

INFOWATCH

InfoWatch Traffic Monitor 7.6

User Guide

02/03/2023

© JSC “InfoWatch”

Tel/Fax +7 (495) 229-00-22

http://www.infowatch.com

TABLE OF CONTENTS

1 InfoWatch Traffic Monitor Overview 9
1.1 Objects Interception 11
1.2 Object Analysis and Verdict 12
1.3 Retrospective Data Analysis, User Decision on an Object 15
1.4 InfoWatch Traffic Monitor Transport Modes 16
1.5 Uploading Object to Database 17
1.6 Specific Features of Blocking HTTP-queries and Messages Sent through Web Services 17
2 Traffic Monitor Management Console: General Information 19
2.1 System Operation Before Configuring 20
2.2 Configuring the System 20
2.3 Displaying Actual Data in Management Console 23
3 Interface of Traffic Monitor Management Console 24
3.1 Dashboard Section 26
3.1.1 Dashboard Widgets 27
Dynamics of Violations over the Period 28
Top Violators 29
Quantity of Violations over Period 29
Selection 30
Dynamics of Statuses 31
Policy Statistics 32
Statistics on Protected Objects 32
Statistics on Catalogues of Protected Objects 33
3.1.2 Dashboard Report 34
3.2 Events Section 36
3.2.1 Queries 37
Standard Mode of Creating Queries 39
Advanced Mode 47
Search on the Event Text 48
3.2.2 Object Interception 50
Event Tile 53
Table view of Events 54
Brief Event Viewing Form 55
Detailed Event Viewing Form 56
3.2.3 Contact Identification in Event 59

3.3 Reports Section 60
3.3.1 Report Creation Form 62
3.3.2 Widgets of Reports 62
3.3.3 Queries 65
3.4 Technologies Section 66
3.4.1 Categories and Terms 67
Categories 68
Terms 68
3.4.2 Text Objects 70
Text Object Patterns 71
3.4.3 Sample Documents 73
3.4.4 Blanks 74
3.4.5 Stamps 76
3.4.6 Database Unloadings 76
Automatically Updated Database Unloadings 79
3.4.7 Graphical Objects 80
3.4.8 Autolinguist 81
3.5 Protected Objects Section 82
3.5.1 Elements of Technologies 83
3.5.2 Detection Conditions 84
3.6 Persons Section 87
3.6.1 Persons 89
3.6.2 Computers 90
3.6.3 Screenshots 91
3.7 Policies Section 92
3.7.1 Rules and their Viewing Form 93
Rule of Transfer 95
Rule of Copying 96
Application activity rule 98
Person Control Rule 99
File Operations Rule 99
3.8 Lists Section 100
3.8.1 Tags 100
3.8.2 Web Resources 101
3.8.3 Statuses 102
3.8.4 Perimeters 102
3.8.5 File Types 104
3.9 Administration Section 105
4 Cases Solving in Traffic Monitor Management Console 106
4.1 Typical Actions 106

4.1.1 Login to the Management Console ... 106
4.1.2 Applying System Configuration ... 107
4.1.3 Editing Element ... 109
4.1.4 Deleting Element ... 109
4.1.5 Pages Navigation ... 109
4.1.6 Changing User Password ... 110
4.1.7 Selecting Interface Language ... 110
4.1.8 Calling Help File ... 111
4.1.9 Viewing Information on System ... 111
4.2 Managing Persons and Computers ... 111
4.2.1 Creating Group of Persons or Computers ... 112
4.2.2 Creating Persons and Computers ... 113
4.2.3 Exporting and Importing Persons ... 114
Features of exporting and importing the organzational structure ... 115
4.2.4 Configuring Person's Card ... 115
Adding Contact to Person ... 116
Adding Computer to Person ... 117
Adding Person to Group ... 117
4.2.5 Configuring Computer Card ... 118
Adding Contact to Computer ... 118
Adding Person to Computer ... 118
Adding Computer to Group ... 119
4.2.6 Adding Status to Persons ... 119
4.2.7 Viewing Screenshots ... 120
4.3 Managing Catalogues ... 122
4.3.1 Managing Tags ... 122
4.3.2 Managing Web Resources ... 123
4.3.3 Managing Statuses ... 124
4.3.4 Managing Perimeters ... 125
4.4 Managing Base of Technologies ... 129
4.4.1 Defining the Confidential Information ... 130
Managing Categories and Terms ... 132
Managing Text Objects ... 134
Managing Sample Documents ... 137
Managing Blanks ... 139
Managing Stamps ... 142
Managing DB Unloadings ... 143
Managing Graphical Objects ... 148
Managing Autolinguist ... 149
4.4.2 Exporting and Importing the Base of Technologies ... 151
4.5 Managing Protected Objects ... 153
4.5.1 Creating a Catalogue of Protected Objects ... 154

4.5.2 Creating a Protected Object ... 154
4.5.3 Adding Elements of Technologies ... 161
4.5.4 Adding Detection Conditions ... 162
4.5.5 Creating Policies for Protected Objects and Their Catalogues ... 163
4.5.6 Importing and Exporting Protected Objects ... 164
4.5.7 Activating and Deactivating Protected Objects ... 166
4.6 Managing Interception Objects ... 167
4.6.1 Viewing Summary on Violations/Violators ... 167
Creating Dashboard ... 169
Creating and Configuring Widget ... 169
Creating Dashboard Report ... 171
Viewing Dashboard Report ... 172
4.6.2 Viewing Events ... 173
Creating Queries ... 174
Choosing Event Fields of View ... 186
Viewing Brief Event Form ... 186
Viewing Detailed Event Form ... 187
4.6.3 Making Decision on Object ... 188
4.6.4 Adding and Deleting Tags ... 189
4.6.5 Saving Events (for SMTP mail) ... 189
4.6.6 Event Export ... 189
4.6.7 Dispatching a Quarantined Event ... 192
4.7 Configuring System Response ... 193
4.7.1 General Information on Policies ... 194
4.7.2 Preset Policies ... 201
Data Protection Policy ... 202
Person Control Policy ... 203
Policy that Regulates Transferring Password-Protected Data ... 203
Policies that Regulate Visiting Web Resources ... 204
Policy that Excludes Mailing Lists from Interception ... 206
4.7.3 Creating Data Protection Policy ... 207
Examples of Using Data Protection Policy ... 208
4.7.4 Creating Data Protection Policy on Agents ... 212
4.7.5 Creating Person Control Policy ... 214
4.7.6 Creating Rules ... 215
4.7.7 Determining System Response to Policy Violations ... 217
4.7.8 Configuring Notifications in Rules ... 219
4.7.9 Determining System Default Response ... 219
4.7.10 Filtering the List of Policies ... 221
4.7.11 On Data Protection Policy on Agents ... 221
4.7.12 On Data Protection Policy ... 222
4.7.13 On Person Control Policy ... 223
4.8 Managing Reports ... 223

4.8.1 Creating and Viewing Reports ... 223
Creating Folder with Reports ... 226
Creating Report ... 227
Creating and Configuring Widget ... 228
Viewing Ready Reports ... 230
4.8.2 Examples of Using Reports ... 231
4.9 Administrating the System ... 236
4.9.1 Managing Integration with LDAP Catalogues ... 237
Creating Connection to Server ... 237
Editing Connection to Server ... 241
Deleting Connection to Server ... 241
Running Synchronization with Server Manually ... 241
4.9.2 Managing System Users and their Roles ... 242
Users ... 242
Roles ... 246
Visibility Scopes ... 248
4.9.3 Managing Licenses ... 252
Checking License Validity ... 253
Installing a License ... 253
Deleting License ... 253
Requesting a License ... 253
4.9.4 Healthcheck ... 254
Configure Notifications ... 255
4.9.5 Collecting Diagnostic Data ... 255
4.9.6 User Actions Audit ... 257
Audit Events ... 257
Filtering and search ... 258
4.9.7 Integrity Monitoring ... 259
Manual Integrity Monitoring ... 259
Automatic Integrity Monitoring ... 259
Accepting Result as Standard ... 259
4.9.8 Plugins ... 260
Adding Plugin ... 262
Deleting Plugin ... 262
Working with Tokens ... 263
4.9.9 Configuring Connection to Mail Server ... 264
4.9.10 Configuring Notifications ... 265
Creating Notification ... 266
Testing Notification ... 267
Preset Notifications ... 268
5 Licensing Information ... 269

5.1 User License Agreement 269

6 Glossary 271

1 InfoWatch Traffic Monitor Overview

InfoWatch Traffic Monitor allows you to control data traffic in the corporate network in order to detect and prevent unauthorized use of confidential data.

Main functions of InfoWatch Traffic Monitor are listed below.

> **Note:**
>
> The set of supported functions depends on the operating system installed on the server (for more details please see the knowledge base article "Traffic Monitor and Device Monitor functionality differences according to OS used").

InfoWatch Traffic Monitor Main Features:

- Interception of SMTP, IMAP, and POP3 traffic. It is possible to intercept traffic (or the copy of traffic) passed by a mail relay server; the copy of the traffic that passed through the controlled switch.
- Interception of the HTTP and HTTPS traffic. It is possible to intercept the traffic passed through an ICAP-supporting proxy server; the copy of traffic passing through the controlled switch.

  > **Note:**
  >
  > While integrating with the Blue Coat proxy server, the interception of HTTPS traffic is available if the proxy server processes HTTPS traffic as HTTP traffic.

- Intercepting a copy of ICQ traffic (the OSCAR protocol) passing through the controlled switch. When ICQ connects through HTTP, the System intercepts ICQ traffic similar to HTTP traffic.

  > **Warning!**
  >
  > The intercepting and analysis of encrypted ICQ traffic are not supported (including the one transferred by SSL protocol).

- Analyzing Skype traffic, shadow copies of files, print jobs, traffic transferred by HTTP, HTTPS, and FTP protocols; receiving and transmitting mail via SMTP, POP3, IMAP, Outlook; uploading data to cloud storages through HTTPS protocol, controlling data exchange via Jabber (XMPP protocol), Telegram, WhatsApp (desktop version). Voice messages in Skype can also be intercepted. These data is intercepted by InfoWatch Device Monitor system.
- Intercepting and analyzing MS Lync objects via IW Lync Adapter installed on MS Lync server.
- Analyzing the contents of the intercepted traffic in order to detect violations of the corporate security policy.
- Filtering the intercepted traffic by allowing or blocking the delivery of certain data.

  > **Warning!**
  >
  > This feature is not available when the traffic copy is processed.

InfoWatch Traffic Monitor Components:

InfoWatch Traffic Monitor Component	Purpose
Traffic Monitor Server	Interceptors: **IW_SNIFFER**, **IW_ICAP,** and **IW_SMTPD**. **Analysis subsystem** receives event context and checks if the events contain technology elements and correspond to protected objects. **Policy applying subsystem** implements actions defined by the user according to the corporate security policy.
Database	Storage of information associated with the System operations (intercepted data and results of their analysis).
Device Monitor	Interaction with workstations. Controlling user access to the peripherals, monitoring operations (data copying from/to removable storages and FTP, sending data to printing, using messengers) and intercepting the traffic from instant messengers.
Connectors	Integration with external systems, generating events.
Web Management Console	Configuring rules for analyzing and filtering traffic, analysis of intercepted data.

Participants

All participants in the System are divided into two types:

- **Persons in control**
  Security officer - a person (or several persons) whose responsibilities include creating security policies and policy rules and investigating incidents of policy violations. Also, the security officer administers the System, prepares reports, etc.
- **Persons under control**
  Persons - all persons included in the company perimeter. If policy rules are violated, the person is considered the *Event sender* and is reviewed by the security officer.

Functionality

The System functionality allows you to control the two areas:

- Devices (workstations, peripherals, removable media, etc.);
- Communications via traffic channels (mail, instant messengers, external resources, etc.).

To control these areas, interceptors are used.

General principles of the System operation are described in the following articles:

- Object Interception;
- InfoWatch Traffic Monitor Transport Modes;
- Object Analysis and Verdict;
- Uploading Object to Database;
- Retrospective Data Analysis, User Decision on an Object;
- Specific Features of Blocking HTTP-queries and Messages Sent through Web Services;
- InfoWatch Device Monitor Functions (see in *"InfoWatch Device Monitor. User Guide"*).

1.1 Objects Interception

The System objects are the following:

- traffic objects (SMTP, IMAP, and POP3 e-mails, HTTP and HTTPS requests, ICQ, Skype (voice and messages), MS Lync, Telegram, XMPP, Facebook, WhatsApp (desktop version), VK;
- shadow copies of files;
- print jobs.

Warning!

The table contains the general list of protected objects types for all OS supported. Please see more detailed information in the following section:

- "InfoWatch Traffic Monitor. Administration Guide", section "In Stream/At The Gateway Traffic Interception".

It is also recommended to see the article Differences of Traffic Monitor and Device Monitor functionality according to OS used.

There are several ways to intercept objects, depending on their type:

Object type	Object interception options
SMTP, IMAP and POP3	The System intercepts and delivers SMTP, IMAP, and POP3 traffic. It is possible to filter intercepted objects (the delivery can be allowed or blocked). The System receives a copy of SMTP, IMAP, and POP3 traffic from the corporate mail relay server. The System does not participate in traffic delivery. The System receives a copy of SMTP, IMAP, and POP3 traffic passing through the switch equipped with SPAN port. The copy is intercepted by means of Sniffer. The System does not participate in traffic delivery.
HTTP	The System intercepts HTTP traffic by means of integration with an ICAP server. It is possible to filter intercepted objects (the delivery can be allowed or blocked). The System receives a copy of HTTP traffic that passes through a switch with a SPAN port. The copy is intercepted by means of Sniffer. The System does not participate in traffic delivery.
HTTPS	The System receives a copy of traffic from InfoWatch Device Monitor
Outlook	The System receives a copy of traffic from InfoWatch Device Monitor

Object type	Object interception options
FTP	The System receives a copy of traffic from InfoWatch Device Monitor
ICQ (OSCAR)	The System receives a copy of ICQ traffic that passes through a switch with a SPAN port. The copy is intercepted by means of Sniffer. The System does not participate in traffic delivery. When ICQ connects through HTTP, the System intercepts ICQ traffic in the same way as HTTP traffic.
Messages from messengers	The System receives a copy of Skype (including voice messages), Telegram, Facebook, WhatsApp (desktop version), VK traffic from InfoWatch Device Monitor.
MS Lync	The System receives a copy of traffic from IW Lync Adapter installed on MS Lync server
Shadow copies of files and print jobs received from InfoWatch Device Monitor	The System receives a copy of traffic. Blocking user actions (print jobs, access to devices) can be performed only by means of InfoWatch Device Monitor

Interception options and further delivery of objects depend on InfoWatch Traffic Monitor transport modes (see "InfoWatch Traffic Monitor transport modes").

1.2 Object Analysis and Verdict

Processing and analyzing intercepted objects as well as applying security policies to them are performed by the following subsystems of InfoWatch Traffic Monitor:

IW TM subsystem	Subsystem modules	Subsystem/module features
Processing subsystem	SMTP and POP3 Processing module (copy mode), HTTP Processing module (copy mode), ICQ Processing module (copy mode), Shadow Copies Processing module, SMTP Processing module (blocking mode), HTTP Processing module (blocking mode).	• Extracting significant data and attachments from the object • Defining the attachments format • Extracting text data, including attachments, from eml-files • Forwarding the extracted texts to the Analysis subsystem
Analysis subsystem	Linguistic Analysis module	Checking if the object text corresponds to any categories

IW TM subsystem	Subsystem modules	Subsystem/module features
	Text Objects Detecting module	Searching through the object text for specific text objects (e.g. credit card numbers)
	Digital Prints Detecting module	Searching through the object text for quotes from sample documents
	Blanks Detecting module	Searching through the object text for completed forms
	Stamps Detecting module	Searching through the object text for stamp images
	Database Unloadings Detecting module	Searching through the object text for quotes from a database
	Graphic Objects Detecting module	Searching through the object text and attachments for images of particular classes
	Autolinguist module	Checking if the text object corresponds to a category using a classifier which learned on standard documents.
Policies Application subsystem	Active Directory, Samba DC, Domino Directory, Astra Linux Directory, Astra Linux Directory Pro and FreeIPA Integration module	Providing the initial import and periodical synchronization of Active Directory, Samba DC, Domino Directory, Astra Linux Directory, Astra Linux Directory Pro and FreeIPA structure with a list of users and workstations in Traffic Monitor for further binding this information with data from the intercepted objects.
	Decision-Making module	Ensuring corporate security policies by employing policy rules to the intercepted objects

The object analysis is performed in the following order:

1. **Detaching object attributes** – the Processing subsystem detaches object attributes. For example, SMTP letter attributes are the sender and recipient addresses, subject, etc. For the list of available attributes, see "Event tile".
2. **Extracting enclosed files** – the Decision-Making module analyzes enclosed files according to such attributes as the file name and type.
3. **Analysis of text and graphic objects** – the Analysis subsystem processes text and graphic data: texts of e-mails, messages, and queries, texts extracted from attachments of the supported format, and image files.

Note:

For documents of MS Office 2003, 2007 and newer versions the System extracts and analyzes text data.

Note:

It is possible to analyze names and values of properties extracted from PDF documents by Device Monitor agent (see *Example 3* in "Managing Text Objects").

The System supports several types of analysis depending on your product license:

Content analysis technology	**Technology description**
Linguistic analysis	Determining the subject and contents of text according to terms (words and phrases) found in the text. The term search is performed using the base of categories and terms which are specific for an organization. All terms are divided into categories (each term can be correlated with one or more categories). Thus, the presence of a term belonging to a particular category allows relating the text to this category. For example, the *Salary* term can be included in several categories (*Internal payments*, *Working conditions*). The presence of this term in the text means that the text can belong to mentioned categories
Detecting text objects	Search for text objects matching the specified templates (e.g., searching for credit card numbers in the intercepted objects)
Detecting digital prints	Search for fragments of text matching the predefined sample documents (orders, financial reports, contracts, etc.)
Detecting blanks	Search for blanks matching the specified templates (questionnaires, receipts, etc.)
Detecting passports of citizens of the Russian Federation	Search for passport images of Russian Federation citizens. The technology functions if the *Russian Federation citizen passport* text object is enabled
Detecting stamps	Search for stamp images of a preset type. Images of round and triangular impressions used in the organizations can be used as stamps
Detecting database unloadings	Search for quotes from specified database. These can be lists of employees' salary, other personal data, etc.

Detecting graphic objects	Search for images corresponding to any of the preset categories. Graphic objects can be images of passports, credit cards, etc.
Autolinguist	Determining the category of text with a classifier which learned on standard documents. Examples of Autolinguist categories: *Accounting*, *HR*, *Sales*

4. Based on the results of the analysis, the Decision-Making module makes a conclusion on a possible violation of the security policy and determines which actions should be performed in case of violation. Rules, which determine the System actions in case of violation, are set in a policy. The actions can be as follows (the set of possible actions is defined by the rule type):
   - **Assign violation level to event**. Possible values: **High**, **Medium**, **Low**, **No violation**.
   - **Assign status to persons**. A status that will be assigned to violators (for details, see "Statuses").
   - **Assign tags to event**. Tags that will be assigned to the event in the policy is violated (for details, see "Tags").
   - **Assign verdict to event**. The System decision whether the event is a potential violation. Possible values: **Allow**, **Block**, **Quarantine**.
   - **Delete event**. The event will not be saved to the database.

> **Note:**
>
> When detecting files of **xls**, **pdf**, **jpg**, **docx** format the following may occur:
>
> - spliced files policy false positive. See details in the article "Intercepted files are incorrectly marked as spliced" in the knowlege base;
>
> - uncorrect format detecting and file data extraction or failure to perform these operations, if structure of the intercepted file does not correspond the format specification (for example, there can be a floating format signature which is located not in the begining of the file). See details in the article "File format cannot be detected and so unpacking cannot be performed" in the knowlege base.

1.3 Retrospective Data Analysis, User Decision on an Object

Objects in a database are available for analysis in the Management Console. The user can view the result of automatic analysis of the object and make his/her own decision on the object (the *Decision* attribute).
By default, the *Decision* attribute of each object has the *No Decision* value. The user can make one of the following decisions for the object:

- *Violation*. Based on the analysis results, the user has decided that the object violates the corporate security policy.
- *No violation*. The user has decided that the object does not violate the corporate security policy.
- *No decision*. The user has not made a decision if the object violates the corporative security policy or not.
- *Further Analysis is Needed*. The user has decided that the object needs further processing.

The user decision may also result in changing the verdict returned by the System (see "Making Decision on Object") and the sending status of an SMTP mail (see "Dispatching a Quarantined Event").

Note:

When working in the *Inline* mode and applying *No violation* verdict, the email will leave the company perimeter irrespective of the further editing the user decision.

1.4 InfoWatch Traffic Monitor Transport Modes

InfoWatch Traffic Monitor supports two transport modes: ***Blocking*** and ***Copy*** . Conditions that specify the transport mode for different objects are defined in the object analysis script. The transport mode is assigned to the object when the object is analyzed in Traffic Monitor Server (see "Object Analysis and Verdict"). Actions related to the object transporting are performed according to the selected transport mode.

Table 1 shows the available transport modes for different types of objects. The difference between modes is how the objects are transported (see table 2).

Table 1

Transport mode	Description
Blocking	InfoWatch Traffic Monitor intercepts, analyses, and transports objects. In this mode, the verdict defines if the object will be delivered to recipients. Besides, in some cases, the delivery status of the SMTP messages can be changed after changing the user decision (see "Dispatching a Quarantined Event").
Copy	In this mode, the System receives copies of objects. The difference from the blocking mode is that the System does not participate in object transporting. Thus, the System performs object analysis only. As the System analyses the copy of objects, the verdict, and the analysis-based user decision do not impact the object delivery to recipients.

Table 2

Object type	Blocking transport mode	Copy transport mode
SMTP	Yes	Yes (for traffic copy received from mail relay server or from Sniffer)
HTTP request	Yes (only when intercepting traffic over ICAP)	Yes
ICQ message	No	Yes (for traffic copy received from Sniffer)
Skype, Jabber or Telegram, WhatsApp message	No	Yes
MS Lync	No	Yes

Object type	Blocking transport mode	Copy transport mode
Shadow copy of a file	No	Yes

1.5 Uploading Object to Database

After an object is analyzed and the decision is made (see “Object Analysis and Decision on Object”), both the object and its XML context are uploaded to the database. The XML context includes:

- Data (attributes and text) extracted from the object and its attachments
- The results of the object analysis
- Information about the decision on the object.

1.6 Specific Features of Blocking HTTP-queries and Messages Sent through Web Services

If the *Blocking* transport mode (see "InfoWatch Traffic Monitor Transport Modes"), the System decides to block an HTTP-request or a message sent via a web service (for example, *mail.ru*), then the browser of the user who sent a request or a letter will display the blocking message.
If sending mail is performed through mail services built on AJAX technology (such as Gmail, Windows Live Hotmail, etc.), then the user may not receive a message saying that the letter delivery is locked. As a rule, a message sent by the mail service is displayed in this case.
Post requests to a number of Web resources (see table below), are processed by the System in accordance with specific rules:

- on the object info pane (see "Object Interception"), the attributes *From*, *To*, *Copy*, *Subject,* and *Sent* are displayed as well as attachments (if any);
- if these attributes cannot be found and no text can be extracted from headers, such requests can be deleted as "garbage" traffic. For example, background requests for status updates in social networks are considered garbage traffic.

Interception of HTTP/HTTPS requests supports IP Board, phpBB, and vBulletin engine-based forums.

Supported Web resources:

Type of Web resource	Resources	
	Without restrictions	With restrictions
Web mail	mail.ru, mail.yandex.ru, rambler.ru, pochta.ru, km.ru, newmail.ru, inbox.com, hotmail.com, hotmail.ru, live.com	gmail.com, yahoo.com, mail.com, aol.com, gmx.com
Blogs and social networks	blogs.mail.ru, liveinternet.ru (li.ru), my.ya.ru, diary.ru, blogspot.com (blogger.com), loveplanet.ru/a-journal, myspace.com, perfspot.com	facebook.com, myspace.com, blogger.com, vkontakte.ru (vk.com), odnoklassniki.ru, twitter.com, livejournal.com (.ru), wordpress.com, linkedin.com

Type of Web resource	Resources	
	Without restrictions	With restrictions
Job search and CV posting sites		moikrug.ru, hh.ru, job.ru, rabota.ru, jobs.com, eurojobs.com
Forums	forum.ru-board.com, sysadmins.ru, talk.mail.ru, dom.bankir.ru, biznet.ru	forum.ixbt.com, groups.google.ru (.com)

The following file storages and hostings are supported**:**

- blogspot,
- box.net,
- cloud.mail.ru,
- disk.yandex.ru,
- file.qip.ru,
- google drive,
- google plus,
- mail.qip.ru,
- onedrive.live.com,
- office365,
- talk.mail.ru.

2 Traffic Monitor Management Console: General Information

Management Console needs a permanent connection to the database server. To connect to the database server, you need to log in.

During the login process, the following conditions are checked:

- the database contains a user account with the specified credentials;
- the account is not blocked.

You can log into the System only if both conditions are met.

If authorization is successful, you can access the main window of the Management Console. Otherwise, an error message is displayed.

Depending on the role assigned to the account under which you log on, you can have the following rights:

- Administrator role has all the necessary rights for the initial configuration of the Management Console
- Security Officer role has all privileges, except for the initial configuration of the Management Console

> **Note:**
>
> The administrator's tasks are partly described in "Administrating the System". For other information on the initial configuration of the System, see "*Infowatch Traffic Monitor. Administration Guide*".

If you have other InfoWatch products installed in addition to TM, for example Vision, you can configure a Single-Sign-On authorization scheme. With Single Sign-On enabled you can move quick and safe between various InfoWatch products without entering authorization data. On how to set up a Single Sign-On authorization see "*Infowatch Traffic Monitor. Administration Guide*", section "*Configuring Single Sign-On in InfoWatch products*".

After you log on, you can configure the System (on how the System operates after installation and before configuring, see "System Operation before Configuring"). The System configuration consists of the following actions:

- Configuring the base of technologies
- Composing lists
- Creating protected objects
- Configuring notifications
- Configuring policies which determine the System response to employees' actions that violate the corporate security policy

When you finish configuring the System, you need to apply the updated configuration (see "Configuring the System").

> **Note:**
>
> If the System has been configured before, and that configuration is sufficient for your purposes, no additional configuring is required.

Typical user actions are listed in "Solving Cases". After configuring the System, the security officer may view a report on corporate security violations (see "Managing Interception Objects").

The user can also modify the Console interface and perform other tasks.

If several security officers use the Management Console simultaneously, you should periodically refresh the page in order to obtain relevant data (see "Refreshing Data in Management Console").

Warning!

For correct operation of the System, make sure that anti-virus and other blocking software does not block the Internet content. For example, in G DATA Security anti-virus, you need to clear the check box for the **Process Internet content (HTTP)** field.

2.1 System Operation Before Configuring

The installed System which has not yet been configured (on the System configuring, see “Cases Solving") operates in the following way:

- intercepts traffic and checks if interception objects match predefined categories. If the interception objects match some category, the System aassignsa corresponding attribute to the object.

  Warning

  If **Don't preinstall loadable technology settings** option has been selected during the installation of the System, you will need to import the base of technologies (see "Exporting and Importing the Base of Technologies") for the correct operation of analysis.

- allows logging into the System using one of the predefined accounts:
  - *Administrator* (Administrator role);
  - *Officer* (Security officer role).
- Displays information about interception objects in the Management Console. To display information about traffic senders and recipients, you should configure the lists of persons and workstations (see "Managing Persons and Workstations").
- Saves interception objects to the database. During analysis, no actions are performed with the objects. To specify how interception objects should be processed, you should configure the company perimeter (see "Managing Perimeters"). After that, the System will apply actions described in "Default Policies" when analyzing interception objects.

2.2 Configuring the System

The System configuration includes settings required for checking objects on Traffic Monitor Server as well as for data monitoring and analysis.

Each object passed to Traffic Monitor is processed according to the configuration version which is currently actual on the server. After processing, the object is uploaded to the database with all attributes assigned to it as a result of processing.

Warning!

The System does not reprocess the object after the configuration is changed.

The version of an active configuration is displayed in the upper part of the workspace.



Besides, the System uses the active configuration to form a configuration version that is then deployed to Device Monitor Agents.

Note:

The configuration version that is used in Device Monitor is displayed in Device Monitor Console (see " Synchronization of Traffic Monitor Policies " in *"InfoWatch Device Monitor. User Guide"*). If necessary, you can compare version numbers in Traffic Monitor and Device Monitor to make sure that Device Monitor uses an actual version.

The configuration process includes:

- Creating the base of technologies (see "Managing the Base of Technologies"):
  - Selecting terms to be detected - only when using **Linguistic Analysis technology** (see "Terms");
  - Selecting text object types to be detected - only when using **Detecting Text Objects technology** (see "Text objects");
  - Selecting sample documents to be detected - only when using **Detecting Sample Documents technology** (see "Sample Documents");
  - Selecting blanks to be detected - only when using **Detecting Blanks technology** (see "Blanks");
  - Selecting stamps to be detected - only when using **Detecting Stamps technology** (see "Stamps");
  - Selecting database unloadings to be detected - only when using **Detecting Database Unloadings technology** (see "Database Unloadings");
  - Selecting graphical object types to be detected - only when using **Detecting Graphic Objects technology** (see "Graphical objects").
- Creating protected objects based on the elements of the base of technologies (see "Protected objects").
- Creating catalogues of:
  - Persons and computers (see "Managing Persons and Computers");
  - Tags (see "Managing Tags");
  - Web resources (see "Managing Resources Lists");
  - Statuses (see "Managing Statuses");
  - Perimeters (see "Managing perimeters");
- Adding notifications about violations of the security policy (see "Configuring Notifications in Rules");
- Creating policies according to which objects on the Traffic Monitor Server are checked (see " Configuring System Response ")

Note:

A configuration that is sent to Device Monitor includes only the following elements:

- Persons and computers
- Perimeters
- Data protection policies on agents
- Categories and text objects
- Protected objects that contain only categories and text objects

If you change any of the configuration settings, the edited configuration version is saved in the System. Upon this:

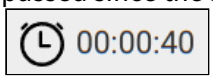
- on the computer of the user who is changing the configuration, the following message is displayed at the top of the browser workspace:
  

- on the computers of users who cannot change the configuration, the following message is displayed at the top of the browser workspace:
  Configuration is being edited by user <security_officer> since 15.06.2015 12:54 PM

Warning!

The changed configuration is available only to the user who is changing it until this configuration is applied, saved or rolled back. Other Console users work with the System configuration version that was applied last and are not allowed to change it.

When you finish editing the configuration, you can choose one of the following actions:

- **Apply configuration** (see "Applying System Configuration") - the updated configuration becomes active on the server.
  Applying the new configuration may take some time. The duration of application does not exceed 3 hours. At the top of the workspace, a counter is displayed. The counter displays the time that has passed since the start of the configuration application process:
  

  You can edit a configuration and apply it even if another configuration is being applied. In this case, the application of the configuration will be interrupted and the application of the edited configuration will start.

- **Save configuration** - the updated configuration becomes accessible for other Console users but it will not be used in the System for traffic control and data analysis.
- **Rollback changes** - the configuration that was last applied on the server will be used in the Console and all changes will be discarded. To discard changes, click **Rollback** in the window with changes. In the **Description** field, you may specify why you are undoing the changes. This information will be stored in the database.

After integration with LDAP catalogues or adding new contacts by means of post-identification, the configuration is updated automatically. Configuration update is performed regardless of its current status.

Note:

Information about contacts added by means of post-identification is updated every 15 minutes.

2.3 Displaying Actual Data in Management Console

Several users can work with the System at the same time. Each user operating the Management Console has access to the data from the last applied configuration (see "Applying System Configuration"), as well as the changes made by this user during the current session of editing configuration.

To keep information about the System up-to-date, you should update the data periodically. The data can be updated both automatically and manually.

The data related to a specific section of Management Console is updated automatically when opening that section. You can also set up automatic update of statistic data on violations and violators.

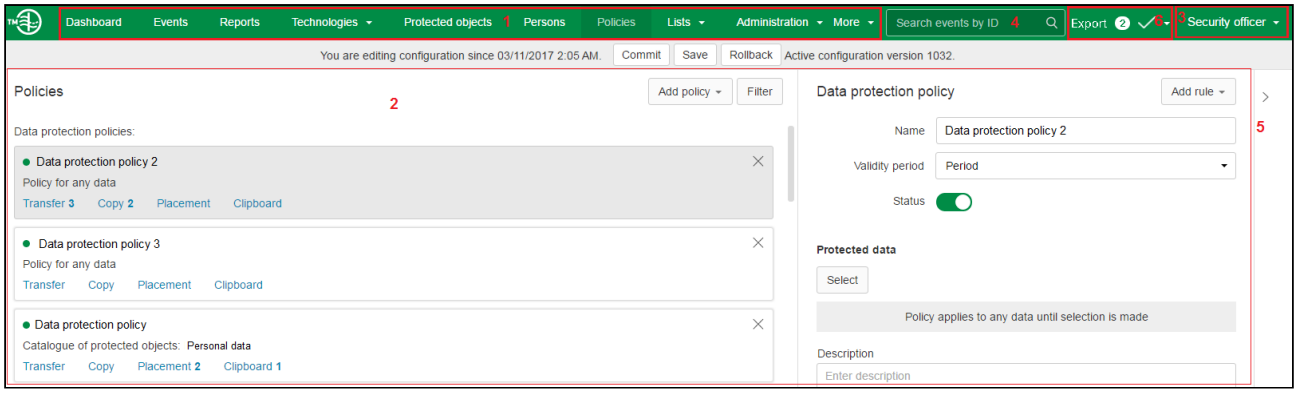
You can also update data manually in any section of the Management Console. To do this, use the standard browser refresh tool: by default the page is refreshed when you press the function key F5).

Note:

While downloading the requested data, the System may display a symbol like  or informational message.

3 Interface of Traffic Monitor Management Console

All windows of InfoWatch Traffic Monitor Management Console have some common elements.



Window elements of the Management Console:

№ on scheme	Console window element	Element purpose
1	Navigation pane	Displays section buttons. Click the section button to go to the selected section of the Management Console.
2	Working area	Displays elements of a selected Management Console section; is used for managing elements of the selected section.
3	User menu button	Displays the user name. Click to open a drop-down list where you can: • Change the password for your account (see "Changing User Password") • Change the interface language (see "Selecting Interface Language") • Call Help for system (see "Calling Help File") • Get information on the System (see "Viewing Information on System") • Log out of the Management Console (see "Login and logout of the Management Console")
4	Field for searching events by ID	Is displayed in all sections of the Console. Allows you to find required events by their ID. If you are searching events not from the "Events" section, you will be redirected to the "Events" section where the search results are displayed.

5	Panel hiding button	Is displayed in sections where workspace is divided into panels (for example, the list of events is located on the panel on the left side of the workspace and information about the selected event is located on the panel on the right side). Allows hiding the panel for easier viewing of information on other panels. Clicking the button again (the arrow will point in the opposite direction) recovers the hidden panel.
6	Button for viewing information on export files	Is displayed in the System contains dashboard reports or event export files or if the event export is in progress. Click the button to view information on ready dashboard reports and event export files as well as export files being created at the moment. For details, see "Viewing Dashboard Report" and "Event Export".

You can work in the Management Console in the sections:

Section	Purpose
Dashboard	Contains statistical information on violations/violators
Events	Contains a list of intercepted objects and tools for managing them
Reports	Contains a sampling of statistical data on intercepted objects
Technologies	Contains a description of analysis technologies being used (categories and terms, text objects, sample documents, etc.)
Protected objects	Contains a list of protected objects and tools for managing them
Persons	Contains a catalogue of persons and workstations of the company IT system, and external contacts.
Policies	Contains the list of the alleged actions of employees and algorithm of the System responses
Lists	Contains editable catalogues of tags, statuses, and perimeters.
Administration	In this section, you can perform initial configuration of the System, view audit events, and configure notifications

You can go to a specific section by clicking the section button.



Events section button

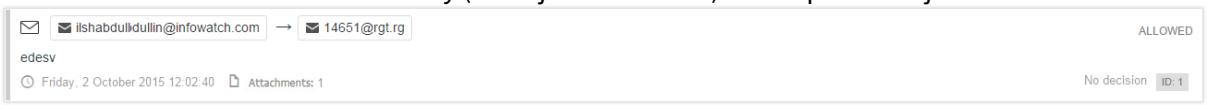
The following interface elements are used in the Management Console:

- **Tab** - allows switching between sets of interface elements within the same window.



Persons section, **Persons** and **Computers** tabs

- **A part of the working area** - working area fragment, separated from other fragments by a vertical line.
- **Tile** - the entire data set for one entry (all object attributes) as a separate object.



Events section, the event tile

You can customize the Management Console interface (for details, see a description of the interface sections).

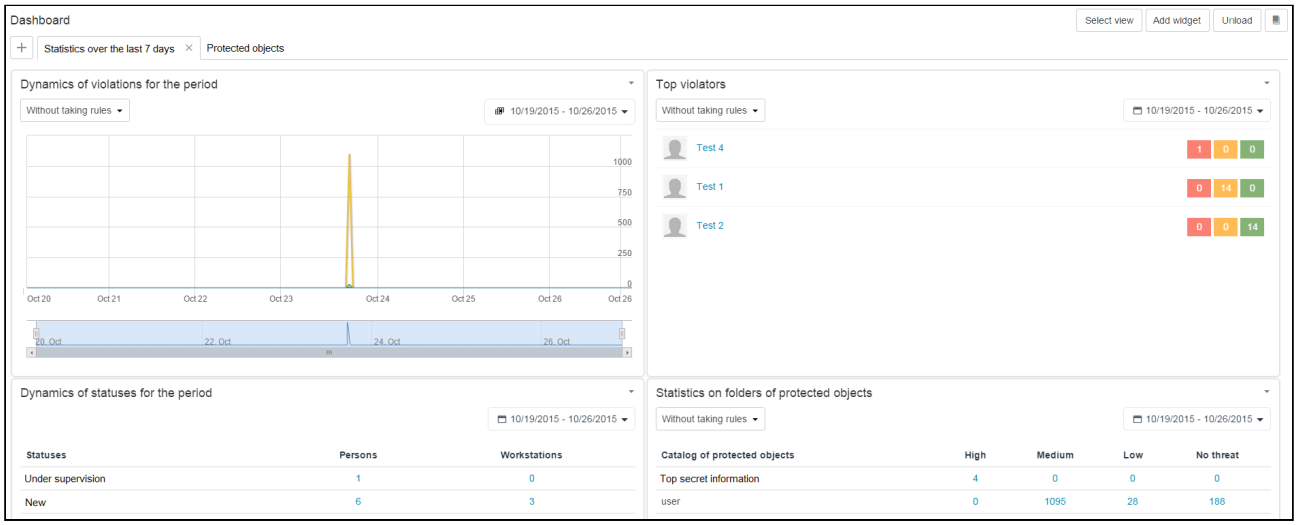
> **Note:**
>
> While downloading the requested data, the System may display the icon or an informational message.

3.1 Dashboard Section

About the section:

The section contains statistical information on violations/violators. Information is displayed on widgets, which are placed on dashboards (tabs). Dashboards are used for grouping widgets with a common subject.

Widgets are useful for daily monitoring as they quickly provide statistics on events.



The **Select view** button allows you to choose how widgets will be displayed on the dashboard. Possible choices:

 - splitting into 3 equal parts

 - splitting in a ratio of 2:1

 - splitting into 2 equal parts

 - splitting in a ratio of 1:2

> **Note:**
>
> For each dashboard, the view is selected separately.

To add a widget to a dashboard, use the button in the right upper corner of the workspace (for details, see "Creating and Configuring Widget").

The **Unload** button allows you to generate a dashboard report in PDF or HTML format (for details, see "Creating Dashboard Report"). To view the list of earlier generated reports, click  .

User's target actions:

- Configuring dashboards and widgets to display information on violations/violators (see "Creating Dashboard" and "Creating and Configuring Widget")
- Viewing information on violations/violators (see "Viewing Events")
- Creating a dashboard report (see "Creating Dashboard Report")

3.1.1 Dashboard Widgets

The workspace of the **Dashboard** section contains dashboards with widgets.

Widgets contain statistical information on violations/violators; appearance and parameters of a widget are defined by its type.

Purpose of different types of widgets and links to their detailed description:

Widget	Description
Dynamics of violations	Quantitative changes of chosen violation types over the selected period
Top violators	A list of the most active violators of a chosen group for the selected time period
Quantity of threats over period	Number of violations of high, medium, and low level for each violation type (transferring, placement, copying) over selected period
Selection	Events for each selection (according to the selected filter)
Dynamics of statuses	Dynamics of statuses over selected period
Policy statistics	The number of violations per policies broken down bythe rules on transferring, copying and placementover selected period

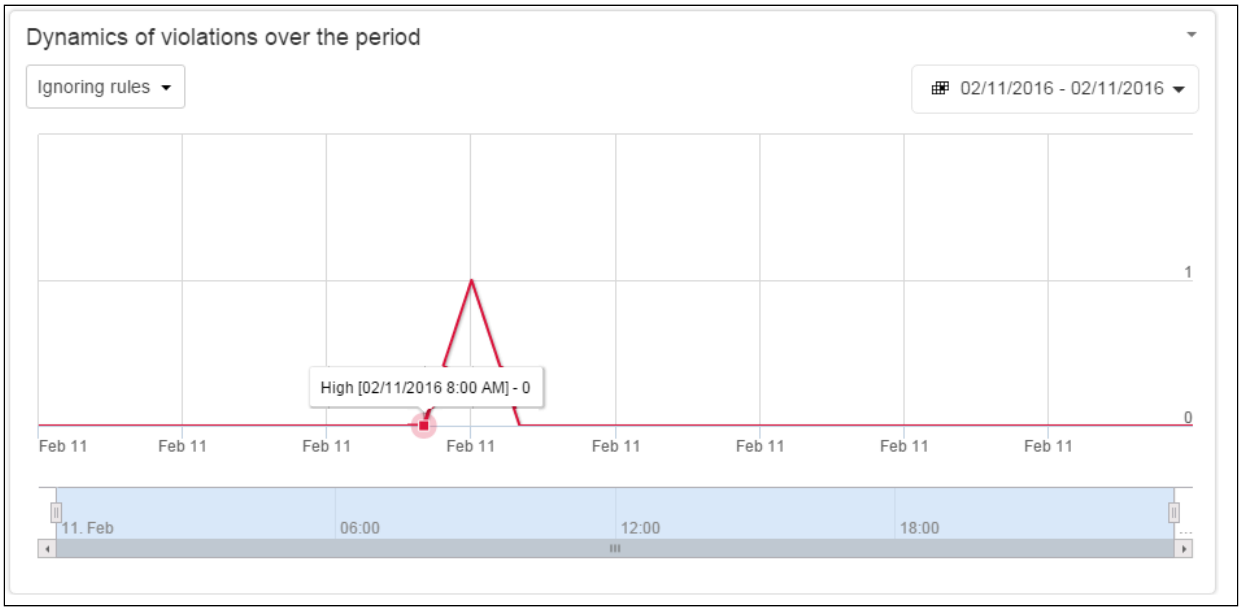
Widget	Description
Statistics on protected objects	The number of violations per protected objects broken down by levels of violations over the selected time period
Statistics on catalogs of protected objects	The number of violations per catalogs of protected objects broken down by levels of violations over the selected time period

User's target actions:

- Configuring widgets to display information on violations/violators (see "Creating and Configuring Widget")
- Moving widget tiles (see "Creating and Configuring Widget")

Dynamics of Violations over the Period

The **Dynamics of violations** widget displays the quantitative changes of chosen violation types over the selected period. Data in the widget are grouped by days.



Violations of high, medium and low level are displayed on separate graphs. When hovering the cursor on the graph, markers are displayed in the interception points of time and the number of violations. Clicking on the marker opens the "Events" section, where you can view violations for the chosen day with the chosen violation level and rule type.

In the right upper corner of the widget, you can see the period over which the data is displayed. You can choose the required period from the drop-down list.

In the left upper corner of the widget, select the type of rules, violations of which will be displayed in the widget. Possible values: *Transfer rules*, *Copy rules*, *Placement rules*, *Ignoring rules*.

To change the widget name or update interval, in the right upper corner click and, from the drop-down list, choose **Edit**. Edit required parameters, then click **Save**.

Top Violators

The **Top violators** widget displays the list of the most active violators broken down to violations of high, medium and low level over a selected time period.

In this widget, you can view what empoloyee has performed most violation of the security policy during the specified period (e.g., for the current day) and then investigate the incidents.



Click the number of violations to open the "Events" section, where you can view the events that meet the conditions specified in the widget settings.

When clicking on the violator's name, the person card is displayed (for identified persons; for details, see "Contact Identification in Event"). To view detailed information on the violator in the "Persons" section, click on the link "Go to person". For not identified violators, the sender's contact is displayed.

In the right upper corner of the widget, you can see the period over which the data is displayed. You can choose the required period from the drop-down list.

In the left upper corner of the widget, select the type of rules, violations of which will be displayed in the widget. Possible values: *Transfer rules*, *Copy rules*, *Placement rules*, *Ignoring rules*.

To edit other widget parameters, in the right upper corner, click and, in the drop-down list, choose **Edit**.

You can edit the following parameters:

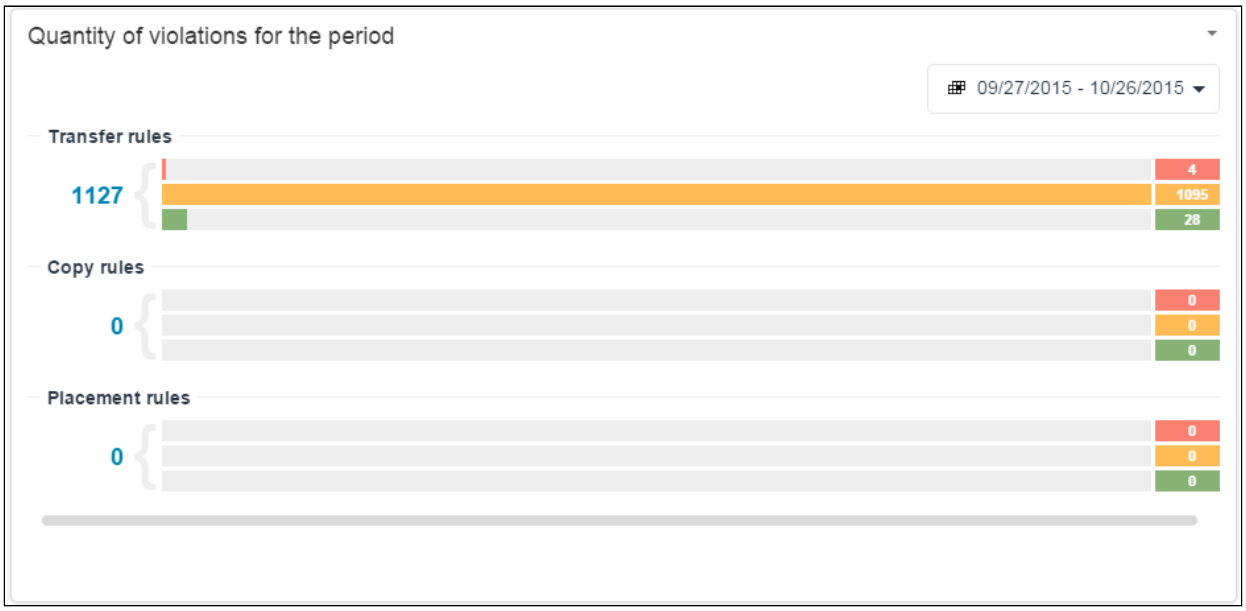
- **Name**;
- **Update interval** for data on the widget;
- **Quantity of violators** for which statistics will be displayed;
- **Groups** to which violation can belong. Statistics on the selected groups will be displayed in the widget. Start typing the group name or click + and select desired groups from the list;
- **Statuses** of persons information on which will be displayed. Start typing the status name or click + and select desired statuses from the list.

Edit required parameters, then click **Save**.

Quantity of Violations over Period

The **Quantity of violations over period** widget displays the number of violations of high, medium, and low level for each rule type (transfer, placement, copying) over a selected period.

Clicking the total number of violations for the selected rule type (highlighted in blue) opens the "Events" section, where you can view violations of a chosen rule type over a selected period.



In the right upper corner of the widget, you can see the period over which the data is displayed. You can choose the required period from the drop-down list.

To edit other widget parameters, in the right upper corner, click and, in the drop-down list, choose **Edit**.

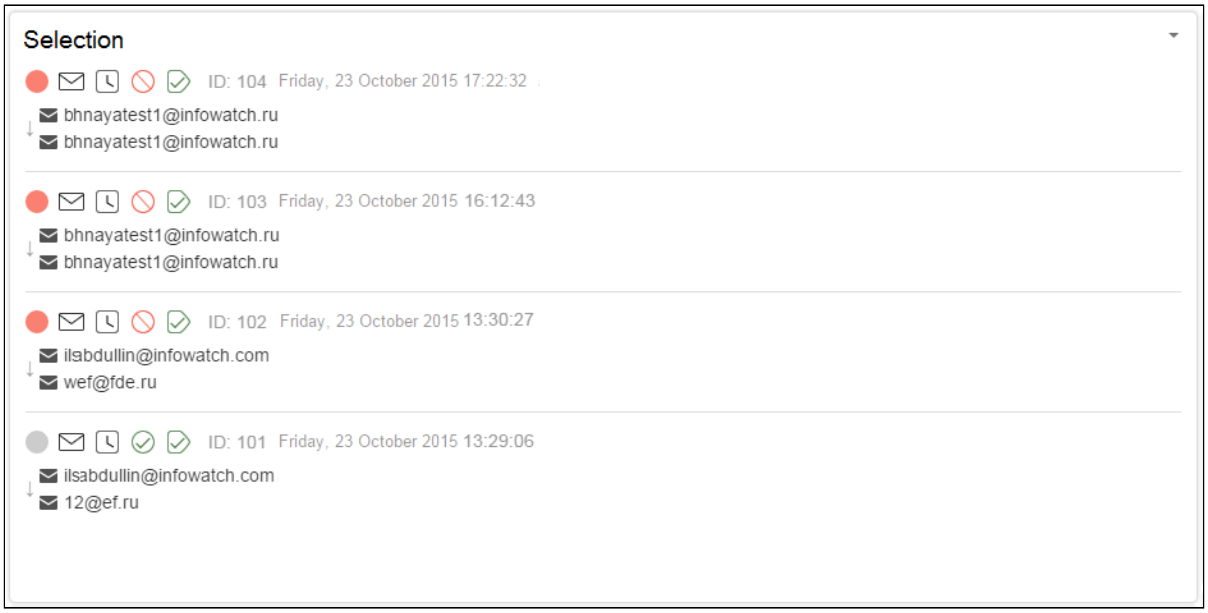
You can edit the following parameters:

- **Name**
- **Update interval**
- **View type** - data representation in the widget. Possible values: *Bar chart (horizontal)* and *Table*.

Edit required parameters, then click **Save**.

Selection

The **Selection** widget displays event tiles for the selection according to the chosen query.



Clicking the event **ID** (highlighted in blue) opens the "Events", where the brief event viewing form is displayed.

To change the widget attributes, in the right upper corner of the widget, click and, in the drop-down list, select **Edit**.

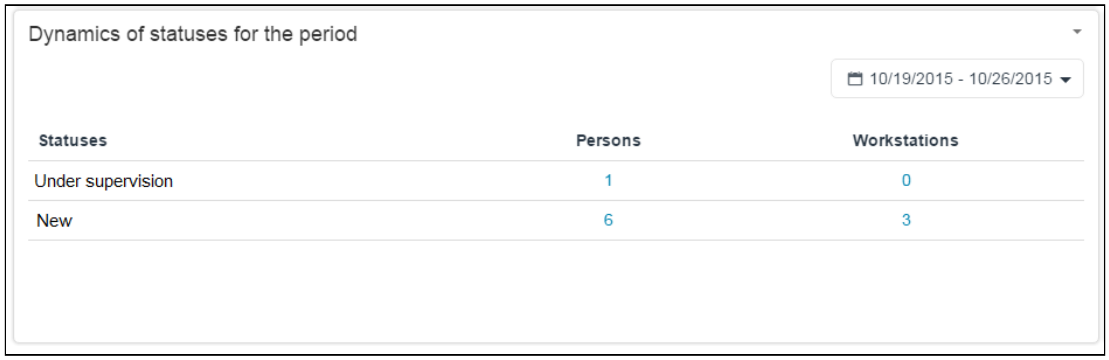
You can edit the following parameters:

- **Name**
- **Update interval** for data on the widget
- **Selection** - a query that will be used for selection. Select a required request from the drop-down list (for details, see "Queries")
- **Events per page** - the number of events displayed on the page

Edit required widget parameters, then click **Save**.

Dynamics of Statuses

The **Dynamics of statuses over period** widget displays the changes of person statuses over the selected time period.



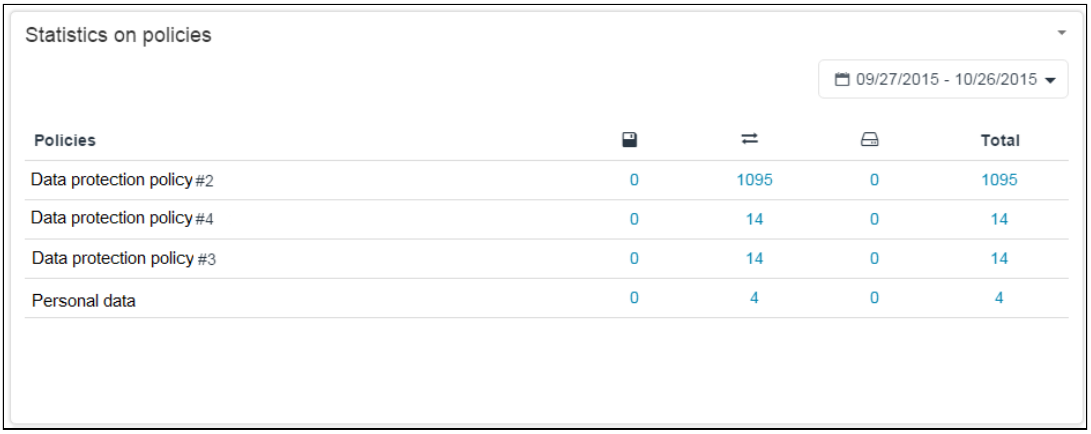
Clicking the number of persons or computers (highlighted in blue) opens the "Persons" section (the **Persons** or **Computers** tab respectively), where you can view the list of persons (or computers) that meet the conditions specified in the widget properties.

In the right upper corner of the widget, you can see the period over which the data is displayed. You can choose the required period from the drop-down list.

To change the widget name or update interval, in the right upper corner click and, from the drop-down list, choose **Edit**. Edit required parameters, then click **Save**.

Policy Statistics

The **Policy statistics** widget displays the number of violations by policies broken down by the rules of transfer, copying, and placement over the selected time period.



Clicking the number of violations of transfer, copying, and placement rules (highlighted in blue) opens the "Events" section, where you can view the events that meet the conditions specified in the widget properties.

In the right upper corner of the widget, you can see the period over which the data is displayed. You can choose the required period from the drop-down list.

To edit other widget parameters, in the right upper corner, click and, in the drop-down list, choose **Edit**.

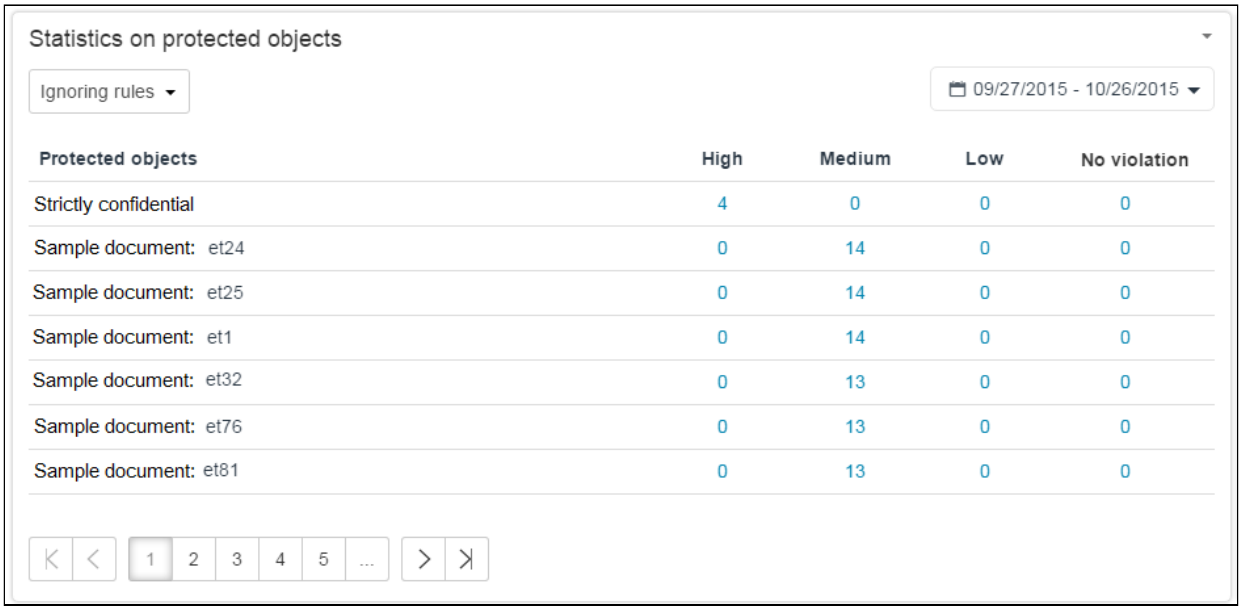
You can edit the following parameters:

- **Name**
- **Update interval** for data on the widget
- **Policies** statistics for which will be displayed. Start typing the policy name or click and select required policies from the list

Edit required widget parameters, then click **Save**.

Statistics on Protected Objects

The **Statistics on protected objects** widget displays the number of violations per protected objects broken down by violation levels over the selected time period.



The event is displayed in statistics if the event contains any of the specified protected objects and any protected object from specified catalogues including sub catalogues.

Clicking the number of violations for each protected object (highlighted in blue) opens the "Events" section, where you can view the events that meet the conditions specified in the widget properties.

In the right upper corner of the widget, you can see the period over which the data is displayed. You can choose the required period from the drop-down list.

In the left upper corner of the widget, select the type of rules, violations of which will be displayed in the widget. Possible values: *Transfer rules*, *Copy rules*, *Placement rules*, *Ignoring rules*.

To edit other widget parameters, in the right upper corner, click and, in the drop-down list, choose **Edit**.

You can edit the following parameters:

- **Name**;
- **Update interval** for data on the widget;
- **Protected object** - protected objects, statistics for which will be displayed. Start typing the object name or click and select desired objects from the list;
- **Catalogue of protected objects** - catalogues of protected objects, statistics for which will be displayed. Start typing the catalogue name or click and select desired catalogues from the list.

Edit required parameters, then click **Save**.

Statistics on Catalogues of Protected Objects

The **Statistics on catalogues of protected objects** widget displays the number of violations per catalogues of protected objects broken down by violation levels over the selected time period.



The event is displayed in statistics for a selected catalogue if the event contains any protected objects from this catalogue (ignoring sub catalogues).

Clicking the number of violations for each catalogue of protected object (highlighted in blue) opens the "Events" section, where you can view the events that meet the conditions specified in the widget properties.

In the right upper corner of the widget, you can see the period over which the data is displayed. You can choose the required period from the drop-down list.

In the left upper corner of the widget, select the type of rules, violations of which will be displayed in the widget. Possible values: *Transfer rules*, *Copy rules*, *Placement rules*, *Ignoring rules*.

To edit other widget parameters, in the right upper corner, click and, in the drop-down list, choose **Edit**.

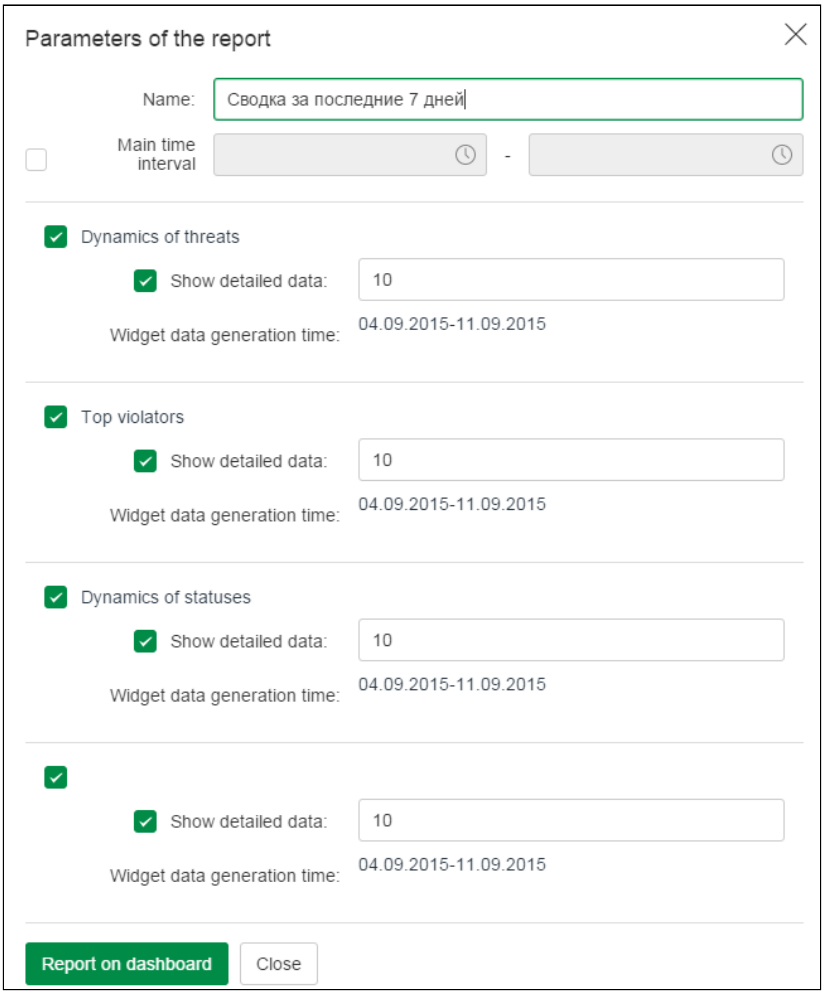
You can edit the following parameters:

- **Name**;
- **Update interval** for data on the widget;
- **Catalog of protected objects** - a catalog of protected objects, statistics for which will be displayed. Start typing the catalog name or click and select desired catalogs from the list.

Edit required parameters, then click **Save**.

3.1.2 Dashboard Report

The dashboard report is needed to display statistical data on intercepted objects. The dashboard report can be represented in PDF or HTML format. You can also print it out on your printer.



Before starting the report generation, specify its name and make sure that all have selected all widgets that should be included in the report.

By default, the report is generated for all widgets of the dashboard. If you do not want to include data from a particular widget, unflag its name.

Select the **Show detailed data** option if you want the report to display particular objects. If necessary, change the number of objects to be displayed (by default, 10 objects are displayed).
For example, for the "Dynamics of Statuses" widget, this option specifies how many persons and computers with each status will be added to the report.

Select the **Common period** option if you want to create a report for all widgets over a common period. Specify the start and the end date.

> **Note:**
>
> By default, a report for each widget is created over the period specified in the widget settings.

User's target actions:

- Creating a dashboard report (see "Creating Dashboard Report")

3.2 Events Section

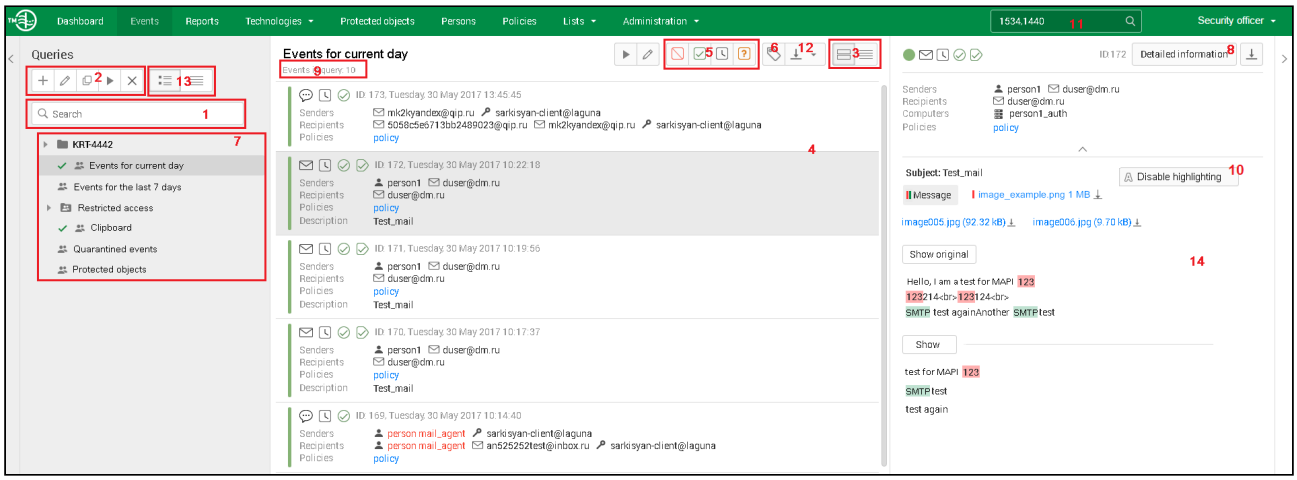
Reference information:
The event is the interception object of network traffic.

The System creates events as a result of traffic interception when employees:

- transfer data to other people;
- publish data to publicly accessible sources;
- copy data to external devices;
- print data.

About the section:

The section contains a list of events (interception objects) and tools for managing them.
The System may contain a large number of events, so a list of events is displayed according to results of user queries.



The query list is located in the left part of the workspace (№7 in the screenshot). You can create a query either in the root or in a folder. For operations with queries and their folders you can use buttons on the toolbar (№2 in the screenshot). You can choose how to display items in the list (№13 in the screenshot):

-  - as folders;
-  - as a flat list.

When you select a folder, its subfolders and queries are displayed.

To search for events, choose a query in the list (№7 in the screenshot) or create a new query by clicking  on the toolbar (№2 in the screenshot).

You can also use the search field to find a folder or a query by its name (№1 in the screenshot).

To run the selected query, click  on the toolbar (№2 in the screenshot).

If you already know the event ID, you can use the **Search event by ID** field (№11 in the screenshot).

> **Note:**
>
> You can enter several IDs separated by a comma, a semicolon or space.

As a result of executing a query or searching events by IDs, a list of found events is displayed (№4 in the screenshot).

Under the query name, a total number of found events is displayed (№9 in the screenshot).

You can choose how to display events (№3 in the screenshot):

-  - in the list as tiles;
-  - as table.

In the right part of the workspace, a brief event viewing form is displayed (№14 in the screenshot). For convenience, highlighting is enabled for triggered protected objects (highlighted in red) and results of search by the event tex (highlighted in green). You can completely disable the highlighting by clicking **Disable highlighting** (№ 10 in the screenshot).

To switch to a detailed event viewing form, click the **Detailed information** button (№8 in the screenshot).

