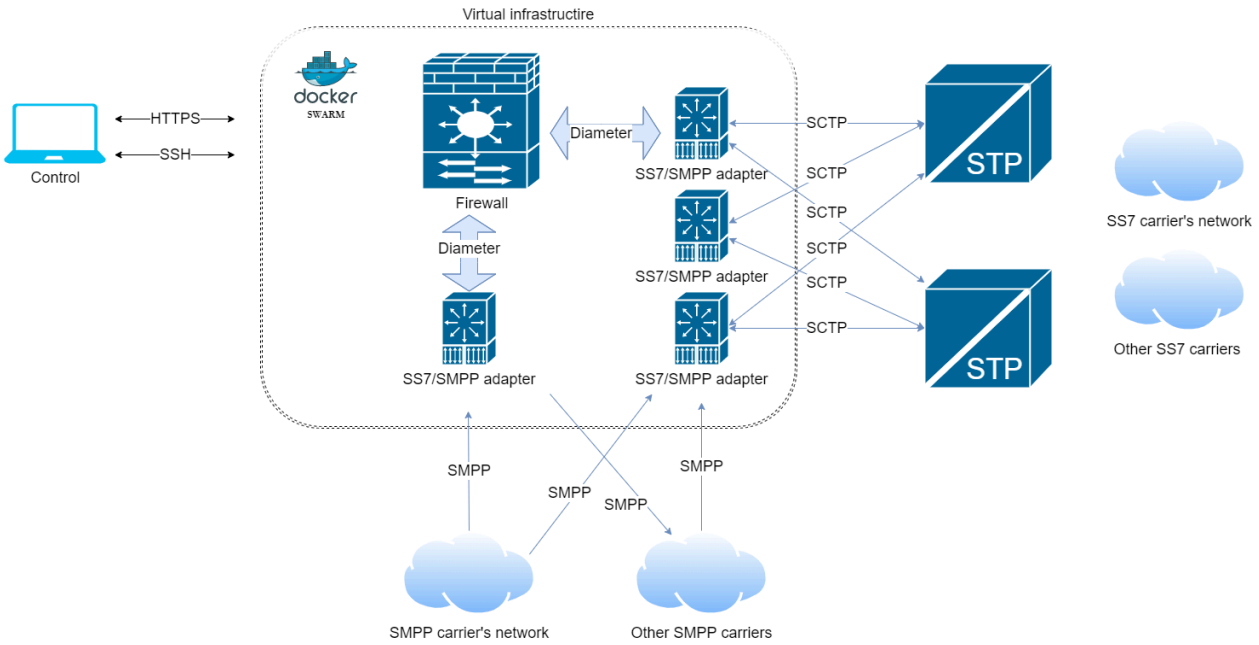
The following trends are characteristic of recent telecom development: the use of messages rather than voice in communication; authentication, authorization and administration with the help of SMS. All of this causes the need to control the purity of SMS traffic and protect it from various types of fraud related with message content and its legitimate delivery.

The SMS Firewall system has been created to handle the following business tasks:

- **Spam filtering**: it allows increasing the loyalty of subscribers as it helps eliminate losses of telecom operators when messages are terminated on a cheaper local level bypassing international channels and international wholesale costs. SPAM filtering is performed through message content analysis.
    - By configuring a set of values in user-defined lists and tags
    - By matching regular expressions to signaling information
    - With the help of a trained neural network
- **Detection of hacks**: minimizing losses incurred by customers and their partners due to fraudulent traffic, through tracking abnormal traffic increases:
    - By source (Originating GT, Sender ID)
    - By destination (Recipient)
    - By text
- **Detection of 'gray' routes and fraudulent SIM gateways**: the SMS Firewall allows reducing losses from fraudulent activities as it detects 'gray' routes and fraudulent SIM gateways by matching the message text patterns from specific sources and corresponding sender IDs.
- **Detection of spoofing**: the System reduces losses caused by fraud. It detects spoofing by matching Originating GT for messages handled by in-depth analysis, and Originating GT values where the subscriber is actually registered.
- **Protection against GT scanners**: the System controls GT scanners with the help of predefined lists of GT values and filtering rules.
- **Filtering of unsolicited traffic**: the System filters traffic in two consecutive steps as follows:
    - Preliminary analysis that involves basic blacklists and whitelists of global rules for parameters to be analyzed.
    - In-depth analysis by a variety of parameter combinations; condition lists can be used for available parameters.

Integration of SMS Firewall into the carrier network

The figure below shows a diagram of comprehensive protection of traffic transmitted over the SS7 protocol.



Comprehensive traffic protection on an SS7 network

System interfaces

Overview

Most interfaces have a similar structure and contain the following elements and controls:

1. A table of records:
    a. A click on a table record opens the *Edit* panel.
    b. The rightmost column of each table contains the ••• icon that unfolds the *Clone* and *Delete* menu items for cloning and deleting the table record, respectively.
2. The *Download* button at the top right corner of the table serves to download the table in MS Excel format.
3. The Search 🔍 field at the top of the page serves for searching the records (exact match or substring search. Multiple space-separated values can be entered. Substring search is supported.

Sign-in form

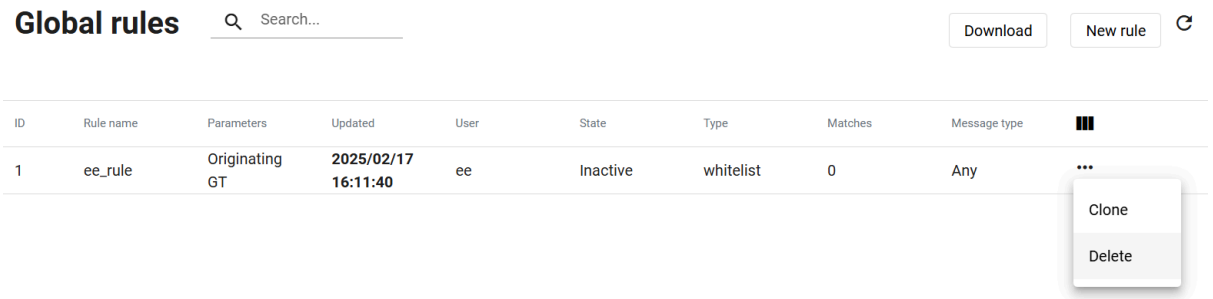
The Sign-in form serves for access to the System. It contains the required login and password fields.

Sign-in form

The profile menu contains the following options:

- Go to Your account interface
- Log out

Global rules



Global rules interface

The *Global rules* interface allows reducing the volume of analyzed traffic due to basic filtering. The interface employs lists that are used in preliminary analysis, before verification by logical rules, speed limits and neural network. Global rules contain lists of values for the parameters (*Sender ID*, *Originating GT, Recipient*, *Message text, Sending MNO, Receiving MNO, SMSc address*) and can filter traffic as whitelists and blacklists respectively. The parameter values can be applied as filters both for complete values (Facebook, Amazon) and values with prefixes (*8434, prom* or *sale*)

The following rule types are available:

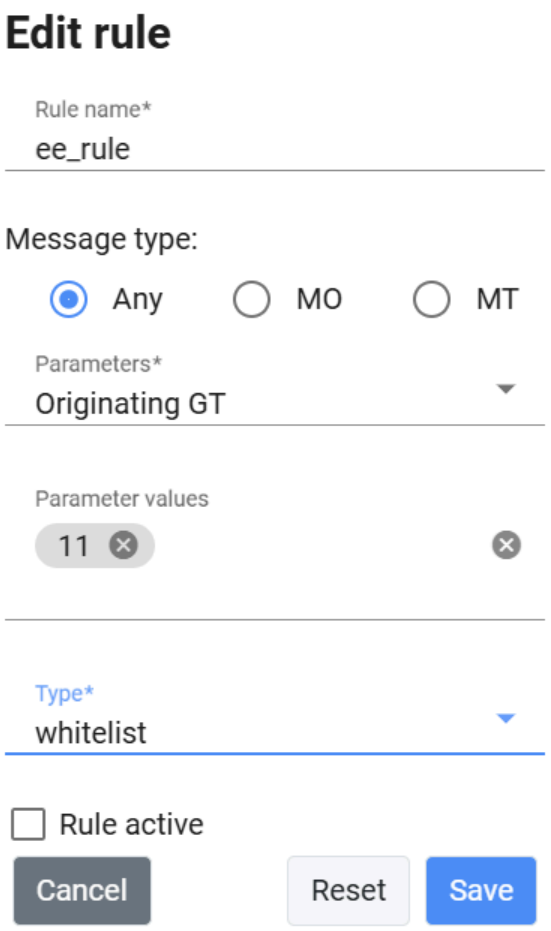
- *Whitelist*: when a match is found, the message is taken for in-depth analysis. If no match is found, the message is rejected. If there is no Whitelist rule or the Whitelist rule is deactivated, the Whitelist match check is not performed, but the Blacklist rule match check is performed.
- *Blacklist*: when a match is found, the message is blocked. If no match is found among the available Blacklist rules, the message is sent for deep analysis. If there is no Blacklist rule or it is deactivated, the match check is disabled and the message is sent for deep analysis.

Global rules are activated based on the following logic. When a message is placed to *Global rules*, for all enabled rules the System verifies that a specific parameter is available in the Whitelist and is not available in all Blacklists. If a message matches both values in the blacklist and whitelist, the message is blocked. If values partially match a specified value prefix or regular expression, a message containing this part is blocked based on the pattern specified in the blacklist. For example, the whitelist rule with the value 34* will be used that allows calls to Spain, followed by the blacklist rule with the value 346* that blocks calls to this Vodafone Spain prefix.

The *Global rules* table contains information about all the global rules available in the System. The table has the following columns:

- **ID** - rule identifier.
- **Rule name** - unique rule name.
- **Direction** - traffic direction.
- **Parameters** - shows the parameter the rule belongs to (*Originating GT, Sender ID, Recipient, Message text, Sending MNO, Receiving MNO, SMSc address*).
- **Updated** - date of the last rule update.
- **User** - name of the System user that created the rule.
- **State** - rule state. Possible values are: *Active* and *Inactive*.
- **Type** - rule type. Possible values are: Whitelist, Blacklist.
- **Matches** - the number of times the rule was applied.
- **Message type** - contains the following values:
  - **Any** - all message types are filtered
  - **MO** - only messages of the MO type are filtered
  - **MT** - only messages of the MT type are filtered
- **actions** - contains the following controls:
  - **Clone** - create a rule with similar parameters.
  - **Delete** - delete the rule.

Click *New rule* at the top of the page to create a new rule. Configure the fields as appropriate. The field values are the same as in the *Global rules* table and are explained above. Click on a record in the table to open the *Edit rule* window.



Editing a global rule

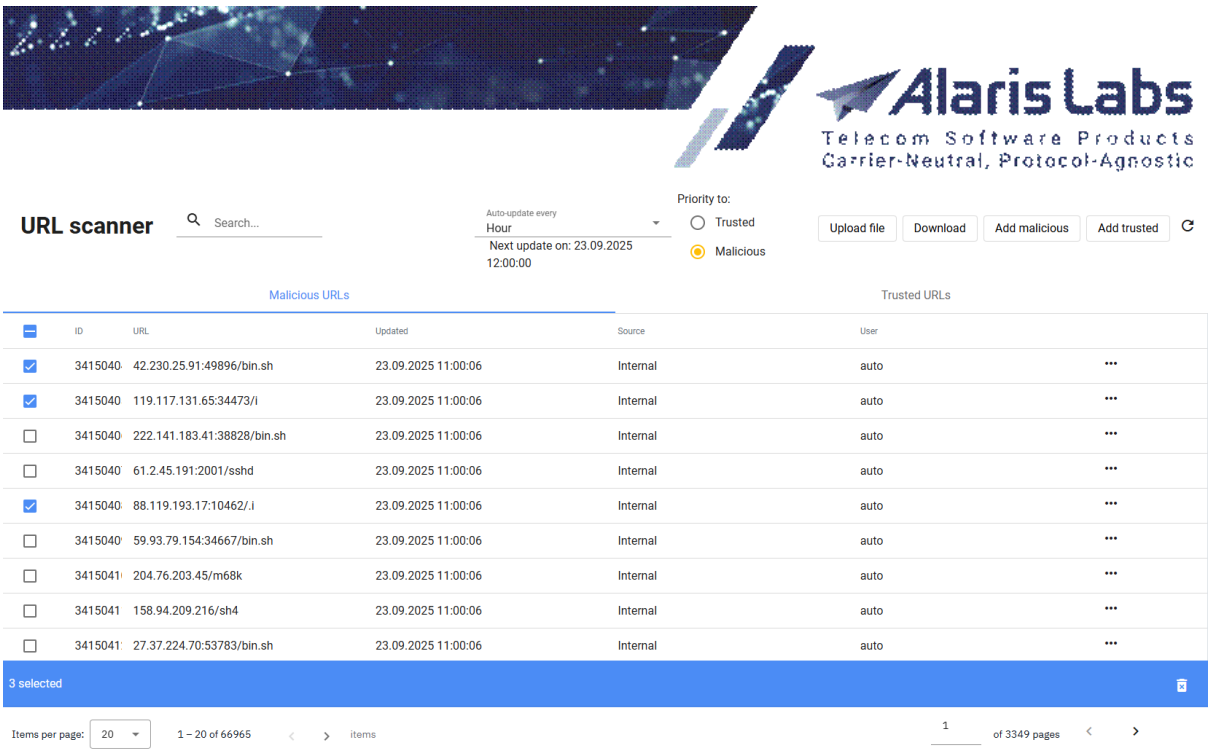
Business logic example:
The user creates a whitelist of *originating GT* addresses of its own network elements and network elements of the telecom operator with which it has agreements. All other messages that are sent not from the specified GTs will be blocked.

URL scanner

The *URL scanner* interface serves to analyze SMS traffic for malicious URLs, detects suspicious URLs and provides detailed reports on the results of analysis.

The *URL scanner* allows the user to:

- Prevent leakage of confidential information: identify and block phishing links aimed at stealing passwords and other personal data.
- Ensure malware protection: identify and block links that lead to sites that distribute viruses, trojans and other malicious programs.
- Reduce network load: block spam messages containing unwanted advertising links.
- Enhance the company's reputation: demonstrate concern for the safety of customers and partners.



URL scanner interface

The *URL scanner* interface contains two tabs: *Malicious URLs* and *Trusted URLs*, and a toolbar at the top of the page.

Malicious URLs tab

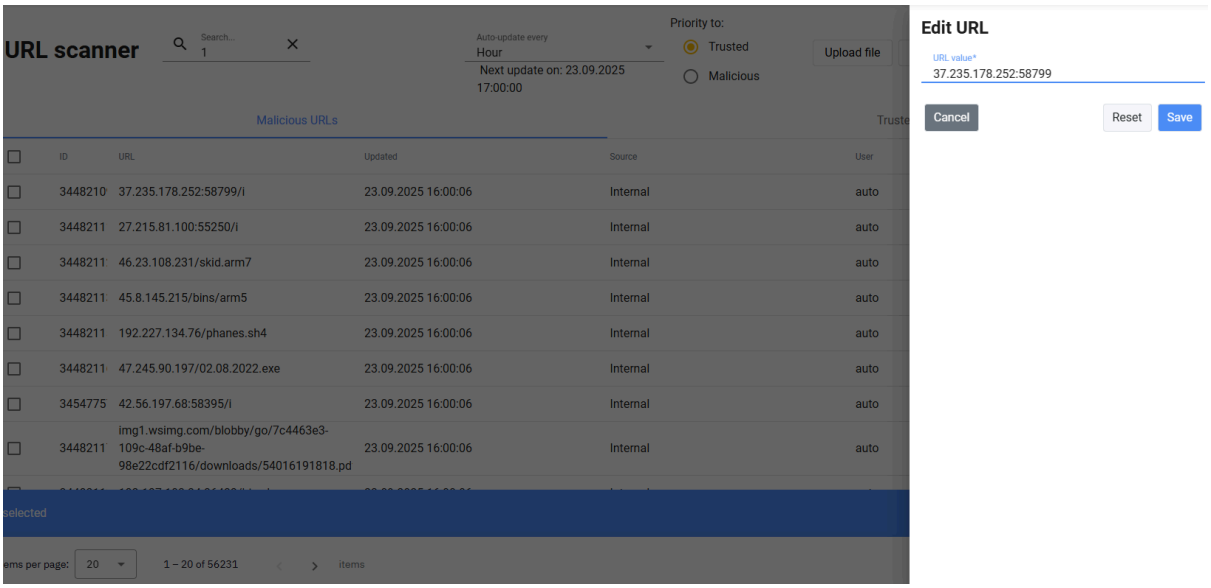
The *Malicious URLs* table contains all known malicious URLs stored in the System and marked with the *Malicious* attribute. The table displays records from the internal URL storage. If, after all global rules are checked, a match is found in the *Malicious URLs* list, the System immediately applies the resolution *Blocked*. New entries can be added to this table manually (one by one), imported from a file, auto-updated from an internal database, or added from an external database through an API (APIs to specific databases can be added by request).

The table has the following columns:

- **ID —** unique identifier for the record.
- **URL** — full URL or prefix used to determine immediate *Block* resolution after all Global rules are evaluated.
- **Updated** — timestamp of the last change (manual edit or automatic update).
- **Source** — source of the URL entry. Possible values: *Manually* (added manually), *Internal* (added from the System's internal storage), *External* (added from an external database).
- **User** — login of the user who created or last modified the record; can be *auto* for automatically added records (for example, those imported from *Internal* / *External* sources).
- ||| actions - contains the *Delete* control that serves to remove the record.

In both tabs, each row has a checkbox for selection. Selecting multiple rows shows the selection bar with the count (for example, *3 selected*) and the bulk *Delete* button.

Click a table record to open the edit form that appears to the right.



URL edit form

Trusted URLs tab

The *Trusted URLs* table contains all known URL entries in the System that are explicitly marked as *Trusted*. The table displays records from the internal URL storage. If, after all global rules are checked, a match is found in the *Trusted URLs* list, the System immediately sends the message for further *deep analysis*.

New values can be added to this table manually (one record at a time) or through file import.

The table has the same columns as the *Malicious URLs* table.

Toolbar controls

The toolbar at the top of the page contains the following controls.

- **Search** — text search by full or partial URL match.
- **Auto-update every** — control that defines the refresh period for the *Malicious URLs* table. Only entries originating from the *Internal* source are refreshed. Records added through *External* imports or entered *Manually* remain unchanged. The *Trusted URLs* table is not affected. Available values are: *Hour, 3 hours, 6 hours, 24 hours, Week.* Select a value from the dropdown list. Click *Apply* to confirm the schedule. After confirmation, a hint is displayed below the field showing the exact date and time of

the next scheduled update in the System time zone. Example: *Next update on 06.02.2025 at 00:00:00.*

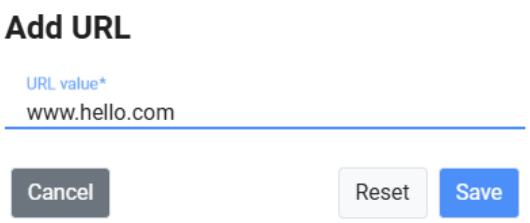
NOTE 1: After each auto-update, changes are written to the *History log*. New entries are marked as *Added*. Old records that were replaced are marked as *Deleted*.

