

INFOWATCH

# InfoWatch Traffic Monitor

## User Guide

09/17/2026

© JSC “InfoWatch”

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

http://www.infowatch.com

# TABLE OF CONTENTS


1 InfoWatch Traffic Monitor Overview ..... 9
1.1 Objects Interception ..... 10
1.2 Object Analysis and Verdict ..... 12
1.3 User Decision on an Object ..... 15
1.4 InfoWatch Traffic Monitor Transport Modes ..... 15
1.5 Uploading Object to Database ..... 16
1.6 Specific Features of Blocking HTTP-queries and Messages Sent through Web Services ..... 16
2 Traffic Monitor Management Console: General Information ..... 18
2.1 System Operation Before Configuring ..... 19
2.2 Configuring the System ..... 19
2.3 Displaying Actual Data in Management Console ..... 21
3 Interface of Traffic Monitor Management Console ..... 23
3.1 Dashboard Section ..... 25
3.1.1 Dashboard Widgets ..... 26
Dynamics of Violations over the Period ..... 27
Top Violators ..... 28
Quantity of Violations over Period ..... 29
Selection ..... 30
Dynamics of Statuses ..... 30
Policy Statistics ..... 31
Statistics on Protected Objects ..... 31
Statistics on Catalogues of Protected Objects ..... 32
3.1.2 Dashboard Report ..... 33
3.2 Events Section ..... 35
3.2.1 Queries ..... 36
Standard Mode of Creating Queries ..... 38
Advanced Mode ..... 48
Search on the Event Text ..... 48
3.2.2 Object Interception ..... 50
Event Tile ..... 53
Table view of Events ..... 54
List of Attachments ..... 55
Brief Event Viewing Form ..... 56
Detailed Event Viewing Form ..... 58

3.2.3 Contact Identification in Event ... 61
3.3 Reports Section ... 62
3.3.1 Report Creation Form ... 63
3.3.2 Widgets of Reports ... 64
3.3.3 Queries ... 67
3.4 Technologies Section ... 68
3.4.1 Categories and Terms ... 70
Categories ... 71
Terms ... 72
3.4.2 Text Objects ... 73
Text Object Patterns ... 74
3.4.3 Sample Documents ... 76
Automatic sample documents ... 78
3.4.4 Blanks ... 78
3.4.5 Stamps ... 79
3.4.6 Database Unloadings ... 80
Detection Conditions for Unloading ... 82
Automatically Updated Database Unloadings ... 89
3.4.7 Graphical Objects ... 90
3.4.8 Autolinguist ... 91
3.5 Protected Objects Section ... 92
3.5.1 Elements of Technologies ... 94
3.5.2 Detection Conditions ... 94
3.6 Persons Section ... 98
3.6.1 Persons ... 99
3.6.2 Computers ... 101
3.6.3 Screenshots ... 102
3.7 Policies Section ... 102
3.7.1 Rules and their Viewing Form ... 104
Rule of Transfer ... 106
Rule of Copying ... 107
Rule of Placement ... 109
Application activity rule ... 110
Person Control Rule ... 112
File Operations Rule ... 112
3.8 Lists Section ... 113
3.8.1 Tags ... 114
3.8.2 Web Resources ... 114
3.8.3 Statuses ... 115
3.8.4 Perimeters ... 116
3.8.5 File Types ... 117

3.9 Administration Section ..... 127

4 Cases Solving in Traffic Monitor Management Console ..... 128

4.1 Typical Actions ..... 128
4.1.1 Login to the Management Console ..... 128
4.1.2 Applying System Configuration ..... 129
4.1.3 Editing Element ..... 130
4.1.4 Deleting Element ..... 131
4.1.5 Page Navigation ..... 131
4.1.6 Changing User Password ..... 132
4.1.7 Selecting Interface Language ..... 132
4.1.8 Calling Help File ..... 132
4.1.9 Viewing Information on System ..... 133

4.2 Managing Persons and Computers ..... 133
4.2.1 Creating Group of Persons or Computers ..... 134
4.2.2 Creating Persons and Computers ..... 135
4.2.3 Exporting and Importing Persons ..... 136
Features of exporting and importing the organizational structure ..... 137
4.2.4 Configuring Person's Card ..... 138
Adding Contact to Person ..... 139
Adding Computer to Person ..... 140
Adding Person to Group ..... 140
4.2.5 Configuring Computer Cards ..... 141
Adding Contacts to Computers ..... 141
Adding Persons to Computers ..... 141
Adding Computers to Groups ..... 142
4.2.6 Setting Statuses to Persons and Computers ..... 142
4.2.7 Viewing Screenshots ..... 143
4.2.8 Viewing Events Involving Person's Contact ..... 145

4.3 Managing Catalogues ..... 146
4.3.1 Managing Tags ..... 146
4.3.2 Managing Web Resources ..... 147
4.3.3 Managing Statuses ..... 149
4.3.4 Managing Perimeters ..... 150

4.4 Managing Base of Technologies ..... 156
4.4.1 Defining the Confidential Information ..... 156
Managing Categories and Terms ..... 157
Managing Text Objects ..... 160
Managing Sample Documents ..... 163
Managing Blanks ..... 165
Managing Stamps ..... 169
Managing DB Unloadings ..... 170

Managing Graphical Objects ... 172
Managing Autolinguist ... 174
4.4.2 Exporting and Importing the Base of Technologies ... 176
4.5 Managing Protected Objects ... 178
4.5.1 Creating a Catalogue of Protected Objects ... 178
4.5.2 Creating a Protected Object ... 179
4.5.3 Adding Elements of Technologies ... 185
4.5.4 Adding Detection Conditions ... 186
4.5.5 Creating Policies for Protected Objects and Their Catalogues ... 187
4.5.6 Importing and Exporting Protected Objects ... 188
4.5.7 Activating and Deactivating Protected Objects ... 190
4.6 Managing Interception Objects ... 191
4.6.1 Viewing Summary on Violations/Violators ... 191
Creating Dashboard ... 193
Creating and Configuring Widget ... 193
Creating Dashboard Report ... 195
Viewing Dashboard Report ... 196
4.6.2 Viewing Events ... 197
Creating Queries ... 197
Choosing Event Fields of View ... 210
Viewing Brief Event Form ... 211
Viewing Detailed Event Form ... 212
4.6.3 Making Decision on Object ... 213
4.6.4 Adding and Deleting Tags ... 214
4.6.5 Saving Events (for SMTP mail) ... 214
4.6.6 Event Export ... 214
4.6.7 Dispatching a Quarantined Event ... 217
4.7 Configuring System Response ... 218
4.7.1 General Information on Policies ... 219
4.7.2 Preset Policies ... 226
Data Protection Policy ... 227
Person Control Policy ... 228
Policy that Regulates Transferring Password-Protected Data ... 229
Policies that Regulate Visiting Web Resources ... 229
Policy that Excludes Mailing Lists from Interception ... 234
Competitors Control Policy ... 235
Clipboard Control Pollicy ... 235
4.7.3 Creating Data Protection Policy ... 236
Examples of Using Data Protection Policy ... 237
4.7.4 Creating Data Protection Policy on Agents ... 240
4.7.5 Creating Person Control Policy ... 244
4.7.6 Creating Rules ... 245

4.7.7 Determining System Response to Policy Violations ... 248
4.7.8 Configuring Notifications in Rules ... 250
4.7.9 Determining System Default Response ... 251
4.7.10 Filtering the List of Policies ... 252
4.7.11 On Data Protection Policy on Agents ... 253
4.7.12 On Data Protection Policy ... 254
4.7.13 On Person Control Policy ... 254
4.7.14 Exporting and Importing policies ... 255
Exporting policies ... 255
Importing policies ... 255
Features of exporting and importing policies ... 256
4.8 Managing Reports ... 258
4.8.1 Creating and Viewing Reports ... 259
Creating Folder with Reports ... 261
Creating Report ... 262
Creating and Configuring Widget ... 263
Viewing Ready Reports ... 265
4.8.2 Examples of Using Reports ... 266
4.9 Managing the System ... 271
4.9.1 Managing Integration with LDAP Catalogues ... 272
Creating Connection to Server ... 272
Editing Connection to Server ... 277
Deleting Connection to Server ... 277
Running Synchronization with Server Manually ... 277
4.9.2 Managing System Users and their Roles ... 278
Users ... 278
Roles ... 281
Visibility Scopes ... 284
4.9.3 Managing Licenses ... 289
Checking License Validity ... 290
Installing a License ... 291
Deleting License ... 291
Requesting License ... 291
Viewing License Usage Statistics ... 291
4.9.4 Healthcheck ... 292
Configure Notifications ... 293
4.9.5 Collecting Diagnostic Data ... 294
4.9.6 User Actions Audit ... 295
Audit Events ... 296
Filtering and search ... 297
4.9.7 Integrity Monitoring ... 298
Manual Integrity Monitoring ... 298

Automatic Integrity Monitoring ..... 298
Accepting Result as Standard ..... 298
4.9.8 Plugins ..... 298
Default Plugins ..... 299
Custom Plugins ..... 299
Work with Plugins in Traffic Monitor ..... 299
Plugin Types ..... 300
Adding Plugin ..... 302
Deleting Plugin ..... 303
Working with Tokens ..... 303
4.9.9 Configuring Connection to Mail Server ..... 304
4.9.10 Configuring Notifications ..... 305
Creating Notification ..... 306
Testing Notification ..... 308
Preset Notifications ..... 308
4.9.11 Managing Tablespaces ..... 309
5 END-USER LICENSE AGREEMENT ..... 311
6 Glossary ..... 316

# 1 InfoWatch Traffic Monitor Overview

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

Main functions of InfoWatch Traffic Monitor are listed below.

> **Note:**
>
> The set of supported functions depends on the operating system installed on the server (for more details please see the Knowledge Base article *Traffic Monitor and Device Monitor Functionality Differences According to OS Used*).

**InfoWatch Traffic Monitor Main Features:**

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

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

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

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

**InfoWatch Traffic Monitor Components:**

| InfoWatch Traffic Monitor Component | Purpose |
|---|---|
| Traffic Monitor Server | Interceptors: **IW_SNIFFER**, **IW_ICAP,** and **IW_SMTPD**.**Analysis subsystem** receives event context and checks if the events contain technology elements and correspond to protected objects. |

| InfoWatch Traffic Monitor Component | Purpose |
|---|---|
| | **Policy applying subsystem** implements actions defined by the user according to the corporate security policy. |
| Database | Storage of information associated with the System operations (intercepted data and results of their analysis). |
| Device Monitor | Interaction with workstations. Controlling user access to the peripherals, monitoring operations (data copying from/to removable storages and FTP, sending data to printing, using messengers) and intercepting the traffic from instant messengers. |
| Connectors | Integration with external systems, generating events. |
| Web Management Console | Configuring rules for analyzing and filtering traffic, analysis of intercepted data. |

**Participants**

All participants in the System are divided into two types:

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

**Functionality**

The System functionality allows you to control the two areas:

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

To control these areas, interceptors are used.

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

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

## 1.1 Objects Interception

The System objects are the following:

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

**Warning!**

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

- *InfoWatch Traffic Monitor. Administration Guide. In Stream/At The Gateway Traffic Interception*.

It is also recommended to see the article *Traffic Monitor and Device Monitor Functionality Differences According to OS Used*.

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

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

| Object type | Object interception options |
|---|---|
| FTP | The System receives a copy of traffic from InfoWatch Device Monitor |
| Messages from messengers | The System receives a copy of Skype (including voice messages), Telegram, Facebook, WhatsApp (desktop version), VK traffic from InfoWatch Device Monitor. |
| MS Lync | The System receives a copy of traffic from IW Lync Adapter installed on MS Lync server |
| Shadow copies of files and print jobs received from InfoWatch Device Monitor | The System receives a copy of traffic. Blocking user actions (print jobs, access to devices) can be performed only by means of InfoWatch Device Monitor |

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

## 1.2 Object Analysis and Verdict

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

| Traffic Monitor subsystem | Subsystem modules | Subsystem/module features |
|---|---|---|
| Processing subsystem | • SMTP and POP3 Processing module (copy mode)<br>• HTTP Processing module (copy mode)<br>• ICQ Processing module (copy mode)<br>• Shadow Copies Processing module<br>• SMTP Processing module (blocking mode)<br>• HTTP Processing module (blocking mode) | • Extracting significant data and attachments from the object<br>• Defining the attachments format<br>• Extracting text data, including attachments, from EML files<br>• Forwarding the extracted texts to the Analysis subsystem |
| Analysis subsystem | Linguistic Analysis module | Checking if the object text corresponds to any categories |
| | Text Objects Detecting module | Searching through the object text for specific text objects (e.g. credit card numbers) |
| | Digital Prints Detecting module | Searching through the object text for quotes from sample documents |

| Traffic Monitor subsystem | Subsystem modules | Subsystem/module features |
|---|---|---|
| | Blanks Detecting module | Searching through the object text for completed forms |
| | Stamps Detecting module | Searching through the object text for stamp images |
| | Database Unloadings Detecting module | Searching through the object text for quotes from a database.<br>Recipient validation when sending personal data by email |
| | Graphic Objects Detecting module | Searching through the object text and attachments for images of particular classes |
| | Autolinguist module | Checking if the text object corresponds to a category using a classifier which learned on standard documents. |
| Policies Application subsystem | Integration Module for Directory Service: Active Directory, Samba DC, Domino Directory, Astra Linux Directory, Astra Linux Directory Pro or FreeIPA | Providing the initial import and periodical synchronization of Directory Service structure with a list of users and workstations in Traffic Monitor for further binding this information with data from the intercepted objects. |
| | Decision-Making module | Ensuring corporate security policies by employing policy rules to the intercepted objects |

**The object analysis is performed in the following order:**

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

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

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

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

Based on the results of the analysis, the Decision-Making module makes a conclusion on a possible violation of the security policy and determines which actions should be performed in case of violation. Rules, which

determine the System actions in case of violation, are set in a policy. The actions can be as follows (the set of possible actions is defined by the rule type):

- **Assign violation level to event**. Possible values: *High*, *Medium*, *Low*, *No*.
- **Assign status to persons**. A status that will be assigned to violators (for details, see *Statuses*).
- **Assign tags to event**. Tags that will be assigned to the event in the policy is violated (for details, see *Tags*).
- **Assign verdict to event**. The System decision whether the event is a potential violation. Possible values: *Allow*, *Block*, *Quarantine*.
- **Delete event**. The event will not be saved to the database.

> **Note:**
>
> For details on file formats, for which Traffic Monitor supports detection and extraction, see *File Types* article.

## 1.3 User Decision on an Object

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

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

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

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

## 1.4 InfoWatch Traffic Monitor Transport Modes

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

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

**Table 1**

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

**Table 2**

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

## 1.5 Uploading Object to Database

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

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

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

If the *Blocking* transport mode (see *InfoWatch Traffic Monitor Transport Modes*), the System decides to block an HTTP-request or a message sent via a web service (for example, *mail.ru*), then the browser of the user who sent a request or a letter will display the blocking message.

If sending mail is performed through mail services built on AJAX technology (such as Gmail, Windows Live Hotmail, etc.), then the user may not receive a message saying that the letter delivery is locked. As a rule, a message sent by the mail service is displayed in this case.
Post requests to a number of Web resources (see table below), are processed by the System in accordance with specific rules:

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

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

Supported Web resources:

| **Type of Web resource** | **Resources** | |
|---|---|---|
| | **Without restrictions** | **With restrictions** |
| Web mail | mail.ru, mail.yandex.ru, rambler.ru, pochta.ru, km.ru, newmail.ru, inbox.com, hotmail.com, hotmail.ru, live.com | gmail.com, yahoo.com, mail.com, aol.com, gmx.com |
| Blogs and social networks | blogs.mail.ru, liveinternet.ru (li.ru), my.ya.ru, diary.ru, blogspot.com (blogger.com), loveplanet.ru/a-journal, myspace.com, perfspot.com | facebook.com, myspace.com, blogger.com, vkontakte.ru (vk.com), odnoklassniki.ru, twitter.com, livejournal.com (.ru), wordpress.com, linkedin.com |
| Job search and CV posting sites | | moikrug.ru, hh.ru, job.ru, rabota.ru, jobs.com, eurojobs.com |
| Forums | forum.ru-board.com, sysadmins.ru, talk.mail.ru, dom.bankir.ru, biznet.ru | forum.ixbt.com, groups.google.ru (.com) |

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

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

# 2 Traffic Monitor Management Console: General Information

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

During the login process, the following conditions are checked:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**Warning!**

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

## 2.1 System Operation Before Configuring

The installed System which has not yet been configured (on the System configuring, see *Cases Solving in Traffic Monitor Management Console*) operates in the following way:

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

  **Warning**

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

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

## 2.2 Configuring the System

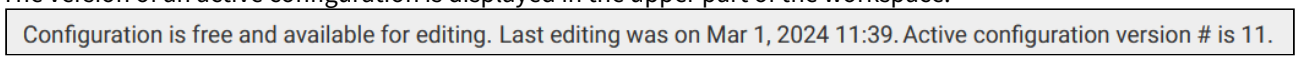
The System configuration includes settings required for checking objects on Traffic Monitor Server as well as for data monitoring and analysis.

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

**Warning!**

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

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




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

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

**The configuration process includes:**

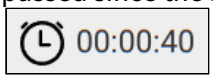
- Creating the base of technologies (see *Managing the Base of Technologies*):
  - Selecting terms to be detected – only when using **Linguistic Analysis technology** (see *Terms*);
  - Selecting text object types to be detected – only when using **Detecting Text Objects technology** (see *Text objects*);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

> **Note:**
>
> A configuration that is sent to Device Monitor includes only the following elements:
>
> - Persons and computers
> - Perimeters
> - Data protection policies on agents

- Categories and text objects
- Protected objects that contain only categories and text objects

If you change any of the configuration settings, message about editing will be displayed to each user in the System. Users with the privilege to reset other user's unsaved configurations can cancel the configuration. Other users are enabled to change the configuration only after the edited version has been saved. See *Displaying Actual Data in Management Console* for details.

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

- **Apply configuration** (see *Applying System Configuration*) – the updated configuration becomes active on the server.
  Applying the new configuration may take some time. The duration of application does not exceed 3 hours. At the top of the workspace, a counter is displayed. The counter displays the time that has passed since the start of the configuration application process:
  
  
  You can edit a configuration and apply it even if another configuration is being applied. In this case, the application of the configuration will be interrupted and the application of the edited configuration will start.
- **Save configuration** – the updated configuration becomes accessible for other Console users but it will not be used in the System for traffic control and data analysis.
- **Reset changes** – the configuration that was last applied on the server will be used in the Console and all changes will be discarded.

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

**Note:**

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

## 2.3 Displaying Actual Data in Management Console

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

*Reset another user's configuration* privilege enables you to reset configuration that is being edited by another user before it has been saved. Once the configuration has been saved, each user regardless of the privilege can reset another user's configuration before it has been applied. For details on assigning privileges, see *Creating a Role* and *Editing a Role*.

**Example:**

The following users are registered with the System:

- *Main security officer* holding *Administrator* role with *Reset another user's configuration* privilege assigned;
- *Security officer #2* and *Security officer #3* holding *Security officer* role without the privilege.

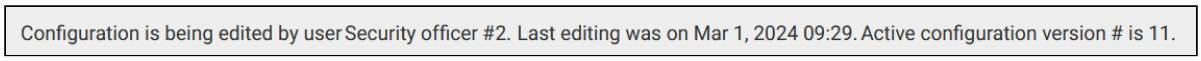
*Security officer #2* is editing a data protection policy on *Policies* tab. The configuration is not saved yet. The area under the Navigation panel contains the following message with buttons:




*Main security officer*'s Management Console is displaying the message with **Reset** button:




At the same time, resetting is unavailable for *Security officer #3*:




Once *Security officer #2* has saved the changes, *Security officer #3* also can reset the configuration if it has not been applied yet.

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

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

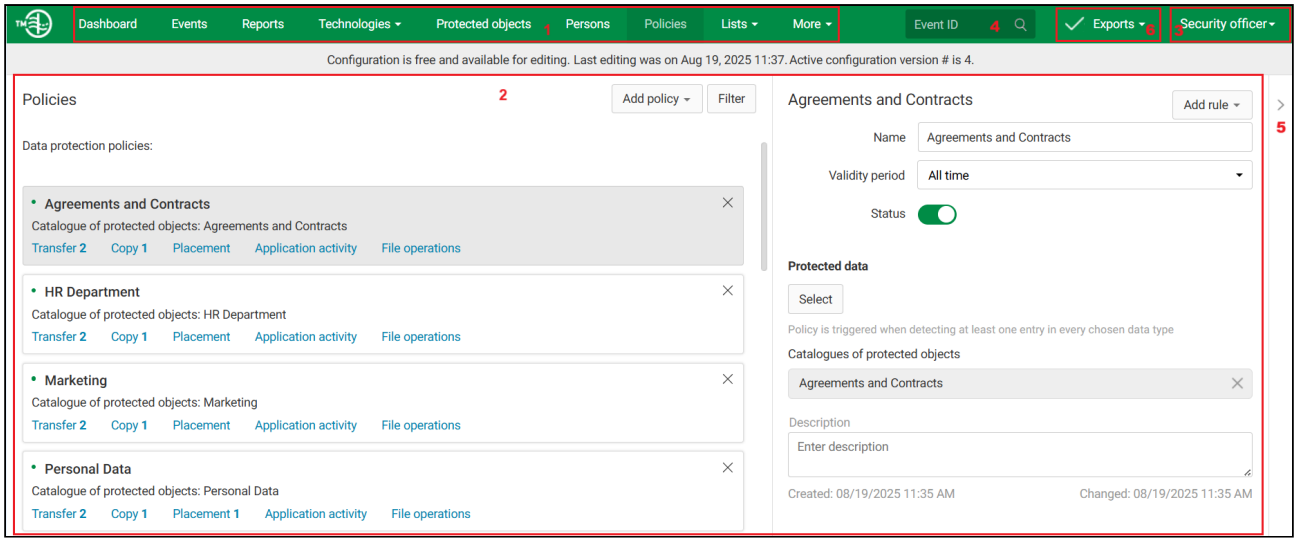
You can also update data manually in any section of the Management Console. To do this, use the standard browser refresh tool: by default the page is refreshed when you press the function key F5.

**Note:**

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

# 3 Interface of Traffic Monitor Management Console

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




Window elements of the Management Console:

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

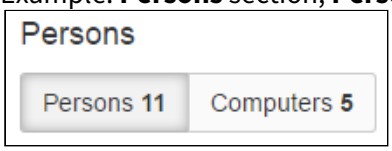
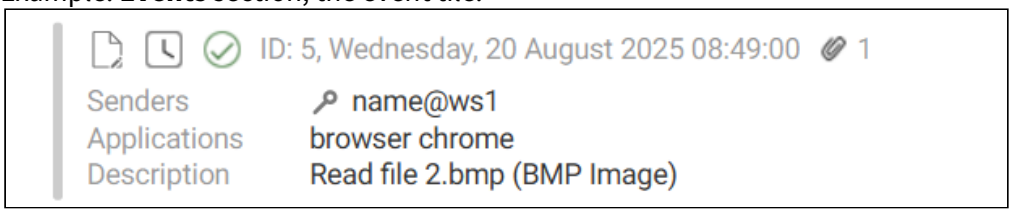
| | | |
|---|---|---|
| | | you will be redirected to the "Events" section where the search results are displayed. |
| 5 | Panel hiding button | Is displayed in sections where workspace is divided into panels (for example, the list of events is located on the panel on the left side of the workspace and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

You can work in the Management Console in the sections:

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

You can go to a specific section by clicking the section button. For example, **Events** section button: 

The following interface elements are used in the Management Console:

- **Tab** – allows switching between sets of interface elements within the same window.
  Example: **Persons** section, **Persons** and **Computers** tabs:
  
  
- **Panel** – interface area that displays a set of data or contains a set of interface elements. It is separate from other areas.
  Example: toolbar:
  
- **A part of the working area** – working area fragment, separated from other fragments by a vertical line.
- **Tile** – the entire data set for one entry (all object attributes) as a separate object.
  Example: **Events** section, the event tile:
  
  

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

**Note:**

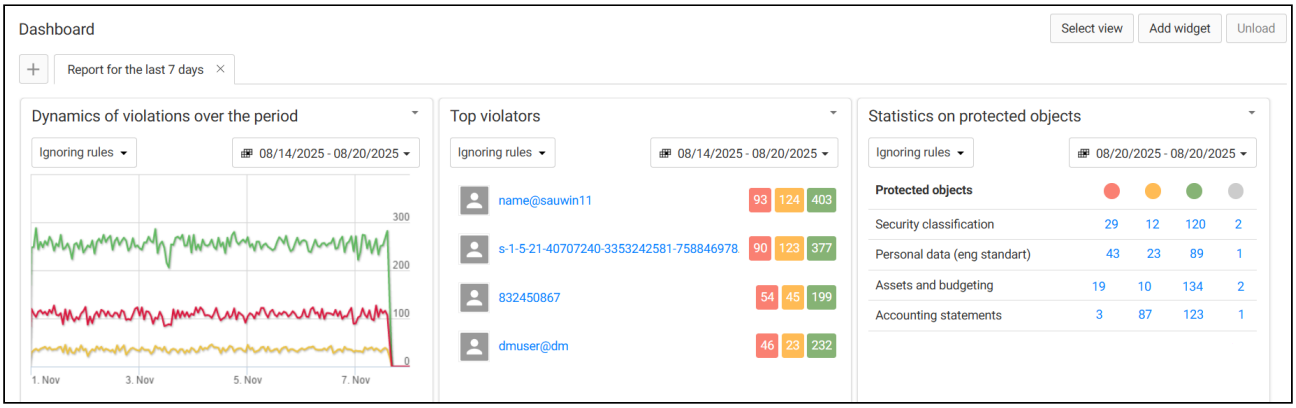
While downloading the requested data, the System may display the icon or an informational message.

## 3.1 Dashboard Section

**About the section:**

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

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




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

 – splitting into 3 equal parts;

 – splitting in a ratio of 2:1;

 – splitting into 2 equal parts;

 – splitting in a ratio of 1:2.

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

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

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

**User's actions:**

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

## 3.1.1 Dashboard Widgets

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

Widgets contain statistical information on violations/violators. The appearance and parameters of widgets are defined by their type.

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

| Widget | Description |
|---|---|
| Dynamics of violations over the period | Quantitative changes of chosen violation types over the selected period |

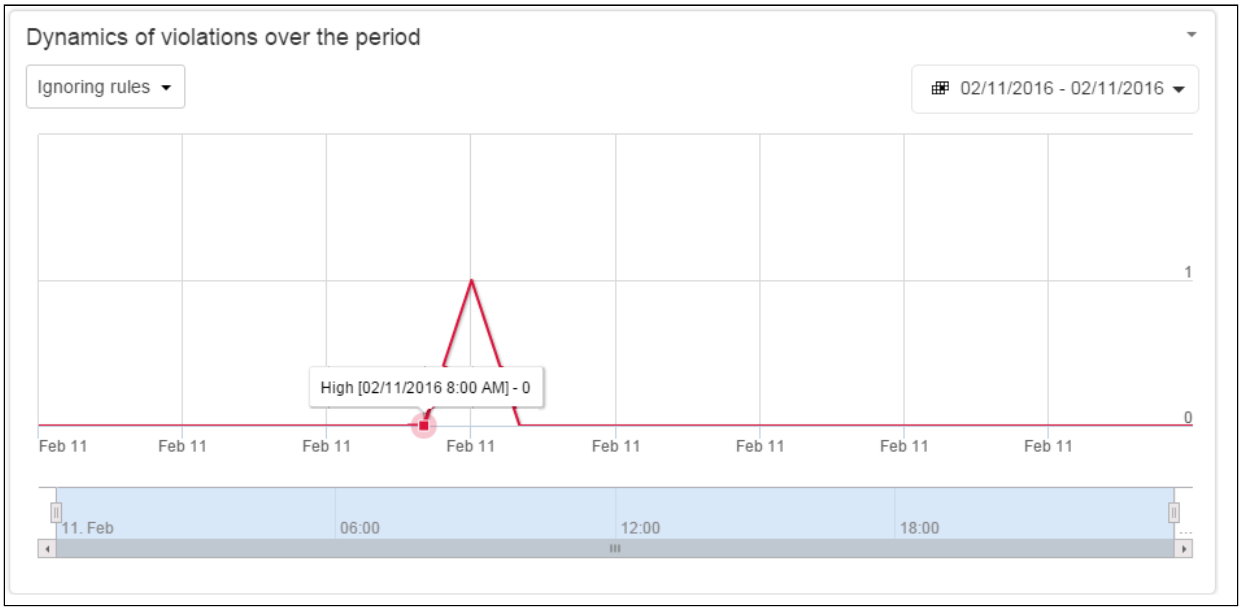
| Widget | Description |
|---|---|
| Top violators | A list of the most active violators of a chosen group for the selected time period |
| Quantity of threats over period | Number of violations of high, medium, and low level for each violation type (transferring, placement, copying) over selected period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

**User's actions:**

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

### Dynamics of Violations over the Period

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




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

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

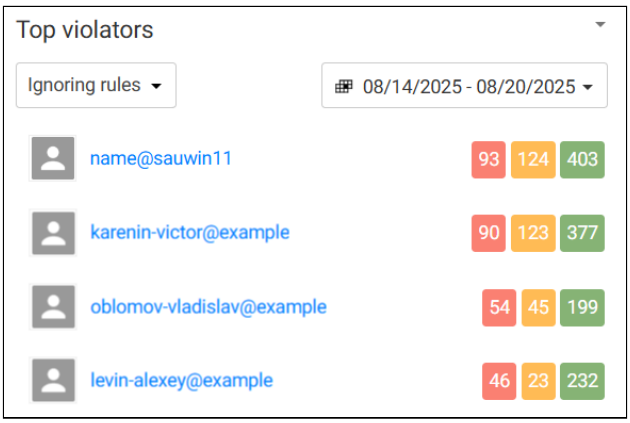
In the left upper corner of the widget, select the type of rules, violations of which will be displayed in the widget. Possible values: *Transfer rules*, *Copy rules*, *Placement rules*, *Ignoring rules*.

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

## Top Violators

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

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




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

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

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

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

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

You can edit the following parameters:

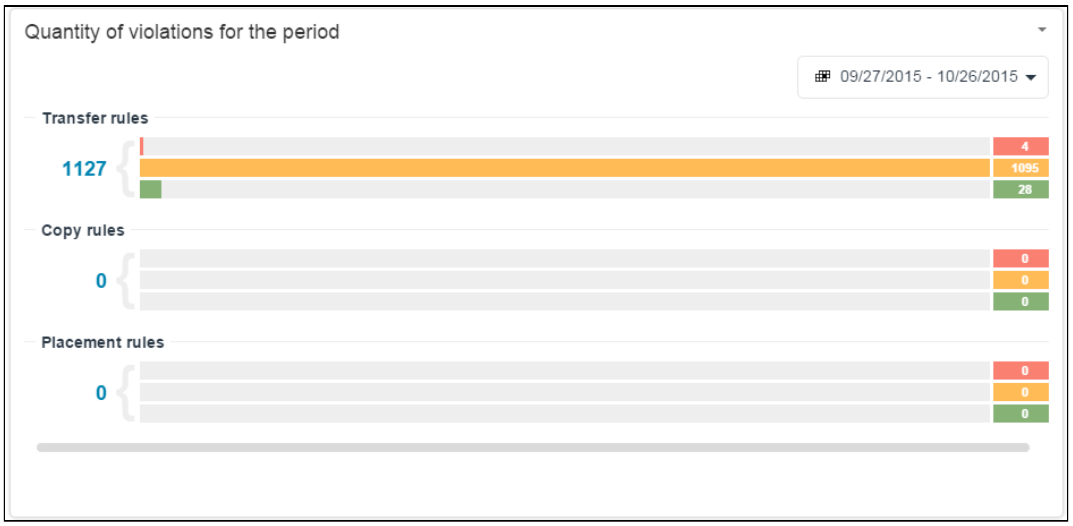
- **Name**;
- **Update interval** for data on the widget;
- **Quantity of violators** for which statistics will be displayed;
- **Groups** to which violation can belong. Statistics on the selected groups will be displayed in the widget. Start typing the group name or click  and select desired groups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

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

## Quantity of Violations over Period

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

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




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

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

You can edit the following parameters:

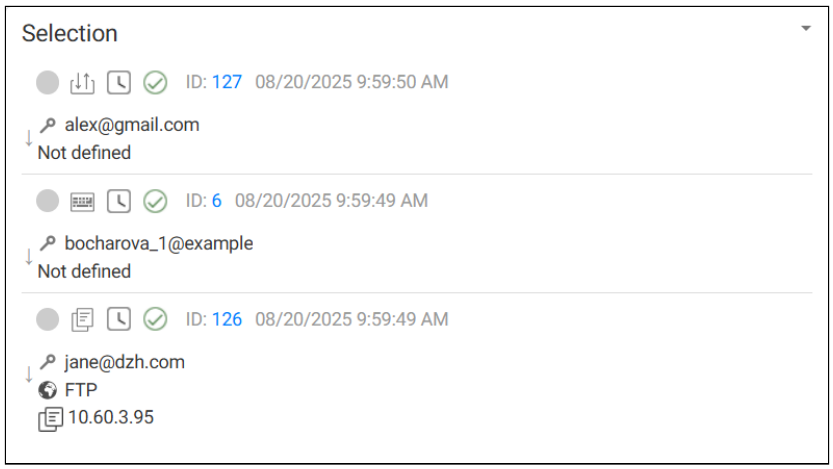
- **Name**;
- **Update interval**;

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

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

## Selection

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




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

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

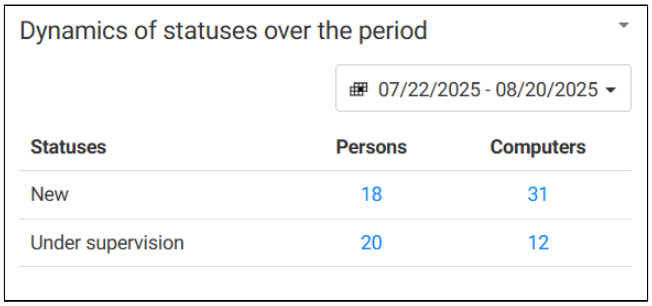
You can edit the following parameters:

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

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

## Dynamics of Statuses

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




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

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

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

## Policy Statistics

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




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

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

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

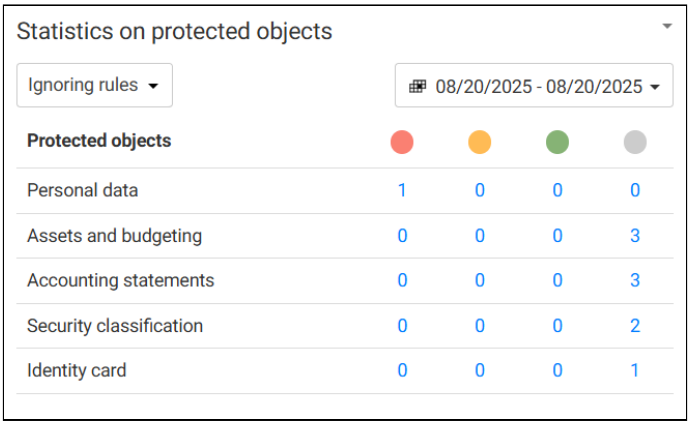
You can edit the following parameters:

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

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

## Statistics on Protected Objects

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




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

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

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

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

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

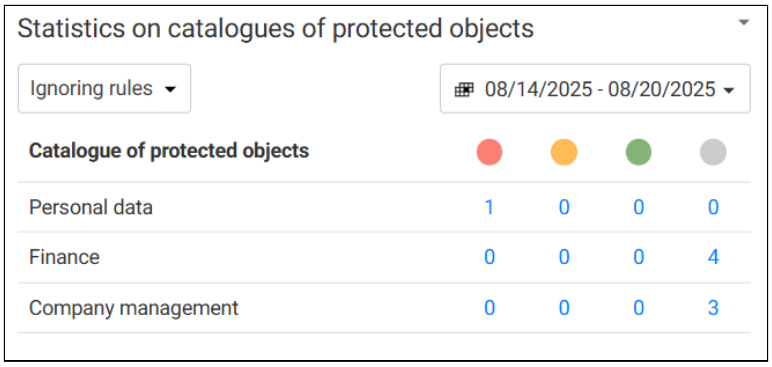
You can edit the following parameters:

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

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

## Statistics on Catalogues of Protected Objects

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



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

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

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

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

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

You can edit the following parameters:

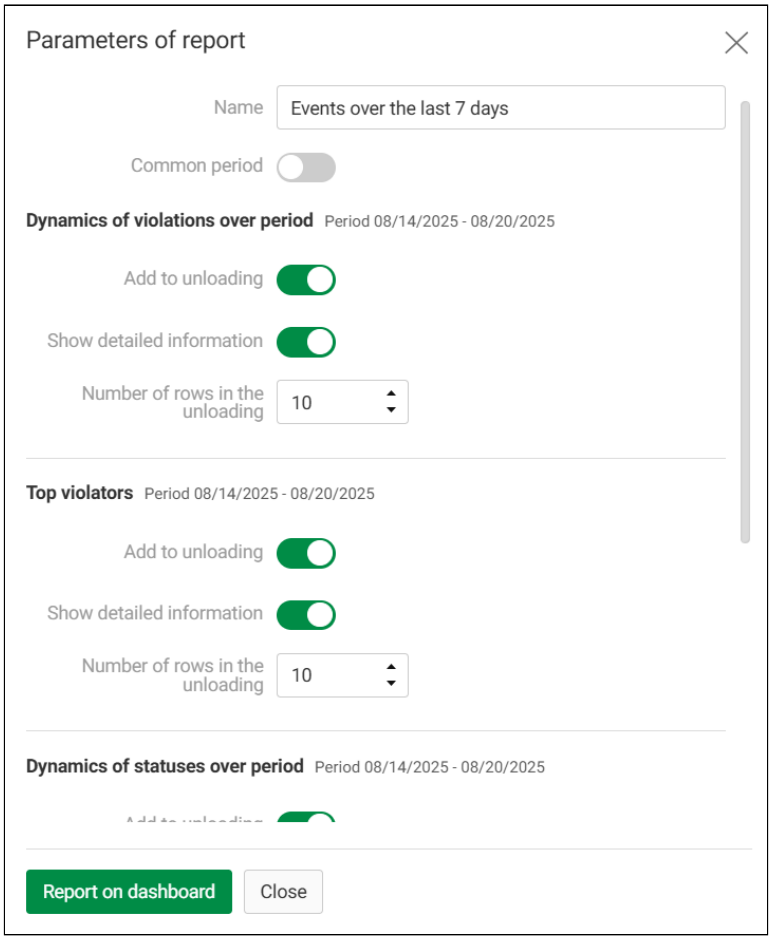
- **Name**;
- **Update interval** for data on the widget;
- **Catalog of protected objects** - a catalog of protected objects, statistics for which will be displayed. Start typing the catalog name or click  and select desired catalogs from the list.

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

## 3.1.2 Dashboard Report

The dashboard report allows you to display statistics on intercepted objects. The dashboard report can be in PDF or HTML format. You can also print it out on your printer.

> **Примечание:**
>
> Dashboard report is not available in Traffic Monitor installed on Red Hat Enterprise Linux 8, Oracle Linux 8, AlmaLinux 8 or Rocky Linux 8.




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

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

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

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

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

**User's actions:**

- Creating a dashboard report (see *Creating Dashboard Report*).

## 3.2 Events Section

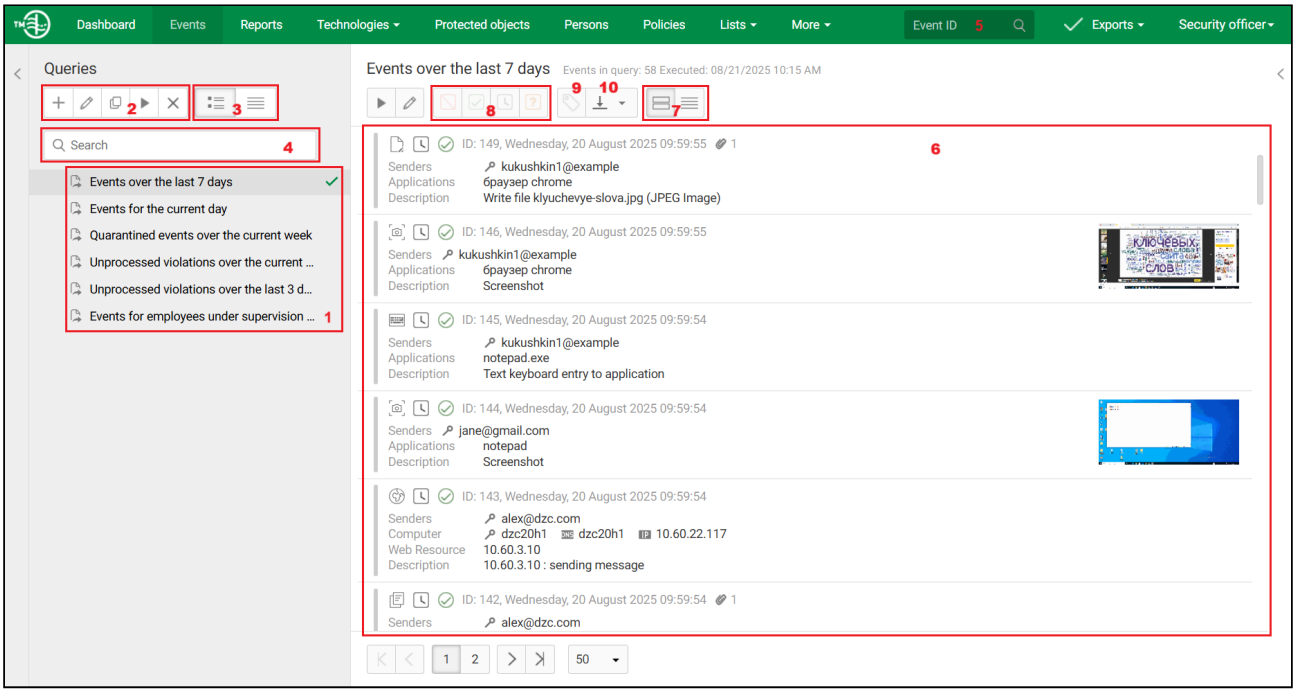
**Reference information:**
The event is the interception object of network traffic.

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

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

**About the section:**

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




The query list is located in the left part of the workspace (№ 1 in the screenshot). You can create a query either in the root or in a folder. For operations with queries and their folders, you can use buttons on the toolbar (№ 2 in the screenshot).

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

-  – as folders;
-  – as a flat list.

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

To search for events, choose a query in the list (№ 1 in the screenshot) or create a new query by clicking  on the toolbar (№ 2 in the screenshot).

You can also use the search field to find a folder or a query by its name (№ 4 in the screenshot).

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

If you already know the event ID, you can use the **Search event by ID** field (№ 5 in the screenshot).

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

As a result of executing a query or searching events by IDs, a list of found events is displayed (№ 6 in the screenshot).

You can choose how to display events (№ 7 in the screenshot):

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

If you perform *search for analogues* of an attachment in an event, then the results will be displayed as the *list of attachments*.

In the right part of the workspace, a *brief event viewing form* is displayed. To switch to a *detailed event viewing form*, click the **Detailed information** button.

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

- make a decision on the event (select the required verdict using buttons on the toolbar – № 8 in the screenshot)
- assign a tag to the event (№ 9 in the screenshot)
- export the event or save debug information on the event (№ 10 in the screenshot)

**User's actions:**

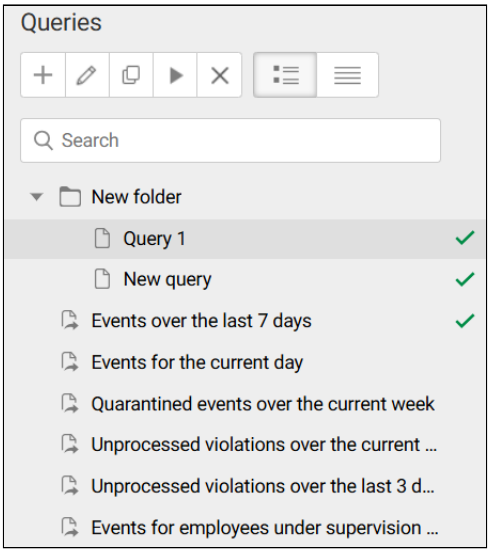
- Filtering events (see *Creating Queries*);
- Viewing event details (see *Viewing Brief Event Form* and *Viewing Detailed Event Form*);
- Making decision on the event (see *Making Decision on Object*);
- Adding/removing tags (see *Adding and Deleting Tags*);
- Saving the event (see *Saving Events (for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

### 3.2.1 Queries

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

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

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




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

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

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

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

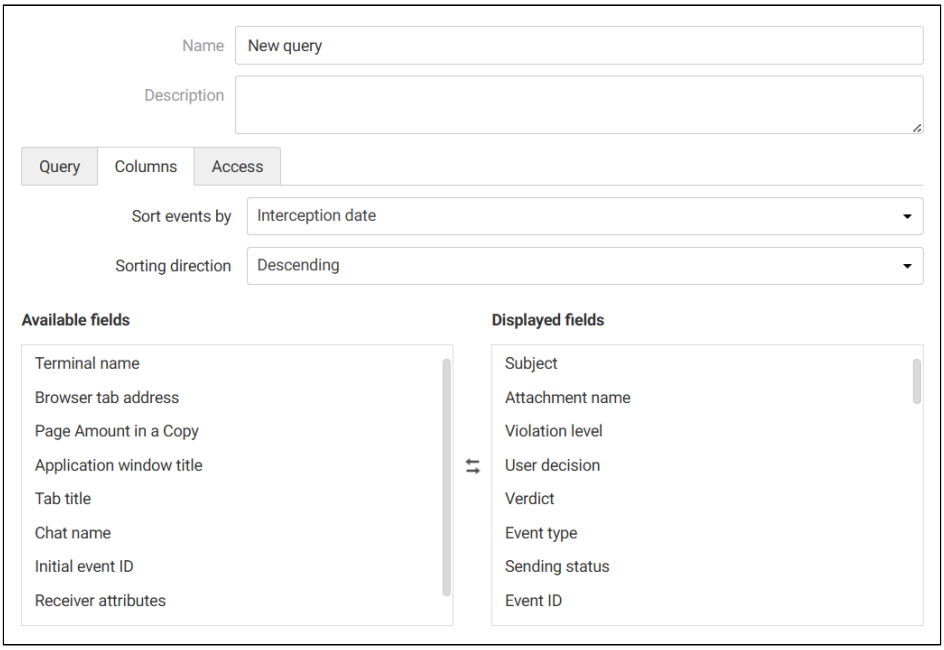
If the query is being executed at the moment, the icon is displayed next to its name . For queries whose execution failed, the icon is displayed .