For the selected event, you can perform the following actions:

- make a decision on the event (select the required verdict using buttons on the toolbar - №5 in the screenshot)
- assign a tag to the event (№6 in the screenshot)
- export the event or save debug information on the event (№12 in the screenshot)

User's target actions:

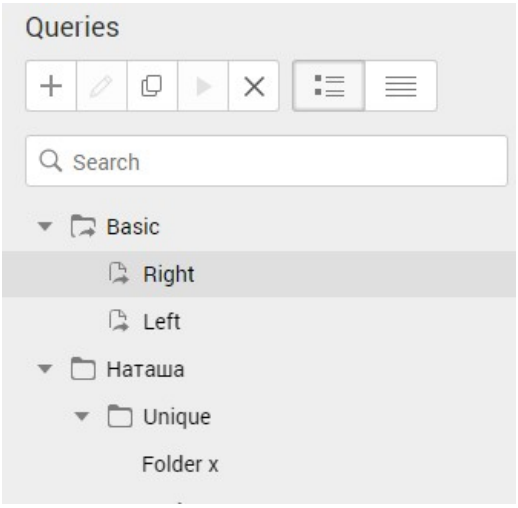
- Filtering events (see "Creating Queries")
- Viewing event details (see "Viewing Brief Event Form" and "Viewing Detailed Event Form")
- Making decision on the event (see "Making Decision on Object")
- Adding/removing tags (see "Adding and Deleting Tags")
- Saving the event (see "Saving Events (for SMTP mail)")
- Dispatching a blocked event (see "Dispatching Blocked Event")
- Exporting events (see "Event Export")
- Viewing contacts of the event senders and recipients (see "Identifying Contacts in Event")

3.2.1 Queries

Objects checked by the System are stored in the database. To view information about these objects in the Management Console, you need to create and execute a query.

The query allows you to get a selection of intercepted objects according to specified conditions.

To make operations with queries more convenient, the folders are used. Folders allow you to group queries with a common subject, specify access rights for a group of queries, inherit access rights, etc. A folder may include both queries and subfolders.



When creating a folder, you should specify access rights. For subfolders the access rights can be inherited from a parent folder or specified individually (for details, see "Creating Folder with Queries"). Folders available only to the owner are marked with . If the folder is also available to other users of the Console, it has icon .

You can create a query in a folder chosen or in the root. If you create a query within the folder, access rights are either inherited from the folder or to be specified individually. If the query is available not only to the owner but also to other users of the Console, it has icon .

If the query has already been executed and contains actual data, it is marked with . When you click on such a query, the events found are displayed in the viewing form on the right.

> **Note:**
>
> The storage period is set by administrator. By default, the report execution results are deleted once a day.

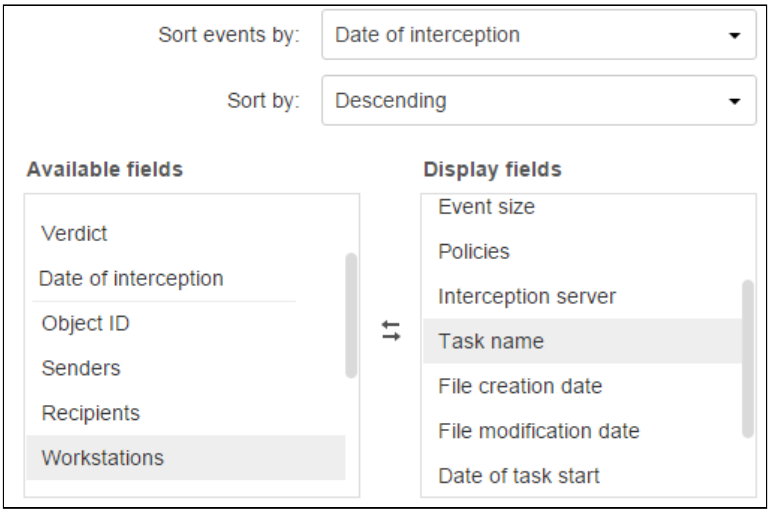
If the query is being executed at the moment, the icon is displayed next to its name . For queries whose execution failed, the icon is displayed .

To create a new query, click on the toolbar and, in drop-down list, choose the type of query you want to create.

There are two query creation modes: standard (allows you to select required conditions from the list) and advanced (enables more flexible configuring of search options).

The query creation form contains the following tabs:

- **Query**. On this tab, you can specify search conditions in a standard or advanced mode.
- **Columns**. On this tab, you can select fields to be displayed for events. The **Available fields** list contains all event attributes and the **Displayed fields** list contains attributes to be displayed in the table viewing form and will be exported to a file in `.xslx` format.



If no attributes selected, the table form and the export file will include all the attributes.

> **Warning!**
>
> **Receiver attributes** aggregation column is not included in event export, even if added to **Displayed fields** list (for more information about **Receiver attributes** column see "Table view of Events").

You can also select the field to sort the list by and specify the sorting direction.

- **Access**. On this tab, you can configure access to the query. Possible choices:
  - If you create a query within a folder and the **Apply rights for related queries** option is selected, then access rights for the query will be the same as the access rights specified for the folder. Editing access rights to the query is unavailable.
  - If you create a query within a folder and the **Apply rights for related queries** option is not selected, or you create a query in the root, then you can specify access parameters for the query. By default, the query is available to the owner only. To provide access to the query to other users, select required users in the list and set the checkboxes next to their names in a field with the required access level (**View and execute access** or **Full access**).

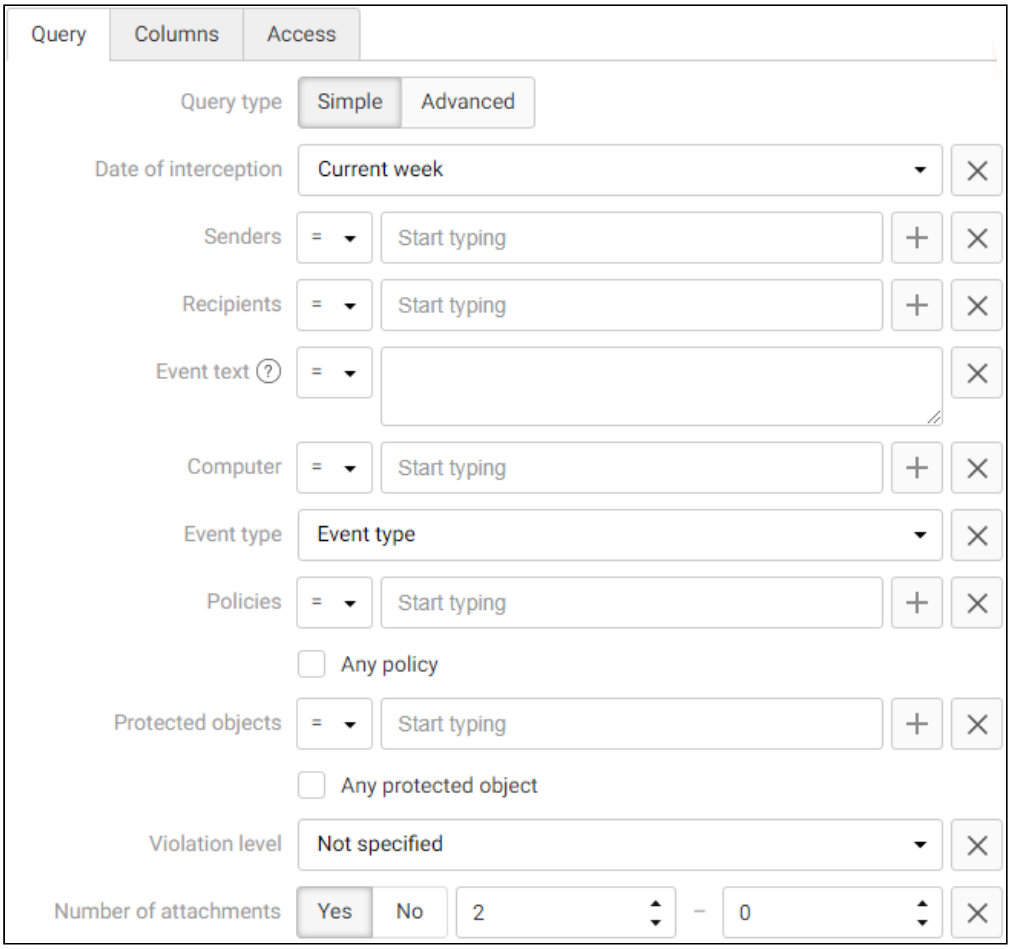
User's target actions:

- creating a folder with queries (see "Creating Folder with Queries")
- configuring parameters of the query (see "Creating queries")
- defining fields of view (see "Choosing event fields of view")

Standard Mode of Creating Queries

In a standard mode, you can specify values of required attributes and if necessary, apply negation to the attribute. Attribute values are specified on the **Query** tab.

All conditions are joined by the logical "AND". Values specified for an attribute are joined by the logical "OR".



By default, most commonly used conditions are displayed.

In the **Add condition** drop-down list, you can choose additional search options.

The full list of available conditions:

Condition	**Description**
Main	
Event ID	A unique identifier of the event. Multiple values may be specified, separated by commas.
Date of interception	The date when the event was created. By default, events for the current week are displayed. Possible values: ▪ All time ▪ From ▪ To ▪ Current day/week/month ▪ Last several hours/days ▪ Last 3/7/30 days ▪ Period (from a calendar)

Event type	Specifies that the event belongs to a particular interceptor. Event types are grouped by category. When selecting a category, all event types of this category will be displayed. Possible values: • Multimedia recording: - Screenshot • Application activity: - Clipboard - Keylogger • Internet activity: - Web message • File sharing: - FTP - Removable devices - Cloud storage - Terminal session - Network resources • Printers and MFPs - Print • Email - Mail on Client - Mail in Browser • Messenger - Telegram - Facebook - WhatsApp - VKontakte - MS Lync - ICQ - XMPP - MMP - Skype - MS Teams (if MS Teams adapter is installed) - Kribrum • File operations: - Read file - Write file
Interceptor	Interceptor by which the event was received. Possible values: • ICAP • DM • Adapter • SMTPD • Sniffer • PushAPI
Protocol	Protocol over which the traffic was transferred. Possible values: • FTP • HTTP

	• HTTPS • IMAP • MAPI • MMP • NRPC • OSCAR • POP3 • SIP • Skype • SMTP/ ESMTP • Telegram • XMPP • WhatsApp
Copy sources and receivers	Sources and receivers, copy is performed from/to. Configuration options: • Copy receiver: - Computer - Removable device - Network resource - Terminal session - FTP - Cloud storage • Copy source: - Computer - Removable device - Network resource - Terminal session • Route direction: - One direction - Both directions You may specify Path to a file or address, Device name, Device ID. The value can be specified using wildcards: • "?" - to replace a single character in the beginning or at the end of the string • "*" - to replace any number of characters in the beginning or at the end of the string **Note**: Depending on the selected type of the copy source/receiver, there can be different recommendations on how to fill in the **Path to file or address** field (see "Recommendations on how to fill in the Path to file or Address field"). **Warning**: The type of the **Path to file or address** attribute value for the "Terminal session" copy receiver depends on the Traffic Monitor version. The attribute value types are different in the events of file exchange via terminal session:

	• **For events created in Traffic Monitor version below 7.5**: the attribute contains the name of the copied file, for example: `file.txt` • **For events created in Traffic Monitor version 7.5 and above**: the attribute contains the IP address of the device that was used to remotely connect to the employee's workstation and to which the file was copied, for example: `192.0.2.0` To search for events created in Traffic Monitor version 7.5 and above, it is recommended to edit existing queries. Existing queries must be edited if they use an obsolete type of the **Path to file or address** attribute value for "Terminal session" copy receiver. If a file name is specified in this attribute in the query, the required events may not match the query condition, because new events have an IP address in this attribute.
Mandate level	Mandate level of confidentiality. It is recognized by Traffic Monitor, starting from version 6.10.10 on Astra Linux OS.
Recipients	
Senders	The list of object senders. May include persons, person groups, statuses, or contact values (except SID). For contacts, a value can be specified using wildcards: • "?" - to replace a single character in the beginning or at the end of the string • "*" - to replace any number of characters in the beginning or at the end of the string
Recipients	The list of object recipients. May include persons, person groups, statuses, or contact values. For contacts, a value can be specified using wildcards: • "?" - to replace a single character in the beginning or at the end of the string • "*" - to replace any number of characters in the beginning or at the end of the string
Number of recipients	The number of object recipients
Entered perimeters	Perimeter the object recipient belongs to
Left perimeters	Perimeter the object sender belongs to
Computer	The computer from which the object was sent. You can specify a computer name or an IP address. The value can be specified using wildcards: • "?" - to replace a single character in the beginning or at the end of the string

	• "*" - to replace any number of characters in the beginning or at the end of the string
Computer type	Type of computer from which the object was sent. Possible values: • workstation • terminal server
Resources	Internet resource or a group of resources (see "List of resources"). Start typing and choose the desired resource or group from the list of suggestions. The value can be specified using wildcards: • "?" - to replace a single character • "*" - to replace any number of characters **Note**: If you want to specify a particular resource, choose icon (for example, facebook.com)
Working in applications	
Source application	Application from which data has been copied
Receiver application	Application to which data has been pasted from the clipboard
Analysis results	
Violation level	The level of violation of the corporate security policy. Possible values: *High*, *Medium*, *Low*, *No violation*.
Tags	Tags assigned to the object (see "Tags")
Policy	List of policies triggered on the object
Violation type	Type of rule that was violated. Possible values: ▪ *Violation of transfer* ▪ *Violation of copy* ▪ *Violation of placement*
User decision	A decision the user made for the object. Possible values: ▪ *Violation* ▪ *No violation* ▪ *No decision* ▪ *Requires additional processing*
Verdict	The verdict passed by the System on the object. Possible values:

	▪ *Allowed* ▪ *Blocked* ▪ *Quarantine*
Technologies	Elements of technologies included in protected objects that were triggered on events. If you add a text object, you can specify its value. If you add a text object and apply negation to the attribute, then the query results will not include events that contain the selected text object with the specified value. See also "Examples of Using Queries", *Example 6*. **Note:** The text and graphic objects which were migrated from the previous versions of the System, as well as previously deleted ones, are available to be added to the search. Their names will be marked red in the search line.
Protected objects	List of triggered protected objects. You can select separate protected objects as well as catalogues.
Event content	
Number of attachments	Using **Yes**/**No** switcher, specify if the event contains attachments. For events with attachments, specify the minimum and the maximum number of attachments the event may include. If you click **Yes** and do not set the number of attachments, the query results will include all events with attachments. Attachments in the archives are also taken into account
Attachment name	The name of the object attachment. Both file name and extension must be specified. You can specify the value using wildcards: • "?" - to replace a single character in the beginning or at the end of the string • "*" - to replace any number of characters in the beginning or at the end of the string **Note**: If the attachment name contains a comma, the comma must be screened with \. For example, the 'test1,2.txt' attachment name should be specified as 'test1\,2.txt'. See also the "How to find the event by its attachment" knowledge base article.
Attachment format	Attachment format. You can select multiple values from the list and specify if it is required to search for: • Encrypted file; • Spliced file; • Incorrespondence of signature and extension
Path to file	File source. You can specify the value using wildcards:

	• "?" - to replace a single character in the beginning or at the end of the string • "*" - to replace any number of characters in the beginning or at the end of the string
File creation date	Attachment creation date
File modification date	Attachment modification date
Attachment size	Size of the attached file. You can specify a minimum or maximum file size or both parameters.
Event text	Specify the search text. Search results will include events whose text contains all listed words regardless of their location and order, letter case and morphology. Search is performed through all the event contents. Wildcards ("*", "?") are not supported. When the condition is denied, events whose text contains all specified words will be excluded from search results. **Note:** Search results will contain only those events that have already been indexed at the moment of the query execution. Events are indexed every ten minutes, however, under a heavy load on the server, this interval may increase.
User attributes	
	Attributes which can be added into the System via plugins, registered in Traffic Monitor (see Plugins). Thus increasing the amount of information to be processed and transmitted via adding attributes of third-party systems that are events sources. User attributes can be used in the rules of data protection policies. Examples of possible user attributes: • conversation duration • event identificator in initial system • hyperlink to event in initial system • type of action in network media
Terminal name	The name of the device that was used to remotely connect to the employee's workstation. The attribute is specified for the "Terminal session" copy receiver in the events of file exchange via terminal session. Terminal name is a user attribute of the default InfoWatch Device Monitor plugin.
Browser tab address	Address of the active browser tab at the moment when the event was created. The browser tab address is a user attribute of the default InfoWatch Device Monitor plugin.

After condition is selected you should specify its value in the line. The first characters you've input will search the first 10 results in the following fields: *Senders, Receivers, Entered perimeters, Left perimeters, Computers, Resources, Tags, Applications, Source application, Receiver application.*

For example, for *Senders* condition no more than 10 statuses, 10 persons, 10 groups will be displayed as result. To find the entity which is not displayed yet, input few characters more.

By default, all attributes are checked for equality to specified values (parameter next to the attribute name). Results of the query execution will include events whose parameters have specified values.

To exclude events with specified values from the results, apply negation to the required attributes.

Equality or negation parameter can be set for the following attributes:

- Event ID
- Senders
- Recipients
- Entered perimeters
- Left perimeters
- Computers
- Resources
- Tags
- Policy
- Attachment name
- Attachment format
- Event text
- Analysis results
- Protected objects
- Terminal name
- Browser tab address

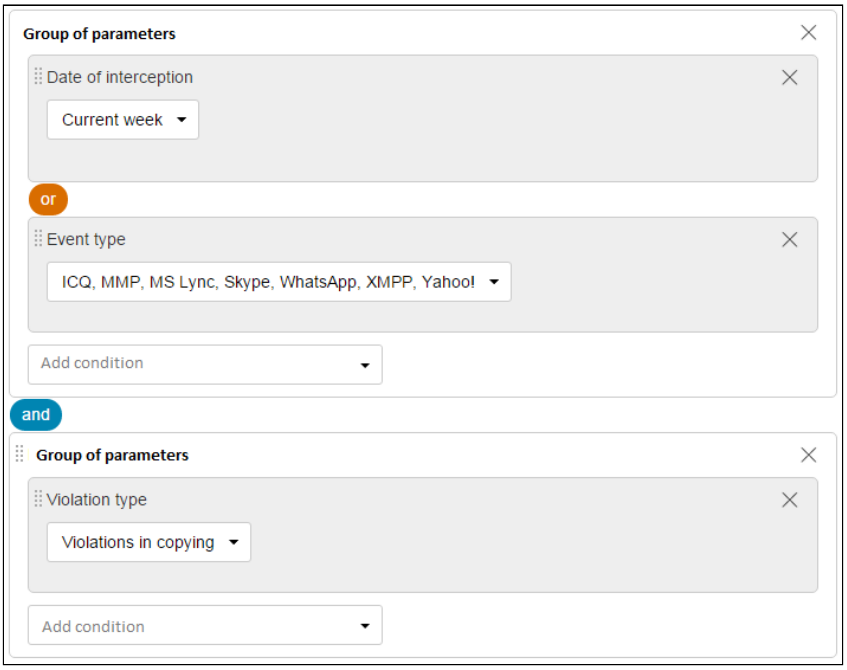
If a negation parameter is applied to an attribute with multiple values, then events that contain specified values will be excluded from search results. For example, if `user1@example.com` and `user2@example.com` users are specified as Senders, then events with the sender `user1@example.com` or `user2@example.com` will be excluded from search results.

User's target actions:

- Creating a standard query (see "Query Creation in Standard Mode")

Advanced Mode

The advanced mode is intended for more flexible adjustment of the query parameters.



When creating a query, you can use the following elements:

- Event attributes – a set of attributes assigned to the intercepted object
- *Group of parameters* element – a container which logically separates parts of the query
- = – a parameter of attribute equality. Indicates that the query results will include events with specified parameter values;
- ≠ – a parameter of attribute negation. Indicates that events with specified parameter values will be excluded from the query results.

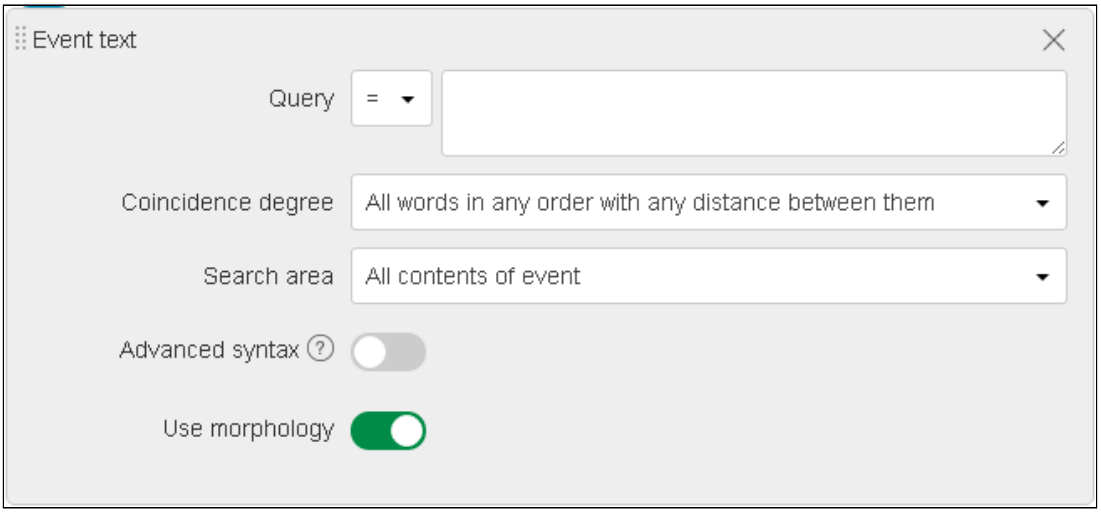
In the advanced mode, you can also perform a flexible search on the text of events.

User's target actions:

- Configuring advanced queries (see "Query Creation in Advanced Mode")

Search on the Event Text

When creating a request in the advanced mode, you can specify conditions of search on the event text.



Full-text search parameters:

Parameter	Description
Query	The text which the event contains (if the attribute is applied =) or does not contain (if negation ≠ is applied to the attribute)
Coincidence degree	Specify the required coincidence degree: • **All words following each other in specified order** - search results will include events whose text contains all listed words arranged in the specified order. If the condition is negated, search results will include events whose text does not contain listed words arranged in the specified order. • **All words following each other in any order** - search results will include events whose text contains all listed words in any order. If the condition is negated, search results will include events whose text does not contain listed words irrespective of their order. • **All words in any order with any distance between words** - search results will include events whose text contains all listed words irrespective of their order and distance between words. If the condition is negated, search results will include events whose text does not contain listed words or contains not all of them. • **At least one of the words** - search results will include events whose text contains, at least, one of the listed words. If the condition is negated, search results will include events whose text does not contain any specified word.

Parameter	Description
Search area	Specify the area in which the search will be performed: • **All contents of event** - search on all contents of the event will be performed. • **Message body** - search on the message text and message subject will be performed. • **Message subject** - search on the message subject will be performed. • **Attachment** - search on the attachments text and file names will be performed. • **File name** - search on the attachment file names will be performed.
Advanced syntax	Enable this setting if you want to specify the sought-for text using boolean operators. For details, see "Using advanced syntax".
Use morphology	If this setting is disabled, search results will include only those events which contain the sought-for words in a specified grammar form. **Note:** Search by exact match (without consideration of morphology) can be performed only if events were indexed with enabled "`IndexExactWords`" option. For detailed information on this setting, please see the document *"Traffic Monitor. Configuration Files Guide".*

Please note that:

- Words must be divided with spaces
- Search in not case-sensitive
- Using wildcards ("*", "?") is not supported
- Hyphen ("-") is not taken into account while searching. Search is performed by each word, which is a part of a word with hyphen used

> **Note:**
>
> Search results will contain only those events that have already been indexed at the moment of the query execution. Indexing of events is performed every ten minutes, however, under a heavy load on the server, this interval may increase.

User's target actions:

- Configuring an advanced query (see "Query Creation in Advanced Mode")
- Using advanced syntax in queries (see "Using Advanced Syntax")

3.2.2 Object Interception

The query results (see "Queries") contain a list of events which satisfy the query conditions.

Information on the event is presented in following ways:

- the event tile (or the table entry) contains general information about the event;

- each event table row contains information on the attributes selected on **Columns** tab;
- the brief event viewing form displays the most commonly required information;
- the detailed event viewing form displays complete information about the interception object.

Event attributes:

Element	Description
Object ID	Event unique identifier in the System
User decision	Decision the user made for the event. Possible choices: • *No decision* • *Violation* • *No violation* • *Requires additional proceeding*
Event type	The source of actions which led to the event creation. Possible choices: •  - Clipboard (copy and paste data using clipboard) •  - Internet activity (post requests to Web resources) •  - File exchange (copying files to an external device or to a shared folder, transfer via FTP) •  - Printer and MFP (sending files to print) •  - Recording media (sending or receiving photos) •  - Email (sending and receiving data via mail on client or mail in browser) •  - Messenger (sending or receiving messages through Skype, MS Teams (if the adapter is installed), MS Lync, ICQ(OSCAR), XMPP, Telegram, WhatsApp) •  - File operations (file recording and reading) •  - File storage (in SharePoint 2007/2010/2013 file storage, shared network resources and on local drives of workstations)
Sending date	Date and time when a mail server received the mail (only for e-mails)
Senders	The list of traffic senders
The sender's computer	The name of the computer from which traffic was sent
Recipients	The list of traffic recipients

Element	Description
Policies	List of policies triggered on analysis of this event
Categories	List of categories assigned to this event
Protected objects	List of protected objects triggered for this event
Elements of analysis	The list of elements of analysis contained in the triggered protected object
Website topic	Type of inappropriate resources visited by the employee
Tags	List of tags assigned to this object
Date of interception	Date and time when traffic was intercepted by the System
Insert date	Date and time when the event was saved into the Database
Size	Size of the event (in bytes)
Violation level	Characteristics of the violation assigned to the event. Possible choices: • *None* - is marked with a gray (■) colour on the tile • *High* - is marked with a red (■) colour on the tile • *Medium* - is marked with an orange (■) colour on the tile • *Low* - is marked with a green (■) colour on the tile
Delivery status	Indication of whether the message was delivered (only for SMTP messages when the System operates in the “inline” mode. See the document “*Infowatch Traffic Monitor. Installation Guide*"). Possible choices: ▪ *Pending* ▪ *Successfully delivered* ▪ *Failed* ▪ *Delivery Attempt Failed* ▪ *Blocked*
Verdict	The conclusion which the System assigned to the object as a result of analysis. Possible choices: • *Allowed* ( ) • *Blocked* ( ) • *Quarantined* ( )

Element	Description
Interception server	The name or IP address of the server which intercepted the object

See also:

- "Event Tile" - on presenting the event and its attributes.
- "Table view of Events" - on displaying information on selected event attributes.
- "Brief Event Viewing Form" - on displaying general information about the event.
- " Detailed Event Viewing Form" - on displaying advanced information about the event.

Event Tile

In event list, each event is displayed as a tile:



The event tile contains general information about the event: the list of senders and recipients, the event ID, the date and time when the event was generated, a description of the event.

Also, the event tile displays the following data (the number is the number of an element in the screenshot).

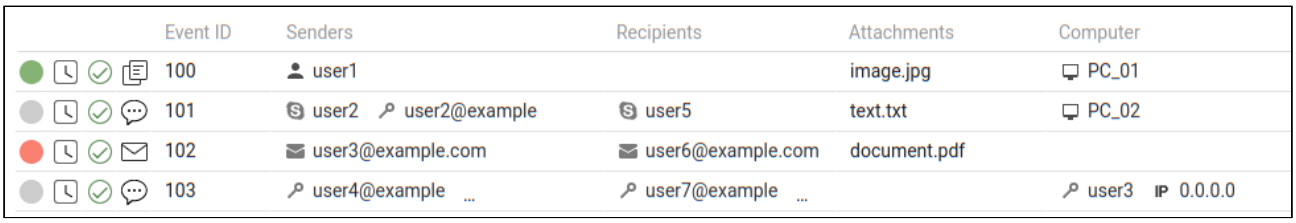
> **Note:**
>
> The set of displayed attributes depends on the event type.

1. The colour of the violation level. Possible values: *High*, *Medium*, *Low*, *No violation*.
2. The event type. Possible values: *Clipboard, Keyboard input, Screenshot, Web message, Facebook, WhatsApp, ICQ, MS Lync, Mail.ru Agent, Skype, MS Teams* (if the adapter is installed), *Telegram, XMPP, Vkontakte, Mail on Client, Mail in Browser, FTP, Removable device, Cloud storage, Terminal session, Print, Read file, Write file*.
3. The user desicion. Possible values: *Violation*, *No violation*, *No decision*, *Requires additional processing*.
4. The verdict. Possible values: *Allowed*, *Blocked*, *Quarantine*.
5. The sending status. Possible values: *Sent, Not sent, Waiting for sending.*
6. The list of triggered policies.
7. Tags assigned to the event. For details, see "Tags".
8. The screenshot indicator. Is displayed if a screenshot has been created for a person or computer.
9. The attachment indicator. If the event contains attachments, an indicator with the number of attachments is displayed. Attachments in the archives are also taken into account.
10. Screenshot thumbnail. If an event has a screenshot, a thumbnail image of the screenshot is displayed. Clicking on a thumbnail will open the original image.

You can view more data on the event in a brief or detailed event viewing form.

Table view of Events

Table view of events is displayed when using table mode:



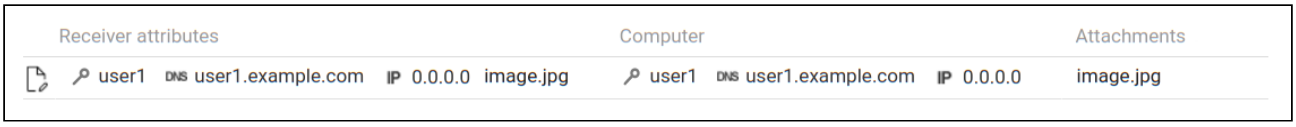
Each column of the table corresponds to an event attribute. On **Columns** tab, when creating or editing query, you can select the columns that will be displayed in the table (see "Queries").

To change sorting order of the rows, left-click the column title you want to sort by. Table records will be sorted by attribute values in ascending/descending order.

> **Note:**
>
> Sorting is not possible by *Subject*, *Computer type*, *File creation date*, *File modification date*, *Scanning target*, *Task name*, *Task start date, Receiver attributes, Terminal name, Browser tab address* columns.

To move a column, left-click and hold the column title, move it along the title row. Release the button, column will be moved to the specified location.

Receiver attributes column:
In addition to columns corresponding to a single event attribute, **Receiver attributes** aggregation column is available.



Depending on event type, **Receiver attributes** column may contain information from the following columns:

- *Attachment name*
- *Path to file or receiver address*
- *Computer*
- *Receiving device name*
- *Source application*
- *Receiver application*
- *Recipients*

> **Note:**
>
> By default, **Receiver attributes** column is not displayed in the table, you can find it in **Available fields** list.

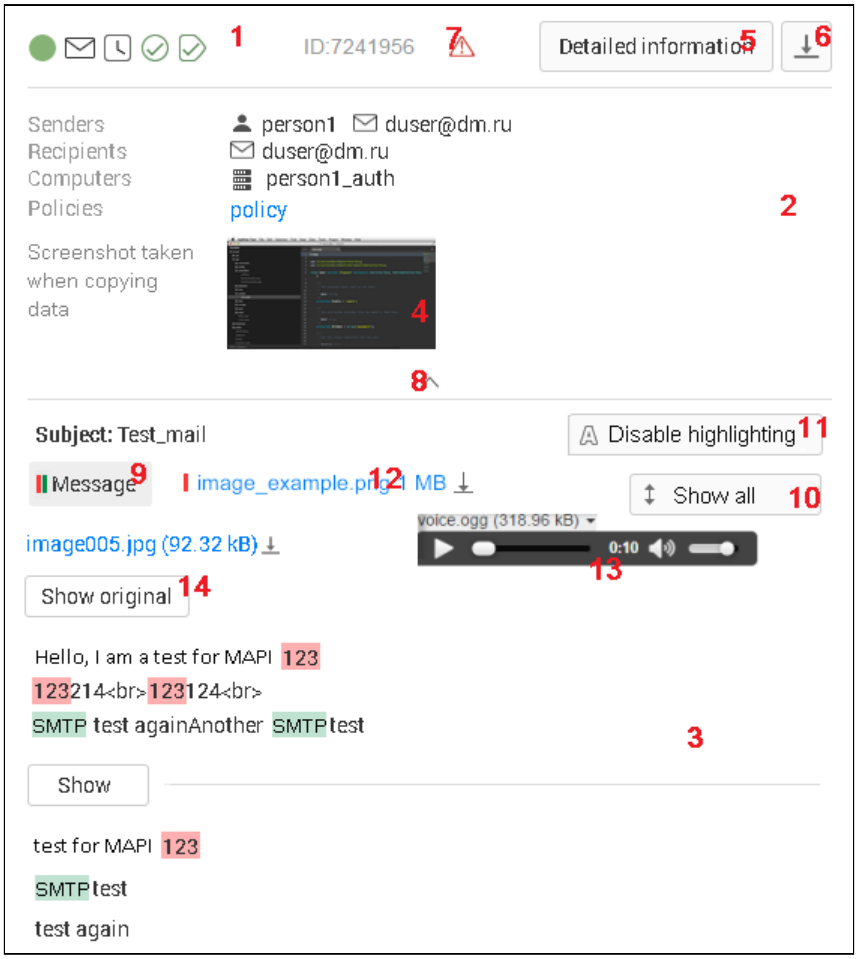
> **Warning!**
>
> **Receiver attributes** column is not included in event export, even if added to **Displayed fields** list.

User's target actions:

- view information about events (see "Viewing events")
- choose event fields (see "Choosing Event Fields of View")

Brief Event Viewing Form

A brief event viewing form is displayed in the right part of the workspace when you select an event in the list and allows you to get general information about the event.



The brief event viewing form includes the following areas (a set of elements in each area may differ depending on the event type):

1. The upper part of the form (№ 1in the screenshot) where you can see:
   - event ID;
   - indicators of the following event attributes: the violation level, the event type, the user decision, the verdict, a delivery status (for possible attribute values, see "Event Tile");
   - the **Detailed** button (№ 5 in the screenshot), clicking which opens the detailed event viewing form (see "Detailed Event Viewing Form");
   - button (№ 6 in the screenshot) which allows you to save a shadow copy of the event (see "Saving Events (for SMTP mail)"). The button is displayed for SMTP messages only;

- the indicator of processing errors (№ 7 in the screenshot). Is displayed if errors occurred during processing. You can see more details on the errors in the detailed event viewing form.

2. The area for viewing the event parameters (№ 2 in the screenshot).
   In the viewing area, you can see information on senders, recipients, triggered policies, and protected objects. Protected objects and policies that have been removed from the System are marked in red. For events containing a screenshot, a thumbnail of the screenshot is displayed (№ 4 in the screenshot).
   Click on a thumbnail of the screenshot to open the screenshot. To hide the area with the event parameters, click ^ (№8 in the screenshot). To restore the area, click v .
3. The area for viewing the event content (№ 3 in the screenshot).
   In the viewing area, you can view the event text, attachments, and sound files.
   By default, the event content is highlighted: triggered protected objects are highlighted in red, results of a search by the event text are highlighted in green. The colour (№ 9 in the screenshot) indicates that the event contains triggered protected objects and/or found text.

   > **Note:**
   >
   > In a brief event viewing form, all triggered protected objects are highlighted in the same colour. To view protected objects to which the highlighted text corresponds, use the detailed event viewing form.

   By default, the viewing form displays not all event text, but snippets which contain triggered protected objects or the found text. To unfold text between the two snippets, click **Show**. To view the whole text of the event, click **Show all** (№ 10 in the screenshot).
   For emails with HTML markup or attachments which can be displayed in an original format (images, PDFs), a button for choosing a viewing mode is displayed (№ 14 in the screenshot). Possible values:
   - **Show extracted text** - the text is displayed without formatting. This option allows you to view hidden text (e.g., white text or text in the picture name);
   - **Show original** - this option allows you to view pictures, tables, and markup.

   To completely disable the highlighting, click **Disable highlighting** (№ 11 in the screenshot).
   If the event contains an intercepted voice message from Skype, then you can listen to the message using tools for voice messages (№ 13 in the screenshot).

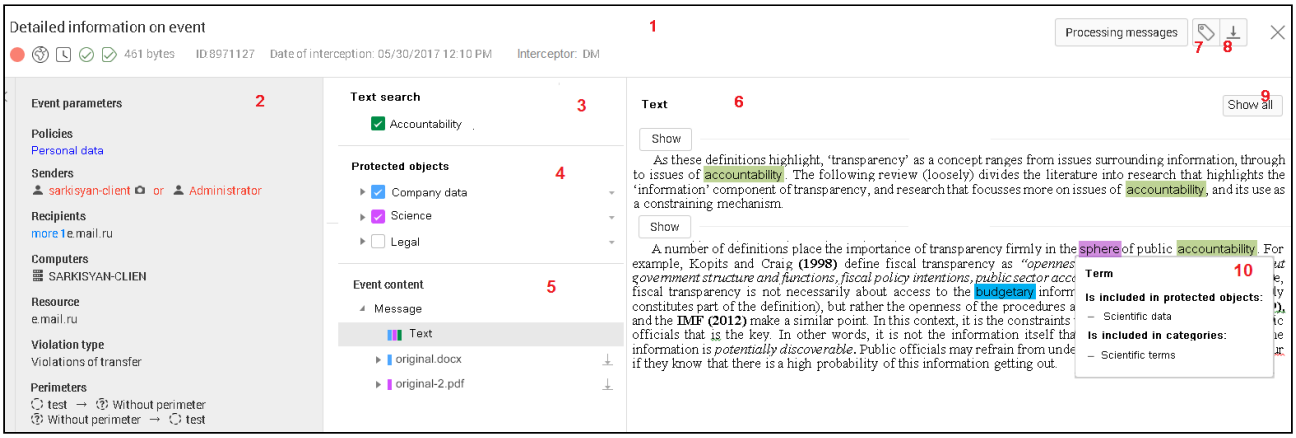
   To save an attachment to your computer, click ↓ (№ 12 in the screenshot) next to the attachment name.

User's target actions:

- Viewing Brief Event Form

Detailed Event Viewing Form

A detailed event viewing form for a selected event opens when you click **Detailed information** in the brief event viewing form (see "Brief Event Viewing Form").



The detailed event viewing form contains the following areas (a set of elements in each area depends on the event type):

1. The upper part of the form (№ 1 in the screenshot), which displays:
   - indicators of the event attributes: a violation level, the event type, the user decision, a verdict, a sending status (possible attribute values are described in "Event Tile");
   - event size;
   - event ID;
   - date and time when the event was intercepted;
   - an interceptor by which the event was received;
   - **Processing messages** button clicking which opens a window with system messages about processing stages and errors if any;
   - button (№ 7 in the screenshot) which allows you to set a tag to the event (for details, see "Tags");
   - button (№ 8 in the screenshot) which allows you to save a shadow copy of the event (see "Saving Events"). The button is displayed for SMTP messages only.
2. The **Event parameters** area (№ 2 in the screenshot) which displays information on senders, recipients, triggered policies, protected objects, perimeters, etc.
   For events containing screenshot, a thumbnail of the screenshot is displayed.
3. The **Text search** area (№ 3 in the screenshot). It is displayed, if the query conditions include a search for the event text.
4. The **Protected objects** area (№ 4 in the screenshot). A list of triggered protected objects and elements of technologies that are included in these protected objects. Protected objects and elements of technologies that have been removed from the System are marked in red.
5. The **Event content** area (№ 5 in the screenshot). Displays the event content: the message text, attachments, voice messages.

   The button next to the attachment name allows you to save a selected file to your computer.
6. The viewing area (№ 6 in the screenshot). Allows you to view the message text and the text extracted from attachments.

> **Note:**
>
> If the text is extracted from PDF document by Device Monitor agent, the text will contain information about document properties.

Be default, in the viewing area (№ 6 in the screenshot), the text is displayed as snippets which contain triggered protected objects or the found text.

To unfold the text between the two snippets, click the **Show** button between the selected snippets. To view the whole text, click **Show all** (№ 9 in the screenshot).

Protected objects and found text within snippets are highlighted. When highlighting is enabled, the elements are highlighted as follows:

- For each protected object, a separate colour is used. All triggered elements of technologies related to the protected object are highlighted in the same colour.
- For a triggered Autolinguist category, up to 50 terms belonging to the category are highlighted in the text.

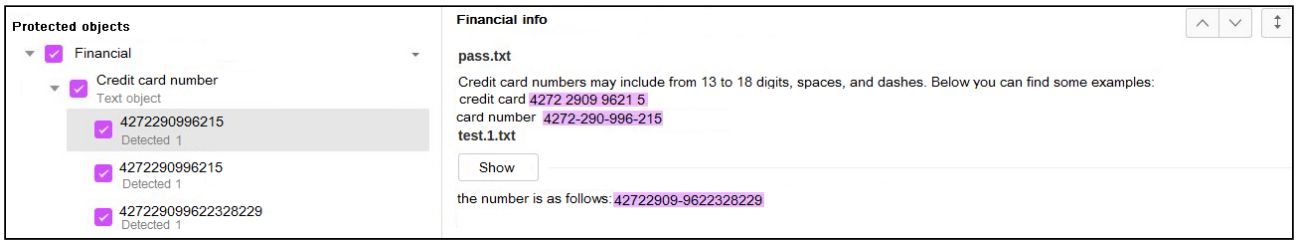
> **Note:**
>
> The term highlighting for Autolinguist categories is not supported for events created in Traffic Monitor version 7.4 and earlier.

- If a part of the text belongs to several elements of technologies, this part is highlighted in gray.
- Results of a search by the event text are highlighted in green. The result is highlighted in green, even if the result belongs to technology elements.

> **Important!**
>
> If transliteration was used for analysis of intercepted text, then the analysis results can be highlighted with offset.

You can adjust the highlighting in the **Text search** and **Protected objects** areas by selecting checkboxes next to desired values. You can enable highlighting for a selected text search query, selected protected objects or separate elements of technologies included in the protected object.

For system text objects detected in intercepted data, values are reduced to the normal form. Thus, in the **Protected objects** area (№ 4 in the screenshot), all values of the same text object are represented in the same way.



> **Note:**
>
> For custom text objects, values are not reduced to the normal form, thus the **Protected objects** area displays the real value of a custom text object.

When hovering over the highlighted text in the viewing area, you can see additional information on the element (№ 10 in the screenshot):

- for a term - a category that includes the term;
- for a text object - the text object name.

To completely disable the highlighting, deselect all checkboxes - in this case, the whole event text is displayed without highlighting.

In the **Event content** area, the colour indicator shows technologies which were triggered for a given element. For example, in the event shown in the screenshot, the following technologies are triggered:

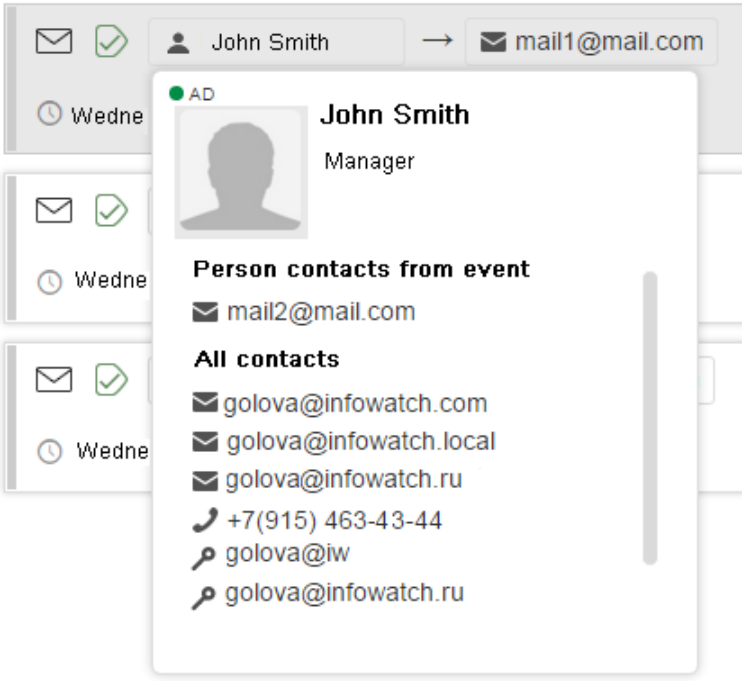
- for `original.docx` attachment - the *Company data* protected object;
- for `original-2.pdf` attachment - the *Science* protected object;
- for the event text - the *Company data* and *Science* protected objects; besides, the search text is found.

User's target actions:

- Viewing Detailed Event Form

3.2.3 Contact Identification in Event

Based on data extracted from the event, the System determines traffic senders and recipients (persons, groups of persons, and computers). This process is called contact ***identification***. For identified senders and recipients, a name of the person, group or computer is displayed on the event tile. Clicking this name opens the sender or recipient card. The card contains contacts extracted from the event as well as contact data which are stored in the System.



If while processing an event, the System detects new private contacts of a person, detected contacts are added to the person card automatically. The process of automatic adding new contacts to existing persons is called ***post identification***. As a result of post identification, such data as email address, mobile phone, accounts in messengers (ICQ, Skype, Telegram, MS Teams (if the adapter is installed), WhatsApp) and social networks accounts (Facebook, VK) can be added to the person card.

Note:

Post identification applies to traffic senders only. Contacts of traffic recipients are not identified.

Note:

For the following resources, post identification is not supported:

- odnoklassniki.ru
- gmail.com

Note:

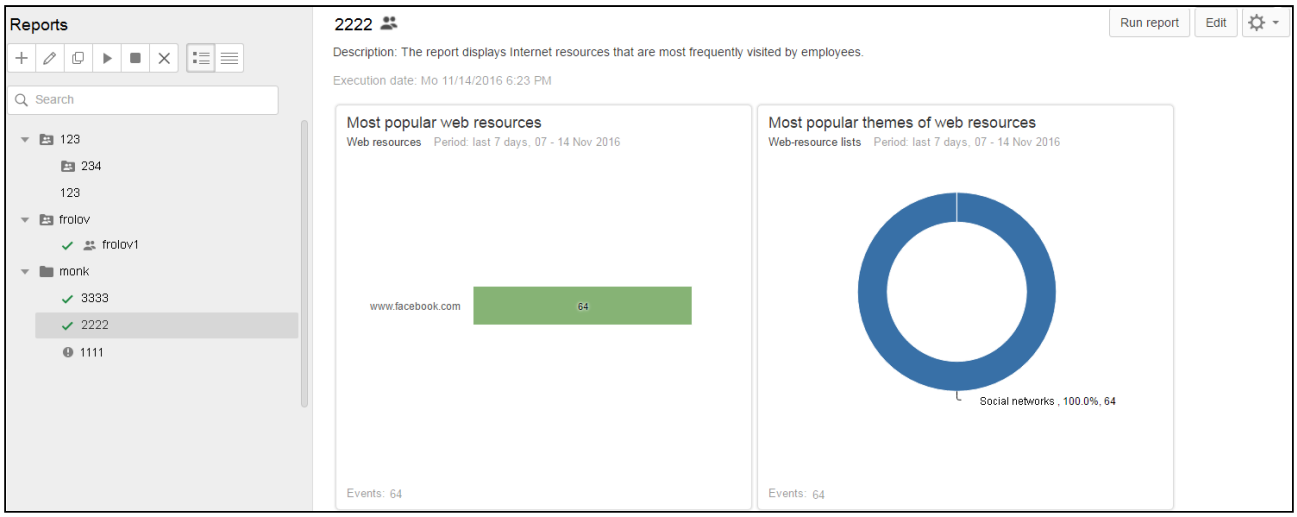
It can happen that personal cards of different users who work on different computers may contain the same accounts in messengers (e.g., Skype) as their contacts. This can happen if those users have logged into different computers under the same domain name or if they have logged into the same computer under different domain names.

3.3 Reports Section

About the section:

Contains a list of reports and tools for managing them.

The report is a set of widgets which contain data on intercepted objects in the form of charts and diagrams (see "Widgets of Reports").



In the left part of the workspace, you can see a list of reports, a toolbar, and a search field. The right part of the workspace displays a selected report or the report creation/editing form (see "Report Creation Form").

Reports can be located in the root or within folders. Folders make it possible to group reports with a common subject, define access rights for a group of reports, inherit access rights for subfolders, etc. A folder may include both reports and subfolders. On how to create a folder, see "Creating Folder with Reports".

You can choose how to display folders and reports in the list: as folders (button on the toolbar) or as a flat list (button on the toolbar).

Folders that are available only to the owner are marked with . If the folder is also available to other users of the Console, it has icon.

The **Pre-installed reports** folder includes reports that are available to all users of the System:

- *Statistics on activity over the last 7 days* - displays information on the number of events intercepted by the System, the most active senders and recipients, as well as the most popular content routes between senders and recipients;
- *Activity on the Internet over the last 7 days* - displays Internet resources to which the company employees send requests most frequently;
- *Transfer of secured data over the last 7 days* - displays protected objects contained in events intercepted by the System and the information security policies applied to the events.

When you create a report in a folder, access rights are either inherited from the folder or specified individually. If the report is available not only to the owner but also to other users of the Console, it has icon.

To view required statistics, select a report in the list or create a new one (see "Creating report").

> **Tip.**
>
> To find a folder or report by its name, use the **Search** field.

To run a selected report, click on the toolbar or use the **Run report** button in the right upper corner of the form. Once the report execution is complete, the System displays a notification.

If the report has already been executed and contains actual data, it is marked with . When you select such a report, its widgets with statistics on intercepted objects are displayed to the right.

If the report is being executed at the moment, the icon is displayed next to its name. For reports whose execution failed, the icon is displayed.

When you select a query in the list, the button is displayed in the right upper corner of the form. Clicking this button opens a drop-down list, where you can choose the required action
:

- open the report execution history;
- copy the report;
- delete the report;
- save the report as a file in one of the supported formats.

User's target actions:

- Creating folder with reports
- Creating report
- Creating and Configuring Widget
- Viewing ready reports

3.3.1 Report Creation Form

When you create or edit a report, the form is displayed where you can specify the report parameters.



You can specify the following settings:

- **Name**;
- **Description** (optional parameter);
- **Use common interception date** - select this option if you want all queries that are used in the report widgets to be generated for the same period. When selecting this option, a drop-down list is displayed where you can specify the desired period. By default, the option is disabled and, for each widget, the interception date is specified independently in the query parameters.
- **Widgets** - click **Add widget** button on the **Widgets** tab to add widgets on which required statistics will be displayed (for details, see "Widgets of Reports").
- **Access** - on the **Access** tab, specify access rights for the report. Possible choices:
    - If you create a report within a folder and the **Apply rights for related reports** option is selected, then access rights for the report will be the same as access rights specified for the folder. Editing access rights to the report is unavailable.
    - If you create a report within a folder and the **Apply rights for related reports** option is not selected, or you create a report in the root, then you can specify access rights for the report. By default, the report is available only to the owner. To provide access to the report to other users, select required users in the list and set checkboxes next to their names in a field with the required access level (**View and execute access** or **Full access**).

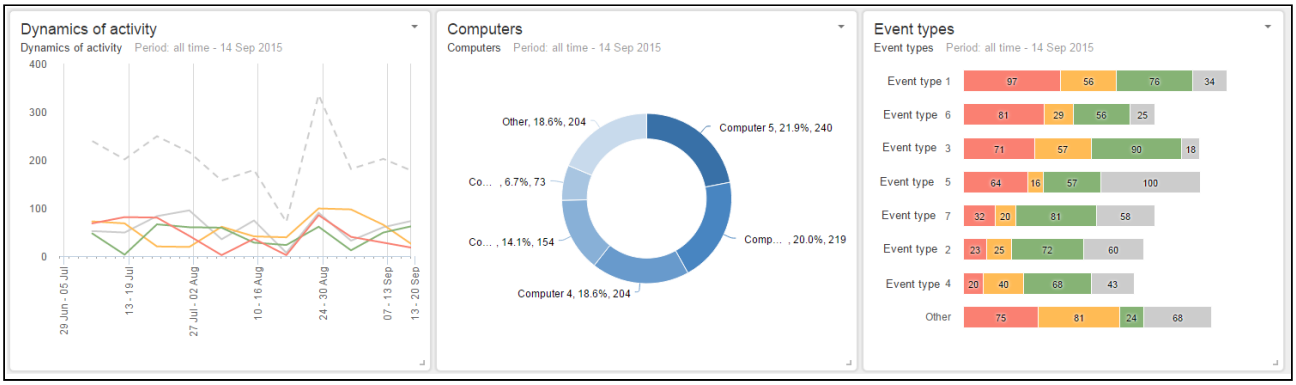
User's target actions:

- Creating report

3.3.2 Widgets of Reports

Widgets are designed to display statistical information in reports.

As a result of the report execution the right part of the workspace displays widgets with data on intercepted objects over a specified period of time.



Widgets can be created for the following data:

Type of statistics	Description
Web resources	Web resources to which the company employees sent requests most frequently
Dialogs	Routes of transferring messages (irrespective of direction) for which the System registered the largest number of events
Dynamics of activity	Dynamics of the number of events intercepted by the System
Catalogs of protected objects	Catalogues of protected objects which are most frequently encountered in data intercepted by the System
Computers	Computers for which the System registered the largest number of events
Protected objects	Protected objects which are most frequently encountered in data intercepted by the System
Senders	Senders for which the System registered the largest number of events
Policies	Policies that were applied to intercepted data most frequently
Recipients	Recipients for which the System registered the largest number of events
User decisions	Statistics on the decisions which the security officer made for events intercepted by the System
Web resource lists	Web resources to which the company employees sent requests most frequently
Event types	Distribution of the number of events into types (mail, Skype, external devices, etc.)

For the chosen type of statistics, you can specify how to display data. Select either of the following:

-  - bar chart with grouping;
-  - bar chart with accumulation;
-  - pie chart;
-  - graph.

> **Note:**
>
> For the *Dynamics of activity* statistics type, only the “graph” diagram can be used. For other types of statistics, the “graph” type is unavailable.

Widget parameters for the “Dynamics of activity” statistics type:

Parameter	Description
Violation levels	Events with a specified violation level will be added to the widget. Select checkboxes next to desired values.
Grouping period	Specify a period for which events will be grouped. Possible values: • minute; • hour; • day; • week; • month; • quarter; • year.

Widget parameters for other types of statistics:

Parameter	Description
Chart type	The following types are available: • bar chart with grouping • bar chart with accumulation • pie chart (except for the "Dialogs" diagram type)
Number of records	The number of records that will be displayed in the widget. Specify a value from 1 to 100. **Note**: For the "User decisions" statistics type, this option is not displayed.
Merge other records into “Other” item	Select this option if you want to add the “Other” item that will combine the rest of records on the widget. **Note**: For the "User decisions" statistics type, this option is not displayed.

Parameter	Description
Show values	Select this option for numerical values to be displayed on the widget.
Show proportions	This option is available for the pie chart only.

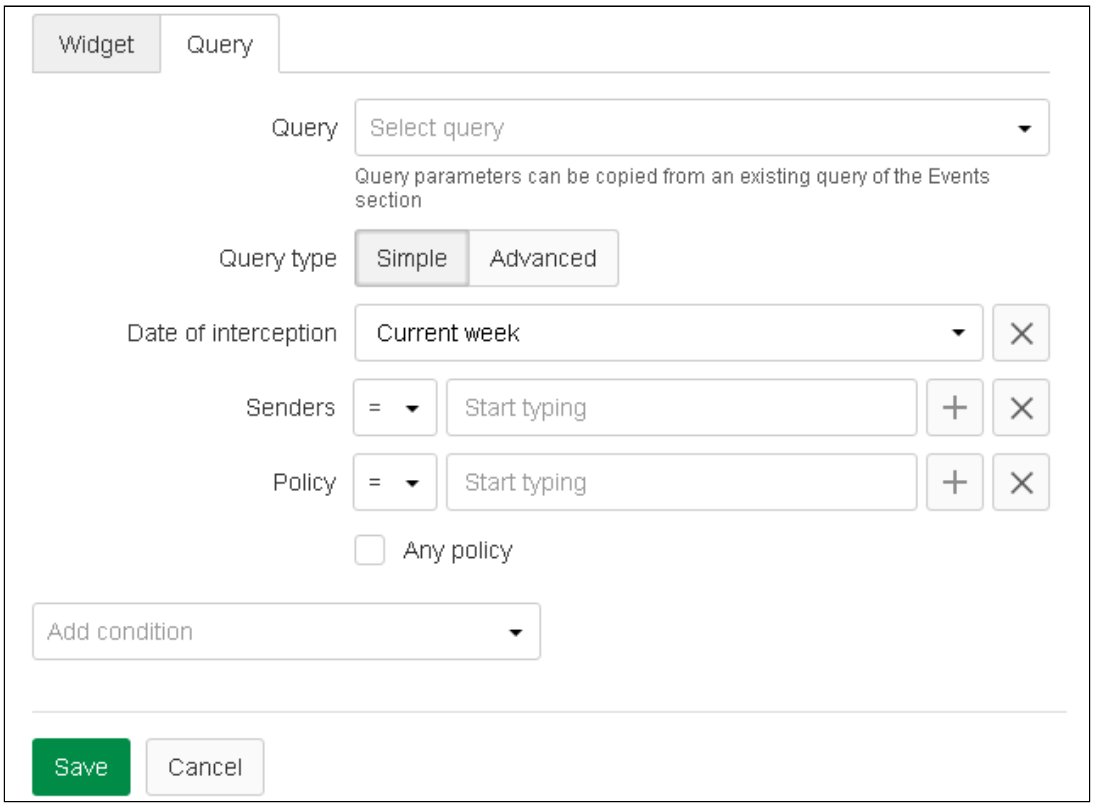
User's target actions:

- Configuring widgets to display statistical information (see "Managing widgets of reports")

3.3.3 Queries

A query allows you to specify conditions according to which data on interception objects will be displayed in the widget.

To create a query, open the **Query** tab in the widget creation window (see "Widgets of Reports").



The **Query** tab in the widget creation window

You can copy parameters of a query that has been added in the Events section (for this, in the **Query** field, select the required query from the drop-down list), or create a new query.

You can create a query in a standard or advanced mode:

- *Standard mode* - allows you to specify parameter values and, if necessary, apply the negation ≠ to the parameter. All conditions are joined by the conjunction (logical "AND"). For details, see "Condition".

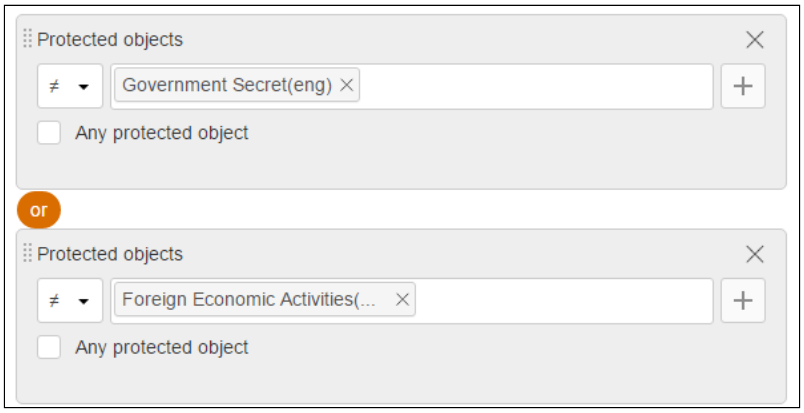
- *Advanced mode* - allows you to perform more flexible configuration of the query conditions using the conjunction (logical "AND") and disjunction (logical "OR"). For details, see "Advanced mode".

To select the mode, use **Standard** or **Advanced** button in the **Query type** field.

> **Tip.**
>
> If while creating a query in the simple mode, you find out that you need a more flexible configuration, you can switch to the extended mode. All entered parameters will be saved.

Example of using the disjunction:

If parameters in the condition are joined by the logical "OR" and the negation is applied to them, then the report will include only those events which do not contain all specified elements at the same time.



In this example, an event will not be included in the report if the event contains both the "Government secret" and the "Foreign economic activities" protected objects.

User's target actions:

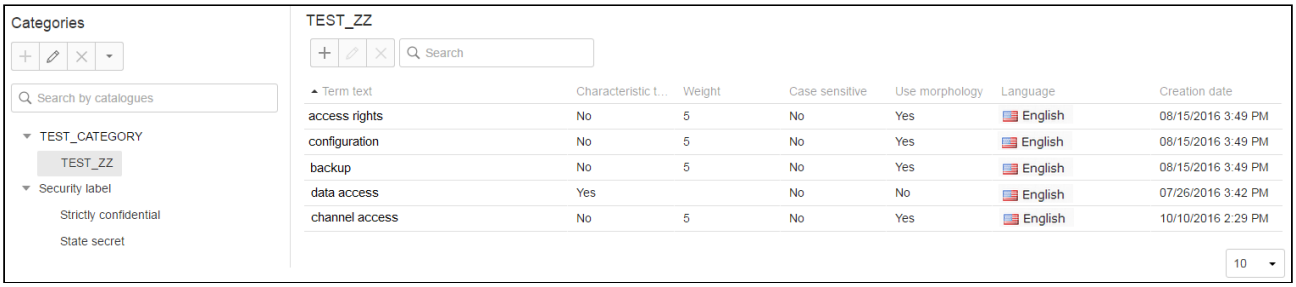
- creating a query (see "Query Creation in Standard Mode" and "Query Creation in Advanced Mode").

3.4 Technologies Section

Reference information:
Technologies are sets of data used for the analysis of interception objects.

About the section:
The section contains:

- editable catalogues of categories and terms, text objects, sample documents, blanks, stamps, DB unloadings
- the automatic classifier of graphical objects and Autolinguist



Technologies section, **Categories and terms** subsection

User's target actions:

- Creating categories and terms
- Creating text objects and their values
- Managing sample documents
- Creating blanks
- Creating stamps
- Creating DB unloadings
- Graphical Objects
- Managing Autolinguist

3.4.1 Categories and Terms

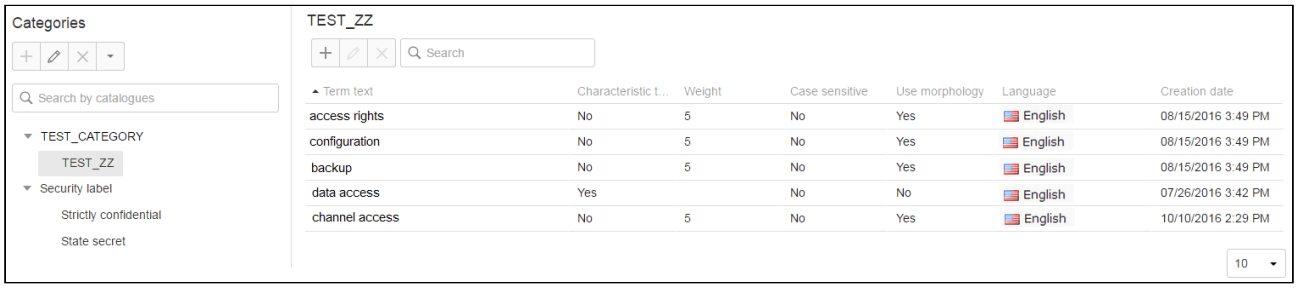
Reference information:

Categories and terms are a set of words and phrases required for linguistic analysis. Each category contains a list of terms.

Categories classify possible violations of a security policy. If the text contains a term that belongs to some category, the System correlates the text with this category.

For example, the *Finance* category contains financial terms (*payment*, *investors*, *prices,* etc.). In this case, the presence of terms "payment", "investors" or "prices" in text allows the System to correlate this text with the *Finance* category.

On the toolbar on the right part of the workspace there is a list of terms within the selected category. The System can perforrm a cross-cutting search of the term by name, the search is to be performed within the selected or enclosed categories. To perform the search through all the section's categories, select the root catalogue. The name of term should be entered in search line within the the right part of the workspace.



User's target actions:

- Creating a list of categories and terms (see "Creating Categories and Terms")
- Importing and exporting categories and terms as a part of the base of technologies (see "Exporting and Importing the Technologies Database")
- Adding categories to protected objects ("Creating a Protected Object")

Categories

Reference information:

The ***category*** is a set of elements corresponding to a specific topic (for example, *Contract documents* or *Tax records*). It contains either the list of categories (subcategories) or the list of elements related to the category.

For categories, the following attributes are specified: a name and a description (if necessary).

For terms included in the category, the following attributes are specified:

- Weight - a value from 1 to 10 specified for all terms of the category as the **Weight** attribute. The default value is 5;
- Language - the language of category terms. The default language is Russian;
- Use morphology - if this option is selected, analysis is performed with respect to all morphological forms of the term. By default is is enabled;
- Case sensitive - if this option is selected, the analysis is performed with respect to the letter case. By default it is disabled.

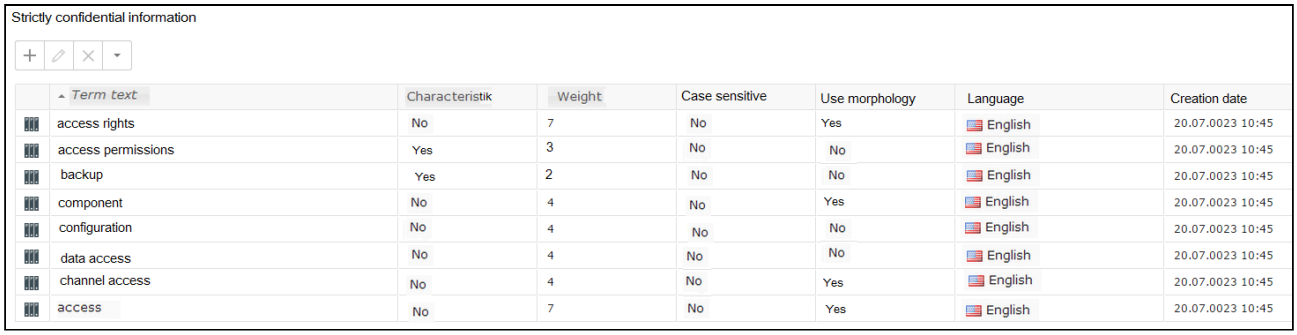
For the category to be detected in intercepted data, it must be included in protected objects.

User's target actions:

- creating subject areas of confidential data (see "Creating Categories and Terms")
- including categories in protected objects (see "Creating a Protected Object")

Terms

Reference information:
The ***term*** is a word or phrase which (if found in the analyzed text) increases the degree of conformity of the text to the category of the found term.



Term text	Characteristik	Weight	Case sensitive	Use morphology	Language	Creation date
access rights	No	7	No	Yes	English	20.07.0023 10:45
access permissions	Yes	3	No	No	English	20.07.0023 10:45
backup	Yes	2	No	No	English	20.07.0023 10:45
component	No	4	No	Yes	English	20.07.0023 10:45
configuration	No	4	No	No	English	20.07.0023 10:45
data access	No	4	No	No	English	20.07.0023 10:45
channel access	No	4	No	Yes	English	20.07.0023 10:45
access	No	7	No	Yes	English	20.07.0023 10:45

Term attributes:

Parameter	Description
Term text	A word or phrase, which maximum length can be 256 characters, including only letters, spaces and hyphens
Characteristic	If this attribute is enabled, then finding the term in traffic certainly assigns the term category to the object
Weight	Indicator of the term significance

Parameter	Description
Case sensitive	Indicates if the case is matched in traffic analysis
Use morphology	Indicates if morphology is used in traffic analysis
Language	The language of the term

Note:

The **Case sensitive** and **Use morphology**, as well as **Language** and **Weight** parameters are set by default when specifying these parameters for the category. Parameters of the term can be then edited and saved. In this case, when editing case and morphology settings of the category, these changes will not apply to the terms.

User's target actions:

- Creating and editing terms (see "Creating Categories and Terms")

Recommendations how to create Categories with Terms

Documents with hardly predicted structures are to be analyzed the same way all other types of documents do. These kinds of documents in large amounts are stored in company's document management system. They are created, resent and printed, etc. A document content is to be analyzed in accordance with limited number of subjects.

Example:

In case you require fixing the messages with tax documentation, so it's required to detect all types of tax declarations, earnings reports or tax debts docs, advance payments calculations, etc. To solve this task you should define the *Key words*, which can be met in all these documents. These words can be for example, as follows: "imputed income", "revenues and expenses", "taxpayer representative", etc. As a result, absolutely different documents can be intercepted: certificate, declaration or tax form. The System analyzes the document's subject.

Main recommendations to create Categories with Terms:

1. Use phrases as terms (phrases contain few words). If you require narrowing your search and detecting one type of documens only (e.g., tax declarations, but statistical tax forms or certificates are not required), you should select longer phrases. The longer phrases are used, the more likely it won't be met in other documents.

   Note:

   Maximum allowed lenght of the Term is 256 characters.