NOTE 2: Auto-update fully replaces the original database with the updated one. Therefore, the number of records in the table may be changed after the update. Records added manually remain intact.

- **Priority to** — radio button selector that defines the System's behavior when a URL value is found in both the *Malicious* and *Trusted* databases simultaneously. Available options:
  - *Malicious* — the URL is treated as malicious, and the System applies the *Blocked* resolution.
  - *Trusted* — the URL is treated as trusted and passed to further processing.
- **Upload file** — import a file in Excel or CSV format containing a single column with full URL values or URL prefixes. The file size limit is 5 MB. The file will be uploaded to the tab that is currently open - *Malicious URLs* or *Trusted URLs*, respectively.

  NOTE: Uploading the file will replace the existing database with the new one from the file.

- **Download** — export the table to a file in Excel format.
- **Add trusted** — add a new trusted URL entry manually.
- **Add malicious** — switch to adding a malicious URL entry.
- **Refresh** — refresh the table.



Add URL form (identical for malicious and trusted URLs)

Business logic examples:

Example 1. The user relies on a **preinstalled database of malicious URLs** to immediately secure SMS traffic without any additional configuration.

- A dedicated microservice is responsible for maintaining the database of known malicious URLs.

Example 2. The user enables **automatic periodic updates** of the preinstalled malicious URL database to ensure the highest level of protection based on up-to-date information.

- A scheduler (*cron*) is used to trigger updates at a time convenient for the user.

Example 3. The user manages entries in the **preinstalled database of malicious URLs** to perform fine-tuning in line with business requirements.

- The interface provides controls for bulk management and search across records.

Example 4. The user configures **exception lists** in the preinstalled database of malicious URLs to fine-tune filtering according to business needs.

- A trusted URL list ensures that certain URLs are always excluded from inspection.

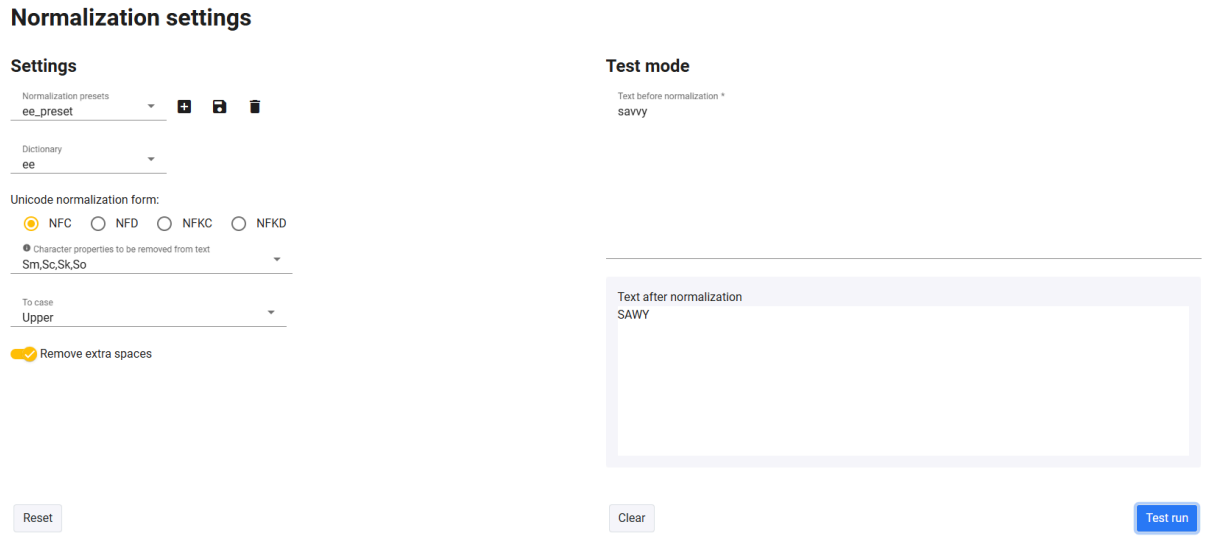
Example 5. The user integrates with an **external paid verification service** to validate unknown URLs and automatically enrich the preinstalled database of malicious URLs to provide protection at the highest level based on up-to-date data.

- The System sends a request to the paid service to obtain a response for messages that should have the *Allowed* resolution.
- If the service responds positively regarding the presence of a URL in the malware database, the pre-installed database is automatically enriched with this URL.

NOTE: For integrations with external verification services, contact the Alaris technical support team.

Text normalization

Text normalization in SMS Firewall is a security process that converts incoming SMS text into a consistent, standardized form in order to detect and block malicious manipulations. Malicious actors often exploit **character substitution, mixed alphabets, or look-alike symbols** to disguise phishing links, impersonate trusted senders, or bypass traditional filtering systems. Normalization eliminates these tricks by mapping suspicious or non-standard characters back to their canonical equivalents.



Normalization settings

The *Text normalization* interface is designed to:

- Prevent phishing by detecting and blocking messages containing obfuscated links to fraudulent websites.
- Protect against social engineering attacks by revealing mimicry that imitates trusted brands or official sources.
- Reduce data leakage risks by stopping SMS with altered characters that might evade filters.
- Increase customer confidence by demonstrating proactive protection against potential threats.

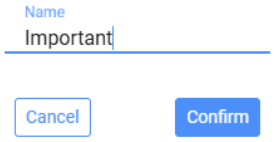
The *Text normalization* interface consists of two subsections: Normalization settings and *Mimicry dictionary*.

Normalization settings

The *Normalization settings* interface serves to configure presets with custom parameters for text normalization. The user can then select a preset when configuring a tag in the Tags interface. It is divided into two sections: *Settings* for configuring normalization filters and *Test mode* for validating the configuration on sample text. The configured options can be applied immediately in test mode, both before and after saving the preset.

The *Settings* panel contains the following controls:

- **Normalization presets** – a dropdown menu for selecting, creating, saving, or deleting presets. A preset defines a reusable set of normalization filters. By default, the *Default preset* is selected.
    - Click the **+** button to open a dialog for creating a new preset.



New preset dialog

  - Click the disk icon to save changes to the currently open preset.
  - Click the trash icon to remove a custom preset. If the preset is in use, a confirmation dialog warns that linked tags will be affected.

- **Dictionary** – select a dictionary to which the preset will be linked. When a preset is selected in tags, the characters specified in the dictionary will also be normalized. Select *None* if no dictionary is required.

- **Unicode normalization form** – a radio button group defining the normalization method. Available values: *NFC, NFD, NFKC, NFKD*. *NFC* is selected by default.

- **Character properties to be removed from text** – a multi-select dropdown list of Unicode categories (letters, marks, numbers, punctuation, symbols, separators, control characters, etc.). Select the properties you want to remove when normalizing text. Possible values are:
  - *Lu: Letter, uppercase* – uppercase letters that will be removed. For example, the text *Value* will be normalized to *alue*.
  - *Ll: Letter, lowercase* – lowercase letters that will be removed. For example, the text *value* will be normalized to *V*.
  - *Lt: Letter, titlecase* – titlecase letters (used in some scripts as special uppercase forms) that will be removed. For example, a word starting with *Dž* will lose its first letter.
  - *Lm: Letter, modifier* – modifier letters used to change the sound of other letters (e.g., ː in phonetics). Removing them strips pronunciation markers.
  - *Lo: Letter, other* – letters from alphabets that do not fit standard upper/lowercase categories (e.g., Chinese or Arabic characters). Removing them deletes such letters entirely.
  - *Mn: Mark, nonspacing* – diacritical marks that combine with base characters but do not add width (e.g., ´ in é). Removing them converts *é* to *e*.
  - *Ms: Mark, spacing combining* – marks that combine with base characters but occupy space (rare in Unicode). Removing them eliminates visible combining marks.
  - *Me: Mark, enclosing* – enclosing marks that draw circles, boxes, or other shapes around characters. For example, ① (digit one enclosed in a circle) becomes 1.
  - *Nd: Number, decimal digit* – decimal digits 0–9 (or equivalents in other scripts). Removing them deletes numeric digits from text.

- *Nl: Number, letter* – numbers expressed as letters (e.g., Roman numerals Ⅰ, Ⅴ). Removing them strips such symbols.
- *No: Number, other* – numeric symbols that are not standard digits or letters (e.g., ⅓, ½). Removing them deletes these fraction-like forms.
- *Pc: Punctuation, connector* – connector symbols such as underscores (_) that link words. Removing them turns user_name into username.
- *Pd: Punctuation, dash* – dash and hyphen symbols (-, —). Removing them turns well-known into wellknown.
- *Ps: Punctuation, open* – opening brackets or quotation marks (e.g., (, {, [). Removing them deletes only the opening sign.
- *Pe: Punctuation, close* – closing brackets or quotation marks (e.g.,), },]). Removing them deletes only the closing sign.
- *Pi: Punctuation, initial quote* – opening quotation marks («, “). Removing them leaves the text without an opening quote.
- *Pf: Punctuation, final quote* – closing quotation marks (», ”). Removing them leaves the text without a closing quote.
- *Po: Punctuation, other* – all other punctuation (e.g., !, ?, …). Removing them strips such symbols.
- *Sm: Symbol, math* – mathematical operators (+, =, ∑). Removing them erases math expressions.
- *Sc: Symbol, currency* – currency signs (€, $, ¥). Removing them deletes financial symbols.
- *Sk: Symbol, modifier* – modifier symbols (e.g., ^, `). Removing them strips diacritical-style standalone symbols.
- *So: Symbol, other* – miscellaneous symbols (e.g., ☺, ♥, ©). Removing them deletes decorative or special-use signs.
- *Zs: Separator, space* – space characters between words. Removing them merges words (e.g., *data base* → *database*).
- *Zl: Separator, line* – line separators (Unicode U+2028). Removing them joins text lines together.
- *Zp: Separator, paragraph* – paragraph separators (Unicode U+2029). Removing them merges paragraph breaks.
- *Cc: Other, control* – control characters (e.g., tab, newline, carriage return). Removing them cleans invisible formatting.
- *Cf: Other, format* – invisible formatting marks (e.g., zero-width joiner). Removing them prevents hidden manipulations.
- *Cs: Other, surrogate* – surrogate code points used in UTF-16 for special characters. Removing them avoids broken encoding artifacts.
- *Co: Other, private use* – private-use characters defined outside Unicode standard. Removing them deletes system-specific symbols.

Refer to https://en.m.wikipedia.org/wiki/Unicode_character_property for more detail.

- **To case** – select the target case of normalized text. Possible values:
  - *Upper*: normalize all to uppercase
  - *Lower*: normalize all to lowercase
- **Remove extra spaces** – select to remove redundant spaces.

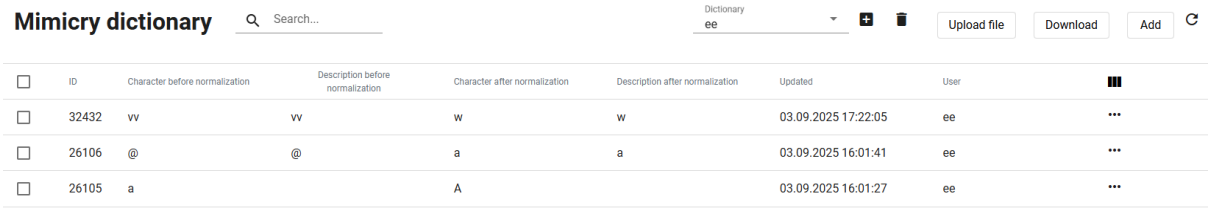
The *Test mode* panel provides tools for verifying normalization settings on sample input. It contains the following controls:

- **Text before normalization** – an input field for entering raw text, up to 1000 characters. Special characters are supported.
- **Text after normalization** – a read-only output field that shows the normalized text. Users can manually copy text or select all results with **Ctrl+A**. If the output exceeds the visible area, a vertical scrollbar appears. Hover over each character to display a tooltip with additional details.
- **Test run** – click to apply the currently selected normalization settings to the input text.
- **Clear** – click to resets both input and output fields to empty values.

NOTE: It is recommended to run tests prior to saving a preset to make sure that the normalization results are as expected.

Mimicry dictionary

The *Mimicry dictionary* interface allows managing homoglyphs (mimicry characters) that are normalized into standard characters. This ensures that visually similar or deceptive characters are consistently transformed into their correct equivalents, reducing the risk of bypassing security filters. Multiple dictionaries can be created. Dictionaries are only used when associated with presets.



Mimicry dictionary

The *Mimicry dictionary* table displays the dictionary selected in the same-name field in the toolbar at the top of the page, and contains the following columns:

- **ID** – unique record identifier.
- **Character before normalization** – unique homoglyph character that is normalized into the corresponding standard character in the *Character after normalization* column.
- **Description before normalization** – description of the homoglyph.
- **Character after normalization** – standard character into which the homoglyph is normalized.
- **Description after normalization** – description of the standard character.
- **User** – login of the user who added or updated the record.
- **Last updated** – date and time of the last modification or creation of the record.
- ||| actions - contains the *Delete* control that serves to remove the record.

The toolbar at the top of the page provides the following controls:

- **Dictionary** – serves to select a dictionary.
-  - click to add a new dictionary.
-  - click to remove the currently selected dictionary.

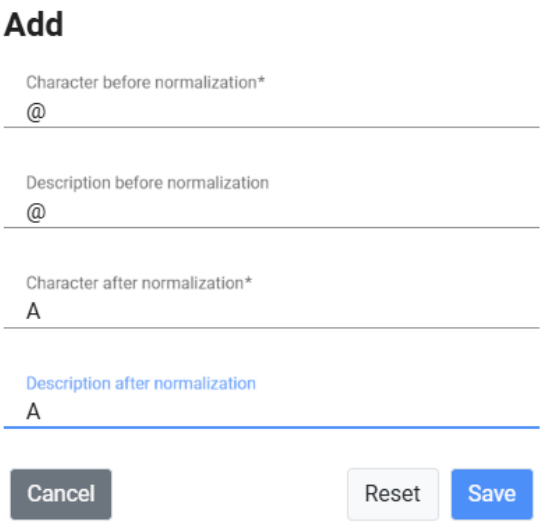
  NOTE: If the dictionary is used in one or more presets, it cannot be deleted.

- **Upload file** – click to upload a .txt file for the selected dictionary. The existing dictionary is completely overwritten with the uploaded file. It is recommended to download a current dictionary to get a sample file format. The file format must be as follows:

  homoglyph_code ;\t normalized_code ;\t MA :\t # (homoglyph → normalized) homoglyph_description → normalized_description\n

NOTE: The System comes with a pre-installed dictionary of homoglyphs. If needed, this dictionary can be re-uploaded from https://www.unicode.org/Public/security/13.0.0/confusables.txt.

- **Download** – click to download the dictionary data as an Excel file. If no rows are selected, the entire dictionary is downloaded; otherwise, only selected records are exported.
- **Add** – click to open the form for creating a new dictionary record.



Create a new dictionary record

The following fields are available:

- **Character before normalization**
- **Description before normalization**
- **Character after normalization**

- **Description after normalization**

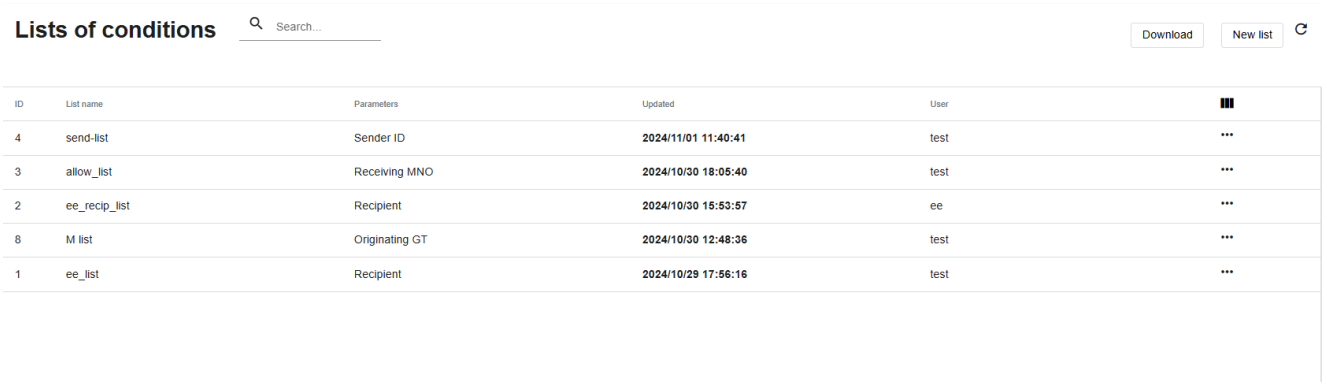
Click *Save* to save the record or *Cancel* to discard the changes.

Traffic analysis

The *Traffic analysis* section consists of the following interfaces: *Lists of conditions*, *Tags, Speed limits*, *Logical rules* and *Watchdog*.

Lists of conditions

Lists of conditions are used as lists of values for the parameters (*Sender ID*, *Originating GT*, *Recipient*, *Message text*, *Sending MNO* and *Receiving MNO*) for filtering traffic in tags. One and the same list can be used in multiple tags.

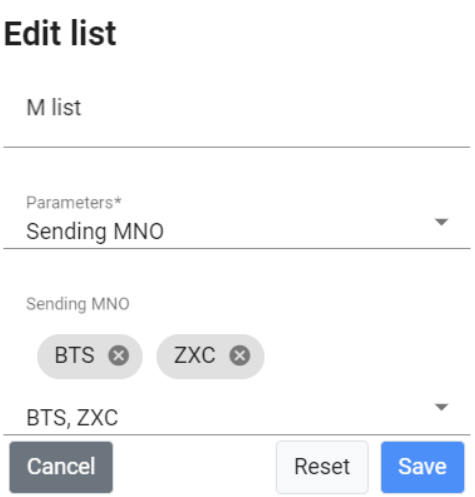


Lists of conditions interface

The table has the following columns:

- **ID** - rule identifier.
- **List name** - unique list name.
- **Parameters** - shows the message parameter to which the list of conditions belongs (*Originating GT*, *Recipient, Sender ID*, *Message text*, *Sending MNO* and *Receiving MNO*).
- **Updated** - date of the last update of the list.
- **User** - name of the System user that created the rule.
- actions - contains the following controls:
    - Clone - create a rule with similar parameters.

