

INFOWATCH

InfoWatch Traffic Monitor 6.1

User Guide

InfoWatch Traffic Monitor 6.1

User Guide

© AO “InfoWatch”

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

http://www.infowatch.com

Revision date: 2016-10-24

TABLE OF CONTENTS

1 INTRODUCTION 7

1.1 WHO SHOULD READ THIS GUIDE 7
1.2 SET OF DOCUMENTS 7
1.3 TECHNICAL SUPPORT 7

2 INFOWATCH TRAFFIC MONITOR OVERVIEW 9

2.1 OBJECT INTERCEPTION 10
2.2 OBJECT ANALYSIS AND VERDICT 12
2.3 RETROSPECTIVE DATA ANALYSIS, USER DECISION ON AN OBJECT 15
2.4 INFOWATCH TRAFFIC MONITOR TRANSPORT MODES 15
2.5 UPLOADING OBJECT TO DATABASE 16
2.6 SPECIFIC FEATURES OF BLOCKING HTTP-QUERIES AND MESSAGES SENT THROUGH WEB SERVICES 17

3 MANAGEMENT CONSOLE: GENERAL INFORMATION 18

3.1 SYSTEM OPERATION BEFORE CONFIGURING 19
3.2 CONFIGURING THE SYSTEM 19
3.3 DISPLAYING ACTUAL DATA IN MANAGEMENT CONSOLE 21

4 MANAGEMENT CONSOLE INTERFACE 22

4.1 DASHBOARD SECTION 25
4.1.1 Dashboards 26
4.1.2 Dashboard widgets 26
4.1.2.1 Dynamics of violations over the period 27
4.1.2.2 Top violators 28
4.1.2.3 Quantity of violations over period 29
4.1.2.4 Selection 30
4.1.2.5 Dynamics of statuses 31
4.1.2.6 Policy statistics 32
4.1.2.7 Statistics on protected objects 33
4.1.2.8 Statistics on catalogues of protected objects 35
4.1.3 Dashboard summary 36
4.2 EVENTS SECTION 37
4.2.1 Queries 39
4.2.1.1 Condition 40
4.2.1.2 Displayed Fields 44
4.2.1.3 Access Parameters 45
4.2.1.4 Advanced Mode 45
4.2.1.5 Search on the Event Text 46
4.2.2 Object Interception 48
4.2.2.1 Event tile 50
4.2.2.2 Brief Event Viewing Form 52
4.2.2.3 Detailed Event Viewing Form 53
4.2.3 Contact Identification in Event 55
4.3 REPORTS SECTION 55
4.3.1 Widgets of Reports 57
4.3.2 Queries 59
4.3.3 Report Execution History 60
4.3.4 Report Creation Form 61
4.3.5 Report Folder Creation Form 61
4.4 TECHNOLOGIES SECTION 62
4.4.1 Categories and Terms 63
4.4.1.1 Categories 64
4.4.1.2 Terms 66

4.4.2 Text Objects ... 67
4.4.2.1 Text objects patterns ... 68
4.4.3 Sample Documents ... 69
4.4.4 Blanks ... 72
4.4.5 Stamps ... 74
4.4.6 Database Unloadings ... 76
4.4.6.1 Automatically Updated Database Unloadings ... 78
4.4.7 Graphical Objects ... 79
4.5 PROTECTED OBJECTS SECTION ... 80
4.5.1 Elements of Analysis ... 81
4.5.2 Detection Conditions ... 83
4.6 PERSONS SECTION ... 84
4.6.1 Group of Persons and Workstations ... 86
4.6.2 Persons ... 87
4.6.3 Workstations ... 88
4.7 POLICIES SECTION ... 90
4.7.1 Policies and their Viewing Form ... 91
4.7.2 Rules and their Viewing Form ... 92
4.7.2.1 Rule of Transfer ... 93
4.7.2.2 Rule of Copying ... 95
4.7.2.3 Rule of Placement ... 96
4.7.2.4 Person Control Rule ... 98
4.7.3 Filter Settings area ... 98
4.7.4 Form of adding policy ... 99
4.8 LISTS SECTION ... 99
4.8.1 Tags ... 100
4.8.2 List of Resources ... 101
4.8.3 Statuses ... 102
4.8.4 Perimeters ... 103
4.8.5 List of Files ... 105
4.9 CRAWLER SECTION ... 106
4.9.1 Scanner ... 108
4.9.2 Scanning Job ... 109
4.9.3 Launch History ... 113

5 CASES SOLVING ... 115

5.1 TYPICAL ACTIONS ... 115
5.1.1 Login and Logout of the Management Console ... 116
5.1.2 Applying System Configuration ... 117
5.1.3 Editing Element ... 118
5.1.4 Deleting Element ... 118
5.1.5 Pages Navigation ... 118
5.1.6 Changing User Password ... 119
5.1.7 Selecting Interface Language ... 120
5.1.8 Calling Help file ... 120
5.1.9 Viewing Information on System ... 120
5.2 MANAGING PERSONS AND WORKSTATIONS ... 120
5.2.1 Creating a Group of Persons and Workstations ... 121
5.2.2 Creating Persons and Workstations ... 122
5.2.3 Viewing Events of a Person ... 123
5.2.4 Viewing a Summary on Person ... 123
5.2.5 Adding Status to a Person ... 123
5.2.6 Adding a Person to Perimeter ... 124
5.2.7 Configuring Person's Card ... 125
5.2.7.1 Adding Contact to a Person ... 125
5.2.7.2 Adding Workstation to a Person ... 126

5.2.7.3 Adding a Person to Group 127
5.2.8 Configuring Worksation Card 127
5.2.8.1 Adding Contact to Computer 128
5.2.8.2 Adding Person to a Computer 128
5.2.8.3 Adding Computer to a Group 129
5.3 MANAGING CATALOGS 130
5.3.1 Managing Tags 130
5.3.2 Managing Web Resources 131
5.3.3 Managing Statuses 132
5.3.4 Managing perimeters 133
5.4 MANAGING BASE OF TECHNOLOGIES 135
5.4.1 Defining the Confidential Information 135
5.4.1.1 Managing Categories and Terms 137
5.4.1.1.1 1. To create a category. 137
5.4.1.1.2 2. Creating a term. 138
5.4.1.2 Managing Text Objects 140
5.4.1.2.1 1. Create a catalog of text objects. 140
5.4.1.2.2 2. Create a text object and specify its value. 140
5.4.1.3 Managing Sample Documents 142
5.4.1.4 Managing Blanks 144
5.4.1.5 Managing Stamps 146
5.4.1.6 Managing DB Unloadings 147
5.4.1.6.1 Detection Conditions for Unloading 149
5.4.2 Exporting and Importing the Technologies Database 151
5.5 MANAGING PROTECTED OBJECTS 153
5.5.1 Creating a Catalog of Protected Objects 154
5.5.2 Creating a Protected Object 154
5.5.3 Adding Elements of Analysis 157
5.5.4 Adding Detection Conditions 157
5.5.5 Creating Policies for Protected Objects and their Catalogs 158
5.5.6 Import and Export of Protected Objects 159
5.5.7 Activating and Deactivating Protected Objects 160
5.6 MANAGING CRAWLER SUBSYSTEM 161
5.6.1 Configuring Scanner 162
5.6.2 Creating a Job 162
5.6.3 Launching and Stopping the Job 163
5.6.4 Editing the Job 164
5.6.5 Cleaning the Hash Base 164
5.6.6 Viewing Launch History 165
5.6.7 Saving Scan Report 165
5.7 MANAGING INTERCEPTION OBJECTS 166
5.7.1 Viewing summary on violations/violators 166
5.7.1.1 Creating Dashboard 167
5.7.1.2 Creating Widget 167
5.7.1.3 Editing Widget 169
5.7.2 Viewing Events 169
5.7.2.1 Creating queries 169
5.7.2.1.1 Query Creation in Standard Mode 170
5.7.2.1.2 Query Creation in Advanced Mode 171
5.7.2.1.3 Using Advanced Syntax 174
5.7.2.2 Choosing Event Fields of View 175
5.7.2.3 Viewing Brief Event Form 175
5.7.2.4 Viewing Detailed Event Form 176
5.7.3 Managing Dashboard Summaries 176
5.7.3.1 Creating a Summary 177
5.7.3.2 Viewing a Summary 178
5.7.4 Making Decision on Object 179
5.7.5 Adding and Deleting Tags 179

5.7.6 Saving Events (for SMTP mail) ... *180*
5.7.7 Event Export ... *180*
5.7.8 Dispatching a Quarantined Event ... *181*
5.8 CONFIGURING SYSTEM RESPONSE ... 182
5.8.1 General Information on Policies ... *183*
5.8.1.1 Dividing events to sub-events ... 183
5.8.1.2 Dividing rules to sub-rules ... 184
5.8.1.3 Determining the priority sub-rule ... 185
5.8.1.4 Order of applying actions according to the selected priority rules ... 186
5.8.1.5 Example: ... 186
5.8.2 Preset Policies ... *188*
5.8.2.1 Data Protection Policy ... 188
5.8.2.2 Person Control Policy ... 189
5.8.2.2.1 Rule of transfer ... 190
5.8.2.3 Policy Regulating the Transfer of Password-Protected Data ... 190
5.8.2.3.1 Policy rules ... 190
5.8.2.4 Policies that Regulate Visiting Web Resources ... 190
5.8.2.4.1 Inappropriate Use of Resources ... 190
5.8.2.4.1.1 Policy rules ... 191
5.8.2.4.2 Disloyal Employees ... 191
5.8.2.4.2.1 Policy rules ... 191
5.8.2.4.3 Concealing Employees' Actions ... 192
5.8.2.4.3.1 Policy rules ... 192
5.8.2.4.4 Suspicious Activity ... 192
5.8.2.4.4.1 Policy rules ... 192
5.8.3 Creating Data Protection Policy ... *193*
5.8.4 Creating Person Control Policy ... *194*
5.8.5 Editing Policy ... *195*
5.8.6 Creating Rules ... *195*
5.8.7 Editing Rules ... *197*
5.8.8 Determining System Response to Policy Violations ... *197*
5.8.9 Determining System Default Response ... *198*
5.8.10 Filtering the List of Policies ... *200*
5.8.11 Sending Notifications on Responded Rule ... *200*
5.9 MANAGING REPORTS ... 201
5.9.1 Creating a Folder with Reports ... *202*
5.9.2 Creating a Report ... *202*
5.9.3 Managing Widgets of Reports ... *203*
5.9.3.1 Creating and Configuring Widget ... 204
5.9.4 Managing Ready Reports ... *205*

6 LICENSING INFORMATION ... 206

6.1 END-USER LICENSE AGREEMENT ... 206
6.1.1 License Agreement ... *206*
6.1.1.1 1. Definitions ... 206
6.1.1.2 2. Grant of License ... 207
6.1.1.3 3. Restrictions ... 207
6.1.1.4 4. Limited Warranty and Disclaimer ... 208
6.1.1.5 5. Limitation of Liability ... 208
6.1.1.6 6. Software Products ... 208
6.1.1.7 7. Open Source (Free) Software ... 208
6.1.1.8 8. Intellectual Property Rights ... 209
6.1.1.9 9. Rightholder Contact Information ... 209
6.2 THIRD-PARTY LICENSES ... 209

7 GLOSSARY ... 210

1 INTRODUCTION

InfoWatch Traffic Monitor (also referred to as InfoWatch Traffic Monitor or the System) is a distributed multi-component system designed to control different types of traffic (SMTP, IMAP, POP3, HTTP, HTTPS, ICQ, NRPC). InfoWatch Traffic Monitor also analyses data received from InfoWatch Device Monitor.

The Management web console (also referred to as Management Console or MC) is a part of the InfoWatch Traffic Monitor system. The web console allows you to configure the System settings and monitor the System operation.

The Management Console has a user-friendly interface, so this Guide contains only general information and examples to represent functionality of the System.

1.1 Who Should Read this Guide

Information in this guide is intended for users who manage the System (perform the System configuration, analyze information objects, etc.).

The Guide is intended for users with basic knowledge of Microsoft Windows.

1.2 Set of Documents

For more information see the following documents:

- «*InfoWatch Traffic Monitor. User Guide*».

The document describes operation with InfoWatch Traffic Monitor: configuration setting, data export/import, creating policies for objects processing.

- «*InfoWatch Traffic Monitor. Administration Guide*».

Contains information on System administration (database, server-end).

- *«InfoWatch Device Monitor. User Guide»*

Contains a description of the InfoWatch Device Monitor system operation principles as well as instructions on installation, configuration of a system, and system maintenance.

1.3 Technical Support

For support with the issues and questions related to the software you may contact the Technical Support Service:

- If you have purchased the product from a partner of InfoWatch, you should contact the Technical Support Service of this partner company.

- If you purchased the product directly from InfoWatch, you can contact our Technical Support Service at support@infowatch.com. The representatives of our Technical Support Service are available to assist you from Monday through Friday from 7 AM to 9 PM (Moscow time), except weekends and Russian public holidays.

You can also visit InfoWatch Customer Portal: http://cp.infowatch.com/en/.

Before contacting Technical Support, please refer to our Knowledge Base: https://kb.infowatch.com. The Knowledge Base may already contain the answer to your question or description of the problem you are experiencing.

2 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.

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 or the copy of the traffic that passes through the hardware with the CISCO SPAN.
- Interception of the HTTP and HTTPS traffic. It is possible to intercept either traffic passed through an ICAP-supporting proxy server or the copy of traffic that goes through the CISCO SPAN-enabled equipment.

> **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 equipment that supports the CISCO SPAN technology. 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 one transferred by SSL protocol).

- Reviewing files located in the corporative network (open network folders, workstation local discs, and SharePoint 2007/2010/2013 file storage) with the Crawler subsystem.
- Analyzing Skype-, Yahoo- traffic, shadow copies of files, print jobs, traffic transferred by HTTP, HTTPS and FTP protocols; receiving and transmitting mail via SMTP, POP3 and IMAP using MAPI interface, controlling data exchange via Jabber (XMPP protocol), Mail.Ru Agent (MMP protocol), WhatsApp (WhatsApp protocol) and SMS. Interception of the listed data is performed by InfoWatch Device Monitor system.
- Analyzing shadow copies of files intercepted by DeviceLock version 6.3 or higher (provided by SmartLine, Inc.).
- 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 copy of traffic 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	Controlling user access to the peripherals, monitoring operations (data copying to removable storages and FTP, sending data to printing, using messengers) and intercepting the traffic from instant messengers.
Crawler	Checking files from the corporate network (open network folders, local disks of workstations, and SharePoint 2007/2010/2013 file storage).
Connectors	Integration with external systems, generating events.
Web Management Console	Configuring rules for analyzing and filtering traffic, analysis of intercepted data.

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

- Object Interception
- Object Analysis and Verdict
- Retrospective Data Analysis, User Decision on an Object
- InfoWatch Traffic Monitor Transport Modes
- Uploading Object to Database
- Specific Features of Blocking HTTP-queries and Messages Sent through Web Services

2.1 Object Interception

The System objects are the following:

- traffic objects (SMTP, IMAP, and POP3 e-mails, HTTP and HTTPS requests, ICQ, Skype, Yahoo, MS Lync, XMPP, WhatsApp, Mail.Ru agent or SMS messages);
- shadow copies of files;

- print jobs.

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.
MAPI	The System receives a copy of traffic from InfoWatch Device Monitor.
FTP	The System receives a copy of traffic from InfoWatch Device Monitor.
ICQ	• 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.
Skype, Yahoo and Mail.Ru Agent messages	The System receives a copy of Skype, Yahoo, Mail.Ru Agent, WhatsApp traffic from InfoWatch Device Monitor.
MS Lync	The System receives a copy of traffic from IW Lync Adapter installed on MS Lync server.
Files located in the corporate network	The System receives copies of files from the Crawler subsystem.
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.
Shadow copies of files received from DeviceLock	The System receives a copy of traffic. Blocking user actions (access to devices) can be performed only by means of DeviceLock.

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

2.2 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 enclosures from the object, defining the enclosure format, and forwarding the extracted texts to the Analysis subsystem.
Analysis subsystem	Linguistic Analysis module	Checking if the object text corresponds to any categories
	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 enclosures for images of particular classes
Policies Application subsystem	Active Directory and Domino Directory Integration module	Providing the initial import and periodical synchronization of Active Directory and Domino Directory structure with a list of users and workstations in Traffic Monitor for further binding this information with data from the intercepted objects.

IW TM subsystem	Subsystem modules	Subsystem/module features
	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 MS Office 2007 and 2010 document, the System also analyzes metadata specified in document properties (in the **Description** block of the **Details** tab).

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 impressions used in the organizations can be used as sample 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.

4. Based on the results of the analysis, the Decision-Making module makes a conclusion on 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.

2.3 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.

2.4 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.

Warning!

The transport mode can be specified only once for each object.

Table 1 shows 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 "Specific Features of Blocking HTTP-queries and Messages Sent through Web Services").
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 the 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, Yahoo, Jabber, Mail.Ru Agent, or WhatsApp message	No	Yes
SMS	No	Yes
MS Lync	No	Yes
Shadow copy of a file	No	Yes
Photo	No	Yes

2.5 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.

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

If the normal transport mode (see "InfoWatch Traffic Monitor Transport Modes"), the System decides to block a 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 processes 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, gmail.com, inbox.com, hotmail.com, hotmail.ru, mail.com, live.com	yahoo.com, mail.com, aol.com, gmx.com
Blogs and social networks	facebook.com, blogs.mail.ru, liveinternet.ru (li.ru), my.ya.ru, diary.ru, blogspot.com (blogger.com), loveplanet.ru/a-journal, myspace.com, perfspot.com	myspace.com, blogger.com, vkontakte.ru (vk.com), odnoklassniki.ru, twitter.com, livejournal.com (.ru), wordpress.com, linkedin.com
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, google drive, cloud.mail.ru, disk.yandex.ru, mail.qip.ru, file.qip.ru, onedrive.live.com, google plus, talk.mail.ru.

3 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.

The following conditions are checked during the login process:

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

If at least one of the conditions is not met, the user will not be able to log into the System.

If authorization is successful, the user gets access to 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:

This guide does not describe actions of Administrator. All information on this subject is contained in "Infowatch Traffic Monitor. Administration Guide".

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

- configuring the base of technologies,
- composing reference catalogues,
- creating protected objects,
- configuring System response to employees' actions which violate the corporate security policy.

Configuring the System is completed by applying the updated configuration (see "Configuring the System").

Note:

If the System has been configured before, and the implemented configuration is sufficient for all user tasks, no additional configuration is required.

Typical user actions are listed in "Solving Cases". After completing the configuration of 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 refresh data in order to obtain relevant data (see "Refreshing Data in Management Console").

Warning!

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

3.1 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 matches some category, the System assignes a corresponding attribute to the object.
- 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.

3.2 Configuring the System

The System configuration is a set of adjustments needed for checking objects at the Traffic Monitor Server as well as for monitoring and analysis of data.

Each object passed to the 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 the attributes assigned to as a result of processing.

Warning!

The System does not perform reprocessing of the object after the configuration is changed.

The configuration process includes:

- Creating a technology database (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 sample blanks to be detected - *only when using Detecting Sample Blanks technology (see "Blanks")*;
  - Selecting sample stamps to be detected - *only when using Detecting Sample Stamps technology (see "Stamps")*;
  - Selecting database unloadings to be detected - *only when using Detecting Database Unloadings technology (see "Database Unloadings")*;
  - Selecting graphical objects 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 workstations *(see "Managing Persons and Workstations")*;
  - Tags *(see "Managing Tags")*;
  - Resource lists *(see "Managing Resources Lists")*;
  - Statuses *(see "Managing Statuses")*;
  - Perimeters *(see "Managing perimeters")*;
- Creating policies according to which checking objects on the Traffic Monitor Server will be performed *(see "Configuring System Response")*

If at list one of the setting listed above has been changed in the Console, the configuration version that is currently being edited is saved in the System. Upon this:

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



- on the computers of users who do not have access to changing 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.
- **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 the changes made will be discarded. To undo changes, click **Cancel** in the window with the list of changes that will open. 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 evere 15 minutes.

3.3 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.

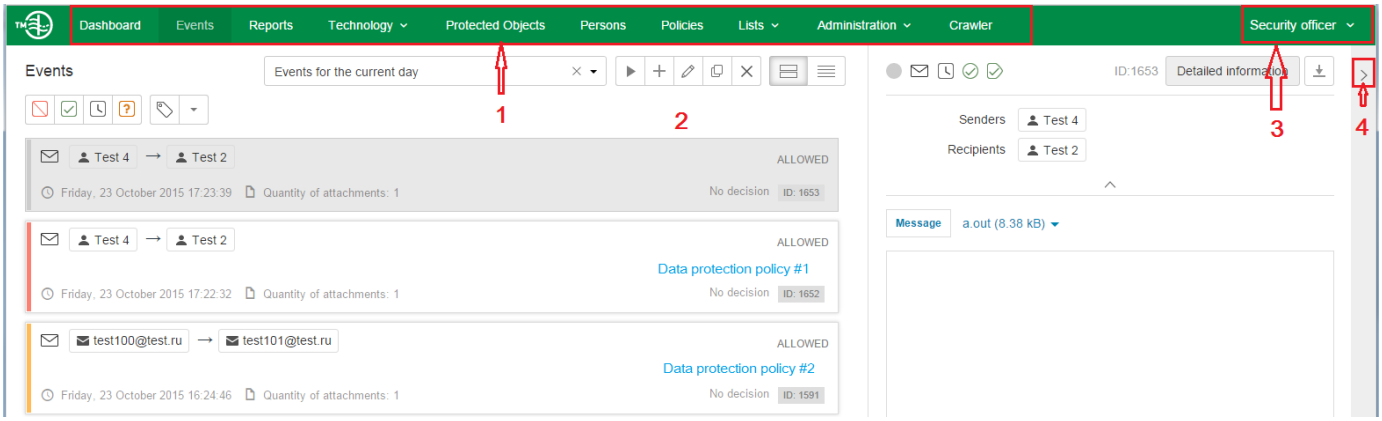
You can also update data manually in any section of the Management Console. To do this, use the standard browser refresh tool: by default the page is refreshed when you press the function key F5).

Note:

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

4 MANAGEMENT CONSOLE INTERFACE

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



Window elements of the Management Console:

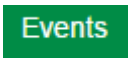
№ on scheme	Console window element	Element purpose
1	Navigation pane	Displays section buttons. Click the section button to go to the selected section of the Management Console.
2	Working area	Displays elements of a selected Management Console section; is used for managing elements of the selected section.
3	User menu button	Displays the user name. Click to open a drop-down list were 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	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.

Operating the Management Console is performed in thematic 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 catalog 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 catalogs of tags, statuses, and perimeters.
Administration	Operations performed in this section are described in *«Infowatch Traffic Monitor. Administration Guide»*
Crawler	Contains tools for creating, editing, and running jobs for the Crawler subsystem.

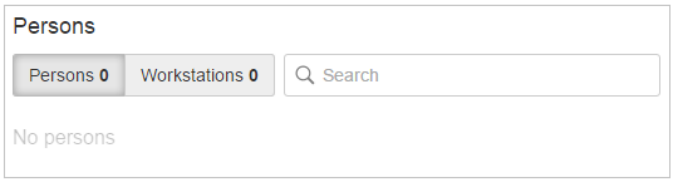
You can go to a specific section by clicking the section button.



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 **Workstations** tabs

- **Panel** - a separated interface area displaying a set of data or interface elements.

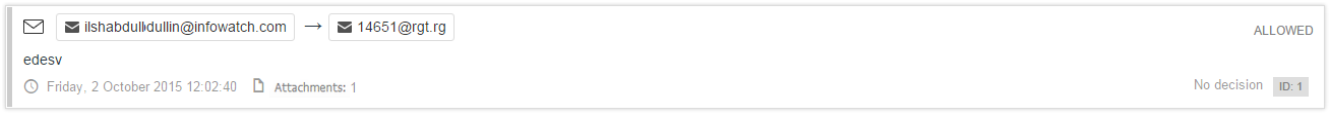
Note:

See also:In the System, the *Panel* also refers to the entity of the Dashboard section (see “Dashboards").



Toolbar

- **A part of 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.



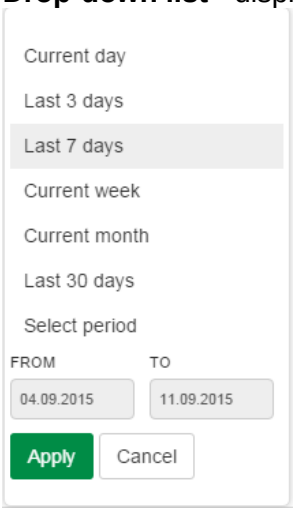
Events section, event tile

- **Field** - element to output the string data or for data input from the keyboard or from the Clipboard.



Search field

- **Drop-down list** - displays a list of elements when clicked at.



Dashboard section, a drop-down list on the widget

You can customize the Management Console interface (for details, see the thematic sections).

Note:

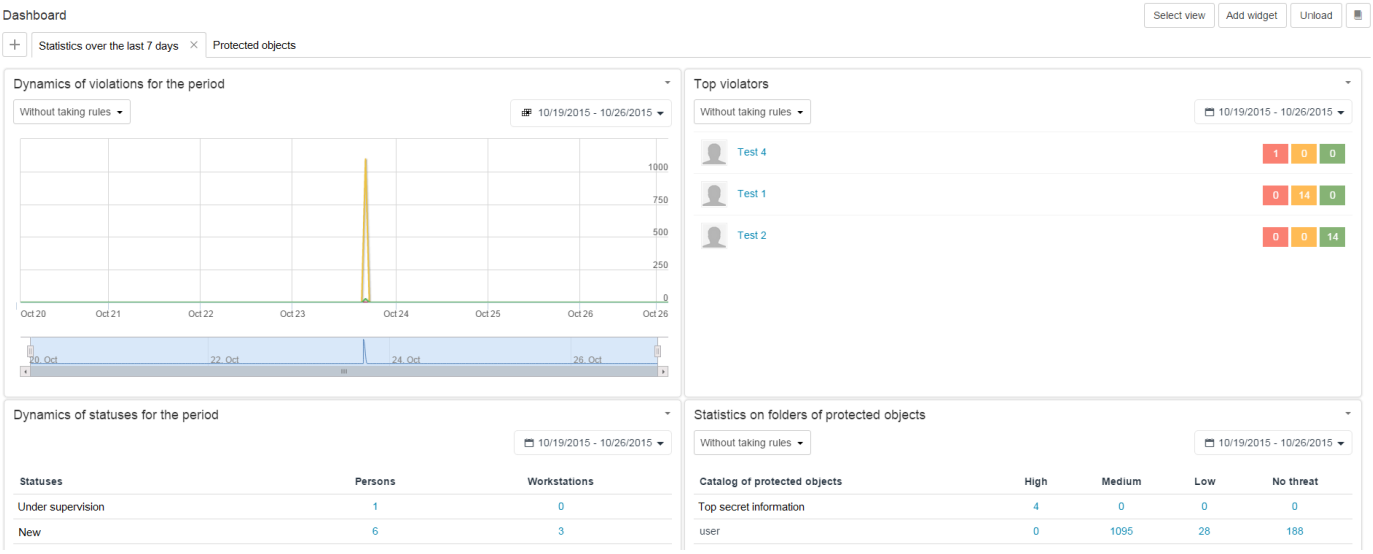
While downloading the requested data, the System may display a symbol like  or informational message.

4.1 Dashboard Section

About the section:

The section contains statistical information on violations/violators.

Information is displayed on widgets, which are placed on dashboards (tabs).



The section contains the following elements:

Element	Purpose
Widgets	Contains information on violations/violators
Dashboards	Contains widgets
+ **Add dashboard** button	Adds a dashboard
Select view button	Allows you to choose a method of splitting the workspace into two parts in proportions convenient for the user. 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
Add widget button	Adds a widget
Unload button	Dashboard summary on violations/violators (see "Dashboard Summary" - on a summary parameters, and "Summary Creating" - on actions required to generate a summary)

Element	Purpose
View the list of summaries button	Viewing a list of created summaries

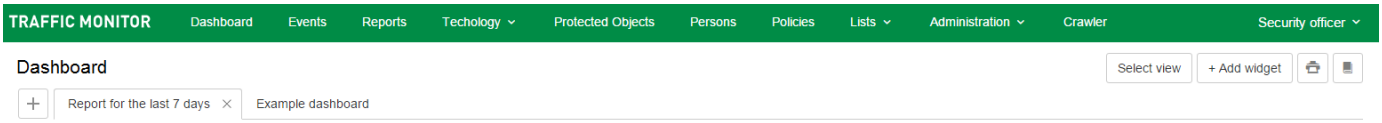
User's target actions:

- Configuring dashboards and widgets to display information on violations/offenders (see "Creating Dashboard" and "Creating Widget");
- Viewing information on violations/violators (see "Viewing Events");
- Creating a dashboard summary (see "Managing Summaries").

4.1.1 Dashboards

The workspace of the **Dashboard** section contains one or more dashboards which allow you to view statistics on violations and violators.

Panels are designed for ergonomic usage of workspace in the **Dashboard** section.



Dashboard section, **Example dashboard** dashboard

Dashboard attributes:

Parameter	Description
Name	Dashboard name
View	Data layout on the dashboards
Set of widgets	Widgets of the dashboard

User's target actions:

- Creating and configuring dashboards to display information on violations/violators (see "Creating Dashboard" and "Creating Widget")

4.1.2 Dashboard widgets

The workspace of the **Dashboard** section contains dashboards used for displaying 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

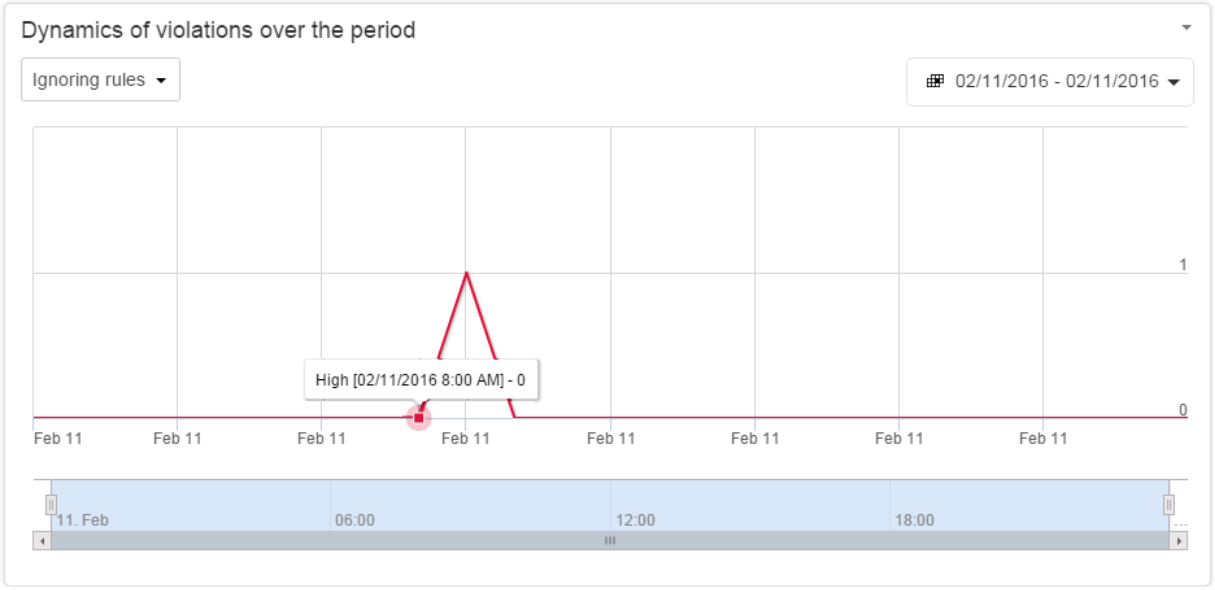
Widget	Description
Dynamics of violations	Quantitative changes of chosen violation types over the selected period
Top violators	A list of the most active violators of a chosen group for the selected time period
Quantity of threats over period	Number of violations of high, medium, and low level for each 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
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 "Editing Widget")
- Moving widget tiles (see "Creating Widget")

4.1.2.1 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.

Widget parameters:

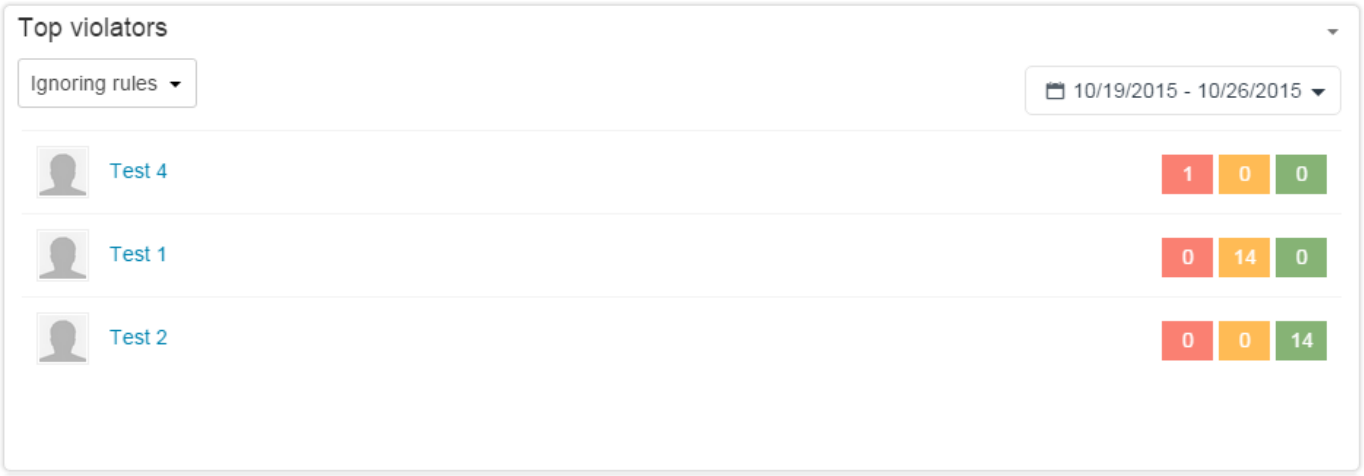
Parameter	Description
Name	Widget name
Rules	In the drop-down list in the left upper corner of the widget, select the type of rules, violations of which will be displayed in the widget. Possible values: *Transfer rules*, *Copy rules*, *Placement rules*, *Ignoring rules*.
Update interval	The frequency of data update on the widget
Period	In the drop-down list in the left upper corner of the widget, specify the time period, over which the data is displayed

Note:

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

4.1.2.2 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.



Clicking on the number of violations opens 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.

Widget attributes:

Parameter	Description
Name	Widget name

Parameter	Description
Rules	In 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*.
Update interval	The frequency of data update in the widget
Period	In the drop-down list in the left upper corner of the widget, specify the time period, over which the data is displayed.
Top violators	The number of violators, a summary for which will be displayed
Groups	Groups, to which violators 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	Persons statuses, information on which will be displayed. Start typing the status name or click + and select desired statuses from the list.

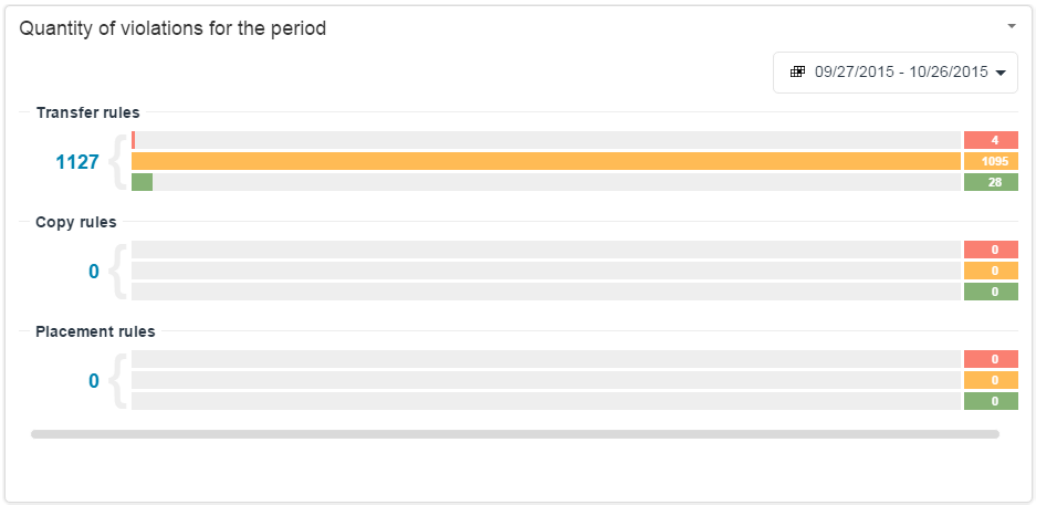
Note:

To change the widget name, choose the update interval, groups, and statuses, and specify the number of violators, in the right upper corner click ▾ and, in the drop-down list, select **Edit**. Edit required widget parameters, then click **Save**.

4.1.2.3 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.



Widget attributes:

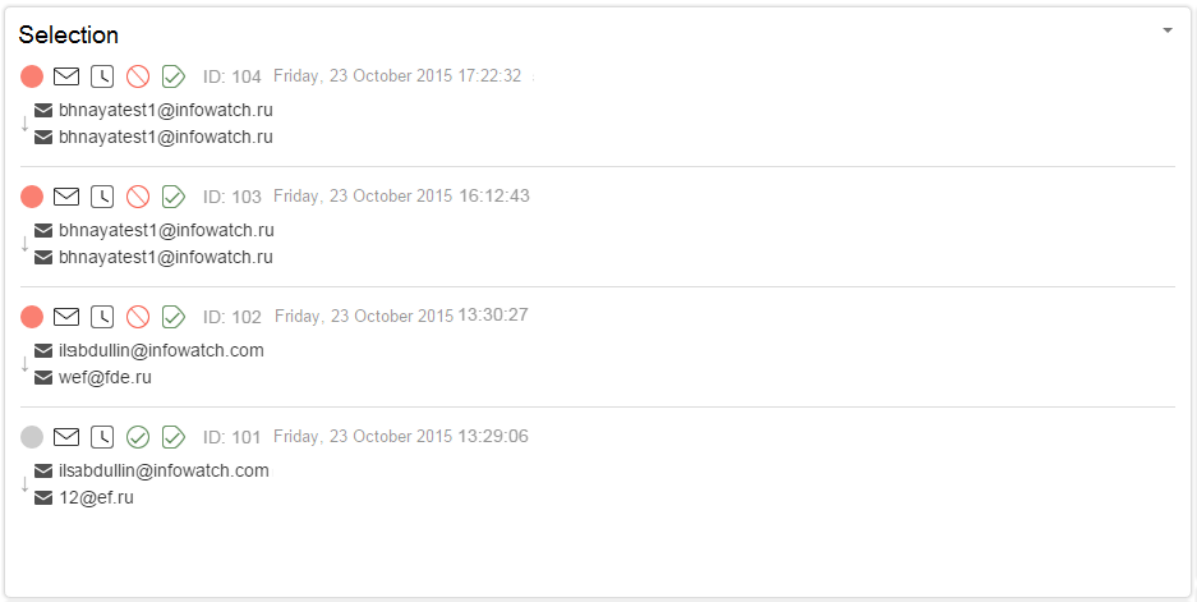
Parameter	Description
Name	Widget name
Update interval	The frequency of data update on the widget
Period	In the drop-down list in the left upper corner of the widget, specify the time period, over which the data is displayed.
View type	Data representation in the widget. Possible values: *Bar chart (horizontal)* and *Table*.

Note:

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

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

Widget attributes:

Parameter	Description
Name	Widget name
Update interval	The frequency of data update in the widget
Selection	The 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

Note:

When generating a dashboard summary (see "Dashboard Summary"), data of the **Selection** widget is not added to the summary.

4.1.2.5 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.

Widget attributes:

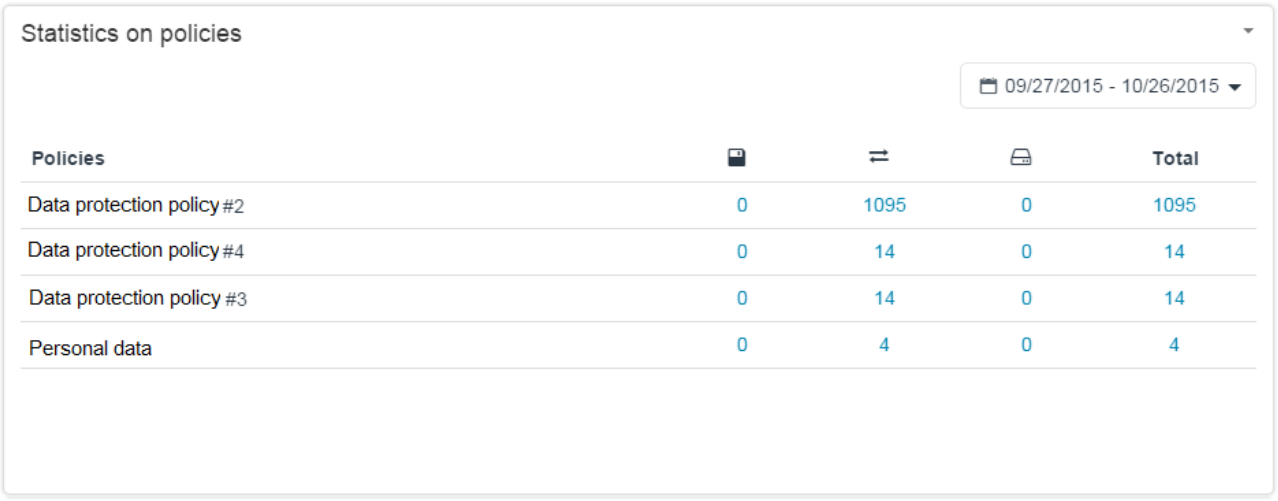
Parameter	Description
Name	Widget name
Update interval	The frequency of data update on the widget
Period	In the drop-down list in the left upper corner of the widget, specify the time period, over which the data is displayed.