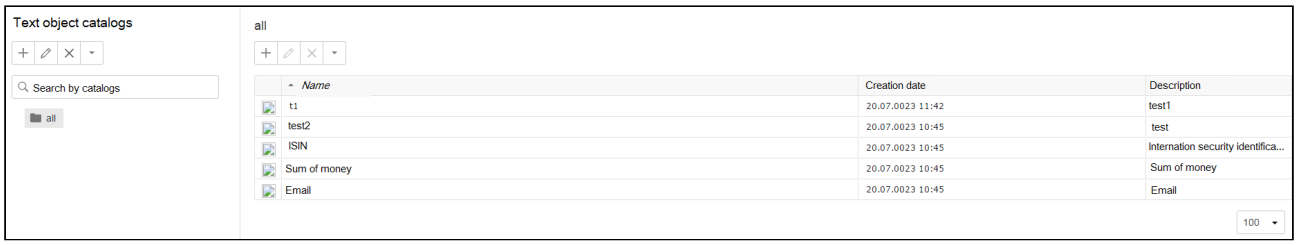
2. You should avoid one word terms (especially the commonly used words, such as "labour', "highest', 'checked"), polysemantic words (e.g., "leak" gas vs data), functional words and meaningful words (e.g., "therefore", "is", etc.).
3. The Term text may contain alphabetic characters, space and hyphen. Since the punctuation marks are ignored during the linguistic analisys, the term "plan for the year" will be found both in "plan

for the year" and in "plan for the year 2022". In case you require detecting messages, which contain non-alphabetic characters (e.g. "TO.P234.67), you should enter this as it is.

4. Characteristic terms show the relevancy to the category in case it is met in the message. Thus, to define the category of the document it is enough to have any characteristic term. Text should contain at least 3 non-characteristic terms. This is required the category with related subject would work.
5. The Weight is used to show the frequency of the term used in the text and related to each other. We do not recommend calculating the frequency of each word, but to leave the default weight value. If you see at once the word used more often, you should use the higher weight value, the less - the lower (e.g., in contract the phrase "this agreement' is often met, so this can be given the highest value). This is not to influence the detection accuracy and will let you minimize the time to create a category.
6. The Term Language is defined to use correct rules to change the word forrms (morphology) of a certain language.
7. Morphology and register parameters are related to each other: if you set the value "Use morphology", the register will become inactive" and vice versa. You can also disable both parameters. Using the morphology let you detect the terms in its different word forms: e.g., tender - tenders. Using a register will let you detect the word in one defined form only.

3.4.2 Text Objects

Reference information:
The ***text object*** is text data extracted from the object body and attachments. It contains no formatting or markup. Text objects are used for analysis and search.



Text objects are created within catalogues. For operations with catalogues (creating, editing or deleting a catalogue; search by catalogues), tools on the left side of the working area are used. Text objects of a selected catalogue and tools for operations with text objects are located on the right side of the working area.

Text objects which are a part of catalogue and tools used to manage text objects (create, edit, delete and cross-cutting search within catalogues) are located on the right part of the workspace. A cross-cutting search is performed in accordance with the name of text object and it is performed within selected catalogue or enclosed ones. To perform the search through all the section's categories, select the root catalogue.

Both system and user-created text objects can be used in the System. The text object value is specified with a pattern.

When you create a text object, specify its name and, if necessary, add a description. To add a pattern for the text object, switch to the edit mode.

For the text object to be detected in intercepted data, it should be included in a protected object.

User's target actions:

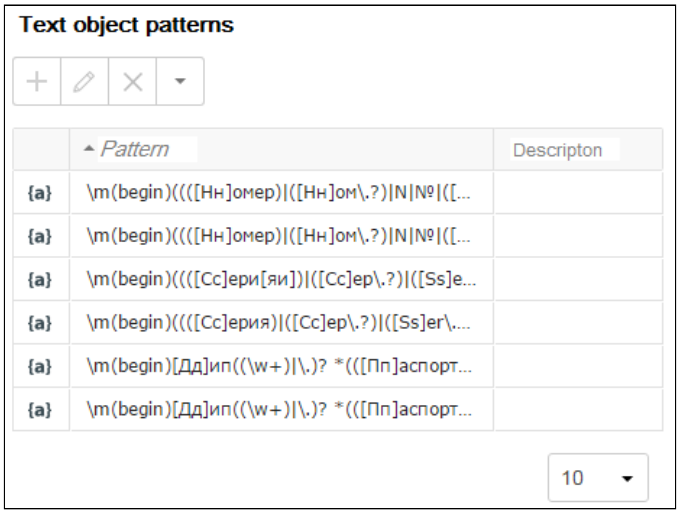
- Creating text objects and their catalogues (see "Managing Text Objects")
- Adding system text object to a selected catalogue (see "Managing Text Objects")

- Importing and exporting text objects as a part of technologies base (see “Exporting and Importing the Technologies Database")
- Adding text objects to protected objects (see "Creating a Protected Object")

Text Object Patterns

Reference information:
The *text object pattern* is a value of the text object set in a form of the exact sequence of characters or with a regular expression. Patterns allow you to specify one or several values for each text object.

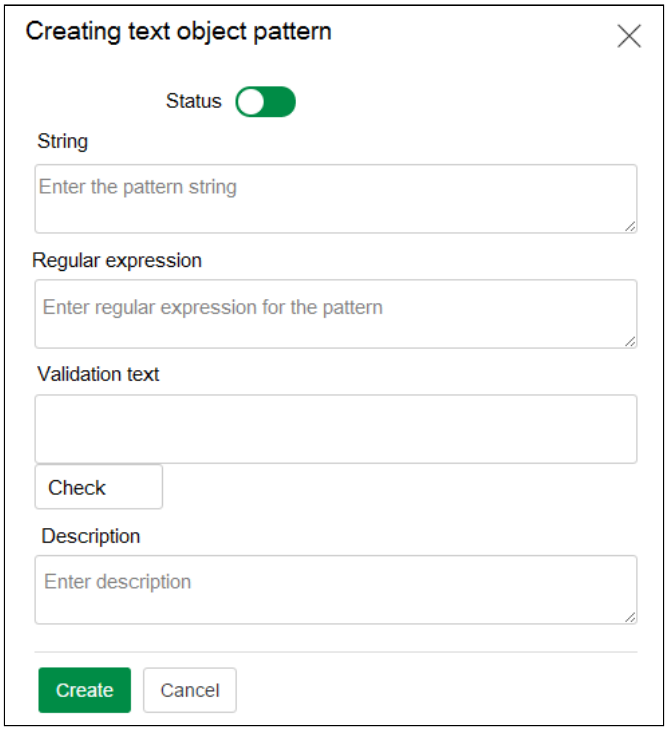
Patterns for a selected text object are displayed when switching to the edit mode of the text object.



The toolbar contains tools for creating, editing, and deleting patterns. The button allows you to change the pattern status: for this, in the drop-down list, select **Activate**/**Deactivate**. The current status is displayed in the left column of the table: active patterns are marked with , inactive ones are marked with .

Warning!

Editing and deleting preinstalled patterns of the system text objects is unavailable.



When adding or editing a pattern, you can specify the following attributes:

Parameter	Description
Status	Indicates if this text object value is used.Possible values: *Active* or *Inactive*
Pattern type	Specify how you want to set the template: as a string or a regular expression.
String	Appears if you select the type of template - *String*. The exact value of the text object specified as a sequence of characters. *For example*, the pattern `example@company.com` will find only the exact matching - `example@company.com`
Regular expression	Appears if you select the type of template - *Regular expression*. Configurable template. For more information on regular expressions, see the Knowledge Base articles: "Syntax of regular expressions" and "Description of macros for text object patterns".
Validation text	Appears if you select the type of template - *Regular expression*. An example of a text for finding the regular expression. Enter the verification text and click **Check**.
Description	If necessary, add a description

User's target actions:

- Creating a text object

3.4.3 Sample Documents

Reference information:
The *sample document* is a document containing quotes for text analysis. Memos, financial reports, contracts, and other sensitive documents can all be used as sample documents. Sample documents are stored in the system as digital prints, their text is not available to either users or System administrators. Sample documents are grouped into catalogues.

Warning!

To operate in the System correctly the sample document should be as follows:

- binary data size - from 128 bytes to 128 Mbytes;
- text data size - from 128 bytes to 30 Mbytes;
- length of simple text for text data - from 10 characters;
- image size - from 100 pixels on one side;
- image sides ratio - no more than 5:1;
- vector data size - from 300 Kbytes (800 primitives);

Sample documents are created within the catalogues. For operations with sample documents catalogues (creating, editing or deleting a catalogue; search by catalogues) tools on the left side of the working area are used.

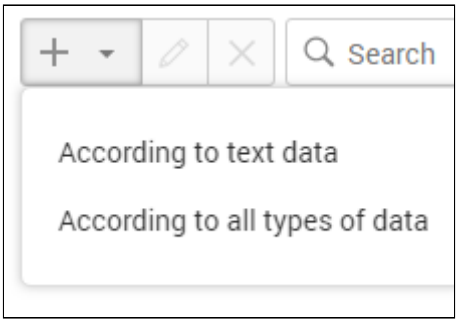
List of sample documents within the selected catalogue and tools for operations with sample documents (create, edit, delete and cross-cutting search within catalogues) are located on the right side of the working area. A cross-cutting search is performed in accordance with the name of sample document and it is performed within selected catalogue or enclosed ones. To perform the search through all the section's categories, select the root catalogue.



When creating a catalogue of sample documents, you can specify the following attributes:

- **Name**;
- **Text data quotation threshold** - the percentage of the sample document that is sufficient for referring the intercepted object to this sample document. For text objects detecting (document text);
- **Binary data quotation threshold** - the percentage of the sample document that is sufficient for referring the intercepted object to this sample document. For detecting binary objects (images, executable files, etc.);
- **Description**.

When adding a sample document to the catalogue, specify the type of added data (**Text** or **All types**) and choose files for loading.



When editing a sample document, you can specify the following attributes:

- **Name**;
- **Text data quotation threshold** - the percentage of the sample document that is sufficient for referring the intercepted object to this sample document. For text objects detecting (document text);
- **Binary data quotation threshold** - the percentage of the sample document that is sufficient for referring the intercepted object to this sample document. For detecting binary objects (images, executable files, etc.);
- **Description**.

To switch to the update mode of the sample document, click the **Update** button in the document edit window.

For the sample document to be detected in intercepted data, it must be included in a protected object.

User's target actions:

- Creating Sample Documents and their Catalogues (see "Managing sample documents")
- Importing and exporting sample documents as a part of the technologies base (see "Exporting and Importing the Technologies Database")
- Updating the sample document (see "Creating Sample Documents")
- Adding sample documents to protected objects (see "Creating a Protected Object")

3.4.4 Blanks

Reference information:
Blank is a formsheet whose version (filled or not) is searched for in the network traffic. Blanks are stored in the System as digital fingerprints, their text is not available for viewing either by users or by the System administrators. The blanks may be surveys, questionnaires and other documents completed in a predefined form.
Technically the blank is a file each line of which contains one field of the blank. Rows are separated by line break. The blank contains at least 2 fields.

Warning!

For correct operation in the System blank should possess the following attributes:

- text data size - to 30 Mb;
- vector data size - from 300 KB (800 primitives);
- number of fields, containing more than 1 word, - 1-2 fields.

How the technology works: search for names of the blank fields is performed, then their order is checked, then, if necessary, the presence of text between fields of the blank is checked. Based on these checks, the System defines whether the blank is filled out.

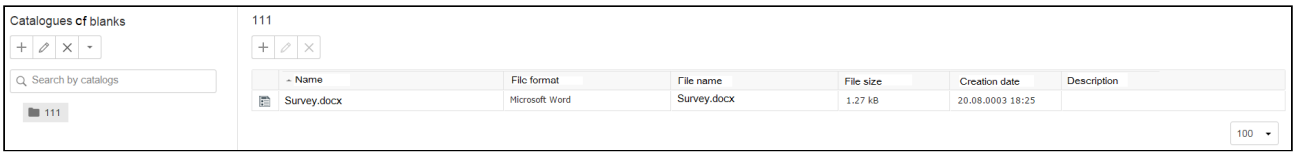
For the blank to be detected in intercepted data, it must be included in a protected object.

Warning!

To match an interception object with a blank the following requirements must be met:

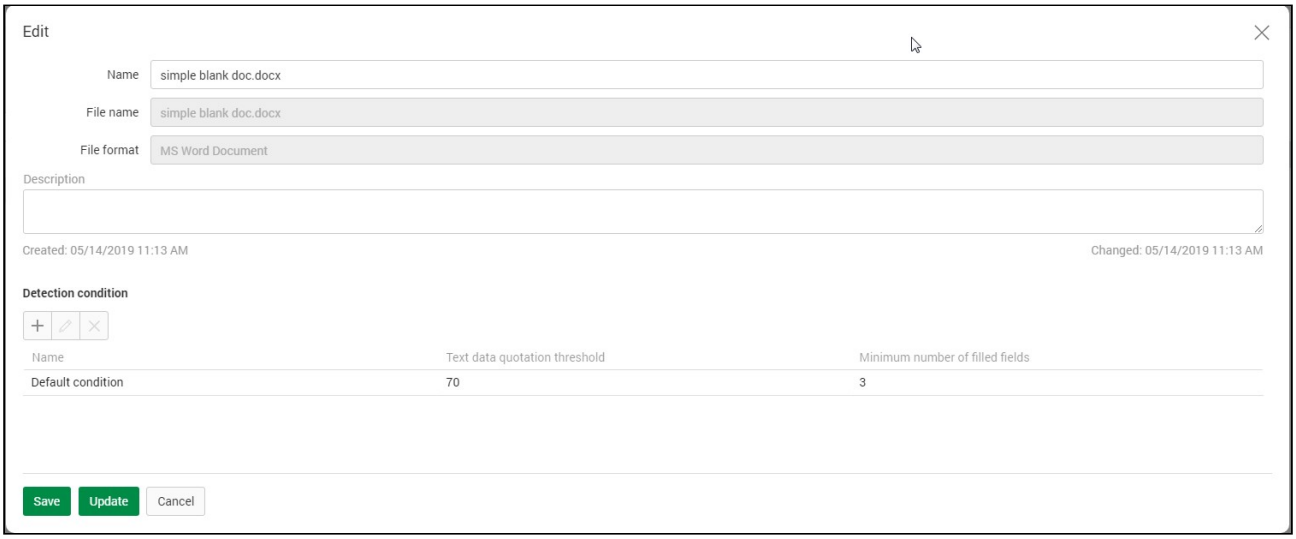
- the object text contains, at least, one field from blank;
- if the number of fields detected in the object text is more than one, then the fields should be in the same order as in the digital print uploaded to the System;
- if detection of filled blanks is set up, then, at least, one character should be placed between the adjacent rows.

Blanks are created within catalogues. For operations with catalogues (creating, editing or deleting a catalogue; search by catalogues), tools on the left side of the working area are used. Blanks of a selected catalogue and tools for operations with blanks (add, edit, delete and cross-cutting search within catalogues) are located on the right side of the working area. The cross-cutting search is performed in accordance with a blank name and it is performed in the selected catalogues as well as the enclosed ones.



In the **Edit** mode, you can view and, if necessary, change attributes of the selected blank. You can also switch to updating the selected blank by clicking the **Update** button.

Detection condition can be specified only when using the editing mode.



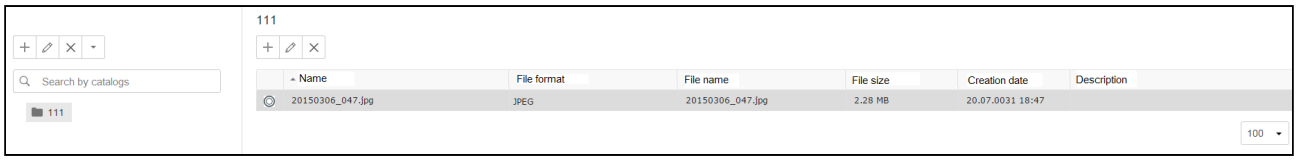
User's target actions:

- Creating blanks and their catalogues (see "Managing Blanks")
- Importing and exporting blanks as a part of the technologies base (see "Exporting and Importing the Technologies Database")
- Updating a blank (see "Managing Blanks")
- Adding blanks to protected objects (see "Creating Protected Object")

3.4.5 Stamps

Reference information:
The ***stamp*** is a stamp image that is searched in the network traffic. Stamps can be images of round or triangular impressions used in organizations.

Stamps are created within catalogs. For operations with stamp catalogues (creating, editing or deleting a catalogue; search by catalogues), tools on the left side of the working area are used. Stamps of a selected catalogue and tools for operations with stamps (create, edit, delete and cross-cutting search within catalogues) are located on the right side of the working area. A cross-cutting search is performed in accordance with the name and it is performed within selected catalogue or enclosed ones. To perform the search through all the section's categories, select the root catalogue.



To successfully load a stamp (round or triangular) to the System, the following conditions should be met:

- stamp image should be against a white background with a minimum amount of white colour along the stamp edges;
- resolution of the stamp should be 150 dpi or higher;
- the minimum image size is 500x500 pixels;
- the maximum image size is to 30 Mb;
- all elements of the stamp should be clearly visible;
- a stamp should have a solid frame around its perimeter;
- a ***triangular*** stamp should face downwards, its base should be horizontal.

For the stamp to be detected in intercepted data, it must be included in a protected object.

User's target actions:

- Creating stamps and their catalogs (see "Managing Stamps")
- Adding stamps to protected objects (see "Creating a Protected Object")
- Importing and exporting stamps as a part of the technologies base (see "Exporting and Importing the Technologies Database")

3.4.6 Database Unloadings

Reference information:
Database unloading is a part of database. Citations from the unloading are searched for in analyzed text. Database unloadings can be lists of salaries, personal data, etc.

Warning!

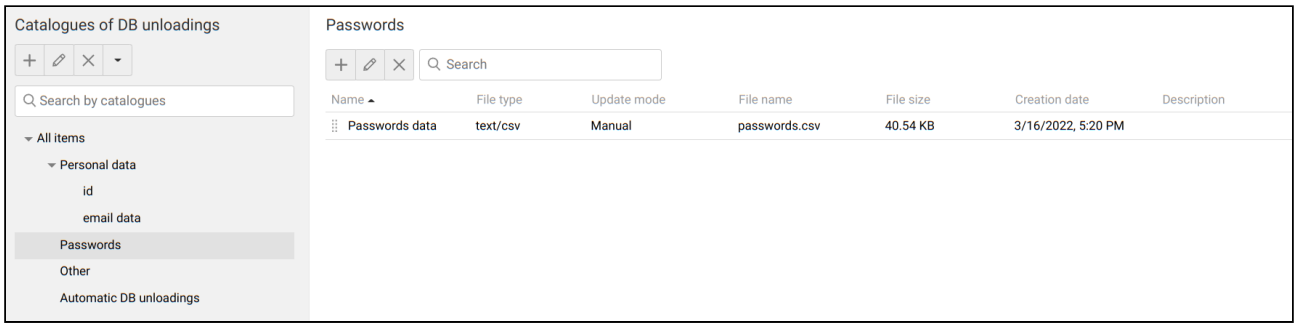
For correct operation in the System, the database unloading should have the following characteristics:

- file format - CSV or TSV;
- file size - from 128 bytes to 300 MB;
- number of columns is no more than 32;
- number of words in one cell is no more than 256;

- number of rows is no more than 1 million (for 8 GB RAM server) or no more than 3.5 million (for 16 GB RAM server);
- number of characters in the heading of table (1st row) - no more than 4000, including titles of columns and additional characters used by CSV and TSV for column spacing: quotation marks, commas.

Unloadings are created within catalogues. For operations with unloading catalogues (create, edit, move or delete a catalogue; search by catalogues), tools on the left side of the working area are used. DB unloadings of a selected catalogue and tools for operations with unloadings are located on the right side of the working area.

List of unloadings within the selected catalogue and tools for operations with unloadings (create, edit, delete, move or copy an unloading; perform a cross-cutting search through the catalogues) are located on the right side of the working area. The cross-cutting search is performed in accordance with the name of unloading and it is performed within the selected catalogue or enclosed ones. To perform the search through all the section's catalogues, select the root catalogue.



The preinstalled catalogue **Automatic DB unloadings** contains unloadings received from external systems (for further details, see "Automatically Updated Database Unloadings").

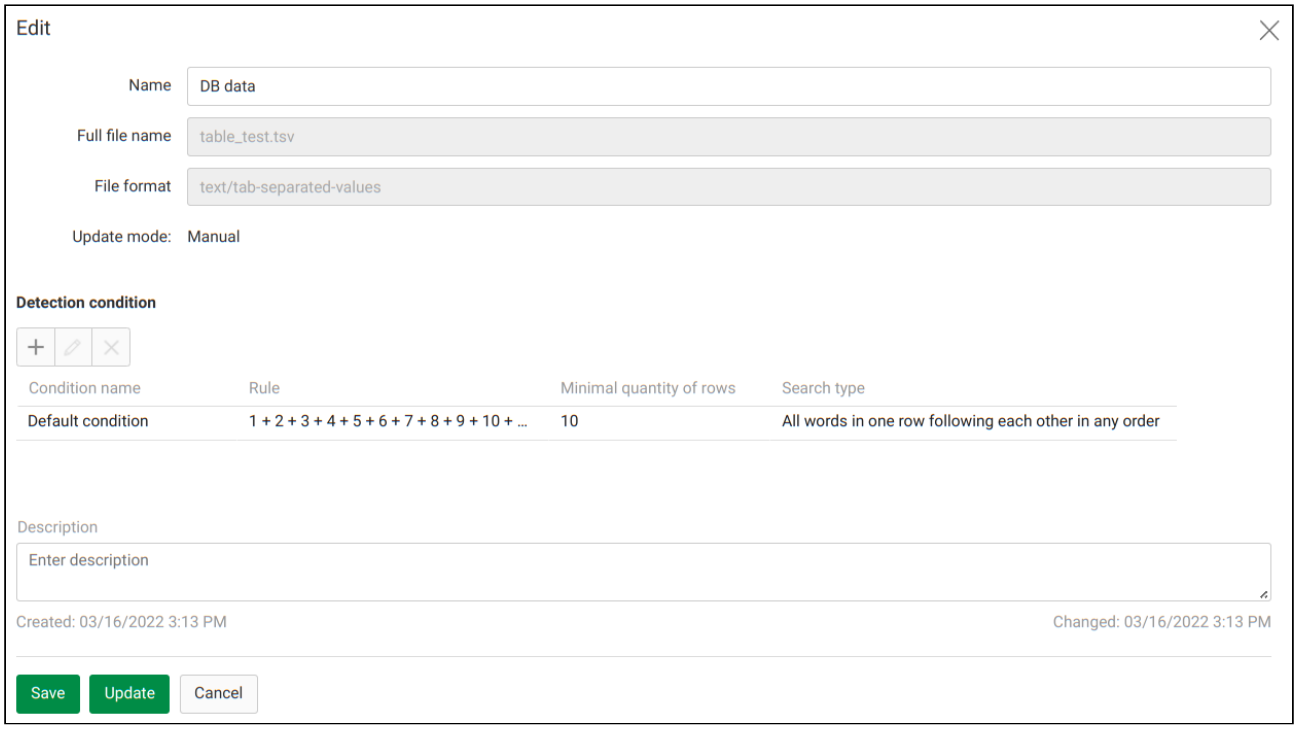
Note:

The **Automatic DB unloadings** catalogue is a system catalogue and it cannot be deleted.

In the edit mode, the detection conditions for the unloading are displayed. Detection conditions define:

- logical relationships between table columns;
- the minimum number of rows detected that is required for triggering the unloading;
- citation search type.

To switch to the update mode of the unloading, click **Update**.



For the unloading to be detected in intercepted data, it must be included in a protected object.

Obsolete unloadings:
Obsolete unloading is an unloading created in Traffic Monitor with a version lower than 7.4. Obsolete unloadings can be added to the System:

- if you import base of technologies/protected objects from Traffic Monitor with a version lower than 7.4;
- if you update Traffic Monitor from a version lower than 7.4.

Obsolete unloadings are marked with .

Warning!

An obsolete unloading cannot be edited and updated. It is recommended to delete it and create the unloading again.

User's target actions:

- Creating database unloadings and their catalogues (see "Managing DB Unloadings")
- Updating the unloading (see "Managing DB Unloadings")
- Moving/copying the unloading (see "Managing DB Unloadings")
- Adding detection conditions for the unloading (see "Detection Conditions for Unloading")
- Automatic update of the unloading (see "Automatically Updated Database Unloadings")
- Add DB unloadings to protected objects (see "Creating a Protected Object")

Automatically Updated Database Unloadings

Automatically updated DB unloadings are unloadings created by an external system. An external system (a connector) initiates adding and subsequent updating automatic unloadings.

Warning!

Simultaneous editing configuration via the Management Console and SDK can cause conflict, so a connector developer should be familiar with the general principles of configuring the System . if a conflict arises, you should first view error messages sent by SDK to the connector.

Unloadings generated by an external system are placed in a preinstalled catalogue **Automatic DB unloadings**. External systems are authorized in Traffic Monitor by means of plugin (on plug-in installation, see the document “ *InfoWatch Traffic Monitor. Administration Guide* ").

Note:

You can view and edit the **Automatic DB unloadings** catalogue provided that you have a license for using this technology.

When an automatic unloading is created, attributes of the unloading are generated based on the data received from an external system:

Parameter	Description
Name	The name of the unloading in the System
Columns	A list of unloading columns. The default detection condition is generated based on the list (see "Detection Conditions for Unloading").
Note	Accompanying information

Note:

When you create an unloading, its file can be empty if:

- loading the contents ended with a force quit;
- connection was lost while loading the contents;
- validation of the contents failed.

When the System operation is restored, then, if the System contains an empty unloading, an external application can use this unloading and fill it with new contents without creating a new unloading.

Automatic unloading cannot be updated manually in Traffic Monitor console.

All unloadings in the catalogue can be edited or deleted. These operations are performed using buttons on the toolbar in the right part of the workspace.

Warning!

If an unloading created by an external system is deleted, automatic update of this unloading becomes unavailable.

Warning!

An obsolete automatic unloading cannot be edited and updated. It is recommended to delete it and create the unloading again.

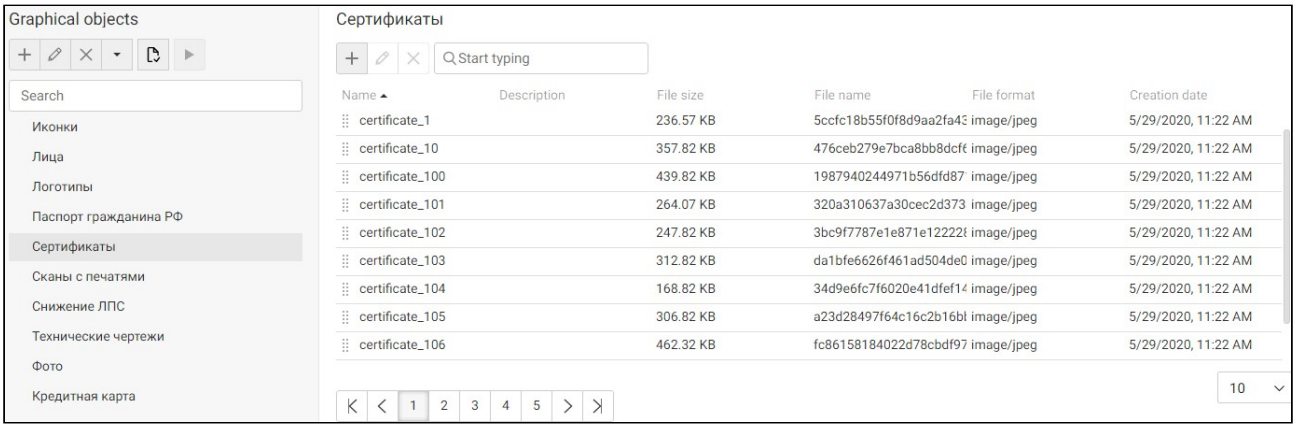
For automatic unloading to be detected in intercepted data, it must be included in a protected object .

3.4.7 Graphical Objects

Reference information:

Graphical objects are a technology for analyzing images or other graphic data extracted from the object body or its attachments.

Graphical objects consist of categories which contain documents. To work with categories (creating, editing, deleting categories, search by categories), tools in the left part of the working area are used.
In the right part of the working area, you can see the list of documents within the selected category of graphical objects and tools for working with documents: creating, editing, deleting categories, verifying, learning, pass-through search by the document name in the selected category only.



Depending on the license type, the System may contain the following predefined graphical objects:

- Passport of a citizen of the Russian Federation
- Technical drawings
- Geographic maps
- Certificates
- Faces
- Photos
- Scans with stamps
- Icons
- Logos

- Decreasing false-positives and uneditable graphical objects:

Name	Description
Credit card	Front side image of a VISA, Visa Electron, MasterCard, Maestro or Mir credit card.
Identification card of a citizen of Malaysia	A group of identification documents of the citizens of Malaysia including: • `MyKad` – a general card for citizens of Malaysia over 12 years old (front side) • `MyKid` – a card for children under 12 (front side) • `MyPR` – a card for residents of Malaysia who received a residence permit (front side) • `MyTentera` – a card for those who serve in the army (front side)

If necessary, you can expand the set of graphical objects by learning Automatic classifier to detect other image types: passport of a citizen of the Russian Federation, certificates, images of faces, photos, technical drawings, maps, scanned images of stamps, icons, logos, decreasing false-positives and create your graphical objects. The preset collection of graphical objects will be learned automatically when you install a valid license for the technology.

For graphic objects to be detected in intercepted data, they must be included in protected objects. For this, create a protected object using graphical objects (see "Creating a Protected Object").

User's target actions:

- Creating categories ("Managing Graphical Objects")
- Adding documents ("Managing Graphical Objects")
- Learing a classifier ("Managing Graphical Objects")
- Checking files with a classifier ("Managing Graphical Objects")
- Importing and exporting protected objects as a part of the base of technologies ("Exporting and Importing the Base of Technologies")
- Adding graphical objects to a protected object (see "Creating a Protected Object").

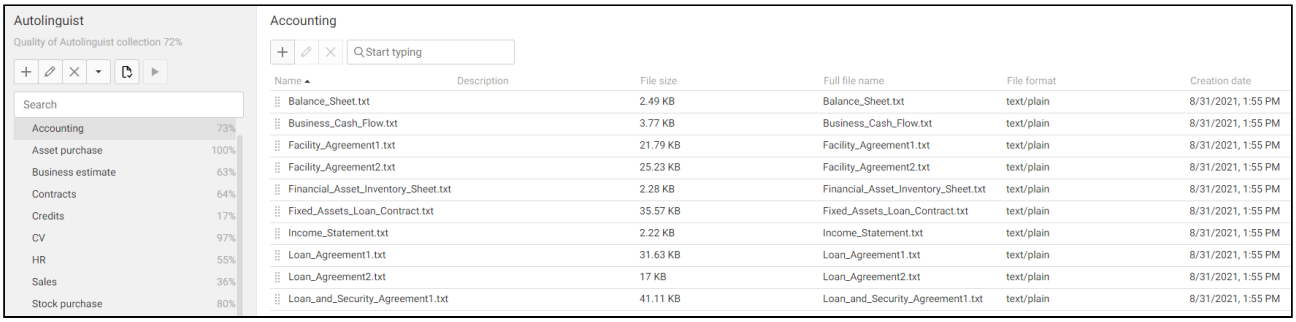
3.4.8 Autolinguist

General information:

Autolinguist – is a technology created to analyze text data. If you need to ptotect a big volume of standard company documents, this technology allows to automatically classify the documents in order to succesfully detect classified documents in outcoming traffic. All standard documents are grouped by categories which can relate to company departments: NDA, tender documents and others. Text documents loaded to Autolinguist are used to create protected objects.

Use the tools located in the left part of the working area to create, edit, remove categories and also search through them. Documents are created in the categories of Autolinguist.

In the right part of the working area you can see the list of documents created inside a selected category and also the tools to work with the documents (add, edit, remove, search through them). You can search through the documents by their name (only inside the selected category).



User can:

- Create categories (see "Managing Autolinguist");
- Add documents (see "Managing Autolinguist");
- Learn classifier (see "Managing Autolinguist");
- Check files using classifier (see "Managing Autolinguist");
- Import and export text objects which contain in the base of technologies (see "Exporting and Importing the Base of Technologies");
- Add text objects to protected objects (see "Creating a Protected Object").

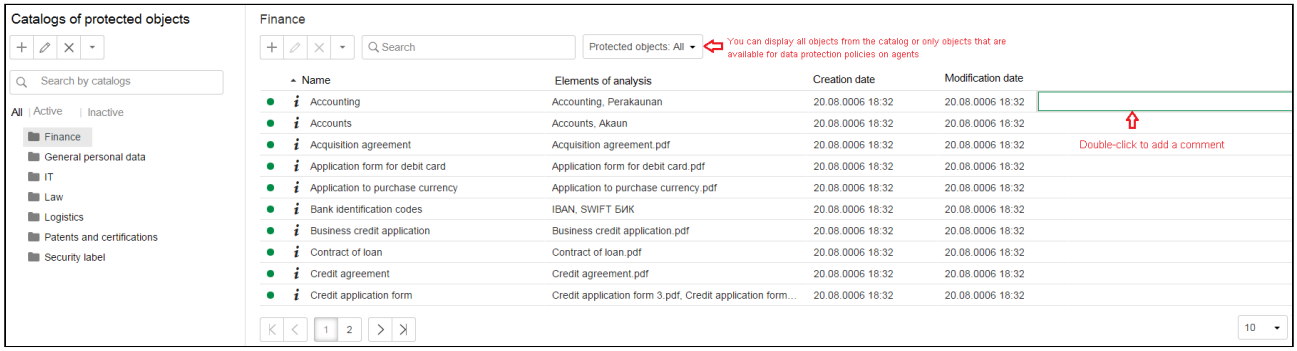
3.5 Protected Objects Section

Reference information:

The ***protected object*** is a set of elements of technologies. Protected objects are used to determine whether the intercepted data correspond to specific business documents.

About the section:

The section contains a list of events (interception objects) and tools for managing them.



The catalog list includes both custom and preset protected objects and it is located on the left side of the working area.

For each catalogue, its status is displayed (*Active* or *Inactive*). The catalogue status applies to all nested catalogs and protected objects.

In the right part of the workspace, protected objects for the selected catalogue are displayed as well as tools for operations with it, incluidng the cross-cutting search within catalogues.

A cross-cutting search is performed in accordance with the name of protected object and the name of technologies elements which are a part of protected object. Search is performed within selected catalogue and the enclosed ones. To perform the cross-cutting search through all the section'scatalogues, select the root catalogue.

You can switch to all protected objects to be displayed in the catalogue orto display only protected objects, available for data protection policy on agents.

For each protected object, the following attributes are displayed: status (*Active* or *Inactive*), name, elements of technologies included in the protected object, creation and modification dates, description.

> **Note:**
>
> If a protected object is selected as a result of end-to-end catalogue search, its status cannot be changed.

When you create a new protected object, a window for adding elements of technologies is displayed where you can choose elements or catalogues that will form the protected object (for more information on technologies used in the System, see "Defining the Confidential Information").

> **Note:**
>
> If the **Create a protected object for each selected element** is selected, then for each element of technologies, a separate protected object will be created. Attributes of the protected object will be set by the System.

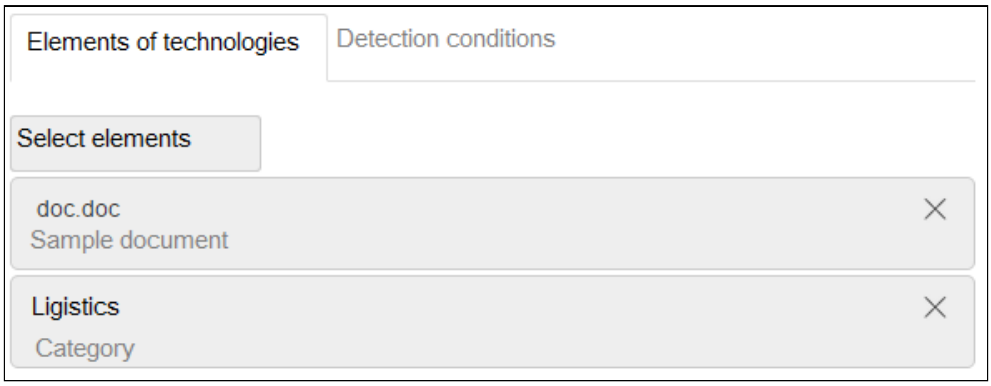
In the edit mode of the protected object, you can change the list of elements of technologies and specify detection conditions.

User's target actions:

- Creating a Catalogue of Protected Objects
- Creating a Protected Object
- Adding Elements of Technologies
- Creating Policies for Protected Objects and Their Catalogues
- Importing and Exporting Protected Objects

3.5.1 Elements of Technologies

Reference information:
Elements of technologies are elements or catalogues that are used when creating protected objects. They can be text objects, sample documents, etc.



Elements of technologies tab for a protected object

The **Elements of technologies** tab appears when creating a protected object, once the desired elements or catalogues are selected in the adding elements of technologies window or switching to edit mode of a previously created protected object.

On the **Elements of technologies** tab, you can add more elements of technologies or catalogues to a protected object (the **Select elements** button) or delete them (the X button in the upper right corner of the element panel).

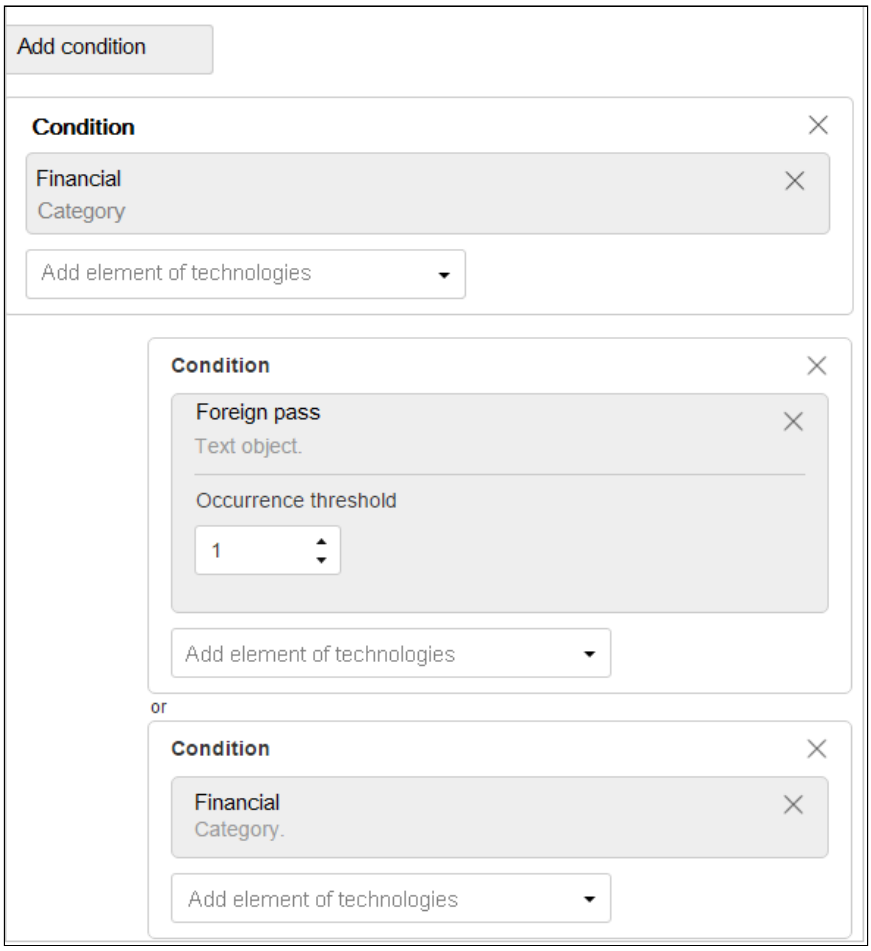
You can specify detection conditions for added elements of technologies on the **Detection conditions** tab.

User's target actions:

- Adding elements of technologies

3.5.2 Detection Conditions

The **Detection Conditions** tab is displayed when creating or editing a protected object.



You can specify detection conditions when creating a protected object after the desired elements are selected in the window of adding elements of technologies or when switching to the edit mode of a previously created protected object.

Detection conditions can be added within a single block and combined using the operation of conjunction (logical AND) or added to different blocks which are combined with the operation of disjunction (logical OR).

The catalogue will be detected if any element which belongs to the catalogue is being detected.

For each condition you can enable detection within event element. In this case, to detect protected object, all the elements of technologies specified in the condition should be detected in one element of event.
Event element is a detected in traffic:

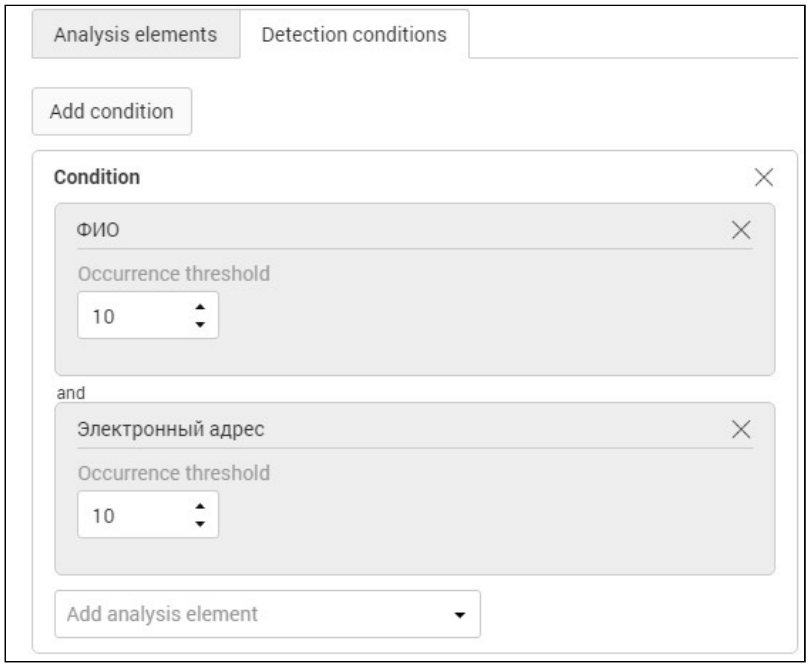
- email text
- email subject
- communication in messenger. All messages in an event are considered one element
- file
- file name

You can enable negation for an element of technologies so if it is detected, the System does not detect protected object.

> **Note:**
>
> At least one element without negation is required in the detection condition.
>
> If protected object is added to the policy of data protection on agents, you cannot enable negation and detection within event element.

Detection conditions for the elements of technologies are as follows:

Element name	Detection condition
Sample document	Checks whether the interception object contains a specified sample document
Category	Checks whether the interception object matches the specified categories. For categories that contain sub-categories, checks if the interception object matches any subcategory
Text object	Checks whether the interception object contains a specified text object. Additional detection condition is a occurrence threshold. It determines the least number of times the text object must be present in the interception object. The default value is 1. The maximum value is 20000. Depending on the pattern type, the number of occurrences of the text object is calculated as follows: • if the text object pattern is specified as a regular expression, then one pattern value is counted as one occurrence even if it is detected several times within a document • if the text object pattern is specified as a string, all its occurrences are counted. Catalogue also has a quotation threshold defined. Text objects which are a part of this parameter will be detected in accordance with its detection condition.
Blank	Checks whether the interception object contains at least one of the specified blanks. Additional detection condition - blank detection condition. It is used when editing the blank and includes the following:

Element name	Detection condition
	• text data quotation threshold - per cent of matching between intercepted blank and sample one. The default condition value is 70%; • minimum number of filled fields. The default condition value is 3. To be detected the intercepted blank should meet **both** conditions above. Always specify one detection condition. In case the technology element is a catalogue of blanks, one of the following conditions should be selected: • **Default condition** - the blanks inside the catalogue will have its default conditions applied; • **All conditions from catalogue as per OR** - for each blank within the catalogue any detection condition from it will be applied. 
Stamp	Checks whether the interception object contains a specified stamp
Graphical object	Checks whether the interception object contains a specified graphical object. Additional detection condition is a occurrence threshold. It determines the least number of times the gpaphical object must be present in the interception object. The default value is 1. The maximum value is 20000. The detection condition is specified for the entire category.

Element name	Detection condition
	Note: Occurrence threshold can not be specified for the following predefined graphical objects: • Credit card; • Identification card of a citizen of Malaysia.
Database unloading	Checks whether the interception object contains a specified unloading. Additional condition is unloading detection. It is created during editing of unloading. At least one detection condition should be selected always. In case you've selected DB unloadings catalogue, you should select one as follows: **Default condition** - for blanks within the catalogue its default conditions will be applied. **All conditions from catalogue as per OR** - for each unloading within the catalogue any its condition will be applied.

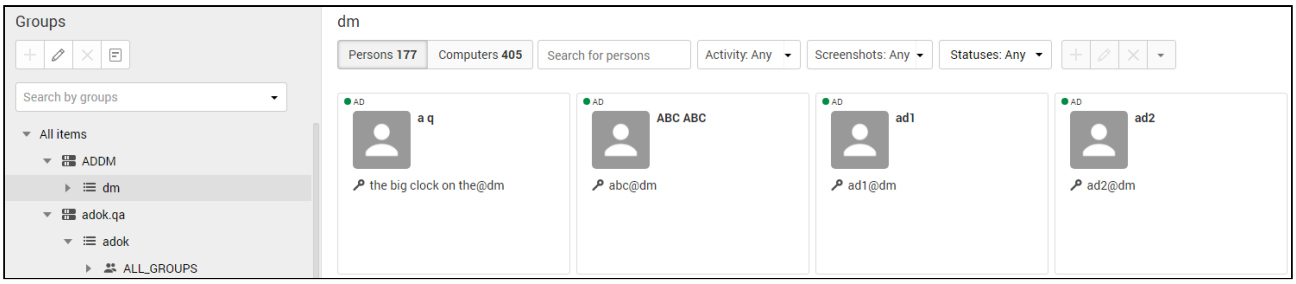
See also: Elements of technologies

User's target actions:

- Adding detection conditions

3.6 Persons Section

About the section:
The section contains a catalogue of persons and computers of the company information system.



In the left part of the workspace, groups of persons and computers are displayed.

You can add groups of persons and computers from Active Directory, Samba DC, Domino Directory, Astra Linux Directory, Astra Linux Directory Pro and FreeIPA or create them in Traffic Monitor (see "Creating Group of Persons or Computers").

Note:

For groups synchronized with LDAP, special icons are displayed:

 – for groups synchronized with Active Directory

 – for groups synchronized with Domino Directory

 – for groups synchronized with Astra Linux Directory, Astra Linux Directory Pro or FreeIPA

 – for groups synchronized with Samba DC

Using tools in the left part of the workspace you can create, edit or delete an earlier created user group.

The button  allows you to create a policy for the selected group (for details, see "Creating Person Control Policy").

You can also export or import groups, persons and computers (for details, see "Exporting and Importing Persons").

When you select a group in the list, the right part of the workspace displays persons and computers of this group. To view the list of persons and computers, use **Persons** and **Computers** tabs respectively.

To search for desired persons or computers use thy fields **Search by persons** and **Search by computers**. To switch to another field you should switch the tabs **Persons** or **Computers**. A cross-cutting search is performed in accordance with the name and surname of selected person, computer name and contatcs details and it is performed within selected catalogue or enclosed ones. To perform the search through all the section's categories, select the root catalogue. Mask search is supported (e.g., `*name`).

Important!

Using * in a search query may negatively affect the search speed in case of a large number of persons loaded from Active Directory, Samba DC, Domino Directory, Astra Linux Directory, Astra Linux Directory Pro and FreeIPA.

When searching for required persons and computers, you can use the following filters:

- selecting active/inactive persons and computers (obtained from LDAP);
- filtering by the presence of screenshots;
- choosing persons and computers with a specific status (for details, see "Statuses").

The toolbar in the left part of the workspace is used for working with groups, while the toolbar in the right part of the workspace allows you to work with persons and computers within a selected group.

User's target actions:

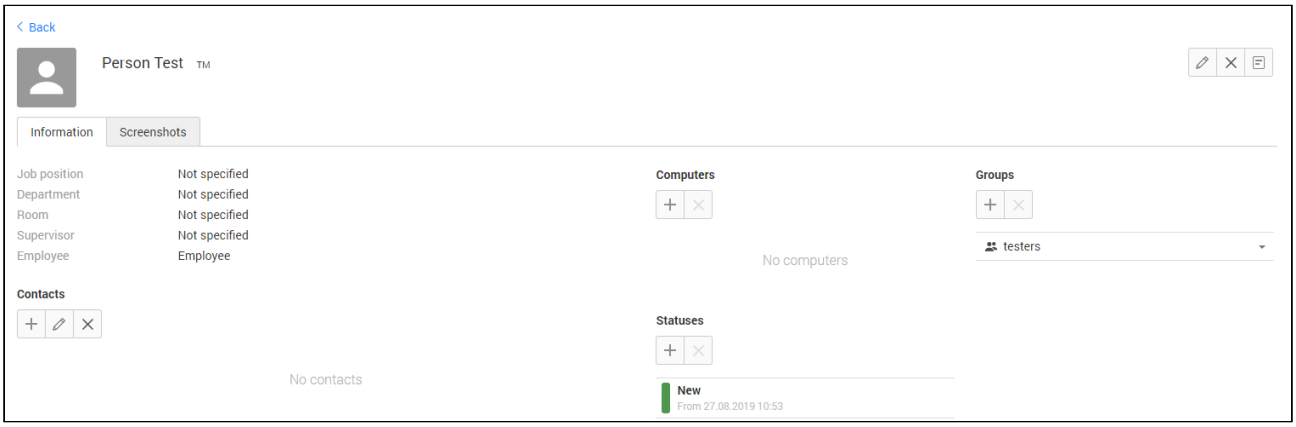
- Creating a group of persons and computers (see “Creating Group of Persons and Computers")
- Creating a list of persons and computers (see “Creating List of Persons and Computers")
- Exporting and importing persons ("Exporting and Importing Persons")
- Viewing widgets with information on persons and computers (see "Viewing Summary on Person or Computer")
- Creating a filter by persons and computers (see "Creating Queries")
- Creating a policy for persons and computers (see "Adding Person or Computer to Policy")
- Managing statuses of persons and computers (see "Adding Status to Person or Computer")
- Viewing screenshots for persons and computers (see "Viewing Screenshots")
- Adding persons in perimeters (see "Adding a Person to Company Perimeter")

3.6.1 Persons

The list of persons included in the selected group is displayed on the **Persons** tab in the right part of the workspace.

> **Note:**
>
> For persons whose data is imported from Active Directory, Samba DC, Astra Linux Directory, Astra Linux Directory Pro and FreeIPA, the colour indicator appears in the upper left corner of the profile photo:
> - for active employees, including employees whose accounts in AD/Samba DC/ALD/ALD Pro/ FreeIPA have expired;
> - for employees disabled in AD/Samba DC/ALD/ALD Pro/FreeIPA.

To view the person card, double-click the selected person. The person card contains two tabs: **Information** and **Screenshots**.



The **Information** tab contains the following attribute of the person:

- Job position
- Department
- Room
- Supervisor
- Employee
- Contacts (you can specify personal or working contacts of the person including email, phone number, Skype login, ICQ or web address on the Internet, social networks and messengers account)

- Computers (computers linked with the person account)
- Statuses (statuses assigned to the person)
- Groups (groups which include the person)

To change these attributes, as well as **Name**, **Last name**, **Member of company** attributes or to edit the person's photo, use button in the right part of the workspace.

On the **Screenshots** tab, you can view screenshots included in events for this person (see "Screenshots").

To return to the list of persons, click **< Back**.

The button allows you to switch to the "Policies" section to create a policy for the selected person.

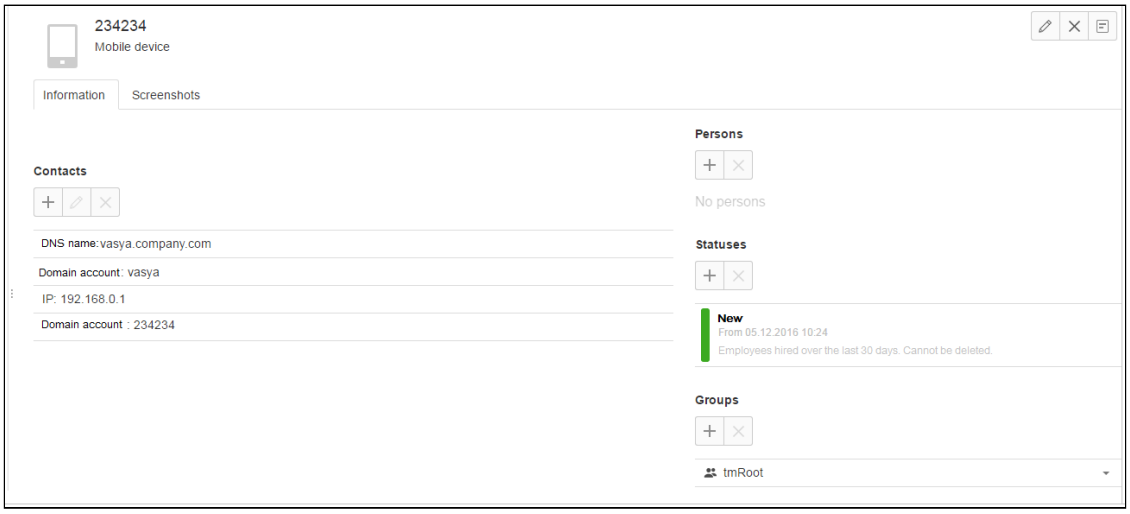
User's target actions:

- Creating a filter by persons (see "Creating Queries")
- Configuring a person card (see "Configuring Person Card")
- Creating a policy for persons (see "Adding Person or Computer to Policy")
- Managing statuses of the person (see "Adding Status to Person or Computer")
- Added a person to a perimeter (see "Adding Person to Company Perimeter")
- Viewing screenshots for a person (see "Viewing Screenshots")

3.6.2 Computers

The list of computers included in the selected group is displayed on the **Computers** tab in the right part of the workspace.

To view the computer card, double-click the selected computer. The computer card contains the two tabs: **Information** and **Screenshots**.



The **Information** tab contains the following attributes:

- OS (operating system installed);
- Update package (update package installed);
- Version (update package version);
- Contacts (you can specify DNS name, IP address and domain account);
- Persons (persons to whose accounts the computer is linked);
- Statuses (statuses assigned to the computer);
- Groups (groups which include the computer).

To change these attributes or the computer name or type, use button in the right part of the workspace.

On the **Screenshots** tab, you can view screenshots included in events for this computer (see "Screenshots").

To return to the list of computers, click **< Back**.

The button allows you to switch to the "Policies" section to create a policy for the selected computer.

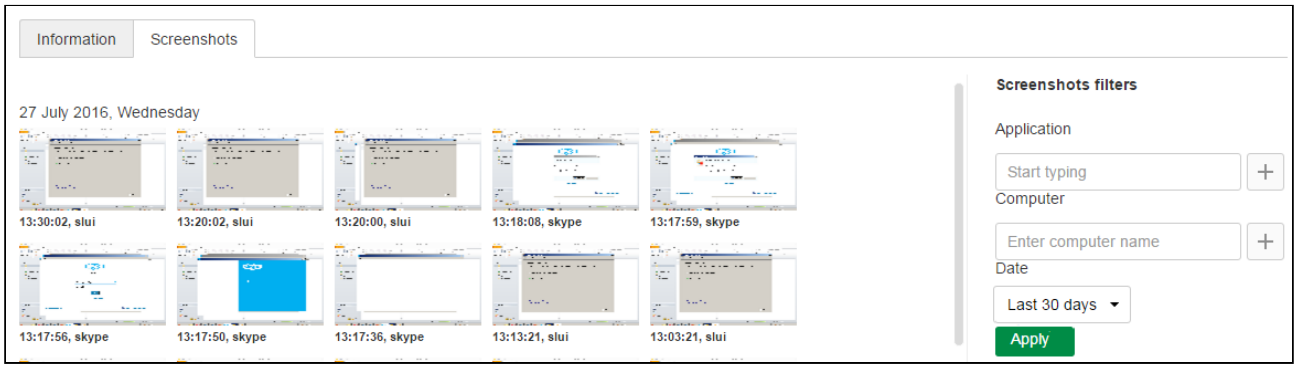
User's target actions:

- Managing groups of computers (see "Creating Group of Persons and Computers")
- Managing computers (see "Creating List of Persons and Computers")
- Creating a policy for computers (see "Adding Person or Computer to Policy")
- Managing computer statuses (see "Adding a Status to Person or Computer")
- Viewing screenshots for a computer (see "Viewing Screenshots")

3.6.3 Screenshots

Cards of persons (see "Persons") and computers (see "Computers") contain **Screenshots** tab, where you can view information about screenshots for a selected person or computer.

You can also go to screenshots from "Events" section when you view information about a person or computer in the brief event viewing form (see "Viewing Brief Event Form").



By default, screenshots for all dates and for all applications are displayed. Screenshots are sorted by date.

The **Application**, **Computer**/**Person** and **Date** filters allow you to search screenshots by specified conditions.

Clicking a screenshot opens its enlarged image and attributes:

- **Person** - a person who made the screenshot;
- **Computer** - a computer where the screenshot was made;
- **Time** - date and time when the screenshot was made;
- **Application** - the application that was active when the screenshot was made.

You can use tools in the right part of the workspace to change the image scale (**+** and **-** buttons) or save the image to your computer (button).

To navigate to the next or the previous image, use **<** and **>** buttons. You can also find the desired screenshot in the list which is located in the lower part of the workspace. To quickly move between elements of the list, hover over the list, hold down the left mouse button and scroll through the list in the desired direction.

To close the viewer and continue working with the selected person or computer, click **X**.

User's target actions:

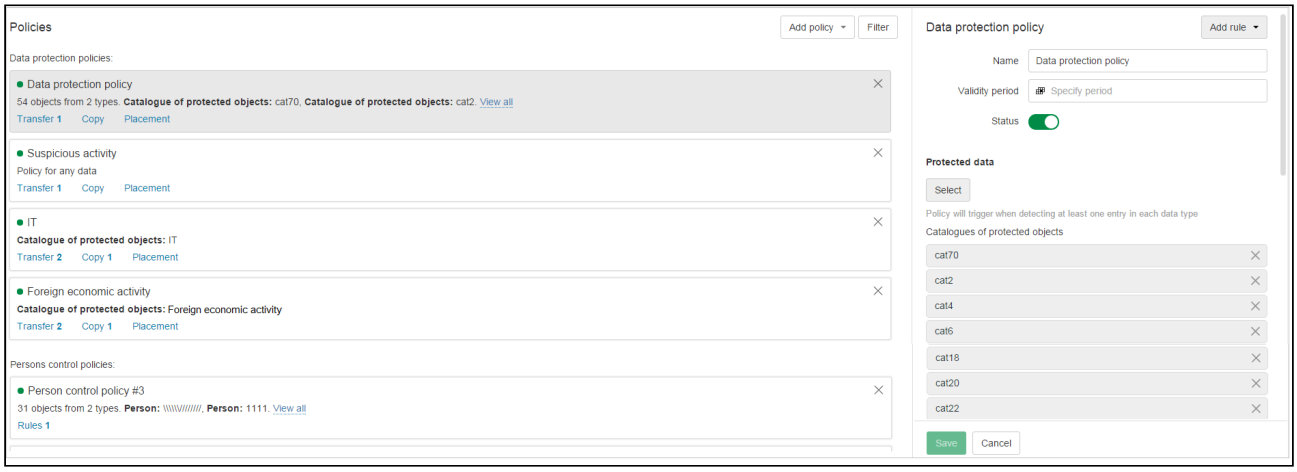
- Viewing Screenshots

3.7 Policies Section

Reference information:
Policies are a set of rules according to which analysis and processing of interception objects are performed. The ***rule*** consists of condition sets by which the object is checked and the actions performed when those conditions are fulfilled or not.

> **Warning!**
>
> As a result of the analysis, the System will not perform any actions if at least one of the following conditions is met:
>
> - the System has no policies;
> - all policies existing in the System are disabled;
> - none of the policies in the System have active rules (or the default actions for active policies are not defined).

About the section:
The section contains the list of policies and tools for working with them.



Policies in the list are grouped by type: data protection policies, data protection policies on agents, and person control policies.

When you choose a policy, the policy viewing form is displayed in the right part of the workspace. In this form, you can edit the policy attributes. When you add a rule for the policy, the rule viewing form is displayed in the right part of the workspace.

To add a new policy, use the + button and, in the drop-down list, choose the policy type. A new policy is added to the list, and the policy viewing form is displayed in the right part of the workspace.

In the policy viewing form, you can:

- specify the policy attributes (name, validity period, status, description);
- choose protected data (for data protection policies). Protected data may include protected objects, their catalogs, and file formats;
- specify senders whose actions the policy will control (for person control policies). You can choose individual persons, a group of persons, or persons with a common status;
- add policy rules.

When you click the **Filter** button, in the right part of the workspace, the **Filter settings** area is displayed where you can filter policies by name or by objects of research.

User's target actions:

- Adding a new policy (see "Creating Data Protection Policy", "Creating Data Protection Policy on Agents", and "Creating Person Control Policy")
- Adding rules to the policy (see "Creating Rules")
- Filtering policies (see "Filtering List of Policies")

3.7.1 Rules and their Viewing Form

Information on the rules is displayed in the tile of the selected policy. Clicking the link with the rule type opens the list of added rules of this type.



When you select a rule in the list, a viewing form for a selected rule is displayed on the right side of the workspace.

In the upper-right corner of the tile, × icon is displayed. Clicking this icon removes the selected rule.

For each **data protection policy**, you can configure one or several rules:

- Rule of Transfer - regulates sending and receiving protected data.
- Rule of Copying - regulates copying and printing protected data;
- Clipboard rule - regulates clipboard usage and keyboard input;
- File Operations Rule - regulates if an application can read a file or write to it.

For each **data protection policy on agents**, you can configure one or several rules:

- Rule of Transfer
- Rule of Copying
- Application activity rule

When creating rules of transfer and rules of copying, in order to select LDAP domain as *Sender* or *Recipient* you should first configure synchronization with the LDAP server and add the domain using the **Groups** tab.

Also, for *Sender* and *Recipient*, you can specify the following parameters:

Parameter	Description
Contacts	Specify contacts of the traffic senders/recipients. For this, in the first drop-down list on the left, select the contact type:  - ICQ account. Integer number from 10000 to 999999999999;  - Skype account. String from 6 to 32 characters long, must begin with a letter; may contain only letters, digits, and the characters ".", ",", "-", "_";  - Azure AD contact (if the adapter is installed), string of 1 or more characters;  - mobile phone number. String no less than three characters, can contain only numbers, space and symbols"-","_", "( )","+",".");  - landline phone number.String of 3 or more characters,can contain only digits, space, and the characters:"-","_", "( )","+",".");  - E-mail address. Address (in RFC format);  - Telegram account (string of 1 or more characters);  - Facebook account (string of 1 or more characters);  - WhatsApp account (string no less than one character)  - Lotus e-mail address. String of 3 or more characters when entering data in the input field, or string of 1 or more characters when entering data in the **Senders** window (opens when clicking the  button) ;  - identifier on a web resource. A string of 3 or more characters when entering data in the input field, or string of 1 or more characters when entering data in the **Senders** window (opens when clicking the  button) .
Groups	Specify groups whose members can be traffic senders/recipients.
Persons	Specify persons who can be traffic senders/recipients.
Domains	Specify domains whose members can be traffic senders/recipients.
Perimeters	Specify perimeters whose elements can be traffic senders/recipients.

Person control rules regulate actions of selected persons. They also allow you to apply existing data protection policies and data protection policies on agents to selected persons.

User's target actions:

- Adding rules to the policy (see "Creating Rules")

Rule of Transfer

For the transfer rule, the following parameters are specified:

- **Direction of route**. Possible values:
  - **In single direction** - the rule is triggered only when traffic is passed from senders to recipients;
  - **In both directions** - the rule is triggered when traffic is passed both from senders to recipients and from recipients to senders.
- **Event type** - the type of traffic passing which triggers the rule. Possible values:
  - **Internet activity**
    - Web message
  - **Messenger** (for data protection policies only)
    - ICQ
    - MS Lync
    - Skype
    - Telegram
    - MS Teams (if the adapter is installed)
    - XMPP
    - Facebook
    - WhatsApp
    - Vkontakte
    - Kribrum
  - **Mail**
    - Mail on Client
    - Mail in Browser
- **Computers** - computers from which data has been sent.
- **Senders** - if persons or computers from this list send traffic (or traffic leaves specified domains and perimeters), it triggers the rule;
- **Recipients** - if persons, computers, domains or perimeters from this list receive traffic, it triggers the rule;

> **Note:**
>
> If you select a protected object based on a graphical object as policy protected data and specify the **Mail in Browser** event type, then the policy can be triggered only if no persons are specified in the **Recipients** field. This restriction is due to the fact that for webmail events, a recipient of enclosures is not an email, but a domain. For example, if a message with enclosures is sent to the `user1@example.com` email address, the enclosure recipient will be the `example.com` domain. Thus, if particular persons are specified as recipients, events with enclosed graphical objects will not be covered by the policy.

- **Rule validity days**;
- **Rule validity time**.

> **Important!**
>
> Selected conditions are joined by logical "AND". Within the same condition, values are joined in the following way:

- by logical "OR" if equality to the attribute is selected;
- by logical "AND" if negation is applied to the attribute.

In the **Actions when the rule is triggered** area, specify the required actions (for details, see "Determining the System Response to Rule Violations").

User's target actions:

- Creating Rule
- Configuring Notifications in Rules

Rule of Copying

For the copy rule, the following parameters are specified:

- **Route direction**. Possible values:
  - **One way direction** - the rule is triggered when traffic is sent from sender to recipient;
  - **Both ways direction** - the rule is activated when traffic is sent from sender to recipient and from recipient to sender.
- **Event type** - the type of traffic copying which triggers the rule. Possible values:
  - **Files exchange**
    - Removable device
    - FTP
    - Cloud storage
    - Network resource
    - Terminal session
  - **Printer and MFD** (for data protection policies only)
    - Print
- **Computers**;

> **Note:**
>
> If you specify a domain, the rule will apply to its subdomains as well. For example, if you add the `domain.com` domain, the rule will apply to the `subdomain.domain.com` domain as well.

- **Senders** - the list of persons and computers, domains, perimeters, and resources. Sending traffic by this kind of senders triggers the rule;
- **Copy receiver**;

> **Warning!**
>
> The type of the **Path to file or address** attribute value for the "Terminal session" copy receiver depends on the Traffic Monitor version. The attribute value types are different in the events of file exchange via terminal session:
>
> - **For events created in Traffic Monitor version below 7.5**: the attribute contains the name of the copied file, for example: `file.txt`

- **For events created in Traffic Monitor version 7.5 and above**: the attribute contains the IP address of the device that was used to remotely connect to the employee's workstation and to which the file was copied, for example: `192.0.2.0`

To ensure that policies work correctly for the events created in Traffic Monitor version 7.5 and above, it is recommended to edit existing copy rules in policies. Existing copy rules must be edited if they use an obsolete type of the **Path to file or address** attribute value for "Terminal session" copy receiver. If a file name is specified in this attribute in the rule, the rule will not work correctly with the new events, because new events have an IP address in this attribute.

- **Copy source**;

> **Note:**
>
> Depending on the selected type of the copy source/receiver, there can be different recommendations on how to fill in the **Path to file or address** field (see "Recommendations on how to fill in the Path to file or Address field").

- **Rule validity days**;
- **Rule validity time**.
- **Terminal name** – the name of the device that was used to remotely connect to the employee's workstation. The attribute is specified for the "Terminal session" copy receiver in the events of file exchange via terminal session.

> **Note:**
>
> **Terminal name** is a user attribute of the default InfoWatch Device Monitor plugin. The attribute can be used only in the rules of data protection policies. The attribute is not available in the rules of data protection policies on agents.

> **Important!**
>
> Selected conditions are joined by the "logical AND" operation. With a condition, values are joined as follows:
>
> - by the "logical OR" operation if the equality parameter is selected;
> - by the "logical AND" if negation is applied to the attribute.

