

INFOWATCH

InfoWatch Traffic Monitor 5.5

User Guide

INFOWATCH TRAFFIC MONITOR 5.5

User Guide

© ZAO “InfoWatch”
Tel/fax +7 (495) 229-00-22
http://www.infowatch.com
Last edited: March 2015

Contents

Part I Introduction 9

1.1 Glossary 9

1.2 Additional Documentation 14

Part II InfoWatch Traffic Monitor Overview 15

2.1 Object Interception and Analysis 16

2.1.1 Object Interception 17

2.1.2 InfoWatch Traffic Monitor Transport Modes 18

2.1.3 Object Analysis and Verdict 19

2.1.4 Uploading Object into Database 20

2.1.5 Retrospective Data Analysis, User Decision on anObject 21

2.1.6 Specific Features of Blocking HTTP and HTTPS-queries and Messages Sent Through Web-services

Part III Management Console: General Information 22

3.1 System Operation Before Configuring 23

3.2 Configuring the System 24

3.3 Refreshing Data in Management Console 25

Part IV Management Console Interface 25

4.1 Management Console Window 28

4.2 Dashboard Section 29

4.2.1 Dashboards 31

4.2.2 Widgets 31

4.2.2.1 Dynamics of threats over period 32

4.2.2.2 Top violators 33

4.2.2.3 Quantity of threats over period of time 34

4.2.2.4 Selection 35

4.2.2.5 Dynamics of statuses over period 36

4.2.2.6 Policy statistics 37

4.2.2.7 Category statistics 38

4.2.3 Dashboard Report 39

4.3 Events Section 40
4.3.1 Queries 41
4.3.1.1 Condition 43
4.3.1.2 Display Fields 46
4.3.1.3 Access Parameters 46
4.3.1.4 Extended Mode 47
4.3.2 Objects of Interception 49
4.3.2.1 Event Tile 51
4.3.2.2 Short Event Viewing Form 52
4.3.2.3 Detailed Form of Events Viewing 53
4.3.3 Export Events 54
4.4 Classifier Section 56
4.4.1 Categories 57
4.4.2 Terms 59
4.4.3 Text Objects and their Values 60
4.4.4 Sample Documents 62
4.4.5 Sample Forms 63
4.4.6 Sample Stamps 64
4.4.7 Sample Database Uploadings 65
4.5 Files Section 66
4.6 Persons Section 67
4.6.1 Groups of Persons and Workstations 68
4.6.2 Persons 69
4.6.3 Workstations 71
4.7 Policies Section 72
4.7.1 Policies and their Viewing Form 73
4.7.2 Rules and their Viewing Form 74
4.7.3 Form of Filter Settings 78
4.7.4 Form of Adding a Policy 78
4.8 Lists Section 79
4.8.1 Tags 80
4.8.2 Resources Lists 80

4.8.3 Statuses 81
4.8.4 Perimeters 82
4.9 Crawler Section 83
4.9.1 Scanner 85
4.9.2 Scanning Jobs 87
4.9.3 Launch History 90
Part V Cases Solving 91
5.1 Typical Actions 92
5.1.1 Log In and Log Out the Management Console 92
5.1.2 Applying the System Configuration 93
5.1.3 Creating an Element 94
5.1.4 Editing the Element 95
5.1.5 Deleting the Element 95
5.1.6 Pages Navigation 96
5.1.7 Changing User's Password 96
5.1.8 Selecting Interface Language 97
5.1.9 Calling Help File 97
5.1.10 Viewing Information on System 98
5.2 Managing Persons and Workstations 98
5.2.1 Creating a Group of Persons and Workstations 99
5.2.2 Creating a List of Persons and Workstations 100
5.2.3 Viewing Person's or Workstation's Events 100
5.2.4 Viewing Person's or Workstation's Summary 101
5.2.5 Adding a Person or Workstation to Data Protection Policy 101
5.2.6 Adding a Status to Person or Workstation 102
5.2.7 Adding a Person or Workstation to Perimeter 103
5.2.8 Configuring Person's Card 103
5.2.8.1 Adding a Contact to Person 104
5.2.8.2 Adding a Workstation to Person 104
5.2.8.3 Adding a Person to Group 105
5.2.9 Configuring Workstation's Card 105
5.2.9.1 Adding IP or DNS to Workstation 105

5.2.9.2 Adding Person to Workstation 106
5.2.9.3 Adding Workstation to Group 106
5.3 Configuring the Analysis of Employees Actions 107
5.3.1 Defining the Confidential Information 108
5.3.1.1 Creating Classifier Base 108
5.3.1.2 Grouping the Confidential Data by Subject Areas 109
5.3.1.3 Defining the Confidential Data 109
5.3.1.3.1Creating Terms 111
5.3.1.3.2Creating Text Objects and their Values 112
5.3.1.3.3Creating Sample Documents 116
5.3.1.3.4Creating Sample Forms 117
5.3.1.3.5Creating Sample Stamps 117
5.3.1.3.6Creating Sample Database Uploadings 118
5.3.1.4 Enabling and Disabling the Analysis on Subject Areas 121
5.3.1.5 Enabling and Disabling the Analysis on Confidential Data 121
5.3.1.6 Exporting and Importing the Classifier Database 122
5.3.2 Specifying Inappropriate Resources 123
5.4 Configuring System Response 124
5.4.1 Default Policies 126
5.4.1.1 Data Protection Policy 126
5.4.1.2 Control of Persons Policy 127
5.4.1.3 Policy Regulating the Transfer of Password-Protected Data 127
5.4.1.4 Policy Regulating the Transfer of Data Proceeded with Error 128
5.4.2 General Information on Policies 129
5.4.3 Creating a Policy 133
5.4.4 Editing Policy 134
5.4.5 Creating a Rule 134
5.4.6 Editing Rules 135
5.4.7 Determining System Response to Policy Violations 136
5.4.8 Determining System Default Response 136
5.4.9 Filtering a List of Policies 137
5.4.10 Sending Notifications on Responded Rule 138

5.5 Managing Interception Objects 139
5.5.1 Viewing Violations and Violators Summary 139
5.5.1.1 Managing Dashboards 140
5.5.1.1.1Creating a Dasboard 140
5.5.1.1.2Deleting a Dashboard 140
5.5.1.2 Managing Widgets 141
5.5.1.2.1Adding a Widget 141
5.5.1.2.2Editing a Widget 141
5.5.1.2.3Deleting a Widget 142
5.5.2 Viewing Events 142
5.5.2.1 Events Filtering 142
5.5.2.1.1Query Creation in Standard Mode 143
5.5.2.1.2Query Creation in Extended Mode 144
5.5.2.1.3Creating Query with Negation in Standard Mode 147
5.5.2.1.4Creating Query with Negation in Extended Mode 148
5.5.2.2 Selecting Event Display Fields 150
5.5.2.3 Viewing Short Event Form 151
5.5.2.4 Viewing Detailed Event Form 151
5.5.3 Managing Reports 152
5.5.3.1 Creating a Report 152
5.5.3.2 Viewing a Report 153
5.5.4 Making Decision on Object 154
5.5.5 Adding and Deleting a Tag 154
5.5.6 Creating Notification on Event 155
5.5.7 Saving an Event (for SMTP Objects) 155
5.5.8 Dispatching Blocked Object 155
5.6 Managing Crawler Subsystem 156
5.6.1 Configuring Scanner 157
5.6.2 Creating a Job 158
5.6.3 Launching and Stopping the Job 159
5.6.4 Editing the Job 159
5.6.5 Cleaning the Hash Base 160

5.6.6 Viewing Launch History 160
5.6.7 Saving Scan Report 161
5.7 Managing Catalogues 161
5.7.1 Managing Tags 162
5.7.2 Managing Resources Lists 162
5.7.3 Managing Statuses 163
5.7.4 Managing Perimeters 163
5.8 Interface Customization 164
5.8.1 Selecting Dashboard Layout 165
5.8.2 Selecting Event Displaying Style 166
5.8.3 Workspace Partitioning 166
5.8.4 Moving Widget Tiles 166
Part VI Licensing Information 167
6.1 End-User License Agreement 167
6.2 Third-Party Licenses 170

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, IMAP4, POP3, HTTP, ICQ). The System also analyses data received from InfoWatch Device Monitor.

The management web-console (web-console, Management Console, MC) is a part of the InfoWatch Traffic Monitor system. The web-console allows configuring System settings and monitoring operations of the System.

The Management Console has a user-friendly interface so this guide contains only general information and examples which represent functionality of the whole System.

This guide explains how to use the System (configure settings, analyze information objects, etc.) with the help of the Management Console.

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

This guide contains the following sections:

- InfoWatch Traffic Monitor Overview – general description of the System and methods of checking the data.
- Management Console: General Information – contains introductory information and basic actions description.
- Management Console Interface – contains description of interface elements and entities used in the System.
- Cases Solving – describes the configuring of settings and rules used for monitoring and analysis of intercepted data. Contains the information on principles of creating the rules of analyzing the objects entering the System (letters, requests and so on).

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 7AM to 9PM (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.

1.1 Glossary

Term	Definition
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: *Script*.
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 Roles*, *Security Officer*.
AJAX	Asynchronous JavaScript and XML is a group of interrelated Web development techniques

	used on the client-side to create asynchronous Web applications.
Attachment	A file attached to the intercepted object (at any level). See also: *Object.*
Category	A Classification element that corresponds to a certain area (e.g. security labels or project terms). Contains subcategories or terms. See also: *Term*, *Classification.*
Case Sensitivity	A setting that defines if the term search is case-sensitive (uppercase and lowercase letters are considered different) or not. See also: *Term* .
Characteristic Term	Term setting: If a text contains a characteristic term that referrers to a certain category, the text is classified as referring to this category. See also: *Term.*
Citation Index	How close the sample document matches the text of the document being analyzed. See also: *Sample document.*
Classification	Referencing of the analyzed text to any category of the Classifier. See also: Classification, *Object context.*
Classifier	A set of data required to perform the linguistic analysis of a text. Contains the list of various security policy violation categories. If the text contains a term from a certain category, it is matched with this category. It also assigns a certain classification category for the text. See also: *Category*, *Term*, *Linguistic Analysis*, *Object context.*
Classification base	See *Classifier.*
Configuration	A group of settings required to check objects, to monitor and analyze data. See also: *Classification*; *Script*, *Lists*, *Text object.*
Configuration Version	A fixed state of the configuration designed to monitor changed settings of the object 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.*
Copy mode	One of the transport modes of InfoWatch Traffic Monitor. In this mode the actual traffic bypasses the System. The copy of traffic is analyzed. In this mode the traffic cannot be filtered by the System. See also: *Transport Mode.*
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.
Crawler	Traffic Monitor Subsystem which allows to perform files scanning for violations of corporate security policies inside the corporate network.
Database	An organized collection of data.
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: *Monitor*, *Object 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, IMAP4, and POP3), Web (HTTP), instant messaging services (ICQ and Skype), shadow copies of files, connected/disconnected workstation events, and print jobs.
Decision	A decision made by the user: whether the intercepted object violates the corporate security policy or not. Possible values: `No Decision`, `Violation`, and `No Violation`. See also: *Verdict*, *Object attributes*
Delivery Status	An object attribute that specifies if an object is delivered to recipients after analysis. If the object is approved for delivery, the value of this attribute will match the delivery state (delivered/blocked). See also: *Object attributes.*
Detecting Text Objects	A technology that searches for text objects (such as credit card numbers) in the text. See also: *Text object*, *Text object template .*
Detecting Digital	A technology that searches for sample document quotes in the text. See also: *Sample*

Fingerprints	*document*, *Quote.*
Device Monitor	InfoWatch Device Monitor is both software and hardware appliance designed to control the access to the peripherals and to monitor messengers and data either copied to removable media and FTP or sent to printing.
DeviceLock	Data loss prevention system providing endpoint device/port control and data leak prevention.
DeviceLock Adapter	A Device Monitor interceptor that integrates with DeviceLock (by Smart Line, Inc.); it intercepts the shadow copies of the files copied to the removable devices. See also: *Device Monitor*, *Shadow copy of a file*
Digital Fingerprint	A method of storing a sample document in a database in the form of a set of quotes. See also: *Sample document*, *Quote*
File mask	A pattern of characters and wildcards used to match folder and file names.
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.
Group	Groups of users and workstations. Groups are stored in the system directories. The groups are divided into AD Groups (imported from Active Directory) and TM Groups (created using InfoWatch Traffic Monitor). See also: *Persons, workstations, and groups directories*
GTalk	An instant messaging service that provides both text and voice communication.
Host profile	A group of settings related to the tasks performed by the given host. See also: *Host setting*
Host setting	A group of settings related to the tasks performed by the given host. See also: *Host profile*
HTTP	HyperText Transfer Protocol, an application-tier protocol used to transfer the data in the text format. **Note:** the HTTP protocol has extension HTTPS (Hypertext Transfer Protocol Secure) which supports traffic encryption.
HTTP request	A request formed according to the HTTP standards (POST requests, GET requests etc.) See also: *HTTP*, *Object*
HTTPS	Hypertext Transfer Protocol Secure is a network protocol for secure communication over a computer network.
ICAP	(Internet Content Adaptation Protocol) a protocol that allows to control the incoming and outgoing HTTP traffic. It also makes it possible to modify the content of the HTTP requests (InfoWatch Traffic Monitor controls only outgoing traffic).
Jabber	Messanging and information exhange system based on the open XMPP protocol.
ICQ	An Internet instant messaging service, currently owned by Digital Sky Technologies.
ICQ message	A message sent through the ICQ-OSCAR protocol. See also: *Object*
Identification Error	A situation when one value of the Sender, Recipients, or Workstation attribute has several matches in the persons and workstations directory. See also: *Persons, workstations, and groups directories*
IMAP4	Internet Message Access Protocol is a protocol for e-mail retrieval and storage.
InfoWatch Traffic Monitor	The InfoWatch Traffic Monitor software suite (IW TM). It is designed to control various types of traffic (SMTP, HTTP, ICQ) and shadow copies of the data copied to the removable media and sent to printing.
Interceptor	Also: Sniffer, Network Traffic Analyzer, Monitor. An InfoWatch Traffic Monitor component that receives data (SMTP, HTTP, ICQ traffic) from external clients, prepares it for further analysis and sends to Traffic Monitor Server.
Jabber	An instant messaging and presence service based on XMPP.
Linguistic Analysis	A text classification technology that works by matching this text with certain categories.

	See also: *Classification*, *Category*
Lists	Lists of the similar data generated by Management Console to be used in the object analysis scripts. See also: *Configuration*, *Script*
Management Console	Graphic user web-interface. Designed to manage InfoWatch Traffic Monitor (system administration, configuring settings, object analysis, etc.)
Mail.Ru Agent	An instant messaging service.
MAPI	Messaging Application Programming Interface is a messaging architecture and a Component object model based API for Microsoft Windows.
MC	See *Management Console*
MMP	The protocol of connection between Mail.Ru Agent and general Mail.Ru network.
Morphology	Term setting: if morphology is used, the text search will detect all word forms of this term. See also: *Term*
Monitor	See: *Interceptor*
MS Lync	Microsoft instant messaging clients for corporate environments.
IW Lync Adapter	An interceptor, which is being installed on Microsoft Lync Server to transmit messages to Traffic Monitor for further analysis.
Normal transport mode	A traffic analysis and filtering mode. In this mode it's possible to block the illegal traffic. See also: *Transport Mode*
Notification	An e-mail sent via Management Console to notify other Management Console users about one or more intercepted objects. Contains the numbers of the selected objects and the corresponding message. It is also a selection of the statistics about the intercepted objects. See also: *Management Console*
Object	Traffic objects (SMTP e-mails, HTTP requests, ICQ messages, and Skype messages), shadow copies of files, and print jobs.
Object analysis	The procedure of additional attributes assignment and processing of the attributes, attached files, and text of the intercepted objects. See also: *Script*, *Object attributes*
Object attributes	Structured data extracted from the intercepted objects and assigned according to the processing results. See also: *Script*, *Verdict*, *Solution*, *Transport Mode*, *Tag*
Object Body	An object without its attached files. See also: *Object*
Object Context	An internal representation of an intercepted object. XML data (attributes, text) extracted from the object and its attachments. After processing the analysis results and the decision are added to the context. See also: *Object*
Object Headers	An arbitrary, dynamically updated set of headers. See also: *Object attributes*
Object Text	Text information extracted from the object body and attachments. Does not contain formatting or markup. Used for search and analysis purposes. See also: *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.
Persons, workstations, and groups directories	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 intercepted objects information.
Policy	A set of rules according to which the analysis and processing facilities are performed. Usually consists of a set of conditions under which the object is being checked and actions are carried out in the performance or non-specified conditions. See also: *Active Policy* Essence to define the system in response to certain actions of securable objects.

POP3	Post Office Protocol 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 request	A query method designed to request that a web server accept the data enclosed in the request message body for storage.
Privilege	An entity that defines the actions (or sets of actions) available for a user to work with the System.
Proxy server	A server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers.
Query	Management Console database query is used to get the updated data. See also: *Management Console*
Quote	A quote from the sample document database found in the intercepted object text. See also: *Sample document*
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 captured objects statistic data.
Sample database unloading	A part of the database, which quotes are searched in in the analyzed text. Lists of person's salaries, other personal data and so on can all be used as sample database unloadings.
Sample document	Quotes from these documents 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 as digital fingerprints. The text cannot be viewed by users or administrators. See also: *Detecting Text Objects*, *Digital Fingerprint*, *Quote*
Sample Document Database	Storage of digital fingerprints captured from sample documents. Required to search for quotes in the analyzed text. See also: *Sample document*, *Detecting Digital Fingerprints*, *Digital Fingerprint*, *Quote*
Sample form	A formsheet: its filled version is searched in the network traffic. Different checklists, questionnaires, vouchers and so on can all be used as sample forms. Sample forms are stored in the System as a data unavailable for viewing both for users and System administrators.
Sample stamp	An image of a seal searched in the network traffic. Images of round impressions used in the organizations can be used as sample stamps.
Script	A set of rules used to analyze and process objects. A rule consists of a set of conditions for analyzing objects and actions to be performed when the specified conditions are met/not met. See also: *Active script*
Security Officer	A preset role and user account in Management Console; has all privileges. See also: *User Roles*, *Administrator*
Set scope	A way to separate the intercepted objects to restrict the user access from Management Console. The objects belonging to a certain responsibility zone are visible to the users who belong to this responsibility zone (if the user has privileges to view or/and handle the objects). See also: *Privilege*
Shadow copy of a file	A copy of the file created on a removable storage media. The copy is created only if the file is successfully saved on the removable storage device. The shadow copies of files are analyzed by InfoWatch Traffic Monitor.
Skype	A voice-over-IP service and instant messaging client currently developed by the Microsoft Skype Division.
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 e-mail	An e-mail formed according to SMTP standards. See also: *SMTP*, *Object*
SPAN	Switched Port Analyzer is a technology that allows to mirror the network traffic from one port to another.
SPAN Copy	A variety of the "Copy" transport mode. In this case the traffic passes through a CISCO switch. The copy of the traffic is sent to Traffic Monitor Server for analysis. See also: *SPAN*
SSL	Secure Sockets Layer is a cryptographic network protocol developed for transmitting private documents via the Internet.
Tag	A text markup that defines the intercepted object. See also: *Object attributes*
Term	Either word or phrase that increases the matching rate if found in the text. See also: *Category*
Term Weight	How the term is characterized for the given category. If a term with a higher weight is detected in a text, then this text will be more likely associated with the category of this term. In the Management Console – an integer between 1 and 10. See also: *Term*
Text Object	The data from the analyzed text that were considered matching the pattern by the text object detection module. See also: *Text object template*, *Detecting Text Objects*
Text Object Template	Unified description of all possible text objects with a typical structure: passport numbers, credit card numbers, phone numbers, medical codes etc. See also: *Detecting Text Objects*
Transparent Transport Mode	The mode of transferring the traffic without being filtered. The System only analyzes the intercepted traffic. See also: *Transport Mode*
Transport Mode	Object 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: *Verdict*, *Copy mode*, *Normal transport mode*, *Transparent transport mode*, *Delivery Status*, *Object attributes*
User	InfoWatch Traffic Monitor users: administrator, security officer etc.
User role	A set of privileges that define the actions available for the user. See also: *Administrator*, *Security Officer*, *Management Console*, *Privilege*
Verdict	An object attribute with the conclusion about the presence (or absence) of violations in an object. Together with the Transport Mode attribute determines if the object can be delivered further on. This is a mandatory attribute of an object. See also: *Transport Mode*, *Delivery Status*, *Object Attributes*
Verdict Reason	Object attribute that describes the reason why a certain verdict was assigned to the object. See also: *Verdict*
Violation	The value of the `Decision` attribute; means that the corporate security policy has been violated. See also: *Solution*, *Corporate Security Policy*
Widget	Interface element in the form of an isolated area that displays the specified statistic information on violations / violators. See also: *Violation*
XMPP	Extensible Messaging and Presence Protocol is a communications protocol for message-oriented middleware based on XML.
Yahoo	System for fast messages and information exchange based on open YMSG protocol.

1.2 Additional Documentation

For more information see the following documents:

- *"InfoWatch Traffic Monitor. Installation and Configuration Guide"*
  This document describes how to install the InfoWatch Device Monitor and configure its basic settings.

- *"InfoWatch Traffic Monitor. Administration Guide"*
  Describes how to administrate the database (working with tablespaces) and the server end of the InfoWatch Traffic Monitor.
- *"InfoWatch Device Monitor. User Guide"*
  This document describes the principles of working with the InfoWatch Device Monitor system.
- *"InfoWatch DeviceLock Adapter. Installation and Configuration Guide"*
  This document describes how to set up InfoWatch DeviceLock Adapter and how to configure its basic settings.
- *"InfoWatch DeviceLock Adapter. Administration Guide"*
  This document describes how to configure and monitor InfoWatch DeviceLock Adapter.
- *"InfoWatch Autolinguist. User Guide"*
  The document describes how to operate InfoWatch Autolinguist.

The mentioned documents are supplied together with the corresponding software products.

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 the SMTP, IMAP4 and POP3 traffic. It's possible to intercept either the traffic (or the copy of traffic) relayed by a mail relay server or the copy of the traffic that passes through the hardware with the CISCO SPAN features support.
- Interception of the HTTP, HTTPS-traffic. It's possible to intercept either the traffic passing through an ICAP-supporting proxy server or the copy of the traffic that passes through the CISCO SPAN-enabled equipment.

  Note

  While integrating 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) transmitted through the equipment supporting the CISCO SPAN. When ICQ connects through HTTP, the System intercepts ICQ traffic in a way that is 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 file storage) with Crawler subsystem.
- Analyzing Skype-, Yahoo- traffic, shadow copies of files, print jobs, traffic transferred by HTTPS and FTP protocols; receiving and transmitting mail via SMTP, POP3, IMAP and MAPI interface, controlling data shared through Jabber (XMPP protocol) and Mail.Ru Agent (MMP protocol). Interception of listed data is performed by InfoWatch Device Monitor system.
- Analyzing the shadow copies of files intercepted by DeviceLock version 6.3 or higher (provided by SmartLine, Inc.) to detect the violations of the corporate security policy.
- Intercepting and analyzing MS Lync objects via IW Lync Adapter installed on MS Lync server.
- Analyzing the contents of the intercepted traffic to detect the violations of the corporate security policy.

- Filtering the intercepted traffic by allowing or blocking 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
Server part	**Traffic Monitor Server**: intercepting, analyzing, and filtering the traffic, analysis of data received from InfoWatch Device Monitor and DeviceLock systems. **Sniffer**: intercepting the copy of traffic going through commutator's SPAN-port. **IW ICAP Module**: interception, analysis and filtering of HTTP-traffic going through ICAP protocol. **Crawler**: checking of files from corporate network (open network folders, local disks of workstations, and SharePoint 2007/2010 file storage). **Remote Database Management Module**: transferring the data for storing to remote database trough slow channels.
Database	Storage of intercepted objects data, analysis and policy application of results, and ability of viewing stored information using management console queries.
Management Web-Console	Configuring rules of traffic analysis and filtering, analysis of intercepted data

2.1 Object Interception and Analysis

Description of objects interception and analysis is provided in the following articles:

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

2.1.1 Object Interception

The system *objects* are the following:

- traffic objects (SMTP e-mails, HTTP- and HTTPS-requests, ICQ messages, messages of Skype, Yahoo, GTalk, MS Lync and Mail.Ru Agent);
- shadow copies of files;
- print jobs.

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

Object type	Object interception options
SMTP, IMAP4 and POP3	• The System intercepts and delivers the SMTP traffic. There is an opportunity of filtering the intercepted objects (the delivery can be allowed or blocked). • The System receives a copy of SMTP traffic from the corporate mail relay server. The System does not take part in traffic delivery. • The System receives a copy of SMTP traffic that goes through the switches with a SPAN port. The copy is intercepted using Sniffer. The System does not take part in traffic delivery.
HTTP	• The System intercepts the HTTP using the ICAP server integration. There is an opportunity of filtering the intercepted objects (the delivery can be allowed or blocked). • The System receives a copy of the HTTP traffic that passes through a switch with a SPAN port. The copy is intercepted using Sniffer. The System does not take part in traffic delivery.
HTTPS	System receives traffic copy from InfoWatch Device Monitor.
MAPI	System receives traffic copy from InfoWatch Device Monitor.
FTP	System receives traffic copy from InfoWatch Device Monitor.
ICQ	• The System receives a copy of the ICQ traffic that passes through a switch with a SPAN port. The copy is intercepted using Sniffer. The System does not take part in traffic delivery. • When ICQ connects through HTTP, the System intercepts the ICQ traffic in the same way as the HTTP traffic.
Skype messages, Yahoo, GTalk messages, and Mail.Ru Agent messages	The System receives a copy of traffic from InfoWatch Device Monitor.
MS Lync	System receives traffic copy from IW Lync Adapter , installed on MS Lync server.
Files located in corporate network	The System receives copies of files from Crawler subsystem.
Shadow copies of files and print jobs received from InfoWatch Device Monitor	The System receives a copy of traffic. Blocking user actions (printing, access to the devices) is possible only using InfoWatch Device Monitor.
Shadow copies of files received from DeviceLock	The System receives a copy of traffic. Blocking user actions (access to the devices) is possible only using DeviceLock.

The intercepting options and further objects delivery is connected with InfoWatch Traffic Monitor transport modes (see "InfoWatch Traffic Monitor Transport Modes").

2.1.2 InfoWatch Traffic Monitor Transport Modes

InfoWatch Traffic Monitor supports two transport modes: ***normal*** and ***copy***. The 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"). The selected transport mode defines further delivery of the object.



Important!

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

The difference between modes lies in the features of objects delivery (see the table below).

Transport Mode	Description
Normal	InfoWatch Traffic Monitor intercepts, analyses, and forwards objects. In this mode the verdict defines if the object will be delivered to recipients. Moreover, in some cases the delivery status of the SMTP messages can be changed after the user decision was changed (see "Specific features of blocking HTTP-queries and messages sent through web-services").
Copy	In this mode the System receives copies of objects. This mode differs from normal as the objects are transported without using the System. In this way, the System performs the object analysis only. Since the copies of the objects are analyzed, the verdict and the analysis-based user decision do not impact the object delivery to the recipients.

The following table lists the possible transport modes for different types of objects.

Object type	Transport modes	
	Normal	**Transparent**
SMTP e-mail	Yes	Yes (for traffic copy received from mail relay server or from Sniffer)
HTTP query	Yes (only when intercepting traffic over ICAP)	Yes
ICQ message	No	Yes (for traffic copy received from Sniffer)
Skype, Yahoo, Jabber, GTalk, Mail.Ru Agent message	No	Yes
MS Lync	No	Yes
Shadow copy of a file	No	Yes

For more information about transport modes for different types of objects see "*InfoWatch Traffic Monitor. Installation and Configuration Guide" and "InfoWatch Traffic Monitor. Administration Guide".*

2.1.3 Object Analysis and Verdict

Object processing and analysis with supplement of the security policies are performed by the following InfoWatch Traffic Monitor subsystems:

Traffic Monitor subsystem	Subsystem modules	System/subsystem 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 the valuable data and enclosures from the object, defining enclosures format, and forwarding the extracted texts to the Analysis subsystem.
Analysis subsystem	Linguistic Analysis module	Text classification by searching if it corresponds to any categories.
	Text Objects Detecting module	Searching through the objects text for text objects (e.g. credit card numbers).
	Digital Fingerprints Detecting module	Searching through the objects text for quotes from sample documents.
Policies Application subsystem	Active Directory Integration module	Providing the initial import and periodical synchronization of Active Directory structure with Traffic Monitor users and workstations directory for further binding this information with data from the intercepted objects.
	Decision Making module	Providing maintenance of corporate security policies by adding them to objects.

The object analysis is performed in the following order:

1. **Detaching object attributes** – Processing subsystem detaches object attributes: for example, SMTP letters have sender and receivers addresses, subject, etc. The list of available attributes see in "Event tile".
2. **Extracting enclosed files** – Decision Making module analyzes enclosed files according to attributes, for example, file name or file type.
3. **Analysis of the text** – the Analysis subsystem processes text data: texts of e-mails, messages, and queries as well as text files extracted from attachments of the supported format.

   The system supports three types of analysis depending on your product licence:

Content analysis technology	Technology description
Linguistic analysis	Determining the subject and content of a text according to the terms (words and phrases) found in this text. The search for the terms is performed using the Classification. The Classification includes the organization-specific terminology. 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 category allows to relate the text to this category. For example, the *Salary* term could be included in *Internal payments* and *Working conditions* categories. The presence of the term in the text means that the text can belong to mentioned categories.
Detecting text objects	Search for text objects matching the specified templates (like searching for credit card numbers in the intercepted objects).
Detecting digital fingerprints	Search for fragments of a text matching the predefined template documents (orders, financial reports, contracts, etc.).
Detecting sample forms	Search for filled forms of a preset sample. Questionnaires, receipts and so on can be a sample form.
Russian Federation citizens passport detection	Search for Russian Federation citizens passport images. Technology functions with *Russian Federation citizen* passport text object enabled.
Detecting sample stamps	Search for stamp images of a preset type. Images of round prints,which are used in organizations can be sample stamps.
Detecting sample database uploadings	Search for quotes from specified database. List of employees' salary, other personal data an so on can be sample database uploadings.

4. Based on the results of the analysis, the Decision Making module applies configured rules and assigns a **verdict** – a conclusion on the possible policy violation. The following verdicts are provided:
   - *Forbidden*. The object is qualified as violating the corporate security policy. In the normal transport mode this object is blocked and will not be delivered.
   - *Allowed*. The object does not contain any violations of the corporate security policy. After being analyzed, the object will be delivered to the recipients if the normal transport mode is used.
   - *Quarantined*. Object is a potential violation. In normal transport mode such object delivery will be performed only in case user assigns *No threat* level to event. Functions only for SMTP-mail when system works in "inline" mode - see document "InfoWatch Traffic Monitor. Installation and configuration guide".
   - *Deleted*. Object might be a violation, but is not being saved in the System for some reason.

2.1.4 Uploading Object into Database

After the object is analyzed and the decision is made (see "Object analysis and verdict"), the object is uploaded to the database. Both the object and the XML context of the object are uploaded to the database. The XML context includes:

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

2.1.5 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 value of the *Decision* attribute to each object is *No Decision*. Then the user can make one of the following decisions:

- *Violation*. The user found out that the object violates the corporate security policy (resting on the analysis results).
- *No Violation*. The user has concluded that the object doesn't violate the corporate security policy.
- *No Decision*. User didn't make the decision if the object violates the corporative security policy or not.
- *Further Analysis is Needed*. User concluded that further object processing is needed.

If the System is configured to filter the SMTP traffic, a decision can allow or deny the delivery of the SMTP e-mail (see "Making the decision about an object").

Note

The SMTP traffic is filtered only if messages are delivered by the System and the normal transport mode is used for the SMTP traffic.

Note

Working in *Inline mode* and applying *No violation* verdict, email will leave company perimeter no matter how the verdict will be edited further.

2.1.6 Specific Features of Blocking HTTP and HTTPS-queries and Messages Sent Through Web-services

If in 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, then the request/message sender's web-browser will display the blocking message.

If an e-mail is sent through AJAX-based mail services (such as Gmail, Windows Live Hotmail, etc.), then the user may not get the blocking message. As a rule, the web mail service message is displayed instead.

For POST requests to some websites (see the table below) the System has pre-defined rules:

- at the **Object Info** pane (see "Interception Objects") the *From*, *To*, *CC*, *Subject*, and *Sent* fields and attachments (if present) are displayed.
- if no aforementioned attributes can be found and no text can be extracted from headers, these POST

requests may be deleted as a garbage traffic. For example, background status requests in social networks are such a garbage traffic.

Interception of HTTP/HTTPS queries supports following forum engines:

- IP Board
- phpbb
- vBulletin

Web resource type	Resources	
	Without limitations	**With limitations**
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)

Additional: 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 logon process:

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

If at least one condition isn't met, the user won't be able to log into the System.

If the authorization was successful, you will access the MC main window. In other case the error message will be displayed.

Depending on the role assigned to the account entering the System the user can have the following rights:

- **Administrator** is the role having all needed privileges for initial configuring of the Management Console;
- **Security Officer (SO)** is the role having all privileges except the initial configuring of the MC.

Note:

This Guide does not describe protocols for Administrator. All required information is represented in "*InfoWatch Traffic Monitor. Administration Guide"* document.

After authorization the user can configure the System:

- configure the analysis of employees' actions (see details in "Configuring the Analysis of Employees Actions");
- configure the System response to stated employees' actions (see details in "Configuring System Response").

Note

The way how the System operates after installation and before configuring is described in "System Operation Before Configuring".

Configuring the System should be ended by applying the updated configuration (see details in "Configuring the System").

Note

If the System is already configured and all use cases are provided by implemented configuration, then there is no need in additional System configuring.

After configuring the Security Officer can use configured System by making reports on violations of corporate security rules (see details in "Managing Interception Objects"). Also he/she can modify the Console interface (see details in "Interface Customization") and perform other tasks.

The full list of user decisions is given in "Cases Solving".

Configuring the Crawler subsystem is described in "Managing Crawler Subsystem".

When several SO use the Console, you can get an actual data by refreshing data (see "Refreshing Data in Management Console").