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

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

The query creation form contains the following tabs:

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




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

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

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

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

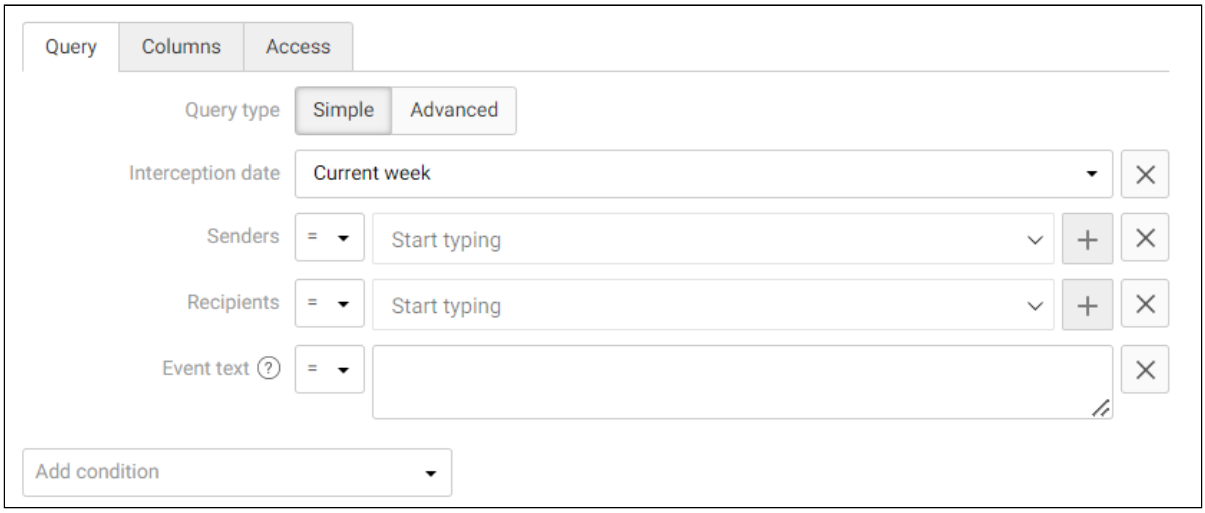
**User's actions:**

- Creating a folder with queries (see *Creating Folder with Queries*);
- Configuring parameters of the query (see *Creating queries*);
- Defining fields of view (see *Choosing event fields of view*).

## Standard Mode of Creating Queries

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

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



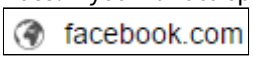

By default, most commonly used conditions are displayed. In the **Add condition** drop-down list, you can choose additional search options.

The full list of available conditions:

| **Condition** | **Description** |
|---|---|
| *Main* | |
| Event ID | A unique identifier of the event. Multiple values may be specified, separated by commas. |
| Interception date | The date when the event was created. By default, events for the current week are displayed. Possible values:<br>▪ All time<br>▪ From<br>▪ To<br>▪ Current day/week/month<br>▪ Last several hours/days<br>▪ Last 3/7/30 days<br>▪ Period (from a calendar) |
| Event type | Specifies that the event belongs to a particular interceptor.<br>Event types are grouped by category. When selecting a category, all event types of this category will be displayed. Possible values:<br>• Recording media:<br>- Screenshot<br>• Application activity:<br>- Clipboard<br>- Keylogger<br>• Web activity:<br>- Web message<br>• File exchange:<br>- FTP<br>- Removable devices |

| | |
|---|---|
| | - Cloud storage<br>- Terminal session<br>- Network resource<br>• Printers and MFDs:<br>- Print<br>• Storing files:<br>- Data Discovery<br>• Email:<br>- Email<br>- Web email<br>• Messenger:<br>- Telegram<br>- Facebook<br>- WhatsApp<br>- VK<br>- Yandex messenger<br>- MS Lync<br>- ICQ<br>- XMPP<br>- Skype<br>- MS Teams (if MS Teams adapter is installed)<br>• File operations:<br>- Read file<br>- Write file |
| Copy sources and receivers | Sources and receivers of copying.<br>Configuration options:<br>• Copy receiver:<br>- Computer<br>- Removable device<br>- Network resource<br>- Terminal session<br>- FTP<br>- Cloud storage<br>• Copy source:<br>- Computer<br>- Removable device<br>- Network resource<br>- Terminal session<br>• Route direction:<br>- In single direction<br>- In both directions<br>You may specify Path to a file or address, Device name, Device ID.<br>The value can be specified using wildcards:<br>• "?" – to replace a single character in the beginning or at the end of a string;<br>• "*" – to replace any number of characters in the beginning or at the end of a string. |

| | |
|---|---|
| | **Note:** Depending on the selected type of the copy source/receiver, there can be different recommendations on how to fill in the **Path to file or address** field (see *Recommendations on how to fill in the Path to file or Address field*).<br><br>**Warning:** The type of the **Path to file or address** attribute value for the "Terminal session" copy receiver depends on the Traffic Monitor version. The attribute value types are different in the events of file exchange via terminal session:<br>• **For events created in Traffic Monitor version below 7.5**: the attribute contains the name of the copied file, for example: `file.txt`<br>• **For events created in Traffic Monitor version 7.5 and above**: the attribute contains the IP address of the device that was used to remotely connect to the employee's workstation and to which the file was copied, for example: `192.0.2.0`<br><br>To search for events created in Traffic Monitor version 7.5 and above, it is recommended to edit existing queries. Existing queries must be edited if they use an obsolete type of the **Path to file or address** attribute value for *Terminal session* copy receiver. If a file name is specified in this attribute in the query, the required events may not match the query condition because new events have an IP address in this attribute. |
| Senders | The list of object senders. May include persons, person groups, statuses, contact values (except SID) or contact metadata. For contacts and contact metadata, a value can be specified using wildcards:<br>• "?" – to replace a single character at the end of the string;<br>• "*" – to replace any number of characters at the end of the string.<br><br>By default, if you use wildcards, the initial part of the string must contain at least 3 characters," e.g. " `use*` ". You can configure this parameter. For details, see *InfoWatch Traffic Monitor. Administration Guide. Configuring Settings of Search Using Wildcards* article. |
| Recipients | The list of object recipients. May include persons, person groups, statuses, contact values (except SID) or contact metadata. For contacts and contact metadata, a value can be specified using wildcards:<br>• "?" – to replace a single character in the beginning or at the end of the string<br>• "*" – to replace any number of characters in the beginning or at the end of the string<br><br>By default, if you use wildcards, the initial part of the string must contain at least 3 characters," e.g. " `use*` ". You can configure this parameter. For details, see *InfoWatch Traffic Monitor. Administration Guide. Configuring Settings of Search Using Wildcards* article. |
| Number of recipients | The number of object recipients |
| Entered perimeters | Perimeter the object recipient belongs to |
| Left perimeters | Perimeter the object sender belongs to |

| | |
|---|---|
| Computer type | Type of computer from which the object was sent. Possible values:<br>• Workstation<br>• Terminal server<br>• Mobile device |
| Computer | The computer from which the object was sent. You can specify a computer name or an IP address. The value can be specified using wildcards:<br>• "?" – to replace a single character in the beginning or at the end of the string;<br>• "*" – to replace any number of characters in the beginning or at the end of the string. |
| Resources | Internet resource or a group of resources (see *Web Resources*). Start typing and choose the desired resource or group from the list of suggestions.<br>The value can be specified using wildcards:<br>• "?" – to replace a single character;<br>• "*" – to replace any number of characters.<br>**Note:** If you want to specify a particular resource, choose the  icon (for example, ) |
| Device ID<br>Device name | ID and name of a removable storage device from which or to which a file was copied. The values are case-sensitive.<br>The values can be specified using wildcards:<br>• "?" – to replace a single character;<br>• "*" – to replace any number of characters. |
| Application | Start typing and choose the desired resource or group from the list of suggestions.<br>The value can be specified using wildcards:<br>• "?" – to replace a single character;<br>• "*" – to replace any number of characters. |
| *Interception* | |
| Interceptor | Interceptor by which the event was received. Possible values:<br>• ICAP<br>• DM<br>• DM Mobile<br>• Adapter<br>• SMTPD<br>• Sniffer<br>• PushAPI<br>• Data Discovery |
| Protocol | Protocol over which the traffic was transferred. Possible values: |

| | |
|---|---|
| | • FTP<br>• HTTP<br>• HTTPS<br>• IMAP<br>• MAPI<br>• MMP<br>• NRPC<br>• OSCAR<br>• POP3<br>• SIP<br>• Skype<br>• SMTP/ESMTP<br>• XMPP<br>• WhatsApp |
| *Application activity* | |
| Source application | Application from which data has been copied |
| Receiver application | Application to which data has been pasted from the clipboard |
| *Analysis results* | |
| Violation level | The level of violation of the corporate security policy. Possible values: *High*, *Medium*, *Low*, *None*. |
| Tags | Tags assigned to the object (see *Tags*) |
| Policies | List of policies triggered on the object |
| Violation type | Type of rule that was violated. Possible values:<br>▪ *Transfer violation*<br>▪ *Copy violation*<br>▪ *Violation of placement*<br>▪ *File operations violation*<br>▪ *Application activity violation* |
| User decision | A decision the user made for the object. Possible values:<br>▪ *Violation*<br>▪ *No violation* |

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

| | |
|---|---|
| address | |
| Attachment size | Size of the attached file. You can specify a minimum or maximum file size or both parameters. |
| Event text | Specify the search text. Search results will include events whose text contains all listed words regardless of their location and order, letter case and morphology. Search is performed through all the event contents. Wildcards ("*", "?") are not supported.<br>When the condition is denied, events whose text contains all specified words will be excluded from search results.<br>**Note:** Search results will contain only those events that have already been indexed at the moment of the query execution. Events are indexed every ten minutes, however, under a heavy load on the server, this interval may increase. |
| Errors of processing | Specify if there are data processing errors. |
| *Data Discovery* | |
| Task name | For information on attribute values, see *InfoWatch Data Discovery. User Guide. Traffic Monitor Event* |
| Task start date | |
| Create date | |
| Modify date | |
| Scanning target | The value **Shared network resources** is always specified. |
| *User attributes* | |
| Attributes which can be added into the System via plugins registered in Traffic Monitor (see *Plugins*). Thus increasing the amount of information to be processed and transmitted via adding attributes of third-party systems that are events sources. User attributes can be used in the rules of data protection policies.<br>Examples of possible user attributes:<br>• Conversation duration<br>• Event identificator in initial system | |

| | |
|---|---|
| | • Hyperlink to event in initial system<br>• Type of action in network media |
| Terminal name | The name of the device that was used to remotely connect to the employee's workstation. The attribute is specified for the *Terminal session* copy receiver in the events of file exchange via terminal session.<br>*Terminal name* is a user attribute of the default InfoWatch Device Monitor plugin. |
| Browser tab address | Address of the active browser tab at the moment when the event was created.<br>The *browser tab address* is a user attribute of the default InfoWatch Device Monitor plugin.<br>To specify multiple values, after entering each value, press **Enter**.<br>The values can be specified using wildcards:<br>• "?" – to replace a single character in the beginning or at the end of the string;<br>• "*" – to replace any number of characters in the beginning or at the end of the string. |
| Page amount in a copy | Page amount in a copy of printed document when intercepting print event.<br>*Page amount in a copy* is a user attribute of the default InfoWatch Device Monitor plugin.<br>You can specify this attribute as a range of values.<br>In case you are using Device Monitor version 7.13 or earlier, you can see page amount in Traffic Monitor events only. |
| Application window title | Window title of used application when intercepting keyboard input event.<br>*Application window title* is a user attribute of the default InfoWatch Device Monitor plugin. |
| Tab title | Tab title of a browser when intercepting keyboard input event.<br>*Tab title* is a user attribute of the default InfoWatch Device Monitor plugin. |
| Chat name | Name of a chat when intercepting sending messages to a WhatsApp or Telegram group chat.<br>*Chat name* is a user attribute of the default InfoWatch Device Monitor plugin.<br>To specify multiple values, after entering each value, press **Enter**.<br>The values can be specified using wildcards:<br>• "?" – to replace a single character in the string;<br>• "*" – to replace any number of characters in the string. |
| Decrypted data | Whether an event contains decrypted files.<br>*Decrypted data* is a user attribute of the default InfoWatch Password Disclosure Adapter plugin. |
| Initial event ID | ID of the initial event of intercepting an email with an encrypted file attached.<br>*Initial event ID* is a user attribute of the default InfoWatch Password Disclosure Adapter plugin. |

**Note:** Traffic Monitor analyzes the contents of an encrypted file in the event generated by the adapter after decrypting, not in the initial event.

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

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

**Note:**

Attribute values in search logic:

- By default, all attributes are checked for equality to specified values (the  parameter next to the attribute name). Results of the query execution will include events whose parameters have specified values.
- If a value of an attribute is not set, search process will be based on other attributes that satisfy the rule.
- To exclude events with specified values from the results, apply negation  to the required attributes.

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

- Event ID;
- Senders;
- Recipients;
- Entered perimeters;
- Left perimeters;
- Computer;
- Resources;
- Tags;
- Policies;
- Attachment name;
- Attachment format;
- Technologies;
- Protected objects;
- Terminal name;
- Browser tab address;
- Page amount in a copy;
- Application window title;
- Tab title;
- Chat name;
- Initial event ID;
- Event text;
- Device ID;
- Device name;
- Application;
- Source application;
- Receiver application.

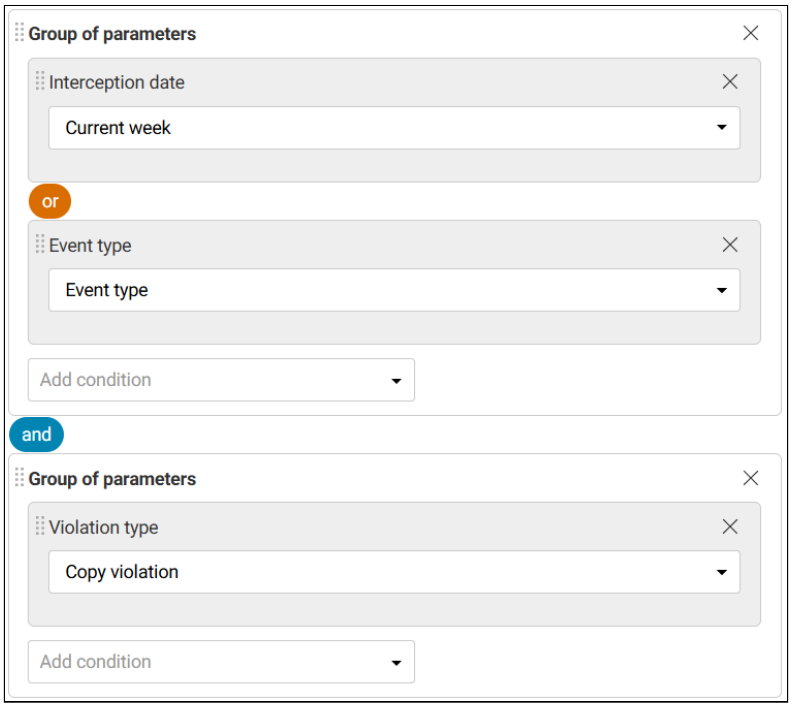
If a negation parameter is applied to an attribute with multiple values, then events that contain specified values will be excluded from search results. For example, if `user1@example.com` and `user2@example.com` users are specified as Senders, then events with the sender `user1@example.com` or `user2@example.com`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

**User's actions:**

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

## Advanced Mode

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




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

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

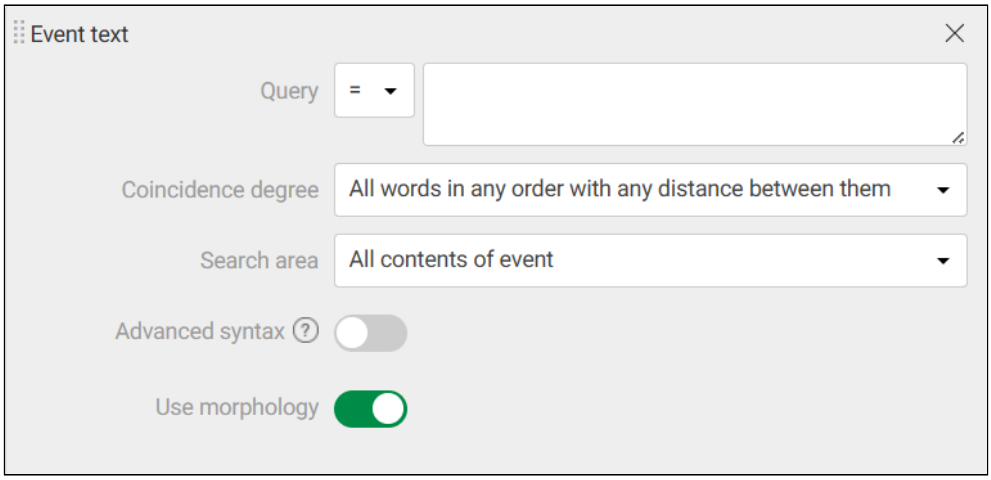
In the advanced mode, you can also perform a *flexible search on the text of events*.

**User's actions:**

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

## Search on the Event Text

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




**Full-text search parameters:**

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

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

**Please note that:**

- Words must be divided with spaces;
- Search is not case-sensitive;
- Using wildcards ("*", "?") is not supported;
- Hyphen ("-") is not taken into account while searching. Search is performed by each word, which is a part of a word with hyphen used;
- Period ( ".") and "@" symbol are not taken into account while searching. In case words are divided with a period or an "@" symbol, the search is performed by each of the words.

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

**User's actions:**

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

### 3.2.2 Object Interception

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

Information on the event is presented in following ways:

- The event tile (or the table entry) contains general information about the event
- Each event table row contains information on the attributes selected on the **Columns** tab
- The list of attachments contains the attachments found during search for analogues and grouped by events
- The brief event viewing form displays the most commonly required information
- The detailed event viewing form displays complete information about the interception object

Event attributes:

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

| Element | Description |
|---|---|
| The sender's computer | The name of the computer from which traffic was sent |
| Recipients | The list of traffic recipients |
| Policies | List of policies triggered on analysis of this event |
| Categories | List of categories assigned to this event |
| Protected objects | List of protected objects triggered for this event |
| Elements of analysis | The list of elements of analysis contained in the triggered protected object |
| Website topic | Type of inappropriate resources visited by the employee |
| Tags | List of tags assigned to this object |
| Date of interception | Date and time when traffic was intercepted by the System |
| Insert date | Date and time when the event was saved into the Database |
| Size | Size of the event (in bytes) |
| Violation level | Characteristics of the violation assigned to the event. Possible choices:<br>• *No* – is marked with a gray (■) colour on the tile<br>• *High* – is marked with a red (■) colour on the tile<br>• *Medium* – is marked with an orange (■) colour on the tile<br>• *Low* – is marked with a green (■) colour on the tile |
| Delivery status | Indication of whether the message was delivered (only for SMTP messages when the System operates in the "inline" mode. For details, see the *InfoWatch Traffic Monitor. Administration Guide*. *Inline mode* article).<br>Possible choices:<br>▪ *Pending*<br>▪ *Successfully delivered*<br>▪ *Failed*<br>▪ *Delivery Attempt Failed*<br>▪ *Blocked* |
| Verdict | The conclusion which the System assigned to the object as a result of analysis. Possible choices: |

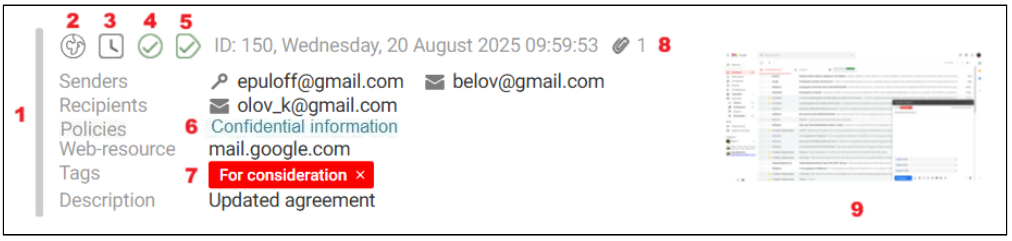
| Element | Description |
|---|---|
| | • *Allowed* ( ) <br> • *Blocked* ( ) <br> • *Quarantined* ( ) |
| Interception server | The name or IP address of the server which intercepted the object |

**See also:**

- Event Tile – on presenting the event and its attributes
- Table view of Events – on displaying information on selected event attributes
- List of Attachments – on displaying attachments found during search for analogues
- Brief Event Viewing Form – on displaying general information about the event
- Detailed Event Viewing Form – on displaying advanced information about the event

## Event Tile

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




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

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

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

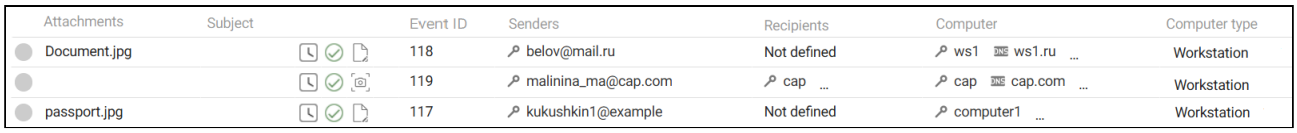
1. The colour of the violation level. Possible values: *High*, *Medium*, *Low*, *No*.
2. The event type. Possible values: *Clipboard, Keyboard input, Screenshot, Web message, Facebook, WhatsApp, ICQ, MS Lync, Mail.ru Agent, Skype, MS Teams* (if the adapter is installed), *Telegram, XMPP, VK (VKontakte),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

9. Screenshot thumbnail. If an event has a screenshot, a thumbnail image of the screenshot is displayed. Clicking on a thumbnail will open the original image.

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

## Table view of Events

The **table view of events** is displayed when using a table mode:



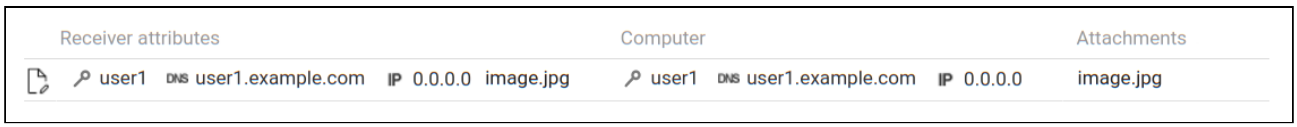

Each column of the table corresponds to an event attribute. On the **Columns** tab, when creating or editing a query, you can select columns that will be displayed in the table (see *Queries*).

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

> **Note:**
>
> Sorting is not possible by *Subject*, *Computer type*, *File creation date*, *File modification date*, *Scanning target*, *Task name*, *Task start date, Receiver attributes, Terminal name, Browser tab address, Page amount in a copy, Application window title, Tab title, Initial event ID, Chat name* columns.

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

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




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

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

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

**Warning!**

The **Receiver attributes** column is not included in event export, even if added to the **Displayed fields** list.

**User's actions**:

- Viewing information about events (see *Viewing events*);
- Choosing the event fields (see *Choosing Event Fields of View*).

## List of Attachments

The results of *search for analogues* are displayed as the list of attachments grouped by events.




Each event tile contains:

- general information about the event;
- attachments from this event found during search for analogues. If the event contains other attachments, they are not displayed.

You can:

- view the attachment content. For this, select the attachment. Its content will be displayed in the right part of the workspace;
- save an attachment to your computer. For this, click  next to the attachment name;
- search for analogues of the selected attachment.

**Примечание:**

In the list of attachments you cannot:

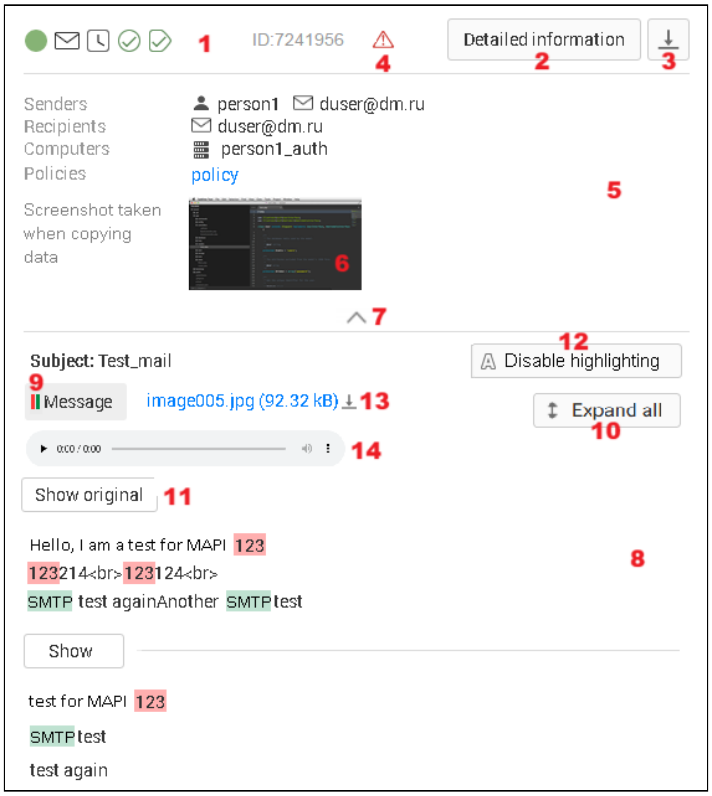
- make a decision on the event
- assign a tag to the event
- export the event or save debug information on the event

To perform listed actions, switch to the detailed event viewing form, to the list view or to the table view.

You can find more information on the event in a *brief* or *detailed* event viewing form.

## Brief Event Viewing Form

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




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

1. The upper part of the form (№ 1 in the screenshot) where you can see:
   - event ID;
   - indicators of the following event attributes: the violation level, the event type, the user decision, the verdict, a delivery status (for possible attribute values, see *Event Tile*);
   - the **Detailed information** button (№ 2 in the screenshot), clicking which opens the detailed event viewing form (see *Detailed Event Viewing Form*);
   - the  button (№ 3 in the screenshot) which allows you to save a shadow copy of the event (see *Saving Events (for SMTP mail)*). The button is displayed for SMTP messages only;
   - the indicator of processing errors (№ 4 in the screenshot). Is displayed if errors occurred during processing. You can see more details on the errors in the *detailed event viewing form*.
2. The area for viewing the event parameters (№ 5 in the screenshot).
   In the viewing area, you can see information on senders, recipients, number of pages in shadow copy of the file that is sent to printing, triggered policies and protected objects. Protected objects and policies that have been removed from the System are marked in red. For events containing a screenshot, a thumbnail of the screenshot is displayed (№ 6 in the screenshot).

Click on a thumbnail of the screenshot to open the screenshot. To hide the area with the event parameters, click  (№ 7 in the screenshot). To restore the area, click .

3. The area for viewing the event content (№ 8 in the screenshot).
   In the viewing area, you can view the event text, attachments, and sound files.
   By default, the event content is highlighted: triggered protected objects are highlighted in red, results of a search by the event text are highlighted in green. The colour (№ 9 in the screenshot) indicates that the event contains triggered protected objects and/or found text.

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

   By default, the viewing form displays not all event text, but snippets which contain triggered protected objects or the found text. To unfold text between the two snippets, click **Show**. To view the whole text of the event, click **Expand all** (№ 10 in the screenshot).
   For emails with HTML markup or attachments which can be displayed in an original format (images, PDFs), a button for choosing a viewing mode is displayed (№ 11 in the screenshot).
   Possible values:
   - **Show extracted text** – the text is displayed without formatting. This option allows you to view hidden text (e.g., white text or text in the picture name);
   - **Show original** – this option allows you to view pictures, tables, and markup.

   To completely disable the highlighting, click **Disable highlighting** (№ 12 in the screenshot).
   If the event contains an intercepted voice message from Skype, then you can listen to the message using tools for voice messages (№ 14 in the screenshot).

If the event contains a merged file, the warning sign  will appear next to the file name.

To save an attachment to your computer, click  (№ 13 in the screenshot) next to the attachment name.

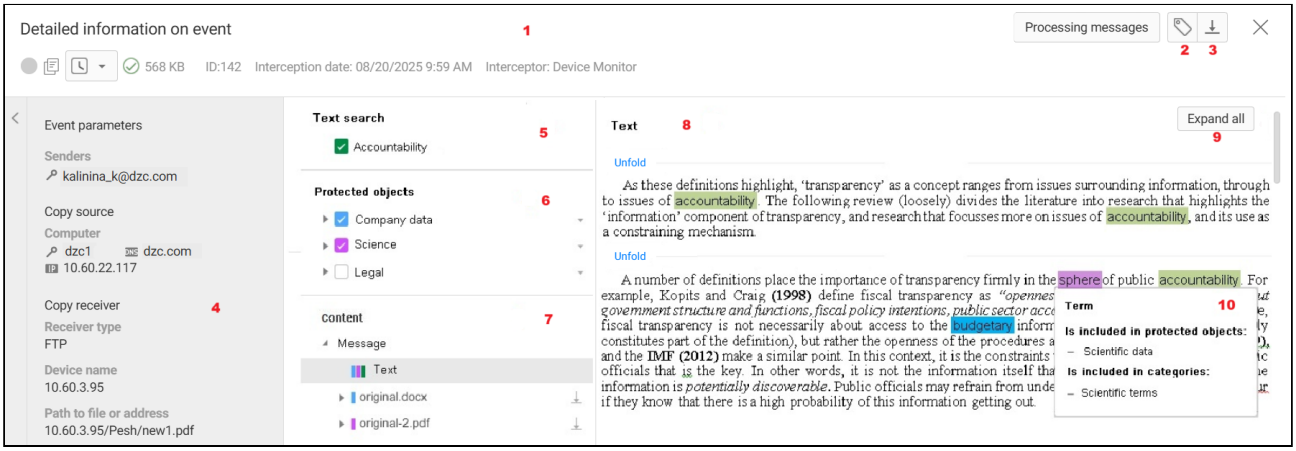
> **Note:**
>
> In case an event:
>
> - Contains attachment or text which have been deleted according to the policy rule (the action to delete *Attachments only* or *Attachments and extracted text* is selected)
>   or
> - Does not contain a shadow copy,
>
> then:
>
> - These attachments and text have the icon  displayed. When you point the cursor at the icon, the *Attachment is not available* tip is shown.
> - For these deleted attachments, the System displays their name, format and size. The attachments and texts (in case the option *Attachments and extracted text* is selected) cannot be viewed or loaded.
> - Instead of text (in case the option *Attachments and extracted text* is selected), the System displays Event text is deleted message.

**User's actions:**

- Viewing Brief Event Form.

## Detailed Event Viewing Form

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




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

1. The upper part of the form (№ 1 in the screenshot), which displays:
   - Indicators of the event attributes: a violation level, the event type, the user decision, a verdict, a sending status (possible attribute values are described in *Event Tile*)
   - Event size
   - Event ID
   - Date and time when the event was intercepted
   - An interceptor by which the event was received
   - **Processing messages** button clicking which opens a window with system messages about processing stages and errors if any
   - The  button (№ 2 in the screenshot) which allows you to set a tag to the event (for details, see *Tags*)
   - The  button (№ 3 in the screenshot) which allows you to save a shadow copy of the event (see *Saving Events*). The button is displayed for SMTP messages only
2. The **Event parameters** area (№ 4 in the screenshot) which displays information on senders, recipients, triggered policies, number of pages in shadow copy of the file that is sent to printing, protected objects, perimeters, etc.
   For events containing screenshot, a thumbnail of the screenshot is displayed.
3. The **Text search** area (№ 5 in the screenshot). It is displayed, if the query conditions include a search for the event text.
4. The **Protected objects** area (№ 6 in the screenshot). A list of triggered protected objects and elements of technologies that are included in these protected objects. Protected objects and elements of technologies that have been removed from the System are marked in red.
5. The **Content** area (№ 7 in the screenshot). Displays the event content: the message text, attachments, voice messages.
   The  button next to the attachment name allows you to save a selected file to your computer.

**Note:**

If the event includes an attachment, but the attachment name was not extracted, the MIME type of the file will be displayed instead of the name.

If the event includes a merged file, the sign  will appear next to the file name. The System will display the sign next to files which contain CDATA section. In case the System detects CDATA section next to OOXML (Office Open XML), it will mark the attachment with the sign of a merged file as well.

Text data extracted from CDATA section will be sent for analysis together with the main contents of the file. In case the System detects encoded data, like Base64 or UUE, inside CDATA section, after decoding it will display the contents in a child branch.

The System converts HEIC and JIF (JIFF) images into JPEG format and creates a child branch for the converted image. You can save both parent and child formats to your computer.




If the event includes an attachment with UUE encoded data, the information about the attachment is displayed in email event content, when you point the cursor on the  sign next to the file name.

**Note:**

In case the event:

- Contains attachment or text which have been deleted according to the policy rule (the action to delete *Attachments only* or *Attachments and extracted text* is selected) or
- Does not contain a shadow copy,

then:

- These attachments and text have the icon  displayed. When you point the cursor at the icon, the *Attachment is not available* tip is shown.
- For these deleted attachments, the System displays their name, format and size. The attachments and texts (in case the option *Attachments and extracted text* is selected) cannot be viewed or loaded.
- Instead of text (in case the option *Attachments and extracted text* is selected), the System displays *Event text is deleted* message.

6. The viewing area (№ 8 in the screenshot). Allows you to view the message text and the text extracted from attachments.

**Note:**

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

By default, in the viewing area (№ 8 in the screenshot), the text is displayed as snippets which contain triggered protected objects or the found text.

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

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

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

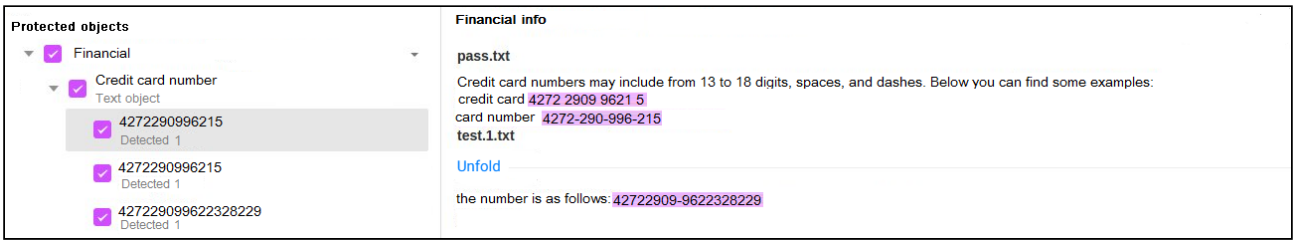
> **Note:**
>
> The term highlighting for Autolinguist categories is not supported for events created in Traffic Monitor version 7.4 and earlier.

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

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

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

For system text objects detected in intercepted data, values are reduced to the normal form. Thus, in the **Protected objects** area (№ 6 in the screenshot), all values of the same text object are represented in the same way.




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

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

- for a term – a category that includes the term;

- for a text object – the text object name.

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

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

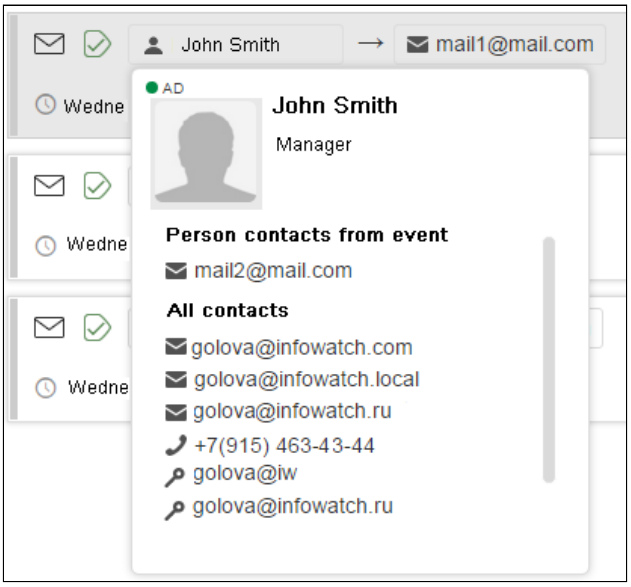
- for `original.docx` attachment – the *Company data* protected object;
- for `original-2.pdf` attachment – the *Science* protected object;
- for the event text – the *Company data* and *Science* protected objects; besides, the search text is found.

**User's actions:**

- Viewing Detailed Event Form.

### 3.2.3 Contact Identification in Event

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




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

> **Note:**
>
> Post identification applies to traffic senders only. Contacts of traffic recipients are not identified.

**Note:**

For the following resources, post identification is not supported:

- odnoklassniki.ru
- gmail.com

**Note:**

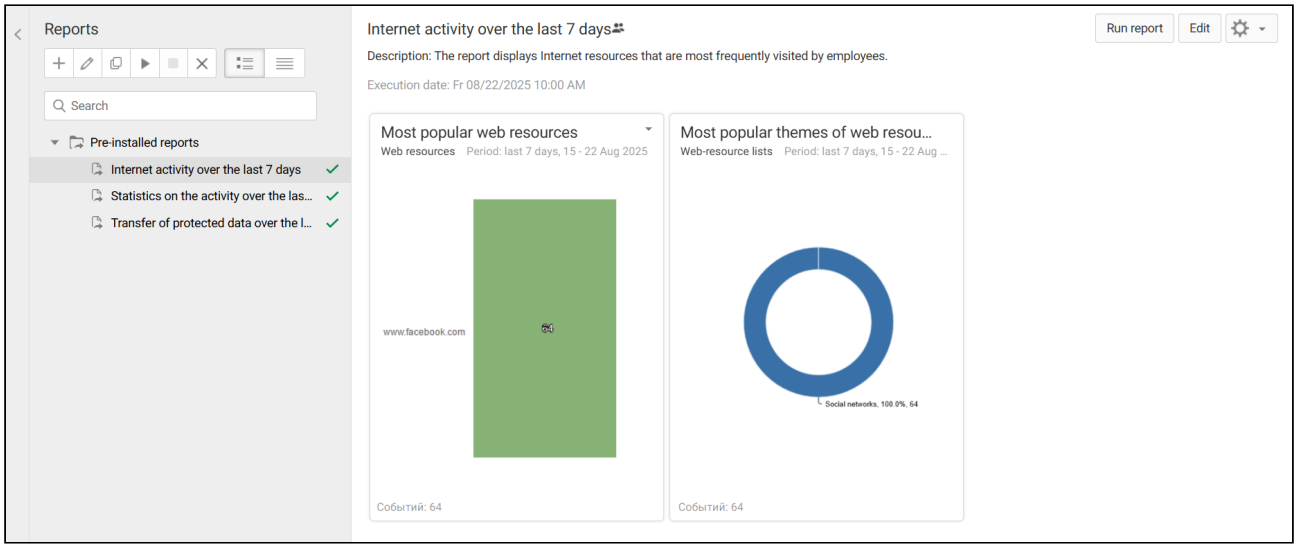
It can happen that personal cards of different users who work on different computers may contain the same accounts in messengers (e.g., Skype) as their contacts. This can happen if those users have logged into different computers under the same domain name or if they have logged into the same computer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

## 3.3 Reports Section

**About the section:**

Contains a list of reports and tools for managing them.

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




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

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

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

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

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

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

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

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

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

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

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

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

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

- Open the report execution history;
- Copy the report;
- Delete the report;
- Save the report as a file in one of the supported formats.

**User's actions:**

- Creating Folder with Reports;
- Creating Report;
- Creating and Configuring Widget;
- Viewing Ready Reports.

## 3.3.1 Report Creation Form

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




You can specify the following settings:

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

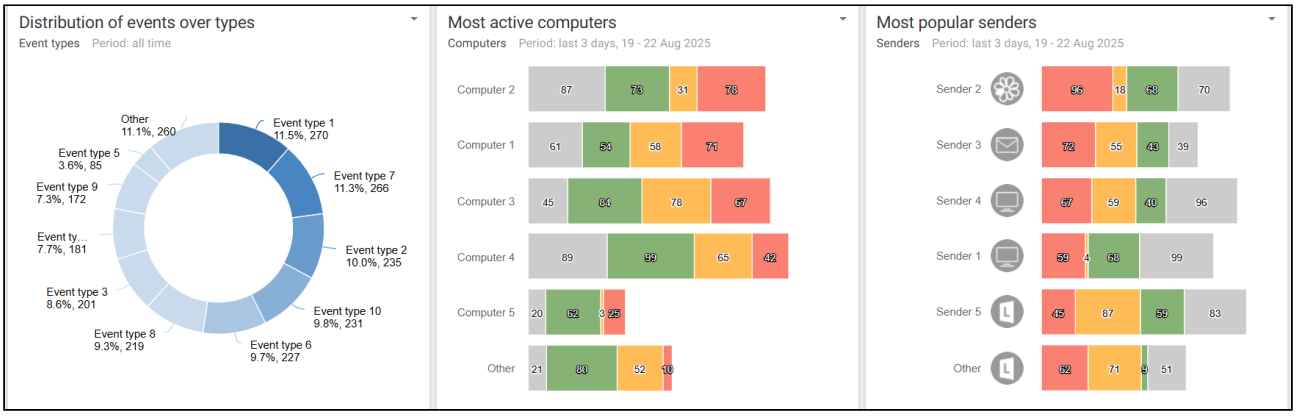
**User's actions:**

- Creating report.

## 3.3.2 Widgets of Reports

Widgets are designed to display statistical information in reports.

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




Widgets can be created for the following data:

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

| Type of statistics | Description |
|---|---|
| Event types | Distribution of the number of events into types (mail, Skype, external devices, etc.) |

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

-  – bar chart with grouping
-  – bar chart with accumulation
-  – pie chart
-  – grap

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

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

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

**Widget parameters for other types of statistics:**

| Parameter | Description |
|---|---|
| Chart type | The following types are available:<br>• bar chart with grouping<br>• bar chart with accumulation<br>• pie chart (except for the "Dialogs" diagram type) |
| Number of records | The number of records that will be displayed in the widget. Specify a value from 1 to 100.<br>**Note**: For the "User decisions" statistics type, this option is not displayed |

| Parameter | Description |
|---|---|
| Merge other records into “Other” item | Select this option if you want to add the “Other” item that will combine the rest of records on the widget.<br>**Note**: For the "User decisions" statistics type, this option is not displayed |
| Show values | Select this option for numerical values to be displayed on the widget |
| Show proportions | This option is available for the pie chart only |

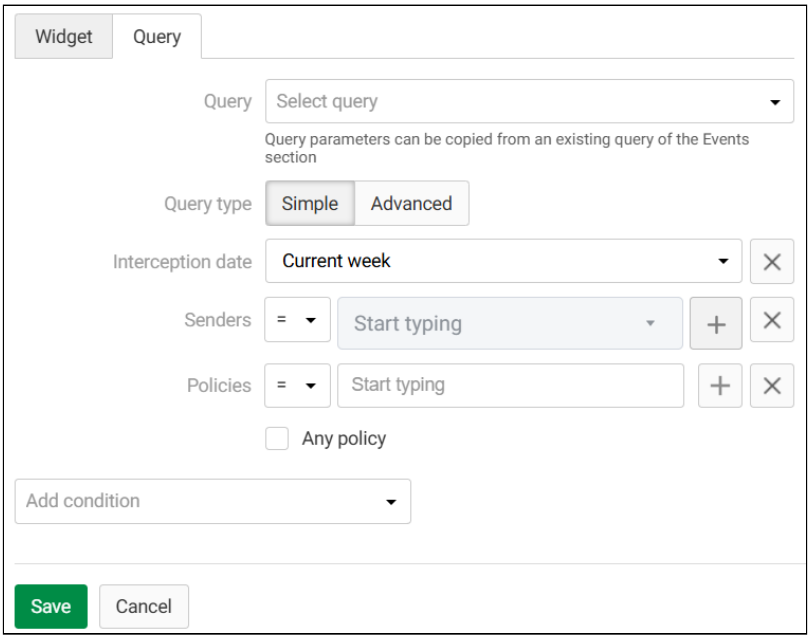
**User’s actions:**

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

### 3.3.3 Queries

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

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




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

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

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

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

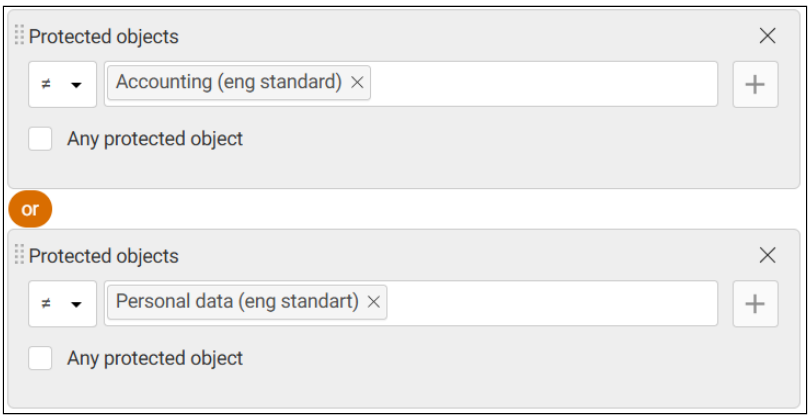
- *Advanced mode* – allows you to perform more flexible configuration of the query conditions using the conjunction (logical "AND") and disjunction (logical "OR"). For details, see *Advanced mode*.

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

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

**Example of using the disjunction:**

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




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

**User's actions:**

- Creating a query (see *Query Creation in Standard Mode* and *Query Creation in Advanced Mode*).