> **Important!**
>
> A policy where the copy source and receiver are specified may not work in some cases. For details, see KB article "Restrictions imposed on Data Protection Policy on Agents".

In the **Actions when the rule is triggered** area, specify the required actions (for details, see "Determining System Response to Policy Violations").

User's target actions:

- Creating Rules
- Configuring Notifications in Rules

Application activity rule

For the clipboard rule, the following parameters are specified:

- **Event type** - the type of traffic operating which triggers the rule. Possible values:
  - **Clipboard**;
  - **Keyboard input**.

> **Note:**
>
> For the Application activity rule added to data protection policy on agents:
>
> - only the type of event **Clipboard** is available
> - the option **Terminal session only** is always active
> - exclude computers option is not available.

- **Persons** - the list of persons, their groups, and perimeters. When traffic is sent by specified persons or groups or leaves specified perimeters, it triggers the rule.
- **Computers** - the list of computers. When traffic is sent from specified computers, it triggers the rule.
- **Applications** (for the **Keyboard input** event type only) - working in specified applications triggers the rule.
- **Terminal session only** (for the **Clipboard** event type only) - select this option if the receiver application is a terminal session. If the option is selected, choosing the receiver application manually is unavailable.
- **Source application** (for the **Clipboard** event type only) - copying data from specified applications triggers the rule. If **Terminal session only** parameter is enabled, the option is unavailable;
- **Receiver application** (for the **Clipboard** event type only) - pasting data from the clipboard to specified applications triggers the rule. If **Terminal session only** parameter is enabled, the option is unavailable.
- **Rule validity days**
- **Rule validity time**

> **Important!**
>
> Selected conditions are joined by logical "AND". Within a condition, values are joined as follows:
>
> by logical "OR" if the equality attribute is selected;
>
> by logical "AND" if negation is applied to the attribute.

In the **Actions when the rule is triggered** area, specify the required actions (for details, see "Determining System Response to Policy Violations").

User's target actions:

- Creating Rules
- Configuring Notifications in Rules

Person Control Rule

For the person control rule, the following parameters are specified

- **Violation level** - The System will intercept events with the specified violation level;
- **Connect with policy** - specify data protection policies and data protection policies on agents which trigger the rule when the policy itself is triggered (assuming that the violation level matches the value specified in the **Intercept with violation level** field).

In the **Actions when the rule is triggered** area, specify the required actions (for details, see "Determining System Response to Rule Violations").

User's target actions:

- Creating Rules
- Configuring Notifications in Rules

File Operations Rule

For a file operations rule, you need to specify the following parameters:

- **Event type** - actions with files that trigger the rule. Possible values:
  - **Writing to a file**
  - **Reading a file**
- **Persons** - if persons, groups, or perimeters from this list execute operations with files, it triggers the rule
- **Computers** - if operations with files are performed on computers from the list, it triggers the rule
- **Applications** - actions in applications from the list trigger the rule
- **Rule validity days**
- **Rule validity time**
- **Browser tab address** - address of the active browser tab. This is an additional attribute

Important!

Selected conditions are joined by logical "AND". Within the same condition, values are joined in the following way:

- by logical "OR" if equality to the attribute is selected;
- by logical "AND" if negation is applied to the attribute.

In the **Actions when the rule is triggered** area, specify the required actions (for details, see "Determining System Response to Policy Violations").

Important!

To enable operation of this rule, you should configure the **File Operations Monitor** rule in the Device Monitor Management Console (see "File Operations Monitor Rule" in *"InfoWatch Device Monitor. User Guide"*).

3.8 Lists Section

Reference information:
Lists are sets of similar data used for creating policies. They can be preinstalled or generated by means of the management console.

About the section:
Contains editable catalogues of tags, web resources, statuses, perimeters, and an uneditable list of files.

	Name	Description
●	Fired	Employees who have worked for the company before.
●	New	Employees hired over the last 30 days. Cannot be removed.
●	On probationary period	Employees on probationary period.
●	To fire	Employees who filed an application for dismissal.
●	Under supervision	Employees under close attention of Security Officers.

Lists section, the list of statuses

The section contains the following catalogues:

- Tags
- Statuses
- Perimeters
- Web resources
- File Types

User's target actions:

- Creating a list of tags (see "Managing Tags")
- Creating a list of resources (see "Managing Web Resources")
- Creating a list of statuses (see "Managing Statuses")
- Building perimeters (see "Managing Perimeters")
- Adding file formats to policy (see "Creating Data Protection Policy" and "Creating Data Protection Policy on Agents")

3.8.1 Tags

Reference information:
A ***tag*** is a mark which gives a brief characteristic of the intercepted object. For each tag, a special color marker is set.

There are the following preset tags in the System:

- **Under supervision** - events that indicate persons' suspicious activity
- **VIP** - events from persons who belong to the company authorities

User's target actions:

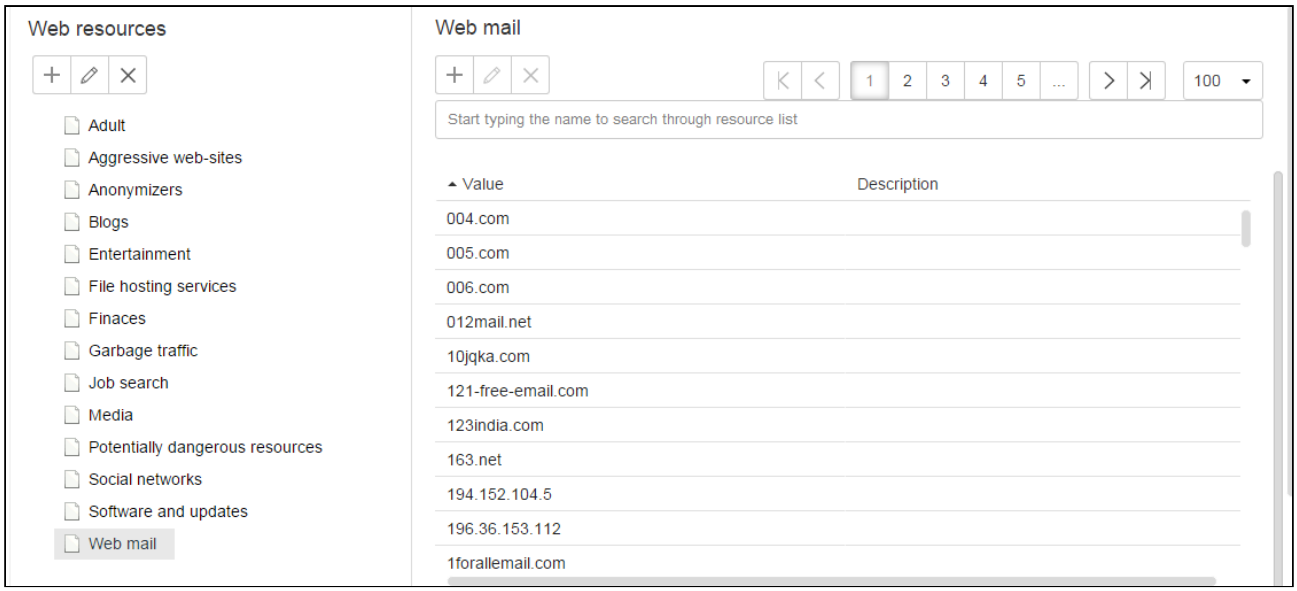
- Creating a list of tags (see "Managing Tags")

3.8.2 Web Resources

Reference information:
Web resources are a set of Internet resources, which are treated by the System as inappropriate use of working time.

Web resources are added to the lists. For operations with web resources lists (creating, editing or deleting the list) tools on the left side of the working area are used.

List of web resources and tools for operations with web resources (create, edit, delete and cross-cutting search within catalogues) are located on the right side of the working area. A cross-cutting search is performed in accordance with the value of web resource and it can be performed within selected list or all the lists of section. To perform the search through all the section's lists, select the root catalogue.



The System includes the following preset lists of web resources:

- Anonymizers
- Blogs
- Webmail
- Media
- Software and updates
- Job search
- Potentially dangerous resources
- Entertainment
- Aggressive web-sites
- Social networks
- Adult
- File hosting services
- Finance

User's target actions:

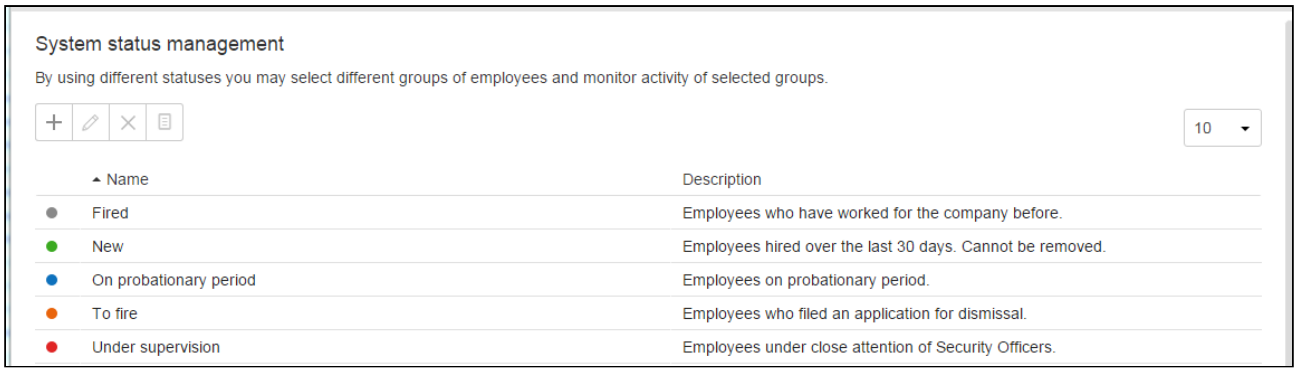
- Creating a list of resources (see "Managing Web Resources")

3.8.3 Statuses

Reference information:
The person ***status*** is a label which can be created in one of the following ways:

- automatically assigned to a person according to the status of a user or a computer imported from Active Directory, Samba DC, Domino Directory, Astra Linux Directory, FreeIPA and Astra Linux Directory Pro
- manually assigned to a person by the security officer
- automatically assigned to a sender when a rule is triggered

For each status, a colour mark is set.



The System includes the following preset statuses: *On probationary period*, *To fire*, *New*, *Under supervision*, and *Fired*.

> **Note:**
>
> The *New* status cannot be deleted.

User's target actions:

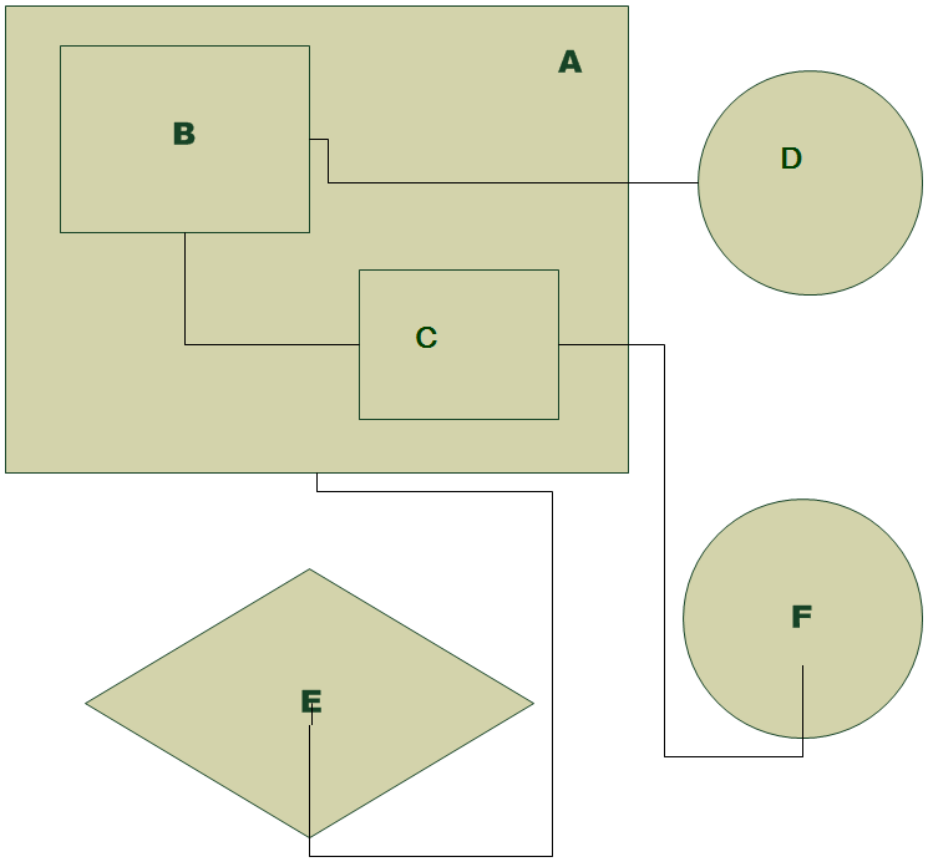
- Creating a list of statuses (see "Managing statuses")
- Manual assigning status to a person or workstation to monitor its activities or to visually distinguish them (see "Adding a Status to Person or Workstation")
- Automatic assigning status to a sender when the rule is triggered (see "Rules and their Viewing Form", **Set status** attribute)
- When creating a Person Control Policy - choosing persons and workstations with a specific status as objects of research (see "Creating Person Control Policy")

3.8.4 Perimeters

Reference information:
Perimeter is a container of company infrastructure elements (employees, workstations, domain and so on) and contact information. The perimeter is used to logically divide your organization into structural elements and track the traffic of each element.

For example:

- There is a company with infrastructure A which contains subdivisions B and C;
- The company interacts with organizations D, E, F.



By building perimeters for all named objects (A, B, C, D, E, F), the security officer can configure traffic control:

- inside the company (within the perimeter A)
- outside the company (between the perimeter A and one of the perimeters D, E or F)

Warning!

For more flexible work with structural elements, we recommend allocating smaller perimeters in larger ones (in this example - the perimeters B and C are parts of the perimeter A).

The System includes the following preset perimeters:

- ***Company*** - to control sending data out of the company;
- ***Exclude from interception*** - is used in the ***Excluding from Interception*** (see "Policy that Excludes Mailing Lists from Interception") preset policy.

Note:

When adding persons or groups to a perimeter, you can use the **Use only work contacts** option. An example of usage: if the option is selected, sending messages from employees' personal mailboxes is not treated as sending data out of the perimeter.

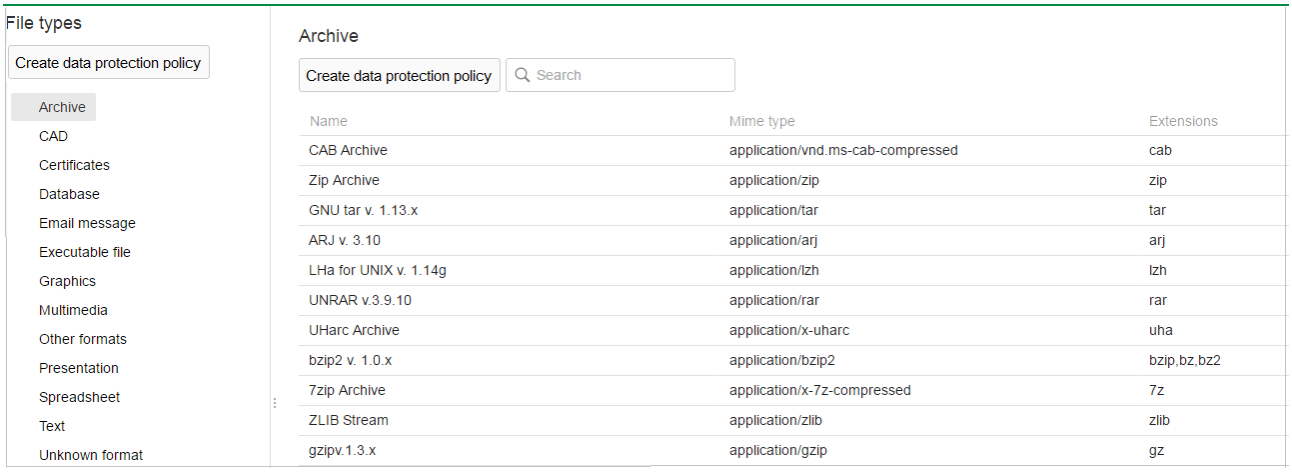
User's target actions:

- Building perimeters (see "Managing perimeters")

3.8.5 File Types

Reference information:

File types are a set of files that are detected in the System.



Files of different formats are divided into groups depending on the subject area. For example, the **Archive** type contains files in ZIP, RAR and other formats.

The tab contains the following elements:

Element	Purpose
The list of file types	Located in the left part of the workspace. Contains a set of subjects that use one or more file formats.
List of formats of the selected type	Located in the right part of the workspace. Contains a list of attributes for all files of the selected type that are detected in the System. This is a table with the following attributes: **Name**, **MIME type**, and **Extension**.
Create data protection policy button	A button for adding a new policy for the selected file type or format. Click the button and, in the drop-down list, select the required action: • Create data protection policy • Create policy on agent A policy creation form for the selected file format will open in the "Policies" section. **Note:** For formats, analysis of which is not supported in Device Monitor, **Create policy on agent** item is unavailable.

Element	Purpose
Cross-cutting search field	It is located on the right side of the working area. A cross-cutting search is performed in accordance with the name and extension of file. Search is performed within selected list of files and all section's lists. To perform the search through all the section's lists, select the root catalogue.

Warning!

The list of file types is defined by the System and cannot be modified.

User's target actions:

- Adding file types to policies (see "Creating Data Protection Policy" and "Creating Data Protection Policy on Agents")

3.9 Administration Section

The **Administration** section includes the following subsections:

- LDAP synchronization
- Licenses
- Users and roles
- System state
- Audit
- Integrity monitoring
- Services
- Plugins
- Mail server
- Mail notifications

On working in this section, see "Administrating the System".

4 Cases Solving in Traffic Monitor Management Console

Working in the management console, the Security Officer generally solves the following cases:

- Managing Persons and Workstations
- Managing Catalogs
- Working with the Base of Technologies
- Managing Protected Objects
- Managing Interception Objects
- Configuring System Response
- Managing Reports
- Administrating the System

> **Note:**
>
> Some operations in the Administration section are performed by the administrator.

Solving all cases you have to perform typical actions which are described in "Typical Actions".

On the interface elements of the Management Console sections, see:

- Dashboards Section
- Раздел "События"
- Reports Section
- Technologies Section
- Раздел "Объекты защиты"
- Persons Section
- Раздел "Политики"
- Раздел "Списки"
- Administration Section

4.1 Typical Actions

Why do you need typical actions?
To perform the same operations in the Management Console.

Typical actions include the following:

- Login to the Management Console
- Applying System configuration
- Editing Element
- Deleting Element
- Page Navigation
- Changing User Password
- Choosing Interface Language
- Calling Help
- Viewing System Information

4.1.1 Login to the Management Console

Purpose:

Log into the Management Console.

Solution:

To log into the Management Console:

1. Open the current version of Google Chrome or Mozilla Firefox internet browser (in case there is no specified browser installed, you may download it following the links below: Google Chrome or Mozilla Firefox).
2. Open the address provided by the system administrator. The browser window will display the Management Console start page.
3. In the **Login** field, specify the username.
4. In the **Password** field, specify the password.

   > **Note:**
   >
   > The username and the password can be obtained from the administrator of InfoWatch Traffic Monitor.

5. Click **Login**.

To log out of the Management Console:

1. Click the user menu button (see "Management Console Interface").
2. Select **Logout**.

4.1.2 Applying System Configuration

Reference information:
The System configuration includes the following sections of the Console:

- Technologies
- Protected objects
- Persons
- Policies
- Lists

When you finish editing elements of these sections, you need to apply changes: after this, the changes take effect and the System starts working according to them.

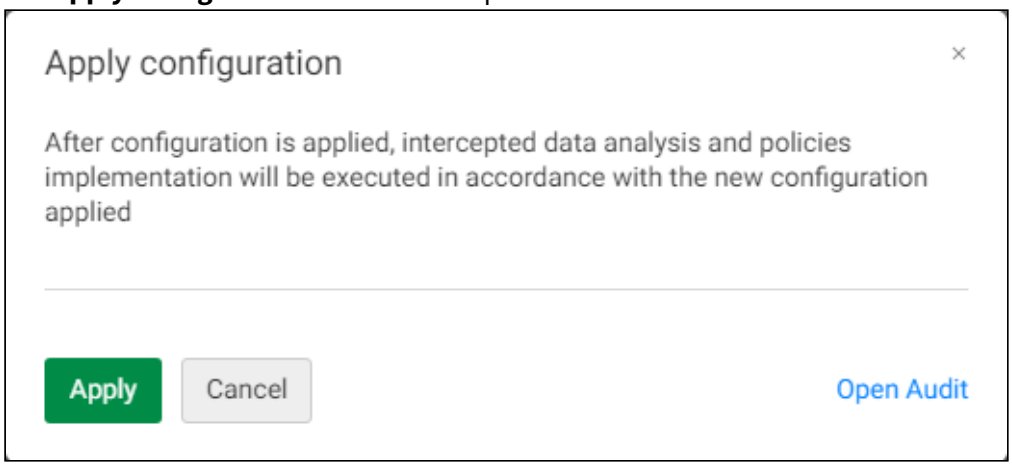
Purpose:
Apply the System configuration.

Solution:

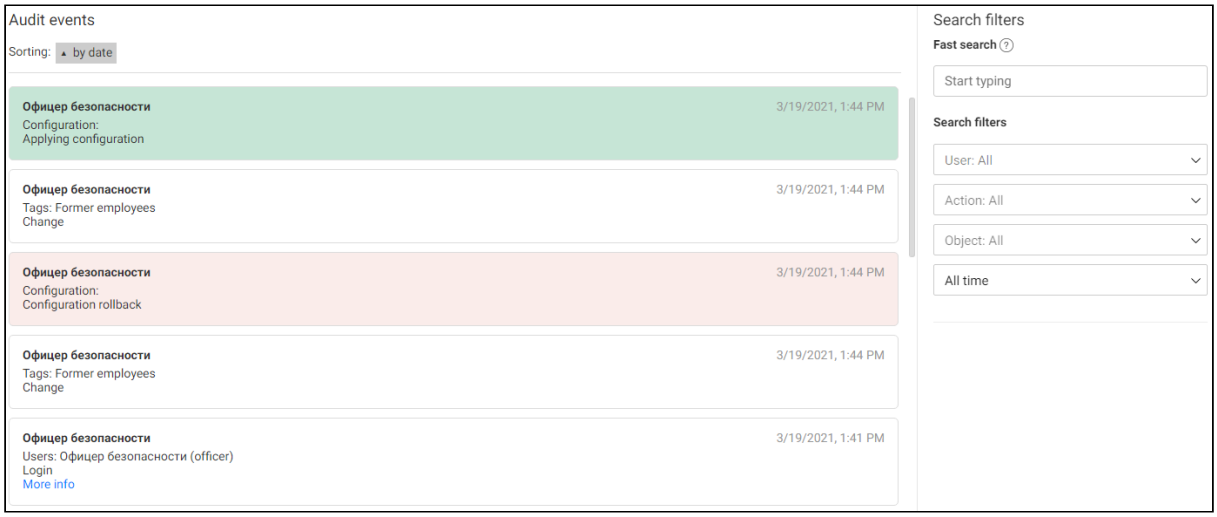
1. When you finish editing the configuration, then, at the top of the browser window, click **Apply** in the bar:



The **Apply configuration** window will open:

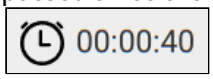


2. To view details about changes being applied, click **Open Audit**. The action is available when Applying, Saving, Reseting configuration. When clicking **Open Audit**, the section Audit will be opened in a new browser tab. Events of Applying and Reseting configuration will be highlighted in Audit section.



> **Note:**
>
> **Open Audit** option is available only for the user having access to Audit section.

3. In the **Apply configuration** window, click **Apply**.
4. Wait for the application of the configuration to complete.
   Applying the new configuration may take some time. The duration of application does not exceed 3 hours. At the top of the workspace, a counter is displayed. The counter displays the time that has passed since the start of the configuration application process:



   You can edit a configuration and apply it even if another configuration is being applied. In this case, the application of the configuration will be interrupted and the application of the edited configuration will start.

4.1.3 Editing Element

Purpose:
Change attributes of an earlier created element.

Solution:

1. Go to the target section.
2. If necessary, go to the target subsection or tab.
3. Select the target element by clicking the left mouse button or select it from the drop-down list, and click **Edit**.
4. Enter required attributes (attributes of all elements are described in "Management Console Interface").
5. Click **Save**.

4.1.4 Deleting Element

Purpose:
Delete an element.

Solution:

1. Go to the target section.
2. If necessary, go to the target subsection or tab.
3. Select the target element by clicking the left mouse button or select it from the drop-down list.

> **Note:**
>
> To delete several elements, select them holding *Shift* or *CTRL*.

4. Click **Delete**.
5. In the confirmation window, click **Yes**.

4.1.5 Pages Navigation

Reference information:
Page navigation can be performed only in multi-page interface view mode.
Multi-page view mode is used for ergonomic work area usage. It is available when browser displays the page navigation pane:



Pages navigation panel

Purpose:
To go to the desired page in the multi-page mode.

Solution:

1. Go to the target section.
2. If needed, go to the target subsection or tab.
3. In the drop-down list located in right part of the page navigation pane, select a number of elements per page.

4. For page navigation, use buttons with page numbers. You can also use the following buttons:
    - **|<** - to go to the first page;
    - **<** - to go to the previous page;
    - **>** - to go to the next page;
    - **>|** - to go to the last page;

> **Note:**
>
> When using list sorting, navigation buttons act according to updated list.
> For example, when sorting the list beginning with letter "A", the **>|** button will lead to he page with elements beginning with "Z". But if the sorting is backward, the **>|** button will lead to he page with elements beginning with "A".

4.1.6 Changing User Password

Reference information:
Users can change the password for the account under which they are authorized in the System.

Purpose:
To change the password.

Solution:

1. Click the user menu button and select **Change password**.
   The **Change password dialog box** will appear.
2. In this dialog box, type a new password for the account in the fields:
    - **Password**;
    - **Confirm password**.

    > **Note:**
    >
    > Consult detailed guidelines for passwords described in the document "*Infowatch Traffic Monitor. Administration Guide*".

3. Click **Save**.

4.1.7 Selecting Interface Language

Purpose:
Change the interface language of the Management Console.

Solution:

1. ClickClick the user menu button (see "Interface of Traffic Monitor Management Console") and in the **Change language** block, choose a desired language.
2. In the **Change language** dialog window that opens, click **Yes**.

Do the same steps to revert English language if necessary.

4.1.8 Calling Help File

Purpose:
Get the reference information on how to work in the System.
Solution:

1. In the right upper corner of the workspace, click the user menu button (see "Management Console Interface").
2. In the drop-down list, under the **Help** caption, choose the desired type:
   - **Online** - to open the online version of documentation;
   - **Offline** - to open the offline version of documentation.

   In a new browser tab, InfoWatch Traffic Monitor help file in the selected format will open.
3. Read the information and then close the tab in the standard way.

4.1.9 Viewing Information on System

Purpose:
Get general information about the System.

Solution:

1. Click the user menu button (see "Interface of Traffic Monitor Management Console"), and choose **About**.
   The **About** window will be displayed on the screen, where you can view information about the System.
2. Read the information and then close the window in the standard way.

4.2 Managing Persons and Computers

Why do you need persons and computers:

Persons and computers make it easier for the security officer to work with intercepted objects. This is due to storing information about senders, recipients, and computers participating in data transfer.

> **Warning!**
>
> For the changes described in this section to be used in the System, you should apply the renewed System configuration (see details in "Configuring the System" and "Applying the System Configuration").

Creating lists of persons and computers include the following steps:

1. Creating a group where persons and computers will be added (see "Creating Group of Persons or Computers")
2. Filling the created group (see "Creating Persons and Computers").
3. Configuring cards for added persons and computers (see "Configuring Person's Card" and "Configuring Computer Card").
4. Assigning a status to a person or a computer (see "Adding Status to Persons").

You can export created groups, persons and computers in order to move the configuration to another server. Or you can import a configuration that was loaded from a different server (see "Exporting and Importing Persons").

When you have created groups of persons and computers, you can perform the following actions with them:

- Add a person or a group to a perimeter (see "Managing Perimeters")
- Create a person control policy for individual persons or for a group (see "Creating Person Control Policy")
- Create a query to find events associated with a person or a computer (see "Creating Queries")
- View a summary for a person or a computer (see "Viewing Summary on Violations/Violators")
- View screenshots for a person or a computer (see "Viewing Screenshots")

See also:

- "Persons Section" - about the section where you can create lists of persons and computers
- "Perimeters" - about the section where you can configure perimeters
- "Events Section" - about the section where you can create search queries
- "Dashboard Section" - about the section where you can view a summary on interception objects

4.2.1 Creating Group of Persons or Computers

Purpose:
Create a group of persons or computers.

Solution:

1. Go to the **Persons** section.
2. In the left part of the workspace, select  **User Groups**.
3. On the toolbar in the left part of the workspace, click  **Create group**.
4. In the window that opens, specify the name of a new group and, if necessary, add a description. You can also specify the group contacts. The contacts may include **Email** and **Lotus Email**.
5. Click **Save**.

> **Warning!**
>
> If a new group is created, events for this group are displayed starting from the moment of applying the configuration.

You can add existing Active Directory, Samba DC, Domino Directory, Astra Linux Directory, Astra Linux Directory Pro and FreeIPA groups to a user group. In this case, when you add or remove persons in an Active Directory, Samba DC, Domino Directory, Astra Linux Directory, Astra Linux Directory Pro or FreeIPA, contents of the corresponding user group will be updated automatically.

To add an Active Directory, Samba DC, Domino Directory, Astra Linux Directory, Astra Linux Directory Pro or FreeIPA group to a user group, select a desired Active Directory/Samba DC/Domino Directory/Astra Linux Directory/Astra Linux Directory Pro/FreeIPA group with a mouse and drag and drop it at the required user group.

Groups from different domains can be added to the same user group. You can also use drag-and-drop to add individual domain users to a user group.

> **Note**
>
> To enable automatic update for user groups which contain Active Directory, Samba DC, Domino Directory, Astra Linux Directory, Astra Linux Directory Pro or FreeIPA groups, run synchronization with the LDAP server.

On filling created groups, see "Creating Persons and Computers".

Example:

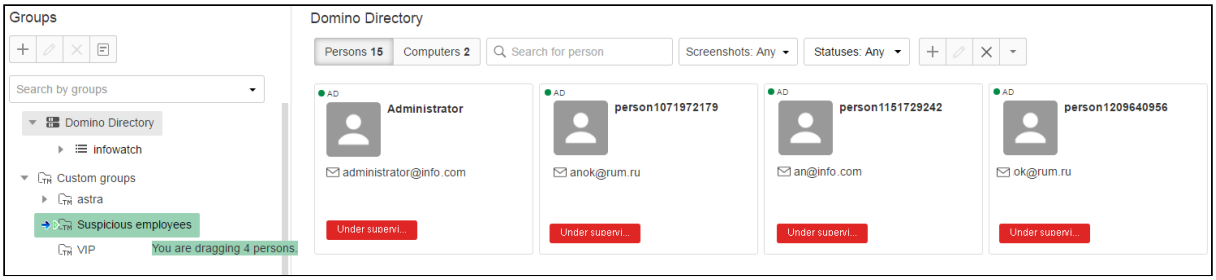
You need to add suspicious employees to a separate group. For this:

1. In the **User Groups** node, create "Employees under suspicion" group.
2. Using **Search for person** field or filters find persons which you want to add to the group.

> **Tip**
>
> Using filters you can find all active employees with "Under supervision" status.

3. Add the found persons to the group.

> **Tip**
>
> You can select cards of the required persons and drag them to the group with a mouse.



You can use the created group "Employees under suspicion" for real-time monitoring, creating person control rules, or searching for events by employees with the "Under supervision" status.

Additional information:

Editing and deleting groups of persons and computers are performed by standard means:

- Editing Element
- Deleting Element

4.2.2 Creating Persons and Computers

Reference information:
You can fill groups of persons and computers in the following ways:

- from LDAP - this is configured by the System administrator (see the document "*Infowatch Traffic Monitor. Administration Guide*");
- by means of Traffic Monitor - the list is created by the security officer as described in this topic.

Purpose:
To fill a group of persons and computers.

Solution:

1. Go to the **Persons** section.
2. On the left part of the workspace, left-click the target group.

3. On the right part of the workspace, click on the tab:
   - **Persons** - to add a person;
   - **Computers** - to add a computer.
4. On the toolbar in the right part of the workspace, click **Add**.
5. Specify parameters of a new user or computer (see “Persons" and "Computers").
6. Click **Save**.

To add a person from the contact in event:

1. Click to select an unidentified contact in event.
2. In the window that opens select **Create new person**.
3. Specify new person parameters and click **Add.**

Additional information:
You can edit or delete persons and computers by standard means:

- Editing Element
- Deleting Element

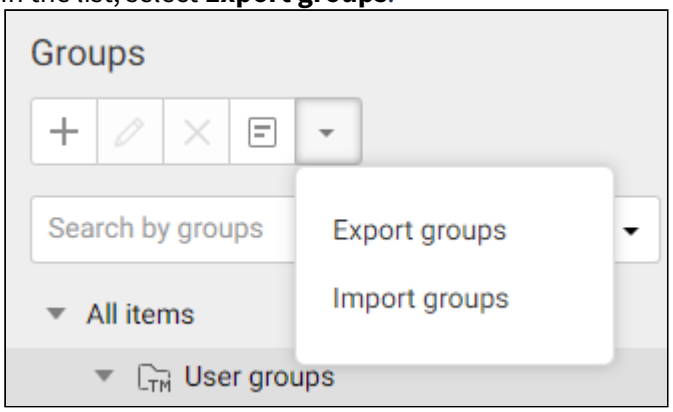
4.2.3 Exporting and Importing Persons

In Traffic Monitor, you can **export** and **import** groups of persons. That makes it easier to save the configuration and move it to another server.

Before the export, make sure that Traffic Monitor configuration is not being edited and the user has the **Import and export of organizational structure** privilege. All groups, persons and computers are exported.

To **export** groups of persons from Traffic Monitor:

1. Go to the **Persons** section.
2. Click .
3. In the list, select **Export groups**.



4. The System will prepare the data to be exported, the progress will be displayed in the lower rigth corner.As a result, a ZIP archive will be saved to the computer. The archive contains an XML file with a desription of configuration elements. The archive name includes the date of the export, for example: `iwtm-group-20221213_141243.zip`.
   You can use the archive to import configuration elements to another server.

To import groups of persons, you should firts apply a configuration. Make sure that the configuration has been applied and the user has the **Import and export of organizational structure** privilege.

To **import** groups of persons to Traffic Monitor:

1. Go to the **Persons** section.

2. Click .
3. From a drop-down list, select **Import groups**.
4. In the window that opens, select an earlier exported ZIP archive with a description of groups of persons.
5. Wait for the data import to complete, the progress will be displayed in the lower right corner.
6. Apply the configuration and update the page. After that, added groups, persons and computers will be displayed in the Traffic Monitor Management Console.

Features of exporting and importing the organzational structure

Features of export:

- Only applied configuration can be exported.
- Only entities that have been created or edited in Traffic Monitor can be exported. When exporting contatcs and attributes, they are linked to persons.
  Example: if a person was added to the System after LDAP synchronization, only those attributes and contacts that have been edited in Traffic Monitor can be exported.
- Deleted entities are not exported.
- In Traffic Monitor 7.6, statuses of persons and computers are not exported.

Features of import:

- When importing groups, the hierarchy of groups is preserved.
- To successfully import groups, persons or computers that were added during LDAP synchronization, there should be a similar entity in the System. Otherwise, an error will occur, however, the import process will continue.
- If an entity being imported and an entity in the System have the same names but different identifiers (ID), the entity will not be impoted.
- If an entity being imported and an entity in the System have the same identifiers (ID) but different names, the entity will be imported.
- If both the names and the identifiers match, new contacts and attributes will be added to the entity. If the entity already has attributes and contacts, then:
  - for entities created after LDAP synchronization, existing contacts and attributes will be replaces with values from the file;
  - for entities created in Traffic Monitor, existing contacts and attributes will remain unchanged.

4.2.4 Configuring Person's Card

Purpose:

Fill the card of person with data.

Configuring the person’s card consists of the following actions:

Action	Description
Adding Contact to a Person	Add contact information for the created person
Adding Compuer to Person	Add a computer associated with the person
Adding Person to Group	Adding the person to an existing group

Adding Contact to Person

Purpose:
Add or edit contact information for the person.

Solution:

1. Go to the **Persons** section.
2. On the left part of the workspace, left-click the target group.
3. In the right part of the workspace, open the **Persons** tab.
4. Double-click the target person. The person card will open.
5. On the **Information** tab, in the **Contacts** block, click .
6. In the **Add contact** form that opens, specify required parameters:
   - type of contact: e-mail, Lotus mail, mobile phone, landline phone, Skype, ICQ, web contact, domain account, social networks account, etc.;
   - whether the contact is personal or working;
   - contact value (number or address);
   - optional description.
7. Click **Save**.

> **Note:**
>
> Contact values must be specified in the following format:
>
> -  - mobile phone (string of 3 or more characters; may contain only digits, space, and the characters: “-”,”_”, “( )”,”+”);
> -  - landline phone (string of 3 or more characters; may contain only digits, space, and the characters: “-”,”_”, “( )”,”+”);
> -  - e-mail (e-mail address in RFC format);
> -  - Lotus e-mail (e-mail address in RFC format).
> -  - domain account (e-mail address in RFC format);
> -  - Skype contact (string of 1 or more characters);
> -  - MS Teams account, if the adapter is installed (string of 1 or more characters);
> -  - ICQ contact (string of 1 or more characters);
> -  - Facebook account (string of 1 or more characters);
> -  - VK account (string of 1 or more characters);
> -  - Telegram account (string of 1 or more characters);
> -  - WhatsApp account (string of 1 or more characters);
> -  - other Web-account (string of 1 or more characters).
>
> WhatsApp and Telegram messengers use their own identifier formats. It is recommended to use Mobile phone type of contact for associating the person with the intercepted messenger contact.

To edit previously specified contact details:

1. Select the desired contact using the left mouse button and, on the toolbar, click .
2. Edit parameters of the contact.
3. Click **Save**.

To add new contact from the event to the person:

1. Click on an unidentified contact from the event.
2. In the window that opens, select **Add contact to the person**.
3. Select person from the list and click **Save**.
4. Click **Yes** to confirm contact adding.
5. In the window that opens, click **Go to person** to check that the new contact has been added.

Adding Computer to Person

Purpose:
To add a computer that will be linked to a particular person.

Solution:

1. Go to the **Persons** section.
2. On the left part of the workspace, left-click the target group.
3. In the right part of the workspace, open the **Persons** tab.
4. Double-click the target person. The person card will open.
5. On the **Information** tab, in the **Computers** block, click .
6. In the **Add workstation** window that opens, select required computers.
7. Click **Save**.

Adding Person to Group

Purpose:
Add a person to an existing group.

Solution:

1. Go to the **Persons** section.
2. In the left part of the workspace, left-click the target group.
3. In the right part of the workspace, open the **Persons** tab.
4. Double-click the target person. The person card will open.
5. On the **Information** tab, in the **Groups** block, click .
6. In the **Add group** window that opens, select desired groups.
7. click **Save**.

If you need to remove a person from the current group:

1. On the **Persons** tab, select the desired person.
2. On the toolbar in the right part of the workspace, click and in the drop-down list select **Remove from group**.
3. In the confirmation window, click **Yes**.

> **Warning!**
>
> If the person is included in this only group, then this command will delete the person.

4.2.5 Configuring Computer Card

Purpose:
Add data to a computer card.

Configuring a computer card consists of the following actions:

Action	Description
Adding contact to computer	Adding an IP/DNS contact or a domain account to the computer
Adding person to computer	Adding a person associated with this computer
Adding computer to group	Adding computer to an existing group

Adding Contact to Computer

Purpose:
Specify the IP address, DNS name, or domain account for the computer.

Solution:

1. Go to the **Persons** section.
2. On the left part of the workspace, left-click the target group.
3. In the right part of the workspace, open the **Computers** tab.
4. Double-click the target computer. The computer card will open.
5. On the **Information** tab, in the **Contacts** block, click +.
6. In the **Add contact** form that opens, specify required parameters:
   - contact type: **IP**, **DNS** or **Domain account**;
   - account value: IP address, DNS name, or a domain account name;
   - optional description.
7. Click **Save**.

Adding Person to Computer

Purpose:
Add a computer linked to a person.

Solution:

1. Go to the **Persons** section.
2. On the left part of the workspace, left-click the target group.
3. In the right part of the workspace, open the **Computers** tab.
4. Double-click the target computer. The computer card will open.
5. On the **Information** tab, in the **Persons** block, click +.
6. In the **Add person** window that opens, flag required persons.
7. Click **Save**.

To remove the added person, select the person in the list and click ×.

Adding Computer to Group

Purpose:
Add computer to an existing group.

Solution:

1. Go to the **Persons** section.
2. On the left part of the workspace, left-click the target group.
3. In the right part of the workspace, open the **Computers** tab.
4. Double-click the target computer. The computer card will open.
5. On the **Information** tab, in the **Groups** block, click +.
6. In the **Add group** window that opens, flag required groups.
7. Click **Save**.

If you need to remove a computer from the current group:

1. Select the required computer on the **Computers** tab.
2. On the toolbar in the right part of the workspace, click ▾ and in the drop-down list select **Remove from group**.
3. In the confirmation window, click **Yes**.

> **Warning!**
>
> If the computer belongs to this only group, then this command will result in deleting the computer.

4.2.6 Adding Status to Persons

Purpose:
To add status to a person or computer.

Solution:

1. Go to the **Persons** section.
2. On the left part of the workspace, left-click the target group.
3. On the right part of the workspace, click on the tab:
   - **Persons** - to add status to a person;
   - **Computers** - to add status to a computer.
4. Select the target user or the target computer.
5. On the toolbar in the right part of the workspace, click ▾ and, in the drop-down list, select **Set status**.
6. In the dialog box that appears, specify the desired status and, if necessary, enter a description.
7. Click **Save**.

> **Note:**

The *New* status is assigned to a person or computer when they are created in the System. This status is preserved for 30 days. For persons and computers imported from Active Directory, Samba DC, Domino Directory, Astra Linux Directory, FreeIPA or Astra Linux Directory Pro, the *New* status is preserved for 30 days starting from the moment the records are created in Active Directory, Samba DC, Domino Directory, Astra Linux Directory, FreeIPA or Astra Linux Directory Pro resrectively).

See also:

- "Statuses" - on the section where you can manage statuses of persons and computer

4.2.7 Viewing Screenshots

Preliminary settings:

For screenshots to be displayed in cards of persons and computers, synchronization with Active Directory or Samba DC is required.

If you do not use Active Directory or Samba DC in your company, or, due to technical restrictions, synchronization is unavailable, then, to enable viewing screenshots, do the following:

1. Create cards of persons and computer, for which you want to retrieve screenshots (see "Creating List of Persons and Computers").

   Примечание:

   On workstations with Astra Linux OS, screenshots are not created.

2. For persons, specify a domain account (see "Adding Contact to Person").

   Note:

   Specify the domain account in the following format: *name@client* where *name* is the user name and *client* is the name of the computer.

3. For computers, specify a NetBIOS or device name (see "Adding Contact to Computer").

Note:

In the case of synchronization with Domino Directory, Astra Linux Directory, Astra Linux Directory Pro or FreeIPA, it is also possible to specify a domain account for persons.

Important!

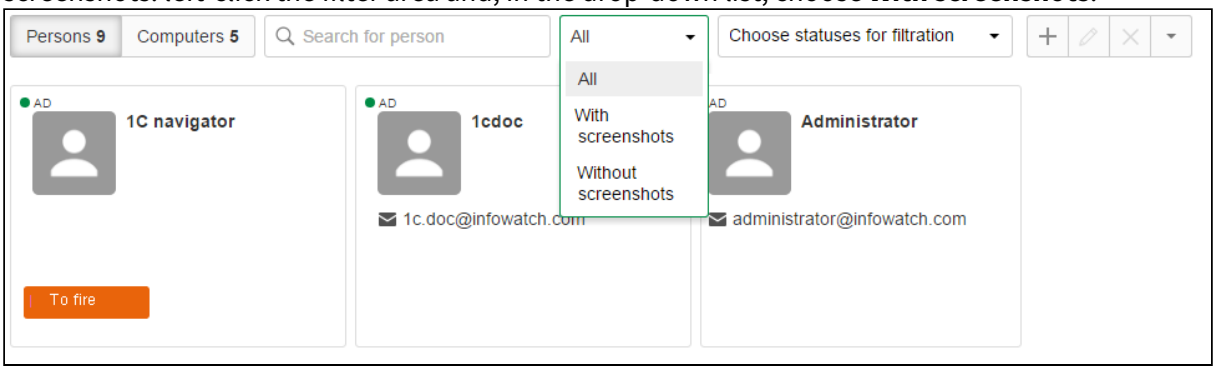
It is necessary to perform specified actions prior to creating a Device Monitor rule (see "ScreenShot Monitor Rule (DM)" in *"InfoWatch Device Monitor. User Guide"*) and deploying the Device Monitor policy, which includes this rule, to workstations. Otherwise, the System will not display screenshots.

Purpose:

View intercepted screenshots for a person or a computer.

Solution:

1. Go to the **Persons** section.
2. In the left part of the workspace, left-click the desired group.
3. In the right part of the workspace, open the desired tab: **Persons** or **Computers**. The list of persons or computers included in the selected group will be displayed.
4. You can find the desired person or computer using the **Search for person** field (search by a person name or the computer IP address is available).
   In the case of a large number of persons/computers, you can filter elements by the presence of screenshots: left-click the filter area and, in the drop-down list, choose **With screenshots**.



   As a result, persons or computers that meet the filtering criteria will be displayed.
5. To view screenshots for the selected person or computer, do either of the following:
   - select the person or computer in the list, then, on the toolbar, click and, from the drop-down list, select **Show screenshots**;
   - double-click the desired person or computer and, in the person or computer card that opens, switch to the **Screenshots** tab.

   The **Screenshots** tab contains all screenshots taken for this person or computer.
6. You can specify the following criteria for displaying screenshots:
   - **Application** - start typing the application name and choose the desired application from suggestions. Or click and, in the dialog box that opens, check the boxes of the selected applications, then click **Save**.

     > **Note:**
     >
     > If you enter the application name manually, you can use * in the beginning or in the end of the line to replace any number of characters.

   - **Person**/**Computer** - when viewing screenshots for a person, you can filter them by the computer name. Similarly, when viewing screenshots for a computer, you can specify a person and view screenshots for this person.
   - **Date** - specify the period for which to display screenshots. By default, screenshots for all time are displayed.

> **Note:**
>
> When you select a period in the calendar, you can specify the date and the time. Dates, for which screenshots are available, are highlighted in blue.

7. When you specify all required criteria, click **Apply**. The System will display screenshots that meet the specified criteria.
8. To view detailed information on a screenshot, click the desired screenshot. The System will display the screenshot and its attributes.
9. You can increase or decrease the image scale, go to the previous or the next image (for details, see "Screenshots").
10. To close the viewer, click **X**.

4.3 Managing Catalogues

> **Warning!**
>
> If you want changes described in this section to be used in the System, apply the configuration: see "Configuring the System" and "Applying System Configuration".

What for do you need catalogs?
To group data of similar types that used in the System for creating policies.

Managing catalogs includes the following actions:

- Managing Tags
- Managing Web Resources
- Managing Statuses
- Managing Perimeters

See also:

- "Lists Section" - on the section where you can manage catalogs

4.3.1 Managing Tags

Purpose:
To create a tag.

Solution:

1. Go to the **Lists** section, subsection **Tags**.

2. On the toolbar click + **Create tag**.



3. Specify attributes of the added tag (see "Tags").
4. Click **Save**.
5. If necessary, repeat the adding procedure to fill the catalog of tags.

Additional information:
Editing and deleting tags are performed by standard means:

- Editing Element;
- Deleting Element.

4.3.2 Managing Web Resources

Purpose:
Specify web resources, which the System treats as inappropriate use of working time. To do this:

1. Create a list of web resources.
2. Add resources to the list.

Solution:

1. Creating a group of resources
   a. Go to the **Lists** section, the **Web resources** subsection.
   b. In the left part of the workspace, click + **Create web resource list.**
   c. In the window that opens, type a name and description of the resource list.
   d. Click **Save**.
2. Adding a resource
   a. Go to the **Lists** section, **Web resources** subsection.
   b. In the left part of the workspace, left-click the target resource list.
   c. On the toolbar in the right part of the workspace, click + **Add web resource**.



d. In the **Adding web resource** window that opens, enter the resource attributes:
   - in the **Value** field - the resource name on the Internet;
   - in the **Description** field - a comment to the resource (optional).

e. Click **Save**.

> **Warning!**
>
> When you have finished editing the resource list, you need to apply the updated configuration (see "Applying System Configuration").

Additional information:

Web resources and their groups can be edited and deleted by standard means:

- Editing Element
- Deleting Element

4.3.3 Managing Statuses

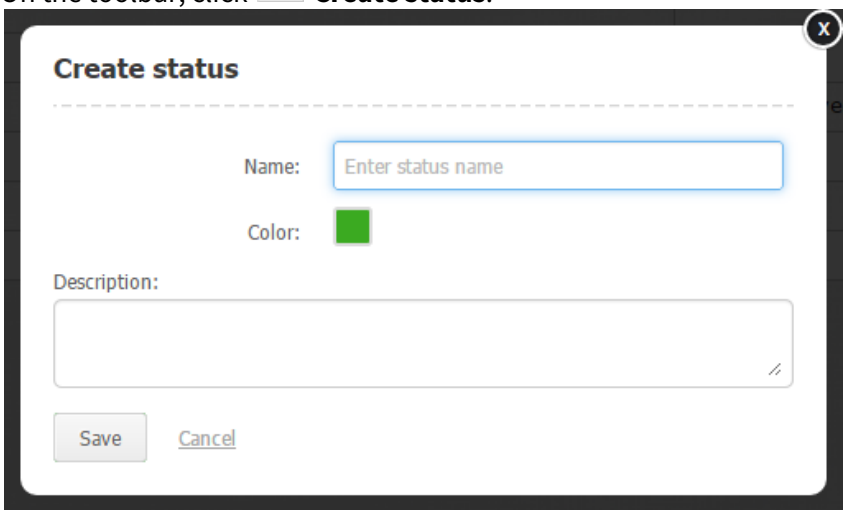
Purposes::

1. Create a status that characterizes a person or a computer.
2. Create a person control policy for persons and computer with a specific status.

To create a new status:

1. Go to the **Lists** section, **Statuses** subsection.

2. On the toolbar, click **Create status**:



3. Specify attributes of the new status (see "Statuses").
4. Click **Save**.

To create a person control policy directly from Statuses subsection:

1. Go to the **Lists** section, **Statuses** subsection.
2. In the list of statuses, select the desired status.
3. On the toolbar, click **Create policy**.
   The **Policies** section will open. It displays the new person control policy for persons and computers with the selected status (for detail, see "Policies Section").

Additional information:

Statuses can be edited and deleted by standard means:

- Editing Element
- Deleting Element

4.3.4 Managing Perimeters

Reference information:

Perimeters allow you to logically divide your organization into structural units and track where the traffic goes. Perimeters may include elements of different types: domain, groups of persons and computers, web resources, etc.

By default, the System includes the following perimeters:

- *Company* – to control sending data outside the company;
- *Exclude from interception* – to be used in the preset policy *Excluding from Interception* (see "Policy that Excludes Mailing Lists from Interception").

Preset perimeters do not contain elements, you should add elements manually (see *Purpose 2* in this article).

Besides preset perimeters, you can also create perimeters based on the following elements:

- Person
- Person group
- Web resource
- Contacts:
  - Email address

- Phone
- Skype contact
- ICQ contact
- Domain
- Lotus contact

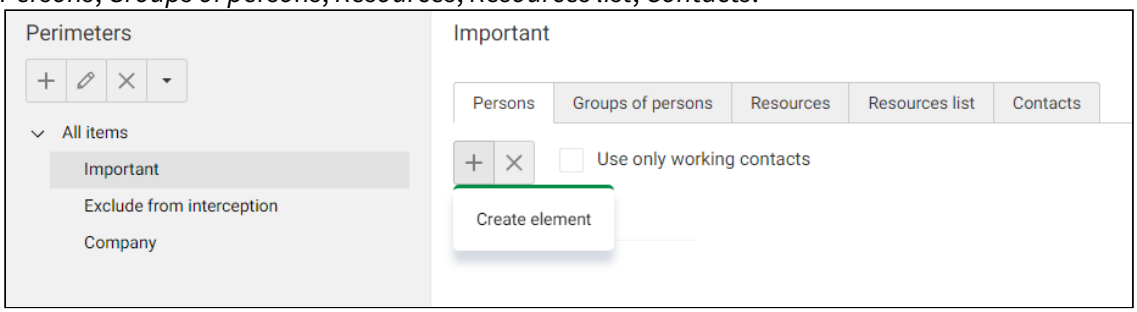
> **Note:**
>
> To choose LDAP domain, you should first configure synchronization with LDAP server and add the domain via the **Groups** tab.

Purpose:

1. Create a perimeter.
2. Add an element to the perimeter.

Solution:

1. Creating a perimeter.
   a. Go to the **Lists** section, **Perimeters** subsection.
   b. In the left part of the workspace, click + **Create perimeter**.
   c. In the window that opens, in the **Name** field, specify the name of the perimeter.
   d. In the **Description** field, enter a description (optional).
   e. Click **Save**.
2. To add an element to the perimeter.
   a. Go to the **Lists** section, **Perimeters** subsection.
   b. In the left part of the workspace, left-click the target perimeter in the list of perimeters.
   c. In the right part of the workspace, click **Create element** + on one or several tabs: *Persons*, *Groups of persons*, *Resources*, *Resources list*, *Contacts*.



   d. In the field that appears, specify one or more elements doing one of the following:
      - For Persons, Group of persons or Resources list:
        - start typing the name of the item in the field and select the desired entry from the drop-down list;
        - click + **Add** to the right of the field and, in the dialog window that opens, select desired elements. To find the element you require, use the search line;
        - if you need to use working contacts only, mark the checkbox **Use only working contacts**. Personal contacts will not be used in the perimeter. Then click **Save**.
          After adding persons/groups of persons to perimeter, you can go to the person's card in **Persons** section. For this, click on the name of person's or groups of persons.

- For *Resources* and *Contacts* enter the name or value into the field and press **Enter**.
  - click [+], enter the element's name and press **Save**. For *Contact* specify the type: *Email address*, *Mail domain*, *ICQ contact*, *Lotus contact*, *Phone*, *Skype*
  - click [⬇] **Items bulk upload** and add a cvs file containing the list of elements, wait until its load is complete and press **Save**.

> **Note:**
>
> CVS file should represent a list containing one column with no headline. One row can contain only one email address, mail domain or resource.

3. Entered values will be added to the list of elements. To remove an element or more from the list, select them and click [×] **Remove element/elements**.

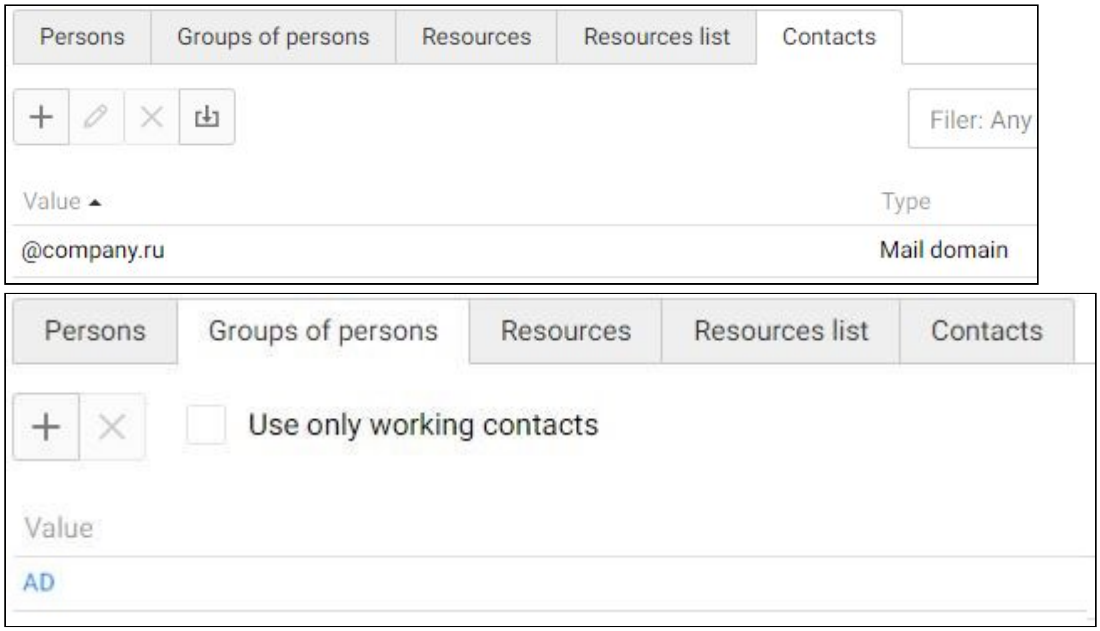


> **Warning!**
>
> We recommend not creating more than 15 perimeters that contain more than 2000 elements each.

Example:

The company uses corporate email with a dedicated domain. For new employees, the email is generated automatically from a template `lastname@ company.com`. It is required to control the transmission of confidential information outside the company by email. Sending documents within the company is legitimate. In this case:

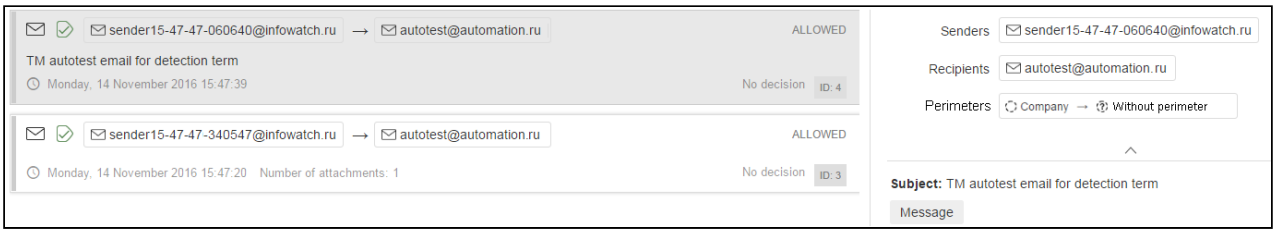
1. Create a *Company* perimeter (if the System already includes the *Company* perimeter, skip this step).
2. Add the following elements to the perimeter: `@ company.com` mail domain and a group of AD persons which contains the company employees.



3. Save the perimeter.

Now the System will treat messages sent to private email addresses as sending data outside the company perimeter.

If you create a query in the "Events" section, you can quickly find all events of sending data outside the company.



You can **export** and **import** perimeters in Traffic Monitor. This makes it easier to save the configuration and move it to another server.

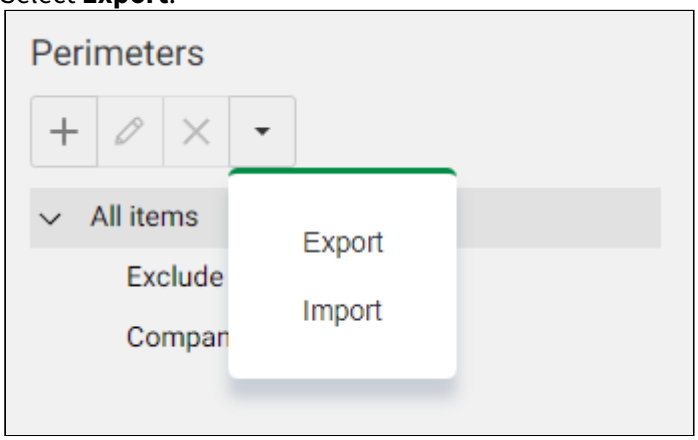
> **Warning!**
>
> In the current version, you can only move elements of the Resouces and Contacts tabs.

Before exporting, make sure that Traffic Monitor configuration is not being edited and you have a sufficient privillege for exporting. The System exporst all perimeters, not only a selected one.

To **export** perimeters from Traffic Monitor:

1. Go to **Lists** section, **Perimeters** subsection.

2. Click .
3. Select **Export**.



4. The System will prepare perimeters to be exported. You will see the progress bar in the lower right corner.

As a result, a ZIP archive containing XML file with description of configuration elements will be saved to the computer. Archive name will contain the export date, e.g. `iwtm-perimeter-20220808_193432.zip`.

Use this archive to import configuration elements to another server.

Before importing perimeters, you should first apply the configuration. Make sure that Traffic Monitor configuration has been applied and you have a sufficient privilege for importing.

To **import** perimeters to Traffic Monitor:

1. Go to **Lists** section, **Perimeters** subsection.
2. Click .
3. Select **Import**.
4. In the dialog box, specify a zip archive with a description of perimeters you've exported earlier.
5. Wait until perimeters are exported, the progress bar will be displayed in the lower right corner.
6. Apply the configuration and refresh the page. The Management Console will display added perimeters and elements.

Additional information:

Perimeters can be edited and deleted by standard means:

- Editing Element
- Deleting Element

4.4 Managing Base of Technologies

> **Warning!**
>
> If you want changes described in this section to be used in the System, apply the configuration: see "Configuring the System" and "Applying System Configuration".

What do you need the base of technologies for?
Using elements of the technologies base, you can denote to the System which information is confidential within the

company (disclosure of this information is a violation of the corporate security policy). The base of technologies is used for analyzing actions of persons, as a result of which violations of the corporate security policy can be identified (for example, sending a confidential document outside the company perimeter). The *base of technologies* is a set of elements (terms, text objects, sample documents, etc.), used for analysis of intercepted data.

In addition to the base of technologies, person's actions can also be analyzed by means of the resource list. This list allows identifying improper use of working time (for example, visiting entertaining Internet sites from working computer). For more information on specifying inappropriate resources, see "Managing Resources Lists".

Configuring analysis of the person's actions includes the following:

1. Defining the confidential information - creating the base of technologies.
2. Specifying inappropriate resources - creating a list of resources visiting which from a workplace is considered inappropriate use of working time.
3. Creating protected objects based on the elements of the base of technologies.

Then you can create a policy and denote to the System how to respond if protected objects are detected in intercepted data, or if requests are sent to inappropriate resources (see "Configuring System Response").

See also:

- "Technologies Section" - on the section where you can manage the base of technologies
- "Web Resources" - on the subsection where you can manage web resources
- "Protected Objects Section" - on the section where you can manage protected objects

4.4.1 Defining the Confidential Information

Purpose:

Add elements to the base of technologies that will be used by the System to detect confidential data in interception objects.

Solution:

1. Go to a subsection of the **Technologies** section (**Categories and terms**, **Text objects**, **Sample Documents**, **Blanks**, **Stamps** or **Database Unloadings**).
2. Create a new category in the **Categories and terms** subsection or a new catalog in other subsections.
3. Fill the created category (or created catalog) with examples of confidential data that will indicate violations of the security policy if found in traffic.
4. If necessary, repeat steps 2 and 3.

> **Warning!**
>
> When you have finished configuring the base of technology, you need to apply the updated configuration (see "Applying System Configuration").

For more information about adding elements for each technology, see the following articles:

Technology name	Technology description	Action
Categories and terms	A set of terms and their categories. The term is a word or phrase which (if found in the analyzed text) increases the degree of	Creating terms and their categories

Technology name	Technology description	Action
	conformity of the text to the category of the found term.	
Text objects	Text information extracted from the object body and its attachments. Contains no formatting or markup. Applies and solving analysis tasks and search.	Creating text objects
Sample documents	Document quotes from which are searched in the analyzed text. Memos, financial reports, contracts, and other sensitive documents can all be used as sample documents. Sample documents are stored in the system as digital prints, their text is not available to either users or System administrators	Creating Sample Documents
Blanks	Blank whose version is searched for in the network traffic. Blanks may be different questionnaires, receipts, etc. Blanks are stored in the System as digital fingerprints, their text is not available for viewing either by users or by the System administrators.	Creating Forms
Stamps	Stamp image that is searched in the network traffic. Stamps can be images of round impressions used in organizations.	Creating Stamps
Database unloadings	A part of a database quotes from which are searched in the analyzed text. Database unloadings can be lists of salaries, other personal data, etc.	Creating Database Unloadings
Graphical objects	Image of particular type that is searched in the network traffic. Graphical objects can be images of credit cards or technical drawings.	Managing Graphical Objects
Autolinguist	Learning automatic classifier based on standard text documents that are to be detected in the traffic. The text documents can be the files of different formats used in the company.	Managing Autolinguist

See also:

- "Technologies Section" - on the section where managing the base of technologies is performed

Managing Categories and Terms

Reference information:
Terms are a set of words and phrases required to perform the linguistic analysis of the text. Terms are grouped into *categories*.
Categories allow classifying possible violations of security policy. If a text contains a term from a certain category, the text is matched with this category.

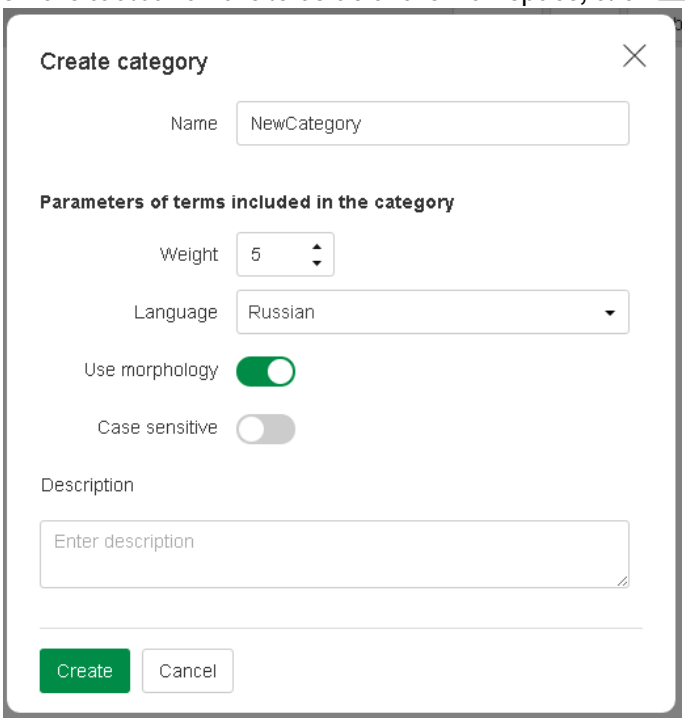
Purposes:

1. Create a category of terms.
2. Create a term within a category.

Solution:

1. To create a category.

a. Go to the **Technologies**->**Categories and terms** section.
b. On the toolbar on the left side of the workspace, click + **Create category**.



c. Specify required attributes for the category (see "Categories").
d. Click **Create**.

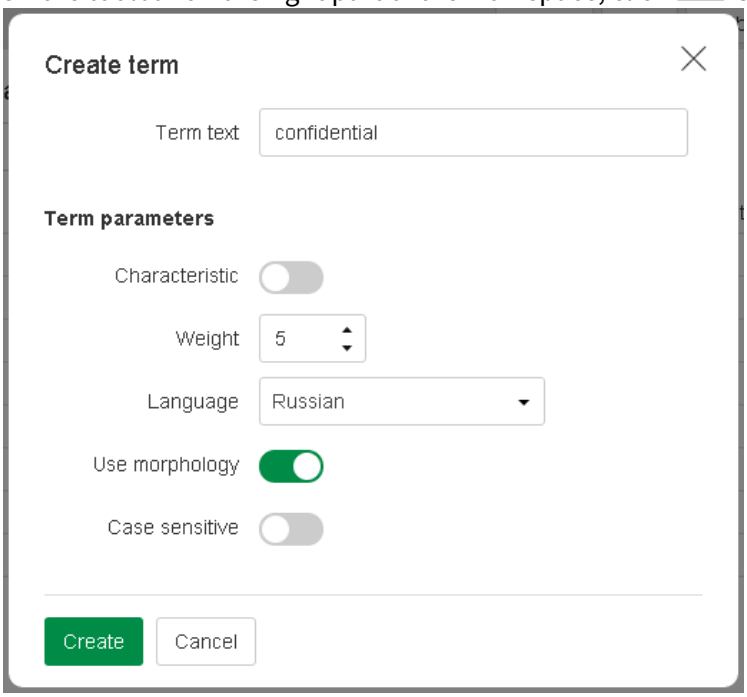
2. Creating a term.

a. Go to the **Technologies**->**Categories and terms** section.
b. On the left part of the workspace left-click the target category.