Warning!

The correct System operation requires the antivirus programs and other blocking software not to block internet content.

For example, in G DATA Security antivirus the deselecting of **Process Internet content (HTTP)** check box is needed.

3.1 System Operation Before Configuring

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

- intercepts traffic and checks if interception objects match predefined categories. If an interception object matches any category, the System assigns a corresponding attribute to the object.
- allows logging into the System using one of 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 person and workstation lists (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 configuring of the System is a set of adjustments needed for checking the objects at the Traffic Monitor Server and for data monitoring and analysis.

Each object handled to the Traffic Monitor is processed according to the configuration version which is currently actual at the server and then is uploaded to the database with all the attributes assigned to the object as a result of processing.



Warning!

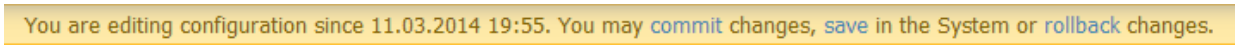
The System do not perform the reprocessing of the object using a newly updated configuration.

The configuration is:

- Creating classification database (see "Configuring the Analysis of Employees Actions"):
  - Selecting terms to detect - *only when using the Linguistic Analysis* (see "Terms");
  - Selecting text object types to detect (see "Text Objects and their Values") - *only when using the Detecting Text Objects;*
  - Selecting sample documents to detect - *only when using the Detecting Sample Documents* (see " Sample Documents");
  - Selecting sample forms to detect - *only when using the Detecting Sample Forms* (see "Sample Forms ");
  - Selecting sample stamps to detect - *only when using the Detecting Sample Stamps* (see "Sample Stamps");
  - Selecting sample database uploadings to detect - *only when using the Detecting Database Uploadings* (see "Sample Database Uploadings").
- Creating catalogues:
  - Persons and workstations (see "Managing Persons and Workstations");
  - Tags (see "Managing Tags");
  - Resources lists (see "Managing Resources Lists");
  - Statuses (see "Managing Statuses");
  - Perimeters (see "Managing Perimeters").
- Creating policies according to which the checking of objects on Traffic Monitor Server is performed (see " Configuring System Response").

If any of settings listed above was changed in the Console, the editing configuration version is saved in the System. Upon this:

- in the top of the browser workspace of user who changes the configuration the following message is displayed:



- in the top of the browser workspace of user who cannot access configuration changing the following message is display:



Warning!
The changed configuration is available only to the user who changes it till this configuration is applied, saved or rolled back. Other Console users do not have an access to the System configuration.

You can complete the configuration editing by one of the following actions:

- **Apply configuration** (see details in "Applying System Configuration") - updated configuration becomes active on the server.
- **Save configuration** - 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 in the Console will remain the last applied configuration on the server and all made changes will be deleted. To cancel changes, press **Save** in the opened changes window. In *Description* field, when necessary, add explanation of changes deletion. This information will be saved in database.

3.3 Refreshing Data in Management Console

Several users are able to work with the System at the same time. To keep the information about the system up-to-date you should refresh the data periodically. The data is refreshed either automatically or manually.

The data related to a specific Management Console section is **refreshed automatically** when you go to this section. You can set up automatic refresh of statistic data on violations and violators.

You can also update data **manually** in each section of the Management Console. To do this use the standard browser refresh tool: by default the page is refreshed by pressing **F5** function key.

Note:

While downloading the requested data, the System is displaying a symbol like .

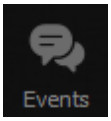
4 Management Console Interface

The Management Console is organized in special sections:

Section	Purpose
Dashboard	Contains statistical information about violations and violators
Events	Contains list of intercepted objects and tools to manage them
Classifier	Contains the Classification (classification database) settings

Files	Contains the catalogue of files to detect
Persons	Contains the catalogue of persons and workstations of company IT system
Policies	Contains the list of persons' expected actions and the reaction algorithm of the System
Lists	Contains editable catalogues of tags, resources, statuses, and perimeters
Administration	Operations performed in this section are described in "*InfoWatch Traffic Monitor. Administration Guide"* document
Crawler	Contains tools to create, edit, and run tasks for Crawler subsystem

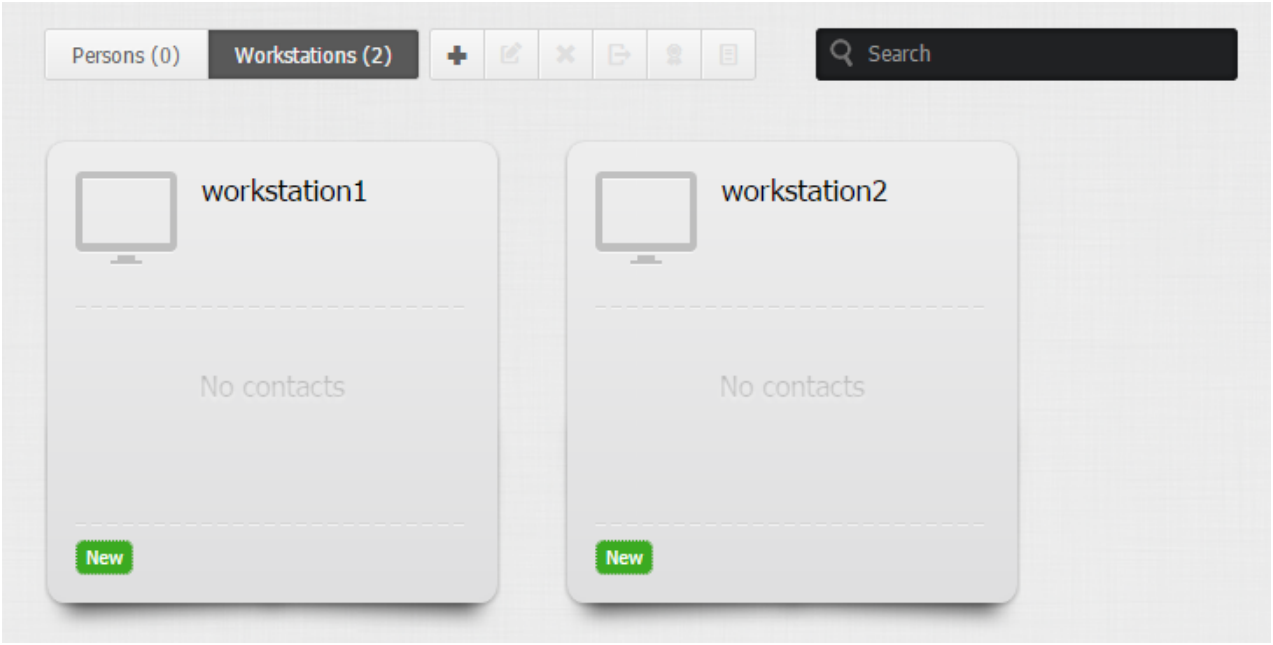
You can go to the section by clicking the section button.



Events button

There are following interface elements used in the Management Console:

- **Tab** - allows to switch between interface elements set in the same window.



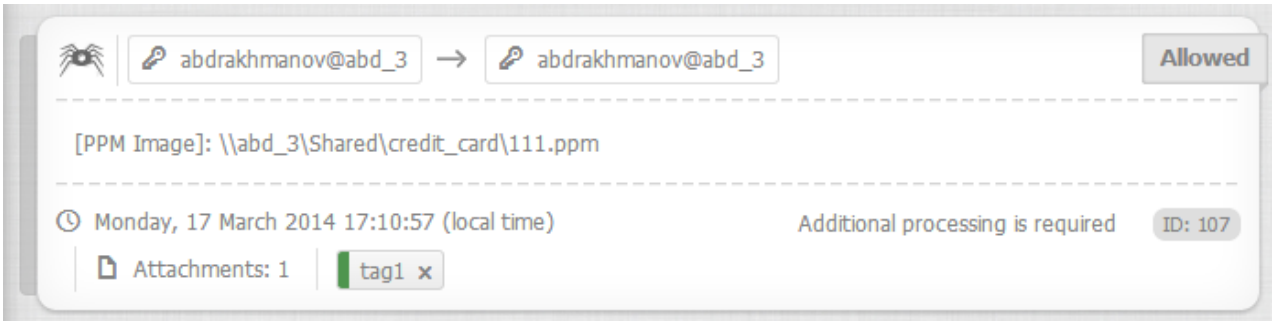
Persons section, **Workstations** tab

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



Classifier section, toolbar panel

- **Part of the working area -** working area fragment, separated from another by a deviding vertical line.
- **Tile** - all data of one entry (all object attributes) as a separate object.



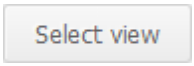
Events section, event tile

- **Table**

Object ID	*User decision*	Event type	Intercept date
107	Additional proces...		Monday, 17 March 2014 17:10:57 (local time)
202	No decision		Thursday, 20 March 2014 22:14:41 (local time)
9	No decision		Monday, 17 March 2014 16:35:16 (local time)
8	No decision		Monday, 17 March 2014 16:35:15 (local time)
108	No decision		Monday, 17 March 2014 17:10:57 (local time)
7	No decision		Monday, 17 March 2014 16:35:15 (local time)
6	No decision		Monday, 17 March 2014 16:35:14 (local time)
106	No decision		Monday, 17 March 2014 17:10:56 (local time)
5	No decision		Monday, 17 March 2014 16:35:09 (local time)
105	No decision		Monday, 17 March 2014 17:10:55 (local time)
4	No decision		Monday, 17 March 2014 16:35:12 (local time)
104	No decision		Monday, 17 March 2014 17:10:54 (local time)

Events section, event table

- **Button**



Dashboard section, **Select view** button

- **Field** - a string either to enter or view data.



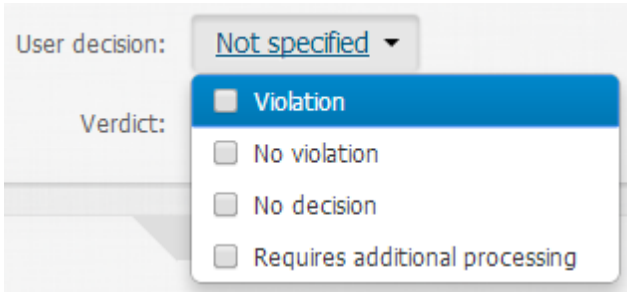
Persons sections, search field

- **List -** displays a list containing elements.

	Name	Description
	To fire	
	Fired	
	New	
	Under supervision	
	On probationary period	

Lists section, **Statuses** tab, list of statuses

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



Dashboard section, drop-down list on a widget

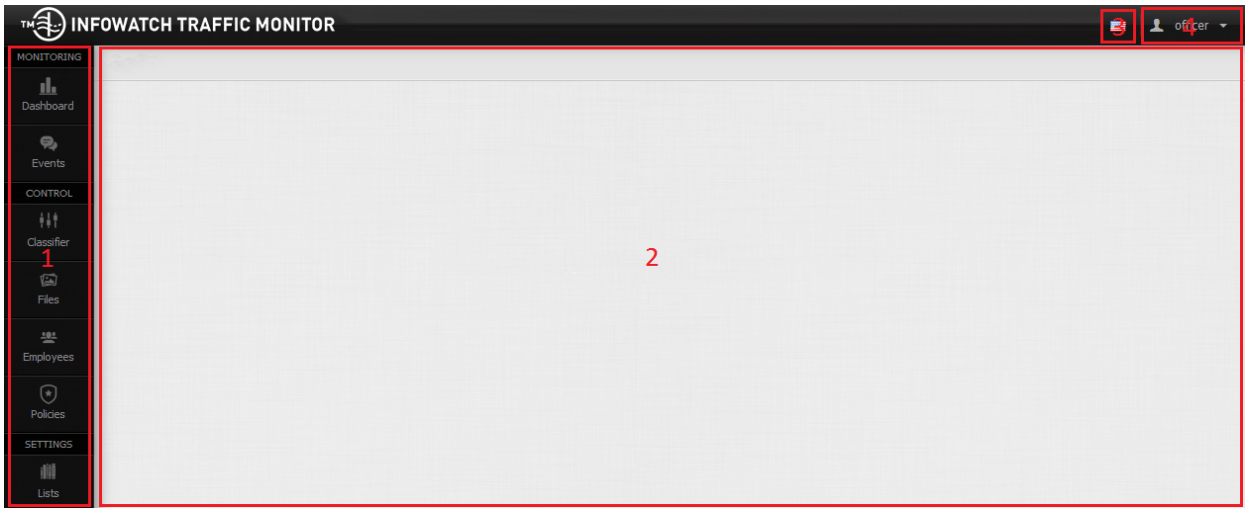
You can configure the Management Console interface (see "Interface Customization").

Note

While downloading the requested data, the System is displaying a symbol like this .

4.1 Management Console Window

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



Management Console start window

Window elements are listed in the following table.

Main window element	Number on scheme	Element purpose
Navigation pane	**1**	Displays sections buttons. Click to go to selected section of the Management Console.
Workspace	**2**	Displays elements of selected Management Console section; it is used for managing elements of selected section.
Language icon	**3**	Displays a flag of a country which language was selected for Management Console interface. Click to open a drop-down list of interface languages to select from (see "Selecting Interface Language").
User menu	**4**	Displaying user's name and avatar. Click to open a drop-down list were you can: • Change password of your account (see "Changing User's Password"); • Call for file with help information on the System (see "Calling Help File"); • Gain an information on the System (see "Viewing Information on System"); • Exit the Management Console (see "Log In and Log Out the Management Console").

Elements of main window are available from any section.

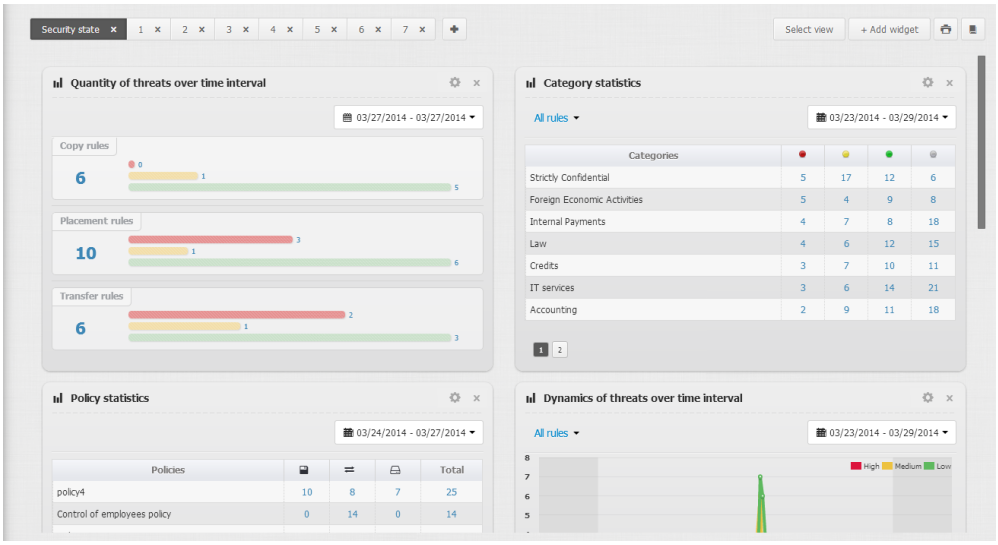
See also:

- Dashboard Section
- Events Section
- Classifier Section
- Files Section
- Persons Section
- Policies Section
- Lists Section
- Crawler Section

4.2 Dashboard Section

About the section:

The section contains statistical information about violations and violators.
The information is displayed on widgets located on dashboards (tabs).



Dashboard section

This section contains the following elements:

Element	Purpose
Widgets	Contains information about violations and violators
Dashboards	Contains widgets
Add dashboard button	Adds a dashboard
Select view **Select view** button	Selecting a type of workspace separation (see details in "Selecting Dashboard Layout")
+ Add widget **+Add widget** button	Adds a widget
Generate report button (see "Dashboard Report")	Creating a report on violations/violators (see "Managing Reports")
View list of reports button	Viewing a list of created reports

User's target actions:

- configuring dashboards and widgets to display information on violations/violators (see "Managing Dashboards", "Managing Widgets");
- viewing information on violations/violators (see "Viewing Events");
- creating a report on selected dashboard (see "Managing Reports").

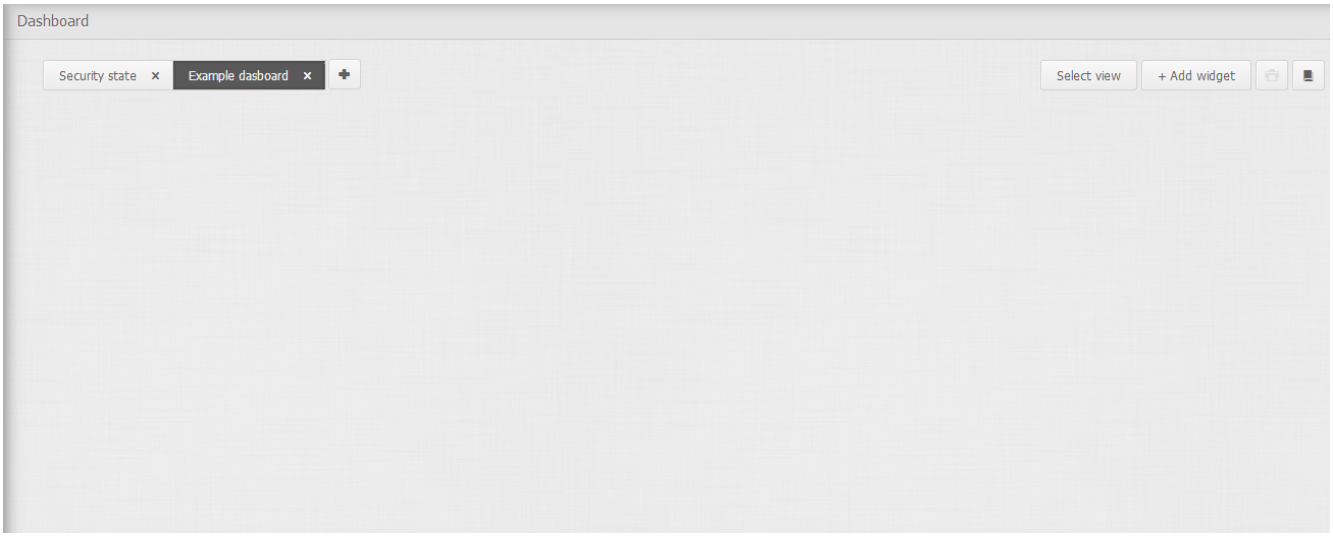
User's additional actions:

- selecting dashboard layout (see "Selecting Dashboard Layout");
- moving widget tiles (see "Moving Widget Tiles").

4.2.1 Dashboards

The workspace of the section may contain one or several dashboards as tabs. The dashboards are intended to contain widgets which allows user to view the statistics on violations and violators.

The dashboard is a tab for ergonomic usage of the workspace in the **Dashboard** section.



Dashboard section, *Example dashboard*

Dashboard parameters are described in the following table:

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

User's actions:

- configuring dashboards to display information on violations and violators (see "Managing Dashboards");
- selecting dashboard layout (see "Selecting Dashboard Layout").

4.2.2 Widgets

The workspace of the **Dashboard** section contains widgets on the dashboards (see "Dashboards"). The widget is a tile containing statistical information on violations and violators depending on a widget type.

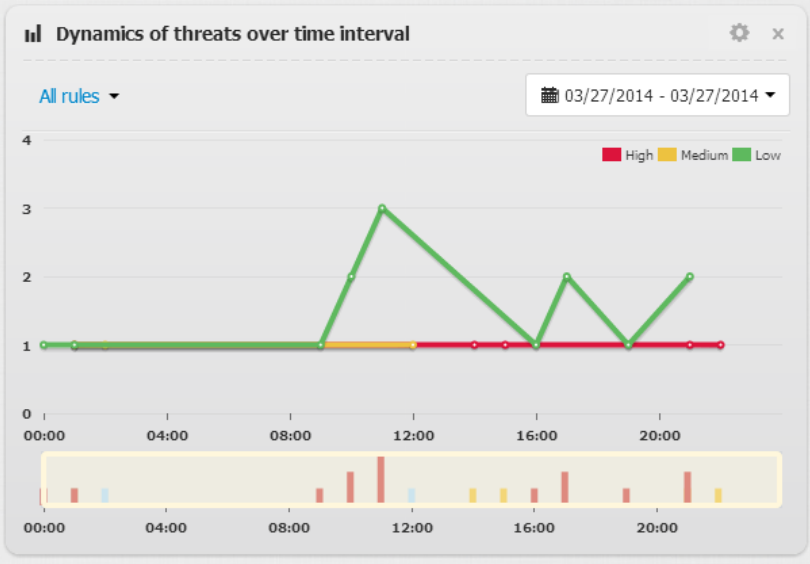
The functionality of different widget types is described in the table:

Widget	Description
Dynamics of threats over period	Quantitative changes of chosen violation types over selected period
Top violators	List of the most distinguished violators in chosen group over selected period
Quantity of threats over period of time	Number of violations of high, medium, and low level for each violation type over selected period
Selection	Events for each selection (with selected filter)
Dynamics of statuses over period	Dynamics of statuses over selected period
Policy statistics	Number of violations per policies in view of users' activities over selected period
Category statistics	Number of violations per categories in view of users' activities over selected period

Users actions:

- configuring widgets to display information on violations and violators (see "Managing Widgets");
- moving widget tiles (see "Moving Widget Tiles").

4.2.2.1 Dynamics of threats over period



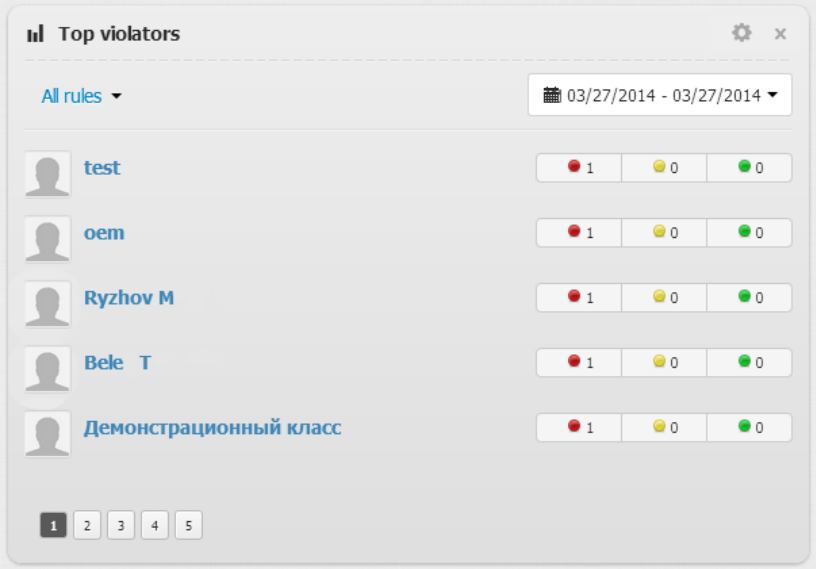
Dynamics of threats over period widget

Widget parameters are described in the table:

Parameters	Description
Name	Widget name

Parameters	Description
Rules	Drop-down list of rule categories with their treats displayed on the widget
Update interval	Period of data updating on the widget
Period	Time of data displaying

4.2.2.2 Top violators



Top violators widget

Widget parameters are described in the table:

Parameter	Description
Name	Widget name
Rules	Drop-down list of rule categories with their treats displayed on the widget
Update interval	Period of data updating on the widget
Period	Time of data displaying
Quantity of top	Quantity of violators to display the summary
Groups	Group to display the summary
Statuses	Statuses to display the summary

4.2.2.3 Quantity of threats over period of time



Quantity of threads over period of time widget

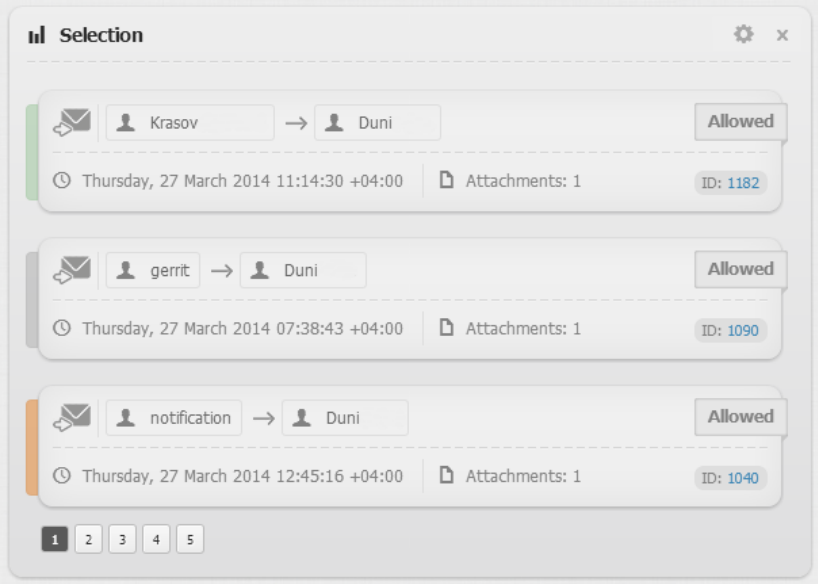
Widget parameters are described in the table:

Parameter	Description
Name	Widget name
Update interval	Period of data updating on the widget
Period	Time of data displaying
View type	View of data representation

Note:

By pressing on violation number (marked blue), System will go to **Events** tab displaying violations list.

4.2.2.4 Selection



Selection widget

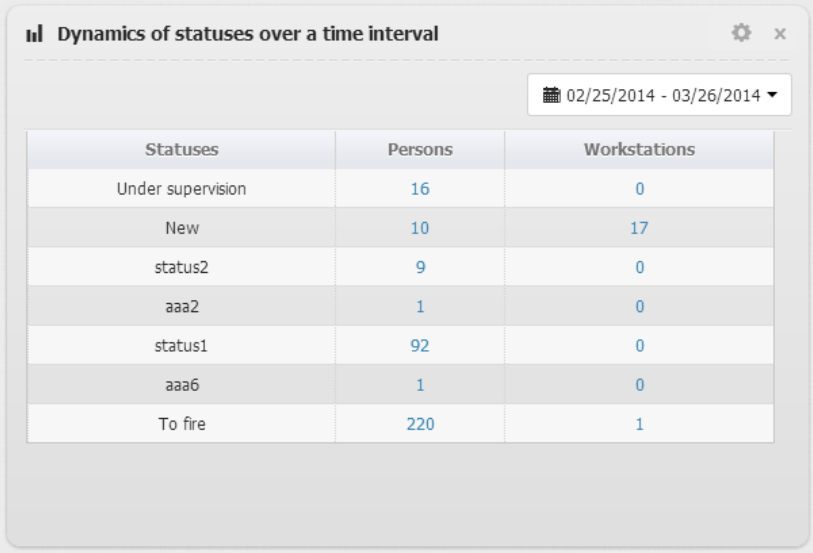
Widget parameters are described in the table:

Parameter	Description
Name	Widget name
Update interval	Period of data updating on the widget
Period	Time of data displaying
Selection	Name of the selection filter (see "Filters")
Events per page	Quantity of events displayed on the page

Note

By clicking on object ID (highlighted in blue), MC goes to the **Events** section displaying the selected object.

4.2.2.5 Dynamics of statuses over period



Dynamics of statuses over period widget

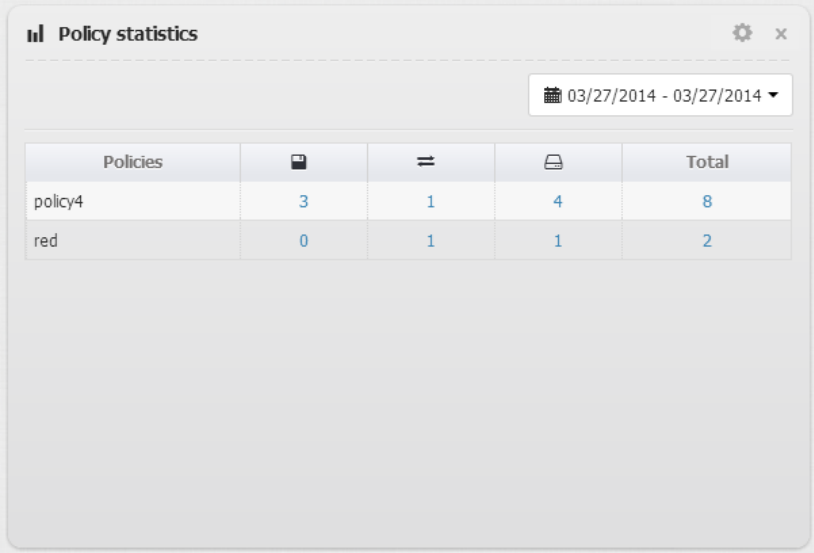
Widget parameters are described in the table:

Parameter	Description
Name	Widget name
Update interval	Period of data updating on the widget
Period	Time of data displaying

Note:

By pressing on number of persons and workstation (marked blue), System will go to **Persons** and **Workstations** tabs accordingly.

4.2.2.6 Policy statistics



Policy statistics widget

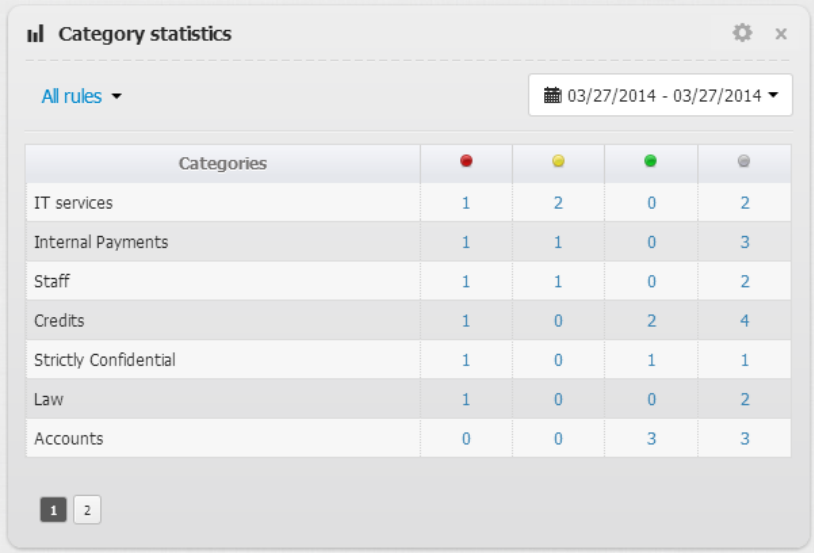
Widget parameters are described in the table:

Parameter	Description
Name	Widget name
Update interval	Period of data updating on the widget
Period	Time of data displaying
Policies	Policies to display the summary

Note:

Clicking on a number of copying policies violations (marked blue), System goes to **Events** tab displaying violations list.

4.2.2.7 Category statistics



Category statistics widget

Widget parameters are described in the table:

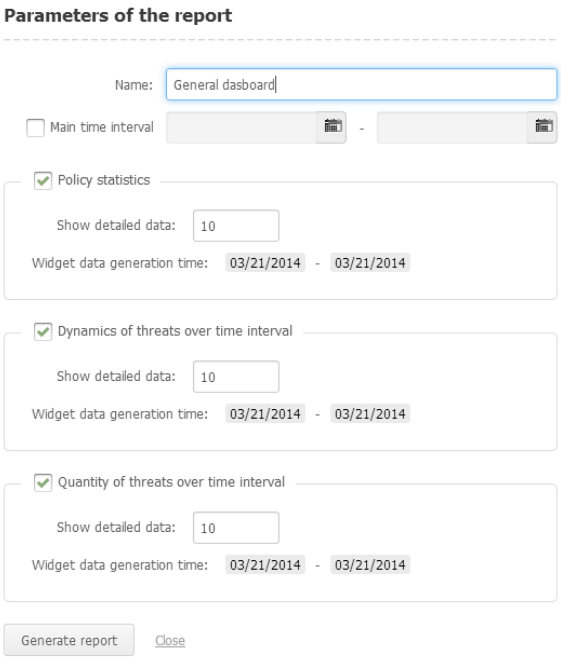
Parameter	Description
Name	Widget name
Update interval	Period of data updating on the widget
Period	Time of data displaying
Categories	Categories to display the summary

Note:

Clicking on number of violations of each category (marked blue), System will go to **Events** tab displaying violators list.

4.2.3 Dashboard Report

Reports are intended to visually represent statistical data on intercepted objects. Reports can be either outputted to PDF or HTML format or printed.



Report creating window

Report parameters are described in the following table:

Parameter	Description
Name	Report name
Main period	Period of report creating
Widget block	Indicates if the data from the widget are included to the report
Display detailed data	Indicates if the report displays certain objects. Specified quantity corresponds to the number of widget objects displayed in the report

User's actions:

- Creating dashboard report (see "Managing Reports").

4.3 Events Section

Reference information:

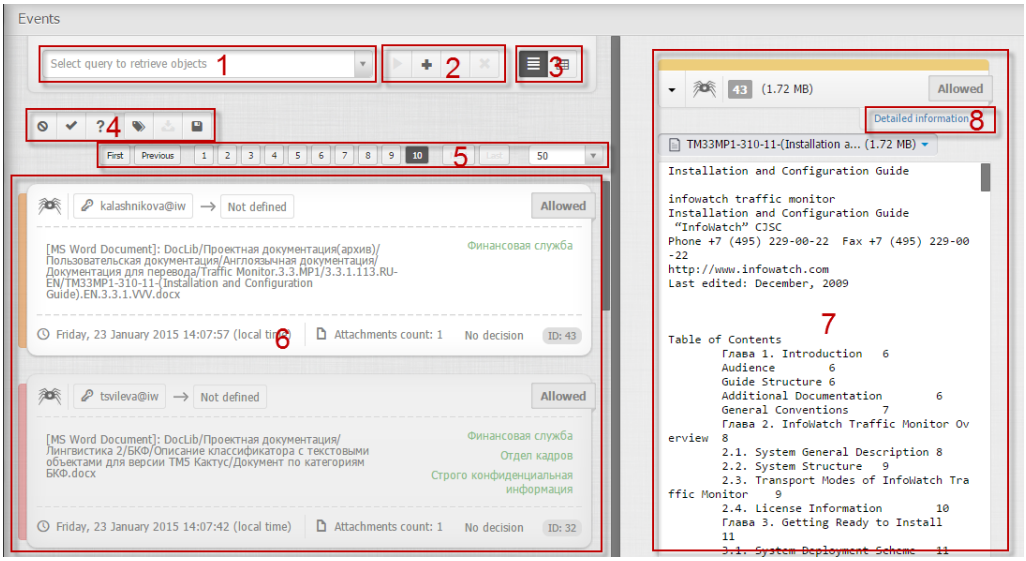
Event is the interception object of the network traffic.