Note:

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

4.1.2.6 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.

Widget attributes:

Parameter	Description
Name	Widget name
Update interval	The frequency of data update on the widget
Period	In the drop-down list in the left upper corner of the widget, specify the time period, over which the data is displayed.
Policies	Policies, a summary for which will be displayed. Start typing the policy name or click + and select required policies from the list.

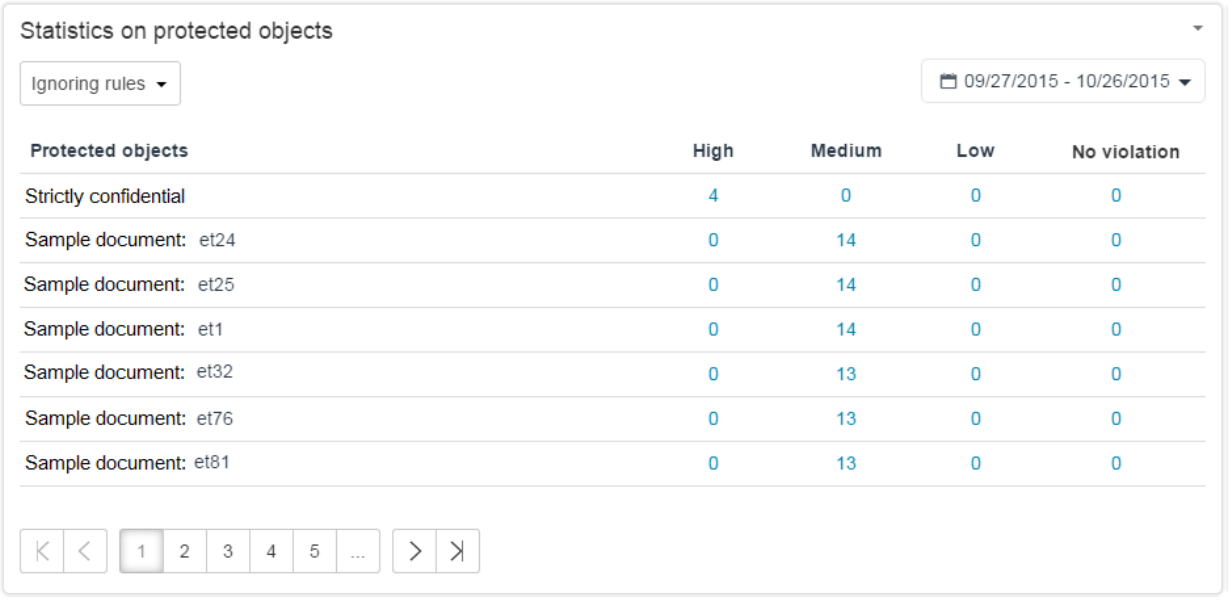
Note:

To change the widget name and choose the update interval and policies, in the right upper corner, click

and, in the drop-down list, select **Edit**. Edit required widget parameters, then click **Save**.

4.1.2.7 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.

Widget attributes:

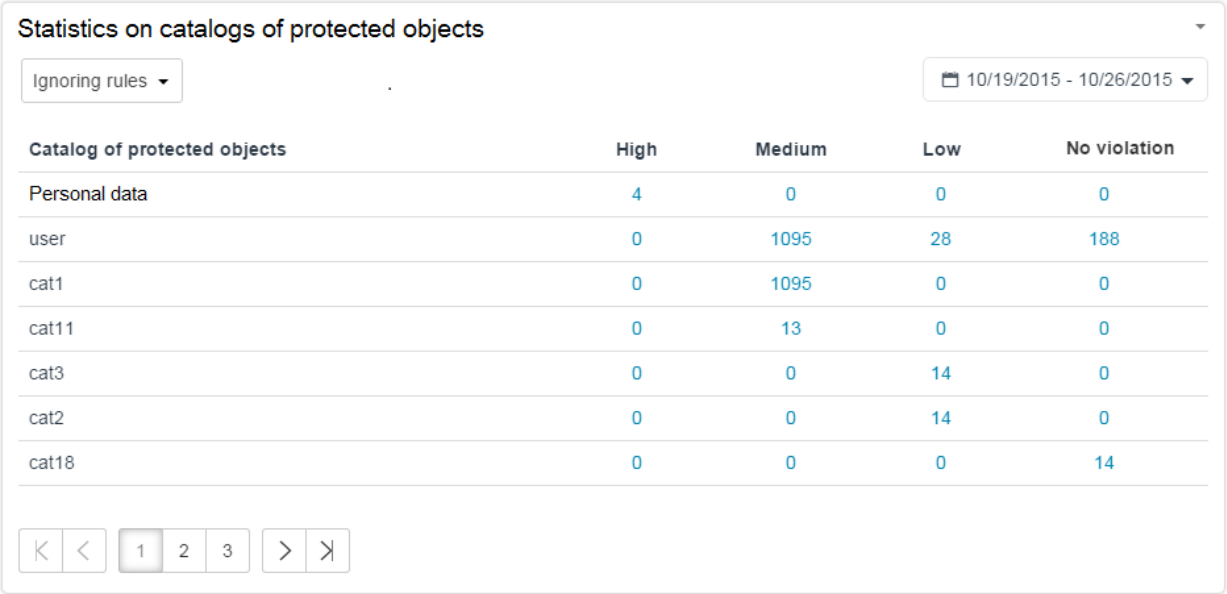
Parameter	Description
Name	Widget name
Rules	In the drop-down list in the left upper corner of the widget, select the type of rules, violations of which will be displayed in the widget. Possible values: *Transfer rules*, *Copy rules*, *Placement rules*, *Ignoring rules*.
Update interval	The frequency of data update on the widget
Period	In the drop-down list in the left upper corner of the widget, specify the time period, over which the data is displayed.
Protected objects	Protected objects, statistics for which will be displayed. Start typing the object name or click + and select desired objects from the list.
Catalog of protected objects	Catalogue of protected objects, statistics for which will be displayed. Start typing the catalogue name or click + and select desired catalogues from the list.

Note:

To change the widget name, choose the update interval, protected objects, and their catalogues, in the right upper corner click ▾ and, in the drop-down list, select **Edit**. Edit required widget parameters, then click **Save**.

4.1.2.8 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.

Widget attributes:

Parameter	Description
Name	Widget name
Rules	In 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*.
Update interval	The frequency of data update on the widget
Period	In the drop-down list in the left upper corner of the widget, specify the time period, over which the data is displayed.
Catalog of protected objects	Catalogue of protected objects, statistics for which will be displayed. Start typing the catalogue name or click + and select desired catalogues from the list.

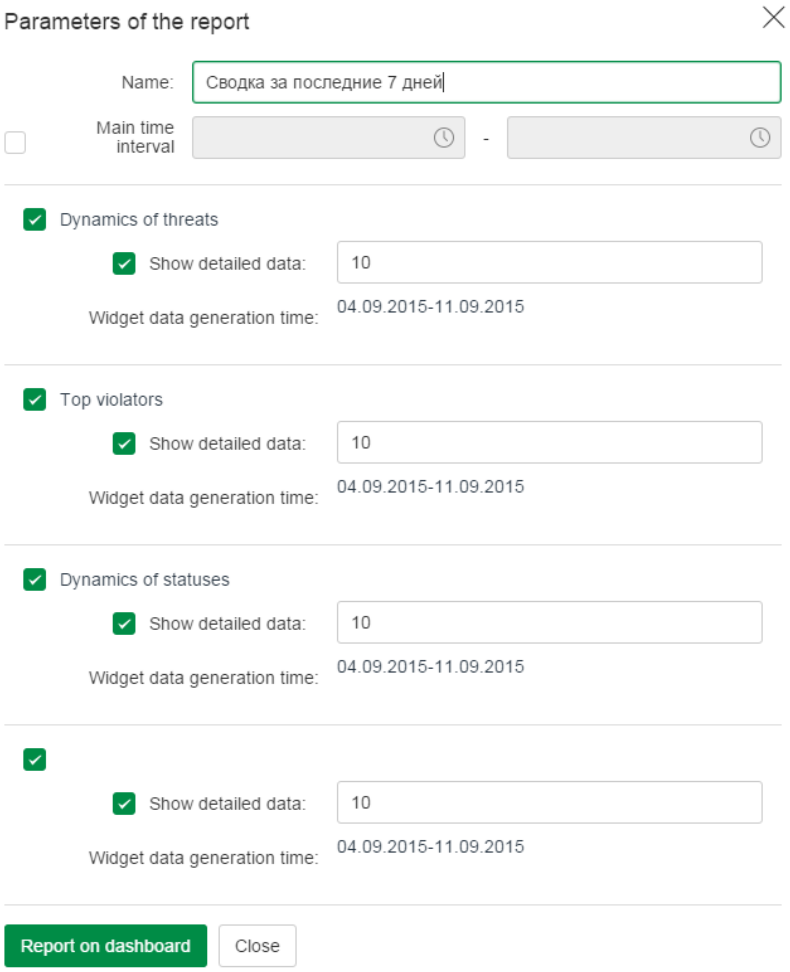
Note:

To change the widget name, choose the update interval and catalogues of protected objects, in the right upper corner, click ▾ and, in the drop-down list, select **Edit**. Edit required widget parameters,

then click **Save**.

4.1.3 Dashboard summary

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



Summary attributes:

Parameter	Description
Name	Summary name
Common period	Select this option if you want to create a summary for all widgets over a common period. Specify the start and the end date. **Note:** By default, a summary for each widget is created over the period specified in the widget settings.

Parameter	Description
Widget block	Indicates whether data of the widget are included in the summary. By default, the summary is created for all widgets of a dashboard. If you do not want to include data from a particular widget, deselect the checkbox next to its name. **Important!** The summary does not include data from the "Selection" widget.
Display detailed data	Select this option if you want the summary 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 summary.

User's target actions:

- Creating a dashboard summary (see "Managing Summaries").

4.2 Events Section

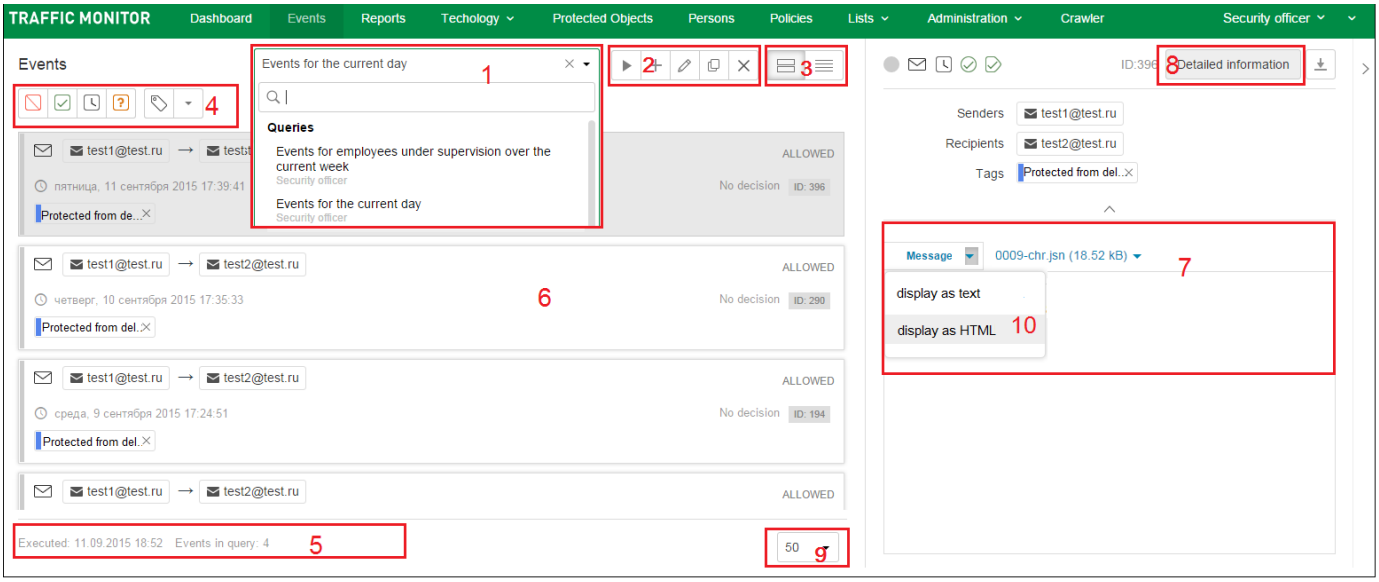
Reference information:
Event is the interception object of network traffic.

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 section contains the following elements:

№ on scheme	Element	Purpose
1	Drop-down list of queries	Contains a list of available queries used for filtering interception objects (see "Queries") **Note:** for each query, its name and the user who has created this query are specified
2	Toolbar for working with queries	A set of tools for working with queries
3	Buttons to select style of event display	Switching between the styles of displaying events:  - displaying events as tiles;  - displaying events as a table;
4	Toolbar for events	A set of tools for working with events
5	Event attributes: execution time and the number of found events	Displays the date of the query execution in the format MM/DD/YY, execution time and the number of found events
6	List of events	A list of interception objects found as a result of the query execution (see "Object Interception"). **Note:** On characteristics of the event tile, see "Event tile"
7	Brief Event Viewing Form (see “Brief Event Viewing Form")	The most frequently used information on the event (see "Brief Event Viewing Form")
8	Detailed information on the event (see "Detailed Event Viewing Form")	Complete information on the event
9	Drop-down list with the number of records on the page	Allows you to choose the number of events to be displayed
10	Event viewing mode (only for messages with HTML markup)	Allows you to choose the event viewing mode. Possible values: **display as text** - is used for displaying message text without formatting. Allows viewing hidden text (for example, white text or text contained in the picture name); **display as HTML** - allows viewing pictures, tables, and text markup.

User’s target actions:

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

4.2.1 Queries

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

The query is a selection of intercepted objects according to specified conditions.

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

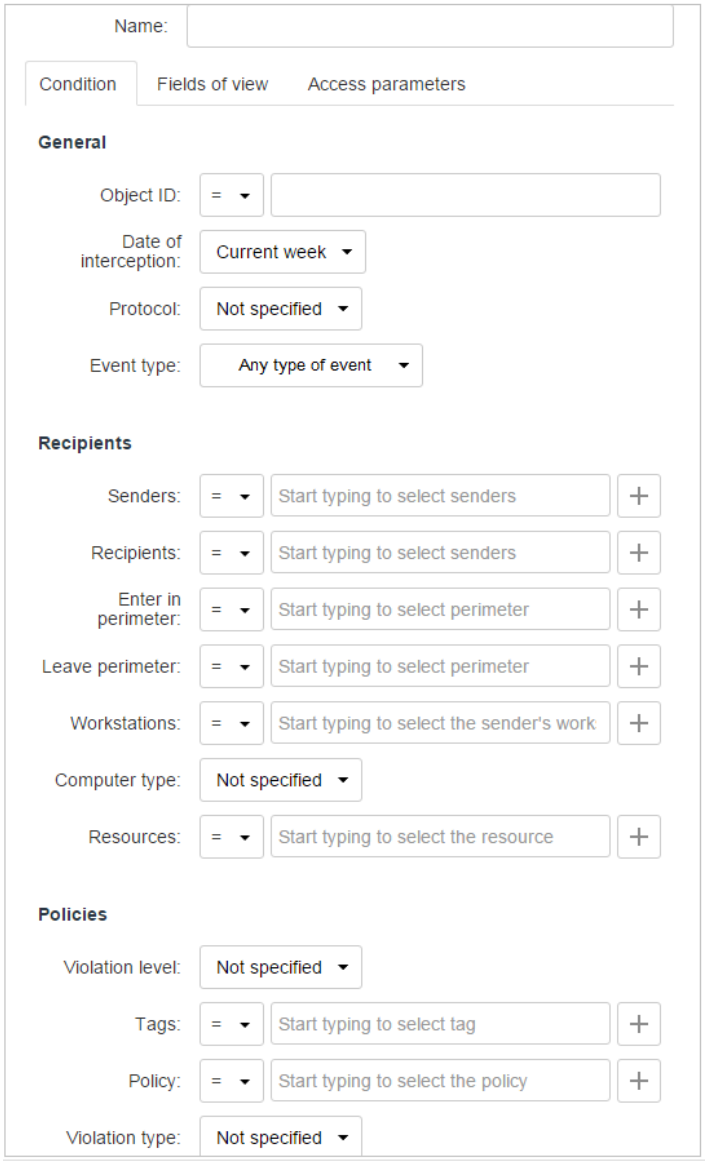
The query creation form contains the following tabs:

Element	Purpose
Condition	On this tab you can specify criteria of search
Display fields	On this tab you can choose fields to be displayed in event records
Access parameters	On this tab you can configure access to the query and make it available to the owner only

User's target actions:

- configuring parameters of the query (see "Creating queries");
- defining fields of view (see "Choosing event fields of view").

4.2.1.1 Condition



Events section, **Condition** tab for a selected query

The query attributes:

Parameter	**Description**
=	Parameter of attribute equality
≠	Parameter of attribute negation
Date of interception	The date when the event was created. By default events for the current week will be displayed.
Object ID	Unique identifier of the event. Multiple values may be specified, separated by commas.

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: • Internet activity: - Web-message • File sharing: - FTP - External device • Printers and MFPs - Print • Multimedia recording - Photography • Storage - Crawler • Email - Email - Webmail • Messenger WhatsApp - Yahoo! -MS Lync - ICQ - XMPP - MMP - Skype • Cellular communication - SMS
Protocol	Protocol through which the traffic is transferred
Senders	The list of object senders
Recipients	The list 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
Computer type	Type of computer from which the object was sent. Possible values: • computer • mobile device • 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. **Note**: If you want to specify a particular resource, choose icon (for example, facebook.com)
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	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*.
Task name	Name of the scanning task.
Date of task start	The date when the task was started
Type of scanning source	Type of the location where the object was found. Possible values: • Shared network resources • Local drives of workstations • SharePoint file storage
Attachment name	The name of the object attachment. The file name and extension must be specified.
Attachment format	Attachment format. You can select multiple values from the list.
Encrypted file	Whether the attachment is encrypted or not
Path to file	File source
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. Indexing of events is performed every ten minutes, however under a heavy load on the server, this interval may increase.
Analysis results	Elements of technologies included in protected objects that were triggered on events
Protected objects	List of triggered protected objects

When adding or editing conditions, you can specify positive or negative parameters of the query:

- For a required attribute to be included in search results, set the equality parameter next to it.
- For a required attribute to be excluded from search results, set the negation parameter  next to it.

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

- Object ID
- Senders
- Recipients
- Entered perimeters
- Left perimeters
- Sender's workstation;
- Resources
- Tags
- Policy
- Attachment name
- Attachment format
- Event text
- Results of analysis
- Protected objects

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.

For **Senders**, **Recipients**, **Computers** (computer name or IP address), **Resources**, **Task name**, **Attachment name** and **Path to file** attributes, you can specify values using wildcards:

- ? - for a separate character

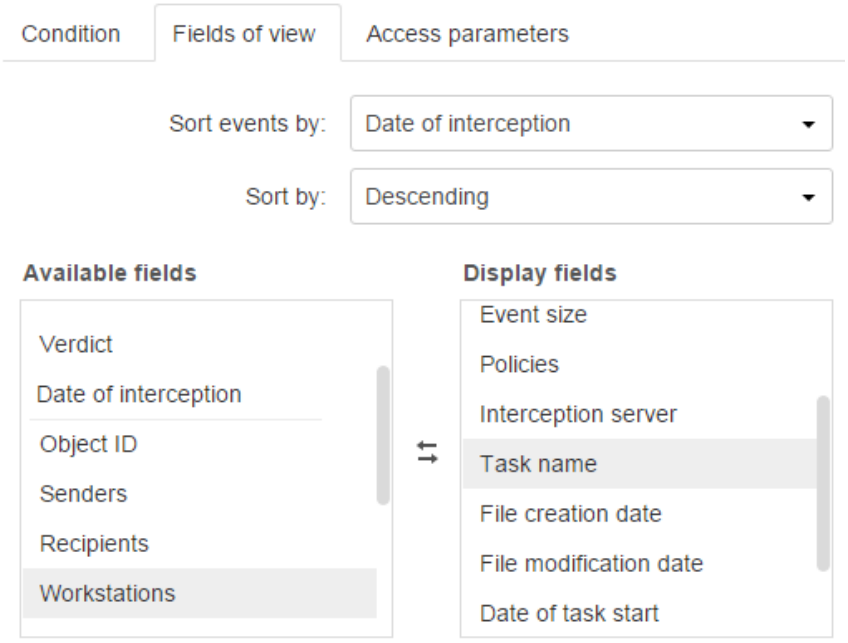
- * - for a number of characters.

User's target actions:

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

4.2.1.2 Displayed Fields

The left field contains the list of available event attributes, and the right one contains event attributes that will be displayed in a table view and unloaded to the export file in `.xslx` format. If there are no selected attributes, then both the table view and the unloading will contain all attributes.

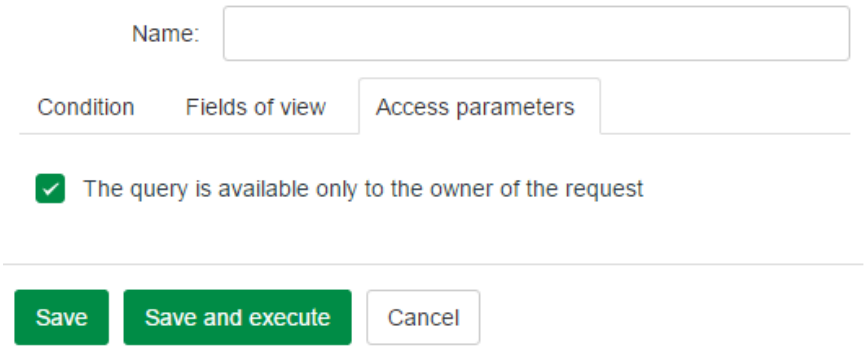


Events section, **Displayed fields** tab for a selected query

User's target actions:

- Specifying the fields that will be displayed in the event information (see "Choosing event fields of view")
- Exporting events (see "Unloading event")

4.2.1.3 Access Parameters



Events section, **Access parameters** tab for a selected query

To forbid viewing and editing the query by other users:

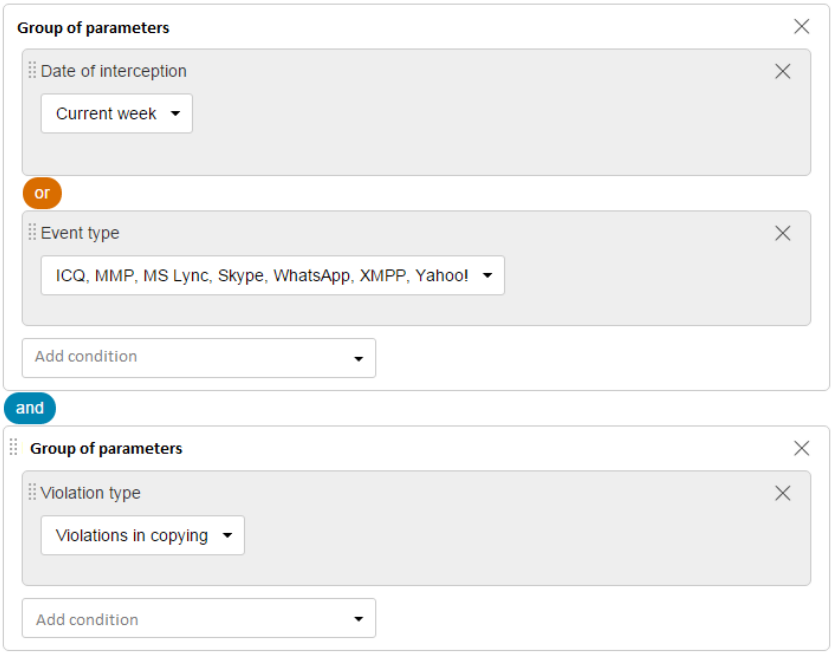
1. Select the check box **The query is available only to the owner**.
2. Click **Save**.

To permit viewing and editing query by other users:

1. Clear the check box **The query is available only to the owner** (by default, the check box is selected).
2. Click **Save**.

4.2.1.4 Advanced Mode

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



The following elements are used for creating a query:

- A list of event attributes. This is a set of attributes assigned to the intercepted object
- Group of parameters. This is a container intended for a logical separation of query parts

- = – parameter of attribute equality. Indicates that events will be filtered with respect to the presence of the attributes to which this parameter is assigned;
- ≠ – parameter of attribute negation. Indicates that search results will not contain events to which this parameter is assigned.

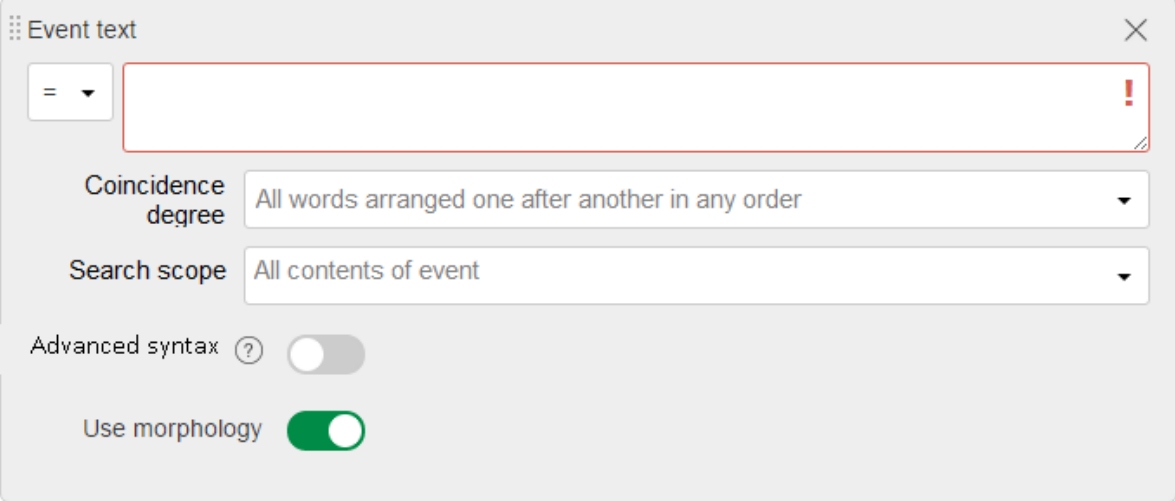
In the advanced mode, you can also perform a flexible search on the text of events..

User's target actions:

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

4.2.1.5 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
Condition	Parameter of attribute equality. Possible values: = - indicates that filtering results will contain events with attributes for which this parameter has been assigned; ≠ - indicates that events with attributes for which this parameter has been assigned will be excluded from search results.

Parameter	Description
Coincidence degree	Specify the required coincidence degree: • **All words arranged one after another in a 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 arranged one after another 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 irrespective of their order and 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 specified 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.
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 text** - 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:** The **Use morphology** option is available only if the construction of the morphological index is enabled in database settings. For detailed information on this setting, please see the document *"Traffic Monitor. Administration Guide".*

Please note that:

- Words must be divided with spaces.
- Search in not case-sensitive.
- Using wildcards ("*", "?") is not supported.

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.

Warning!

In case of using Oracle database to store events (see "InfoWatch Traffic Monitor. Administration guide", article "Oracle"), events, which contain non-printable characters (for example, emoticons), are not indexed and, respectively, are not available for search.

User's target actions:

- Configuring an advanced query (see "Query Creation in Advanced Mode").

4.2.2 Object Interception

he list of events displays intercepted objects which confirm query conditions.

Information on the event is represented in following ways:

- the event tile (or the table entry) contains general information about the event;
- the short form viewing event displays the most commonly required information;
- the detailed event viewing form displays complete information about the interception object.

Attributes of interception objects:

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*.

Element	Description
Event type	The source of actions which led to the event creation. Possible choices: •  - Internet activity (post requests to Web resources); •  - File exchange (copying files to an external device, transfer via FTP); •  - Printer and MFP (sending files to print); •  - Recording media (sending or receiving photos); •  - Email (sending and receiving electronic data via email and Web-mail); •  - Messenger (sending or receiving messages through Skype, Mail.ru Agent (MMP), MS Lync, ICQ(OSCAR), XMPP, Yahoo, WhatsApp); •  - Cellular communication (sending or receiving messages via SMS); •  - 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
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 event (in bytes)

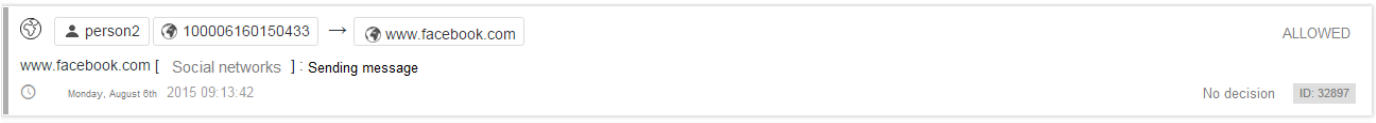
Element	Description
Violation level	Characteristics of the violation assigned to the event. Possible choices: • *None* - is marked with a gray (■) color on the tile; • *High* - is marked with a red (■) color on the tile; • *Medium* - is marked with an orange (■) color on the tile; • *Low* - is marked with a green (■) color 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 (see "Object analysis and verdict"). Possible choices: • *Allowed* ( ) • *Blocked* ( ) • *Quarantined* ( ) **Note:** Events with *Deleted* verdict are deleted from the System and are not displayed in the Management Console.
Interception server	The name of the server which intercepted the object.

See also:

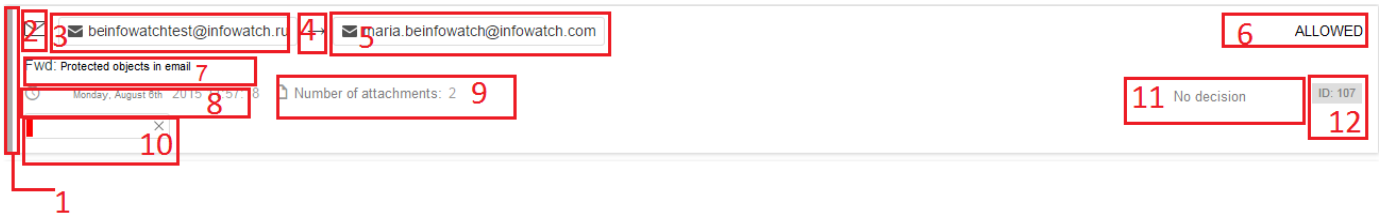
- "Event Tile" - on the structure of the element outputting information about the event by default.
- "Brief Event Viewing Form" - on displaying general information about the event.
- "Detailed Event Viewing Form" - on displaying advanced information about the event.

4.2.2.1 Event tile

The event tile looks like following:

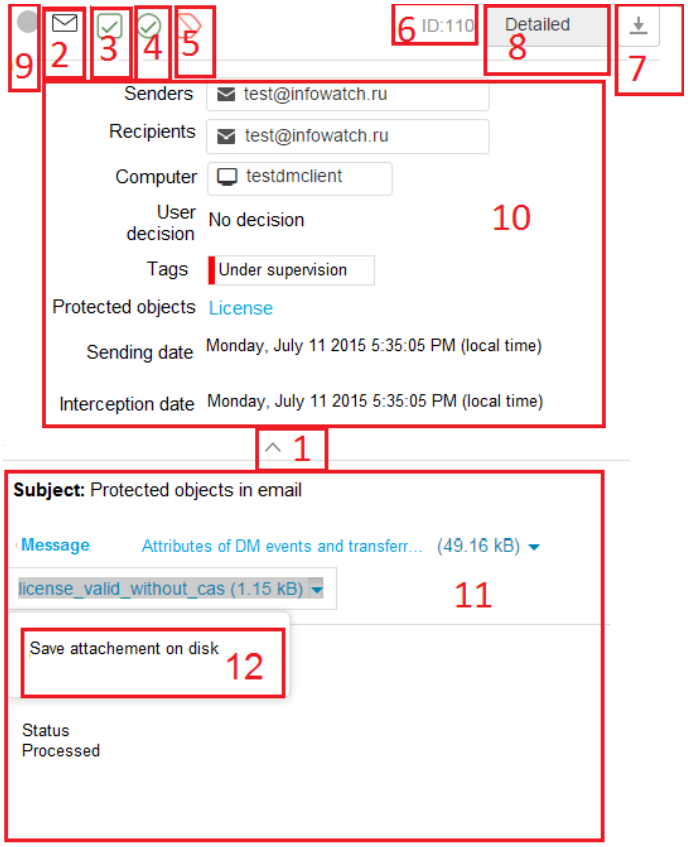


It consists of the following elements:



where
1 - Color of violation level. Possible values: *High*, *Medium*, *Low*, *No violation*.
2 - Event type. Possible values: *Web message*, *FTP*, *External device*, *Print*, *Photo*, *Crawler*, *Email*, *Webmail*, *WhatsApp*, *Yahoo!*, *MS Lync*, *ICQ*, *XMPP*, *MMP*, *Skype*, *SMS*.
3 - Sender (the list of senders)
4 - Traffic direction
5 - Recipient (the list of recipients)
6 - Verdict. Possible values: *Allowed*, *Blocked*, *Quarantine*.
7 - Event preview (brief information on how the event appeared: in the first example, the reason is sending a message in a social network, in the second one - sending a letter)
8 - Event creation date
9 - Attachment indicator
10 - Assigned tags (see "Tags")
11 - User decision. Possible values: *Violation*, *No violation*, *No decision*, *Requires additional processing*.
12 - Object ID

4.2.2.2 Brief Event Viewing Form



Events section, a detailed viewing form of the selected event

A brief event viewing form contains the following entities:

№ on scheme	Entity	Description
1	Button that shows/hides event attributes	Shows/hides event attributes
2	Icon of event type	Displays an icon of the event type. Possible values: *Web message*, *FTP*, *External device*, *Print*, *Photo*, *Crawler*, *Email*, *Webmail*, *WhatsApp*,*Yahoo!*, *MS Lync*, *ICQ*, *XMPP*, *MMP*, *Skype*, *SMS*.
3	User decision	Displays the value of the **User decision** attribute. Possible violations: *Violation*, *No violation*, *No decision*.
4	Verdict	Displays the value of the **Verdict** attribute. Possible values: *Allowed*, *Blocked*, *Quarantine*.
5	Sending status	Displays the value of the **Sending status** attribute. Possible values: *Sent*, *Not sent*, *Waiting for sending*.
6	Object ID	Displays the value of the **Object ID** attribute

№ on scheme	Entity	Description
7	Button for saving event	Button that allows you to save the event to disk (see "Saving Events"). The button is displayed for SMTP letters only.
8	Button for calling a detailed event viewing form	Opens the detailed event viewing form
9	Violation level	Displays a color designation of the **Violation level** attribute. Possible values: *High*, *Medium*, *Low*, *No violation*.
10	Event attributes	Extracted attributes of the interception object
11	Field of viewing the event and its attachments	Displays the event text and its attachments
12	**Save attachment to disk** command	The Security Officer can save attachments to the disk

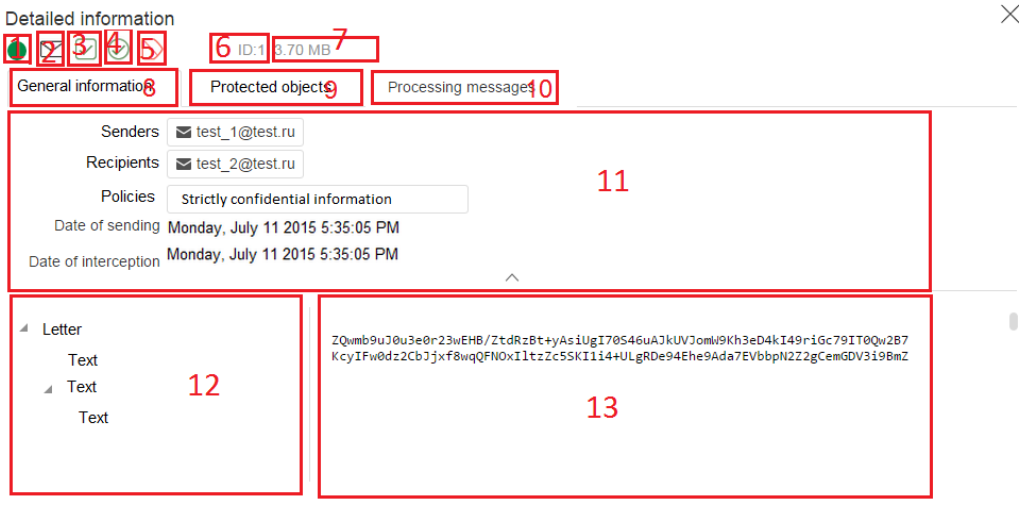
Note:

The set of objects on the brief event viewing form may vary depending on extracted attributes.

User's target actions:

- Getting acquainted with general information about the event (see. "Viewing Brief Event Form")

4.2.2.3 Detailed Event Viewing Form



Events section, a detailed viewing form of the selected event, **General information** tab

A Detailed Event Viewing Form contains the following tabs:

Tab	Purpose
General information tab	Displays general information represented in a brief event viewing form
Protected objects	Displays information about triggered protected objects and their elements of analysis
Processing messages	Displays system messages on the stages of object processing and problems that encountered during processing

The Detailed Event Viewing Form contains the following entities:

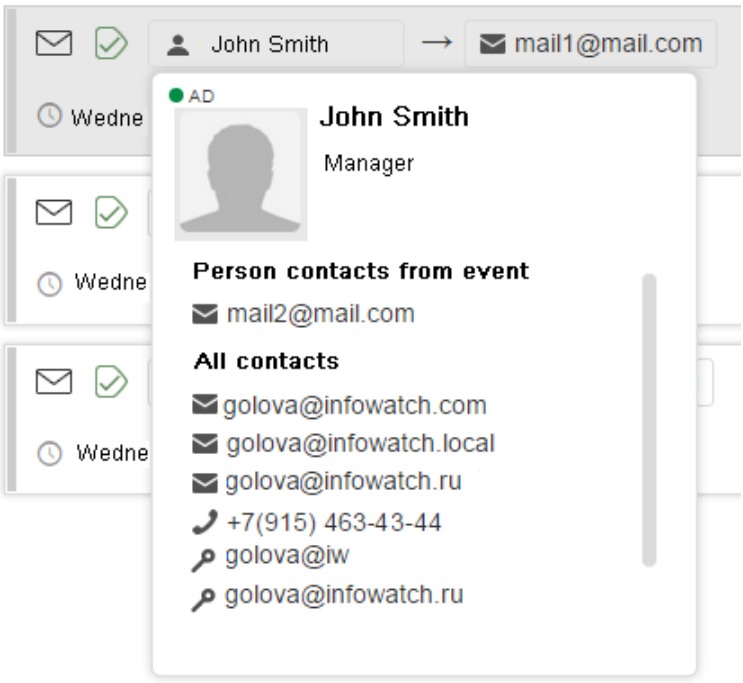
№ on scheme	Entity	Description
1	Violation level	Displays a color designation of the **Violation level** attribute. Possible values: *High*, *Medium*, *Low*, *No violation*.
2	Event type	Displays the value of the **Event type** attribute. Possible values: *Web message*, *FTP*, *External device*, *Print*, *Photo*, *Crawler*, *Email*, *Webmail*, *WhatsApp*, *Yahoo!*, *MS Lync*, *ICQ*, *XMPP*, *MMP*, *Skype*, *SMS*.
3	User decision	Displays the value of the **User decision** attribute. Possible violations: *Violation*, *No violation*, *No decision*, *Additional processing is required*.
4	Verdict	Displays the value of the **Verdict** attribute. Possible values: *Allowed*, *Blocked*, *Quarantine*.
5	Sending status	Displays the value of the **Sending status** attribute. Possible values: *Sent*, *Not sent*, *Waiting for sending*.
6	Object ID	Displays the value of the **Object ID** attribute
7	Size of event	Displays the value of the **Size of event** attribute
8	General information tab	Information represented in a brief event viewing form
9	Protected objects	List of triggered protected objects and catalogs to which those protected objects belonged at the time of interception
10	Processing messages	Object processing messages
11	Panel of viewing a selected tab	Viewing information, depending on the selected tab (**General information tab**, **Protected objects** or **Processing messages**)
12	Panel with the extracted attributes	Viewing titles of the extracted object attributes
13	Panel of viewing an extracted attribute	Viewing attributes extracted from the object

User's target actions:

- Getting acquainted with extended information about the event (see "Viewing Detailed Event Form")

4.2.3 Contact Identification in Event

Based on data extracted from 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.