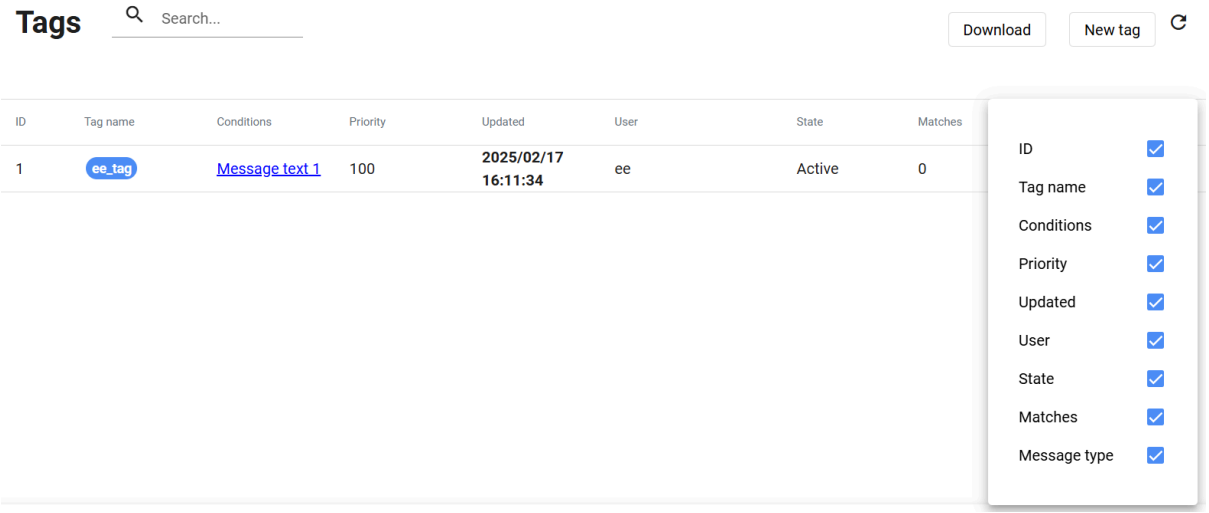
Delete - delete the rule.Click *New list* at the top of the page to create a new list of conditions. Configure the fields as appropriate. The field values are the same as in the *List of conditions* table and are explained above.
To open the *Edit list* window, click on a record in the table.



Editing a list of conditions

Tags

The *Tags* interface serves to configure the filtering criteria for in-depth analysis phase by various parameters in a combination.



Tags interface

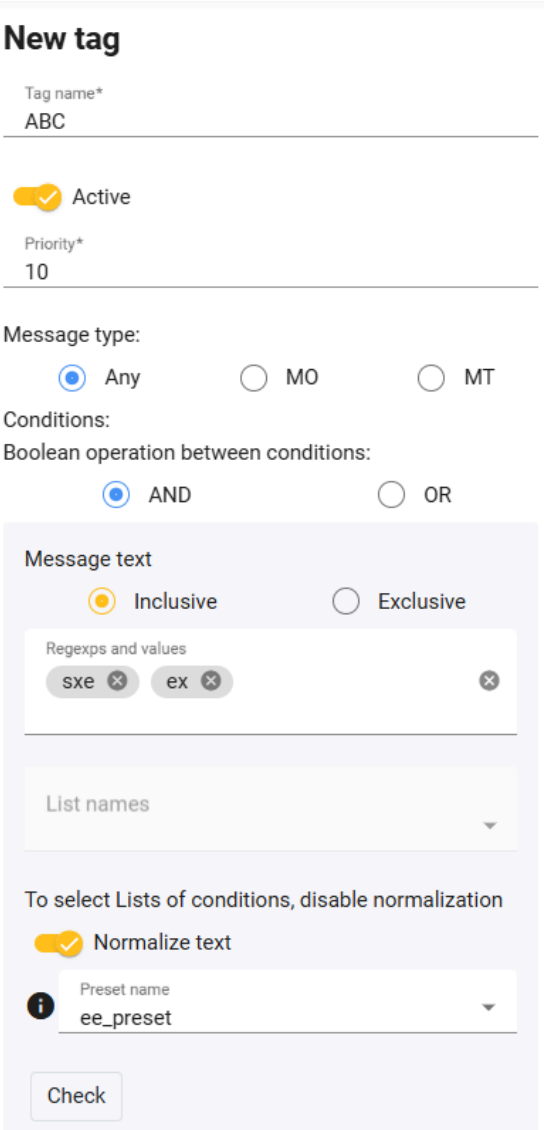
The table has the following columns:

- **ID** - tag identifier.
- **Tag name** - unique tag name.
- **Conditions** - shows the message parameters by which the message is analyzed (*Originating GT*, *Recipient, Sender ID*, *Message text*, *Sending MNO* and *Receiving MNO*).
- **Priority** - the tag priority. If two tags have the same priority, the newer tag will have a higher priority.
- **User** - name of the System user that created the tag.
- **State** - the tag state (*Active* or *Inactive*).

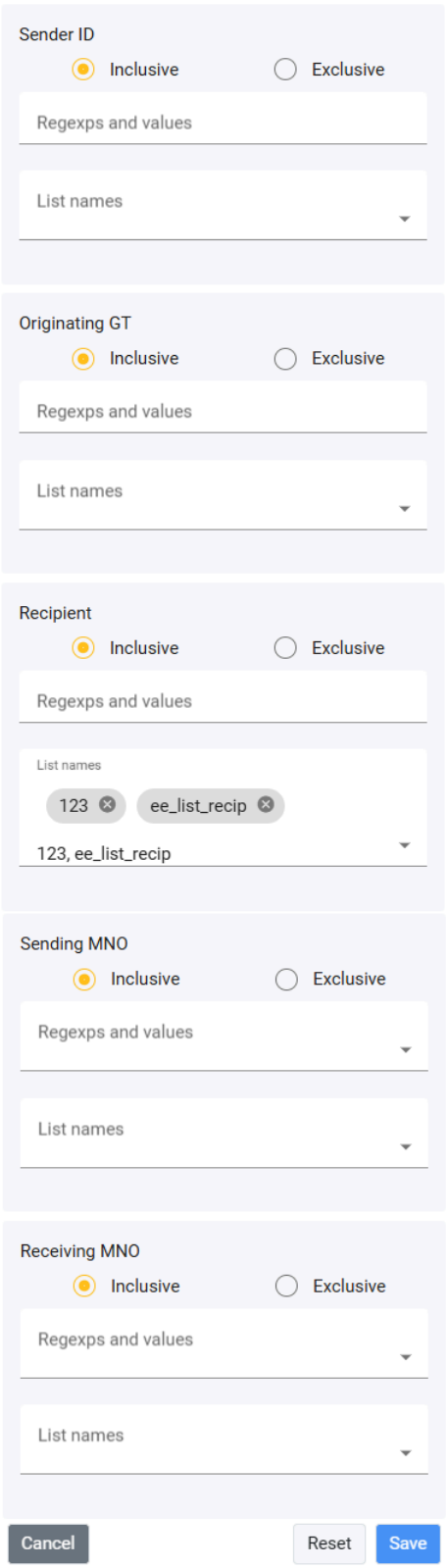
- **Matches** - the number of times the tag was triggered.
- **Message type** - contains the following values:
    - **Any** - all message types are filtered
    - **MO** - only messages of the MO type are filtered
    - **MT** - only messages of the MT type are filtered
- **actions** - contains the following controls:
    - **Clone** - create a tag with similar parameters.
    - **Delete** - delete the tag.

Messages are analyzed by the following parameters: *Recipient, Sender ID, Originating GT, Message text*, *Sending MNO* and *Receiving MNO*. All parameters can be combined using the logical operators ‘and’ and ‘or’, and as inclusive or exclusive lists. Parameters can be configured with the help of previously created lists of conditions (provided that at least one list of conditions has been created for the parameter).

Click *New tag* at the top of the page to create a new list of conditions. Configure the fields as detailed below.



Creating a tag (1)



Creating a tag (2)

The following fields are available:

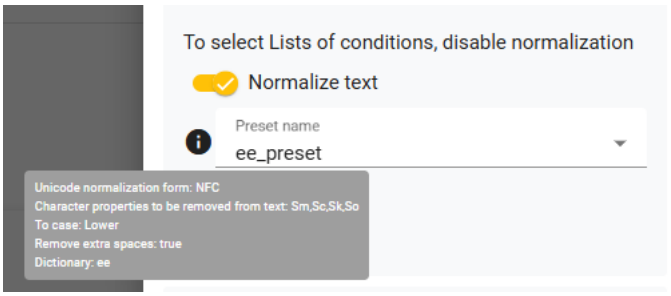
- **Tag name** – name of the tag.

- **Active** – toggle for enabling or disabling the tag.
- **Priority** – numeric field defining tag priority. Allowed values: 1–100. If two tags have the same priority, the newer tag will have a higher priority. Only one tag can be associated with one Speed limit and one Logical rule at the same time.
- **Message type** – radio button selection of message type. Options:
    - *Any (default)*
    - *MO*
    - *MT*
- **Boolean operation between conditions** – radio button for selecting the logical operator between tag conditions. Options:
    - *AND* (default) – all conditions must match.
    - *OR* – at least one condition must match.
- **Conditions** – configuration block for message parameter filters.
- **Message text** – the text of the message.
- **Inclusive / Exclusive** – radio button defining how conditions are applied:
    - *Inclusive (default)* – the tag triggers if the message matches the listed values.
    - *Exclusive* – the tag triggers if the message does not match the listed values.
- **Regexps and values** – add parameter values or regular expressions. Press Enter to add a new value. The parameter values are applied as filters for complete standalone values (Facebook, Amazon), as values with prefixes (*8434, prom* or *sale*) or as regular expressions. Below are some examples:

.	Matches any single character.
?	Matches the preceding element once or not at all.
+	Matches the preceding element once or more times.
*	Matches the preceding element zero or more times.
^	Matches the starting position within the string.
$	Matches the ending position within the string.
|	Alternation operator.
[abc]	Matches a or b, or c.
[a-c]	Range; matches a or b, or c.
[^abc]	Negation, matches everything except a, or b, or c.
\s	Matches white space character.
\w	Matches a word character; equivalent to [a-zA-Z_0-9]

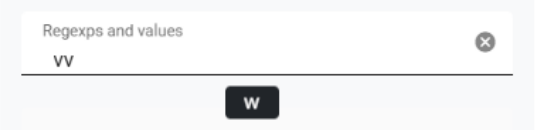
For a full version go to GOlang regexp syntax.

- **List names** – dropdown list for selecting preconfigured Lists of conditions.
- **Normalize text** – toggle to enabling local text normalization at the tag level. When enabled, the Preset name field becomes available (presets are configured in the Text normalization interface). If Lists of conditions are used, the toggle is blocked, as normalization is available for Regexps and values only.
    - *Preset name* – select the preset that must be applied for normalization. Hover over the i icon to view a tooltip with the preset settings:



Normalization preset details

- *Check* – click for validating normalization results for values in Regexps and values. Hover over the value to view the normalization result.



Normalization result

- **Sender ID**, **Recipient**, **Originating GT**, **Sending MNO**, **Receiving MNO** – message parameters that can be configured in the same way as *Message text*.

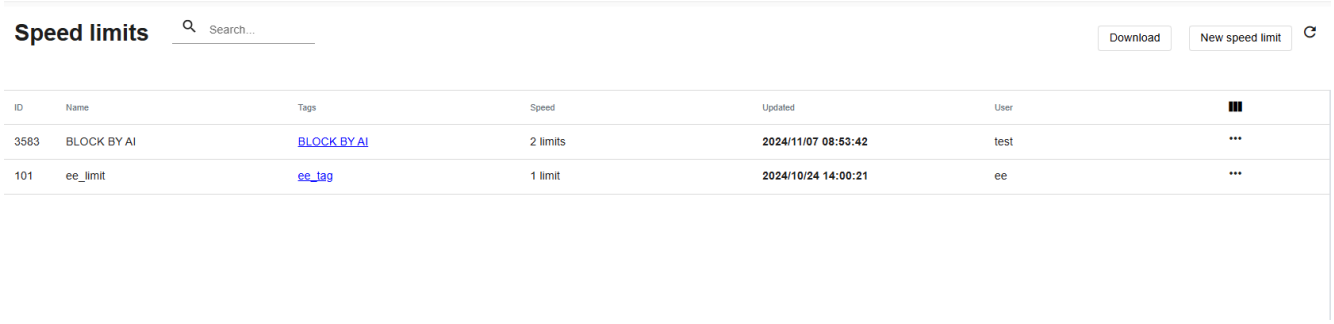
Click *Save* to save the changes or *Cancel* to reset the form. To edit a tag, click on a record in the table. The *Edit tag* form will appear on the right.

Business logic examples:

You can assign a new group of counterparties to a separate tag, based on their Sender ID and GT values, or create another tag based on obscene and other undesirable words.

Speed limits

The *Speed limits* interface serves to set limitations that are activated for tags.



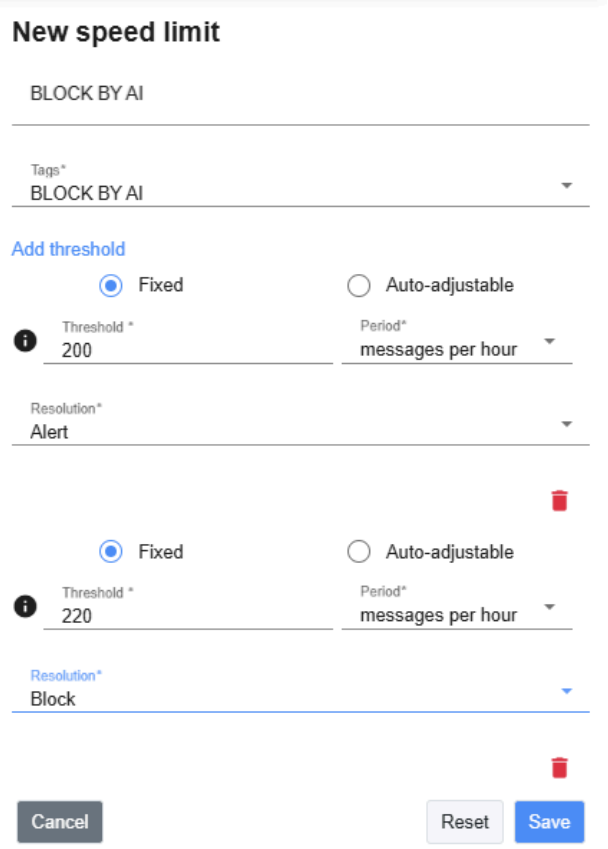
Speed Limits interface

The table has the following columns:

- **ID** - record identifier.

- **Name** - unique speed limit name.
- **Speed** - the number of limits.
- **Updated** - date when the speed limit was last updated.
- **User** - name of the System user that created the tag.
- **actions** - contains the following controls:
  - **Clone** - create a record with similar parameters.
  - **Delete** - delete the record.

Click *New speed limit* at the top of the page to create a new list of conditions.

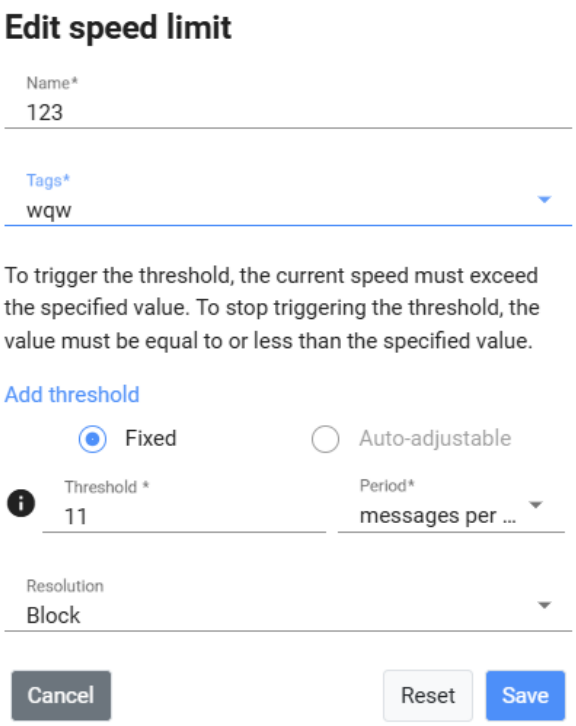


The *Speed limits* interface allows setting a threshold equal to the number of messages per minute, hour or day. When the threshold is reached, the System can either block the traffic or send an alert to the user. When the traffic decreases below the threshold, the block is not applied. It is possible to configure alerts and traffic blocking for multiple thresholds within one tag.

Additionally, a threshold value can be set as a fixed amount of messages per time unit (the default option) or as a deviation from average value in percent.

When adding a threshold value for a selected tag the user can view the tag's statistics of the average traffic speed per minute, hour or day. Hover over the icon ⓘ to view the stats. If no statistics is available for the selected tag, average values will be displayed as 0.

The *Edit speed limit* form is illustrated in the figure below.



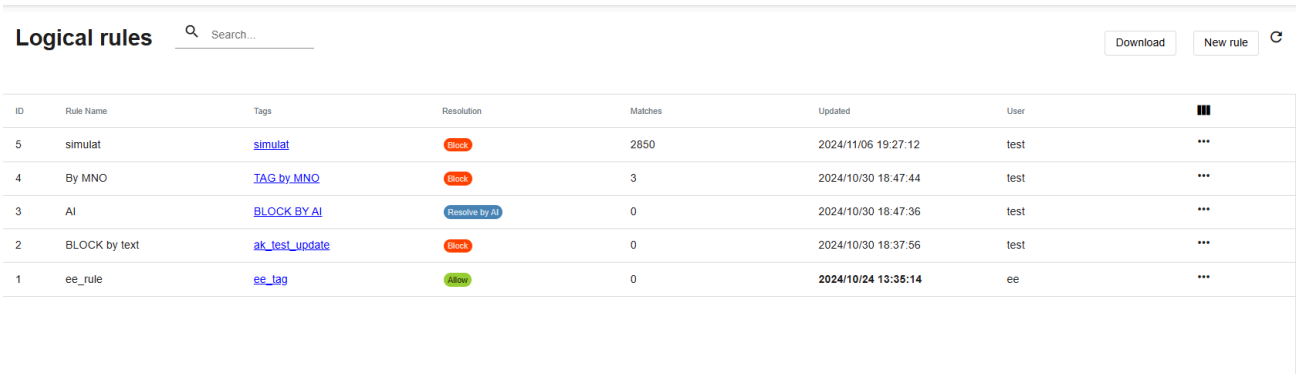
Configuring an average speed deviation

Business logic examples:
A threshold of messages per minute can be set for new partners in selected *Untrusted* tags.

Traffic volume thresholds can be set for partners (*Originating GT*), destinations (*Recipient*) or sources (*Sender ID*).