The System creates events as a result of traffic interception during:

- data transfer made by employees to other persons;
- data publications in publicly accessible sources;
- copying the data to external devices;
- printing the data.

About the section:

The section contains a list of events (interception objects) and means to work with them.
The System can contain a large number of events, therefore a list of events is displayed according to filtering results.



Events section

This section contains the following elements:

Elements	Number on scheme	Purpose
Expanding list of queries	**1**	Contains a list of available queries used for filtering interception objects (see "Queries")
Toolbar for queries	**2**	Set of tools to manage queries
Buttons to select a style of events list displaying	**3**	Switching between displaying events in form of tiles or table
Toolbar for events	**4**	Set of tools to manage events
Pages navigation panel	**5**	Set of buttons to view page containing entries (if not all entries fit one

Elements	Number on scheme	Purpose
		page)
Events list	**6**	List of interception objects passed through the applied filter (see "Objects of Interception"). **Note:** Information on event tile characteristics see "Event Tile"
Shortcut event viewing form	**7**	Set of the most frequently used information on the event (see "Shortcut Event Viewing Form")
Detailed information button	**8**	A button calling a form with full set of data on event (see "Detailed Form of Events Viewing")

User actions:

- filtering events (see "Managing Dashboards", "Managing Widgets");
- viewing events (see "Managing Dashboards", "Managing Widgets");
- making decision on object (see "Making Decision on Object");
- adding/deleting a tag of an object (see "Adding and Deleting a Tag");
- sending an e-mail notification on event (see "Creating Notification on Event");
- saving an event (see "Saving an Event (for SMTP Objects)");
- dispatching blocked event (see "Dispatching Blocked Object");
- selecting a style of events display (see "Selecting Event Displaying Style")
- downloading information on selected events to the file (see "Export Events").

4.3.1 Queries

The objects checked by System are stored into the database. To view the information on objects stored in DB in the Management Console you should create and apply a query.

The query is a selection of intercepted objects confirming specified conditions.

The query contains following elements:

Element	Purpose
Condition (see "Condition")	This tab is intended to specify conditions to filter by
Display fields (see "Display Fields")	This tab is intended to select view fields to be displayed in event entries
Access parameters (see "Access Parameters")	This tab is intended to set access access parameters to the query
Extended mode (see "Extended Mode")	Intended for more flexible filter configuring

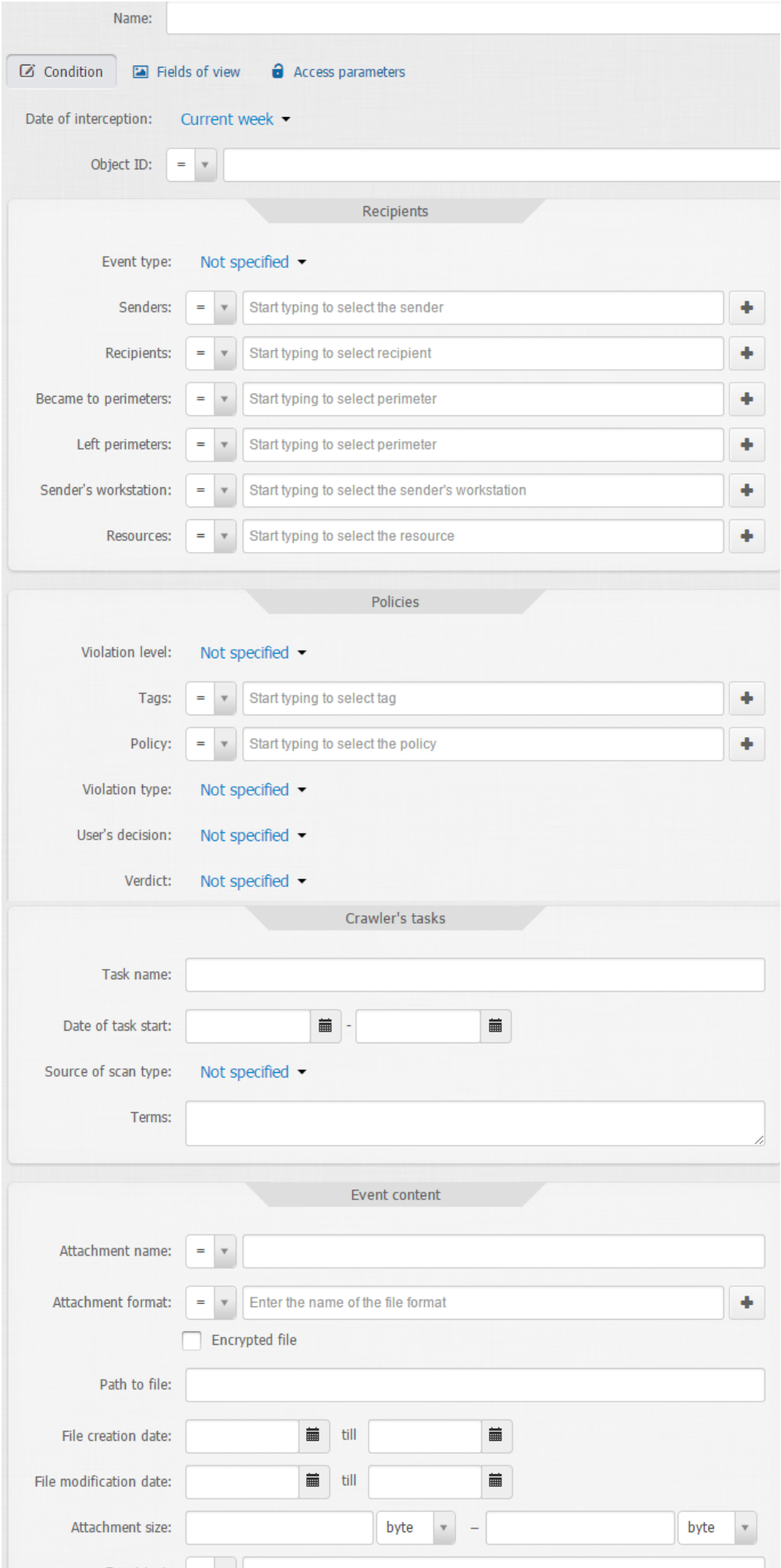
Note:

By default the number of events which can be found as a result of a query execution is limited to 10.000. For information on how to change this restriction, please refer to *«InfoWatch Traffic Monitor. Administrator's guide».*

User's actions:

- configuring a query (see "Events Filtering");
- defining view fields (see "Selecting Event's Display Fields").

4.3.1.1 Condition



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

The parameters of query condition are described in the following table:

Parameter	Description
	Parameter of attribute equality
	Parameter of attribute negation
Date of interception	The date of task creation. By default events for the current week are displayed.
Object ID	Unique events indicator. You can specify several values divided by commas.
Event type	The type of the event. Specify if the event belongs to a particular interceptor.
Senders	The list of object senders
Recipients	The list of object recipients
Entered perimeters	Perimeter the object sender belongs to
Left perimeters	Perimeter the object recipients belongs to
Sender's workstation	Workstation, from which an object has been sent
Resources	The resource the object was stored at
Violation level	The level of violation of the corporate security policy
Tags	Tags assigned to the object
Policy	The list of policies the object corresponds to
Violation type	The type of rule which was violated
User's decision	The decision which user made for the object
Verdict	The decision which System made for the object
Task name	Name of the scanning task
Date of task start	Date of the task initiation
Source of scan type	Type of the source to scan
Attachment name	Name of the attachment
Attachment format	Format of data the object contains
Encrypted file	Whether file is encrypted or not
Path to file	Destination location for the object
File creation date	Date of file creation
File modification date	Date of file modification

Parameter	Description
Attachment size	Size of data the object contains
Event text	The text the object contains. Events whose text contains all specified words irrespective of their order will be found. If a negation parameter is specified for the attribute, events whose text contains all specified words will be excluded from search results. If morphological index construction is enabled in database settings, search for all grammar forms of specified words is performed (for more details on this setting, see *«InfoWatch Traffic Monitor. Administrator's guide»*). The search is not case-sensitive. **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.
The result of the analysis	The correspondence of the object to some element from the classification database
Any analysis technology	Correspondence to classification database does not matter

One can assign positive or negative parameters to attributes creating query conditions:

- For query result to include required attribute, set equality parameter .
- To exclude required attribute from query results, set negation parameter .

Parameters of equality or negation are available for the following attributes:

- Object ID;
- Senders;
- Recipients;
- Entered perimeters;
- Left perimeters;
- Sender's workstation;
- Resources;
- Tags;
- Policy;
- Attachment name;
- Attachment format;
- Event text;
- The result of the analysis.

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

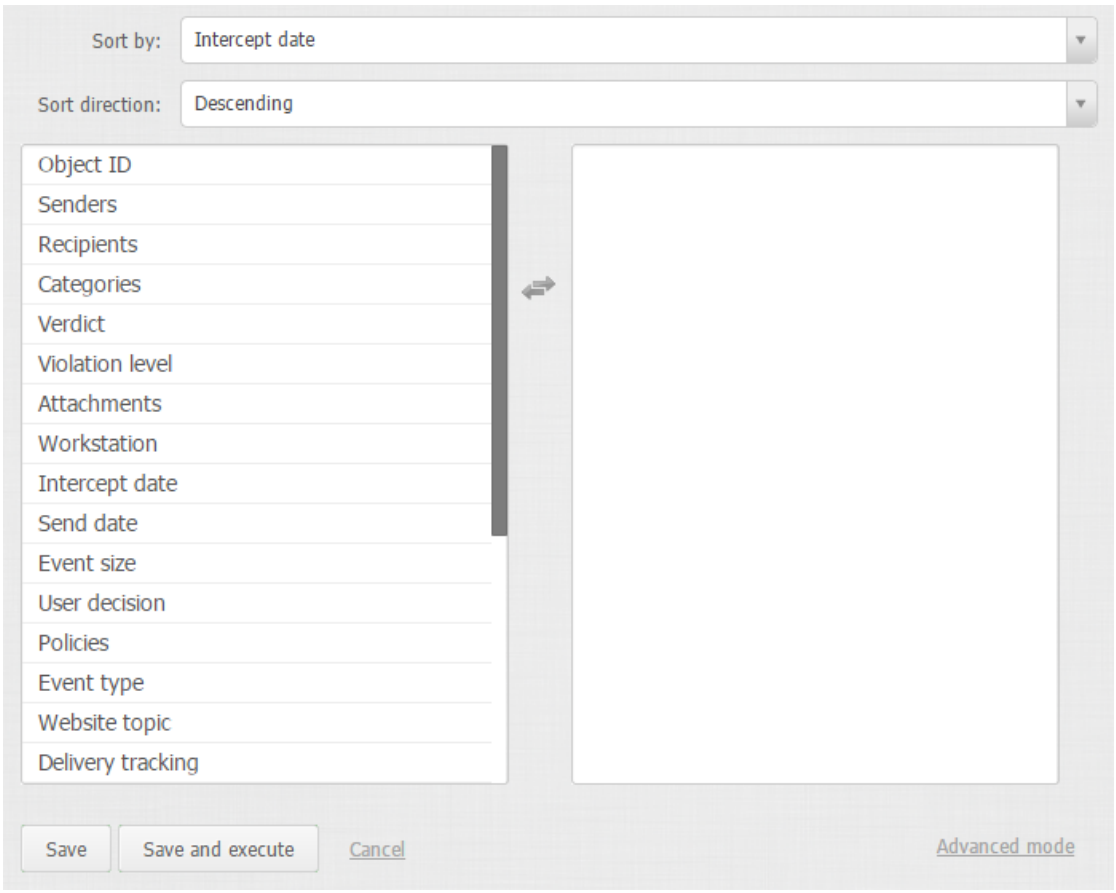
excluded from search results.

User's actions:

- "Query Creation in Standard Mode";
- "Query Creation in Extended Mode".

4.3.1.2 Display Fields

The left tab displays a list of available event attributes, whereas the right one represents attributes which will be displayed either at the event tiles or in the events table and unloaded in xslx. In case no attribute is chosen, all the attributes will be displayed in the event table when exported.

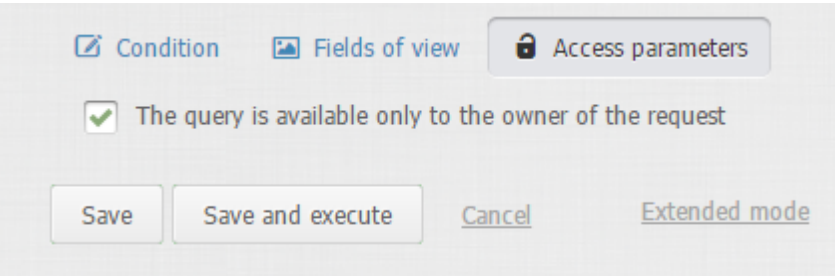


Events section, **Display field** tab for selected query

User's actions:

- "Selecting Event's Display Fields".

4.3.1.3 Access Parameters



Events section, **Access Parameters** tab for selected query

To forbid viewing and editing query by other users:

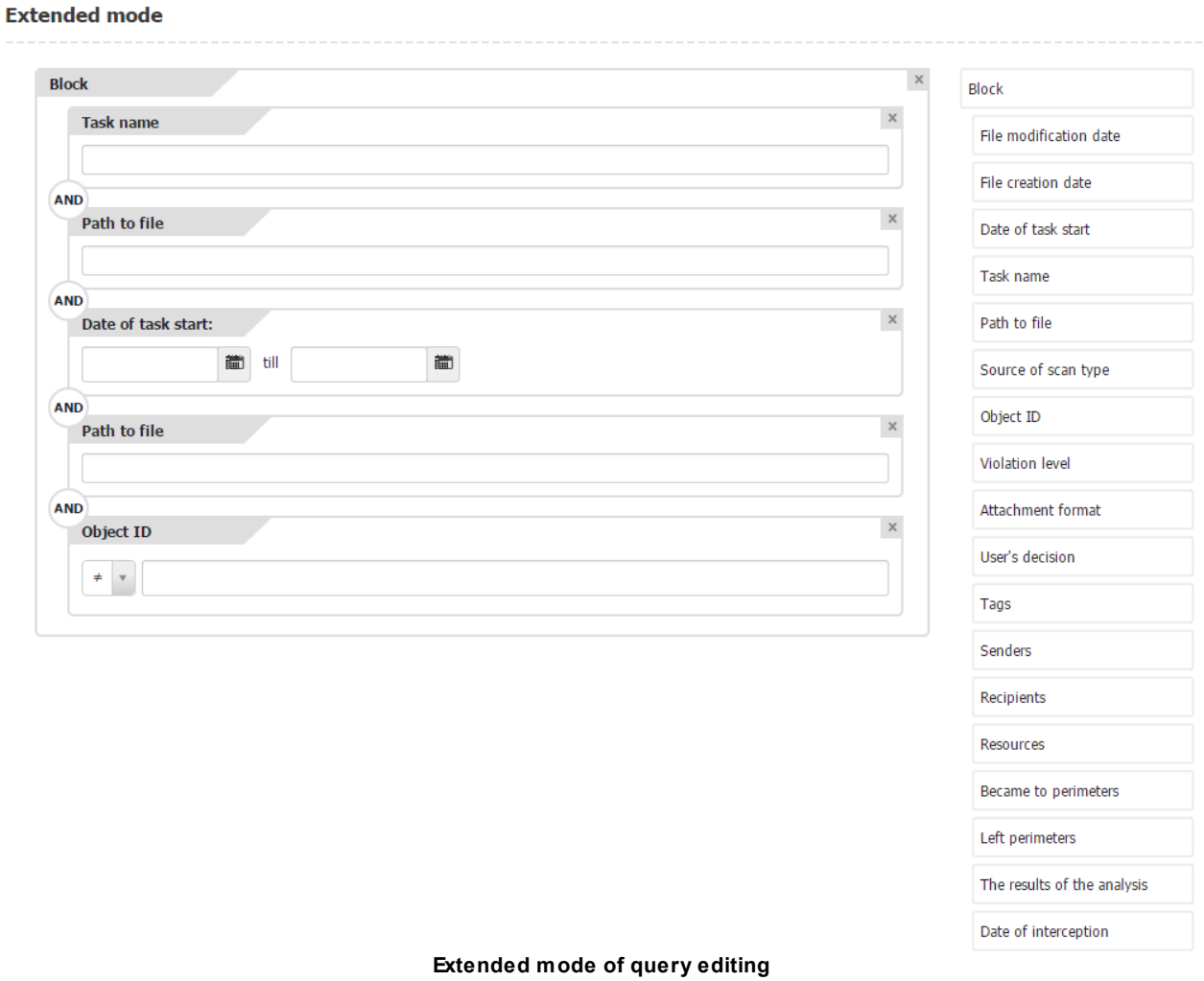
1. Check the **The query is available only to the owner of the request** box.
2. Click **Save**.

To permit viewing and editing query by other users:

1. Unchek the **The query is available only to the owner of the request** box (by default the box is checked).
2. Click **Save**.

4.3.1.4 Extended Mode

The extended mode is intended to show the detailed query configuring.



Extended mode of query editing

These are the following items used in query creating :

- list of events attributes is a set of attributes assigned to the intercepted object;
- *Block* element is a container intended for building the logical construction of a query.
-

- parameter of attribute equality. Indicates that event filtering will take place considering events

which have attributes with this parameter assigned.

- ≠ - parameter of attribute negation. Indicates that in filtering results there will be no events with the attributes, to which parameter has been assigned.

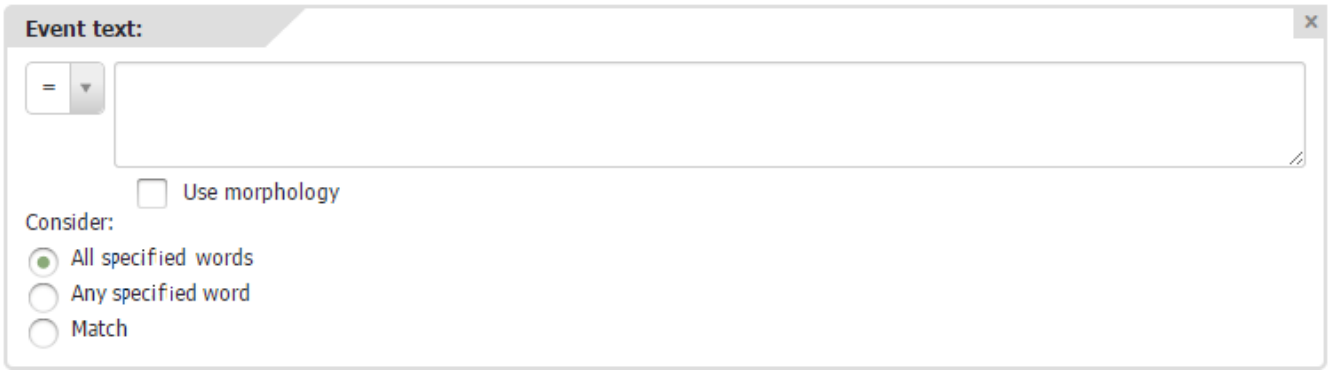
In the extended mode, you can also perform a flexible text search for the events.

You can select one of the following search modes:

- All specified words – events whose text contains all specified words in any order will be found.
  If the condition is denied, events whose text contains all specified words will be excluded from search results.

- Any specified word – events whose text contains at least one specified word will be found.
  If the condition is denied, events whose text contains at least one specified word will be excluded from search results.

- Exact phrase – events whose text contains all listed words in the specified order will be found.
  If the condition is denied, events whose text contains all listed words in the specified order will be excluded from search results.



Specifying conditions for event text search

If the **Use morphology** option is selected, search for all grammar forms of specified words will be performed. If the option is deselected, the query result will contain only those events whose text contains specified words in a given form.

> **Note:**
>
> The **Use morphology** option is available only if morphological index construction is enabled in database settings. For more details on this setting, see *«InfoWatch Traffic Monitor. Administrator's guide».*

Specifics of text search:

- Words should be divided with a space.
- Search is not case-sensitive.

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

User's actions:

- "Query Creation in Extended Mode".

4.3.2 Objects of Interception

The list of events displays intercepted objects which confirm query conditions (see "Queries").

Information on the event is represented in following elements:

- in event tile (or event entry in the table) the general data is displayed;
- in short event viewing form the most frequently needed information is displayed;
- in detailed form of events viewing all available information is displayed.

Object attributes are listed in the following table:

Element	Description
Object ID	Unique object identifier in the System
User Decision	Decision which the user made for the event. Available values: • *No decision* • *Violation* • *No violation* • *Requires additional proceeding*
Event type	Source of actions which resulted event creation. Available values: •  - *FTP* (sending files by FTP protocol) •  - *File exchange* (copying files to\from device) •  - *Incoming email* (receiving a message by e-mail: POP3 and IMAP protocols, MAPI interface) •  - *E-mail* (sending messages by e-mail: SMTP protocol, MAPI interface) •  - *ICQ, Skype, MS Lync, Mail.Ru Agent, XMPP, Yahoo* (sending or receiving messages using instant messengers) •  - *Print* (sending file to print) •  - *Web-mail* (publishing data to the internet - POST-requests to web-resources) •  - *Crawler* (data storing in SharePoint 2007/2010 file storage, shared network resources, and local disks of workstations)
Send date	Date and time when mail server received the mail (for the e-mails only)
Senders	List of traffic senders

Element	Description
Workstation	Name of workstation the traffic was sent from
Recipients	List of traffic recipients
Policies	List of policies actuated in analysis of this object
Categories	List of categories assigned to this object
Website topic	Type of inappropriate resource visited by employee
Tags	List of tags assigned to this object
Intercept date	Date and time when the System intercepted the traffic
Size	Object size (in kilobytes)
Violation level	Characteristics of the violation assigned to the object. Available values: • *None* - displayed by grey (■) color on the tile • *High* - displayed be red (■) color on the tile • *Medium* - displayed by orange (■) color on the tile • *Low* - displayed by green (■) color on the tile
Delivery tracking	Marks if the message was delivered (only for SMTP letters in blocking mode of System operation - see *InfoWatch Traffic Monitor. Administration Guide"*). Available values: • *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"). Available values: • *Allowed* • *Forbidden* • *Quarantine* **Note:** Events with *Deleted* verdict assigned are deleted from the System and are not displayed in the Management Console
Capture server	The name of the server which intercepted the object

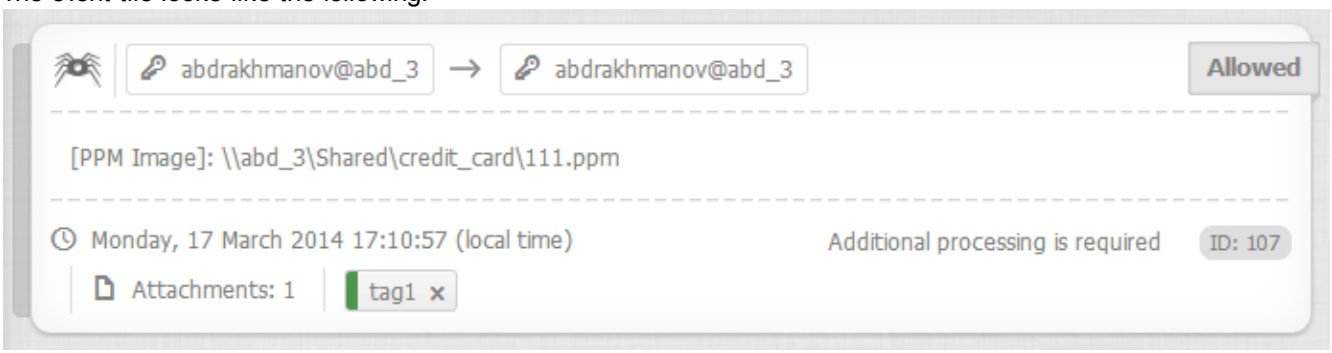
See also:

- Event Tile;
- Shortcut Event Viewing Form;

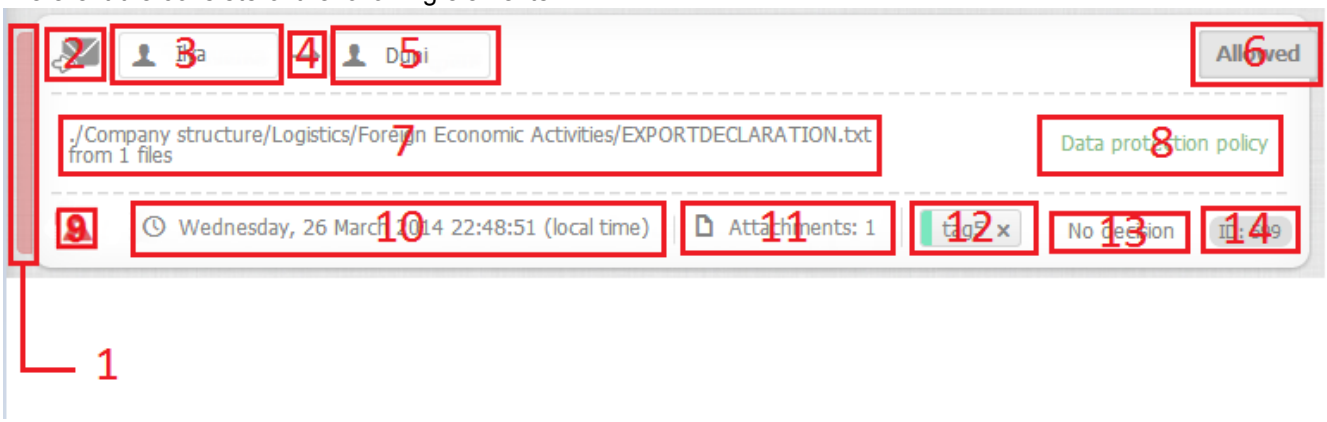
- Detailed Form of Events Viewing.

4.3.2.1 Event Tile

The event tile looks like the following:



The event tile consists of the following elements:



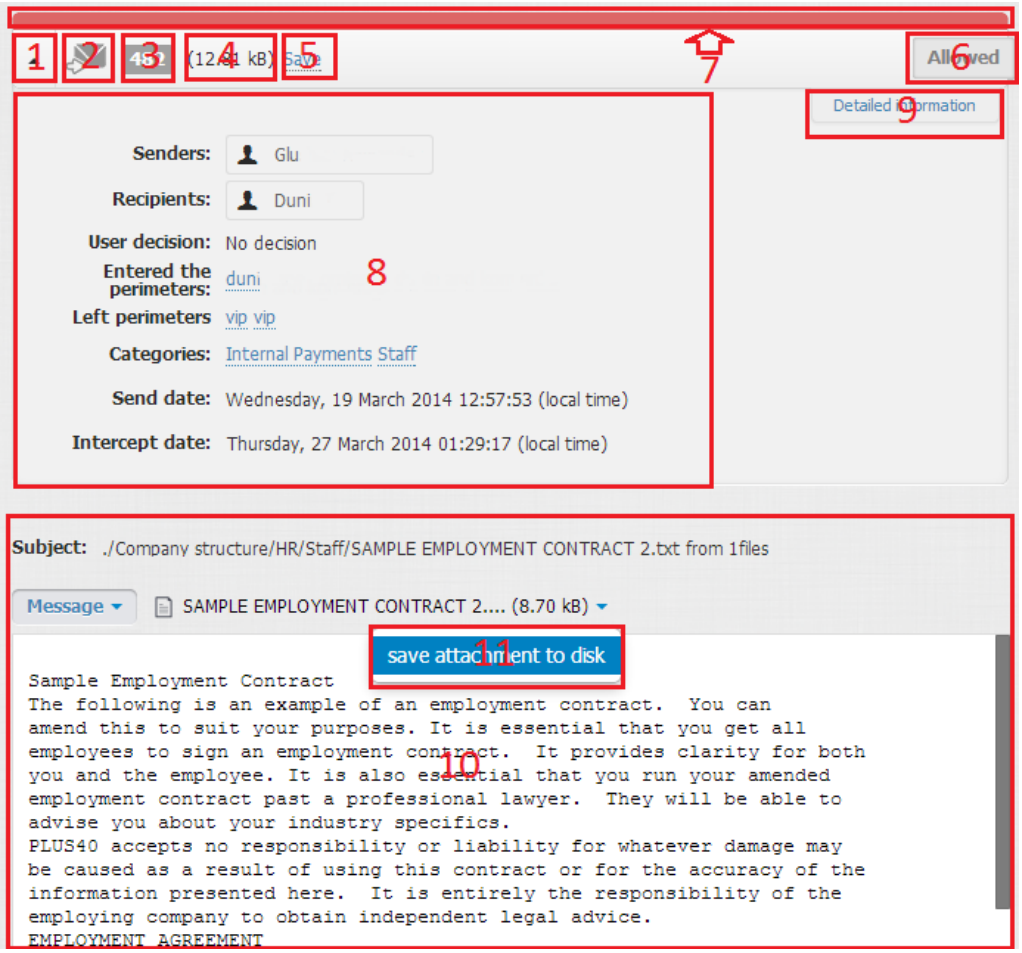
Here:

1 - Color of violation level
2 - Event type
3 - Sender(s)
4 - Traffic direction
5 - Recipient(s)
6 - Verdict
7 - Event preview
8 - List of triggered policies
9 - Errors indicator
10 - Date of event creation
11 - Attachments indicator
12 - Assigned tags
13 - User decision
14 - Object ID

Note

Event preview displays a short information on the event origin - for example, in this case the sending of *Text_object_samples.txt* file is shown.

4.3.2.2 Short Event Viewing Form



Events section, short form of viewing the selected event

These are the following items of the short event viewing form:

Item	№ on schema	Description
Button of displaying / hiding object attributes	1	Click to open or hide object attributes
Icon of object type	2	Displays a graphic image of object type
Object ID	3	Displays unique identifier of the intercepted object
Size of shadow copy	4	Displays a size of the shadow copy of the intercepted object
Button of saving the shadow copy	5	Click to save the shadow copy of the object to disk
Verdict	6	Displays verdict of the System on the intercepted object
Violation level	7	Displays color key of violation level assigned to the object
Object attributes	8	Extracted attributes of the intercepted object

Item	№ on schema	Description
Button calling the detailed event viewing form	9	Click to go to to the detailed viewing form
Field of viewing the event and attachments	10	Displays event contents: text and attachments (depending on tab)
Button of saving the attachment	11	Located on attachments tab. Click to save attachment to disk

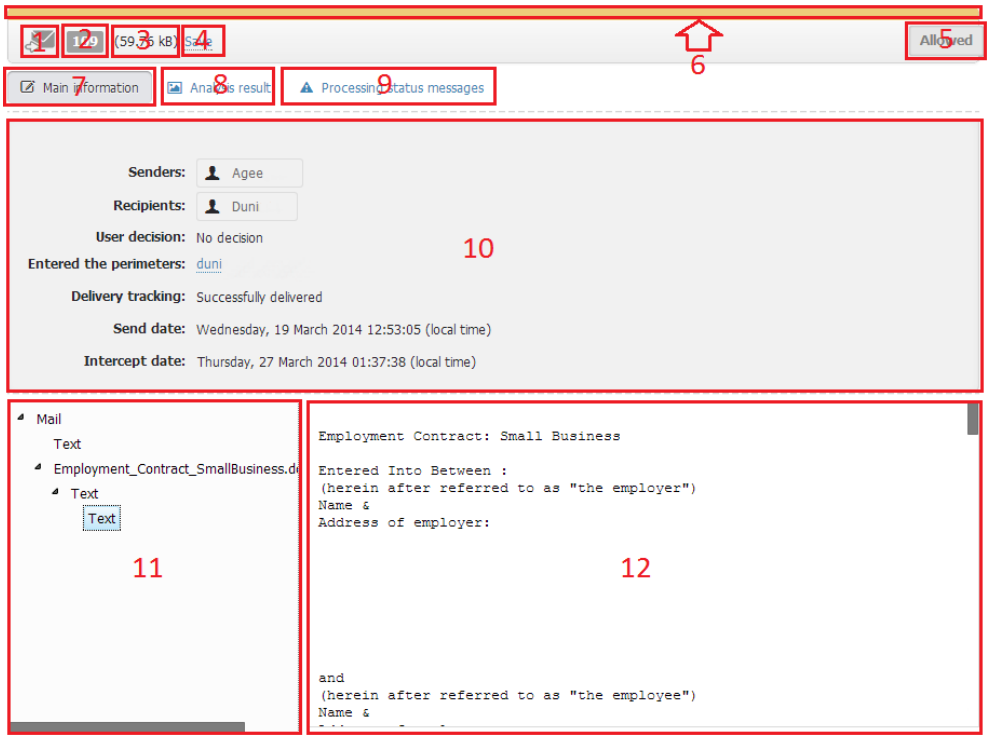
Warning!

The set of items on the short event viewing form can slightly vary depending on extracted attributes.

User's actions:

- Review the general information on the event (see "Viewing Short Event Form").

4.3.2.3 Detailed Form of Events Viewing



Events section, the detailed form of displaying the selected event

There are three tabs in the detailed event viewing form, each tab has its own purpose:

Entity	№ on schema	Description
Event type	1	**Event type** attribute value
ID	2	**Object ID** attribute value
Event size	3	**Event size** attribute value
Save button	4	Calls for a dialog box of object saving
Verdict	5	**Verdict** attribute value
Violation level	6	**Violation level** attribute value
General information tab	7	Tab with general information. Contains information represented in the short form of event viewing
Analysis results tab	8	Tab with results of event analysis. Contains data on analysis results: activated policies, assigned categories and their elements
Processing messages tab	9	Tab with object processing messages. Contains system messages on object processing and troubles if they arose
Panel of selected tab viewing	10	Viewing the information depending on selected tab
Panel with extracted attachments	11	Viewing names of extracted attachments
Panel of extracted attachments viewing	12	Viewing extracted attachments

User's actions:

- "Viewing Detailed Event Form".