## 3.4 Technologies Section

**Reference information:**

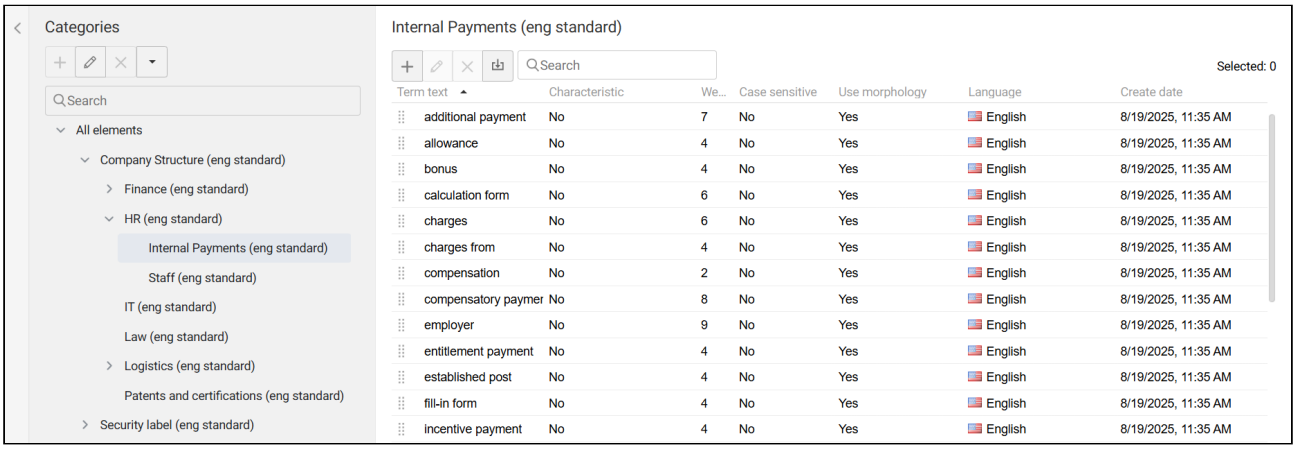
***Technologies*** are a set of methods, which enable the System to detect confidential data in intercepted objects using user- or algorithm- predefined features.

Below are the technologies and data types to which you can apply them:

| Technology | Purpose | Data type |
|---|---|---|
| Categories and Terms | Attribute a text to a certain category using specified key terms. Used for dynamic information, with large document flow and a limited set of categories | text |
| Text Objects | Detect text objects (phone numbers, passport numbers etc) using a specified pattern | text |

| Technology | Purpose | Data type |
|---|---|---|
| Sample Documents | Detect sample documents, fully or partially quoted in intercepted data. Used for static information, documents that are not subject to change or rarely alter | text, graphical, vector, binary |
| Blanks | Detect forms, spreadsheets, surveys using a specified sample | text, vector |
| Stamps | Detect stamps using a specified sample | graphical |
| Database Unloadings | Detect confidential data from databases | text |
| Graphical Objects | Attribute an image to a certain category using an automatic classifier | graphical |
| Autolinguist | Attribute a text to a certain category using an automatic classifier | text |

**About the section:**




The section contains:

- Editable catalogues, which you can enrich by your own categories and samples:
  - Categories and terms;
  - Text objects;
  - Sample documents;
  - Blanks;
  - Stamps;
  - DB unloadings.
- Automatic classifiers, which you can retrain with your own data:
  - Graphical object classifier;
  - Autolinguist.

**User's actions:**

- Creating categories and terms
- Creating text objects and their values
- Managing sample documents
- Creating blanks

- Creating stamps
- Creating DB unloadings
- Graphical Objects
- Managing Autolinguist

### 3.4.1 Categories and Terms

**Reference information:**

The technology enables the System to use topic-specific key words or collocations to determine topics of analyzed texts. The System selects a topic from a limited list of ***categories***. Each category consists of ***terms***, i.e. key words by which the System attributes a text to a certain category. For example, if the text contains terms like *interest income*, *imputed earnings*, *taxpayer*, the System attributes the text to *Taxes* category.

Some terms are so rare that they can only be found in texts on a single topic, which makes it possible to attribute a text with this term to the topic unambiguously. Such terms are called ***characteristic***. For example, *strictly confidential information* can be a characteristic term for *Security label* category.

Thus, Traffic Monitor attributes a text to a category if:

- The text contains at least three topic-specific terms
  or
- The text contains at least one term with *Characteristic* attribute.

Text analysis also depends on other attributes: weight (the ratio of term frequencies in the text), language, morphology, and case sensitivity. You can configure the attributes in category and term settings. For attribute description, see *Terms*.

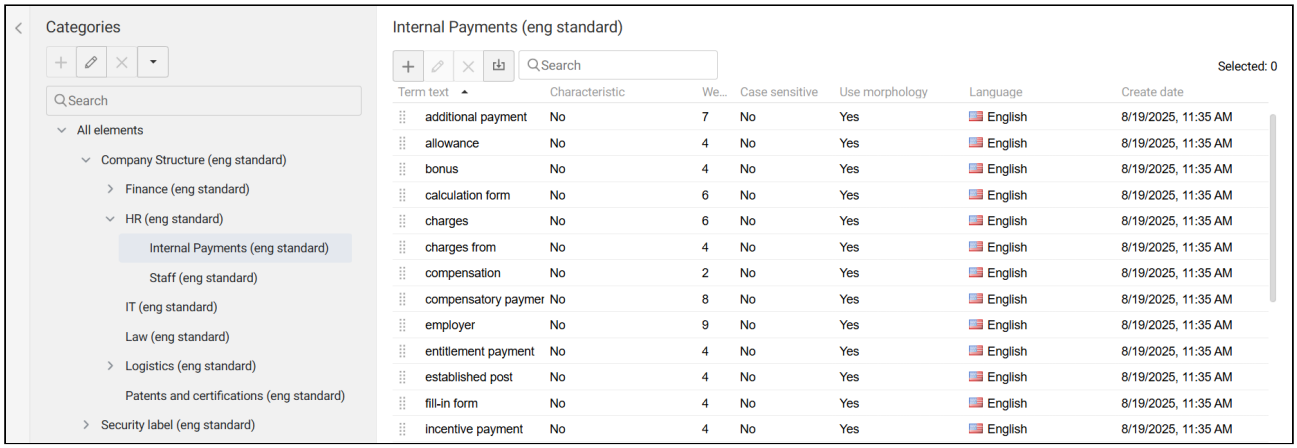
The preinstalled English categories with configured settings are the following:

- *Company Structure*:
  - *Finance*:
    - *Accounting*;
    - *Accounts*;
    - *Credits*;
    - *Taxes*.
  - *HR*:
    - *Internal Payments*;
    - *Staff*.
  - *Law*;
  - *Logistics*:
    - *Foreign Economic Activities*;
    - *Tenders*.
  - *Patents and certifications*.
- *Security label*;
  - *Company Specification*;
  - *Company Secret*;
  - *Company Confidential*.

You can edit preinstalled categories as well as create your own ones.

**About the section:**

Categories section contains a hierarchical list of categories. By clicking a category, you can view the list of terms it includes.




On the left side of the working area, find tools for operations with categories:

- Create, edit, move, delete, import/export a category;
- Search by categories.

On the right side of the working area, find:

- List of terms within the selected category;
- Tools for operations with terms:
    - Create, edit, move, copy or delete a term;
    - Perform a cross-cutting search for a term. The cross-cutting search is performed within the selected category and enclosed ones. To perform the search through all the section's categories, select the root category.

**User's actions:**

- Create a list of categories and terms, see *Managing Categories and Terms*;
- Import and export categories and terms as a part of the base of technologies, see *Exporting and Importing the Technologies Database*;
- Add categories to protected objects, see *Creating a Protected Object*.

## Categories

**Reference information:**

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

The System attributes a text only to the category directly containing the term. For example, if a parent category named *Finance* has a child category named *Taxes*, and a text contains *interest income* term, the System attributes the text to *Taxes*, not *Finance*.

For the System to detect a category in intercepted data, include the category in a protected object.

In edit mode, you can add category description, as well as specify the attributes, which each term within the category will inherit:

- **Weight**
- **Language**
- **Use morphology**
- **Case sensitive**

For attribute description, see *Terms* article.

**User's actions:**

- Create subject areas of confidential data, see *Managing Categories and Terms*;
- Include categories in protected objects, see *Creating a Protected Object*.

## Terms

**Reference information:**

***Term*** is a word or collocation found in analyzed texts which makes it possible to attribute a text to a specific topic.




**Term attributes:**

| Parameter | Description |
|---|---|
| Term text | A word or collocation[1] including only letters, spaces and hyphens; maximum length is 256 characters<br>Supported characters[2]: alphabetic characters, space and hyphen<br>In the term text, you can specify the distance between words as an *{X, Y}* range. You can create terms with the same words but with different distances between them.<br>Example: "*Word1 {1, 25} Word2*" means that there can be from 1 to 25 different words between *Word1* and *Word2*.<br>Minimum value for *X*: 1 character. Maximum value for *Y*: 1000 characters. *X* must not exceed *Y*. |
| Characteristic | The term with this attribute is enough to assign a category to the text without other conditions<br>Disabled by default |
| Weight | Indicator of the term significance. We recommend using the default weight values. If, when scanning your documents, you see the word used more often, use the higher weight value, the less the lower.<br>Example: *this agreement* is quite frequent in contracts, so you can specify the highest weight for it.<br>Supported values: 1 to 10<br>Default value[3]: 5 |
| Case sensitive[4] | Indicates if the case is matched in traffic analysis. |

| Parameter | Description |
|---|---|
| | Example: If the parameter is enabled for *access rights* term, the System ignores collocations typed as *Access Rights*, *Access rights*, *access Rights*, and so on.<br>Disabled by default[3] |
| Use morphology[4] | Indicates if morphology is used in traffic analysis<br>Example: If the parameter is enabled for *wage* term, the System detects both *wage* and *wages*.<br>Disabled by default[3] |
| Language | The language of the term. Allows using correct morphology rules of a certain language.<br>Default value[3]: Russian |

**Note:**

[1] Avoid terms that:

- Consist of a single word, especially if it is commonly used, like *labour*, *highest*, *checked*;
- Can be ambiguous, like *leak*, which can relate to *gas* or *data*;
- Are functional words or contain little conceptual content words, like *therefore*, *is*, etc.

We recommend using collocations as terms. Use longer collocations to narrow your search in order to detect one type of documents only, for example, if you need to detect tax declarations, but not statistical tax forms or certificates. The longer collocations are used, the more likely they will not be found in other documents.

[2] The System ignores punctuation marks and numbers during the linguistic analysis, so the term *delivered goods* will be found both in *delivered goods* and in *delivered 143 goods*. To detect messages with non-alphabetic characters like *TO.P234.67*, create a text object.

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

[4] **Case sensitive** and **Use morphology** parameters are mutually exclusive. You can enable only one of them or disable both.

**User's actions:**

- Create and edit terms, see *Managing Categories and Terms*.

## 3.4.2 Text Objects

**Reference information:**

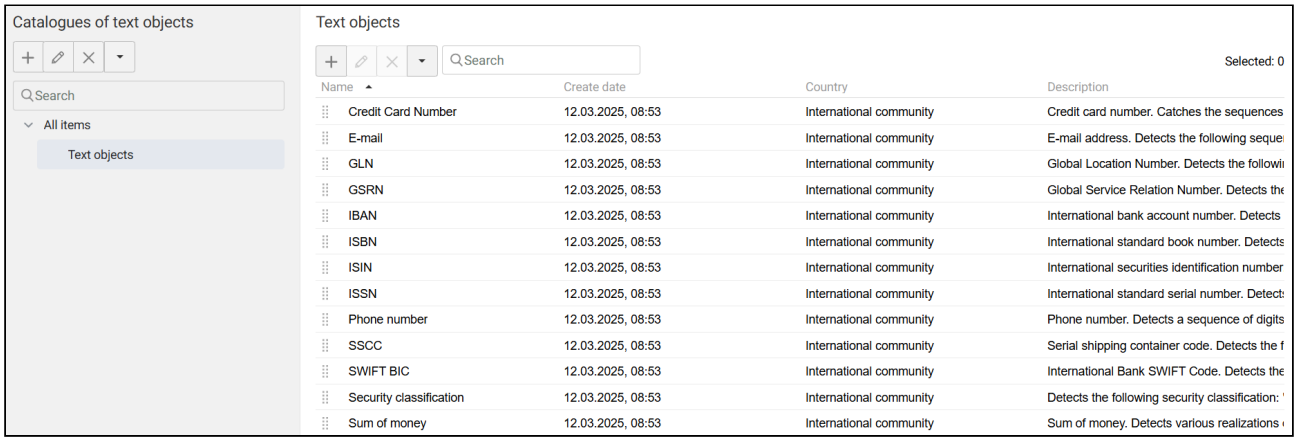
***Text objects*** are data with a fixed structure which can be described with a *pattern*. The System uses patterns to detect text objects during text content analysis. Examples of text objects include passport numbers, credit card numbers, email addresses and so on.

You can use preinstalled text objects, as well as create new ones.

For the System to detect a text object in intercepted data, include it in protected object.

**About the section:**

The section contains a hierarchical list of catalogues within which you can create text objects. Further, when creating a protected object, you can add both single text objects and entire catalogues to it.




On the left side of the working area, find tools for operations with catalogues:

- Create, edit, move, delete, import/export a catalogue;
- Search by catalogues.

On the right side of the working area, find:

- List of text objects within the selected catalogue;
- Tools for operations with text objects:
  - Create, edit or delete an object;
  - Add a system text object;
  - Perform a cross-cutting search by the name of a text object. The cross-cutting search is performed in accordance with the name of unloading and it is performed within the selected catalogue or enclosed ones. To perform the search through all the section's catalogues, select the root catalogue.

**User's actions:**

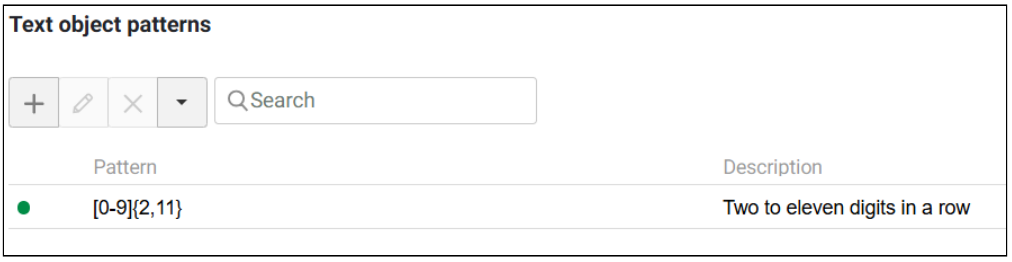
- Create text objects and their catalogues, see *Managing Text Objects*;
- Add system text objects to a selected catalogue, see *Managing Text Objects*;
- Import and export text objects as a part of technologies base, see *Exporting and Importing the Technologies Database*;
- Add text objects to protected objects, see *Creating a Protected Object*.

## Text Object Patterns

**Reference information:**

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

To view the patterns for a selected text object, switch to the edit mode of the text object.




**Actions with patterns**

Use the toolbar buttons to:

- create patterns;
- edit patterns;
- delete patterns;
- activate/deactivate patterns. The System uses color indicators to display the current status of a pattern:
  - active;
  - inactive.

> **Warning!**
>
> Editing and deleting preinstalled patterns of the system text objects is unavailable.

**Pattern attributes**

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

| Parameter | Description |
|---|---|
| Status | Indicates if this text object value is used.<br>Supported values: *Active* or *Inactive* |
| Pattern type | Specify how you want to set the pattern: as a string or a regular expression |
| String | Displayed for *string* type. The exact value of the text object specified as a sequence of characters.<br>For example, `example@company.com` pattern matches only `example@company.com` string |
| Regular expression | Displayed for *regular expression* type. Configurable template. For details on regular expressions, see the Knowledge Base articles: *Syntax of regular expressions* and *Description of macros for text object patterns* |

| Parameter | Description |
|---|---|
| Validation text | Displayed for *regular expression* type. An example of a text to verify how the regular expression works. Enter the verification text and click **Check**. |
| Description | If necessary, add a description |

**User's actions:**

- Create a text object.

## 3.4.3 Sample Documents

**Reference information:**

***Sample documents*** are a collection of exemplary documents which are not subject to change, or which can be altered rarely: strategic plans, annual reports, contracts and so on. The technology enables the System to search for quotations from sample documents in intercepted objects. The text is considered containing confidential data only in case the number of quotations exceeds the *quotation threshold* specified by the Security Officer.

We recommend uploading all exemplary documents whose contents are partially or fully critical for protection.

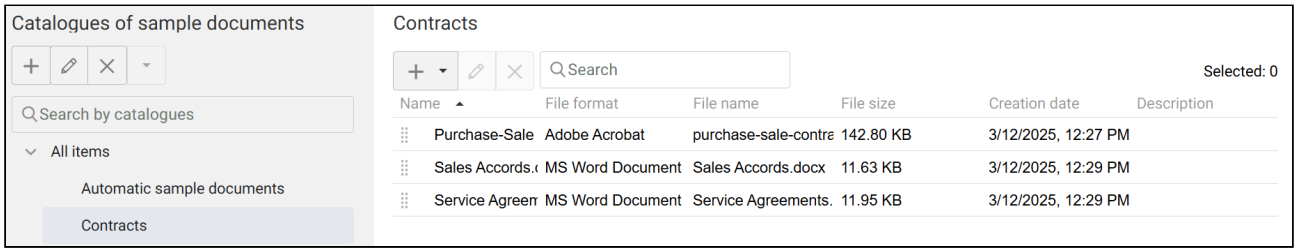
The System stores sample documents as *digital prints*, their text is not available to either users or System administrators.

You can upload sample documents which contain text, binary, graphical or vector data.

For the System to detect quotations from a sample document in intercepted data, included the document in a protected object.

**About the section:**

The section contains a hierarchical list of catalogues within which you can create sample documents. Further, when creating a protected object, you can add both single sample documents and entire catalogues to it.




**Note:**

Preinstalled Automatic sample documents contains documents received from an external system. You cannot delete this catalogue. For details, see *Automatic sample documents*.

On the left side of the working area, find tools for operations with catalogues:

- Create, edit, move, delete, import/export a catalogue;
- Search by catalogues.

On the right side of the working area, find:

- List of documents within the selected catalogue;

- Tools for operations with documents:
    - Create, edit or delete a document;
    - Perform a cross-cutting search by a document name. The cross-cutting search is performed within the selected catalogue and enclosed ones. To perform the search through all the section's catalogues, select the root catalogue.

When editing a catalogue, you can add catalogue description, as well as specify attributes, which will be common for all sample documents within the catalogue.

When editing a document, you can:

- Specify attributes of the document[1];
- Update the documents.

**Sample document attributes**

| Attribute | Description |
|---|---|
| **Name** | Full file name by default |
| **Full file name** | The System defines the values automatically. Editing is unavailable. |
| **File format** | |
| **Text data quotation threshold** | The percentage of the sample document that is sufficient for referring the intercepted object to this sample document. Used for text object detection (document text)<br>Default value[1]: 10% |
| **Binary data quotation threshold** | the percentage of the sample document that is sufficient for referring the intercepted object to this sample document. Used for binary object detection (images, executable files, etc.)<br>Default value[1]: 10% |

**Note:**

[1] When you create a document, the System specifies attribute values configured in catalogue settings. You can change attribute values for certain documents. The System does not apply changed settings to already created documents.

**User's actions:**

- Create sample documents and their catalogues, see *Managing Sample Documents*;
- Import and export sample documents as a part of the technologies base, see *Exporting and Importing the Base of Technologies*;
- Update the sample document, see *Managing Sample Documents*;
- Add sample documents to protected objects, see *Creating a Protected Object*;
- Work with automatic sample documents, see *Automatic sample documents*.

### Automatic sample documents

**Reference information:**

***Automatic sample documents*** are created by an external system and added to Traffic Monitor in one or several ways:

- Via an adapter, from the network catalogue. For details on how to install the adapter and work with it, see *InfoWatch Sample Documents Autoupdate Adapter. Setup and Configuration Guide* document.
  or
- Via programming interface. For details, see *InfoWatch Traffic Monitor. Administration Guide. Uploading Sample Documents and DB unloadings (REST API SDK)* section.

The external system (connector) initiates addition of automatic sample documents and their further update.

Traffic Monitor stores sample documents created by the external system in the preinstalled **Automatic sample documents** catalogue.

In order to work with automatic sample documents:

- Authorize the external system in Traffic Monitor using the plugin. See *InfoWatch Traffic Monitor. Administration Guide* document.
- To detect an automatic sample document in intercepted data, add it to a protected object.

**Operations with automatic sample documents:**

By default, you can view and edit **Automatic sample documents** catalogue.

You can edit and delete all automatic sample documents inside the catalogue. Use the toolbar buttons in the right part of the working area.

In Traffic Monitor Management Console, you cannot manually update automatic sample documents from the unloading.

> **Warning!**
>
> Simultaneous configuration editing via Management Console and via SDK can cause a conflict. So, when developing a connector, it is recommended to check out general principles of *configuring the System*.
>
> In case of a conflict, first you should check errors returned to the connector from SDK.

## 3.4.4 Blanks

**Reference information:**

A **blank** is a form sheet with fields to be filled in: questionnaires, surveys and so on. The System can recognize blanks both with filled and not filled fields. Blanks can be a text file or a spreadsheet.

The System stores blanks in the System as *digital fingerprints*. Their text is not available for viewing either by users or by the System administrators.

Technically, a blank is a file, each line of which contains one field of the blank. Rows are separated by a line break. Each blank contains at least two fields.

**When working with blanks, the System:**

1. Detects fields in the uploaded blank:

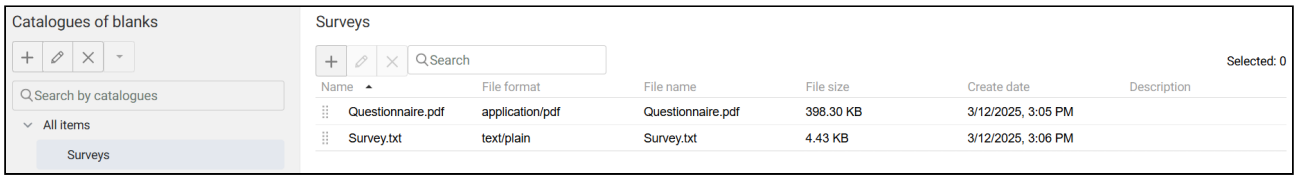
a. Extracts the text.
b. Divides the text into fields.
c. Extracts hashes from the fields, saves their order and quantity.

2. Searches for blank field names in the event text. The text must contain at least one field of the blank.
3. Checks the order of fields. In case there are more than one fields found, they must follow the same order as in the digital fingerprint.
4. If needed, detects whether the blank was filled. For this, it checks if there is text between blank fields. At least one symbol is required between two adjacent lines.

For the System to detect blanks in intercepted data, include it in in a protected object.

**About the section:**

The section contains a hierarchical list of catalogues within which you can create blanks. Further, when creating a protected object, you can add both single blanks and entire catalogues to it.




On the left side of the working area, find tools for operations with catalogues:

- Create, edit, move, delete, import/export a catalogue;
- Search by catalogues.

On the right side of the working area, find:

- List of blanks within the selected catalogue;
- Tools for operations with blanks:
  - Create, edit, delete, move or copy a blank;
  - Perform a cross-cutting search by a blank name. The cross-cutting search is performed within the selected catalogue and enclosed ones. To perform the search through all the section's catalogues, select the root catalogue.

When editing a blank, you can:

- Configure detection conditions, which define the quotation threshold and minimal sufficient number of filled fields;
- Update the blank.

**User's actions:**

- Create blanks and their catalogues, see *Managing Blanks*;
- Import and export blanks as a part of the technologies base, see *Exporting and Importing the Technologies Database*;
- Update a blank, see *Managing Blanks*;
- Add blanks to protected objects, see *Creating Protected Object*.

## 3.4.5 Stamps

**Reference information:**

The **stamp** is a stamp image that Traffic Monitor searches for when analyzing interception objects. Stamps can be images of round or triangular impressions used in organizations.

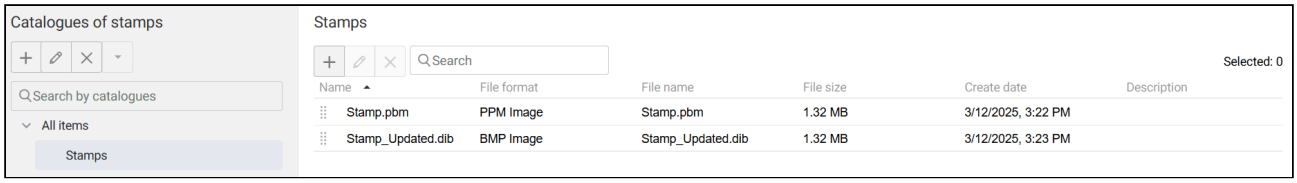
Unlike detection conditions for sample images, detection conditions for stamps are less strict, because stamps can:

- Be overlapped by text (by up to 50%);
- Be turned at different angles;
- Have different brightness level or background colour.

**To use the technology**, include the stamp in protected object. See *Managing Protected Objects*.

**About the section:**

The section contains a hierarchical list of catalogues within which you can create stamps. Further, when creating a protected object, you can add both single stamps and entire catalogues to it.




On the left side of the working area, find tools for operations with catalogues:

- Create, edit, move, delete, import/export a catalogue;
- Search by catalogues.

On the right side of the working area, find:

- List of stamps within the selected catalogue;
- Tools for operations with stamps:
  - Create, edit, move, copy or delete a stamp;
  - Perform a cross-cutting search by a stamp name. The cross-cutting search is performed within the selected catalogue and enclosed ones. To perform the search through all the section's catalogues, select the root catalogue.

**User's actions:**

- Create stamps and their catalogues, see *Managing Stamps*;
- Add stamps to protected objects, see *Creating a Protected Object*;
- Import and export stamps as a part of the technologies base, see *Exporting and Importing the Base of Technologies*.

## 3.4.6 Database Unloadings

**Reference information:**

The technology enables you to search for data of a certain template in analyzed texts. For this, the technology uses ***database unloadings***, that is structured data represented as a table and preloaded into Traffic Monitor. Database unloadings can be lists of salaries, personal data, and so on.

**How the technology works:**

After you upload the unloading to the System, the technology generates a reference unloading. It:

1. Divides an uploaded table into rows, rows into cells, cells into words.
2. Deletes stop words to prevent false positives: digits, letters and words, which do not trigger the technology. See *Stop Words List for Sample Database Unloadings* article.
3. Creates a *digital fingerprint* from the rest of the words. Thus, the unloading is stored in encrypted form.

When analyzing intercepted data, the System detects a cell:

- Only if the extracted text contains all words from the reference cell. If the set of words inside the cell is less than that in the reference, the cell is not detected. For example, when *Peter James Johnson* is the reference and the transmitted file has *Peter Johnson.*
- Even if the word order of a cell differs from the word order of the reference. For example, if *Peter James Johnson* is the reference and the transmitted file has *John, Peter James*.
- Even if a cell of a transmitted file contains other words, which are not present in the reference. For example, if *Peter James Johnson* is the reference and the transmitted file has *John, Peter James; the manager* or *manager, Peter James Johnson*.

The technology operation also depends on a search type and minimal number of rows to trigger the condition. For details, see *Detection Conditions for Unloading*.

**Additional features:**

- *Automatic recipient validation*
  Traffic Monitor can use database unloadings to control sending data by email. The System checks whether the data recipient matches the key (data owner's email) specified in the unloading. If the values do not match, Traffic Monitor creates an event with violation and highlights the protected data in it.In the "Blocking" transport mode (the in-line mode), Traffic Monitor allows you to block sending emails with protected data or send them to quarantine.
- *Detection of data in different formats*
  With the technology, the System can detect mobile phone, bank card, and bank account numbers written in a format different from the one specified in the unloading. For example, if the unloading contains a number written as `79121234567`, in the intercepted data the System detects formats like + `7(912)1234567`, `89121234567`, `+7 912 123-45-67`, and so on.

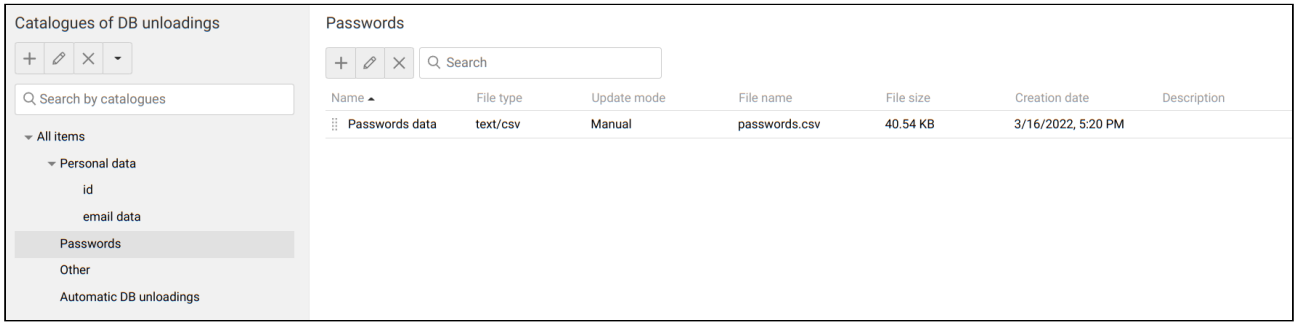
**To use Database Unloadings technology:**

- Prepare an unloading file before uploading it to Traffic Monitor. See *Recommendations on Preparing Unloadings*.
- Include the unloading to a protected object. See the *Managing Protected Objects* section.
- If needed, enable automatic recipient validation (disabled by default). See *InfoWatch Traffic Monitor. Administration Guide. Using a database unloading for automatic recipient validation*.

**About the section:**

The section **Database Unloadings** contains a hierarchical list of catalogues within which you can create unloadings. Further, when creating a protected object, you can add separate unloadings as well as entire catalogues to it. See *Adding Elements of Technologies*.

The preinstalled *Automatic DB unloadings* catalogue contains unloadings received from an external system. You cannot delete this catalogue. For details, see *Automatically Updated Database Unloadings*.




On the left side of the working area, you can see the tools for operations with unloading catalogues:

- Create, edit, move, delete, or import/export a catalogue.
- Search by catalogues.

On the right side of the working area, you can see the:

- List of unloadings within the selected catalogue.
- Tools for operations with unloadings:
  - Create, edit, move, delete, or copy an unloading.
  - Perform a cross-cutting search by unloading name. The cross-cutting search is performed within the selected catalogue or enclosed ones. To perform the search through all the section's catalogues, select the root catalogue.

In the edit mode, you can:

- Set the detection conditions which define:
  - Logical relationships between table columns.
  - The minimum number of rows from the unloading in the analyzed text that is needed to fulfill the condition.
  - Citation search type in the text.
- Update the unloading – upload a new file. Its data will complement the existing unloading or overwrite it.

**Obsolete unloadings:**

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

- If you import the base of technologies/protected objects from Traffic Monitor version lower than 7.4.
- If you update Traffic Monitor from a version lower than 7.4.

The System uses  symbol to mark obsolete unloadings.

> **Warning!**
>
> An obsolete unloading cannot be edited and updated. We recommend deleting it and creating the unloading again.

**User's actions:**

- Prepare an unloading before loading it into Traffic Monitor. See *Recommendations on Preparing Unloadings*.
- Create database unloadings and their catalogues. See *Managing DB Unloadings*.
- Update the unloading. See *Managing DB Unloadings*.
- Move/copy the unloading. See *Managing DB Unloadings*.
- Add detection conditions for the unloading. See *Detection Conditions for Unloading*.
- Use automatically updated unloadings. See *Automatically Updated Database Unloadings*.
- Add unloadings to protected objects. See *Creating a Protected Object*.

## Detection Conditions for Unloading

**Reference information:**

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

You can specify several (up to 20) detection conditions for the unloading. In this case, one satisfied condition is sufficient to associate the interception object with this unloading.

**Note:**

In case you are using the unloading for automatic recipient validation and/or detection of data in different formats, take into account the *peculiarities of unloadings with keys*.

**Detection condition parameters:**

- **Detection condition:**
  The detection condition contains column numbers and logical relations between them. If the analyzed interception object contains data from specified cells, given the set relations, then this row is considered triggered.
  Logical relations are defined using the following symbols:

| Symbol | Definition | Examples | |
|---|---|---|---|
| | | Condition | Definition |
| **+** | Conjunction of cells (logical "AND") | **1+3+4** | The row is considered to be triggered if its first, third and fourth cells are triggered. |
| **\|** | Disjunction of cells (logical "OR")<br>**Note:** a disjunction condition should be in parentheses | **(1\|5)** | The row is considered to be triggered if its first or fifth cell is triggered. |
| **()** | Condition grouping<br>**Note:** the disjunction symbol cannot be used to divide groups in parentheses. Thus, a condition like **(1+8+11*)\|(2+3*)** should be specified as two separate conditions: **1+8+11*** and **2+3***. | **1+(2\|3)** | The row is considered to be triggered if the following is triggered:<br>• its first cell<br>and<br>• either its second or its third cell. |
| | | **(1\|3)+(5\|4)** | The row is considered to be triggered if the following is triggered:<br>• its first or third cell<br>and<br>• its fifth or forth cell. |
| ***** | Considering blank cells | **1+2*+3** | If the second cell is unfilled, the System ignores it during the analysis. In this case, the condition is equivalent to the condition **1+3**.<br>If the second cell is filled, the System involves it in the analysis |

| Symbol | Definition | Examples | |
|---|---|---|---|
| | | Condition | Definition |
| | | | and the condition is equivalent to the condition **1+2+3**. |

Default detection condition: *1+2+...+N*, where N is the number of unloading columns.

> **Note:**
>
> The technology does not consider special characters, so if the column contains an email address, specify an additional column (such as "Full name") in order to reduce false positives.

- **Minimal quantity of rows:**
  The minimal number of rows that must be detected to trigger the condition. For example, if a condition like **1+(2|3)** is specified and the minimal quantity of rows is set to **10**, then for triggering the condition the analyzed text should contain at least **10** different rows that satisfy the condition **1+(2|3)**.

  Default minimal quantity of rows: *10*. If an unloading contains less than 10 rows, the value of the parameter will be equal to the number of rows in the unloading.
- **Search type:**
  The parameter defines the type of citation search. It also defines the features of highlighting detected rows in the detailed event view form.
  Available search types:

| Search type | Description | Example | |
|---|---|---|---|
| | | Reference cell | Detected data in intercepted file |
| *All words in one cell in any order with any distance between* | The System detects a cell even if the words from it are spread throughout the extracted text.<br>Used in the default condition.<br>When the conditions are triggered, all detected rows will be highlighted in the detailed event view form in attachments, including those that | ***+7 (846) 979-78-00*** | ***7** example **846** of **979** intercepted **78** text **00*** |

| Search type | Description | Example | |
|---|---|---|---|
| | | Reference cell | Detected data in intercepted file |
| | repeat within the same attachment. | ***Peter Johnson*** | *+**7 (846) 979-78-00*** |
| *All words in one cell following each other in the exact order* | The System detects a cell only if the words from it follow each other. The order is specified.<br>When using this type, the System does not delete stop words from an unloading.<br>When the conditions are triggered, all detected rows will be highlighted in the detailed event view form in attachments, including those that repeat within the same attachment. | ***+7 (846) 979 -78-00*** | *+**7 (846) 979-78-00*** |
| | | | ***+7 (846) 979 78 00*** |
| | | | *+**7.(846).979.78.00*** |
| | | | ***7 846 979 78 00*** |
| | | ***Peter Johnson*** | *sales manager **Peter Johnson*** |
| | | | ***Peter, Johnson*** |

<table>
<tr><th rowspan="2">Search type</th><th rowspan="2">Description</th><th colspan="2">Example</th></tr>
<tr><th>Reference cell</th><th>Detected data in intercepted file</th></tr>
<tr><td rowspan="6">All words in one cell following each other in any order</td><td rowspan="6">The System detects a cell only if the words from it follow each other. The order does not matter.<br>When using this type:<ul><li>The System does not delete stop words from an unloading;</li><li>Text analysis stops if the detection condition is satisfied. In the event text, the System highlights only those fragments that it had detected before the condition was satisfied;</li><li>Speed of text analysis may decrease</li></ul>When conditions are triggered, only unique rows will be highlighted in each attachment in the detailed event view form. Rows that repeat within the attachment will not be highlighted.</td><td rowspan="4">+7 (846) 979-78-00</td><td>+7 (846) 979-78-00</td></tr>
<tr><td>+7 846 979 78 00</td></tr>
<tr><td>7 979 846 78 00</td></tr>
<tr><td>00 78 979 846 7</td></tr>
<tr><td rowspan="2">Peter Johnson</td><td>sales manager Johnson, Peter M.</td></tr>
<tr><td>Johnson, Peter</td></tr>
</table>

**Примечание:**

If the unloading has cells with the same values, then the technology can detect these cells in the same text fragment.

**Peculiarities of detection conditions for unloadings with keys**

If you use the unloading for automatic recipient validation and/or detection of data in different formats:

- In the **Minimum quantity** of rows field, enter *1* as one key corresponds to data of one row.
- In the **Search type** field, specify *All words in one cell following each other in any order* search type for better System operation.
- In the **Detection condition** field, do not specify the last column with keys in the detection condition.

**Detection condition examples**

- **Example 1:**
  You need the System to mark the interception object as phone numbers when detecting 5 or more rows with filled columns *1* and *3* from the table with the following structure:

| Full name | City | Phone number |
|---|---|---|
| *John Smith* | *London* | *+0 (012) 345-67-89* |
| *Tom Johns* | *Moscow* | *+0 (012) 345-67-88* |
| *William Williams* | *Los Angeles* | *+0 (012) 345-67-87* |
| *Jane Green* | *New York City* | *+0 (012) 345-67-86* |
| *Jillian Taylor* | *London* | *+0 (012) 345-67-85* |
| *Michael Davis* | *Dublin* | *+0 (012) 345-67-84* |

  It is also necessary that the words from the cell follow each other in the text:

  - The text "***John** Taylor, Tom **Smith***" should not be marked as containing the words from the cell "***John Smith***".
  - The text "***+0 (012) 345**-00-00, +0 (000) 000-**67-89***" should not be marked as containing the words from the cell "***+0 (012) 345-67-89***".

  > **Note:**
  >
  > A word is defined as any sequence of letters or numbers.

  To create a protected object according to the requirements above:

  a. Save the table in CSV or TSV format and upload this file to the System.
  b. Configure the detection condition:
     - In the **Minimal quantity of rows** field, specify *5.*
     - In the **Search type field**, specify *All words in one cell following each other in any order.*
     - In the **Detection condition** field, specify *1+3*.
  c. Create a *protected object* *PHONE_NUMBERS* based on the created database unloading.
  d. Apply the configuration.

  When detecting specified data columns in the transferred traffic, *PHONE_NUMBERS* protected object is triggered in the System.

- **Example 2:**
  The unloading contains the following data:

| Full name | City | Phone number | Card number | Email address |
|---|---|---|---|---|
| *John Smith* | *London* | *+0 (012) 345-67-89* | *4561352115347682* | *j.smith@example.com* |
| *Tom Johns* | *Moscow* | *+0 (012) 345-67-88* | *5212608941790399* | *t.johns@example.com* |
| *William Williams* | *Los Angeles* | *+0 (012) 345-67-87* | *4869196835902098* | *w.williams@example.com* |
| *Jane Green* | *New York City* | *+0 (012) 345-67-86* | *4529196433932047* | *j.green@example.com* |
| *Jillian Taylor* | *London* | *+0 (012) 345-67-85* | *4869196835902097* | *j.taylor@example.com* |
| *Michael Davis* | *Dublin* | *+0 (012) 345-67-84* | *5314602942712364* | *m.davis@example.com* |

You need the System to create an event with violation if data from the unloading is sent to a recipient who is not specified in the row key. The System must detect a violation if the email contains:

- Full name and phone number
  or
- Full name and card number

To do this:

a. Enable automatic recipient validation. By default, the functionality is disabled. To learn how to enable the functionality, see the *InfoWatch Traffic Monitor. Administration Guide* document, *Using a database unloading for automatic recipient validation*.
b. Save the table as CSV or TSV (requirements for unloadings are listed in the *Recommendations on Preparing Unloadings* article).
c. Add the first code line: `DB Table with Row keys` and 4 tabs to the unloading. After you add the code line, the System will consider the values of the **Email address** column as keys and use them to validate recipients.
d. Upload the unloading file into the System.
e. Set up the detection condition:
   - In the **Minimum quantity of rows** field, enter *1*.
   - In the **Search type** field, select *All words in one cell following each other in any order.*
   - In the **Detection condition** field, enter *1+(3|4)*.
f. Create a *protected object* based on the created database unloading.
g. Apply the configuration.

When a person sends an email with data from the specified columns to a recipient who is not listed in the row key, Traffic Monitor will create an event with violation. In the event, you can see the number of detected unique rows from the unloading. Detected protected data will be highlighted.

## Automatically Updated Database Unloadings

***Automatically updated database unloadings*** are unloadings created by an external system. An external system (a connector) initiates addition and subsequent update of automatic unloadings.

Traffic Monitor places unloadings generated by an external system in a preinstalled catalogue named **Automatic DB unloadings**.

**To work with automatically updated unloadings, you have to:**

- Upload the plugin to Traffic Monitor, so that an external system can authorize in Traffic Monitor. See *InfoWatch Traffic Monitor. Administration Guide* for details;
- Upload the license to Traffic Monitor, so that you can view and edit **Automatic DB unloadings** catalogue;
- Include the unloading to a protected object. See *Managing Protected Objects* for details.

Traffic Monitor generates **attributes of the unloading** based on the data received from an external system:

- **Name** of the database unloading;
- **Columns**, representing the list of columns that the System uses to generate a default detection condition. See *Detection Conditions for Unloading*;
- **Note**.

> **Note:**
>
> When you create an unloading, its file can be empty if:
>
> - Loading the contents ended with a force quit;
> - Connection was lost while loading the contents;
> - Validation of the contents failed.
>
> When the System operation is restored, then, if the System contains an empty unloading, an external application can use this unloading and fill it with new contents without creating a new unloading.

**Operations with automatic unloadings**

You can edit or delete any unloading in the catalogue. For this, use the buttons on the toolbar on the right side of the working area.

The following operations are unavailable:

- Editing or updating an obsolete automatic unloading. We recommend deleting it and creating the unloading again.
- Updating an automatic unloading manually in Traffic Monitor console;
- Updating an unloading automatically if the unloading was deleted.

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

## 3.4.7 Graphical Objects

**Reference information:**

***Graphical objects*** are a complex of technologies for analyzing images or other graphic data extracted from the object body or its attachments.

There are two types of graphical objects in the System, which are based on two different technologies:

- *Graphical classifier*, which learns on the collection of images and their categories. During training, the classifier extracts text features from a collection of images with specified category tags, in order to use the features to automatically attribute images to the categories;
- *Image search within an image*. The System contains preinstalled images as samples.

Below are the types of graphical objects which the System classifies using one of the two technologies:

| Graphical classifier | Image search within an image |
|---|---|
| Standard English license:<br>• *Internal Passport of the Russian Federation*<br>• *Technical drawings*<br>• *Certificates*<br>• *Faces*<br>• *Photos*<br>• *Stamp scans*<br>• *Icons*<br>• *Logos*<br>• *Decreasing false-positives*<br>Other license types:<br>• *Geographic maps*<br>• *Military identity card*<br>• *Transborder passport of a citizen of the Russian Federation*<br>• *Individual insurance account number (SNILS)*<br>• *Passport of a citizen of the Republic of Belarus*<br>• *Water supply schemes* | Standard English license:<br>• *Credit card*: front side image of a VISA, Visa Electron, MasterCard, Maestro or Mir credit card<br>Standard Malaysian license:<br>• *Identification card of a citizen of Malaysia*, i.e. a group of identification documents of the citizens of Malaysia, including:<br>• *MyKad*, a general card for citizens of Malaysia over 12 years old (front side)<br>• *MyKid*, a card for children under 12 (front side)<br>• *MyPR*, a card for residents of Malaysia who received a residence permit (front side)<br>• *MyTentera*, a card for those who serve in the army (front side) |

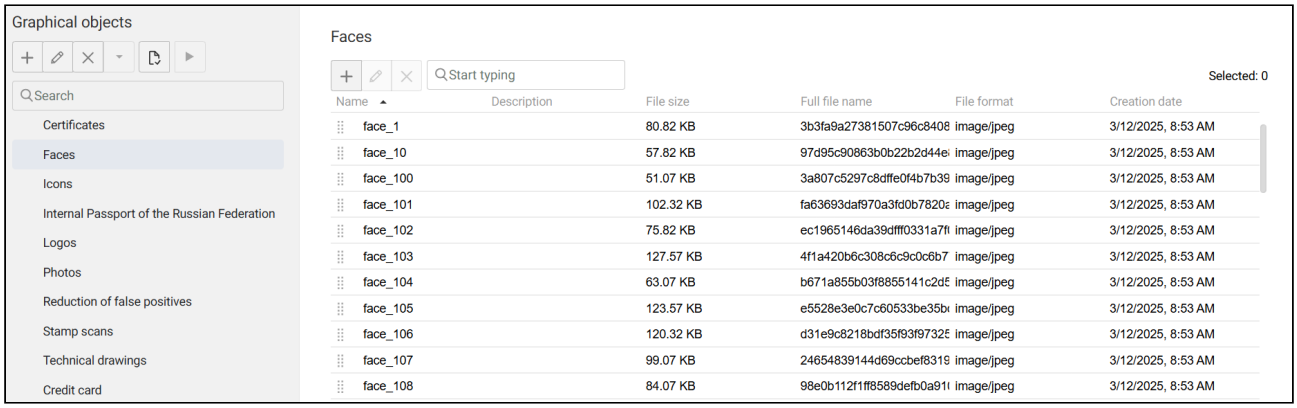
If necessary, you can train the automatic classifier to detect other image types.

You cannot edit categories used for image search within an image.

**For graphic objects to be detected in intercepted data**, include the categories in protected objects. See *Creating a Protected Object*.

**About the section:**

Graphical objects consist of categories which contain documents.




On the left side of the working area, find tools for operations with categories:

- Create, edit, move, delete, import/export a category;
- Check to which category the technology will attribute a sample graphical object;
- Train the classifier;
- Search by categories.

On the right side of the working area, find:

- List of objects within the selected category;
- Tools for operations with graphical objects:
    - Create, edit, move or delete an object;
    - Perform a cross-cutting search by object name. The cross-cutting search is performed within the selected category and enclosed ones. To perform the search through all the section's categories, select the root category.