> **Note:**

For terms adding only those categories that do not include other nested categories are available.

c. On the toolbar on the right part of the workspace, click + **Create term**.



d. Specify required attributes (see “Terms").
e. Click **Save**.

Note:

The terms added to category inherit the category parameters by default. When creating and editing the term you can change its parameters.

Example 1:
If you need that the System should mark the interception object as DOCUMENT_ISSUE_DATE if it contains, at least, one occurrence of the phrase "document issue date”, then:

1. Select a target category.
2. Add the *Document issue date* term to this category.
3. Enable the **Characteristic** option.

If intercepted data contains this phrase, the System assigns the *Document issue date* category to the object.

Example 2:
If you need that the System should mark the intercepted object as code leakage if the traffic contains fragments of program code, then:

1. Create a *Code leakage* category.
2. Add *Procedure* and *Result* terms to the category.

Note:

In case the parameters are default, two terms are not enough to make the category work. We recommend using 3 terms minimum.

If during analysis of transmitted data, those terms are found, the System assigns the *Leaked code* category to the intercepted object.

Warning!

The interception object receives only the category that contains the actuated element (term, sample document, etc.).
For example:
Category A contains category B. Category B includes the term C. During the event analysis, the System detected the presence of the term C in the event body.
In this case, only the term C and category B will be assigned to the interception object.

Additional information:

Editing and deleting terms are performed by standard means:

- Editing Element;
- Deleting Element.

Managing Text Objects

Purposes:

1. Create a catalogue of text objects.
2. Create a text object and specify its value.
3. Add a system text object to the selected catalogue.

Solution:

1. Create a catalogue of text objects.

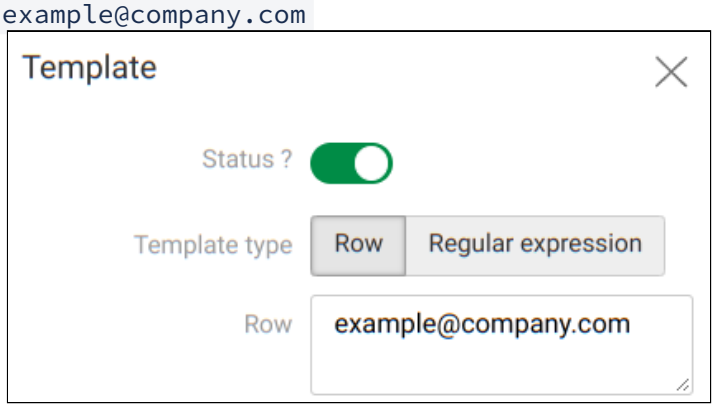
a. Go to the **Technologies** -> **Text objects** section.
b. On the toolbar on the left side of the workspace, click  **Create a catalogue of text objects**.
c. In the window that opens, type a name and description for the catalogue.
d. Click **Save**.

2. Create a text object and specify its value.

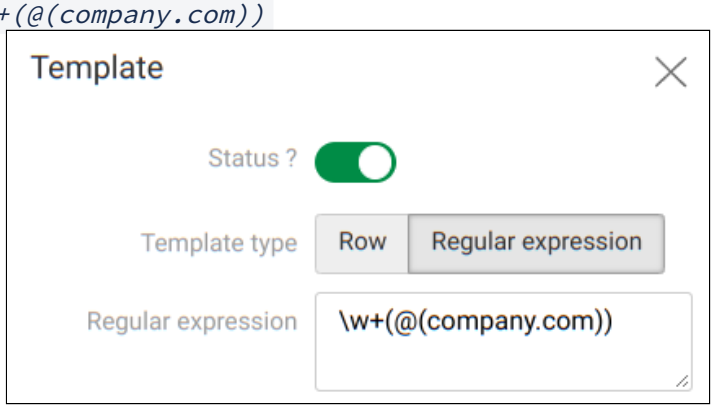
1. Go to the **Technologies** -> **Text objects** section.
2. On the left part of the workspace, select a catalogue to which you want to add a text object.
3. On the toolbar for working with text objects located on the right side of the workspace, click  **Create a text object**.
4. Enter the name and description of the text object.

5. Click **Create**. The new text object will be added to the list.
6. Select the text object in the list and click  **Edit**.
7. Create a template for the text object and specify its parameters (see "Text objects patterns").
8. Click **Save**.

- ***Example 1:***
  If you want the System to determine the presence of the email address "example@company.com" in traffic and define it as a text object EXAMPLE_MAIL, then:
  1. Create an active text object *EXAMPLE_MAIL*.
  2. Select the object and switch to the edit mode.
  3. Create a new active template for the text object and specify the following string as the template value: `example@company.com`



- ***Example 2:***
  If you want the System to determine the presence of email address with the domain “company.com” in traffic and define it as a text object *COMPANY_MAIL*, then:
  1. Create an active text object *COMPANY_MAIL.*
  2. Select the object and switch to the edit mode.
  3. Create a new active template for the text object and specify the following regular expression as its value: `\w+(@(company.com))`



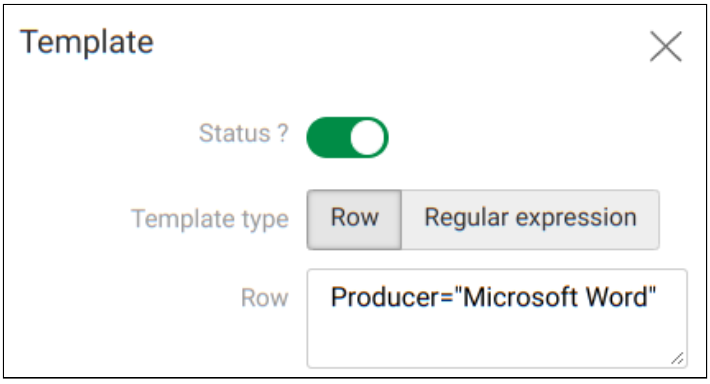
> **Note:**
>
> For more information on regular expressions, see the Knowledge Base articles: "Syntax of regular expressions" and "Description of macros for text object patterns".

- ***Example 3:***
  You want Device Monitor agent to block the transfer of a PDF file if the document has been converted to PDF format using Microsoft Word.

> **Note:**
>
> Device Monitor agent extracts information about document properties from PDF files. Property data is added to the end of the extracted text.
>
> **About extraction of PDF document properties**
>
> Names and values of the following PDF document properties are extracted:
>
> - Author
> - Title
> - Subject
> - Keywords
> - Creator (application, in which the original document was created)
> - Producer (application, in which the document was converted to PDF)
>
> Data about each document property is added to the end of the extracted text in the following format: *property name="property value"*. Data about property is added, if property value is specified. Each name-value pair is added on a new line:
>
> ```
> Author="John Green"
> Creator="Microsoft Word"
> Keywords="document; project; new"
> Producer="Microsoft Word"
> Subject="New Draft"
> Title="Project Draft"
> ```
>
> **Warning:** If the value of Keywords property has been deleted, the record with the last specified Keywords value will still be added to the end of the extracted text.

To define *Producer="Microsoft Word"* in the extracted PDF document properties as *PDF_PRODUCER* text object:

1. Create an active text object *PDF_PRODUCER*.
2. Select the object and switch to the edit mode.
3. Create a new active template for the text object and specify the following string as the template value: *Producer="Microsoft Word"*



4. Add PDF_PRODUCER text object to a protection object and create a data protection policy on agents (see "Creating a Protected Object" and "Creating Data Protection Policy on Agents").

3. Add a system text object to the catalogue.

a. Go to the **Technologies** -> **Text objects** section. On the left part of the workspace, left-click the target category.
b. On the left part of the workspace, select a catalogue to which you want to add a text object.
c. On the toolbar on the right side of the workspace, click  and in the drop-down list, select **Add system text object**.
d. In the window that opens, select check boxes next to the text objects you want to add.

> **Note:**
>
> To find required text objects in the list, enter the text in the **Search** field.

e. Click **Add**.

Additional information:
Text objects, their templates, and catalogues are edited and deleted by standard means:

- Editing Element;
- Deleting Element.

Managing Sample Documents

Purposes:

1. Create a catalogue of sample documents
2. Create a sample document inside the catalogue.
3. Update a sample document.

Solution:

1. Create a catalogue of sample documents

a. Go to the section **Technologies**->**Sample Documents**.
b. On the toolbar in the left part of the workspace click  **Create catalogue of sample documents** .
c. In the window that opens, specify parameters for the new catalogue (see "Sample Documents").
d. Click **Create**.

2. To create a sample document

a. Go to the section **Technologies**->**Sample Documents**.
b. On the left part of the workspace by clicking the left mouse button, select the catalogue inside which you want to create a sample document.
c. On the toolbar for working with sample documents located on the right side of the workspace, click  **Add**.
d. In the dialog window that opens, select type of the data a sample document may contain: **Text** or **All types** (may contain text, images, and binary data).

e. Click **Choose files** and in the window that opens, specify the document which you want to use for creating a digital print. Click **Open**.
   Choose a text file, an image or an archive to be uploaded according to the data type specified in step **d**. The following rules apply when uploading files:
   - If the format of the selected file is not supported by the System, the digital fingerprint will be uploaded as binary data.
   - If you upload an archive, then files from this archive will be added as sample documents.

f. When the uploading is finished, the sample document will be added to the catalogue. All necessary attributes are assigned to a newly created sample document by default.

> **Note:**
>
> If the System cannot load the file sample document, the download window will display an error message

> **Warning!**
>
> Requirements for file size:
>
> - Maximum size of binary data - 128 MB;
> - Maximum size of text data - 30 MB;
> - Minimal size of binary and text data – 128 bytes;
> - Minimal plain text size of text data - 10 characters;
> - Minimal image size - 100 pixels on one side;
> - Minimal size of vector data - 300 KB (about 800 primitives)
> - Permissible sides ratio - not bigger than 5 : 1.

g. To change the sample document attributes specified by the System, on the toolbar click **Edit** and change the required parameters (see “Sample Documents").

3 Update a sample document

a. Go to the section **Technologies**->**Sample Documents**.
b. On the left side of the workspace, select the desired catalogue.
c. In the list in right part of the workspace, select the sample document you want to update.
d. Click **Edit**.
e. In the edit window that opens, click **Update**.
f. Click **Choose file**.
g. In the dialog window that opens, select a document that will be used for update, and click **Open**.
h. The file download will begin.After the download is finished, the sample document will be supplemented with new data in accordance with the selected update mode. If the System cannot perform an update, the download window will display an error message.

> **Note:**

When updating a sample document, the System replaces data of the document being updated with the data from the update file.

Example 1:
If you need the System to react to transferring the "Internal regulations of the company" document if the traffic contains at least 30% of text from this document, then:

1. Select a catalogue of sample documents or create a new one.
2. Add a new document to this catalogue and specify the **Text** data type, as the document does not contain images or drawings.
3. Upload the "Internal rules of the company" file as a sample document.
4. Specify the sample document name, e.g., *INTERNAL_COMPANY_RULES.*
5. For the **Text data quotation threshold** attribute, specify the **30** value.

Note:

The quotation threshold is configured depending on the type of the protected document. Here, a low quotation threshold is specified, as the document consists of many pages and can be transferred in parts.

Example 2:
If you need the System to react to transferring the "Setup.exe" executable file if the traffic contains at least 10% of the binary content from this file, then:

1. Select a catalogue of sample documents or create a new one.
2. Add a new document to this catalogue and specify the **All data** type.
3. Upload the "Setup.exe" file as a sample document.
4. Specify the sample document name, e.g., *SETUP_EXE.*
5. For the **Text data quotation threshold** attribute, specify the **10** value.

For the System to track the presence of sample documents in the traffic, they must be included in protected objects.

Additional information:
Editing and deleting the sample documents and their catalogues are performed by standard means:

- Editing Element;
- Deleting Element.

Managing Blanks

Purpose:

1. Create a catalogue of blanks.
2. Create a blank.
3. Create a detection condition.
4. Update a blank.

Solution:

1. Create a catalogue of blanks

a. Go to the **Technologies**->**Blanks** section.

b. On the toolbar on the left part of the workspace, click  **Create a catalogue of blanks.**
c. In the window that opens, type a name and description of the catalogue.
d. Click **Create**.

2. Create a blank

a. Go to the **Technologies**->**Blanks** section.
b. On the left part of the workspace by clicking the left mouse button, select a catalogue inside which you want to create a blank.
c. On the toolbar for managing blanks which is located on the right part of the workspace, click  **Add**.
d. In the dialog window that opens, select a document that will be used as a blank and click **Open**. You can upload a document in one of the following formats: DOC, DOCX, DOT, DOTM, DOTX, XLS, XLSX, XLT, XLTM, XLTX, ODS, ODT, RTF, TXT, VSD, HTML, HTM, PDF, CHM.
e. When the download is finished, the blank will be added to the catalogue

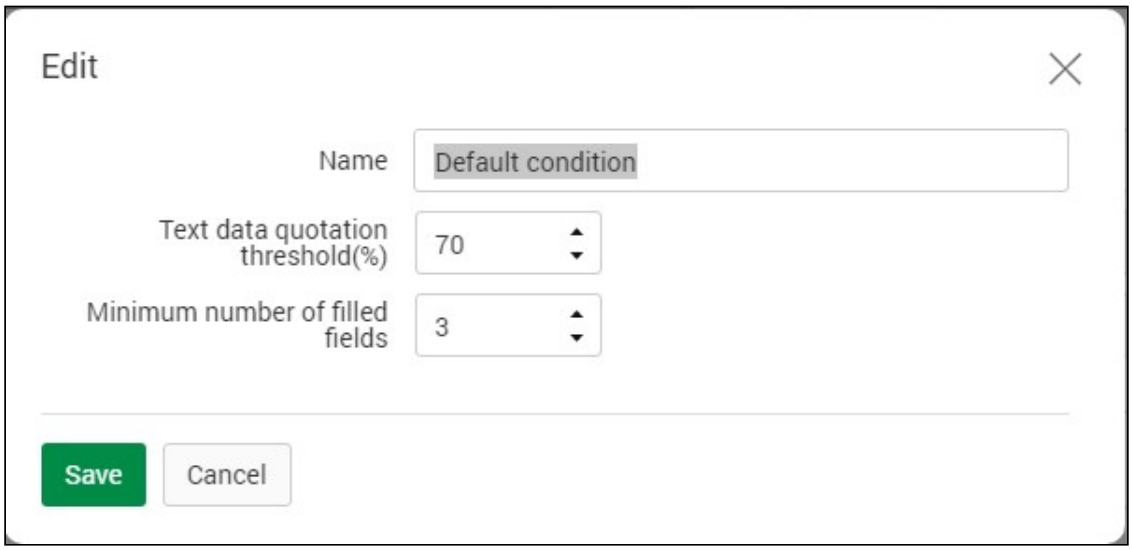
> **Note:**
>
> If the System cannot load the file of the blank, the download window will display an error message.

f. . All necessary attributes are assigned to a newly created blank by default.
g. To change attributes of the blank specified by the System, click  **Edit** on the toolbar and change required attributes (see “Blanks").

3. Create a detection condition

a. Go to the **Technologies**->**Blanks** section.
b. On the left side of the workspace, select the desired catalogue.
c. In the list on the right part of the workspace, select the blank you want the detection condition to be set.
d. Click  **Edit**.
e. On the right part of the workspace click  **Create**.
f. In the dialog window that opens, enter the name and specify the parameters of detection conditions:
Text data quotation threshold

Minimum number of filled fields



g. After data input click **Save**.
h. To add few detection conditions, repeat ection e-g.

> **Note:**
>
> It is recommended to create **no more than 20** detection conditions per one blank.

i. Click**Save**.

4. Update a blank

a. Go to the **Technologies**->**Blanks** section.
b. On the left side of the workspace, select the desired catalogue.
c. In the list on the right part of the workspace, select the blank you want to update.
d. Click **Edit**.
e. In the edit window that opens, click **Update**.
f. Click **Choose file**.
g. In the dialog window that opens, select a file that will be used for update, and click **Open**. The file download will begin.
h. Data of the blank will be replaced with data from the update file.
If the System cannot perform an update, the download window will display an error message.

Example:

If you need the System to mark the interception object as RECRUITMENT_CHECKLIST if the traffic contains fragments of the questionnaire "Recruitment checklist" (filled or not):

1. Create *RECRUITMENT_CHECKLIST* blank.
2. Load the document file “Recruitment checklist” as a blank.
3. Create a detection condition with **Minimum number of filled fields = 0**. Also you may edit the default condition which is created in accordance with the blank.
4. Create a protected object based on the *RECRUITMENT_CHECKLIST* blank and specify the detection condition you require.

Additional information:
Editing and deleting detection conditions, blanks and its catalogues are performed by standard means:

- Editing Element;
- Deleting Element.

Managing Stamps

Purposes:

1. Create a catalogue of stamps.
2. Create a stamp.

Solution:

1. Create a catalogue of stamps.

a. Go to the section **Technologies**->**Stamps**.
b. On the toolbar on the left side of the workspace, click  **Create a catalogue of stamps.**
c. In the window that opens, specify parameters for the new catalogue.
d. Click **Create**.

2. Create a stamp

a. Go to the section **Technologies**->**Stamps**.
b. On the left part of the workspace by clicking the left mouse button, select the catalogue inside which you want to create a stamp.
c. On the toolbar in the right part of the workspace, click  **Add**.

> **Warning!**
>
> The uploaded file must contain only one stamp image.

d. In the dialog window that opens, select a document that will be used as a stamp sample and click **Open**.
e. When the download is finished, the stamp will be added to the catalogue. All necessary attributes are assigned to a newly created stamp by default.

> **Note:**
>
> If the System cannot load the file of the stamp, the download window will display an error message.

f. To change the stamp attributes specified by the System, on the toolbar click  **Edit** and change the required attributes.

> **Note:**
>
> For more details on creating stamps, see the Knowledge Base article "Stamps".

Example:
If you need to protect legal documents sealed with a company stamp, then:

1. Prepare a file with the image of the company stamp.
2. In the **Technologies**->**Stamps** section, select the required catalogue or create a new one.
3. Create a new stamp in the catalogue and upload the prepared file with the stamp image.

For the stamp to be detected in intercepted data, it must be included in protected objects.

Additional information:
Editing and deleting stamps and their catalogues are performed by standard means:

- Editing Element;
- Deleting Element.

Managing DB Unloadings

Purpose:

1. Create a catalogue of unloadings.
2. Create a database unloading.
3. Update the unloading.
4. Move/copy the unloading

Solution:

1. Create a catalogue of unloadings

a. Go to the **Technologies**->**DB Unloadings** section.
b. On the toolbar on the left side of the workspace, click  **Create catalogue of DB unloadings**.
c. In the window that opens, type a name and description for the catalogue.
d. Press **Create**.

2. Create a database unloading

a. Go to the **Technologies**->**DB Unloadings** section.
b. In the left side of the workspace, select the group to which you want to add the unloading.
c. On the toolbar in the right part of the workspace, click  **Add**.
d. In the dialog window that opens, select a file in CSV or TSV format that you want to upload and press **Open**.

> **Note:**
>
> The uploaded file is then compiled. The amount of RAM consumed during compilation can be approximately calculated by the following formula:
>
> `Memory(GB) = 0.05 * unique_words(M) * cells(M)`, where M stands for million.
>
> For example, 10 million cells can fit in a table with 2 columns and 5 million rows, or in a table with 4 columns and 2.5 million rows.

> **Warning!**
>
> The unloading size should not exceed 300 MB.

e. When the file is uploaded, select the unloading you have created and click .
f. Specify required attributes (see “DB Unloadings" and "Detection Conditions for Unloading").
g. Press **Save**.

3. Update the unloading

1. Go to the **Technologies**->**DB Unloadings** section.
2. On the left side of the workspace, select the desired catalogue.
3. In the list in the right part of the workspace, select the unloading you want to update.
4. Click **Edit**.
5. In the edit window that opens, press **Update**.
6. Specify the desired update mode: **Adding new records** or **Removing old records and adding new ones**.
7. Press **Choose file**.
8. In the dialog window that opens, select a file that will be used for update, and press **Open**. The file download will begin.
9. After the download is finished, the unloading will be supplemented with new data in accordance with the selected update mode. If the System cannot perform an update, the download window will display an error message.

4. Move/copy the unloading

1. Go to the **Technologies**->**DB Unloadings** section.
2. On the left side of the workspace, select the catalogue in which the unloading is located.
3. Left-click on next to the unloading name and hold down while moving the unloading to the location of the catalogue to which you want to move/copy the uploading. Release the mouse button.
4. In the window that opens, press **Move** or **Copy**.
5. The unloading will be moved/copied to the catalogue.

> **Note:**
>
> If you edit or update the original unloading, all copies of that unloading will also be changed. If you edit or update a copy of an unloading, the original and all copies of that unloading will also be changed.

Additional information:
Editing and deleting unloadings and their catalogues are performed by standard means:

- Editing Element;
- Deleting Element.

Detection Conditions for Unloading

Reference information:

Satisfying the detection conditions allows the System to associate the interception object with a particular unloading.

When you create an unloading, a default detection condition is created with the following parameter values:

Parameter	Value
Condition name	Default condition
Detection condition	1+2+...+n, where n is the number of unloading columns
Minimal quantity of rows	10 **Note:** If an unloading contains less than 10 rows, the value of the parameter will be equal to the number of rows in the unloading.
Search type	All words in one cell in any order with any distance between

You can specify several (up to 20) detection conditions for the unloading. In this case, one satisfied condition is sufficient to associate the interception object with this unloading.

Purpose:

Add a detection condition for an unloading.

Solution:

1. Go to the **Technologies**->**Database Unloadings** section.
2. In the left part of the working area, select the desired catalog.
3. In the right part of the working area, select a desired unloading from the list and click **Edit**. The unloading edit form will open.
4. On the toolbar under the **Conditions of unloading detection** caption, click **Add**.
5. In the dialog window that opens, specify the following parameters (you can find a detailed description of these parameters below):
    a. **Condition name**;
    b. **Minimal quantity of rows**;
    c. **Search type;**
    d. **Detection condition**.
6. Click **Create**.

When editing detection condition parameters, consider the following recommendations:

Detection condition:
The detection condition contains column numbers and logical relations between them. If the analyzed interception object contains data from specified cells, given the set relations, then this row is considered triggered.

Warning!

To avoid false positives, the System uses stop-words: numbers, letters. and words, whose presence in cells results in not triggering these cells. You can find the whole list of stop-words in the InfoWatch Knowledge Base article " List of stop-words for database unloadings ".

The **Available columns in selection** list contains columns that can be used for creating conditions.
The **Search** field allows you to find a required column by its name.

Logical relations are defined using the following symbols:

1. "+" - conjunction of cells (logical "AND");
2. "|" - disjunction of cells (logical "OR");

   Note:

   A condition like (1|3) should be in parentheses

3. "()" - a grouping of conditions. For example, a condition like 1+(2|3) means that the row is considered to be triggered if its first cell and either its second or its third cell are triggered.
   A condition like (1|3)+(5|4) means that the row is considered to be triggered if both the first or the third cells and the fifth or the fourth cells are triggered.

   Warning!

   The "|" cannot be used to divide groups in parentheses. Thus, a condition like (1+8+11*)|(2+3*) should be specified as two separate conditions: 1+8+11* and 2+3*.

4. "*" - the asterisk symbol allows you to consider blank cells as well. For example, a condition like 1+2* means that the row is considered to be triggered if its first and second cells are triggered, wherein the second cell may be unfilled.

   Warning!

   The analysis technology does not consider special characters, so if the column contains an email address, then it is recommended that you should specify an additional column (e.g., Full name) in order to reduce false positives.

Minimal quantity of rows:
The minimal number of rows that must be detected to trigger the condition.

For example, if a condition like 1+(2|3) is specified and the minimal quantity of rows is set to 10, then for triggering the condition it is required that the analyzed text should contain at least 10 different rows that satisfy the condition 1+(2|3).

Search type:
The parameter defines the type of citation search. Available search types:

- All words in one cell in any order with any distance between
- All words in one cell following each other in any order

Warning!

The use of **All words in one cell following each other in any order** search type may reduce the speed of text analysis.

Note:

If **All words in one cell following each other in any order** search type is used, text analysis will be stopped in case the detection condition is satisfied. In the event text, only the text fragments that were detected before the condition was satisfied will be highlighted.

Example:
You need the System to mark the interception object as PHONE_NUMBERS when detecting 5 or more rows with filled columns 1 and 3 from the table with the following structure:

Full Name	City	Phone number
John Smith	London	+0 (012) 345-67-89
Tom Johns	Moscow	+0 (012) 345-67-88
William Williams	Los Angeles	+0 (012) 345-67-87
Jane Green	New York City	+0 (012) 345-67-86
Jillian Taylor	London	+0 (012) 345-67-85
Michael Davis	Dublin	+0 (012) 345-67-84

It is also necessary that the words from the cell follow each other in the text:

- The text "**John** Taylor, Tom **Smith**" should not be marked as containing the words from the cell "**Jonh Smith**";
- The text "**+0 (012) 345**-00-00, +0 (000) 000-**67-89**" should not be marked as containing the words from the cell "**+0 (012) 345-67-89**".

Note:

A word is defined as any sequence of letters or numbers.

To create a protected object according to the requirements above:

1. Save the table in CSV or TSV format and upload this file to the System.
2. Configure the detection condition:
    - in the **Detection condition** field, specify **1+3**
    - in the **Minimal quantity of rows** field, specify 5

- in the **Search type field**, choose **All words in one cell following each other in any order**

3. Create a protected object "PHONE_NUMBERS" based on the created DB unloading.

When detecting specified data columns in the transferred traffic, the protected object *PHONE_NUMBERS* is triggered in the System.

Additional information:
Editing and deleting detection conditions for the unloading are performed in a standard way:

- Editing Element
- Deleting Element

Managing Graphical Objects

To configure an automatic classifier of graphical objects:

1. Create a category of text objects:
   a. Go to the **Technologies**->**Graphical objects** section.
   b. On the toolbar in the left part of the working area, click .
   c. Specify the name and description of the new category.
   d. Click **Save**.
2. Upload images:
   a. In the left part of the working area, click the category to which you want to add images
   b. On the toolbar in the right part of the working area, click 
   c. Select one or more files on a disk and click **Open**. Choose files from which graphical data can be extracted.
   d. Make sure that the selected files have been successfully added to the category. A pop-up window on the right displays the process status.
3. Learn the classifier:
   a. Create at least two categories that contain one or more images.
   b. Click  and wait until the end of the learning process. The process can take several minutes. After the learning, there can be errors inn some categories. In this case, delete all images from such a category, add new images and learn the classifier again.
   c. In the upper part of the working area, click **Apply**.
   d. In the **Applying configuration** window, check out the new configuration and click **Apply**. The new configuration will become the active one on the server.

Note:

For the technology to work correctly, follow these recommendations:

- There should be a lot of images in the collection. Images should be divided into categories. Each category should include at least 50 images.
- Images in a category should not be of different subjects. Each category should only those images that are related to its subject
- The sizes of different categories should be close.
- Learning time and System performance depend on the number of uploaded images.
- The minimum image size is 150 pixels on one side.
- The maximum image resolution is 10,000 by 10,000 pixels.
- The maximum image aspect ratio is 8:1.

- Allowed image rotation is 90+-10, 180+-10, 270+-10 degrees.
- Supported image types: `bmp, gif, jpeg, jp2, pbm, pgm, png, ppm, ras, tiff`. Herewith:
  - If the file is an unencrypted archive, then a separate document is created from each file. All created documents are placed to the category that was selected when creating the document.
  - If the file is an encrypted archive, the document is not created or is created with an error.

To improve detection accuracy of documents from one category, learn the classificator using this and other categories. Those images that do not refer to any category but cause false positive responses, should be transferred to *Decrease false positives* category. The category balances all others, which improves the quality of technology's work.

To check individual files with the already learned classifier:

1. In the left part of the working area, click .
2. Click **Start new check**.
3. Select one or more files and click **Open**. Do not select archives to be checked.
4. Wait until the check is complete and read the results. The classifier will detect categories of graphical objects to which the images belong. You can add these images to specified categories and learn the classifier anew.

Note!

Images check to match any graphical object is run only for the graphical objects which can be edited. For more details, please see "Graphical Objects").

If you are not satisfied with the results of document processing (for example: for some files, categories are not defined; not all images are detected by the classifier or they are detected incorrectly), upload additional files to the category or delete earlier added files. Then learn the classifier anew.

Managing Autolinguist

To make classifier specify correctly the document's category membership, make it configure and learn.

To configure Autolinguist:

1. Create category in Autolinguist:
   a. Go to **Technologies** -> **Autolinguist**.
   b. On the tools panel on the left of the working area, click .
   c. In the opened window enter the name and description of the new category.
   d. Click **Save**.
2. Load a standard document to category:
   a. Go to **Technologies** -> **Autolinguist**.
   b. On the left of the working area left click on the category to which the document is to be loaded.

Note:

You can load a file of any format detectable by the System and containing any data it can extract. Herewith there are some restrictions:

- In case of unencrypted archive a separate document will be created for each file extracted from it. However there will be no document created for the whole archive. Created documents will be added to the category, selected at the moment of the document creation.

- If a file is an encrypted archive, then the document will not be created or will be created with error.

- One document will be created for a file of *Container* type.

c. On the tools panel on the right of the working area click .
d. In the opened window select one or several files and click **Open**. Use the documents from which some text data can be extracted.
e. Make sure the file you selected was added to the category. You can see the process status in a pop-up box on the right.

3. Learn the technology on the new collection:
   a. Create at least two categories containing one or several standard documents.
   b. Click  and wait till the end of the process. It may take a few minutes. After the learning ends, some categories may contain errors. In this case we recommend to remove all documents from the category, then add new ones and learn the technology again. The results of learning are displayed via categories and the whole collection quality indicators in per cent.
   c. On the top of the working area click **Apply**.
   d. In **Apply configuration** window click **Apply**. New configuration will be activated on server.

Note:

The number of documents and its contents influence the quality of technology learning. The more documents with the same topic are in the category, the more accurate Autolinguist function is.

Recommendations for correct work of the technology:

- You need to create at least two categories, each category should contain minimum one document.
- Text in the document should contain minimum 5 words, each word should contain at least 3 symbols.
- The time needed for thechnology to learn and its productivity depend on number of documents you load, so the process may take several minutes.

You can check the function of Autolinguist learning. To do this, upload a document to make the classifier specify its membership to a category.

To check certain files in the technology after learning:

1. Click  **Check document.**
2. In the window click **Start new check**.
3. Select one or several files and click **Open**. The size of a file should be from 256 bytes up to 26 MB.
4. Wait till the end of the process and then view the results.

5. Apply the new configuration. The technology will define to which categories the text objects of loaded documents relate. You can add these documents to those categories and initiate the learning process again.

If the results of documents processing are not satisfactory (for example, there are files with non defined category, not all the documents are detected or not they are not detected correctly), then load some additional files to the category or remove from it the files you loaded before, and then learn the technology again.

4.4.2 Exporting and Importing the Base of Technologies

Purpose:

- Save the archive containing the base of technologies to a hard drive of the computer;
- Load the base of technologies, which is stored on your computer as an archive with `.cfb` extension, for using in the InfoWatch Traffic Monitor management console.

> **Note:**
>
> You cannot export the base of technologies, if the System configuration is being edited. You cannot import the base of technologies, if the System configuration has not been applied. Otherwise, you will receive an error message.

To export the base of technologies:

1. Go to a subsection of the **Technologies** section (**Categories and terms**, **Text objects**, **Sample Documents**, **Blanks**, **Stamps**, **Database Unloadings**, or **Graphical Objects**).
2. On the toolbar on the left part of the workspace, click  and, in the drop-down list, select **Export**.
3. Preparing the base of technologies export will start. After the preparation is finished, an archive with `.cfb` extension will be loaded to your computer `.` This file contains the following elements:
   - categories and terms;
   - text objects, including pre-installed ones;
   - sample documents;
   - blanks;
   - stamps;
   - database unloadings;
   - graphical objects.
4. The structure of catalogues is preserved for all elements.

> **Warning!**
>
> As a result, the whole base of technologies will be exported, not a selected section only.
>
> The base of technologies from the last applied configuration is exported (see “Configuring the System").

To import the base of technologies which is stored on your computer as an archive with `.cfb` extension:

1. Go to a subsection of the **Technologies** section (**Categories and terms**, **Text objects**, **Sample Documents**, **Blanks**, **Stamps**, **Database Unloadings** , or **Graphical Objects**) .
2. On the toolbar on the left part of the workspace, click  and in the drop-down list select **Import**.
3. In the **Open** dialog window, select an archive with `.cfb` extension that you want to upload.
4. Click **Open** and wait till the data is loaded into the System.

> **Note:**
>
> If the catalogue name in the import file matches the catalogue name in the System, but paths to a catalogue differ, then the catalogue from the import file will not be added. If the catalogue name in the import file matches the catalogue name in the System, and paths to catalogue also match, then data from the import file will be merged with the data in the System.

Features of merging data during import:

1. For catalogues, the following items missing in the System are added:
   a) child catalogues;
   b) elements of technologies.
2. For category, the terms that are missing in the System will be added.
3. For text object, templates that are missing in the System will be added.

   > **Note:**
   >
   > The verifying functions that are present in the System will be replaced by functions from the file.

4. To add sectoral and customized categories and terms into the System, you should use XML files that are compatible with InfoWatch Traffic Monitor System. After this XML file has been uploaded into the System, all appropriate categories and terms are to be automatically added to the System's management console, **Technologies** section (**Categories and terms**, **Text objects**, **Sample Documents**, **Blanks**, **Stamps**, **Database Unloadings, or Graphical Objects**).

   > **Note:**
   >
   > Sectoral and customized categories and terms used for InfoWatch Traffic Monitor are unique and they cannot be imported to other DLP systems at present.

5. For a DB unloading, representations of the sample unloading will be added, if the contents of unloading in the System and the file are the same.

   > **Warning!**
   >
   > Unloadings created in Traffic Monitor with a version lower than 7.4 are considered obsolete.
   >
   > Obsolete unloadings are marked with .

An obsolete unloading cannot be edited and updated. It is recommended to delete it and create the unloading again.

4.5 Managing Protected Objects

Warning!

For the changes described in this section to be used in the System, apply the configuration: see "Configuring the System" and "Applying System Configuration".

What are protected objects needed for:

Protected objects make it possible to check if intercepted data contain all specified elements of analysis: for example, a sample document, a text object, and a database unloading. You can also specify the elements, detection of which means for the System not to detect protected objects. Thus, you can configure the System so that it could detect or ignore certain business documents: for example, a vehicle registration certificate or a declaration of insurance payment.

Working with protected objects includes the following actions:

Action	Description
Creating a Catalogue of Protected Objects	Creating a catalogue to which protected objects will be added
Creating a Protected Object	Creating a protected object and specifying its parameters
Adding Elements of Technologies	Adding elements of analysis to a protected object
Adding Detection Conditions	Specifying conditions for detecting added elements of analysis
Creating Policies for Protected Objects and Their Catalogues	Creating a data protection policy for selected protected objects and their catalogues
Importing and Exporting Protected Objects	Importing and exporting catalogue structure, protected objects included in these catalogues and elements of analysis used in these protected objects
Activating and Deactivating Protected Objects	Changing status of protected objects and their catalogues

See also:

- "Protected Objects Section" - on the section where you can manage protected objects

4.5.1 Creating a Catalogue of Protected Objects

Purpose:
Create a catalogue that will contain protected objects.

Solution:

1. Go to the **Protected objects** section.
2. On the toolbar in the left part of the workspace, click  **Create catalogue of protected objects**.

   > **Note:**
   >
   > You can create a new catalogue of protected objects inside an existing catalogue. To do this, select the target catalogue in the list.

3. In the dialog box that appears, specify the catalogue attributes.
4. Click **Create**.

You can move the selected catalogue using drag and drop. To do this, select the catalogue in the list, press the left mouse button and move the catalogue to the desired location in the catalogue structure holding the left mouse button pressed. Then release the mouse button.

> **Note:**
>
> The catalogue will be moved with all nested elements including subcatalogues and protected objects. When you move a catalogue, its status changes to the status of the catalogue to which you are moving it.

Additional information:

Editing and deleting catalogues of protected objects are performed by standard means:

- Editing Element;
- Deleting Element.

4.5.2 Creating a Protected Object

Purpose:
Create a protected object based on elements of technologies that are present in the System.

Solution:

1. Go to the **Protected objects** section.
2. On the left side of the workspace, select a catalogue to which you want to add a new protected object, or create a new catalogue (see "Creating a Catalogue of Protected Objects").
3. On the toolbar in the right part of the workspace, click  **Create Protected Object**.
4. In the window that opens, select elements based on which the protected object will be created (see "Adding Elements of Technologies").
5. Determine whether selected items should be included in one protected object, or a separate protected object should be created for each element:

- If **Create a protected object for each selected item** option is selected, a set of protected objects for each selected element of technologies will be created. Attributes of the created protected objects are generated automatically. Object names are generated based on the name technology and the element name, for example: "*Text object: Credit card number*".
- If **Create a protected object for each selected item** option is not selected, then clicking **Create** opens an additional window where you can specify settings for the protected object: see step 7.

6. Click **Create**.
7. If **Create a protected object for each selected item** option has not been selected at step 5, the **Creating a protected object** window will open. In this window:
   a. Enter the name of protected object.
   b. On the **Elements of technologies** tab, that contains the selected items (see "Elements of Technologies"), you can add additional elements of technologies (for this, click **Select elements**) or remove elements from the list: for this, click ' x ' button in the row of the selected element.
   c. On the **Detection conditions** tab, specify conditions under which protected objects should be detected in intercepted data (for details, see "Adding Detection Conditions").
   d. If necessary, enter a description in the **Description** field.
   e. Click **Create**.

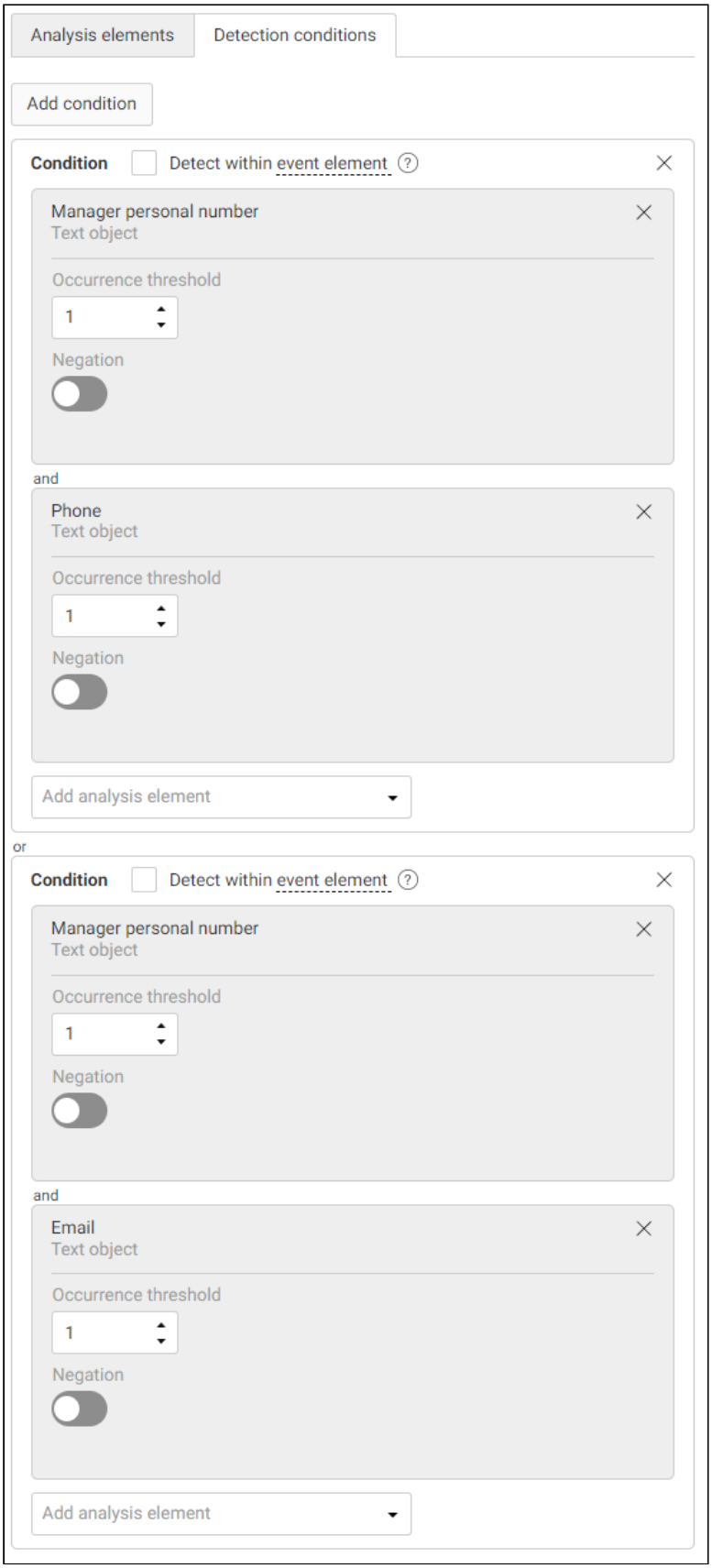
As a result, a protected object is created in the selected catalogue (if you have selected the **Create a protected object for each selected item** option, several protected objects are created).
You can move the created protected object to another catalogue.
To do this, select the required protected object in the list, press the left mouse button and move the protected object to the desired catalogue holding the left mouse button pressed. Then release the mouse button.

Example 1:
If you need to create a protected object *"Manager Personal Number"* that should be detected in the System when one of the following conditions is fulfilled:

- the interception object contains a personal number of the manager and an email;
- the interception object contains a personal number of the manager and a phone number.

Then:

1. Create a new protected object and add the following elements of technologies:
   - a text object *"Manager Personal Number"*
   - a text object *"E-mail"*
   - a text object *"Phone"*
2. Specify the following detection conditions for the elements of technologies:

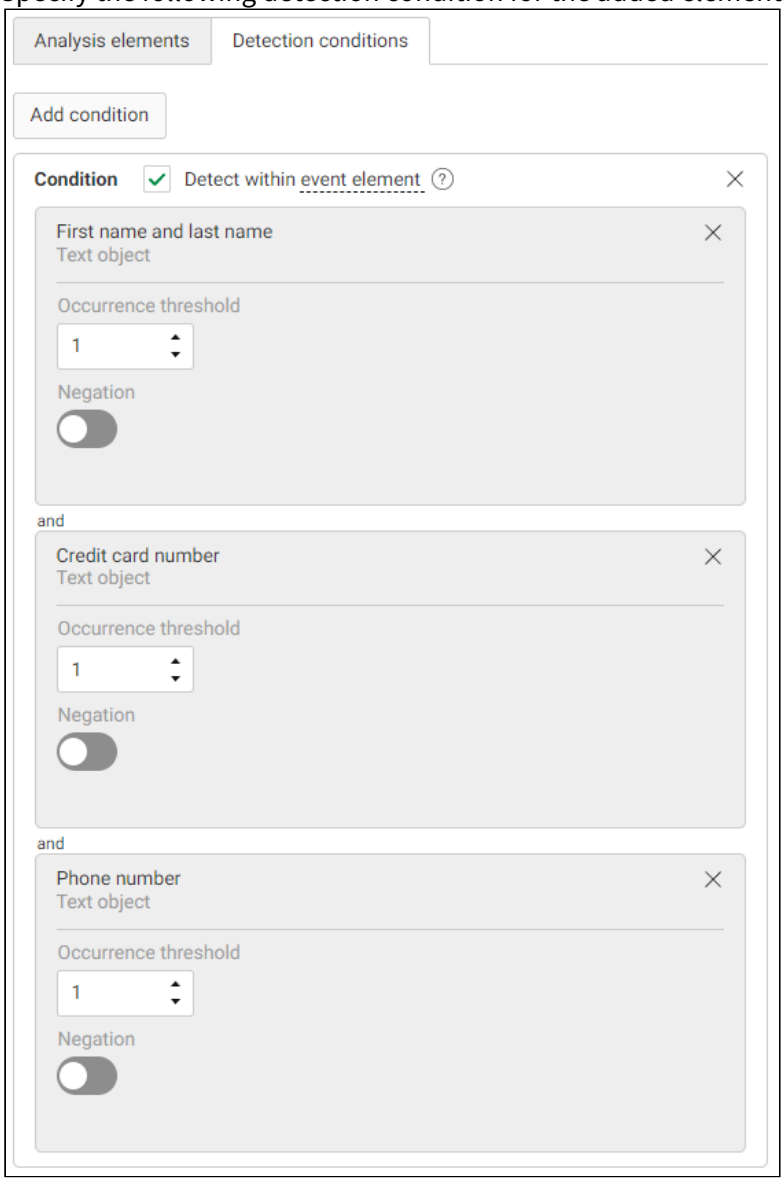


Example 2:
If you need to create a protected object that should be detected in the System when the following condition is

fulfilled: intercepted object within one element of event contains first and last name, phone and credit card number.

Then:

1. Create protected object and add elements of technologies to it:
    - text object *"First and last name"*;
    - text object *"Phone number"*;
    - text object *"Credit card number"*.
2. Specify the following detection condition for the added elements of tecnologies:



Pay attention that to complete the condition you must enable the function **Detect within event element**. In this case the System will detect the protected object if all protected data is detected in one element, for example in email body or attached file.

Example 3:

If you need to create a protected object that should be detected in the System when one of the following conditions is fulfilled:

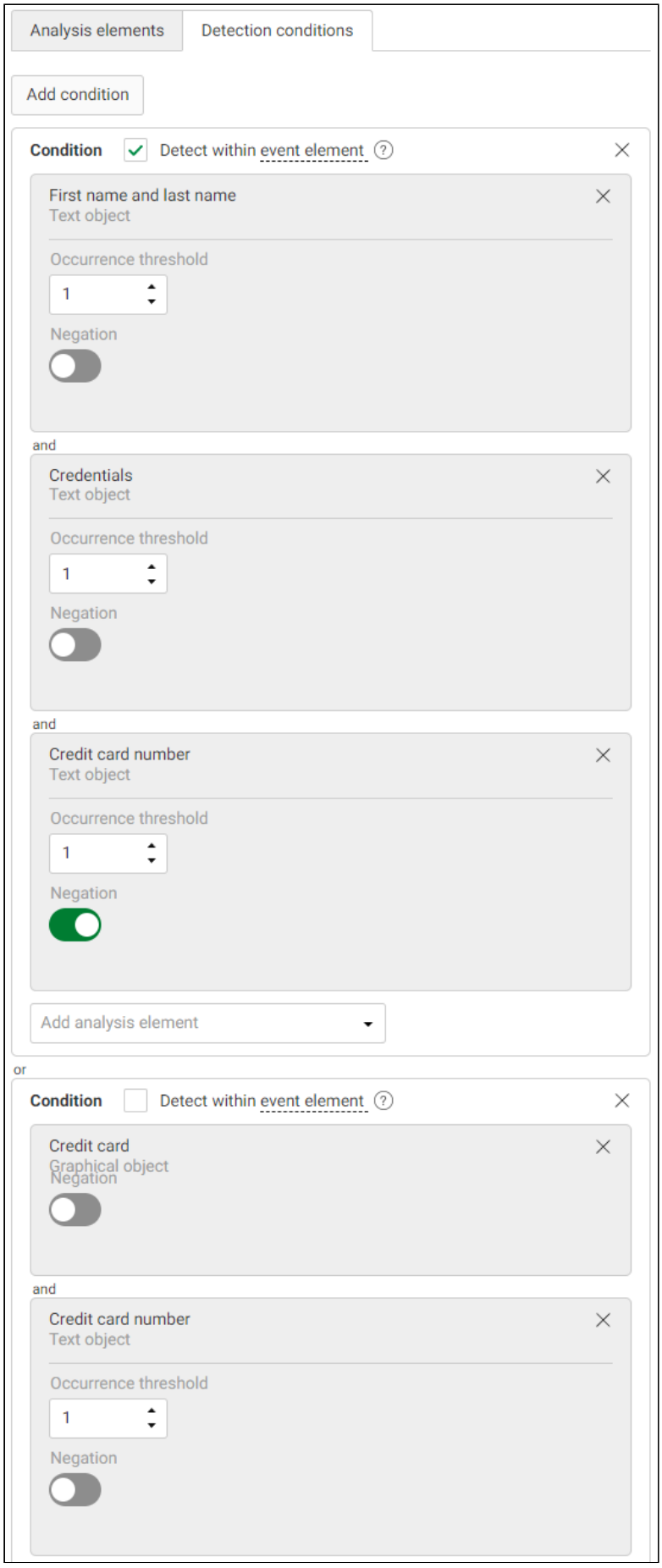
- detected object for one element of event contains first and last name, account data, but must not contain a credit card number;

- detected object contains a credit card number and its image.

Then:

1. Create a protection object and add elements of technologies to it:
    - text object *"First name and last name"*;
    - text object *"Account data"*;
    - *text object "Credit card number"*;
    - graphical object "*Credit card*".

2. Specify the following conditions of detection for added elements of technologies:


Analysis elements
Detection conditions
Add condition
Condition
Detect within event element
First name and last name
Text object
Occurrence threshold
1
Negation
and
Credentials
Text object
Occurrence threshold
1
Negation
and
Credit card number
Text object
Occurrence threshold
1
Negation
Add analysis element
or
Condition
Detect within event element
Credit card
Graphical object
Negation
and
Credit card number
Text object
Occurrence threshold
1
Negation

Pay attention that to complete the first condition you must enable the function **Detect within event element** and enable **Negation** for the element of technologies the presence of which cancels detection.
In this case protected object will be detected by the System by the first condition only if one element of event contains all elements of technologies without negation, and element containing negation **must not** be there.
If in one element of event all listed text objects are detected, protected object will not be detected by the System by the first condition. But if in the protected object a specified graphic object will also be detected, the System detects a protected object by the second condition. Negation from the first condition does not interfere detection by second condition.

Additional information:

Protected objects can be edited and deleted by standard means:

- Editing Element
- Deleting Element

4.5.3 Adding Elements of Technologies

Purpose:
Add elements of technologies to a protected object.

Solution:

You can add elements of technologies when creating a new protected object or when editing an earlier created protected object (see "Creating Protected Objects").

If you are creating a new protected object:

1. In the **Create Protected Object** window, open a tab with desired elements.
2. From the list of available elements, select elements, you want to add.

> **Note:**
>
> When you select a category that contains subcategories (the **Category** tab), all subcategories will also be selected. If you want to add particular subcategories, click on the arrow to the left of the category name, and, from the drop-down list, select check boxes in required fields.
>
> This can be used when selecting catalogues and sub-catalogues.
>
> Adding catalogue as protected object is possible for sample documents, stamps, text objects, blanks and DB unloadings.
>
> When adding a catalogue to protected objects, all elements of technologies which are a part of the catalogue will be included as well.
>
> If new elements of technologies will be added after the protected object was created within the working catalogue, they will also let detecting the protected object within the intercepted traffic.
>
> If you delete elements of technologies from the catalogue that was added into protected object the detection by deleted elements will be finished.

3. To create a protected object based on several technologies, repeat steps 1-2 until you add all desired elements.
4. Click **Create**.

> **Note:**
>
> If the **Create a protected object for each selected item** option is selected, then, for each element of analysis, a separate protected object is created. Attributes of the protected object are set by the System automatically.

If you are editing an earlier created protected object:

1. In the **Edit Protected Object** window, click **Select elements**.
2. In the **Select elements of technologies** window that opens, open a tab with desired elements.
3. From the list of available elements, select elements you want to add.

> **Note:**
>
> If the protected object is included in a data protection policy on agents (see "Creating Data Protection Policy on Agents"), then you can only add categories and text objects to this protected object.

4. Click **Save**.

You can delete elements or technologies catalogues, added earlier. For this, on the **Elements of technologies** tab, click on the cross to the opposite of the desired element.

4.5.4 Adding Detection Conditions

Reference information:

A protected object can be detected in the event if:

1. The protected object status is **Active**.
2. The event contains elements of technologies included in the protected object with respect to specified detection conditions.

A catalogue of protected objects will be detected in the event if:

1. A status of the catalogue of protected objects is **Active**.
2. The event contains at least one protected object from the catalogue.

> **Note:**
>
> When exporting a protected object (see "Importing and Exporting Protected Objects"), the protected object includes only those elements of technologies for which detection conditions are specified.

Purpose:

Add detection conditions for a protected object.

Solution:

Detection conditions are added when creating protected objects. After you add selected elements of technologies to the protected object (see "Adding Elements of Technologies"), you need to specify detection conditions.

> **Note:**
>
> You can also add detection conditions when editing an earlier created protected object.

To add detection conditions for a protected object:

1. On the **Detection Conditions** tab, in the **Add element of technologies** field, click and, in the drop-down list, select the desired element.
2. The selected element will be added to the list of conditions. For some elements of technologies, you can specify additional detection conditions (see "Detection conditions").
3. If there are several elements of technologies in the protected object, you can add detection conditions for the other elements in one of the following ways:
   - If you need conditions to be combined with a conjunction (logical "AND"), add conditions as described in step 1.
     In this case, all added conditions will be placed in the same **Condition** block and combined with a conjunction.
   - If you need conditions (or groups of conditions) to be combined with a disjunction (logical “OR"), click the **Add condition** button.
     A new **Condition** block will be added. In this block, you can add conditions as described in step 1.
     In this case, all the **Condition** blocks will be combined with each other with a disjunction, and conditions within a single block will be combined with a conjunction.
   - If you need the System to detect protected object if the condition is complete within one element of event (email body, file, communication in messenger), click the **Detect within event element** button.
   - If you need the System **not** to detect protected object when the specified element of technology is detected, then you should enable **Negation** for this element.

     > **Note:**
     >
     > At least one element without negation is required in the detection condition.
     >
     > If protected object is added to the policy of data protection on agents, you cannot enable negation and detection within event element.

4. Click **Create** if you are in the create mode, or **Save** if you are in the edit mode.

Additional information:

If you need to delete conditions, do either of the following:

- to delete a single condition, click X in the upper right corner of the panel with the required condition;
- to delete a block that contains conditions, click X in the upper right corner of the block.

4.5.5 Creating Policies for Protected Objects and Their Catalogues

Purpose:

Create a policy for protected objects and their catalogues directly from the "Protected objects" section.

To create a policy for a catalogue of protected objects:

1. Go to the **Protected objects** section.
2. In the **Catalogues of protected objects** list on the left side of the workspace, select the desired catalogue.
3. On the toolbar in the left part of the workspace, click and, in the drop-down list, select one of the following items:
   - **Create data protection policy**
   - **Create policy on agent**

   > **Note:**
   >
   > For policies on agents in the selected catalogues only the protected objects with disabled negation and detection within event element will work.

4. In the policy creation form that opens, specify the required settings (for more information, see "Policies Section").
5. Click **Save**.

The created policy will be triggered when detecting at least one protected object from the selected catalogue.

To create a policy for selected protected objects:

1. Go to the **Protected objects** section.
2. In the **Catalogues of protected objects** list in the left part of the workspace, select the desired catalogue.
3. In the right part of the workspace, a list of protected objects included in the selected catalogue will be displayed. Left-click the desired protected object. To select multiple objects, use the Shift or Ctrl key.
4. On the toolbar in the right part of the workspace, click and, in the drop-down list, select one of the following items:
   - **Create data protection policy**
   - **Create policy on agent**

   > **Note:**
   >
   > If negation and detection within event element is enabled for protected object, it cannot be added to data protection policy on agents.

5. In the policy creation form that opens, specify the required settings (for more information, see "Policies Section").
6. Click **Save**.

The created policy will be triggered when detecting at least one of the selected protected objects.

4.5.6 Importing and Exporting Protected Objects

Purpose:

- export to a file catalogue structure containing protected objects and elements of technologies used in them;

- load from file an earlier created catalogue structure containing protected objects and elements of technologies used in them.

> **Note:**
>
> You cannot export protected objects, if the System configuration is being edited. You cannot import protected objects, if the System configuration has not been applied. Otherwise, you will receive an error message.

To export protected objects:

1. Go to the section **Protected objects** and select a catalogue.
2. On the toolbar in the left part of the workspace, click  and in the drop-down list select **Export**.
3. Preparing the loading will start; then the archive will be saved on the computer.

The saved archive contains XML files that store information about the protected objects and their elements of technologies. The structure of catalogues and elements of technologies is preserved when exporting.

> **Note:**
>
> When exporting protected objects, beware that the order of elements of technologies in detection condition will not be kept. Therefore, if you import those protected objects later, note that the order of elements of technologies may differ from the order at the moment of the protected objects export.

To import protected objects:

1. Go to the section **Protected objects**.
2. On the toolbar in the left part of the workspace, click  and in the drop-down list select **Import**.
3. In the window that opens, select a previously exported file that you want to upload.
4. Wait till the protected objects are loaded into the System.

> **Note:**
>
> If the catalogue name in the import file matches the catalogue name in the System, but paths to a catalogue differ, then the catalogue from the import file will not be added. If the catalogue name in the import file matches the catalogue name in the System, and paths to catalogue also match, then data from the import file will be merged with the data containing in the System.

Features of merging data when importing:

1. For catalogues, the following items missing in the System are added:
   a) child catalogues of protected objects;
   b) protected objects.
2. For protected objects, the following items missing in the System are added:
   a) elements of technologies;

Warning!

Unloading created in Traffic Monitor with a version lower than 7.4 are considered obsolete.

Obsolete unloadings are marked with .

An obsolete unloading cannot be edited and updated. It is recommended to delete it, create the unloading again and then add it to protected object.

b) detection conditions.

3. For detection conditions, new nested conditions, including detecting parameters (for text objects, blanks and database unloadings) will be added.

4.5.7 Activating and Deactivating Protected Objects

By default, the status of all created protected objects and their catalogs is *Active* ( icon). If necessary, you can deactivate a created catalog of protected objects or a particular protected object in the catalog.

To deactivate a catalog of protected objects:

1. On the toolbar in the left part of the workspace, click and, in the drop-down list, select **Deactivate**.
2. The catalog status will change to *Inactive* ( icon).

If you need to reactivate a deactivated catalog, click and, in the drop-down list, select **Activate**.

To deactivate a selected protected object:

1. On the left part of the workspace, select the desired catalog.
2. On the left part of the workspace, left-click the desired protected object in the list.
3. On the toolbar in the right part of the workspace, click and, in the drop-down list, select **Deactivate**.
4. The status of the protected object will change to *Inactive* ( icon).

If you need to reactivate a deactivated protected object, click and, in the drop-down list, select **Activate**.

Note:

If a protected object is selected as a result of end-to-end catalogue search, you cannot change its status when editing it or using **Activate**/**Deactivate** buttons. To change the protected object status, choose it in the catalogue.

This limitation is due to the fact that a protected object can belong to different catalogues including inactive ones.

Warning!

Protected objects and their catalogs can be detected in intercepted data only if they are active.

4.6 Managing Interception Objects

Why do you need objects of interception?

- track the statistics on violations of the corporate security policy;
- view information on a particular object;
- display interception objects by specified criteria.

To perform daily monitoring or to get statistics promptly, we recommend using widgets in the Dashboard section .

If you need to view a large number of events over a period, you can create a query in the Events section.

Working with interception objects includes the following actions:

Action	Description
Viewing Summary on Violations/Violators	Viewing statistical information and selections on events
Viewing Events	Viewing data on every interception object
Creating Dashboard Report	Generating summary on violations/violators
Viewing Dashboard Report	Viewing generated summaries
Making Decision on Object	Making user decision concerning the object
Adding and Delete Tags	Adding a tag to the event
Saving Events (for SMTP mail)	Saving the event to the disk in EML format
Event Export	Saving information on events to the computer hard drive
Dispatching Blocked Event	Sending a blocked message to the recipient
Creating Queries	Filtering interception object by specified criteria

See also:

- "Events Section" - on the section, where you can search for interception objects
- "Dashboard Section" - on the section, where you can view statistics on interception objects

4.6.1 Viewing Summary on Violations/Violators

The operation is performed in the **Dashboard** section (see "Dashboard Section")

Purpose:
View a summary on violations/violators.

Solution:

1. Go to the **Dashboard** section.
2. Configure a dashboard where widgets will be added (see “Creating a Dashboard").
3. Add and configure the desired widget (see "Creating and Configuring Widget").
4. Examine the summary in the widget.

You can export a report with the summary as PDF or HTML page (see "Creating Dashboard Report").

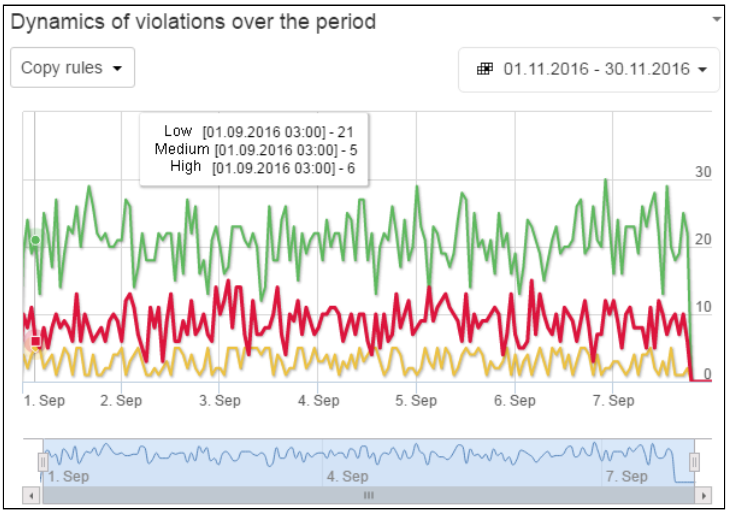
All generated reports are stored in the System. You can view the required report or delete reports which you do not need to store (see "Viewing Dashboard Report").

Example 1:
It is required to track dynamics of copying files which contain confidential data (see the list of actions that are considered data copying in "Rule of Copying").

For this:

1. Create a new dashboard or open an earlier created one.
2. Add "Dynamics of violations over the period" widget (for details on configuring this widget, see "Dynamics of Violations over the Period").
3. In the right upper corner of the widget, choose *Current month* as a period.
4. In the left upper corner of the widget, choose *Copy rules* from the list of rules.

The widget will display charts that show the dynamics of violating copy rules for the current month.



To view events for a particular date and hour, click the point where the timeline intersects the violation number curve.

Example 2:
It is required to display all interception objects for the current week where John Smith is either a sender or a recipient (it is supposed that John Smith person has already been created in the **Persons** section).

For this:

1. Create a new dashboard or open an earlier created one.
2. Add "Selection" widget (for details on configuring this widget, see "Selection").
3. Switch to the widget edit mode and for the Selection parameter, specify an earlier created *Smith* query (see Example 2 in "Examples of Using Queries").
4. Save the widget.

.

Creating Dashboard

Purpose:
Create a dashboard that will contain widgets.

Solution:

1. Go to the **Dashboard** section.
2. In the left part of the workspace, click  **Add**.
3. Specify the name of a new dashboard.
4. Click **Save**.

Additional information:

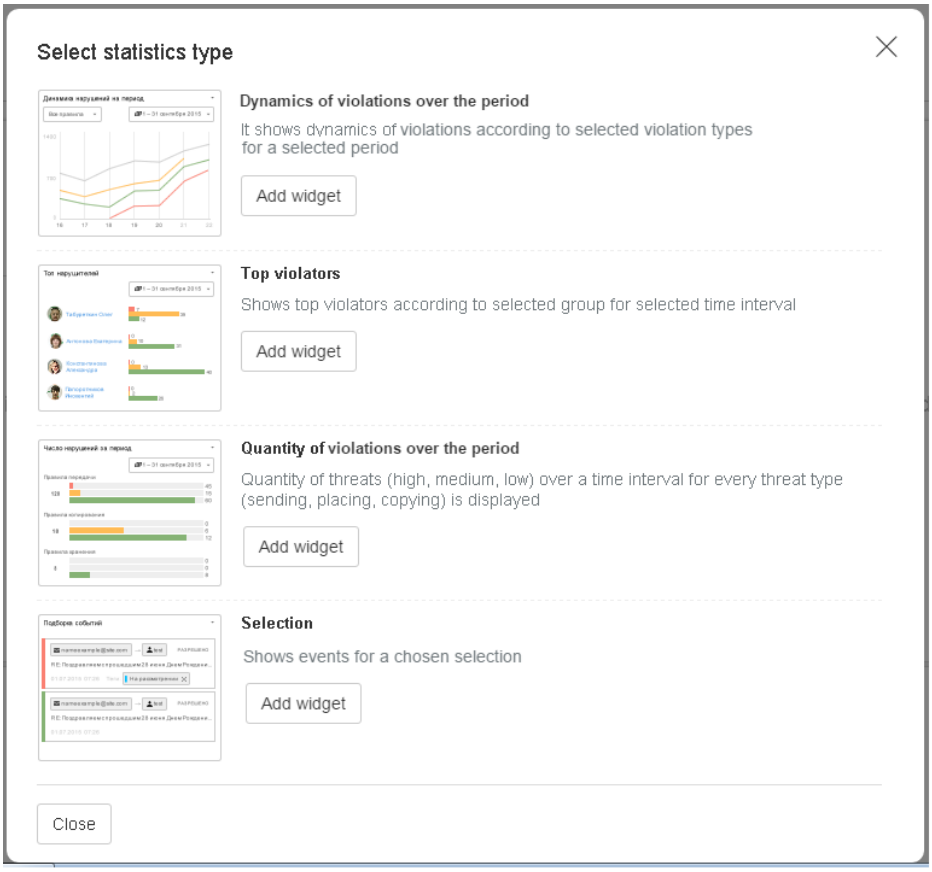
- Filling a dashboard is described in "Creating and Configuring Widget".
- To delete a dashboard, go the dashboard which you want to delete and, on the tab with its name, click . In the confirmation window, click **Delete**.

Creating and Configuring Widget

Purpose:
Create a widget in the dashboard pane.

Solution:

1. Go to the **Dashboard** section.
2. Select the dashboard, to which you want to add a widget, or create a new dashboard (see "Creating Dashboard").
3. Click **Add widget**.
4. In the **Select statistics type** window that opens, select the desired widget and click **Add widget** under its description (for details on widget types, see "Dashboard Widgets").



Note:

You can add several widgets in succession. To do this, click **Add widget** under other widgets you want to add: selected widgets will be added to the dashboard.

Tip

You can add multiple widgets of the same type, and then configure them to display different types of data: for example, several widgets of **Summary** type to display events based on results of queries (for details on queries, see "Creating Queries").

5. Click **Close** or use ✕ button in the upper right corner of the window.
6. Configure added widgets to display required data (parameters of different widgets are listed in the "Dashboard Widgets" subsection).

Additional information:

1. You can move widget tiles to place them in a convenient order. To do this:
   a) Hover the mouse pointer over the tile header so that a standard cursor changed to a four-way arrow key.
   b) Hold down the left mouse button and, keeping it pressed, move the tile over the workspace until the target position of the tile is displayed as a dotted line.
   c) Release the left mouse button.