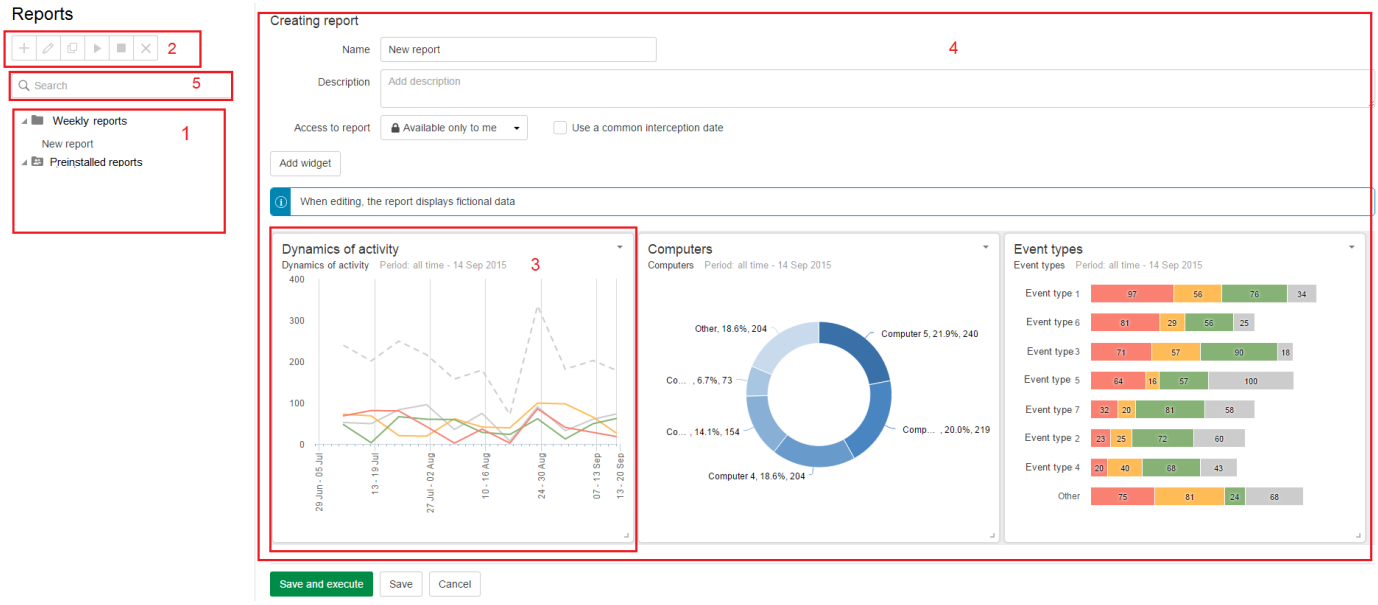
If during processing an event, the System detects new private contacts of a person, detected contacs are added to the person card automatically. The process of automatic adding new contacts to existing persons is called ***post identification***. As a result of post identification, such data as email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

4.3 Reports Section

About the section:

Contains a sampling of statistical data on intercepted objects.

Statistical data is displayed on widgets in the form of charts and diagrams. Each report can contain one or more widgets.



The section contains the following elements:

№ on scheme	Element	Purpose
1	Drop-down list of folders with reports	Contains the list of folders in which the available reports are grouped
2	Toolbar for reports	Set of tools for working with reports
3	Report widgets	Contain a graphical representation of statistical data on intercepted objects
4	Report creation or edit window	Contains report parameters and added widgets
5	Search field	Start typing to search for reports and folders by their names

The **Preinstalled reports** folder contains the following reports:

Report	Description
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

Preinstalled reports are available to all users of the System.

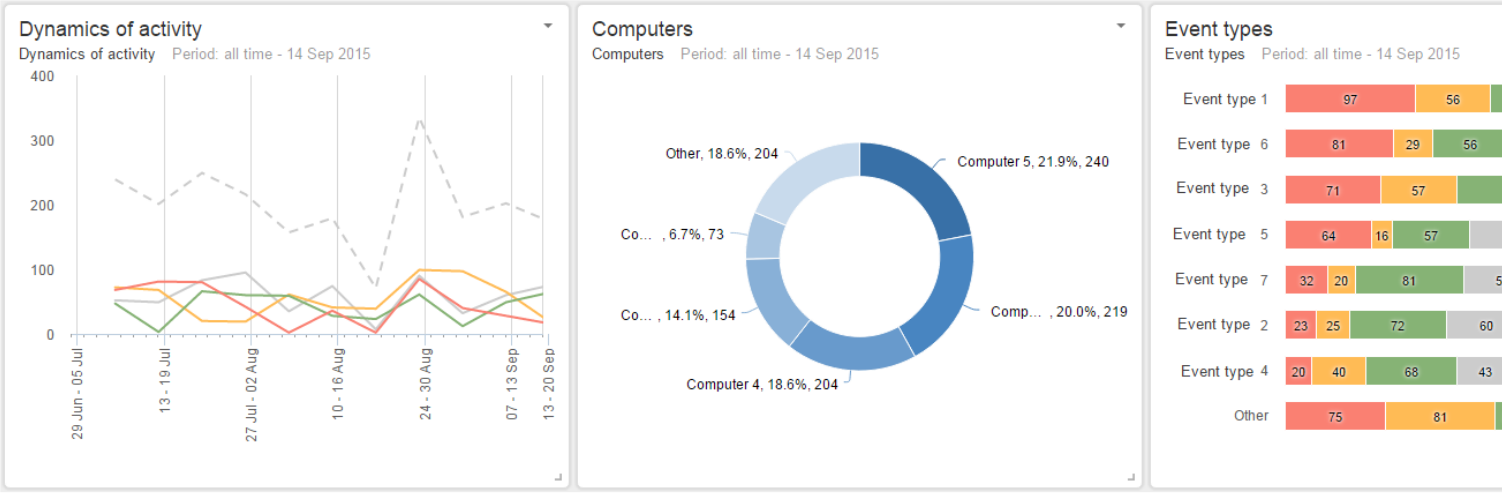
User's target actions:

- Creating report
- Customizing widgets to display statistical information

- Creating folder with reports
- Working with ready reports

4.3.1 Widgets of Reports

The workspace of the **Reports** section contains widgets.



Widgets of the **Reports** section

Widgets are designed to display statistical information on intercepted objects for 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
Catalogues 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

Type of statistics	Description
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 of diagram 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

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.
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.

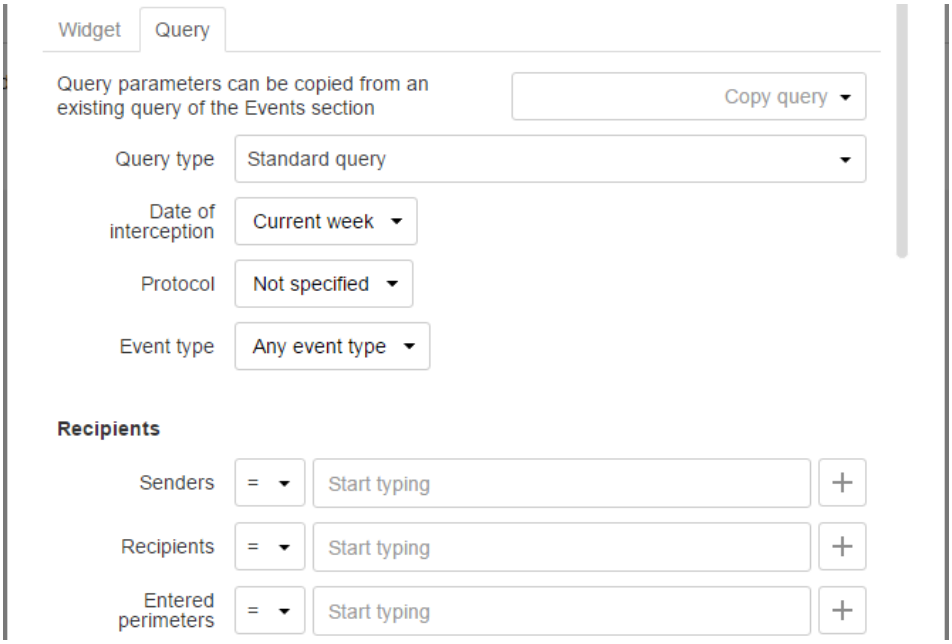
User’s target actions:

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

4.3.2 Queries

A query allows you to select interception objects to be displayed in the widget.

You can copy parameters of a query that has been added in the **Events** section, or create a new query.



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

A query can be created in the standard or advanced mode.

The standard mode allows you to select query conditions from the list (for details, see "Condition").

In the advanced mode, you can perform a more flexible configuration of query conditions (for details, see "Advanced mode").

User's target actions:

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

4.3.3 Report Execution History

Report execution history allows you to view executed reports, delete obsolete report versions, and save selected versions to a file.



Attributes of the report execution history:

Parameter	Description
Execution date	Date and time of the report execution
Comment	Comment to the report added by the user

User's target actions:

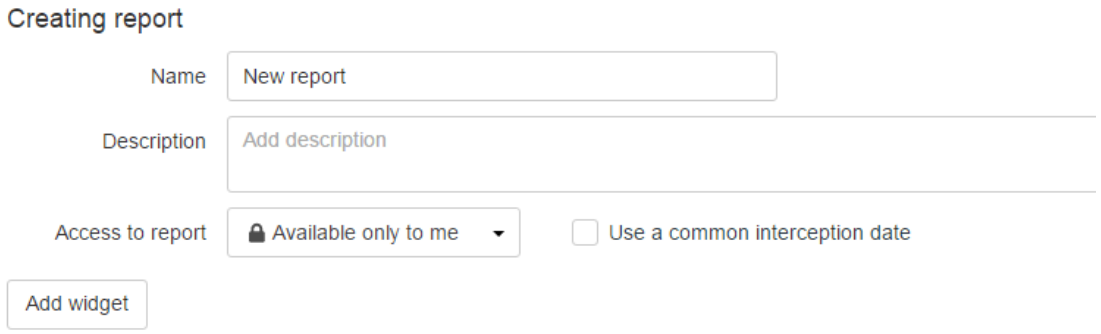
- viewing report execution history and, if necessary, deleting selected report versions or saving selected versions to file (see "Managing ready reports").

4.3.4 Report Creation Form

The report creation (edit) form is displayed when you create a new report or edit an existing one.

In the left part of the working area of the **Reports** section, you can see the list of folders that contain reports.

Reports allow you to generate statistics based on data stored in the System.



Report parameters:

Parameter	Description
Name	Report name
Description	Description in any form
Access to report	Specify if the report is available only to the owner or to all users. This option is available only to reports of the first level. When creating a report within a folder, the access level specified for the folder defines the access level for the report.
Use common interception date	Select this check-box if you want to use the specified interception date for all added queries. When selecting this option, a drop-down list is displayed where you can specify a desired period.

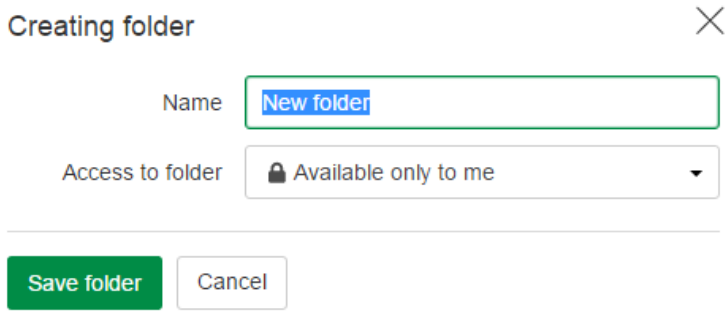
User's target actions:

- creating a report

4.3.5 Report Folder Creation Form

In the left part of the working area of the **Reports** section, the list of folders is displayed.

Folders allow you to group reports on some basis, inherit permissions and copy a selected group of reports.



Folder attributes:

Parameter	Description
Name	The name of the folder
Access to folder	Specify if the folder will be available only to the owner or to all users. This option is available only to folders of the first level. When creating subfolders, the access level is inherited from the parent folder.

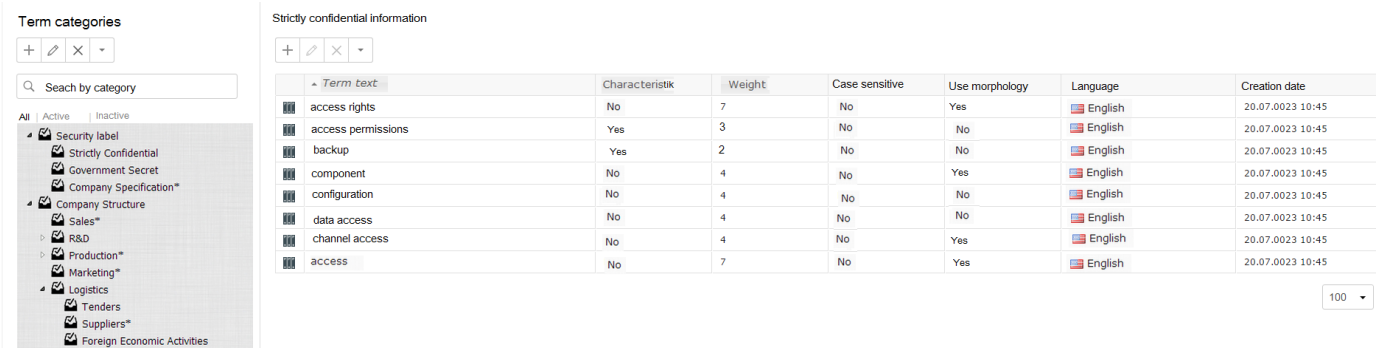
User's target actions:

- creating a folder with reports

4.4 Technologies Section

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

About the section:
The section contains editable catalogs of categories and terms, text objects, sample documents, blanks, stamps, database unloadings as well as the list of preinstalled graphical objects.



Technologies section, **Categories and terms** subsection

The section contains the following elements:

Element	Purpose

Element	Purpose
Tabs with types of catalogs: • Categories and terms • List of text objects • List of sample documents • List of blanks • List of stamps • List of DB unloadings • List of graphical objects	Contain the lists of elements and tools for a selected catalog
Toolbar	A set of tools for working with a selected catalog
Page navigation panel	The set of buttons for browsing pages with entries (if not all entries can be placed on one page)
Control of the entries number	The drop-down list where you can set the number of entries per page

User's target actions:

- Creating a list of categories and terms (see "Creating categories and terms")
- Creating a list of text objects (see "Creating text objects and their values")
- Creating a list of sample documents (see "Managing sample documents")
- Creating a list of sample blanks (see "Creating sample blanks")
- Creating a list of sample stamps (see "Creating sample stamps")
- Creating a list of DB unloadings (see "Creating DB unloadings")

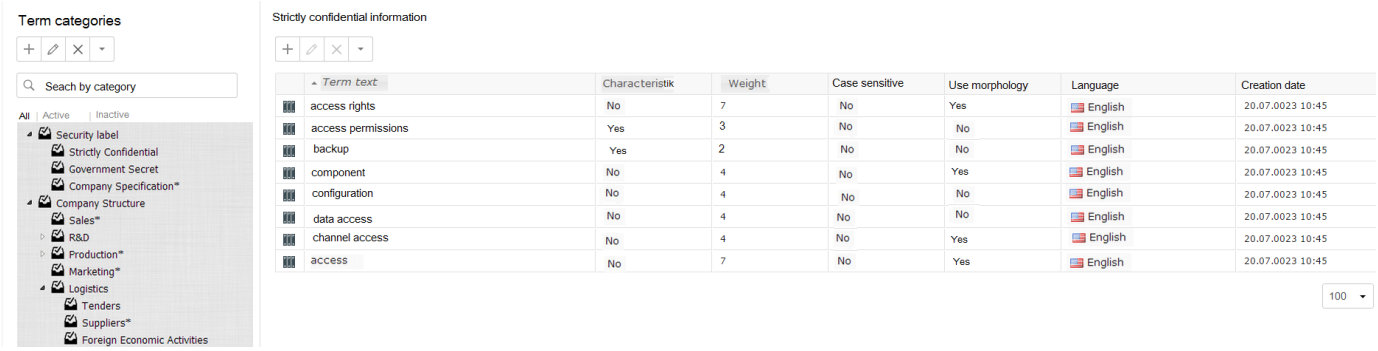
4.4.1 Categories and Terms

Reference information:

Categories and terms are a set of data required for linguistic analysis.

Categories classify possible violations of a security policy. If the text contains an element 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.*



The subsection contains the following elements:

Parameter	Description
List of categories	A set of subject areas the intercepted objects can correspond to
List of terms	A set of terms for the selected category
Toolbar	A set of tools for categories and category elements
Search string	A string where you can enter some text to search for by categories
Page navigation panel	The set of buttons for browsing pages with entries (if not all entries can be placed on one page)
Control of the entries number	The drop-down list where you can set the number of entries per page

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")

4.4.1.1 Categories

Reference information:

The ***category*** is a set of elements corresponding to a specific topic (for example, *Security labels* or *Project terms*). It contains either the list of categories (subcategories) or the list of elements relating to the category.



Note:

Preset categories marked with an asterisk (*) do not contain objects. Such categories are filled during the System implementation or later during customization.

Category attributes:

Parameter	Description
Name	Category name
Weight	The value specified by default for all terms of the category as the **Weight** attribute
Language	The language of category terms
Use morphology	Indicates if morphological forms of a term are taken into account in traffic analysis
Case sensitive	Indicates if the case is matched in traffic analysis
Description	Description in any form
Creation date	The date and time of category creation
Modification date	Date and time of the last modification of the category This attribute is displayed in the edit mode only.

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")

4.4.1.2 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.


Strictly confidential information

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 (if found in the analyzed text) increases the degree of conformity of the text to the term category
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
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
Creation date	The date and time of term creation
Modification date	Date and time of the last modification of the term. This attribute is displayed in the term edit mode only.

Note:

The **Case sensitive** and **Use morphology** 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.

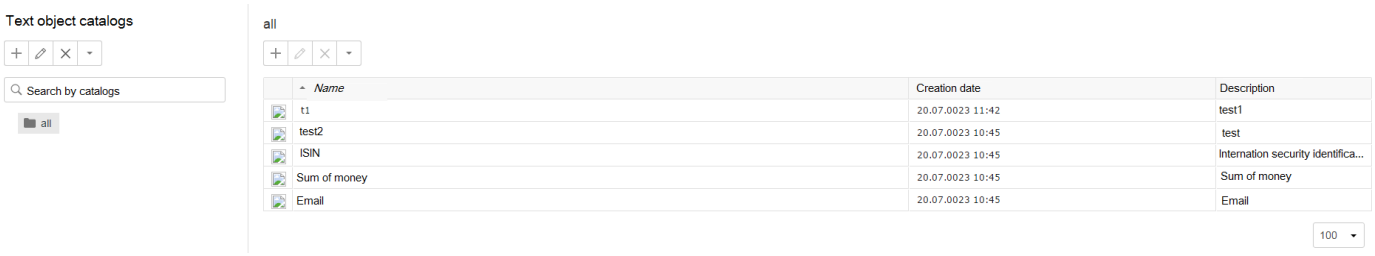
User's target actions:

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

4.4.2 Text Objects

Reference information:
The ***text object*** is a text information extracted from the object body and attachments. Contains no formatting or markup. Is used for analysis and search.

Both system and user-created text objects can be used in the System.
Text objects are created within catalogs. For operations with catalogs (creating, editing or deleting a catalog; search by catalogs), tools on the left side of the working area are used. Text objects of a selected catalog and tools for operations with text objects are located on the right side of the working area.



For adding an object to the catalog, the + toolbar button on the right side of the working area is used.

Editing properties of an added text object is done with the button. When clicking on this button, the edit window opens where you can view and change (if necessary) attributes of a selected object. To delete the selected text objects, use the × button.

> **Warning!**
>
> When deleting a system text objects from a catalog, user templates created for this object will also be deleted.

Text object parameters:

Parameter	Description
Name	Category name
Creation date	Date and time of the text object creation
Modification date	Date and time of the last modification of the text object. This attribute is displayed in the term edit mode only.
Text objects patterns	Value of the text object defined in a form of the exact sequence of symbols or using a regular expression. This attribute is displayed in the term edit mode only.
Description	Description in any form

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

User's target actions:

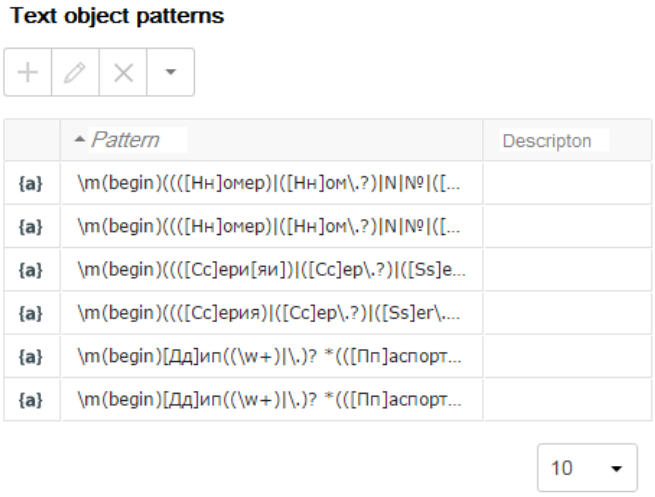
- Creating text objects and their catalogs (see "Managing Text Objects");

- Adding system text object to a selected catalog (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")

4.4.2.1 Text objects patterns

Reference information:
The *text object pattern* is a value of the text object set in a form of the exact sequence of symbols 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.

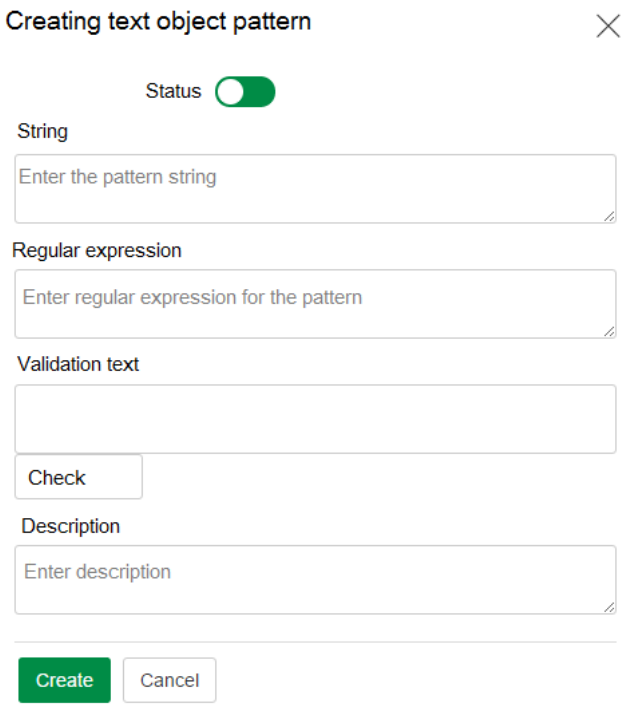


Using buttons of the toolbar you can add a new pattern (button), switch to the edit mode of a selected pattern (button), delete selected templates (button), and change pattern status (for this, click and in the drop-down list select **Activate**/**Deactivate**). The current status of a pattern is displayed 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 a pattern, a pattern creation window opens where you can specify the pattern attributes.



Pattern attributes:

Parameter	Description
Status	Indicates if this text object value is used.Possible values:*Active* and *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*. 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 creating custom templates, see the Internet article "Regular Expression Language".
Validation text	Appears if you select the type of template - *Regular expression*. Example of a text for finding the regular expression. Enter the verification text and click **Check**.
Description	Description in any form

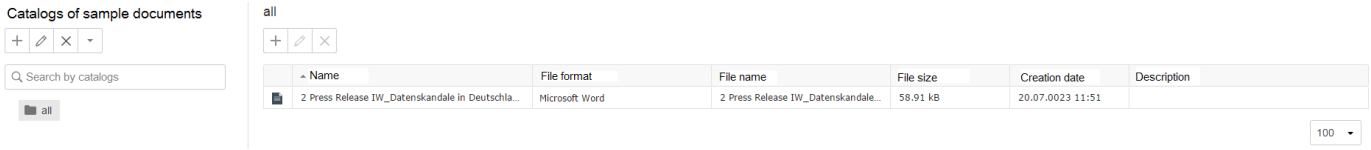
User's target actions:

- Creating a text object

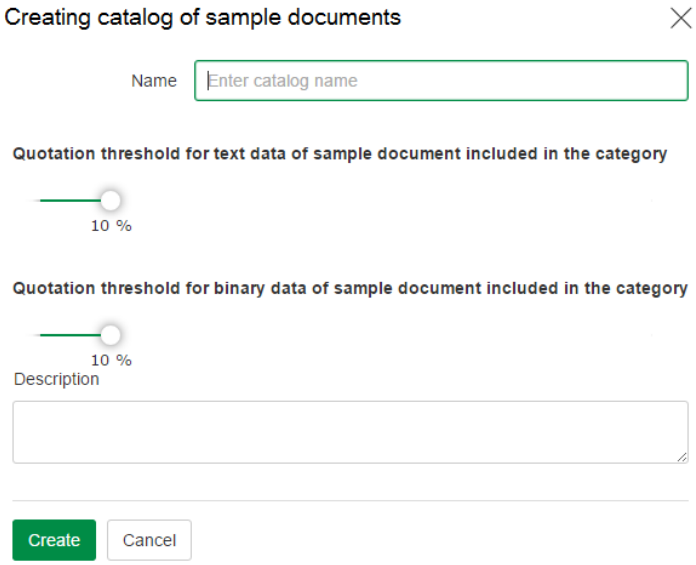
4.4.3 Sample Documents

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 catalogs.



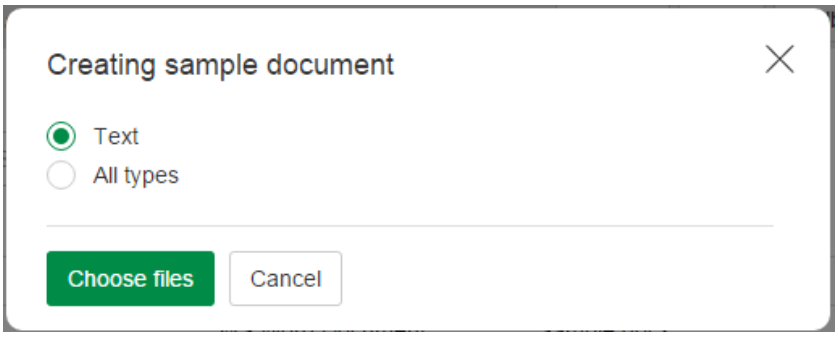
Clicking on the  button on the toolbar on the left side of the working area opens a catalog creation window where you can specify its attributes.



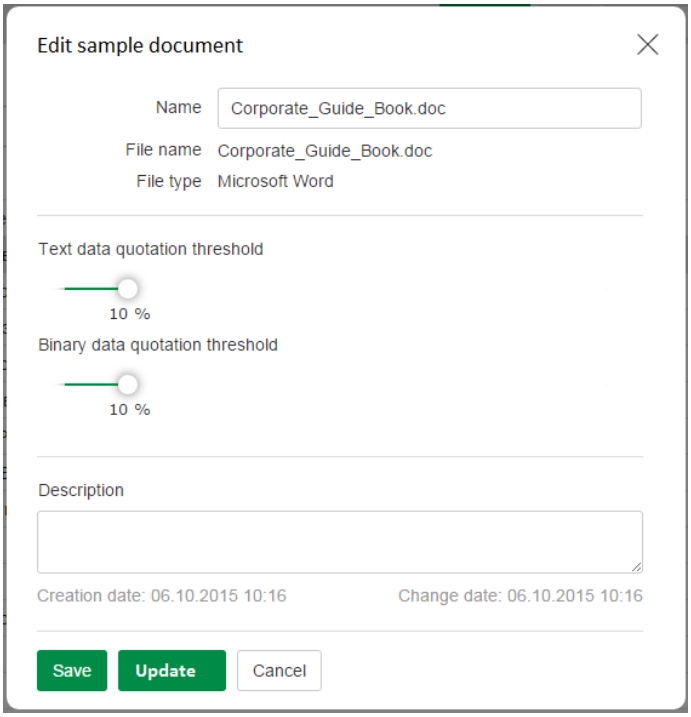
Attributes of the catalog of sample documents:

Parameter	Description
Name	Name of the catalog of sample documents:
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	Description in any form

Adding a file of the sample document to a created catalog is performed with the  toolbar button on the right side of the working area. In the dialog window that opens, specify the data type (**Text** or **All types)** and choose files to be downloaded.



Editing properties of an added sample document is performed with the button on the toolbar. In the window that opens, you can view and change (if necessary) the attributes of the selected sample document.



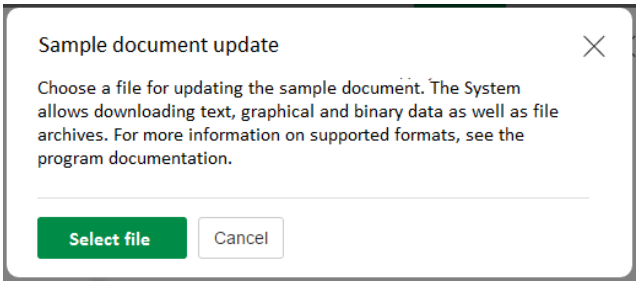
Sample document edit window

Attributes of the sample document:

Parameter	Description
Name	Sample document name
File name	The name of the file loaded as a sample document
File format	Type of the file: text, image, etc.
File size	The size of the file loaded as a sample document
Creation date	The date and time when the sample document was created
Modification date	The date and time of the last modification of the sample document. This attribute is displayed in the edit mode only.

Parameter	Description
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).This attribute is displayed in the edit mode only.
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.).This attribute is displayed in the edit mode only.
Description	Description in any form

Switching to the update mode of the sample document is performed with the **Update** button in the document edit window.



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

User's target actions:

- Creating Sample Documents and their Catalogs (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")

4.4.4 Blanks

Reference information:
Sample blank is a formsheet whose version (filled or not) is searched for in the network traffic. Sample 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 sample blanks may be surveys, questionnaires and other documents completed in a predefined form. Technically the sample 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.

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

Warning!

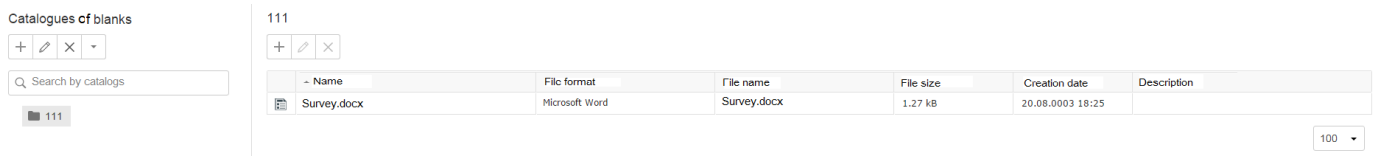
To match an interception object with the protected object which contains a sample blank, the following requirements must be met:

- the object text contains, at least, one field from the sample blank;

- if the number of fields detected in the object text is more than one, then fields should be in the same order as in the digital print uploaded to the System;
- if the **Detect only filled blanks** option is selected, then, at least, one character should be placed between the adjacent rows.

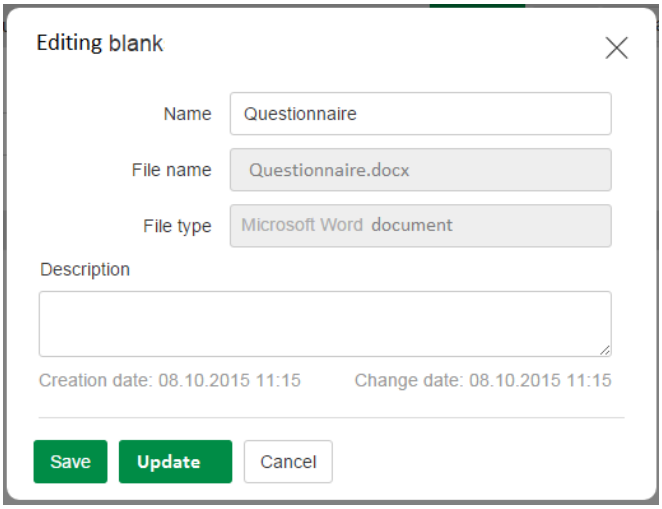
The principle of technology is: a search for names of the blank fields is performed, then their order is checked, then, if necessary, the presence of text between fields of the blank is checked. Based on these checks, the System defines whether the blank is filled out.

Sample blanks are created within catalogues. For operations with catalogs (creating, editing or deleting a catalog; search by catalogs), tools on the left side of the working area are used. Sample blanks of a selected catalog and tools for operations with sample blanks are located on the right side of the working area.



The list of sample blanks and their catalogues

Adding a file of the sample blank to a created catalogue is performed with the + toolbar button on the right side of the working area is used. Editing properties of the added sample blank is performed with the button. Clicking the button opens a window where you can view and change (if necessary) attributes of the selected blank.



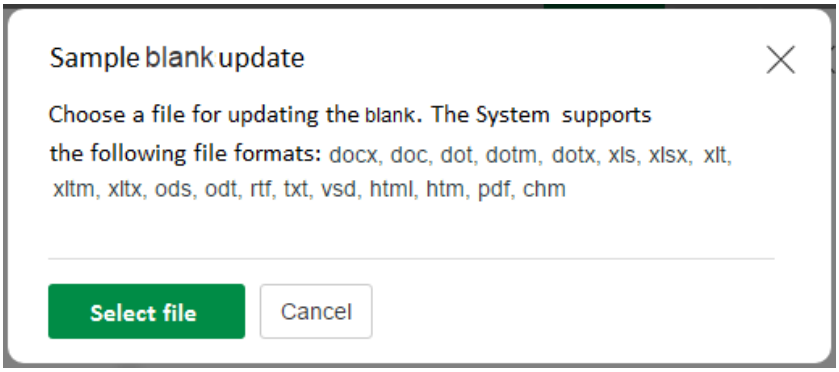
Sample blank edit window

Sample blank attributes:

Parameter	**Description**
Name	The name of the sample blank
File type	File format. The following formats are supported: DOCX, DOC, DOT, DOTM, DOTX, XLS, XLSX, XLT, XLTX, XLTM, ODS, ODT, RTF, TXT, HTM, HTML, VSD, PDF, CHM

Parameter	Description
File name	The format of the file that was loaded as a sample blank
Description	Description in any form
Creation date	The date and time of blank creation
Modification date	Date and time of the last modification of the blank. This attribute is displayed only when editing the blank.

Switching to the update mode of the sample blank is performed with the **Update** button in the blank edit window.



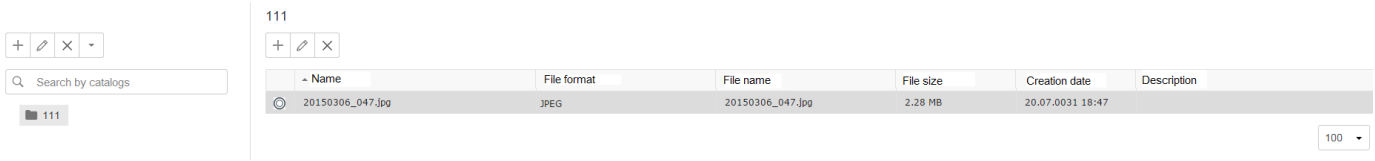
User's target actions:

- Creating sample 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 sample blank (see "Managing Blanks")
- Adding sample blanks to protected objects (see "Creating a Protected Object")

4.4.5 Stamps

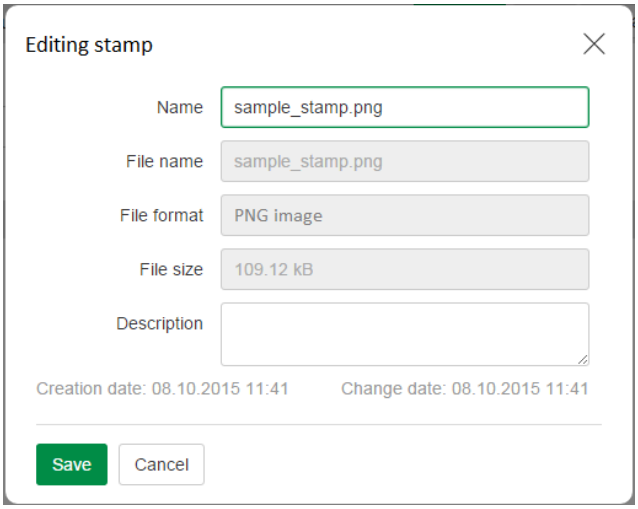
Reference information:
The *sample stamp* is a stamp image that is searched in the network traffic. Sample stamps can be images of round impressions used in organizations.

Sample stamps are created within catalogs. For operations with stamp catalogs (creating, editing or deleting a catalog; search by catalogs), tools on the left side of the working area are used. Sample stamps of a selected catalog and tools for operations with sample stamps are located on the right side of the working area.



Adding a file of the sample stamp to a created catalog is performed with the + toolbar button on the right side of the working area is used.Editing properties of the added sample stamp is performed with the

button. Clicking this button opens a window where you can view and if necessary change attributes of the selected stamp.



Sample stamp edit window

Sample stamp attributes:

Parameter	Description
Name	The name of the sample stamp
File format	The image format. The following formats are supported: BMP, DIB, JPEG, JPG, JPE, JP2, PNG, PBM, PGM, PPM, SR, RAS, TIF, TIFF.
File name	The name of the file that was loaded as a sample stamp
File size	The size of the file that was loaded as a sample stamp
Description	Description in any form
Creation date	The date and time when the sample stamp was created
Modification date	Date and time of the last modification of the sample stamp. This attribute is displayed in the edit mode only.

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

User's target actions:

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

4.4.6 Database Unloadings

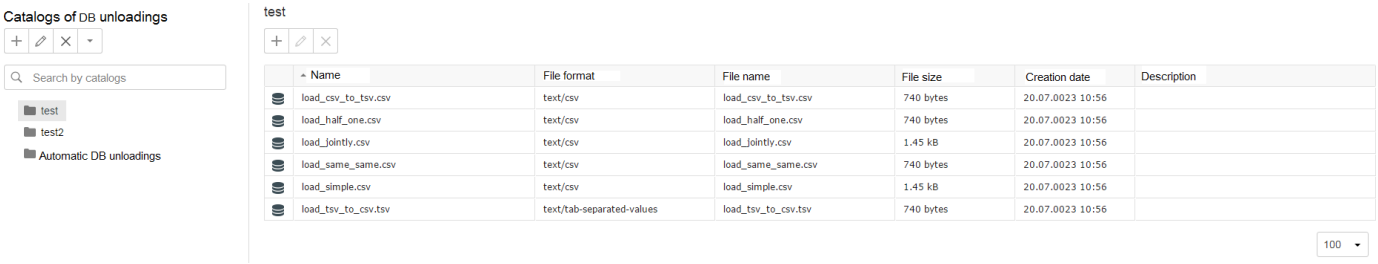
Reference information:
Sample database unloading is a part of database citations from which are searched for in analyzed text. Sample database unloadings can be lists of salaries, personal data, etc.

Warning!

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

- the number of columns is no more than 32;
- the number of words in one cells is no more than 256;
- the number of rows is no more than 1 million (for 8 GB RAM server) or no more than 3.5 millions (for 16 GB RAM server);
- unloading size maximum of 1 Gb in case Postgre SQL is used.

Sample unloadings are created within catalogs. For operations with unloading catalogs (creating, editing or deleting a catalog; search by catalogs), tools on the left side of the working area are used. Sample DB unloadings of a selected catalog and tools for operations with sample stamps are located on the right side of the working area.