**User's actions:**

- Create categories, *Managing Graphical Objects*;
- Add documents, *Managing Graphical Objects*;
- Train the classifier, *Managing Graphical Objects*;
- Check files with the classifier, *Managing Graphical Objects*;
- Import and export protected objects as a part of the base of technologies, *Exporting and Importing the Base of Technologies*;
- Add graphical objects to a protected object, see *Creating a Protected Object*.

## 3.4.8 Autolinguist

**General information:**

***Autolinguist*** is an automatic text classifier. Like *Categories and terms* technology, Autolinguist attributes a text to a certain category. However, instead of a set of key terms, the technology uses machine learning classification algorithms. During training, Autolinguist extracts text features from a collection of texts with specified category tags, in order to use the features to automatically attribute documents to the categories.

Autolinguist is pretrained on a collection of texts within preinstalled categories:

- *Accounting*;
- *Asset purchase*;
- *Business estimate*;
- *Contacts*;
- *Credits*;
- *CV*;
- *HR*;

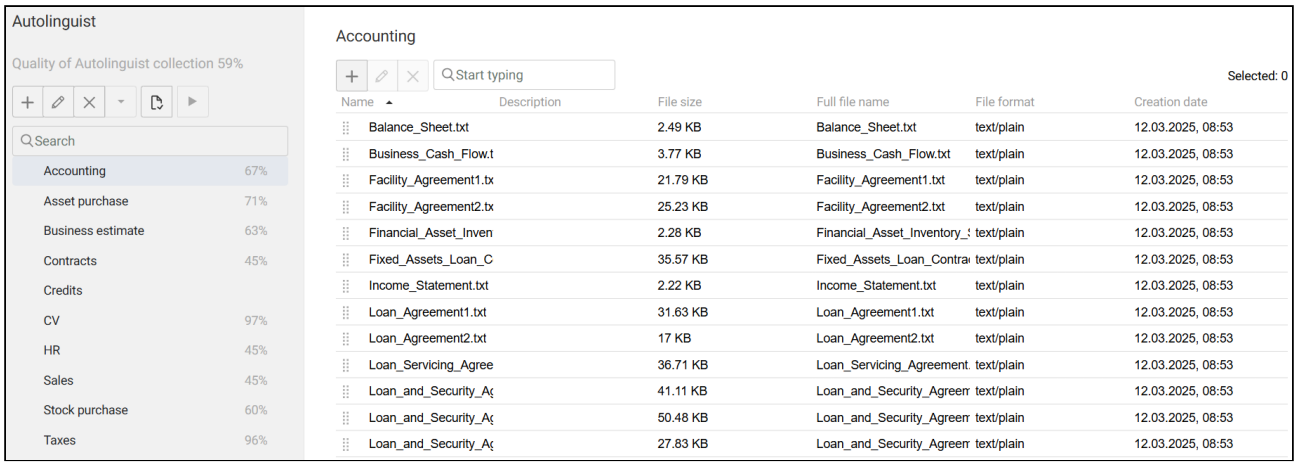
- *Sales*;
- *Stock purchase*;
- *Taxes*.

You can retrain Autolinguist by adding new documents to existing categories and/or creating new categories.

**In order to use the technology**, include categories in protected object. See *Managing Protected Objects*.

**About the section:**

The section contains a list of categories. By clicking a category, you can view the list of documents it includes.




On the left side of the working area, find tools for operations with categories:

- Create, edit, move, delete, import/export a category;
- Check to which category the technology will attribute a sample text;
- Train Autolinguist;
- Search by categories.

On the right side of the working area, find:

- List of documents within the selected category;
- Tools for operations with documents:
  - Create, edit, move or delete a document;
  - Perform a cross-cutting search for a document. The cross-cutting search is performed within the selected category and enclosed ones. To perform the search through all the section's categories, select the root category.

**User's actions:**

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

## 3.5 Protected Objects Section

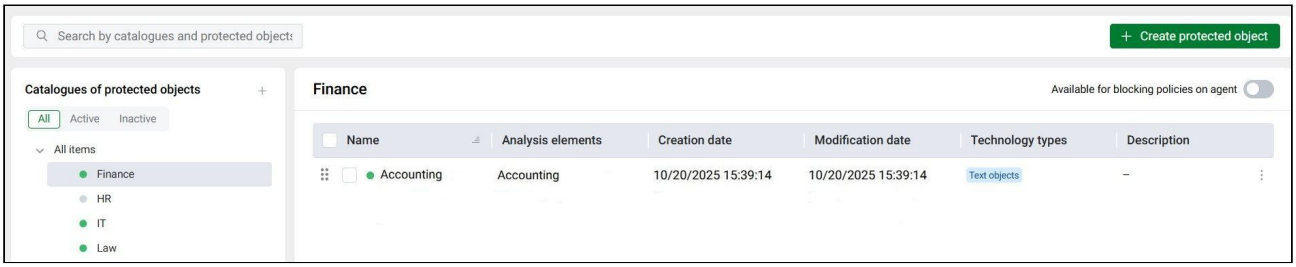
**Reference information:**

The ***protected object*** activates the analysis using the technology. If you add several technologies to the protected object, you need to set up logical conditions between them.

If the technology is not included in any protected object, it does not work during the analysis.

**About the section:**

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




The catalogue list is located in the left part of the workspace and includes both custom and preset protected objects.

The right part of the workspace displays protected objects for the selected catalogue. For each protected object, the following attributes are available:

- its name
- *elements of technologies* included in the protected object
- creation and modification dates
- types of technologies used in the protected object
- description

Each catalogue and each protected object have a status indicator: *Active* or *Inactive*. The catalogue status applies to all nested catalogues and protected objects.

**Filtering**

You can manage which catalogues are displayed based on their activity status. For this, use the buttons above the catalogue list: **All**, **Active**, **Inactive**.

Besides, you can choose whether the System displays all protected objects in the catalogue or only protected objects available for data protection policy on agents. For this, use **Available for blocking policies on agent** toggle above the protected object list.

**Search**

The upper part of the workspace contains a box for cross-cutting search of protected objects and catalogues. The System performs search throughout all catalogues.

Search for a catalogue is performed by its name; search for a protected object is performed by the name of the protected object and the name of technologies elements which are a part of protected object.

When you enter a part of a name into the search box, the drop-down list of the search box displays all relevant protected objects and catalogues. To select a catalogue or protected object, you can right-click it or use keyboard button: *Up*/*Down* and *Enter*.

To view the list of all relevant protected objects, click **View all results** in the drop-down window.

**Adding a comment**

In order to add a comment to a protected object, in the corresponding row click and select **Edit**. In the edit window, enter the comment in **Description** field.

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

**Creating a protected object**

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

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

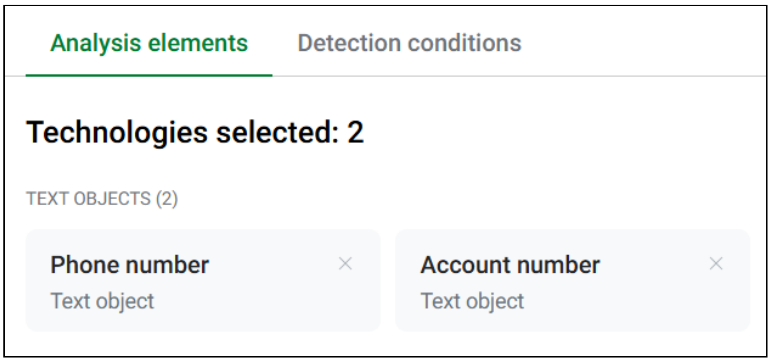
**User's actions:**

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

## 3.5.1 Elements of Technologies

**Reference information:**

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




The **Elements of technologies** tab appears when creating or editing a protected object.

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

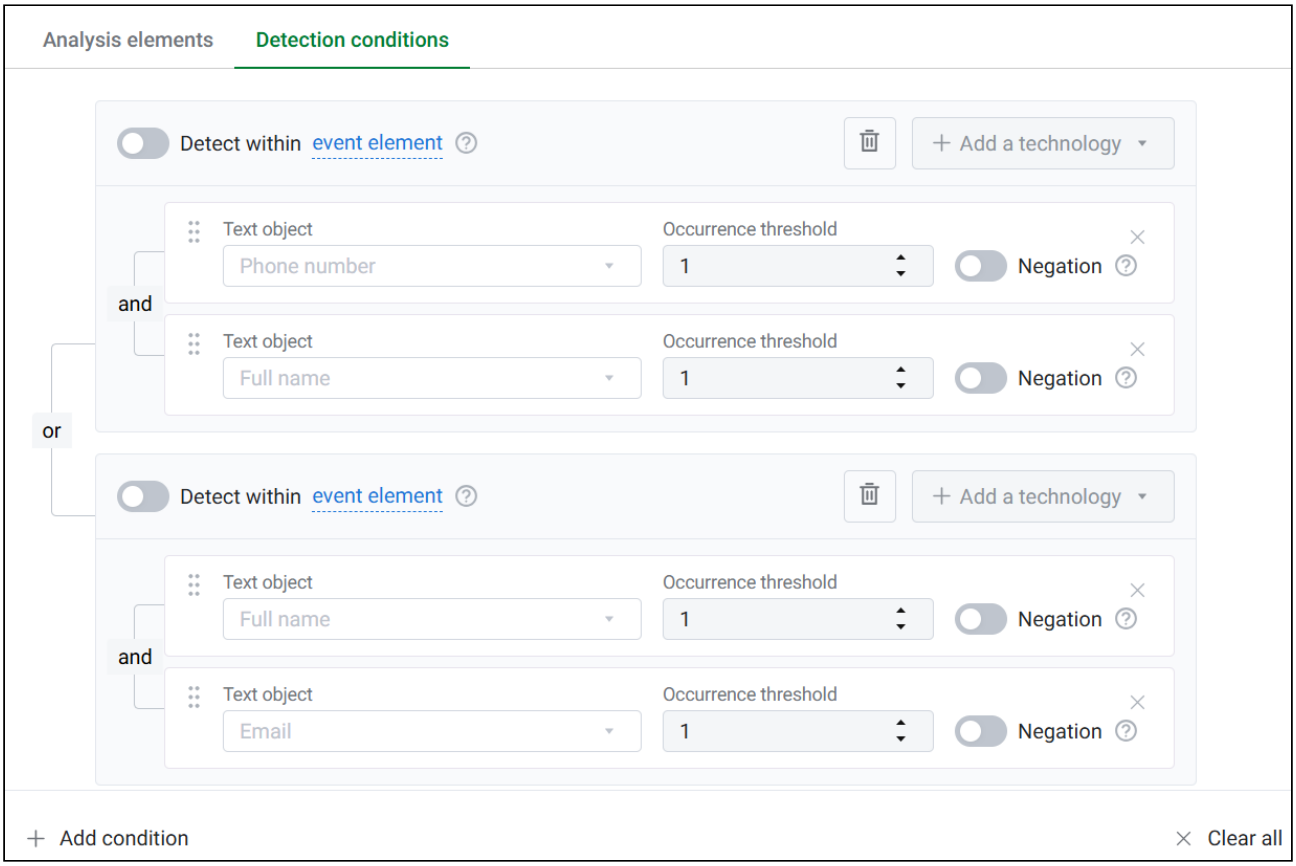
You can specify detection conditions for added elements of technologies on the ***Detection conditions*** tab.

**User's actions:**

- Adding Elements of Technologies.

## 3.5.2 Detection Conditions

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




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

The catalogue can be detected if at least one element which belongs to the catalogue is being detected.

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

Event element is a detected in traffic:

- Email text
- Email subject
- Communication in messenger. All messages in an event are considered one element
- File
- File name

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

**Note:**

At least one element without negation is required in the detection condition.

If protected object is added to the policy of data protection on Agents, you cannot enable detection within the event element.

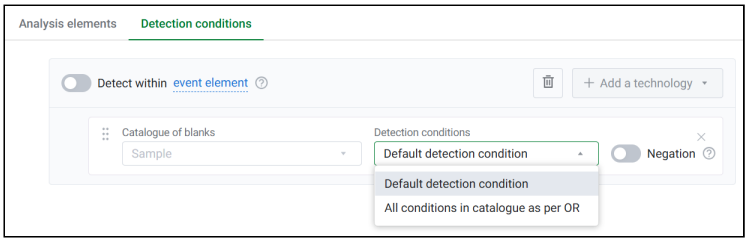
Protected objects with enabled negation are not triggered in case of:

- Device Monitor version 7.9 or earlier
  and/or

- Agents installed on workstations running Linux-family OS.

Detection conditions for the elements of technologies are as follows:

| Element name | Detection condition |
|---|---|
| Sample document | Checks whether the interception object contains a specified sample document |
| Category (Categories and terms) | Checks whether the interception object matches the specified categories. For categories that contain sub-categories, checks if the interception object matches any subcategory |
| Text object | Checks whether the interception object contains a specified text object.<br>Additional detection condition is a occurrence threshold. It determines the least number of times the text object must be present in the interception object. The default value is 1. The maximum value is 20000.<br>Depending on the pattern type, the number of occurrences of the text object is calculated as follows:<br>• If the text object pattern is specified as a regular expression, then one pattern value is counted as one occurrence even if it is detected several times within a document<br>• If the text object pattern is specified as a string, all its occurrences are counted<br>Catalogue also has a quotation threshold defined. Text objects which are a part of this parameter will be detected in accordance with its detection condition. |
| Blank | Checks whether the interception object contains at least one of the specified blanks. Additional detection condition - blank detection condition. It is used when editing the blank and includes the following:<br>• Text data quotation threshold – per cent of matching between intercepted blank and sample one. The default condition value is 70%<br>• Minimum number of filled fields. The default condition value is 3<br>To be detected the intercepted blank should meet **both** conditions above.<br>Always specify one detection condition.<br>In case the technology element is a catalogue of blanks, one of the following conditions should be selected: |

| Element name | Detection condition |
| --- | --- |
| | • **Default detection condition** – the blanks inside the catalogue will have its default conditions applied;<br>• **All conditions in catalogue as per OR** – for each blank within the catalogue, any detection condition from it will be applied.<br> |
| Stamp | Checks whether the interception object contains a specified stamp |
| Graphical object | Checks whether the interception object contains a specified graphical object.<br>Additional detection condition is a occurrence threshold. It determines the least number of times the graphical object must be present in the interception object. The default value is 1. The maximum value is 20000.<br>The detection condition is specified for the entire category.<br>**Note:**<br>Occurrence threshold can not be specified for the following predefined graphical objects:<br>• Credit card<br>• Identification card of a citizen of Malaysia |
| Database unloading | Checks whether the interception object contains a specified unloading. Additional condition is unloading detection. It is *created* during editing of unloading.<br>At least one detection condition should be selected always.<br>In case you've selected DB unloadings catalogue, you should select one as follows:<br>**Default detection condition** – for blanks within the catalogue, its default conditions will be applied.<br>**All conditions in catalogue as per OR** – for each unloading within the catalogue, any its condition will be applied. |
| Category (Autolinguist) | Checks whether the interception object matches the specified category.<br>Additional condition is probability threshold of category membership. Default value is 10%. Available values: 10 to 100%. |

See also: *Elements of technologies*.

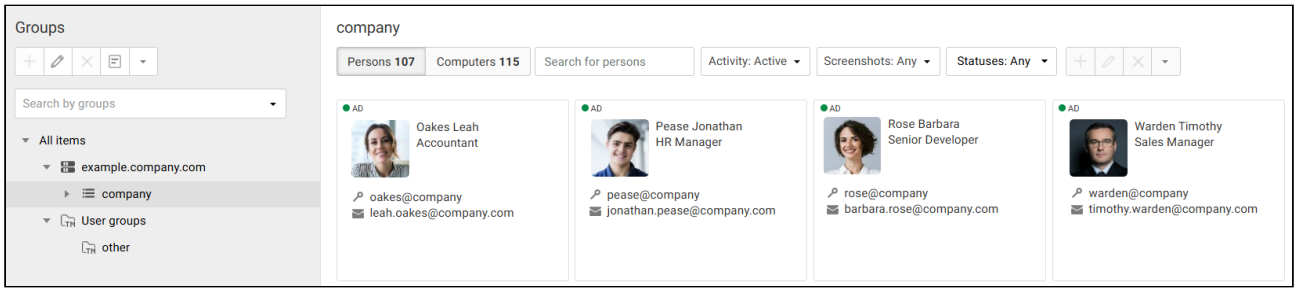
**User's actions:**

- Adding Detection Conditions.

## 3.6 Persons Section

**About the section:**

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




**Groups of persons and computers**

In the left part of the workspace, the System displays groups of persons and computers visible to the current user. See *Visibility Scopes* for details.

You can add groups of persons and computers from an LDAP server or create them in Traffic Monitor, see *Creating Group of Persons or Computers*.

Using tools in the left part of the workspace, you can:

-  – create a user group;
-  – edit a group;
-  – delete a user group;
-  – create a policy for the selected group, see *Creating Person Control Policy*;
-  – export or import groups, persons and computers, see *Exporting and Importing Persons*.

**Persons and computers**

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

For each person/computer, the System displays account data sources as follows:

- **AD** – Active Directory;
- **DD** – Domino Directory;
- **A/F** – Astra Linux Directory, Astra Linux Directory Pro or FreeIPA;
- **SM** – Samba DC;
- **TM** – Traffic Monitor.

Depending on the attributes of a person/computer in the domain catalogue, the System can add domain accounts of the following formats:

- Fully qualified domain name (FQDN): *<sAMAccountName>@<UPN-suffix>*
  Example: *johnson@company.ru*, *paul.pitt@exampledomain.com*
- Short domain name (NetBIOS or DNS): *<sAMAccountName>@<NetBIOS-domain>*
  Example: *johnson@company*, *paul.pitt@ed*

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

> **Important!**
>
> Using * in a search query may negatively affect the search speed in case of a large number of persons loaded from an LDAP-server.

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

- Selecting active/inactive persons and computers (obtained from LDAP);
- Filtering by the presence of screenshots;
- Choosing persons and computers with a specific status (for details, see *Statuses*).

To work with persons and computers within a selected group, use the toolbar in the right part of the workspace.

**User's actions:**

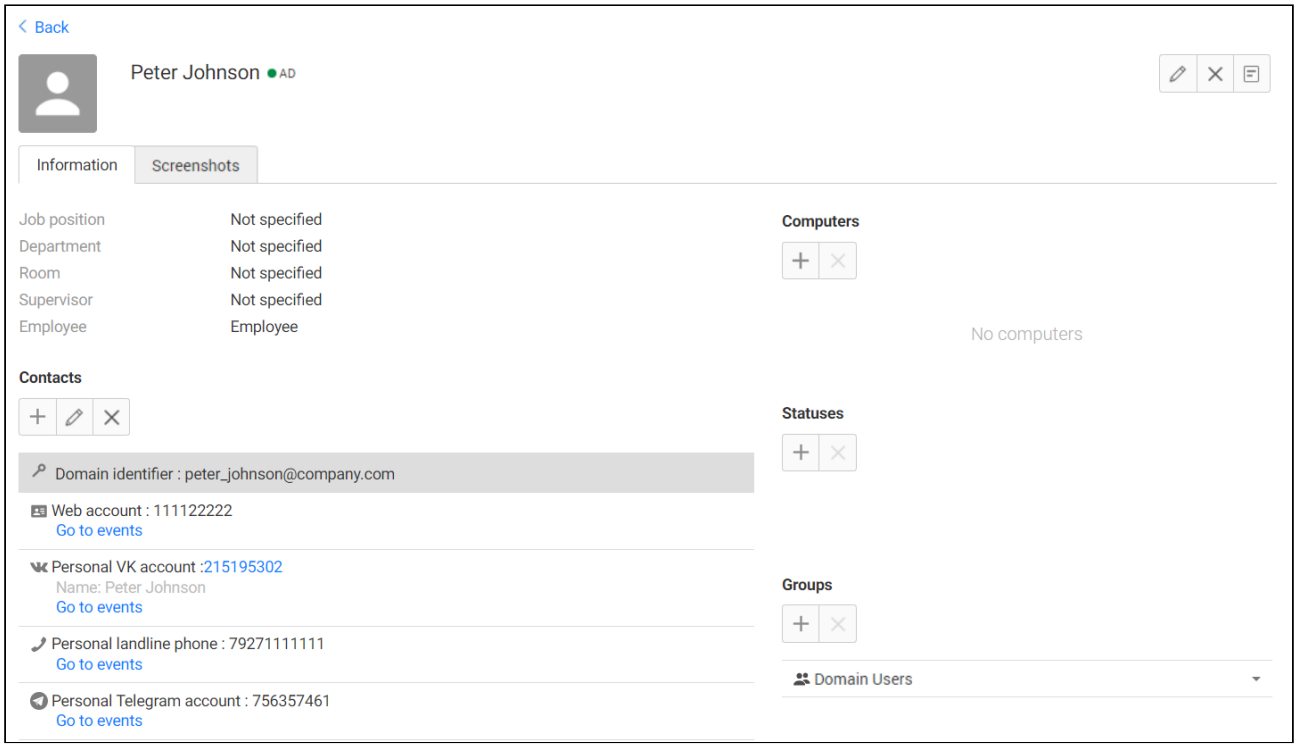
- Creating a group of persons and computers (see *Creating Group of Persons and Computers*);
- Creating a list of persons and computers (see *Creating List of Persons and Computers*);
- Exporting and importing persons (see *Exporting and Importing Persons*);
- Viewing widgets with information on persons and computers (see *Viewing Summary on Violations/Violators*);
- Creating a filter by persons and computers (see *Creating Queries*);
- Creating a policy for persons and computers (see *Creating Person Control Policy*);
- Managing statuses of persons and computers (see *Setting Statuses to Persons and Computers*);
- Viewing screenshots for persons and computers (see *Viewing Screenshots*);
- Adding persons in perimeters (see *Managing Perimeters*).

### 3.6.1 Persons

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

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

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




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

- Job position;
- Department;
- Room;
- Supervisor;
- Employee;
- Contacts (you can specify personal or working contacts of the person including email, phone number, Skype login, ICQ or web address on the Internet, social networks and messengers account);
- Computers (computers linked with the person account);
- Statuses (statuses assigned to the person);
- Groups (groups which include the person).

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

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

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

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

**User's actions:**

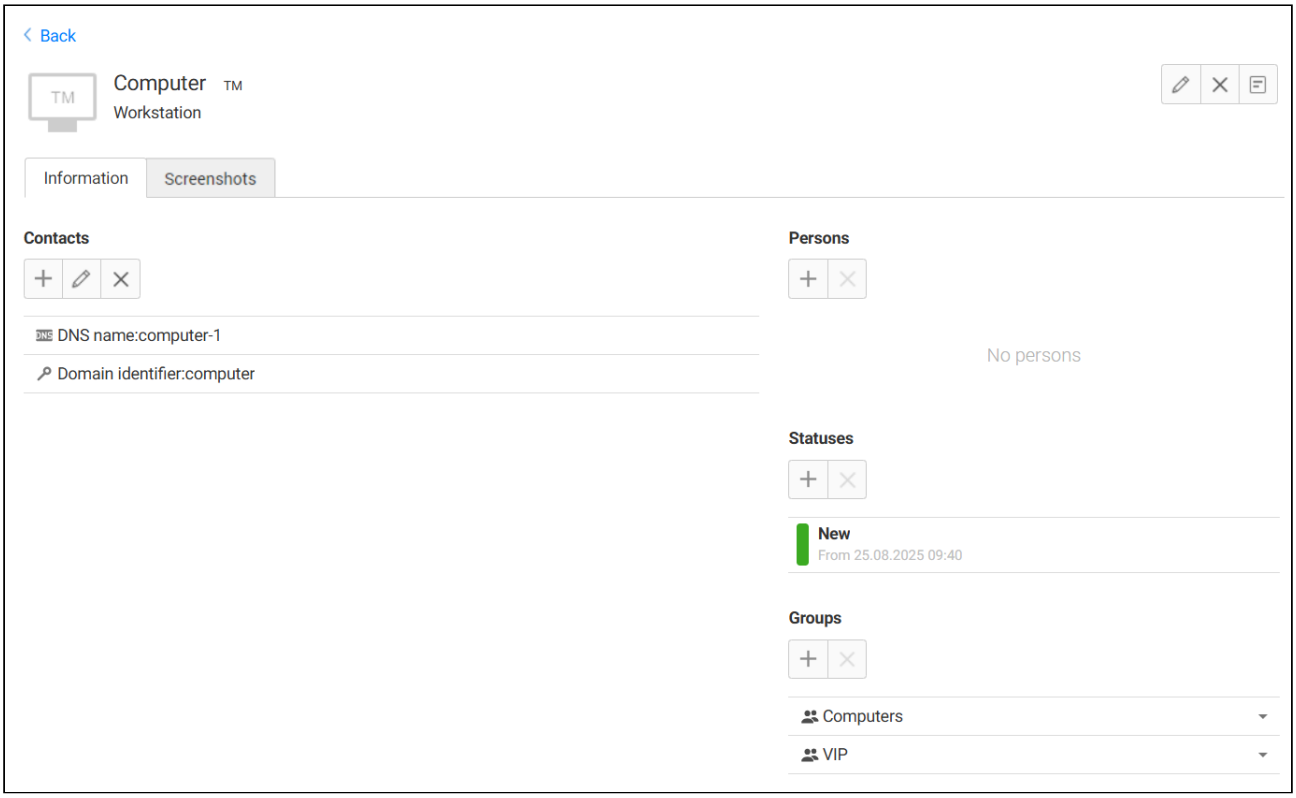
- Creating a filter by persons (see *Creating Queries*);
- Configuring a person card (see *Configuring Person's Card*);
- Creating a policy for persons (see *Creating Person Control Policy*);
- Managing statuses of the person (see *Setting Statuses to Persons and Computers*);
- Added a person to a perimeter (see *Managing Perimeters*);
- Viewing screenshots for a person (see *Viewing Screenshots*);

- Viewing a list of events which involve a certain contact of a person (see *Viewing Events Involving Person's Contact*).

## 3.6.2 Computers

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

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




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

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

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

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

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

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

**User's actions:**

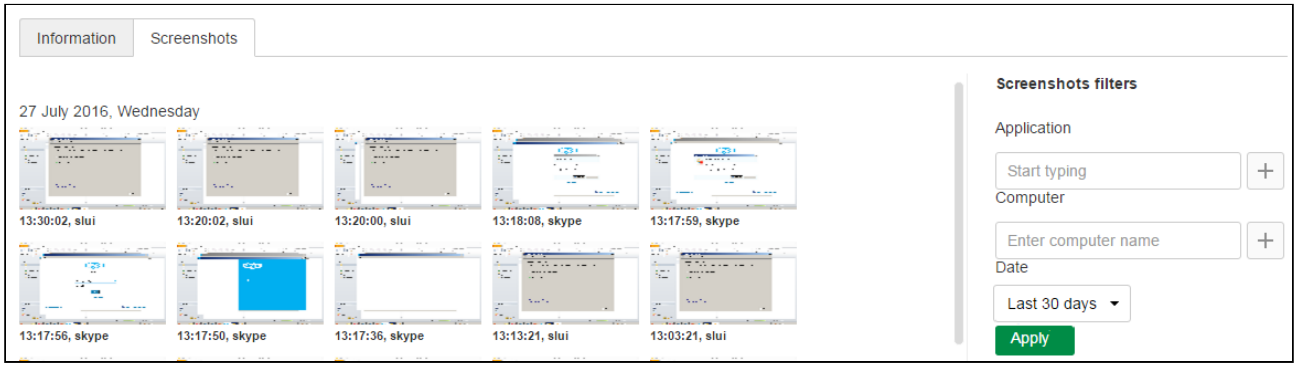
- Managing groups of computers (see *Creating Group of Persons and Computers*);

- Managing computers (see *Creating Persons and Computers*);
- Creating a policy for computers (see *Creating Person Control Policy*);
- Managing computer statuses (see *Setting Statuses to Persons and Computers*);
- Viewing screenshots for a computer (see *Viewing Screenshots*).

### 3.6.3 Screenshots

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

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




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

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

Clicking a screenshot opens its enlarged image and attributes:

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

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

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

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

**User's actions:**

- Viewing Screenshots.

## 3.7 Policies Section

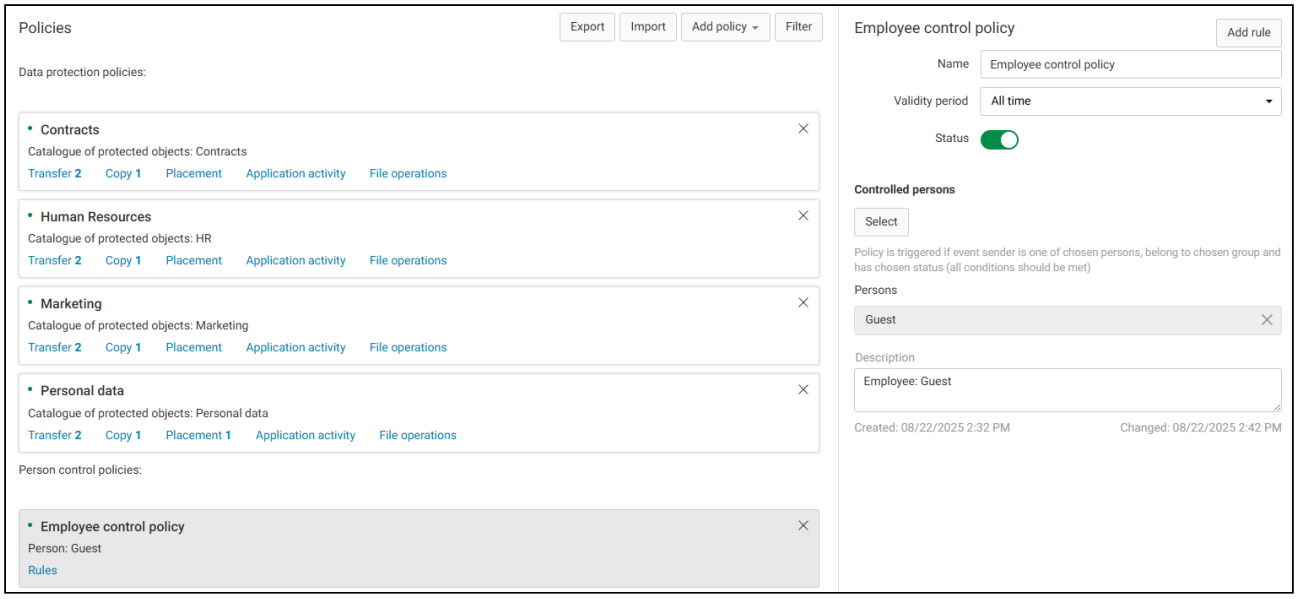
**Reference information:**
***Policies*** are a set of rules according to which analysis and processing of interception objects are performed. The ***rule*** consists of condition sets by which the object is checked and the actions performed when those conditions are fulfilled or not.

**Warning!**

As a result of the analysis, the System will not perform any actions if at least one of the following conditions is met:

- The System has no policies
- All policies existing in the System are disabled
- None of the policies in the System have active rules (or the default actions for active policies are not defined)

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




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

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

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

To transfer policies from one server to another or to back up policies, use the **Export** and the **Import** buttons.

In the policy viewing form, you can:

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

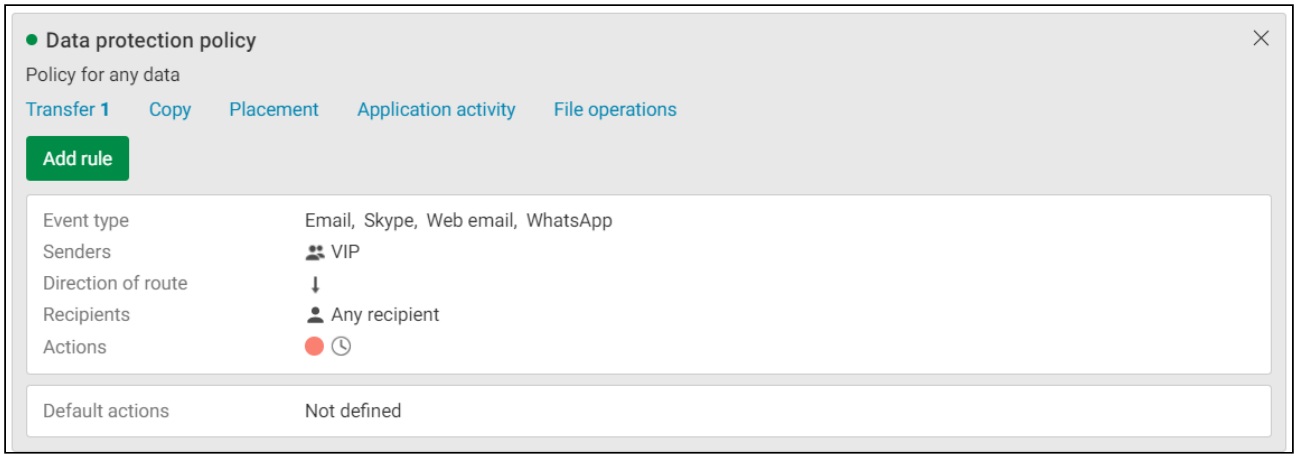
When you click the **Filter** button, in the right part of the workspace, the **Filter settings** area is displayed where you can filter policies by name or by objects of research.

**User's actions:**

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

### 3.7.1 Rules and their Viewing Form

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




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

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

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

- The Rule of Transfer regulates sending and receiving protected data;
- The Rule of Copying regulates copying and printing protected data;
- The Rule of Placement regulates storing protected data;
- The Application Activity Rule regulates clipboard usage and keyboard input;
- The File Operations Rule regulates if applications can read a file or write to it.

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

- Rule of Transfer;
- Rule of Copying;
- Application Activity Rule.

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

When entering text in *Senders* or *Recipients* search box, you will be prompted with a contact, group, person or perimeter initiating data transfer or receiving the task. You can also specify *Senders* and *Recipients* parameters in a separate window by pressing  on the right to the search box.

All the parameters are listed in the table:

<table>
<tr><th>Parameter</th><th colspan="2">Description</th></tr>
<tr><td rowspan="13">Contacts</td><td colspan="2">Specify contacts of the traffic senders/recipients. For this, in the first drop-down list on the left, select the contact type:</td></tr>
<tr><td>Contact type</td><td>Contact format</td></tr>
<tr><td>ICQ</td><td>Integer number from 1000 to 9999999999</td></tr>
<tr><td>Skype</td><td>String from two to 32 characters long, must begin with a letter; may contain only letters, digits, and the characters ".", ",", "-", "_"</td></tr>
<tr><td>Facebook account</td><td rowspan="8">String of one or more characters</td></tr>
<tr><td>Telegram account</td></tr>
<tr><td>WhatsApp account</td></tr>
<tr><td>VK account</td></tr>
<tr><td>YandexID contact</td></tr>
<tr><td>Azure AD account (if the adapter is installed)</td></tr>
<tr><td>Web account</td></tr>
<tr><td>Lotus email</td></tr>
<tr><td>Mobile phone</td><td rowspan="2">String of 3 or more characters, can contain only digits, space, and the characters: "-","_", "( )","+","."</td></tr>
<tr><td>Landline phone</td></tr>
<tr><td>Email</td><td>Address in RFC format</td></tr>
<tr><td>Groups</td><td colspan="2">Specify groups whose members can be traffic senders/recipients</td></tr>
<tr><td>Persons</td><td colspan="2">Specify persons who can be traffic senders/recipients</td></tr>
<tr><td>Domains</td><td colspan="2">Specify domains whose members can be traffic senders/recipients</td></tr>
</table>

| Parameter | Description |
|---|---|
| Perimeters | Specify perimeters whose elements can be traffic senders/recipients |

*Person Control Rule* regulates actions of selected persons. They also allow you to apply existing data protection policies and data protection policies on agents to selected persons.

**Note:**

The logic of applying policies in view of the attributes specified in the rule:

- By default, all attributes are checked for equality with specified values (the parameter  near the attribute's name). The policy wil be applied to events whose parameters have specified values;
- If no value is specified for an attribute, the policy applies to all events that match the rule by other parameters;
- To prevent the policy from applying to events whose attributes have specific values, use negation  for these attributes.

**User's actions:**

- Adding rules to the policy (see *Creating Rules*).

## Rule of Transfer

For the transfer rule, the following parameters are specified:

- **Direction of route**. Possible values:
  - **In single direction** – the rule is triggered only when traffic is passed from senders to recipients
  - **In both directions** – the rule is triggered when traffic is passed both from senders to recipients and from recipients to senders
- **Event type** – the type of traffic passing which triggers the rule. Possible values:
  - **Internet activity**
    *- Web message*
  - **Messenger** (for data protection policies only)
    *- MS Lync*
    *- ICQ*
    *- Skype*
    *- Telegram*
    *- MS Teams* (if the adapter is installed)
    *- XMPP*
    *- Facebook*
    *- WhatsApp*

- *Vkontakte*
- *Yandex messenger*
- *Kribrum*

- **Mail**
  - *Email*
  - *Web email*

- **Computers** – computers from which data has been sent. To add a computer, enter its name in the field, or click  and select the required computer from the list
- **Senders** – if persons or computers from this list send traffic (or traffic leaves specified domains and perimeters), it triggers the rule
- **Recipients** – if persons, computers, domains or perimeters from this list receive traffic, it triggers the rule

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

- **Rule validity days**
- **Rule validity time**

> **Important!**
>
> Selected conditions are joined by logical "AND". Within the same condition, values are joined in the following way:
>
> - By logical "OR" if equality to the attribute is selected
> - By logical "AND" if negation is applied to the attribute

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

**User's actions:**

- Creating Rule;
- Configuring Notifications in Rules.

### Rule of Copying

For the copy rule, the following parameters are specified:

- **Route direction**. Possible values:
  - **One way direction** – the rule is triggered when traffic is sent from sender to recipient
  - **Both ways direction** – the rule is activated when traffic is sent from sender to recipient and from recipient to sender

- **Event type** - the type of traffic copying which triggers the rule. Possible values:
  - **Files exchange**
    - *Removable device*
    - *FTP*
    - *Cloud storage*
    - *Network resource*
    - *Terminal session*

    > **Note:**
    >
    > The *Terminal session* type is not supported on Device Monitor Agents installed on Linux-based workstations.

  - **Printer and MFD** (for data protection policies only)
    - *Print*
- **Computers**

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

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

  > **Warning!**
  >
  > The type of the **Path to file or address** attribute value for the "Terminal session" copy receiver depends on the Traffic Monitor version. The attribute value types are different in the events of file exchange via terminal session:
  >
  > - **For events created in Traffic Monitor version below 7.5**: the attribute contains the name of the copied file, for example: `file.txt`
  > - **For events created in Traffic Monitor version 7.5 and above**: the attribute contains the IP address of the device that was used to remotely connect to the employee's workstation and to which the file was copied, for example: `192.0.2.0`
  >
  > To ensure that policies work correctly for the events created in Traffic Monitor version 7.5 and above, it is recommended to edit existing copy rules in policies. Existing copy rules must be edited if they use an obsolete type of the **Path to file or address** attribute value for *Terminal session* copy receiver. If a file name is specified in this attribute in the rule, the rule will not work correctly with the new events, because new events have an IP address in this attribute.

- **Copy source**;

  > **Note:**

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

- **Rule validity days**
- **Rule validity time**
- **Terminal name** – the name of the device that was used to remotely connect to the employee's workstation. The attribute is specified for the *Terminal session* copy receiver in the events of file exchange via terminal session.
  The values can be specified using wildcards:
  - "?" – to replace a single character in the beginning or at the end of the string;
  - "*" – to replace any number of characters in the beginning or at the end of the string.

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

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

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

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

**User's actions:**

- Creating Rules
- Configuring Notifications in Rules

### Rule of Placement

For the placement rule, the following parameters are specified:

- **Event type** – the type of traffic placement of which triggers the rule. Possible values:
  - **Data Discovery**

- **Storage** – storing secured data in these storages triggers the rule. To specify a storage, click  and in the dialogue box that opens click the required tab:
  - **Computers**. The tab displays computers received from LDAP. Select checkboxes next to required computers.
  - **Network resources.** To add a new network resource, enter the following values in the field:
    - In the **Enter network resource** field, enter IP address or the full DNS name of the host.
    - In the **Enter path** field, enter a host path. Formats:
      - For SMB hosts: `share/folder`, where `share` is the name of the resource;
      - For SSH hosts: `/home/folder`;
      - For SharePoint hosts: `path/lib/folder`, where `path` is the path to the site with the document library and `lib` is the document library.
- **File storages**. To add SharePoint file storage, enter the following values in the fields:
  - In the **Enter server** field, enter IP address or the full DNS name of the file storage.
  - In the **Enter path** field, enter the path to the storage in the following format: `<directory>/<subdirectory>` (do not use group symbols `?` and `*`). Example: `Lib/Project documentation`.

> **Note:**
>
> Conditions on the **File storages** tab are not used for events received from Data Discovery.

Once you have specified all required storages, click **Save**.

- **File owners** – the rule is triggered when specified persons, groups or perimeters are detected among file owners.
- **Who has access to file** – the rule is triggered if specified persons, groups, and perimeters have access to the file.

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

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

**User's actions:**

- Creating Rules;
- Configuring Notifications in Rules.

### Application activity rule

For the clipboard rule, the following parameters are specified:

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

- **Keyboard input**

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

- **Persons** – the list of persons, their groups, and perimeters. When traffic is sent by specified persons or groups or leaves specified perimeters, it triggers the rule.
- **Computers** – the list of computers. When traffic is sent from specified computers, it triggers the rule.
- **Applications** (for the **Keyboard input** event type only) – working in specified applications triggers the rule.
  To add an application, enter its name in the field. The value can be specified using wildcard "*" to replace any number of characters in the beginning or at the end of the string.
  You can also click  and select the required application from the list. The list is formed based on **Keyboard input** events recieved form Device Monitor.
- **Terminal session only** (for the **Clipboard** event type only) – select this option if the receiver application is a terminal session. If the option is selected, choosing the receiver application manually is unavailable.
- **Terminal session direction** – (only for Data protection policy on agents). Copying data from applications or that and also pasting data from the clipboard to applications trigger the rule.
- **Source application** (for the **Clipboard** event type only) – copying data from specified applications triggers the rule. If the **Terminal session only** parameter is enabled, the option is unavailable.
  To add an application, enter its name in the field. The value can be specified using wildcard "*" to replace any number of characters in the beginning or at the end of the string.
  You can also click  and select the required application from the list. The list is formed based on **Clipboard** events recieved form Device Monitor.
- **Receiver application** (for the **Clipboard** event type only) – pasting data from the clipboard to specified applications triggers the rule. If the **Terminal session only** parameter is enabled, the option is unavailable.
  To add an application, enter its name in the field. The value can be specified using wildcard "*" to replace any number of characters in the beginning or at the end of the string.
  You can also click  and select the required application from the list. The list is formed based on **Clipboard** events recieved form Device Monitor.
- **Rule validity days**
- **Rule validity time**

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

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

**User's actions:**

- Creating Rules;
- Configuring Notifications in Rules.

### Person Control Rule

For the person control rule, the following parameters are specified:

- **Violation level** – the System will intercept events with the specified violation level (values: *Low*, *Medium*, *High*, *Any*) or events without violation (*No*).
- **Connect with policy** – specify data protection policies and data protection policies on agents which trigger the rule when the policy itself is triggered (assuming that the violation level matches the value specified in the **Intercept with violation level** field).

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

**User's actions:**

- Creating Rules;
- Configuring Notifications in Rules.

### File Operations Rule

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

- **Event type** – actions with files that trigger the rule. Possible values:
  - **Write file** – exporting a file from the application;
  - **Read file** – uploading a file to the application.
- **Persons** – if persons, groups, or perimeters from this list execute operations with files, it triggers the rule.
- **Computers** – if operations with files are performed on computers from the list, it triggers the rule.
- **Applications** – actions in applications from the list trigger the rule.
  To add an application, enter its name in the field. The value can be specified using wildcard "*" to replace any number of characters in the beginning or at the end of the string.
  You can also click  and select the required application from the list. The list is formed based on **Write file** or **Read file** events recieved form Device Monitor.
- **Rule validity days**
- **Rule validity time**
- **Browser tab address** – address of the active browser tab. To specify multiple values, after entering each value, press Enter.
  The values can be specified using wildcards:
  - "?" – to replace a single character in the beginning or at the end of the string;
  - "*" – to replace any number of characters in the beginning or at the end of the string.

> **Note:**

Browser tab address is a user attribute of the default InfoWatch Device Monitor plugin. The attribute can be used only in rules of data protection policies. The attribute is not available in rules of data protection policies on agents.

**Important!**

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

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

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

**Important!**

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

**User's actions:**

- Creating Rules;
- Configuring Notifications in Rules.

## 3.8 Lists Section

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

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




**Lists** section, the list of statuses

The section contains the following catalogues:

- Tags;
- Statuses;
- Perimeters;
- Web Resources;

- File Types.

**User's actions:**

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

## 3.8.1 Tags

**Reference information:**
A ***tag*** is a label that gives a brief description of an intercepted object. For each tag, a special colour marker is set.

There are the following preset tags in the System:

- **VIP** – events from persons who belong to the company authorities
- **Web-email** – events of email sending via web-email;
- **Under supervision** – events that indicate persons' suspicious activity

**User's actions:**

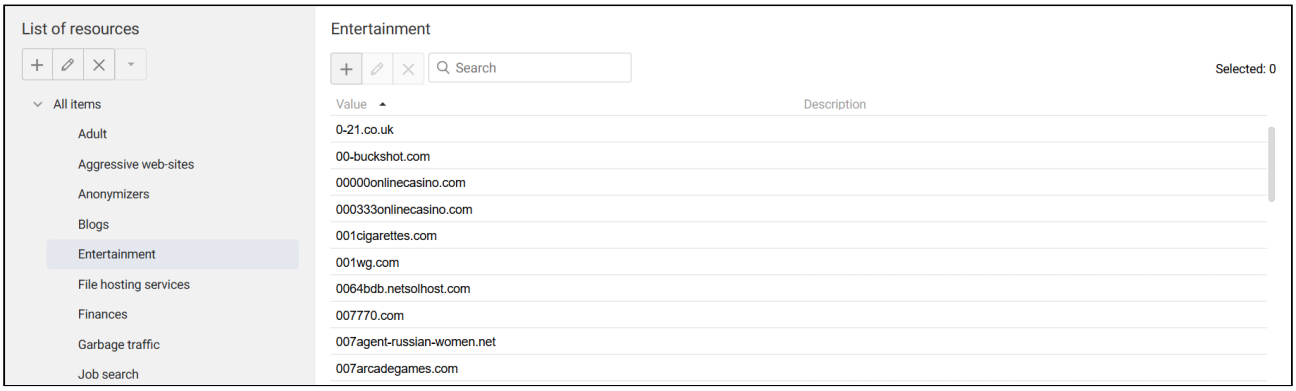
- Creating a list of tags (see *Managing Tags*).