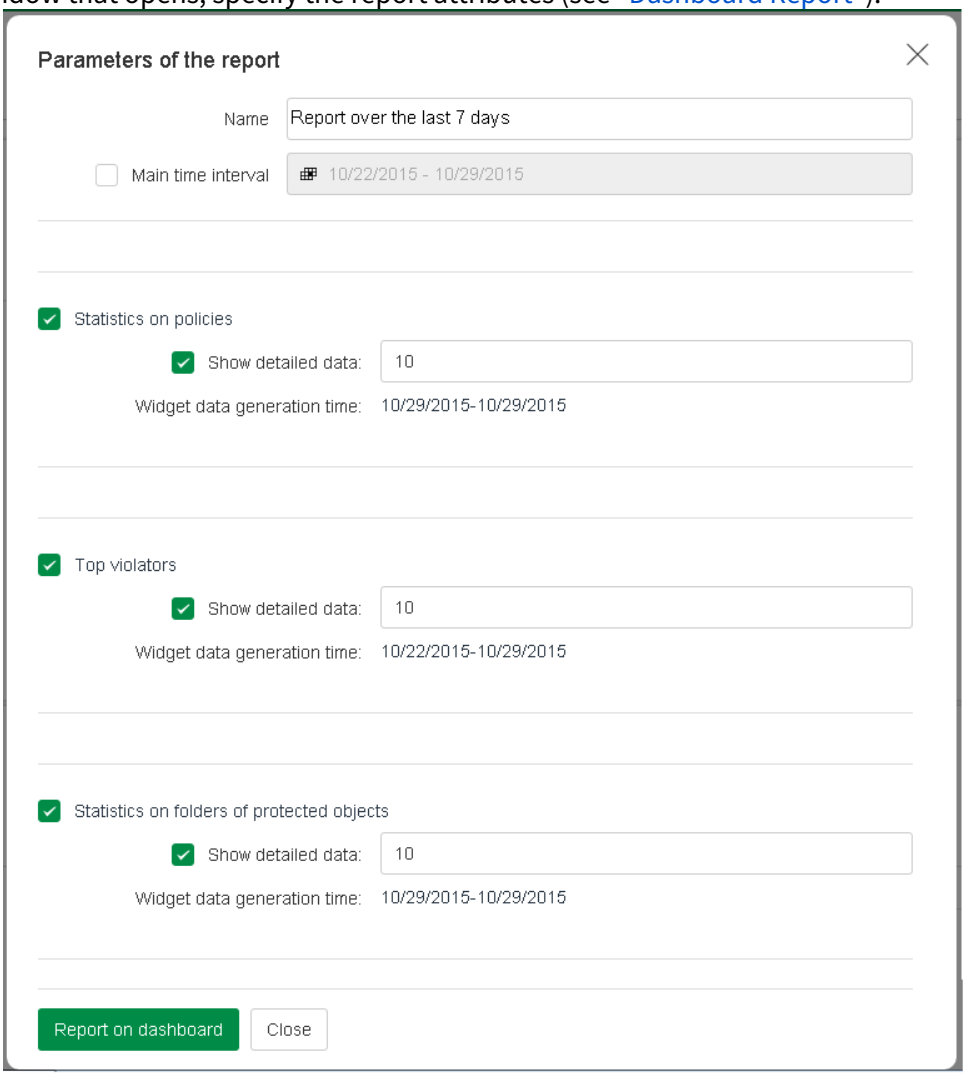
2. To edit a widget, in the right upper corner, click and, from the drop-down list, select **Edit**. In the **General widget settings** window that opens, change the required settings, then click **Save**.
3. To delete a widget, in the right upper corner, click and, from the drop-down list, select **Delete**. In the confirmation window, click **Yes**.

Creating Dashboard Report

Purpose:
To create a report on a dashboard with the summary on intercepted objects.

Solution:

1. Go to the **Dashboard** section.
2. Open the dashboard for which you want to generate a report.
3. In the right upper corner, click **Unload**.
4. In the window that opens, specify the report attributes (see "Dashboard Report").



5. Make sure that you have selected checkboxes of all widgets whose data you want to include in the report.
6. If you want to manually specify the period, for which the report will be generated, select the **Common period** check box and enter the start and the end date. If this option is deselected,

then, for each widget, the report will be generated for the period specified in the widget properties.

7. Click **Report on dashboard**.

In the upper right corner of the workspace, you can see information on the report status.

Once the report is generated, you will be prompted to open it in PDF or HTML format.

All created reports are stored in the System and are available by clicking **Show list of reports** in the right upper corner of the workspace. For details, see “Viewing Dashboard Report".

You can also view information about created reports from any section of the Management Console by clicking the **Export** button on the navigation panel (see "Interface of Traffic Monitor Management Console", №6 in the screenshot).

> **Note:**
>
> If you remove or modify a widget which is included in the report, then the already created report will not be changed.

Viewing Dashboard Report

Purpose:
View a report on intercepted objects.

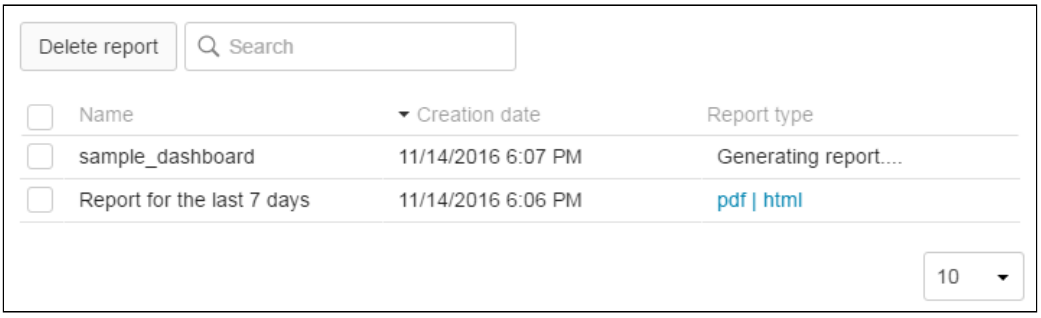
Solution:
When the report generation is complete, a message is displayed in the right upper corner of the workspace. In this message, you are offered to open the report in PDF or HTML format.



Click on the **pdf** or **html** link to open the report in a new browser window. You can also save, send or print the created report by standard means of your browser and operating system.
All created reports are stored in the System.

To view the list of generated reports, in the right upper corner, click the **Show list of reports** button. The **Reports** window will open where you can view information on the reports.

> **Note:**
>
> You can sort reports by date or use the **Search** field to find the required report by the name.



To view a selected report, in the **Report type** column, next to the desired report, click:

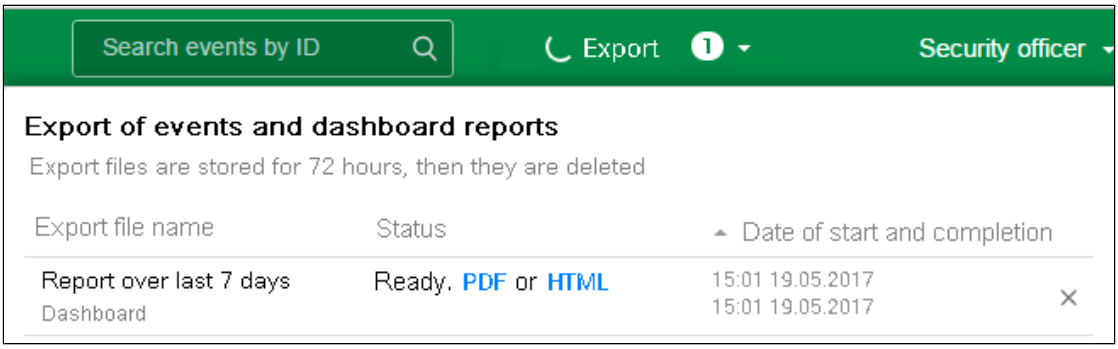
- **PDF** - if you want to display the report in PDF format;
- **HTML** - if you want to display the report in HTML format.

A new browser tab will display the selected report.

To delete selected reports:

1. Select checkboxes next to the reports you want to delete. To select all rows, select the checkbox in the header.
2. Click **Delete report**.

You can also view the list of reports from any section of the Management Console. For this, click the **Export** button in the Navigation page.



For each report, the list displays its name, status, date of start and completion, and links to PDF and HTML files. To open the report in a new browser tab, click the selected format.

To remove the report data from the list, click ✕ in the row of the selected report.

4.6.2 Viewing Events

Purpose:
View information on the interception object.

Solution:

1. Go to the **Events** section (see "Events Section").
2. Create a query and run it (see "Creating Queries").

> **Note:**
>
> The list displays the last 10000 events. Events are sorted by ID-number in descending order.

3. If necessary, change the list of displayed fields (see "Choosing event fields of view").

4. View information on the event tile or in the table row (see point 3 in the picture in the " Events Section ").
5. For more information on the interception object, use a brief or detailed form.

Creating Queries

Purpose:
Create a query to search for required events.

Solution:

1. Go to the **Events** section (see "Events Section").
2. If you want to create a query within a folder, select a folder in the list or create a new folder (see "Creating Folder with Queries").
3. Create a query in a standard or advanced mode. You can create a query in a folder or in the root.
4. To run the query, select it in the list and click  **Run query** on the toolbar (or you can use **Save and run** button in the query creation form).

If necessary, you can copy or move an earlier created folder or query.

To copy a folder and its queries:

1. Select the folder in the list.
2. On the toolbar in the left part of the workspace, click  **Copy**.

If you are trying to copy a subfolder and you have full access to the parent folder, then the copy will be added to the same folder as the copied folder. If you don't have full access to the parent folder or you are copying a top-level folder, then the copy will be added to the root of the folder tree.

To copy a query:

1. Select the query in the list.
2. On the toolbar in the left part of the workspace, click  **Copy**.

If you are copying a query inside a folder and you have full access to the folder, then the copy will be added to the same folder as the copied query. If you don't have full access to the folder or you are copying a top-level query, then the copy will be added to the root of the folder tree.

To move a folder, select it in the list and holding the left mouse button move it to the desired location, then release the mouse button.

> **Note:**
>
> To move a folder, you need to have full access both to the folder you are moving and to the destination folder. If the folder includes queries, then you also need full access to the queries. For details, see the table below.

To move a query, select it in the list and holding the left mouse button move it to the desired location, then release the mouse button.

> **Note:**

To move a query, you need to have full access both to the query and to the destination folder. For details, see the table below.

The table below shows what access rights are needed to manage queries:

Action	**Access rights**			
	View and execute folder	Full access to folder	View and execute query	Full access to query
View the folder	+			
Edit the folder attributes (name, description, access rights)	+	+		
Copy the folder	+			
Create a new item (a query or a subfolder) in the folder	+	+		
Move an empty folder to a different folder	+	+		
Move a folder which includes at least one query	+	+	+	+
Delete an empty folder	+	+		
Delete a folder which includes at least one query	+	+	+	+
View and run the query	+		+	
Edit the query parameters (including access rights)	+		+	+
Copy the query	+		+	
Move the query to a different folder	+		+	+
Delete the query	+		+	+

Note:

If after editing access rights, a query/folder becomes unavailable to any user of the System, then full access to the query/folder is automatically provided to the current user.

See also:

- Creating Folder with Queries
- Query Creation in Standard Mode
- Query Creation in Extended Mode
- Examples of Using Queries

Creating Folder with Queries

Purpose:
Create a folder where queries will be grouped.

Solution:

1. Go to the **Events** section.
2. In the list of folders and queries in the left part of the workspace, choose where to create a folder. You can create a folder in the root or inside an existing folder with queries.

   Note:

   If you do not have sufficient rights to create items within a selected folder, a warning will be displayed. In this case, you should create a folder at a different place.

3. Click  and, in the drop-down list, choose **Create query folder**.
4. In the form that opens, enter the folder name.
5. Specify if access rights to the folder should be inherited for subfolders and queries. By default, the **Apply rights for related queries** option is deselected.

   Note:

   If you create a folder inside a folder with the **Apply rights for related queries** option enabled, then actions described in steps 5-6 are unavailable.

6. Specify who can access the folder and define access rights. For this:
   a. Find required users in the list.

      Tip.

      To find required users, use the **Search** field.

   b. Next to the user name, set the checkbox in one of the fields:
      - **View and execute access** - to provide access for viewing and copying the folder. Access rights to queries in the folder are specified when you create a query;
      - **Full access** - to provide full access to the folder.

> **Note:**
>
> To provide access to the folder to all users of the System, set a checkbox in the field with the required access level next to the **All users** value.

7. Click **Save**.

To edit the folder, click the  button on the toolbar.

To delete the folder, click .

> **Note:**
>
> To edit or delete a folder, full access to the folder is required. If you can only view and execute the folder, then instead of  button,  button is displayed, and  button is unavailable.

Query Creation in Standard Mode

Purpose:
Create a query to search for events which satisfy specified conditions.

Solution:

1. Go to the **Events** section.
2. In the list of folders and queries in the left part of the workspace, choose where to create a query. You can create a query in the root or inside an existing folder with queries.

> **Note:**
>
> If you do not have sufficient rights to create items within a selected folder, a warning will be displayed. In this case, you should choose another location for the query.

3. Click  and, in the drop-down list, choose **Create standard query**.
4. In the form that opens, enter the query name and, if necessary, add a description.
5. On the **Query** tab, edit the query parameters. By default, the most commonly used parameters are displayed. For parameters that you need, specify the required values in the entry fields. To remove parameters that you do not want to use in the query, click  in the right upper corner of the selected parameter.
6. To add a parameter, in the **Add condition** drop-down list, choose the required parameter (for the whole list of available parameters, see "Condition").
7. On the **Columns** tab, select attributes whose values will be displayed for the found events.
8. On the **Access** tab, specify who can access the query and define the access permissions.

> **Important!**

If you create a query in a folder with the **Apply rights for related queries** option enabled, then access rights for the query will be the same as for the folder. In this case, editing access right to the query is unavailable.

To specify access rights to the query:

a. Find the required users in the list.

> **Tip.**
>
> To find users in the list, use the **Search** field.

b. Next to the user name, set the checkbox in one of the fields:
   - **View and execute access** - to provide the user access for viewing, copying, and executing the query;
   - **Full access** - to provide the user full access to the query.

> **Note:**
>
> To provide access to the query to all users of the System, set a checkbox in the field with the required access level next to the **All users** value.

9. Click:
   - **Save** - to save the query;
   - **Save and execute** - to save and run the query.

> **Tip.**
>
> If while creating a query, you find out that you need to specify more flexible conditions, you can use the advanced mode. For this, in the **Query type** field, click **Advanced**. The advance query creation mode will open. All specified parameters of the query will be saved.

To edit the query, click on the toolbar.

To delete the query, click .

> **Note:**
>
> To edit, move, or delete a query, full access to the query is required. If you can only view and execute the query, then instead of button, button is displayed, and button is unavailable.

The "Examples of using queries" article contains an example of creating a simple query.

Query Creation in Advanced Mode

Purpose:
To flexibly configure search conditions for events.

Solution:

1. Go to the **Events** section.
2. In the list of folders and queries in the left part of the workspace, choose where to create a query. You can create a query in the root or inside an existing folder with queries.

> **Note:**
>
> If you do not have sufficient rights to create items within a selected folder, a warning will be displayed. In this case, you should choose another location for the query.

3. On the toolbar, click + and, in the drop-down list choose **Create advanced query**.
4. In the form that opens, enter the query name and, if necessary, add a description.
5. On the **Query** tab edit the parameters used in the query. By default, the most commonly used parameters are displayed. For parameters that you need, specify the required values in the entry fields. To remove parameters that you do not want to use in the query, click × in the right upper corner of the selected parameter.
6. To add a parameter, in the **Add condition** drop-down list, choose the required parameter.
7. By default, added parameters are joined by the logical AND. To change the operation type, left-click the and icon. The icon will change to or that indicates logical OR.
8. Use **Group of parameters** element to separate attributes joined by the logical AND from attributes joined by the logical OR (see "Advanced mode").
9. On the **Display fields** tab, select attributes whose values will be displayed for found events.
10. On the **Access** tab, specify who can access the query and define the access rights.

> **Important!**
>
> If you create a query in a folder with the **Apply rights for related queries** option enabled, then access rights for the query will be the same as for the folder. In this case, editing access right to the query is unavailable.

To specify access rights to the query:

a. Find the required users in the list.

> **Tip.**
>
> To find users in the list, use the **Search** field.

b. Next to the user name, set the checkbox in one of the fields:
   - **View and execute access** - to provide the user access for viewing, copying, and executing the query;
   - **Full access** - to provide the user full access to the query.

> **Note:**
>
> To provide access to the query to all users of the System, set a checkbox in the field with the required access level next to the **All users** value.

11. Click:
    - **Save** - to save the query;
    - **Save and execute** - to save and run the query.

> **Note:**
>
> If while creating a query, you want to switch to the standard mode, then, in the **Query type** field, click **Standard**. The standard query creation mode will open. All specified parameters of the query will be saved. However, if already specified conditions can be implemented in the advanced mode only, then switching to the standard mode is unavailable.

To edit the query, click  on the toolbar.

To delete the query, click  .

> **Note:**
>
> To edit, move, or delete a query, full access to the query is required. If you can only view and execute the query, then instead of  button,  button is displayed, and  button is unavailable.

The "Examples of Using Queries" article contains examples of creating advanced queries.

Using Advanced Syntax

Purpose:
Configure full-text search through the event text by using extended syntax.

Solution:

1. Switch to the advanced mode of the query creation.
2. On the **Query** tab, in the **Add condition** drop-down list, select the **Event text** parameter.
3. Select **Advanced syntax**.
4. In the **Query** field, enter text using logical operators:"|","-", "!", "()", etc.

> **Note:**
>
> When **Advanced syntax** is enabled, search for special characters can be performed via shielding. To shield the special character, use '\' character placed before the character to be shielded.

5. Specify other parameters of the query (for details, see "Query Creation in Advanced Mode").
6. Click **Save**.

You can find detailed information on using logical operators for creating queries in the Internet article.

> **Note:**
>
> Please, not that the search area is defined explicitly in the **Search area** field (see "Search on the Event Text"), so you needn't specify the search area with Sphinx operators.

Example:

If you want to find the event whose text:

- contains *“personal data”* and *“private data”* words;
- does not contain the phrase *"confidential information"*,

create the following query using the advanced syntax:

```
(personal | private) data - "confidential information"
```

Examples of Using Queries

Example 1:

You need to view all email messages for the current day sent by employees under the supervision. For this:

1. Create a simple query and specify its name.
2. Specify the following query parameters:
   - **Interception date** - *Current day*;
   - **Event type** - *Email*.
3. In the **Senders** field, specify the *Employees under supervision* group (see how to create such a group in "Creating Group of Persons or Computers").
4. Save and run the query.

> **Tip**
>
> If there is a lot of traffic in your company and it takes much time to execute the query, you can continue working with other tasks while the query is running in the background. As soon as the query execution is complete, the System will notify you with a balloon tip.

Example 2:

An employee John Smith is suspected of misusing of confidential information. The incident has happened this week. To investigate the incident, you need to find events for John Smith.

For this:

1. Create an advanced query and specify its name - *Smith*.
2. Add the following conditions:



3. Save and run the query.

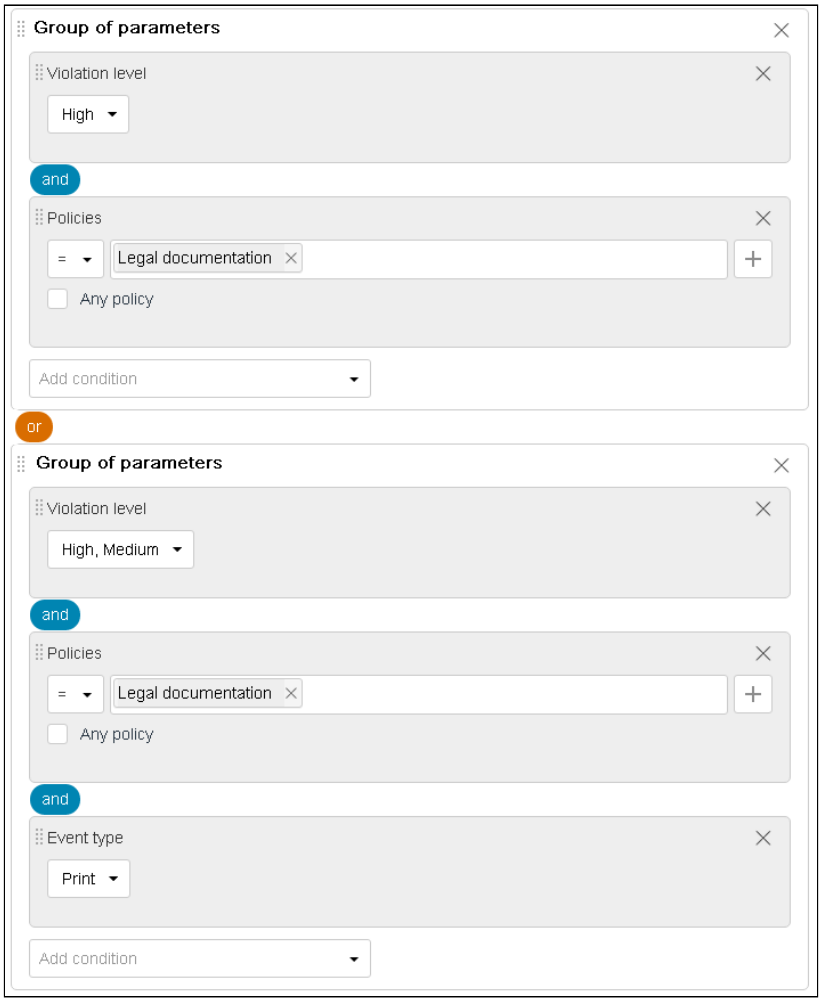
Example 3:

You need to find the events:

- with *High* violation level and the *Legal documentation* policy
- with *High* and *Medium* violation levels, the *Legal documentation* policy, and the *Stamp* event type

For this:

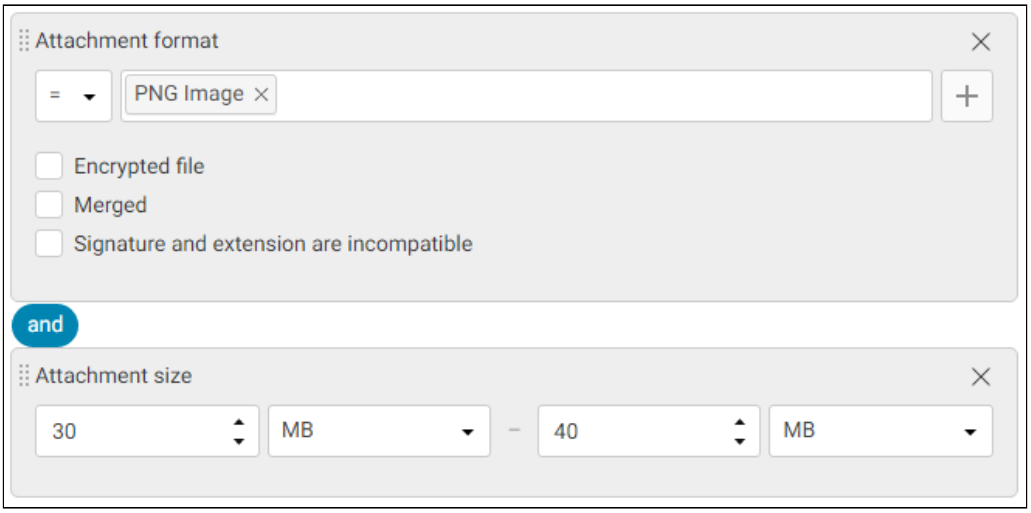
1. Create an advanced query and specify its name.
2. Add two *Group of parameters* elements, joined by logical OR.
3. Within the first group, add the following attributes joined by logical AND:
    - **Violation level** - *High*;
    - **Policy** - *Legal documentation.*
4. Within the second group, add the following attributes joined by logical AND:
    - **Violation level** - *High* and *Medium*;
    - **Policy** - *Legal documentation*;
    - **Event type** - *Print.*
5. Save and run the query.



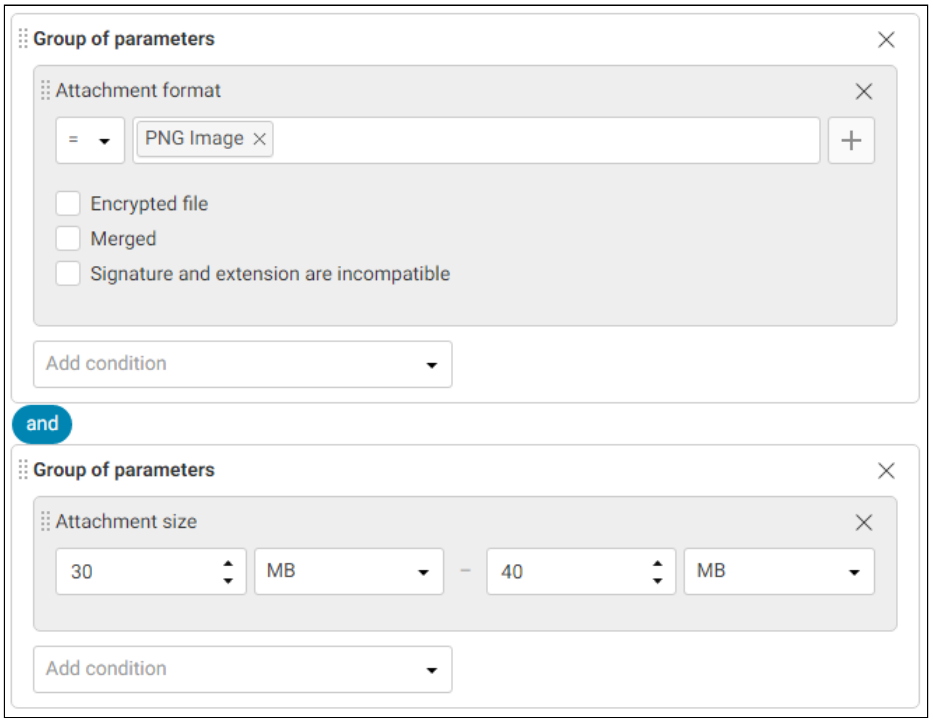
Example 4:

If conditions are specified for object attachments, then, for objects with several attachments, the conditions will apply the following way:

1. If several conditions within a group of parameters are combined by the operation of the logical “AND”, then query results will contain objects with at least one attachment that satisfies all specified conditions. In the example below, the query results will display objects with at least one attachment of PNG format whose size is between 30 and 40 MB.



2. If each condition is in a separate group of parameters and groups are combined by the operation of the logical “AND”, then query results will contain objects, for which all conditions are satisfied, but not necessarily for the same attachment. In the example below, the query results will display objects with at least one attachment of PNG format and at least one attachment whose size is between 30 and 40 MB.



Example 5:

You need to find the events containing eml attachments.

For this:

1. Create an advanced query and specify its name.
2. Add *Attachment format* element.
3. Set the value *Email* for the element.
4. Save and run the query.

Example 6:

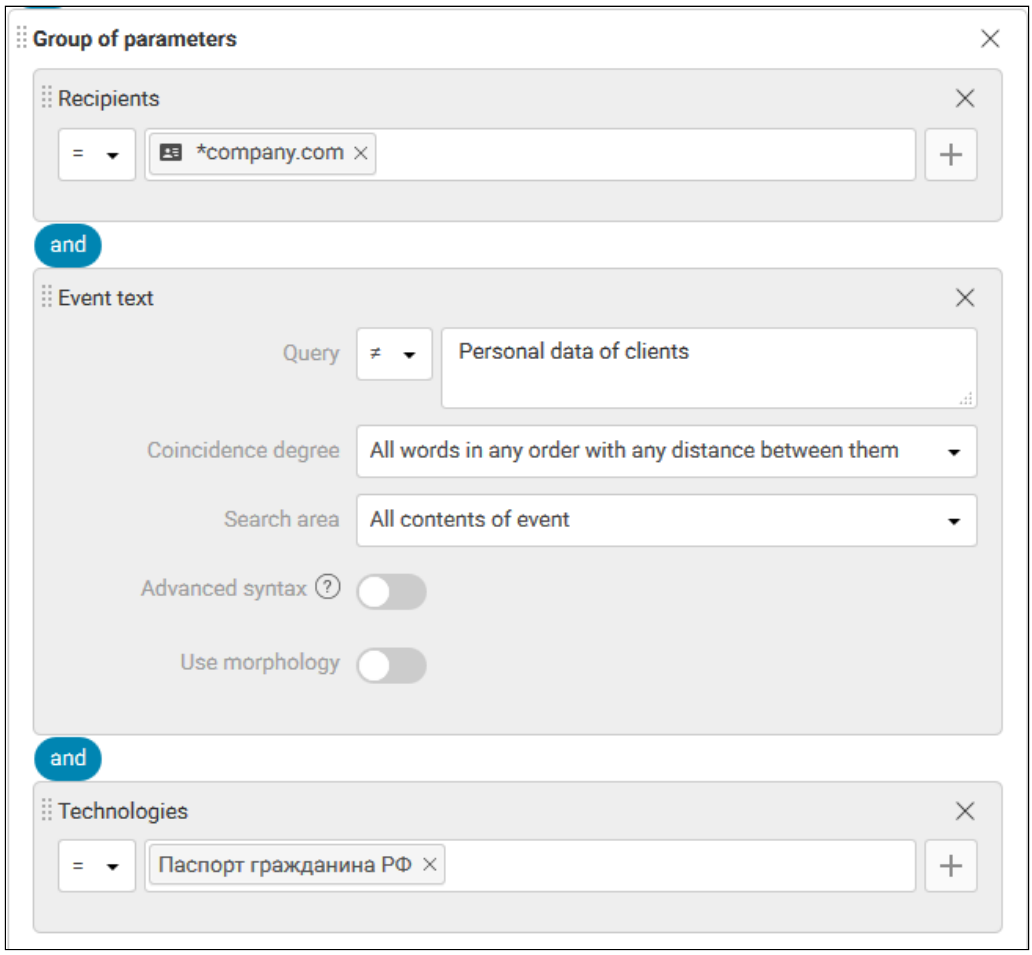
You need to find the events:

1. transferred inside the company
2. without *"Personal data of clients"* text object
3. containing passport numbers

For this:

1. Create a query in advanced mode and specify its name.
2. Add *Group of parameters* element.
3. Whithin the group of parameters specify the attributes bound by the logical “AND”:
   a. `Recipients –` **company.com*
   b. `Event text –` "*Personal data of clients*", herewith select the coincidence degree *All words regardless of their order and distance among them*, and apply negation to the attribute
   c. `Search area` - "All contents of event"
   d. `Technologies –` the "*Russian Federation citizen passport"* text object

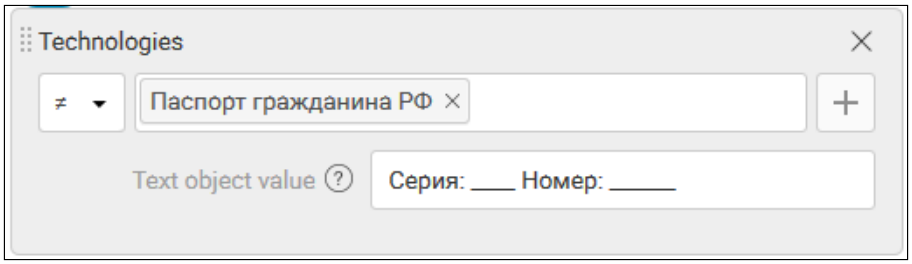
4. Save and run the query.



Example 7:

You need to find the events with the "*Russian Federation citizen passport*" text object.
For this:

1. Create an advanced query and specify its name.
2. Add *Technologies* element.
3. Select the "*Russian Federation citizen passport*" as a value and apply negation to the attribute.
4. Save and run the query.



The query results will include the events:

1. which do not contain triggered protected objects;
2. where triggered protected objects do not contain the "*Russian Federation citizen passport*" text object.

If you specify a passport serial number (e.g., 4505 and 123456), then the query results will include the events:

1. which do not contain triggered protected objects;
2. where triggered protected objects do not contain the "*Russian Federation citizen passport*" text object with serial number "4505" and "123456" value.

Choosing Event Fields of View

Reference information:
By default, event table displays all event attributes.

> **Note:**
>
> By default, **Receiver attributes** aggregation column is not displayed in the table, you can find it in **Available fields** list.

Purpose:
To select attributes of interception objects that will be displayed.

Solution:

1. Go to the **Events** section.
2. Do either of the following:
   - Edit an existing query. For this, click **Edit query**;
   - Create a new query.

   > **Note:**
   >
   > There are two ways to create a query: standard mode and advanced mode .

3. On the right part of the workspace select **Columns** tab.
4. Move all target attributes to the right field and all unwanted ones - to the left:
   - Left-click on the entry in the left field to move it to the right field;
   - Left-click on the entry in the right field to move it to the left field.
5. Click:
   - **Save** - to save a query.
   - **Save and execute** - to save and apply the changed query.

Viewing Brief Event Form

Purpose:
Viewing brief information on interception objects.

Solution:

1. Go to the **Events** section.
2. Create a query or run an earlier created query (see "Creating Queries").
3. Select the tile of the target event in the list (or a raw of the target event in the event table).
4. View the summary in the right part of the workspace. In the upper part of the form, you can view the event parameters; in the lower part, the event contents is displayed.

> **Note:**
>
> You can adjust the data representation in the viewing area. By default, the event content is displayed as snippets where all triggered protected objects and results of the text search are highlighted.

5. To view information on senders, recipients or computers, click the desired value. A card for the selected person or computer will be displayed.
   To view data on senders, recipients or computers, click the desired value. A card for selected person or computer will be displayed.
   When viewing the card, you can:
   a. Assign a status to a person/computer. For this, click Set status link and, in the **Adding status** window, select desired statuses. Then click **Save**.
   b. View detailed information on a person/computer in "Persons" section. For this, click Person profile link (for persons) or Go to computer link (for computers).
   c. View screenshot for a person/computer (if there are screenshots for a person, then icon is displayed next to the person name). For this, click Screenshots link. The **Screenshots** tab for the selected person or computer will open.

> **Note:**
>
> If there are screenshots taken within an hour before or after the event, the Screenshots near the event link is displayed for persons. Clicking this link opens the **Screenshots** tab with the screenshot whose creation time is closest to the event.

6. To view information about the triggered policy in the "Policies" section, click the name of the triggered policy.
7. If the event has attachments, you can save them to your computer. For this, click next to the attachment name.
8. To get detailed information on the event, in the right upper corner of the form, click **Detailed information**.

See also:

- "Brief Event Viewing Form" - on the form with general information about the event.
- "Viewing Detailed Event Form" - on displaying detailed information about the event.
- "Viewing Screenshots" - on viewing screenshots for persons or computers

Viewing Detailed Event Form

Purpose:
To view a detailed information on the interception object.

Solution:

1. Go to the **Events** section.
2. Create a query or run an earlier created query (see “Creating Queries").
3. Select a tile of the target event in the list (or a row of the target event in the table). The right part of the workspace will display a brief event viewing form.
4. To open the detailed viewing form, click **Detailed information**.

5. In the **Detailed information on event** window that appears, view the needed information. Information on the event is presented in the following blocks: **General information**, **Text search**, **Protected objects**, and **Event content** (see "Detailed Event Viewing Form“).

> **Note:**
>
> You can adjust the data representation in the viewing area. By default, the event content is displayed as snippets where all triggered protected objects and results of the text search are highlighted.

6. When viewing the event parameters, you can get additional information about persons, computers, and policies of the event (see "Viewing Brief Event Form“, i. 5-6).
7. To close the detailed form, click ✕ in the upper right corner of the window.

See also:

- "Detailed Event Viewing Form“ - on the detailed event viewing form
- "Viewing Brief Event Form“ - on displaying general information about the event

4.6.3 Making Decision on Object

Purpose:
To make a decision on the object.

Solution:

1. Go to the **Events** section.
2. Left-click the target event to select it.
3. On the toolbar, click
   - **Violation** - for events that violate the corporate security policy. For events with *Quarantine* verdict, the verdict value will change to *Blocked*.
   - **No violation** - for events that do not violate the corporate security policy. For events with *Quarantine* verdict, the verdict value will change to *Allowed*.

     > **Warning!**
     >
     > If the *Block* mode is used in the System, then as a result of this decision, SMTP messages quarantined by the System will be dispatched and the message sender will be notified via email. For details, see “Dispatching Blocked Event".

   - **No decision** - if for now the user has not decidede a decision whether the event violates the corporate security policy.
   - **Requires additional proceeding** - if additional actions are needed to make a decision.

Example

Security Officer views the events marked as No violation and decides that some events have violations. So the Officer marks these events as *Violation*. Such events will be transferred in DB daily table spaces containing events with violations. The data may be useful in future in case investigation is needed. Daily table spaces containing events with violations are stored longer than ones that keep events without violation. The period to store the daily table spaces can be set manually (see how to do it in the articles "Traffic Monitor Administration Guide. Managing daily table spaces)".

See also:

- "Retrospective data analysis, user decision on an object“ - on making user decision.

4.6.4 Adding and Deleting Tags

Purpose:
Add a tag to the interception object.

Solution:

1. Go to the **Events** section.
2. Left-click the target event to select it.
3. On the toolbar, click  **Set tag**.
4. In the window that opens, select the desired tag by flagging it.
5. Click **Save**.

To delete a tag, click X next to the tag name in the event tile.

See also:

- "Tags" - on the interface of Management console section where tags are managed
- "Managing Tags" - on filling a tag catalogue

4.6.5 Saving Events (for SMTP mail)

Purpose:
Save interception object (SMTP-letter).

Solution:

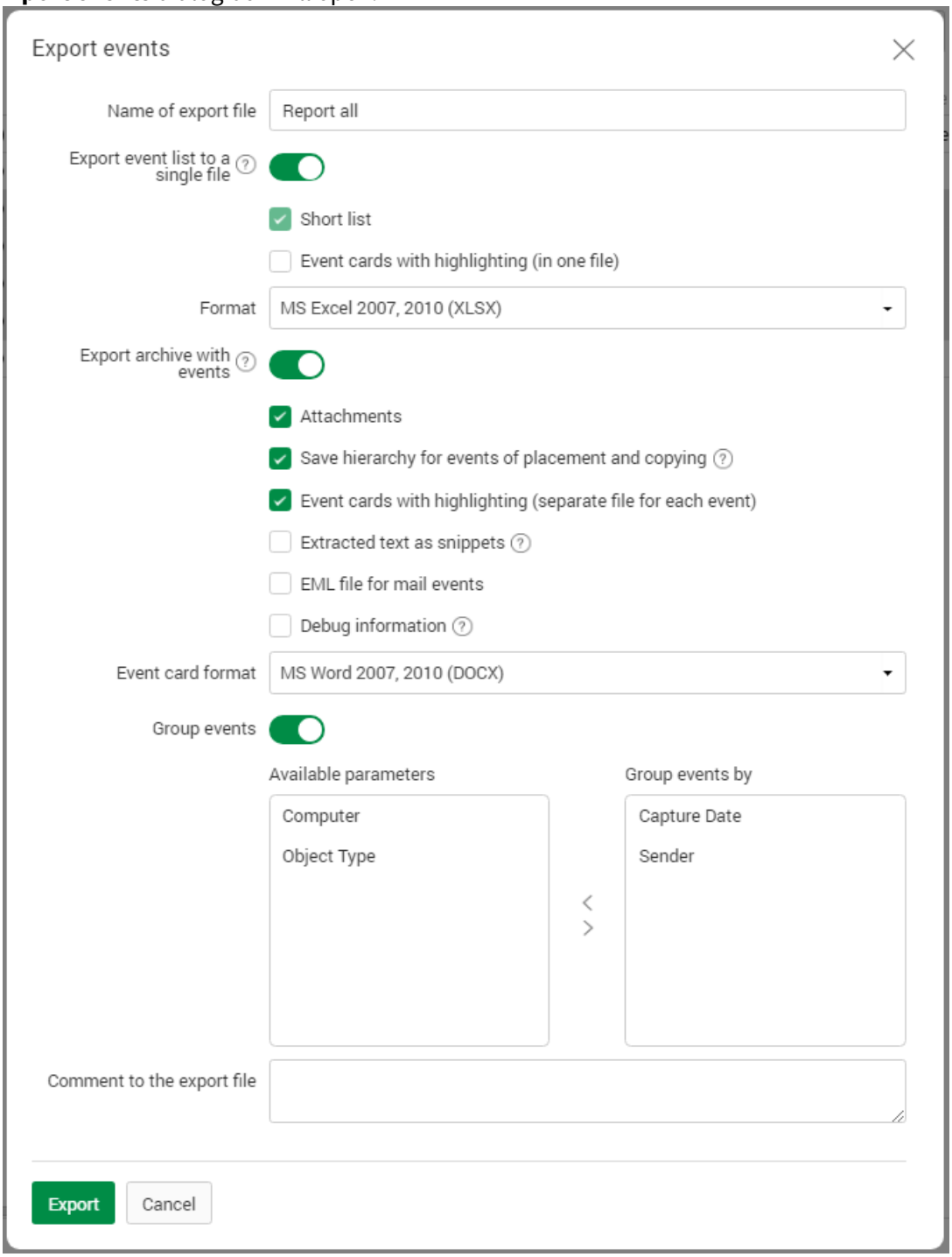
1. Go to the **Events** section.
2. Left-click the target event to select it.
3. In the brief event viewing form located in the right part of the workspace, click .
   The download process will start. When downloading is complete, you can open the event file and view its contents.

4.6.6 Event Export

Purpose:
Save information on events to the computer hard drive.

Solution:

1. Go to the **Events** section.
2. Choose a query from the list and run it or create a new query (see "Creating Queries").
3. Select the event you want to export. To select multiple events, use the **Shift** or **Ctrl** key.
4. On the toolbar, click  and in the drop-down list select **Export events** or **Export all events**. The **Export events** dialog box will open.



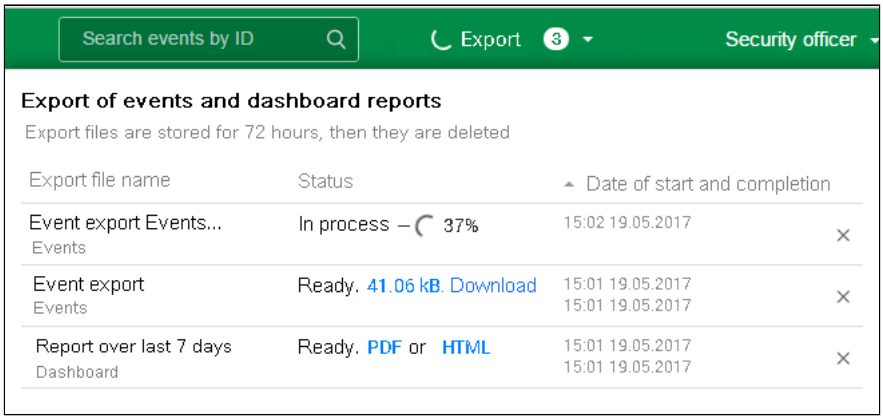
5. If you have selected more than one event, specify how they should be exported (otherwise, go to step 7).
   You can choose one option or both:
   - **Export event list to a single file** - a file with data on all selected events will be created;

- **Export archive with events** - an archive with a separate folder for each event will be created.

6. If you have chosen **Export event list to a single file**:
    a. Choose the list view. You can choose one option or both:
        - **Short list** - for each event, a list of its main parameters is exported;
        - **Event card with highlighting** - for each event, a list of its parameters is exported. Besides, the export file includes the event text and the text extracted from attachments where all triggered protected objects are highlighted.
    b. Choose the export format. The following formats are available:
        - MS Excel 2007, 2010 (XLSX) - unavailable if the **Event card with highlighting** view is selected;
        - MS Excel 2003 (XLS) - unavailable if the **Event card with highlighting** view is selected;
        - MS Word 2007, 2010 (DOCX);
        - Adobe Acrobat (PDF) - you can export not more than 100 events.
7. If you have chosen **Export archive with events** or the export file includes only one event, specify the following settings:
    - **Attachments** - original attachment files will be exported.
      By default the option is disabled to reduce RAM usage;
    - **Save hierarchy for events of placement or copying** - is displayed if the **Attachments** option is selected. Events of the same type will be saved to the "External device" or "FTP" folder depending on the event type;
    - **Event card with highlighting** - a file in DOCX format is created for the event; the file includes a list of the event parameters, the event text and the text extracted from attachments in which all triggered protected objects are highlighted;
    - **Extracted text as snippets** - is displayed if the **Event card with highlighting** option is selected. Text extracted from attachments will be exported in the form of snippets with triggered protected objects;
    - **EML file for mail events** - an EML file of the form [Event ID]_[Email subject] will be exported;
    - **Debug information** - for each exported file, debug information is added to the archive.
8. If you have chosen **Export archive with events**, you can specify additional settings:
    - **Group events** - select this option if you want to group events in the archive and add required parameter from the **Available parameters** field to the **Group events by** field. Events can be grouped by the following parameters: *Computer, Event type, Interception date, Sender.*
    - **Comment to the export file** - the added comment in DOCX format will be exported to the root folder
9. When you have specified all needed parameters, click **Create**.

When the operation is completed, in the upper right corner you will see a notification. To view the export file, click **download** and save it to your computer.

You can monitor the export progress by clicking the **Export** button on the navigation pane.



For each export process, you can view its name, status, start date and time. For already created files, the System also displays their size, creation date and time, and the **Download** link clicking which allows you to save the export file to your computer.

For export files that are being created at the moment, the progress in a percent format is displayed. If you want to cancel the export file generation (e.g., if the process takes a long time), click ✕ in the row of the selected file. The file generation will be canceled.

Besides event export files, the list also displays information on created dashboard reports (see "Viewing Dashboard Report").

The **Export** button is available from all sections of the Management Console.

4.6.7 Dispatching a Quarantined Event

Reference information:
If the System (in the *Blocking* transport mode) recognizes a transferred SMTP-letter as a potential violation and moves it to quarantine, the security officer can then review the decision of the System and allow sending this letter. In this case, the System dispatches the letter and notifies the person who has sent it.

Purpose:
Send a quarantined letter to the addressee.

Solution:

> **Warning!**
>
> You can dispatch the object with a *Quarantine* verdict. Objects with a *Blocked* verdict cannot be dispatched.

1. Go to the **Events** section.
2. Left-click the target event.
3. On the toolbar in the left part of the workspace, click **No violation**.

See also:

- "Retrospective Data Analysis, User Decision on an Object" - general information on making decisions
- "Making Decision on Event" - on how to make a decision on the object

4.7 Configuring System Response

> **Warning!**
>
> For the changes described in this section to be used in the System, apply the configuration. For details, see "Configuring the System" and "Applying System Configuration".

Reference information:
The System response determines the actions that the System performs when detecting violations of the corporate security policy. You can specify these actions when creating rules for data protection policies and person control policies.(see "Policies Section").The System also includes preset policies (see "Default Policies").
Sometimes during operation of the System, the analysis and decision-making subsystems cannot use the policy: for example, the policy has not been created or has been deleted, or an error occurred when applying the policy. In this case, no attributes are assigned to the objects, and the **Processing messages** window of the detailed event viewing form displays information about errors that occurred during the processing (see "Detailed Event Viewing Form").

Why do you need to configure the System reactions:
When you configure the System reactions you can specify that in the case of corporate security policy violations (e.g. sending a confidential document outside the company) or detecting the improper use of work time (e.g. visiting entertaining websites from the office computer), the System should:

- send notifications to violators and inform the security officer and other interested persons;
- assign a verdict to the interception object;
- assign a violation level, statuses, and tags to the interception object.

Configuring the System response includes:

Action	Description
Creating data protection policies	Data protection policy is a set of rules that regulate data transfer, copying, placement, and usage of the clipboard. Allows you to specify actions that may trigger policy rules.
Creating data protection policies on agents	Data protection policy on agents is a set of transfer and copy rules that apply directly on Device Monitor agents. Allows you to specify actions that may trigger policy rules.
Creating person control policies	Allows you to specify the list of controlled persons whose actions may trigger policy rules
Creating rules	Defining what is a violation of policy rules, and what actions will be done in the event of violation
Configuring Notifications in Rules	If the rule is triggered, the System sends notification to specified recipients

> **Note:**

If there are a lot of policies in the Management Console, you can filter the policy list by specified criteria (for details, see “Filtering the List of Policies").

See also:

- "Policies Section" - on the section where you can manage policies

4.7.1 General Information on Policies

The section describes how the System policies are configured (a set of rules according to which objects are analyzed and processed) are applied to events (intercepted objects of network traffic).

The System policies are divided into three groups:

- Data Protection Policies - allow you to set up rules of transfer, copying, placement, and using clipboard
- Data Protection Policies on Agents - allow you to set up transfer and copy rules that apply directly on Device Monitor agents
- Person Control Policies - allow you to set up rules for monitoring actions of individual persons and groups

The System applies policies to events in the following order:

1. The System checks if the event conforms to any active data protection policy on agents.
2. If the event has triggered a policy, the sub-events are considered.
3. For each sub-event, the matching rules are selected (rules triggering to this sub-event).
4. Triggered rules are divided into sub-rules.
5. From sub-rules corresponding to the event, the ones with the highest priority are selected.
6. The actions specified in triggered sub-rules of the highest priority apply to the interception object.
7. If there are sub-events without matching rules, default actions are executed (if they are specified for this type of rules).

Then steps 2-7 are repeated for all active data protection policies and then for all active person control policies.

For more information about accompanying processes, see:

1. Dividing events into sub-events
2. Dividing rules into sub-rules and choosing matching rules
3. Determining the priority sub-rule
4. Order of applying actions according to selected priority rules

The article also includes an example of applying a policy.

1. Dividing events to sub-events

During processing the event, the System divides it into sub-events:

1. For events related to transfer rules: by a pair of keys "Sender" - "Recipient".
2. For events related to copy rules: by the key "Sender".
3. For events related to clipboard rules: by the key "Persons".
4. For events related to storage rules: by a pair of keys "File owners" - "Who has access to file".

If any attribute of the event gets multiple values (for example, multiple recipients of SMTP messages), the System treats this event as a combination of several sub-events with unique attribute values.

For example, if an intercepted event has the following attributes:

Sender	Recipient	Event type	Date
Person: Smith, Person: Johns	Person: Williams, Person: Johns, Person: Smith	Skype	09:23

then the System divides it into the following sub-events:

Sender	Recipient	Event type	Date
Person: Smith	Person: Williams	Skype	09:23
Person: Smith	Person: Johns	Skype	09:23
Person: Smith	Person: Smith	Skype	09:23
Person: Johns	Person: Williams	Skype	09:23
Person: Johns	Person: Johns	Skype	09:23
Person: Johns	Person: Smith	Skype	09:23

2. Dividing rules to sub-rules and choosing appropriate sub-rules

Each rule of opearting policy is divided into sub-rules by the following keys:

1. For transfer rules: by a pair of keys "Sender" - "Recipient".

   > **Note:**
   >
   > If the **Direction of route** parameter has **In both directions** value, then a pair of keys "Recipient" - "Sender" will be added.

2. For copy rules: by the key "Sender".
3. For clipboard rules: by the key "Persons".
4. For storage rules: by a pair of keys "File owners" - "Who has access to file".

For example, the following rules:

Sender	Direction	Recipient	Event type	Date	Reaction
Group: Lawyers, The Person: Smith, Person: Johns	->	Group: Marketing, Person: Williams	Mail on Client	08:00-20:00	Notify: Thomas Violation level: Low
Group: Logistics	->	Group: Sales, Group: Delivery	Skype	10:00-19:00	Notify: Johns Violation level: Medium

Sender	Direction	Recipient	Event type	Date	Reaction
Group: Financial	-> <-	Group: Lawyers, Group: Sales			Notify: Miller Violation level: High

are divided into the following sub-rules:

Sender	Direction	Recipient	Event type	Date	Reaction
Group: Lawyers	->	Group: Marketing	Mail on Client	08:00-20:00	Notify: Thomas Violation level: Low
Group: Lawyers	->	Person: Williams	Mail on Client	08:00-20:00	Notify: Thomas Violation level: Low
Person: Smith	->	Group: Marketing	Mail on Client	08:00-20:00	Notify: Thomas Violation level: Low
Person: Smith	->	Person: Williams	Mail on Client	08:00-20:00	Notify: Thomas Violation level: Low
Person: Johns	->	Group: Marketing	Mail on Client	08:00-20:00	Notify: Thomas Violation level: Low
Person: Johns	->	Person: Williams	Mail on Client	08:00-20:00	Notify: Thomas Violation level: Low
Group: Logistics	->	Group: Sales	Skype	10:00-19:00	Notify: Johns Violation level: Medium
Group: Logistics	->	Group: Delivery	Skype	10:00-19:00	Notify: Johns Violation level: Medium
Group: Financial	->	Group: Lawyers			Notify: Miller Violation level: High
Group: Financial	->	Group: Sales			Notify: Miller Violation level: High

Sender	Direction	Recipient	Event type	Date	Reaction
Group: Lawyers	->	Group: Financial			Notify: Miller Violation level: High
Group: Sales	->	Group: Financial			Notify: Miller Violation level: High

Then, for each sub-event, the System chooses sub-rules whose conditions match the sub-event (for more details on rule attributes, see "Rule of Transfer", "Rule of Copying", and "Application activity rule").

3. Determining the priority sub-rule

For sub-rules that match the sub-event, a rule with the maximum weight is selected. The weight of a sub-rule is determined as the sum of weights of all matching conditions according to the table below:

Sender/Recipient	Weight (if the attribute is enabled)	Weight (if the attribute is disabled)
Contact	10000	3
Person	5000	7
Group	2500	15
Domain	1250	35
URL	600	75
List of resources	300	150
Perimeter (for data protection policies)	Mimimum weight of the perimeter element	Maximum weight of the perimeter element
Perimeter (for data protection policies on agents)	300	150
Device ID	50	25
Cloud storage address	50	does not apply
Address and path to file	20	
Device name	10	5
Source type/receiver type	1	does not apply

Sender/Recipient	Weight (if the attribute is enabled)	Weight (if the attribute is disabled)
Storage	1,25	
Computer	1,25	does not apply
Source-application / Reciever-application	0,415	0,1
Terminal session = Enabled	0,83	does not apply
Days of the week	0,15	does not apply
Time (interval when the rule is active)	0,15	does not apply
Event type	0,1	does not apply
User attribute	1	0,5
If the attribute is not filled: • Sender (for transfer and copy rules) • Recipient (for transfer rules) • Person (for application activity rules, file operations) • File owners/Who has access to file (for placement rules)	1	does not apply
If the attribute is not filled: • Event type (for all rules) • Day of the week (for transfer, copy, and application activity rules) • Time (for transfer, copy, and application activity rules) • Computer (for transfer, copy, application activity rules and file operations) • Storage (for placement rules) • Terminal session (for application activity rules) • Source-application/Reciever-application (for application activity rules and file operations)	0	does not apply

Sender/Recipient	Weight (if the attribute is enabled)	Weight (if the attribute is disabled)
• Copy source/Copy reciever (for copy rules) • User attribute		

For example, the rule with a condition of forwarding from any sender to a specific contact (10000 + 1 = 10001) has a higher priority than the rule with a condition of forwarding from a particular person to a group of persons (5000 + 2500 = 7500).
If for the same sub-event, there are two or more sub-rules with the same priority, the several rules with the highest priority are selected.
If a sub-event has no matching rules, then a default rule is selected (see "Determining System Default Response").

4. The order of applying actions according to selected priority rules

The System assigns the reaction by performing actions from selected priority rules in the following order:

1. If the **Delete event** option is selected, then the actions specified in the rule are not executed and the event is not saved to the database.
2. The event is assigned a verdict with the highest priority from priorities in the selected rules. Verdicts have the following priorities:
   - for **Block** verdict, the priority is 2;
   - for **Quarantine** verdict, the priority is 1;
   - for **Allow** verdict, the priority is 0.

   Note:

   A verdict assigned to the event as a result of applying a data protection policy on agents is not replaced with a verdict specified in rules of data protection policies and person control policies.

   A verdict assigned to the event as a result of applying a data protection policy is not replaced with a verdict specified in rules of a person control policy.
3. The event is assigned the highest violation level from violation levels in the selected rules.
4. Tags specified in the selected rules are added to existing tags.
5. For identified senders, statuses specified in the selected rules are added to existing statuses.
6. Persons specified in the selected rules are notified.

Example:

Let the System have two policies:

Policy №1					
Catalogue of protected objects: Accounts					
Rule number	Sender	Recipient	Date	**Event type**	Reaction
1.1	Group: Sales Department	Group: Accounts Department	08:00-20:00	Mail on Client	Violation: None

Policy №1					
Catalogue of protected objects: Accounts					
Rule number	Sender	Recipient	Date	**Event type**	Reaction
1.2	Smith	Group: Accounts Department		Mail on Client	Violation: None
1.3	Smith	<>Perimeter: Company			Violation: Medium
1.4	Default:				Violation: High

Policy №2					
Catalogue of protected objects: Contract					
Rule number	Sender	Recipient	Date	**Event type**	Reaction
2.1	Group: Sales Department	<>Perimeter: Company	08:00-20:00	Mail on Client	Violation: None
2.2	Smith	<>Perimeter: Company		Mail on Client	Violation: None
2.3	Default:				Violation: None

Smith is a member of the "*Sales Department*" group. Johns belongs to the group "*Accounts Department*". E-mail `williams@mail.com` is outside the compony perimeter.
There is an event:

Data	Sender	Recipient	Date	**Event type**
Protected objects: Accounting, Contract	Smith	Johns, williams@mail.com	19:00	Mail on Client

This event consists of two sub-events, with different "sender-recipient" pairs: "Smith->Johns" and "Smith->williams@mail.com".

1. Check for conformance to policy №1.

The event confirms to the policy №1 as it contains a *Group of protected objects - Accounts*.
The "Smith->Johns" sub-event is considered:

Sender	Recipient	Date	**Event type**
Smith	Johns	19:00	Mail on Client

This event has two sub-rules: №1.1 and 1.2. The more priority one is the sub-rule №1. Therefore, the rule №1.2 is selected.
The "Smith-> williams@mail.com" sub-event is considered:

Sender	Recipient	Date	**Event type**
Smith	williams@mail.com	19:00	Mail on Client

This sub-event confirms to the sub-rule №1.3 only. Therefore, the rule №1.3 is selected

2. Check for conformance to policy №2.

The event confirms to the policy №2 as it contains a *Group of protected objects Contract.*

The "Smith->Johns" sub-event is considered:

Sender	Recipient	Date	**Event type**
Smith	Johns	19:00	Mail on Client

This sub-event confirms to the sub-rule №2.3 only. Therefore, the rule №2.3 is selected
The "Smith->williams@mail.com" sub-event is considered:

Sender	Recipient	Date	**Event type**
Smith	williams@mail.com	19:00	Mail on Client

This event has two sub-rules: №2.1 and 2.2. The more priority one is the sub-rule №1. Therefore, the rule №2.2 is selected.

3 The selected actions are applied : №1.2, №1.3, № 2.3, №2.2

4.7.2 Preset Policies

There are the following preset policies in the System:

- Data protection policies for confidential data
- Person control policy
- Policy regulating transfer of password-protected data
- Policy regulating visiting web resources
- Policy that excludes mailing lists from interception

Note:

When deleting the database scheme (see "*Infowatch Traffic Monitor. User Guide*", "Deleting the Database Scheme" article), policies (including preset ones) are also deleted from the System.

To redeploy the preset policies, do the following:

1. Create **/opt/iw/tm5/www/backend/protected/runtime/first_run** file on behalf of **iwtm** user;
2. Restart **iw_kicker** process:
   `iwtm restart kicker`

Then you need to create other policies anew (see "Creating Data Protection Policy", "Creating Data Protection Policy on Agents", and "Creating Person Control Policy").

Data Protection Policy

By default, the System contains one data protection policy for each preinstalled catalogue of protected objects (for the list of preinstalled catalogues, see "Protected Objects").

Default policies have the following attribute values:

Attribute	Value
Policy name	<Name of the catalogue of protected objects>
Status	Active
Period of activity	Not limited
Type of objects of research	<Name of the catalogue of protected objects>

where <Name of the catalogue of protected objects> is the name of the catalogue for which the policy is created.

Each policy contains the following rules:

Rules of transfer

1. *A rule that regulates transferring confidential data outside the company perimeter*.
   If an employee sends traffic of any type outside the company perimeter any day of the week,
   Then the System performs the following actions:
   - sets the *Allowed* value to the *Verdict* attribute of the event;
   - sets one of the following values to the *Violation level* attribute of the event:
     - *High* - for the following catalogues of protected objects: Security label, Personal data;
     - *Low* - for the following catalogues of protected objects: Law, HR, IT;
     - *Medium* - for all other catalogues of protected objects;
   - sets the *None* value to the *Status* attribute of the person who sends the traffic.
2. *A rule regulating the transfer of confidential data by heads of the company*.
   If an employee from the VIP group sends traffic of any type to any recipient any day of the week,
   Then the System performs the following actions:
   - sets the *Allowed* value to the *Verdict* attribute of the event;
   - sets the *None* value to the *Violation level* attribute of the event;
   - sets the *VIP* tag to the event.

Rules of copying

A rule that regulates copying confidential data to removable devices.

If an employee copies confidential data related to any category to the removable device (including one within terminal session), cloud storages, or using FTP protocol any day of the week,
Then the System performs the following actions:

- sets one of the following values to the *Violation level* attribute of the event:
  - *High* - for the following catalogues of protected objects: Security label, Personal data;
  - *Low* - for the following catalogues of protected objects: Law, HR, IT;
  - *Medium* - for all other catalogues of protected objects;

- sets the *None* value to the *Status* attribute of the person who sends the traffic.

Rules of placement

A rule that regulates storing confidential data. The rule is added only for the policies with the following protected data: Security Label or Personal Data catalogues of protected objects.

If a person stores protected data in any location,
Then the System performs the following actions:

- sets the *High* value to the *Violation level* attribute of the event*;*
- sets the *None* value to the *Status* attribute of the person who owns the data*.*

Person Control Policy

By default the System has a person control policy with the following attribute values:

Attribute	Value
Policy name	Persons under supervision
Status	Active
Period of activity	Not limited
Statuses	Under supervision

Policy Rules

The rule that regulates transferring data by persons with Under Supervision status.

If a person with the *Under supervision* status sends traffic of any type to any recipient,
Then the System sets:

- the *Allow* value to the *Verdict* attribute of the event;
- the *For consideration* value to the *Tag* attribute of the event.

Policy that Regulates Transferring Password-Protected Data

By default, the System has a policy that regulates transferring password-protected data.

The default policy has the following attribute values:

Attribute	Value
Policy type	Data protection policy
Policy name	Password-protected data
Status	Active
Period of activity	Not limited

Attribute	Value
Protected data	Encrypted files of all formats

Policy rules

The rule that regulates transferring password-protected data outside the company perimeter.

If a person sends traffic of any type outside the company perimeter any day of the week,
Then the System performs the following actions:

- sets the *Allowed* value to the *Verdict* attribute of the event;
- sets the *Medium* value to the *Violation level* attribute of the event;
- assigns the *For consideration* tag to the event.

Policies that Regulate Visiting Web Resources

By default the System has the following data protection policies that control visiting web resources by the company employees:

- Social Networks
- Disloyal Employees
- Concealing Employees' Actions
- Suspicious Activity

Social Networks

By default the System has a policy that controls visiting web resources by the company employees.

The default policy has the following attribute values:

Attribute	Value
Policy type	Data protection policy
Policy name	Social networks
Status	Active
Period of activity	Not limited
Protected data	Any data

Policy rules

The rule of transfer that regulates sending requests to entertaining resources.

If a person sends a request to a web resource included in "Social networks" group (for more details, see "Web Resources") any day of the week,
Then the System performs the following actions:

- sets the *Allowed* value to the *Verdict* attribute of the event
- sets the *Low* value to the *Violation level* attribute of the event.

Disloyal Employees

By default, the System has a preset policy that monitors actions of disloyal employees.

The default policy has the following attribute values:

Attribute	Value
Policy type	Data protection policy
Policy name	Disloyal employees
Status	Active
Period of activity	Not limited
Protected data	Any data

Policy rules

The rule of transfer that regulates sending requests to resources related to job search.

If a person sends a request to a web resource included in the "Job search" group (for more details, see "Web Resources") any day of the week,
Then the System performs the following actions:

- sets the *Allowed* value to the *Verdict* attribute of the event;
- sets the *Low* value to the *Violation level* attribute of the event.

Concealing Employees' Actions

By default, the System contains a policy that monitors attempts of employees to conceal their actions or bypass access restrictions.

The default policy has the following attribute values:

Attribute	Value
Policy type	Data protection policy
Policy name	Concealing employees' actions
Status	Inactive
Period of activity	Not limited
Protected data	Any data

Policy rules

The rule of transfer that regulates sending requests to anonymizers.

If a person sends a request to a web resource included in the "Anonymizers" group (for more details, see "List of Resources") any day of the week,
Then the System performs the following actions:

- sets the *Allowed* value to the *Verdict* attribute of the event;
- sets the *Low* value to the *Violation level* attribute of the event.

Suspicious Activity

By default, the System has a preset policy that controls suspicious activities of employees on the Internet.

The default policy has the following attribute values:

Attribute	Value
Policy type	Data protection policy
Policy name	Suspicious activity
Status	Inactive
Period of activity	Not limited
Protected data	Any data

Policy rules

The rule of transfer that regulates sending requests to potentially dangerous resources.

If a person sends a request to a web resource included in the "Potentially dangerous resources", "Sites of aggressive orientation" or "Sites for adults" group (for details, see "Web Resources") any day of the week,
Then the System performs the following actions:

- sets the *Allowed* value to the *Verdict* attribute of the event;
- sets the *Low* value to the *Violation level* attribute of the event;
- set the *For consideration* tag to the event.

Policy that Excludes Mailing Lists from Interception

By default, the System has a preset policy that excludes mailing lists from interception.

The default policy has the following attribute values:

Attribute	Value
Policy type	Data protection policy
Policy name	Exclude from interception
Status	Disabled
Period of activity	Not limited

Attribute	Value
Protected data	Any data

Policy rules

Rule that regulates sending data by persons from the "Exclude from Interception" perimeter

If a person who belongs to the *Exclude from interception* perimeter (see "Perimeters") sends traffic to any recipient any day of the week,
Then the System deletes the event.

4.7.3 Creating Data Protection Policy

Purpose:
Create a policy that determines the System reaction to actions with data.

Solution:

1. Go to the **Policies** section.
2. In the left part of the workspace, click **Add policy** and, in the drop-down list, select **Data Protection Policy**.
   A new policy will be added to the **Data protection policies** group, and, on the right side of the workspace, a policy adding form will be displayed.
3. Specify the policy attributes:
   - Name;
   - Description;
   - Status;
   - Period of action.

   Important!

   When you fill the **Validity period** attribute, consider the possible time zone difference between branches of your organization. The time of interception for the event is the local time on the server which intercepts data. If the local time of interception does not fall within the specified range, the policy does not apply to the event.

4. To add protected data to the policy, click **Select**.

   Note:

   If you do not select any protected data, then the policy will apply to any data.

5. In the window that appears, set the check boxes next to desired values. Protected data may include protected objects, their catalogs, and file formats.
   For file formats, you can also set an additional restriction on the file size (in bytes) and specify the signs as follows:
   - encrypted;
   - merged;
   - signature and extension are incompatible.

> **Warning!**
>
> If protected data of several types are specified for the policy, then for triggering the policy rules (see "Rules and their Viewing Form"), it is necessary that the intercepted event should contain violations of each type.
>
> For example, a catalog of protected objects, several file formats and several attributes are specified as protected data for the policy. In this case, for the policy to be triggered, it is necessary that intercepted data contain at least one protected object from the specified catalog, at least one file of the specified format and all specified attributes.

6. After you have selected protected data, click **Save**.
7. Add rules to the policy (see "Creating Rules").
8. To save the new policy, in the policy creation form, click **Save**.

To edit the policy:

1. Select the desired policy in the list.
2. In the right part of the workspace, edit the necessary parameters.
3. To change the protected data, in the **Protected data block**, click **Select** and then click **Save**.
4. Click **Save** in the policy edit form.

To delete the policy, in the right upper corner of the policy, click ✖ and confirm the action in the confirmation window.