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

Note:

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

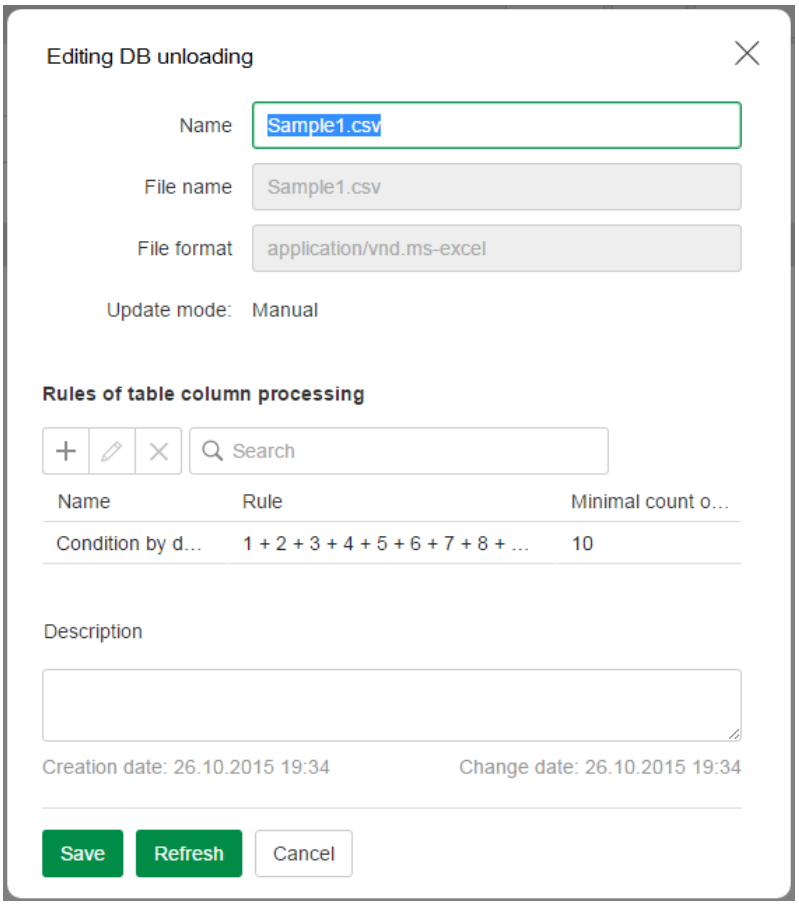
Adding a file of the sample unloading to a created catalog is performed with the + toolbar button on the right side of the working area is used.

A loaded file of a sample unloading 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.

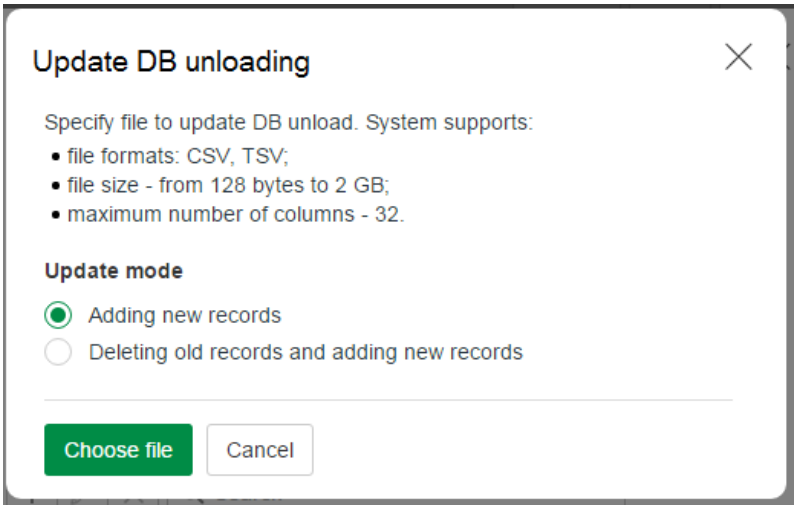
Editing properties of the added sample unloading is performed with the button on the toolbar on the right side of the workspace. In the window that opens, you can view and change (if necessary) the attributes of the selected sample unloading.



Attributes of sample database unloading:

Parameter	Description
Name	The name of the sample unloading
File name	The name of the file that was loaded as a sample database unloading
File format	Type of file
Update mode	Possible choices: **Manual** or **Automatic**
Description	Description in any form
Creation date	The date and time when the unloading was created
Modification date	Date and time of the last modification of the unloading. This attribute is displayed in the edit mode only.
Rules of processing table columns	Describes the logical correlation between table columns and the minimal number of non-blank rows in a table required for triggering the sample unloading.

Switching to the update mode of the sample unloading is performed with the **Update** button in the unloading edit window.



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

User's target actions:

- Creating sample database unloadings and their catalogs (see "Managing DB Unloadings")
- Updating the sample unloading (see "Managing DB Unloadings")
- Adding detection conditions for the unloading (see "Detection Conditions for Unloading")
- Automatic update of the sample unloading (see "Automatic creation and update of DB unloading ")
- Add sample DB unloadings to protected objects (see "Creating a Protected Object")

4.4.6.1 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.

Sample unloadings generated by an external system are placed in a preinstalled catalog **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** catalog provided that you have a license for using this technology.

Attributes of automatic unloading are generated based on the data received from an external system:

Parameter	Description
Name	The name of the unloading in the System
Update source	A system which is a source of file with unloading
Comment to the unloading	Accompanying information
Triggering condition	Detection of all filled columns. The minimum number of columns is`10` For example: If the number of columns is`3`, the condition will be as follows: `1+2+3`, and the minimum number of columns is `10`.

You can also add sample unloadings to the **Automatic DB unloadings** catalog manually using the



toolbar button on the right side of the working area is used. For manually added sample unloading, the update will be performed in a standard way (see "Managing DB Unloadings").

Note:

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

- 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.

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

Warning!

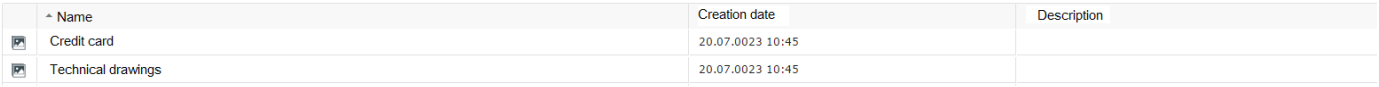
If a sample unloading created by an external system is deleted, automatic update of this unloading will become unavailable.

For automatic sample unloading to be detected in intercepted data, it must be included in protected objects.

4.4.7 Graphical Objects

Reference information:

The ***graphical object*** is an image extracted from the object body or its enclosures. The presence of certain features in the image makes it possible to attribute it to a particular class of preset graphical objects. Graphical objects are used when creating protected objects.



Graphical object attributes:

Parameter	Description
Name	Name of the graphic object
Creation date	Date and time of object creation
Description	Description of a graphical object

The System may contain the following graphical objects (the set of graphical objects depends on the license type):

Name	Description
Credit card	Front side image of a VISA, Visa Electron, MasterCard, or Maestro credit card. Is included in the **Personal data** preset protected object (or in the **Credit card information** preset protected object for the Malaysian version).
Topographic maps	A topographic map or its part
Technical drawings	Technical drawings in a form of black lines against a white background
Identification card of a citizen of Malaysia	Is available for the Malaysian version only. 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) Is included in the **Personal ID** preinstalled protected object.

Only preinstalled graphical objects with preset attributes are used in the System. Adding, editing or deleting graphical objects is not available.

For graphic objects to be detected in intercepted data, they must be included in protected objects.

User's target actions:

- creating a protected object based on graphical objects (see "Creating a Protected Object").

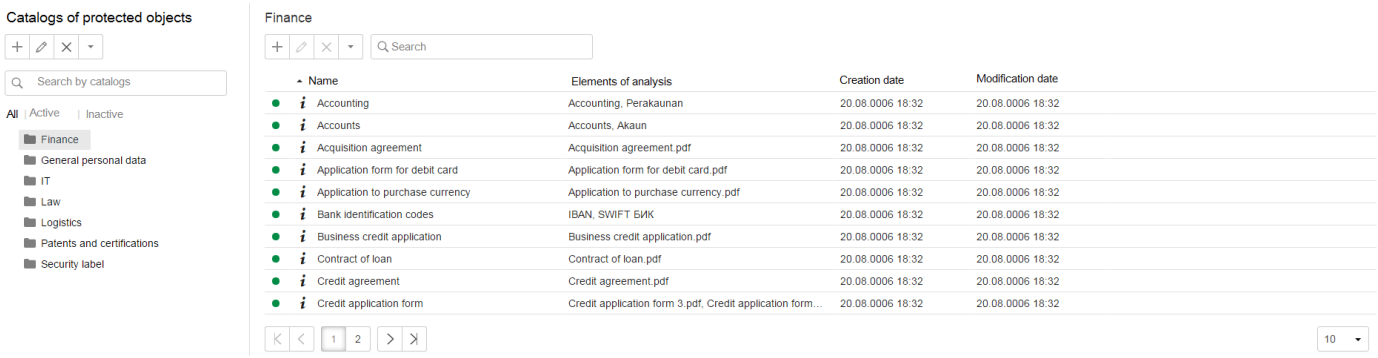
4.5 Protected Objects Section

Reference information:

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

About the section:

The section contains a list of protected objects and tools for managing them.



The section contains the following elements:

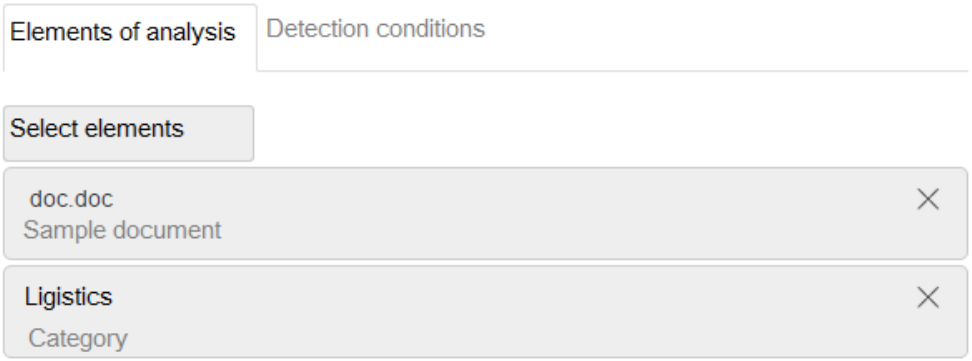
Element	Purpose
Catalogs of protected objects	The list of added catalogs that contain protected objects. Is located in the left part of the workspace.
Protected objects	The list of protected objects contained in the selected catalog. Appears when you select a catalog
Toolbar	Tools for protected objects and their catalogs
Search field	Filtering of protected objects
Page navigation panel	A set of buttons for browsing pages with entries (if not all entries can be placed on one page). You can go to the next or previous page, move to the beginning or end of the list or go to the page with the selected number.
Control of the entries number	The drop-down list where you can set the number of entries per page

The list of catalogs contains preinstalled catalogs of protected objects. For preinstalled protected objects, the elements of analysis and the detection conditions are specified.

The System contains preinstalled protected objects, the list of which may vary depending on the delivery.

4.5.1 Elements of Analysis

Reference information:
Elements of analysis are the elements of configuring technologies based on which the protected objects are created (for example, text objects, sample documents, etc.).



Protected objects section, **Elements of analysis** tab when creating or editing a protected object

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

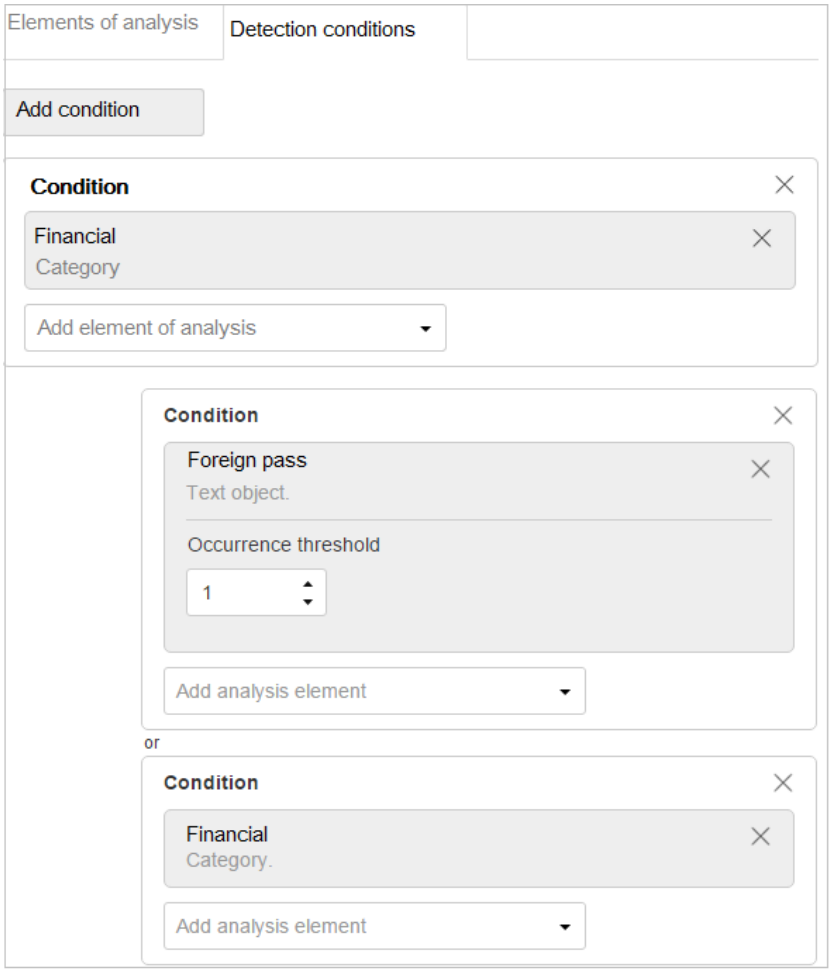
On the **Elements of analysis** tab, you can add more elements of analysis to a protected object (the **Select elements** button) or delete elements of analysis (the X button in the upper right corner of the element panel).

Detecting conditions for added elements of analysis are specified on the **Detection conditions** tab.

User's target actions:

- Adding elements of analysis

4.5.2 Detection Conditions



The **Detection Conditions** tab which 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 analysis or when switching to 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).

Detection conditions of the elements of analysis:

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.

Element name	Detection condition
Text object	Checks whether the interception object contains a specified text object. Additional detection conditions is a quantity threshold. It determines the least number of times the text object must be present in the interception object. The default value is 3. 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.
Blank	Checks whether the interception object contains at least one of the specified sample blanks. Additional detection conditions: • search through filled and unfilled blanks. If you want all blanks to be detected, select the **Filled and unfilled** checkbox. By default only filled blanks are detected; • a minimum number of matching entries. The default value is 3.
Stamp	Checks whether the interception object contains a specified sample stamp
Graphical object	Checks whether the interception object contains a specified graphical object
Database unloading	Checks whether the interception object contains a specified sample unloading.You must select one of the representations of unloading

See also: Elements of analysis

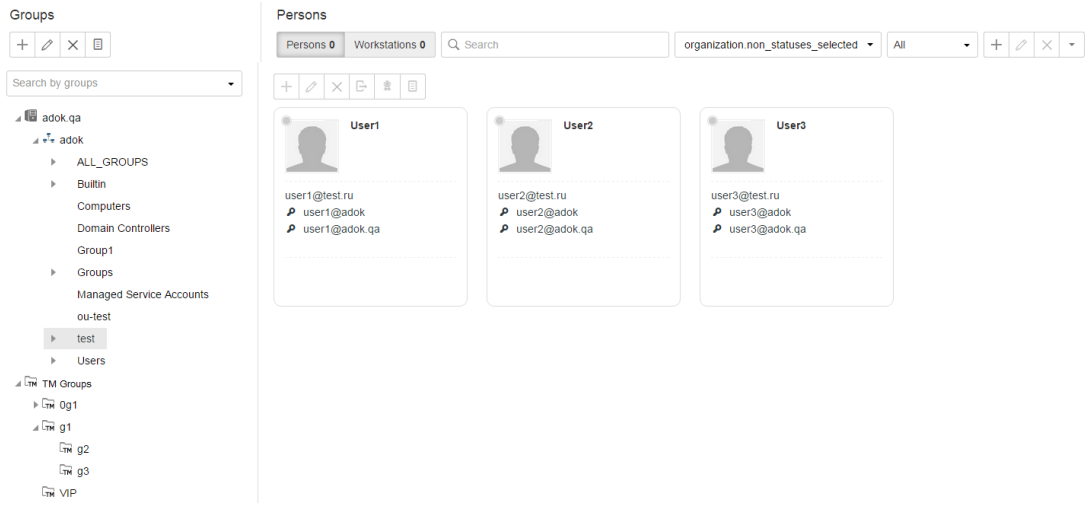
User's target actions:

- Adding detection conditions

4.6 Persons Section

Reference information:
Lists of users and workstations make it easier for the security officer to work with intercepted objects. This is due to the accounting of information about senders, recipients (persons) and workstations using special catalogs.

About the section:
The section contains a catalog of persons and workstations of the company information system.



Persons section

Warning!

If the number of persons whose events are processed exceeds the number of persons supported by the current license, the following message is displayed at the top of the browser window: **Attention! The threshold on the number of persons processed by the System is exceeded by 1.**

This is an informational message and it does not affect the functionality of the System.
The number of persons whose events are processed in the System is equal to the number of employees who sent any type of traffic over the last 30 days.
The number of employees allowed by the current license is displayed in the license information, **Licensed users** attribute (for details see the document "*Infowatch Traffic Monitor. Administration Guide*").

The section contains the following elements:

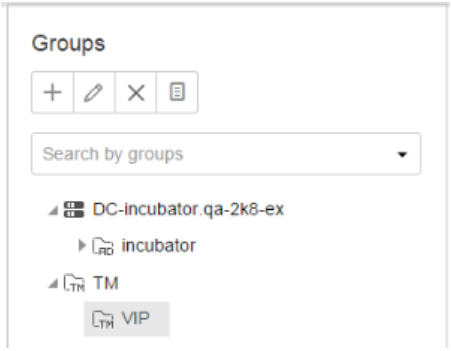
Element	Purpose
Groups of persons/workstations from Active Directory	Located in the left part of the workspace. Contains the structure of the organization from Active Directory.
Groups of persons/workstations from Domino Directory	Located in the left part of the workspace. Contains the structure of the organization from Domino Directory.
Groups of persons/workstations created by means of Traffic Monitor	Located in the left part of the workspace. Contains the structure of the organization created by means of Traffic Monitor.
Persons tab for the selected group	Located in the right part of the workspace. Contains a list of persons included in the selected group.
Workstations tab for the selected group	Located in the right part of the workspace. Contains a list of workstations included in the selected group.
Toolbars	Set of tools for groups, persons, and workstations

Element	Purpose
Search by groups field	Filtering groups of persons and workstations
Search field	Filtering persons and workstations
Filter by statuses field	Filtering persons and workstations by **Status** attribute

User's target actions:

- Creating a group of persons and workstations (see "Creating a Group of Persons and Workstations")
- Creating a list of persons and workstations (see "Creating a List of Persons and Workstations")
- Viewing widgets with information on persons and workstations (see "Viewing a Summary on Person or Workstation")
- Creating a filter by persons and workstations (see "Viewing a Summary on Person or Workstation")
- Creating a policy for persons and workstations (see "Adding a Person or Workstation to the Policy")
- Managing statuses of persons and workstations (see "Adding a Status to Person or Workstation")
- Adding persons and workstations in perimeters (see "Adding a Person or Workstation to the Company Perimeter")

4.6.1 Group of Persons and Workstations



Note:

Groups synchronized with Active Directory are marked with .

Attributes of groups of persons and workstations:

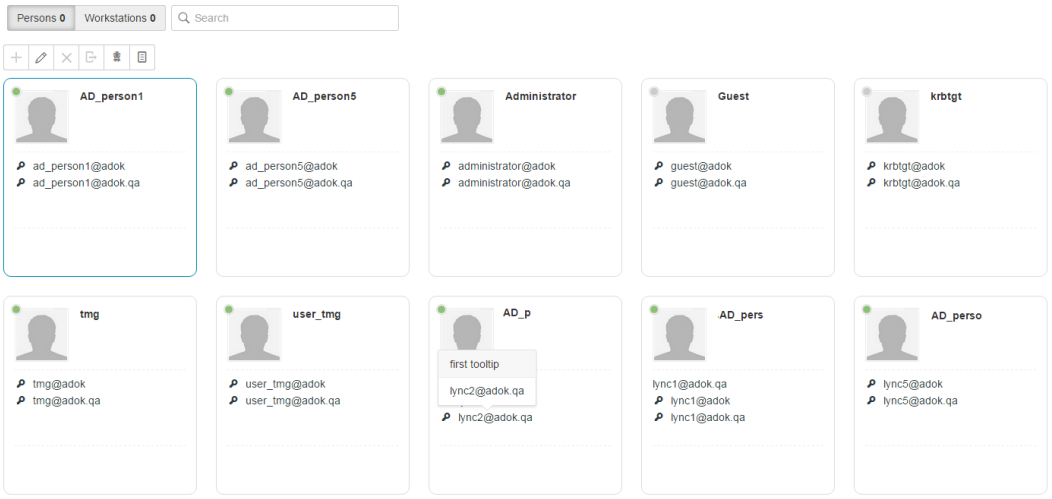
Parameter	Description
Name	Group name
Contacts	Group contact information
Contains groups	List of groups included in this group
Included in groups	List of groups this group is included in

Parameter	Description
Note	Description in any form

User's target actions:

- Creating a Group of Persons and Workstations

4.6.2 Persons



Note:

For persons whose data is imported from Active Directory, the color indicator appears in the upper left corner of the profile photo:
- for active employees;
- for employees disabled in AD.

Person's attributes:

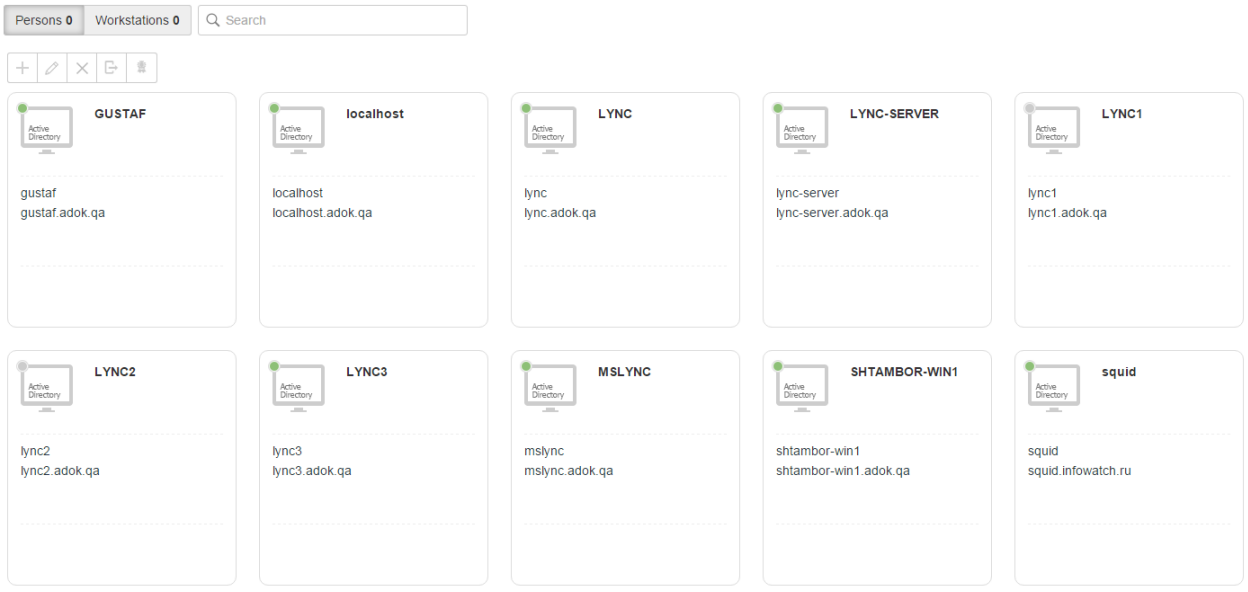
Parameter	Description
Last name	The last name of the person
Name	The first name of the person
Employee/Not employee	Indication whether a person is an employee of the company
Job position	The position of the person
Department	The department in which the person works
Room	The room in which the person works
Manager	The person's manager

Parameter	Description
Note	Optional description
Contacts	Person's contact information: security officer can specify home or business contacts, including e-mail address, phone number, Skype login, ICQ or Internet site address)
Groups	The groups the person is included in
Workstations	Workstations assigned to the person
Statuses	Status assigned to the person by the security officer
Photo	Picture of the person

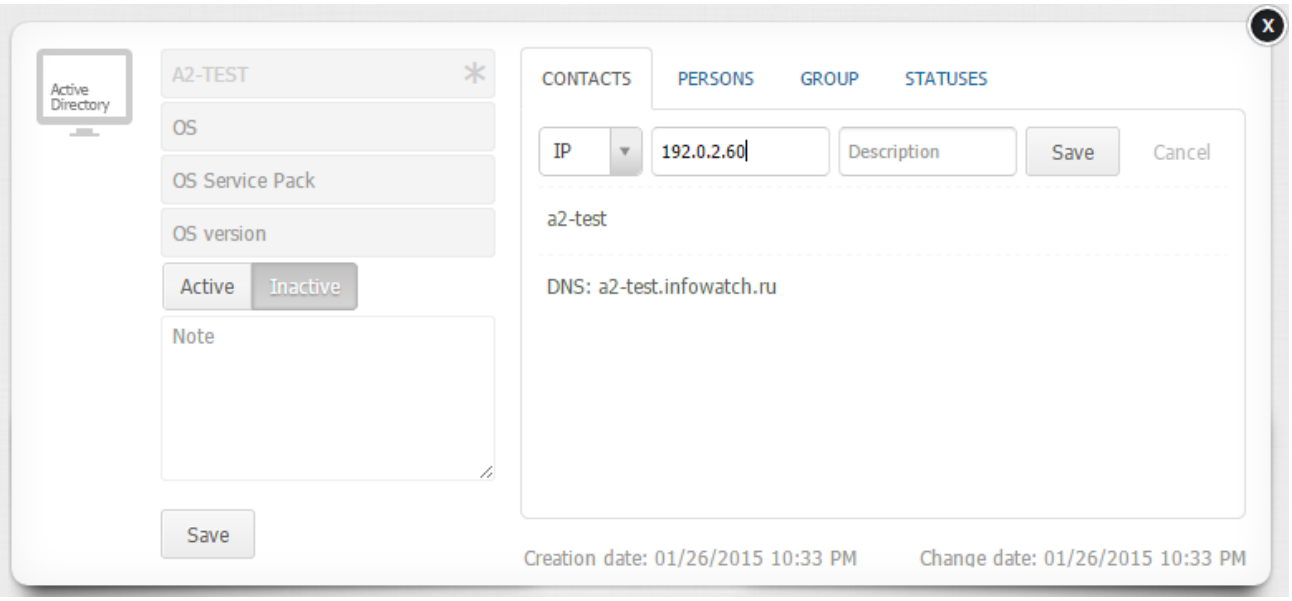
User's target actions:

- Working with groups of persons (see "Creating a Group of Persons and Workstations")
- Viewing widgets with information on persons and workstations (see "Viewing a Summary on Person or Workstation")
- Creating a filter by persons (see "Viewing a Summary on Person or Workstation")
- Configuring the Card of a Person (see "Configuring Person's Card")
- Creating a policy for persons (see "Adding a Person or Workstation to the Policy")
- Managing statuses of the person (see "Adding a Status to Person or Workstation")
- Added the person to a perimeter (see "Adding a Person or Workstation to the Company Perimeter")

4.6.3 Workstations



Example of a list of workstations



Example a workstation edit dialog

Workstation attributes:

Parameter	Description
Name	Name of workstation
Note	Optional description
Contacts	Workstations identifier in the network: • IP • DNS In the first of the two fields, you should specify IP or DNS name (depending on the selected option). In the second field, add a comment if necessary.
Persons	Employees to whose accounts the workstation is linked
Groups	Groups the workstation is included in
Status	Status the security officer assigns to the workstation

User's target actions:

- Managing groups of workstations (see "Creating a Group of Persons and Workstations")
- Managing workstations (see "Creating a List of Persons and Workstations")
- Viewing widgets with information on workstations (see "Viewing a Summary on Person or Workstation")
- Creating a filter by workstations (see "Viewing a Summary on Person or Workstation")
- Creating a policy for workstations (see "Adding a Person or Workstation to the Policy")
- Managing statuses workstations (see "Adding a Status to Person or Workstation")

- Defining workstations included in perimeters (see "Adding a Person or Workstation to the Company Perimeter")

4.7 Policies Section

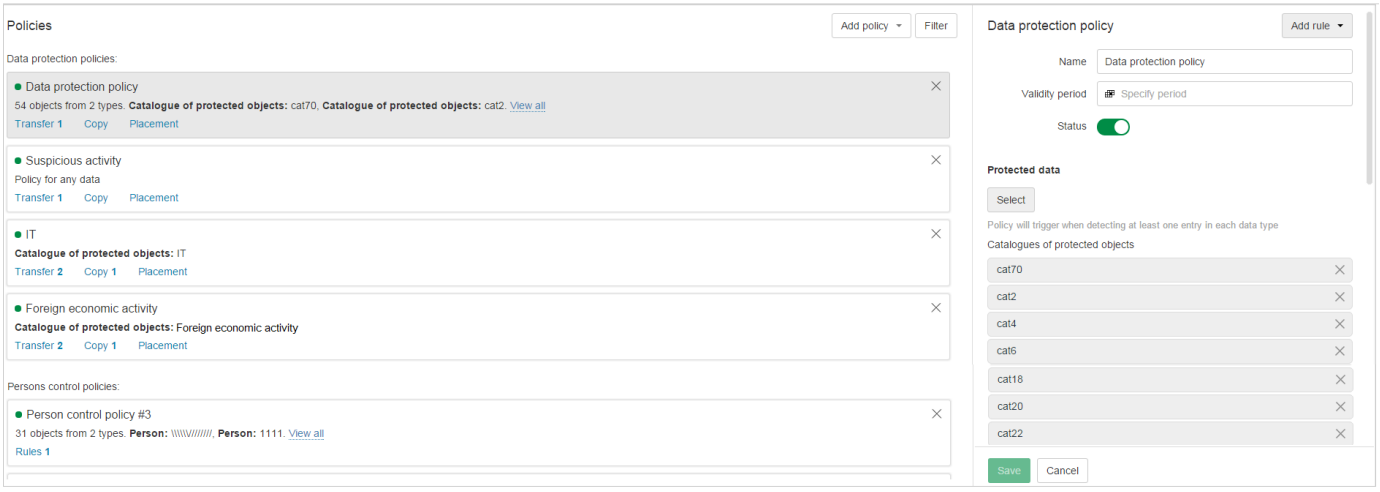
Reference information:
Policies are a set of rules according to which analysis and processing of interception objects is performed. The ***rule*** consists of condition sets by which the object is checked and the actions performed when those conditions are fulfilled or not.

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 actions performed by the System in response to actions of persons and workstations.



The section contains the following elements:

Element	Purpose
List of policies	Contains available policies. Policies in the list are divided into two groups: data protection policies and person control policies.

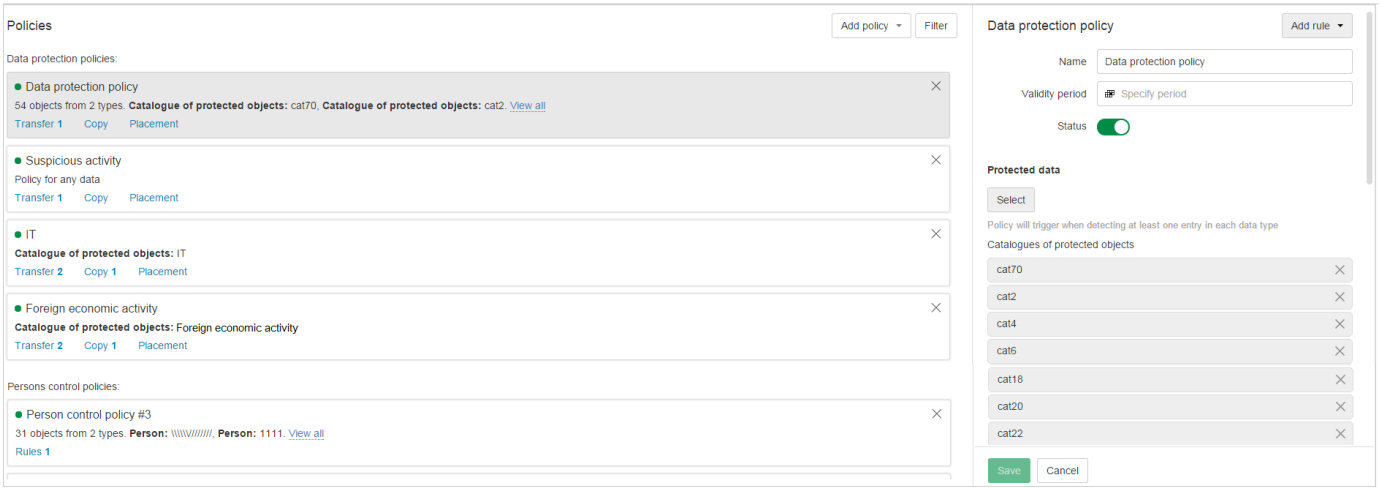
Element	Purpose
Policy viewing form	Contains the attributes of the selected policy
Rule viewing form	Allows configuring a rule for the selected policy
Filter button	Displays the **Filter settings** area
Filter settings area	Allows filtering policies by specified attributes
Add policy button 	Allows you to select the type of policy from the drop-down list. Possible values: • Data Protection Policy • Person Control Policy For the added policy, a viewing form is displayed in the right part of the workspace
Policy viewing form	Allows you to specify parameters of the created policy

User's target actions:

- Adding a new policy (see "Creating Data Protection Policy" and "Creating Person Control Policy")
- Modifying a previously created policy (see "Editing Policy")
- Adding rules to the policy (see "Creating a Rule")
- Modifying previously created rules (see "Editing Rules")
- Filtering policies (see "Filtering the List of Policies")

4.7.1 Policies and their Viewing Form

Policy viewing form is displayed in the right part of the workspace when you select a policy in the list.



Policy attributes:

Parameter	Description
Name	Policy name

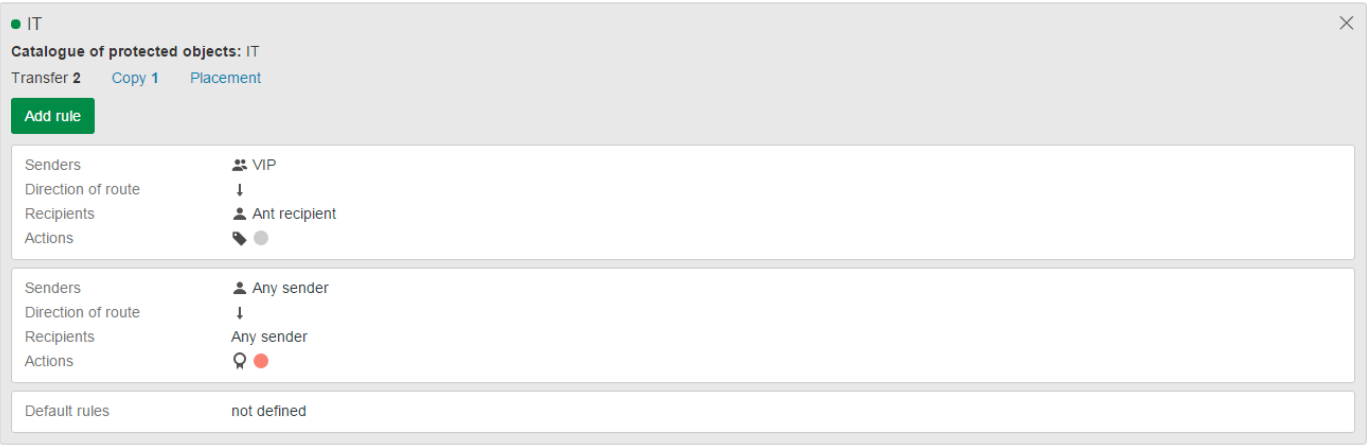
Parameter	Description
Status	Indicates whether the policy is enabled in the System
Period of activity	The time period when the policy applies
Protected data (only for data protection policies)	The list of protected objects, their catalogs and file formats controlled by the policy
Controlled persons (only for a person control policies)	The list of persons, whose actions are controlled by the policy
Policy rules	The list of actions performed by the System when the policy is triggered
Description	Description of the policy. An optional parameter.

User's target actions:

- Adding a new policy (see "Creating Data Protection Policy" and "Creating Person Control Policy")
- Modifying a previously created policy (see "Editing Policy")

4.7.2 Rules and their Viewing Form

Information on the rules is displayed in the tile of a policy for which they are defined. Clicking on the link with the type of rules in a policy tile opens the list of added rules of this type.



When you select a rule in the list on the right side of the workspace displays a form view of the selected rule.

Also in the upper-right corner of a tile there is ✕ icon, by clicking on that you can remove the selected rule.

There are three categories of rules for a **data protection policy**:

The rule	Description
Transfer rule	The rule that regulates sending and receiving protected data
Copy rule	The rule that regulates copying, printing and photographing protected data

The rule	Description
Placement rule	The rule that regulates storing protected data

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 options:

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 ".", ",", "-", "_"; - 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); - 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 at the Web resource. 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 controlled persons. They also allow you to apply existing data protection policies to selected persons.

User's target actions:

- Adding rules to the policy (see "Creating a Rule")
- Modifying previously created rules (see "Editing Rules")

4.7.2.1 Rule of Transfer

Attributes of the rule of transfer

Parameter	Description
Route direction	There may be two types of directions: → 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 that triggers the rule provided that other conditions are satisfied. Possible choices: • Web-message • Email • Webmail • ICQ • XMPP • Mail.ru Agent • Jabber • Skype • MS Lync • Yahoo! • WhatsApp • SMS • Photography
Days of rule activity	The list of days of the week on which the rule can be triggered
Hours of rule activity	The time interval during the day when the rule can be triggered
Computers	Workstations of the sender
Senders	If persons and workstations from this list copy traffic, it will (provided that other conditions are satisfied) = - trigger the rule ≠ - do not trigger the rule

Parameter	Description
Recipients	If persons and workstations from this list receive traffic, it will (provided that other conditions are satisfied) - trigger the rule - do not trigger the rule **Note:** If you select a protected object based on a graphical object as policy protected data and specify the **Webmail** 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.
Send notification	List of user of the Console who will be notified when the rule is triggered **Note:** If after the rule is created, the user or his e-mail are deleted from the System (on managing user accounts, see *"Administration Guide"*, "Users" section), a notification will not be sent to this user.
Notify senders	Enable this setting if you want to send notifications to traffic senders when the rule is triggered. By default, this setting is disabled.
Assign verdict	A verdict which will be assigned to the object when the rule is triggered. Possible values: *Allow*, *Block*, *Quarantine*.
Assign violation level	A violation level that will be assigned to the object when the rule is triggered. Possible values: *High*, *Medium*, *Low*, *No violation*.
Assign tags	The list of tags which will be assigned to the object when the rule is triggered (see "Tags")
Assign status	A status that will be assigned to senders when the rule is triggered (see "Statuses")
Delete event	If this option is selected, then the event will not be saved to the database and the actions specified in the rule will not be performed. By default, this setting is disabled.

User's target actions:

- Adding rules to the policy (see "Creating Rule")
- Modifying previously created rules (see "Editing Rules")
- Adding actions to the policy (see "Determining the System Response to Rule Violations")

4.7.2.2 Rule of Copying

Attributes of the rule of copying:

Parameter	Description
Event type	The type of traffic copying which triggers the rule provided that other conditions are met Possible choices: • Copying to an external device • FTP • Stamp • Photography
Days of rule activity	The list of days of the week on which the rule can be triggered
Hours of rule activity	The time interval during the day when the rule can be triggered
Workstations	The list of workstations copying the traffic who (provided that other conditions are met) trigger the rule
Senders	The list of persons and workstations copying the traffic who (provided that other conditions are met) - trigger the rule  - do not trigger the rule
Send notification	List of user of the Console who will be notified when the rule is triggered **Note:** If after the rule is created, the user or his e-mail are deleted from the System (on managing user accounts, see *"Administration Guide"*, section "Users"), a notification will not be sent to this user.
Assign violation level	The violation level which will be assigned to the object when the rule is triggered. Possible values: *High*, *Medium*, *Low*, *No violation*.
Assign tags	The list of tags which will be assigned to the object when the rule is triggered (see "Tags")
Assign status	The status which will be assigned to senders when the rule is triggered (see "Statuses")
Delete event	If this option is selected, then the event will not be saved to the database and actions specified in the rule will not be performed. By default, this setting is disabled.

User's target actions:

- Adding rules to the policy (see "Creating Rules")
- Modifying previously created rules (see "Editing Rules")
- Adding actions to the policy (see "Determining System Response to Policy Violations")

4.7.2.3 Rule of Placement

Attributes of the rule of placement

Parameter	Description

Parameter	Description
Event type	The type of traffic the placement of which triggers the rule provided that other conditions are met. Possible choices: • Crawler
Storage	Storing secured data in these storages will: = - trigger the rule ≠ - do not trigger the rule **Note:** When adding a network resource, use the following format: `//<workstation>/<directory>` where • `<workstation>` is a workstation name; • `<directory>` is a target folder on the workstation. When you add a file storage, enter the following values: • in the **Enter a source** field, enter address of the SharePoint database server; • in the **Enter a path to storage** field, enter the name of SharePoint database instance.
File owners	The rule is triggered when specified persons, groups or elements of perimeters are detected among file owners. If the attribute is denied, the rule is triggered when persons, groups or elements of perimeters not included in the list are detected among file owners.
Who has access to file	The rule is triggered if specified persons, groups and elements of perimeters have access to the file. If the attribute is denied, the rule is triggered when persons, groups or elements of perimeters not included in the list have access to the file.
Send notification	List of the Console users who will be notified when the rule is triggered **Note:** If after the rule is created, the user or his e-mail are deleted from the System (on managing user accounts, see *"Administration Guide"*, section "Users"), a notification will not be sent to this user.
Assign violation level	A violation level which will be assigned to the object when the rule is triggered. Possible values: *High*, *Medium*, *Low*, *No violation*.
Assign tags	The list of tags which will be assigned to object when the rule is triggered (see "Tags")
Assign status	A status which will be assigned to senders when the rule is triggered (see "Statuses")
Delete event	If this option is selected, then the event will not be saved to the database and actions specified in the rule will not be performed. By default, this setting is disabled.