Logical rules

The *Logical rules* interface serves to link traffic resolution applicable to previously created tags.



Logical rules interface

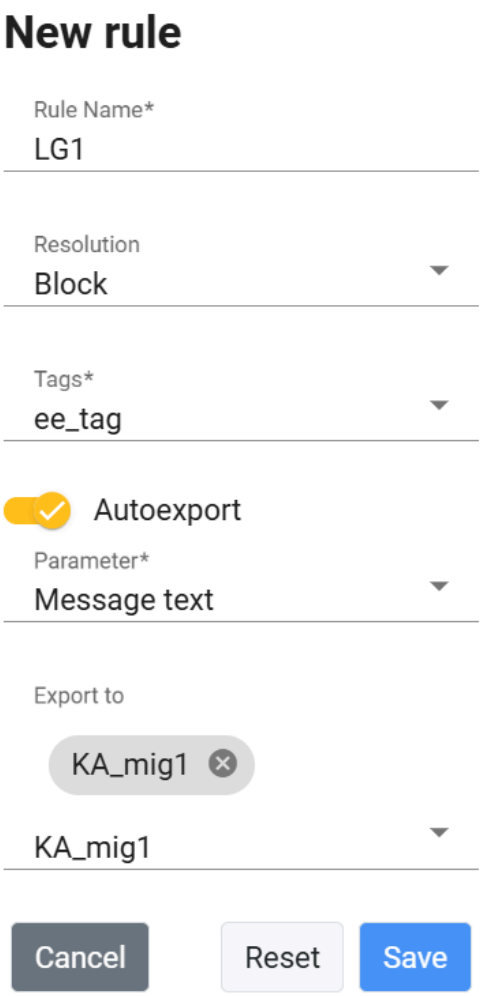
Logical rules are applied to a message when a specific tag is detected and triggers the following:

- Allow traffic
- Block traffic
- Resolve by AI: the artificial intelligence communicates to the System whether the message is SPAM and what is the prognosis accuracy of that. The accuracy for each message is written to the EDR which allows analyzing the AI efficiency. Note that the feature is charged separately. Contact your account manager to enable it.

The table has the following columns:

- **ID** - record identifier.
- **Rule Name** - name of the logical rule.
- **Tags** - the tags the rule is associated with.
- **Resolution** - the user-defined way to resolve the rule (*Block*, *Allow, Resolve by AI*).
- **Matches** - the number of times the logical rule was applied.
- **Updated** - date when the rule was last updated.
- **User** - name of the System user that created the rule.
- **actions** - contains the following controls:
  - **Clone** - create a record with similar parameters.
  - **Delete** - delete the record.

Click *New rule* at the top of the page to create a new logical rule. Configure the fields as detailed below.



Creating a logical rule

- **Rule Name** - name of the logical rule.
- **Resolution** - the way to resolve the rule (*Block*, *Allow, Resolve by AI*).
- **Tags** - the tags the rule is associated with.
- **Autoexport** - select to enable automatic export of parameter values from messages detected by the rule to the *Global rules* or *Lists of conditions.* When selected, the following fields become available:
    - **Parameter** - select the parameter whose values must be exported. Possible options are: *Sender ID, Originating GT, Message text, Recipient, Sending MNO, Receiving MNO, SMSs address*.

NOTE 1: Automatic export of the *Sending MNO* and *Receiving MNO* values is performed only if the MCCMNC reference book contains Network names corresponding to the received MCCMNCs. If the Network name is not available in the reference book or the message has no indication of it, no auto export is performed.

NOTE 2: If as a result of auto export the parameter value contains a forbidden character from the field *Forbidden characters list for export* in System settings, auto export will not be executed for such message and an alert will be sent as a popup and a record in alerts.

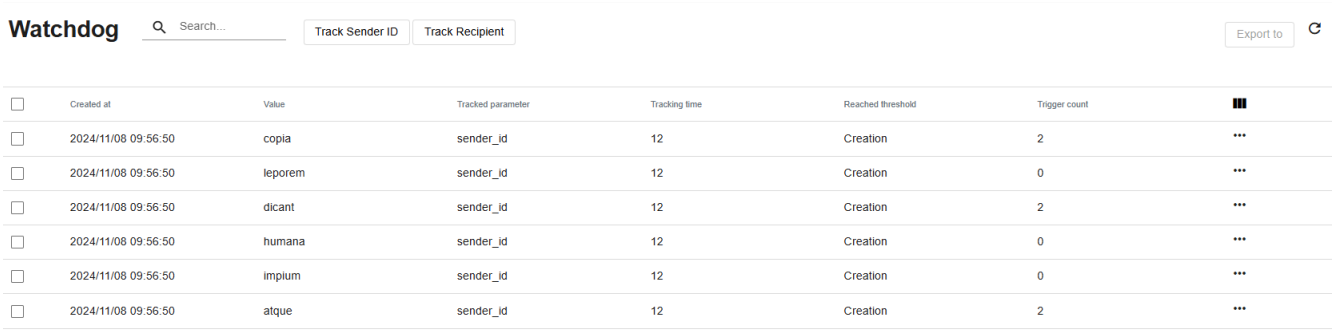
- **Export to** - select the name of the global rule or list of conditions.
- Click **Save** to save the changes.

Business logic example:

If any of the following keywords are detected in the *Message text* field of a specific tag: *Credit*, *Buy* or other *obscene words* etc, taking into account the local *Sender ID,* the message is sent to the *AI* to analyze whether the keyword is related to fraud.

Watchdog

The Watchdog interface serves for automatic traffic monitoring for any Sender ID or Recipient.

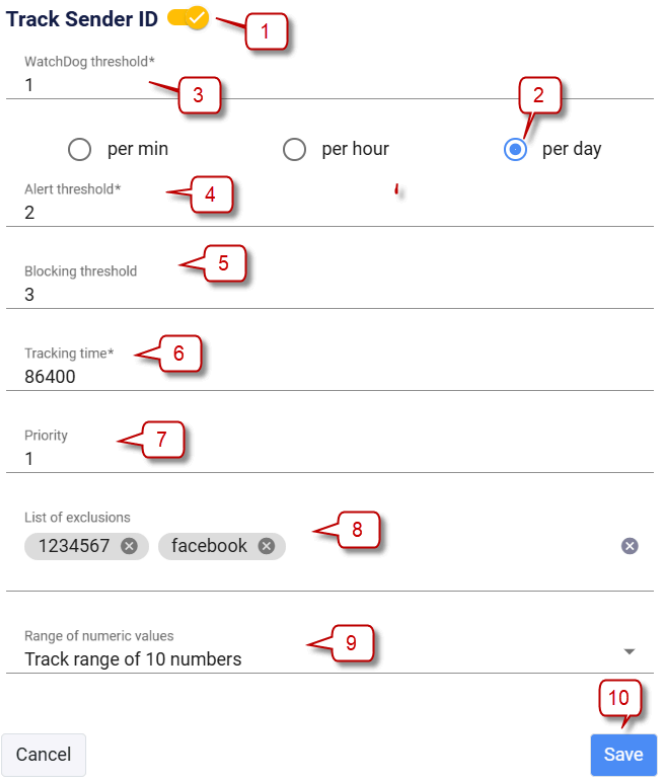


Watchdog interface

The table has the following columns:

- **Created at** - the record creation date.
- **Tracked value** - the parameter value that is being monitored.
- **Tracked parameter** - the message parameter that is being monitored (Sender ID or Recipient).
- **Tracking time** - the record validity period (with real-time countdown).
- **Reached threshold** - the previous reached threshold and its type (*Creation*, *Alert*, *Block*).
- **Trigger count** - the number of times the watchdog rule was triggered.
- **actions** - contains the following controls:
  - **Clone** - create a record with similar parameters.
  - **Delete** - delete the record.

Click *Track Sender ID* at the top of the page to configure traffic tracking by Sender ID. Click *Track Recipient* to track by Recipient.



Track Sender ID

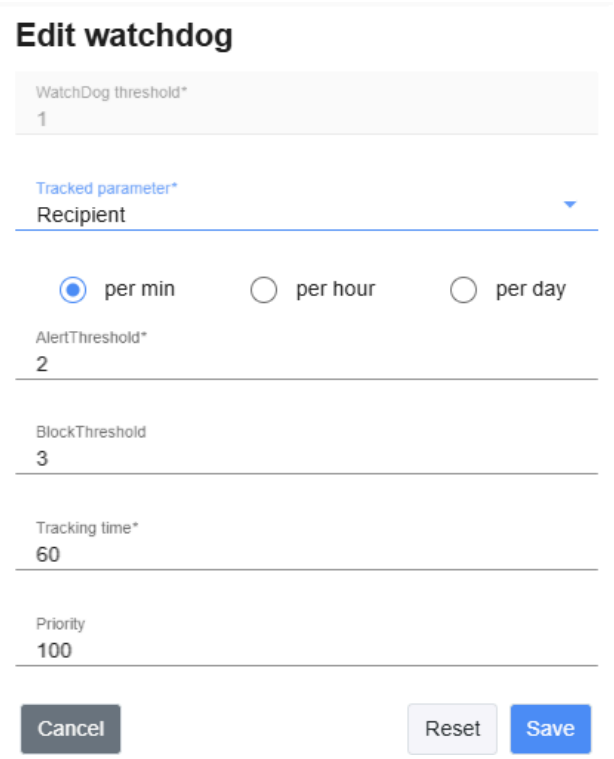
Configure the following:

1. Click to enable the record
2. Select the time period in which the frequency of the parameter usage in messages will be tracked (*per min*, *per hour* or *per day*).
3. **Watchdog threshold** - specify the frequency of the parameter usage in messages to activate the watchdog (it records the event to further use it in *Alert threshold* and *Blocking threshold*).
4. **Alert threshold** - specify the frequency of the parameter usage in messages to trigger sending an alert.
5. **Blocking threshold** - specify the frequency of the parameter usage in messages to trigger traffic blocking.
6. **Tracking time** - the rule validity period (in seconds).
7. **Priority** - the rule priority. The field value is coordinated with the tag priorities.
8. **List of exclusions** - parameter values that must be excluded from monitoring. Type the value and press Enter. Multiple values are allowed.
9. **Range of numeric values** - allows selecting a range of 100 or 10 numbers for monitoring. It allows for faster analysis and detection of entire number ranges. Possible values are:
    - **None** - the feature is disabled (monitor whole numbers, not ranges)
    - **Track range of 10 numbers** - when selected, the System tracks and transfers to the *Watchdog* and *Alerts* interfaces prefixes of a 10-number range (the last digit of each number is not taken for analysis)

- **Track range of 100 numbers** - when selected, the System tracks and transfers to the *Watchdog* and *Alerts* interfaces prefixes of a100-number range (the last two digits of each number are not taken for analysis).

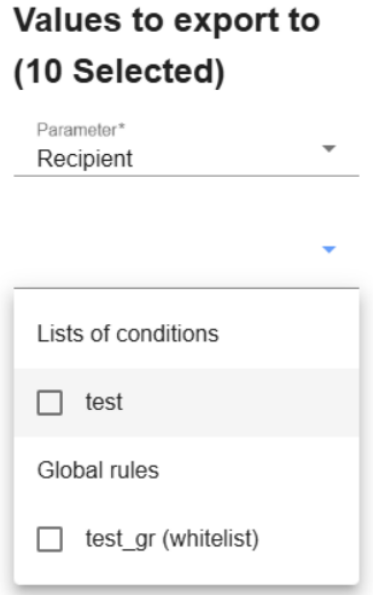
10. Click *Save* to save the rule.

The *Edit watchdog* window is illustrated in the figure below.



Edit watchdog

Click *Export to* to export the message parameter values to *Global rules* or *Lists of conditions*.



Export to

1. **Parameter** - select *Sender ID* or *Recipient*.
2. Expand the list.
3. Select the items to be exported to *List of conditions* and/or *Global rules*.
4. Click *Save* to proceed with export. The values will be displayed in the selected list of conditions or global rules.

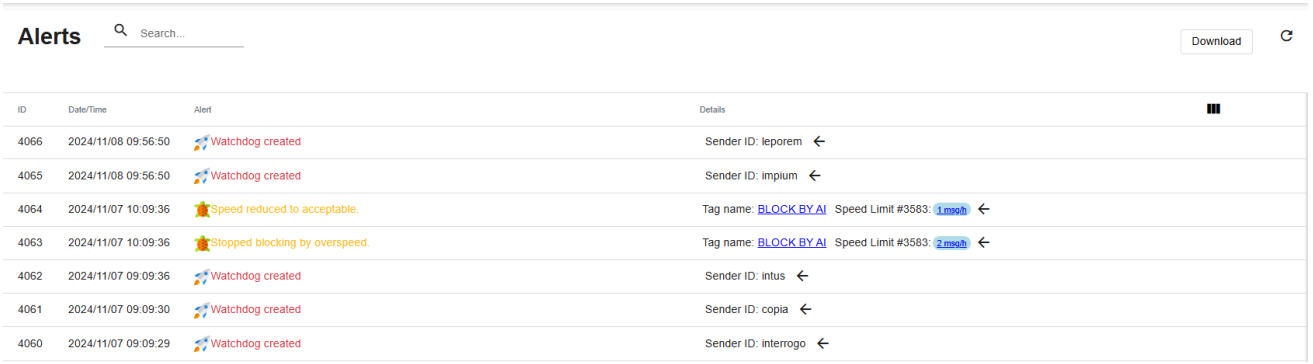
NOTE: If a value belongs to a record with *Tracked parameter=Sender ID*, and the user selected *Parameter=Recipient* in the *Values to export* form, the value will not be exported. The same is true for *Tracked parameter=Recipient* and *Parameter=Sender ID.*

Traffic monitoring

The *Traffic monitoring* section contains the following two interfaces: *Alerts* and *Analytics*

Alerts

The *Alerts* interface contains notifications on events that require user attention and prompt reaction.



Alerts

The table has the following columns:

- **ID** - record identifier.
- **Date/Time** - alert date and time.
- **Alert** - alert type. Possible values include:
    - *Overspeed detected!* - the speed exceeds the alert threshold for the tag.
    - *Speed reduced to acceptable* - the speed is equal to or below the alert threshold for the tag.
    - *Blocked by overspeed!* - the speed exceeds the block threshold for the tag.
    - *Stopped blocking by overspeed* - the speed is equal to or below the block threshold for the tag.
    - *WatchDog created!* - the frequency of use exceeds the watchdog alert threshold.
    - *Value is back to normal frequency of use* - the frequency of use is equal to or below the watchdog alert threshold.

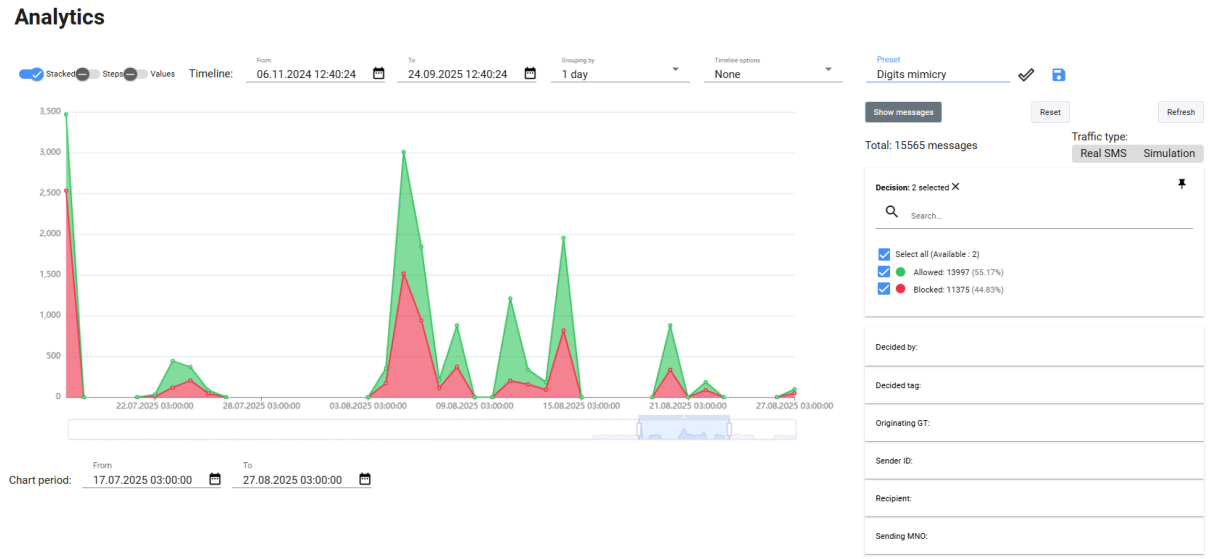
    - *Blocked by excessive use of value!* - the frequency of use has reached the watchdog block threshold.
    - *Stopped blocking by excessive use of value* - the frequency of use is equal to or below the watchdog block threshold.
    - Autoexport forbidden! - an attempt has been detected to add a value with a forbidden character to the active Lists of conditions or Global rules.
    - Export forbidden! - an attempt has been detected to add a value with a forbidden character to the active Lists of conditions or Global rules.
- **Details** - the alert details that show the triggered object. The field has the following format:
    - For tag and speed limit alerts:
        - *Tag name: <Entity name>*, the tag name with a hyperlink leading to the *Edit tag* form.
        - *Speed limit #<ID>: <threshold>*, the threshold that was exceeded, with a hyperlink leading to the *Edit speed limit* form.
    - For watchdog rules with expired timeout: *<Parameter>:<Value>.*
    - For watchdog rules with non expired timeout: *Watchdog name: <wd_name>* with a hyperlink leading to the *Edit watchdog* form
    - For the *Autoexport forbidden!* and *Export forbidden!* alerts: clickable name with routing to the Logical rule, List of conditions/Global rules forms

Business logic example:
Under normal conditions, the partner's traffic does not significantly aberrate. Suppose a partner was hacked and an unusually high amount of traffic is coming from the partner. In this case the System can reject traffic that exceeds a predefined threshold and/or notify the user in the *Alerts* interface.

The same can be applied to destinations. Suppose the System owner has historically low traffic to a pricey destination (for example, South Africa). A partner may wish to test carriers offering traffic for this destination, which may result in a traffic surge. The user can set a traffic limit for the destination and configure a 'threshold exceeded' alert in the *Alerts* interface.

Analytics

The *Analytics* interface allows tracking statistics for a specific time period.



Analytics

The following toggle switches are located in the toolbar at the top of the page:

- *Stacked*: serves to switch between the fill chart view (default) and no-fill chart view.
- *Steps*: serves to switch between line chart view and bar chart view.
- *Values*: serves to display/hide (default) chart values.

The period to access traffic data is defined by setting a start (*From*) and end (*To*) date and time in the *Timeline* field (last 24 hours by default) located at the top toolbar. When entering values manually, submit the value by pressing *Enter* or *Apply* control in the *Date picker* form.