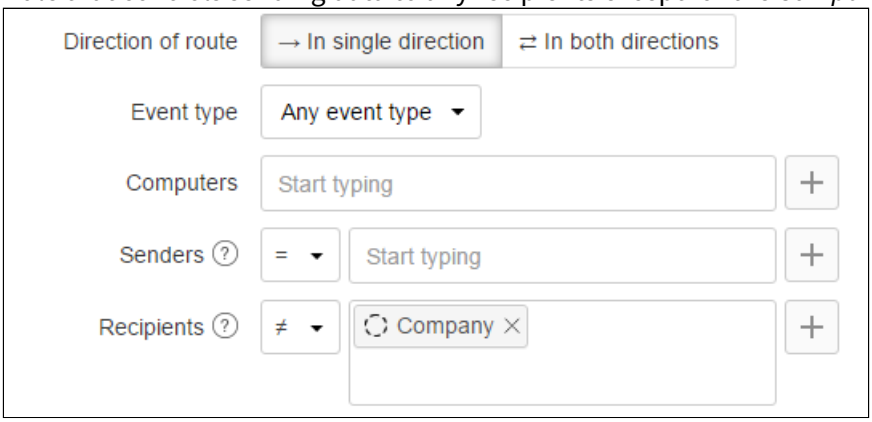
Examples of tasks where a data protection policy can be used are given in the "Examples of Using Data Protection Policy" article.

Examples of Using Data Protection Policy

Example 1:

It is required to control transferring the company statute outside the company which includes sending the document by email or copying it to removable devices. For this:

1. Create a data protection policy and name it *Protection of transferring company statute*.
2. Specify the *Company statute* protected object as protected data.
3. Add a transfer rule that controls sending data to any recipients except for the *Company* perimeter.



4. Specify what actions to perform if the rule is triggered (e.g., assign *Low* violation level to the event).

5. If in addition, you want to control employees under the supervision, add one more transfer rule and specify the *Employees under supervision* group as senders (see "Creating Group of Persons or Computers").
6. Specify what actions to perform if the rule is triggered (e.g., assign *Medium* violation level and *For consideration* tag to the event).
7. To control copying the document to a removable device, add a copy rule to the policy.

The System will detect a violation of the data protection policy when:

- an email whose body or attachment contains data related to the *Company statute* protected object is sent outside the *Company* perimeter;
- a file with information on the *Company statute* protected object is copied to a removable device.

Example 2:

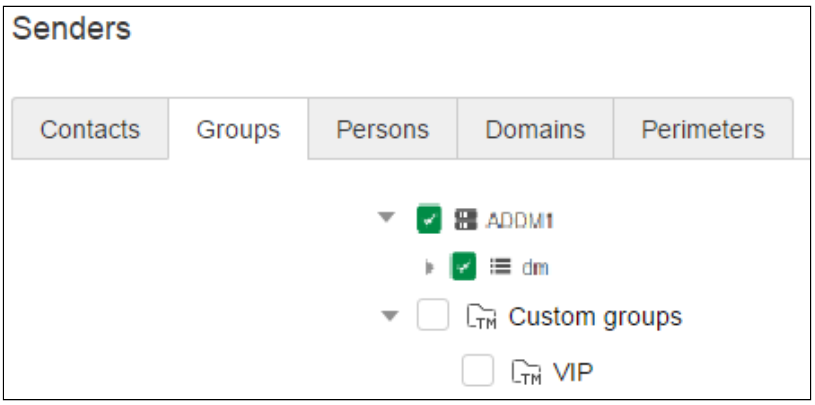
It is required to identify employees who visit job search sited. For this:

1. Create a data protection policy and name it *Identifying disloyal employees*.

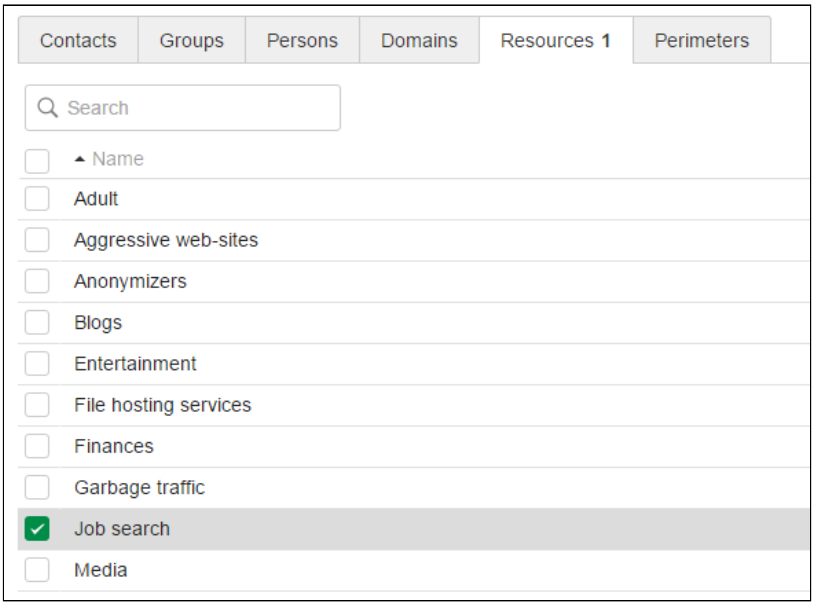
   Tip

   Add the policy description to easily identify it in the policy list. For example, "Identifying employees who send requests to job search sites".

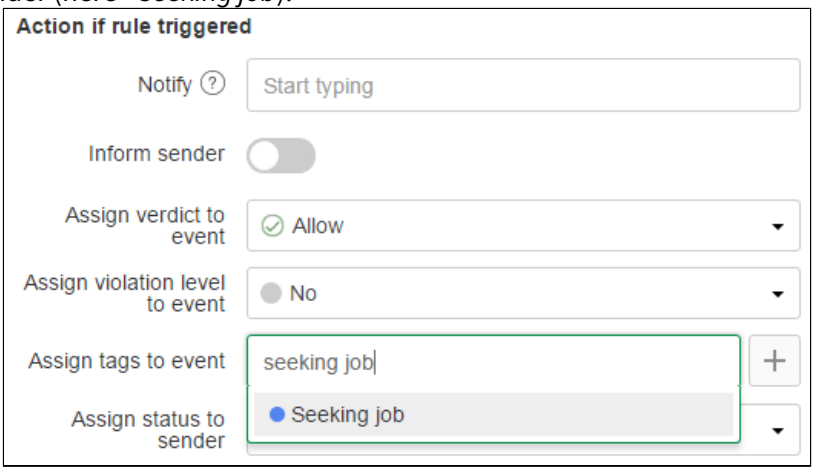
2. Add a transfer rule and specify the group of company employees imported from Active Directory, Samba DC, Domino Directory, Astra Linux Directory, FreeIPA or Astra Linux Directory Pro as senders.



3. Specify the *Job search* list of web resources as recipients.



4. Specify what actions to perform if the rule is triggered. For example, you can assign a specific status to the sender (here - *Seeking job*).



5. Save the rule and apply the changes of configuration.

Now, if an employee sends a request to a job search site, the System will assign the "Seeking job" status to the employee.

If necessary, you can find all such events. For this, create a query and specify on of the following search conditions:

- *Identifying disloyal employees* policy;
- senders with the *Seeking job* status.

Example 3:
It is required to identify employees who communicate with undesired destinations, i.e., fired employees, competitors, etc.

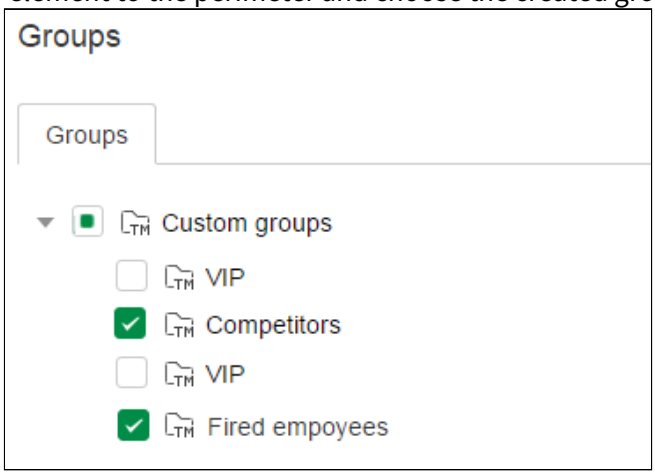
For this, you need to create a perimeter that will include fired employees, competitors, etc. and then create a data protection policy that tracks sending data to this perimeter.

Note:

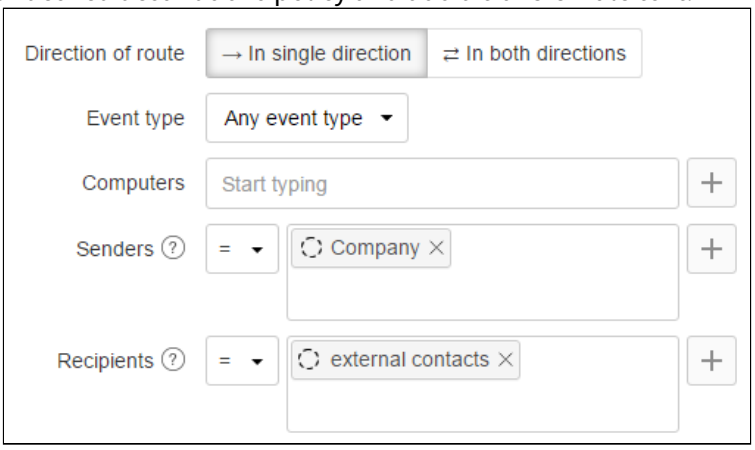
You can add separate person contacts or create user groups, e.g., *Fired employees* and *Competitors*. This example illustrates creating a perimeter based on user groups.

Perform the following steps:

1. Create *Fired employees* group and fill it in one of the following ways:
   - create cards for fired employees manually;
   - import persons from Active Directory, Samba DC, Domino Directory, Astra Linux Directory, FreeIPA or Astra Linux Directory Pro (if the person card is not deleted from the Directory Service when a person is fired).
2. Create *Competitors* group and fill it in one of the following ways:
   - create a separate card for each person in the group, e.g., John Williams from "New company";
   - create a card for each competitor company and add contacts of the company employees to this card.
3. If necessary, create groups for other undesired destinations.
4. Create a perimeter that will include the created groups and name it, for example, *External contacts*.
5. Add a *Group of persons* element to the perimeter and choose the created groups.



6. Create *Identifying undesired destinations* policy and add a transfer rule to it.



7. Specify what actions to perform if the rule is triggered, e.g., assign *Medium* violation level to the event.
8. Apply the configuration to put the configured policy in action.

If an email is sent to a fired employee or a competitor, the System will determine the policy violation.

If necessary, you can find all such events: for this, create a query and specify the *Identifying undesired destinations* policy in search conditions.

4.7.4 Creating Data Protection Policy on Agents

Purpose:

Create a policy that determines the System reaction to actions with data and applies directly on Device Monitor agents. This policy allows you to operatively prevent data leaks on computers where Device Monitor agents are installed.

> **Note:**
>
> On Device Monitor agents installed on OC Astra Linux, data protection policies on agents are not supported.

Solution:

1. Go to the **Policies** section.
2. In the left part of the workspace, click **Add policy** and, in the drop-down list, select **Data Protection Policy on Agents**.
   A new policy will be added to the **Data protection policies on agents** group, and, in the right part of the workspace, a policy adding form will be displayed.
3. Specify the policy attributes:
   - Name;
   - Description;
   - Status;
   - Period of action.

   > **Warning!**
   >
   > When you fill the **Validity period** attribute, consider the possible time zone difference between branches of your organization. The time of interception for the event is the local time on Device Monitor agent. If the local time of interception does not fall within the specified range, the policy does not apply to the event.

4. To add protected data to the policy, click **Select**.

   > **Note:**
   >
   > If you do not select any protected data, then the policy will apply to any data.

5. In the **Choose protected data** window that appears, set checkboxes next to desired values. Protected data may include:
   - **Protected objects**
     You can select protected objects that contain only categories and text objects and for which the negation or detection within event element are not enabled.
   - **Catalogues of protected objects**
     From selected catalogues, the policy will use only those protected objects that are based on

categories and text objects, and for which the negation or detection within event element are not enabled.

- **File formats**
  For file formats, you can also set an additional restriction on the file size (in bytes) and specify if the policy should apply to all files or in accordance with signs as follows:
- encrypted;
- file signature and extension do not match.
  If **Encrypted** option is selected, then the policy is triggered only if a file is encrypted or the System failed to determine the file format.

> **Warning!**
>
> If protected data of several types are specified for the policy, then for triggering the policy rules (see "Rules and their Viewing Form"), it is required that the intercepted object should contain violations of each type.
>
> For example, a catalogue of protected objects and several file formats are specified as protected data for a policy. In this case, for the policy to be triggered, it is necessary that intercepted data should contain at least one protected object from the specified catalogue and at least one specified file format.

6. After you have selected protected data, click **Save**.
7. Add rules to the policy (see "Creating Rules").
8. To save the new policy, in the policy creation form, click **Save**.

To edit the policy:

1. Select the desired policy in the list.
2. In the right part of the workspace, edit the necessary parameters.
3. To change the protected data, in the **Protected data block**, click **Select** and then click **Save**.
4. Click **Save** in the policy edit form.

To delete the policy, in the right upper corner of the policy, click ✖ and confirm the action in the confirmation window.

Example 1:

If you want the System to assign the *Block* verdict and the *Medium* violation level to the event in case of uploading data to cloud storages, take the following steps:

1. Create a data protection policy on agents.
2. Add a copy rule (see "Creating Rules").
3. In the rule attributes (see "Rule of Copying"), set the value of the **Event type** attribute to *Cloud storage*.
4. In the **Copy receiver** field, specify cloud storages uploading data to which should be blocked.
5. In the **Actions when the rule is triggered** block, set the following values to the attributes:
   - to the **Assign verdict to the event** attribute - the *Block* value;
   - to the **Assign violation level to event** attribute - the *Medium* value.

Example 2:

If you want the System to block data transfer via terminal session using clipboard, send notification to Security officer and assign the status *Under supervision* to violator, take the following steps:

1. Create data protection policy on Agents.

2. While creating the policy, specify the protected data the transfer of which, if detected, will be blocked by the System.
3. Add the Clipboard rule (see. "Creating Rules").
4. As the rule attributes (see. "Application activity rule") specify **Persons** and **Computers**, for which the policy will work, and also rule validity days and time.
5. In the block **Actions when the rule is triggered** specify the values to the attributes as follows:
    a. **Send notification** - specify notification template. For example, select the default template **Notification to security officer**.
    b. **Assign verdict to event** - the value *Block*;
    c. **Assign status to senders** - select the default status **Under supervision**.

    After applying the configuration, the created policy will be sent through Device Monitor server to Agents. If the protected data will be detected in transferred text data, the transfer will be blocked and the clipboard will be cleared. Also, the event will be created, Security officer will receive a notification about it, and the violator will get a status "Under supervision" in the System.

For details about policy creating specifics, see "Intercepting Features and Restrictions when Copying Files (Data Protection Policy on Agents)".

4.7.5 Creating Person Control Policy

Purpose:
Create a policy that determines the System reaction to actions of certain persons. The policy applies only to actions of traffic senders.

Solution:

1. Go to the **Policies** section.
2. In the left part of the workspace, click **Add policy** and, in the drop-down list, select **Person Control Policy**.
3. In the window that appears, set the check boxes next to the items that you want to add, and then click **Save**. Research objects may be:
    - individual persons (employees or computers);
    - a group of persons and computers;
    - persons and computers with the same status.

    > **Note:**
    >
    > If elements of different types are selected (for example, persons and statuses), then the policy is triggered when at least one object of each type is detected.

4. A new policy is added to the **Person Control Policies** group, and, in the right part of the workspace, a policy viewing form is displayed.
5. In the policy form, fill in the required fields (see "Policies and their Viewing Form") and click **Save**.

    > **Important!**
    >
    > When you fill the **Validity period** attribute, consider the possible time zone difference between branches of your organization. The time of interception for the event is the local time on the server which intercepts data. If the local time of interception does not fall within the specified range, the policy does not apply to the event.

To edit the policy:

1. Select the desired policy in the list.
2. In the right part of the workspace, edit the necessary parameters.
3. To change the protected data, in the **Protected data block**, click **Select** and then click **Save**.
4. Click **Save** in the policy edit form.

To delete the policy, in the right upper corner of the policy, click and confirm the action in the confirmation window.

You can also add person control policies directly from **Persons** (see "Persons") and **Statuses** (see "Statuses") sections.

To add a policy for a group of persons or computers:

1. Go to the **Persons** section.
2. Select the desired group in the list.
3. On the toolbar in the left part of the workspace, click .

To add a policy for selected persons or computers:

1. Go to the **Persons** section.
2. Select the desired person or computer. To select multiple elements, use Shift or Ctrl keys.
3. On the toolbar in the right part of the workspace, click and, in the drop-down list, select **Create policy**.

To add a policy for a selected status:

1. Go to **Lists**->**Statuses** section.
2. Select the desired status from the list.
3. On the toolbar, click .

Example:

If you want to control the person *Smith* (we assume that this person has already been created in **Persons** section) so that intercepted objects with *High* violation level sent by Smith would be assigned the verdict *Allow*, Smith would be assigned the *Under supervision* status and the user with the email *example@company.com* would be notified about the incident:

1. Go to the **Policies** section and create a person control policy named *Smith*.
2. Create a rule for the policy *Smith* and set the following values to the attributes:
   - attribute **Intercept with the violation level** - *High* value;
   - attribute **Send notifications** - *example@company.com* value (for details, see “Configuring Notifications in Rules");
   - attribute **Assign verdict** - *Allow* value;
   - attribute **Set status** - *Under supervision* value.
3. Save the policy.

4.7.6 Creating Rules

Reference information:

Each policy can include one or more rules.

If the policy is triggered on the interception object, then, depending on the number of triggered rules, the following variants are possible:

- If one rule is triggered, the System performs actions specified in this rule.
- If several rules are triggered and
  - their actions contradict, then the System chooses the priority action and performs it (on the order of selecting priorities, see “General Information on Policies");
  - their actions do not contradict, then the System performs all specified actions.
- If no rule is triggered or rules are not specified, then the System performs the actions specified in the default rule (see “Determining System Default Response").

> **Note:**
>
> If the interception object triggers multiple policies, and each policy has its own rules, then the System chooses the action with the highest priority and performs it (on the order of selecting priorities, see "General Information on Policies"). Actions that do not contradict other actions are performed in full.

Purpose:
Determine what actions with protected data cause a reaction of the System and how the System should respond to these actions.

Solution:

1. Go to the **Policies** section.
2. Select the required policy in the list or create a new policy (see "Creating Data Protection Policy", "Creating Data Protection Policy on Agents", and "Creating Person Control Policy").
3. Add a rule in one of the following ways:
   - on the tab of the selected rule group, click **Add rule**.
   - in the right upper corner of the form, click **Add rule**, and, from the drop-down list, select the desired rule.
4. Configure the rule using a form on the right part of the workspace (see “Rules and their Viewing Form").
5. In the **Actions when the rule is triggered** block, specify what actions the System should perform when the rule is triggered (see "Determining System Response to Policy Violations").
6. Click **Save**.

To edit the rule:

1. Select the required policy in the list.
2. In the policy tile, select the required rule group. Rules are grouped on the following tabs:
   - **Transfer**, **Copy**, **Placement**, **Application activity, and File operations** - for data protection policies;
   - **Transfer, Copy** - for data protection policies on agents;
   - **Rules** - for person control policies.
3. The policy tile will display the list of rules of the selected group. Left-click the desired rule in the list.
4. The rule edit form will open in the right part of the workspace. Edit the necessary fields, then click **Save**.

To delete the rule, in the right upper corner of the rule tile, click ✕ and confirm the action in the confirmation window.

Example:

If a person transfers files included in the *Strictly confidential* protected object on Saturdays and Sundays, the System should assign the *Sending confidential data on weekends* tag to the event and set the *Medium* violation

level:
For this:

1. Create the *Sending confidential data on weekends* tag (see "Managing Tags").
2. Create a data protection policy for the *Strictly confidential* protected object (see "Creating Data Protection Policy").
3. Add a transfer rule and assign the *Saturday* and *Sunday* values to the **Days of rule activity** attribute.
4. In the **Actions when the rule is triggered** block, assign the following values to attributes:
   - **Set violation level** attribute - *Medium* value;
   - **Tags** attribute - *Sending confidential data on weekends* value.

4.7.7 Determining System Response to Policy Violations

Reference information:
For each policy, you can specify actions the System performs in case of the rule violation. For this, choose actions in the **Actions when the rule is triggered** area while creating or editing the rule (see "Creating Rule").
Available actions are determined by the rule type:

Action	**Data protection policies**				**Data protection policies on agents**		**Person control policies**
	Transfer rule	**Copy rule**	**Placement rule**	**Clipboard rule**	**Transfer rule**	**Copy rule**	**Person control rule**
Send notification	Available	Available	Available	Available	Available	Available	Available
Assign verdict to event	Available	Not available	Not available	Not available	Available	Available	Available
Assign violation level to event	Available	Available	Available	Available	Available	Available	Available
Assign tags to event	Available	Available	Available	Available	Available	Available	Available
Assign status to senders	Available	Available	Available	Available	Available	Available	Available
Delete event	Available	Available	Available	Available	Not available	Not available	Available

A detailed description of actions:

Action	Description
Send notification	Allows you to specify which notifications to send if the rule is triggered. To configure sending notifications, click + next to the field. In the dialog box that opens, choose a notification from the list or create a new one. For details, see "Configuring Notifications in Rules". A selected notification template should match the verdict specified in the rule. **Note:** If after the rule is created, the person or the person's e-mail are deleted from the System (on managing user accounts, see *"InfoWatch Traffic Monitor. Administration Guide"*, "Users" section), a notification will not be sent to this person.
Assign verdict to event	The event is assigned a verdict which is a preliminary System decision concerning possible violation of the security policy. Possible values: • **Allow** - the object is not a potential violation and can be delivered to senders. • **Block** - the object is a potential violation. In the "Block" mode, the object delivery is blocked. • **Quarantine** (for data protection policies on agents, this verdict is unavailable) - the user should make a decision whether the object is a violation or not. In the "Block" mode, the object delivery is postponed until the user decision is made. Depending on the user decision, the verdict value will change either to **Allowed** (in this case, the message is delivered) or to **Blocked** (for details, see "Making Decision on Object"). Dispatching messages is available only for SMTP letters when the System operates in the inline mode (for details see the document "*Infowatch Traffic Monitor. Installation Guide*".
Assign violation level to event	A violation level will be assigned to the event. Possible values: **High**, **Medium**, **Low**, **No violation**.
Assign tags to event	The event will be assigned tags, for example, **Under supervision**. For details, see "Tags".
Assign status to senders	The security policy violators will be assigned a specified status, for example, **Under supervision**. For details, see "Statuses".
Delete event	The event will not be saved to a database and actions specified in the rule will not be performed either.

See also:

- Creating Rule

- Configuring Notifications in Rules

4.7.8 Configuring Notifications in Rules

When you create or edit a rule, you can specify who should receive notifications if the rule is triggered.

For this:

1. In the **Actions when the rule is triggered** area, in the **Send notifications** field, click .
2. In the **Choosing mail notifications** dialog box, set checkboxes next to selected notifications. You can choose several notifications to be sent to different recipients.

> **Note:**
>
> If there are no notifications in the System, a corresponding message is displayed. In this case, you can create a notification by clicking **Create notification** in the message window.

3. If there is no appropriate notification in the list, you can create a new notification. For this, click **Create a new one** in the left upper corner of the window.

> **Note:**
>
> To edit a notification from the list, click the notification name.

> **Note:**
>
> You can also create notifications from the **Administration** -> **Notifications** section (see "Configuring Notifications").

4. In the notification create/edit form, specify the notification parameters as described in "Creating Notification".
5. To return to the notification list, click **Back to notifications** in the left upper corner of the form.
6. When you have chosen all required notifications, click **Save**.

> **Important!**
>
> A verdict in the notification should match the verdict in the rule. Otherwise, the notification will not be sent.

4.7.9 Determining System Default Response

Reference information:
If after applying the policy, there are sub-events with no matching rules, the System performs default actions (on dividing events into sub-events, see "General Information on Policies"). Default actions are specified by the user.

> **Note:**
>
> If default actions are not specified and none of the rules is triggered on the interception object, the policy is not triggered on this interception object either.

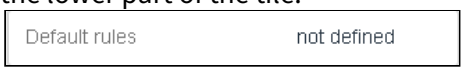
Purpose:

Determine how the System should respond if the event contains a sub-event to which neither of the policy rules matches.

> **Note:**
>
> Default actions can only be specified for data protection policies and data protection policies on agents.

Solution:

1. Go to the **Policies** section.
2. On the left side of the workspace, left-click the target policy.
3. In the policy tile, select the target tab (**transfer**, **copying**, **placement** or **clipboard**) and left-click the lower part of the tile:



4. In the right part of the workspace, specify required actions in the single **Actions** block (see "Rules and their Viewing Form") and click **Save**.

Additional information:

For *Web message* and *Mail in Browser* event types, a default rule can be false triggered. Such a situation may arise when:

The System contains a rule that regulates data transfer from person A to person B. If person A sends data to person B via a website, the System creates an event which is divided into two sub-events:

Sender	Recipient	Protocol
Person A	Person B	HTTP
Person B	Website domain	HTTP

Since the route **Person A**->**Website domain** is not specified in the policy rules, the default actions are executed.

To avoid false triggering of the default rule for*Web message* and *Mail in Browser* event types, do either of the following:

- in the transfer rule attributes, add the website domain or a list of websites that can be used for data transfer;
- do not specify default actions.

Example:

You want the System to assign the *Under supervision* status to the card of the person who copies data if:

- the copied data from a *State secret* protected object, and
- no copy rules are triggered.

For this:

1. Create a data protection policy for the *State secret* protected object (see "Creating Data Protection Policy").
2. Start configuring default policy actions.
3. In the only **Actions** block, set the *Under supervision* value to the **Set status** attribute.

4.7.10 Filtering the List of Policies

Purpose:
Filter the list of policies in case of a large number of policies.

Solution:

1. Go to the **Policies** section.
2. In the left part of the workspace, click **Filter**.
3. In the **Filter settings** area, specify filtering criteria in one of the fields or in both of them:
    - **Filter by policy name** - start typing and select the name of the needed policy (repeat to select several policies)
    - **Filter by objects of research** - start typing and select the name of needed object (repeat to select several objects)
      For data protection policies and data protection policies on agents, you can specify the following objects of research:
        - catalogue of protected objects;
        - protected object;
        - file format.

      For person control policies, you can specify the following objects of research:
        - person;
        - group of persons;
        - status.
4. Click **Apply**.

4.7.11 On Data Protection Policy on Agents

Why do you need data protection policies?

Policies of this type apply first and directly on DM agents. It does not apply on TM. The policy is a tool of a security officer who is using it to control activity on workstations and prevent leaks of confidential data.

The policy controls such actions as:

- data transfer (Internet activity, Mail on Client, Mail in Browser)
- data copy (FTP, cloud storages, external storages, network resources, terminal sessions)
- work in applications (clipboard).

How the policy works:

1. To control traffic on workstations the security officer creates and configures the policy in TM console. The policy is then deployed on workstations.
2. A person performs illegitimate actions (e.g., sends confidential data via email in a browser).
3. DM agent on the workstation analyzes the data being transferred.
4. If the policy is triggered, DM agent performs actions specified in the policy (e.g. blocks sending if Block verdict is specified in the rule). Then DM sends the event and its analysis to TM, and the user gets the following message (if configured) «According to security policy the data transfer is

blocked as confidential information has been detected in the data». The action or process initialized by the user is not complete.
5. TM receives the event, processes and analyzes it.
6. In the console, the security officer sees the intercepted event and its analysis results got from DM agent and TM server.
7. The security officer analyzes the information and takes necessary actions.

What do you need to create a policy?

- Add policy rules
- Select protected data. This can be:
  - protected objects containing text objects, categories and terms and catalogues of protected objects
  - file formats
    If no protected data is selected, the policy is applied to actions with any data
- Specify a period during which the policy will apply (can be unlimited or have defined dates).

The following rules can be added: transfer rule, copy rule, application activity rule.

For details see Rules and their Viewing Form, Rule of Transfer, Rule of Copying, Application activity rule.

4.7.12 On Data Protection Policy

Why do you need data protection policies?

Policies of this type apply in TM after data protection policies on agents. They allow you to monitor the following channels of data leaks:

- Messengers
- Screenshots, printing
- File operations
- Clipboard
- Keyboard input

How the policy works:

1. The security officer creates and configures the policy for extended control of data protection. The channels listed above are to be controlled..
2. A person performs illegitimate actions (e.g., tries to print a file with confidential data).
3. TM analyses received data.
4. If the policy is triggered (policy rules are violated), an event is created. The message is sent to the recipient (its shadow copy is created in TM) or sending is blocked (if *Blocked* verdict is applied according to the rule). An event is created.
5. In the console, the security officer can see the event and the results of its analysis received after processing the event on TM server.
6. The security officer analyses the information and can take necessary actions.

What do you need to create a policy?

- Add policy rules.
- Choose protected data. This can be any combinations of protected objects, catalogues of protected objects, file formats. If no protected data is selected, the policy is applied to actions with any data.
- Specify a period during which the policy will apply (can be unlimited or have defined dates).

The following rules can be added: transfer rule, copy rule, rule of placement, clipboard rule.

For details see Rules and their Viewing Form, Rule of Transfer, Rule of Copying, Clipboard Rule, File Operations Rule.

4.7.13 On Person Control Policy

Why do you need data protection policies?

Policies of this type can be used if the security officer needs to monitor actions of a particular person.

How the policy works:

1. The security officer configures a person control policy and specifies the controlled person.
2. If actions of this person trigger the policy rules, information about these actions is sent to TM.
3. TM analyses the received information.
4. The security officer sees the event with analysis results and takes necessary actions.

What do you need to create a policy?

- Add person control rule (see "Person Control Rule").
- Specify controlled objects (they can be persons, person groups, or statuses).

> **Note:**
>
> The policy applies to event initiators only. Traffic recipients are not controlled by this policy.

4.8 Managing Reports

What for do you need reports?

Reports are used for monitoring user activities and investigating incidents and allow you to get statistics on required parameters.

Reports are convenient when you need to flexibly configure parameters, while widgets in the "Dashboard" section contain fewer conditions and provide you with timely statistics.

Tools in the "Reports" section also allow you to create printed reports based on results of monitoring or investigations.

Working with reports includes the following actions:

- Creating Folder with Reports
- Creating a report
- Creating and Configuring Widget
- Managing ready reports

The "Examples of Using Reports" article contains examples of using reports for monitoring user activities and investigating incidents.

See also:

- "Reports Section" - on the section where you can manage reports

4.8.1 Creating and Viewing Reports

Purpose:
Create a report to view statistics on interception objects.

Solution:

1. Go to the **Reports** section (see "Reports Section").
2. If you want to create a report within a folder, select a folder in the list or create a new folder (see "Creating Folder with Reports").
3. Create a report within a selected folder or in the root (see "Creating Report").
4. Add widgets to the report (see "Creating and Configuring Widget").
5. To run the report execution, select the report in the list and click  on the toolbar or the **Run report** button in the report viewing form (or you can use **Save and run** button in the report creation form).
6. To view results of an earlier executed report, select the report in the list in the left part of the workspace. Besides, you can view results of the report execution for different dates and save selected report versions to your computer (for details, see "Viewing Ready Reports").

If necessary, you can copy or move an earlier created folder or report.

To copy a folder and its reports:

1. Select the folder in the list.
2. On the toolbar in the left part of the workspace, click  **Copy**.

If you are trying to copy a subfolder and you have full access to the parent folder, then the copy will be added to the same folder as the copied folder. If you don't have full access to the parent folder or you are copying a top-level folder, then the copy will be added to the root of the folder tree.

To copy a report:

1. Select the report in the list.
2. On the toolbar in the left part of the workspace, click  **Copy**.

If you are copying a report inside a folder and you have full access to the folder, then the copy will be added to the same folder as the copied report. If you don't have full access to the folder or you are copying a top-level report, then the copy will be added to the root of the folder tree.

To move a folder, select it in the list and holding the left mouse button move it to the desired location, then release the mouse button.

> **Note:**
>
> To move a folder, you need to have full access both to the folder you are moving and to the destination folder. If the folder includes reports, then you also need full access to the reports. For details, see the table below.

To move a report, select it in the list and holding the left mouse button move it to the desired location, then release the mouse button.

> **Note:**
>
> To move a report, you need to have full access both to the report and to the destination folder. For details, see the table below.

The table below shows what access rights are needed to manage reports:

Action	Access rights			
	View and execute folder	Full access to folder	View and execute report	Full access to report
View the folder	+			
Edit the folder attributes (name, description, access rights)	+	+		
Copy the folder	+			
Create a new item (a report or a subfolder) in the folder	+	+		
Move an empty folder to a different folder	+	+		
Move a folder which includes at least one report	+	+	+	+
Delete an empty folder	+	+		
Delete a folder which includes at least one report	+	+	+	+
View and run the report	+		+	
Edit the report parameters (including access rights)	+		+	+
Copy the report	+		+	
Move the report to a different folder	+		+	+
Delete the report	+		+	+

See also:

- Creating Folder with Reports
- Creating Report
- Examples of Using Reports

Creating Folder with Reports

Purpose:
Create a folder for grouping reports with a common theme.

Solution:

1. Go to the **Reports** section.
2. In the list of folders and reports in the left part of the workspace, choose where to create a folder. You can create a folder in the root or inside an existing folder.

> **Note:**
>
> If you do not have sufficient rights to create items within a selected folder, a warning will be displayed. In this case, you should find a different location for your folder.

3. Click  and, in the drop-down list, select **Create folder**.
4. In the form that opens, enter the folder name.
5. Specify if access rights to the folder should be inherited for subfolders and reports. By default, the **Apply rights for related reports** option is deselected.

> **Note:**
>
> If you create a folder inside a folder with the **Apply rights for related reports** option enabled, then actions described in steps 5-6 are unavailable.

6. Specify who can access the folder and define access rights. For this:
   a. Find required users in the list.

> **Tip.**
>
> To find required users, use the **Search** field.

   b. Next to the user name, set the checkbox in one of the fields:
      - **View and execute access** - to provide access for viewing and copying the folder. Access rights to reports in the folder are specified when you create a query;
      - **Full access** - to provide full access to the folder.

> **Note:**
>
> To provide access to the folder to all users of the System, set a checkbox in the field with the required access level next to the **All users** value.

7. Click **Save folder**.

To edit the folder, click the  button on the toolbar.

To delete the folder, click .

> **Note:**
>
> To edit or delete a folder, full access to the folder is required. If you can only view and execute the folder, then instead of  button,  button is displayed, and  button is unavailable.

Creating Report

Purpose:
Create a report that contains statistical data on interception objects.

Solution:

1. Go to the **Reports** section.
2. In the list of folders and reports in the left part of the workspace, choose where to create a report. You can create a report in the root or inside an existing folder.

   > **Note:**
   >
   > If you do not have sufficient rights to create items within a selected folder, a warning will be displayed. In this case, you should choose a different location for the report.

3. Click  and, in the drop-down list, choose **Create report**.
4. In the form that appears, specify required parameters (for more information, see "Report Creation Window").
5. On the **Widgets** tab, click **Add widget**.
6. In the **Widget Creation** window that opens, specify the widget parameters (for details, see “Managing widgets of reports") and click **Save**.
7. If necessary, add more widgets as described at step 6. When you are done, close the **Adding widget** window by clicking  in the right upper corner.
8. Open the **Access** tab to specify who can access the report and define the access rights.

   > **Important!**
   >
   > If you create a report in a folder with the **Apply rights for related reports** option enabled, then access rights for the report will be the same as for the folder. In this case, editing access right to the report is unavailable.

   For this:
   a. Find required users in the list.

      > **Tip.**
      >
      > To find required users, use the **Search** field.

   b. Next to the user name, set the checkbox in one of the fields:

- **View and execute access** - to provide the user access to viewing, copying, and executing the report;
- **Full access** - to provide the full access to the report.

> **Note:**
>
> To provide access to the report to all users of the System, set a checkbox in the field with the required access level next to the **All users** value.

9. Click:
   - **Save** - to save the report.
   - **Save and execute** - to save and execute the report.

You can also copy a previously created report. To do this:

1. Select a report in the list using the left mouse button.
2. On the toolbar in the left part of the workspace, click **Copy** (or click in the right part of the workspace and, in the drop-down list, select **Copy**).

The copy will be added to the report structure at the same level as the report you have copied.

You can change the location of the report using drag-and-drop. To do this, select the required report in the list, press the left mouse button and move the report to the desired location holding the left mouse button pressed. Then release the mouse button.

> **Warning!**
>
> When moving a report to a folder, access parameters specified for the folder will be applied to the report being moved.

To edit the report, click on the toolbar.

To delete the report, click .

> **Note:**
>
> To edit, move, or delete a report, full access to the report is required. If you can only view and execute the report, then instead of button, button is displayed, and button is unavailable.

Creating and Configuring Widget

Purpose:
Create a widget for displaying statistics.

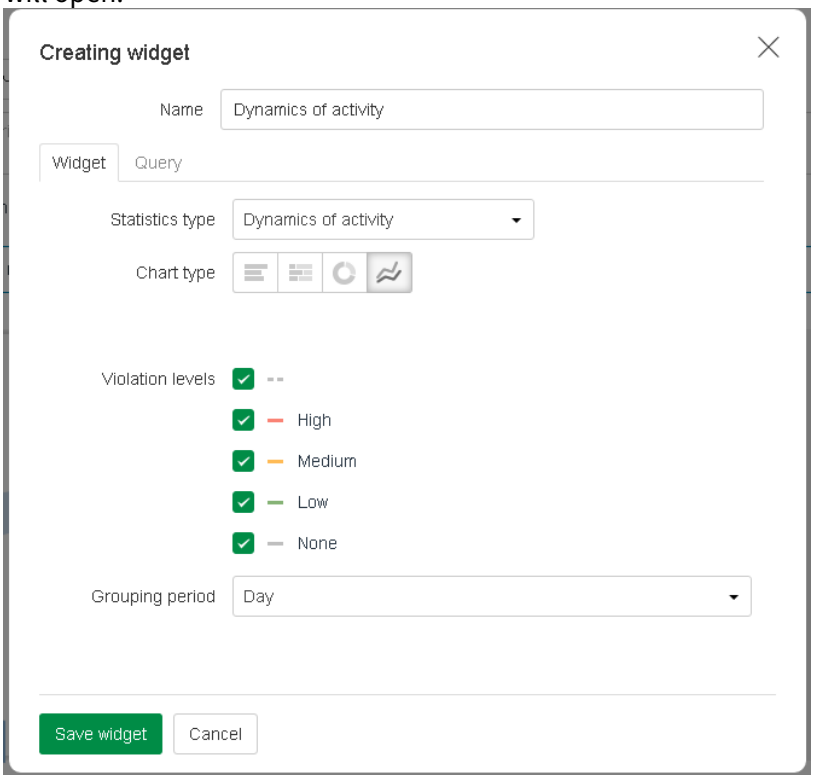
Solution:

1. Go to the **Reports** section.

2. In the left part of the workspace, select a report to which you want to add a widget or create a new report (see "Creating a report").

> **Note:**
>
> To add a widget to an earlier created report, switch to the report edit mode.

3. In the form that appears, open the **Widgets** tab and click **Add widget**. The **Creating Widget** window will open.



4. Fill in the required fields:
   a. In the **Name** field, enter the name of the widget.
   b. On the **Widget** tab, choose the type of statistics. Other settings (a chart type, the number of records, the grouping period, etc.) are available depending on the chosen type of statistics (for more details on the types of statistics, see "Widgets").
   c. On the **Query** tab, specify the parameters based on which events will be filtered (for more information about available settings, see "Queries").
5. Click **Save Widget**.

You can duplicate an earlier created widget to a different report. For this:

1. Switch to the edit mode of a report with the required widget.
2. In the upper-right corner of the desired widget, click ▾ and in the drop-down list select **Duplicate**.
3. In the report list in the left part of the workspace, select the report to which you want to duplicate the widget.

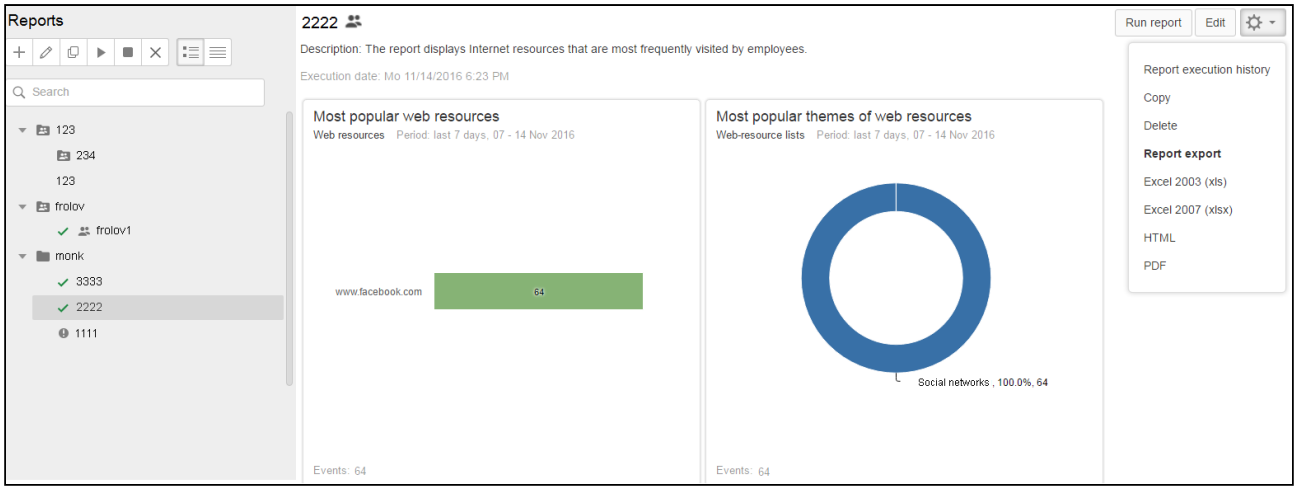
Additional information:

To edit or delete a widget, switch to the report edit mode and select the desired widget. Then:

- To edit the widget, in the upper-right corner of the widget, click and, in the drop-down list, choose **Edit**.
- To delete the widget, in the upper-right corner of the widget, click and, in the drop-down list, choose **Delete**.

Viewing Ready Reports

To view the last executed version of the report, choose the required report in the list. Widgets for the selected report will be displayed in the right part of the workspace. Date and time of the report execution are displayed above the widgets.



If you want to view events information about which is displayed in the widget, in the right upper corner, click and from the drop-down list, select **Go to events**. You will switch to the list of events in the "Events".

You can save the report as a file in one of the following formats:

- Excel 2003
- Excel 2007
- HTML
- PDF

To export the report, in the right upper corner, click and, in the drop-down list under the **Report export** caption, choose the desired format. A report in the selected format will be saved to you computer.

To view report versions for other dates, open the report execution history. For this, in the right upper corner, click and, in the drop-down list, choose **Report execution history**. In the window that opens, you can view information about the report execution.



For each report version, you can view the execution date and time and a comment field. To add a comment to a report version, double-click the field next to the selected version.

If the report execution was cancelled, icon is displayed next to the report version.

You can view required report versions, delete versions that are no longer needed, or save selected versions to a file.

To view a report version, click the row with the date and time of the report execution. Widgets for the selected report version will be displayed.

To delete selected report versions:

1. Select check boxes for the versions which you want to delete. To select all rows, select the check box in the header field.
2. Click **Delete**.

To export selected report versions:

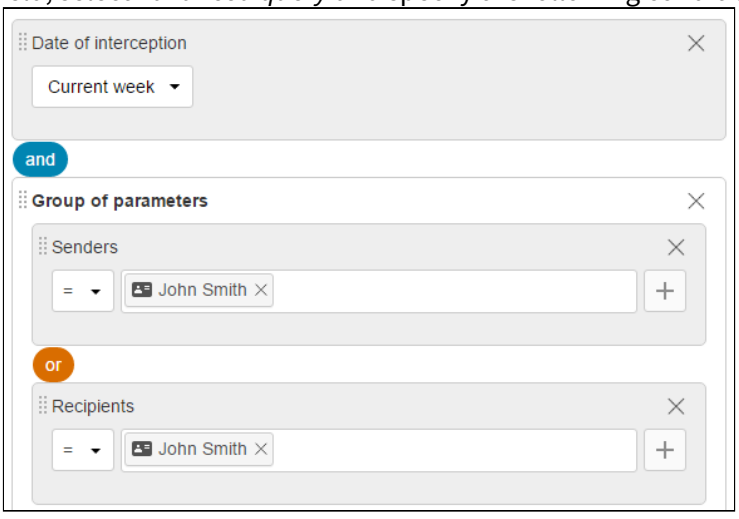
1. Select check boxes for the versions which you want to save as a file. To select all rows, select the check box in the header field.
2. Click **Export** and, in the drop-down list, choose the required format.: Excel 2007, Excel 2003, HTML, or PDF. A file in the specified format will be saved to your computer.

4.8.2 Examples of Using Reports

Example 1:
The employee John Smith is in the list of the most active violators of the week (statistics on the most active violators in displayed in the "Top Violators" widget). An investigation is required to get detailed information on activities of this employee. The investigation can be carried out in several steps.

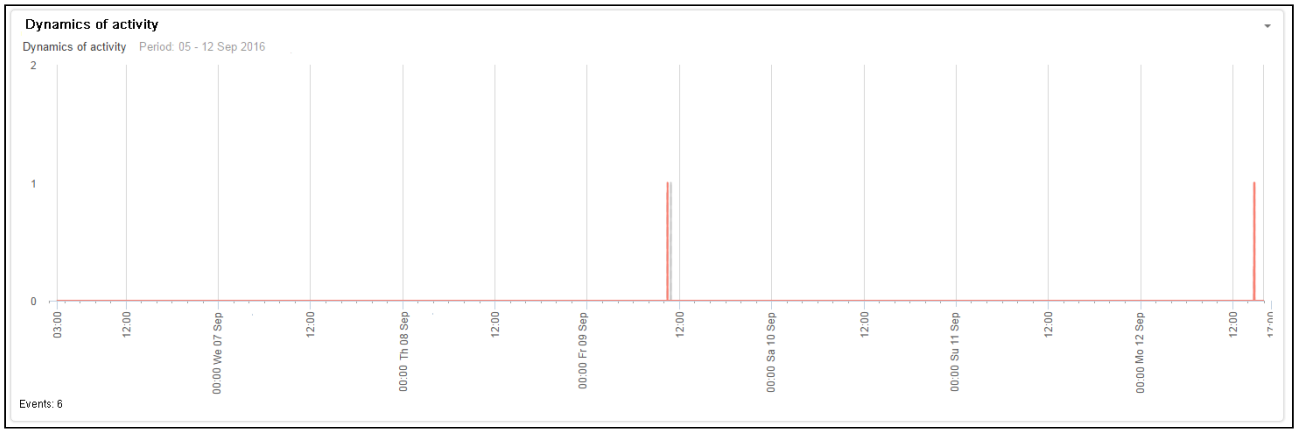
Step 1. Get information about the dynamics of violations. For this:

1. Create a report and add *Dynamics of activity* widget to it.
2. Open the **Query** tab of the widget.
3. In the **Query type** field, select *Advanced query* and specify the following conditions:



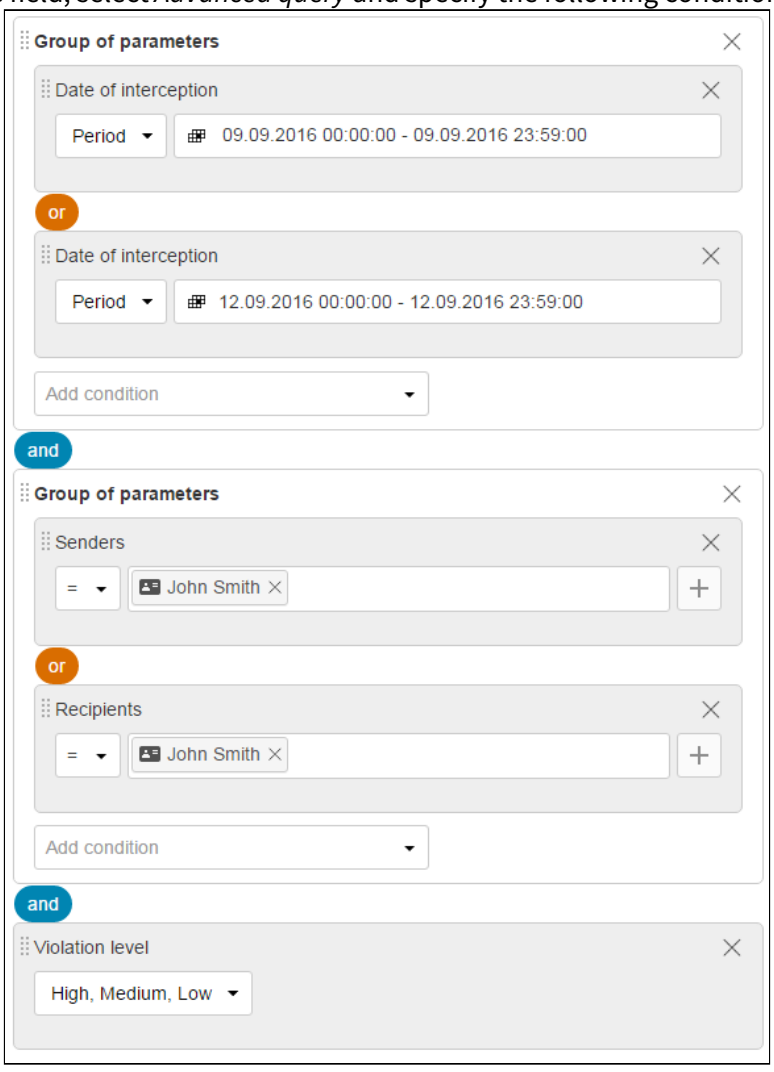
4. Save and run the report.

On the chart, you can see that the employee committed most violations on 09.09 and 12.09.



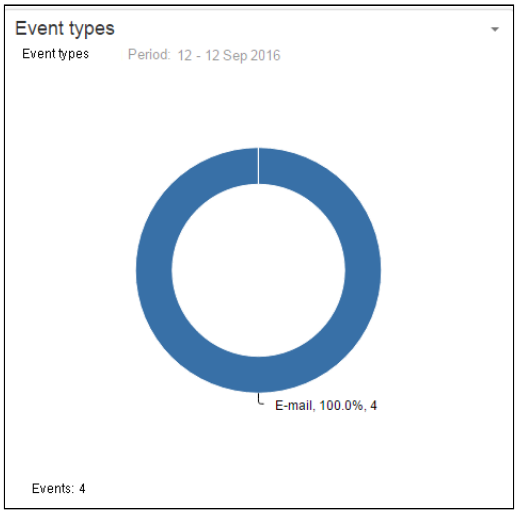
Step 2. Determine the channels through which the data was leaked. For this:

1. Add *Event types* widget to the created report.
2. Open the **Query** tab of the widget.
3. In the **Query type** field, select *Advanced query* and specify the following conditions:



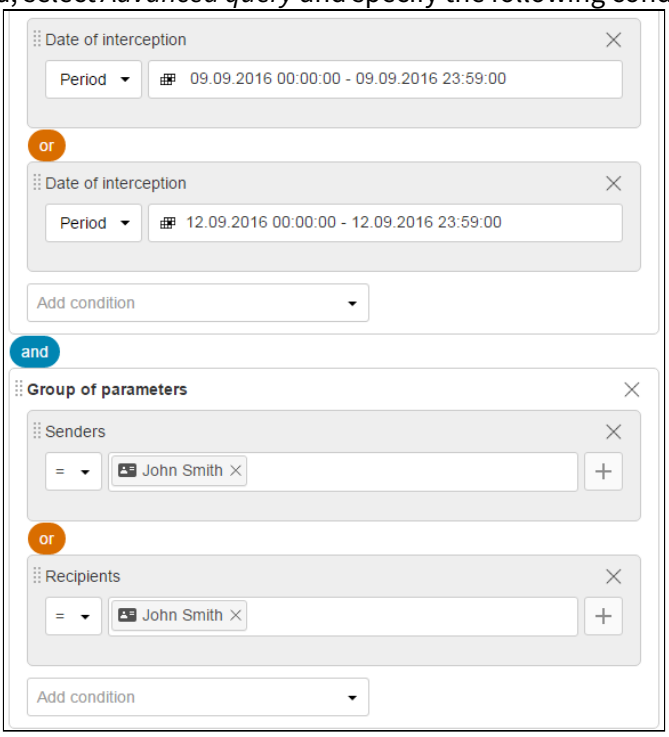
4. Save and run the report.

In the report, you can see, that most violations are related to sending data via email.



Step 3. Determine what protected objects were leaked. For this:

1. Add *Protected objects* widget to the created report.
2. Open the **Query** tab of the widget.
3. In the **Query type** field, select *Advanced query* and specify the following conditions:



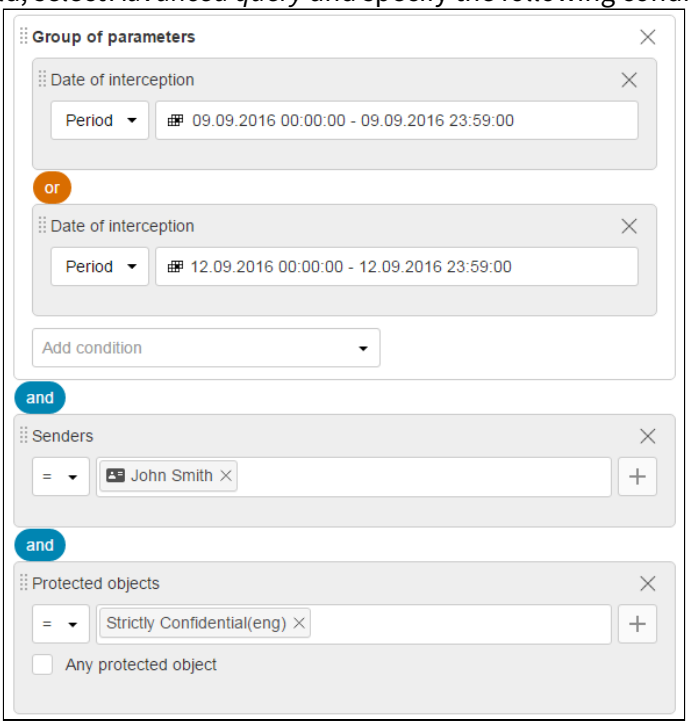
4. Save and run the report.

In the report, you can see, that the employee emailed documents included in the *Strictly confidential information* protected object.



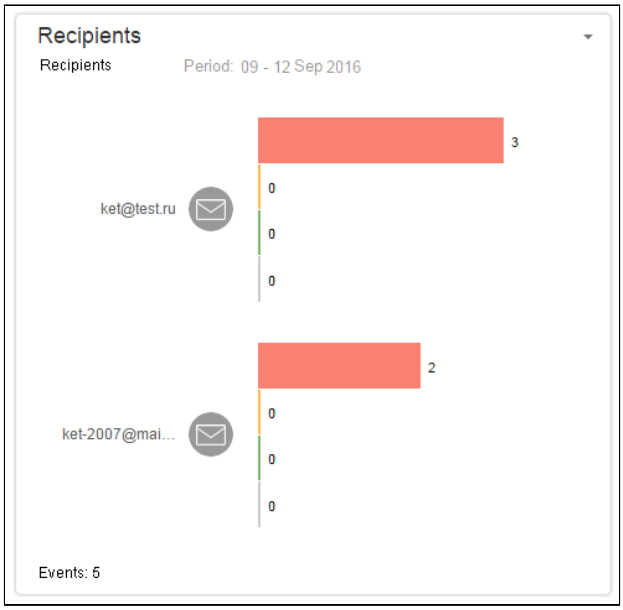
Step 4. Determine, to whom John Smith sent confidential data. For this:

1. Add *Recipients* widget to the created report.
2. Open the **Query** tab of the widget.
3. In the **Query type** field, select *Advanced query* and specify the following conditions:



4. Save and run the report.

In the report, you can see the emails to which confidential data was sent.

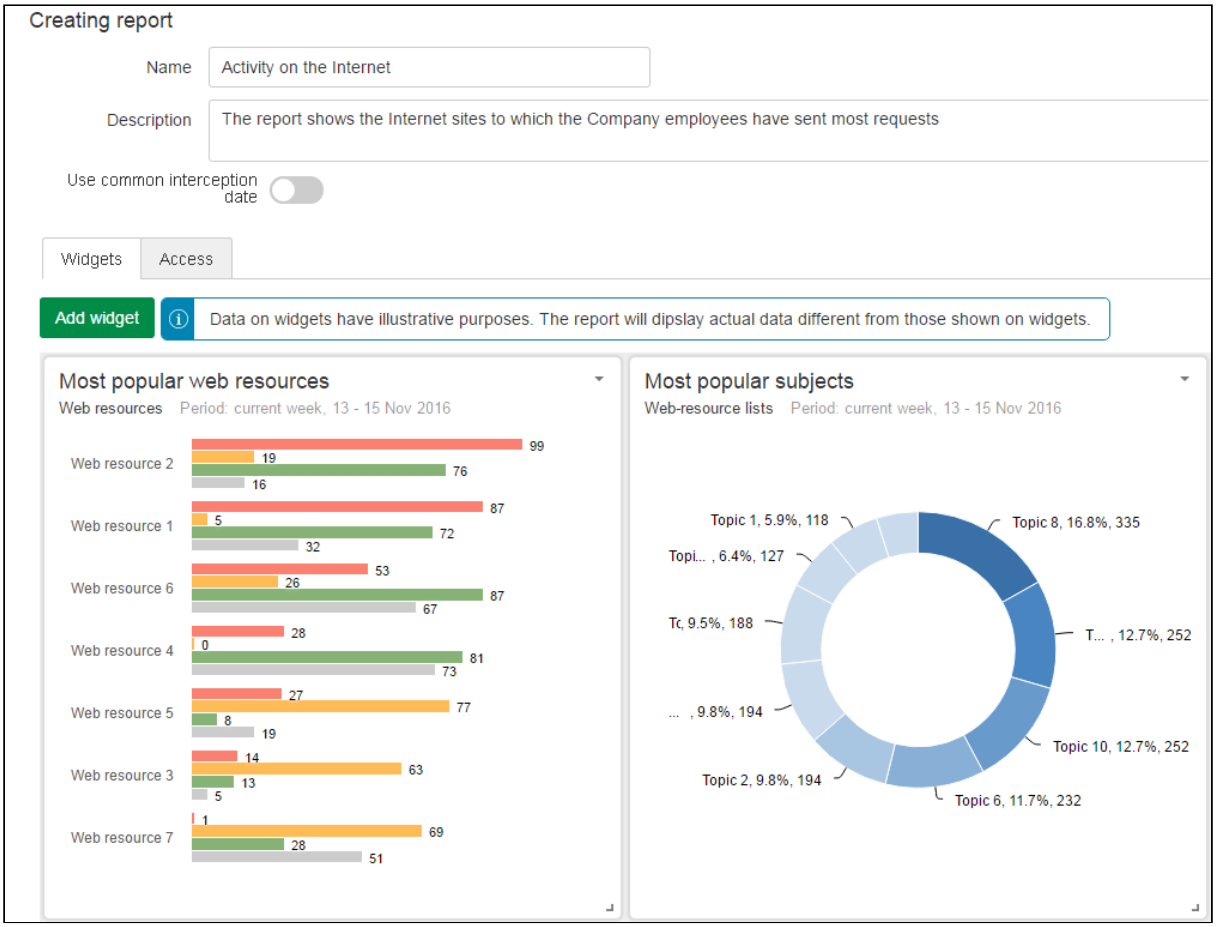


As a result of the investigation, you have determined when, through which channels, and to what recipients the violator leaked confidential data. Now you can easily find the needed events: for this, create a query and specify already known parameters in it (see "Creating Queries"). In the found events, you can see what exactly the violator leaked.

Example 2:

It is required to track the dynamics of attending web resources and the most popular subjects. For this:

1. Create *Activity on the Internet* report.
2. Add a widget and specify *Web resources* statistics type for it.
3. Add one more widget and specify *Web resource lists* statistics type for it.



4. On the **Query** tab, select the required period for each widget and specify additional parameters if necessary.
5. Save and run the report.

4.9 Administrating the System

The section is configured by the System administrator, except for the "Audit" and "Mail notifications" subsection operated by the security officer.

Administrating the System includes the following actions:

- Managing Integration with LDAP Catalogs
- Managing Licenses
- Managing System Users and their Roles
- Healthcheck
- Collecting Diagnostic Data
- Plugins
- User Actions Audit
- Integrity Monitoring
- Configuring Connection to Mail Server
- Configuring Notifications

4.9.1 Managing Integration with LDAP Catalogues

Configuring the synchronization with LDAP catalogues is performed in **Administration -> LDAP Synchronization** section.

> **Warning!**
>
> If you have Adblock Plus installed for the browser then you should disable this extension to provide correct operation of this web console section.

The toolbar is located in the left part of the **LDAP server** workspace.
Above the toolbar, you can find the list of servers for which synchronization with LDAP catalogues has been configured.
The toolbar contains a set of tools for working with the connection.
In the central part of the workspace, parameters for the selected connection, status and synchronization schedule are displayed:

Configuring integration with LDAP catalogues is described below:

- Creating Connection to Server
- Editing Connection to Server
- Deleting Connection to Server
- Running Synchronization with Server Manually

Creating Connection to Server

To create a connection to the server:

1. Go to **Administration** -> **LDAP Synchronization**.
2. On the toolbar, click  **Create**.
3. Specify parameters for a new connection:

Parameter	Description
General parameters	
Server name	Connection identifier used in the Management console **Warning!** It is not allowed to change the server name between the last synchronization and System update
Server type	Indicates what kind of server is used: *Active Directory, Samba DC, Domino Directory, Astra Linux Directory* or *Astra Linux Directory Pro/Free IPA.*
Synchronization	• *Manual* - user starts synchronization manually • *Automatic* - synchronization is performed according to schedule

Parameter	Description
	Important! We recommend that the frequency of automatic synchronization with the Domino Directory server should be 10 minutes or more. We recommend not running manual synchronization more ofter than once every 10 minutes.
Synchronization period	Type of synchronization repeating • *Every N minutes* • *Every N hours* • *Every N days* • *Every N weeks*
Retry parameters	Value of synchronization repeating period if *Automatic synchronization* is selected ***For example***, with the following values: • *Synchronization period* – `Every N minutes` • *Retry parameters* – 60 `minutes` the synchronization will be performed every 60 minutes.
Configuring connection	
LDAP server	The IP address of the server whose LDAP catalogues are synchronized
Connection type	Selecting connection type with Active Directory, Samba DC, Domino Directory, ALD or ALD Pro/Free IPA that will be configured: • Unsecured connection (LDAP) • Secured connection using LDAP + StartTLS protocol • Secured connection LDAPS (SSL) **Warning!** Connection without using a certificate is not secure. When installing a secure connection, you can additionally load a file containing the certificate in .pfx format. **Warning!** If the file that is being loaded contains several user certificates, the System will operate with the first of them and its private key. Correct work requires creating a file with one user certificate. **Note:** For Samba DC, using unsecured connection is not supported. **Warning!** Synchronization using the secure connection is supported only for Active Directory and Samba DC. For Samba DC, you can choose only secured connection using LDAP + StartTLS protocol
Server certificate	Loading a certificate file in PEM format.

Parameter	Description
	Note: For Samba DC, this option is unavailable
User certificate	Loading a certificate file in PEM format. When using a user certificate, it is necessary that you additionally load a file containing a private key of the user certificate. **Note:** For Samba DC, this option is unavailable
Private key of user certificate	Loading a file containing a key in PEM format. **Note:** For details, see "Getting Client Certificate and Server Certificate". **Note:** For Samba DC, this option is unavailable
Use Kerberos protocol	Indicates if Kerberos protocol is used for authentication (protocol of client and server mutual identification). For details, see "Specifics of LDAPS connection and synchronization using Kerberos protocol". **Warning!** You should enable this only when **Use client certificate to authenticate** is disabled. These two principals are mutually exclusive and if you enable both of them, connection will not work.
Global LDAP port	A port for connecting the global LDAP catalogue. **Note:** This setting is available for Active Directory and Samba DC only
LDAP port	Port for connecting a domain catalogue
Use global catalogue	Indicates if the global LDAP catalogue is used for synchronization **Note:** This parameter is only available for Active Directory and Samba DC

LDAP request	**Note:** the setting is required only Active Directory and Samba DC only.
	Filtering attributes which are the full path to the specified catalogue. You can specify only one catalogue in the Active Directory, Samba DC, Domino Directory, Astra Linux Directory or Astra Linux Directory Pro/FreeIPA organizational structure.
	To improve the AD search, you can use separate hierarchy levels of the base:
	`C- countryName`
	`O- organizationName`
	`OU- organizationalUnitName`
	`DC- domainComponent`
	`CN- commonName`

Parameter	Description
	Example for AD, Samba DC, ALD, ALD Pro/FreeIPA: to use the `Users` branch located in the company domain as the search base, enter: `cn=users,dc=company,dc=com` **Example for DD:** a request may contain one or several values: `o=company,ou=department,ou=group` **Important!** To enable a partial synchronization using an LDAP request, you should firth sync with the entire LDAP catalogue (`dc=company,dc=ru`) and then run synchronization using a narrower LDAP request. To update information about groups/ persons/computers for this synchronization, you should run complete synchronization with the entire LDAP catalogue and then a partial synchronization using an LDAP request.
Use user certificate for authentification	Whether is it allowed to use a client certificate for secure connection types instead of entering a password. **Important!** You should use this option only if the **Use Kerberos protocol** option is disabled. These options are mutually exclusive and if you select both options, the connection will not work
Anonymous access	Indicates if the connection to the LDAP server is performed on behalf of an anonymous user **Note:** For Astra Linux Directory Pro and FreeIPA, the option is unavailable
Login	Login to access the synchronization server
Password	Password to access the synchronization server

4. Click **Check connection**, to perform control check of connection to the server.

5. Click **Save**.

Note:

Starting from Traffic Monitor version 7.5, you do not need to fill in the `DnsRootDefault` and `Netbios NameDefault` fields in the **adlibitum.conf** configuration file. AUTH contacts for persons will be automatically added during synchronization with ALD, ALD Pro or FreeIPA. Values of these parameters specified in earlier Traffic Monitor version will be ignored.

Important!

When synchronizing with ALD, we recommend enabling the **Use Kerberos protocol** option in LDAP server settings. If this option is disabled, synchronization with ALD will work only with the **Anonymous access** parameter enabled. In this case, authentification for users imported from ALD will not work.

Encrypted connection support

You can send data over a secure connection for synchronization with LDAP servers only if you choose the following connection types:

- LDAP with StartTLS function, which allows you to establish a secure connection over an existing unsecured one on ports 389 or 3268 if the global catalogue is used. You can synchronize with AD or Samba DC both using Kerberos protocol and anonymous access.
- LDAPS, where data is sent over a secured channel: on ports 636 or 3269 if the global catalogue is used.

Editing Connection to Server

To edit connection to server:

1. Go to **Administration -> LDAP Synchronization**.
2. By left-click select required server.
3. On the toolbar click  **Edit**.
4. Change connection parameters (see "Creating Connection to Server").
5. Click **Check connection**, to perform control check of connection to server.
6. Click **Save**.

Deleting Connection to Server

To delete existing Server connection:

1. Go to **Administration -> LDAP Synchronization**.
2. By left-click select required server.
3. On the toolbar click  **Delete**.

> **Note:**
>
> To delete several connections at a time, highlight them (for example, holding **<SHIFT>** or **<CTRL>**) and click **Delete** .

4. In the opened window click **Yes**.

Running Synchronization with Server Manually

To run synchronization with Server manually:

1. Go to **Administration -> LDAP synchronization**.
2. Left-click at the target server on the left.
3. Click **Starting synchronization** button located on the toolbar.

Information on the synchronization results will be displayed in *Last synchronization, Status of the synchronization, Next synchronization status* strings.

Note:

If the ***Synchronize*** connection attribute has *Every N minutes*, *Every N hours, Every N days* or *Every N week* values, then the automatic synchronization will be performed with specified frequency after last manual running.