User's target actions:

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

- Modifying previously created rules (see "Editing Rules")
- Adding actions to the policy (see "Determining the System Response to Rule Violations")

4.7.2.4 Person Control Rule

Attributes of the person control rule:

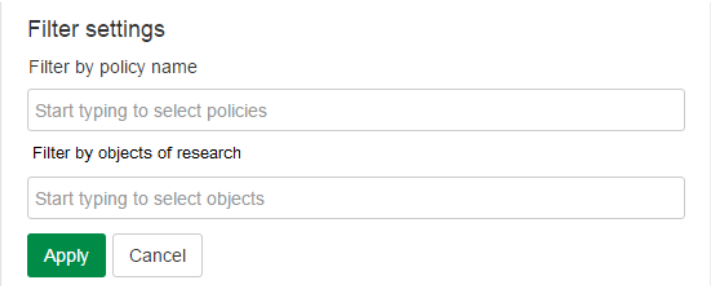
Parameter	Description
Intercept with violation level	Events with a specified violation level will be intercepted
Connect with policy	Data protection policies which trigger the rule when the policy itself is triggered (assuming that the violation level matches the value specified in the **Intercept with violation level** field)
Send notification	List of the Console users who will be notified when the rule is triggered **Note:** If after the rule is created, the user or user e-mail are deleted from the System (on managing user accounts, see *"Administration Guide"*, "Users" section), a notification will not be sent to this user.
Notify senders	In case the rule is triggered, the traffic sender will be notified
Assign verdict	A verdict which will be assigned to the object when the rule is triggered. Possible values: *Allow*, *Block*, *Quarantine*.
Assign violation level	A violation level which will be assigned to the object when the rule is triggered. Possible values: *High*, *Medium*, *Low*, *No violation*.
Assign tags	The list of tags which will be assigned to the object when the rule is triggered (see "Tags")
Delete event	If this option is selected, then the event will not be saved to the database and actions specified in the rule will not be performed. By default, this setting is disabled.

User's target actions:

- Adding rules to the policy (see "Creating Rules")
- Modifying previously created rules (see "Editing Rules")
- Adding actions to the policy (see "Determining the System Response to Rule Violations")

4.7.3 Filter Settings area

The area is displayed when clicking the **Filter** button in the **Policies** section.



Filter attributes:

Parameter	Description
Filter by policy name	Filtering is based on specified policies
Filter by objects	Filtering is based on specified secured data

User's target actions:

- Filtering policies (see "Filtering the List of Policies")

4.7.4 Form of adding policy

Policy attributes are described in "Policies and their Viewing Form". When you create a new policy, you can specify protected data (for a data protection policy) and controlled persons (for a person control policy).

The appearance of the form for adding policy differs depending on the selected type:

Policy type	Description of the form for adding a policy
Data Protection Policy	When selected, a new policy is added to the list of data protection policies, and, in the right side of the workspace, a policy viewing form is displayed. Clicking the **Select** button opens a dialog box where you can specify secured data which are included in one of the following categories: • Catalog of protected objects • Protected objects • File format
Person Control Policy	When selected, a dialog box appears where you can specify senders whose actions are controlled by this policy. You can select individual persons, groups of persons, or persons with a particular status.

User's target actions:

- Adding a new policy (see "Creating Data Protection Policy" and "Creating Person Control Policy")

4.8 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 catalogs of tags, statuses, perimeters and 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, **Statuses** tab

The section contains the following elements:

Element	Purpose
Tabs of different types of catalogs • Tags • List of resources • Statuses • Perimeters • List of files	Contain the lists of elements and tools for a selected catalog
List of elements or their groups for the selected catalog	Opens when you select a catalog. Contains a list of catalog elements or a group of lists with catalog elements
Page navigation panel	The set of buttons for browsing pages with entries (if not all entries can be placed on one page)
Toolbar	A set of tools for catalogs

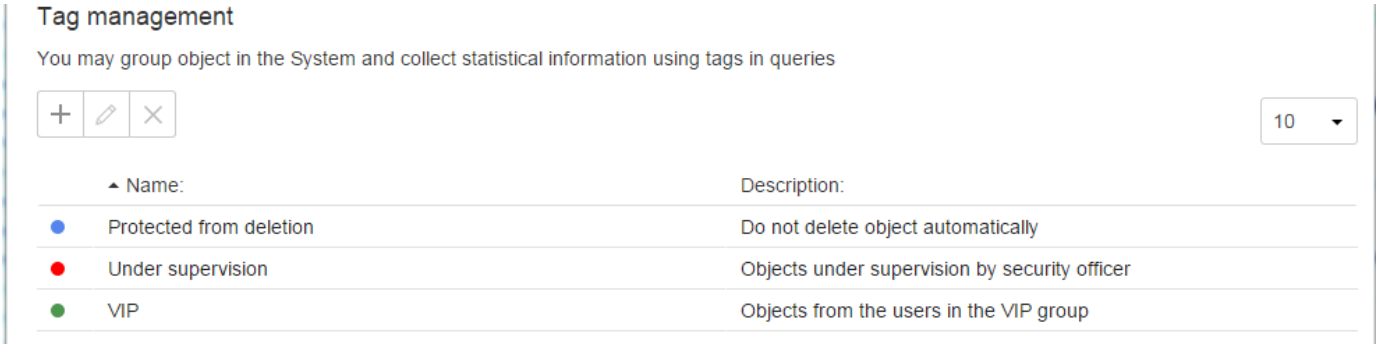
User's target actions:

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

4.8.1 Tags

Reference information:

Tag is a mark which gives a brief characteristic of the intercepted object.



Tag attributes:

Parameter	Description
Color	Color marker which is added together with the tag
Name	Tag name
Description	Optional note

There are the following preset tags in the System:

- **Protection from deletion** - Events that are not removed during the process of releasing space in the database

> **Note:**
>
> This tag is only available for Traffic Monitor Standard based on Oracle Standard (for more information, see "*Infowatch Traffic Monitor. Administration Guide*")

- **Under supervision** - Events that indicate employees' suspicious activity

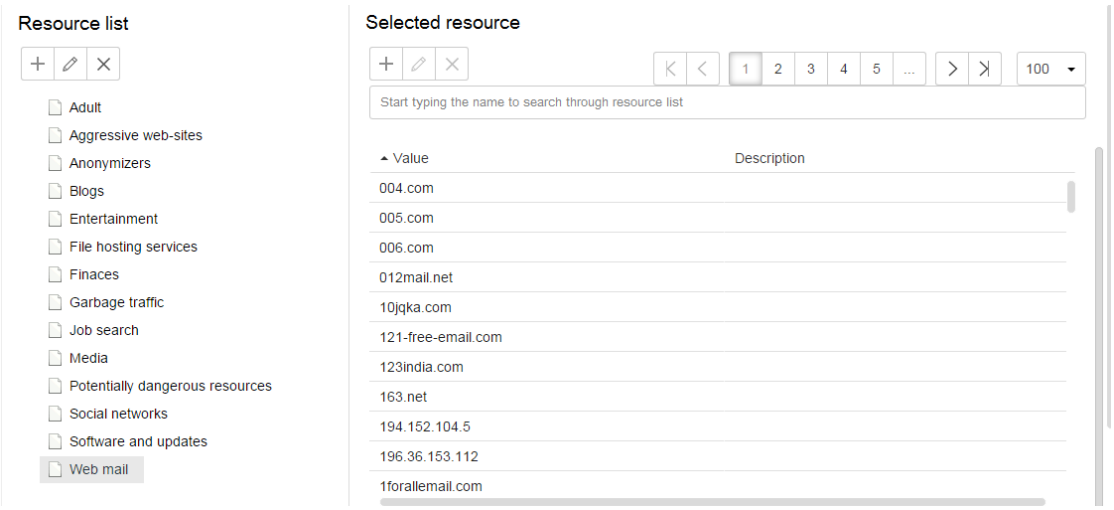
- **VIP** - Events from persons who belong to the VIP group

User's target actions:

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

4.8.2 List of Resources

Reference information:
The ***list of resources*** is a set of Internet resources, which are detected by the System as inappropriate use of working time.



Resources are organized into lists according to their subject.

Resource attributes:

Parameter	Description
Value	The resource name on the Internet
Description	Optional note

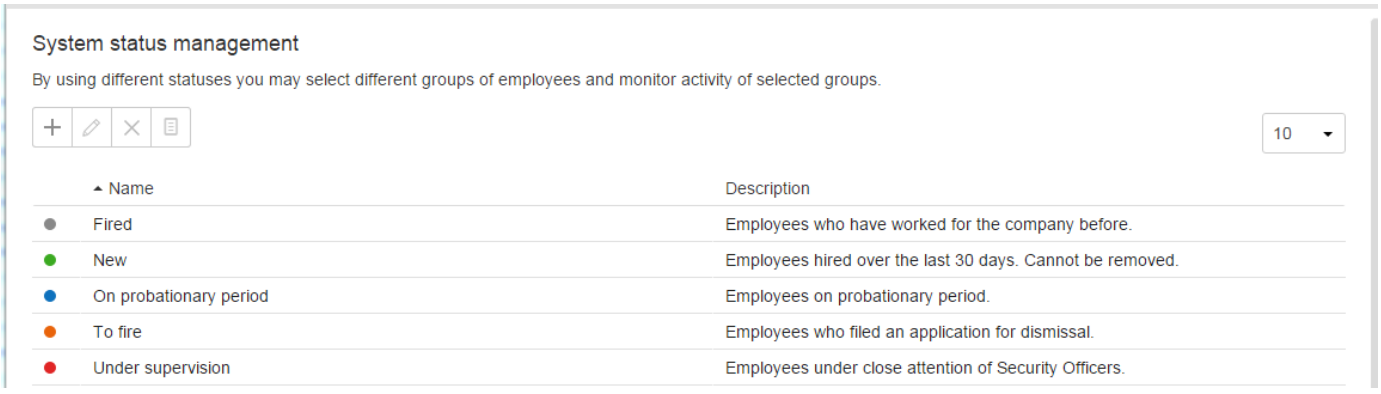
User's target actions:

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

4.8.3 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 workstation imported from Active Directory, or
- manually assigned to a person by Security officer, or
- automatically assigned to a sender as a result of rule triggering.



The statuses *On probationary period*, *To fire*, *New*, *Under supervision*, and *Fired* are preset in the System.

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

Attributes of the person status:

Parameter	Description
Color	Color mark added together with the status
Name	Status name
Description	Status description. Optional parameter

User's target actions:

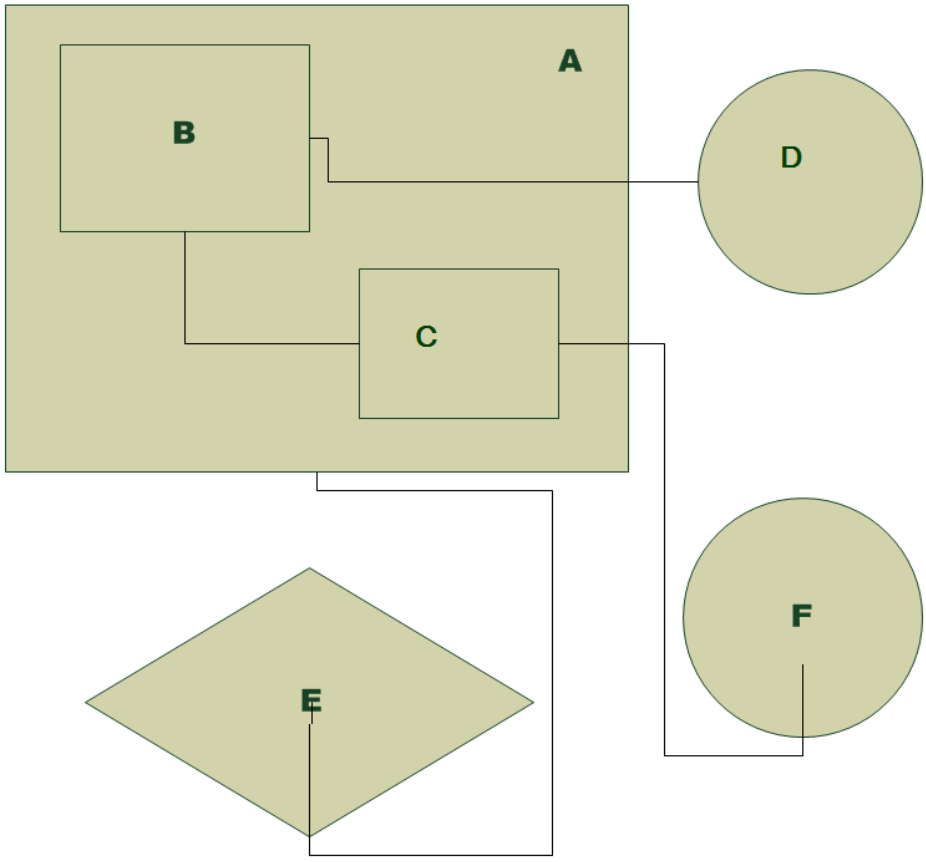
- Creating a list of statuses (see "Managing statuses")
- Manual assigning status to a person or workstation to monitor its activities or to visually distinguish them (see "Adding a Status to Person or Workstation")
- Automatic assigning status to a sender when the rule is triggered (see "Rules and their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

4.8.4 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.

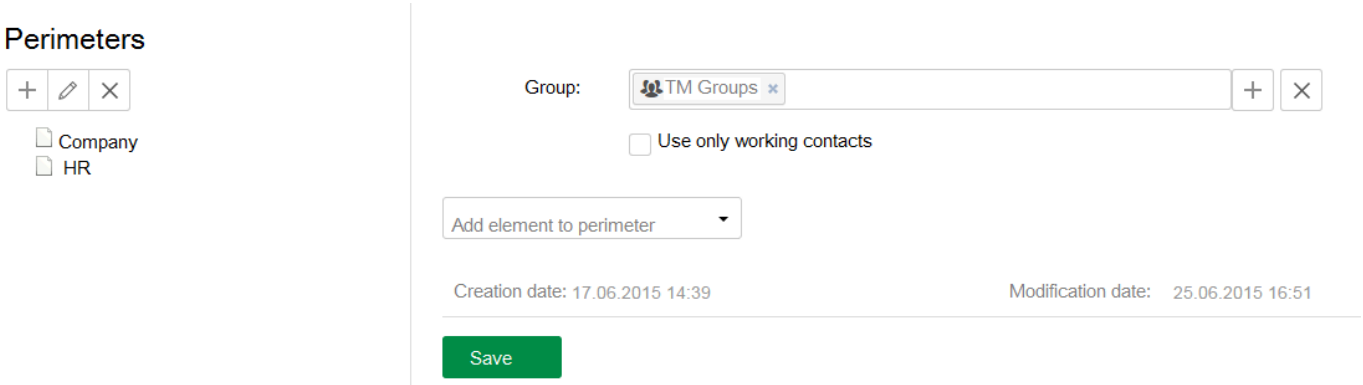


By building perimeters for all named objects (A, B, C, D, E, F), the security officer can configure traffic control:

- 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).



Perimeter attributes:

Parameter	Description
Name	The name of the perimeter
The list of elements	Elements within the perimeter **Warning!** When adding persons or groups to the perimeter, the **Use only work contacts** option is available. Example of using: if the option is selected, sending messages from the employee's personal mailbox will not be treated as sending data outside the perimeter.
Creation date	The date and time the perimeter was created
Modification date	Date and time of the last modification of the perimeter

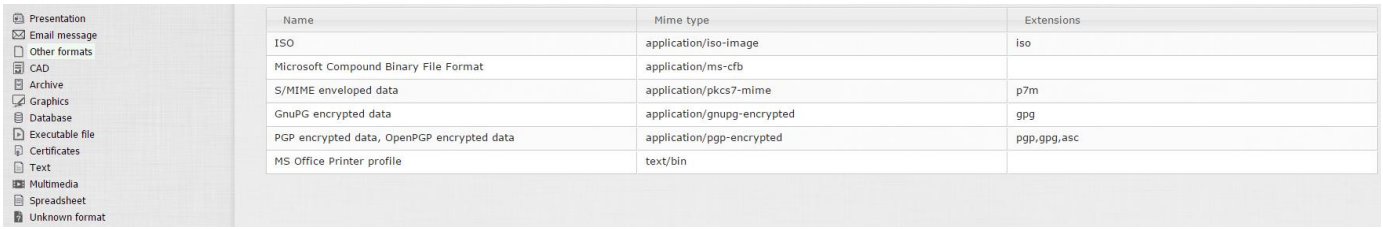
User's target actions:

- Building perimeters (see "Managing perimeters")

4.8.5 List of Files

Reference information:

List of files is a set of files which are detected by 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 the file types	Located in the left part of the workspace. Contains a set of subjects that use one or more of the files formats.
List of file formats of the selected type	Located in the right part of the workspace. Contains attribute list for all files of this type, which are detected in the System.This is a table that contains a description of the **Name**, **MIME type** and **Extension**.
Create policy button	Creates a data protection policy where the secured data is the selected file format or file type **Note:** Clicking the button opens a window for adding a new policy in the **Policies** section.

Warning!

File lists are strictly defined by the System and cannot be modified.

User's target actions:

- Working with policies (see "Creating policy")

4.9 Crawler Section

Reference information:
The Crawler subsystem of InfoWatch Traffic Monitor system allows you to check files in the corporate network for violations of the corporate security policies. Therefore InfoWatch Crawler allows to monitor file resources to detect and prevent unauthorized usage of confidential data.

InfoWatch Crawler provides the following functions:

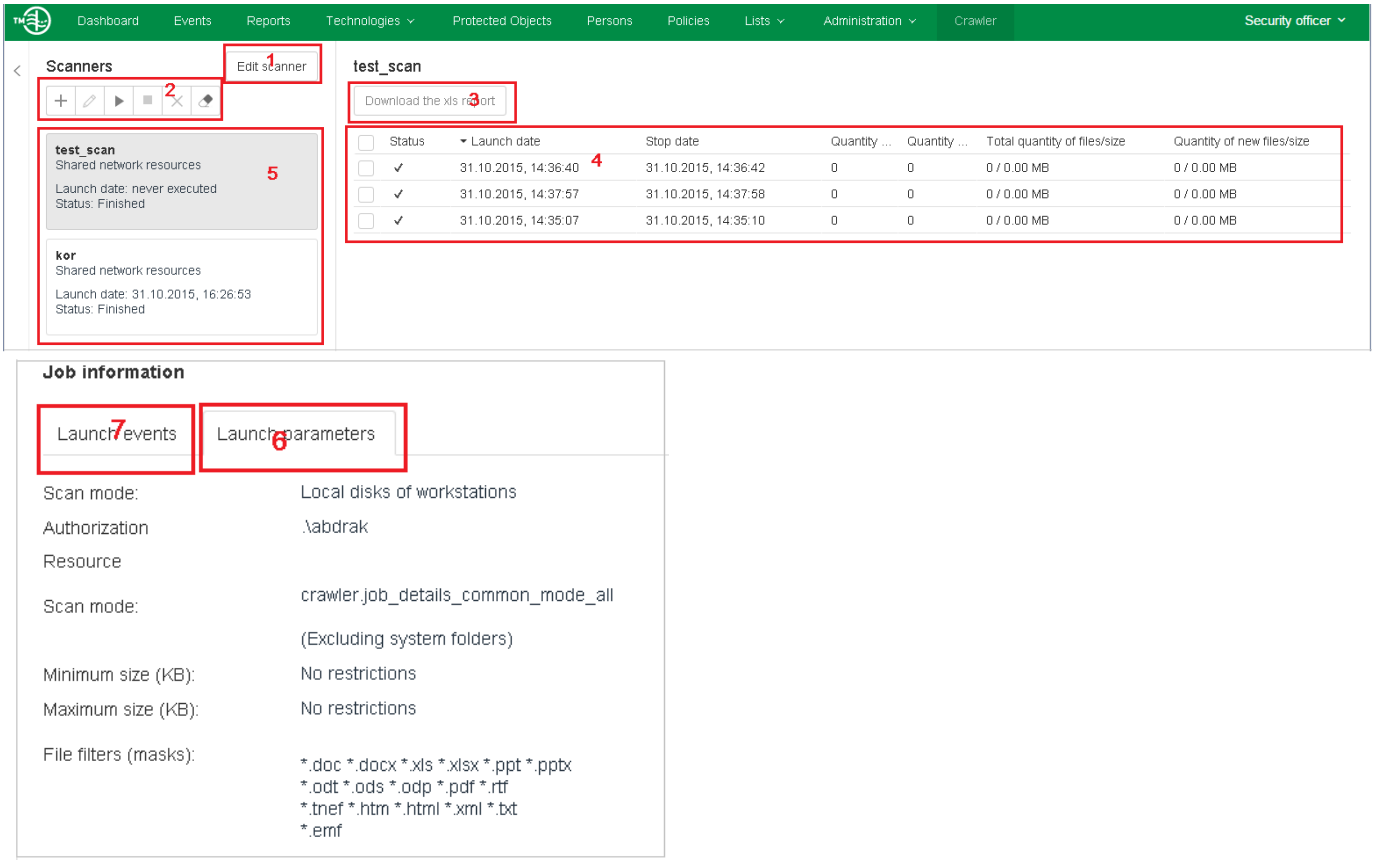
- Scanning network folders open for remote access by using the SMB protocol.
- Scanning local drives of workstations under Windows OS.
- Scanning the SharePoint file storage. Examines documents stored in Microsoft SharePoint 2007/2010/2013 database. Considers only the current versions of files: change log is not investigated.
- Customizing scan settings: speed of files downloading from scanned resources and settings of file queue to load objects to Traffic Monitor server.
- Creating a scan job where you can specify:
    - the list of folders and network nodes, where the scanning will be performed;
    - masks of processed files;
    - restrictions on the size of processed files;
    - schedule of job launching (you can also start it manually).
- Selection of only new and changed files: previously processed files do not send to the InfoWatch Traffic Monitor server.
- Transferring files to the InfoWatch Traffic Monitor server for analysis with user-defined sending parameters.
- Saving files according to the policy settings (by default only incidents are stored - files, recognized as the potential violation of the security policy)
- Representing the scanning results in the Management Console: using object queries and reports (including preset ones).

InfoWatch Crawler does not delete, move, rename, encrypt, or any other action on files - even when they recognized as a potential violation. The Crawler performs only informing of the security officer about the incident: the InfoWatch Traffic Monitor Management Console provides viewing files, recognized as a potential violation, with detailed information on their location and users who have access to it.

Managing Crawler is performed in InfoWatch Traffic Monitor Management Console, in the **Crawler** section.

About the section:

The section contains tools for creating, editing, and running jobs for the Crawler subsystem.



The section contains the following elements:

№ on scheme	Element	Purpose
1	Button of scanner editing	When clicked, on the right part of the workspace the form of scanner editing is displayed
2	Toolbar	Set of tools for scan jobs
3	**Download xls report** button (see "Saving Scan Report")	Allows you to save a report on the task execution in XLS format
4	Field of viewing the history of launching the scan job (see “Launch History")	Provides information about stages of scan job execution
5	List of scan jobs (see “Scanning Job")	Contains a list of scan jobs for the selected scanner
6	**Launch parameters** tab	Displays data on selected scan job
7	**Launch events** tab	Provides information about scanning events: the date and time the event occurred, and the message with the content of the event

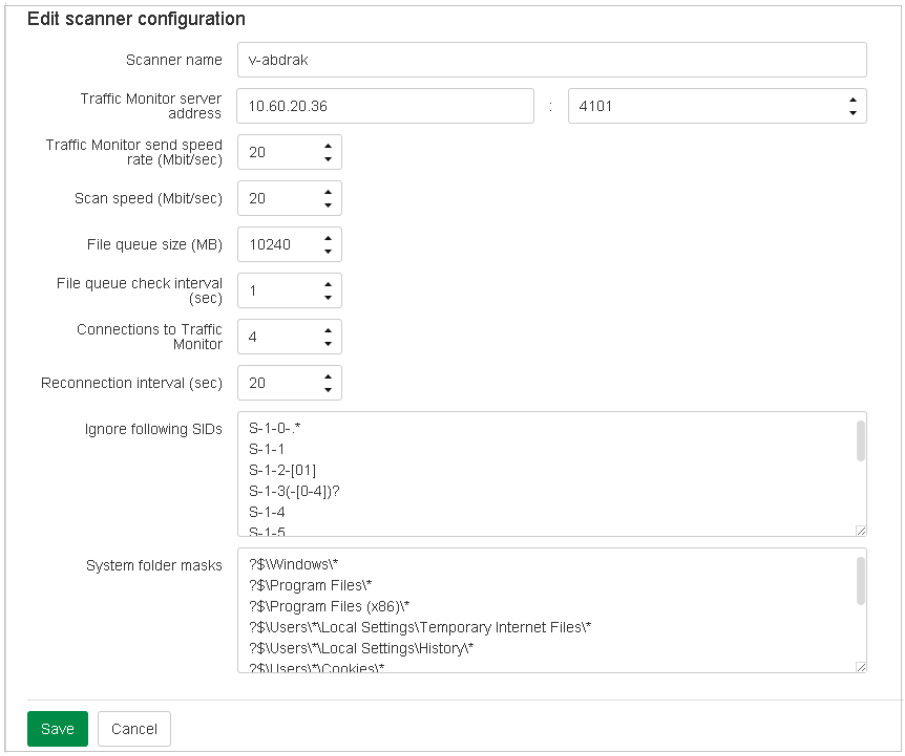
User’s target actions:

- Editing scanners installed in the System (see "Configuring Scanner")
- Creating the scanning job (see "Creating a Job")
- Starting and stopping the scanning job (see "Launching and Stopping the Job")
- Modifying the scanning job (see "Editing the Job")
- Cleaning the hash base of scanning jobs (see "Cleaning the Hash Base")
- Viewing the history of scanning jobs (see "Viewing Launch History")
- Saving the report of completing the scan job to the hard disk (see "Saving Scan Report")

4.9.1 Scanner

Reference information:
Scanner is the module of Crawler subsystem which scans data storages (such as Microsoft SharePoint 2007/2010/2013 storage, local disks of workstations, and shared network resources) defined by the user by means of scan jobs.

> **Note:**
>
> When scanning Sharepoint repository it is important, that Sharepoint and Scanner are located in the same domain.



Scanner attributes:

Parameter	Description

Parameter	Description
Scanner name	Name of the scanner
TM server address	The IP-address of the Traffic Monitor server hosting `iw_expressd`
Traffic Monitor sending speed (Mbit/s)	Maximum speed of uploading files to the Traffic Monitor server, Mbit/s Allows reducing the load on the Traffic Monitor server if the number of transmitted files is large
Scanning speed (Mbits/sec)	Maximum speed of downloading files from scanned resources to temporary storage (Mbits/sec) Allows reducing the load on the workstation on which scanning is performed
Size of the file queue (MB)	The maximum total size of the queue that stores detected files before sending them to the Traffic Monitor server, MB **Warning!** When the maximum total size is reached, the jobs are stopped and all files from this buffer are deleted without sending them to Traffic Monitor.
Interval of checking the queue (sec)	Interval (in seconds) at which the Crawler server will check for objects in the queue to be uploaded to the Traffic Monitor server. If there is at least one object in the queue, it will be passed to the Traffic Monitor server
Connections to Traffic Monitor	The maximum number of concurrent connections to the Traffic Monitor server
Reconnection interval (sec)	Interval (in seconds) at which the Crawler server will try to restore connection with the Traffic Monitor server if the connection is lost
Do not display the following SID	Allows you to configure a filter of persons
System folder masks	Folder masks, that will not be scanned

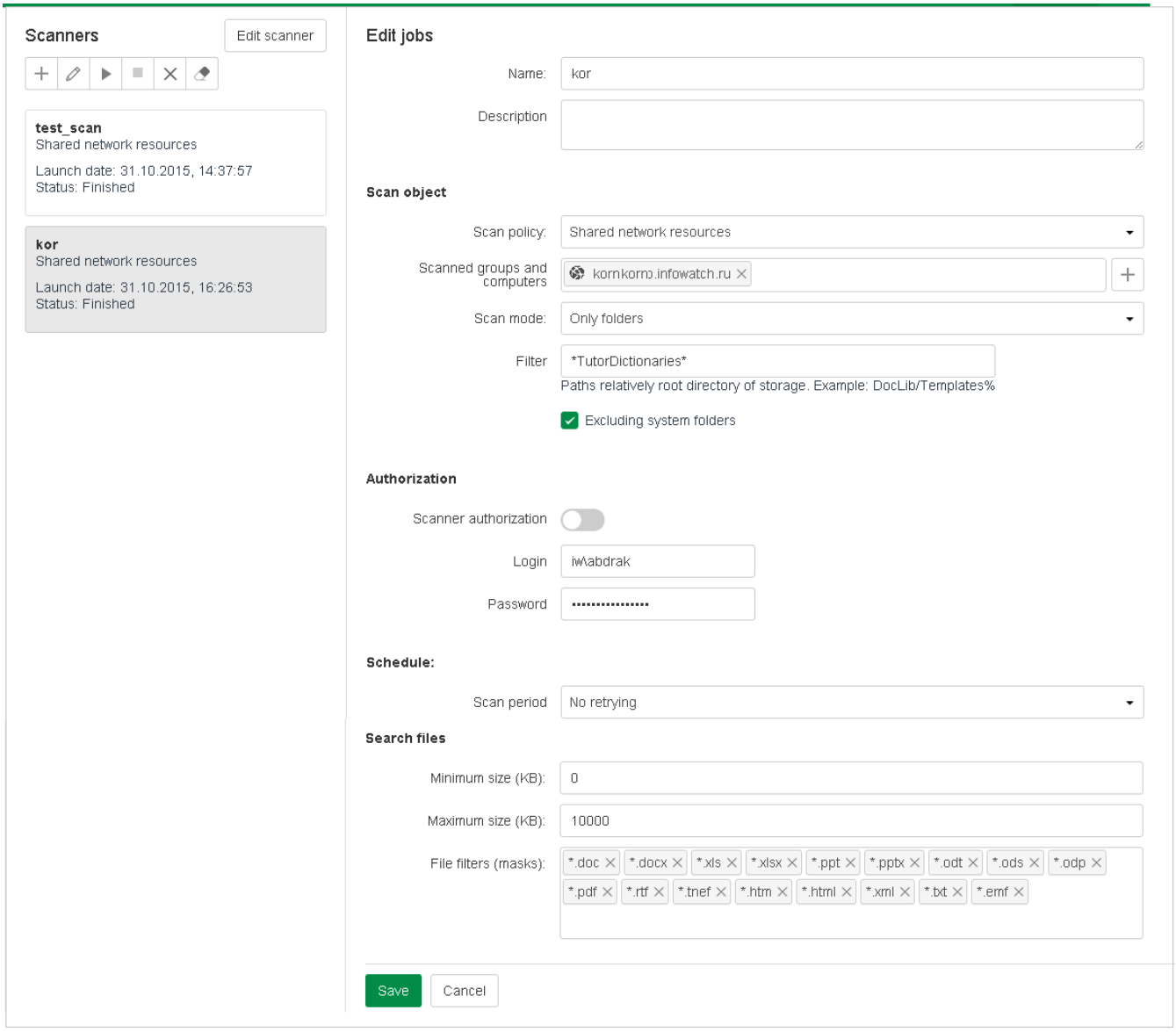
User's target actions:

- Editing scanners installed in the System (see "Configuring Scanner")
- Creating the scanning job (see "Creating a Job")
- Starting and stopping the scanning job (see "Launching and Stopping the Job")
- Modifying the scanning job (see "Editing the Job")
- Cleaning the hash base of scanning jobs (see "Cleaning the Hash Base")
- Viewing the history of scanning jobs (see "Viewing Launch History")
- Saving the report of completing the scan job to the hard disk (see "Saving Scan Report")

4.9.2 Scanning Job

Reference information:

Scanning job is a single or repeated operation of checking target storage locations (Microsoft SharePoint 2007/2010/2013 storage, local drives of workstations, shared network resources) if they store confidential data (for more details about the list of confidential data, see "Defining the confidential information"). Job attributes are displayed when you switch to edit mode.



Scanning job and its edit form

Job attributes:

Parameter	**Description**
Name	Name of the job
Description	Optional note

Scan policy	Type of scan job: • **Shared network resources** • **Local drives of workstations** When using the **Local drives of workstations** policy, the **Use simple file sharing** option must be disabled on workstations where Windows XP is installed (**Control Panel** -> **Folder Options**, **View** tab) • **SharePoint file storage** Depending on SharePoint version, specify the following parameters: **For SharePoint 2007 and 2010:** ○ **SharePoint version** - SharePoint version: 2007 or 2010; ○ **Address of DB resource** - enter address of SharePoint database server, e.g. `sharepoint-test`; ○ **Name of DB resource** - enter the name of SharePoint database instance, e.g. `wss_content`. **For SharePoint 2013:** ○ **SharePoint version** - SharePoint version: 2013; ○ **SharePoint server address** - enter address of SharePoint database server with the protocol (http:// or https://).
Scanned groups and computers	Group of persons and workstations to be scanned

Scan mode	**All folders** - scans all folders on the workstation **All folders except** - scans all folders on the workstation except the specified ones **Only folders** - only scans folders specified by the user **Note:** If you want to scan all folders including system folders, clear the check box **Exclude system folders**. By default, system folders are not scanned. **To specify scanning paths, you can use the following symbols:** *- any characters (0 and more) ?- any single character $- a character that is used by Windows to indicate the hidden folder **Warning!** The scanning path should end with ***** or ****. For example, the path can look like: "C?\folder*" or "C?\folder\". **When scanning the shared network resources or SharePoint storage you can use the following queries:** `Docs*` - will scan the Docs folder and all its subfolders. `text_example` - will search for “text_example” in the path. `.file_format` - will scan files of specified format (.txt) **When scanning local discs and folders, you can use the following queries:** `C$\Docs*` - will scan the Docs folder and all its subfolders on C:\ drive `*\Docs*` - will scan the Docs folder and its subfolders, regardless of their location. `?$\Docs*` - will scan any folder whose name has 1 character and the Docs folder with all subfolders. (C$\Docs\, D$\Docs) `\Docs????*` - will scan any folder that has Docs in its name with 4 additional characters (Docs1234) **Warning!** In the **All folders** scanning mode, only local drives of the workstation will be scanned.
Authorization	You can use scanner authentication (in this case, scanning will run under the user account under which the scanner is started) or specify the login and password of the user account manually. By default scanner authentication is used. **Warning!** When scanning the SharePoint storage, the user of the MS SQL Server that hosts the target database must be specified. **Warning!** Crawler uses access to domain controller to receive information about users or groups by unique identifier (SID). To provide access, use domain account with read rights for the resource to scan.
Scan period	Schedule of scanning **Warning!** If the **Monthly** period is selected, the scan job will start only when the current month contains the date specified in the **Day of month** parameter. For example, if the value of 30 is selected, then the scanning job will not run in February.
Minimum size (KB)	The minimum size of scanned files, in kilobytes
Maximum size (KB)	The maximum size of scanned files, in kilobytes

File formats	Extension of scanned files **To add a new format:** 1. In the field with the list of formats, type the desired extension and then press **Enter**. 2. The entered value will be added to the list of formats. 3. To delete a value, click x next to the required format.

User's target actions:

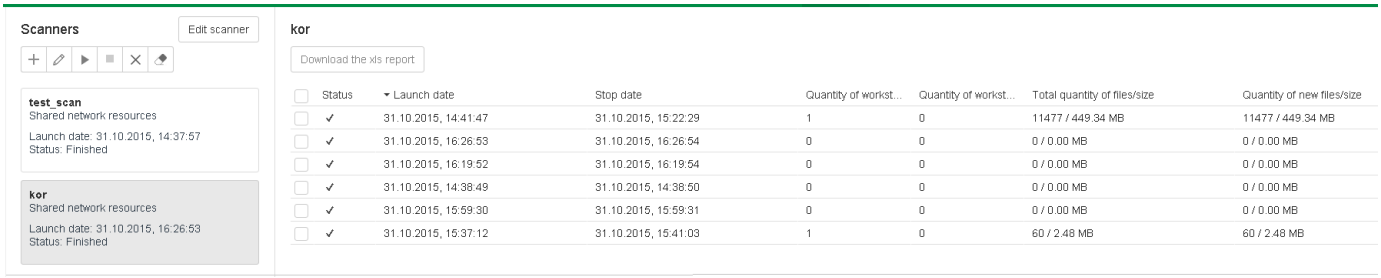
- Creating the scanning job (see "Creating a Job")
- Starting and stopping the scanning job (see "Launching and Stopping the Job")
- Modifying the scanning job (see "Editing the Job")
- Cleaning the hash base of scanning jobs (see "Cleaning the Hash Base")
- Viewing the history of scanning jobs (see "Viewing Launch History")
- Saving the report of completing the scan job to the hard disk (see "Saving Scan Report")

4.9.3 Launch History

Reference information:
The right part of the working area displays an information about launches of the selected scan job.

When you select a table entry, the detailed information about the selected launch is displayed on the tabs:

- **Launch events** - the tab contains system information about the launch of scanning job
- **Launch parameters** - the tab contains the list of attributes of scanning job (see "Scanning Job")



Scanning job and its viewing form

Attributes of the history entry:

Parameter	Description
Status	Identifier of the job status: ▶ - *Running*, ■ - *Stopped*, ✓ - *Completed*)
Launch date	The date and time the job run
Stop date	The date and time the job stopped
Quantity of workstations proceeded	Number of target workstations processed while the job was run

Parameter	Description
Quantity of workstations not proceeded	Number of target workstations which are not processed yet
Total quantity of files/size	Number and total size of files on target workstations processed while the job was run
Quantity of new files/size	The number and total size of files which were not processed previously on target workstations

User’s target actions:

- View information about the scan task execution phases (see "Viewing Launch History")

5 CASES SOLVING

Working in the Management Console, the Security Officer generally solves the following cases:

- Managing Persons and Workstations;
- Managing Catalogues;
- Working with the Base of Technologies;
- Managing Protected Objects;
- Managing Crawler Subsystem;
- Managing Interception Objects;
- Configuring System Response;
- Managing Reports.

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

Warning!

Administrating the Management Console is beyond the authority of the Security Officer and is not described in this document. You can find the necessary information in the document "*Infowatch Traffic Monitor. Administration Guide*".

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

- Dashboards Section
- Events Section
- Reports Section
- Technologies Section
- Protected Objects Section
- Persons Section
- Policies Section
- Lists Section
- Crawler Section

5.1 Typical Actions

Why the typical actions are needed?
To perform the same-type operations in the Management Console.

Typical actions include the following:

Action	Description
Log in and log out the Management Console	Is required to get authorized in the Microsoft Management Console to start working and then exit the Management Console
Applying System configuration	System configuration changes become active when updated configuration is applied
Editing the Element	You can edit entities required for configuring the System, displaying the interception objects and their processing
Deleting the Element	You can delete the entities used for configuring the System, displaying the interception objects and their processing
Pages Navigation	Numerous elements can be viewed in multi-page mode: navigation buttons are used to go to particular page with elements
Changing User's Password	To order of changing a password required to log into the System
Selecting Interface Language	Changing the interface language of the Management Console
Calling Help File	Access to the reference information
Viewing Information on System	Calling the general information on the System

5.1.1 Login and Logout of the Management Console

Purpose:

1. Log into the Management Console.
2. Log out of the Management Console.

Solution:

1. **To log into the Management Console:**
    a. Open the Google Chrome browser version 30 or higher (if the browser is not installed, you can download it by clicking on the link).
    b. Go to the address given to you by the system administrator. The browser window will display the start page of the Management Console.
    c. In the **Login** field, specify the user name.
    d. In the **Password** field, specify the password.
    Note:
    Username and password can be obtained from the administrator of InfoWatch Traffic Monitor.
    e. Click **Login**.
2. **To log out of the Management Console:**
    a. Click the user menu button (see "Management Console Interface").
    b. Select **Logout**.