## 3.8.2 Web Resources

**Reference information:**
***Web resources*** are a set of Internet resources. The System treats visits to these resources as misuse of working time.

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

The list of web resources and tools for operations with them (creating, editing, deleting and end-to-end search within catalogues) are located on the right side of the working area. End-to-end search is carried out by the web resource value and can be performed within either a selected list or all lists of the section. To search through all lists of the section, select the root catalogue.




The System includes the following preset lists of web resources:

- Adult;
- Aggressive web-sites;

- Anonymizers;
- Blogs;
- Entertainment;
- File hosting services;
- Finances;
- Garbage traffic;
- Job search;
- Media;
- Potentially dangerous resources;
- Social networks;
- Software and updates;
- Web mail.

**User's actions:**

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

### 3.8.3 Statuses

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

- Automatically assigned to a person according to the status of a user or a computer imported from the Directory Service;
- Manually assigned to a person by the Security Officer;
- Automatically assigned to a sender when a rule is triggered.

For each status, a colour indicator is set.




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

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

**User's actions:**

- Creating a list of statuses (see *Managing Statuses*);
- Manual assigning status to a person or workstation to monitor its activities or to visually distinguish them (see *Setting Statuses to Persons and Computers*);
- Automatic assigning status to a sender when the rule is triggered (see *Rules and their Viewing Form*, **Set status** attribute);

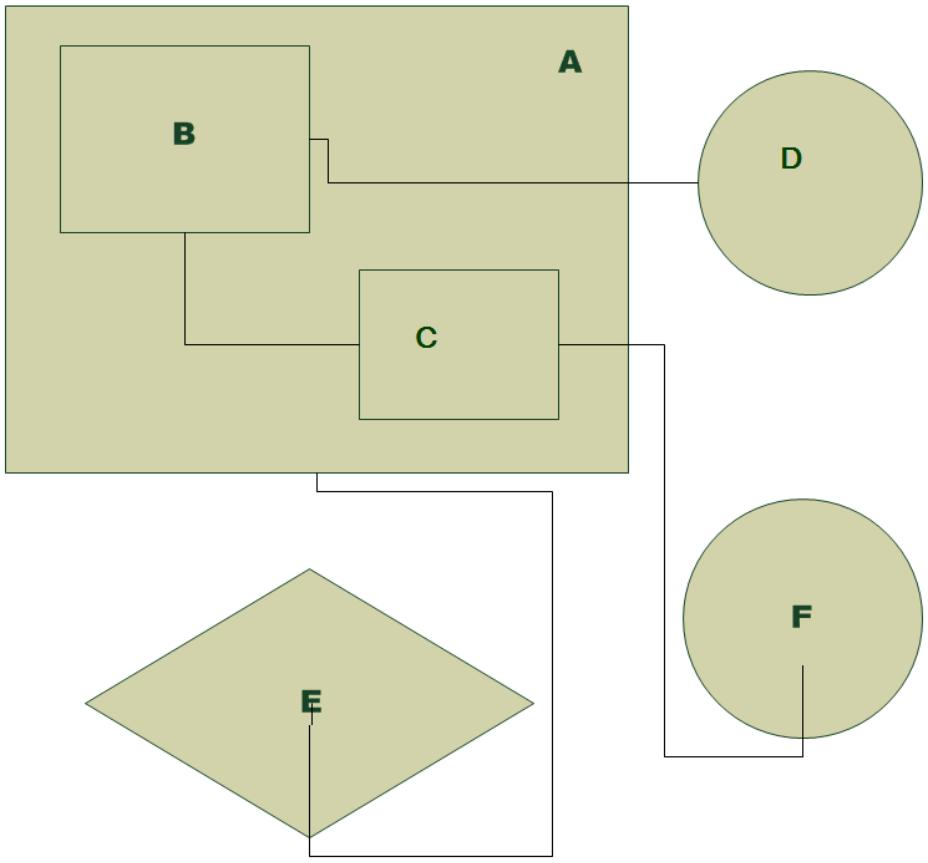
- Choosing persons and workstations with a specific status as objects of research when creating a Person Control Policy (see *Creating Person Control Policy*).

### 3.8.4 Perimeters

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

**For example:**

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




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

- Inside the company (within the perimeter A)
- Inside one subdivision – within the perimeter B or C;
- Only between the company subdivisions – within the perimeter B and C;
- Outside the company (between the perimeter A and one of the perimeters D, E or F)
- Outside the company only for one subdivision – within the perimeter B or C and one of the perimeters D, F, E.

**Warning!**

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

Perimeters can have a common content, but you cannot place one perimeter into another and create an hierarchical structure.

The System includes the following preset perimeters:

- ***Financials*** – includes a list of bank's websites.
- ***Free email domains*** – includes a list of popular email domains. Is used in preinstalled policy *Sending to free email domains*;
- ***Public authorities*** – includes a list of public authorities' websites.
- ***Trusted recipients*** – to control sending data out of the company.
- ***Exclude from interception*** – includes a list of popular email web resources and preinstalled lists of web resources "Software and updates" and "Garbage traffic". Is used in the ***Excluding from Interception*** (see *Policy that Excludes Mailing Lists from Interception*) preset policy;
- ***Artificial intelligence*** – includes a list of artificial intelligence web resources.
- ***Company*** – to control sending data out of the company;
- ***Converters*** – includes a list of popular file converter websites.
- ***Competitors*** – to control sending data out of the company.

Perimeters can be used to create new data protection policies and new data protection policies on agent.

For the classification base in English the preset perimeters ***Company***, ***Trusted recipients***, ***Competitors***, ***Financials*** and ***Public authorities*** do not contain elements, you should add the elements manually (for details, see *Managing Perimeters*).

**Note:**

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

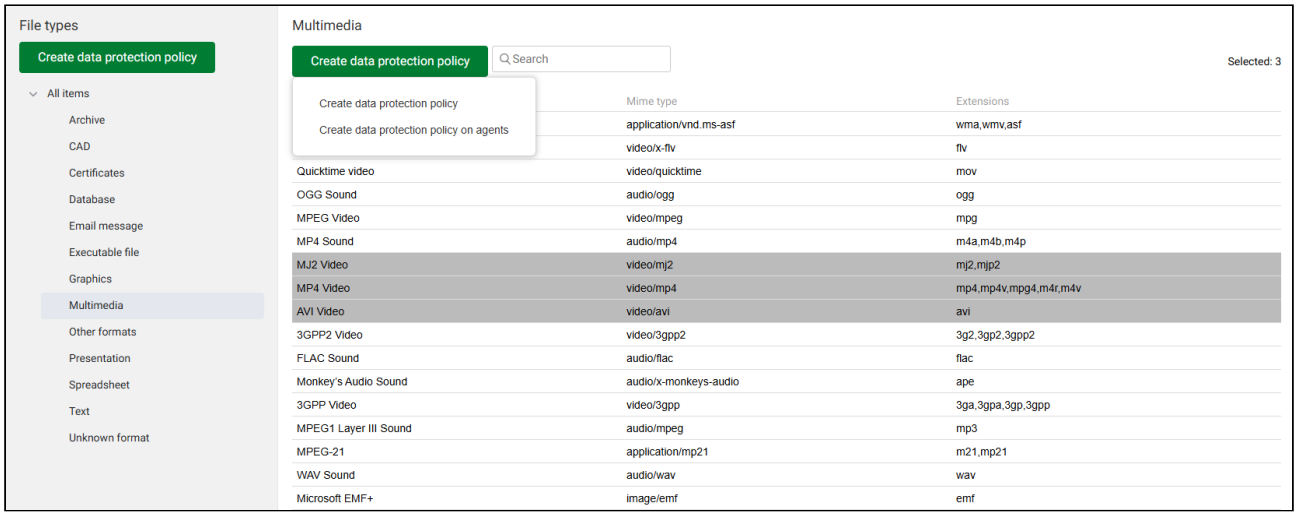
**User's actions:**

- Building perimeters (see *Managing perimeters*).

## 3.8.5 File Types

**Reference information:**

***File types*** are a set of files that are detected in the System. For some types, the System supports data extraction.




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

The tab contains the following elements:

| Element | Purpose |
|---|---|
| The list of file types | Located in the left part of the workspace. Contains a set of subjects that use one or more file formats |
| List of formats of the selected type | Located in the right part of the workspace. Contains a list of attributes for all files of the selected type that are detected in the System. This is a table with the following attributes: **Name**, **MIME type**, and **Extension** |
| **Create data protection policy** button | A button for adding a new policy for the selected file type or format. Click the button and, in the drop-down list, select the required action:<br>• Create data protection policy<br>• Create policy on agent<br>A policy creation form for the selected file format will open in the *Policies* section.<br>**Note:**<br>For formats, analysis of which is not supported in Device Monitor, **Create data protection policy on agents** item is unavailable |
| End-to-end search field | It is located on the right side of the working area. End-to-end search is carried out by the name and extension of the file. Search is performed within a selected list of files and all section's lists. To search through all lists of the section, select the root catalogue |

**Warning!**

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

File formats for which Traffic Monitor supports detection and extraction:

| File type | Format | Extension |
|---|---|---|
| **Archive** | *Detection and data extraction*[1]*:* | |
| | • Self-extracting archive | EXE |
| | • 7zip Archive | 7Z |
| | • ARJ v. 3.10.22 | ARJ |
| | • bzip2 v. 1.0.x | BZIP, BZ, BZ2 |
| | • gzipv.1.3.x | GZ |
| | • LHa archive | LZH |
| | • UNRAR v.3.9.10 | RAR |
| | • GNU tar v. 1.13.x | TAR |
| | • XZ archive | XZ |
| | • Zip Archive | ZIP, ZIPX |
| | *Detection only:* | |
| | • CAB Archive | CAB |
| | • UHarc Archive | UHA |
| | • Archive .z | Z, LZW |
| | • ZLIB Stream | ZLIB |
| **CAD** | *Detection and data extraction:* | |

| File type | Format | Extension |
|---|---|---|
| | • AutoCAD | DWG. DWT, DWS |
| | *Detection only:* | |
| | • Filmbox format | FBX |
| | • IGES format | IGS |
| | • SolidWorks document | SLDPRT, SLDASM, SLDDRW, PRTDOT, ASMDOT, DRWDOT |
| | • Gerber Technology file | - |
| | • ACIS file | SAT |
| | • CATIA V5 | CATPart, CATProduct, CATDrawing, CATProcess, CATAnalysis, CATCatalog, CATMaterial |
| | • DXF (Drawing eXchange Format) | DXF |
| | • MicroStation DGN | DGN |
| | • Revit | RVT, RFA |
| | • STEP / IFC model | STEP, STP, IFC |
| | • 3D Unigraphics NX | PRT |
| | • Компас 3D | CDW, M3D, A3D, A3T, CDT, SPT, SPW, FRT, FRW, KDT, KDW, M3T, T3D |
| | • HPGL Plot File | PLT |
| **Certificates** | *Detection only:* | |
| | • DER Encoded X509 Certificate | DER |
| | • Detached S/MIME signature | P7S |
| **Database** | *Detection only:* | |

| File type | Format | Extension |
|---|---|---|
| | • 1C archive | DT |
| | • MSAccess ACE DB or JET DB | ACE, MDB, ACCDB |
| | • MS SQL | BAK, TRN, FULL |
| | • Oracle | DMP |
| | • 1C config | CF |
| | • 1C table file | MXL |
| | • vCard file | VCS, VCARD |
| **Email message** | *Detection and data extraction:* | |
| | • Outlook inner object | MSG |
| | • MS TNEF container | TNEF, TNF, WINMAIL.DAT |
| **Executable file** | *Detection only:* | |
| | • Linux Library | SO |
| | • Dynamic Link Library | DLL |
| | • MS Executable | EXE |
| | • Linux Package | RPM |
| **Graphics** | *Detection and data extraction:* | |
| | • Scalable Vector Graphics | SVG |
| | • HP PCL printer job | PCL |
| | • Adobe Illustrator | AI |
| | • Adobe Photoshop | PSD |
| | • BMP Image | BMP |

| File type | Format | Extension |
|---|---|---|
| | • GIF Image | GIF |
| | • HEIF Image | HEIC |
| | • JPEG Image[2] [3] | JPEG, JPG, JPE |
| | • JPEG2000 image | JP2 |
| | • Microsoft WMF | WMF |
| | • PBM Image | PBM |
| | • PGM Image | PGM |
| | • PNG Image | PNG |
| | • PostScript | PS |
| | • PPM Image | PPM |
| | • Sun Raster Image | SUN, RAS, RAST, RS, SR, SCR, IM1, IM8, IM24, IM32 |
| | • TIFF Image | TIF, TIFF |
| | • WebP Image | WEBP |
| | • Microsoft clipboard metafile | WMF |
| | • Microsoft EMF+ | EMF |
| | *Detection only:* | |
| | • OpenDocument Graphics | ODGH |
| | • ZjStream printer job | ZJS |
| | • Corel Draw | CDR |
| | • JPEG XR Image | JXR, HDR, WDP |

| File type | Format | Extension |
|---|---|---|
| | • Windows Icon | ICO |
| **Multimedia** | *Detection and data extraction:* | |
| | • Microsoft EMF+ | EMF |
| | *Detection only:* | |
| | • FLAC Sound | FLAC |
| | • Monkey's Audio Sound | APE |
| | • MP4 Sound | M4A, M4B, M4P |
| | • MPEG1 Layer III Sound | MP3 |
| | • OGG Sound | OGG |
| | • WAV Sound | WAV |
| | • 3GPP Video | 3GA, 3GPA, 3GP, 3GPP |
| | • 3GPP2 Video | 3G2, 3GP2, 3GP2, 3GPP2 |
| | • AVI Video | AVI |
| | • Fly video (FLV) | FLV |
| | • MJ2 Video | MJ2, MJP2 |
| | • MP4 Video | MP4, MP4V, MPG4, M4R, M4V |
| | • MPEG Video | MPG |
| | • MPEG-21 | M21, MP21 |
| | • MXF | MXF |
| | • Quicktime video | MOV |
| | • Windows Media | WMA, WMV, ASF |

| File type | Format | Extension |
|---|---|---|
| **Other formats** | *Detection and data extraction:* | |
| | • MS Office Printer profile | OXPS, XPS |
| | • Base64 encoded data[4] | - |
| | • UUE encoded data | - |
| | • ISO | ISO |
| | • CDATA section[5] | - |
| | • Microsoft Compound Binary File Format[3] [6] | DOCX, XLSX, PPTX |
| | *Detection only:* | |
| | • Vector data | - |
| | • KeePass | KDB, KDBX |
| | • Windows Imaging (WIM) Image | WIM |
| | • Torrent | TORRENT |
| | • GnuPG encrypted data | GPG |
| | • PGP encrypted data, OpenPGP encrypted data | PGP, GPG, ASC |
| | • S/MIME enveloped data | P7M |
| | • Open Type | OTF |
| | • Shortcut | LNK |
| **Presentation** | *Detection and data extraction:* | |
| | • MS PowerPoint Document | PPTX, PPT, POT, POTM, POTX |

| File type | Format | Extension |
|---|---|---|
| | • OpenOffice.org Presentation Document | DWG, DWT, DWS |
| **Spreadsheet** | *Detection and data extraction:* | |
| | • MS Excel document[3] | XLSX, XLT, XLTM, XLTX, XLS, XLSB |
| | • OpenOffice.org Spreadsheet Document[7] | ODS |
| **Text** | *Detection and data extraction:* | |
| | • Adobe Acrobat[3] | PDF |
| | • CHM Document | CHM |
| | • HTML Document | HTML, HTM |
| | • JSON Document | JSON, JSN |
| | • MS Visio[8] | VSD, VSDX |
| | • MS Word Document[3] [6] (2003 and later) | DOC, DOCX, DOT, DOTX, DOCM |
| | • MS Project | MPP |
| | • OpenOffice.org Word Processor Document[7] | ODT |
| | • RTF Document | RTF |
| | • XML Document | XML |
| | • XPS Document | OXPS, XPS |
| | • ActiveSync Request | STG |
| | • E-mail message | MSG |
| | • Plain text Document | TXT, TSV, CSV |

| File type | Format | Extension |
|---|---|---|
| | • E-mail | EML |
| | • Open Publication Structure eBook file | EPUB |
| | • Web archive | MHT |
| | *Detection only:* | |
| | • DjVu Document | DJV, DJVU |
| | • Microsoft Publisher Document | PUB |
| | • MS Word Document 6.0 and earlier versions | DOC, DOT |
| | • Windows Event Log (ASCIIDOC) | EVTX |
| **Unknown format** | *Detection only:* | |
| | • Binary data | - |

**Note:**

[1] In case the System intercepts a multi-volume archive, it extracts and analyses its name.
In case processing of objects with complex structure takes too much time and fails with an error, adjust parameters in the `/opt/iw/tm5/etc/lua.conf` file. See *InfoWatch Traffic Monitor. Configuration Files Guide. lua.conf*.

[2] For the System, in case it intercepts a JPEG file merged with an archive, to extract text from the archive, specify additional settings in `/opt/iw/tm5/etc/config-perm/bookworm/extractors_customization.xml` configuration file. See *InfoWatch Traffic Monitor. Administration Guide. The `extractors_customization.xml` Configuration File* article for details.

[3] With files of XLS, PDF, JPG and DOCX format, the following may occur:

- Merged files policy false positive. See details in the article *Intercepted files are incorrectly marked as merged* in the Knowledge Base;
- Incorrect format detecting and file data extraction or failure to perform these operations, if structure of the intercepted file does not correspond the format specification (for example, there can be a floating format signature which is located not in the beginning of the file). See details in the article *File format cannot be detected and so unpacking cannot be performed* in the Knowledge base.

[4] For the System to detect a Base64 sequence in case a file contains regular text, configure the heuristic algorithm. For details, see *InfoWatch Traffic Monitor. Configuration Files Guide. extractors.conf*.

[5] CDATA section cannot be detected along the path `/docProps/core.xml` within OOXML (Office Open XML).

[6] The System extracts and analyzes enclosed data from files of both strict and standard (Office Open XML package) DOCS, PPTX, XLSX formats.

[7] When processing OOXML files with ODT and ODS extensions, the System also analyzes header and footer data. In case file name, file path and sheet name were added as parameters in header and footer settings, they may be displayed incorrectly.

[8] For VSD and VSDX files, only text extraction is supported.

**User's actions:**

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

## 3.9 Administration Section

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

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

On working in this section, see *Managing the System*.

# 4 Cases Solving in Traffic Monitor Management Console

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

- Managing Persons and Computers;
- Managing Catalogues;
- Managing Base of Technologies;
- Managing Protected Objects;
- Managing Interception Objects;
- Configuring System Response;
- Managing Reports;
- Managing the System.

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

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

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

- Dashboards Section;
- Events Section;
- Reports Section;
- Technologies Section;
- Protected Objects Section;
- Persons Section;
- Policies Section;
- Lists Section;
- Administration Section.

## 4.1 Typical Actions

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

**Typical actions include the following:**

- Login to the Management Console;
- Applying System Configuration;
- Editing Element;
- Deleting Element;
- Page Navigation;
- Changing User Password;
- Selecting Interface Language;
- Calling Help File;
- Viewing Information on System.

### 4.1.1 Login to the Management Console

**Purpose:**

Log into the Management Console.

**Solution:**

**To log into the Management Console:**

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

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

5. Click **Login**.

**To log out of the Management Console:**

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

## 4.1.2 Applying System Configuration

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

- Technologies;
- Protected objects;
- Persons;
- Policies;
- Lists.

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

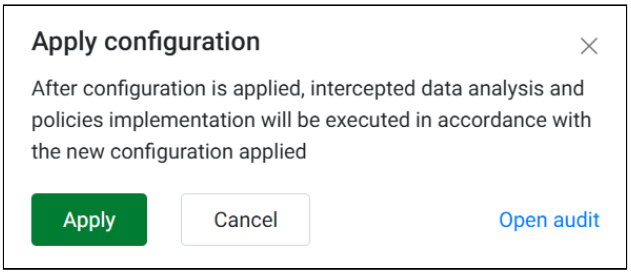
**Purpose:**
Apply the System configuration.

**Solution:**

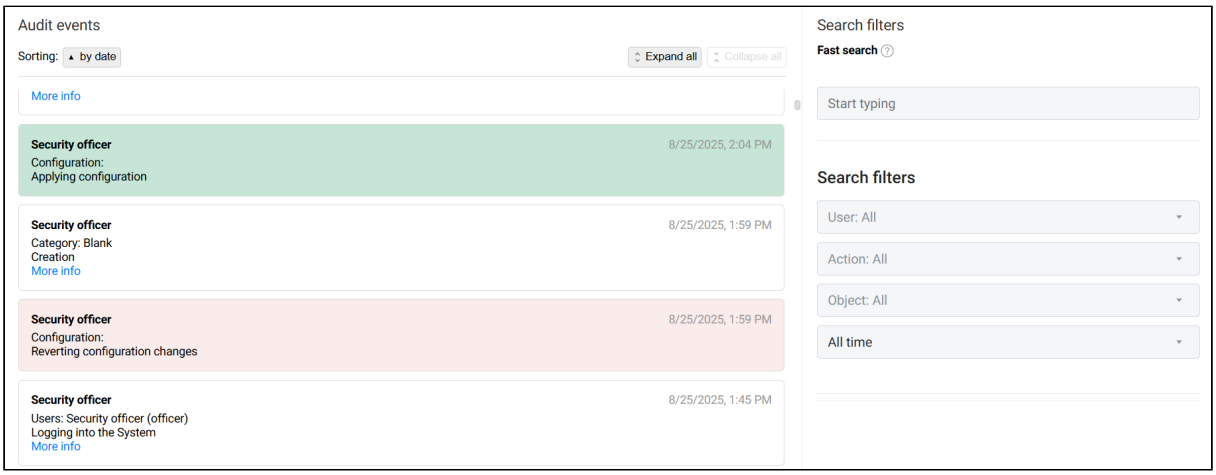
1. When you finish editing the configuration, then, at the top of the browser window, click **Apply** in the bar:

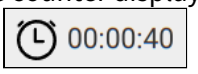
   The **Apply configuration** window will open:




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




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

3. In the **Apply configuration** window, click **Apply**.
4. Wait for the application of the configuration to complete.
   Applying the new configuration may take some time. The duration of application does not exceed 3 hours. At the top of the workspace, a counter is displayed. The counter displays the time that has passed since the start of the configuration application process: 
   
   You can edit a configuration and apply it even if another configuration is being applied. In this case, the application of the configuration will be interrupted and the application of the edited configuration will start.

### 4.1.3 Editing Element

**Purpose:**
Change attributes of an earlier created element.

**Solution:**

1. Go to the desired section.
2. If necessary, go to the desired subsection or tab.

3. Select an element by clicking the left mouse button or select it from the drop-down list, and click **Edit**.
4. Enter required attributes (attributes of all elements are described in *Interface of Traffic Monitor Management Console*).
5. Click **Save**.

### 4.1.4 Deleting Element

**Purpose:**
Delete an element.

**Solution:**

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

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

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

### 4.1.5 Page Navigation

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




Pages navigation panel

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

**Solution:**

1. Go to the desired section.
2. If needed, go to a subsection or tab.
3. In the drop-down list in right part of the page navigation pane, select a number of elements per page.
4. For page navigation, use buttons with page numbers. You can also use the following buttons:
   - **|<** - to go to the first page;
   - **<** - to go to the previous page;
   - **>** - to go to the next page;
   - **>|** - to go to the last page;

**Note:**

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

### 4.1.6 Changing User Password

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

**Purpose:**
To change the password.

**Solution:**

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

   **Note:**

   Consult detailed guidelines for passwords described in the document *InfoWatch Traffic Monitor. Administration Guide*.

3. Click **Save**.

### 4.1.7 Selecting Interface Language

**Purpose:**
Change the interface language of the Management Console.

**Solution:**

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

Do the same steps to revert English language if necessary.

### 4.1.8 Calling Help File

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

**Solution:**

1. In the right upper corner of the workspace, click the user menu button (see *Interface of Traffic Monitor Management Console*).

2. In the drop-down list, under the **Help** caption, choose either of the following:
   - **Online** – to open the online version of documentation
   - **Offline** – to open the offline version of documentation

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

### 4.1.9 Viewing Information on System

**Purpose:**
Get general information about the System.

**Solution:**

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

## 4.2 Managing Persons and Computers

**Why do you need persons and computers:**

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

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

**Creating lists of persons and computers include the following steps:**

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

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

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

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

**See also:**

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

## 4.2.1 Creating Group of Persons or Computers

**Purpose:**
Create a group of persons or computers.

**Solution:**

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

> **Warning!**
>
> If a new group is created, events for this group are displayed as soon as you *apply the configuration*.

To edit a group, select the required group and click . To delete a group, select it in the list and click .

You can add existing groups of the Directory Service to a user group. In this case, when you add or remove persons in the Directory Service, contents of the corresponding user group will be updated automatically.

To add a group of the Directory Service to a user group, select a desired group with a mouse and drag and drop it at the required user group.

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

> **Note:**
>
> To enable automatic update for user groups which contain groups of the Directory Service, run synchronization with the LDAP server.

You can add or move a user group or a person from a user group to another user group. For this:

1. Select a group/person/computer with a mouse and drag and drop it to the required user group.
2. In the window that opens, select "Add" or "Move".

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

***Example:***

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

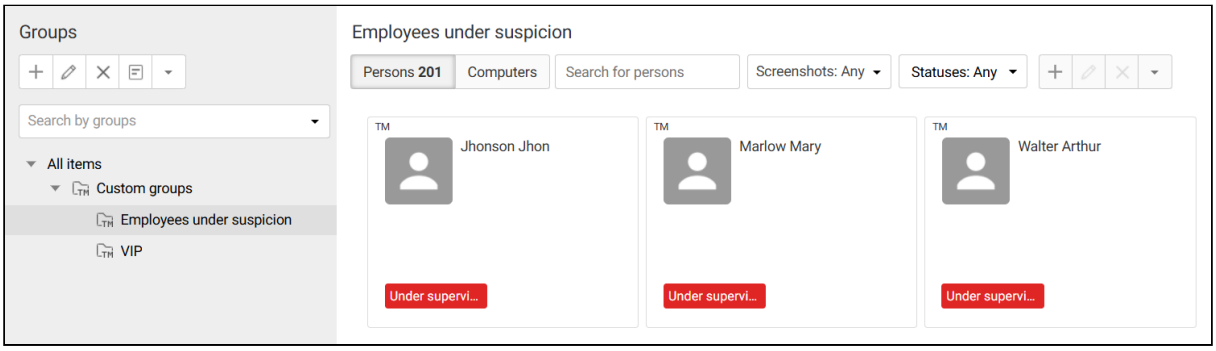
1. In the  **User Groups** node, create *Employees under suspicion* group.

2. Using **Search for person** field or filters find persons which you want to add to the group.

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

3. Add the found persons to the group.

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




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

## 4.2.2 Creating Persons and Computers

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

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

**Purpose:**
To fill a group of persons and computers.

**Solution:**

1. Go to the **Persons** section.
2. On the left part of the workspace, left-click the required group.
3. On the right part of the workspace, click one of the following tabs:
   - **Persons** – to add a person
   - **Computers** – to add a computer
4. On the toolbar in the right part of the workspace, click  **Add**.
5. Specify parameters of a new user/computer (see *Persons* and *Computers*).
6. Click **Save**.

**To edit** a person/computer, select the required person/computer in the list and click .

**To delete** a person/computer, select the required person/computer in the list and click .

**To add a person from the contact in the event:**

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

### 4.2.3 Exporting and Importing Persons

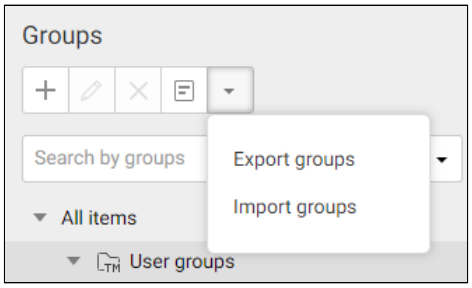
To make it easier to move the configuration to another server, Traffic Monitor allows the user to **export** and **import** groups of persons and computers.

> **Note:**
>
> If the user has restricted access to groups of persons in the visibility scope, that user is not allowed to export and import groups of persons, regardless of their role and privileges.

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

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

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




4. The System will prepare the data to be exported, the progress will be displayed in the lower right corner. As a result, a ZIP archive will be saved to the computer. The archive contains an XML file with a description of configuration elements. The archive name includes the date of the export, for example: `iwtm-group-20231213_141243.zip`.
   You can use the archive to import configuration elements to another server.

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

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

1. Go to the **Persons** section.
2. Click .
3. From a drop-down list, select **Import groups**.
4. In the window that opens, select an earlier exported ZIP archive with a description of groups of persons.
5. Wait for the data import to complete, the progress will be displayed in the lower right corner.

6. Apply the configuration and refresh the page. After that, added groups, persons, computers and statuses will be displayed in the Traffic Monitor Management Console.
   New statuses will be displayed in the **Statuses** subsection of the **Lists** section.
   Persons and computers will get their statuses according to the imported configuration. The time when the statuses are assigned to persons and computers is also defined by the imported configuration.

## Features of exporting and importing the organizational structure

Features of export:

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

Features of import:

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

**Errors while importing the organizational structure**

If an error occurs, importing will not be aborted, but Traffic Monitor will process the next configuration element being imported.

If there are errors, Traffic Monitor will make a report as a text file when importing is finished. The notification about the generated report will appear in the lower right corner of the configuration importing window.

To download the report on your computer, click  after the notification text.

The report contains records about all errors that occurred during the importing. If the report is generated during the next importing, it will only contain new error records. Error records in the report are listed in chronological order. The record contains an error type and information about the object that caused the error.

The error types are listed in the table below:

| Error type in the file | Description |
|---|---|
| `group_not_found` | An object (group/person/computer) being imported and an object in the System have the same names and the same types, but different identifiers (ID) |
| `person_not_found` | |
| `workstation_not_found` | |
| `ldapgrouptogroup_not_found` | The System cannot find the related group for the LDAP object (group/person/computer) being imported |
| `ldappersontogroup_not_found` | |
| `ldapworkstationtogroup_not_found` | |
| `ldappersontoworkstation_not_found` | The System cannot find the related computer for the LDAP object (person) being imported |
| `group_save_failed` | Error while saving an object (group/person/computer) |
| `person_save_failed` | |
| `workstation_save_failed` | |

**Note:**

If an error while saving an object ( `failed` ) occurs, the record will contain the `errors` part. Fields that caused the validation error are listed in this part.

### 4.2.4 Configuring Person's Card

**Purpose:**

Fill the card of person with data.

**Configuring the person's card consists of the following actions:**

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

## Adding Contact to Person

**Purpose:**
Add or edit contact information for a person.

**Solution:**

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

> **Note:**
>
> Contact values must be specified in the following format:
>
> - Mobile phone number (string of 3 or more characters; may contain only digits, space, and the characters: “-”,”_”, “( )”,”+”);
> - Landline phone number (string of 3 or more characters; may contain only digits, space, and the characters: “-”,”_”, “( )”,”+”);
> - E-mail (e-mail address in RFC format);
> - Lotus e-mail (e-mail address in RFC format);
> - Domain account (e-mail address in RFC format);
> - Skype contact (string of 1 or more characters);
> - MS Teams account, if the adapter is installed (string of 1 or more characters);
> - ICQ contact (string of 1 or more characters);
> - Facebook account (string of 1 or more characters);
> - VK account (string of 1 or more characters);
> - Telegram account (string of 1 or more characters);
> - WhatsApp account (string of 1 or more characters);
> - YandexID contact (string of 1 or more characters);
> - Another web account (string of 1 or more characters).
>
> WhatsApp and Telegram messengers use their own identifier formats. We recommend using Mobile phone type of contact for associating the person with the intercepted messenger contact.

**To edit** a previously specified contact:

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

**To add a new contact** from an event to a person:

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

## Adding Computer to Person

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

**Solution:**

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

## Adding Person to Group

**Purpose:**
Add a person to an existing group.

**Solution:**

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

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

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

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

## 4.2.5 Configuring Computer Cards

**Purpose:**
Add data to a computer card.

**Configuring a computer card consists of the following actions:**

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

### Adding Contacts to Computers

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

**Solution:**

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

### Adding Persons to Computers

**Purpose:**
Add a computer linked to a person.

**Solution:**

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

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

### Adding Computers to Groups

**Purpose:**
Add computer to an existing group.

**Solution:**

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

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

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

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

## 4.2.6 Setting Statuses to Persons and Computers

**Purpose:**
To set a status to a person or computer.

**Solution:**

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

> **Note:**

The *New* status is assigned to a person or computer when they are created in the System. This status is preserved for 30 days. For persons and computers imported from the Directory Service, the *New* status is preserved for 30 days starting from the moment the records are created in the Directory Service respectively.

**See also:**

- Statuses – about the section where you can manage statuses of persons and computers.

### 4.2.7 Viewing Screenshots

**Preliminary settings:**

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

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

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

   **Note:**

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

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

   **Note:**

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

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

**Note:**

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

**Important!**

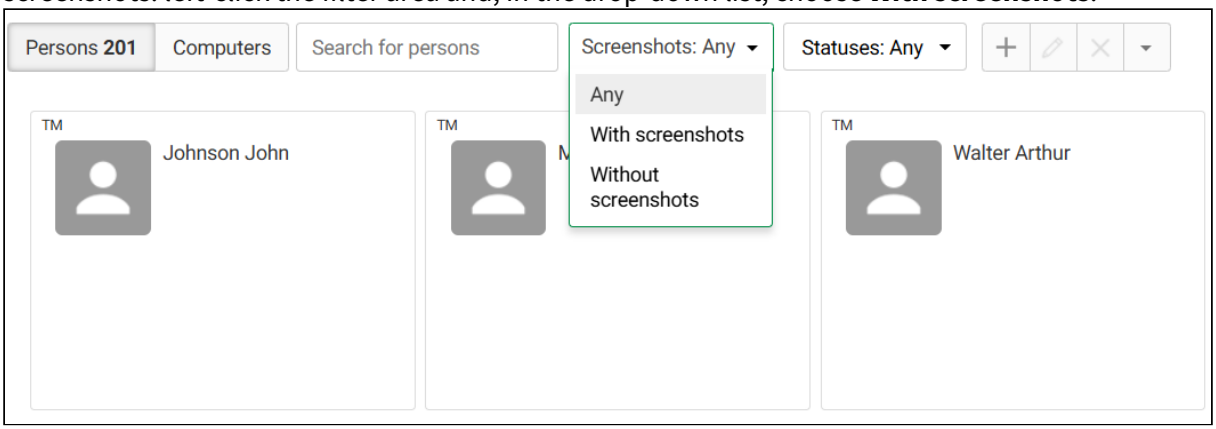
It is necessary to perform specified actions prior to creating a Device Monitor rule (see *InfoWatch Device Monitor. User Guide. ScreenShot Monitor Rule*) and deploying the Device Monitor policy, which includes this rule, to workstations. Otherwise, the System will not display screenshots.

**Purpose:**

View intercepted screenshots for a person or a computer.

**Solution:**

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




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

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

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

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

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

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

### 4.2.8 Viewing Events Involving Person's Contact

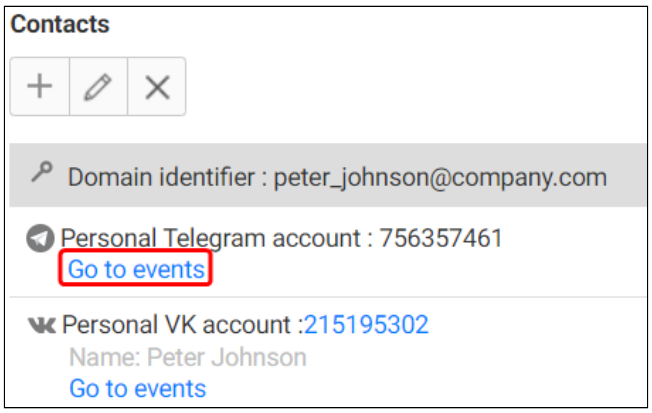
**Purpose:**

View events which involve a certain contact of a person.

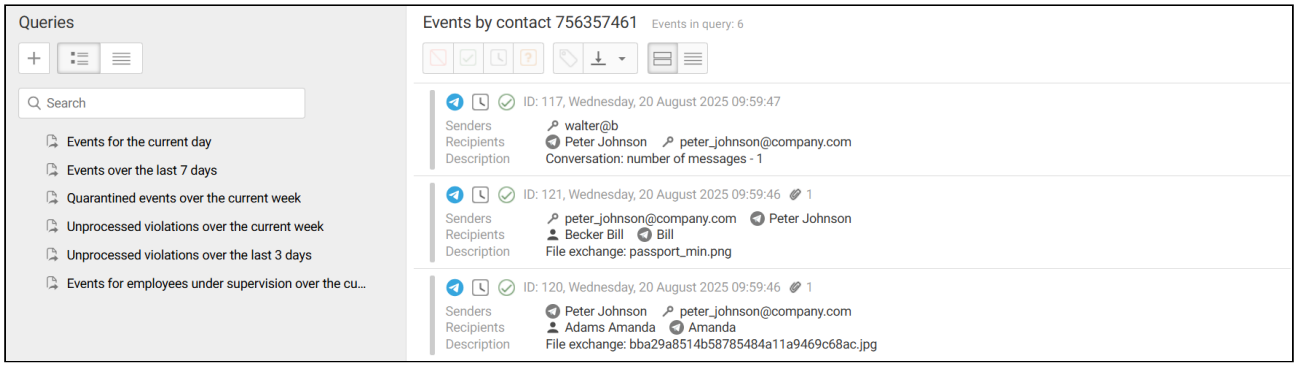
> **Note:**
>
> You can view events involving a person's contact only if a contact was added manually or by means of post-identification.

**Solution:**

In the person's card, on the contact's line, click **Go to events**.




**Events** page will open. Here you can find a list of all events in which the contact is involved as a sender or recipient.




**Note:**

The System does not display the query which it used to filter events. You cannot edit the query.

## 4.3 Managing Catalogues

**Warning!**

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

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

**Managing catalogs includes the following actions:**

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

**See also:**

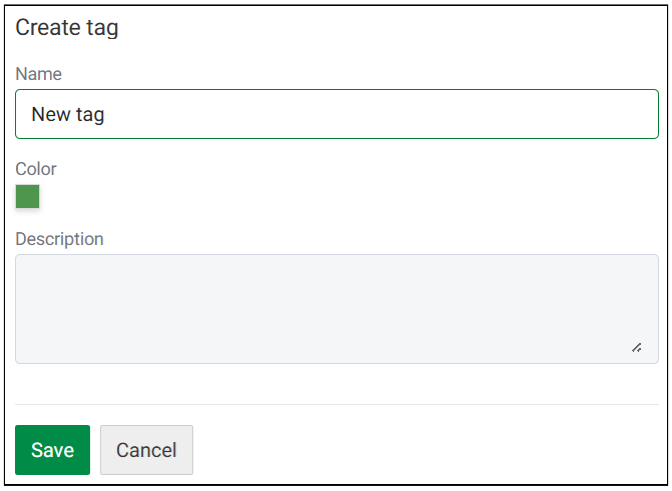
- Lists Section - on the section where you can manage catalogs.

### 4.3.1 Managing Tags

**Purpose:**
Create a tag.

**Solution:**

1. Go to **Lists** -> **Tags**.
2. On the toolbar, click + **Create tag**.




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

To edit a tag, select the desired tag in the list. The editing panel will open on the right side of the screen.

To delete a tag, select the desired tag in the list and click ×.

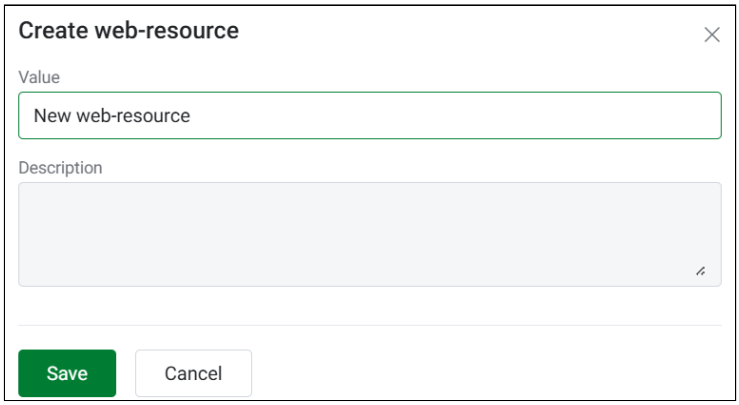
### 4.3.2 Managing Web Resources

**Purpose:**
Specify web resources that the System will treat as inappropriate use of working time. Managing web resources includes:

1. Creating a list of web resources.
2. Adding resources to the list.
3. Exporting/importing lists of web resources.

**Solution:**

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




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

e. Click **Save**.

To edit a resource list or a separate resource, select the desired list/resource and click .

To delete a resource list or a separate resource, select the desired item and click .

**Note:**

If you enter the EXAMPLE.COM domain name in the Value field, next level domains (e.g., LIBRARY.EXAMPLE.COM) will be added as well.

**Warning!**

When you finish editing the resource list, apply the updated configuration (see *Applying System Configuration*).

***Example:***

If you need the System to mark the interception object of visiting the EXAMPLE.COM site as INAPPROPRIATE_SITE:

1. Create the INAPPROPRIATE_SITE web resource list.
2. Add the *EXAMPLE.COM* resource to the created list.

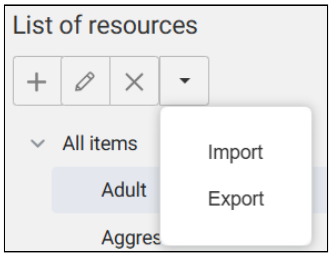
**3. Exporting and importing resource lists**

To make it easier to transfer the configuration to another server, you can **export** and **import** lists of web resources.

Before exporting, make sure the Traffic Monitor configuration is not being edited and the user has the **Import and export web resources** privilege. All lists of web resources will be exported.

To **export** lists of web resources from Traffic Monitor:

1. Go to the **Lists** section, the **Web resources** subsection.
2. Click .
3. In the list, select **Export**.




4. The System will prepare data to be exported, the progress will be displayed in the lower right corner.
   As a result, a ZIP archive will be saved to the computer. The archive contains an XML file with a description of lists of web resources. The archive name includes the date of the export, e.g. `iwtm-system-list-20230424_112137.zip`.
   You can use the archive to import lists of web resources to another server.

To import lists of web resources, you should first apply the configuration. Make sure the Traffic Monitor configuration has been applied and the user has the **Import and export web resources** privilege.

To **import** lists of web resources into Traffic Monitor:

1. Go to the **Lists** section, the **Web resources** subsection.
2. Click .
3. In the list, select **Import**.
4. In the window that opens, select an earlier exported ZIP archive with the description of the web resource lists.
5. Wait for the data import to complete, the progress will be displayed in the lower right corner.
6. Apply the configuration and **refresh** the page to view the added lists of web resources in the Traffic Monitor Management Console.

> **Примечание:**
>
> If a list being imported and a list in the System have the same names but different identifiers (ID), the list will not be imported.
> If a list being imported and a list in the System have the same names and identifiers (ID), new elements will be added to the existing list. Existing elements of the list will remain unchanged. If elements in the list have the same value, they will not be duplicated.

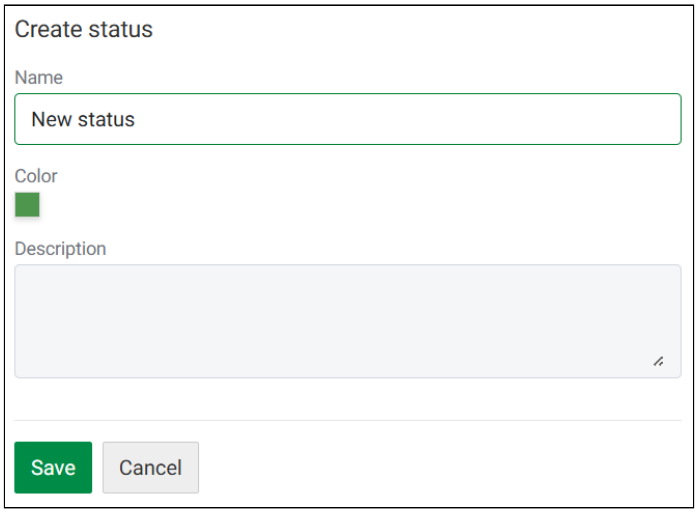
### 4.3.3 Managing Statuses

**Purposes:**:

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

**To create a new status:**

1. Go to the **Lists** section, **Statuses** subsection.
2. On the toolbar, click **Create status**.




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

To edit a status, select the desired status. The editing panel will open on the right side of the screen.

To delete a status, select the desired status and click .

**To create a person control policy from Statuses subsection directly**:

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

## 4.3.4 Managing Perimeters

**Reference information:**

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

There are the following perimeter types in the System:

- Preset perimeters (for details, see *Perimeters*)
- Perimeters created manually based on the following elements:
  - Person
  - Person group
  - Web resource
  - Contacts:
    - Email address
    - Phone
    - Skype contact
    - ICQ contact
    - Domain
    - Lotus contact

**Note:**

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

**Purposes:**

1. Create perimeters.
2. Add elements to perimeters.
3. Export/import perimeters.

**Solution:**

**Purpose 1. Creating perimeters.** To create a perimeter:

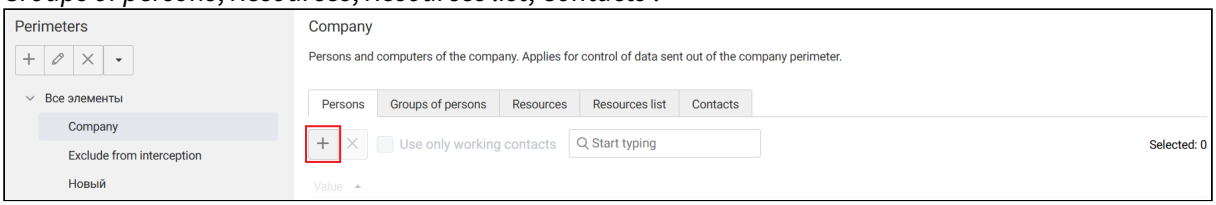
1. Go to the **Lists** section, **Perimeters** subsection.
2. In the left part of the workspace, click  **Create perimeter**.
3. In the window that opens, in the **Name** field, specify the name of the perimeter.
4. In the **Description** field, enter a description (optional).
5. Click **Save**.