Then configure the period interval in the *Grouping by* field (one hour by default). The period interval defines the chart scale.

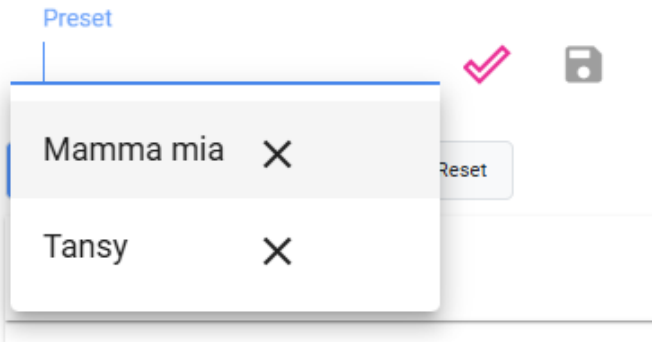
NOTE: If the *Selected timeline* is below 24 hours, the *day* value in the *Grouping by* field will be unavailable. The same applies to other period intervals.

The *Timeline options* allows quickly filling the From/To data for the *Timeline* and *Chart period* fields. Possible values are: *Last minute, Last hour, Last 3 hours, Last 6 hours, Last 12 hours, Last 24 hours, Last week, Last month, Last 3 months, None*.

The *Selected period* field below the chart defines the period for which the chart is displayed. The period can also be adjusted with the help of the slider located under the chart. This control allows zooming in a specific period and viewing the data in more detail. For example, if the *Selected timeline* is a month long, and a traffic anomaly happened on a specific day, the user may want to view this day in high detail, and set the *Selected period* to the specific day. The *Selected period* is for viewing convenience only; all data in the *Selected timeline* will continue to be available.

The right hand panel contains the *Preset* toolbar and a set of filters.

The *Preset* toolbar allows the user to save the parameters of the *Analytics* page and then access them when necessary. To save a new preset, enter its name in the edit box and click . To open a preset, insert the cursor in the empty edit box, select the preset in the drop-down list and click . To remove a preset, select it in the list and click .



The filters serve to access traffic data that are displayed on the chart and can be exported as EDRs or message parameters.

On top of the filter panel the following details and controls are displayed:

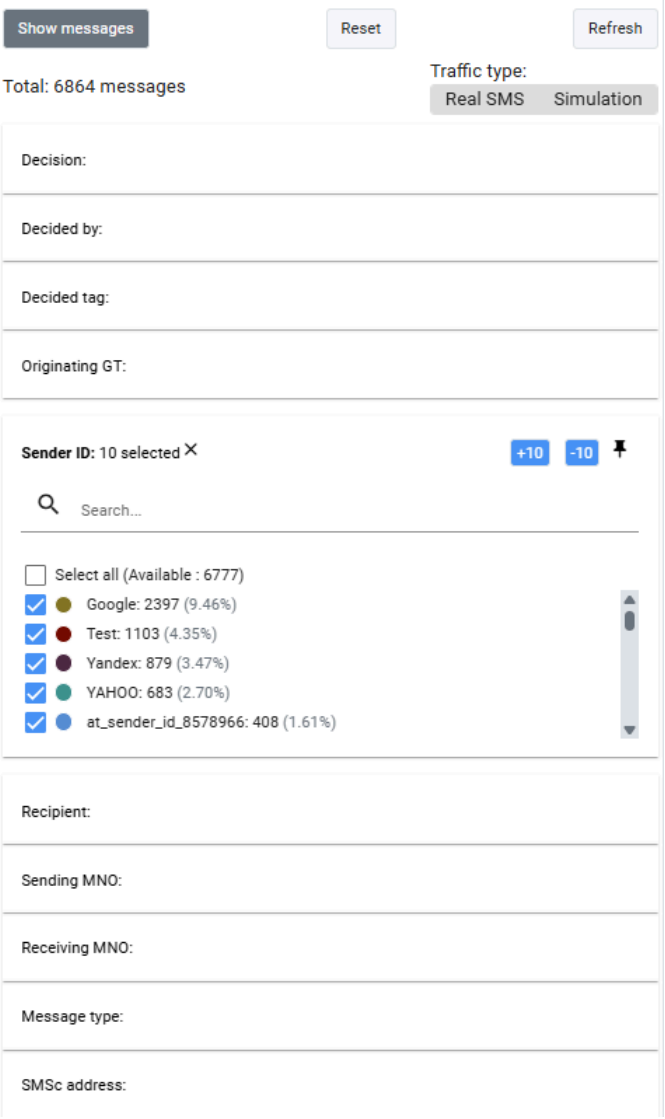
- *Total*: shows the total number of messages for the selected filter.
- *Traffic type*: *Real SMS* or *Simulation*. Click the appropriate value(s) to display the details on real-life and/or simulated traffic.

The filter panel contains the following filters:

- *Decision* (selected by default): date on which the decision on a message was taken *Decided by*: the reason based on which the the decision was made
- *Triggered tag* (see *NOTE* below): the tag that triggered filtering of the message
- *Originating GT*
- *Sender ID*
- *Recipient*
- *Sending MNO,*
- *Receiving MNO*
- *Message type*: *MT* or *MO*
- *SMSc address*

NOTE: The *Triggered tag* filter also contains the *Tag not triggered* value. It shows traffic for which the tag was not triggered but the default decision was taken (configured in Settings\System settings).
The chart displays the traffic share for each filter value in descending order in percentage. Each filter allows working with all data available for the *Selected timeline.* However, by default only the first 10 matches in each filter value are shown. . Click the +10 control next to

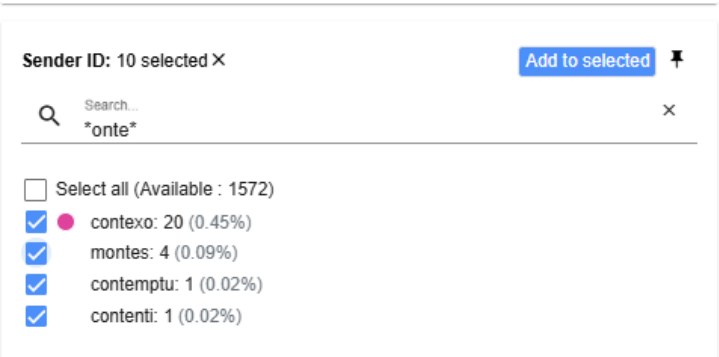
the filter value to select the next 10 available matches for display as shown in the figure below. The control will change to -10. Click it to deselect the matches.



Selecting additional matches for display on the chart

Select checkboxes next to the filter values to show them on the chart.

For exact match search enter the keyword in the filter edit box (only single-word search is supported). For partial match search use the symbol ***** to search for any number of any characters before or after the keyword. Use the symbols **?** to denote any character before or after the keyword (for example, to search for the value *message* use the expression mes????).



Select checkboxes found in the search and add to the selected filter sample by pressing the control Add to selected *Add to selected*.

Once you switch between the filters (*Triggered tag*, *Originating GT*, *Sender ID* etc.), the selected values of the previously accessed filter are reset. To combine the values of several filters, use the control 📌 *Pin* located next to each filter name.

The following controls are located at the top of the filter panel:

- *Show log (Hide log)*: serves to toggle the bottom table with records from *Messages* displayed based on preset filters.
- *Reset*: serves to clear the filters and resets all fields to default values.
- *Refresh*: serves to refresh the filter values and update the *Messages* data in the bottom table.

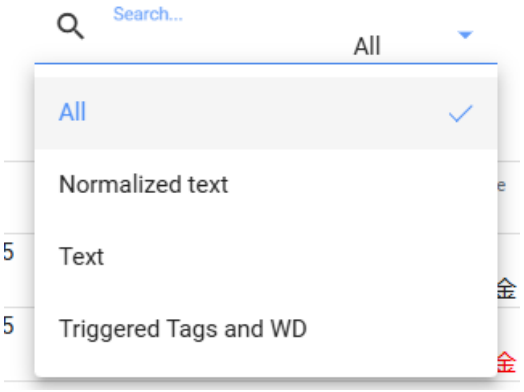
Business logic example:
The user monitors the statistics and finds time intervals when mass fraud occurred. Then the *Messages* table is used for analysis of the reason for the traffic surge.

Click *Show messages* in the top right panel to display the table *Messages* that contains logs of decisions made to messages. Each log record corresponds to one message and contains the following information:

- **Decided at** - Date on which a decision on a message was taken
- **Decision** - The decision to pass or reject the message
- **Decided by** - The reason based on which the the decision was made. Possible values include:
  - *Global rule*
  - *Logical rule*
  - *Threshold*
  - *Watchdog*
  - *Default No rule decision*
  - *AI after rule*
  - *Default AI No rule*

  - *AI No rule*
  - *Default AI after rule*
  - *URL scanner* - only for *Decision=blocked*
  - *MO spoofing* - only for *Decision=blocked* and *Message type=MO*
  - *Default MO spoofing* - only for *Decision=blocked* and *Message type=MO*
  - *Binary SMS* - only for *Decision=blocked*
  - *Binary SMS check* - only for *Decision=blocked*
- **Message text**
- **Normalized text** - text after normalization that triggered the rule. Normalization is configured in the Text normalization interface.
- **Sender ID**
- **Recipient**
- **Originating GT**
- **Sending MNO**
- **Receiving MNO**
- **Message type**: *mo* or *mt*

All records are displayed in descending order by date. Use the *Search* field to locate the records.



Search field

- Select *All* to search in columns: *Message text, Cleaned up text, Sender ID, Recipient, Originating GT, Sending MNO, Receiving MNO.*
- Select *Normalized text, Text* or *Triggered Tags and WD* to search by the fields *Normalized text, Text,* or tag name and Watchdog rule, respectively.

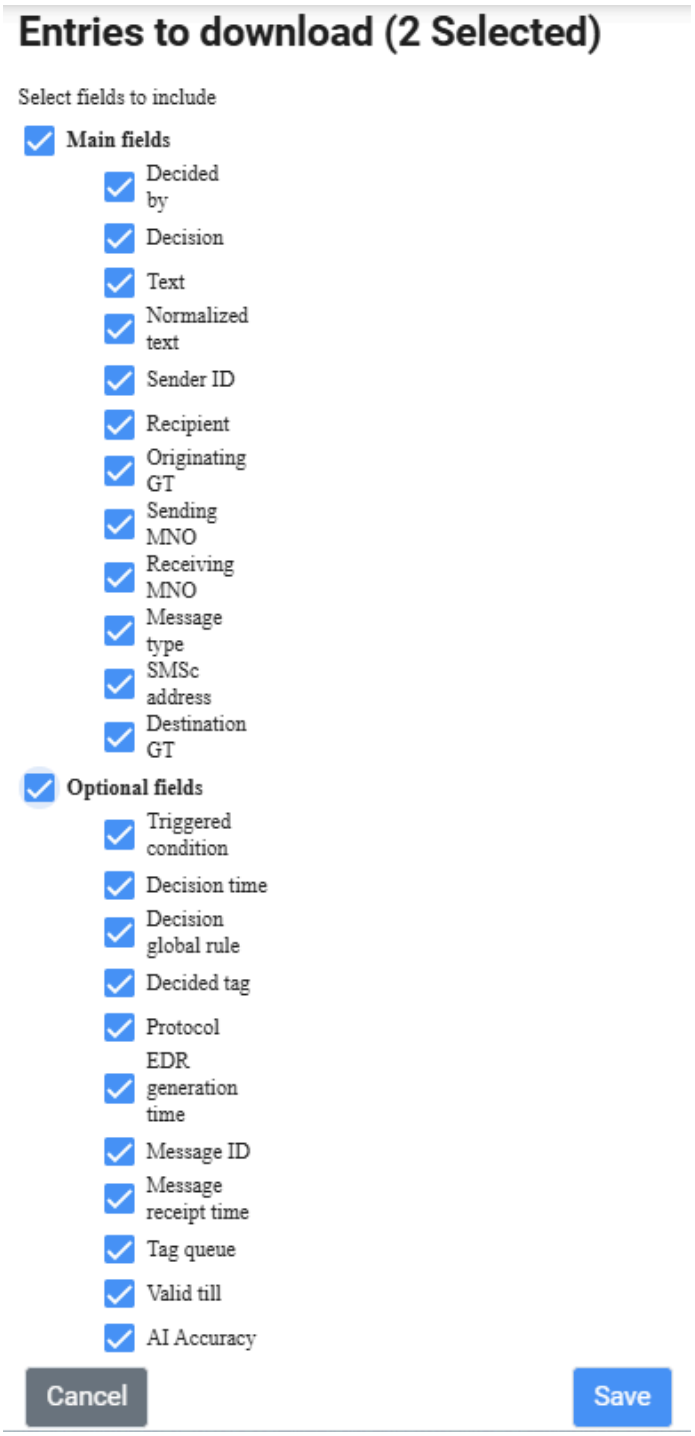
Use the multiple keywords to search for exact matches with spaces. Matches found in search are highlighted in yellow. Message parts or parameters that triggered the rule are highlighted in red or not highlighted if no rule was found. Multiple parameters can be highlighted in red if the rule with multiple parameters combined by AND was triggered.

Decided at	Decision	Decided by	Message text	Normalized text	Sender ID	Recipient	Originating GT	Sending MNO	Receiving MNO	Message type	SMSc address	Destination GT
24.09.202 16:28:38	Blocked	Default No rule decision	vv @@		YAHOO	12000000	GT2	555055	555055	mt	123123	111111
24.09.202 16:27:42	Blocked	by logical rule	vv @@		YAHOO	12000000	GT2	555055	555055	mt	123123	111111
24.09.202 16:12:24	Blocked	by logical rule	vv @@		YAHOO	12000000	GT2	555055	555055	mt	123123	111111
24.09.202 16:06:21	Blocked	by logical rule	vv @@		YAHOO	12000000	GT2	555055	555055	mt	123123	111111
24.09.202 14:53:01	Blocked	Default No rule decision	vv @@		YAHOO	12000000	GT2	555055	555055	mt	123123	111111
24.09.202 14:52:25	Blocked	by logical rule	vv @@		YAHOO	12000000	GT2	555055	555055	mt	123123	111111
24.09.202 14:51:05	Blocked	by logical rule	vv @@		YAHOO	12000000	GT2	555055	555055	mt	123123	111111
24.09.202 14:45:25	Blocked	by logical rule	vv @@		YAHOO	12000000	GT2	555055	555055	mt	123123	111111
24.09.202 14:44:04	Blocked	by logical rule	vv @@		YAHOO	12000000	GT2	555055	555055	mt	123123	111111
22.09.202 18:12:18	Blocked	by logical rule	vv @@		YAHOO	12000000	GT2	555055	555055	mt	123123	111111

Analytics interface with open Messages

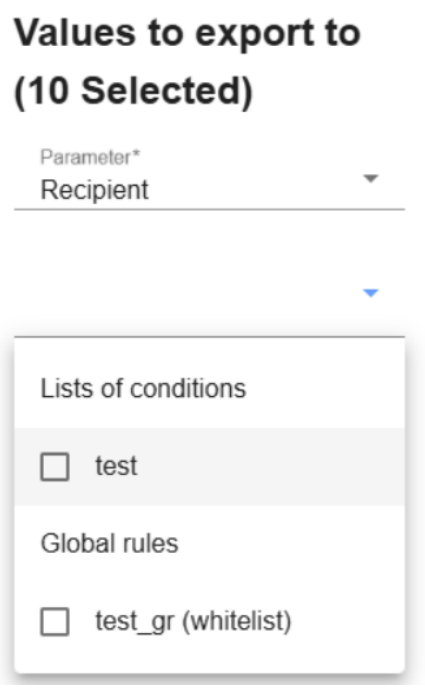
The interface allows selecting specific records or all records. The user can download selected records as EDRs in the CSV format for specific main and optional fields or export parameters values to the interface: to the available *Lists of conditions* and *Global rules*. If a record is already included in another list, the System allows adding it to another list irrespective of whether the list is enabled or disabled.

NOTE: The maximum number of records that can be downloaded is 100,000.
To download EDRs, click Download *EDR,* select the fields as shown in the figure below and click *Save*.



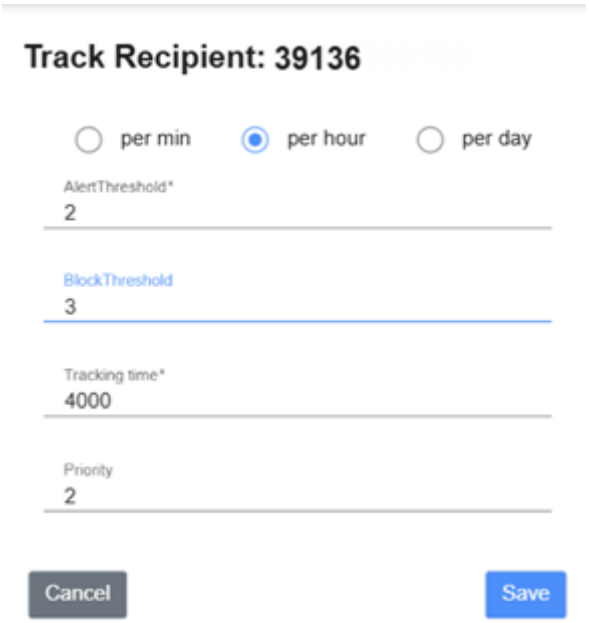
Download EDR

Click *Export to interface* to export the values to the interface (to *Global rules* or *Lists of conditions*). The functionality is similar to export from the Watchdog interface.

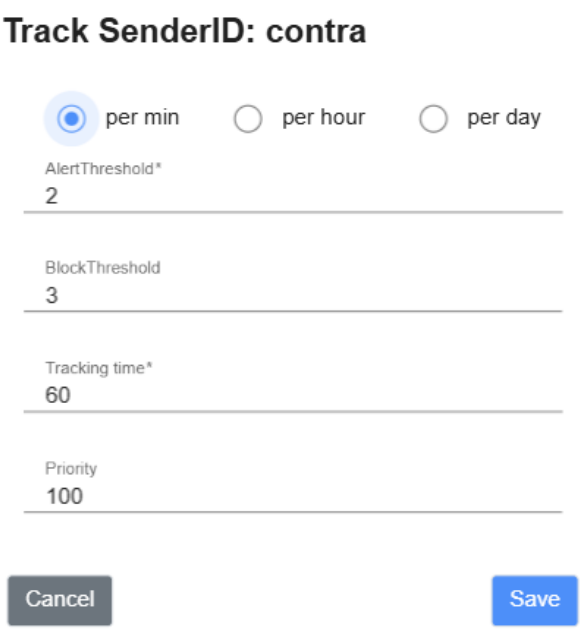


Export to interface

Click *Track Sender ID* to configure traffic tracking by Sender ID (by watchdog). Click *Track Recipient* to track by Recipient. The functionality is the same as detailed in the Watchdog interface.