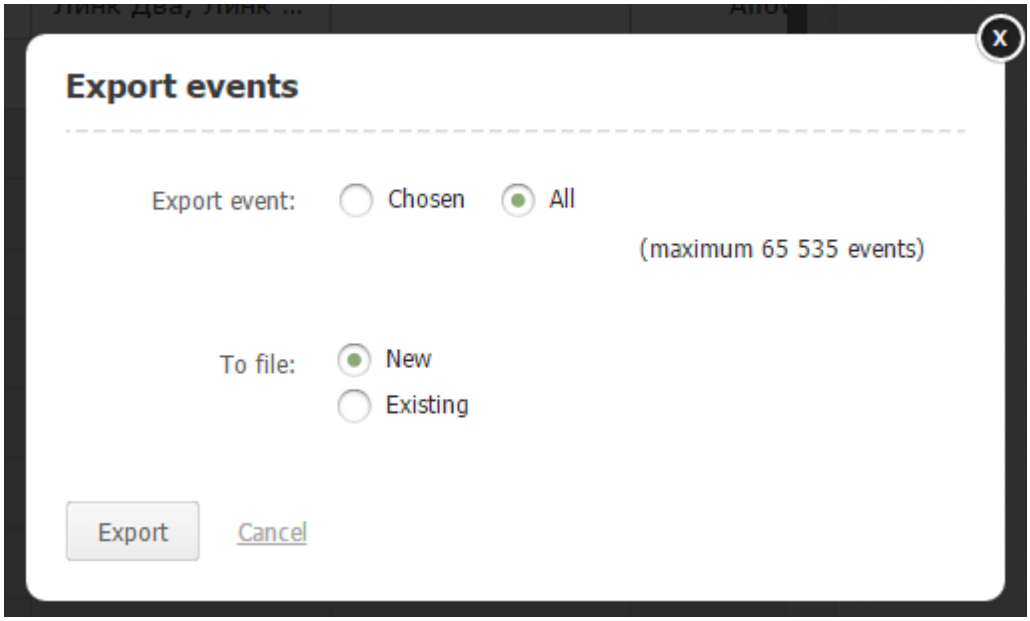
4.3.3 Export Events

To export events:

1. Go to **Events** tab.
2. Click  icon on toolbar.
3. Select query to retrieve objects.

To export all events:

1. Click  **Export events** icon on the panel.
2. In the pop-up window check, that **All** option is selected.



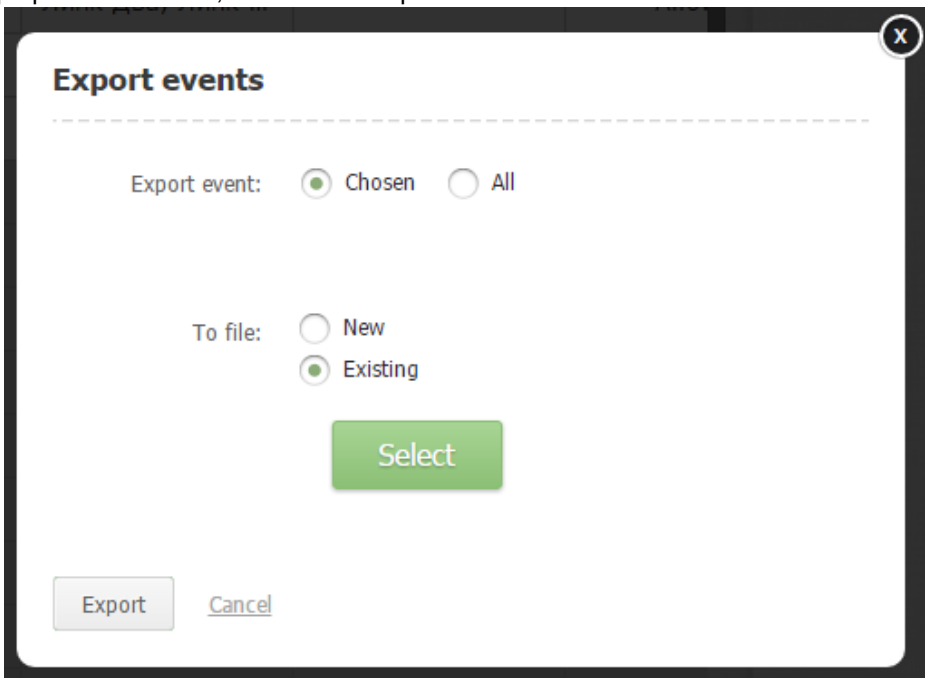
3. Specify output file:
   a) To create a new file select **New**.
   b) To use existing file select **Existing**, then click **Select**. In the opened dialog window specify the file and click **Open**.

> **Note**
> Output file should have format of MS Excel 2003 (xls) or MS Excel 2007 (xlsx).

4. Click **Export** .

To export one or several events:

1. Choose event/events you want to export.
2. Click  **Export events** icon on the panel.
3. In the pop-up window check, that **Chosen** option is selected.



4. Specify output file:
   c) To create a new file select **New**.
   d) To use existing file select **Existing**, then click **Select**. In the opened dialog window specify the file and click **Open**.

> **Note**
>
> Output file should have format of MS Excel 2003 (xls) or MS Excel 2007 (xlsx).

5. Click **Export**.

Then in the upper-right of the window the notifying message will be displayed. When the downloading will be ended, click **download** to open a newly created or specified file.

4.4 Classifier Section

Reference information:

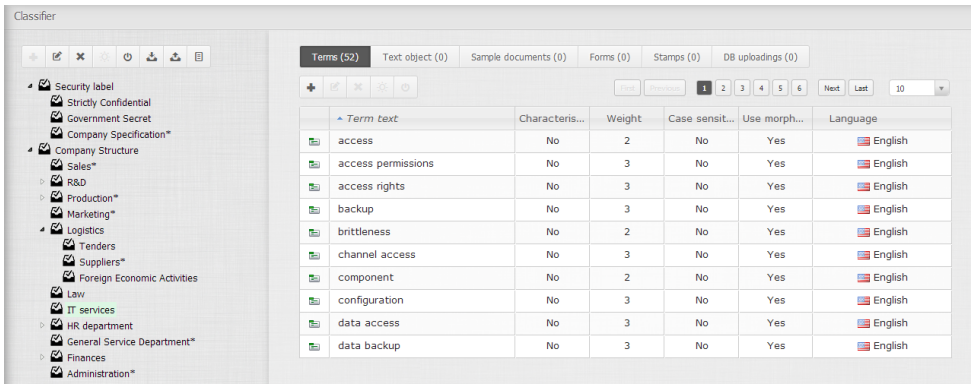
Classifier (classification database) is a set of data required for linguistic analysis.

The classifier contains a list of *categories* classifying possible violations of the security policy. If there is an element belonging to some category presented in the text, then the System can correlate the text with this category.

For example, the *Finance* category contains financial terms (*payment*, *investors*, *prices*, etc.). Thus the presence of the terms *payment*, *investors*, *prices* in the text allows to correlate it with the *Finance* category.

About section:

The section contains a description of the Classifier (classification database).



Section **Classifier**

The section contains the following elements:

Element	Purpose
List of categories	Set of subject areas which the intercepted objects can be corresponded to
List of terms	Set of terms for the selected category
List of text objects	Set of text objects for the selected category
List of sample documents	Set of sample documents for the selected category

Element	Purpose
List of sample forms	Set of sample forms for the selected category
List of sample stamps	Set of sample stamps for the selected category
List of sample database uploadings	Set of sample database uploadings for the selected category
Toolbars	Set of tools for categories and category elements
Page navigation panel	Set of buttons for browsing pages containing entries (if not all entries can be placed on one page)
Control of the entries number	Drop-down list to set the number of entries per page

User's actions:

- Creating Classifier Base;
- Grouping the Confidential Data by Subject Areas;
- Defining the Confidential Data;
- Enabling and Disabling the Analysis on Subject Areas;
- Enabling and Disabling the Analysis on Confidential Data;
- Exporting and Importing the Classifier Database.

4.4.1 Categories

Reference information:

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



List of categories

Note

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

Category attributes are described in the following table:

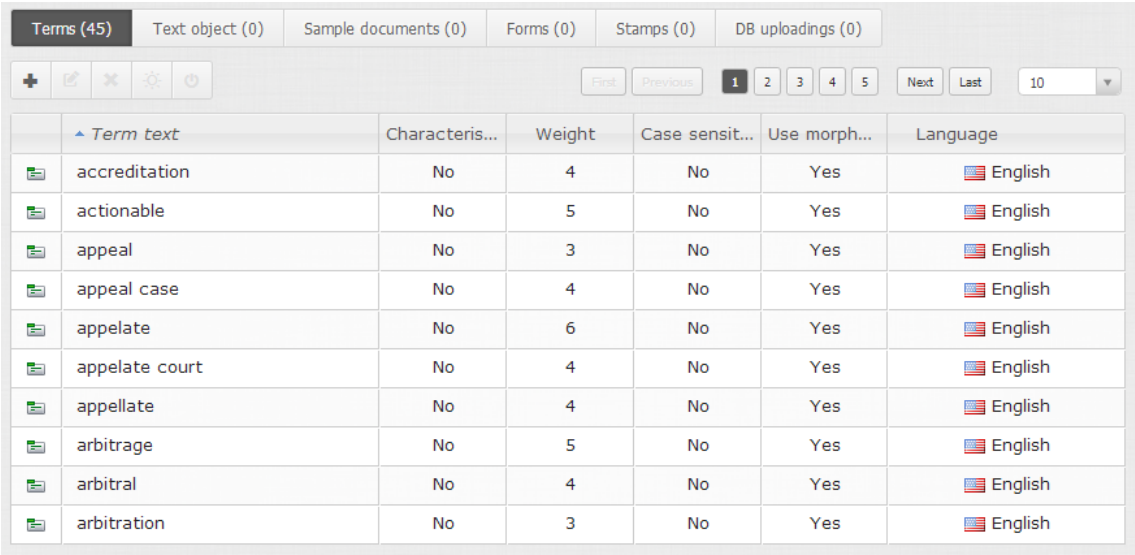
Parameter	Description
Name	Category name
Status	Indicates if this category is used in the traffic analysis . There are active ( icon) and inactive ( icon) categories
Weight	The *Weight* attribute value specified by default for all terms of the category
Language	The language of category terms
Use morphology	Indicates if the morphological changing of terms is taken into account in the traffic analysis
Case sensitive	Indicates if the terms case is taken into account in the traffic analysis
Quotation threshold for sample document text data of the category	The percentage of the reference document that is sufficient for referring the intercepted object to this category. For detection performed by the Text Objects module
Quotation threshold for sample document binary data of the category	The percentage of the reference document that is sufficient for referring the intercepted object to this category. For detection performed by the Digital Fingerprints module
Description	Optional note
Creation date	The date and time of category creation
Change date	Date and time of the last modification of the category

User's actions:

- managing categories (see "Grouping the Confidential Data by Subject Areas").

4.4.2 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.



Term text	Characteris...	Weight	Case sensit...	Use morph...	Language
accreditation	No	4	No	Yes	English
actionable	No	5	No	Yes	English
appeal	No	3	No	Yes	English
appeal case	No	4	No	Yes	English
appelate	No	6	No	Yes	English
appelate court	No	4	No	Yes	English
appellate	No	4	No	Yes	English
arbitrage	No	5	No	Yes	English
arbitral	No	4	No	Yes	English
arbitration	No	3	No	Yes	English

List of terms

Term attributes are described in the following table:

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
Status	Indicates if this term is used in the traffic analysis
Characteristic	If this attribute is enabled (*Yes* value), 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 terms case is taken into account in the traffic analysis
Use morphology	Indicates if the morphological changing of term is taken into account in the traffic analysis
Language	The language of the term
Creation date	The date and time of term creation
Change date	Date and time of the last modification of the term

Note

Case sensitive and *Use morphology* parameters are being applied for terms from the same parameters of category. Terms parameters can be changed and saved as a separate procedure. Re-editing these parameters for category, changes will not be repeatedly applied for terms.

Note

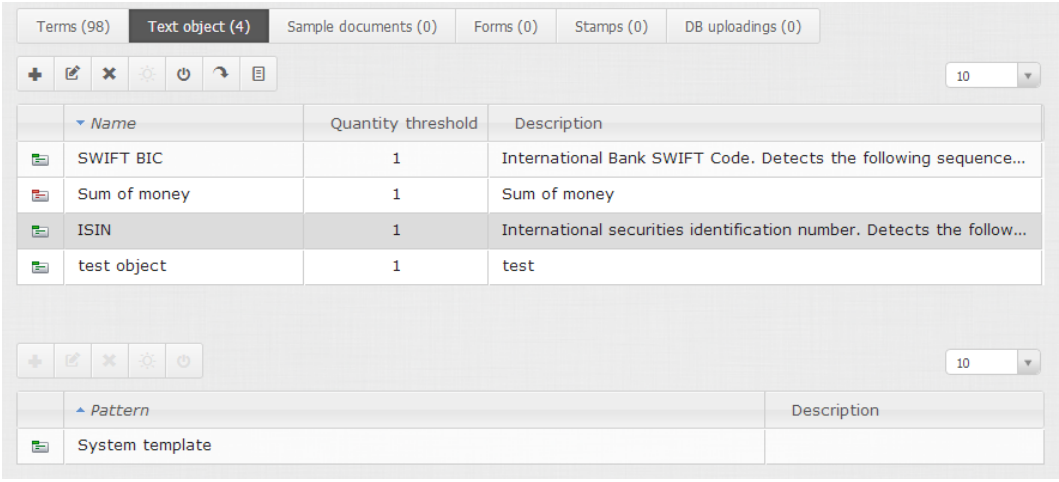
Creation Date and *Change Date* attributes are available only in editing regime

User's actions:

- managing terms (see. "Creating Terms").

4.4.3 Text Objects and their Values

Reference information:
The text object is a text information extracted from the object body and attachments. Contains no formatting or markup elements. Used for analysis and search tasks solution.



List of text objects

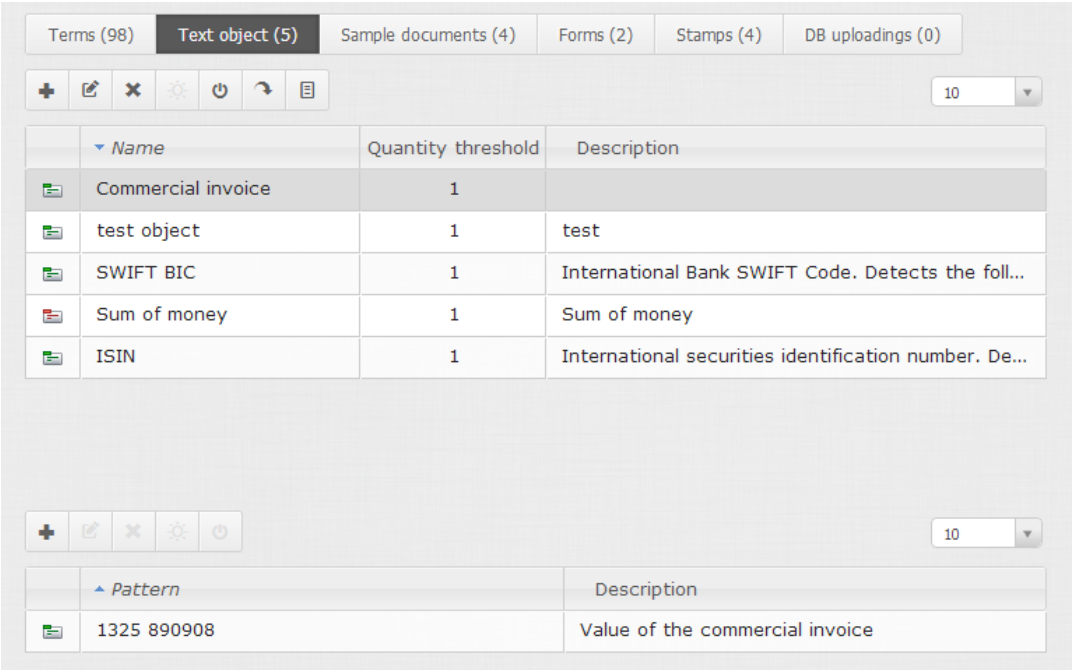
The text object attributes are described in the following table:

Parameter	Description
Name	Category name
Status	Indicates if the text object is used in the traffic analysis
Quantity threshold	The minimum number of text object citations in the text which results in assigning the text object to the event
Description	Optional note

Note

Creation Date and *Change Date* attributes are available only in editing regime

Each of the text objects in the System can have one or more *values*.
For the selected text object there is a values list displayed below the text objects list.



The text object attributes are described in the following table:

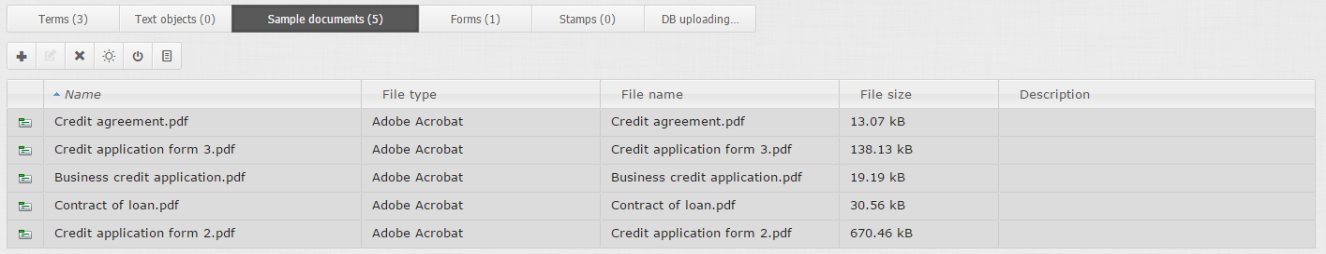
Parameter	**Description**
Description	Optional note
Status	Indicates if this text object value is used in the traffic analysis.
Type	Indicates if the pattern (*String* type) or regular expression (*Regular expression* type) will be used in analysis
Pattern	The exact meaning of the text object **Note:** the specified template *example@company.com* finds the only exact matching - *example@company.com*
Regular expression	Configurable template. For more information see the Internet article " Regular Expression Language"
Validation text	Example of text for finding the regular expression

User's actions:

- managing text objects and their values (see "Creating Text Objects and their Values");
- adding system text object to the category (see "Creating Text Objects and their Values").

4.4.4 Sample Documents

Reference information:
Sample document is a document containing quotes for text analysis. Sample documents may be samples of orders, financial statements, contracts, and other confidential documents. Sample documents are stored in the system as digital prints, their text is not available for either users or System administrators.



List of sample documents

Attributes of sample document are described in the following table:

Parameter	Description
Name	The name of the sample document
Status	Indicates if this sample document is used in the traffic analysis.
File type	Type of the file: text, image, etc.
File name	The name of the file that was loaded as a sample document
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 (documents texts)
Binary data quotation threshold	The percentage of the sample document that is sufficient for referring the intercepted object to this sample document. For detection of the binary objects (images, executable files, etc.)
Description	Optional note
Creation date	The date and time of the sample document creation
Change date	Date and time of the last modification of the sample document

Note

Creation Date and *Change Date* attributes are available only in editing regime

User's actions:

- managing sample documents (see "Creating Sample Documents").

4.4.5 Sample Forms

Reference information:

The sample form is a formsheet which completed version is searched in the network traffic. Sample forms are stored in the System as digital fingerprints, their text is not available for either users or System administrators

The reference forms may be surveys, questionnaires, and other documents completed in a predefined form.

Technically the reference form is a file each line of which contains one form field. Rows are separated by line break. The form contains at least 2 fields.

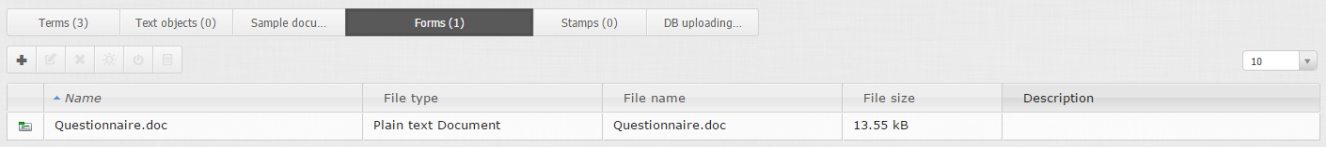
Warning!
To match an interception object with the sample form category:

- the object text should contain at least one field from the reference form;
- if the number of fields detected in the object text is more than one, then fields should replicate the order of the digital print uploaded to the System;
- if a detection of completed forms only (*Detect only filled forms* attribute) is set, then at least one character should be placed between one pair of adjacent rows.

The principle of technology is:

1. The searching for form fields names is performed.
2. Then their order is checked.
3. Then, if necessary, the presence of text between form fields is checked.

That defines whether the form is filled out or not.



List of sample forms

Attributes of sample forms are described in the following table:

Parameter	Description
Name	The name of the sample form
Status	Indicates if this sample form is used in the traffic analysis .
Detect only filled forms	Indicates if the completed sample form only is detected
File type	Type of the file: text, image, etc.
File name	The name of the file that was loaded as a sample form
Description	Optional note
Creation date	The date and time of the sample form creation

Change date	Date and time of the last modification of the sample form

Note

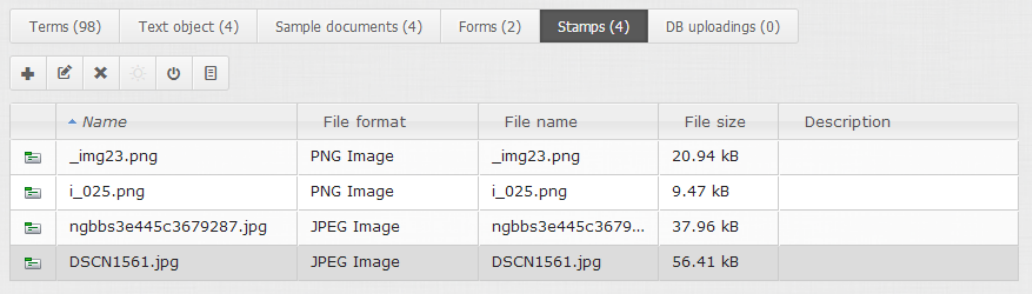
Creation Date and *Change Date* attributes are available only in editing regime

User's actions:

- managing sample forms (see "Creating Sample Forms").

4.4.6 Sample Stamps

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



List of sample stamps

Attributes of sample stamp are described in the following table:

Parameter	Description
Name	The name of the sample stamp
Status	Indicates if this sample stamp is used in the traffic analysis.
File type	Type of the file: text, image, etc.
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	Optional note
Creation date	The date and time of the sample stamp creation
Change date	Date and time of the last modification of the sample stamp

Note

Creation Date and *Change Date* attributes are available only in editing regime

User's actions:

- managing sample stamps (see "Creating Sample Stamps").

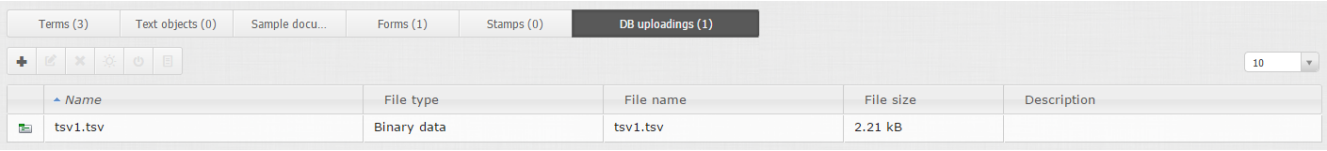
4.4.7 Sample Database Uploadings

Reference information:
The sample database uploading is a part of a database containing citations for text search. The sample database uploadings may be lists of salaries, other personal data, etc.

Warning!

For the correct operation the sample database uploading should have the following characteristics:

- The number of columns is no more than 32.
- The number of words in one cell 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).



List of sample database uploadings

Attributes of sample database uploading are described in the following table:

Parameter	Description
Name	The name of the sample uploading
File type	Type of file
File name	The name of the file that was loaded as a sample database uploading
File size	The size of the file that was loaded as a sample database uploading
Description	Optional note
Status	Indicates if this sample database uploading is used in the traffic analysis .
Rules of table column proceeding	Describes the logical correlation between table columns and the minimal number of non-blank rows in a table required to actuate the sample uploading

Parameter	Description
Creation date	The date and time of creation of the sample DB uploading
Change date	Date and time of the last modification of the sample DB uploading

Note

Creation Date and *Change Date* attributes are available only in editing regime

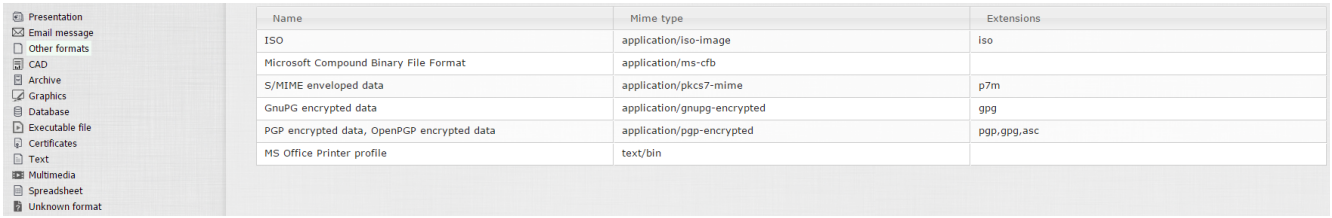
User's actions:

- managing sample database uploadings (see "Creating Sample Database Uploadings")

4.5 Files Section

About section:

The section contains a catalogue of files which are detected by the System.



Files Section

Warning!

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

The section contains the following elements:

Element	Purpose
The list of file types	Located in the right part of the workspace. Contains a set of subjects which use one or more files formats. ***For example,*** the Archive type contains files with formats ZIP, RAR and so on.
List of files of the selected type	• Located in the right part of the workspace. Contains attributes list for all files of this type which are detected in the System. It is a table, which contains descriptions: **Name**, **Mime type**, **Extensions**.
Create policy button	Creates a data protection policy with either the selected file or selected file type as a secured object **Note:** Clicking the button opens a form for adding a new policy in the **Policies** section

User's actions:

- Creating a Policy.

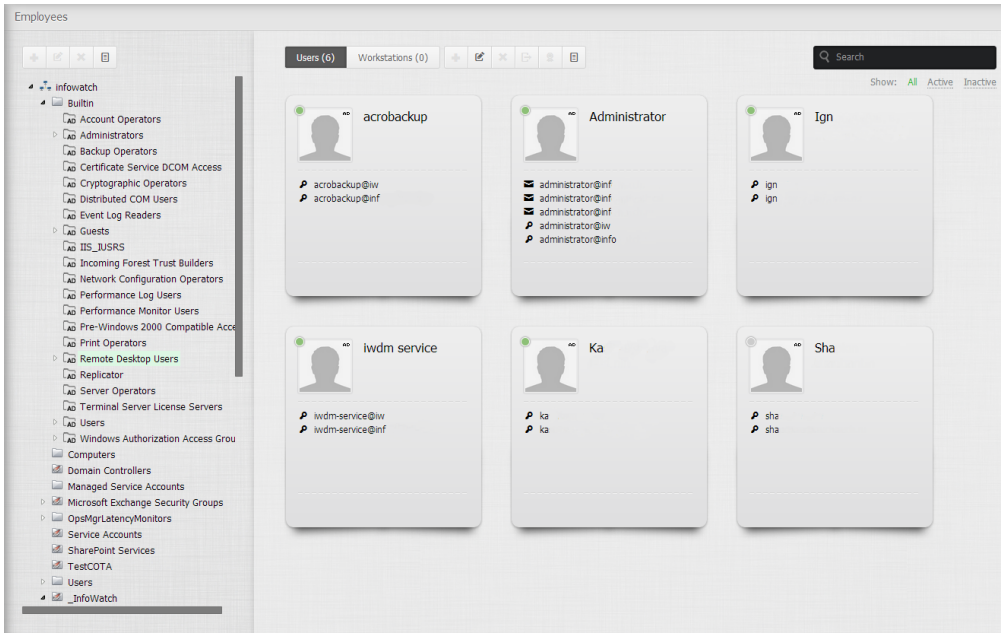
4.6 Persons Section

Reference information:

The lists of users and workstations facilitates work with intercepted objects to security officer. It happens due to the accounting of information about senders, recipients (persons), and workstations in special catalogues.

About section:

The section contains a catalogue of persons and workstations of a company information system.



Section **Persons**

Warning!

If the current license is exceeded by the number of persons whose events are processed, the following message is displayed at the top of the browser window:

Warning! Number of employees exceeds license limit at 212

This does not change the performance of a System: the message is for your information.

The number of employees whose events are processed in the System is equal to the number of employees who sent any type of traffic in 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 document *"InfoWatch Traffic Monitor. Administrator Guide"*).

The section contains the following elements:

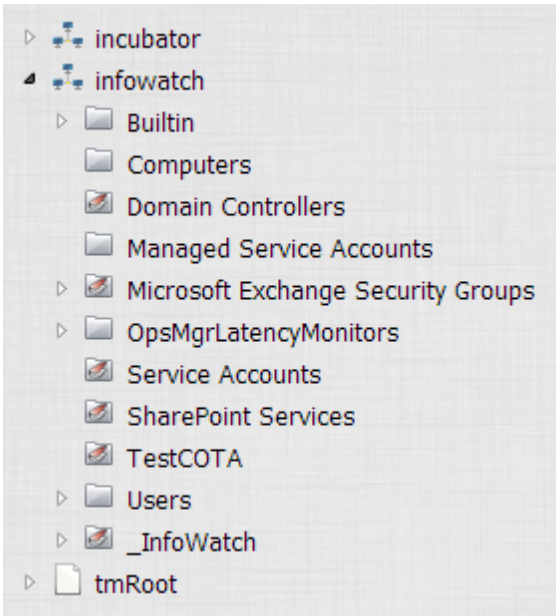
Element	Purpose
Groups of persons/workstations from Active Directory	Located in the left part of the workspace. Contains the structure of the organization from Active Directory.
Groups of persons/workstations	Located in the left part of the workspace. Contains the structure of the

Element	Purpose
created by means of the Traffic Monitor	organization created by means of the Traffic Monitor.
Persons tab for selected group	Located in the right part of the workspace. Contains a list of persons included to the selected group.
Workstations tab for selected group	Located in the right part of the workspace. Contains a list of workstations included to the selected group.
Toolbars	Set of tools for groups, persons, workstations.
Search box	Filtering of users and workstations.
Show filter	Filtering of users and workstations by *Status* attribute. Available only for groups of persons and workstations obtained from Active Directory.

User's actions:

- Creating a Group of Persons and Workstations;
- Creating a List of Persons and Workstations;
- Viewing a Summary on Person or Workstation;
- Viewing Events of Person or Workstation;
- Adding a Person or Workstation to the Policy;
- Adding a Status to Person or Workstation;
- Adding a Person or Workstation to the Perimeter.

4.6.1 Groups of Persons and Workstations



Note:

Groups for which syncronization was performed are marked with .

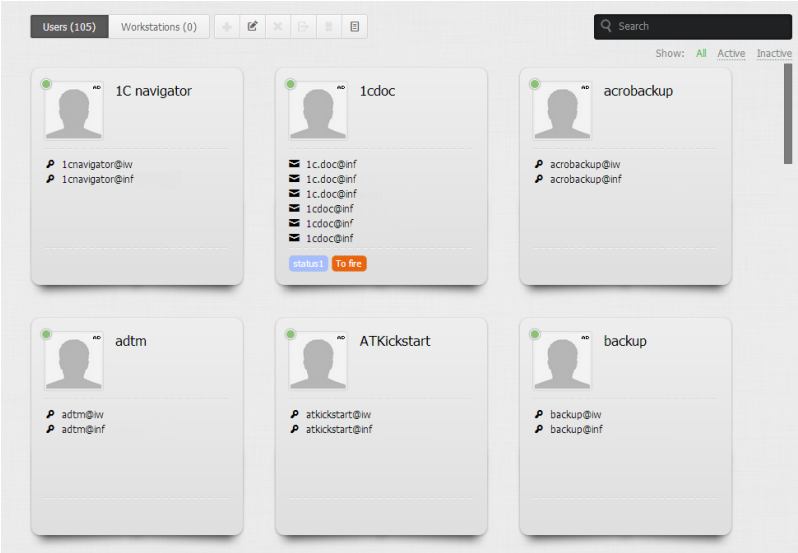
Attributes of groups of persons and workstations are described in the following table:

Parameter	Description
Name	Group name
Contacts	Group contact information
Contains groups	List of groups included to this group
Included in groups	List of groups the group is included to
Note	Optional note

User's actions:

- Creating a Group of Persons and Workstations.

4.6.2 Persons



Note

Persons imported from the Active Directory have a color indicator in the upper left corner of profile photo:

- - for active persons;
- - for persons disabled in AD.

Attributes of persons and workstations groups are described in the following table:

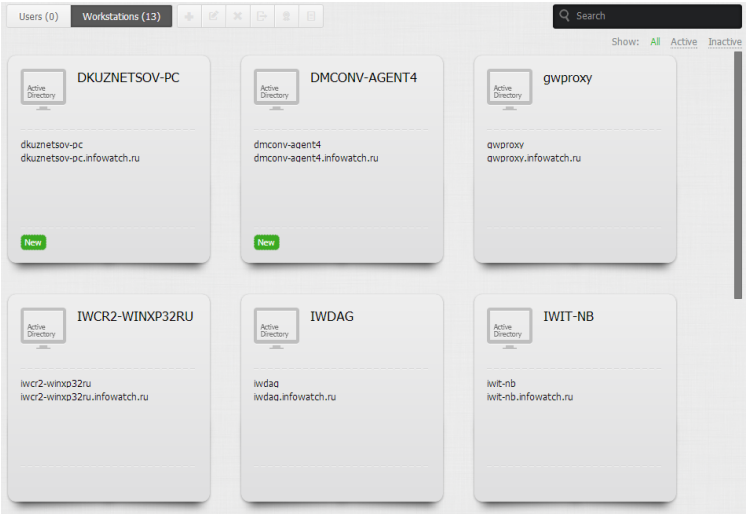
Parameter	Description
Last name	Person's family name

Parameter	Description
Name	Name of the person
Employee/Not an employee	Indicates if the person is working or fired
Job position	Person's occupation
Department	The department in which the person works
Room	The room in which the person works
Manager	Person's manager
Note	Optional description
Contacts	Person's contact information
Groups	The groups the person is included to
Workstations	Workstations assigned to the person
Statuses	Status, applied by Security Officer
Photo	Person's photo

User's actions:

- Managing groups of persons and workstations (see "Creating a Group of Persons and Workstations");
- Viewing widgets with information on persons and workstations (see "Viewing Summary on Person or Workstation");
- Viewing queries on persons and workstations (see "Viewing Events of 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");
- Associating persons and workstations with perimeters (see "Adding Person or Workstation to the Perimeter").