5.1.2 Applying System Configuration

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

- Technologies
- Protected objects
- Persons
- Policies
- Lists

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

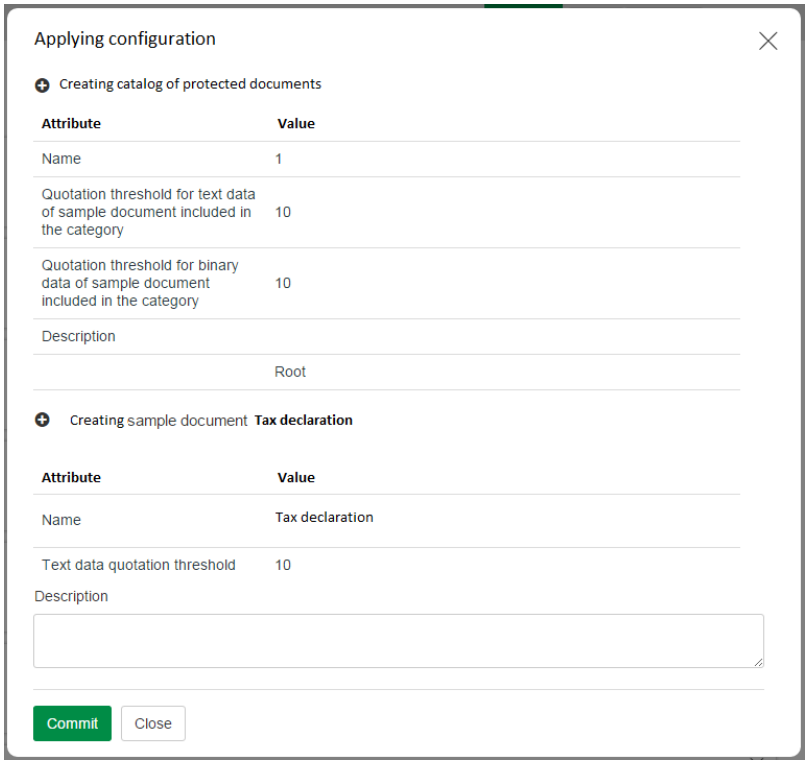
Purpose:
Apply the System configuration.

Solution:

1. When editing configuration is finished, at the top of your browser window, click **Save** in a line like the following:



The **Configuration change** window will open. It contains information about the changes:



2. If necessary, enter text in the **Description** field.
3. Click **Save**.

5.1.3 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**.

5.1.4 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**.

5.1.5 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".

5.1.6 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**.

5.1.7 Selecting Interface Language

Purpose:
Change the interface language of the Management Console.

Solution:

1. ClickClick the user menu button (see "Management Console Interface") 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.

5.1.8 Calling Help file

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

1. Click the user menu button (see "Management Console Interface"), and choose **Help**.
   The InfoWatch Traffic Monitor help file will appear in new browser tab.
2. Read the information and then close the tab in the standard way.

5.1.9 Viewing Information on System

Purpose:
Get general information about the System.

Solution:

1. Click the user menu button (see "Management Console Interface"), 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.

5.2 Managing Persons and Workstations

Warning!

To apply described changes to the System operation you should apply the renewed System configuration (see details in "Configuring the System" and "Applying the System Configuration".

Why the managing of persons and workstations is needed?
Lists of persons and workstations makes security officer's management of intercepted objects easier. This

comes from accounting of the data about senders, recipients (persons, employees), and workstations in special catalogues.

Managing persons and workstations includes following actions:

Action	Description
Creating a Group of Persons and Workstations	Creating a structural element of a catalogue
Creating a List of Persons and Workstations	Filling the catalogue
Viewing a Summary on Person or Workstation	Configuring widgets to display statistical data on person or workstation
Viewing Person's or Workstation Events	Viewing interception objects on target person or workstation
Adding a Status to Person or Workstation	Marking person or workstation to monitor its activities
Adding a Person or Workstation to the Perimeter	Adding person or workstation to configured lists of a company
Configuring Person's Card	Filling the person's entry with data
Configuring Workstation Card	Filling the workstation entry with data

See also:

- "Persons Section" - information on the section where the management of users' and workstations lists is performed.

5.2.1 Creating a Group of Persons and Workstations

Purpose:
Create a group of persons and workstations.

Solution:

1. Go to the **Persons** section.
2. In the left part of the workspace select **TM Groups**.
3. On the toolbar in the left part of the workspace, click **Create group**.
4. Specify attributes of the new group (see "Group of Persons and Workstations").
5. Click **Yes**.

Warning!

If a new group is created, events for this group will be displayed starting from the moment of applying configuration.

You can add existing Active Directory groups to a TM group. In this case, when you add or remove persons within an Active Directory group, contents of a corresponding Traffic Monitor group will be updated automatically.

To add an Active Directory group to a Traffic Monitor group, select a desired Active Directory group with a mouse and drag and drop it at the required TM group.
Groups from different domains can be added to the same Traffic Monitor group. You can also use drag-and-drop to add individual domain users to a Traffic Monitor group.

> **Note**
>
> To enable automatic update for TM groups which contain Active Directory groups, run synchronization with the LDAP server.

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

Additional information:

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

- Editing Element;
- Deleting Element.

5.2.2 Creating Persons and Workstations

Reference information:
A list of persons and workstations can be filled in two ways:

- from Active Directory of the company - this way 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 list of persons and workstations.

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;
    - **Workstations** - to add a workstation.
4. On the toolbar in the right part of the workspace, click + **Add**.
5. Specify parameters of the new user or workstation (see "Persons" and "Workstations").
6. Click **Save**.

Additional information:
Editing and deleting persons and workstations are performed by standard means:

- Editing Element;
- Deleting Element.

5.2.3 Viewing Events of a Person

Purpose:
To view events of a person or workstation.

Solution:

1. Create a query and specify the target person in its parameters (for more details, see "Creating queries").
2. Run the query you created.

Viewing workstation events is performed in a similar way.

Example:
If you need to display all the interception objects sent by Smith during the current week (assuming that the *Smith* person has already been created in the **Persons** section):

1. Go to the **Events** section and create a query named *Smith* where:
    - **Date of interception** attribute has the *Current week* value;
    - **Senders** attribute has the *Smith* value (selected from a list of previously created persons).
2. Save and apply the created query.

As a result, a list containing all found events will be displayed.

5.2.4 Viewing a Summary on Person

Purpose:
To view summary on a person or workstation.

Solution:

1. Create a query and specify the target person in its parameters (for more details, see "Creating queries").
2. Create a **Selection** widget and in the **Summary** attribute, specify an earlier created query (see “Creating Widget")

Viewing summary on workstation is performed in a similar way.

Example:
If you need to display all interception objects sent by Smith during the current week (assuming that the *Smith* person has already been created in the **Persons** section):

1. Go to the **Dashboard** section.
2. Create a widget named *Smith* where the **Summary** attribute has the value of an earlier created query *Smith* (see "Viewing Events of a Person").
3. Save and apply the created widget.

The **Dashboard** section displays the *Smith* widget with all required events.

5.2.5 Adding Status to a Person

Purpose:
To add status to a person or workstation.

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;
   - **Workstations** - to add status to a workstation.
4. Select the target user or the target workstation.
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 description.
7. Click **Save**.

Note:

The *New* status is assigned to a person or workstation when they are created in the System and is preserved for 30 days (in case employees and workstations are imported from Active Directory, the *New* status is preserved for 30 days from the moment the records were created in Active Directory)

See also:

- "Statuses" - on the section where managing user statuses is performed

5.2.6 Adding a Person to Perimeter

Purpose:
Add a person or a group to an existing perimeter.

Solution:

1. Go to the **Lists**->**Perimeters** section.
2. By clicking the left mouse button select a target perimeter from the list (see "Perimeters").
3. In the right part of the workspace click **Add element to perimeter** and in the drop-down list select **Person**.
4. In the **Person** field that appears, specify the target person by doing one of the following:
   - start typing the name or surname and select the desired entry from the drop-down list;
   - click **Add**, and in the dialog box that opens, select the check box for the target person (you can select multiple persons), then click **Save**.
5. In the perimeter editing area, click **Save**.

In the same way, you can add a group of persons to the perimeter.

Example:

If you want the perimeter*Accounts* to include the group *Financial*:

chose the *Accounts* perimeter in the list of perimeters and then add the *Financial* group:

1. click **Add element to perimeter**;
2. in the drop-down list, select **Group of persons**;
3. in the **Group of persons** specify *Financial* and clicks **Save**.

See also:

- "Perimeters" - on the section where managing perimeters is performed

5.2.7 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 a created person
Adding a workstation to a person	Add a workstation associated with a person
Adding a Person to Group	Adding a person to an existing group

5.2.7.1 Adding Contact to a 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. On the right part of the workspace, open the **Persons** tab and do either of the following:
   - double-click the left mouse button to select the target record;
   - click the left mouse button to select the target record, and on the toolbar click **Edit**.

   The person card editing form will open.
4. On the right part of the edit form, click **Contacts**.
5. Click **Add contact** and specify the required parameters:
   - type of contact: e-mail, Lotus mail, mobile phone, landline phone, Skype, ICQ, web contact;
   - whether the contact is personal or working;
   - contact value (number or address);
   - optional description.
6. 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);
- - Skype contact (string of 1 or more characters);
- - Skype contact (string of 1 or more characters);
- - WEB-identifier, for example, a profile on a social network (string of 1 or more characters);
- - Lotus e-mail (string of 1 or more characters).

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**.

5.2.7.2 Adding Workstation to a Person

Purpose:
To add a workstation 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. On the right part of the workspace select the **Persons** tab and do one of the following:
   - double-click the left mouse button to select the target record;
   - click the left mouse button to select the target record and on the toolbar, click **Edit**.

   The edit form of the person card editing will open.
4. On the right part of the person card edit form, click the **Computers** tab.
5. Click **Add workstation**.
6. In the window that opens, flag required workstations and click **Yes**.
7. Click **Save**.

5.2.7.3 Adding a 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, select the **Persons** tab and do either of the following:
   - double-click the left mouse button to select the target record;
   - select the target record using the left mouse button and on the toolbar on the right part of the workspace, click **Edit person**.

   The edit form of the person card will open.
4. On the right part of the person card edit form, click the **Groups** tab.
5. Click **Add group**.
6. In the window that appears, select a check box next to desired groups, and then click **Add**.
7. Click **Save**.

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

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

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

5.2.8 Configuring Worksation Card

Purpose:
Fill the workstation card with data.

Configuring a workstation card consists of the following actions:

Action	Description
Adding contact to computer	Adding an IP/DNS contact or a domain account to the computer

Action	Description
Adding a person to computer	Adding a person associated with this computer
Adding computer to a group	Adding computer to an existing group

5.2.8.1 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. On the right part of the workspace select the **Computers** tab and do either of the following:
   - select a target workstation by double-clicking the left mouse button;
   - left-click a target workstation and on the toolbar click **Edit**.

   The edit form of the computer card will open.
4. On the right part of the computer card editing form go to the **Contacts** tab.
5. Click **Add contact** and specify required parameters:
   - contact type: **IP**, **DNS** or **Domain account**;
   - account value: IP address, DNS name, or the domain account name;
   - optional description.
6. Click **Save**.

5.2.8.2 Adding Person to a 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. On the right part of the workspace select the **Computers** tab and do one of the following:
   - double-click the left mouse button to select the target computer;
   - click the left mouse button to select the target computer and on the toolbar, click **Edit**.

   The edit form of the computer card will open.
4. On the right part of the computer card editing form go to the **Persons** tab.

5. Click  **Add person**.
6. In the window that opens, flag required persons and click **Save**.
7. Click **Save** on the edit form.

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

5.2.8.3 Adding Computer to a 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. On the right part of the workspace select the **Computers** tab and do one of the following:
   - double-click the left mouse button to select the target computer;
   - click the left mouse button to select the target computer and on the toolbar, click  **Edit**.

   The edit form of the computer card will open.
4. On the right part of the edit form, click the **Groups** tab.
5. Click  **Add group**.
6. In the window that opens, flag required groups and click **Add**.
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 **Leave the current group**.
3. In the confirmation window, click **Yes**.

> **Warning!**
>
> If the computer is included in this only group, then executing this command will result in deleting the computer.

5.3 Managing Catalogs

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 add, edit, or delete catalogs used in the System.

Managing catalogs includes the following actions:

Action	Description
Managing Tags	Editing the list of tags
Managing Resources Lists	Editing the list of resources
Managing Statuses	Creating the list of statuses
Managing perimeters	Editing the list of perimeters

See also:

- "Lists Section" - on the section where managing catalogs is performed

5.3.1 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.

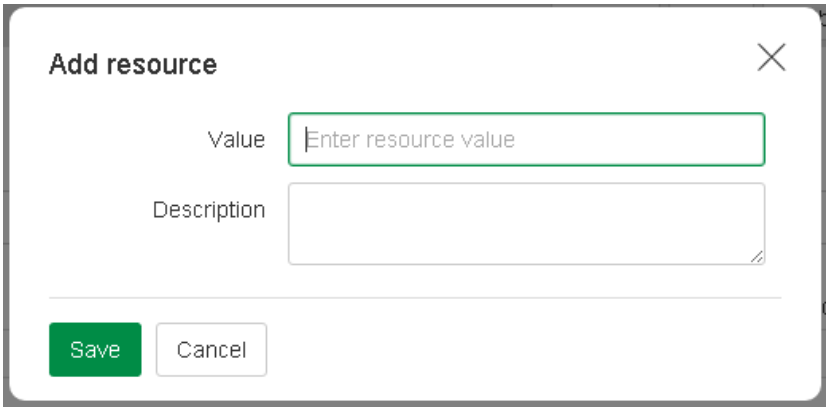
5.3.2 Managing Web Resources

Purpose:
Specify Internet resources, which are detected by the System as inappropriate use of working time. To do this, you need to:

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

Solution:

1. Creating a group of resources.
    a. Go to the **Lists** section, the **Resources** subsection.
    b. In the left part of the workspace, click + **Create 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, **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 + **Create resource**.



    d. In the **Adding resource** window that opens, enter the resource attributes:
        - in the **Value** field - the resource name on the Internet;

- in the **Description** field - a comment on the record on the resource (optional).

e. Click **Save**.

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

Example:

If you want to System to mark the interception object as *IMPROPER_SITE* when employees visit the EXAMPLE.COM site:
create the *IMPROPER_SITE* resource group and in the group, create the resource *EXAMPLE.COM*.

Additional information:

- Editing and deleting resources and their groups are performed by standard means:
  - Editing Element;
  - Deleting Element.

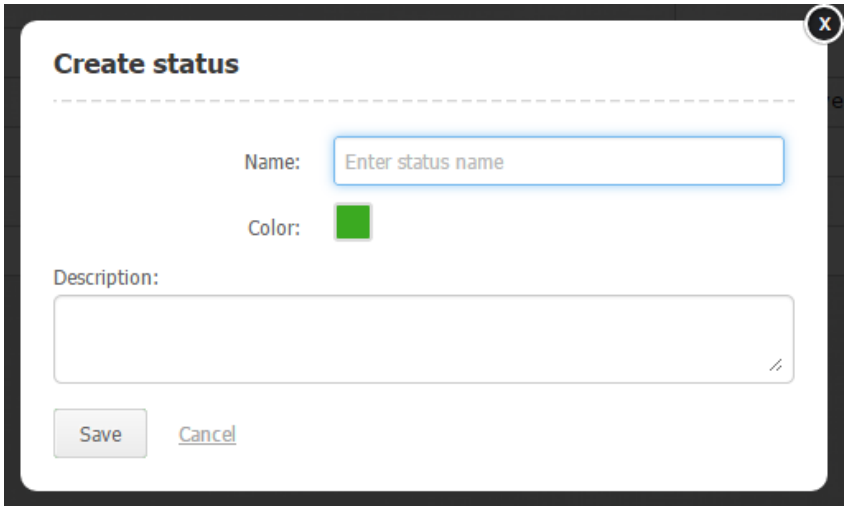
5.3.3 Managing Statuses

Purposes::

1. Create a status characterizing a person or workstation.
2. Create a person control policy for persons with the same 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 added status (see "Statuses").

4. Click **Save**.

To create a person control policy directly from the 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 will display the new person control policy for persons with a specified status and form its viewing form (for more detail, see "Policies and their viewing form").

Additional information:

Editing and deleting statuses is performed by standard means:

- Editing Element;
- Deleting Element.

5.3.4 Managing perimeters

Reference information:

Perimeters allow you to logically divide your organization into structural elements and track the traffic of each element.

By default, the company perimeter is created in the System (perimeter name may vary). For the actions specified in predefined policies to be applied to interception objects, you need to add elements to the perimeter (see Purpose 2 in this article).

> **Note:**
>
> If you choose LDAP domain when creating a perimeter, you should first configure synchronization with the LDAP server and add the domain via the **Groups** tab.

Purpose:

1. Create a perimeter.
2. Add an element to 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 dialog window that opens, in the **Name** field specify the name of the perimeter.
   d. In the **Description** field, enter a description of the perimeter (optional).
   e. Click **Save**.
2. To add an item 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 **Add element to perimeter** and in the drop-down list select the desired element type.

d. In the field that appears, specify one or more elements doing one of the following:

- For *Persons*, *Group of persons* or *Resource topic*:
  - 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. Click **Add**.
- For *E-mail address*, *Web-resource*, *Phone*, *Skype*, *ICQ*, *Domain* and *Lotus contact* - enter the name (for example, of *Web-resource*) or value (for example, of *IP address*) in the field and click **Enter** on the keyboard.

> **Warning!**
>
> To include the domain in the perimeter, you should use its full name. If you specify a domain name of the first level, domains of nested levels will not be included in the perimeter. For example, when you add the `domain.com` domain in the perimeter, the `basic.domain.com` domain of the nested level will not be considered.

e. Entered values will be added to the list of elements. To remove a single element from the list, click the X next to the element name. To delete the entire list of elements of a particular type, click the × button next to the line with a list of elements.



Example:

1. If you want to create an *Accounts* perimeter:
   Add a new perimeter and assign it the name *Accounts*.
2. If you want the perimeter *Accounts* o include the *Financial* group (including all the contact details of all persons belonging to the specified group), and the employee John Smith (assumes that *John Smith* person has already been created in the **Persons** section), not included in the *Financial* group:
   chose the *Accounts* perimeter in the list of perimeters Then:
   - addthe *Financial* group:
     - click **Add element to perimeter**;
     - in the drop-down list select **Group of persons**;
     - in the **Group of persons** specify *Financial*;
   - add the *John Smith* person:
     - click **Add element to perimeter**;

- in the drop-down list select **Person**;
- in the **Person** field specify *John Smith*.

Additional information:

- Editing perimeter is performed by standard means (see "Editing Element").
- Deleting perimeter is performed by standard means (see “Deleting Element").

5.4 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 managing the base of technologies is performed
- "List of Resources" - on the subsection where managing the list of resources is performed
- "Protected Objects Section" - on the section where managing protected objects is performed

5.4.1 Defining the Confidential Information

Purpose:

136

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**).

> **Note:**
>
> The Graphical Objects subsection contains only preset elements. Adding, editing or deleting these elements is unavailable.

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 conformity of the text to the category of the found term.	Creating terms and their categories
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. Sample blanks may be different questionnaires, receipts, etc. Sample 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 Sample Forms

Technology name	Technology description	Action
Stamps	Stamp image that is searched in the network traffic. Sample stamps can be images of round impressions used in organizations.	Creating Sample Stamps
Database unloadings	A part of a database quotes from which are searched in the analyzed text. Sample database unloadings can be lists of salaries, other personal data, etc.	Creating Sample 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.	The System contains only preset graphical objects. Creating or editing graphical objects is unavailable.

See also:

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

5.4.1.1 Managing Categories and Terms

Reference information:
Terms are a set of data required to perform the linguistic analysis of 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.

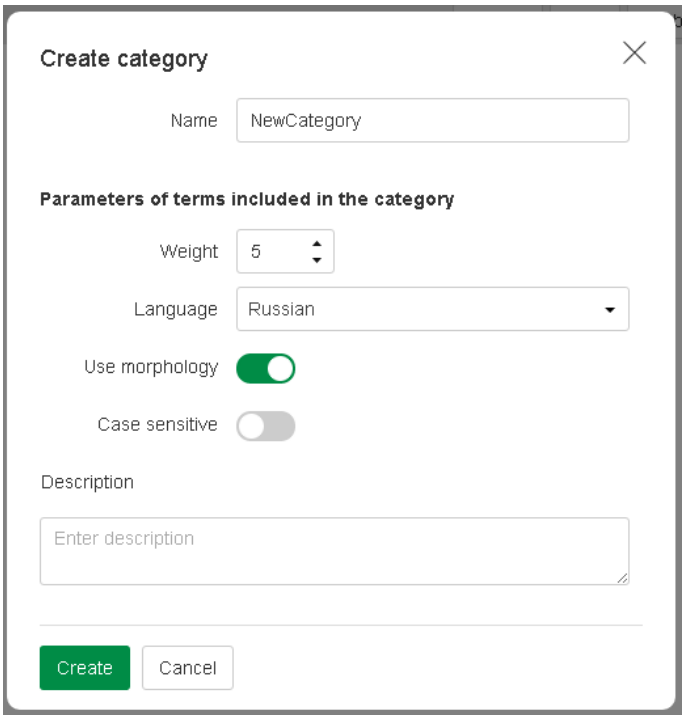
Solution:

5.4.1.1.1 1. To create a category.

1.

   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**.

5.4.1.1.2 2. Creating a term.

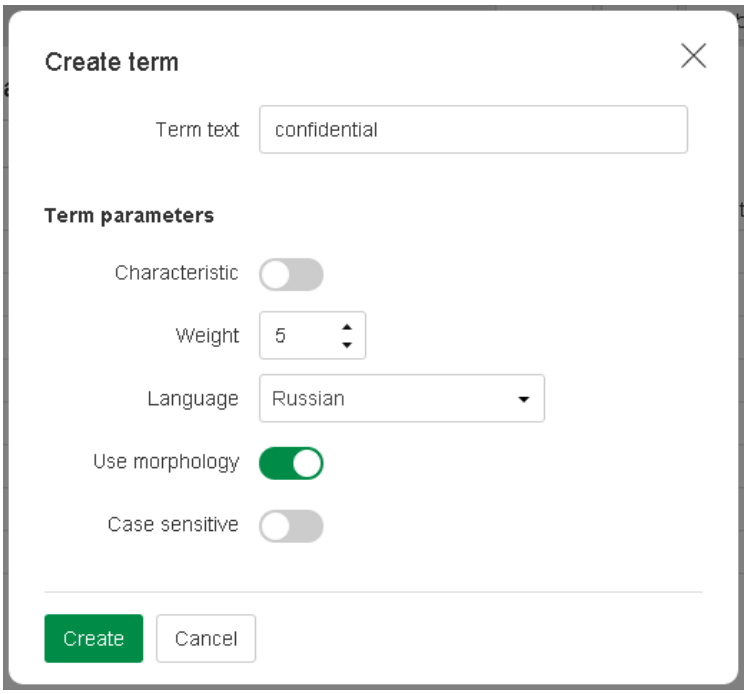
1.

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**.

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

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

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

Example 2:
If you need that in case traffic contains fragments of program code, the System would mark the intercepted object as code leakage:
The security officer creates a C*ode leakage* category, and adds the terms: *Procedure* and *Result*. 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 is performed by standard means:

- Editing Element;
- Deleting Element.

5.4.1.2 Managing Text Objects

Purposes:

1. Create a catalog of text objects.
2. Create a text object and specify its value.
3. Add a system text object to the selected catalog.

Solution:

5.4.1.2.1 1. Create a catalog of text objects.

1.

a. Go to the section **Technologies** -> **Text objects**.

b. On the toolbar on the left side of the workspace, click  **Create a catalog of text objects**.

c. In the window that opens, type a name and description for the catalog.

d. Click **Save**.

5.4.1.2.2 2. Create a text object and specify its value.

1.

a. Go to the section **Technologies** -> **Text objects**.

b. On the left part of the workspace by clicking the left mouse button, select the catalog inside which you want to create a text object.

c. On the toolbar for working with text objects located on the right side of the workspace, click  **Create a text object**.

d. Enter the name and description of the text object.

e. Click **Create**. The new text object will be added to the list.

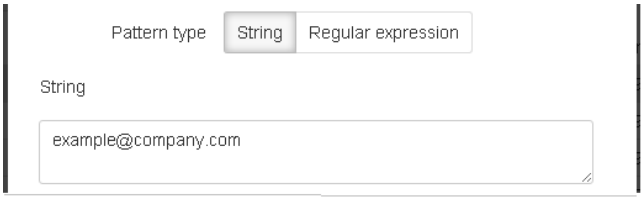
f. Select the text object in the list and click  **Edit**.

g. Create a template for the text object and specify its parameters (see "Text objects patterns").

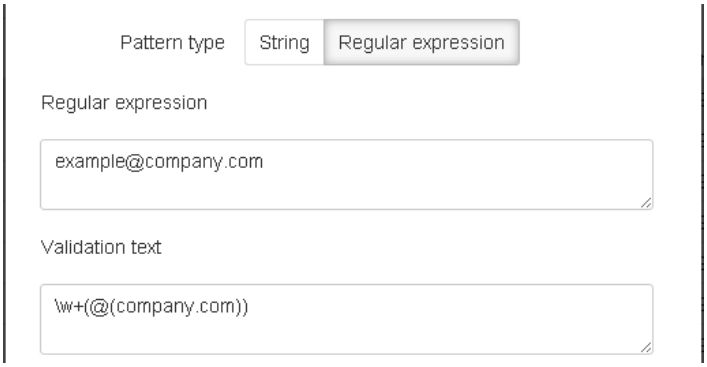
h. Click **Save**.

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:
the security officer creates an active text object *EXAMPLE_MAIL*. The Security Officer then selects the created text object with a mouse, switches to the object edit mode, creates a new active template for the text object, and specifies the following string as template value:`example@company.com`:



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*:
the security officer creates an active text object *COMPANY_MAIL.* The Security Officer then selects the created text object by clicking the left mouse button, switches to the object edit mode, creates a new active template, and specifies the following regular expression as its value:`w+(@(company.com))`



Note:

The System uses a standard regular expression language. Detailed information about regular expressions you can find, for example, in an online article "Regular Expression Language".

3 Add a system text object to the catalog.

1.

a. Go to the section **Technologies** -> **Text objects**. On the left part of the workspace left-click the target category.

b. On the left part of the workspace by clicking the left mouse button, select the catalog to which you want to add a text object..

c. On the toolbar for working with text objects located 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** string.

e. Click **Add**.

Note:

System text objects already contain pre-installed templates. However, you can also add a custom template to a selected system object. To do this, do the steps **f**-**h** from item **2. Create a text object and specify its value**.

Additional information:
Editing and deleting text objects and their values and catalogs are performed by standard means:

- Editing Element;
- Deleting Element.

5.4.1.3 Managing Sample Documents

Purposes:

1. Create a catalog of sample documents
2. Create a sample document inside catalog.
3. Update a sample document.

Solution:

1. Createa catalog of sample documents

1.

a. Go to the section **Technologies**->**Sample Documents**.

b. On the toolbar in the left part of the workspace click  **Create catalog of sample documents** .

c. In the window that opens, specify parameters for the new catalog (see "Sample Documents").

d. Click **Create**.

2. To create a sample document

1.

a. Go to the section **Technologies**->**Sample Documents**.

b. On the left part of the workspace by clicking the left mouse button, select the catalog 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 at 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.

- When the uploading is finished, the sample document will be added to the catalog. 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 for binary data - 128 Mb;
> - Maximum size for text data - 30 Mb;
> - Minimal size for binary and text data – 128 байт;
> - Minimal plain text size for text data - 10 symbols;
> - Minimal image size - 100 pixels on one side;
> - Allowable aspect ratio - not bigger than 5 : 1.

a. 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

1.

a. Go to the section **Technologies**->**Sample Documents**.

b. On the left side of the workspace, select a desired catalog.

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:
If you need the System to mark the interception object as INTERNAL_COMPANY_RULES when traffic contains at least 30% of text from the document "*Internal regulations of the company*":

1.

a. The security officer goes to the required catalog,

b. loads the document file "internal rules of the company" as a sample document,

c. for the **Name** attribute, specifies the value *INTERNAL_COMPANY_RULES*

d. for the **Text data quotation threshold** attribute, specifies the value **30**.

If you need that the System marks the interception object as SETUP_EXE when the traffic contains at least 10% of the binary content of the "`Setup.exe`" executable file:

1.

a. The security officer goes to the required category,

b. loads the file "`Setup.exe`" as a sample document,

c. for the **Name** attribute, specifies the value *SETUP_EXE,*

d. for the **Binary data quotation threshold** attribute, specifies the value **10**.

Additional information:
Editing and deleting the sample documents and their catalogs are performed by standard means:

- Editing Element;
- Deleting Element.

5.4.1.4 Managing Blanks

Purpose:

1. Create a catalog of sample blanks.
2. Create a sample blank.
3. Update a sample blank.

Solution:

1. Create a catalog of sample blanks

1.

a. Go to the **Technologies**->**Blanks** section.

b. On the toolbar on the left part of the workspace, click + **Create a catalog of sample forms.**

c. In the window that opens, type a name and description of the catalog.

d. Click **Create**.

2. Create a sample blank

1.

a. Go to the **Technologies**->**Blanks** section.

b. On the left part of the workspace by clicking the left mouse button, select a catalog inside which you want to create a sample 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 sample 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 sample blank will be added to the catalog. All necessary attributes are assigned to a newly created blank by default.

> **Note:**
>
> If the System cannot load the file of the sample blank, the download window will display an error message.

f. To change attributes of the sample blank specified by the System, click  **Edit** on the toolbar and change required attributes (see “Blanks").

3 Update a sample blank

1.

a. Go to the **Technologies**->**Blanks** section.

b. On the left side of the workspace, select a desired catalog.

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 sample 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. the Security Officer creates a *RECRUITMENT_CHECKLIST* blank,

2. loads the document file “Recruitment checklist” as a sample blank,
3. creates a protected object based on the *RECRUITMENT_CHECKLIST* blank,
4. in detection conditions, selects **Filled and unfilled** checkbox.

Additional information:
Editing and deleting sample forms and their catalogs are performed by standard means:

- Editing Element;
- Deleting Element.

5.4.1.5 Managing Stamps

Purposes:

1. Create a catalog of sample stamps.
2. Create a sample stamp.

Solution:

1. Create a catalog of sample stamps.

1.
    a. Go to the section **Technologies**->**Stamps**.
    b. On the toolbar on the left side of the workspace, click
    
    Create a catalog of sample stamps.
    c. In the window that opens, specify parameters for the new catalog.
    d. Click **Create**.

2. Create a sample stamp

1.
    a. Go to the section **Technologies**->**Stamps**.
    b. On the left part of the workspace by clicking the left mouse button, select the catalog inside which you want to create a sample stamp.
    c. On the toolbar in the right part of the workspace, click  **Add**.
    d. In the dialog window that opens, select a document that will be used as a sample stamp and click **Open**.
    e. When the download is finished, the sample stamp will be added to the catalog. All necessary attributes are assigned to a newly created sample stamp by default.

> **Note:**
>
> If the System cannot load the file of the sample stamp, the download window will display an error message.

f. To change the sample stamp attributes specified by the System, on the toolbar click **Edit** and change the required attributes (see "Stamps").

> **Note:**
>
> For more details on creating sample stamps, see the Knowledge Base article "How to use a detector of sample stamps".

Example:
If you need the System to mark the interception object as ROUND_SEAL if it contains an image of stamp used in the organization:

1.

a. the Security Officer prepares the file "`Stamp.png`" where the full-size square image of the stamp is placed against a white background,

b. goes to the required catalog,

c. loads the image file "Stamp.png" as a sample stamp,

d. creates a protected object *ROUND_SEAL* based on the created sample stamp.

Additional information:
Editing and deleting stamps and their catalogs are performed by standard means:

- Editing Element;
- Deleting Element.

5.4.1.6 Managing DB Unloadings

Purpose:

1. Create a catalogue of sample unloadings.
2. Create a sample database unloading.
3. Update a sample unloading.

Solution:

1. Create a catalogue of sample unloadings

1.

a. Go to the **Technologies**->**DB Unloadings** section.

b. On the toolbar on the left side of the workspace, click



Create catalog of DB unloadings.

c. In the window that opens, type a name and description for the catalog.

d. Click **Create**.

2. Create a sample database unloading

1.

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 click **Open**.

> **Warning!**
>
> When running Postgre SQL sample unloading size can be no bigger, than 1GB.

e. When the file is uploaded:

- click **Configure DB unloading** - to customize the sample unloading, or
- close the **Creating DB unloading** window - to exit without additional configuration.

f. Specify required attributes (see “DB Unloadings" and "Detection Conditions for Unloading").

g. Click **Save**.

3 Update a sample unloading

1. Go to the **Technologies**->**DB Unloadings** section.
2. On the left side of the workspace, select the desired catalog.
3. In the list in the right part of the workspace, select the sample unloading you want to update.
4. Click  **Edit**.
5. In the edit window that opens, click **Update**.
6. Specify the desired update mode: **Adding new records** or **Removing old records and adding new ones**.
7. Click **Choose file**.
8. In the dialog window that opens, select a file that will be used for update, and click **Open**. The file download will begin.
9. After the download is finished, the sample 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.

Additional information:
Editing and deleting sample unloadings and their catalogs are performed by standard means:

-
    - Editing Element;
    - Deleting Element.

5.4.1.6.1 Detection Conditions for Unloading

Reference information:

Satisfying the detection conditions allows the System to associate the interception object with a particular sample unloading.

You can specify several (up to 20) detection conditions for a sample 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 catalogue.
3. In the right part of the working area, select a desired sample unloading from the list and click

   Edit.
   The sample 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. **Detection rule**.
6. Click **Create**.

When editing detection condition parameters, consider the following recommendations:

Detection rule.

The detection rule 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.

Note:

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 sample 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 rule it is required that the analyzed text should contain at least 10 different rows that satisfy the condition 1+(2|3).

Example:

If you need the System to mark the interception object as PHONE_NUMBERS when detecting 7 or more rows with filled columns 1 and 4 from the table with the following structure:

Last name	Name	Phone number
Smith	John	89441234347

Last name	Name	Phone number
Johns	Tom	83531355424
Williams	William	83544593406
White	Jane	83245446441
Black	Jillian	84534359243
Davis	Michael	83544352925

1. save the table in CSV or TSV format and upload this file to the System;
2. configure the detection rule:
    - in the **Detection rule** field, specify **1+4**
    - in the **Minimal quantity of rows** field, specify **7**
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

5.4.2 Exporting and Importing the Technologies Database

Purpose:

- Save the XML document containing the base of technologies to a hard drive of the computer;
- Load the technologies database stored on your computer as XML document, for using in the InfoWatch Traffic Monitor Management Console.

> **Note:**
>
> Export and import of technologies cannot be performed, if the System configuration is being edited. In this case, an error message will be displayed.

To export the technologies base:

1. Go to a subsection of the **Technologies** section (**Categories and terms**, **Text objects**, **Sample Documents**, **Blanks**, **Stamps** or **Database Unloadings**).
2. On the toolbar on the left part of the workspace, click ▾ and in the drop-down list select **Export**.
3. In the dialog window **Save as** that opens, specify the location on disk where the xml file will be saved.

4. Click **Save**. The XML file will be saved 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.

The structure of catalogs is preserved when exporting.

> **Warning!**
>
> The base of technoligies included in the last applied configuration is exported (see “Configuring the System").

To export the technologies base stored on your computer in the form of XML document:

1. Go to a subsection of the **Technologies** section (**Categories and terms**, **Text objects**, **Sample Documents**, **Blanks**, **Stamps** or **Database Unloadings)** .
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 XML file that you want to load.
4. Click **Open** and wait till the data is loaded into the System.

> **Note:**
>
> If the catalog name in the import file matches the catalog name in the System, but paths to a catalog differ, then the catalog from the import file will not not added. If the catalog name in the import file matches the catalog name in the System, and paths to catalog also match, then data from the import file will be merged with the data contained in the System.

Features of merging data when importing:

1. For catalogs, the following items missing in the System are added:
   a) child catalogs;
   b) elements of technologies.
2. For categories, the terms that are missing in the System will be added.
3. For a 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. 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.

5.5 Managing Protected Objects

What are protected objects needed for:

Using protected objects allows you to check if intercepted data contain several elements of analysis at the same time: for example, a sample document, a text object and a database unloading. Thus you can configure the System so that it detected certain business documents: for example,vehicle certificate or declaration of insurance payment.

Working with protected objects includes the following actions:

Action	Description
Creating a catalog of protected objects	Creating a catalog to which protected objects will be added
Creating a protected object	Creating a protected object and specifying its parameters
Adding elements of analysis	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 catalogs	Creating a data protection policy for selected protected objects and their catalogs
Import and export of protected objects	Importing and exporting catalog structure, protected objects included in these catalogs and elements of analysis used in these protected objects
Activating and deactivating protected objects	Changing status of protected objects and their catalogs

See also:

- "Protected Objects Section" - on the section where managing protected objects is performed

5.5.1 Creating a Catalog of Protected Objects

Purpose:
Create a catalog 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 catalog of protected objects**.

> **Note:**
>
> You can create a new catalog of protected objects inside an existing catalog. To do this, select the target catalog in the list.

3. In the dialog box that appears, specify the catalog attributes.
4. Click **Create**.

You can move the selected catalog using drag and drop. To do this, select the catalog in the list, press the left mouse button pressed and move the catalog to the desired location in the catalog structure holding the left mouse button pressed. Then release the mouse button.

> **Note:**
>
> The catalog will be moved with all nested elements including subcatalogs and protected objects. When you move a catalog, its status changes to the status of the catalog to which you are moving it.

Additional information:

Editing and deleting catalogs of protected objects are performed by standard means:

- Editing Element;
- Deleting Element.

5.5.2 Creating a Protected Object

Purpose:
Create a protected object based on the elements of analysis that are present in the System.

Solution:

1. Go to the **Protected objects** section.
2. On the left side of the workspace, select a catalog to which you want to add a new protected object, or create a new catalog (see "Creating a catalog 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 analysis").

5. Determine whether the selected items will be included in one protected object, or for each element, a separate protected object will be created:
    - If the **Create an protected object for each selected item** option is selected, a set of protected objects for each selected element of analysis will be created. Attributes of the created protected objects will be generated automatically. Object names will be generated based on the element name and its technology, for example: "*Text object: Credit card number*".
    - If the **Create an protected object for each selected item** option is not selected, then after clicking **Create** an additional window will open where you can specify settings of the protected object: see step 7.
6. Click **Create**.
7. If the **Create an 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 analysis** tab, that contains the selected items (see "Elements of analysis"), you can add additional elements of analysis (for this, click **Select elements**), as well as remove elements from the list: for this, click on the ' x ' button in the row of the selected element.
    c. On the **Detection conditions** tab, specify the conditions under which protected objects will be detected in the intercepted data (for details, see "Adding detection conditions").
    d. If necessary, enter optional text in the **Description** field.
    e. Click **Create**.

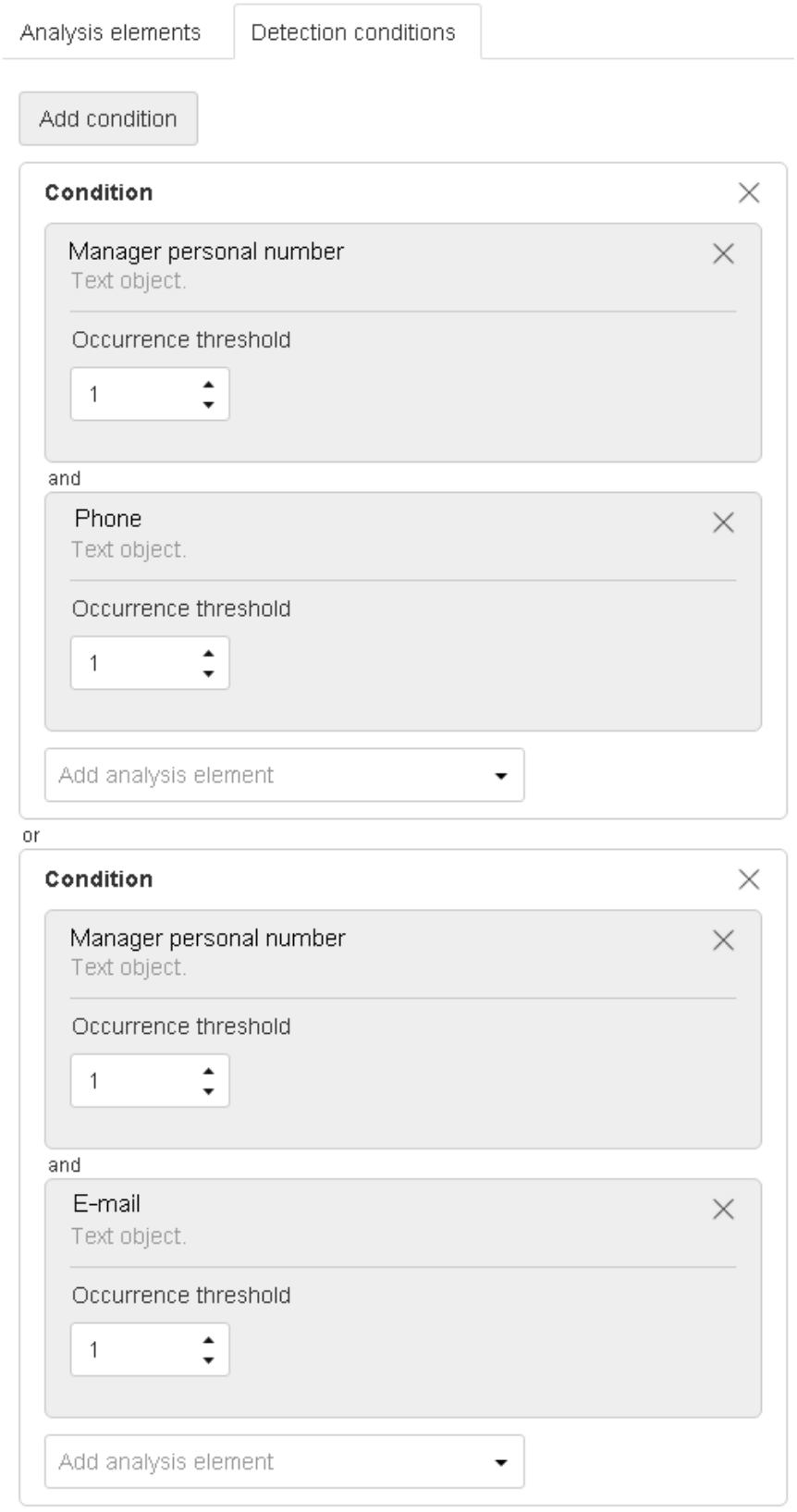
As a result, a protected object will be created in the selected catalog (if you have selected the **Create an protected object for each selected item** option, several protected objects will be created).You can move the created protected object to another catalog.To do this, select the required protected object in the list, press the left mouse button and move the protected object to the desired catalog holding the left mouse button pressed. Then release the mouse button.
Example:You need to create a protected object *"Manager Personal Number"* that will be detected in the System when one of the following conditions is fulfilled:

- the interception object contains a personal number of the manager and E-mail;
- the interception object contains a personal number of the manager and a phone number;

In this case, create a new protected object and add the following elements of analysis:

- a text object *"Manager Personal Number"*;
- a text object *"E-mail"*;
- a text object *"Phone"*;

and specify the following detection conditions for selected elements of analysis:



Additional information:

Editing and deleting protected objects are performed by standard means:

- Editing Element;
- Deleting Element.