Track Recipient

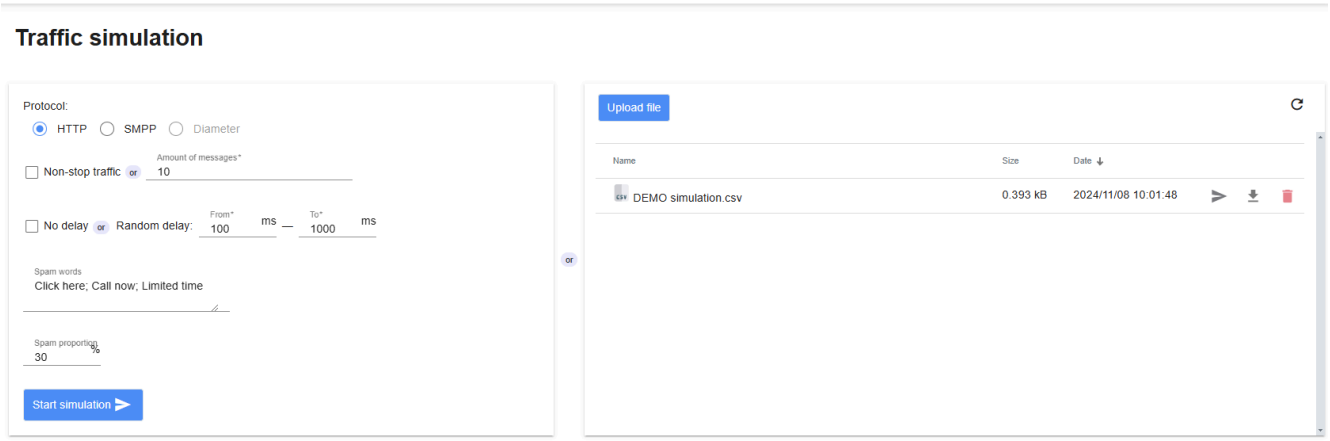


Track Sender ID

Business logic example:
Tracking fraud in specified periods to determine regularities. Based on this information, lists are updated. For example, the list of known local numbers (Originating GTs) used in SIM gateways.

Traffic simulation

Traffic Simulation serves for traffic generation in two modes: for analysis of elementary fraud and more complex fraud.



Traffic simulation interface

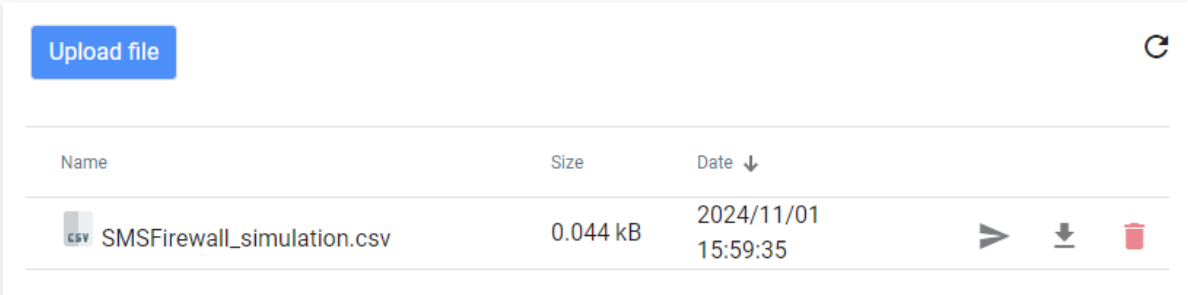
Both modes allow traffic simulation with verification of all filters applicable to real-life traffic.

Traffic generation for analysis of elementary fraud does not require loading a CSV file and is based on a preconfigured template. Traffic can be generated in HTTP and SMPP formats. The user can define the number of messages for analysis (*Amount of messages)* or allow *Non-stop traffic* that can be interrupted at any time by clicking *Stop traffic simulation*. Besides, the System allows sending messages with no delay (*No delay* control) or sending traffic non stop (*Non-stop traffic* control) that can be interrupted at any time by clicking the *Stop traffic simulation* icon.

Additionally, the user can configure sending *No delay* or *Random delay* messages within a predefined range. It is also possible to configure comma-separated spam words for analysis of elementary fraud (*Spam words* field). The user can control the spam share in generated traffic by setting a percentage value in the *Spam proportion* field. Click *Start traffic simulation* to launch simulation.

To analyze more complex types of fraud, generation based on a CSV file is used. It allows uploading messages with all parameters needed for analysis: *Sender ID*, *Recipient*, *Message text*, *Originating GT etc*.

Traffic can also be generated from CSV files. Generation from file is mainly intended for CDR/EDR files. Click *Upload file* to upload the file to the System. Then click ➤ to launch simulation.



Simulation from file

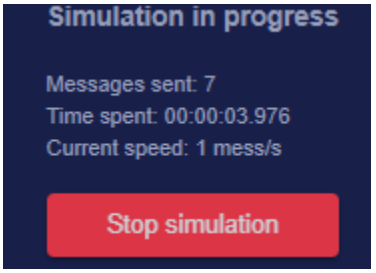
NOTE: Currently the System allows uploading CSV files after manual parsing only. The file must contain fields separated by semicolon (no blank space), following in the exact order detailed below. The simulation starts from the first row in the file; no header is required. The fields are as follows (must come in the order as specified, all are required, all can be void):

- **Protocol** - traffic protocol.
- **Number of segments** - the number of message segments.
- **Segment number** - the segment's counting number.
- **Message text** - message text.
- **Originating GT** - the source global title.
- **Sender ID** - sender ID.
- **Recipient** - recipient number.
- **Sending MNO** - sender's network number.
- **Receiving MNO** - recipient's network number.

- **Message type** - the message type.
- **SMSc address** - the SMSc address obtained from the Query Constructor (Alaris SS7 Suite).
- **Destination GT** - the source's Global title.

NOTE: If at least one of the fields is missing, all the fields will be ignored during simulation.

Once simulation is started, its statistics is shown in the bottom left area of the page as shown in the figure below.



Simulation stats

Click *Stop simulation* to interrupt the process. Once simulation is complete or interrupted, the *Stop simulation* button is replaced with *Go to messages* that opens the *Analytics* interface showing details of the simulation.

The interface allows the user to:

- Check filtering rules with lists of values.
- Generate a test file based on EDRs and run it through SMS Firewall to see its capabilities.
- Check and improve the neural network dataset.

Flash call detection

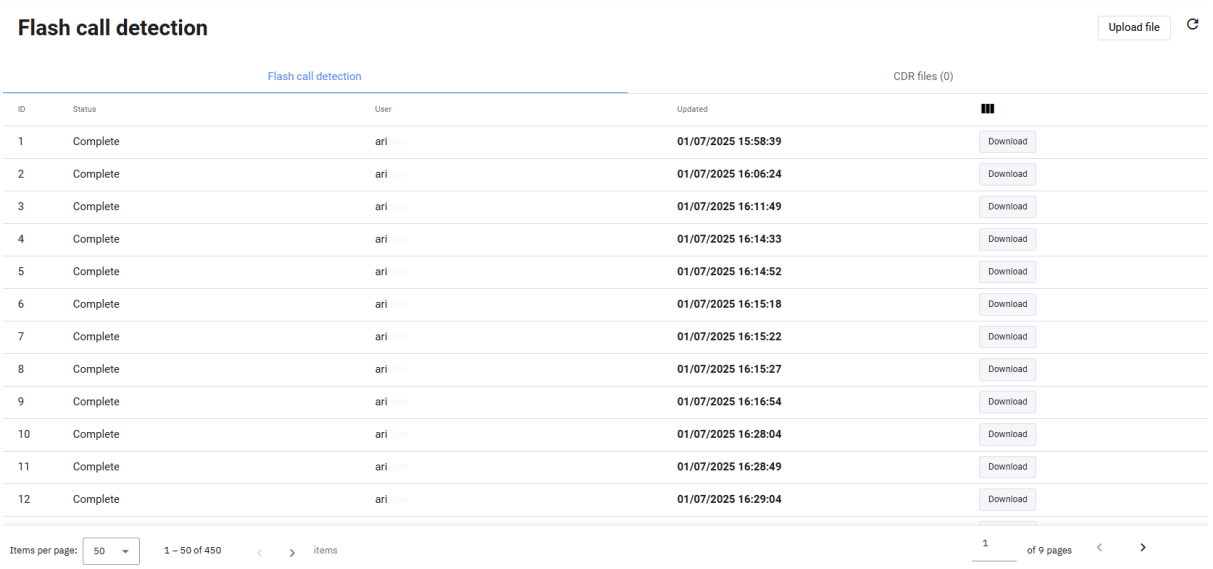
Note that this feature is charged separately. Contact your account manager to enable it.

Flash calls are a new and innovative way to remotely authenticate end users. In a flash call, the network works the same way as in a regular call but no real conversation happens.

- **Problem**: since the call is not formally "completed", the operator does not receive money, although resources were spent.
- **Solution**: consider not only the call, but also the fact of the attempt to be billable, in order to compensate for the load on the network and monetize this traffic.

The first step to monetizing and controlling flash calls is successful detection of such calls, with a high level of accuracy and low false positive rate. Once a dedicated trunk group is created, independent of existing international voice trunk groups, MNOs can enable flash call termination and call billing on attempts.

Incoming flash calls can be **blocked** and redirected through alternative authentication channels such as SMS. This may result in an immediate increase in SMS A2P traffic.



Flash call detection

The Flash call detection interface consists of two tabs - *Flash call detection* and *CDR files*, and a toolbar at the top with the *Upload file* button and the refresh button .

The procedure is as follows:

1. The user uploads a CDR file for analysis and detection of flash calls (*Upload file* button).
2. The user configures and launches the analysis task in the CDR files tab.
3. The user views the analysis result and can download it in the *Flash call detection* tab.

Business logic example:

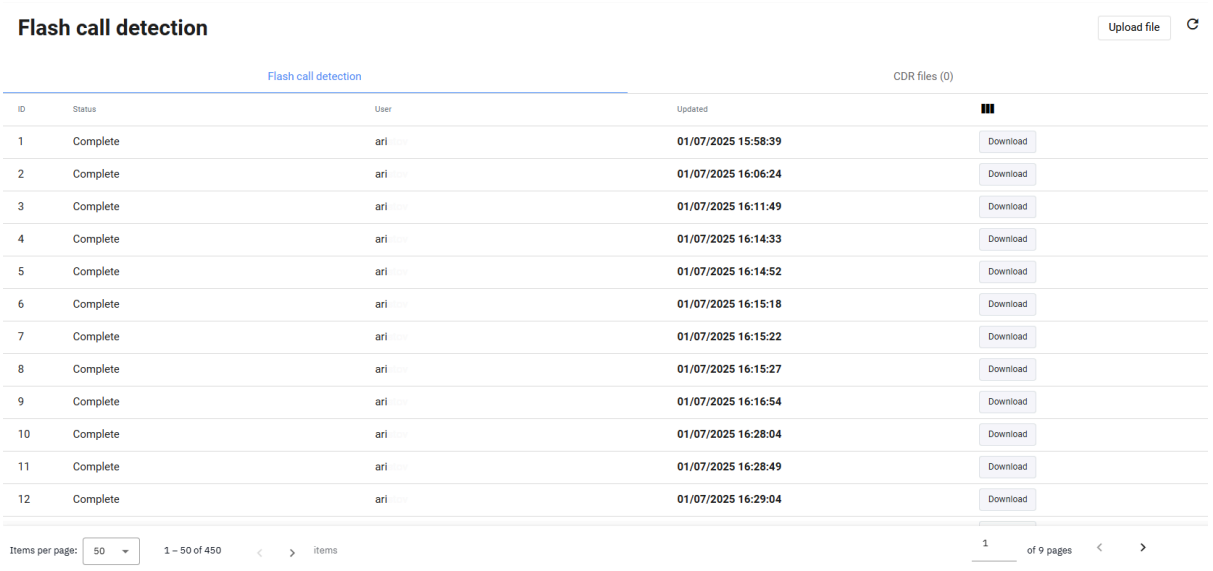
1. An SMS firewall user wants to import CDRs to monitor the bulk calls and analyze the data for unauthorized use of voice authentication.
    - The System allows manual mapping of data by columns to be included in the parameter analysis, and columns to be included in the report.
    - The System performs CDR analysis by: the number of CGPN calls, call duration in seconds, and disconnect code.

Use case: The CDR file contains 1,000 rows. The A-number analysis settings are as follows: the minimum threshold is 10 calls, the percentage of toxicity is 50%, and the duration is not more than 10 seconds. In the report, the flash call profile will include numbers with zero duration according to the minimum threshold.

2. An SMS firewall user wants to generate a report with lists of A-numbers detected as a result of analysis, to exclude repeated unauthorized use of flash calls.

- Report contents: number of CGPN calls (total number of calls from the A-number), Traffic type (calls belonging to a certain type of traffic), and Trunk code (calls belonging to a trunk).
- Traffic type is separated by the following profiles: Flash call or Invalid, if no profile is matched.
- possibility to download the report or send it by email to a specified address
- report data sorting by columns.
- restart analysis of the same CDRs but for ranges of 10, 100, 1000, 10000, 100000, 1000000 numbers.

Flash call detection tab



Flash call detection tab

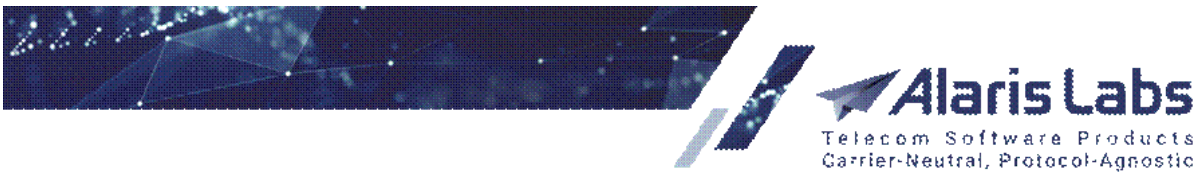
The *Flash call detection* tab contains a table of tasks started at the *CDR files* tab.

The table has the following columns:

- **ID** - record identifier.
- **User** - user that started the task.
- Updated - date of the task creation.
- **actions** - contains the *Download* button that serves to download the report in an Excel file.

CDR files tab

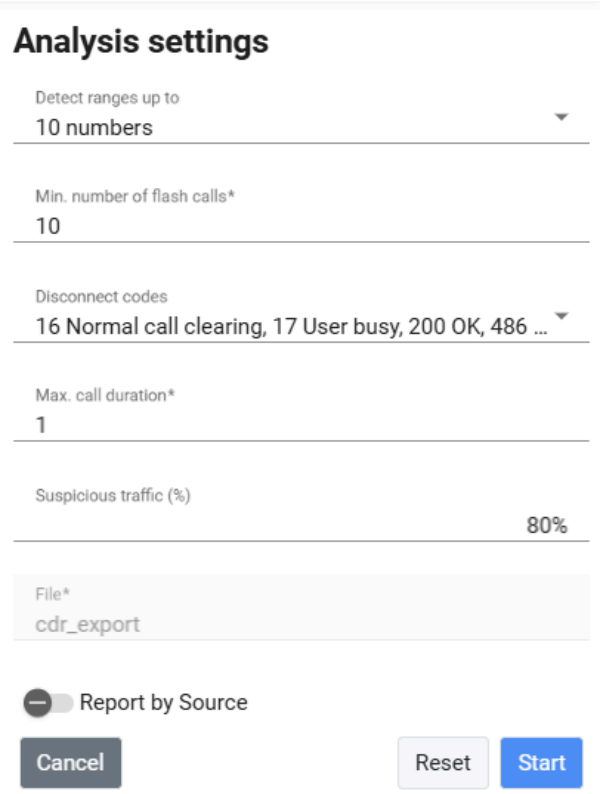
The *CDR files* tab contains a table that shows all CDR files uploaded to the System for analysis. It serves for configuring and launching analysis tasks.



CDR files tab

Proceed as follows:

1. Click *Upload file* to upload a CDR file to the System (csv, separated by semicolon ;). The file must contain the following columns:
    a. **CGPN** (required) - the calling number. Max. length is 15 characters, min. length is 3 characters; only positive integers are allowed.
    b. **CallDuration** (required) - duration of the call in seconds. The length is 2 characters, positive integers only.
    c. **DisconnectCode** (required) - call disconnection code for the calling number. Only Q.931, Q.850 and SIP classification codes are accepted: an array of those set in System settings.
    d. **Source** (optional) - call source, in fact the data can be taken from Trunk group code or Product ID of Alaris InVoice. The value length is 15 characters, including letters and special characters.
    e. **Timestamp** (optional): time and date of the call. The date and time format is checked with the System settings.
2. The file will appear as a row in the table. Click Analyze in the appropriate row and configure the analysis settings as detailed below:



Analysis settings

a. **Detect ranges up to _____** - select the number range in the drop-down list. Available values are: *None, 10 numbers, 100 numbers, 1000 numbers, 10000 numbers, 100000 numbers, 1000000 numbers*. If *1000000 numbers* is selected, the System detects repeated use of a range of numbers up to 6 digits inclusive, if *10 numbers* is selected, the number range up to 6 digits is detected, if *None* is selected, only the whole number reuse is detected.

b. **Min. number of flash calls** - minimum number of flash calls that will be analyzed by Suspicious traffic percentage. If less than the specified number is detected, the data is ignored and not included in the report.

c. **Disconnect codes** - list of call disconnect codes to analyze the pool of numbers. Possible values are:

16 Normal call clearing (Q.931)
17 User busy (Q.931)
16 Normal call clearing (Q.850)
17 User busy (Q.850)
200 OK (SIP)
486 Busy here (SIP)
18 No user responding (Q.931)
19 No answer from user (Q.931)
18 No user responding (Q.850)
19 No answer from user (Q.850)
487 Call cancelled (SIP)

480 Temporarily unavailable (SIP)

This is a default list that comes with the System. Users can add their own codes in System settings. By default the following codes are selected: 16 Normal call clearing (Q.931), 17 User busy (Q.931), 16 Normal call clearing (Q.850), 17 User busy (Q.850) 200 OK (SIP), 486 Busy here (SIP).