4.6.3 Workstations



Attributes of workstations are described in the following table:

Parameter	Description
Name	Name of workstation
Note	Optional description
Contacts	Workstations identifier in the network: • IP • DNS In one of two fields, type in IP and DNS-name (depending on chosen option). In second field, if necessary, leave your comment.
Users	Persons which the workstation is assigned to
Group	Groups the workstation is included to
Statuses	Status, which is being assigned to workstation

User's actions:

- Managing groups of persons and workstations (see "Creating a Group of Persons and Workstations");
- Managing persons and workstations (see "Creating a List of Persons and Workstations");
- Viewing widgets with information on persons and workstations (see "Viewing Summary on Person or Workstation");
- Viewing queries on persons and workstations (see "Viewing Events of Person or Workstation");
- Creating a policy for persons and workstations (see "Adding Person or Workstation to the Policy");
- Managing statuses of persons and workstations (see "Adding a Status to Person or Workstation");
- Associating persons and workstations with perimeters (see "Adding Person or Workstation to the Perimeter").

4.7 Policies Section

Reference information:
A policy is a set of rules determining the analysis and processing of intercepting objects. A rule is a set of conditions (to test object with) and actions performed when those conditions are fulfilled or not.

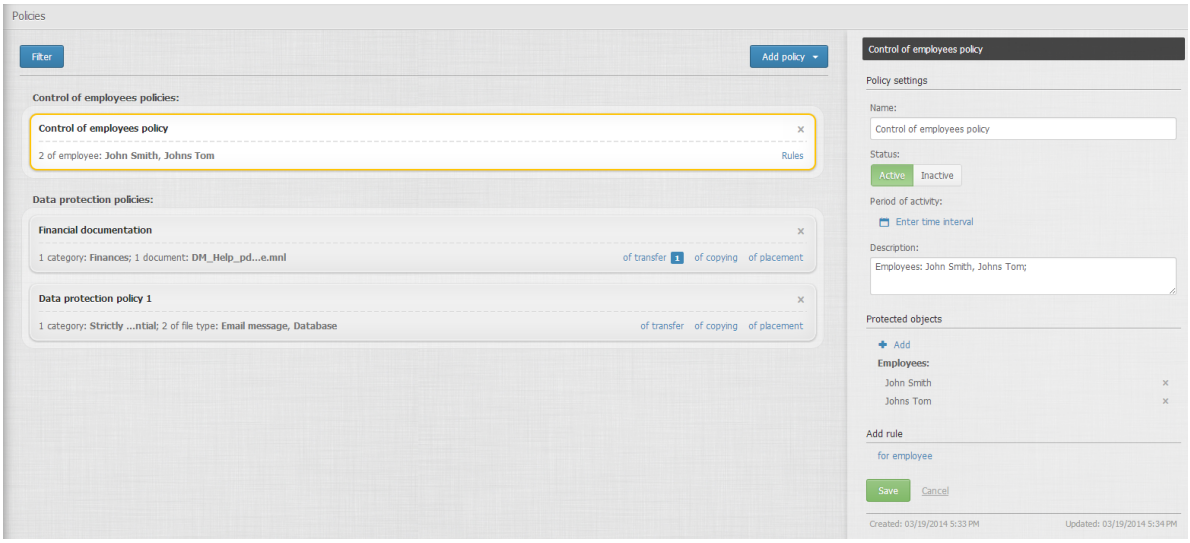
Warning!

As a result of the analysis the System will not perform any action if at least one of the following conditions is fulfilled:

- the System has no policies;
- all policies existing in the System are disabled;
- no policies existing in the System has active rules (or the default actions for active policies are not defined).

About section:

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



Policies section

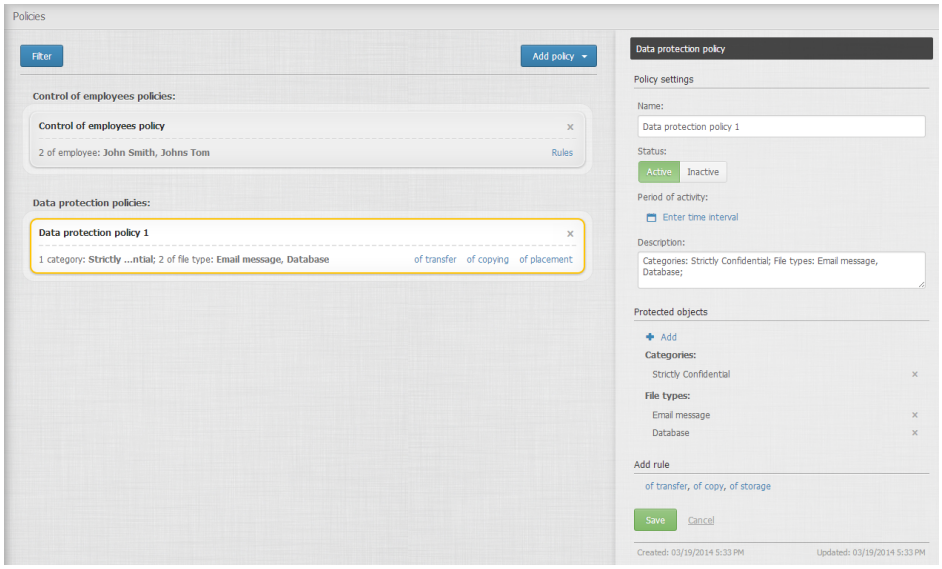
The section contains the following elements:

Element	Purpose
List of policies	Contains available policies of data protection
Policy viewing form	Contains attributes of data protection policy
Rule viewing form	Allows to configure a rule for the data protection policy
Button **Filter**	Opens **Filter settings** form
Form **Filter settings**	Allows to filter the data protection policies on specified attributes
Button **Add policy**	Opens the form of selecting the research object
Form of policy adding	Allows to create the policy of either data protection or employees control

User's actions:

- Adding a new policy (see "Creating a Policy");
- Modifying previously created policy (see "Editing Policy");
- Adding rules to the policy (see "Creating a Rule");
- Modifying previously established rules (see "Editing Rules");
- Adding actions to the policy (see "Determining System's Response to Policy Violations");
- Filtering policies (see "Filtering a List of Policies").

4.7.1 Policies and their Viewing Form



Policy attributes are described in the table:

Parameter	Description
Name	Policy name
Description	Note
Status	Indicates whether the policy is enabled in the System or not
Period of activity	The time period when the policy is active
Protected objects	List of confidential data or employees who are under control of this policy
Policy rules	List of actions performed by the System when the policy is triggered

User's actions:

- Adding a new policy (see "Creating a Policy");
- Modifying previously created rules (see "Editing Policy").

4.7.2 Rules and their Viewing Form



Information on the rule is displayed in the tile of a policy for which it is defined.

Note

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

There are three categories of rules:

Rule of transfer

Attributes of a transferring rule are described in the following table:

Parameter	Description
Route direction	There may be two types of directions: ↔ - the rule is triggered if traffic is passing from the sender to the recipient and from the recipient to the sender → - the rule is triggered only if traffic is passing from the sender to the recipient
Event type	The type of traffic triggering the rule. Available options: • Web-message • Income mail • Outcome mail • Web-mail • ICQ • Mail.ru Agent • Jabber • Skype • MS Lync • Yahoo!
Days of week of rule activity	List of days of the week when the rule should trigger

Parameter	Description
Period of rule activity during the day	The time interval during the day when the rule should trigger
Workstations	Sender workstations
Senders	List of persons and workstations which will: - trigger the rule when traffic is sent - leave the rule inactive when traffic is sent
Recipients	List of persons and workstations which will: - trigger the rule when traffic is received - leave the rule inactive when traffic is received
Send notification	List of persons notified when the rule is triggered
Notify senders	Click "YES" to notify traffic senders when the rule is triggered. By default the value is set to "NO".
Assign verdict	The verdict which will be assigned to object when the rule triggers
Set threat level	The threat level which will be assigned to object when the rule triggers
Tags	The list of tags which will be assigned to object when the rule triggers
Set status	The status which will be assigned to object when the rule triggers

Rule of copying

Attributes of a copying rule are described in the following table:

Parameter	Description
Days of week of rule activity	List of days of the week when the rule should trigger
Event type	The type of traffic triggering the rule. Available options: • Copy to external device • FTP

Parameter	Description
	• Print
Period of rule activity during the day	The time interval during the day when the rule should trigger
Workstations	Sender workstations
Senders	List of persons and workstations which will trigger the rule when traffic is stored
Send notification	List of persons notified when the rule triggers
Assign verdict	The verdict which will be assigned to object when the rule triggers
Set threat level	The threat level which will be assigned to object when the rule triggers
Tags	The list of tags which will be assigned to object when the rule triggers
Set status	The status which will be assigned to object when the rule triggers

Rule of placement

Attributes of a placement rule are described in the following table:

Parameter	Description
Event type	The type of traffic triggering the rule. Available options: • Crawler
Senders	List of persons and workstations which will: - trigger the rule when traffic is stored - leave the rule inactive when traffic is stored
Storage	A list of storages which will: - trigger the rule if protected objects are stored there - leaves the rule inactive if protected objects are stored there Note: When you add *a network resource* use the following format:

Parameter	Description
	`//<workstation>/<directory>` where • `<workstation>` is a name of workstation • `<directory>` is the target directory on the workstation. When you add *a file storage* enter the following values to fields: • to the field **Enter a source** - an address of the SharePoint database server; • to the field **Enter a path to storage -** a name of the SharePoint database instance.
Send notification	List of persons notified when the rule triggers
Assign verdict	The verdict which will be assigned to object when the rule triggers
Set threat level	The threat level which will be assigned to object when the rule triggers
Tags	The list of tags which will be assigned to object when the rule triggers
Set status	The status which will be assigned to object when the rule triggers

When adding senders and recipients of the rule, the following parameters can be specified:

Parameter	Description
Contacts	Specify contacts of traffic senders/recipients. For this, from a drop-drown list on the left, select contact type:  - ICQ account;  - Skype account;  - mobile phone number;  - landline phone number;  - e-mail;  - user/user group contact in Lotus Domino;  - contact at a web resource.
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.

User's actions:

- Adding rules to the policy (see "Creating a Rule");

- Modifying previously configured rules (see "Editing Rules");
- Adding actions to the policy (see "Determining System's Response to Policy Violations").

4.7.3 Form of Filter Settings

Filter attributes are described in the following table:

Parameter	Description
Filter by policy name	Filtering based on specified policies
Filter by objects	Filtering based on specified protected objects

User's actions:

- Filtering policies (see "Filtering a List of Policies").

4.7.4 Form of Adding a Policy

Policy attributes are described in "Policies and their Viewing Form". When creating a new policy, you need to specify objects included to the selected type of protected objects.

There are various forms of policy adding depending on the type:

Policy type	Description of the form of adding a policy
Data Protection Policy	When selected, a dialog box displaying the classifier appears.
Control of Persons Policy	When selected, a dialog box displaying a list of employees, groups, and employee's statuses appears.
Technical Policy of Preprocessing	Internal system-specific function. **Warning!** It is strongly recommended not to customize this setting without support of an authorized specialist of a company maintaining the System.
Technical Policy of Post-processing	Internal system-specific function. **Warning!** It is strongly recommended not to customize this setting without support of an authorized specialist of a company maintaining the System.

User's actions:

- Adding a new policy (see "Creating a Policy").

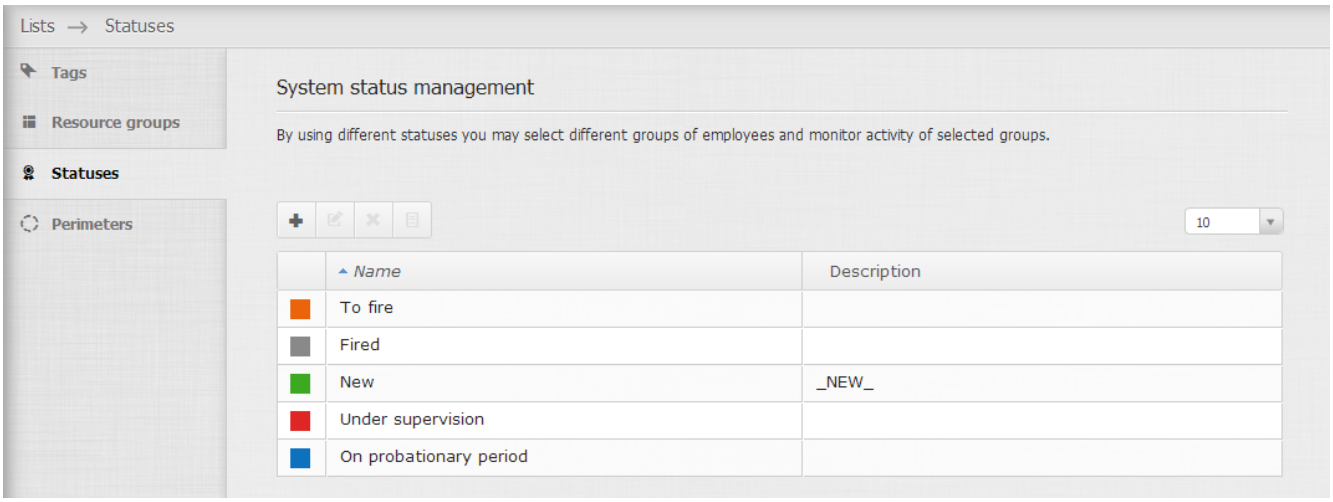
4.8 Lists Section

Reference information:

Lists are sets of similar data generated by the Management Console or preset for creating policies.

About section:

The section contains editable catalogues of tags, statuses, and perimeters.



Section **Lists**

This section contains the following elements:

Element	Purpose
Tabs of different types of catalogues • Tags • Resources Lists • Statuses • Perimeters	Contain lists of elements and tools for the selected catalogue
List of elements or element groups for the selected catalogue	Located in the right part of the workspace. Contains either a list of catalogue elements or a group of catalogue elements lists
Page navigation panel	The set of buttons for browsing pages containing entries (if not all entries can be placed on one page)
Control of the entries number	The drop-down list which sets the number of entries per page
Toolbar	A set of tools for catalogues

User's actions:

- Managing Tags;
- Managing Resources Lists;
- Managing Statuses;
- Managing Perimeters.

4.8.1 Tags

Reference information:

Tag is a mark which gives a short characteristic of an intercepted object.



Tag attributes are described in the table:

Parameter	Description
Color	Color mark indicating the tag
Name	Name of the tag
Description	Optional note

There are the following preset tags in the System:

Protection from deletion - Events that cannot be removed.

Note:

This tag is only available using **IWTMSX** installation type (For more information see *InfoWatch Traffic Monitor. Administration guide*)

Under supervision - Events that indicate employee's suspicious activity.
VIP - Objects from the users in VIP group.

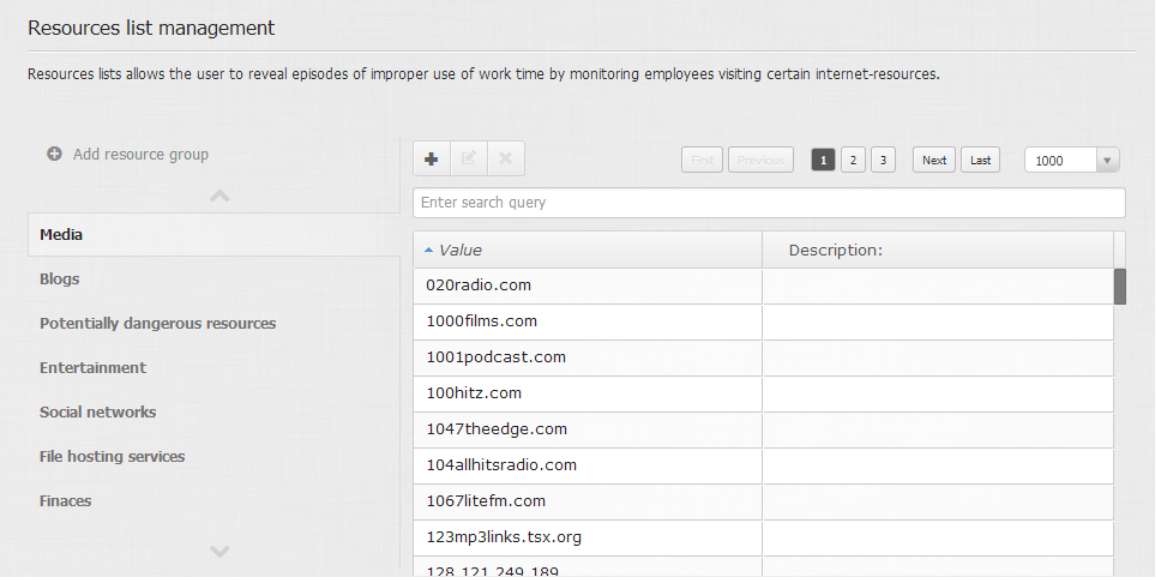
User's actions:

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

4.8.2 Resources Lists

Reference information:

The list of resources contains web-addresses detected by the System as improper usage of work time for employees (see "Specifying Improper Resources").



Resources are organized into thematic lists.

Resources attributes are described in the table:

Parameter	Description
Value	Internet-address of the resource
Description	Optional note

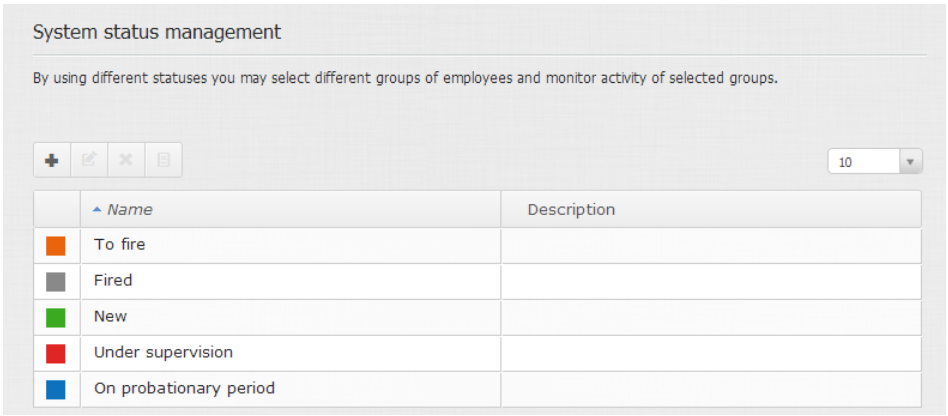
User's actions:

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

4.8.3 Statuses

Reference information:

Status is a mark which gives a short characteristic of the employee or a workstation.



Statuses attributes are described in the table:

Parameter	Description
Color	Color mark indicating the status
Name	Name of the status
Description	Optional note

User's actions:

- Creating a list of statuses (see "Managing Statuses")

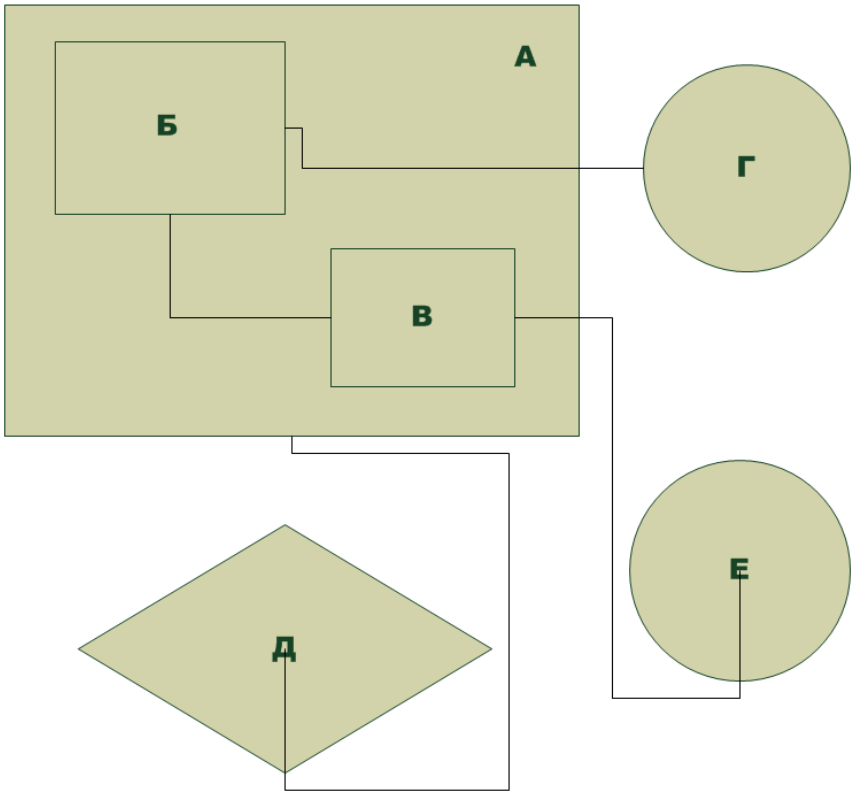
4.8.4 Perimeters

Reference information:

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

For example:

- There is a company with infrastructure A and there are subdivisions B and C;
- The company cooperates with organizations D, E, F.



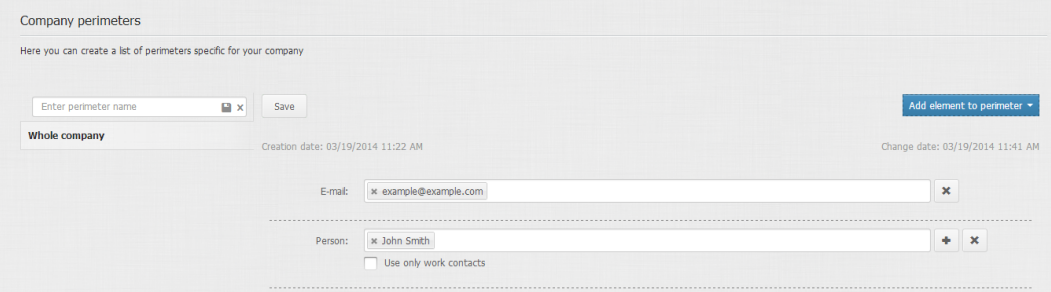
By selecting the perimeters of all named objects (A, B, C, D, E, F) the security officer can configure traffic monitoring:

- Inside the company (within the perimeter A)

- Outside the company (between the perimeter A and one of the perimeters D or E or F)

Warning!

For more flexible work with structural elements we recommend you to allocate smaller perimeters in large ones (in this example - the perimeters B and C in the perimeter A).



Resources are situated in themed lists.
The attributes of the employees and workstations groups are described in the following table:

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. For example, you can use this option for a case when employee sends a message from his\her personal e-mail address, and the System should consider this is not a sending outside the perimeter.

User's actions:

- Managing perimeters.

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

database. Considers only the current versions of files: change log is not investigated.

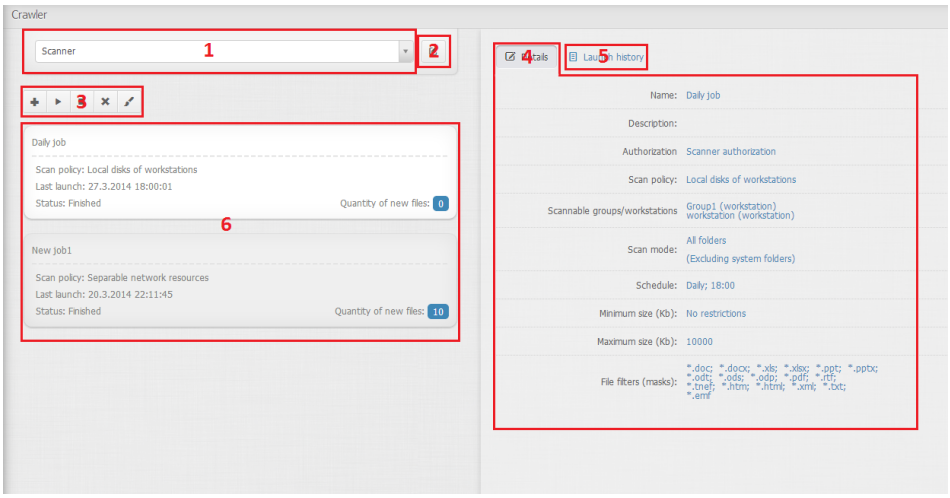
- Customizing scan settings: speed of files downloading from scanned resources and settings of file queue for loading objects to Traffic Monitor server.
- Creating a scan job where you can specify:
  - the list of folders and network nodes where the scanning is performed;
  - masks of processed files;
  - 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 are not sent 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 results of the scanning in the Management Console: using object queries and reports (including preset ones).

InfoWatch Crawler does not delete, move, rename, encrypt, or perform any other action on files even when they are recognized as a potential violation. The Crawler only informs 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 them.

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

About section:

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



Section **Crawler**

The section contains the following elements:

Element	Number on scheme	Purpose
List of available	1	Drop-down list which determines what information from the installed

Element	Number on scheme	Purpose
scanners		scanners will be displayed (see "Scanner")
Button of scanner editing	2	When clicked, the form of scanner editing is displayed on the right part of the workspace
Toolbar	3	Set of tools for scan jobs
Tab of viewing scan job	4	Displays data on selected scan job
Tab of viewing the history of scan job launches	5	Provides information about stages of scan job execution (see "Launch History")
List of scan jobs	6	Contains a list of scan jobs for the selected scanner (see "Scanning Jobs ")

User's 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 launches (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 storage locations (such as Microsoft SharePoint 2007/2010 storage, local disks of workstations, and shared network resources). The method of scanning is defined by user in the scanning job.



Scan viewing form *Scanner 2*

Attributes of the scanner are described in the table:

Parameter	Description
Name	The name of the scanner
Traffic Monitor server address	Traffic Monitor IP-address hosting `iw_expressd` service
Traffic Monitor send speed rate (Mbit/sec)	Maximum speed of file uploading to Traffic Monitor server, Mbit/sec
Scan speed (Mbit/sec)	Maximum speed of file uploading to temporary directory from the being scanned resources, Mbit/sec
File queue size (Mb)	Maximum size of queue for detected files being prepared for sending to Traffic Monitor server, Mbytes **Warning!** When the summarized maximum size is reached, all the tasks are stopped and all files from this buffer are deleted without sending to TM.

Parameter	Description
File queue check interval (sec)	Using the specified interval (in seconds) the Crawler server will check if there are any objects in the queue to upload to Traffic Monitor server. The transferring of the object to the Traffic Monitor server will be executed if the queue has at least one object
Connections to Traffic Monitor	Maximum count of the connections with the Traffic Monitor sever at the one moment
Reconnection interval (sec)	Using the specified interval (in seconds) the Crawler server will attempt to reconnect with the Traffic Monitor server in case of disconnection
Display of users in events	The filter of employees
System folder masks	Masks of directories that will not be scanned by the scanner

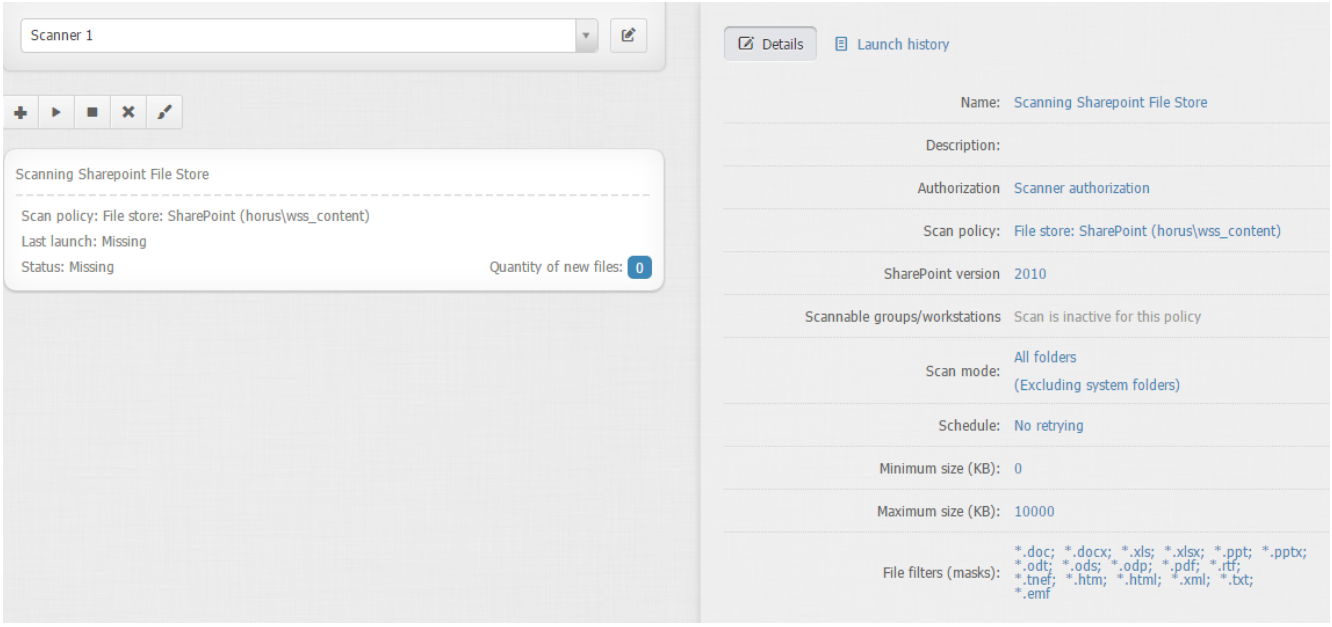
User's actions:

- 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 launches (see "Viewing Launch History");
- Saving the report of completing the scan job to the hard disk (see "Saving Scan Report").

4.9.2 Scanning Jobs

Reference information:

Scanning job is a single or scheduled repeating operation that verifies the target storage locations (Microsoft SharePoint 2007/2010 storage, local drives of workstations, and shared network resources) for storage the confidential data (more on list of protected data see "Defining the Confidential Information").



Scanning job and its viewing form (Details tab)

Job attributes are described in the table:

Parameter	Description
Name	Name of the job
Description	Optional note
Authorization	The account under which the scanning is performing
Scan policy	Type of scan job: • Shared network resources • Local disks of workstations **Note:** The **Local disks of workstations** needs the disabling of **Use simple file sharing** option (**Control Panel -> Folder Options**, **View** tab) at the workstations under Windows XP • SharePoint 2007 **Note:** for policy **SharePoint 2007/2010** the following parameters are specified: ○ in the field **Address of DB resource** - address of the SharePoint database server; ○ in the field **Name of DB resource** - name of the SharePoint database instance.
SharePoint version	• 2007 • 2010
Scannable groups/workstations	Groups and workstations on which the scanning is performed

Parameter	Description
Scan mode	**All folders** - scans all the directories on the workstation **All folders except**: - scans all the directories on the workstation except the specified ones. **Only:** - scans only directories specified by user. **To specify scanning paths you can use the following symbols:** * - 0 and more of any symbols ? - any one symbol $ - symbol used by Windows for indicating the hidden directory **When scanning the shared network resources or Sharepoint storage you can use the following queries:** Docs* - will scan Docs folder and all its subfolders. *text_example* - will search for "text_example" in the path. *.file_format* - will scan files of specified (*.txt* for example) **When scanning local discs and folders you can use the following queries:** C$\Docs\ - will scan Docs folder and its subfolders on C: drive \share\Docs\ - will scan Docs folder and its subfolders in share directory *\Docs\ - will scan Docs folder and its subfolders regardless of their location ?$\Docs\ - will scan any directory, which name has 1 symbol and Docs folder with its subfolders (C$\Docs\, D$\Docs) \Docs***\ - will scan any folder, which has Docs in its name with 4 additional symbols (Docs1234)  **Warning!** The **All folders** scanning mode provides the scanning of local discs only.
Schedule	Schedule of scanning
Minimum size (Kb)	The minimum size of scanned file, in kilobytes
Maximum size (Kb)	The maximum size of scanned file, in kilobytes
File filters (masks)	Expansions of scanned files **To add a new file format:** 1. Click the link to the file formats. 2. Specify the mask in **Enter the file mask** field. 3. Click  4. Click

User's actions:

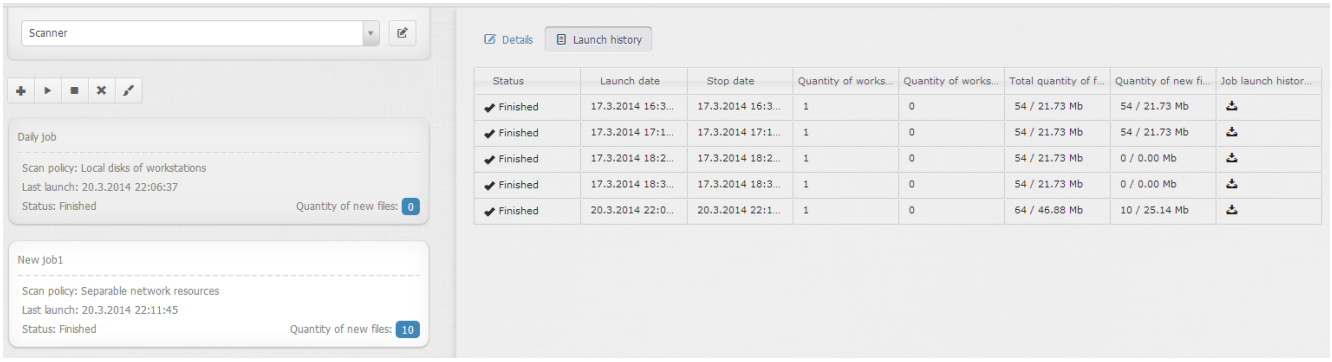
- Creating the scanning job (see "Creating a Job");
- Starting and stopping the scanning job (see "Launching and Stopping the Job");
- Modifying the scanning job (see "Editing the Job");
- Cleaning the hash base of scanning jobs (see "Cleaning the Hash Base");
- Viewing the history of scanning jobs launches (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 **Launch History** tab displays an information about launches of the selected scan job.
When you select one of the entries in the table, the detailed information about the selected launch is displayed including tabs:

- **Launch events** - provides system information about the launch of scanning job.
- **Launch settings** - contains the list of attributes of scanning job (see "Scanning Job").
- **Current status** - contains information about the current status of a launched job (for jobs with status other than *Launched* this tab is unavailable).