5.5.3 Adding Elements of Analysis

Purpose:
Add elements of analysis to a protected object.

Solution:

1. Switch to create or edit mode (see "Creating a Protected Object") of a protected object. If you are in the edit mode, click **Select elements**.
2. In the **Elements of analysis** window that opens, go to the desired tab.
3. From the list of elements, choose 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.

4. Click **Create** if you are in the create mode, or **Add** if you are in the edit mode.

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

If you want to delete a protected object, click on the cross to the opposite of the desired element.

5.5.4 Adding Detection Conditions

Reference information:

A protected object will be detected in event if:

1. The protected object status is **Active**.
2. The event contains elements of analysis of this protected object with respect to specified detection conditions.

A catalog of protected objects will be detected in event if:

1. A status of the catalog of protected objects is **Active**.
2. The event contains at least one protected object from the catalog.

Purpose:

Add detection conditions for a protected object.

Solution:

1. Go to the edit mode of the protected object, to the **Detection conditions** tab.

> **Note:**
>
> Detection conditions can be also specified when creating a protected object (see "Creating a Protected Object", step 7c).

2. In the **Add element of analysis** field, click on the arrow and in the drop-down list select a desired element.
   The selected element will be added to the list of conditions. For some elements of analysis, you can also specify additional detection conditions (see "Detection conditions").
3. If there are several elements of analysis in the protected object, add detection conditions for the rest of the elements in one of the following ways:
   - If you need conditions to be combined using the operation of conjunction (logical "AND"), add a condition, as described in step 2.
     In this case, all added conditions will be placed in one **Condition** block and combined with the operation of conjunction.
   - If you need conditions (or groups of conditions) to be combined using the operation of disjunction (logical “OR"), click the **Add condition** button.
     A new **Condition** block will be added. Within this block you can add conditions as described in step 2.
     In this case, all the **Condition** blocks will be combined with each other using the disjunction operation, and conditions within a single will be combined using the conjunction operation.
4. Click **Save**, if you are in the edit mode, or **Create**, if you are in the mode of creating a protected object.

Additional information:

Deleting conditions is performed in the following way:

- to delete a 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.

5.5.5 Creating Policies for Protected Objects and their Catalogs

Purpose:

Create a data protection policy for protected objects directly from the "Protected objects" section.

To create policy for a catalog of protected objects:

1. Go to the section **Protected objects**.
2. In the **Catalogs of protected objects** list on the left side of the workspace, select the desired catalog.

3. On the toolbar in the left part of the workspace, click and, in the drop-down list, select **Create policy**.
4. In the policy creation window that appears, specify the required settings (for more information, see "Policies and their Viewing Form").
5. Click **Save**.

The created data protection policy will be triggered when detecting at least one protected object from the selected catalog.

To create policy for selected protected objects:

1. Go to the section **Protected objects**.
2. In the **Catalogs of protected objects** list in the left part of the workspace, select the desired catalog.
3. In the right part of the workspace, a list of protected objects included in the selected catalog 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 **Create policy**.
5. In the policy creation window that appears, specify the required settings (for more information, see "Policies and their Viewing Form").
6. Click **Save**.

Established data protection policy will be triggered when detecting at least one of the selected protected objects.

5.5.6 Import and Export of Protected Objects

Purpose:

- export to a file catalog structure containing protected objects and elements of analysis used in them;
- load from file an earlier created catalog structure containing protected objects and elements of analysis used in them;

> **Note:**
>
> Export and import of protected objects cannot be performed, if the System configuration is being edited. In this case, an error message will be displayed.

To export 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 **Export**.
3. In the window that opens, specify where you want to save the created archive.

The saved archive contains the .XML files that store information about the protected objects and elements of analysis used in them. Th structure of catalogs and elements of analysis is preserved when exporting.

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 download.
4. Wait till the protected objects are loaded into the System.

Note:

If the catalog name in the import file matches the catalog name in the System, but paths to a catalog differ, then the catalog from the import file will not not added.If the catalog name in the import file matches the catalog name in the System, and paths to catalog also match, then data from the import file will be merged with the data contained in the System.

Features of merging data when importing:

1. For catalogs, the following items missing in the System are added:
   a) child catalogs of protected objects
   b) protected objects
2. For protected objects, the following items missing in the System are added:
   a) elements of analysis
   b) detection conditions
3. For detection conditions, new nested conditions, including detecting parameters (for text objects, blanks and database unloadings) will be added.

5.5.7 Activating and Deactivating Protected Objects

By default, the status of all created protected objects and their catalogs is Active (icon for protected objects and icon for their catalogs). If necessary, you can deactivate a created catalog of protected objects or a particular protected object within 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 catalog of protected objects**.
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 catalog of protected objects**.

To deactivate a selected protected object:

1. On the left part of the workspace, select a desired catalog.
2. On the left part of the workspace left-click the target resource list.
3. On the toolbar in the right part of the workspace, click and in the drop-down list select **Deactivate protected object**.
4. The status of 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 protected object**.

> **Warning!**
>
> Protected objects and their catalogs can be detected in intercepted data only if they are active.

5.6 Managing Crawler Subsystem

What do you need the Crawler subsystem for?

Managing the Crawler subsystem is required for scanning the following file storages:

- Shared network resources
- Local drives of workstations
- SharePoint 2007/2010/2013 file storage

Managing the Crawler subsystem includes the following actions:

Action	Description
Configuring Scanner	After the administrator installs and configures the System, the user will get access to a scanner. To work with the scanner, the user can configure it
Creating a Job	To scan resources, you need to create a job
Launching and Stopping the Job	Running the job starts the scanning of the target file storages; when the job is finished, the scanning stops
Editing the Job	Changing job settings
Cleaning the Hash Base	Discarding file checksums saved in the System
Viewing Launch History	Viewing system information during the job progress
Saving Scan Report	Copying a report to a hard disk of your computer

See also:

- "Crawler Section" - on the section where managing the Crawler subsystem is performed

5.6.1 Configuring Scanner

Purpose:
To configure the scanner of the Crawler subsystem.

Solution:

1. Go to the section **Crawler**.
2. On the toolbar on the left part of the workspace, click the **Edit scanner** button.
3. On the right part of the workspace, scanner attributes will be displayed (see "Scanner").
4. When you change at least one attribute, to the right of the **Edit scanner** button, the  icon will by displayed, indicating that scanning job for this scanner are not performed.
5. Change the required parameters.
6. Click **Save** to save your changes, or **Cancel** to exit the editing mode without saving changes.

When you save the scanner configuration the  icon will disappear, indicating that scanning job for this scanner can be performed.

Additional information:
The value of the **Do not display the following SID** attribute lists the standard SIDs. If necessary, the user can add own SID and set masks using regular expressions.

Entry example:
`S-1-5-21-.*-(498|502|517|527)`
This entry means that when Management Console displays the information on the object, it will not display the information that this file is available to accounts with any SIDs beginning with "S-1-5-21-" , having 0 in the middle or more of any characters, numbers, etc., and ending with " -498" or " -502" or " -517" or " -527".

Matching SIDs:
`S-1-5-21-12345-ABCDEF-498`
`S-1-5-21-527`

Not matching SIDs:
`1S-1-5-21-12345-ABCDEF-498` - does not start with "S-1-5-21-"
`S-1-5-21-527-` S-1-5-21 - starts with "S-527-" but ends with "527" rather than " -527"
`S-1-5-21-ABCDEF-100-` does not end with " -498" or " -502" or " -517" or " -527".
`S-1-5-21-ABCDEF-502--` does not end with " -498" or " -502" or " -517" or " -527".
`S-1-6-21-ABCDEF-502` - does not start with "S-1-5-21-".

> **Note:**
>
> More detail about the format of the regular expression language see in the article "Regular Expression Language".

5.6.2 Creating a Job

Purpose:
Add a scan job.

Solution:

1. Go to the **Crawler** section.
2. On the toolbar click  **Create job**.
3. On the right part of the workspace, on the **Details** tab, enter the job attributes (see “Scanning Job").
4. The following fields are obligatory:
    - **Scanning policy**;
    - **Scanned groups/workstations**;
    - **Schedule**.
5. Click **Save**.

Example:
If you need the System to assign Printed circuit board tag to objects created as result of detecting TXT files containing the phrase “printed board” and stored in existing corporate storage SharePointRepo, CorporateDataBase database:

Create the term with the text “printed circuit board” (see "Creating Terms") and a tag *Printed circuit board* (see "Managing Tags“), then apply the configuration (see “Applying System Configuration").
Then create a scanning job by selecting SharePoint as scanning policy and specifying following values of attributes:

- attribute **Address of DB resource** - value *SharePointRepo*;
- attribute **Name of DB resource** - value *CorporateDataBase*.

Create a policy and a rule of placement in it with the following attribute values:

- **Storage** - *File storage*; attributes have following values:
    - attribute **Enter a source** - value *SharePointRepo*;
    - attribute **Enter a path to storage** - value *CorporateDataBase*;
- **Tags** - tag *Printed circuit board*.

Warning!

While the job runs even with domain administrator rights, you may receive the error:

```
Access to the path <path_to_folder> is denied: Access to the path <path_to_folder>
is denied
```

where `<path_to_folder>` is an absolute path to the folder where the job runs.
This error can occur for example, if a user who is the owner of the folder, prohibited access to it.

5.6.3 Launching and Stopping the Job

Purposes:

1. To launch the scan job.
2. To stop the scan job.

Solution:

1. Launching scan job.

a. Go to the **Crawler** section.
b. Left-click the necessary job in the list.
c. On the toolbar click  **Run job**.

2. Stopping scan job.
   a. Go to the **Crawler** section.
   b. Left-click the necessary job in the list.
   c. On the toolbar click  **Stop job**.

5.6.4 Editing the Job

Purpose:
To edit the scan job.

Solution:

1. Go to the **Crawler** section.
2. Left-click the necessary job in the list.
3. On the toolbar in the left part of the workspace, click  **Edit job**.
4. In the right part of the workspace, in the edit form that appears, modify the job attributes (see "Scanning Job").
5. Click **Save** to save your changes, or **Cancel** to exit the editing mode without saving changes.

5.6.5 Cleaning the Hash Base

Reference information:
To optimize the performance, Crawler provides the storage of **hashes** - checksums of files. If during previous scan job session the hash of some file was saved and in latest session of the same job the hash of this file was not changed, this means that the file was not exposed to changes and it should not be sent to Traffic Monitor server for processing. This reduces a load on a channel between Crawler and Traffic Monitor Server and a load on the Traffic Monitor Server itself; it also excludes duplication of identical events for each start of a scanning job.
Features of storing database of hashes:

- Hash database is saved separately for each scanning job. Therefore if some file was already processed by one job, then when creating and starting another job, it will not be considered.
- Hash sums are stored for files considering workstations at which these files were found. Therefore if the same file is located at several workstations, it will be processed individually for each workstation.

It is recommended to periodically clean the hash base. For example, when the Traffic Monitor configuration was edited - that is, according to a changed policy or the list of terms, etc, the decision if the intercepted object is a potential violation or not will be made by the System using another algorithm. As a result of cleaning the hash base, the job will “forget” that it ever processed any files and will send all files corresponding to conditions of this job for the analysis to the Traffic Monitor Server.

Purpose:
To clear the hash base.

Solution:

1. Go to the **Crawler** section.
2. Left-click the created job in the list.
3. On the toolbar, click  **Purge hashes**.

5.6.6 Viewing Launch History

Reference information:
The right part of the working area displays an information about launches of the selected scan job.

Purpose:
View the history of job launches.

Solution:

1. Go to the **Crawler** section.
2. Left-click the necessary job in the list.
3. View the summary in the right part of the workspace.
4. To view more information about the job and on the launch settings, left-click the necessary launch's entry in the list.
   Extended information is presented in the following tabs:
   - **Launch events** - the tab contains system information about the launch of scanning job
   - **Launch parameters** - the tab contains the list of attributes of scanning job (see "Scanning Job")

   To return to the summary information about the history of launches click the link **< Back**.

5.6.7 Saving Scan Report

Purpose:
To save a report on scanning.

Solution:

1. Go to the **Crawler** section.
2. Left-click the necessary job in the list.
   On the right part of the workspace a history of launching the job will be displayed.
3. Set check-boxes in required rows and click **Download xls report** in the upper part of the workspace.
4. Open the saved file in .xls format with standard means (e.g. MS Excel).

5.7 Managing Interception Objects

What for 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.

Working with interception objects consists of 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
Managing Summaries	Generating summary on violations/violators
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
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 manage interception objects
- "Dashboard Section" - on the section, where you can view statistics on interception objects

5.7.1 Viewing summary on violations/violators

The operation is performed in the **Dashboard** section (see "Dashboard Section")

Purpose:
View summary on violations/violators

Solution:

1. Go to the **Dashboard** section.
2. Configure the toolbar (see “Creating a Dashboard").
3. Add and configure the desired widget (see "Creating Widget" and "Editing Widget").
4. Examine the summary provided on the widget.

5.7.1.1 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:

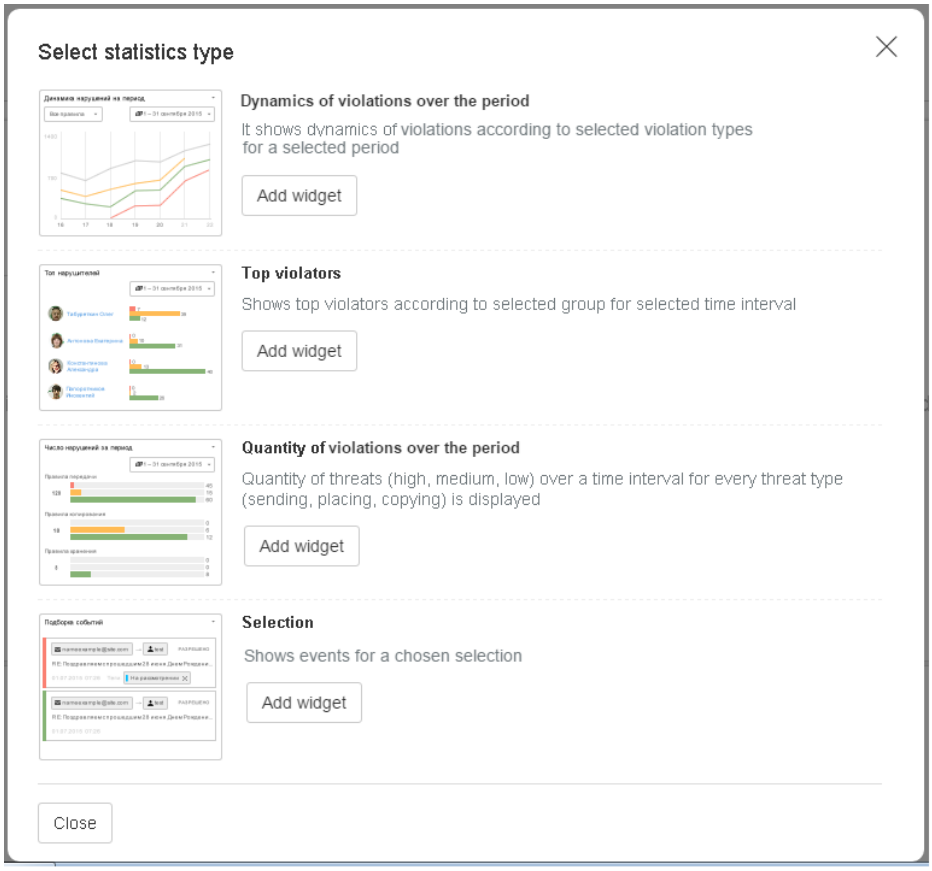
- Filling a dashboard is described in "Creating Widget".
- To delete a dashboard, go the dashboard which you want to delete and, on the tab with its name, click ×. In the confirmation window, click **Delete**.

5.7.1.2 Creating 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 a desired widget and click **Add widget** under its description.



See details on widget types in "Widgets".
You can add several widgets in succession. To do this, click **Add widget** under other widets you want to add: selected widgets will be added to the dashboard.
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 creating queries, see "Query Creation in Standard Mode" and "Query Creation in Advanced Mode").

5. Click **Close** or use ✕ button in the upper right corner of the window.
6. Configure added widgets to display required data: see "Configuring Widget".

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**.

5.7.1.3 Editing Widget

Purpose:
Configure a widget.

Solution:

1. Go to the **Dashboard** section and open the desired dashboard.
2. Select the desired widget or create a new one (see "Creating Widget").
3. Use interface elements located in the widget to specify the following parameters: the type of the rules whose violations will be displayed in the widget and the time period.
4. To change other parameters, click ▾ and, in the drop-down list, choose **Edit**.
5. In the **General widget settings** window that opens, specify required parameters (see "Widgets").
6. Click **Save**.

5.7.2 Viewing Events

Purpose:
View information on the interception object.

Solution:

1. Go to the **Events** section (see "Events Section").
2. Apply event filtering by creating and running a query (see "Creating queries").

> **Note:**
>
> The list displaysthe last 10000 events. Events are sorted by ID-number in descending order.

3. If required, change the list of fields to be displayed (see "Choosing event fields of view").
4. View event information on the event tile or in the string of a table (see point 3 in the diagram in "Events Section ").
5. If necessary, use a brief and detailed forms of viewing events.

5.7.2.1 Creating queries

Purpose:
Create a query that allows you to filter the interception objects.

Solution:

1. Go to the **Events** section (see "Events Section").
2. Select a query from the drop-down list of selections in the upper string of the left part of workspace or create a new one.

Note:

There are two ways to create a query: standard mode and advanced mode.

3. Apply the query by clicking  **Execute query** (when creating a query, you can use **Save and execute**).

Note:

To hide the results of the query, to the right of the name of the query in the query list, click .

See also:

- "Query Creation in Standard Mode" - on how to create a standard query
- "Query Creation in Extended Mode" - on how to create an extended query

5.7.2.1.1 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. On the toolbar in the upper string of the left side of workspace click  **Add query**.
3. In the drop-down list, select **Standard query**. In the right part of the workspace, a query creation form will open.
4. In the **Name** field, specify the name of the query.
5. On the **Condition** tab, fill in the fields which will be used for search of events (see "Condition").
6. On the **Display fields** tab, select attributes whose values will be displayed for the found events (see "Display fields").
7. To allow other users to view and edit the query, on the **Access parameters** tab, clear the **The query is available only to the owner** check box (by default, the check box is selected).
8. Click:
   - **Save** - to save the filter.
   - **Save and execute** - to save and apply the filter.

Note:

For more flexible configuration of search conditions, you can use the advanced mode.

Example:

If you want the System to display events with a *High* violation level and the assigned policy *Legal documentation*:
then create a filter in the standard mode and specify the following attributes: for **Violation level** attribute, specify the *High* value; for **Policy** attribute - the *Legal documentation* value.

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

- Editing Element;
- Deleting Element.

5.7.2.1.2 Query Creation in Advanced Mode

Purpose:
Configure search conditions for events more clearly.

Solution:

1. Go to the **Events** section.
2. On the toolbar in the upper string of the left side of workspace click  **Add query**.
3. In the drop-down list, select **Advanced query**. A query creation window will open.
4. In the **Name** field, specify the name of the query.
5. On the **Condition** tab, in the **Add condition** drop-down list, select parameters based on which search will be performed.
6. By default, added attributes are associated with conjunction operation (logical AND). To change the operation type, left-click on the 

icon. The icon will change to 

that stands for the disjunction operation (logical OR).
7. Use **Group of parameters** element to separate attributes combined with conjunction operation (logical AND) from attributes combined with disjunction operation (logical OR) (see "Advanced mode").
8. On the **Display fields** tab, select attributes whose values will be displayed for found events (see "Display fields").
9. To allow other users to view and edit the query, on the **Access parameters** tab, clear the **The query is available only to the owner** check box (by default, the check box is selected).
10. Click **Save**.

Example 1:
If you want the System to display events:

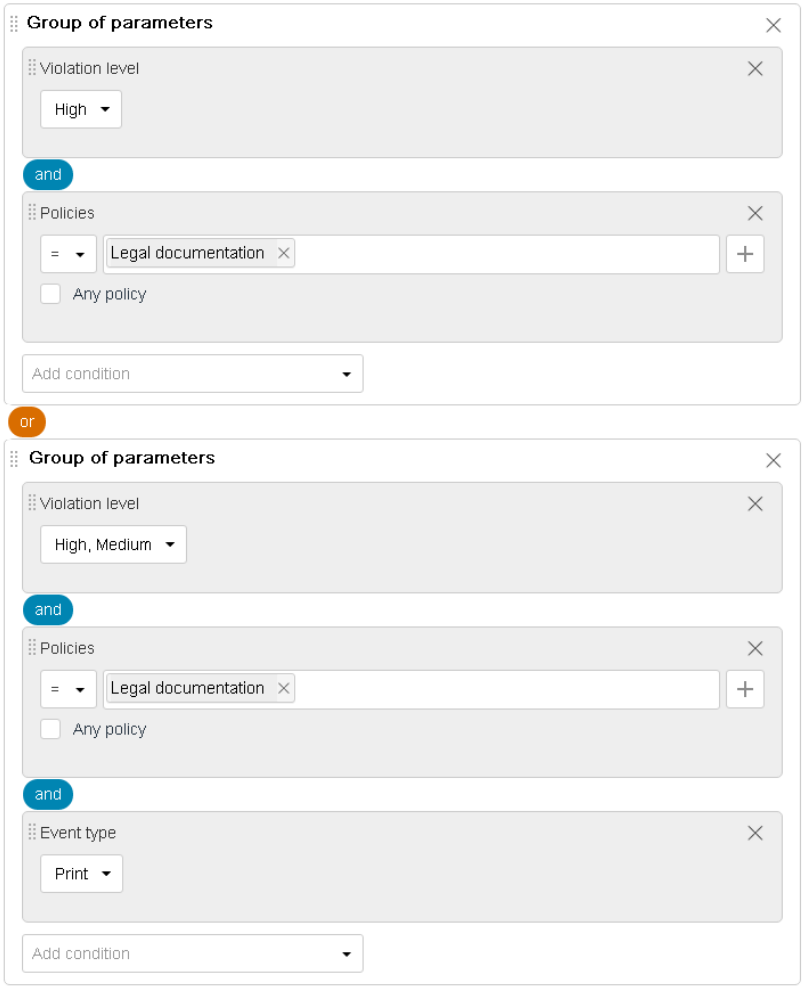
- with *High* violation level and the assigned policy *Legal documentation*;
- with the levels of violation *High* and *Medium* and the assigned policy *Legal documentation* and event type *Stamp*:

Then create a query in the advanced mode and specify two groups of parameters combined with the disjunction operation (see the picture below):

- The first group of parameters contains attributes with the following values:
    - **Violation level** - *High*;
    - **Policy** - *Legal documentation*;
- The second group of parameters contains attributes with the following values:

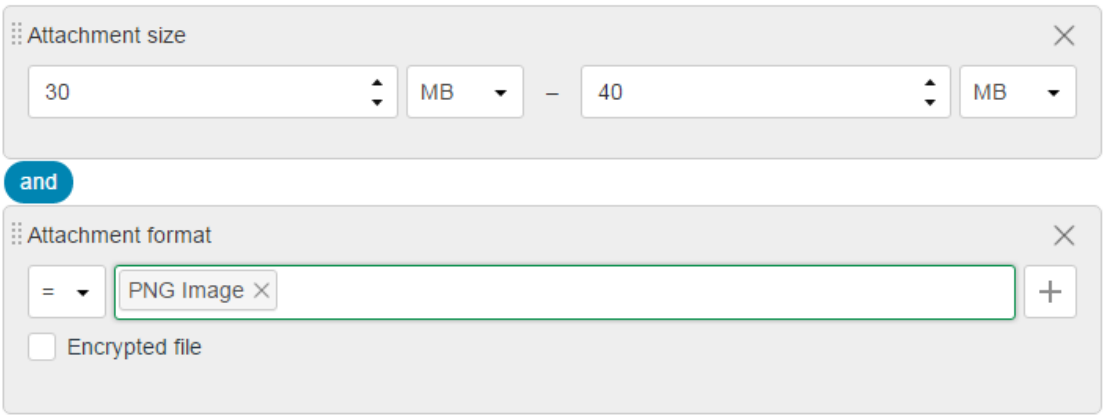
- **Violation level** - *High* and *Medium*;
- **Policy** - *Legal documentation*;
- **Event type** - *Stamp*;

- Attributes within groups are combined with the conjunction operation.

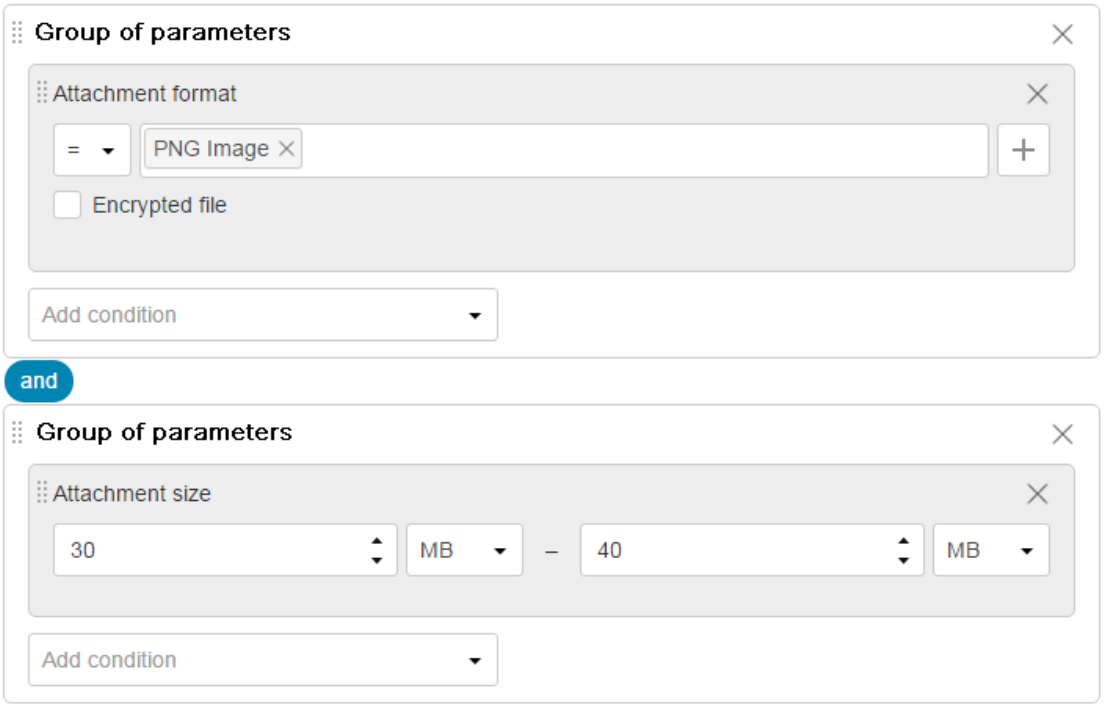


Example 2:
If conditions are specified for object attachments, then, for objects with several attachments, the conditions will apply the following way:

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.

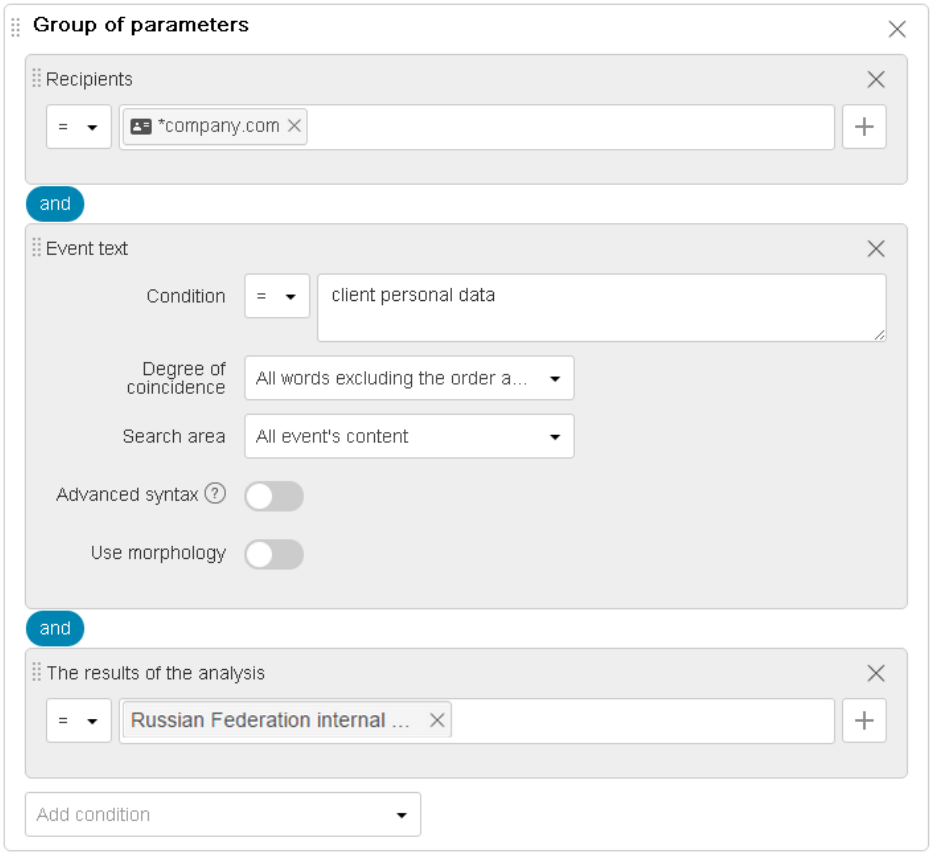


Example 3:
If you want the System to display events:

- are sent within the company;
- not containing the words *Client personal data* in the text of the event;
- contain pass numbers:

Create a query in the advanced mode and, within one group of parameters, specify the following attributes combined with the conjunction operation (see the picture below):

- `Recipients` - **company.com*;
- `Event text` - *“Client personal data”*; the search is performed in the *All words irrespective of their order and distance between words* mode and a negation parameter is applied to the attribute;
- `Search area` - *“All contents of event”*;
- `Results of analysis` - the text object *"Pass number"*.



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

- Editing Element;
- Deleting Element.

5.7.2.1.3 Using Advanced Syntax

Purpose:
Configure full-text search of events by using extended syntax.

Solution:

1. Switch to the advanced mode of the query creationю
2. On the **Condition** tab, in the **Add condition** drop-down list, select the **Event text** parameter.
3. Select **Advanced syntax**.
4. In the **Condition** field, enter search text using logical operators:"|","-", "!", "()" and others.
5. Specify other query parameters (for details, see "Query Creation in Advanced Mode").
6. Click **Save**.

Detailed information on query creation using logical operators you can find in the internet article about Search query language Sphinx.

Example:

If you want that the event text:

- contained words *“personal data”* and *“private data”*;
- did not contain the phrase *"confidential information"*,

create the following query using advanced syntax:

```
(personal | private) data - "confidential information"
```

5.7.2.2 Choosing Event Fields of View

Reference information:
By default the event tile (or table string - depending on chosen style) displays all event attributes.

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 the **Display fields** tab.
4. Move all target attributes to the right field and all unwanted ones - to the left (see "Display fields"):
    - 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.

5.7.2.3 Viewing Brief Event Form

Purpose:
To view a brief 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 the tile of a target event from the list (or a string of target event from the table).
4. To open the brief form, click ⌄ in the upper string of the right part of the workspace (to hide the brief form, click ⌃).
5. View the summary in the right part of the workspace.

See also:

- "Brief Event Viewing Form" - on displaying general information about the event.
- "Viewing Detailed Event Form" - on displaying advanced information about the event.

5.7.2.4 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 target event from the list (or a string of target event from the table). The right part of the workspace will display a brief event viewing form.
4. To open the detailed viewing form, click **Details** in the upper string of the right part of the workspace.
5. In the window that appears, view the detailed information about the event:
    - the **General information** tab displays the event attributes (for example, **Senders**, **Recipients**,**Tags**, **Policies**, **Sending date**, **Date of interception**);
    - the **Protected objects** tab displays protected objects detected in the event; triggered technologies, included in these protected objects; and catalogs to which the protected objects belonged at the time of interception.
    - the **Processing messages** tab displays errors that occurred during processing the event.
6. To view information on the tabs, click ⌄. To hide the information pane, click ⌃.
7. To close the detailed form, click **Close** or the standard close button in the upper right corner of the window.

See also:

- "Detailed Event Viewing Form“ - on the advanced event viewing form.
- "Viewing Brief Event Form“ - on displaying general information about the event.

5.7.3 Managing Dashboard Summaries

Purpose:
Create and view dashboard summaries.

Solution:
Includes the following actions:

Action	Description
Creating a summary	Creating an unloading on the configured dashboard
Viewing a Summary	Viewing files that contain the generated unloading in PDF or HTML

See also:

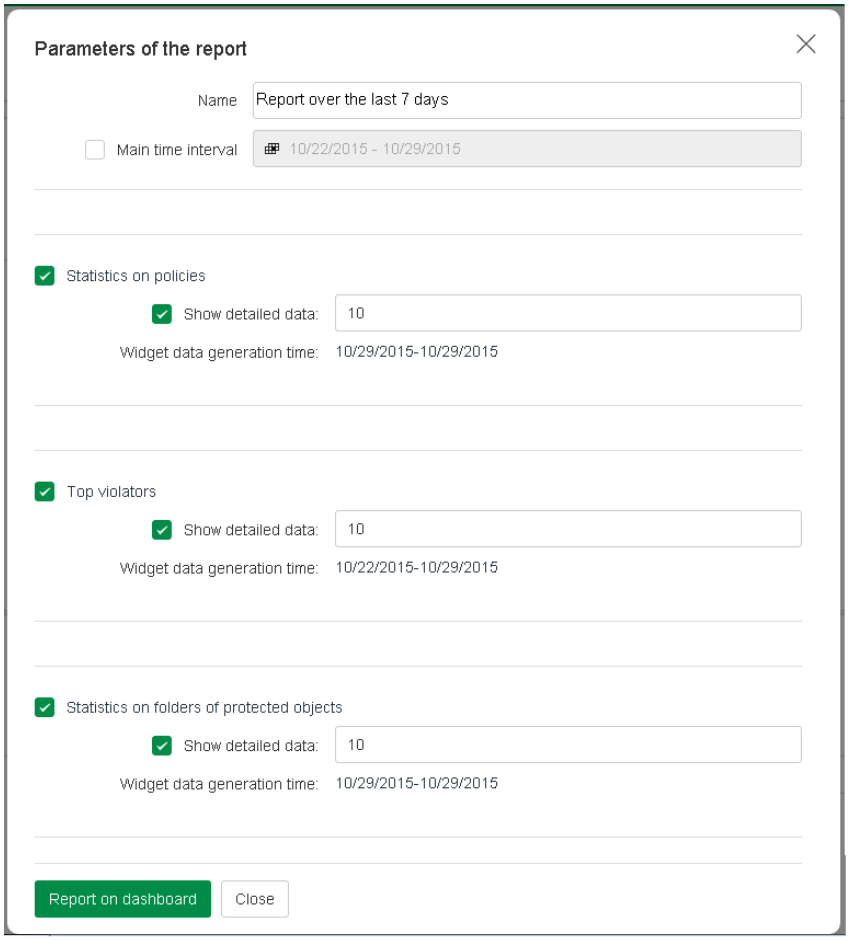
- "Dashboard summary" - on the section where managing summaries is performed

5.7.3.1 Creating a Summary

Purpose:
To create a dashboard summary for intercepted objects.

Solution:

1. Go to the **Dashboard** section.
2. In the right upper corner, click **Unload**.
3. In the window that opens, specify the summary attributes (see "Dashboard Summary").



4. Make sure that you have selected checkboxes of all widgets whose data you want to include in the summary.

Note:

The dashboard summary does not include data from the "Selection" widget.

5. If you want to manually specify the period, for which the summary 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 summary will be generated for the period specified in the widget properties.
6. Click **DReport on dashboard**.

In the upper right corner of the workspace, you can see information on the summary status.

Once the summary is generated, you will be prompted to openit in PDF or HTML format.

All created summaries are stored in the System and are available by clicking **View the list of summaries** in the right upper corner of the workspace. For details, see “Viewing Summary".

Note:

If you remove or modify a widget, then already created summaries, which contain that widget, will not be changed.

5.7.3.2 Viewing a Summary

Purpose:
View a created summary on intercepted objects.

Solution:
When the summary generation is complete, a message is displayed in the right upper corner of the workspace. In this message, you are offered to open the summary in PDF or HTML format.



Click on the **pfd** or **html** link to open the summary in a new browser window. You can also save, send or print the created summary by standard means of your browser and operating system.
All created summaries are stored in the System. To view the list of summaries, click the **View the list of summaries** button.

To view the list of summaries:

1. Go to the **Dashboard** section.
2. In the right upper corner of the workspace, click **View the list of summaries**.
3. The **Reports** window with the list of generated summaries will open. In the Report type column, next to the desired summary, click:
   - **PDF** - if you want to display the summary in PDF format;
   - **HTML** - if you want to display the summary in HTML format.

> **Note:**
>
> You can sort reports in the list by creation date or use the **Search** field to find the desired report by name.

4. A new browser tab will display the summary you have created.

5.7.4 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.

See also:

- "Retrospective data analysis, user decision on an object“ - on making user decision.

5.7.5 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 catalog

5.7.6 Saving Events (for SMTP mail)

Purpose:
Save interception object (SMTP-letter).

Solution:

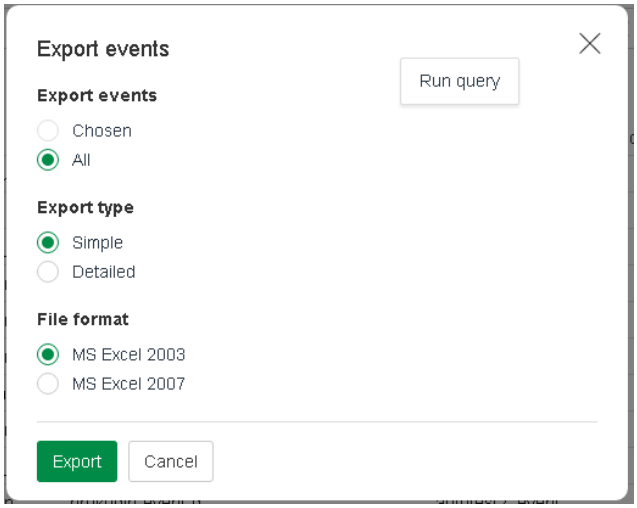
1. Go to the **Events** section.
2. Left-click the target event to select it.
3. In the brief event viewing form located in the right part of the workspace, click .
   The download process will start. When downloading is complete, you can open the event file and view its contents.

5.7.7 Event Export

Purpose:
Save information on events to the computer hard drive.

Solution:

1. Go to the **Events** section.
2. Click the table viewing form icon .
3. Run the query to retrieve objects.
4. Select the event you want to export. To select multiple events, use the Shift or Ctrl key.
   If you want to generate unloading for all available events, skip this item.
5. On the toolbar click  and in the drop-down list select **Export event**.
   The **Export events** dialog box will open.



6. Make sure that for the **Export event** parameter, the correct value is set: **Chosen**, if you want to export individual events, or **All**, if you want to generate unloading for all detected events.
7. Specify other export options: export type (Simple or Detailed) and export file format (MS Excel 2003 or MS Excel 2007).
8. Click **Export**.