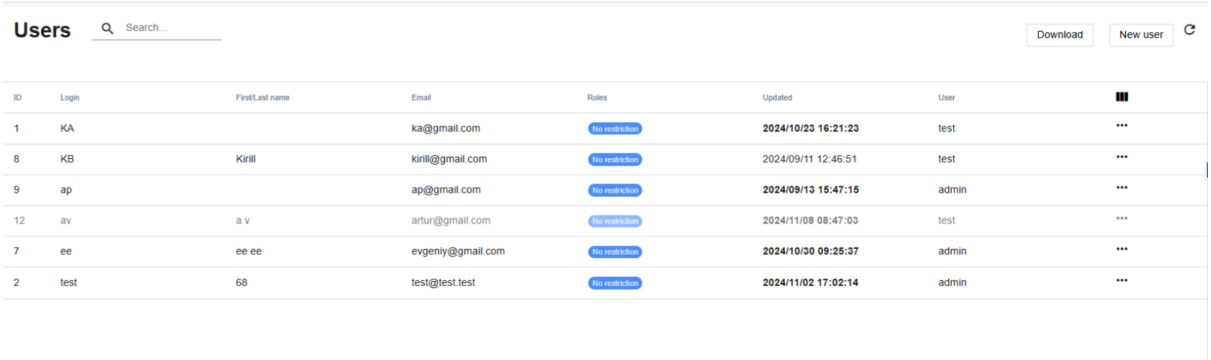
d. **Max. call duration** - max. call duration in seconds for analyzing the number pool. The default value is 1. The minimum value is 0, the maximum value is 99.
e. **Suspicious traffic (%)** - percentage of flash calls among all calls from this A-number to be added to the report. The percentage is calculated based on the specified *Min. number of flash calls*, *Max call duration* and *Disconnect codes*. The default value is 80%.
f. **Report by Source -** enable reporting breakdown by source - if the *source* column with data is available.When enabled, the report archive will contain an additional file with flash calls grouped by source.
g. Click *Start* to launch the task. The task will appear in the *Flash call detection* tab. Once it is completed, Click *Download* to get a copy the report (an archive with Excel files).

3. In the *Flash call detection* tab, click *Open file* to view the CDR. Click *Delete* to delete the file.

Users and Roles

Users

The *Users* interface serves to control user accounts, to which roles with various permission sets are assigned.



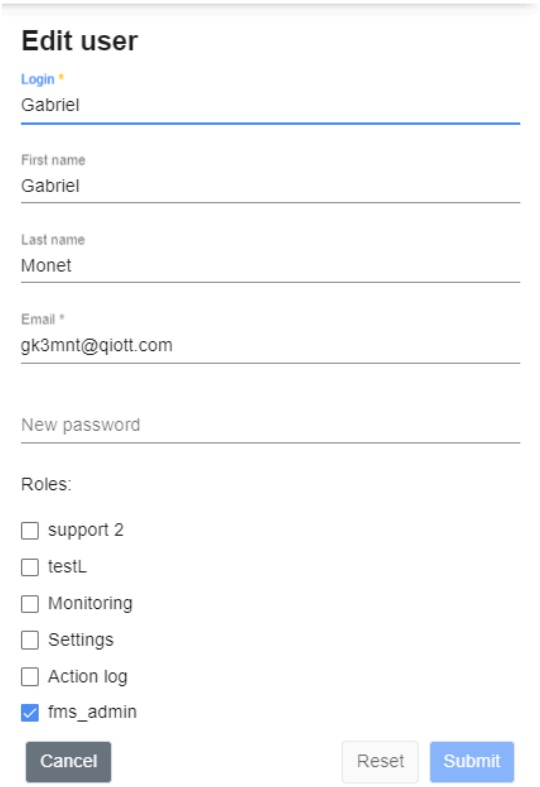
Users interface

The table has the following columns:

- **ID** - record identifier.
- **Login** - the user's login name.
- **First name** - the user's first name.

- **Last name** - the user's last name.
- **Email** - the user's email address.
- **Roles** - name of the user's role (configured in the Roles interface). A user can be assigned multiple roles.
- **Updated** - date of the last record update.
- **User** - login of the user that created or updated the record.
- **actions** - contains the following controls:
  - **Disable/Enable** - deactivate/activate the user record. If a user has been disabled while it is logged in the System, its session will not be terminated. However, the user will not be able to log in next time.
  - **Delete** - delete the record.

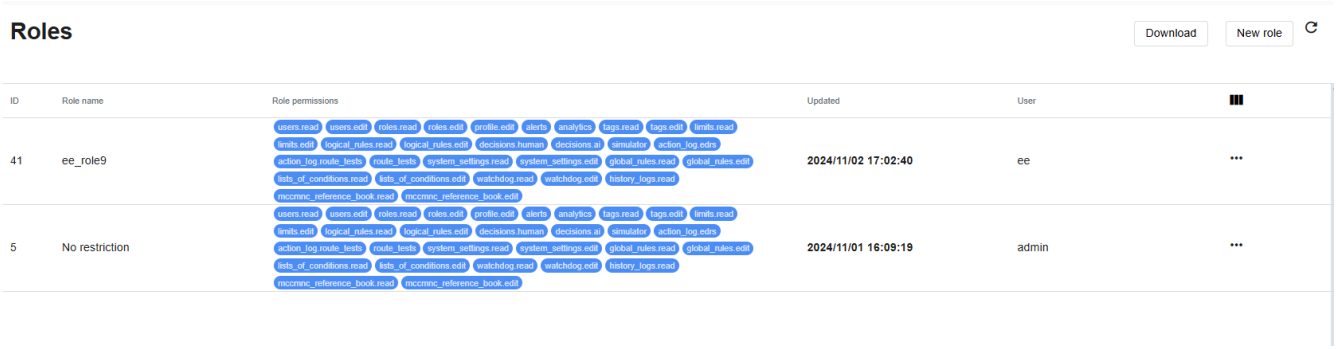
Click *New user* to create a user record. To edit a user, click on the appropriate record in the table. The *Edit user* panel is shown in the figure below.



Editing a user

Roles

The *Roles* interface serves to manage roles and their permission sets.

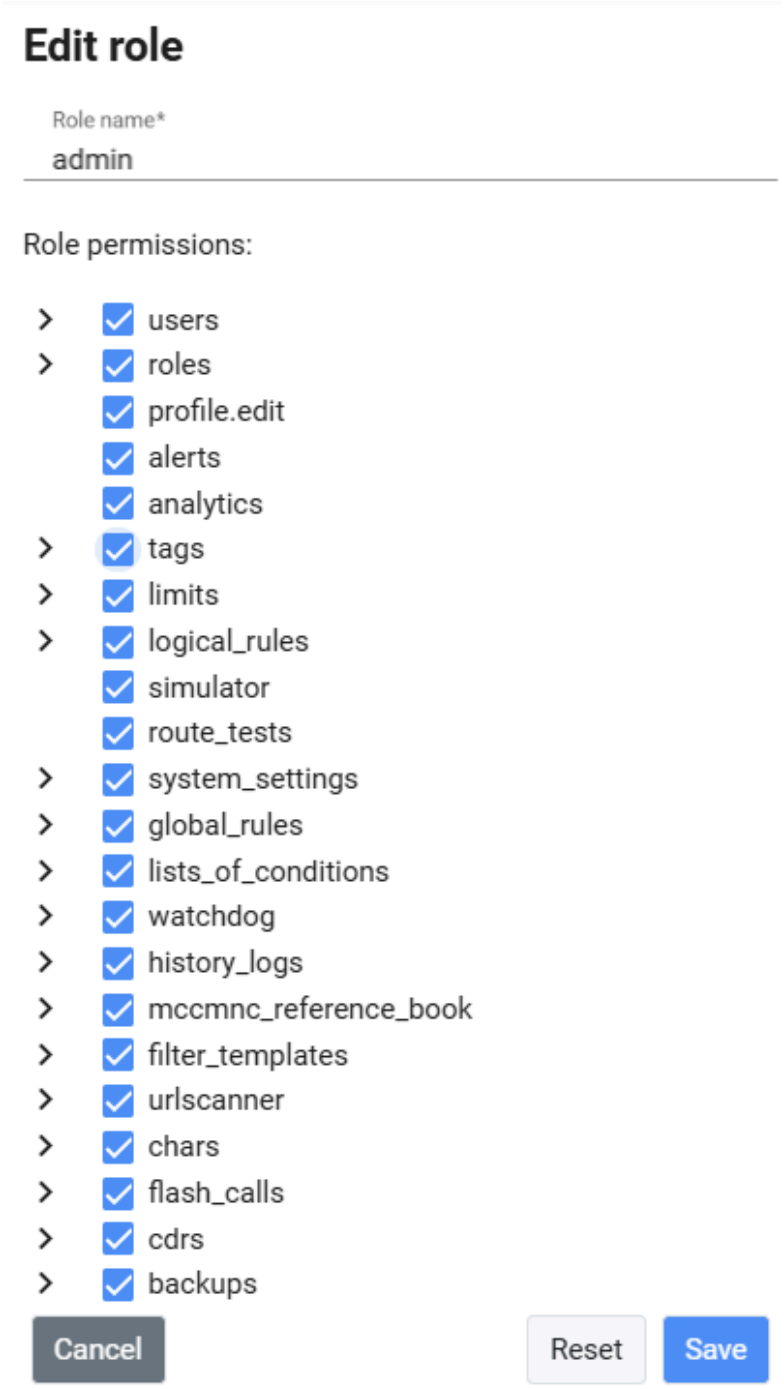


Roles interface

The table has the following columns:

- **ID** - record identifier.
- **Role name** - name of the role.
- **Role permissions** - names of permissions that are included in the role.
- **Updated** - date of the last record update.
- **User** - login of the user that created or updated the record.
- **actions** - contains the following controls:
  - **Clone** - create a record with similar parameters.
  - **Delete** - delete the record.

Click *New role* to create a user record. To edit a role, click on the appropriate record in the table. The *Edit role*panel is shown in the figure below.



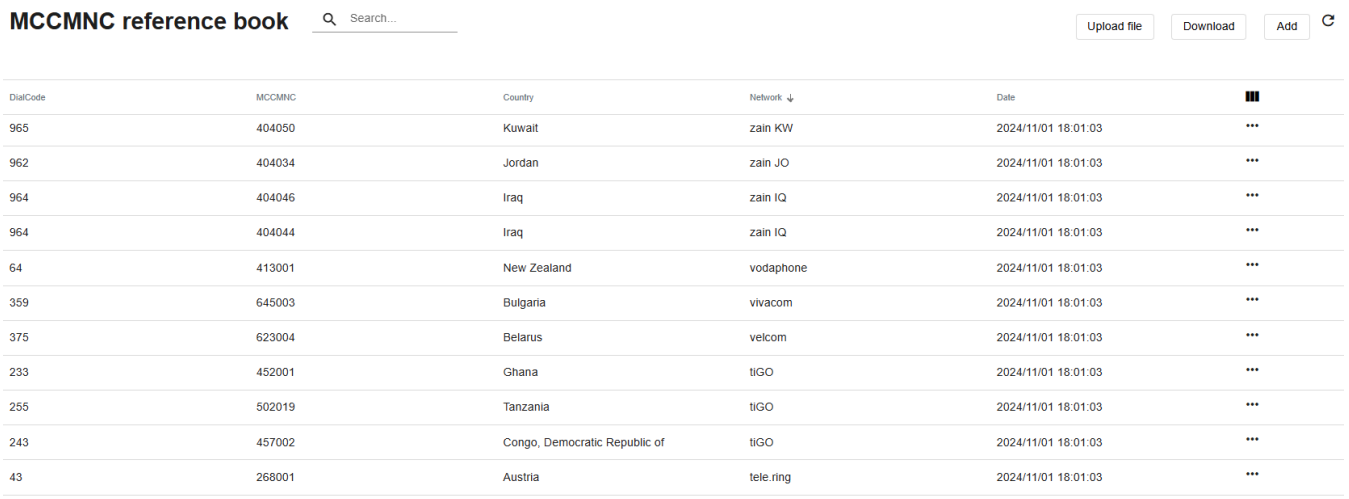
Editing a role

Business logic example:
The interface allows the user to single out first line technical support by assigning them view only rights.

MCCMNC reference book

The *MCCMNC reference book* serves for matching MCCMNC received from MNP servers with network names configured in the reference book. This allows using the network names in tags, global rules and lists of conditions for more convenient data filtering by operator.

The reference book table contains information about all MCCMNC records available in the System.



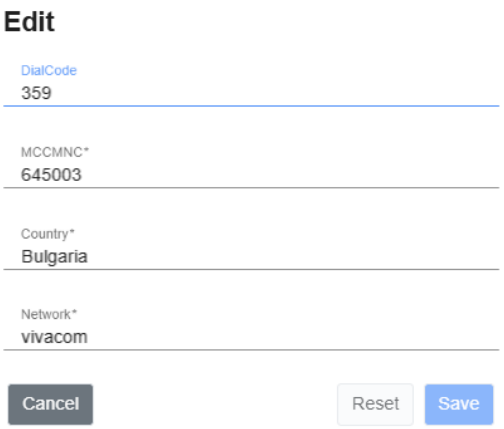
DialCode	MCCMNC	Country	Network	Date	
965	404050	Kuwait	zain KW	2024/11/01 18:01:03	•••
962	404034	Jordan	zain JO	2024/11/01 18:01:03	•••
964	404046	Iraq	zain IQ	2024/11/01 18:01:03	•••
964	404044	Iraq	zain IQ	2024/11/01 18:01:03	•••
64	413001	New Zealand	vodaphone	2024/11/01 18:01:03	•••
359	645003	Bulgaria	vivacom	2024/11/01 18:01:03	•••
375	623004	Belarus	velcom	2024/11/01 18:01:03	•••
233	452001	Ghana	tiGO	2024/11/01 18:01:03	•••
255	502019	Tanzania	tiGO	2024/11/01 18:01:03	•••
243	457002	Congo, Democratic Republic of	tiGO	2024/11/01 18:01:03	•••
43	268001	Austria	tele.ring	2024/11/01 18:01:03	•••

MCCMNC reference book

The table has the following columns:

- **Dialcode**
- **MCCMNC**
- **Network**
- **Country** - country name
- **Date** - date of the last record update.
- **actions** - contains the following control:
  - **Delete** - delete the record.

Click *Add* to add a new record to the reference book.



Create new record

Configure the appropriate fields and click *Save*.
To edit an entry, click on a record in the table.

Click *Upload file* to import the reference book from an MS Excel file. The new reference book will completely overwrite the existing one.

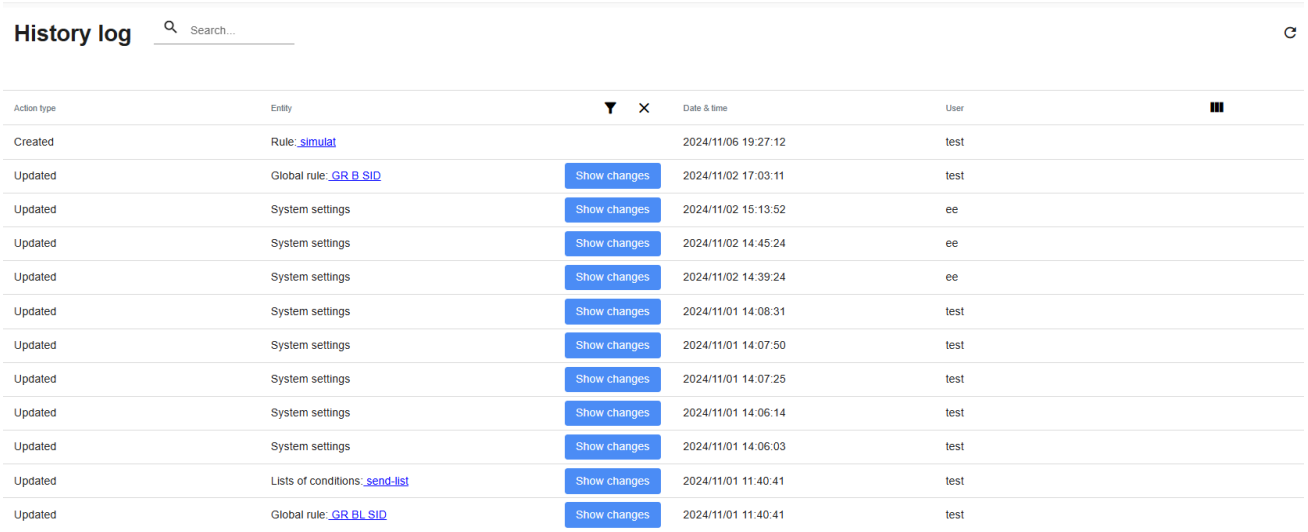
NOTE: Currently the System allows uploading Excel files after manual parsing only. If a mandatory field is not available in the file, the import is failed. The import starts from the second row in the file; headers are required.

The file must contain the following columns in the following exact order with headers:

- **Country code (value is optional)**
- **MCCMNC**
- **Network name**
- **Country** - country name

History log

The *History log* interface serves to view the user and System activity history, which comes instrumental for troubleshooting purposes. Data can be filtered by any column to quickly locate the needed information.



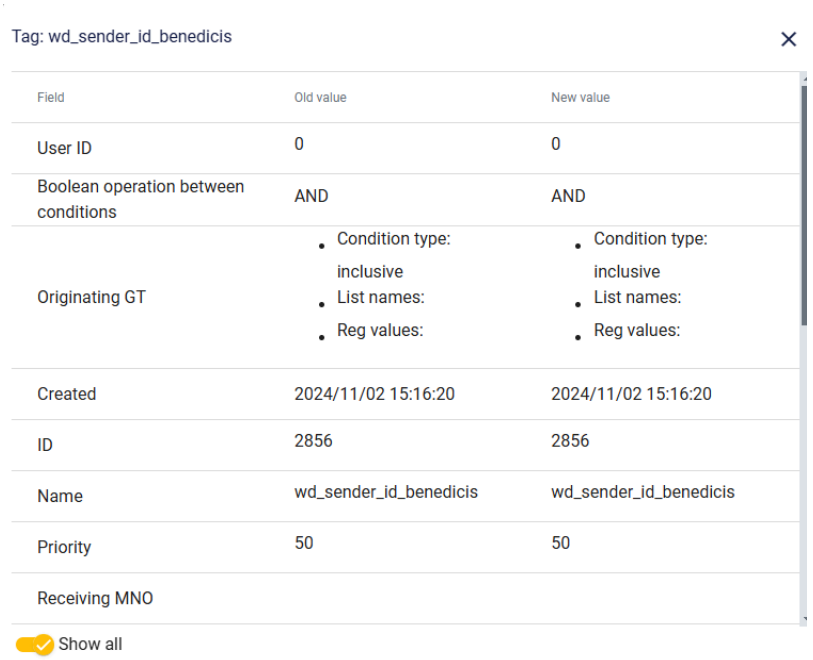
History log

The table has the following columns:

- **Action type** - the activity type. Possible values are: *Created* / *Deleted* / *Updated* / *Uploaded / Bulk uploaded / Bulk deleted / Installed/.*
- **Entity** - the interface entity in which the activity was performed. Possible values are:
  - *Logical rules*
  - *Lists of conditions*
  - *Tags*
  - *Speed limits*
  - *System settings*
  - *Global rules*
  - *MCCMNC reference book*
  - *Preset*
  - *Watchdog*

Click on a hyperlink in the *Entity* column to open the entity in the respective interface. If the entity has been removed, the value has no hyperlink.