Scanning Job and its viewing form (Launch history tab)

Attributes of the history entry are described in the table:

Parameter	Description
Status	Current state of the launch
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
Quantity of workstations not proceeded	Number of target workstations which are not processed yet

Parameter	Description
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
Job launch history report	Icon: click to save .xls files with the launch report to the hard drive

User's actions:

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

5 Cases Solving

Security Officer generally uses the Management Console to solve following business cases:

- Managing Persons and Workstations
- Configuring the Analysis of Employees Actions
- Configuring System Response
- Managing Interception Objects
- Managing Crawler Subsystem
- Managing Catalogues

Upon that he/she makes similar actions described in topic:

- Typical Actions

Security officer can customize the view and displaying style of some interface elements of the Management Console:

- Interface Customization



Warning!

Management Console administrating is out of officer's authorities and out of scope of this document. You can find an information about Console administrating in *"InfoWatch Traffic Monitor. Administration Guide"* document.

See also:

- Dashboard Section;
- Events Section;
- Classifier Section;
- Files Section;
- Employees Section;
- Policies Section;
- Lists Section;
- Crawler Section.

5.1 Typical Actions

Why the typical actions are needed?

For performing the same-type operations in the Management Console.

Includes following actions:

Action	Description
Log In and Log Out the Management Console	Authorization in the Management Console and exit from it
Applying the System Configuration	System configuration changes become active when updated configuration is applied
Creating an Element	GUI allows to create entries needed for System configuring, displaying, and processing the interception objects
Editing the Element	Editing entries needed for System configuring, displaying, and processing the interception objects
Deleting the Element	Deleting entries needed for System configuring, displaying, and processing the interception objects
Pages Navigation	Numerous elements can be viewed in multipage mode: navigation buttons are used to go to particular page with elements
Changing User's Password	Procedure for changing the user's own password
Selecting Interface Language	How to change the interface language
Calling Help File	Call for Reference Information
Viewing Information on System	Call for general information about the System

5.1.1 Log In and Log Out the Management Console

Purpose 1:

Login the Management Console.

Solution:

1. Open Google Chrome browser v.30 (if you don't have this browser installed, download from the link).
2. Go to the address given you by your Traffic Monitor administrator.

   The browser window will display Management Console home page.
3. Enter user name in the **Login** field.
4. Enter a password in the **Password** field.

   Note
   Ask your Traffic Monitor administrator for you login and password.
5. Click **Login**.

Purpose 2:

Exit the Management Console.

Solution:

Click the user menu button and choose **Logout**.

5.1.2 Applying the System Configuration

Reference information:

The System configuration is changed when editing the following Management Console sections:

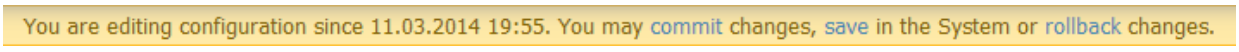
- Classifier
- Employees
- Policies
- Lists

Purpose:

Apply System configuration.

Solution:

1. When configuration editing is finished, at the top of browser window, click commit **commit** on the string like the following:

   The window **Configuration changes** with information on changes made will be opened:



2. If needed, enter a text to the **Description** field.
3. Click **Save**.

5.1.3 Creating an Element

Warning!

You can not create interception objects because such objects are formed by the System automatically basing on the active configuration.

Purpose:

Add an element.

Solution:

1. Go to the target Console section.
2. If needed, go to the target subsection or tab.
3. To create target element click **Add** or:
   - + Add widget - to add a widget (see "Adding a Widget");
   - Add policy - to add a policy (see "Creating a Policy");
   - Add resource group - to add a resources list (see "Managing Resources Lists");
   - Add perimeter - to add a perimeter (see "Managing Perimeters");
   - Add element to perimeter - to add a perimeter element (see "Managing Perimeters").

4. Specify attributes of a new element (element attributes are described in subsections of "Management Console Interface" section).
5. Click **Save**.

5.1.4 Editing the Element

Purpose:

Edit the element.

Solution:

1. Go to the target Console section.
2. If needed, go to the target subsection or tab.
3. Left-click the target element from the list and select **Edit**.
4. Specify attributes of the element (element attributes are described in subsections of "Management Console Interface" section).
5. Click **Save**.

5.1.5 Deleting the Element

Purpose:

Delete the element.

Solution:

1. Go to the target Console section.
2. If needed, go to the target subsection or tab.
3. Left-click the target element from the list.

   Note:
   To delete several elements select them holding **Shift** or **Ctrl** keyboard key.

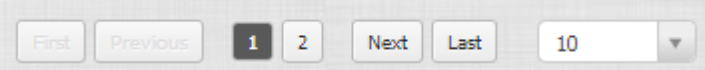
4. Click **Delete**.
5. In the confirmation window click **Yes**.

5.1.6 Pages Navigation

Reference information:

Page navigation can be performed only in multipage interface view mode.

Multipage view mode is used for ergonomic work area usage. It is available when browser displays the page navigation pane:



Pages navigation pane

Purpose:

To navigate pages in multipage mode.

Solution:

1. Go to the target Console section.
2. If needed, go to the target subsection or tab.
3. In the right of the page navigation pane click the drop-down list and select a number of elements per page.
4. To navigate pages use number buttons or the following buttons:
   - **First** - to go to the first page
   - **Previous** - to go to the previous page
   - **Next** - to go to the next page
   - **Last** - 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 from letter "A", the **Last** button will lead to he page with elements beginning from "Z". But if the sorting is backward, the **Last** button will lead to he page with elements beginning from "A".

5.1.7 Changing User's Password

Reference information:

After authorizing in the System User can change his/her password.

Purpose:

To change the user's password.

Solution:

1. Click the user menu button and choose **Change password**.

The dialog box **Change password** will appear.

2. In the appeared dialog box type the necessary password in the following fields:
   - **Password**;
   - **Confirm password**.

   Note:

   Detailed recommendations on the forming of passwords see in document *«InfoWatch Traffic Monitor. Administrator Guide»*.

3. Click **Save**.

5.1.8 Selecting Interface Language

Purpose:

Change the interface language.

Solution:

1. Click the language icon and choose the necessary language.

   The dialog box **Change language** will appear.

2. In the appeared dialog box click **Yes**.

Note:

Do the same steps to revert English language if necessary.

5.1.9 Calling Help File

Purpose:

Get the Reference Information.

Solution:

1. Click the user menu button and choose **Help**.

   The InfoWatch Traffic Monitor help file will appear in the browser new tab.

2. Review the information and then close the tab in the standard way.

5.1.10Viewing Information on System

Purpose:

Get the general information about the System.

Solution:

1. Click the user menu button and choose **About**.

   The window **About** containing the required information will appear.
2. Review 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 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.

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 Person's or Workstation Summary	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 Person or Workstation to Data Protection Policy	Configuring System response to actions of person or workstation
Adding a Status to Person or Workstation	Marking person or workstation monitor its activities
Adding an Person or Workstation to Perimeter	Adding person or workstation to configured lists of a company

Action	Description
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:

To create a group of persons and workstations.

Solution:

1. Go to the **Persons** section.
2. On the left part of the workspace left-click the *TM Groups* group.
3. Click **Add**.
4. Specify attributes of the new group (see "Groups of Persons and Workstations").
5. Click **Yes**.

Important!

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 TM 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 TM group. You can also use drag-and-drop to add individual domain users to a TM group.

Note:

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

Additional information:

Editing and deleting the of users' and workstations groups are performed by standard means:

- Editing the Element;
- Deleting the Element.

5.2.2 Creating a List of Persons and Workstations

Reference information:

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

- from Active Directory of a company - this way is configured by the system administrator (see document *"InfoWatch Traffic Monitor. Administrator Guide"*);
- by means of the Traffic Monitor - this way is performed by security officer as described in this topic.

Purpose:

To fill a list of users 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 user;
   - **Workstations** - to add the workstation.
4. Click **Add**.
5. Specify the parameters of the new user or workstation (see "Persons" and "Workstations").
6. Click **Save**.

Additional information:

Editing and deleting the of users' and workstations lists are performed by standard means:

- Editing the Element;
- Deleting the Element.

5.2.3 Viewing Person's or Workstation's Events

Purpose:

To view events of person (or workstation).

Solution:

1. Create a query on objects by specifying a target person in the desired query attribute (see more about creating a query in "Events Filtering").
2. Apply the created query.

The viewing of events on the workstation 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 person *Smith* is already created in **Persons** section):

1. go to **Persons** section
2. create a query named *Smith* where:
   - attribute *Date of capture* has the *Current week* value;
   - attribute *Senders* has the *Smith* value (selected from a list of previously created persons).
3. save and apply the created query.

The **Events** section displays all the necessary events.

5.2.4 Viewing Person's or Workstation's Summary

Purpose:

To view statistical data on a person (or a workstation).

Solution:

1. Create **Summary** widget and specify its attribute as a query on target person you created before (see " Viewing Person's or Workstation's Events").

The creating of summary on the workstation is performed in a similar way.

Example:

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

1. go to **Summary** section
2. create a widget named *Smith* where:
   - attribute *Summary* has the value of *Smith* query created before (see "Viewing Person's or Workstation's Events").
3. save the created widget.

The **Summary** section displays ***Smith*** widget with all the necessary events.

5.2.5 Adding a Person or Workstation to Data Protection Policy

Purpose:

To create a data protection policy for user or workstation.

Solution:

1. Go to the **Policies** section.
2. Create a policy specifying the target user as a secured object.

   In the same way you can add the following objects to the data protection policy:

- workstations;

- groups of persons and workstations;
- persons and workstations in same status.

Example:

If you need the System to proceed interception of the object sent or received by *Smith* (assuming that the person *Smith* is already created in **Persons** section) and having the *High* threat level in the following way: to assign *Allow* verdict to the object; to assign *Under supervision* status to Smith; to sent incident notification to *example@company.com* e-mail.

1. go to the **Policies** section
2. create a *Control of employees policy* for *Smith*.
3. create a rule for the created policy with following attribute values:
   - ***Intercept with the threat level*** attribute - *High* value
   - ***Send notification*** attribute - *example@company.com* value (for more details see "Sending Notifications on Responded Rule")
   - ***Assign verdict*** attribute - *Allow* value
   - ***Set status*** attribute - *Under the supervision* value.

Additional information:

- "Setting System responses".

5.2.6 Adding a Status to Person or Workstation

Purpose:

To add a status to 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 a status to user;
   - **Workstations** - to add a status to workstation.
4. Select the target user or the target workstation.
5. Click  **Set status**.
6. Specify the desired status and add a description to the status if needed.
7. Click **Save**.



Note

Status *New* is assigned to person and workstation when it was created in the System and remains for 30 days (when imported from Active Directory the status *New* remains for 30 days from the moment of the record creation in Active Directory).

Additional information:

Both editing and deleting of the users and workstations are performed by standard means:

- Editing the Element;
- Deleting the Element.

See also:

- "Statuses" - about the section where the user statuses managing is performed.

5.2.7 Adding a Person or Workstation to Perimeter

Purpose:

To create a data protection policy for user or workstation.

Solution:

1. Go to the **Lists** section and select the **Perimeters** tab.
2. Left-click the target perimeter to select it from the list of perimeters (see "Perimeters").
3. On the right part of the workspace click **Add an item to the perimeter** and select **Person** from the drop-down list.
4. In the appeared **Person** field specify the target person in one of the following ways:
   - start typing the name or surname and select the desired entry from the drop-down list;
   - click **Add,** flag the target person in the opened dialog box, and click **Save**.

In the same way you can add the following objects to the data protection policy:

- workstations;
- groups of persons and workstations.

See also:

- "Perimeters" - about the section where managing the perimeters is performed.

5.2.8 Configuring Person's Card

Purpose:

Fill the card of person with data.

Includes following actions:

Action	Description
Adding a Contact to Person	Creating a structural element of a catalogue
Adding a Workstation to Person	Filling the catalogue
Adding a a Person to Group	Configuring widgets for displaying the statistical information on a person

5.2.8.1 Adding a Contact to Person

Purpose:

Add a contact to 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 **Users** tab and perform one of the following actions:
   - select target user by double-clicking the left mouse button;
   - left-click the target user and on the toolbar click **Edit**.

   The person's card editing form will be opened.
4. On the right part of the person's card editing form go to **Contacts tab**.
5. Click Add contact **Add a contact**.
6. In the first drop-down list select the type of contact: (Home) or (Work).
7. In the second drop-down list select the source of contact: (Mobile phone) or (Home phone) or (e-mail) or (Skype) or (ICQ) or (WEB ID: profile in a social network for example) or (Lotus email).
8. In the field to the right of the drop-down lists specify the number or address of the contact.
9. Click **Save**.

5.2.8.2 Adding a Workstation to Person

Purpose:

To add an associated workstation 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 **Persons** tab and perform one of the following actions:
   - select target person by double-clicking the left mouse button;
   - left-click the target person and on the toolbar click **Edit**.

   The person's card editing form will be opened.
4. On the right part of the person's card editing form go to **Workstations** tab.
5. Click Add workstation **Add workstation**.
6. In the opened window flag required workstations and click **Yes**.
7. Click **Save**.

5.2.8.3 Adding a Person to Group

Purpose:

To add a person to a 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 **Persons** tab and perform one of the following actions:
   - select target person by double-clicking the left mouse button;
   - left-click the target person and on the toolbar click  **Edit**.

   The person's card editing form will be opened.
4. On the right part of the person's card editing form go to **Groups** tab.
5. Click  **Add group**.
6. In the opened window left-click the target group and click **Yes**.
7. Click **Save**.

5.2.9 Configuring Workstation's Card

Purpose:

Filling the card of workstation with data.

Includes following actions:

Action	Description
Adding IP or DNS to Workstation	Creating a structural element of a catalogue
Adding Person to Workstation	Filling the catalogue
Adding Workstation to Group	Configuring widgets for displaying the statistical information on workstation

5.2.9.1 Adding IP or DNS to Workstation

Purpose:

To add IP or DNS address to the 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 select the tab **Workstations** and perform one of the following actions:
   - select target workstation by double-clicking the left mouse button;
   - left-click the target workstation and on the toolbar click **Edit**.

   The workstation card editing form will be opened.
4. On the right part of the workstation card editing form go to **Contacts** tab.
5. Click **Add contact**.
6. From the drop-down list select IP or DNS.
7. In the field to the right of the drop-down list specify the IP address or DNS name.
8. Click **Save**.

5.2.9.2 Adding Person to Workstation

Purpose:

To add an associated person entry to 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 select the tab **Workstations** and perform one of the following actions:
   - select target workstation by double-clicking the left mouse button;
   - left-click the target workstation and on the toolbar click **Edit**.

   The workstation card editing form will be opened.
4. On the right part of the workstation card editing form go to **Users**tab.
5. Click **Add user**.
6. In the opened window flag required persons entries and click **Yes**.
7. Click **Save**.

5.2.9.3 Adding Workstation to Group

Purpose:

To add a workstation to 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 tab **Workstations** and perform one of the following actions:
   - select target workstation by double-clicking the left mouse button;

- left-click the target workstation and on the toolbar click  **Edit**.

The workstation card editing form will be opened.

4. On the right part of the workstation card editing form go to **Groups** tab.
5. Click  **Add group**.
6. In the opened window left-click the target group and click **Yes** .
7. Click **Save** .

5.3 Configuring the Analysis of Employees Actions



Warning!

To make elements changes described in this section affecting the System operation you should apply the System configuration (for more details see "Configuring the System" and "Applying System Configuration").

Why the configuring of employees actions analysis is needed?

The analysis of interception objects discovers following violations:

- violation of corporate security policy (e.g. sending a confidential document outside the company);
- inappropriate use of working time (e.g. viewing entertaining Internet sites from work computer).

For the objective recognition of violations you need to specify to the System:

- what the confidential information is;
- which resources visited from the workplace are inappropriate.

Includes following actions:

Action	Description
Defining the confidential information	Creating *classification database* on the basis of which the interception objects can be assigned to different types and categories of violations
Specifying inappropriate resources	Creating a resource list which is considered as inappropriate using of work time if visited

In this section:

- Defining the Confidential Information;
- Specifying inappropriate resources.

See also:

- "Classifier Section" - about the section where managing of the classification base is performed;
- "List of resources" - about the section where the resources list managing is performed.

5.3.1 Defining the Confidential Information

Purpose:

To denote to the System which information is confidential within the company (disclosure of this information is a violation of the corporate security policy).

Solution:

1. Create a classifier base:
   - Creating of subject areas of confidential data;
   - Defining the confidential data.

   Warning!

   Upon completion of the classification base you should apply updated System configuration (see "Applying System Configuration").

Additional information:

The set of categories and included elements is called the **classification base**.

When using certain technologies, you will need to perform additional steps:

Technology	Action
Digital Fingerprints	Creating sample documents base
Completed Forms	Creating sample forms base
Sample Stamps	Creating sample stamps base
Sample Database Uploadings	Creating base of sample database uploadings

See also:

- "Classifier Section" - about the section where managing of the classification base is performed.

5.3.1.1 Creating Classifier Base

Purpose:

To create a classifier base.

Solution:

1. Go to the **Classifier** section.
2. Create a new category (see "Grouping the Confidential Data by Subject Areas").
3. Fill created category with examples of confidential data which will indicate the violation of the security policy if found in the traffic (see "Defining the Confidential Data").
4. If necessary, repeat steps 2 and 3 for other subject areas.

Additional information:

The set of categories and included elements is called a **Classifier base**.

5.3.1.2 Grouping the Confidential Data by Subject Areas

Purpose:

Define the subject area for confidential data.

Solution:

1. Go to the **Classifier** section.
2. On the left part of the workspace click **Add**.
3. Specify term attributes (see "Categories").
4. Fill the created category with elements which will indicate that the intercepted object corresponds to this category if found in the object (see "Defining the Confidential Data").

Example:

If you need the System to mark the intercepted object as code leakage if the traffic contains a fragment of a program code:

create a category *Leaked code* and add terms *Procedure*, *Result*.

As a result of the analysis of the transmitted data (among which those terms were found) the System assigns the *Leaked code* category to the intercepted object.

Warning!

Interception object receives only the category directly containing 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, the interception object will be marked with the term C and category B.

Additional information:

Both editing and deleting of the categories are performed by standard means:

- Editing the Element;
- Deleting the Element.

Note

There is a list of system text objects which are included in System. That system text objects could be used for any category (see "Creating Text Objects and their Values").

5.3.1.3 Defining the Confidential Data

Purpose:

To denote to the System which data leakage is a leakage of confidential information.

Note

Confidential data may only be specified inside the categories which are subject areas of confidential data (see "Grouping the Confidential Data by Subject Areas").

Solution:

1. Go to the **Classifier section**.
2. By clicking the left mouse button select the category the target example of confidential data will belong to.

   Warning!

   Examples of confidential data can be specified only in categories that do not contain nested categories.
3. Go to one of tabs depending on the data type (see the description below).
4. Add target example of confidential data (see "Creating an Element" and subsections of current document section).

By default the element has status *Active*. You can deactivate it either during configuring or later (see "Enabling and Disabling the Analysis on Confidential Data").

Additional information:

You can define confidential data using the following entities:

Name	Description
Term	Either 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. See "Creating Terms"
Text object	Text information extracted from the body and attachments of an object. Contains no formatting or markup elements. Used for analysis and search tasks solution. See "Creating Text Objects and their Values"
Sample document	Document which quotes are searched for in the analyzed text. Sample documents may be samples of orders, financial statements, contracts, and other confidential documents. Sample documents are stored in the system as digital prints, their text is not available either for users or System administrators. See "Creating Sample Documents"
Sample form	Formsheet which completed version is searched for in the network traffic. Sample form may be different questionnaires, receipts, etc. Sample forms are stored in the System as digital fingerprints, their text is not available either for users or System administrators. See "Creating Sample Forms"
Sample stamp	Stamp image that is searched for in the network traffic. Sample stamps may be images of round seals used in companies. See "Creating Sample Stamps"
Sample database uploading	Part of a database which citations are searched for in the analyzed text. Sample database uploadings may be lists of salaries, other personal data, etc. See "Creating Sample Database Uploadings"

A set of specified entities forms a Category which is the subject area the entities belong to (see Grouping the Confidential Data by Subject Areas).

Example:

If you need the System to assign *Finance department* category to intercepted objects if they contain phrase "invoice", passport numbers or quotations from the hiring contract of a company:

a. in created category *Finance department* add text object *Invoice;*

b. activate text object *Passport;*

c. create a sample document *Hiring contract* (make the digital fingerprint from the template of the hiring contract used in the company).

Additional information:

Both editing and deleting of category elements are performed by standard means:

- Editing the Element;
- Deleting the Element.

5.3.1.3.1 Creating Terms

Purpose:

To create a tag.

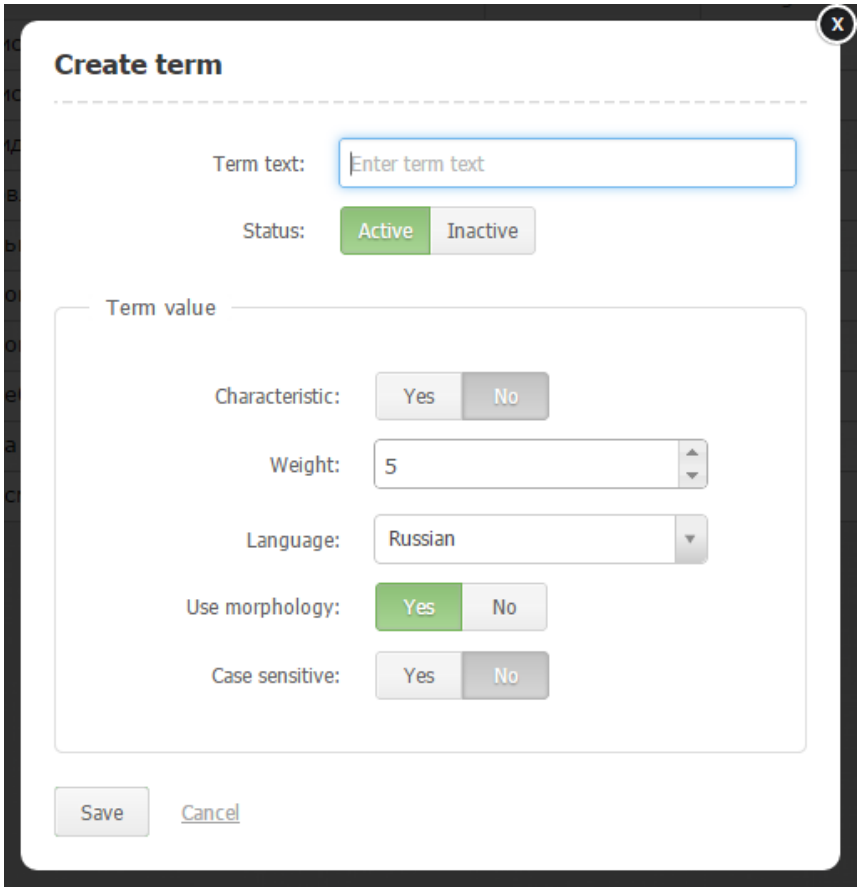
Solution:

1. Go to the **Classifier** section.
2. On the left part of the workspace left-click the target category.

   Note

   Terms can be added only to those categories that do not include other nested categories.

3. On the right part of the workspace (in **Terms** tab) on the toolbar click **Add**.



4. Specify term attributes (see "Terms").
5. Click **Save**.

Example:

If you need the System to mark the interception object as DOCUMENT_ISSUE_DATE if it contains at least one occurrence of phrase "document issue date":

1. select the target category
2. add the term *Document issue date* to it
3. specify **Yes** value to *Characteristic* attribute.

When transferred data containing this phrase is intercepted, the System assigns the *Document issue date* category to the object.

Additional information:

Both editing and deleting of the terms are performed by standard means:

- Editing the Element;
- Deleting the Element.

5.3.1.3.2 Creating Text Objects and their Values

Purpose:

1. To create a text object and set its value.

2. To add system text object to a category.

Solution:

1. Creating a text object and set its value.

    1. Go to the **Classifier** section.
    2. On the left part of the workspace left-click the target category.

    > **Note**
    >
    > For text objects and their values the adding of only those categories that do not include other nested categories is available.

    3. On the right part of the workspace (in **Text objects** tab) on the text objects toolbar click **Add**.
    4. Specify the attributes of the text object (see "Text Objects and their Values").
    5. Click **Save**.
    6. On the toolbar of text object values click **Add**.

    > **Note**
    >
    > The target text object should be selected in the list before clicking **Add** button to supplement it with required value.

    7. Specify the attributes of the text object value (see "Text Objects and their Values").
    8. Click **Save**.

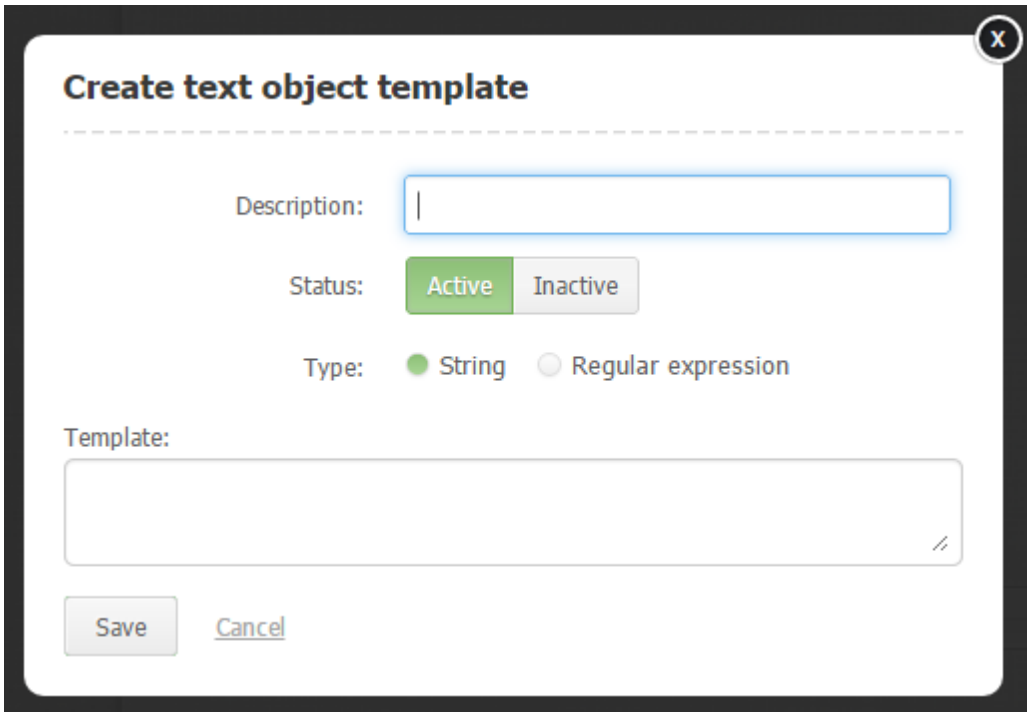
Example:

1) If you need the System to mark the interception object as EXAMPLE_MAIL when the traffic contains "*example@company.com*" e-mail address:

    a. create an active text object *EXAMPLE_MAIL* specifying a threshold value **1** (the text object should response when at least one reference to the address *example@company.com* is found in traffic).

    b. left-click the newly created text object and create a new active value with type *String*

    c. in the field **Pattern** specify the value *example@company.com*.

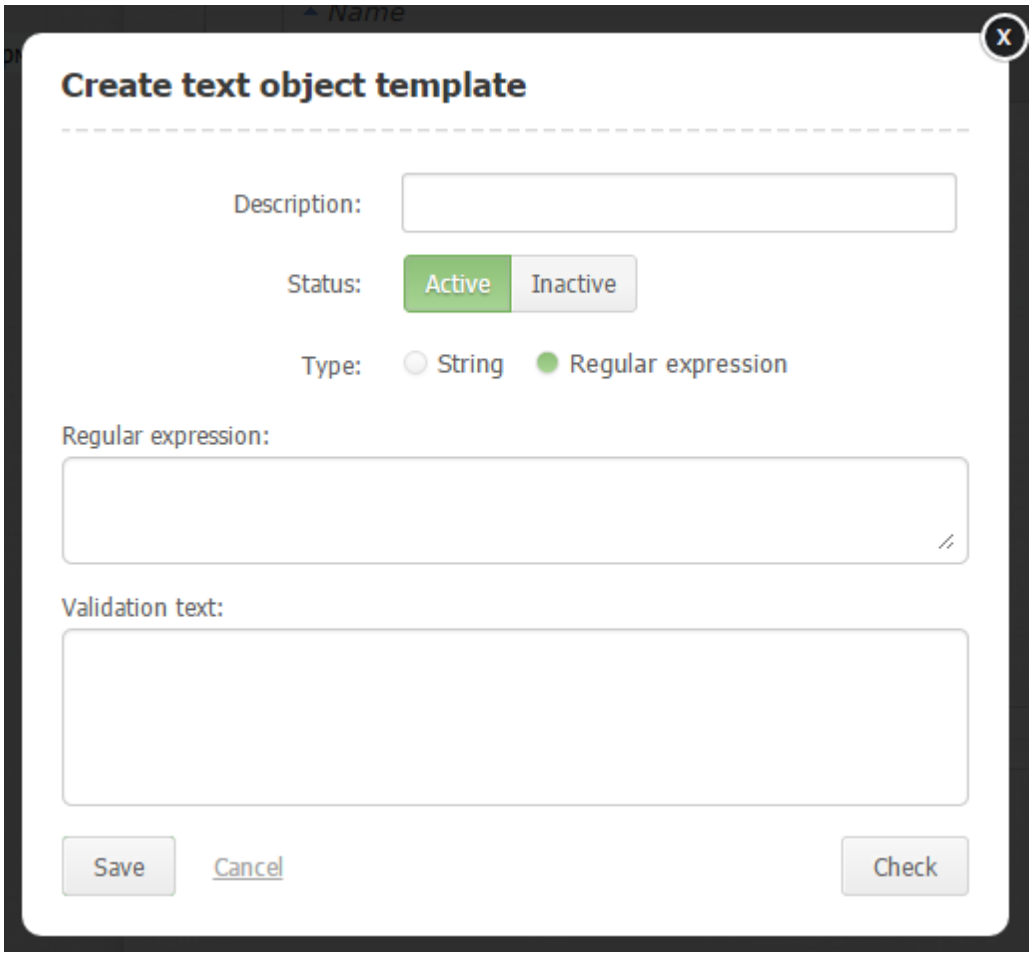


2) If you need the System to mark the interception object as COMPANY_MAIL when the traffic contains e-mail address with domain "*company.com*":

   a. create an active text object *COMPANY_MAIL* specifying a threshold value **1** (the text object should response when at least one reference to the domain *company.com* is found in traffic).

   b. left-click the newly created text object and create a new active value with type *Regular expression*

   c. in the field **Regular expression** specify the following value:
   `\w+ (@ (company.com))`



Note

The system uses a standard regular expression language. For more information about regular expressions see online article "Regular Expression Language".

2. Adding a system text object to a category.

1. Go to the **Classifier** section.
2. On the left part of the workspace left-click the target category.

   Note

   For text objects and their values the adding of only those categories that do not include other nested categories is available.

3. On the right part of the workspace (in **Text objects** tab) on the text objects toolbar click **Add system text object**.
4. Choose the necessary text objects in the appeared window.
5. Click **Save**.

Additional information:

Both editing and deleting of text objects and their values are performed by standard means:

- Editing the Element;
- Deleting the Element.

5.3.1.3.3 Creating Sample Documents

Purpose:

To create a sample document

Solution:

1. Go to the **Classifier** section.
2. On the left part of the workspace left-click the target category.

   Note

   Sample documents can be added only to those categories that do not include other nested categories.

3. On the right part of the workspace (in **Sample Documents** tab) on the toolbar click **Add**.
4. In the opened window click **Download**.
5. In the opened dialog box specify the document which you want to use for creating a digital fingerprint and click **Open**.
6. When file is downloaded, click **Close**.

   All necessary attributes are assigned to newly created sample document by default.

7. To change attributes given by the System on the toolbar click **Edit** (see "Sample Documents").

Example:

1) If you need the System to mark the interception object as INTERNAL_COMPANY_RULES when the traffic contains at least 30% of the text document "Internal Company Rules" document:
   a. go to the target category
   b. load the document file "Internal regulations of the company" as a sample document
   c. specify *INTERNAL_COMPANY_RULES* value for *Name* attribute and value *30* to *Text data quotation threshold* attribute.
2) If you need the System to mark the interception object as SETUP_EXE when the traffic contains at least 10% of the binary content of "Setup.exe" executable file:
   a. go to the target category
   b. load the file "*Setup.exe*" as a sample document
   c. specify *SETUP_EXE* value for *Name* attribute and value *10* to *Binary data quotation threshold* attribute.

Additional information:

Both editing and deleting of the sample documents are performed by standard means:

- Editing the Element;
- Deleting the Element.

5.3.1.3.4 Creating Sample Forms

Purpose:

Create a sample form.

Solution:

1. Go to the **Classifier section**.
2. On the left part of the workspace left-click the target category.

   Note

   Sample forms can be added only to those categories that do not include other nested categories.

3. On the right part of the workspace (in **Forms** tab) on the toolbar click **Add**.
4. In the open window click **Download**.
5. In the appeared dialog box select a document that will be an example of the sample form and click **Open**.
6. When file is downloaded, click **Close**.
   All necessary attributes are assigned to newly created sample document by default.

   Note

   By default only the completed form will be detected (the value of the attribute *Detect only filled forms* is *Yes*). If necessary, change this setting (see step 7 of this instruction).