To edit a perimeter, select the desired perimeter and click .

To delete a perimeter, select the desired perimeter and click .

**Purpose 2. Adding elements to perimeters.** To an element to the perimeter:

1. Go to the **Lists** section, **Perimeters** subsection.
2. In the left part of the workspace, left-click the desired perimeter in the list of perimeters.
3. In the right part of the workspace, click **Create element**  on one or several tabs: *Persons*, *Groups of persons*, *Resources*, *Resources list*, *Contacts* .




4. In the field that appears, specify one or more elements doing one of the following:
   - For *Persons*, *Group of persons* or *Resources* list:
     - Start typing the name of the item in the field and select the desired entry from the drop-down list
     - Click  **Add** to the right of the field and, in the dialogue window that opens, select desired elements. To find the element you require, use the search line.
     - If you need to use working contacts only, mark the checkbox **Use only working contacts**. Personal contacts will not be used in the perimeter. Then click **Save**.

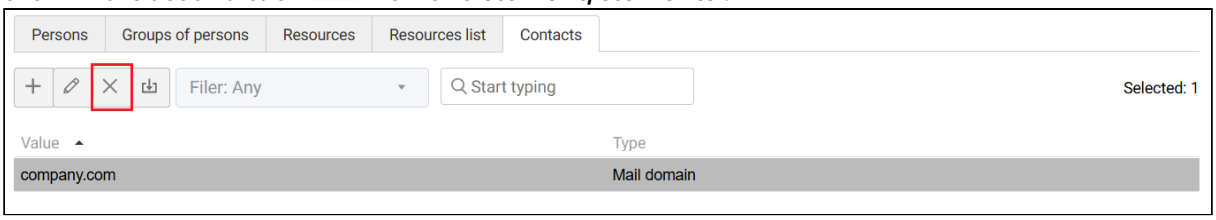
       **Note:**

       After adding persons/groups of persons to a perimeter, you can go to the person/ group card in the **Persons** section. For this, click on the name of the person/group.

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

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

5. Entered values will be added to the list of elements. To remove one or several elements, select them in the list and click [×] **Remove element/elements** .

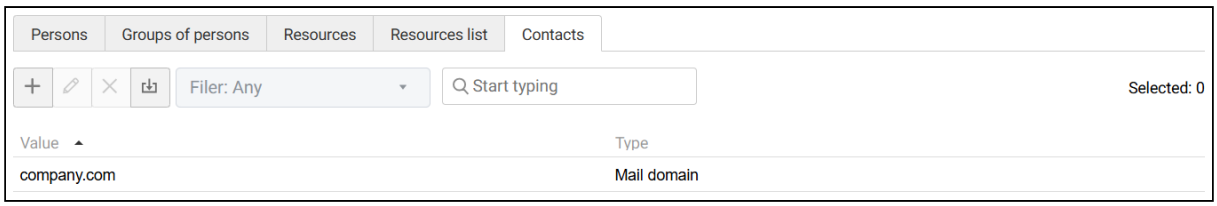



> **Warning!**
>
> We recommend not creating more than 15 perimeters that contain more than 2000 elements each.

***Example:***

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

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

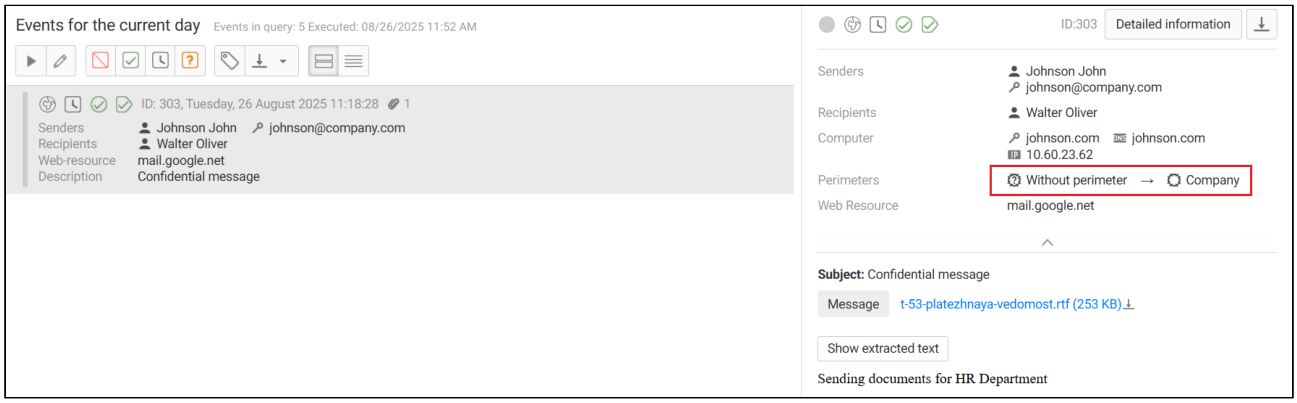





3. Save the perimeter.

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

If you create a query in the **Events** section (see *Creating Queries*), you can quickly find all events of sending data outside the company.




**Purpose 3. Exporting and importing perimeters**

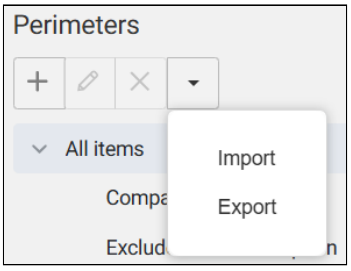
In Traffic Monitor, you can **export** and **import** perimeters. This makes it easier to save the configuration and move it to another server.

> **Note:**
>
> When you export persons/computers, all persons/computers are exported with no dependence of whether they have attributes and contacts added to them.
>
> When you export groups of persons, computers will be exported together with the groups. In case of groups of persons import, the computers will not be imported.
>
> In case a file you are importing contains a person/group which ID is missing on a server where the file is being imported, then:
>
> - for a LDAP object (person/group), the perimeter will be imported without this person/group.
> - for a TM person/group, the person/group will be created during import.
>
> The contacts the type of which was created using plugin will be imported as a part of imported file, even in case if such type of contact (created using plugin) is missing on the server where you import the file.

Before exporting, make sure that Traffic Monitor configuration is not being edited and you have the **Import and export web resources** privilege. The System export all perimeters, not only a selected one.

To **export** perimeters from Traffic Monitor:

1. Go to **Lists** section, **Perimeters** subsection.
2. Click .
3. Select **Export**.




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

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

Use this archive to import configuration elements to another server.

Before importing perimeters, you should first apply the configuration. Make sure that Traffic Monitor configuration has been applied and you have the **Import and export web resources** privilege.

To **import** perimeters into Traffic Monitor:

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

During import, the following operations with matching objects will be performed:

| Object | Matching characteristic | Operation with an original object in the System |
|---|---|---|
| **Match on an identifier (ID)** | | |
| Perimeter | ID | • Attributes are replaced from the file<br>• Added new object elements |
| Traffic Monitor group | ID | • Attributes are replaced from the file<br>• Added new contacts (Type + Value) |
| LDAP group | ID | • Attributes are replaced from the file if they have been modified in Traffic Monitor where export was performed<br>• Added new contacts (Type + Value) |
| Traffic Monitor person | ID | • Attributes are replaced from the file<br>• Added new contacts (Type + Value) |

| Object | Matching characteristic | Operation with an original object in the System |
|---|---|---|
| LDAP person | ID | • Attributes are replaced from the file if they have been modified in Traffic Monitor where export was performed<br>• Added new contacts (Type + Value) |
| List of web resources | ID | • Attributes are replaced from the file<br>• Added new object elements<br>• The existing objects with no matching ID or name, are not modified |
| Contact (perimeter object) | ID | • Attributes are replaced from the file |
| Web resource | ID | • Attributes are replaced from the file |
| **Match on a value** | | |
| Perimeter | Name | • The existing object is not modified<br>• The object from the file is added as a new object with a modified unique name |
| Traffic Monitor group | Name | • The existing object is not modified<br>• The object from the file is added as a new object with a modified unique name |
| Traffic Monitor person | Name and last name (displayname) | • The existing object is not modified<br>• The object from the file is added as a new object with a unique value of the displayname parameter |
| LDAP person<br>LDAP group | Name and last name (displayname)<br>Name | The perimeter will be imported without this object, as for LDAP objects, only identifiers and modified in Traffic Monitor attributes are exported, not the object itself. |
| List of web resources | Name | • The existing object is not modified<br>• The object from the file is added as a new object with a modified unique name |
| Contact (perimeter object) | Type + Value | • Attributes are not modified |

| Object | Matching characteristic | Operation with an original object in the System |
|---|---|---|
| Web resource | Value | • Attributes are not modified |

## 4.4 Managing Base of Technologies

> **Warning!**
>
> For the settings described in this section to take action, apply the configuration: see *Configuring the System* and *Applying System Configuration*.

**What do you need the base of technologies for?**
Using the base of technologies you can tell the System which information is considered confidential within the company. Disclosure of such information will be considered a violation of the corporate security policy. The System uses the base of technologies to analyse persons' actions and detect violations of the corporate security policy (for example, sending a confidential document outside the company perimeter).

The *base of technologies* is a set of elements (terms, text objects, sample documents, etc.) that are used for analysis of intercepted data.

Besides the base of technologies, the System uses the resource list to analyse persons' actions and detect the misuse of working time (for example, browsing Internet entertainment sites from a work computer). For more information on specifying inappropriate resources, see *Managing Web Resources*.

**Configuring analysis of persons' actions includes the following steps:**

1. Defining the confidential information – creating the base of technologies.
2. Specifying inappropriate resources – creating a list of resources that are considered to be inappropriate use of working time.
3. Creating protected objects based on elements of the base of technologies.

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

**See also:**

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

### 4.4.1 Defining the Confidential Information

**Purpose:**

Add elements to the base of technologies, which the System will use to detect confidential data in interception objects.

**Solution:**

1. Go to a subsection of the **Technologies** section.
2. Depending on a technology, create a new *category* or a *catalogue*.

3. Fill the created category (catalogue) with examples of confidential data, which will indicate security policy violations, or train a classifier.
   For details on managing technology elements, see the articles:
   - Managing Categories and Terms;
   - Managing Text Objects;
   - Managing Sample Documents;
   - Managing Blanks;
   - Managing Stamps;
   - Managing DB Unloadings;
   - Managing Graphical Objects;
   - Managing Autolinguist.
4. If necessary, repeat steps 1-3.
5. When you have finished configuring the base of technology, apply the updated configuration. See *Applying System Configuration*.

See description of each technology in articles of *Technologies Section*.

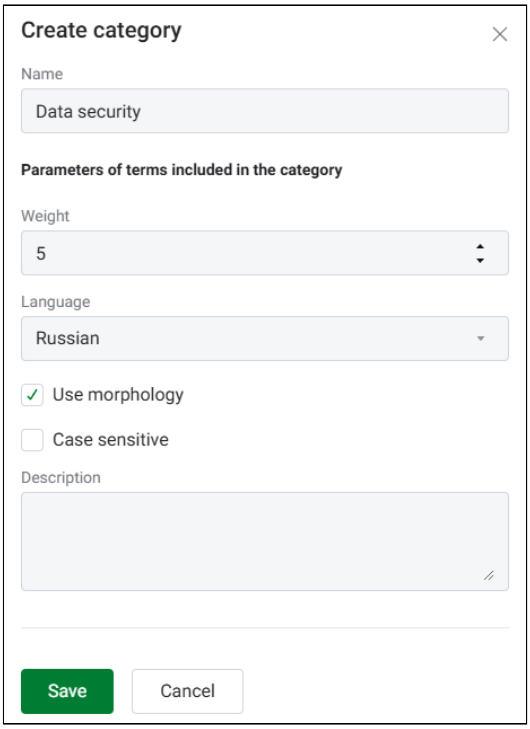
## Managing Categories and Terms

**Purposes:**

- Create a category of terms;
- Create a term within a category;
- Import terms from a file;
- Edit a category/term;
- Delete a category/term;
- Import/export a category.

**Solution:**

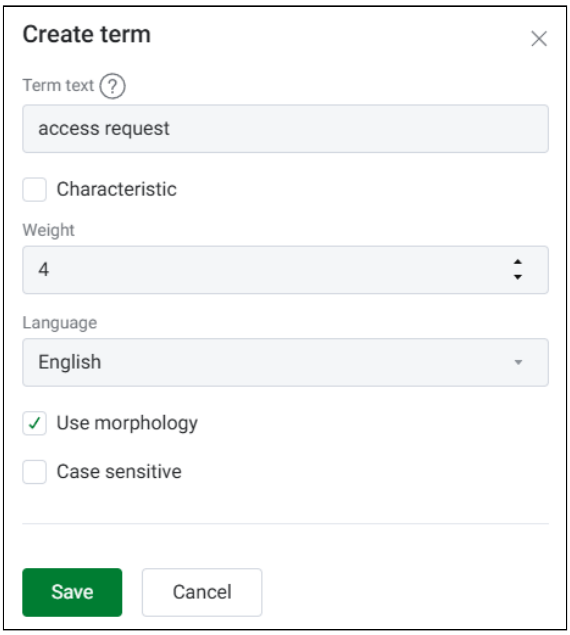
- **To create a category:**
  a. Go to the **Technologies** → **Categories and terms** section.
  b. On the toolbar on the left side of the working area, click  **Create**.
  c. Enter the name.




d. Specify required attributes for the category. See *Categories*.
e. Click **Save**.

- **To create a term:**

a. Go to the **Technologies** → **Categories and terms** section.
b. On the left part of the working area, click the required category. You can add terms only to categories that do not include other nested categories.
c. On the toolbar on the right part of the working area, click  **Create**.
d. Enter the name.




e. Specify attributes:
    - Specify if the term is characteristic.

- If needed, configure the other term parameters: *Weight*, *Language*, *Use morphology*, *Case sensitive*. These attributes were specified in category settings for all the terms within the category, but you can edit attributes for a particular term. See *Terms* for details on attributes.

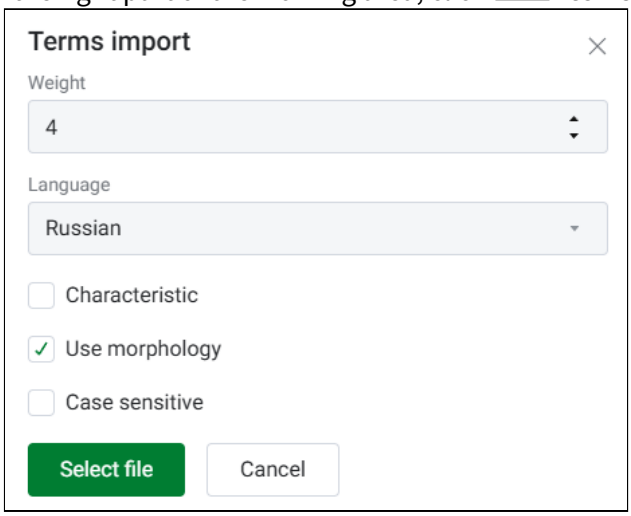
f. Click **Save**.

See also *examples of configuring categories and terms*.

- **To import terms from a file:**

> **Note:**
>
> Apart from creating terms manually, Traffic Monitor supports import of a number of values from file.

a. Make sure the file satisfies the requirements listed in *Recommendations on Preparing a File with Terms* article.
b. Go to the **Technologies** → **Categories and terms** section.
c. In the left part of the working area, select the category in which you are going to add all terms from the file. Import is available only for the categories that do not contain other categories.
d. On the tools panel in the right part of the working area, click **Items bulk upload**.




e. Specify the attributes. See *Terms*.
f. Click **Select file**.
g. Specify the file with terms.
h. Wait until the import of terms is completed.
In case not all the terms were loaded, the System will display the list of terms which failed to load. Click **Download** in the window to save on your computer the file with the terms which:
   - Already exist in the System or have been loaded earlier;
   - Failed to load due to invalid characters;
   - Failed to load due to an error or of the data conflict.

**Examples of configuring categories and terms**

- **Example 1:**
  If you need the System to mark the interception object as *Document issue date* if it contains at least one occurrence of the phrase *document issue date*, then:

  a. Select a required category.
  b. Add the *Document issue date* term to this category.
  c. Enable the **Characteristic** option.

  If intercepted data contains this phrase, the System assigns the *Document issue date* category to the object. If the **Characteristic** option is disabled, then to assign a category to an event, it is required that the event contains at least three different weight terms from the category.

- **Example 2:**
  If you need the System to mark the intercepted object as *Code leakage* if the traffic contains fragments of program code, then:
  1. Create *Code leakage* category.
  2. Add terms like *Procedure, Create Sequence* and *Result* to the category. If you use default parameters, two terms can be not enough to trigger the category. We recommend using at least three terms.

  If during analysis of transmitted data, specified terms are detected, the System assigns the *Code leakage* category to the intercepted object.

Recommendations on Preparing a File with Terms

To import terms from a file, make sure the file meets the requirements:

- File format: TXT.
- File size: 1 byte to 5 MB.
- Encoding: UTF-8 or UTF 16.
- Each term is placed in a separate row.
- Term length: under 256 characters.
- Term text requirements are the same as the requirements for manual creation of terms. See *Terms*.

## Managing Text Objects

**Purposes:**

- Create a catalogue of text objects;
- Create a text object and specify its value;
- Add a system text object to a catalogue;
- Edit a catalogue/text object;
- Delete a catalogue/text object;
- Import/export a catalogue.

**Solution:**

- **To create a catalogue of text objects:**

  a. Go to the **Technologies** → **Text objects** section.
  b. On the toolbar on the left side of the working area, click  **Create**.
  c. Enter the name and description for the catalogue.
  d. Click **Save**.

- **To create a text object and specify its value:**

a. Go to the **Technologies** → **Text objects** section.
b. On the left part of the working area, select a catalogue to which you want to add a text object.
c. On the toolbar on the right side of the working area, click  **Create**.
d. Enter the name and description of the text object.
e. Click **Create**. The new text object will be added to the list.
f. Select the text object from the list and click  **Edit**.
g. Create a template for the text object and specify its parameters. See *Text Object Patterns*.
h. Click **Save**.

- **To add a system text object to the catalogue:**

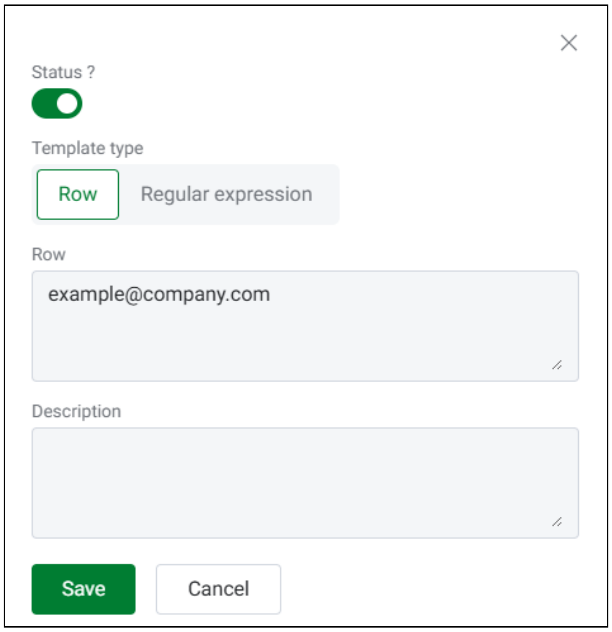
a. Go to the **Technologies** → **Text objects** section.
b. On the left part of the working area, select a catalogue to which you want to add a text object.
c. On the toolbar on the right side of the working area, click  and select **Add system text object**.
d. Select check boxes next to the text objects you want to add.

> **Note:**
>
> To find required text objects in the list, enter the text in the **Search** field.

e. Click **Save**.

**Examples of creating text objects**

- **Example 1:**
  For the System to detect *example@company.com* email address in traffic and define it as *EXAMPLE_MAIL* text object:
  1. Create an active text object *EXAMPLE_MAIL*.
  2. Select the object and switch to the edit mode.
  3. Create a new active template for the text object and specify the following row as the template value: *example@company.com*




- **Example 2:**
  For the System to detect an email address with *company.com* domain in traffic and define it as *COMPANY_MAIL* text object:
  1. Create an active text object *COMPANY_MAIL.*
  2. Select the object and switch to the edit mode.
  3. Create a new active template for the text object and specify the following regular expression as its value: *\w+(@(company.com))*

     > **Note:**
     >
     > For more information on regular expressions, see the Knowledge Base articles: *Syntax of regular expressions* and *Description of macros for text object patterns*.

- **Example 3:**
  For Device Monitor agent to block the transfer of a PDF file if the document has been converted to PDF format using Microsoft Word, the System has to define *Producer="Microsoft Word"* in the extracted PDF document properties as *PDF_PRODUCER* text object. For this:
  1. Create an active text object *PDF_PRODUCER*.
  2. Select the object and switch to the edit mode.
  3. Create a new active template for the text object and specify the following row as the template value: *Producer="Microsoft Word"*.
  4. Add *PDF_PRODUCER* text object to a protection object and create a data protection policy on agents. See *Creating a Protected Object* and *Creating Data Protection Policy on Agents* for details.

  > **Note:**
  >
  > Device Monitor agent extracts information about PDF document properties and adds it to the end of the extracted text.
  >
  > **About extraction of PDF document properties**

The System extracts names and values of the following PDF document properties:

- **Author**
- **Title**
- **Subject**
- **Keywords**
- **Creator** (application in which the original document was created)
- **Producer** (application in which the document was converted to PDF)

Data about each document property is added to the end of the extracted text in the following format: *property name="property value"*. Data about property is added, if property value is specified. Each name-value pair is added on a new line:

```
Author="John Green"
Creator="Microsoft Word"
Keywords="document;project;new"
Producer="Microsoft Word"
Subject="New Draft"
Title="Project Draft"
```

**Warning:** If the value of **Keywords** property has been deleted, the record with the last specified **Keywords** value will still be added to the end of the extracted text.

## Managing Sample Documents

**Purposes:**

- Create a catalogue of sample documents;
- Create a sample document inside the catalogue;
- Update a sample document;
- Edit a catalogue/document;
- Delete a catalogue/document;
- Import/export a catalogue.

**Solution:**

- **To create a catalogue of sample documents:**
  a. Go to **Technologies** → **Sample Documents**.
  b. On the toolbar in the left part of the working area, click  **Create**.
  c. Specify the parameters for the new catalogue. See *Sample Documents*.
  d. Click **Create**.
- **To create a sample document:**
  a. Go to **Technologies** → **Sample Documents**.
  b. On the left part of the working area, select the catalogue inside which you want to create a sample document.
  c. On the toolbar on the right side of the working area, click  and select **According to text data** or **According to all types of data** (may contain text, images, and binary data).

d. Specify the document which you want to use for creating a digital print. Click **Open**. Choose a text file, an image or an archive to be uploaded according to the data type specified in step **c**. The following rules apply when uploading files:
   - If the System does not support the format of the selected file, it will upload the digital fingerprint as binary data.
   - If you upload an archive, the System will add the files from this archive as sample documents.

e. Once uploaded, the sample document will be displayed in the catalogue. The System assigns all required attributes to a newly created sample document by default.

> **Note:**
>
> See file requirements in *Recommendations on Preparing a Sample Document* article.

f. To change the sample document attributes specified by the System, on the toolbar click  **Edit** and change the parameters. See *Sample Documents*.

   Also see *examples of creating sample documents*.

- **To update a sample document, i.e. replace its data with the data from a file:**

a. Go to **Technologies** → **Sample Documents**.
b. On the left side of the working area, select the desired catalogue.
c. In the list on the right side of the working area, select the sample document you want to update.
d. Click  **Edit**.
e. In the edit window, click **Update**.
f. Click **Choose file**.
g. Select a file to use for update and click **Open**. Once the file is uploaded, the System will replace sample document data with data from the file.

**Examples of creating sample documents**

- **Example 1:**
  For the System to react to transferring *Internal regulations of the company* document if the traffic contains at least 30% of text from this document:

a. Select a catalogue of sample documents or create a new one.
b. Add a new document to this catalogue and specify **According to text data**, as the document does not contain images or drawings.
c. Upload *Internal regulations of the company* file as a sample document.
d. Specify the sample document name, e.g., *INTERNAL_COMPANY_REGULATIONS.*
e. For **Text data quotation threshold** attribute, specify **30**.

> **Note:**
>
> The quotation threshold is configured depending on the type of the protected document. Here, a low quotation threshold is specified, as the document consists of many pages and can be transferred in parts.

- ***Example 2:***
  If you need the System to react to transferring *Setup.exe* executable file if the traffic contains at least 10% of the binary content from this file:

  a. Select a catalogue of sample documents or create a new one.
  b. Add a new document to this catalogue and specify **According to text data**.
  c. Upload *Setup.exe* file as a sample document.
  d. Specify the sample document name, e.g., *SETUP_EXE.*
  e. For **Text data quotation threshold** attribute, specify **10**.

Recommendations on Preparing a Sample Document

A sample document has to meet the requirements:

- Data size:
  - Text data: from 128 bytes to 30 MB
  - Binary data: from 128 bytes to 128 MB
  - Vector data: from 300 KB (800 primitives)
- Length of simple text for text data: from 10 characters
- Image size: from 100 pixels on one side
- Image sides ratio: up to 5:1

## Managing Blanks

**Purpose:**

- Create a catalogue of blanks;
- Create a blank;
- Create a detection condition;
- Update a blank;
- Edit a catalogue/blank;
- Delete a catalogue/blank;
- Import/export a catalogue.

**Solution:**

- **To create a catalogue of blanks:**

  a. Go to **Technologies** → **Blanks**.
  b. On the toolbar on the left part of the working area, click  **Create**.
  c. Type the name and description of the catalogue.
  d. Click **Save**.

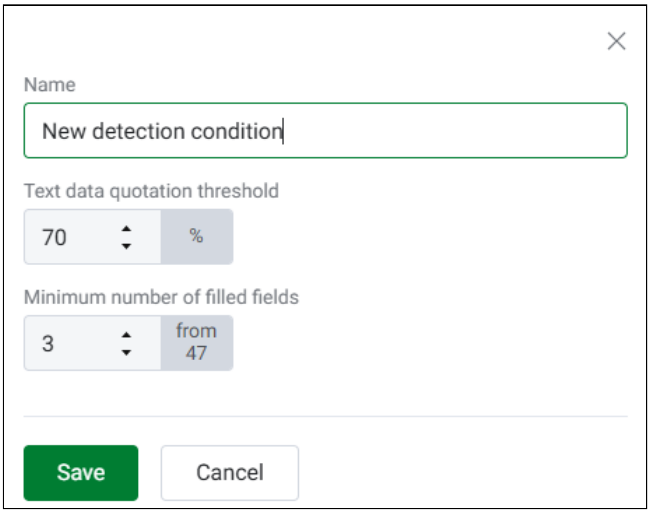
- **To create a blank:**

  a. Go to **Technologies** → **Blanks**.
  b. On the left part of the working area, select a catalogue inside which you want to create a blank.
  c. On the toolbar on the right part of the working area, click  **Create**.
  d. Select a document to use as a blank. You can upload a document in one of the following formats: DOC, DOCX, DOT, DOTM, DOTX, XLS, XLSX, XLT, XLTM, XLTX, ODS, ODT, RTF, TXT, VSD, HTML, HTM, PDF, CHM.
  e. Click **Open**. Once the System uploads the file, it will display it in the catalogue.

f. To change default attributes of the blank specified by the System, click **Edit** on the toolbar and change attributes as needed. For details on attributes, see *Blanks*.

- **To create a detection condition:**

a. Go to **Technologies** → **Blanks**.
b. On the left side of the working area, select the desired catalogue.
c. In the list on the right part of the working area, select the blank for which you want to create the detection condition.
d. Click **Edit**.
e. On the right part of the working area click **Create**.
f. Enter the name and specify the parameters of detection conditions:
   - **Text data quotation threshold**
   - **Minimum number of filled fields**




g. Click **Save**.
h. To add several detection conditions, repeat actions *e-g*. It is recommended to create no more than 20 detection conditions per one blank.
i. Click **Save**.

- **To update a blank:**

a. Go to **Technologies** → **Blanks**.
b. On the left side of the working area, select the desired catalogue.
c. In the list on the right part of the working area, select the blank you want to update.
d. Click **Edit**.
e. Click **Update**.
f. Click **Choose file**.
g. Select a file for update and click **Open**. Once the file is uploaded, the System will replace the data in the blank with the data from the file.

**Example:**

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

1. Create *RECRUITMENT_CHECKLIST* blank.
2. Load *Recruitment checklist* document file as a blank.

3. Create a detection condition with **Minimum number of filled fields = 0**. Also you may edit the default condition which is created in accordance with the blank.
4. Create a *protected object* based on the *RECRUITMENT_CHECKLIST* blank and specify the detection condition you require.

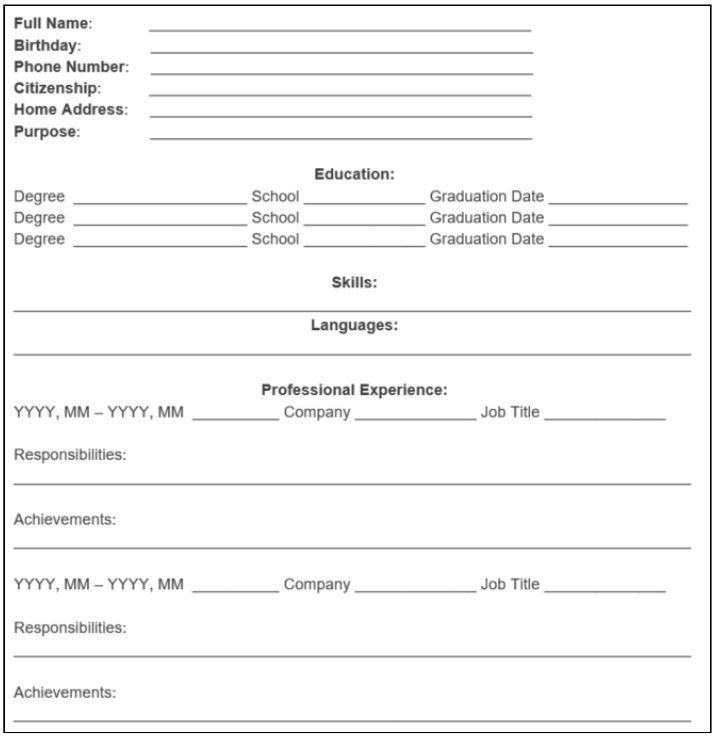
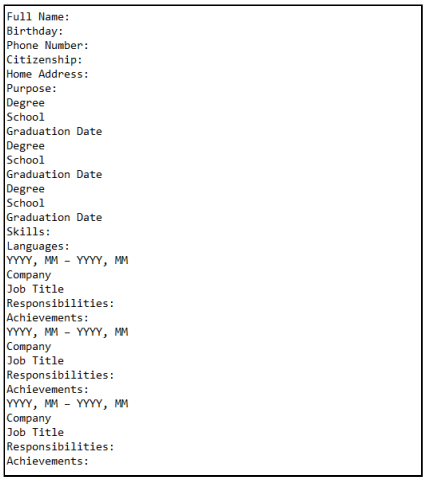
Recommendations on Preparing Blanks

For the System to detect blanks in intercepted objects, make sure the file with a blank satisfies the following conditions:

- Size:
  - Text data: up to 30 MB;
  - Vector data: from 300 KB (800 primitives);
- The blank is not filled in.
- The blank does not contain a header, only fields.
- The blank contains separators of one of the types:
  - Three subsequent whitespaces;
  - Three subsequent underscores;
  - Newline character: `\r\n` or `\n`.
- The number of fields that contain two or more words is under three.
- File format is TXT. Documents created in MS Word or Excel may contain metadata, which the System may recognize as separate fields.

**Example of preparing a reference blank:**

- **Example 1:**
  You want the System to detect resumes of the following sample.
  Enter the fields from the resume into separate lines of the text document. Some fields, like education or job experience details, are repeated. This will not affect detection results, you can enter them several times.

| Resume Sample | Reference Blank Loaded in the System |
| --- | --- |
|  |  |

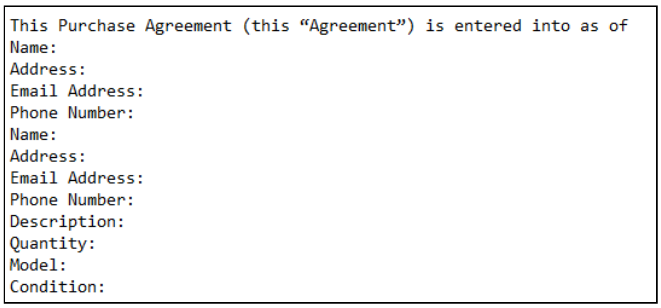




**Note:**

The System defines any text chunks between the fields as field values. Hence, if you want to detect if the fields are filled in, enter such chunks into the reference blank as well. For example, enter a separate line ***Education:*** between ***Purpose:*** and ***Degree*** fields. Otherwise, the System will define ***Education:*** as the value of ***Purpose*** field.

- **Example 2:**
  You want the System to detect purchase agreements of the following sample.
  The fields in the sample already contain examples of answers, which are to be replaced with relevant data by those who will fill the agreement. The reference blank should not contain this text.
  With this blank, the System will detect the agreement in intercepted data. However, there might be ambiguous indication of filled fields because you cannot predict how much people will change the example answers.

| Agreement Sample | Reference Blank Loaded in the System |
| --- | --- |
|  |  |





## Managing Stamps

**Purposes:**

- Create a catalogue of stamps;
- Create a stamp;
- Edit a catalogue/stamp;
- Delete a catalogue/stamp;
- Import/export a catalogue.

**Solution:**

- **To create a catalogue of stamps:**
  a. Go to **Technologies** → **Stamps**.
  b. On the toolbar on the left side of the working area, click  **Create**.
  c. Specify parameters for the new catalogue.
  d. Click **Create**.
- **To create a stamp:**
  a. Make sure the stamp satisfies the requirements listed in *Recommendations on Preparing Stamps* article.
  b. Go to **Technologies** → **Stamps**.
  c. On the left part of the working area, select the catalogue inside which you want to create a stamp.
  d. On the toolbar in the right part of the working area, click  **Create**.
  e. Select a file to use as a stamp sample and click **Open**. The file must contain only one stamp image.
  f. Once the stamp is uploaded, the System will display the stamp in the catalogue.
  g. To change the default stamp attributes, on the toolbar click  **Edit** and change the required attributes.

**Example:**

To protect legal documents sealed with a company stamp:

1. Prepare a file with the image of the company stamp.
2. In **Technologies** → **Stamps** section, select a catalogue or create a new one.
3. Create a new stamp in the catalogue and upload the prepared file with the stamp image.
4. Include the stamp in a *protected object*.

Recommendations on Preparing Stamps

For correct operation of the technology, the stamp should meet the requirements:

- Stamp resolution: at least 150 DPI
- Minimum image size: 500x500 pixels
- Maximum image size: 30 MB
- Stamp image should be against a white background with a minimum amount of white colour along the stamp edges.
- All elements of the stamp should be clearly visible.
- A stamp should have a solid frame around its perimeter.
- A *triangular* stamp should face downwards, its base should be horizontal.

## Managing DB Unloadings

**Purpose:**

- Create a catalogue of unloadings;
- Create a database unloading;
- Update the unloading;
- Move/copy the unloading;
- Edit a catalogue/unloading;
- Delete a catalogue/unloading;
- Import/export a catalogue.

**Solution:**

- **To create a catalogue of unloadings:**
  a. Go **Technologies** → **DB Unloadings**.
  b. On the toolbar on the left side of the working area, click  **Create**.
  c. Enter the name and description for the catalogue.
  d. Click **Save**.
- **To create a database unloading:**
  a. Go to **Technologies** → **DB Unloadings**.
  b. On the left side of the working area, select the group to which you want to add the unloading.
  c. On the toolbar in the right part of the working area, click  **Create**.
  d. Select a file to upload and click **Open**. See unloading file requirements in *Recommendations on Preparing Unloadings* article.
  e. Once the file is uploaded, select the unloading and click  **Edit**.
  f. On the toolbar under the **Conditions of unloading detection** caption, click **Add**.

g. Specify the following parameters:
    i. *Condition name*
    ii. *Minimal quantity of rows*
    iii. *Search type*
    iv. *Detection condition*

> **Note:**
>
> See *Detection Conditions for Unloading* for parameter description.

h. Click **Save** to close the dialogue for creating conditions.
i. If needed, specify additional detection conditions (under 20), repeating steps *f-h*. In case of multiple conditions, one satisfied condition is sufficient to associate the interception object with this unloading.
j. Click **Save** to save the unloading parameters.

> **Note:**
>
> When the System uploads a file, it compiles it. The following formula can approximately calculate the amount of RAM consumed during compilation:
>
> `Memory(GB) = 0.05 * unique_words(M) * cells(M)`, where M stands for million.
>
> For example, 10 million cells can fit in a table with 2 columns and 5 million rows, or in a table with 4 columns and 2.5 million rows.

- **To update the unloading:**

a. Go to **Technologies** → **DB Unloadings**.
b. On the left side of the working area, select the desired catalogue.
c. In the list in the right part of the working area, select the unloading you want to update.
d. Click  **Edit**.
e. Click **Update**.
f. Specify the desired update mode: **Adding new records** or **Removing old records and adding new ones**.
g. Press **Choose file**.
h. Select a file that will be used for update and click **Open**. Once the file is uploaded, the System will update the unloading data using the uploaded file according to the selected update mode.

- **To move/copy the unloading:**

a. Go to **Technologies** → **DB Unloadings**.
b. On the left side of the working area, select the catalogue in which the unloading is located.
c. Click  next to the unloading name and hold down while moving the unloading to the new location of the catalogue. Release the mouse button.
d. Click **Move** or **Copy**. The unloading will be moved/copied to the catalogue.

> **Note:**
>
> If you edit or update the original unloading, all copies of that unloading will also be changed. If you edit or update a copy of an unloading, the original and all copies of that unloading will also be changed.

Recommendations on Preparing Unloadings

In order for the System to detect data from an unloading in analyzed texts, the unloading should have the following characteristics:

- File format: CSV or TSV
- File size: from 128 bytes to 300 MB
- Number of columns: under 32
- Number of words in one cell: under 256
- Number of rows:
  - under 1 million for 8 GB RAM server
  - under 3.5 million for 16 GB RAM server
- Number of characters in the table heading (first row) is under 4000, including column names and additional characters used by CSV and TSV formats for column spacing: quotation marks, commas

In case you want the System to check whether the data recipient matches the data owner and\or detect data represented in a format different from the one specified in the unloading, prepare an *unloading with keys*. Take additional actions:

- Add the code line: "`DB Table with Row keys`" to the beginning of the file. The code line enables the System to define the last column of the unloading as keys by which it should verify recipients.
- Pad the code line with tabs to the total number of columns in the unloading. For example, if an unloading has 5 columns (4 columns with protected data and 1 column with keys), then you need to add 4 tabs in the first line after "`DB Table with Row keys`".
- In the last cell of each line, specify an email address as a key. Recommended length of the field with the key is under 1000 characters. If there is no key in some row, you will see an error message when trying to add the unloading.
- Make sure separators and encoding are correct:
  - Lines must be separated by a newline
  - Columns in a row must be separated by tabs
  - File encoding must be UTF-16LE or UTF-8
- If you want the System to detect data represented in different formats, specify mobile phone, bank card and bank account numbers in the following format:
  - Mobile phone number: 11 digits successively, without separators; for example, `79121234567`
  - Bank card number: 16 digits successively, without separators; for example, `4000001234567890`
  - Bank account number: 20 digits successively, without separators; for example, `40817810099910001234`

## Managing Graphical Objects

**Purpose:**

- Configure the automatic classifier of graphical objects:
  - Create a category of text objects;
  - Upload images to a category;
  - Train the classifier;
  - Test how the classifier works on a sample image.
- Edit a category/object;
- Delete a category/object;
- Import/export a category.

**Solution:**

To configure the automatic classifier of graphical objects:

1. Create a category of text objects:
   a. Go to **Technologies** → **Graphical objects**.
   b. On the toolbar in the left part of the working area, click  **Create**.
   c. Specify the name and description of the new category.
   d. Click **Save**.
2. Upload images:
   a. Make sure your image collection satisfies the requirements listed in *Recommendations on Preparing Image Collection* article.
   b. In the left part of the working area, click the category to which you want to add images.
   c. On the toolbar in the right part of the working area, click  **Add image**.
   d. Select one or more files on a disk and click **Open**. Choose files from which graphical data can be extracted.
   e. Wait for the System to add the selected files to the category. A pop-up window on the right displays the process status.
3. Train the classifier:
   a. Create at least two categories that contain one or more images.
   b. Click  **Learning** and wait until the end of the training process. The process can take several minutes. After the learning, there can be errors in some categories. In this case, delete all images from such a category, add new images and train the classifier again.
   c. In the upper part of the working area, click **Apply**.
   d. In the **Applying configuration** window, check out the new configuration and click **Apply**. The new configuration will become the active one on the server.
4. Test how the classifier works on a sample image:
   a. In the left part of the working area, click  **Check document**.
   b. Click **Start new check**.
   c. Select one or more files and click **Open**. Do not select archives.
   d. Wait until the check is complete and view the results. The technology will define to which categories the loaded images relate. You can add these images to those categories and initiate the learning process again.

> **Note:**
>
> You cannot test how the classifier detects uneditable categories, which are detected with *Image search within an image* technology. For more details, see *Graphical Objects*.

**Enhancing the classifier quality**

- In case the classifier fails to define a certain category or misdefines categories, upload additional files to a category or delete previously added files. Then retrain the classifier.
- *Decreasing false-positives* category balances out other categories, which improves the quality of the classifier. Move images that cause false positive responses and do not belong to any category to this one.

Recommendations on Preparing Image Collection

When preparing an image collection for the classifier, follow these recommendations:

- Each category should contain at least 50 images.
- A category should not contain images from other categories.
- Categories should be of approximately same size.
- Learning time and System performance depend on the number of uploaded images.
- Minimum image size: 150 pixels on one side.
- Maximum image resolution: 10,000x10,000 pixels.
- Maximum image aspect ratio: 8:1.
- Allowed image rotation: 90±10, 180±10, 270±10 degrees.
- Supported image types: BMP, GIF, JPEG, JP2, PBM, PGM, PNG, PPM, RAS, TIFF. Note that:
  - For archives, the System creates a separate document for each extracted file and places them to the category that was selected when creating the document.
  - For encrypted archives, the System does not create a document or creates one with an error.

## Managing Autolinguist

**Purpose:**

- Configure the automatic classifier of graphical objects:
  - Create a category in Autolinguist;
  - Upload documents to a category;
  - Train the classifier;
  - Test how the classifier works on a sample document.
- Edit a category/document;
- Delete a category/document;
- Import/export a category.

**Solution:**

To configure Autolinguist:

1. Create a category in Autolinguist:
   a. Go to **Technologies** → **Autolinguist**.
   b. On the tool bar on the left of the working area, click  **Create**.
   c. Enter the name and description of the new category.
   d. Click **Save**.
2. Upload documents to the category:
   a. Make sure your text collection follows the recommendations listed in *Recommendations on Preparing Autolinguist Text Collection* article.
   b. Go to **Technologies** → **Autolinguist**.

c. On the left side of the working area, select the category to which you want to add the document.
d. On the tool bar on the right side of the working area, click  **Add document**.
e. Select one or several files and click **Open**. Use the documents from which text data can be extracted.
f. Wait for the System to add the selected files to the category. A pop-up window on the right displays the process status.

3. Train the classifier on the new collection:
   a. Create at least two categories containing one or several standard documents.
   b. Click  **Learning** and wait until the end of the process. It may take a few minutes. After the learning, there can be errors in some categories. In this case, delete all documents from such a category, add new documents and train the classifier again. The System displays the quality percentage of detecting each category and the entire collection.
   c. On the top of the working area, click **Apply**.
   d. In **Apply configuration** window, click **Apply**. The System will activate the new configuration.
4. Test how the classifier works on a sample document:
   a. Click  **Check document.**
   b. Click **Start new check**.
   c. Select one or several files and click **Open**. The size of a file should be from 256 bytes up to 26 MB.
   d. Wait untill the end of the process and view the results.
   e. Apply the new configuration. The technology will define to which categories the loaded documents relate. You can add these documents to those categories and initiate the learning process again.

**Enhancing the classifier quality**

In case the classifier fails to define a certain category or misdefines categories, upload additional files to a category or delete previously added files. Then retrain the classifier.

Recommendations on Preparing Autolinguist Text Collection

For correct operation of Autolinguist, follow these recommendations:

- For training, the classifier requires at least two categories, each category should contain at least one document.
- Document size: from 256 bytes to 26 MB.
- Text in the document should contain at least 5 words, each word should contain at least 3 symbols.
- The number of documents and their contents affect the quality of learning. The more documents on a similar topic a category contains, the better the accuracy. On the other hand, the number of documents affects learning time and System performance.
- When uploading the files, note that:
  - For archives, the System creates a separate document for each extracted file and places them in the category that was selected when creating the document.
  - For encrypted archives, the System does not create a document or creates one with an error.
  - For *Container* type files, the System creates a single document.

### 4.4.2 Exporting and Importing the Base of Technologies

**Purpose:**

- Save the archive containing the base of *technologies* to a hard drive of the computer;
- Load the base of technologies, which is stored on your computer as an archive with `.cfb` extension, for using in the InfoWatch Traffic Monitor management console.

> **Note:**
>
> You cannot export the base of technologies, if the System configuration is being edited. You cannot import the base of technologies, if the System configuration has not been applied. Otherwise, you will receive an error message.