Warning!

Synchronization will be performed according to Traffic Monitor server time. If management console is located in different time zone, then specifying synchronization time is required to be done considering difference between time zones of server and management console.

It is required to check connection with LDAP servers after updating from previous versions. To do this, take the following steps:

1. Left-click at the target server.
2. Click on **Check connection.**

Information on the synchronization results will be displayed in a message. If error occurs, set connection parameters.

4.9.2 Managing System Users and their Roles

To manage System users the following entities are used:

- *User* – user's account (see "Users");
- *Role* – a set of rights which can be assigned to User (see "Assigning Role to a User");
- *Visibility scope* – a set of attributes of interception objects: the objects with those attributes will be available to specified users only (see "Visibility Scopes").

Users

Configuring the System users list is performed in the **Administration -> Users and Roles** section, the **Users** tab.

In the work area the list of System users, toolbar and a drop-down menu (defining a number of users displayed at the page) are located.

Account attributes are listed in the following table:

Parameter	**Description**
Login	Name of user account
Full name	User's first name and second name
Email	User's e-mail address
Roles	List of roles assigned to the user
Scopes	List of visibility scopes available for the user

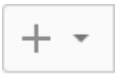
Parameter	**Description**
Description	Note to the account
Status	Indicates whether user role is active or passive

You can perform the following actions while managing users:

- Creating User Account
- Editing User Account
- Deleting User Account
- Changing User Account Password
- Changing User Account State
- Importing User Account from Active Directory
- Assigning Role to a User
- Creating Visibility Scope for User

Creating User Account

To create user account:

1. Go to the **Administration** -> **Users and roles** section.
2. Go to the **Users** tab.
3. On the toolbar click  **Create User**.
4. In the opened window specify account parameters.

Parameter	**Description**
Login	User account name
Status	Indicates if the user account is active or passive
Interface language	Language, which will be assigned to the interface of selected user account
Password	User account password
Confirm password	User account password
Email	User email address
Full name	Full name of the user
Description	User account notes

5. Click **Save**.

Editing User Account

To change existing user account parameters:

1. Go to the **Administration** -> **Users and roles** section.
2. Go to the **Users** tab.
3. In the users list left-click at the target account.
4. Click  **Edit user** on a toolbar.
5. In the opened window change account attributes (see "Users").
6. Click **Save**.

Deleting User Account

To delete user account:

1. Go to the **Administration -> Users and roles** section.
2. Go to the **Users** tab.
3. In the users list left-click at the target account.
4. On the toolbar click  **Delete user**.

   > **Note:**
   >
   > To delete several accounts in one action, select them from the list (for example, by pressing **<SHIFT>** or **<CTRL>**) and click **Delete user** .

5. In the opened window click **Yes**.

Changing User Account Password

To change user account password:

1. Go to the **Administration** -> **Users and roles** section.
2. Go to the **Users** tab.
3. In the users list left-click at the target account.
4. On the toolbar click **Change password**.
5. In the opened window enter a new password to **Password** and **Confirm password** fields.
6. Click **Save**.

Changing User Account State

To change account state:

1. Go to the **Administration -> Users and roles** section.
2. Go to the **Users** tab.
3. In the users list left-click at the target account.
4. On the toolbar click  and choose **Activate user** or **Deactivate user**.

> **Note:**
>
> You can change a status of any account except of **Administrator**.

Importing User Account from Active Directory

You can easily create users by importing their accounts from Active Directory, Samba DC, Domino Directory, Astra Linux Directory, Astra Linux Directory Pro or FreeIPA.

> **Important!**
>
> If AdBlock extension is used in your browser, then disable this extension before importing user accounts, as AdBlock blocks the import.

To import user account:

1. Go to the **Administration -> Users and roles** section.
2. Go to the **Users** tab.
3. On the toolbar, click  **Import users from LDAP**.
4. In the opened window, specify LDAP server which stores the required account.

   > **Note:**
   >
   > You can enter a part of login name to the **Search** field and click **Search**.

5. Flag required user accounts.
6. Click **Save**.

Assigning Role to a User

To assign role to a user:

1. Go to the **Administration -> Users and roles** section.
2. Go to the **Users** tab.
3. In the users list left-click at the target account.
4. Click on the toolbar.
5. Choose **Set role** in the list (see "Roles").
6. Click **Save**.

Creating Visibility Scope for User

To create a visibility scope for a user:

1. Go to the **Administration** -> **Users and roles** section.
2. Open the **Users** tab.
3. In the list of users, click the required account.

4. From the **Scopes** list (see "Visibility Scopes"), set a visibility scope for the user. If you do not specify any visibility scope for the user, then all interception events and screenshots will be unavailable for this user.
5. Click **Save**.

Roles

To control redundant access to system settings, policies of different structural departments, interception objects and other important information, there is role system of access rights differentiation in InfoWatch Traffic Monitor.

Role is a set of rights which can be assigned to user. Assigning a role to user is described in "Assigning Role to a User".

Initially, there are two predefined roles and the two preset user – roles **Adminitrator** and **Security officer**, which are accordingly assigned to Administrator and Officer users.

Administrator role provides an opportunity to carry out the initial configuration of the system (Managing users, roles, visibility scopes, licenses and LDAP synchronization).

Security officer role has all rights except for initial setup.

Configuring the roles list is performed in **Administration -> Users and Roles** section, **Roles** tab.

In the work area the list of System users, toolbar and a drop-down menu (defining a number of roles displayed on the page) are located.

Role attributes are listed in the following table:

Attribute	Description
Name	Role name
Users	First name and second name of the user
Description	Comment to a role

You can perform the following actions while managing roles:

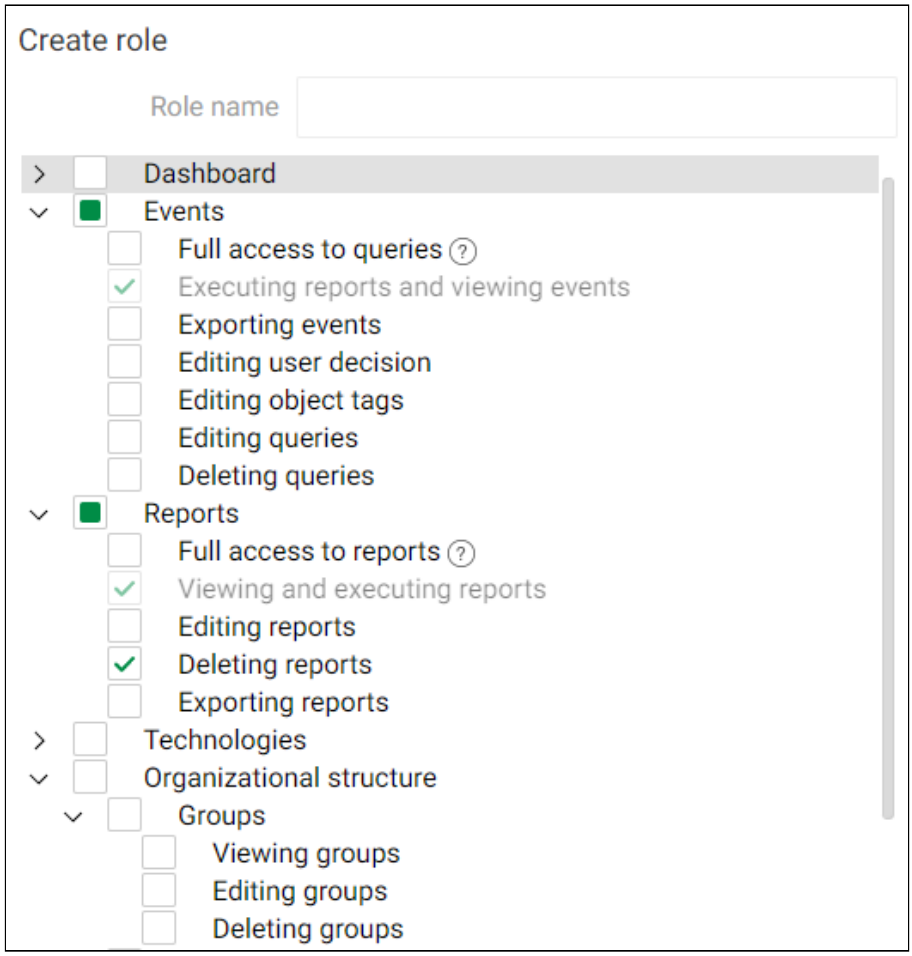
- Creating a Role
- Editing a Role
- Deleting a Role

Creating a Role

To create a new role, follow the steps below:

1. Go to **Administration** -> **Users and roles** section.
2. Go to **Roles** tab.
3. On the toolbar, click  **Create role**.
4. In the opened window specify role attributes. Flag the privileges you want to assign to the role.

> **Note:**
>
> To expand/collapse privileges list, click  or respectively.



> **Note:**
>
> **Viewing roles** and **Viewing visibility scopes** privileges are available by default when selecting **Roles** and **Visibility scopes**.

5. Click **Save**.

Editing a Role

To change parameters of an existing role, follow the steps below:

1. Go to **Administration -> Users and roles** section.
2. Go to **Roles** tab.
3. In the users list left-click at the target role.
4. On the toolbar, click **Edit role**.
5. In the opened window change role attributes. Flag (unflag) the privileges you want to assign (unassign) to the role.

> **Note:**

To expand / collapse privileges list, click ▶ or ◢ accordingly.

> **Note:**
>
> **Viewing roles** and **Viewing visibility scopes** privileges are available by default when selecting **Roles** and **Visibility scopes**.

6. Click **Save**.

Deleting a Role

To delete role:

1. Go to **Administration -> Users and roles** section.
2. Go to **Roles** tab.
3. In the users list left-click at the target role.
4. Click ⊠ **Delete role**.

> **Note:**
>
> To delete several roles at a time, select them in the list (for example, by holding **<SHIFT>** or **<CTRL>**) and click **Delete role**.

5. In the opened window click **Yes**.

> **Note:**
>
> You can change any role except for **Administrator** and **Security officer**.

Visibility Scopes

A visibility scope allows you to perform additional access control to intercepted objects. A visibility scope is created from attributes of intercepted objects. The user will only see those events, whose attributes match the attributes configured in the visibility scope.

Several visibility scopes can be specified for one user.

> **Example:**
>
> The *officer* user 1 has a visibility scope with a person *Smith* and a tag "1". In this case, the *officer* user can only view events with the participation of Smith and tagged "1".

Assigning visibility scopes to user is described in "Creating Visibility Scope for User".

To configure a list of visibility scopes, go to **Administration** -> **Users and Roles** section, **Scopes** tab.

In the working area, you can find a list of scopes, a toolbar, and a drop-down menu.

In the list of scopes, user scopes are displayed.

The toolbar contains a set of tools to work with visibility scopes:

-  - to create a new visibility scope. Double-click a visibility scope to edit it.
-  - to delete an earlier created visibility scope. Preset visibility scopes cannot be deleted.

The  drop-down menu defines the number of scopes to be displayed on the page.

Visibility scope attributes include the scope name and its short description.

You can perform the following actions while managing visibility scopes:

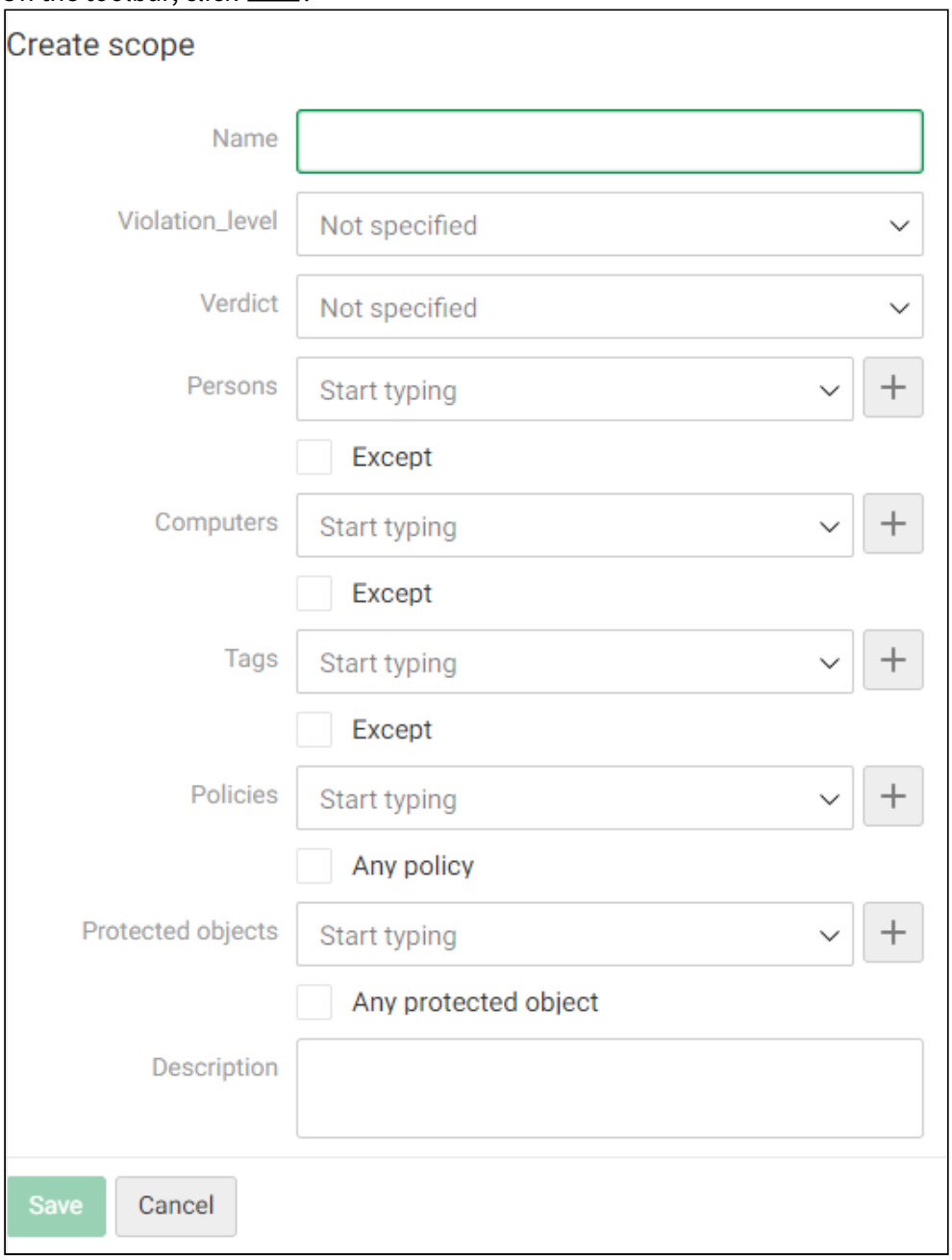
- Creating Visibility scope
- Editing Visibility Scope
- Deleting Visibility Scope

Creating Visibility scope

To create a visibility scope:

1. Go to the **Administration** -> **Users and Roles** section.
2. Open the **Scopes** tab.

3. On the toolbar, click [+].



4. In the **Creaty scope** window, specify the following parameters:
   a. *Name* - enter the name of the visibility scope.
   b. *Violation level* - choose the level from a drop-down menu.
   c. *Verdict* - choose from a drop-down menu.
   d. *Persons*:
      i. enter the first characters of the username, group, or status and choose the required value from a drop-down list
      or
      ii. click [+] and in the window that opens, select required checkboxes on the **Persons**, **Groups**, and **Statuses** tabs. Click **Add**.

e. *Computers* – as described in item d.
f. *Tags*:
    i. enter the first characters of the tab name
    or
    ii. click  and in the window that opens, select required checkboxes in the list of tags. Click **Add**.

    If you want to exclude some persons, computers, or tags from the selection of events and screenshots, select the **Except** option. Fill in the field that appears as described in the previous item. If mutually exclusive rules are selected within the same visibility scope, then all events for the user will be unavailable.
g. *Policy* – as described in item f.
h. *Protected object* – as described in item f.
i. *Description* - enter a short description.

5. Click **Save**.

> **Example:**
>
> If you do not select any value in a field of the visibility scope, then event filtering results will not take this field into account. So if you do not select any person, events of all persons will be available to the user.

Editing Visibility Scope

To change the parameters of a visibility scope:

1. Go to the **Administration -> Users and roles** section.
2. Open the **Scopes** tab.
3. Click the required visibility scope.
4. In the area that opens, edit the required parameters like when creating the scope (see 'Creating visibility scope').
5. Click **Save**.

Deleting Visibility Scope

To delete a visibility scope:

1. Go to the **Administration** -> **Users and roles** section.
2. Open the **Visibility scopes** tab.
3. On the toolbar, click .

> **Note:**
>
> To delete several visibility scopes at a time, select them in the list (for example, by holding **<SHIFT>** or **<CTRL>**) and click **Delete**.

4. In the window that opens, click **Yes**.

4.9.3 Managing Licenses

Warning!

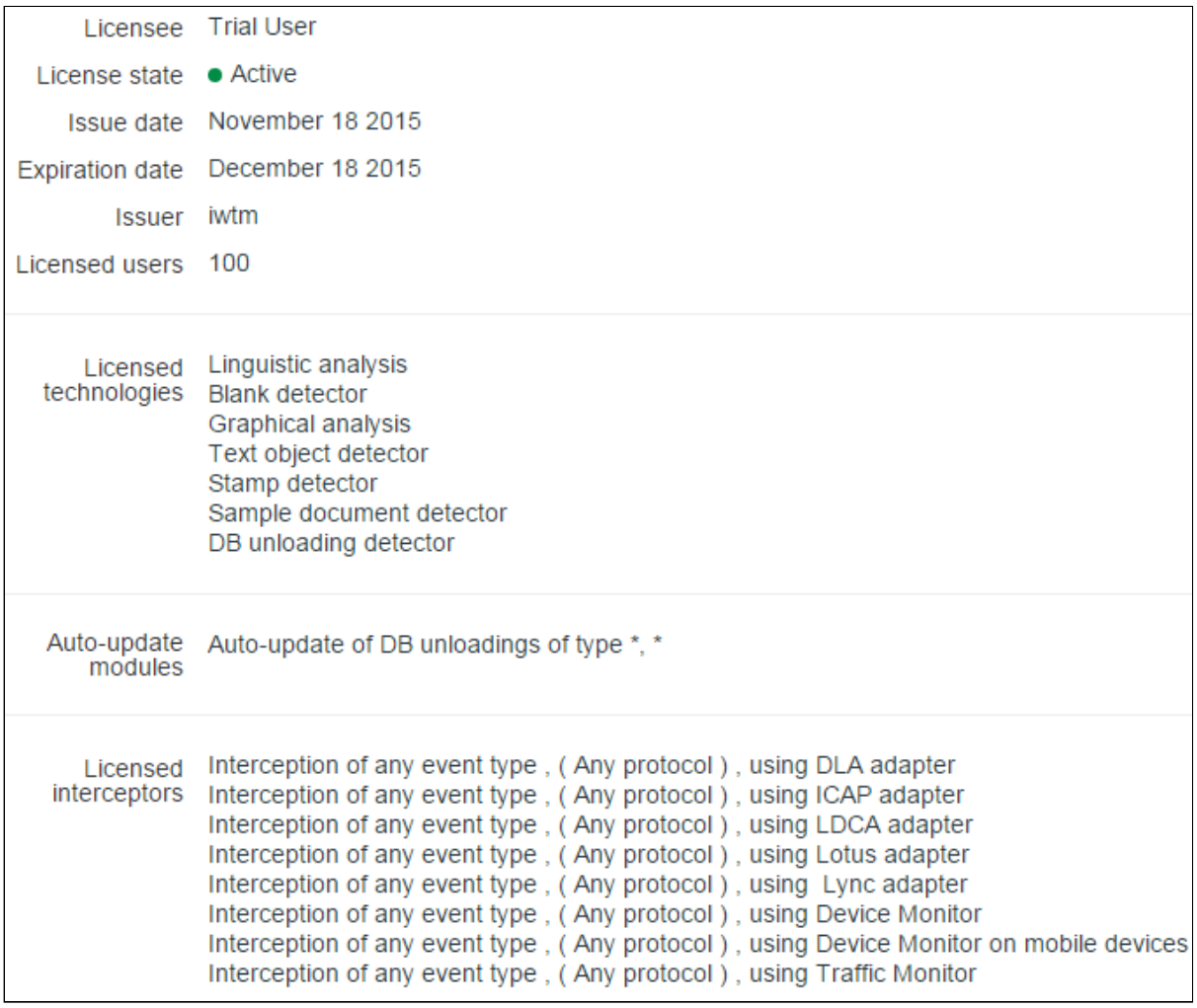
The System licensing is described in the document "InfoWatch Traffic Monitor. Administration Guide", "Licensing" article.

Licenses are managed in the Management Console, the **Administration** –> **Licenses** section:

- In the left part of the working area, you can see the list of licenses and a toolbar.
- In the right side of the working area, you can see information on the selected license.

Note:

Editing licenses is unavailable. You can only upload a new license or delete an earlier created license.



You can perform the following actions with licenses:

- Installing a License

- Deleting License
- Requesting a License

Checking License Validity

Information about licensed technologies and interceptors, state, expiration date and number of licensed users, are available in **Administration –> Licenses**.

To check license validity:

1. Go to **Administration -> Licenses**.
2. Make sure, that **Expiration date** contains future date.
3. Make sure, that **Licensee** field value matches Licensee parameter of **license.conf** configuration file, located in `/opt/iw/tm5/etc` directory.

Installing a License

To install a license:

1. Go to **Administration -> Licenses**.
2. Click  **Add license** on the toolbar.
3. Click **Upload** in the pop-up menu.
4. Choose required license.lic file and click **Open** in the dialog box.
   Information about licenses and licensed technologies and interceptors will be shown in the **License adding** pop-up window.
5. Click **Add**.
6. Click **Yes** in the dialog box.

Browser page will be refreshed and new license will be added to the list. You may leave or remove the expired licenses at your option.

Deleting License

To delete license:

1. Choose the target license from the list.
2. On the toolbar click  **Delete**.

   > **Note:**
   >
   > To delete several several licenses at a time, select them in the list (for example, by holding **<SHIFT>** or **<CTRL>**) and click **Delete** .

3. In the opened windows press **Yes**.

Requesting a License

To request a license:

1. Go to **Administration** - **Licenses**;

2. On the toolbar, press **Request license**.
3. Send an automatically formed email, adding description, if necessary.

4.9.4 Healthcheck

You can monitor the state of each server on which the System is deployed in **Administration**->**System state** section of the Management Console.

For each server that is used in the System, indicators are listed in the table:

Parameter	Details
Current System load	OK - load average: 0.21, 0.15, 0.19
Number of active users	USERS OK - 3 users currently logged in
State of local mail server	SMTP OK - 0.013 sec. response time
System time deviation	NTP OK: Offset -0.01090276241 secs
Errors in the alert log.	OK - no errors found in log
Size of database alert log.	OK - size of PostgresSQL system log is 9047 bytes
State of PostgreSQL database.	OK - database postgres (0.003083 sec.)
Server availability	PING OK - Packet loss = 0%, RTA = 0.06 ms
Free space in root partition	DISK OK - free space: / 96362 MB (71% inode=98%):
State of time syncronization service	OK - ntpd (pid 2491) is running...
State of Syslog service	OK - 'rsyslogd' is running
Server availability via SSH	SSH OK - OpenSSH_5.3 (protocol 2.0)
Swap usage	SWAP OK - 77% free (6145 MB out of 8015 MB)
Queue of processing actions specified in policies applied to the events.	OK - Blackboard queue: 0 item(s), 0.000 MBytes
Number of errors occurred when processing actions from policies applied to events.	OK - Blackboard-errors queue: 0 item(s), 0.000 MBytes
Presense of memory dumps	OK
State of System components	OK
Number of errors occurred when indexing events by INDEXER service.	OK - index_error queue: 0 item(s)
TM_PG_INDEXER_QUEUE	OK - index_queue queue: 0 item(s)
Queue for loading to storage	OK - DB queue: 0 item(s), 0.000 MBytes
Queue processing errors	OK - Errors queue: 0 item(s), 0.000 MBytes
Queue processing mail traffic	OK - SMTP queue: 0 item(s), 0.000 MBytes
Number of errors occurred when processing events by IW_LOADER and IW_XML2LIR...	OK - XML2LIRO-errors queue: 0 item(s), 0.000 MBytes
Number of running processes	PROCS OK: 283 processes with STATE = RSZDT
Free space in /var partition	DISK OK - free space: / 96361 MB (71% inode=98%):

For each indicator, the following information is displayed:

- **State** – the current value of the indicator:
  - 🔴 – CRITICAL, the parameter value is higher than the critical threshold;
  - 🟡 – WARNING, the parameter value is a warning zone (if this zone exists);
  - 🟢 – OK, the parameter value is normal.
- **Parameter** – indicator name.
- **Details** – detailed information on healthcheck results.

> **Warning!**
>
> If the indicator value cannot be obtained, it is assumed, that the current value is higher than a critical threshold.

Values are refreshed:

- Every 5 minutes – for parameters:
  - DB Alert Log Errors
  - Swap usage
  - DB Alert log Size

- Every 10 minutes – for parameters:
  - SSH availability
  - Database Status
  - Oracle TNS Status
- Every 360 minutes – for **NTP time deviation** parameter
- Every 30 minutes – for all other parameters

To refresh the values manually, click **Refresh**.

Configure Notifications

To configure the System condition notifications:

1. Go to **Administration** - **System condition**;
2. Click the button "**Configure notifications**";
3. Enable the option "**Enable notifications**".
4. Specify the values for the following parameters:

Parameter	Description
Mail prefix	Mail prefix is used to sort out the e-mail messages from different monitoring systems. The value you've entered is to be added in the beginning of the line "Subject" of the messages to be sent. The default value is: `IWTM`
Recipients	Email of recipient/recipients. The default value is: `nagios@localhost`

5. Click *Send text message* to check if the settings are correct.
6. Click **Save**.

Notifications will contain the following information:

- Indicator name
- Name of the server where controlled indicator exceeds the threshold value
- IP address of this server
- Current status of the indicator
- Date and time when the indicator threshold value was exceeded
- System message from the source

4.9.5 Collecting Diagnostic Data

Collecting diagnostic data is performed in **Administration** -> **Services** section.

Data collection mode	Description
Normal	Collecting information about System logs, configuration and initial installation.
Extended	Collecting detailed debug information, including errors, content of processes working memory and their emergency stop.

Diagnostic information is to be collected from the following sources:

Data type	Path to files

Logs	`/var/log/infowatch/*.log`
	`/var/log/nagios/nagios.log`
	`/root/iwsetup-install-logs/*`
	`/var/log/nagios/status.dat`
	`/home/oracle/addm/logs/* -` If Oracle DBMS is installed
	`/u01/app/oracle/diag/rdbms/iwtm/iwtm/trace/alert_iwtm.log -` If Oracle DBMS is installed
	`/u01/postgres/pg_log/* -` If PostgreSQL DBMS is installed

Configuration information	`/opt/iw/tm5/etc/*.conf`
	`/opt/iw/tm5/etc/scripts/*.lua`
	`/opt/iw/tm5/etc/config/lua/vademecums/*.info`
	`/opt/iw/tm5/etc/config/lua/vademecums/vademecum.list`
	`/etc/nagios/*`
	`/etc/nagios/objects/*`

Logs and scripts of initial installation of the System	`/root/iw*`

To download a report with results of the last diagnostics:

1. Go to **Administration** -> **Services** section.
2. On the left, select the TM server you need.
3. Press **Collect data**.
4. Select the mode, by marking one of the fields: *Normal* or *Extended*.
5. Press **Run**.
6. Wait till completion of diagnostic information collection.
7. Click the **Results of the latest diagnostics are available** link to download the archive in `dd-mm-yyyy_hh-mm-ss` format.

> **Warning!**
>
> If diagnostics has not been performed earlier, downloading the diagnostics results is unavailable.

To download a report with logs of service:

1. On the left, select the TM server you need.
2. Press **Save** in **Logs** column opposite one or several running services you need. Logs of stopped service cannot be downloaded.

Note:

When working on OS Microsoft Windows it is possible that the downloaded log will be empty. In this case it is recommended to install the program *UnZip* (for Windows) and use it to unzip the archive.

4.9.6 User Actions Audit

The System provides means to track user activity in Management Console.

To review audit events and apply search filters go to **Administration** -> **Audit**.

Audit events section contains the following information from the System:

- log in to System, logouts, switch between InfoWatch products, authorization temporary blocks;
- objects related to access control management (Users, Roles, Visibility Scope);
- user actions related to perimeter management;
- user interactions with organizational structure (persons, groups, computers);
- users interactions with System objects (queries, reports, email notifications, policies, rules, elements of technologies, etc.);
- modifications in System configuration (creation, editing, cancelling);
- modifications in System objects by external systems.

Important!

Audit events section does not contain:

- Information on configuration changes from rollbacks. In this case, only the event of cancelling will be created;
- Information on creation of groups, persons or computers in the process of synchronization with LDAP server, as well as their old values if changed by user;
- Information on any changes to report widget, except for the name change.

After updating to current version, audit events for actions with policy rules, persons, groups and computers that were registered in earlier versions of System will not be changed.

For more on working with audit events, see the following subsections:

- Audit Events
- Extended Information
- Filtering and search

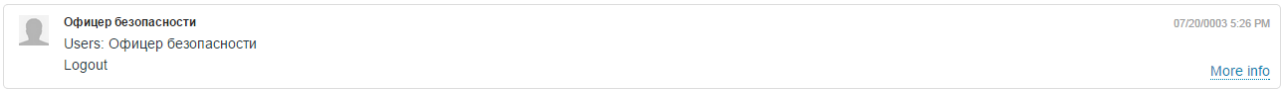
Audit Events

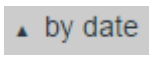
The **Audit Events** area is located in the **Administration -> Audit** section.

The **Audit Events** area displays results of **Search filters**. This is a list of audit events in the form of panels with the following attributes:

- The name of the user who took an action;
- The name of the object the action applied to;
- The type of action that was taken by the user;

- Date ana time of the registered user action;
- Extended information on the audit event (the More info link).



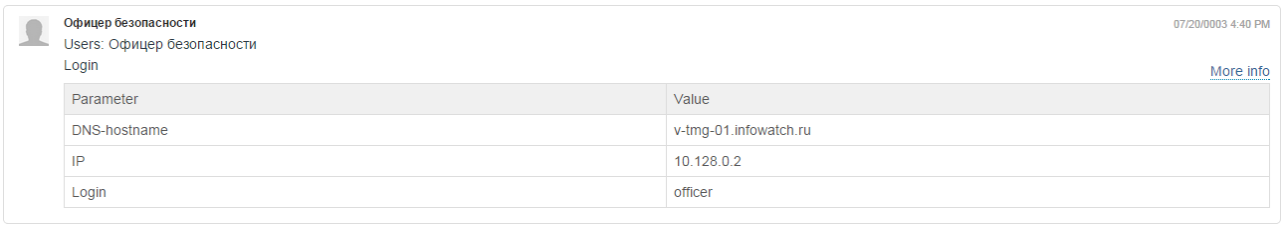
To sort audit events by the creation date, click  in the left upper corner.

Extended Information

The audit event may contain additional information: the list of modified parameters, their new and old values, modification data. To view this data, click **More info** on the desired panel.

For example, when a user logs into the System, the event has the following parameters:

- DNS-name of the computer from which the user logged into the System;
- The IP address of the computer from which the user logged into the System;
- The name of the user who logged into the System.



Warning!

Audit events data can be different depending on *Object* and *Action*.

Filtering and search

To view required audit events, you can use full-text search or filters in the **Search filters** area of the **Audit events** section:

1. In the search bar, type the full name of the desired object. The name should contain at least three letters. To find long word forms, you can type the first three letters of the name and then use the * character.
2. If necessary, select the user name from the **User** drop-down list (see "Managing System Users and their Roles").
3. If necessary, select the user action from the **Action** drop-down list.
4. If necessary, select the object in the System from the **Object** drop-down list.
5. If necessary, select the **Date** parameter and then select:
    a. **All time**, if you need the list of events created for all time
    or
    b. **Period** to specify the start and end dates of the period. Audit events for the specified period will be displayed. Click **Apply**.

You can use both the search bar and filter parameters (some or all of them) at the same time. In this case, found audit events will satisfy both the specified attribute values and the search query.

To save free space in the database, you can set the **Audit events storage period (days)**, after which events will be deleted.

> **Important!**
>
> Audit events and Traffic Monitor events may have different storage periods. If audit events have a larger storage period, there can be audit events without related Traffic Monitor events, as related Traffic Monitor events may already be deleted.

4.9.7 Integrity Monitoring

Integrity monitoring is intended to monitor system foles state. Primary reference amount is automatically generated by the System.

System files integrity monitoring is described in the following sections:

- Manual Integrity Monitoring
- Automatic Integrity Monitoring
- Accepting Result as Standard

Manual Integrity Monitoring

To check system files integrity:

1. Go to **Administration - Integrity monitoring**;
2. In the central part of the working area click **Scan files**.

> **Note:**
>
> In the process of integrity check the **Integrity check is being performed** message is being displayed. Upon check completion, you will see the message with date and time of the last check.

Automatic Integrity Monitoring

To configure system files automatic integrity monitoring:

1. Go to **Administration - Integrity monitoring**;
2. In the central part of the working area enable **Automatic check** setting.
3. In the **Schedule** field set the time of integrity check using **up** and **down** arrows.
4. Click **Save**.

Accepting Result as Standard

To accept result of integrity check as standard:

1. Go to **Administation - Integrity monitoring**;
2. In the central part of the working area click **Accept result as standard**.

4.9.8 Plugins

The System uses plugins to connect additional interceptors. The extension makes it possible to receive events from external interceptors, add user attributes of events, automatically update sample unloadings and provide data to external systems.

Any API/Public API connectors of external systems must be registered in TM by adding a new plugin.

A plugin is an archive in a ZIP format, which contains:

- **licenses** folder with license files;
- **icon** folder with icons for registered contacts and event types;
- **manifest.json** file with information about the plugin. For plugins that are used for receiving events and plugins used for updating sample unloadings, the file structure is different.

> **Note:**
>
> Names of files in the plugin should contain only Latin characters and/or numbers.
>
> Folders **licenses** and **icon** are optional. License files and files with pictograms can be located in the root folder.

Default plugins **InfoWatch Device Monitor**, **InfoWatch Sample documents Autoupdate Adapter** will be displayed in Traffic Monitor management console in case the System contains the active license installed (see "Managing Licenses").

For external systems which are the sources of events the file **manifest.json** should contain the following information:

Name	Compulsory	Description
Version	Yes	Plugin version
Developer company ID	Yes	Matches the company name in the license
Used preinstalled event types, contacts and protocols	No	List of preinstalled event type and protocols intercepted by this plugin
Name	Yes	Plugin unique name
Description	No	Plugin description
"Preinstalled" attribute	No	Whether it is included in the System
Registered event types, contacts, and protocols	No	Contains the following data: • Type of registered events with specifying the service type • Protocols • Actions

Name	Compulsory	Description
		• Code of interceptor type for InfoWatch plugins • Event type names localization at least in one language • Types of registered contacts and their localization at least in one language • Files with icons of registered contacts and event types
Unique identifier	Yes	Unique 128-bit identifier (UUID) of the plugin

For external systems which are the sources of events the file **manifest.json** should contain the following information:

Name	Compulsory	Description
Version	Yes	Plugin version
Developer company ID	Yes	Matches the company name in the license
Name	Yes	Plugin unique name
Data receiving systems	Yes	List of identifiers for systems receiving data from TM that are registered in the plugin
Description	Yes	Plugin description
"Preinstalled" attribute	No	Whether it is included in the System
Unique identifier	Yes	Unique 128-bit identifier (UUID) of the plugin

For external systems receiving data from TM, the **manifest.json** file should contain the following information:

Name	Compulsory	Description
Version	Yes	Plugin version
Developer company ID	Yes	Matches the company name in the license
Name	Yes	Plugin unique name
Data receiving systems	Yes	List of identifiers for systems receiving data from TM that are registered in the plugin

Name	Compulsory	Description
Description	Yes	Plugin description
"Preinstalled" attribute	No	Whether it is included in the System
Unique identifier	Yes	Unique 128-bit identifier (UUID) of the plugin

In **Plugins** sections, you can perform the following actions:

- Adding Plugin
- Deleting Plugin
- Working with Tokens

Warning!

Plugins and tokens are deleted from the System when deleting the DB schema (see "*Infowatch Traffic Monitor. Installation Guide*", "Deleting the Database Schema" article). To restore the Device Monitor plugin:

1. Create the file **/opt/iw/tm5/www/backend/protected/runtime/first_run** on behalf of **iwtm** user.
2. Restart **iw_kicker** process:
   `iwtm restart kicker`

Other plugins should be added manually (see "Adding Plugin").

Adding Plugin

To add plugin:

1. Go to **Administration - Plugins**;
2. In **Plugins** are press .
3. Press **Add**.
4. Review plugin's description and press **Install**.

Note:

To update plugin, add renewed version.

Deleting Plugin

To delete plugin:

1. Go to **Administration - Plugins**;
2. In **Plugins** area press .

3. Press **Yes** to confirm deletion.

> **Warning!**
>
> Preset plugins cannot be deleted.

Working with Tokens

Tokens are designed for authorizing an external which uses Push API (sending events from third-party interceptors to TM) and Public API (loading external unloadings from DB to TM and access to TM data for external systems). When the plugin is added, a token is created automatically. (see "Adding Plugin").

For InfoWatch Device Monitor, a token is created automatically and is available in **Administration** -> **Plugins** -> **Tokens** section of the Management Console.

The following actions with tokens are available:

- Adding Token
- Editing Token Data
- Updating Token Value
- Copying Token
- Deleting Token

Adding Token

o add token:

1. Go to **Administration** - **Plugins**;
2. Choose plugin in **Plugins** area;
3. Go to **Tokens** tab;
4. Press .

> **Note:**
>
> Token value is generated automatically upon token creation and can be defined by user.

Editing Token Data

To edit token data:

1. Go to Administration - Plugins;
2. Choose plugin in **Plugins** area;
3. Go to **Tokes** tab;
4. By double-clicking the left mouse button in the *Name* column or *Description* type in the neccesary data.

Updating Token Value

In case token is compromised or there is a likehood, that it leaks to third-parties, we need to generate a new token value.

To update tokem value:

1. Go to **Administration - Plugins**;
2. Choose plugin in **Plugin** area;
3. Go to **Tokens** tab;
4. Click .

Copying Token

To copy token value to the clipboard:

1. Go to **Administration - Plugins**;
2. Choose plugin in **Plugins** area;
3. Go to **Tokens** tab;
4. Click .

Deleting Token

To delete token:

1. Go to **Administration** - **Plugins**;
2. Choose plugin in **Plugins** area;
3. Go to **Tokens** tab;
4. Press .

4.9.9 Configuring Connection to Mail Server

In the **Administration** -> **Mail server** section, you can specify an SMTP server that will be used for sending notifications about triggered rules (see "Configuring Notifications") and the state of the System (see "Healthcheck").

To configure the connection:

1. In the **Sender's email address** field, specify the address that will be used for sending notifications.
2. Choose the server type. Possible choices:
    - **Embedded in Traffic Monitor** - select this option if you are using a local Traffic Monitor mail server with anonymous access;
    - **External** - select this option if you are using an external server. for example, if sending emails to external servers without authorization is prohibited in your company.
3. If an external server is used, specify the server parameters:
    - **SMTP server address**;
    - **Port**;
    - **Login** - optional parameter;
    - **Password** - optional parameter;

- **Encryption** - If you select the encrypted mode, then STARTTLS protocol and NTLM authentication will be used for connection. To get notifications from Nagios monitoring system, select a mode without encryption.

When you have specified all connection settings, click **Check connection**.

4. Click **Save**.

4.9.10 Configuring Notifications

In the **Administration** -> **Notifications** section, you can configure templates for emails which are sent when the security policy is triggered.

Notifications can be sent to:

- **An employee** who has violated a security policy. If a rule is triggered, the employee is notified that his/her actions violate the corporate security policy. If the System operates in the inline mode, employees also get timely notifications when:
  - their emails are blocked or quarantined and await a decision of the security officer;
  - the security officer has decided on the quarantined email (whether to block it or send it to the recipient).
- **A security officer**. Getting timely notifications about incidents makes it easier for the security officer to promptly respond to important incidents.
- **Other interested persons**, for example, the head of an employee who has violated a security policy.

To create a notification, click  on the toolbar to the left (see "Creating Notification"). Added notifications are used in policy rules: in the **Actions when the rule is triggered** area, **Send notification** field, click  and select the required notification (for details, see "Creating Rules").

> **Note:**
>
> If necessary, you can create or edit notifications when configuring a rule in the **Policies** section. Editing and deleting notifications is only available from the **Notifications** section.

To edit a notification, choose the required notification in the list and click  on the toolbar.

While creating/editing a notification, you can test the resulting template (see "Testing Notification").

To copy an earlier created notification, choose it in the list and click  on the toolbar. The notification copy will be added to the list.

To delete a notification, use  button on the toolbar.

> **Note:**
>
> In this case, the notification is also deleted from all policies where it is used.

Besides user-created notifications, there are also preset notifications in the System (see "Preset Notifications").

Creating Notification

Purpose:
Create a notification that can be sent when rules are violated.

Solution:

1. Go to the **Administration** -> **Notifications** section.
2. On the toolbar to the left, click .
3. In the form that opens, enter the notification name.
4. Choose notification recipients. Possible choices:
    - **Initiator of event** - select this field to create a template that will be sent to the event initiator;
    - **Custom recipients** - select this field and click  to add recipients. In the window that opens, go to the required tab:
        - On the **Persons** and **Security officers** tabs, choose required values from the list. You can sort values in the list by the person/user name.
        - On the **Email** tab, you can enter email addresses of recipients who are not in the list of persons or security officers.
        - On the **Head** tab, enable the switch if you want to notify the head of the event initiator.

    Once you have specified all required recipients, click **Save**.
5. In the **Email template for different verdicts** open the tab with a verdict for which you want to create a template. The following tabs are available:
    - **Allowed** - the rule has the *Allowed* verdict, however, the employee should be informed that his/her actions violate the security policy;
    - **Blocked** - the event is blocked by Traffic Monitor which operates in the inline mode or by Device Monitor agent as a result of applying a data protection policy on agents;
    - **Quarantined** - SMTP email is quarantined by Traffic Monitor and awaits a decision of the security officer (only if the System operates in the inline mode);
    - **Unblocked after quarantine** - the security officer has changed the verdict from *Quarantined* to *Allowed*, and the SMTP email is passed to an external server to be sent to recipients (only if the System operates in the inline mode).
    - **Blocked after quarantine** - the security officer has changed the verdict from *Quarantined* to *Blocked* and forbidden sending the SMTP email (only if the System operates in the inline mode).
6. To create a template for the selected verdict, enable the **Send** switch on the selected tab.
7. In the form that opens, specify what items should be included in the email subject and body. By default, inputs fields are displayed where you can enter required text.
8. To add an item to the message subject or body, click **+Add** in the **Email subject** or **Email body** area respectively and choose the required item from the drop-down list. You can choose the following items:
    - **Event ID** - when you add the event ID to the message body, you can also add a link to view the event in the Management Console;
    - **Senders** and **Recipients** - from the drop-down list, choose what details on senders and recipients should be included in the message subject or body. By default, a name and a contact from the event are added;
    - **Policies** triggered in the event. When adding policies to the message body, you can specify what information about policies should be added: the policy name, a description, or both parameters;

- **Attachments** - from the drop-down list, choose what details on attachments should be included in the message subject or body. By default, the file name and size are added.
- **Sender's computer**;
- **Interception date**;
- **Event type**;
- **Verdict**;
- **Violation level**;
- **Protected objects** triggered in the event;
- **Message subject** for emails sent by employees;
- **Source application and destination application**;
- **Path to file**;
- **Print task name**;
- **Resource**;
- **Perimeters**;
- **Sending date**;
- **Terminal session name**;
- **Browser tab address**.

To delete an item, click × in the right upper corner of the selected item.

9. If you want to add the event card to the notification, enable the **Attach event card** switch. The notification email will include a file with the event text and the text extracted from attachments. Triggered protected objects are highlighted in the text.

> **Important!**
>
> A notification with the event card will be sent to all recipients specified in the **Custom recipients** field. You should see to it that sending event details to external emails should not lead to the leakage of confidential data.

10. Choose the card format: **Microsoft Word** or **PDF**.
11. Specify in what form the highlighted text should be included in the card. Possible choices:
    - **As snippets** - the event text will be exported as snippets which contain triggered protected objects;
    - **All text** - the whole event text will be exported.
12. When you have specified all required parameters, click **Save**.

> **Note:**
>
> While creating a notification, you can test the resulting template (see "Testing Notification").

Testing Notification

While creating or editing a notification, you can test the resulting template. For this:

1. In the right lower corner of the workspace, click **Send test notification**.
2. In the window that opens, specify:
   - **Event ID** - enter an ID of the event which exists in the System;
   - **Recipient** - specify an email address to which a test message should be sent.
3. Click **Send notification**.

A test message with a notification created according to your template will be sent to the specified email address.

Preset Notifications

There are the following preset notifications in the System:

1. *Notification to violator*. Includes templates that can be sent to the event initiator if the event is:
    - allowed;
    - blocked;
    - quarantined;
    - unblocked after quarantine;
    - blocked after quarantine.

    The notification includes a message on the current state of the event and information about senders, recipients, interception date and time, resources, and attachments.
2. *Notification to security officer*. Includes templates that can be sent to the security officer if the event is:
    - allowed;
    - blocked;
    - quarantined.

    The message subject includes information about the incident, its violation level, and the verdict. The message body includes the following data:
    - event ID;
    - interception date and time;
    - event type;
    - violation level;
    - verdict;
    - triggered policies;
    - triggered protected objects;
    - sender's computer;
    - senders;
    - recipients;
    - resource;
    - message subject;
    - attachments.

5 Licensing Information

The licensing information for the System is contained in "User License Agreement" section.

5.1 User License Agreement

ATTENTION! Please read carefully the terms and conditions of the end-user agreement before using the software.
Use of the installed software signifies your unconditional acceptance of the terms and conditions hereof. If you do not agree to the terms and conditions hereof, you must terminate the installation and/or use of the software.

1. License granting

1.1. You are granted a non-exclusive license to use the software (hereinafter, the "Software") (the Software Rights Holder is InfoWatch Laboratory LLC) within the framework of the features described in the Software Documentation (User Manual, Administrator Manual, Installation Manual), provided that you comply with all the technical requirements described in the Software Documentation, as well as all the restrictions and terms of use of the Software specified in this Agreement and the Contract between you and your licensor.

1.2. If you have received, downloaded and/or installed the Software designed for educational purposes, you may only use the Software for educational purposes and during the trial period. Any use of the Software for other purposes or after the trial period shall be prohibited.

1.3. You have the right to make a copy of the Software, provided that such a copy is only intended for archival purposes and for replacement of the copy legally purchased, if the original copy is lost, destroyed or is no longer usable. This copy may not be used for other purposes and must be destroyed if the possession of the Software copy ceases to be legitimate.

1.4. You shall be solely responsible and ensure compliance with the applicable export and import laws, as well as applicable trade sanctions and embargo with regard to the transfer of rights and use of the Software.

2. Restrictions

2.1. You may not decompile, disassemble, modify or perform derivative works based on the Software, in whole or in part.

2.2. You are not allowed to transfer the right to use the Software to third parties.

2.3. It is prohibited to transfer or provide access to the license key to third parties, contrary to the provisions of this Agreement and the Contract between you and your licensor. The license key constitutes confidential information. The Rights Holder shall reserve the right to use authentication tools for the license key installed by you.

2.4. It is prohibited to lease, rent or assign for temporary use the Software, as well as to disclose the results of the Software bench tests.

2.5 It is forbidden to use the Software for purposes contrary to the law.

2.6. The Rights Holder shall have the right to lock the license key if you breach the provisions of this Agreement or the Contract between you and your licensor.

2.7. Anyone who violates intellectual property rights to the Software shall bear civil, administrative or criminal liability therefor under the law.

2.8. You may not use the Software for any purposes or in a manner restricted or prohibited by applicable laws. You shall be solely liable for unlawful use of the Software.

2.9. Should you breach any of the provisions of this Agreement or the Contract between you and your licensor, the Rights Holder or your licensor shall be entitled to terminate the Software license at any time without notice to you and without reimbursement of the cost of the Software or a part thereof.

3. Limited warranty

3.1. The Rights Holder guarantees that the Software shall operate in line with the description set forth in the Software Documentation. However, all of your claims regarding the operability of the Software may only be made against your licensor under the relevant license agreement.

3.2. You agree that no Software shall be error free, and it is recommended that you regularly back up your files.

4. Intellectual property rights

4.1. You agree that exclusive rights to any intellectual property items embodied in the Software and/or any documentation provided to you belong to the Rights Holder. Nothing in this Agreement shall grant you any rights to the said intellectual property items, other than those provided by the Contract between you and your licensor.

4.2. You agree that the source code, the license key for the Software are the property of the Rights Holder.

4.3. You may not remove or alter copyright notices or other proprietary notices on any Software copy.

5. Rights to information, access to which has been obtained by you in the execution of this Agreement

5.1. You agree that you do not own any rights to any information accessed by you as part of the execution of this Agreement.

5.2. This information includes, but is not limited to, systems, mode of operation, other information.

5.3. You shall use the said information only to exercise the contractual rights to the Software, without the right to use this information for your own benefit and outside the scope of the Contract between you and your licensor.

6. You are informed that the Software contains open-source software distributed under certain licenses, which you can find in the licenses.inf file distributed with the Software as part of the distribution. Each of the provided software distributions contains a licenses.inf file that corresponds to the composition of a particular distribution.

7. Software usage information collection notice

7.1. You are hereby notified when you enable the usage statistics collection function in the Software, the Software collects and records the following information:

a) about the hardware, about the operating system of the device on which the software is installed and operated as well as other technical information containing data about the use of hardware, the load on the hardware, and the speed of the software;
b) user activity - anonymized (without specifying information about the user him/herself or information entered by the user) data about the actions of the end user in the software user interface.

7.2. The copyright holder has the right to use the specified data to analyze the features of the operation of the Software and the peculiarities of the use of the Software by the end user to make decisions on the development of functionality and improvement of the operational characteristics of the Software.

7.3. The copyright holder guarantees the confidentiality of the data collected, and not to disclose or transfer collected data to third parties.

8. Contact information of the Software Rights Holder - InfoWatch Laboratory LLC

Tel./Fax: +7(495)229-00-22

Commercial Department: sales@infowatch.com

Technical Support Service: support@infowatch.com

Web site: www.infowatch.ru

6 Glossary

Term	Glossary
Active Directory	LDAP-compatible Microsoft directory services for the Windows NT operating systems family
Active policy	A policy included into a configuration that is uploaded to a host. See also: Policy, Host
Administrator	A preset role and user account in Management Console. An Administrator can modify other accounts and their rights. It is also a System user who installs, configures and maintains the System. See also: User role, Security officer, User
AJAX	Asynchronous JavaScript and XML is a group of interrelated Web development techniques used on the client-side to create asynchronous Web applications
Astra Linus Directory Pro	A software package based on the Astra Linux OS, designed for centralized management of objects of organizations of various sizes
Attachment	File attached to the intercepted event at any nesting level. See also: Event
Audit	Controlling of actions fulfilled by Management Console users: creating and managing the security schema, System administrating. See also: Audit log, Management Console accounts
Blanks	Technology of searching the filled blanks of forms: questionnaires, receipts, etc. Blanks are stored in the System as digital prints, their text is not available for viewing to either users or System administrators. See also: Technologies, Technology element
Case sentive	Term setting: if the term is case-sensitive, the text search will detect only word forms which completely match upper- and lower-case letters defined in a term. See also: Term
Catalogs of persons, computers, and groups	Information about users, workstations, groups of users, and groups of computers imported from Active Directory, Samba DC, Domino Directory, Astra Linux Directory, Astra Linux Directory Pro or FreeIPA or created using Management Console. Used to simplify work with the events information.
Categories and terms	Technology of searching the words and phrases in the event text. The event where the term is found is referred to the category which this term belongs to. Old synonyms: Classifier, CFB. See also: Event, Term, Category, Technologies, Protected object

Term	Glossary
Category	Named term group characterizing some theme. If the System detects any term from the category in the text of the intercepted event, it associates the event with this category. See also: Term
Citation index	A measure of how close the sample document matches the text of the document being analyzed. See also: Sample document, Quote
Computer	A managed computer: workstation or terminal device. See also: Workstation, Terminal device
Configuration	A group of settings required to check events for data monitoring and analyzing. See also: Event, Technologies, Lists, Policy
Configuration version	A fixed state of the configuration designed to monitor changed settings of the event analysis. The configuration version is committed after uploading to a host. The configuration version can be active (currently used), editable (the last version with up-to-date modification) and saved (having changes and editable for users). See also: Configuration
Consul agent	Consul cluster member. It can be server or client.
Controlled persons	Set of persons, groups of persons and person's statuses which detection in the event results in associating this event to the person control policy which defines this set. See also: Persons, Person group, Person status, Person control policy
Copy mode	One of IW TM transport modes. In this mode, the actual traffic does not pass through the System. The copy of traffic is analyzed. In this mode, the traffic cannot be filtered by the System. See also: Transport mode
Copy rule	The rule that regulates copying and printing protected data. See also: Rule, Protected data, Data protection policy
Corporate security policy	A set of technical, organizational, administrative, legal, and physical measures, methods, rules, and guidelines that cover all security aspects in a company
Dashboard	Management console section that displays on widgets the statistical information on the violations and violators. See also: Management Console, Widget, Violation
Data interception	A process of acquiring, parsing, categorizing, and converting data (or a copy) into context. It is possible to intercept data transferred using the following protocols: SMTP, HTTP, ICQ/OSCAR, Skype, IXP, XMPP, MMP, FTP. See also: Interceptor, Event context

Term	Glossary
Data interception channel	A data interception environment that includes technical appliances, software tools, and communication protocols. The System supports the following data interception channels: email (SMTP, IMAP, and POP3), Web (HTTP), instant messaging services (ICQ and Skype), shadow copies of files, connected/disconnected workstation events, and print jobs.
Database	A collection of data stored in accordance with a data scheme. Contains all information needed for the System.
Database unloadings	Technology of searching the quotes the database. Database unloadings may be lists of salaries, other personal data, etc. See also: Technologies
Decision	The security officer's conclusion on whether the event violates the corporate security policy or not. Possible values: "No decision", "Violation:" and "No violation". See also: Security officer, Corporate security policy, Event, Event attributes, Violation, Policy, Verdict
Delivery status	Event attribute that specifies the possibility of event delivery to recipients after the analysis. If the event delivery has been allowed, then the attribute value represents the delivery tracking (completed or failed). See also: Event attributes
Digital print	A method of storing a sample document in the database in the form of a set of quotes. See also: Sample document, Quote
Document shadow copy	A copy of printed document received from the print job initiated on the managed computer. See also: InfoWatch Device Monitor
Domino Directory	IBM Lotus Domino Directory is a directory of information about users, servers, and groups. The Domino Directory is also a tool that administrators use to manage the Domino system.
Event	Objects of traffic interception (SMTP and IMAP and POP3 mail, HTTP requests, ICQ and Skype messages), shadow copies of files and print jobs. Generated by the System as a result of the data exchange between employees and others, including publication in media, copy to external devices and printing.
Event analysis	The procedure of processing of the attributes, attached files, and text of the intercepted events and of assigning additional attributes to the event. See also: Event, Policy, Event attributes
Event attributes	Structured data extracted from the events and assigned according to the processing results. See also: Event, Policy, Verdict, Decision, Transport mode

Term	Glossary
Event context	Internal representation of an intercepted event in the System. XML data (attributes, text) extracted from the event and its attachments. After processing the analysis results and the decision are added to the context. See also: Event, Technologies, Decision
Event text	Text information extracted from the event body and its attachments. Contains no formatting or markup. Is used for analysis and search. See also: Event, Event body
File shadow copy	A copy of file recorded to a removable device.The copy is created only if the file is successfully saved on the removable storage device. See also: InfoWatch Device Monitor
File signature	A constant integer value that uniquely identifies a file of a certain type.
FreeIPA	An open-source set of components for centralized management of users, their groups, hosts, authentication and authorization in Linux systems
FTP	File Transfer Protocol is a network protocol used to transfer computer files from one host to another host over a TCP-based network, such as the Internet.
Graphical object	Technology of searching the images (passports, bank cards, etc) in the text and attachments of the intercepted events. See also: Technologies, Event, Protected object
Group of persons and computers	Group aggregating data on organization's users and computers and on external contacts. The groups can be AD Groups (imported from Active Directory), Samba DC groups (imported from Samba DC), DD groups (imported from Domino Directory), ALD groups (imported from Astra Linux Directory), ALD Pro groups (imported from Astra Linux Directory Pro), FreeIPA groups (imported from FreeIPA) or TM Groups (created using Traffic Monitor). See also: Person, Computer, Contact
GTalk	Google Talk is an instant messaging service that provides both text and voice communication.
Headers	Supplemental data placed at the beginning of a block of data being stored or transmitted. Used for creating the event entity in the System and for determining the attribute values of this event. See also: Event, Event attributes
HTTP	HyperText Transfer Protocol, an application-tier protocol used to transfer the data in the text format. See also: HTTPS, HTTP(S) Monitor

Term	Glossary
HTTP query	A request formed according to the HTTP standards (POST request, GET request etc.) See also: HTTP, Event
HTTPS	Hypertext Transfer Protocol Secure is a network protocol for secure communication over a computer network. See also: HTTP, HTTP(S) Monitor
ICAP	Internet Content Adaptation Protocol is a lightweight HTTP-like protocol that allows you to control the incoming and outgoing HTTP traffic. It also makes it possible to modify the content of the HTTP requests.
ICQ	An Internet instant messaging service. Uses OSCAR protocol.
ICQ message	A message sent through the ICQ-OSCAR protocol. See also: Event
IMAP	Internet Message Access Protocol is a protocol for e-mail retrieval and storage
InfoWatch Device Monitor	IW DM is software appliance designed to control the user access to peripherals and to monitor operations (data either copied to removable media and network storages or sent to print, network activity, applications usage) and intercepting messengers traffic (Skype, Gtalk and Jabber) and so on.
InfoWatchTraffic Monitor	IW TM software suite is designed to control various types of traffic (SMTP, IMAP, POP3, HTTP, HTTPS, IMAP, XMPP, ICQ, NRPC) and shadow copies of the data copied to the removable media and sent to printing.
Initiators	A person whose actions led to the event creation
Inline mode	IW TM system deployment mode which may block mail outgoing from the perimeter, followed by dispatching. IW TM Server is used as a relay server.
IW Lync Adapter	Interceptor of data communication events through MS Lync servers installed in the company infrastructure.
Jabber	Messaging and information exchange system based on the open XMPP protocol.
LAN	Local Area Network

Term	Glossary
License	Right to the System usage. Gained when buying the System and defines available users number, used technologies and interceptors and so on. See also: Technologies, Interceptors
Lists	Lists the similar data generated by Management Console to be used in policies creating. See also: Configuration, Policy
Lotus Adapter	Interceptor installed on the IBM Lotus server to redirect emails to IW TM for analysis. See also: Interceptor
Lotus Domino	IBM mail server which messages are intercepted by Lotus Adapter.
Management Console	A graphical user interface. Designed to manage InfoWatch Traffic Monitor (administration, configuring settings, event analysis, etc.).
Management Console (DM)	GUI element. It is designed to control InfoWatch Device Monitor (system administration, security schema configuration, etc.)
Management Console user	User who manages the System. Each user has a role assigned basing on corporate security policy.
MAPI	Messaging Application Programming Interface is a messaging architecture and a Component object model based API for Microsoft Windows
Mask	A search pattern of characters and wildcards used to match folder and file names.
Monitor	See: Interceptor
Morphology	Term setting: if morphology is used, the text search will detect all word forms of this term. See also: Term
MS Lync	Microsoft instant messaging clients for corporate environments.
MTProto	A cryptographic protocol used in the messaging system to encrypt user correspondence
Normal transport mode	A traffic analysis and filtering mode. In this mode, it’s possible to block the traffic forbidden by the System can be blocked. See also: Transport mode, Inline mode
Notification	E-mail sent in case if the policy triggers on the event. Is sent via Management Console to notify Management Console users, employees or third parties. Contains a summary on the intercepted events and attached message. See also: Policy, Event

Term	Glossary
Occurrence threshold	A number of text objects found in the event enough to detect the protected object where this occurrence threshold is defined. See also: Event, Text objects, Protection object
Perimeter	A container of company infrastructure elements and contact information. The perimeter is used to logically divide a company into structural elements and track the traffic of every element. See also: Group of persons and computers
Person	Account of employee or external contact that is contained in System catalog and allows to process the data belonging to this account as a whole and to user-friendly display data referring to it. See also: Group of persons and computers
Persons control policy	A policy to add rules controlling persons, person groups, and person statuses. See also: Policy, Person control rule, Person, Person status
Persons control rule	Rule that assigns attributes to the event of specified violation level and which senders or recipients contain persons specified in the policy which includes this rule. Allows to re-assign person's status and to send notifications. See also: Rule, Event attributes, Person, Violation level, Person status, Notification, Person control policy
Placement rule	The rule that regulates storing protected data. See also: Rule, Protected data, Data protection policy
Policy	A set of rules according to which the event analysis and processing facilities are performed. See also: Policy, Active policy, Rule
Policy (DM)	A set of file monitoring rules for removable devices, network activity, printing, configuring peripherals access level etc. You can only assign security policy to a group (of employee or workstations.) See also: Rule (DM)
POP3	Post Office Protocol Version 3 is an application-layer network protocol used by local e-mail clients to retrieve e-mail from a remote server over a TCP/IP connection
POST query	A query method designed to request that a web server accepted the data enclosed in the request message body for storage. Often used for file downloading of filled web-form representing
Privilege	Entity defining user’s ability to perform some action (set of actions) when managing the System

Term	Glossary
Protected data	A set of protected objects, their catalogues and file formats which detection in the event allows to characterize this event as fallen under the data protection policy where this set is defined. See also: Protected object, File format, Data protection policy
Protected object	The set of technology elements whose presence in the event allows the System to determine that this event belongs to a particular type of business documents (catalogue of protected objects). Protected objects are used in defining of data protection policies. See also: Technology element, Data protection policy
Proxy Server	The service that allows indirect requests to other network services. Proxy forwards all requests of the client programs to the network, and, having received the reply, sends it back to the client.
Quotation threshold	A percent of the sample document found in the even as quotes, enough to associate the event with this sample document. See also: Event, Sample document, Quote
Quote	A quote from the sample document found in the event text. See also: Sample document
Reference hash sum	Unlike the current hash sum, keeps the representative state of System files. See also: Integrity control
Relay server	A server which allows anyone on the Internet to send e-mail through it, not just mail destined to or originating from known users.
Report	Selection providing a visual display of event statistic data. See also: Management Console, Event
Rule	Entity defining System’s actions in the response to any actions which persons do with secured data.A rule is a set of conditions to test the event with and actions performed when those conditions are fulfilled or not. See also: Event, Policy, Protected object, Person control rule, Copy rule, Transfer rule, Placement rule
Rule (DM)	Set of restrictions and conditions that monitor file operations on removable devices, network activity, printing, configure access to managed peripherals etc. Each interceptor features a separate rule type. A rule can be only applied within its policy. See also: Policy (DM)
Samba DC	Free software implementation of the SMB network protocol. Provides file and print services for various Microsoft Windows clients

Term	Glossary
Sample documents	Technology of searching the quotes from sensitive documents: memos, financial reports, contracts, and others. Sample documents are stored in the System as digital prints, their text is not available for viewing to either users or System administrators. See also: Technologies, Technology element, Digital print, Quote
Security officer	A basic user of the Management console. Also - pre-installed role of the Management Console user that has privileges for all the actions in the system except administrative. See also: Management Console, User, User role, Privilege, Administrator
Skype	A voice-over-IP service and instant messaging client
SMB	Server Message Block operates as an application-layer network protocol mainly used for providing shared access to files, printers, serial ports, and miscellaneous communications between nodes on a network.
SMTP	Simple Mail Transfer Protocol is a networking protocol used to send the email in TCP/IP networks.
S/MIME	A standard for public key encryption and signing of MIME data
SMTP mail	An e-mail formed according to SMTP standards. See also: SMTP, Event
SPAN	Switched Port Analyzer is a technology that allows to mirror the network traffic from one port to another
SPAN copy	A variety of the “Copy” transport mode. In this case the traffic passes through a CISCO switch. The copy of the traffic is sent to Traffic Monitor Server for analysis. See also: SPAN
SSL	Secure Sockets Layer is a cryptographic network protocol developed for transmitting private documents via the Internet.
Status	Characteristics of persons and computers allowing to divide them onto groups for convenient analysis and activity control and to display them on dashboards and reports with special colour indicating. See also: Persons, Computers, Dashboard, Report
Stop word	Numbers, letters and words, whose presence in cells do not trigger these cells. Stop words are used to eliminate false triggering.
Tag	The text label giving a brief description of the event. See also: Event attributes

Term	Glossary
Technologies	Set of analysis tools searching for defined elements in the events' context and adding characterizing attributes to the event. See also: Technology element, Event context, Categories, Terms, Sample documents, Blanks, Database unloadings, Text objects, Graphical objects
Technology element	A part of the System technologies settings. Samples of confidential data. Can be categories and terms, sample documents, blanks, database unloadings, text and graphical objects. See also: Technologies, Categories and terms, Sample documents, Blanks, Database unloadings, Text objects, Graphical objects, Protected object.
Telegram	A messenger for smartphones which allows you to sent text messages, images, audio and video files; uses MTProto protocol
Term	One of the set of words and phrases together defining a topical area. See also: Category
Term Weight	How the term is characterized for the given category; an integer between 1 and 10. If a term with a higher weight is detected in event, then this event will be more likely associated with the category of this term. See also: Term
Text object pattern	Unified description of all possible text objects with the typical structure: passport numbers, credit card numbers, phone numbers, medical codes etc. See also: Text objects
Text objects	Technology of matching the data from the events' text with defined patterns (rules of generating bank card numbers) . See also: Technologies, Event, Technology element, Text object pattern
Transfer rule	The rule that regulates sending and receiving protected data. See also: Rule, Protected data, Data protection policy
Transport mode	Event attribute that defines the level of control when the object is delivered to the recipients. Assigned by the analysis and decision engine during the object analysis. Together with the "Verdict" attribute determines if the object can be delivered further on. See also: Event attributes, Verdict, Copy mode, Normal transport mode, Delivery status
User	IW TM users: administrator, security officer etc. See also: Administrator, Security officer, Person
User interface	The complex of tools and methods by means of whose the user interacts with the system.

Term	Glossary
User role	A set of privileges that define a set of actions available for the user. See also: Administrator, Security officer, Management Console, Privilege
Verdict	An event attribute with the conclusion about the presence (or absence) of violations in an event. Together with the Transport Mode attribute determines if the event can be delivered further on. See also: Event, Transport mode, Delivery status, Event attributes
Verdict reason	Event attribute that describes the reason why a certain verdict was assigned to the event. See also: Event attribute, Verdict
Violation	The value of the «Decision» attribute; means that the corporate security policy has been violated. See also: Decision, Corporate security policy
Violation level	Event attribute indicating (by the colour tag) the level of threat to corporate security policy. See also: Event, Event attributes, Violation
Visibility scope	The way to divide intercepted events to restrict Management console user access to them. Events satisfying criteria of some visibility scope will be visible to those users who have an access to this scope only (given that user has privileges to view or/and manage events). See also: Event, Privilege
Widget	Interface element in the form of an isolated area that displays the specified statistic information on violations and violators. See also: Management console, Violation, Violator
WhatsApp	A messenger for smartphones which allows you to sent text messages, images, audio and video files; uses its own protocol
Workstation	Computer type: desktop or notebook with OS of Windows or Linux or Mac family. See also: Computer
XMPP	Extensible Messaging and Presence Protocol is a communications protocol for message-oriented middleware based on XML.