7. To change attributes given by the System on the toolbar click **Edit** (see "Sample Forms").

Example:

If you need the System to mark the interception object as `RECRUITMENT_CHECKLIST` if the traffic contains even fragments of the blank questionnaire "Recruitment checklist":

1. go to the required category
2. load the document file "Recruitment checklist" as a sample form
3. specify *Yes* value for *Detect only filled forms* attribute

Additional information:

Both editing and deleting of the sample forms are performed by standard means:

- Editing the Element;
- Deleting the Element.

5.3.1.3.5 Creating Sample Stamps

Purpose:

Create a sample stamp.

Solution:

1. Go to the **Classifier** section.
2. On the left part of the workspace left-click the target category.

Note:

Sample stamps can be added only to those categories that do not include other nested categories.

3. On the right part of the workspace (in **Stamps** tab) on the toolbar click **Add**.
4. In the opened window click **Download**.
5. In the appeared dialog box select a document that will be an example of the sample stamp and click **Open**.
6. When file is downloaded, click **Close**.
   All necessary attributes are assigned to newly created sample document by default.
7. To change attributes given by the System on the toolbar click **Edit** (see article "Sample Stamps").

Note:

Details on sample stamps creating see in the InfoWatch Knowledge Base, "Using a Sample Stamp Detector" article.

Example:

If you need the System to mark the interception object as ROUND_SEAL if it contains image of company seal:

1. prepare `Stamp.png` file where the full size image of the company seal is placed on white square background.
2. go to the required category and load the `Stamp.png` file as a sample stamp
3. specify the *ROUND_SEAL* value to *Name* attribute.

Additional information:

Both editing and deleting of the sample stamps are performed by standard means:

- Editing the Element;
- Deleting the Element.

5.3.1.3.6 Creating Sample Database Uploadings

Purpose:

To create a sample database uploading.

Solution:

1. Go to the **Classifier** section.
2. On the left part of the workspace left-click the target category.

Note

Sample database uploadings can be added only to those categories that do not include other nested categories.

3. On the right part of the workspace (in **DB uploadings** tab) on the toolbar click **Add**.
4. In the appeared window click **Upload**.

5. In the appeared dialog box specify the file you want to download and click **Open**.
6. When file is downloaded:
   - click **Configure DB unloading** to customize the sample uploading;
   - close the window **Creating sample DB uploading** to exit without additional configuration.
7. Specify required attributes (see "Sample Database Uploadings").
8. Click **Save**.

Additional information:

You can specify several rules of processing the table columns by clicking **Add rule** and specifying the attributes for the rule. If there are several rules specified for the database upload, then triggering of at least one rule is enough to associate the interception object with this uploading.

Note

When you create or edit rules in the window **Edit rule,** the box **Available columns** displays columns that are available for creating rules on them.

For example:



Entry indicates that processing rule is created only on the first column of the table.

Field **Rules of table column processing** is filled according to following rules:

Condition.

Describes logical relationships between the columns and is used in the search. This part also sets the behavior of the algorithm when it finds empty cells. Condition includes numbers of columns and logical relationship between them.

Note

To avoid false positives the System uses stop-words:numbers, letters, and words which do not allow cells containing them to trigger. To complete list of stop-words see InfoWatch Knowledge Base article "List of stop-words for sample database uploadings".

For example:

condition 1+2 means that if analysis discovered data from the first cell of the row and from the second cell of the row, then this row is presented in the analyzed text (triggers).

condition 1+(2|3) means that the string is considered to be the triggered one if the first cell was triggered as well as either 2 or 3 cell.

condition (1|3)+(4|5) means that the string is considered to be the triggered one if either first or third cell and either fifth or fourth cell were triggered.

Warning!

In some lines of sample tables there may be empty cells. If one of the cells of the logical "and" is empty, the string would be considered to be untriggered. You can change this behavior for individual columns using an asterisk (*) in formula:

1 +2 * means that if the first cell of the string was triggered and the second cell of the same string was empty or contained only stop-words, then this line is considered to be triggered. If in this case the condition were 1 +2, the string would not be triggered.

Minimal quantity of rows.

This field defines the number of rows required to be found for considering the condition to be triggered.

For example:

Processing rule with attributes:

- Condition - 1+(2|3)
- Minimal quantity of rows - 10

means that the condition is triggered if the analyzed text contains 10 or more rows from the current sample table that meet the condition 1+(2|3).

Example:

If you need the System to mark an object as “PHONE_NUMBERS”, if the traffic contains a table (7 or more strings) with employees' phone numbers where both first and third columns are filled and the table has the following structure:

Last name	Name	Phone number
Smith	John	89441234347
Johns	Tom	83531355424
Williams	William	83544593406
White	Jane	83245446441
Black	Jillian	84534359243
Davis	Michael	83544352925

a. save a table in CSV or TSV format
b. load the generated file to the System
c. change the name of the uploading to "PHONE_NUMBERS"
d. configure rules of processing the table columns:
    - in field **Condition** specify: **1+4**
    - in field **Minimal quantity of rows** specify: **7**

When traffic with detected column of data is transferred, the System assigns the *PHONE_NUMBERS* category to the interception object.

Additional information:

Both editing and deleting of the sample DB uploadings are performed by standard means:

- Editing the Element;
- Deleting the Element.

5.3.1.4 Enabling and Disabling the Analysis on Subject Areas

Purpose:

1. To enable the analysis on specified subject areas
2. To disable the analysis on specified subject areas

Solution:

1. Enabling the analysis on specified subject areas
   a. Go to the **Classifier section**.
   b. On the left part of the workspace left-click the category containing target data.
   c. Click  **Activate category**.

2. Disabling the analysis on specified subject areas
   a. Go to the **Classifier section**.
   b. On the left part of the workspace left-click the category containing target data.
   c. Click  **Deactivate category**.



Note

You can disable not the whole category but only some of its components (see "Enabling and Disabling the Analysis on Confidential Data").

Additional information:

Example:

If you need the System to stop assigning the *Legal documentation* category to interception objects containing any element of specified category:

disable *Legal documentation* category.

5.3.1.5 Enabling and Disabling the Analysis on Confidential Data

Purpose:

1. To enable analysis of specified confidential data.
2. To disable analysis of specified confidential data.

Solution:

1. To enable analysis of specified confidential data.
   a. Go to the **Classifier section**.
   b. On the left part of the workspace left-click the category containing target data.

c. On the right part of the workspace go to the tab depending on the type of confidential information.

d. Left-click the needed element.

e. Click **Activate**.

2. To disable analysis of specified confidential data.

a. Go to the **Classifier section**.

b. On the left part of the workspace left-click the category containing target data.

c. On the right part of the workspace go to the tab depending on the type of confidential information.

d. Left-click the needed element.

e. Click **Deactivate**.

Additional information:

Example:

If you need the System to stop assigning *Law* category to objects containing the phrase "appeal case":

turn off *appeal case* term located in *Law* category.

5.3.1.6 Exporting and Importing the Classifier Database

Purpose:

1. To save XML document containing the classifier database to the computer hard drive.
2. To download classifier database stored on your computer as XML document for using it in the InfoWatch Traffic Monitor Management Console.

Solution:

1. Saving XML document containing the classifier database to computer hard drive.

1. Go to the **Classifier** section.
2. Click **Export classification base**.
3. In the appeared dialog box **Save as** specify path for the disk to save the classifier database to.
4. Click **Save**.

> **Warning!**
> Only the last applied classifier database is exported (see "Configuring the System").

2. To download classifier database stored on your computer as XML document for using it in the InfoWatch Traffic Monitor Management Console.

1. Go to the **Classifier** section.
2. Click **Import classification base**.

3. In the appeared dialog box **Import classification base** click **Download**.
4. In the appeared dialog box **Open** specify the file containing target classification database.
5. Click **Open**.

Additional information:

Example:

1) If you need to save the customized classification database for its further usage:

   Security officer should export the customized classification database to save a file containing an identical database to the computer using the Management Console.

2) If you need to load the database classification previously configured and saved as XML to the Management Console:

   using the Management Console Security officer should import the file containing customized classification database to gain an identical database in the Management Console .

5.3.2 Specifying Inappropriate Resources

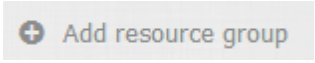
Purpose:

Specify the Internet-resources considered to be an improper usage of a worktime if visited. This is achieved in two actions:

1. Creating a group of resources.
2. Creating a resource.

Solution:

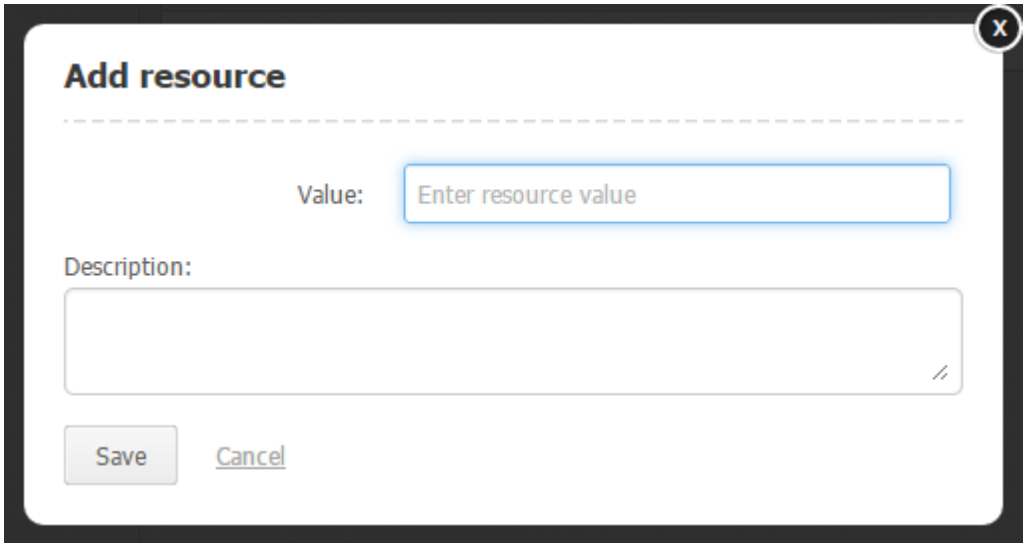
1. Creating a group of resources.

   1. Go to the **Lists** section, **Resource groups** tab.
   2. In the left part of the workspace click 

Add resources group.
   3. Enter a name of resources group into the displayed field **Enter list name**.
   4. Click  on the right corner of **Enter list name** field.

2. Creating a resource.

   1. Go to the **Lists** section, **Resources lists** tab.
   2. On the left part of the workspace left-click the needed resources group.
   3. On the right part of the workspace on the resources toolbar click **Add resource**.



4. On the opened window **Adding a resource** enter resources attributes (see "Lists of Resources").
5. Click **Save**.

> **Warning!**
>
> When editing the resources list is finished, you should apply updated System configuration (see "Configuring the System").

Additional information:

Both editing and deleting of the resource are performed by standard means.

Example:

If you need the System to give *IMPROPER_SITE* mark to the interception object when employee visits the EXAMPLE.COM site, Security Officer should create a group of resources *IMPROPER_SITE* containing *EXAMPLE.COM* resource.

Additional information:

- Editing a group of resources is performed by standard means (see "Editing the Element") but instead of **Edit** button located on a toolbar, the **Edit** button appeared on hover on the field with name of the target resource group is used.

  Deleting a group of resources is performed by standard means (see "Deleting the Element") but instead of **Delete** button located on a toolbar, the **Delete** button appeared on hover on the field with name of the target resource group is used.
- Editing and deleting of resources are performed by standard means:
  - Editing the Element;
  - Deleting the Element.

5.4 Configuring System Response

> **Warning!**
>
> To make elements changes described in this section affect the System operation you should apply the System configuration (for more details see "Configuring the System" and "Applying System Configuration").

Reference information:

By default there are preset policies in the System (see "Default Policies").

There may be a case in the System operation when the Analysis and Decision Making subsystems cannot use a policy (see "Policies Section"): for example, the policy does not exist, has been deleted or has failed. In this case no attributes are assigned to objects and in detailed form of event viewing (on the Messages tab) the messages about processing errors are displayed (see "Detailed Form of Events Viewing").

Why do you need to configure the System reactions:

When the corporate security policy is violated (e.g. sending of a confidential document outside the company) or improper use of work time is detected (e.g. viewing entertaining Internet sites from work computer), the System will perform:

- sending notifications to specified employees or Management Console users;
- appointment of the verdict to interception object;
- assigning the threat level, tags, and status to interception object.

Includes following actions:

Action	Description
Creating a Policy	Specifying reactions of the System to processed interception objects. Politics (in Management Console) is a container storing the action algorithms specified by user (see "Determining System's Response to Policy Violations ") in case of violation of the rules of placement, copying or transferring of protected objects (see "Creating a Rule")
Creating a Rule	Specifying what is a violation of rules for protected objects transferring, copying and placement
Determining System Response to Policy Violations	Specifying actions performed by System if rules for protected objects transferring, copying and placement are violated
Filtering a List of Policies	Selecting from the list of policies for the records that meet the filtering criteria. Is applied when you have a large number of policies in Management Console
Sending Notifications on Responded Rule	If the rule is triggered, the System sends a notification to a specified e-mail

See also:

- "Policies Section" - about the section where managing of the policies is performed.

5.4.1 Default Policies

These are the following default policies preset in the System:

- Data Protection Policy
- Control of Persons Policy
- Policy Regulating the Transfer of Password-Protected Data
- Policy Regulating the Transfer of Data Proceeded with Error

5.4.1.1 Data Protection Policy

There are two default data protection policies preset in the System:

- one for each sub-category of the *Company Structure* category
- one for the *Security label* category

Default policies have the following attribute values:

Attribute	Value
Policy name	<Category name>
Status	Active
Period of activity	Not limited
Type of objects of research	<Category name>

where <Category name> is the name of the category for which the policy is created.

Rules of transfer

1. *The rule regulating the transfer of confidential data outside the company perimeter*.

If a person sends the traffic of any type outside the perimeter of the company in any day of the week

Then the System performs the following actions:

- sets *Allowed* value to *Verdict* attribute of the object;
- sets *High* value to *Threat level* attribute of the object;
- sets *Under supervision* value to *Status* attribute of the person-sender.

2. *The rule regulating the transfer of confidential data by company management*.

If a person from the VIP group sends the traffic of any type to any recipient in any day of the week

Then the System performs the following actions:

- sets *Allowed* value to *Verdict* attribute of the object;
- sets *No threat* value to *Threat level* attribute of the object;
- sets *VIP* tag to the object.

Rules of copying

The rule regulating the copying of confidential information to removable devices.

If a person 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 *Allowed* value to *Verdict* attribute of the object;
- sets *High* value to *Threat level* attribute of the object;
- sets *Under supervision* value to *Status* attribute of the person-sender.

5.4.1.2 Control of Persons Policy

By default the System has a policy to monitor persons. This policy has the following attribute values:

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

Rule of transfer

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

If the person having *Under supervision* status sends the traffic of any type to any recipient

Then the System sets *To quarantine* value to *Verdict* attribute.

5.4.1.3 Policy Regulating the Transfer of Password-Protected Data

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

Default policy have the following attribute values:

Attribute	Value
Policy name	Password-protected data
Status	Active

Period of activity	Not limited
Type of objects of research	File formats

Rule of transfer

The rule regulating the transfer of data protected with password outside the company perimeter.

If a person sends the traffic protected with password outside the perimeter of the company in any day of the week

Then the System performs the following actions:

- sets *Allowed* value to event attribute *Verdict;*
- sets *High* value to event attribute *Threat level;*
- sets *For consideration* tag to the object.

5.4.1.4 Policy Regulating the Transfer of Data Proceeded with Error

By default the System has a policy regulating the transfer of data which processing was ended with error.

Default policy have the following attribute values:

Attribute	Value
Policy name	Processing error
Status	Active
Period of activity	Not limited
Type of objects of research	Processing errors

Rule of transfer

The rule regulating the transfer of data processed with error outside the company perimeter.

If a person sends the traffic of any type outside the perimeter of the company in any day of the week

Then the System performs the following actions:

- sets *Allowed* value to *Verdict* attribute of the object;
- sets *High* value to *Threat level* attribute of the object;
- sets *To approval* tag to the object.

5.4.2 General Information on Policies

This section describes the order of implementing the configured **System policies** (i.e. rules sets determining the analysis and processing of intercepting the objects) to **events** (objects of intercepting the network traffic).

The System applies policies to events in the following order:

1. **The event is checked for all active policies by turns**
2. **If policy 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 are applied to the interception object**

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

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 Verdict"). If any attribute of the event got multiple values (e.g. multiple recipients of the SMTP messages, 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	Channel	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	Channel	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

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 provide this the System selects rules matching the intercepted event from all of the policy rules by following attributes: ***Sender***, ***Recipient***, ***Channel*** for example

Sender	Direction	Recipient	Channel	Date	Reaction
Group: Lawyers, Person: Smith, Person: Johns	->	Group: Marketing, Person: Williams	SMTP	08:00-20:00	Notify: Miller, Threat level: Low
Group: Logistics	->	Group: Sales, Group: Delivery	Skype	10:00-19:00	Notify: Miller, Threat level: Medium
Group: Finance	-> <-	Group: Lawyers, Group: Sales			Notify: Thomas, Threat level: High

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

Sender	Direction	Recipient	Channel	Date	Reaction
Group: Lawyers	->	Group: Marketing	SMTP	08:00-20:00	Notify: Miller, Threat level: Low
Group: Lawyers	->	Person Williams	SMTP	08:00-20:00	Notify: Miller, Threat level: Low
Person Smith	->	Group: Marketing	SMTP	08:00-20:00	Notify: Miller, Threat level: Low
Person Smith	->	Person Williams	SMTP	08:00-20:00	Notify: Miller, Threat level: Low
Person Johns	->	Group: Marketing	SMTP	08:00-20:00	Notify: Miller, Threat level: Low
Person Johns	->	Person Williams	SMTP	08:00-20:00	Notify: Miller, Threat level: Low
Group: Logistics	->	Group: Sales	Skype	10:00-19:00	Notify: Johns, Threat level: Medium
Group: Logistics	->	Group: Delivery	Skype	10:00-19:00	Notify: Johns, Threat level: Medium
Group: Finance	->	Group: Lawyers			Notify: Thomas, Threat level: High
Group: Finance	->	Group: Sales			Notify: Thomas, Threat level: High
Group: Lawyers	->	Group: Finance			Notify: Thomas, Threat level: High
Group: Sales	->	Group: Finance			Notify: Thomas, Threat level: High

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 channel in the rule;
3. Presence of conditions of time in the rule;
4. Presence of conditions of channel 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
List of resources	300
Deny List of resources	150
Deny URL	75
Deny Domain	35
Deny Group	15
Deny Person	7
Deny Contact	3
Any	1.

For example, the rule with condition of forwarding from any sender to specific contact (10000 + 1 = 10001) has higher priority than the rule with condition of forwarding from particular person to person group (5000 + 2500 = 7500).

If two or more rules have equal number of points for sender-recipient, then the presence of conditions of time and channel 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 rule matched, then the default rule is selected (see "Determining System's Default Response").

Order of actions applying 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 notified
3. The highest level of violation specified in the selected rules is assigned to the event
4. The event is removed if deletion is specified in any rule (one rule is enough for deletion)
5. The event is not removed if deletion cancellation is specified in any rule
6. The event is blocked if any rule blocks the sending
7. All tags specified in selected rules are assigned to the event

Example:

Let the System have two policies:

Policy №1					
Category: Accounts					
Rule number	Sender	Recipient	Date	Channel	Reaction

1.1	Group: Sales Department	Group: Accounts Department	08:00-20:00	SMTP	Violation: No violation
1.2	Smith	Group: Accounts Department		SMTP	Violation: No violation
1.3	Smith	<>Perimeter: Company			Violation: Medium
1.4	Default:				Violation: High

Policy №2					
Category: Contract					
Rule number	Sender	Recipient	Date	Channel	Reaction
2.1	Group: Sales Department	<>Perimeter: Company	08:00-20:00	SMTP	Violation: No violation
2.2	Smith	<>Perimeter: Company		SMTP	Violation: No violation
2.3	Default:				Violation: No violation

Let Smith be a member of the "Sales Department" group. Johns is a member of the "Accounts Department" group. E-mail **williams@mail.com** is outside the perimeter of the company.

If there is an event:

Data	Sender	Recipient	Date	Channel
Category: Accounting, Contract	Smith	Johns, williams@mail.com	19:00	SMTP

This event consists of two sub-events with different "sender-receiver" pairs: "Smith->Johns" and "Smith-> williams@mail.com".

1. Check for conformance to policy №1.
The event corresponds to policy №1 as it contains Category - Accounting.

The "Smith->Johns" sub-event is considered:

Sender	Recipient	Date	Channel
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	Channel
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 corresponds to policy №2 as it contains Category - Contract.

The "Smith->Johns" sub-event is considered:

Sender	Recipient	Date	Channel
Smith	Johns	19:00	SMTP

This sub-event corresponds 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	Channel
Smith	w illiams@mail.com	19:00	SMTP

This event has two sub-rules: №2.1 and 2.2. The more priority one is sub-rule №1.2. Therefore the rule №2.2 is selected

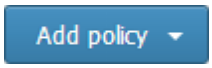
3. The selected actions are applied : №1.2, №1.3, № 2.3, №2.2

5.4.3 Creating a Policy

Purpose:

To create a policy

Solution:

1. Go tho the **Policies** section.
2. On the right part of the workspace 

Add policy and select **Data protection policy** from drop-down list (creating a Control of persons policy is described in "Adding a Person or Workstation to Data Protection Policy" section).
3. In the opened window flag needed objects of research.

   Warning!

   If there is more than one object of research specified for the policy, then for actuating of policy rules (see "Rules and their Viewing Form") the object should have a violation for each object of research.
4. Click **Add**.
5. In the right part of the workspace specify required fields (see "Policies Section") and click **Save**.

Example:

If you want the System to respond to actions with data relating to *State secret* category,

add a policy of data protection and specify *State secret* category as an object of research.

5.4.4 Editing Policy

Purpose:

Edit the policy.

Solution:

1. Go tho the **Policies** section.
2. On the left part of the workspace left-click the target policy.

   Note:
   When you select a policy, point the cursor over tile header. If you select an entry containing a rule, then in the right part of the workspace the configuring panel for rule will be displayed not for policy (see "Editing Rules").
3. On the right part of the workspace specify required fields (see "Policies Section") and click **Save**.

   Note:

   To change a list of protected objects click Add **Add** in **Protected objects** section and edit the list.

5.4.5 Creating a Rule

Reference information:

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

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

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

- If one rule was triggered, the system performs the actions specified in this rule (see "Determining System's Response to Policy Violations").
- If several rules are triggered and:
  - their actions contradict each other, then the System selects the priority action and executes it (about the order of priorities selecting see "General Information on Policies");
  - their actions do not contradict each other, then the System performs all actions that do not contradict others.
- If the rule was not triggered or specified, then the System performs the actions specified for the default rule (see "Determining System's Default Response").

For the policy of persons control you may set rules of interception of events with different levels of threat only (see " Adding a Person or Workstation to Data Protection Policy").

Note

If the interception object triggered several policies and each policy had its own rules, then the System selects the top-priority one and executes it (about the order of priorities selecting see "General Information

on Policies"); actions that do not contradict each other are performed completely.

Purpose:

To determine actions which should be performed to protected objects to cause the System reaction (creating rules for control of persons policy is described in "Adding a Person or Workstation to Data Protection Policy").

Solution:

1. Go to the **Policies section**.
2. Add a rule in one of the following ways:
   - Left-click the target policy and on the right side of the policy tile select appropriate tab (*of transfer*, *of copying*, *of placement*) depending on the required task and click 

Add rule.
   - On the left side of the workspace left-click the target policy and then select the target rule on the right side of the workspace in **Add rule** section.
3. Configure the rule by using a form on the right side of the workspace (see "Rules and their Viewing Form").

Example:

If you want the System to respond to storing the protected objects in the file storage:

select the storage location as a rule of placement of protected objects *File storage* and specify additional characteristics in the form of storage adding.

For more information:

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

5.4.6 Editing Rules

Purpose:

Edit a rule.

Solution:

1. Go tho the **Policies** section.
2. On the left side of the workspace left-click the target policy.
3. On the right side of the target policy tile select a tab (*of transfer*, *of copying*, *of placement*) depending on the desired task and left-click the target rule from the rules list.
4. On the right side of the workspace change required fields in **Rule settings** block (see"Rules and their Viewing Form") and click **Save**.

5.4.7 Determining System Response to Policy Violations

Reference information:

For each data protection policy you can configure System response to following cases:

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

Each control of persons policy can set a System response to interception of events with different levels of threat.

Purpose:

Determine the way of System response to specified actions with the protected data (creating rules for control of persons policy is described in "Adding a Person or Workstation to Data Protection Policy" section).

Solution:

1. Go to the **Policies section**.
2. On the left side of the workspace left-click the target policy.
3. On the right side of the target policy tile select a tab (*of transfer*, *of copying*, *of placement*) depending on the desired task and left-click the target rule from the rules list (on rule creating see “Creating a Rule" section).
4. On the right side of the workspace edit the fields in the block **Action** (see "Rules and their Viewing Form" section) click **Save**.

For example:

If you need the System to assign a *Sending confidential data on weekends* tag and *Medium* treat level to object of transferring a file related to *Strictly confidential* category and transferred is on Saturdays and Sundays, then:

security officer should perform the following actions:

- create a *Sending confidential data on weekends* tag (see "Managing Tags");
- create a policy of data protection for *Strictly confidential* category (see "Creating a Policy");
- create a transfer rule by setting the `Saturday` and `Sunday` values to *Days of week of rule activity* attribute (see "Creating a Rule");
- specify the attributes of **Action** section with the following values:
  - *Set threat level* attribute - `Medium` value;
  - *Tags* attribute - `Sending confidential data on weekends` value.

See also:

- "Editing Rules" section.

5.4.8 Determining System Default Response

Reference information:

If the policy actuated on the interception object but none of the rules triggered or were defined, then the System performs default actions.

Purpose:

Determine the of the System response to specified actions with the protected data if none of the rules triggered.

Warning!

There is no similar possibility for the control of persons policy.

Solution:

1. Go to the **Policies** section.
2. On the left side of the workspace left-click the target policy.
3. On the right side of the target policy tile select a tab (*of transfer*, *of copying*, *of placement*) depending on the required task and left-click the lower part of the tile (below the dotted line).
4. On the right side of the workspace edit the necessary fields in the single block **Action** (see "Rules and their Viewing Form") and click **Save**.

For example:

If you want the System to assign the person's card status by default when this person copies files relating to *State secret* category even if there is no rules actuated:

security officer should perform the following actions:

- create a policy of data protection for data with category *State secret* (see "Creating a Policy");
- go to settings of the default policy actions;
- in the only section **Action** set the r åÇÉê=pì éÉêî áëáçå value to *Set status* attribute:

See also:

- "General Information on Policies".

5.4.9 Filtering a List of Policies

Purpose:

To filter the list of policies.

Solution:

1. Go to the **Policies section**.
2. On the left part of the workspace click **Filter**.
3. Type the filter criteria in one of the fields or in both of them:
   - **Filter by policy name** - start typing and select the name of required policy (repeat to select several policies)
   - **Filter by objects** - start typing and select the name of required object (repeat to select several objects)
4. Click **Apply filter**.

5.4.10Sending Notifications on Responded Rule

Purpose:

Configuring the automatic notification about responded rule to some person.

Warning!

You can use only the e-mail address to send notifications. When you choose the existing contacts, select persons 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. On the right side of the target policy tile select a tab (*of transfer*, *of copying*, *of placement*) depending on the desired task and left-click the target rule from the rules list.
4. On the right side of the workspace in **Send notification** field select contact for notifications in one of the following ways:
   - start typing the contact details and select the desired entry from the drop-down list;
   - click **Add** in the displayed window:
     - add a new contact - on the **Contacts** tab click Add contact **Add contact** and enter contacts for notifications (see the similar procedure described in "Adding a Contact to Person" section).
     - select a contact from the existing ones - select a person entry or Management Console user on **Persons** tab.

Example:

If you need the System to assign the ***Allow*** verdict to the interception object when any confidential data (*Commercially_Confidential* category) is being copied to the removable device on weekends while the copying person gain the ***Under the supervision*** status and *example@company.com* mailbox receives a notification about the incident:

Security officer creates a policy of data protection for category *Commercially_Confidential*.

Then Security officer creates a rule of copying for the created policy, and assigns the following values to attributes:

- attribute *Days of week of rule activity* - *Saturday* and *Sunday* value;
- attribute *Devices* - *Plug-in devices* or *Printers or external devices* value;
- attribute *Send notification* - value *example@company.com* value;
- attribute *Assign verdict* - *Allow* value.

5.5 Managing Interception Objects

Why the managing of interception objects is needed?

To:

- monitor the statistics of corporate security policy violations;
- view data of every single accident;
- make reports on violations / violators.

Includes following actions:

Action	Description
Viewing Violations and Violators Summary	Viewing the statistical information and event selections
Viewing Events	Viewing data on every single interception object
Managing Reports	Generating summary on violations / violators
Making Decision on Object	User decision concerning the object
Adding and Deleting a Tag	Adding a mark to the object
Creating Notification on Event	Sending a report on the object to other Management Console users
Saving an Event (for SMTP Objects)	Saving the object to the disk in EML format
Dispatching Blocked Object	Sending a blocked message to the recipient
Events Filtering	Selecting interception object to display according to chosen attributes

5.5.1 Viewing Violations and Violators Summary

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

Purpose:

View the violations and violators summary.

Solution:

1. Go to **Dashboard** section.
2. Configure toolbar (see "Managing Dashboards").
3. Configure required widget (see "Managing Widgets").
4. View if the configured widget obtain a summary.

5.5.1.1 Managing Dashboards

Managing dashboards includes the following tasks:

Action	Description
Creating a Dasboard	To manage the dashboard you should create it
Deleting a Dashboard	If the dashboard is not needed any more, you may delete it

5.5.1.1.1 Creating a Dasboard

Purpose:

Create the dashboard.

Solution:

1. Go to **Dashboard** section.
2. On the left side of the workspace click **Add dashboard**.
3. Enter a name of a new dashboard.
4. Click **Save**.

5.5.1.1.2 Deleting a Dashboard

Purpose:

Delete a dashboard.

Solution:

1. Go to the **Dashboard** section.
2. On the right side of a tile with dashboard name click .
3. Click **Delete**.

5.5.1.2 Managing Widgets

Managing widgets includes the following tasks:

Action	Description
Adding a Widget	To manage widget you should create it
Editing a Widget	To specify conditions according to which the widget will display a summary, you should configure this widget
Deleting a Widget	If the widget is not needed any more, you may delete it

5.5.1.2.1 Adding a Widget

Purpose:

Create a widget.

Solution:

1. Go to the **Dashboard** section.
2. Go to the required dashboard.
3. Click 

+Add widget.
4. Enter a name of new dashboard.
5. In the string of target widget click **Add**.
6. Click **Close** or standard closing button in the upper right corner of the window.

5.5.1.2.2 Editing a Widget

Purpose:

Configure a widget.

Solution:

1. Go to the **Dashboard** section.
2. Go to the required dashboard.
3. Configure the target widget using interface elements located on the widget (see "Widgets").



Note

You can use a function of advanced widget configuration by clicking  button. Click **Save** when you finish configuring.

5.5.1.2.3 Deleting a Widget

Purpose:

Delete the widget if it is not needed any more.

Solution:

1. Go to the **Dashboard** section.
2. Go to the required dashboard.
3. Click  in the upper right corner of the target widget.

5.5.2 Viewing Events

Purpose:

View information on interception object.

Solution:

1. Go to **Events** section (see "Events Section").
2. Apply event query (see "Events Filtering").
3. If necessary, select event displaying attributes (see "Selecting Event's Display Fields").
4. View event information on the event tile or in the string of a table (see "Selecting Event Displaying Style").
5. If necessary, use short and detailed event forms.

5.5.2.1 Events Filtering

The case is performed in the **Events** section (see "Events Section").

Purpose:

To filter interception objects

Solution:

1. Go to **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 methods of creating a query available: standard mode and extended mode.

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

Note

To hide filter results, click button at the right of the filter name in the filter list.

See also:

- "Query Creation in Standard Mode";
- "Query Creation in Extended Mode".
- "Creating Query with Negation in Standard Mode"
- "Creating Query with Negation in Extended Mode"

5.5.2.1.1 Query Creation in Standard Mode

Purpose:

To create a selection of objects in the standard mode.

Solution:

1. Go to **Events** section.
2. On the toolbar in the upper string of the left side of workspace click **Add**.
3. On the right side of workspace (**Condition** tab) specify values for fields which you want to filter with (see " Condition").
4. On the right side of workspace go to **Display field** tab and specify attributes which values will be displayed for events confirming specified conditions (see "Display Fields").

   To make more precise selection use the extended mode.

   Note

   Editing a query in the extended mode do not let you edit a query in the standard mode subsequently.
5. Click:
   - **Save** - to save a query.
   - **Save and execute** - to save and apply a query.

Example:

If you need the System to display events with *High* violation level and *Financial documentation* policy applied:

then you should create a filter in the standard mode and specify the *High* value for *Violation level* attribute and *Financial documentation* value for *Policy* attribute.

Additional information:

Editing and deleting of the query is performed by standard means:

- Editing the Element;
- Deleting the Element.

5.5.2.1.2 Query Creation in Extended Mode

Purpose:

To create a selection of objects in the extended mode.

Solution:

1. Go to **Events** section.
2. On the toolbar in the upper string of the left side of workspace click **Add**.
3. On the right lower part of workspace click **Extended mode** button.
4. Click **Yes** in the opened window.
5. Drag and drop event attributes and *Block* element to the workspace of **Extended mode** window to create query conditions basing on which the events selection will be performed (see "Extended Mode").

   > **Note**
   >
   > Use *Block* element to separate attributes associated with conjunction operation (AND) from attributes associated with disjunction operation (OR).

   To fix event attributes and *Block* element on the workspace you need to drag and drop it to see dash line marking like the following:

   To change operation left-click the icon (AND , OR) to obtain target value:

   - icon AND for conjunction operation (AND)
   - icon OR for disjunction operation (OR).
6. Click **Save**.
7. On the right side of workspace (**Display field** tab) specify attributes which values will be displayed for events confirming specified conditions (see "Display Fields").
8. Click:
   - **Save** - to save a query.
   - Save and execute - to save and apply a query.