**To export the base of technologies:**

1. Go to a subsection of the **Technologies** section (**Categories and terms**, **Text objects**, **Sample Documents**, **Blanks**, **Stamps**, **Database Unloadings**, or **Graphical Objects**).
2. On the toolbar on the left part of the workspace, click  and, in the drop-down list, select **Export**.
3. Preparing the base of technologies export will start. After the preparation is finished, an archive with `.cfb` extension will be loaded to your computer `.` This file contains the following elements:
   - categories and terms;
   - text objects, including pre-installed ones;
   - sample documents;
   - blanks;
   - stamps;
   - database unloadings;
   - graphical objects.
4. The structure of catalogues is preserved for all elements.

> **Warning!**
>
> As a result, the whole base of technologies will be exported, not a selected section only.
>
> The base of technologies from the last applied configuration is exported (see *Configuring the System*).

**To import the base of technologies which is stored on your computer as an archive with `.cfb` extension:**

1. Go to a subsection of the **Technologies** section (**Categories and terms**, **Text objects**, **Sample Documents**, **Blanks**, **Stamps**, **Database Unloadings** , or **Graphical Objects** ) .
2. On the toolbar on the left part of the workspace, click  and in the drop-down list select **Import**.
3. In the **Open** dialog window, select an archive with `.cfb` extension that you want to upload.
4. Click **Open** and wait till the data is loaded into the System.

**Note:**

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

**Features of merging data during import:**

1. For catalogues, the following items missing in the System are added:
   a) child catalogues;
   b) elements of technologies.
2. For category, the terms that are missing in the System will be added.
3. For text object, templates that are missing in the System will be added.

   **Note:**

   The verifying functions that are present in the System will be replaced by functions from the file.

4. To add sectoral and customized categories and terms into the System, you should use XML files that are compatible with InfoWatch Traffic Monitor System. After this XML file has been uploaded into the System, all appropriate categories and terms are to be automatically added to the System's management console, **Technologies** section (**Categories and terms**, **Text objects**, **Sample Documents**, **Blanks**, **Stamps**, **Database Unloadings, or Graphical Objects** ).

   **Note:**

   Sectoral and customized categories and terms used for InfoWatch Traffic Monitor are unique and they cannot be imported to other DLP systems at present.

5. For a DB unloading, representations of the sample unloading will be added, if the contents of unloading in the System and the file are the same.

   **Warning!**

   Unloadings created in Traffic Monitor with a version lower than 7.4 are considered obsolete.

   Obsolete unloadings are marked with .

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

## 4.5 Managing Protected Objects

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

**What are protected objects needed for:**

The protected object activates the analysis using the technology. If there are several technologies, you need to set up logical conditions between them.

If the technology is not included in any protected object, it does not work during the analysis.

To analyze data for several elements of analysis, combine them in a protected object: for example, a sample document, a text object, and a database unloading. You can also specify the elements, detection of which means for the System not to detect protected objects (see *Adding Detection Conditions*).

**Working with protected objects includes the following actions:**

| Action | Description |
|---|---|
| Creating a Catalogue of Protected Objects | Creating a catalogue to which protected objects will be added |
| Creating a Protected Object | Creating a protected object and specifying its parameters |
| Adding Elements of Technologies | Adding elements of analysis to a protected object |
| Adding Detection Conditions | Specifying conditions for detecting added elements of analysis |
| Creating Policies for Protected Objects and Their Catalogues | Creating a data protection policy for selected protected objects and their catalogues |
| Importing and Exporting Protected Objects | Importing and exporting catalogue structure, protected objects included in these catalogues and elements of analysis used in these protected objects |
| Activating and Deactivating Protected Objects | Changing status of protected objects and their catalogues |

**See also:**

- Protected Objects Section - on the section where you can manage protected objects.

### 4.5.1 Creating a Catalogue of Protected Objects

**Purpose:**

Create a catalogue that will contain protected objects.

**Solution:**

1. Go to the **Protected objects** section.
2. In the left part of the workspace, click  above the list of catalogues.

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

3. In the **Create catalogue** window, specify the catalogue attributes.
4. Click **Create**.

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

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

**Additional information:**

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

- Editing Element;
- Deleting Element.

## 4.5.2 Creating a Protected Object

**Purpose:**

Create a protected object based on elements of technologies that are present in the System.

**Solution:**

1. Go to the **Protected objects** section.
2. In the left part of the workspace, select a catalogue to which you want to add a new protected object, or create a new catalogue (see *Creating a Catalogue of Protected Objects*).
3. In the right part of the workspace, click + **Create protected object**. A new page will open.
4. In the left part of the workspace:
   - Select the protected object creation mode:
     - Standard (default mode). In case you select this mode, then one protected object will be created. You can specify its name and set up its detection conditions.
     - Multiple. In case you select this mode:
       - for each of selected technology elements, a separate protected object will be created;
       - the attributes of created protected objects will be generated automatically;
       - the names of these objects will be generated based on the technology and element name, for example: «Text object: Credit card number».

- In case you need to expand the list of catalogues or change the previously selected catalogue, in the **Catalogues** drop-down list mark all catalogues that will include the new protected object.
- Enter the name of the protected object, and, if required, its description (for Standard mode).
- Detection is enabled by default in case at least one of the selected catalogues has *Active* status. In case this is a draft of a protected object, you can temporarily disable it by switching **Detection** toggle.

5. In the right part of the workspace:
    a. On **Analysis elements** tab, select elements based on which the protected object will be created (see *Adding Elements of Technologies*).
    b. On **Detection conditions** tab, specify conditions under which protected objects should be detected in intercepted data (for details, see *Adding Detection Conditions*).
6. Click **Create protected object**.

You can also create a new protected object based on an existing one. For this:

1. In the entry of the protected object, click  and select **Create from template**. A new page with prefilled fields will open.
2. Change the protected object name and adjust other parameters as required.

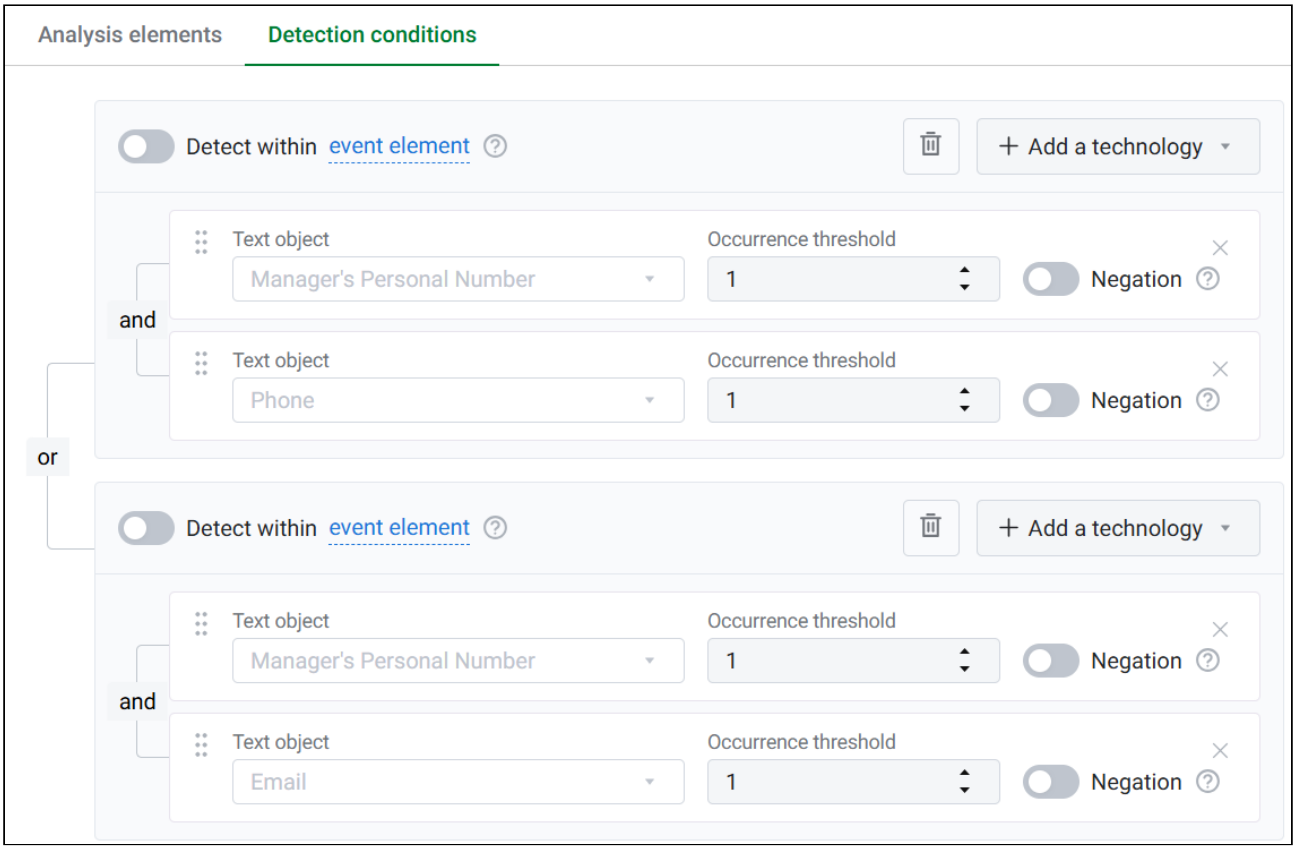
***Example 1:***

You need to create a protected object *Manager's Personal Data* that should be detected in the System when one of the following conditions is fulfilled:

- Interception object contains a personal number of the manager and an email;
- Interception object contains a personal number of the manager and a phone number.

For this:

1. Create a new protected object and add the following elements of technologies:
    - Text object *Manager's Personal Number*
    - Text object *Email*
    - Text object *Phone*
2. Specify the following detection conditions for the elements of technologies:



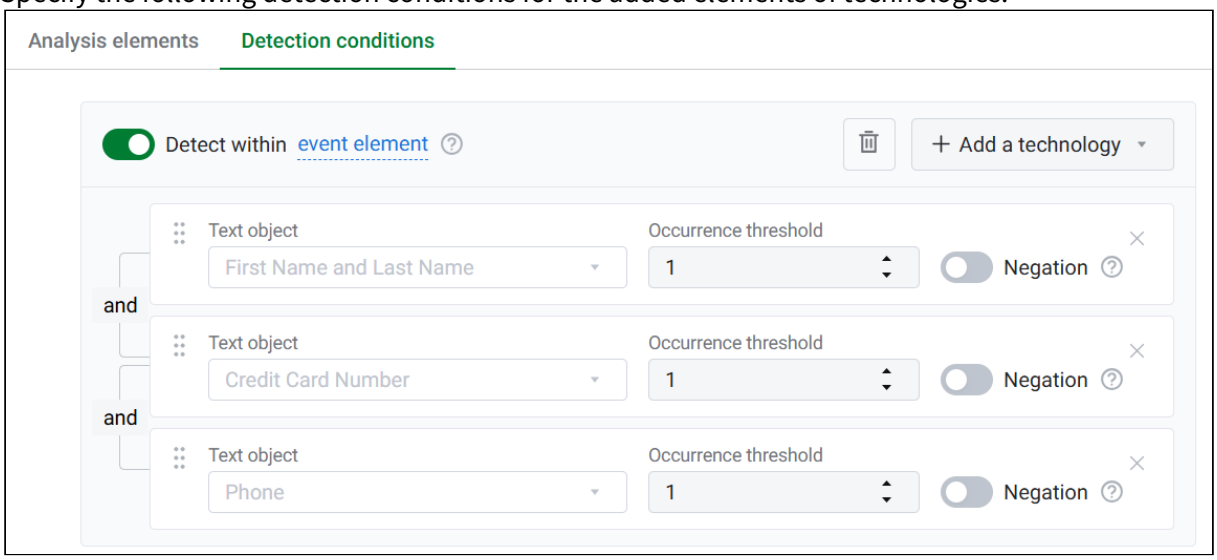

***Example 2:***

You need to create a protected object that should be detected in the System when the following condition is fulfilled: intercepted object within one element of event contains first and last name, phone and credit card number.

For this:

1. Create protected object and add elements of technologies to it:
    - Text object *First Name and Last Name*
    - Text object *Phone*
    - Text object *Credit Card Number*

2. Specify the following detection conditions for the added elements of technologies:




Pay attention that to satisfy the condition you must enable the function **Detect within event element**. In this case the System will detect the protected object if all protected data is detected in one element, for example in email body or attached file.

***Example 3***:

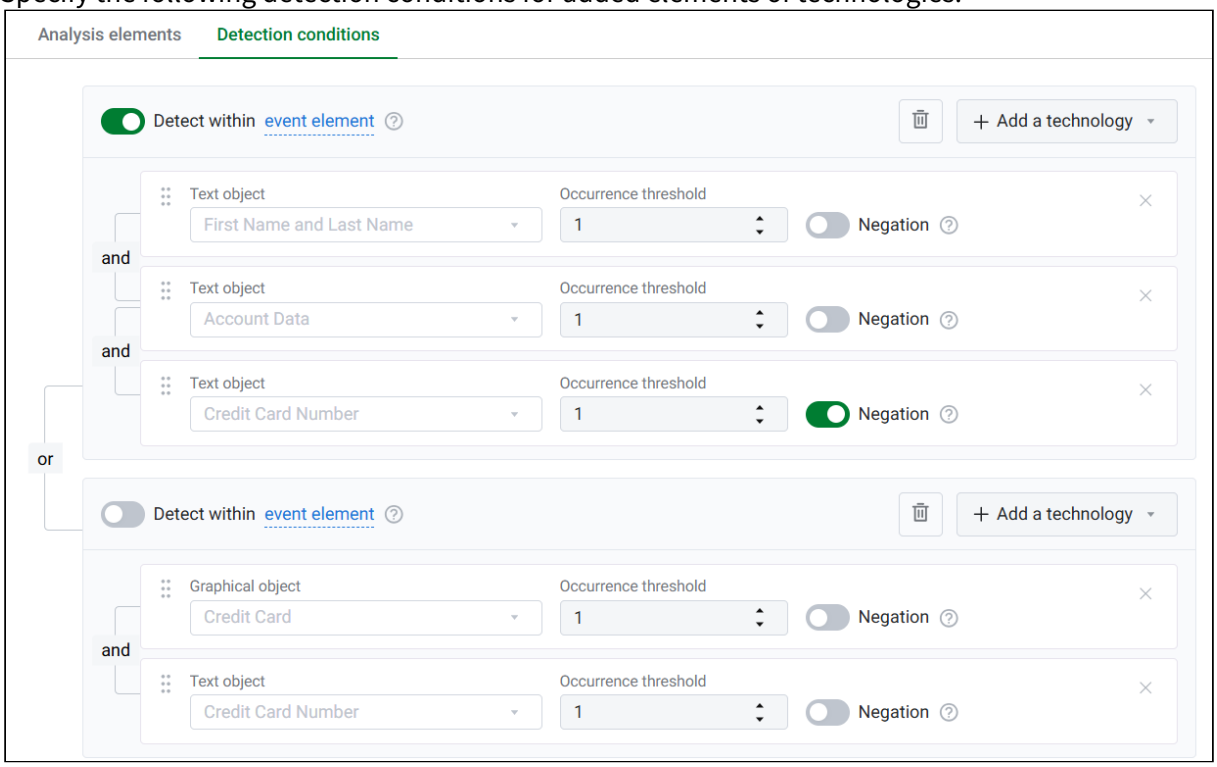
You need to create a protected object that should be detected in the System when one of the following conditions is fulfilled:

- Detected object for one element of event contains first and last name, account data, but must not contain a credit card number;
- Detected object contains a credit card number and its image.

For this:

1. Create a protected object and add elements of technologies to it:
    - Text object *First Name and Last Name*
    - Text object *Account Data*
    - Text object *Credit Card Number*
    - Graphical object *Credit Card*

2. Specify the following detection conditions for added elements of technologies:




Pay attention that to complete the first condition, you must enable the function **Detect within event element** and enable **Negation** for the element of technologies the presence of which cancels detection. In this case protected object will be detected by the System by the first condition only if one element of event contains all elements of technologies without negation, and element containing negation **must not** be there.

If in one element of event all listed text objects are detected, protected object will not be detected by the System by the first condition. But if in the protected object a specified graphic object will also be detected, the System detects a protected object by the second condition. Negation from the first condition does not interfere detection by second condition.

***Example 4***:

The following warning message is used within the company's emails:

> *CONFIDENTIAL*
>
> *This message was sent with corporate email service that belongs to company. This information transmitted (including all attachments) is intended only for the person whom it is addressed and may contain confidential data protected by the Data Protection Act. Hereby notified, that any review, retransmission, dissemination or other use of, or taking of any action in reliance upon this information by persons or entities other than the intended recipient is prohibited.*

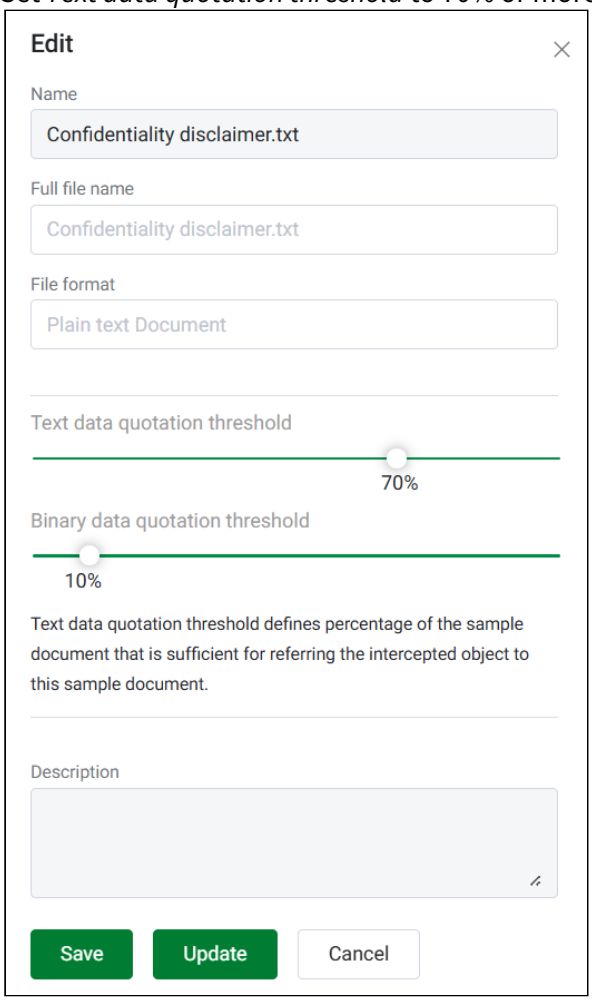
You need to create a protected object for confidential documents detecting.

Traffic Monitor contains *Strictly Confidential* protected object which is intended to detect any documents/messages containing the stamps *Confidential*, *Strictly confidential*, *Confidential information*, *Strictly confidential information*, *For internal use only*, *For official use only*, *Commercial secret*, *Trade secret*. Using this, you will get a lot of false positives and distortion of statistics because of the presence of the term *Confidential* in the email disclaimer.

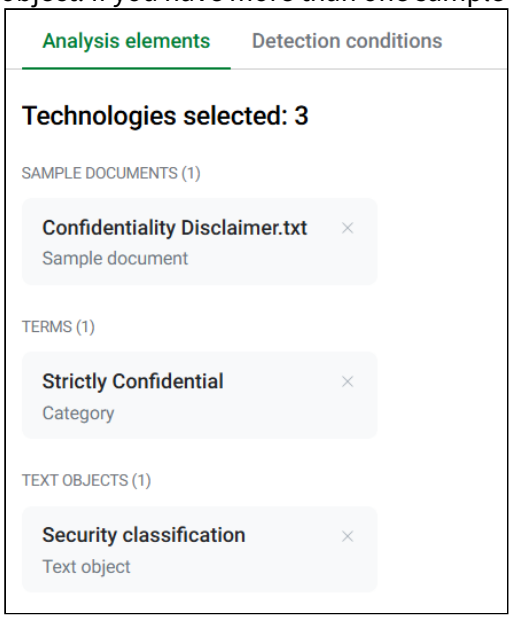
To correctly configure the detection conditions of the protected object:

1. In the **Technologies** -> **Sample documents** section, create a sample document *Confidentiality disclaimer* using the text file containing the email disclaimer.

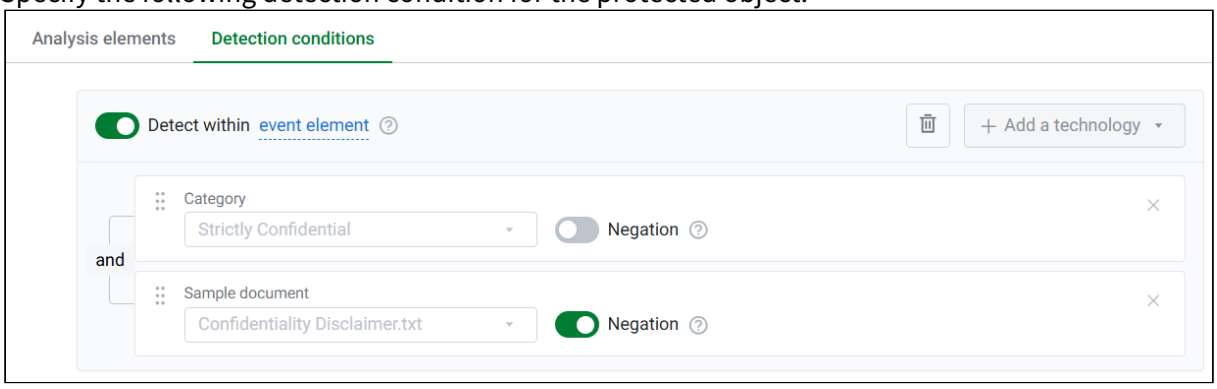
2. Set *Text data quotation threshold* to 70% or more.




3. Create a sample document for each disclaimer or other object, distorting the statistics.
4. In the **Protected objects** section, choose the "*Security label*" catalogue.
5. Add the "*Confidentiality disclaimer*" sample document to the "*Strictly Confidential*" protected object. If you have more than one sample document, add a catalogue of sample documents.



6. Specify the following detection condition for the protected object:




If you enable **Negation** for the analysis element *Confidentiality disclaimer*, the System will detect events with the term *Confidential* but without the confidentiality disclaimer. Thus false positives will not occur.

Pay attention that for this condition it is recommended to enable function *Detect within event elements*. Then the document containing the term *Confidential* will be detected if it is attached to the email with the confidentiality disclaimer. If you disable this function, the whole event will be ignored.

**Additional information:**

Protected objects can be edited and deleted by standard means, for more details please see:

- Editing Element;
- Deleting Element.

## 4.5.3 Adding Elements of Technologies

**Purpose:**

Add elements of technologies to a protected object.

**Solution:**

You can add elements of technologies when creating a new protected object or when editing an earlier created protected object (see *Creating Protected Objects*).

1. In the edit/creating window, open a tab with desired elements.
2. Select the elements you want to add.

> **Note:**
>
> When you select a category that contains subcategories (the **Category** tab), all subcategories will also be selected. If you want to add particular subcategories, click on the arrow to the left of the category name, and, from the drop-down list, select check boxes in required fields.
>
> This can be used when selecting catalogues and sub-catalogues.
>
> Adding catalogue as protected object is possible for sample documents, stamps, text objects, blanks and DB unloadings.
>
> When adding a catalogue to protected objects, all elements of technologies which are a part of the catalogue will be included as well.

If new elements of technologies will be added after the protected object was created within the working catalogue, they will also let detecting the protected object within the intercepted traffic.

If you delete elements of technologies from the catalogue that was added into protected object the detection by deleted elements will be finished.

3. To create a protected object based on several technologies, repeat steps 1-2 until you add all desired elements.
4. Click **Create protected object/Save**.

You can delete elements or technologies catalogues which were added earlier. For this, on the **Elements of technologies** tab, click the cross on the element's tile.

### 4.5.4 Adding Detection Conditions

**Reference information:**

A protected object can be detected in the event if:

1. The protected object status is *Active*.
2. The event contains elements of technologies included in the protected object with respect to specified detection conditions.

A catalogue of protected objects will be detected in the event if:

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

**Note:**

When exporting a protected object (see *Importing and Exporting Protected Objects*), the protected object includes only those elements of technologies for which detection conditions are specified.

**Purpose:**

Add detection conditions for a protected object.

**Solution:**

Detection conditions are added when creating protected objects. After you add selected elements of technologies to the protected object (see *Adding Elements of Technologies*), you need to specify detection conditions. You can also add detection conditions when editing an earlier created protected object.

To add detection conditions for a protected object:

1. On the **Detection Conditions** tab, click **+Add condition**.
2. On the condition panel click **+Add a technology** and select the required element from the drop-down. The selected element will be added to the list of conditions. For some elements of technologies, you can specify additional detection conditions (see *Detection conditions*).
3. If there are several elements of technologies in the protected object, you can add detection conditions for the other elements in one of the following ways:
    - If you need conditions to be combined with a conjunction (logical "AND"), add conditions as described in step 2.
      In this case, all added conditions will be placed in the same **Condition** block and combined with a conjunction.

- If you need conditions (or groups of conditions) to be combined with a disjunction (logical “OR"), click the **+ Add condition** button.
  A new **Condition** block will be added. In this block, you can add conditions as described in step 2.
  In this case, all the **Condition** blocks will be combined with each other with a disjunction, and conditions within a single block will be combined with a conjunction.
- If you need the System to detect protected object if the condition is complete within one element of event (email body, file, communication in messenger), click the **Detect within event element** button.
- If you need the System **not** to detect protected object when the specified element of technology is detected, then you should enable **Negation** for this element.

> **Note:**
>
> At least one element without negation is required in the detection condition.
>
> If protected object is added to the policy of data protection on Agents, you cannot enable detection within the event element.
>
> Protected objects with enabled negation are not triggered in case of:
>
> - Device Monitor version 7.9 or earlier
>   and/or
> - Agents installed on workstations running Linux-family OS.

4. Click **Create protected object** if you are in the create mode, or **Save** if you are in the edit mode.

**Additional information:**

If you need to delete conditions click ✕ in the upper right corner of the panel with the required condition.

## 4.5.5 Creating Policies for Protected Objects and Their Catalogues

**Purpose:**

Create a policy for protected objects and their catalogues directly from the "Protected objects" section.

**To create a policy for a catalogue of protected objects:**

1. Go to the **Protected objects** section.
2. In the **Catalogues of protected objects** list on the left side of the workspace, select the desired catalogue.
3. At the end of the catalogue entry, click ⋮ and, in the drop-down list, select one of the following items:
   - **Create data protection policy**
   - **Create policy on agent**

> **Note:**
>
> For policies on agents in the selected catalogues:

- Only the protected objects with disabled detection within event element will work;
- In case of Device Monitor version 7.9 and earlier, only the protected objects with disabled negation and detection within event element will work.

4. In the policy creation form that opens, specify the required settings (for more information, see *Policies Section*).
5. Click **Save**.

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

**To create a policy for selected protected objects:**

1. Go to the **Protected objects** section.
2. In the **Catalogues of protected objects** list in the left part of the workspace, select the desired catalogue.
3. At the end of the protected object entry, click  and, in the drop-down list, select one of the following items. Left-click the desired protected object. To select multiple objects, use the *Shift* or *Ctrl* key.
4. On the toolbar in the right part of the workspace, click  and, in the drop-down list, select one of the following items:
   - **Create data protection policy**
   - **Create policy on agent**

   **Note:**

   A protected object cannot be added to protection policy on agents if detection within event element is enabled for the object.

   Protected objects with enabled negation are not triggered in case of:

   - Device Monitor version 7.9 or earlier
     and/or
   - Agents installed on workstations running Linux-family OS.
5. In the policy creation form that opens, specify the required settings (for more information, see *Policies Section*).
6. Click **Save**.

The created policy will be triggered when detecting at least one of the selected protected objects.

## 4.5.6 Importing and Exporting Protected Objects

**Purpose:**

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

**Note:**

You cannot export protected objects, if the System configuration is being edited. You cannot import protected objects, if the System configuration has not been applied. Otherwise, you will receive an error message.

**To export all catalogues of protected objects:**

1. Go to the section **Protected objects**.
2. On the left part of the workspace, select **All items** and on the right of the field press .
3. In in the drop-down list select **Export**.
4. Preparing the loading will start; then the archive will be saved on the computer.

The saved archive contains XML files that store information about the protected objects and their elements of technologies. The structure of catalogues and elements of technologies is preserved when exporting.

**Note:**

When exporting protected objects, beware that the order of elements of technologies in detection condition will not be kept. Therefore, if you import those protected objects later, note that the order of elements of technologies may differ from the order at the moment of the protected objects export.

**To export a separate catalogue of protected objects:**

1. Go to the section **Protected objects** and select a protected object catalogue from the list of catalogues.
2. On the right of the catalogue name's field, click  and select **Export**.
3. Preparing the loading will start; then the archive will be saved on the computer.

**To import protected objects:**

1. Go to the section **Protected objects** and select a protected object within a catalogue.
2. At the end of the protected object entry, click  and select **Import**.
3. In the window that opens, select a previously exported file that you want to upload.
4. Wait till the protected objects are loaded into the System.

**Note:**

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

**Features of merging data when importing:**

- For catalogues, the following items missing in the System are added:
  - Child catalogues of protected objects;
  - Protected objects.

- For protected objects, the following items missing in the System are added:
  - Elements of technologies;

    **Warning!**

    Unloading created in Traffic Monitor with a version lower than 7.4 are considered obsolete.

    Obsolete unloadings are marked with .

    An obsolete unloading cannot be edited and updated. It is recommended to delete it, create the unloading again and then add it to protected object.

  - Detection conditions.
- For detection conditions, new nested conditions, including detecting parameters (for text objects, blanks and database unloadings) will be added.

### 4.5.7 Activating and Deactivating Protected Objects

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

**To deactivate a catalogue of protected objects:**

1. In the left part of the workspace, select a catalogue.
2. At the end of the catalogue entry, click  and, in the drop-down list, select **Deactivate**. The catalogue status will change to *Inactive* ( icon).

If you need to reactivate a deactivated catalogue, click  and, in the drop-down list, select **Activate**.

**To deactivate a selected protected object:**

1. In the left part of the workspace, select the desired catalogue.
2. In the right part of the workspace, click the desired protected object in the list.
3. At the end of the catalogue entry, click  and, in the drop-down list, select **Deactivate**. The status of the protected object will change to *Inactive* ( icon).

If you need to reactivate a deactivated protected object, click  and, in the drop-down list, select **Activate**.

**Note:**

If a protected object is selected as a result of cross-cutting catalogue search, you cannot change its status when editing it or using **Activate**/**Deactivate** buttons. To change the protected object status, choose it in the catalogue.

This limitation is due to the fact that a protected object can belong to different catalogues including inactive ones.

**Warning!**

Protected objects and their catalogues can be detected in intercepted data only if they are active.

## 4.6 Managing Interception Objects

**Why do you need objects of interception?**

- track the statistics on violations of the corporate security policy;
- view information on a particular object;
- display interception objects by specified criteria.

To perform daily monitoring or to get statistics promptly, we recommend using widgets in the *Dashboard* section .

If you need to view a large number of events over a period, you can create a query in the *Events* section.

**Working with interception objects includes the following actions:**

| Action | Description |
|---|---|
| Viewing Summary on Violations/Violators | Viewing statistical information and selections on events |
| Viewing Events | Viewing data on every interception object |
| Creating Dashboard Report | Generating summary on violations/violators |
| Viewing Dashboard Report | Viewing generated summaries |
| Making Decision on Object | Making user decision concerning the object |
| Adding and Delete Tags | Adding a tag to the event |
| Saving Events (for SMTP mail) | Saving the event to the disk in EML format |
| Event Export | Saving information on events to the computer hard drive |
| Dispatching Blocked Event | Sending a blocked message to the recipient |
| Creating Queries | Filtering interception object by specified criteria |

**See also:**

- Events Section - on the section, where you can search for interception objects;
- Dashboard Section - on the section, where you can view statistics on interception objects.

### 4.6.1 Viewing Summary on Violations/Violators

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

**Purpose:**
View a summary on violations/violators.

**Solution:**

1. Go to the **Dashboard** section.
2. Configure a dashboard where widgets will be added (see *Creating Dashboard*).
3. Add and configure the desired widget (see *Creating and Configuring Widget*).
4. Examine the summary in the widget.

You can export a report with the summary as PDF or HTML page (see *Creating Dashboard Report*).

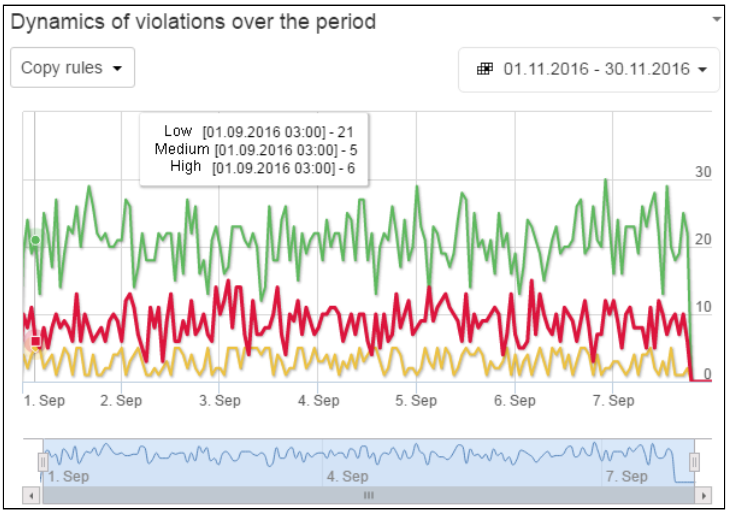
All generated reports are stored in the System. You can view the required report or delete reports which you do not need to store (see *Viewing Dashboard Report*).

***Example 1:***
It is required to track dynamics of copying files which contain confidential data (see the list of actions that are considered data copying in *Rule of Copying*).

For this:

1. Create a new dashboard or open an earlier created one.
2. Add "Dynamics of violations over the period" widget (for details on configuring this widget, see *Dynamics of Violations over the Period*).
3. In the right upper corner of the widget, choose *Current month* as a period.
4. In the left upper corner of the widget, choose *Copy rules* from the list of rules.

The widget will display charts that show the dynamics of violating copy rules for the current month.




To view events for a particular date and hour, click the point where the timeline intersects the violation number curve.

***Example 2:***
It is required to display all interception objects for the current week where John Smith is either a sender or a recipient (it is supposed that John Smith person has already been created in the **Persons** section).

For this:

1. Create a new dashboard or open an earlier created one.
2. Add "Selection" widget (for details on configuring this widget, see *Selection*).
3. Switch to the widget edit mode and for the Selection parameter, specify an earlier created *Smith* query (see Example 2 in *Examples of Using Queries*).
4. Save the widget.

## Creating Dashboard

**Purpose:**
Create a dashboard that will contain widgets.

**Solution:**

1. Go to the ***Dashboard*** section.
2. In the left part of the workspace, click  **Add**.
3. Specify the name of a new dashboard.
4. Click **Save**.

**Additional information:**

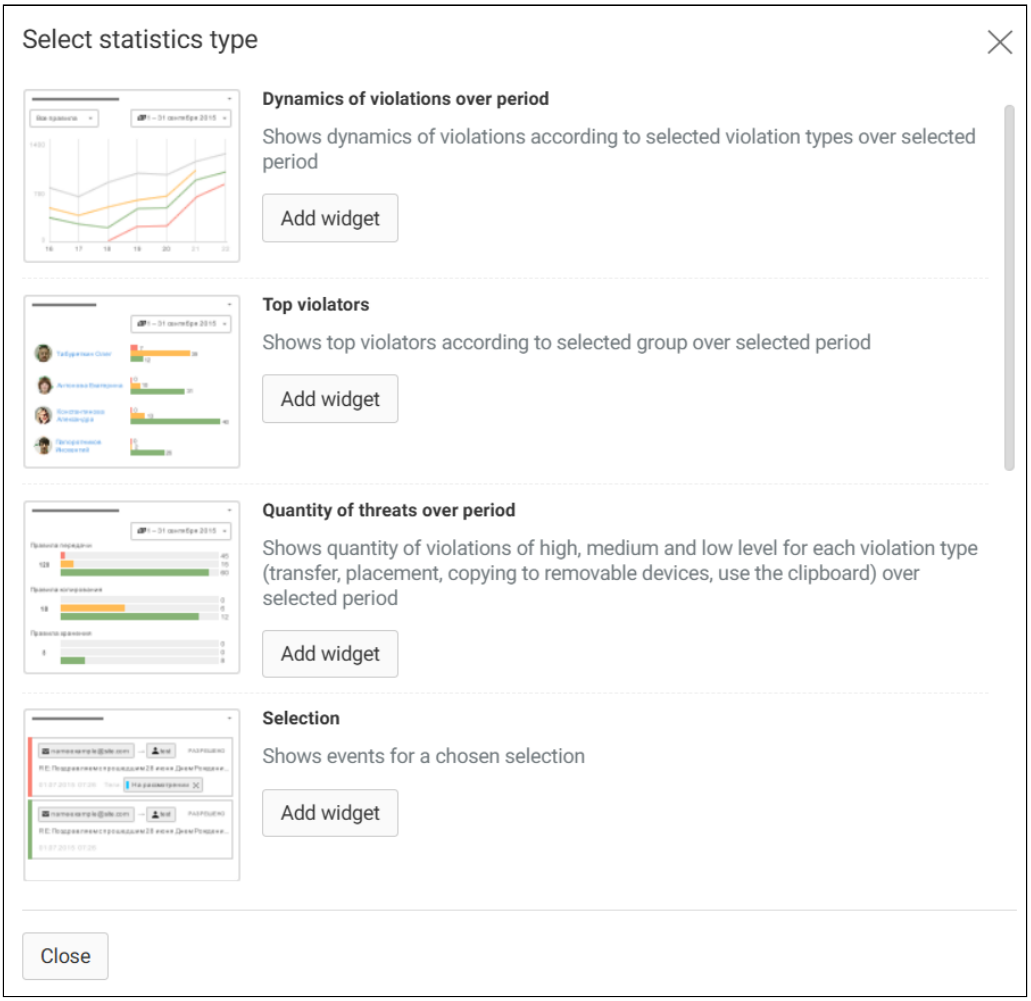
- Filling a dashboard is described in *Creating and Configuring Widget*.
- To delete a dashboard, go the dashboard which you want to delete and, on the tab with its name, click . In the confirmation window, click **Delete**.

## Creating and Configuring Widget

**Purpose:**
Create a widget in the dashboard pane.

**Solution:**

1. Go to the ***Dashboard*** section.
2. Select the dashboard, to which you want to add a widget, or create a new dashboard (see *Creating Dashboard*).
3. Click **Add widget**.
4. In the **Select statistics type** window that opens, select the desired widget and click **Add widget** under its description (for details on widget types, see *Dashboard Widgets*).




**Note:**

You can add several widgets in succession. To do this, click **Add widget** under other widgets you want to add: selected widgets will be added to the dashboard.

**Tip**

You can add multiple widgets of the same type, and then configure them to display different types of data: for example, several widgets of **Summary** type to display events based on results of queries (for details on queries, see *Creating Queries*).

5. Click **Close** or use  button in the upper right corner of the window.
6. Configure added widgets to display required data (parameters of different widgets are listed in the *Dashboard Widgets* subsection).

**Additional information:**

1. You can move widget tiles to place them in a convenient order. To do this:
   a) Hover the mouse pointer over the tile header so that a standard cursor changed to a four-way arrow key.

b) Hold down the left mouse button and, keeping it pressed, move the tile over the workspace until the target position of the tile is displayed as a dotted line.
c) Release the left mouse button.

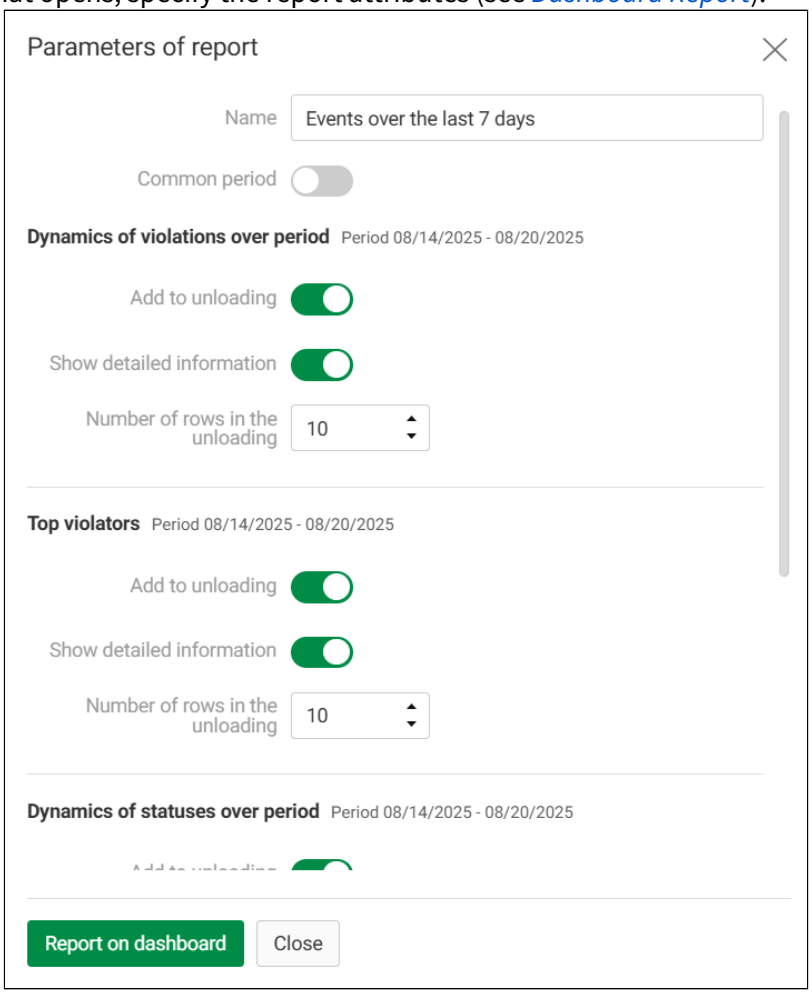
2. To edit a widget, in the right upper corner, click  and, from the drop-down list, select **Edit**. In the **General widget settings** window that opens, change the required settings, then click **Save**.
3. To delete a widget, in the right upper corner, click  and, from the drop-down list, select **Delete**. In the confirmation window, click **Yes**.

## Creating Dashboard Report

**Purpose:**
To create a report on a dashboard with the summary on intercepted objects.

**Solution:**

1. Go to the ***Dashboard*** section.
2. Open the dashboard for which you want to generate a report.
3. In the right upper corner, click **Unload**.
4. In the window that opens, specify the report attributes (see *Dashboard Report*).




5. Make sure that you have selected checkboxes of all widgets whose data you want to include in the report.
6. If you want to manually specify the period, for which the report will be generated, select the **Common period** check box and enter the start and the end date. If this option is deselected,

then, for each widget, the report will be generated for the period specified in the widget properties.

7. Click **Report on dashboard**.

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

Once the report is generated, you will be prompted to open it in PDF or HTML format.

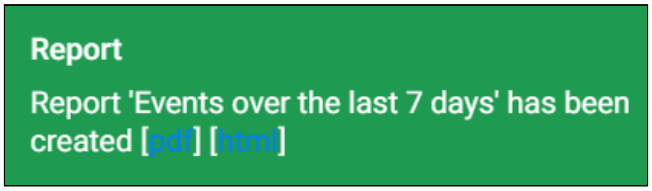
All created reports are stored in the System and are available by clicking the **Export** button on the navigation panel. For details, see *Viewing Dashboard Report*.

> **Note:**
>
> If you remove or modify a widget which is included in the report, then the already created report will not be changed.

## Viewing Dashboard Report

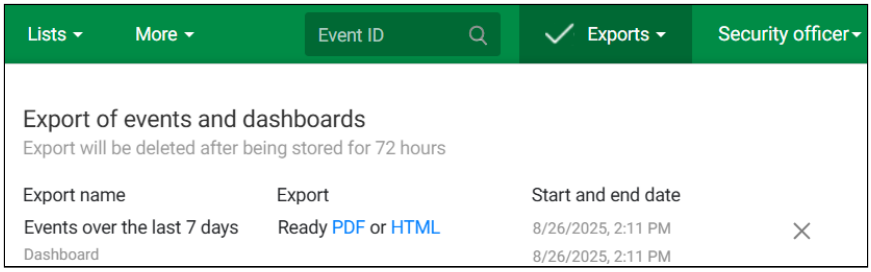
**Purpose:**
View a report on intercepted objects.

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




Click on the **pdf** or **html** link to open the report in a new browser window. You can also save, send or print the created report by standard means of your browser and operating system.
All created reports are stored in the System.

**To view the list of generated reports**, click the **Export** button in the Navigation page. The **Export of events and dashboards** window will open where you can view information on the reports.




For each report, the list displays its name, status, date of start and completion, and links to PDF and HTML files. To open the report in a new browser tab, click the selected format.

To remove the report data from the list, click ☒ in the row of the selected report.

### 4.6.2 Viewing Events

**Purpose:**
View information on the interception object.

**Solution:**

1. Go to the **Events** section (see *Events Section*).
2. Create a query and run it (see *Creating Queries*).

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

3. If necessary, change the list of displayed fields (see *Choosing Event Fields of View*).
4. View information on the event tile or in the table row (see point 3 in the picture in the *Events Section*).
5. For more information on the interception object, use a *brief* or *detailed* form.

#### Creating Queries

**Purpose:**
Create a query to search for required events.

**Solution:**

1. Go to the **Events** section (see *Events Section*).
2. If you want to create a query within a folder, select a folder in the list or create a new folder (see *Creating Folder with Queries*).
3. Create a query in a *standard* or *advanced* mode. You can create a query in a folder or in the root.
4. To run the query, select it in the list and click  **Run query** on the toolbar (or you can use **Save and run** button in the query creation form).

If necessary, you can copy or move an earlier created folder or query.

**To copy a folder** and its queries:

1. Select the folder in the list.
2. On the toolbar in the left part of the workspace, click  **Copy**.

If you are trying to copy a subfolder and you have full access to the parent folder, then the copy will be added to the same folder as the copied folder. If you don't have full access to the parent folder or you are copying a top-level folder, then the copy will be added to the root of the folder tree.

**To copy a query:**

1. Select the query in the list.
2. On the toolbar in the left part of the workspace, click  **Copy**.

If you are copying a query inside a folder and you have full access to the folder, then the copy will be added to the same folder as the copied query. If you don't have full access to the folder or you are copying a top-level query, then the copy will be added to the root of the folder tree.