When the operation is completed, in the upper right corner you will see a notification. To open the export file, click **download**.

5.7.8 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

5.8 Configuring System Response

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".

Reference information:
The System response determines actions performed by the System when detecting violations of the corporate security policy. These actions are specified in rules when creating data protection policies and person control policies.(see "Policies Section").There are also preset policies in the System (see “Default Policies").
During operation of the System, a situation may arise when analysis and decision-making subsystems cannot use 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 not assigned to the objects, and the **Processing messages** tab of the Detailed event viewing form displays messages about errors that occurred during processing (see "Detailed Event Viewing Form").

Why do you need to configure the System reactions:
When the corporate security policy is violated (e.g. sending a confidential document outside the company) or improper use of work time is detected (e.g. visiting entertaining Internet sites from the office computer), the System will perform:

- sending notifications to violators and informing the Management Console users;
- assigning verdict to the interception object;
- assigning a violation level, tags and a status to the interception object.

Configuring System response consists of the following actions:

Action	Description
Creating a data protection policy	Data protection policy is a set of rules of transporting, copying and placement. Allows you to specify actions that may lead to triggering policy rules.
Creating a person control policy	Allows you to specify the list of controlled persons whose actions may lead to triggering policy rules.
Creating a rule	Defining what is a violation of policy rules, and what actions will be done in the event of violation
Sending notifications on responded rule	If the rule is triggered, the System sends notification to specified Console users

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 managing the policies is performed

5.8.1 General Information on Policies

The section describes the order in which configured System policies (that is, the set of rules according to which analyses and processing objects is performed) are applied to events (intercepted objects of network traffic).

The System applies policies to events in the following order:

1. **The event is compared with all active policies one by one**
2. **If a policy is triggered on the event, 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 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)**

More information about accompanying processes see:

- Dividing events to sub-events
- Dividing rules to sub-rules
- Determining the priority sub-rule
- Order of actions applying according to the selected priority rules
- Example of policy application

5.8.1.1 Dividing events to sub-events

As a result of object processing the System assigns a number of attributes to this object (see “Object analysis and Decision on Object"). If any attribute of the event got multiple values (for example, multiple recipients of the SMTP messages, or correspondence of POST request text to multiple categories, etc.), the System treats this event as a collection of several sub-events with unique attribute values.
For example, if intercepted event has the following attributes:

Sender	Recipient	Protocol	Date
Person: Smith, Person: Johns	Person: Williams, Person: Johns, Person: Smith	Skype	09:23

then it is divided into the following sub-events:

Sender	Recipient	Protocol	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

5.8.1.2 Dividing rules to sub-rules

When applying the rules of the active policy, the dividing into sub-rules is also implemented to determine sub-rules with the highest priority.
To enable this, from all of the policy rules the System selects rules matching the intercepted event by the following attributes: ***Sender***, ***Recipient***, ***Protocol***, for example:

Sender	Direction	Recipient	Protocol	Date	Reaction
Group: Lawyers, The Person: Smith, Person: Johns	->	Group: Marketing, Person: Williams	SMTP	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
Group: Financial	-> <-	Group: Lawyers, Group: Sales			Notify: Miller Violation level: High

Then the System splits a rule into sub-rules for each sender-recipient pair. The two-way data transfer (for example, session messages in chat) is split with unification of direction:

Sender	Direction	Recipient	Protocol	Date	Reaction
Group: Lawyers	->	Group: Marketing	SMTP	08:00-20:00	Notify: Thomas Violation level: Low
Group: Lawyers	->	Person: Williams	SMTP	08:00-20:00	Notify: Thomas Violation level: Low
Person: Smith	->	Group: Marketing	SMTP	08:00-20:00	Notify: Thomas Violation level: Low

Sender	Direction	Recipient	Protocol	Date	Reaction
Person: Smith	->	Person: Williams	SMTP	08:00-20:00	Notify: Thomas Violation level: Low
Person: Johns	->	Group: Marketing	SMTP	08:00-20:00	Notify: Thomas Violation level: Low
Person: Johns	->	Person: Williams	SMTP	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
Group: Lawyers	->	Group: Financial			Notify: Miller Violation level: High
Group: Sales	->	Group: Financial			Notify: Miller Violation level: High

5.8.1.3 Determining the priority sub-rule

The priority of a rule is determined by (in descending order):

1. Priority sender-receiver pair;
2. Presence of conditions of time and protocol in the rule;
3. Presence of conditions of time in the rule;
4. Presence of conditions of protocol in the rule.

The priority sender-receiver pair is the one that has the highest total number of points of sender and recipient:

Sender/Recipient	Number of points
Contact	10000
Person	5000
Group	2500
Domain	1250
URL	600

Sender/Recipient	Number of points
List of resources	300
Deny List of resources	150
Deny URL	75
Deny Domain	35
Deny Group	15
Dena Person	7
Deny Contact	3
Any	1

For example, the rule with condition of forwarding from any sender to specific contact (10000 + 1 = 10001) is more priority one than the rule with condition of forwarding from particular person to a group of persons (5000 + 2500 = 7500).
If two or more rules have equal number of points for sender-recipient then the presence of conditions of time and protocol in the rule is taken into consideration. If in this respect these rules are equal too, then several high-priority rules with the same priority are selected.
If sub-event has no matching rules, then default rule is selected (see “Determining System Default Response").

5.8.1.4 Order of applying actions according to the selected priority rules

The system assigns the reaction by performing actions from selected priority rules in the following order:

1. All persons specified in selected rules are notified
2. All statuses specified in selected rules are assigned
3. The highest level of violation specified in the selected rules is assigned to the event
4. The event is deleted if deletion is specified in any rule (one rule is enough for deletion)
5. The event is deleted if deletion is specified in any rule (one rule is enough for deletion)
6. The event is blocked if any rule blocks the sending
7. All tags specified in selected rules are assigned to the event

5.8.1.5 Example:

Let the System have two policies:

Policy №1					
Catalogue of protected objects: Accounts					
Rule number	Sender	Recipient	Date	**Protocol**	Reaction

Policy №1					
1.1	Group: Sales Department	Group: Accounts Department	08:00-20:00	SMTP	Violation: None
1.2	Smith	Group: Accounts Department		SMTP	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	**Protocol**	Reaction
2.1	Group: Sales Department	<>Perimeter: Company	08:00-20:00	SMTP	Violation: None
2.2	Smith	<>Perimeter: Company		SMTP	Violation: None
2.3	Default:				Violation: None

Let Smith be a member of the "*Sales Department*" group. Johns belongs to the group "*Accounts Department*". E-mail `williams@mail.com` is outside the compony perimeter.
If there is an event:

Data	Sender	Recipient	Date	**Protocol**
Protected objects: Accounting, Contract	Smith	Johns, williams@mail.com	19:00	SMTP

This event consists of two sub-events, different "sender-receiver" 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 *Group of protected objects-Accounts*.
The "Smith->Johns" sub-event is considered:

Sender	Recipient	Date	**Protocol**
Smith	Johns	19:00	SMTP

This event has two sub-rules: №1.1 and 1.2. The more priority one is sub-rule №1. Therefore, the rule №1.2 is selected
The "Smith-> williams@mail.com" sub-event is considered:

Sender	Recipient	Date	**Protocol**
Smith	williams@mail.com	19:00	SMTP

This sub-event confirms to 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 *Group of protected objects-Contract.*
The "Smith->Johns" sub-event is considered:

Sender	Recipient	Date	**Protocol**
Smith	Johns	19:00	SMTP

This sub-event confirms to sub-rule №2.3 only. Therefore, the rule №2.3 is selected
The "Smith->williams@mail.com" sub-event is considered:

Sender	Recipient	Date	**Protocol**
Smith	williams@mail.com	19:00	SMTP

This event has two sub-rules: №2.1 and 2.2. The more priority one is sub-rule №1. Therefore the rule №2.2 is selected

3 The selected actions are applied : №1.2, №1.3, № 2.3, №2.2

5.8.2 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

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:
   ```
   service iwtm restart kicker
   ```

Then you need to create other policies anew (see "Creating Data Protection Policy" and "Creating Person Control Policy").

5.8.2.1 Data Protection Policy

By default the System contain one data protection policy for each preinstalled catalogue of protected objects (see the list of preinstalled catalogues at "Protected Objects Section").

Default policies have the following attribute values:

Attribute	**Value**
Policy name	<Name of the catalog of protected objects>

Attribute	Value
Status	Active
Period of activity	Not limited
Type of objects of research	<Name of the catalog of protected objects>

where <Name of the catalog of protected objects> is the name of the catalog for which the policy is created.

Each policy contains the following rules:

Rules of transfer

1. *The rule regulating transfer of confidential data outside the company perimeter*.
   If 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 the *High* value to the *Violation level* attribute of the event;
   - sets the *Under supervision* value to the attribute of the person who sends the traffic *Status*.
2. *The rule regulating the transfer of confidential data by heads of the company*.
   If 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

The rule regulating copying of confidential information to removable devices.

If employee copies the confidential data related to any category to removable device on any day of the week,
Then the System performs the following actions:

- sets the *High* value to the *Violation level* attribute of the event;
- sets the *Under supervision* value to the *Status* attribute of the person who sends the traffic.

5.8.2.2 Person Control Policy

By default the System has a persoin control policy with the following attribute values:

Attribute	Value
Policy name	Persons under supervision
Status	Active
Period of activity	Not limited
Statuses	Under supervision

5.8.2.2.1 Rule of transfer

The rule regulating transfer of data by person having the Under supervision status.

If the person having the *Under the supervision* status sends traffic of any type to any recipient,
Then the System will set the *To quarantine* value to the *Verdict* attribute of the event.

5.8.2.3 Policy Regulating the Transfer of Password-Protected Data

By default the System has a policy regulating transfer of password-protected data.

The default policy has the following attribute values:

Attribute	Value
Policy name	Password-protected data
Status	Active
Period of activity	Not limited
Protected data	Encrypted files of all formats

5.8.2.3.1 Policy rules

The rule regulating transfer of 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 *High* value to the *Violation level* attribute of the event
- assigns the *Under supervision* tag to the event.

5.8.2.4 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:

- Inappropriate Use of Resources
- Disloyal Employees
- Concealing Employees' Actions
- Suspicious Activity

5.8.2.4.1 Inappropriate Use of Resources

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	Inappropriate use of resources
Status	Active
Period of activity	Not limited
Protected data	Any data

5.8.2.4.1.1 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 the "Media", "Blogs", "Entertaining" or "Social networks" groups (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.

5.8.2.4.2 Disloyal Employees

By default the System has a policy that monitors activity 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

5.8.2.4.2.1 POLICY RULES

The rule of transfer that regulates sending requests to resources related to searching a job.

If a person sends a request to a web resource included in the "Job search" 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 *Medium* value to the *Violation level* attribute of the event.

5.8.2.4.3 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	Active
Period of activity	Not limited
Protected data	Any data

5.8.2.4.3.1 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 *Medium* value to the *Violation level* attribute of the event.

5.8.2.4.4 Suspicious Activity

By default, the System has a 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	Active
Period of activity	Not limited
Protected data	Any data

5.8.2.4.4.1 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", "Sites for adults" 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 *High* value to the *Violation level* attribute of the event
- set the *Under consideration* tag to the event.

5.8.3 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  and in the drop-down list select **Data Protection Policy**.
3. A new policy will be added to the **Data protection policies** group, and on the right side of the workspace a form of adding policy will be displayed.
4. To add protected data to the policy, click **Select**.
   If protected data are not selected, a policy for any data will be created.
5. In the window that appears, select the check boxes next to the items that you want to add, and then click **Add**. Protected data may include protected objects, their catalogs, and file formats.

> **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 would contain violations of each type.
>
> For example, a catalog 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 catalog and at least one file of the specified format.

6. In the right part of the workspace, fill the required fields (see “Policies and their Viewing Form"), and click **Save**.

Example 1:
If you want the System to respond to actions performed with data which form the *State secret* protected object:
Security Officer adds a data protection policy and specifies the *State secret* protected object as protected data.

Example 2:
If you want the System to respond to sending any data to a specified resource:

Security Officer adds a data protection policy, specifies the type of resource and the level of violation and adds no protected data.

Additional information:

- Policy editing is described in "Editing Policy".

- The policy is deleted by clicking the button located in the upper right corner of the tile and confirming the deletion in the opened window.

5.8.4 Creating Person Control Policy

Purpose:
Create a policy that determines the System reaction to actions of certain persons.

Solution:

1. Go to the **Policies** section.
2. In the left part of the workspace, click and in the drop-down list select **Person Control Policy**.
3. In the window that appears, select the check boxes next to the items that you want to add, and then click **Create**. Research objects may be:
    - individual persons (employees or workstations);
    - a group of persons and workstations;
    - persons and groups with the same status.

> **Note:**
> The policy is triggered when at least one object from each group is detected.

4. A new policy will be added to the group **Persons Control Policies**, and, on the right side of the workspace, a policy viewing form will be displayed.
5. On the policy form, fill in the required fields (see "Policies and their Viewing Form"), and click **Save**.

You can also add a policy for a selected person, workstation or group directly from the **Persons** section. To do this:

1. Go to the **Persons** section.
2. Select the desired person, workstation or group.
3. On the toolbar in the right part of the workspace, click and, in the drop-down list, select **Create policy**.

Example:
If you want to control the person *Smith* (assumes that this person has already been created in **Persons** section) so that intercepted objects with *High* violation level, which are sent by Smith, would be assigned the verdict *Allow*, Smith would be assigned the *Under supervision* status and the user with the mailbox *example@company.com* would be notified about the incident:

go to the **Policies** section and create a person control policy named *Smith*. Then create a rule for the policy *Smith* and set the following values for the attributes:

- attribute **Intercept with the violation level** - *High* value;
- attribute **Send notification** - *example@company.com* value (for details, see “Sending Notifications on Responded Rule");

- attribute **Assign verdict** - *Allow* value;
- attribute **Set status** - *Under supervision* value.

Additional information:

- Rules editing is described in "Editing Policy".
- The policy is deleted by clicking ✕ button located in the upper right corner of the tile and confirming the deletion in the opened window.

5.8.5 Editing Policy

Purpose:
Change attributes of the created policy.

Solution:

1. Go to the **Policies** section.
2. In the left part of the workspace, left-click the target policy.
3. In the right part of the workspace, fill the required fields (see “Policies and their Viewing Form").
4. To change the list of protected data or controlled persons, in the **Protected data** block (for data protection policies) or **Controlled persons** (for person control policies), click **Select** and edit the list.
5. When you make all required changes, click **Save** in the policy edit form.

5.8.6 Creating Rules

Reference information:
For each **data protection policy** you can configure one or more rules:

- object transferring;
- object copying;
- object placement.

If the policy is triggered on the interception, there are following options, depending on the number of triggered rules:

- If one rule is triggered, the System performs the actions specified in this rule.
- If several rules are triggered and
    - their actions contradict each other, the System selects the priority action and executes it (on the order of priorities selecting see “General Information on Policies");
    - their actions do not contradict each other, the System performs all actions that do not contradict the other ones.
- If no rule is not triggered or rules are not specified, then the System performs the actions specified for the default rule (see “Determining System Default Response").

For each **persons control policies** you can configure rules for intercepting events with the specified violation level. You can also link the rule with data protection policies that are present in the System.

Note:

If the interception triggers multiple policies, each of which has its own rules, the System chooses the action with the highest priority and executes it (on the order of selecting priorities, see. "General Information on Policies"); actions that do not contradict each other are performed in full.

Purpose:
Determine what actions with protected data cause reaction of the System and how the System should respond to these actions.

Solution:

1. Go to the **Policies** section.
2. Add a rule in one of the following ways:
    - Left-click the target data protection policy, and in the left part of the policy tile, select the desired tab (**transfer**, **copying** or **placement**) depending on the needed task and click **Add rule**.
    - Left-click the target policy and then on the right part of the workspace, click **Add rule** and from the drop-down list, select the desired rule.
3. Configure the rule by using a form on the right part of the workspace (see “Rules and their Viewing Form").
4. In the **Actions when the rule is triggered** block, on the rule viewing form, specify which actions the System should perform in the rule is triggered.

Example:

If you want that in case of transferring files which are included in the *Strictly confidential* protected object on Saturdays and Sundays, the System would assign the *Sending confidential data on weekends* tag to the event and set the *Medium* violation level:
Perform the following actions:

1. create a *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. create a rule of transferring by assigning the **Days of rule activity** attribute the *Saturday* and *Sunday* values*;*
4. in the **Actions when the rule is triggered** block, assign the following values to attributes:
    - attribute **Set violation level** - *Medium* value;
    - attribute **Tags** - *Sending confidential data on weekends* value.

Additional information:

- Editing rules is described in "Editing Rules".
- Deleting rules is performed by clicking ✕ button located in the upper right corner of the tile and confirming the deletion in the opened window.

5.8.7 Editing Rules

Purpose:
Edit a previously created rule.

Solution:

1. Go to the **Policies** section.
2. On the left side of the workspace left-click the target policy.
3. In a policy tile, select a target group of rules (**transfer**, **copying** or **placement** tabs for the data protection policy or the **Rules** tab for the persons control policies).
4. The policy tile will display the list of policy rules of the selected group. By clicking the left mouse button, select the desired rule in the list.
5. On the right part of the workspace, the rule editing form will open. Modify required fields (see "Rules and their Viewing Form"), and click **Save**.

5.8.8 Determining System Response to Policy Violations

Reference information:
For each policy, you can specify actions performed by the System in case of rule violation:
Available actions are determined by the rule type:

Action	**Data protection policies**			**Person control policies**
	Transfer rule	**Copy rule**	**Placement rule**	**Person control rule**
Send notification	Available	Available	Available	Available
Notify sender	Available for the "Email" event type only	Not available	Not available	Not available
Assign verdict to event	Available	Not available	Not available	Available
Assign violation level to event	Available	Available	Available	Available
Assign tags to event	Available	Available	Available	Available
Assign status to senders	Available	Available	Available	Available
Delete event	Available	Available	Available	Available

A detailed description of actions:

Action	Description
Send notification	Specified Console users will be notified via email. The list may contain users or their email addresses.
Notify sender	The sender of an intercepted email message will receive a notification

Action	Description
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** - 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 and Configuration Guid*e".
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.

Purpose:

Determine the System response in case the policy rules are violated.

Solution:

1. Go to the **Policies** section.
2. On the left part of the workspace, left-click the target policy.
3. In the policy tile, click on the link with a required group of rules (**Transfer**, **Copy** or **Placement** for data protection policies or **Rules** for person control policies).
4. Left-click a required rule to select it in the list or click **Add rule** to create a new rule (see "Creating a Rule").
5. On the right part of the workspace, in the **Actions** block, specify what action the System should perform if the rule is triggered.
6. Click **Save**.

See also:

- "Editing Rules"- on modifying earlier created rules

5.8.9 Determining System Default Response

Reference information:
If after applying the policy, there are sub-events left which do not have 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 was triggered, the data protection policy will not be triggered on this interception object either.

Purpose:

Determine how the System should respond if an event contains a sub-event to which neither of the policy rules matches.

> **Note:**
>
> Default actions can be specified for data protection policy only.

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 a target tab (**transfer**, **copying** or **placement**) depending on the needed task and left-click the lower part of the tile:



4. In the right part of the workspace edit the needed fields in the single **Actions** block (see "Rules and their Viewing Form"), and click **Save**.

Additional information:

For web-message and web-mail event types, a false triggering of default rule may occur. Such a situation may arise when:

A rule regulating data transfer from person A to person B is created in the System. If person A sends data to person B via 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, default actions are executed.

To avoid false triggering of a default rule for web-message and webmail event types, do either of the following:

- in the tranfer rule attributes, add the website domain or a list of websites that can be used for data transfer;
- do not specify default actions.

200

Example:

You need the System to assign the *Under supervision* status to the person card if no rules of copying are triggered when transferring files which form a *State secret* protected object.
In this case, the Security officer performs the following actions:

1. Creates a data protection policy for the protected object *State secret* (see "Creating a Policy"),
2. Starts configuring default policy actions,
3. In the only **Actions** section, sets the **Under supervision** value to the **Set status** attribute.

5.8.10 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. Specify filtering criteria in one of the fields or in both of them:
    - **Filter by policy name** - start typing and select the name of 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)
4. Click **Save**.

5.8.11 Sending Notifications on Responded Rule

Purpose:
Configure sending automatic notification about responded rule to some users.

> **Warning!**
>
> To send notifications, you can only use e-mail address. When you choose the existing contacts, select user entries with specified e-mail address only.

Solution:

1. Go to the **Policies** section.
2. On the left side of the workspace left-click the target policy.
3. In a policy tile, select the desired tab (**transfer**, **copying** or **placement**) and left-click the target rule from the rule list.
4. The policy tile will display the list of rules of the selected group. By clicking the left mouse button, select the desired rule in the list.
5. In the right part of the workspace, in the **Send notification** field, specify a contact of the Management Console user. To do this, start typing the contact details and select the desired entry from the drop-down list.

Note:

If after the rule is created, the user or his e-mail are deleted from the System (on managing with user accounts, see *"Administration Guide"*, "Users" section), a notification will not be sent to this user.

Example:

If you need that in case of copying confidential data (protected object -*Trade_Secret*) to a removable device, the System would:

- assign the *Allow* verdict to the interception object
- assign the *Under supervision* status
- notify the user with *example@company.com* mailbox about the incident

Create a data protection policy for the *Trade_Secret* protected object. Then create a rule of copying for this policy and assigns the following values to the attributes:

- **Days of rule activity** attribute - *Saturday* and *Sunday* value
- **Devices** attribute - *Removable devices* or *Printers or removable devices* value
- **Send notification** attribute - *example@company.com* value
- **Assign verdict** attribute - *Allow* value

5.9 Managing Reports

What for do you need reports?

In contrast to the brief statistical information provided in the section "Dashboard", reports allow you to perform a more flexible configuration of statistical parameters to demonstrate the results of the System functioning for a specified period of time.

Includes the following actions:

Action	Description
Creating a folder with reports	Create a folder that contains reports
Creating a report	Generating reports with statistical information
Managing widgets	Specifying the search parameters and how to graphically display data in a report
Managing ready reports	Viewing report execution history which provides the ability to remove unneeded versions of the report, or to save report data to a file

See also:

- "Reports Section" - on the section where managing reports is performed

5.9.1 Creating a Folder with Reports

Purpose:
Create a folder for grouping reports with a common theme.

Solution:

1. Go to the **Reports** section.
2. On the toolbar in the left part of the workspace, click + and, in the drop-down list, select **Create folder**.
3. In the window that appears, specify the folder name and access parameters (for more information, see "Report Folder Creation Form").
4. Click **Save folder**.

You can also copy a previously created folder and its reports. To do this:

1. Select the folder in the list using the left mouse button
2. In the window of folder properties that appears, click **Copy**.
3. The folder copy will be added to the folder structure at the same level as the folder being copied.

You can change the location of the folder using drag and drop. To do this, select the folder in the list, press the left mouse button and move the folder to the desired location holding the left mouse button pressed. Then release the mouse button.

Additional information:

Editing and deleting reports are performed by standard means:

- Editing folder is performed by standard means (see "Editing Element").
- Deleting a folder is performed by standard means (see "Deleting Element").

5.9.2 Creating a Report

Purpose:
Create a report that contains statistical data on interception objects.

Solution:

1. Go to the **Reports** section.
2. In the left part of the workspace, select a folder in which you want to create a report, or create a new folder (for details, see "Creating a folder with reports").
3. On the toolbar, click + and in the drop-down list select **Create report**.
4. In the window that appears, specify required settings (for more information, see "Report Creation Window").
5. Click **Add widget**.
6. In the **Widget Creation** window that opens, specify the widget parameters (for details, see “Managing widgets of reports").
7. Click:
    a. **Save** - to save the report.

b. **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**).
3. The copy will be added to the report structure at the same level as the report being 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.

Additional information:

Editing and deleting reports are performed by standard means:

- Editing a report is performed by standard means (see "Editing Element"). Apart from button located on the toolbar, you can also use the **Edit** in the left part of the workspace;
- Deleting a report is performed by standard means (see "Deleting Element"). Apart from button located on the toolbar, you can delete the report by clicking in the right part of the workspace and selecting **Delete**.

5.9.3 Managing Widgets of Reports

Working with widgets includes the following actions:

Action	Description
Creating and Configuring Widget	To specify how to display statistical data and which filtering criteria to use, you need to create and configure the widget
Editing Widget	To edit the widget, switch to the report edit mode, in the upper-right corner of the desired widget click and in the drop-down list select **Edit**.
Duplicating Widget	To duplicate the widget, switch to the report edit mode, in the upper-right corner of the desired widget click and in the drop-down list select **Duplicate**. In the report list in the left side of the workspace, select the report to which you want to duplicate a widget.

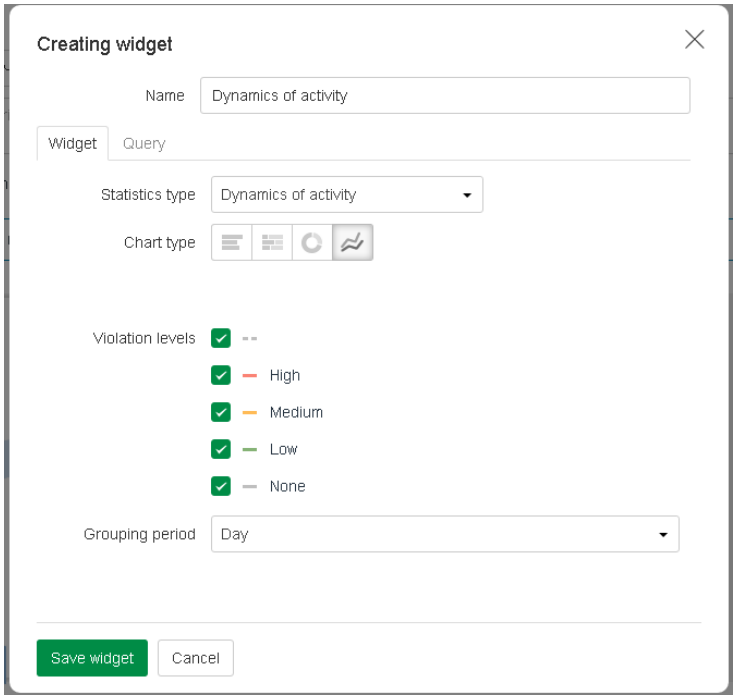
Action	Description
Deleting widget	To delete the widget, switch to the report edit mode, in the upper-right corner of the desired widget click ▾ and in the drop-down list select **Delete**.

5.9.3.1 Creating and Configuring Widget

Purpose:
Create a widget for the selected report and configure its settings.

Solution:

1. Go to the **Reports** section.
2. Select the desired report and switch to the edit mode, or create a new report (for more details, see "Creating a report").
3. In the right part of the workspace, 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"). To copy parameters from a query that was created in the Events section, click Copy query and in the drop-down list select the desired query.

5. Click **Save Widget**.

5.9.4 Managing Ready Reports

Includes the following actions:

- viewing the report execution history:
- view a selected version of the report;
- deleting selected records;
- saving the report to a file.

To view report execution data:

1. Go to the **Reports** section.
2. In the right part of the workspace, click  and, in the drop-down list, select **Report execution history**. In the dialog box that appears, you can view data about the report execution (for details see "Report Execution History").
3. To add a comment to a selected report version, double-click the **Comment** field opposite the selected version and enter the comment.

To view and edit the selected versions of the report:

1. To open the report for a specific date, left-click on the desired date of execution. A list of widgets, which display results of the report execution for the selected date, will open.
2. If you want to go to the "Events" section and view the events represented in the widget, in the upper-right corner of the selected widget, click and, from the drop-down list, select **Go to events**.

To delete selected versions of the report:

1. Select the report versions that you want to delete. To do this, select the check boxes in required rows. To select all rows at once, select the check box in the header field.
2. Click **Delete**.

To save the report:

1. Select the report versions which you want to save to a file. To do this, select the check boxes in required rows. To select all rows at once, select the check box in the header field.
2. Click **Export** and, in the drop-down list, choose the save format. You can save the report in one of the following formats: Excel 2007, Excel 2003, PDF, or HTML. File in the specified format will be saved to your computer.

> **Note:**
>
> To save the current version of the report, in the upper right corner of the workspace, click  and, in the drop-down list, under the **Report export** caption, choose the format in which you want to save the file. File in the specified format will be saved to your computer.

6 LICENSING INFORMATION

The licensing information for the System is contained in the following topics:

- End-User License Agreement
- Third-Party Licenses

6.1 End-User License Agreement

IMPORTANT! Read this End-User License Agreement (EULA) carefully before using the Software.

Clicking the Accept button in the License Agreement box at installation time or any use of the installed Software will signify your irrevocable acceptance of the terms and conditions of this EULA. If you do not accept the terms and conditions of this EULA, You should terminate the installation process and/or the use of the Software.

6.1.1 License Agreement

This End-User Licence Agreement (“Agreement”) is a joinder agreement between InfoWatch (“Rightholder”) and you, a person or legal entity (“User”), legally possessing a copy of InfoWatch Traffic Monitor (“System”).
The System is designed for monitoring, filtering, and the prevention of leaks of data transferred beyond the company frontiers through Right holder, Internet or Internet pagers as well as for network and local printing. The System also allows you to control access to ports and monitor data copied to removable storage devices.

6.1.1.1 1. Definitions

1.1. “Software” means, in whole or in part, the System, the accompanying documentation, and optionally ordered updates to the System, copyrighted by “InfoWatch”.
1.2. Computer” means the hardware that the Software is designed for and where the System will be installed and/or used.
1.3. User (You) means a person or legal entity that installs the Software on its behalf and legally possesses a copy of the Software. If the Software has been downloaded or acquired on behalf of a legal entity, the term "User" (you) means the legal entity for which the Software was downloaded or acquired and that an authorized person accepts the terms and conditions of this Agreement on its behalf.
1.4. "Partners" means the organizations distributing the Software under the agreement with the Rightholder.
1.5. "System Documentation" means the accompanying printed and other materials, User Guide, Administrator Guide, reference book, help file, and similar System-related printed and electronic documents copyrighted by "InfoWatch".

6.1.1.2 2. Grant of License

2.1. The Rightholder grants you a non-exclusive license to use the Software within the functionality as described in the System Documentation provided that you meet all the technical requirements specified in the System Documentation, as well as all the restrictions and terms of use of the System specified in this Agreement.
2.2. Unless otherwise specified, if you have received, downloaded, or installed an evaluation version of the Software, you may use the Software only for evaluation purposes within one evaluation period starting with the software installation date. Any use of the Software for other purposes or after the evaluation period expires is prohibited.
2.3. Unless otherwise specified in the license agreement, if you are using different versions of the Software or versions for different languages, if you have received the Software on several media or otherwise possess several copies of the Software, or if you have received the Software as part of some other software, the total number of your computers where all the versions are installed and/or used must correspond to the number of licenses procured from the Rightholder. Each purchased license gives you the right to install and use the System on a certain number of computers or for a certain number of licensed objects, as set forth in Clause 2.2.
2.4. The User has the right to make a single copy of the Software, provided that this copy is only used for archive purposes or for the replacement of a duly purchased Software copy, should the original be lost, destroyed, or become unusable. This copy cannot be used for any other purposes and must be destroyed, if the User's right to use the Software becomes invalid.
2.5. Any legal transfer of rights for the use of the Software is only possible after entering this Agreement and upon prior consent of the Rightholder or its authorized Partner. The successor of the rights for the use of the Software then becomes a legal successor of the User, provided that the User under this Agreement is fully replaced.
2.6. You are fully responsible for compliance with all applicable export and import laws and regulations as well as trade sanctions and embargoes concerning the transfer of rights for the use of the Software.

6.1.1.3 3. Restrictions

3.1. You shall not decompile, disassemble, or modify the Software as well as produce derived works on its basis, in whole or in part, unless it is allowed by law.
3.2. You shall not transfer or assign your rights to use the Software to any third party except as set forth in Clause 2.6.
3.3. You shall not transfer or provide access to the license key to any third parties except for as set forth in Clause.2.6 of this Agreement. Any other transfer of rights will be considered a violation of this Agreement. A license key is considered confidential information. The Rightholder reserves the right to verify the validity of your license key with the available means.
3.4. You shall not rent, lease, or lend the Software to any third parties or disclose the results of the benchmark testing of the System.
3.5. The Rightholder has the right to block the license key, should the User breach any of the terms or conditions of this Agreement.
3.6. If you are using an evaluation version of the Software, you shall not transfer your copy of the Software to any third party.
3.7. Any violation of the intellectual property rights on the Software will result in civil, administrative, or criminal responsibility under the applicable law.
3.8. You shall not use the Software for any purposes or in any ways restricted or prohibited by the applicable law. You are fully responsible for any unauthorized use of the Software.
3.9. Should you violate any terms or conditions of this Agreement, the Rightholder has the right to terminate this Agreement for the use of the Software at any time without notice or any refund of the cost of the Software full or partial.

6.1.1.4 4. Limited Warranty and Disclaimer

4.1. The Rightholder guarantees that the Software will substantially perform according to the description in the System Documentation.
4.2. You agree that no software is free of errors and are recommended to back up your files regularly.
4.3. The Rightholder does not guarantee proper Software operation if any requirements described in the System Documentation or any terms and conditions of this Agreement are violated by the User.
4.4. EXCEPT AS SET FORTH IN THIS LIMITED WARRANTY, THE SOFTWARE IS PROVIDED "AS IS". THE RIGHTHOLDER OR ITS PARTNERS GIVE NO WARRANTY AS TO ITS USE OR PERFORMANCE. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE RIGHTHOLDER AND ITS PARTNERS MAKE NO WARRANTY, CONDITION, OR REPRESENTATION, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, NON-INFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABILITY, SATISFACTORY QUALITY, INTEGRATION, OR FITNESS FOR A PARTICULAR PURPOSE. YOU ASSUME FULL RESPONSIBILITY FOR SELECTING THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS FOR THE INSTALLATION AND USE OF THE SOFTWARE AND FOR THE RESULTS OBTAINED WITH THE SOFTWARE.

6.1.1.5 5. Limitation of Liability

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE RIGHTHOLDER AND/OR ITS PARTNERS BE LIABLE FOR ANY DAMAGES (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION, LOSS OF INFORMATION, ETC.) IN CONNECTION WITH THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF THE RIGHTHOLDER OR ITS PARTNERS WERE ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN ANY CASE, THE LIABILITY OF THE RIGHTHOLDER OR ITS PARTNERS IN CONNECTION WITH ANY PROVISION OF THIS AGREEMENT IS LIMITED BY THE COST OF THE SOFTWARE, ACTUALLY PAID BY YOU. THESE RESTRICTIONS MAY NOT BE EXCLUDED OR LIMITED UNDER APPLICABLE LAW.

6.1.1.6 6. Software Products

6.1. Any third party technologies the use of which within the Software is necessary or reasonable are specified in the System Documentation. Such a technology is licensed to the end user on the terms and conditions of a license agreement with the third party, specified in the System Documentation. This license agreement with the third party is included in this Agreement by reference.
6.2. The software products making part of the System are only licensed for limited use within the System. When the license agreement for the use of the Software expires, the User must destroy all the copies of the Software.

6.1.1.7 7. Open Source (Free) Software

This product may contain programs that are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or other similar free software/open source licenses which among other rights permit the user to copy, modify, and redistribute certain programs, or portions thereof, and have access to the source code ("Open Source Software"). If such licenses require that for any software distributed in an executable binary format, the source code should also be made available to the user, such source code should be obtained by sending a query to the Rightholder or supplied with the product. If any Open Source Software licenses require that the Rightholder provide rights to use, copy, or modify an Open Source Software program beyond the rights granted in this Agreement, then such rights take precedence over the rights and restrictions in this Agreement.

6.1.1.8 8. Intellectual Property Rights

8.1. You agree that the Software, documentation, other copyright matter, any systems, ideas, methods of operation, documentation, and other information contained in the Software as well as the trademarks are the intellectual property of the Rightholder or its Partners. This Agreement does not grant you any rights to the intellectual property including any trademarks or service marks of the Rightholder or its Partners except for the rights provided by this Agreement.
8.2. You agree that the source code and the license key for the Software are the intellectual property of the Rightholder and its Partners.
8.3. You may not delete or modify any copyright or other proprietary notices on any copy of the Software.

6.1.1.9 9. Rightholder Contact Information

"InfoWatch"
Phone/fax:+7 (495) 229-00-22
Sales department:sales@infowatch.com
Technical support service:support@infowatch.com
Website:http://infowatch.com/

6.2 Third-Party Licenses

The system contains third-party components distributed under the MIT License (http://www.opensource.org/licenses/mit-license.html):

- Lua - http://www.lua.org/license.html
- LuaBind – http://www.rasterbar.com/products/luabind.html
- libxml2 – http://www.xmlsoft.org/

The system also contains software:

- distributed under the terms of the BSD Licenses (http://www.opensource.org/licenses/bsd-license.php):
    - Stringencoders – http://code.google.com/p/stringencoders/
- distributed under the GNU GENERAL PUBLIC LICENSE (http://www.gnu.org/licenses/gpl-2.0.html):
    - - Pdftotext – http://www.foolabs.com/xpdf/
    - - Tnef – http://sourceforge.net/projects/tnef/
    - - Unzip – http://www.info-zip.org/UnZip.html
    - - libcole.so – arturo@directmail.org; andy.scriven@research.natpower.co.uk
    - - libhtmltree.so – pauljlucas@mac.com

7 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
Attachment	File attached to the intercepted event at any nesting level. See also: Event
Audit	Controlling of acrions 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, workstations and groups	Information about users, workstations, groups of users, and groups of workstations imported from Active Directory and 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 caregory which this term belongs to. Old synonyms: Classifier, CFB. See also: Event, Term, Category, Technologies, Protected object
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 mobile device or terminal device. See also: Workstation, Mobile device, Terminal device
Configuration	A group of settings required to check events for data monitoring and analyzing. See also: Event, Tchnologies, 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

Term	Glossary
Controlled persons	Set of persons, groups of persons and person's statuses which detection in the event results in assotiating this event to the person control policy which defines this set. See also: Persons, Persons group, Persons 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, printing and photographing 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
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
DeviceLock	Data loss prevention (DLP) system providing endpoint device/port control and data leak prevention
DeviceLock Adapter	IW DM interceptor that integrates with DeviceLock; it intercepts the shadow copies of the files copied to the removable devices. See also: IW DM, Shadow copy of a file, Interceptor
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.

Term	Glossary
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
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 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.
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) or TM Groups (created using IW TM). 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
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 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.

Term	Glossary
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, photo) and intercepting messengers traffic (Skype, Gtalk, Yahoo, Mail.ru Agent 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, YMSG, ICQ, NRPC) and shadow copies of the data copied to the removable media and sent to printing.
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.
License	Right to the System usage. Gained when bying the System and defines available users number, used technolodies 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 mails to IW TM for analysis. See also: Interceptor
Lotus Domino	IBM mail server which messages are intercepted by Lotus Adapter.
Mail.Ru Agent	An instant messaging service supporting IP telephony, video calls and SMS sending
Management Console	A graphical user interface. Designed to manage the System (administration, configuring settings, event analysis, 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.
MMP	The protocol of connection between Mail.Ru Agent and general Mail.Ru network
Mobile device	Computer type: smartphone or tablet PC with OS of Android or Windows Phone or iOS family. See also: Computer
Monitor	See: Interceptor
Morphology	Term setting: if morphology is used, the text search will detect all word forms of this term. See also: Term

Term	Glossary
MS Lync	Microsoft instant messaging clients for corporate environments.
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
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, persons groups and person statuses. See also: Policy, Persons control rule, Person, Person status
Persons control rule	Rule that assigns attributes to the event of specified violation level and which senders or recepients 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, Persons control policy
Placement rule	The rule that regulates storing protected data. See also: Rule, Protected data, Data protection policy, Crawler
Policy	A set of rules according to which the event analysis and processing facilities are performed. See also: Policy, Active policy, Rule
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 accept 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
Protected data	A set of protected objects, their catalogues and file formats which detection in the event allows to characterize this event as falled 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

Term	Glossary
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 procent 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, Persons control rule, Copy rule, Transfer rule, Placement rule
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
Scan task	Operation (single or repeated) of checking target storage locations (Microsoft SharePoint storage, local drives of workstations, shared network resources) if they store technology elements. See also: Crawler, Scanner, Tecnology element
Scanner	Crawler service whicn checks files in the corporate nerwork if they violate the corporate security policy. See also: Crawler, Corporate security policy
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.
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

Term	Glossary
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 convienent analysus and activity control and to display them on dasboards and reports with special color indicating. See also: Persons, Computers, Dasboard, 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
Task	See Scan task
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.
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 cards numbers) . See also: Tecnologies, 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.
User role	A set of privileges that define a set of actions available for the user. See also: Administrator, Security officer, Management Console, Privilege

Term	Glossary
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 color 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 criterias 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
WhatsApp	Messenger for smartphones that allows you to send text messages, images, audio and video files; as well as the protocol used in it.
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
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 middle-ware based on XML.
Yahoo	System for fast messages and information exchange based on open YMSG protocol.