If *Action type* = Created, Updated, Deleted, Bulk uploaded, Bulk deleted**,** the column shows the *Show changes* button that opens a modal window with the old and new values as illustrated below. Click *Show all* to display all the fields, otherwise only the changed fields will be shown.



Show changes

- **Date & time** - the activity date and time.
- **User** - name of the user that performed the activity. Along with user names, the list contains the *auto* value that serves to filter automatic events that did not involve users, such as *Watchdog created*, *Watchdog deleted* or auto export.

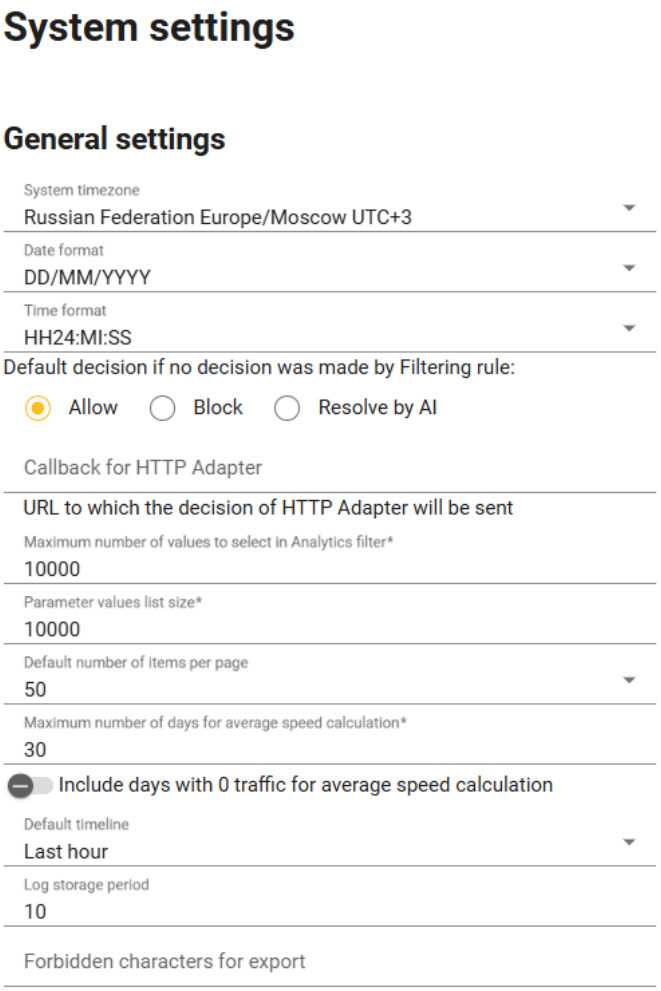
Settings

The *Settings* interface contains the System settings, Your account and Backup settings subsections.

System settings

The *System Settings* interface serves to configure global settings that define the default operation of SMS Firewall.

The interface consists of the following sections and parameters:



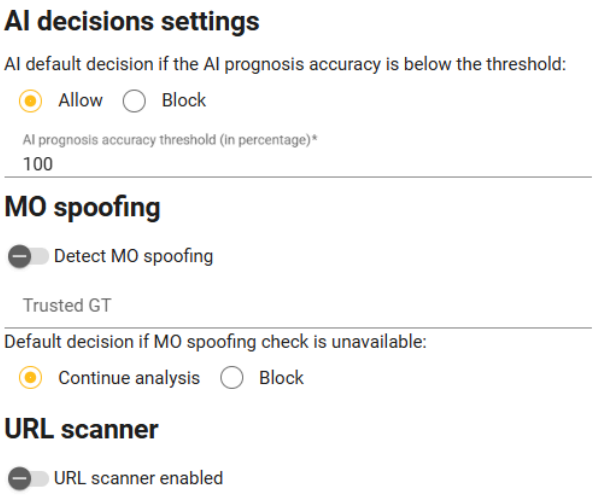
General settings

- *General settings* to configure System-wide parameters:

  - *System timezone*. Select a timezone that applies to the system globally (excluding EDRs which have server time). Use search by country for exact match from the dropdown list.
  - *Date format*. Select the date format from the dropdown list.
  - *Time format*. Select the time format from the dropdown list.
  - *Default decision if no rule was applied*: *Allow* / *Block* / *Resolve by AI (*Note that this feature is charged separately. Contact your account manager to enable it).
  - *Callback for HTTP adapter*. A URL to which the decision of the HTTP adapter will be sent.
  - *Message text clean up* switch (disabled by default). When enabled, upper-case symbols are replaced with low-case, also punctuation marks and blank spaces are removed. When enabled, the cleaned-up text is analyzed rather than the original text, and is shown in the Cleaned up text column of the Messages table in the Analytics interface.The *Message text* column shows the original text. When disabled, the original text is analyzed and

shown in the *Message text* column, while the *Cleaned up text* column is empty. Both the *Message text* and *Cleaned up text* fields are available in the EDR.

- *Maximum number of values to select in the Analytics filter.* The warning will be displayed when selecting the amount of values that exceeds the specified one.
- *Parameter values list size* - maximum number of symbols in the Parameter values list that can be applied in the Tags, Lists of Conditions and Global rules.
- *Default number of items per page* - the maximum number of elements per page.
- *Max. number of days for average speed calculation* - maximum number of days for calculation of speed in the Speed limits interface. For example: if set to 7, the statistics will be moved forward one day every day, so the user will have the statistics for the past 7 days.
- *Include days with 0 traffic for average speed calculation* - when enabled, the days with no traffic are included in the period for calculation of average speed in the Speed limits interface. The speed will be calculated for the exact number of days specified in the parameter *Max. number of days for average speed calculation.* When disabled, zero traffic days will be ignored and subsequent days with traffic will be taken for analysis.
- *Default timeline* - the default timeline period in the Analytics interface.
- *Log storage period* - the log store period in the History log interface.
- *Forbidden characters list for export.* Specify a list of forbidden characters in the value of the message parameter, for which auto-export and manual export are prohibited. The use of ASCII characters is supported, including special characters, both single and a combination of special characters.
- *Backup storage period (days)*. Specify the log storage period (in days) for the *History log* interface.



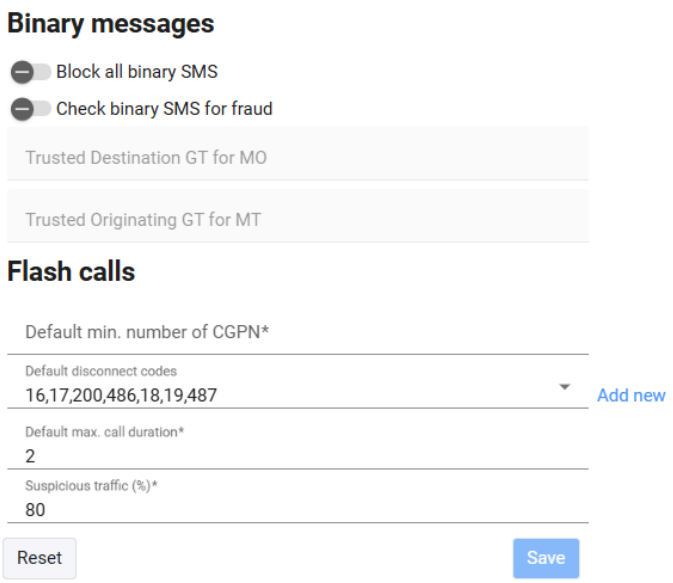
AI decisions settings, MO spoofing, URL scanner

- *AI decisions settings* serve to configure parameters that define System-wide behavior of the AI interface:
  - *AI default decision if the AI prognosis accuracy is below the threshold* - possible values are *Allow* or *Block.*
  - *AI prognosis accuracy threshold (in percentage).* If the result is below the threshold, the message is passed over to the AI default decision.
- *MO spoofing*: serves to configure parameters for System-wide detection of MO spoofing:
  - *Detect MO spoofing* - enables verification that a subscriber uses roaming when sending an MO message. The verification is started after analysis by Global rules and before analysis in Tags.

NOTE: If MO spoofing is not enabled in the internal configuration, the option is disabled. To enable it, contact the Alaris technical support team.

  - *Trusted GT* (available if *Detect MO spoofing* is enabled) - serves to specify Global Titles (GTs) that should not be verified.
  - *Default decision if MO spoofing check is unavailable* - a default resolution in case of any error requesting the SS7 module. Possible values are:
    - *Continue analysis* - does not affect traffic; sends the message for further analysis.
    - *Block* - block traffic.

- *URL scanner*: toggle *URL scanner enabled* to enable the URL scanner interface. When deselected, the interface is hidden.



Binary messages, Flash calls

- *Binary messages:* controls handling messages with the parameter *is_binary*. The section contains the following parameters:
  - *Block all binary SMS* - toggle to block all binary messages. If enabled, absolutely all binary messages are blocked without any checks. If off, all

binary messages are immediately sent for deep analysis or for additional checking for compliance with the network nodes.

- *Check binary SMS for fraud* (available if *Block all binary SMS* is enabled) - check binary messages for their correspondence to the carrier's home nodes. Verification runs after analysis in Global rules, before passing to deep analysis in Tags and (before checking for MO spoofing if validation and MO message type is enabled). When enabled, each MO is checked against the list of home Trusted Destination GTs, and each MT is checked against the list of home Trusted Originating GTs. As a result of this check, if the Destination GT and Originating GT values in the received message match the values or prefixes in the list of Trusted Destination GTs and Trusted Originating GTs, then it is passed on for further analysis with tag and rule lookup. If the GTs did not match for either the MO or MT on one of the exclusion lists, the *Blocked* decision is made immediately.
- *Trusted Destination GT for MO* (available if *Detect binary SMS attacks* is enabled) - specify the list of trusted Destination GTs, for which no fraud verification of binary MO messages is required.
- *Trusted Originating GT for MT* (available if *Detect binary messages* is enabled) - specify the list of trusted Destination GTs, for which no fraud verification of binary MT messages is required.

- *Flash calls*: controls the flash call functionality. Note that this feature is charged separately. Contact your account manager to enable it.

  The section contains the following parameters:
  - *Default min. number of flash calls* - minimum number of flash calls of all calls from the default A-number to analyze by *Suspicious traffic* percentage.
  - *Default disconnect codes* - a list of default disconnect codes for use in the analysis form. Possible values:

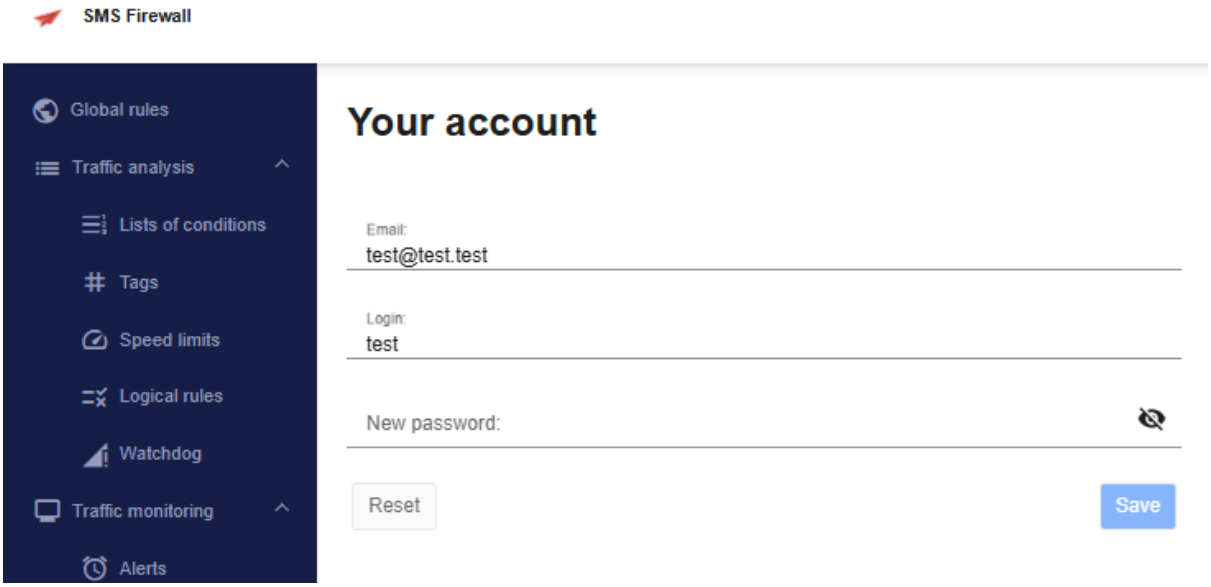
    16 Normal call clearing (Q.931),
    17 User busy (Q.931),
    16 Normal call clearing (Q.850),
    17 User busy (Q.850),
    200 OK (SIP),
    486 Busy here (SIP),
    18 No user responding (Q.931)
    19 No answer from user (Q.931)
    18 No user responding (Q.850)
    19 No answer from user (Q.850)
    487 Call cancelled (SIP)
    480 Temporarily unavailable (SIP)

    This is the default list of codes that comes with the System. To add a new code, click Add new and supply the disconnect code and description.

- *Default max. call duration* - default max. call duration in seconds for use in the analysis form (from 0 to 99).
- *Suspicious traffic (%)* - the percentage of flash calls out of all calls from this A-number that must be added to the report. The percentage is calculated based on the specified *Min. number of flash calls*, *Max call duration* and *Disconnect codes*.

Your account

The *Your account* interface serves to control user accounts. Users can change their email address, login and password.



Your account interface

The bottom left corner contains the details of the current System build and version as illustrated in the figure below.

BuildDate: 2024-10-31T15:27:09
DebugMode: enabled
Name: SMS Firewall
Release: 3310
StartDate: 2024-11-01T10:19:03
Version: 1.3.0

Build and version details

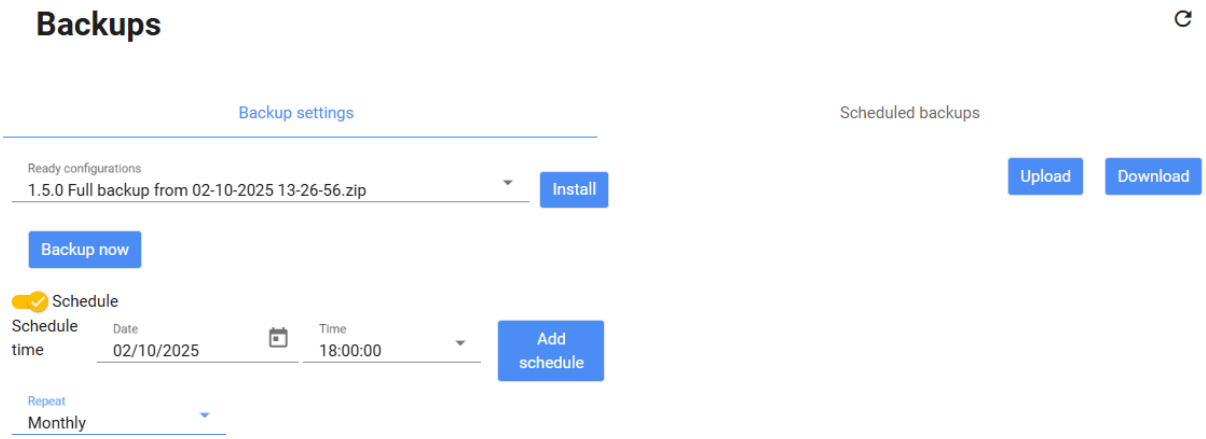
Backups

The *Backups* interface serves to save and restore the System configuration. If as a result of user actions the configuration has changed significantly and important objects have been deleted, the interface allows the user to roll back the System to a certain point in time. The

System version is backed up manually or automatically on schedule. Each created version of the System is stored in the database.
The period for storage of backup configurations is controlled by the System setting *Backup storage period (days)*. Once the period expires, records are deleted from the interface and can only be accessed by contacting the Alaris technical support team.

The interface consists of two tabs: *Backup settings* and *Scheduled backups*. The *Backup Settings tab* is intended for managing the list of ready configurations and for creating new configurations both instantly and on schedule. The *Scheduled backups* tab is intended for managing tasks for creating configurations on schedule.

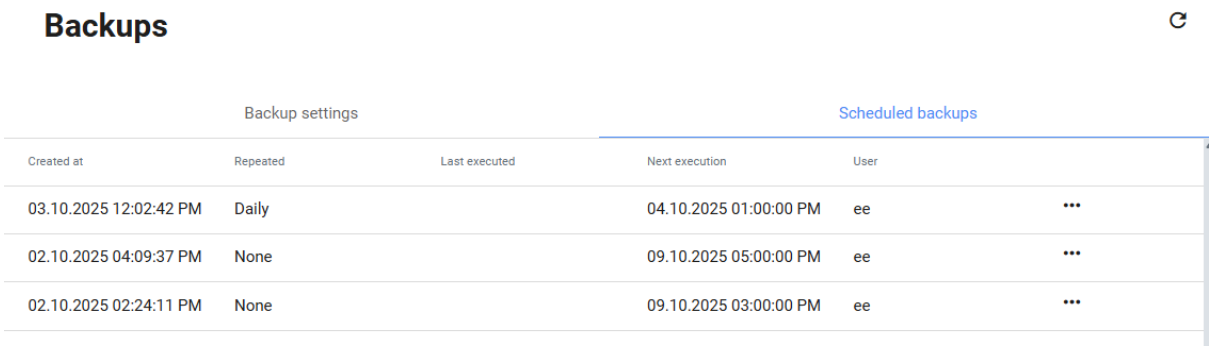
Backup settings



Backup settings

The *Backup settings* tab contains the following fields and controls:

- **List of ready configurations** - list of configurations for rollback.
- **Install** (available if *List of ready configurations* is filled) - click to install the selected ready configuration.
- **Download** (available if *List of ready configurations* is filled) - click to download the selected backup configuration to your computer.
- **Upload** - click to upload a backup configuration to the System. The file will appear in the *List of ready configurations*.
- **Backup now** - click to start the backup process.
- **Schedule** - select to enable backup creation schedule.
    - **Schedule time** - schedule the date and time.
    - **Repeat** - select how often the backup creation must be repeated. Possible values are: *Daily*, *Weekly*, *Monthly*, *None*. If Schedule time contains a value higher than *28* of the month, the *Monthly* value becomes unavailable.
    - **Add schedule** - click to add the task to the *Scheduled backups* tab.



Scheduled backups

The *Scheduled backups* tab contains a table of backup tasks. The table has the following columns:

- **Created at** - schedule task creation time.
- **Repeated** - shows if the task is recurrent. Possible values are: -, *Daily, Weekly, Monthly.*
- **Last executed** - date of the last scheduled task execution.
- **Next execution** - date of the next scheduled task execution.
- **User** - user that created the task.
- **actions** - contains the following control:
    - **Delete** - delete the record.