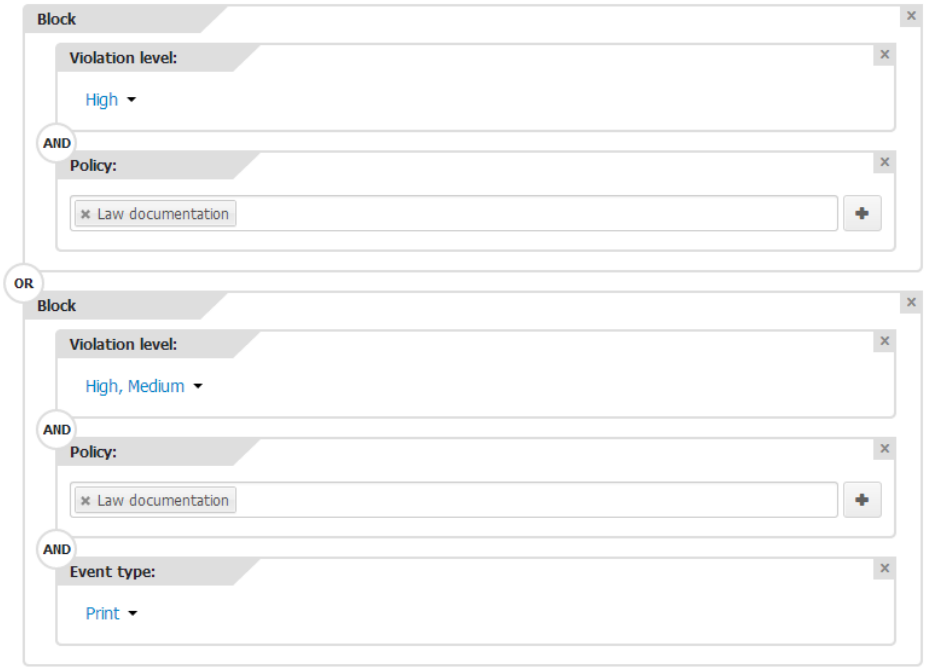
Example 1:

If you need the System to display events:

- with *High* violation level and *Financial documentation* policy applied;
- with *High* and *Medium* violation level and *Financial documentation* policy applied and *Print* event type:

then you should create a filter in the extended mode and specify two blocks combined by the disjunction operation (logical "OR"):

- The first block contains attributes with values:
  - `Violation level` is *High*;
  - `Policy` is *Financial documentation*;
- The second block contains attributes with values:
  - `Violation level` is *High* and *Medium*;
  - `Policy` is *Financial documentation*;
  - `Event type` is *Print*;
- Attributes within blocks are combined by the conjunction operation (logical "AND").



Creating a query in extended mode by conditions

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 block are combined by the operation of the logical "AND", then filtering results will contain objects with at least one attachment that satisfies all specified conditions. In the example below, filtering results will display objects with at least one attachment with the name "*abc*" and of PNG format.



2. If each condition is in a separate block and blocks are combined by the operation of the logical "AND", then filtering results will contain objects, for which all conditions are satisfied, but not necessarily for the same attachment. In the example below, filtering results will display objects with at least one attachment with the name "*abc*" and at least one attachment of PNG format.



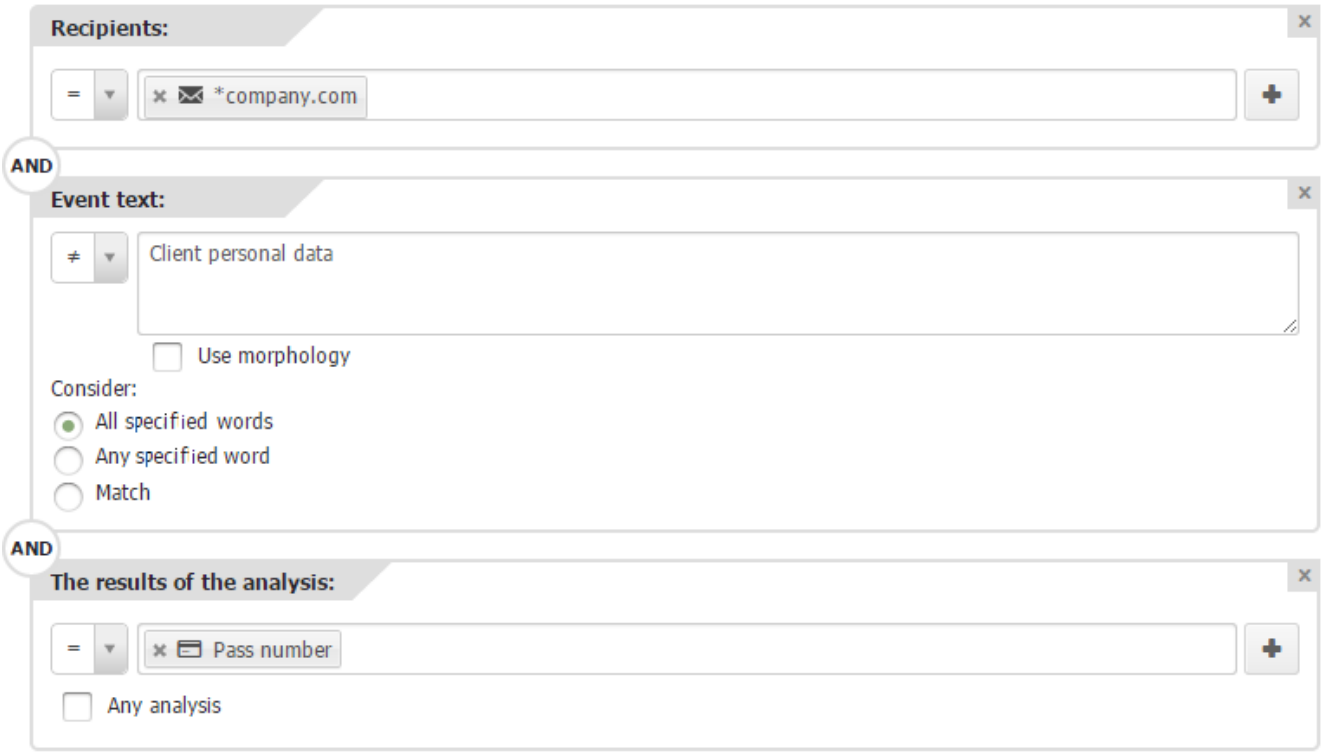
Example 3:

If you need the System to display events that:

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

then you should create a filter in the extended mode and specify the following attributes combined by the conjunction (logical "AND") operation (see the picture below):

- `Recipients` – **company.com*;
- `Event text` – "*Clients personal data*"; the search is performed in the *All specified words* mode and a negation parameter is applied to the attribute;
- `Analysis result` - a text object "*Pass number*".



Additional information:

Editing and deleting of the query is performed by standard means:

- Editing the Element;
- Deleting the Element.

5.5.2.1.3 Creating Query with Negation in Standard Mode

Purpose:

To create a query with negation in the standard mode.

Solution:

1. Go to **Events** section.
2. On the toolbar in the upper string of the left side of workspace click **Add**.
3. On the right side of workspace (**Condition** tab) specify values for fields which you want to filter with (see " Condition").
4. Set negation parameter ≠ (meaning "except") to the attributes which should not be present in search results.

   Note

   Creating negations for attributes with multiple values, negation is being applied to all of them. Thus, in search results, there will be events with none of the negated attribute values or events which do not contain such attribute at all.
5. On the right side of workspace go to **Display field** tab and specify attributes which values will be displayed for events confirming specified conditions (see "Display Fields").

To make more precise selection use the extended mode.

> **Note**
>
> Editing a query in the extended mode do not let you edit a query in the standard mode subsequently.

6. Click:
   - **Save** - to save a query.
   - **Save and execute** - to save and apply a query.

Example:

If you need the System to display events with *High* violation level and any policy except for *Financial documentation* policy or without *Policy* attribute applied:

then you should create a filter in the standard mode and specify the *High* value for *Violation level* attribute and *Financial documentation* value for *Policy* attribute with negation ≠.

Additional information:

Editing and deleting of the query is performed by standard means:

- Editing the Element;
- Deleting the Element.

5.5.2.1.4 Creating Query with Negation in Extended Mode

Purpose:

To create a query with negation in the extended mode.

Solution:

1. Go to **Events** section.
2. On the toolbar in the upper string of the left side of workspace click **Add**.
3. On the right lower part of workspace click Extended mode **Extended mode** button.
4. Click **Yes** in the opened window.
5. Drag and drop event attributes and *Block* element to the workspace of **Extended mode** window to create query conditions basing on which the events selection will be performed (see "Extended Mode").
6. Set negation parameter ≠ (meaning "except") to the attributes which should not be present in search results.

> **Note**
>
> Creating negations for attributes with multiple values, negation is being applied to all of them. Thus, in search results, there will be events with none of the negated attribute values or events which do not contain such attribute at all.

Note

Use *Block* element to separate attributes associated with conjunction operation (AND) from attributes associated with disjunction operation (OR).

To fix event attributes and *Block* element on the workspace you need to drag and drop it to see dash line marking like the following:

To change operation left-click the icon (

, 

) to obtain target value:

- icon 

for conjunction operation (AND)
- icon 

for disjunction operation (OR).

7. Click **Save**.
8. On the right side of workspace (**Display field** tab) specify attributes which values will be displayed for events confirming specified conditions (see "Display Fields").
9. Click:
   - **Save** - to save a query.
   - Save and execute - to save and apply a query.

Example:

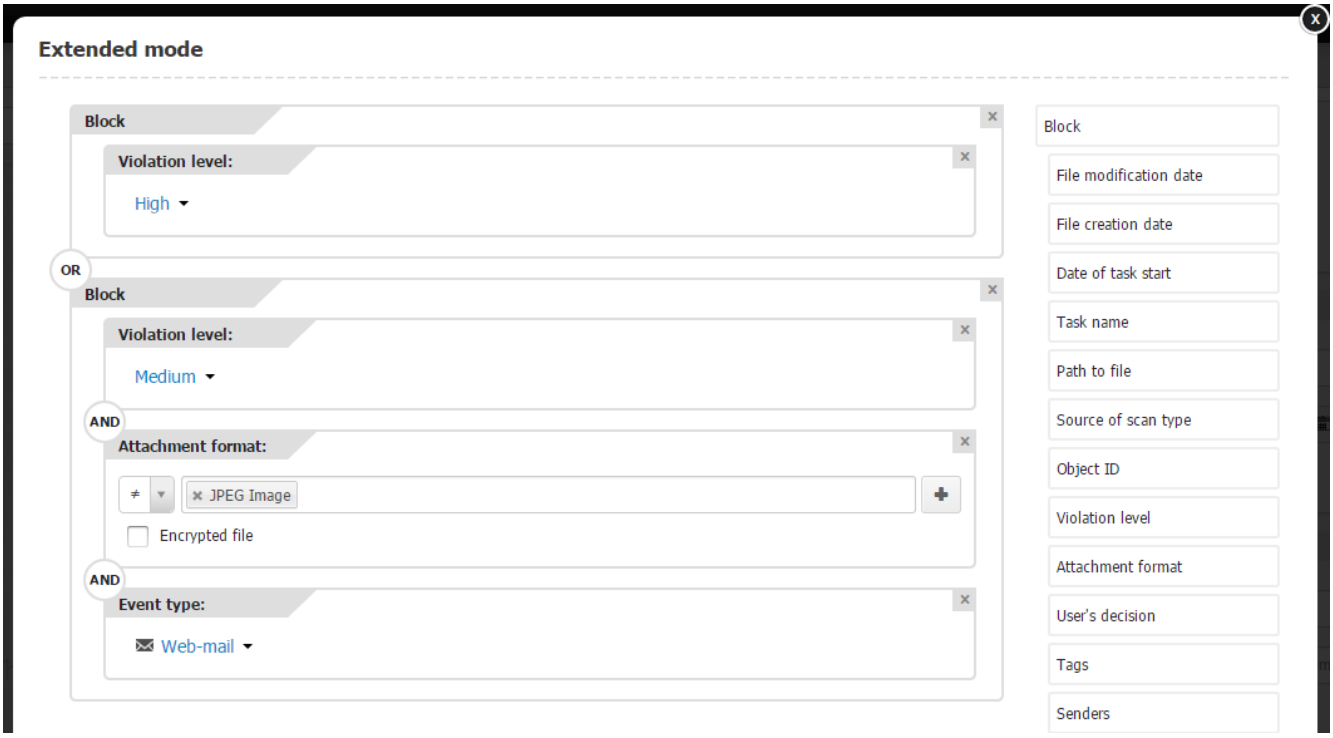
If you need the System to display events:

- with *High* violation level;
- with *Medium* violation level, any attachment format except for *JPEG Image* and with *Web-mail* event type.

then you should create a filter in the extended mode and specify two blocks, connected with disjunction operation:

- First block contains attributes with values:
  - `Violation level` is *High*;
- Second block contains attributes with values:
  - `Violation level` is *Medium*;
  - `Attachment format` is *JPEG Image* with negation parameter

;
  - `Event type` is *Web-mail*;
- Attributes inside blocks are connected with disjunction operation. If edited in extended mode, the query will be looking like the following:



Creating a query in extended mode by conditions

Additional information:

Editing and deleting of the query is performed by standard means:

- Editing the Element;
- Deleting the Element.

5.5.2.2 Selecting Event Display Fields

Reference information:

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

Purpose:

To select displaying attributes of interception objects.

Solution:

1. Go to **Events** section.
2. Perform one of the following actions:
   - Edit existing query by clicking **Edit query** button.
   - Create a new query.

   Note

   There are two methods of creating a query available: standard mode and extended mode.
3. On the right part of workspace go to **Display field** 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.

5.5.2.3 Viewing Short Event Form

Purpose:

To view a short information on the interception object.

Solution:

1. Go to **Events** section.
2. Apply event query (see "Events Filtering").
3. Select a tile of target event from the list (or a string of target event from the table).
4. Click in the upper string of the right part of the workspace to open short form (to hide short form click).
5. View event shortcut in the right part of the workspace.

See also:

- Short Event Viewing Form;
- Viewing Detailed Event Form.

5.5.2.4 Viewing Detailed Event Form

Purpose:

To view a detailed information on the interception object.

Solution:

1. Go to **Events** section.
2. Apply event query (see "Events Filtering").
3. Select a tile of target event from the list (or a string of target event from the table).
4. Click Detailed information **Detailed information** button in the upper string of the right part of the workspace to open detailed form (to hide the detailed form click **Close** or a standard closing button in the upper-right window corner).
5. View detailed event form in the popup window:
   - **Main information** tab displays event attributes (For example, **Senders**, **Recipients**, **User decision**, **Delivery tracking**, **Tags, Send date, Intercept date**)
   - **Analysis result** tab displays **Policy, Category**, **Text Objects**.
   - **Processing status messages** tab displays errors, which occur while object processing.

To view event content, press sign in a lower right corner of the window.

See also:

- Detailed Form of Events Viewing;
- Viewing Shortcut Event Form.

5.5.3 Managing Reports

Purpose:

Create and view reports on interception objects.

Solution actions:

Action	Description
Creating a Report	Creating a report on the configured dashboard
Viewing a Report	Viewing a generated report in file of PDF or HTML format

See also:

- Dashboard Report.

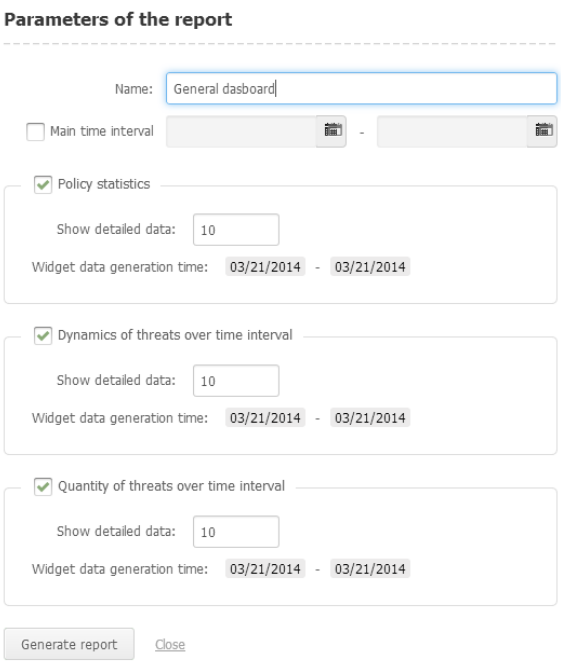
5.5.3.1 Creating a Report

Purpose:

Create a report on the intercepted objects.

Solution:

1. Go to **Dashboard** section.
2. Click **Generate report** button.
3. In the opened window specify report's attributes and click **Generate report** (see "Dashboard Report").



Creating a report

Generated report will be saved in the System and available by clicking **Show list of reports** button (see "Viewing a Report").

Note:
In case widget has been deleted, but there was a report, generated previously with this information, report will not be deleted.

5.5.3.2 Viewing a Report

Purpose:

View a created report on intercepted objects.

Solution:

1. Go to **Dashboard** section.
2. Click **Show list of reports** button.
3. In the opened window, in the string of the needed report, click:

- **PDF** - if you need to display the report in PDF format;
- **HTML** - if you need to display the report in HTML format.

The report will be displayed in a new browser window.

Note
You can save, send or print created report by standard means of your operating system

5.5.4 Making Decision on Object

Purpose:

To make a decision on the object.

Solution:

1. Go to **Events** section.
2. Select a target event by left-clicking on it.
3. At the event toolbar click appropriate button to assign a user decision to the object:

-  **Violation** - to make decision that the object violates the security policy.
-  **No violation** - to make decision that the object does not violate the security policy.
-

No decision - to cancel previously made decision.
-  **Requires additional proceeding** - to cancel previously made decision and leave the object for further consideration.

See also:

- Retrospective Data Analysis, User Decision on an Object.

5.5.5 Adding and Deleting a Tag

Purpose:

To add a tag to the interception object.

Solution:

1. Go to **Events** section.
2. Left-click the target event.
3. On the event toolbar click **Set tag**.
4. In the opened dialog box select the tag by flagging it.
5. Click **Save**.

See also:

- Tags.

5.5.6 Creating Notification on Event

Purpose:

Send a notification on the event to specified contacts.

Solution:

The sending of notifications is performed when a policy is applied. Notifications sending is configured in the following ways:

1. Create a policy (see "Creating a Policy") and a rule for it (see "Creating a Rule").
2. During rule configuration in the **Send notification** field specify target contacts (see details in "Sending Notifications on Responsed Rule").

   When the rule responses to any event, the notification to specified contact will be sent.

5.5.7 Saving an Event (for SMTP Objects)

Purpose:

To save interception object (SMTP-letter).

Solution:

1. Go to **Events** section.
2. Left-click the target event.
3. Call the event saving dialog by one of the following ways:
   - click **Save** in shortcut event viewing form;
   - click **Download** in detailed event viewing form.
4. In the opened dialog box select the directory to save event to.
5. Click **Save**.

5.5.8 Dispatching Blocked Object

Reference information:

If a person sends SMTP-letter recognized as potential violation of security policy and moved to quarantine by the System (*Normal* transport mode), then security officer can allow its sending (see "Making Decision on Object", *No violation* decision) afterwards. In this case the System "dispatches" a letter and person receives a notification.

Purpose:

Send to the addressee a letter which was previously blocked.

Solution:

Warning!

You can dispatch the object which has *Quarantine* status. Deleted and blocked objects cannot be dispatched.

1. Go to **Events** section.
2. Left-click the target event.
3. Click **No violation** on the toolbar.

See also:

- Object Analysis and Verdict.

5.6 Managing Crawler Subsystem

Warning!

To make elements changes described in this section affect the System operation, you should apply the System configuration (for more details see "Configuring the System" and "Applying System Configuration").

Why for the Crawler subsystem is needed:

In order to scan the following file storages:

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

Includes following actions:

Action	Description
Configuring Scanner	After System installation one or several scanners are available and can be configured
Creating a Job	To work with the job you should create it
Launching and Stopping the Job	Running the job starts with the scanning of the target file storage; when the job is finished, the scanning stops
Editing the Job	Changing job settings
Cleaning the Hash Base	Discarding of files checking sums saved in the System
Viewing Launch History	Viewing a history of launching the selected scanning job
Saving Scan Report	Saving a report on the selected scanning job launch

See also:

- Crawler Section.

5.6.1 Configuring Scanner

Purpose:

To configure the scanner of the Crawler subsystem.

Solution:

1. Go to the **Crawler** section.
2. To the right of the scanners drop-down list click  **Edit the scanner configuration**.
3. On the right part of the workspace in **Details** tab enter the scanner attributes (see "Scanner").

   When you change at least one attribute to the right of the button  **Edit scanner configuration,** the icon  will by displayed indicating that scanning jobs for this scanner are not performed.
4. Click **Save**.

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

Additional information:

The attribute value **Display users in events** lists the standard SIDs. If necessary, the user can add 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 - starts with "S-1-5-21-" 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 details about the format of the regular expression language see in the article "Regular Expression Language".

5.6.2 Creating a Job

Purpose:

To add a scanning job

Solution:

1. Go to the **Crawler** section.
2. Click **Create job** on the toolbar.
3. Left-click the necessary job in the list.
4. On the right side of the workspace on the **Details** tab enter job attributes (see "Scanner Jobs"). The following fields are required:
   - **Scanning policy**;
   - **Scannable groups/workstations**;
   - **Schedule**.
5. Click **Save**.

Example:

If you need the System to assign *Printed 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:

a. create a term with text value "printed board" (see "Creating Terms") and *Printed board* tag (see "Managing Tags")

b. apply the configuration (see "Applying the System Configuration")

c. create a scanning job selecting *SharePoint 2007/2010* as scanning policy and specifying following values of attributes:

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

d. create a policy with following values in rule of placement:

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

Warning!

During the job executing by the domain administrator and other users the error message could be appeared:

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

where `<path_to_folder>` is absolute path to the folder where the job works.

That situation can arise if the owner of the folder has restricted operations with the folder.

5.6.3 Launching and Stopping the Job

Purpose:

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

Solution:

1. Launching scan job.
   1. Go to the **Crawler** section.
   2. Left-click the necessary job in the list.
   3. On the toolbar click  **Run job**.
2. Finishing scan job.
   1. Go to the **Crawler** section.
   2. Left-click the necessary job in the list.
   3. On the toolbar click **Stop job**.

5.6.4 Editing the Job

Purpose:

To change parameters of the scanning job.

Solution:

1. Go to the **Crawler** section.
2. Left-click the necessary job in the list.
3. On the right side of the workspace on the **Details** tab change job attributes (see "Scanner Jobs").
4. Click **Save**.

5.6.5 Cleaning the Hash Base

To provide Crawler work optimization the storage of **hashes** (checksums of files) is designed. 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. It reduces a load of a channel between Crawler and Traffic Monitor Server and a load of the Traffic Monitor Server itself; it also excludes duplication of identical events for each start of a scanning job.

Features of hash base storage:

- Hash base is saved separately for each scanning job. Therefore if some file was already processed by one job, then at creation and start of 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 do a periodical cleaning of hash base. For example, it is needed when the Traffic Monitor configuration was edited, in other words, according to new script or term list or etc, the decision if the intercepted object is a potential violation or not will be accepted by 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. Choose the necessary job in the list.
3. Click **Purge hashes** on the toolbar.

5.6.6 Viewing Launch History

Reference information:

On the **Launch history** tab there is an information about launches of the selected scan job displayed (see "Launch History").
When you select one of the entries in the table, the detailed information about the selected launch is displayed.

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 on the right side of the workspace, on the **Launch history**tab.
4. To view more information about the job and the launch settings, left-click the necessary launch entry in the list.

Extended information is presented in the following tabs:

- **Launch events** - provides system information about the launch of scanning job.
- **Launch settings** - contains the list of attributes of scanning job (see "Scanning Jobs" section).
- **Current status** - contains information about the current status of a launched job (for jobs with status other than *Launched* the tab is unavailable).

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

5.6.7 Saving Scan Report

Purpose:

To save a report on scanning job launch.

Solution:

1. Go to the **Crawler** section.
2. Left-click the necessary job in the list.
3. Open **Launch history** tab.
4. In the string of the necessary launch click .
5. Open the downloaded .xls file.

5.7 Managing Catalogues

Warning!

To make changes of elements described here affect the System, you should apply updated System configuration (see details in "Configuring the System" and "Applying System Configuration").

Why the catalogues managing is needed:

To add, edit, delete catalogues used in the System.

Consists of following actions:

Action	Description
Managing Tags	Editing list of tags
Managing Resources Lists	Editing list of resources. **Note:** Main information on this case is held in "Specifying Improper Resources" section
Managing Statuses	Editing list of statuses
Managing Perimeters	Editing list of perimeters

See also:

- Lists Section.

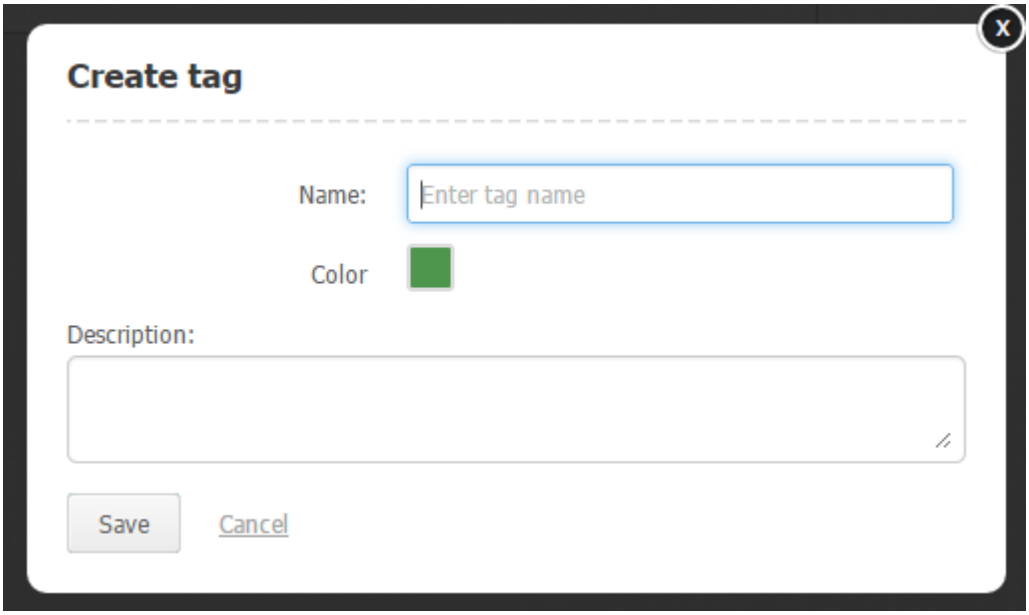
5.7.1 Managing Tags

Purpose:

To create a tag.

Solution:

1. Go to the **Lists section**, to the **Tags tab**.
2. On the toolbar click **Add**.



3. Specify attributes of the added tag (see. "Tags").
4. Click **Save**.
5. If necessary, repeat these steps.

Additional information:

Both editing and deleting the tag are performed by standard means:

- Editing the Element;
- Deleting the Element.

5.7.2 Managing Resources Lists

Purpose:

Add a resource and a list of resources.

Solution:

Creating resources and resources lists is described in "Specifying Improper Resources" section.

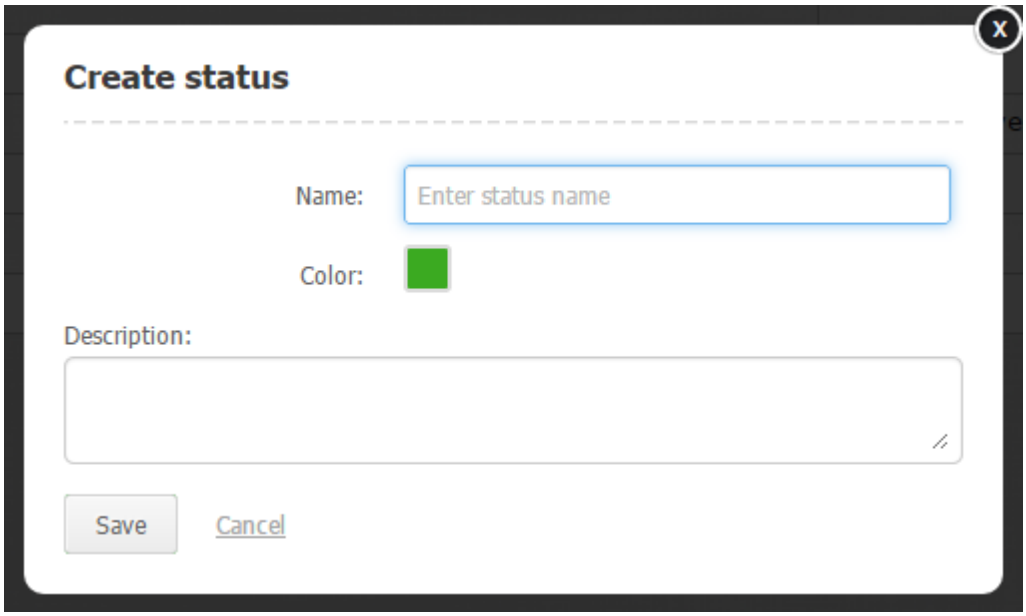
5.7.3 Managing Statuses

Purpose:

Create a status.

Solution:

1. Go to the **Lists** section, **Statuses** tab.
2. Click **Add** on the toolbar.



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

Additional information:

Editing and deleting of the status is performed by standard means:

- Editing the Element;
- Deleting the Element.

5.7.4 Managing Perimeters

Warning!

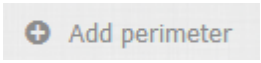
By default the System has a company perimeter (perimeter name may vary). To apply actions from preset policies to interception objects you should add elements to this perimeter (see *Purpose 2* in this topic).

Purpose:

1. To create a perimeter.
2. To add an element to the perimeter.

Solution:

1. Creating a perimeter.

    1. Go to the **Lists** section, **Perimeters** tab.
    2. In the left part of a workspace click 

Add perimeter.
    3. Type a name of a new perimeter to **Enter perimeter name** field.
    4. Click  in the right corner of **Enter perimeter name** field.

2. Adding an element to the perimeter.

    1. Go to the **Lists** section, **Perimeters** tab.
    2. On the left side of a workspace left-click the target perimeter from the perimeters list.
    3. On the right side of a workspace click 

Add element to the perimeter and select element type from the drop-down list.
    4. In the appeared field specify one or several elements by one of following methods:
        - for *Person*, *Workstation*, *Website topic*:
            - start typing element name (or a contact for *Person* element) into the field and select required entry from the drop-down list
            - click **Add** in the right of the field; in the opened dialog box flag the field near target element and click **Save**.
        - for *Group*:
            - start to type group name to the field and select needed entry from the drop-down list
            - click **Add** in the right of the field; in the opened dialog box left-click the target group and click **Save**.
        - for *E-mail*, *Web resource*, Phone, *Skype*, *ICQ*, *IP address*, *DNS*, *Domain* - type a name (for example for *Web resource*) or value (for example for *IP address*) into the field and press **Enter** keyboard key.

Additional information:

- Deleting of the perimeter is performed by standard means (see "Deleting the Element") but instead of **Delete** button located on the toolbar, the  **Delete** button appearing when navigating the mouse cursor over the field with the target perimeter name is used.
- Editing of the perimeter is performed by standard means (see "Editing the Element") but instead of  **Edit** button located on the toolbar, the  **Edit** button appearing when navigating the mouse cursor over the field with the target perimeter name is used.

5.8 Interface Customization

Why the interface customization is needed?

To configure System interface for more convenient user work.

Includes the following actions:

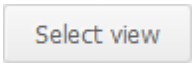
Action	Description
Selecting Dashboard Layout	Dividing the dashboard into parts convenient for the user
Selecting Event Displaying Style	Changing the style of displaying information on interception objects
Workspace Partitioning	Dividing the workspace into two parts in proportions convenient for user
Moving Widget Tiles	Changing widgets locations on the dashboard for convenient viewing

5.8.1 Selecting Dashboard Layout

Purpose:

To divide the working area of the **Dashboard** section into parts convenient for the user.

Solution:

1. Go to **Dashboard** section.
2. Click 

Select view.
3. Left-click to select convenient proportions of the workspace (see the description of panels layout variants below).
4. Click **Save**.

Additional information:

Working area layouts are represented in the table:

Panels layout	Icon
Splits into 3 equal parts	
Splits in ratio of 2:1	
Splits into 2 equal parts	
Splits in ratio of 1:2	

5.8.2 Selecting Event Displaying Style

Purpose:

To select the style of displaying the interception events.

Solution:

1. Go to **Events** section.
2. Apply events filtering (see "Managing Dashboards").
3. Click:
   -  - to select displaying the events as blocks;
   -  - to select displaying the events as a table.

5.8.3 Workspace Partitioning

The workspace cannot be divided in the following Management Console sections:

- **Dashboard** section - not required because of the dashboard interface (see. "Selecting Dashboard Layout ").
- **Lists** section - not required because of logical reasons.

Purpose:

Split the workspace section into two parts in the proportions convenient for the user.

Solution:

1. Go to the target section.
2. In the workspace point over the dividing vertical line so that the cursor becomes two-directions-arrow (depending on your operating system this icon may look different).
3. Press and hold the left mouse button.
4. Move the cursor to move the vertical line over the workspace to set needed proportions.
5. Release the left mouse button.

5.8.4 Moving Widget Tiles

Purpose:

Move the tiles to display them in a user-friendly order.

Solution:

1. Go to the **Dashboard** section.
2. Point over the title of the tile so that the cursor becomes four-directions-arrow (depending on your operating

system this icon may look different).

3. Press and hold the left mouse button.
4. Move the mouse pointer to move the tiles over the workspace unless the target tile position indicates a dotted line.
5. Release the left mouse button.

6 Licensing Information

Summary of the section:

- 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.

Licence Agreement

This End-User Licence Agreement ("Agreement") is a joinder agreement between ZAO 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.

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 ZAO "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 ZAO "InfoWatch".

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.

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.

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.

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. 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.

7. Open (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.

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.

9. **Rightholder Contact Information**

ZAO "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 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.