**To move a folder**, select it in the list and holding the left mouse button move it to the desired location.

**Note:**

To move a folder, you need to have full access both to the folder you are moving and to the destination folder. If the folder includes queries, then you also need full access to the queries. For details, see the table below.

**To move a query**, select it in the list and holding the left mouse button move it to the desired location.

**Note:**

To move a query, you need to have full access both to the query and to the destination folder. For details, see the table below.

The table below shows what access rights are needed to manage queries:

| **Action** | **Access rights** | | | |
|---|---|---|---|---|
| | View folder | Full access to folder | View and execute query | Full access to query |
| View the folder | + | + | + | + |
| Edit the folder attributes (name, description, access rights) | | + | | |
| Copy the folder | + | + | + | + |
| Create a new item (a query or a subfolder) in the folder | | + | | |
| Move an empty folder to a different folder | | + | | |
| Move a folder which includes at least one query | | + | | |
| Delete an empty folder | | + | | |
| Delete a folder which includes at least one query | | + | | |
| View and run the query | + | + | + | + |
| Edit the query parameters (including access rights) | | + | | + |

| | | | | |
|---|---|---|---|---|
| Copy the query | + | + | + | + |
| Move the query to a different folder | | + | | + |
| Delete the query | | + | | + |

**Note:**

If after editing access rights, a query/folder becomes unavailable to any user of the System, then full access to the query/folder is automatically provided to the current user.

**See also:**

- Creating Folder with Queries;
- Query Creation in Standard Mode;
- Query Creation in Extended Mode;
- Examples of Using Queries.

Creating Folder with Queries

**Purpose:**
Create a folder where queries will be grouped.

**Solution:**

1. Go to the **Events** section.
2. In the list of folders and queries in the left part of the workspace, choose where to create a folder. You can create a folder in the root or inside an existing folder with queries.

   **Note:**

   If you do not have sufficient rights to create items within a selected folder, a warning will be displayed. In this case, you should create a folder at a different place.

3. Click  and, in the drop-down list, choose **Create query folder**.
4. In the form that opens, enter the folder name.
5. Specify if access rights to the folder should be inherited for subfolders and queries. By default, the **Apply rights for related queries** option is deselected.

   **Note:**

   If you create a folder inside a folder with the **Apply rights for related queries** option enabled, then actions described in steps 5-6 are unavailable.

6. Specify who can access the folder and define access rights. For this:
   a. Find required users in the list.

> **Tip.**
>
> To find required users, use the **Search** field.

b. Next to the user name, set the checkbox in one of the fields:
   - **View and execute access** - to provide access for viewing and copying the folder. Access rights to queries in the folder are specified when you create a query;
   - **Full access** - to provide full access to the folder.

> **Note:**
>
> To provide access to the folder to all users of the System, set a checkbox in the field with the required access level next to the **All users** value.

7. Click **Save**.

To edit the folder, click the  button on the toolbar.

To delete the folder, click .

> **Note:**
>
> To edit or delete a folder, full access to the folder is required. If you can only view and execute the folder, then instead of  button,  button is displayed, and  button is unavailable.

Query Creation in Standard Mode

**Purpose:**
Create a query to search for events which satisfy specified conditions.

**Solution:**

1. Go to the **Events** section.
2. In the list of folders and queries in the left part of the workspace, choose where to create a query. You can create a query in the root or inside an existing folder with queries.

> **Note:**
>
> If you do not have sufficient rights to create items within a selected folder, a warning will be displayed. In this case, you should choose another location for the query.

3. Click  and, in the drop-down list, choose **Create standard query**.
4. In the form that opens, enter the query name and, if necessary, add a description.
5. On the **Query** tab, edit the query parameters. By default, the most commonly used parameters are displayed. For parameters that you need, specify the required values in the entry fields. To remove

parameters that you do not want to use in the query, click  in the right upper corner of the selected parameter.

6. To add a parameter, in the **Add condition** drop-down list, choose the required parameter (for the whole list of available parameters, see *Standard Mode of Creating Queries*).
7. On the **Columns** tab, select attributes whose values will be displayed for the found events.
8. On the **Access** tab, specify who can access the query and define the access permissions.

> **Important!**
>
> If you create a query in a folder with the **Apply rights for related queries** option enabled, then access rights for the query will be the same as for the folder. In this case, editing access right to the query is unavailable.

To specify access rights to the query:

a. Find the required users in the list.

> **Tip.**
>
> To find users in the list, use the **Search** field.

b. Next to the user name, set the checkbox in one of the fields:
   - **View and execute access** - to provide the user access for viewing, copying, and executing the query;
   - **Full access** - to provide the user full access to the query.

> **Note:**
>
> To provide access to the query to all users of the System, set a checkbox in the field with the required access level next to the **All users** value.

9. Click:
   - **Save** - to save the query;
   - **Save and execute** - to save and run the query.

> **Tip.**
>
> If while creating a query, you find out that you need to specify more flexible conditions, you can use the *advanced mode*. For this, in the **Query type** field, click **Advanced**. The advance query creation mode will open. All specified parameters of the query will be saved.

To edit the query, click  on the toolbar.

To delete the query, click .

**Note:**

To edit, move, or delete a query, full access to the query is required. If you can only view and execute the query, then instead of  button,  button is displayed, and  button is unavailable.

The *Examples of using queries* article contains an example of creating a simple query.

Query Creation in Advanced Mode

**Purpose:**
To flexibly configure search conditions for events.

**Solution:**

1. Go to the **Events** section.
2. In the list of folders and queries in the left part of the workspace, choose where to create a query. You can create a query in the root or inside an existing folder with queries.

   **Note:**

   If you do not have sufficient rights to create items within a selected folder, a warning will be displayed. In this case, you should choose another location for the query.

3. On the toolbar, click  and, in the drop-down list choose **Create advanced query**.
4. In the form that opens, enter the query name and, if necessary, add a description.
5. On the **Query** tab edit the parameters used in the query. By default, the most commonly used parameters are displayed. For parameters that you need, specify the required values in the entry fields. To remove parameters that you do not want to use in the query, click  in the right upper corner of the selected parameter.
6. To add a parameter, in the **Add condition** drop-down list, choose the required parameter.
7. By default, added parameters are joined by the logical AND. To change the operation type, left-click the 

icon. The icon will change to 

that indicates logical OR.
8. Use **Group of parameters** element to separate attributes joined by the logical AND from attributes joined by the logical OR (see *Advanced mode*).
9. On the **Display fields** tab, select attributes whose values will be displayed for found events.
10. On the **Access** tab, specify who can access the query and define the access rights.

    **Important!**

    If you create a query in a folder with the **Apply rights for related queries** option enabled, then access rights for the query will be the same as for the folder. In this case, editing access right to the query is unavailable.

    To specify access rights to the query:
    a. Find the required users in the list.

> **Tip.**
>
> To find users in the list, use the **Search** field.

b. Next to the user name, set the checkbox in one of the fields:
   - **View and execute access** - to provide the user access for viewing, copying, and executing the query;
   - **Full access** - to provide the user full access to the query.

> **Note:**
>
> To provide access to the query to all users of the System, set a checkbox in the field with the required access level next to the **All users** value.

11. Click:
    - **Save** - to save the query;
    - **Save and execute** - to save and run the query.

> **Note:**
>
> If while creating a query, you want to switch to the *standard* mode, then, in the **Query type** field, click **Standard**. The standard query creation mode will open. All specified parameters of the query will be saved. However, if already specified conditions can be implemented in the advanced mode only, then switching to the standard mode is unavailable.

To edit the query, click  on the toolbar.

To delete the query, click .

> **Note:**
>
> To edit, move, or delete a query, full access to the query is required. If you can only view and execute the query, then instead of  button,  button is displayed, and  button is unavailable.

The *Examples of Using Queries* article contains examples of creating advanced queries.

Using Advanced Syntax

**Purpose:**
Configure full-text search through the event text by using extended syntax.

**Solution:**

1. Switch to the advanced mode of the query creation.
2. On the **Query** tab, in the **Add condition** drop-down list, select the **Event text** parameter.
3. Select **Advanced syntax**.
4. In the **Query** field, enter text using logical operators:"|","-", "!", "()", etc.

> **Note:**
>
> When **Advanced syntax** is enabled, search for special characters can be performed via shielding. To shield the special character, use '\' character placed before the character to be shielded.

5. Specify other parameters of the query (for details, see *Query Creation in Advanced Mode*).
6. Click **Save**.

You can find detailed information on using logical operators for creating queries in the *Internet article*.

> **Note:**
>
> Please, not that the search area is defined explicitly in the **Search area** field (see *Search on the Event Text*), so you needn't specify the search area with Sphinx operators.

***Example:***

If you want to find the event whose text:

- contains *"personal data"* and *"private data"* words;
- does not contain the phrase *"confidential information"*,

create the following query using the advanced syntax:

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

Examples of Using Queries

***Example 1:***

You need to view all email messages for the current day sent by employees under the supervision. For this:

1. Create a simple query and specify its name.
2. Specify the following query parameters:
   - **Interception date** - *Current day*;
   - **Event type** - *Email*.
3. In the **Senders** field, specify the *Employees under supervision* group (see how to create such a group in *Creating Group of Persons or Computers*).
4. Save and run the query.

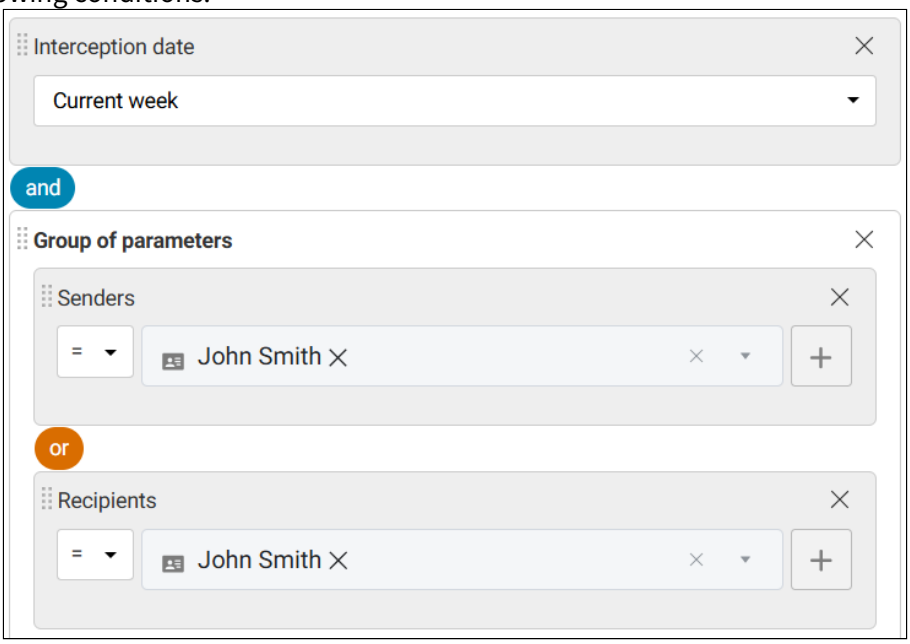
> **Tip**
>
> If there is a lot of traffic in your company and it takes much time to execute the query, you can continue working with other tasks while the query is running in the background. As soon as the query execution is complete, the System will notify you with a balloon tip.

***Example 2:***

An employee John Smith is suspected of misusing of confidential information. The incident has happened this week. To investigate the incident, you need to find events for John Smith.

For this:

1. Create an advanced query and specify its name - *Smith*.
2. Add the following conditions:




3. Save and run the query.

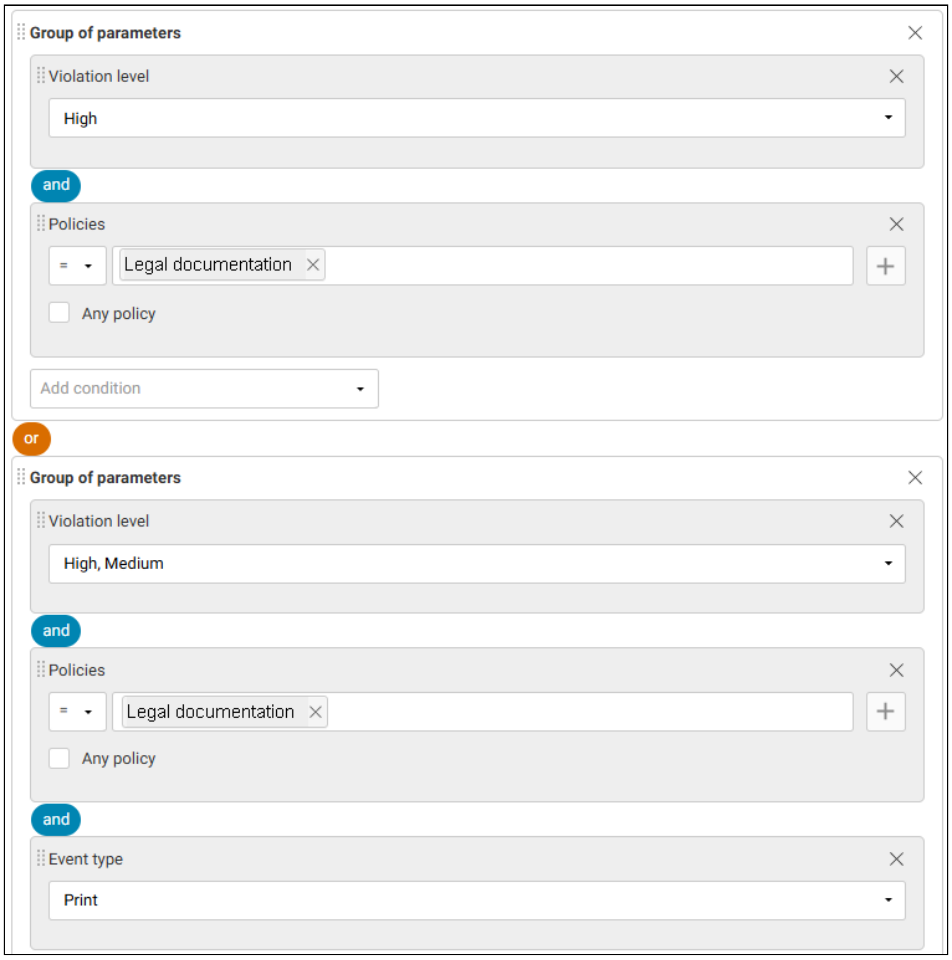
***Example 3:***

You need to find the events:

- with *High* violation level and the *Legal documentation* policy
- with *High* and *Medium* violation levels, the *Legal documentation* policy, and the *Stamp* event type

For this:

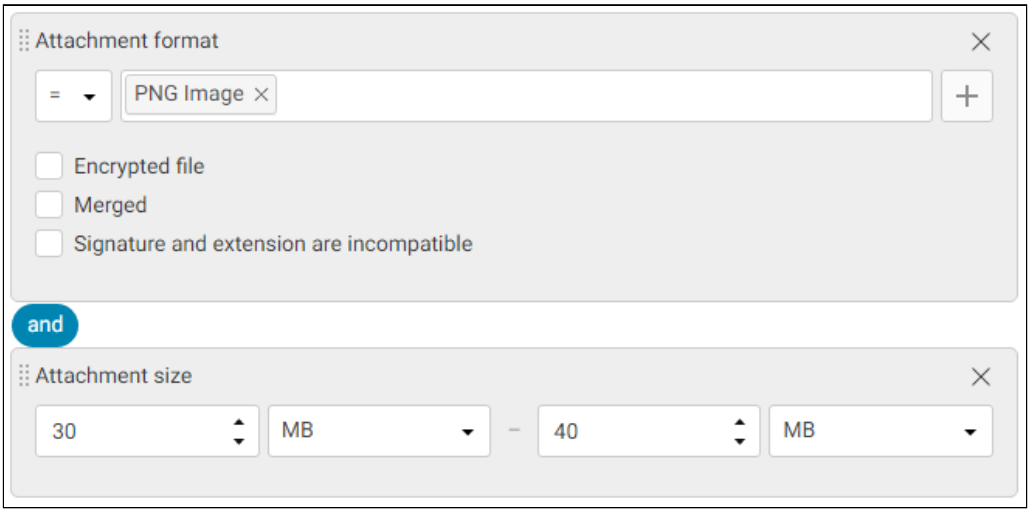
1. Create an advanced query and specify its name.
2. Add two *Group of parameters* elements, joined by logical OR.
3. Within the first group, add the following attributes joined by logical AND:
    - **Violation level** - *High*;
    - **Policy** - *Legal documentation.*
4. Within the second group, add the following attributes joined by logical AND:
    - **Violation level** - *High* and *Medium*;
    - **Policy** - *Legal documentation*;
    - **Event type** - *Print.*
5. Save and run the query.



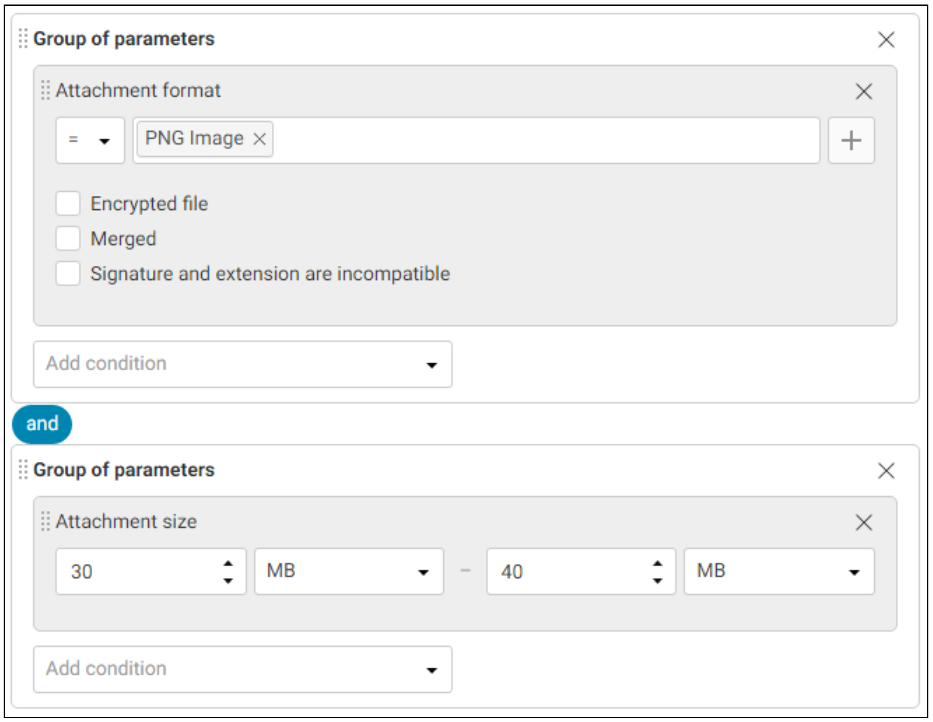

***Example 4:***

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

1. If several conditions within a group of parameters are combined by the operation of the logical “AND”, then query results will contain objects with at least one attachment that satisfies all specified conditions. In the example below, the query results will display objects with at least one attachment of PNG format whose size is between 30 and 40 MB.



2. If each condition is in a separate group of parameters and groups are combined by the operation of the logical “AND”, then query results will contain objects, for which all conditions are satisfied, but not necessarily for the same attachment. In the example below, the query results will display objects with at least one attachment of PNG format and at least one attachment whose size is between 30 and 40 MB.




***Example 5:***

You need to find the events containing eml attachments.

For this:

1. Create an advanced query and specify its name.
2. Add *Attachment format* element.
3. Set the value *Email* for the element.
4. Save and run the query.

***Example 6:***

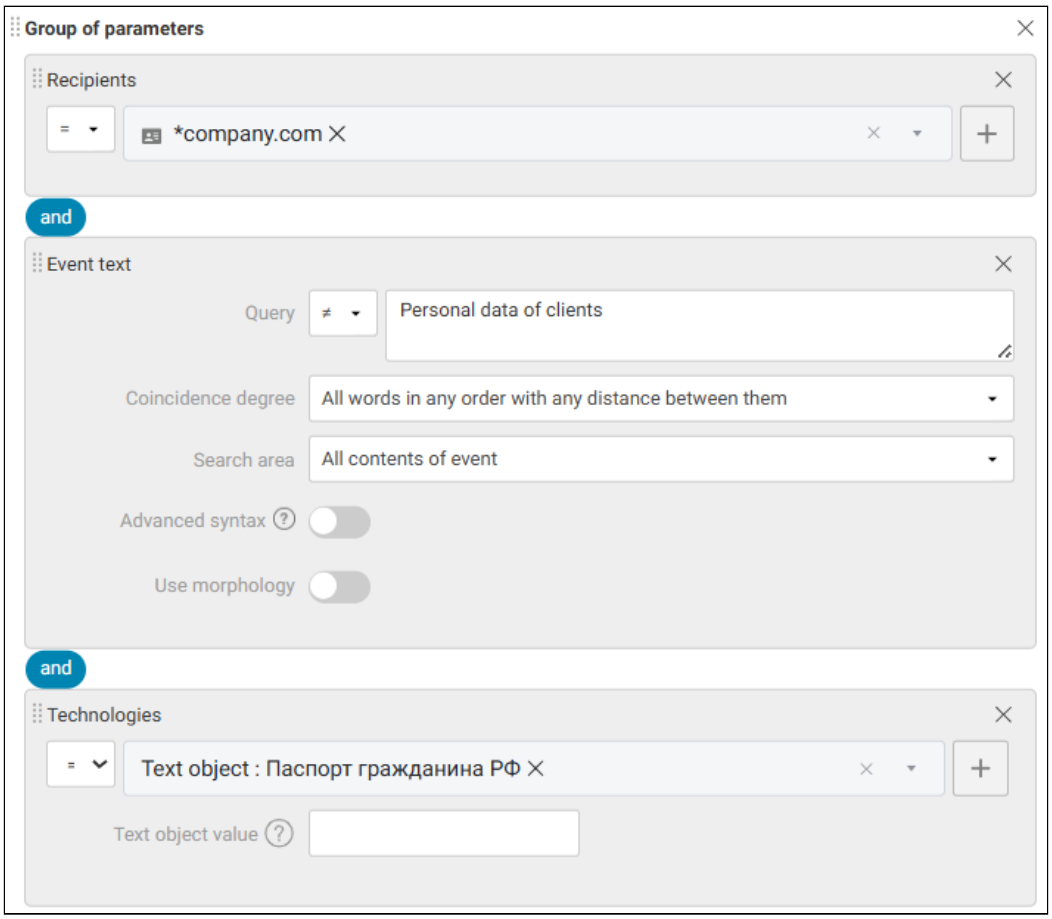
You need to find the events:

1. transferred inside the company
2. without *"Personal data of clients"* text object
3. containing passport numbers

For this:

1. Create a query in advanced mode and specify its name.
2. Add *Group of parameters* element.
3. Within the group of parameters specify the attributes bound by the logical “AND”:
   a. `Recipients –` **company.com*
   b. `Event text –` "*Personal data of clients*", herewith select the coincidence degree *All words regardless of their order and distance among them*, and apply negation to the attribute
   c. `Search area` - "All contents of event"
   d. `Technologies –` the "*Russian Federation citizen passport"* text object

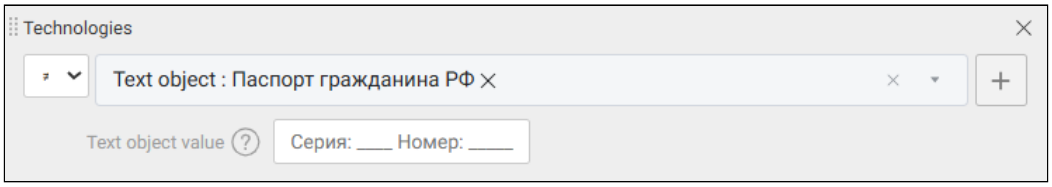
4. Save and run the query.




***Example 7:***

You need to find the events with the "*Russian Federation citizen passport"* text object.
For this:

1. Create an advanced query and specify its name.
2. Add *Technologies* element.
3. Select the "*Russian Federation citizen passport"* as a value and apply negation to the attribute.
4. Save and run the query.




The query results will include the events:

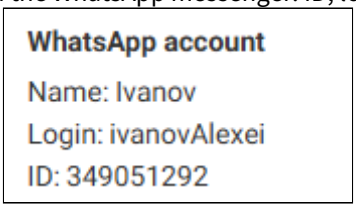
1. which do not contain triggered protected objects;
2. where triggered protected objects do not contain the "*Russian Federation citizen passport"* text object.

If you specify a passport serial number (e.g., 4505 and 123456), then the query results will include the events:

1. which do not contain triggered protected objects;
2. where triggered protected objects do not contain the "*Russian Federation citizen passport"* text object with serial number "4505" and "123456" value.

***Example 8:***

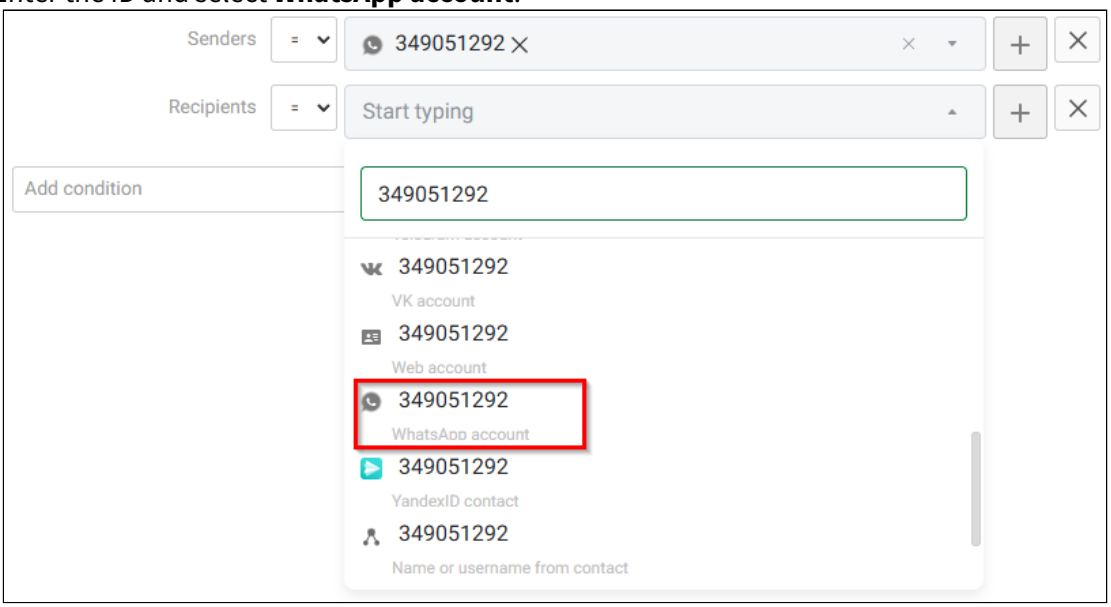
You know the data of the user's account in the WhatsApp messenger: ID, login and display name:



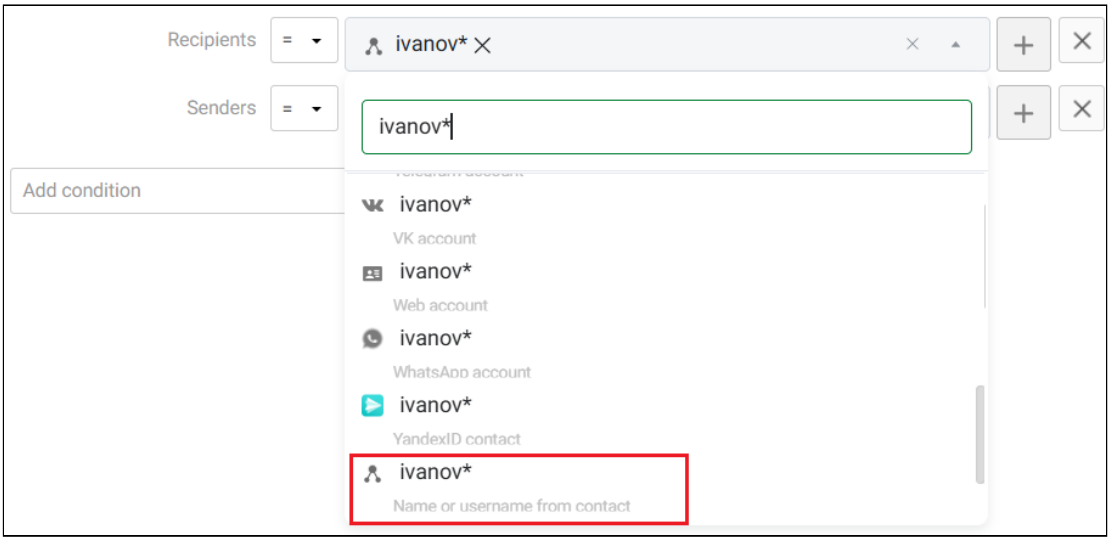

You need to find the events with participation of this user.

For this:

1. Create a query of any kind and specify its name.
2. In the *Senders* and *Recipients* fields, specify one of the following values:
   - **Account ID**.
     Enter the ID and select **WhatsApp account**.




   - **Display name** or **login** of the account - you can specify the value using wildcards. For details, see *Standard Mode of Creating Queries*.
     Enter the name or the login of the account and select **Name or username from contact**.




3. Save and run the query.

## Choosing Event Fields of View

**Reference information:**
By default, *event table* displays all event attributes.

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

**Purpose:**
To select attributes of interception objects that will be displayed.

**Solution:**

1. Go to the **Events** section.
2. Do either of the following:
   - Edit an existing query. For this, click  **Edit query**;
   - Create a new query.

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

3. On the right part of the workspace select **Columns** tab.
4. Move all target attributes to the right field and all unwanted ones - to the left:
   - Left-click on the entry in the left field to move it to the right field;
   - Left-click on the entry in the right field to move it to the left field.
5. Click:
   - **Save** - to save a query.
   - **Save and execute** - to save and apply the changed query.

## Viewing Brief Event Form

**Purpose:**
Viewing brief information on interception objects.

**Solution:**

1. Go to the **Events** section.
2. Create a query or run an earlier created query (see *Creating Queries*).
3. Select the tile of the target event in the list (or a row of the target event in the event table).
4. View the summary in the right part of the workspace. In the upper part of the form, you can view the event parameters; in the lower part, the event contents is displayed.

> **Note:**
>
> You can adjust the data representation in the viewing area. By default, the event content is displayed as snippets where all triggered protected objects and results of the text search are highlighted.

5. To view data on senders, recipients or computers, click the desired value. A card for selected person or computer will be displayed.
   When viewing the card, you can:
   a. Assign a status to a person/computer. For this, click **Set status** and, in the opened window, select desired statuses. Then click **Save**.
   b. View detailed information on a person/computer in the *Persons* section. For this, click **Person profile** (for persons) or **Go to computer** (for computers).
   c. View screenshots for a person/computer (if there are screenshots for a person, then  icon is displayed next to the person name). For this, click **Screenshots**. The ***Screenshots*** tab for the selected person or computer will open.

> **Note:**
>
> If there are screenshots taken within an hour before or after the event, the **Screenshots at the time of event** link is displayed for persons. When clicking this link, the screenshots whose creation time is closest to the event are displayed in full screen mode.

6. To view information about the triggered policy in the *Policies* section, click the name of the triggered policy.
7. If the event has attachments, you can:
   - Save them to your computer. For this, click  next to the attachment name
   - Find events with similar attachments if the attachment is in text format. For this:
     a. Select the attachment.
     b. Click **Find analogues**.
     c. From the drop-down list, choose either of the following:
        - **Find analogues**
        - **Find samples**
8. To get detailed information on the event, in the right upper corner of the form, click **Detailed information**.

**See also:**

- Brief Event Viewing Form – on the form with general information about the event;
- Viewing Detailed Event Form – on displaying detailed information about the event;
- Viewing Screenshots – on viewing screenshots for persons or computers;
- Search for Analogues – on the searching events with similar attachments.

Search for Analogues

If an event in Traffic Monitor contains an attachment and a text is extracted from this attachment, you can find events:

- *With similar attachments*
  Documents are considered similar if they have the same subject. For example, they can be legal documents or contracts. Similar documents may have different structure.
- *With sample attachments*
  Sample attachments are documents that are identical in structure but have minor differences. For example, they can be documents that are drawn up according to a single template, but differ in performers, dates and names of services.

You can search for analogues using the *Brief Event Form*. As a result, a query will be created and run. The query name will include the name of the source attachment and the source event ID. The query results will be displayed as the *list of attachments*.

Detected similar files can be both separate attachments and a part of attached containers, e.g. archives.

**Note:**

If you find a similar file in the attached container, then, in the results of search for analogues, you can see the event containing the file. But the file is not to be displayed. To view the file, switch to the list view or to the table view.

**Important!**

For the **Search for analogues** feature to work, you need to install Data Analysis Service (for details, see *Data Analysis Service. Installation, Configuration and Administration Guide*) and perform preliminary setup (for details, see *InfoWatch Traffic Monitor. Administrator's Guide. Configuring integration with Data Analysis Service* article).

## Viewing Detailed Event Form

**Purpose:**
To view a detailed information on the interception object.

**Solution:**

1. Go to the **Events** section.
2. Create a query or run an earlier created query (see *Creating Queries*).
3. Select a tile of the target event in the list (or a row of the target event in the table). The right part of the workspace will display a *brief event viewing form*.
4. To open the detailed viewing form, click **Detailed information**.

5. In the **Detailed information on event** window that appears, view the needed information. Information on the event is presented in the following blocks: **General information**, **Text search**, **Protected objects**, and **Event content** (see *Detailed Event Viewing Form*).

   > **Note:**
   >
   > You can adjust the data representation in the viewing area. By default, the event content is displayed as snippets where all triggered protected objects and results of the text search are highlighted.

6. When viewing the event parameters, you can get additional information about persons, computers, and policies of the event (see *Viewing Brief Event Form*, i. 5-6).
7. To close the detailed form, click  in the upper right corner of the window.

**See also:**

- Detailed Event Viewing Form - on the detailed event viewing form;
- Viewing Brief Event Form - on displaying general information about the event.

## 4.6.3 Making Decision on Object

**Purpose:**
To make a decision on the object.

**Solution:**

1. Go to the **Events** section.
2. Left-click the target event to select it.
3. On the toolbar, click
   -  **Violation** - for events that violate the corporate security policy. For events with *Quarantine* verdict, the verdict value will change to *Blocked*.
   -  **No violation** - for events that do not violate the corporate security policy. For events with *Quarantine* verdict, the verdict value will change to *Allowed*.

     > **Warning!**
     >
     > If the *Block* mode is used in the System, then as a result of this decision, SMTP messages quarantined by the System will be dispatched and the message sender will be notified via email. For details, see *Dispatching Blocked Event*.

   -  **No decision** - if for now the user has not decided a decision whether the event violates the corporate security policy.
   -  **Requires additional proceeding** - if additional actions are needed to make a decision.

**Example:**

Security Officer views the events marked as No violation and decides that some events have violations. So the Officer marks these events as *Violation*. Such events will be transferred in DB daily table spaces containing events with violations. The data may be useful in future in case investigation is needed. Daily table spaces containing events with violations are stored longer than ones that keep events without violation. The period to store the daily table spaces can be set manually (see how to do it in the articles *InfoWatch Traffic Monitor Administration Guide. Managing daily table spaces*).

**See also:**

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

### 4.6.4 Adding and Deleting Tags

**Purpose:**
Add a tag to the interception object.

**Solution:**

1. Go to the **Events** section.
2. Left-click the target event to select it.
3. On the toolbar, click  **Set tag**.
4. In the window that opens, select the desired tag by flagging it.
5. Click **Save**.

To delete a tag, click X next to the tag name in the event tile.

**See also:**

- Tags - on the interface of Management console section where tags are managed;
- Managing Tags - on filling a tag catalogue.

### 4.6.5 Saving Events (for SMTP mail)

**Purpose:**
Save interception object (SMTP-letter).

**Solution:**

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

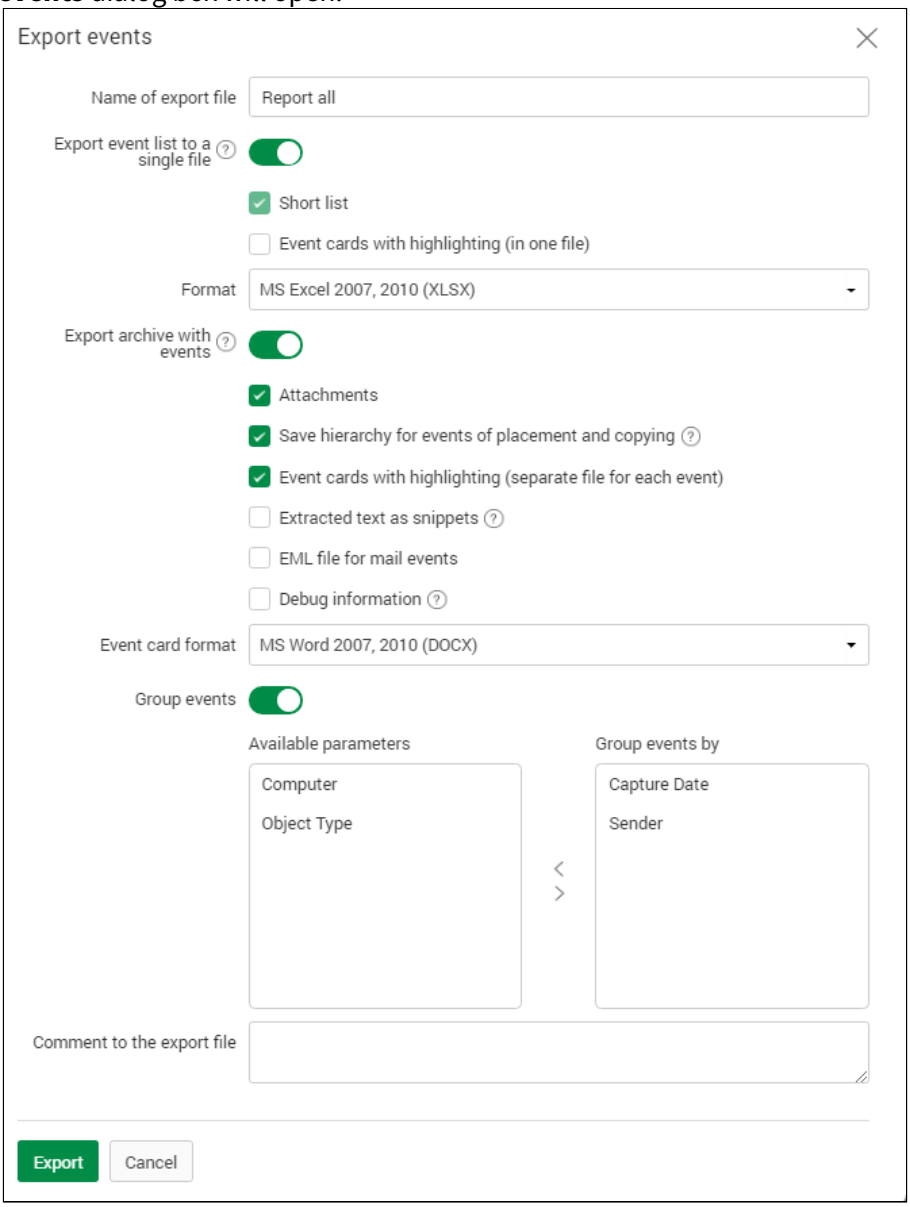
### 4.6.6 Event Export

**Purpose:**

Save information on events to the computer hard drive.

**Solution:**

1. Go to the **Events** section.
2. Choose a query from the list and run it or create a new query (see *Creating Queries*).
3. Select the event you want to export. To select multiple events, use the **Shift** or **Ctrl** key.
4. On the toolbar, click  and in the drop-down list select **Export events** or **Export all events**. The **Export events** dialog box will open.




5. If you have selected more than one event, specify how they should be exported (otherwise, go to step 7).
   You can choose one option or both:
   - **Export event list to a single file** – a file with data on all selected events will be created;
   - **Export archive with events** – an archive with a separate folder for each event will be created.
6. If you have chosen **Export event list to a single file**:
   a. Choose the list view. You can choose one option or both:
      - **Short list** – for each event, a list of its main parameters is exported;
      - **Event card with highlighting** – for each event, a list of its parameters is exported. Besides, the export file includes the event text and the text extracted from

attachments where all triggered protected objects are highlighted.

> **Note:**
>
> In the file with the event list, a field corresponding to *Senders* column contains additional information about persons (if present): branch, department and position.

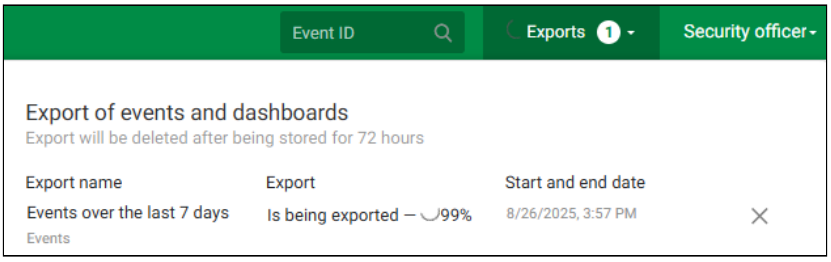
b. Choose the export format. The following formats are available:
   - MS Excel 2007, 2010 (XLSX);
   - MS Excel 2003 (XLS);
   - MS Word 2007, 2010 (DOCX);
   - Adobe Acrobat (PDF) – you can export not more than 100 events.

> **Примечание:**
>
> MS Excel formats are unavailable if the **Event card with highlighting** view is selected.
>
> File with the event list will include the first 7 columns of the table, other columns will be ignored.

7. If you have chosen **Export archive with events** or the export file includes only one event, specify the following settings:
   - **Attachments** – original attachment files will be exported.
     By default the option is disabled to reduce RAM usage;
   - **Save hierarchy for events of placement or copying** – is displayed if the **Attachments** option is selected. Events of the same type will be saved to the *External device*, *FTP* or *Data Discovery* folder depending on the event type;
   - **Event card with highlighting** – a file in DOCX format is created for the event; the file includes a list of the event parameters, the event text and the text extracted from attachments in which all triggered protected objects are highlighted;
   - **Extracted text as snippets** – is displayed if the **Event card with highlighting** option is selected. Text extracted from attachments will be exported in the form of snippets with triggered protected objects;
   - **EML file for mail events** – an EML file of the form *[Event ID]_[Email subject]* will be exported;
   - **Debug information** – for each exported file, debug information is added to the archive.
8. If you have chosen **Export archive with events**, you can specify additional settings:
   - **Group events** – select this option if you want to group events in the archive and add required parameter from the **Available parameters** field to the **Group events by** field. Events can be grouped by the following parameters: *Computer, Event type, Interception date, Sender.*
   - **Comment to the export file** - the added comment in DOCX format will be exported to the root folder
9. When you have specified all needed parameters, click **Create**.

When the operation is completed, in the upper right corner you will see a notification. To view the export file, click **download** and save it to your computer.

You can monitor the export progress by clicking the **Export** button on the navigation pane.




For each export process, you can view its name, status, start date and time. For already created files, the System also displays their size, creation date and time, and the **Download** link clicking which allows you to save the export file to your computer.

For export files that are being created at the moment, the progress in a percent format is displayed. If you want to cancel the export file generation (e.g., if the process takes a long time), click ✕ in the row of the selected file. The file generation will be canceled.

Besides event export files, the list also displays information on created dashboard reports (see *Viewing Dashboard Report*).

The **Export** button is available from all sections of the Management Console.

## 4.6.7 Dispatching a Quarantined Event

**Reference information:**
If the System (in the *Blocking* transport mode) recognizes a transferred SMTP-letter as a potential violation and moves it to quarantine, the security officer can then review the decision of the System and allow sending this letter. In this case, the System dispatches the letter and notifies the person who has sent it.

**Purpose:**
Send a quarantined letter to the addressee.

**Solution:**

> **Warning!**
>
> You can dispatch the object with a *Quarantine* verdict. Objects with a *Blocked* verdict cannot be dispatched.
>
> If, according to policy configuration, the System has deleted event attachments and moved the event to quarantine, an email dispatched to the recipient will be empty.

1. Go to the **Events** section.
2. Left-click the target event.
3. On the toolbar in the left part of the workspace, click ☑ **No violation**.

**See also:**

- User Decision on an Object - general information on making decisions;
- Making Decision on Event - on how to make a decision on the object.

## 4.7 Configuring System Response

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

**Reference information:**
The System response determines the actions that the System performs when detecting violations of the corporate security policy. You can specify these actions when creating rules for data protection policies and person control policies.(see *Policies Section*).The System also includes preset policies (see *Default Policies*).
Sometimes during operation of the System, the analysis and decision-making subsystems cannot use the policy: for example, the policy has not been created or has been deleted, or an error occurred when applying the policy. In this case, no attributes are assigned to the objects, and the **Processing messages** window of the detailed event viewing form displays information about errors that occurred during the processing (see *Detailed Event Viewing Form*).

**Why do you need to configure the System reactions:**
When you configure the System reactions you can specify that in the case of corporate security policy violations (e.g. sending a confidential document outside the company) or detecting the improper use of work time (e.g. visiting entertaining websites from the office computer), the System should:

- send notifications to violators and inform the security officer and other interested persons;
- assign a verdict to the interception object;
- assign a violation level, statuses, and tags to the interception object.

**Configuring the System response includes:**

| Action | Description |
|---|---|
| Creating data protection policies | Data protection policy is a set of rules that regulate data transfer, copying, placement, and usage of the clipboard. Allows you to specify actions that may trigger policy rules. |
| Creating data protection policies on agents | Data protection policy on agents is a set of transfer and copy rules that apply directly on Device Monitor agents.<br>Allows you to specify actions that may trigger policy rules. |
| Creating person control policies | Allows you to specify the list of controlled persons whose actions may trigger policy rules |
| Creating rules | Defining what is a violation of policy rules, and what actions will be done in the event of violation |
| Configuring Notifications in Rules | If the rule is triggered, the System sends notification to specified recipients |

In addition to creating policies, you can import them, for example, from another Traffic Monitor server. For details, see *Exporting and Importing policies*.

**Note:**

If there are a lot of policies in the Management Console, you can filter the policy list by specified criteria (for details, see *Filtering the List of Policies*).

**Note:**

If any parameter of the policy is no longer relevant and blocks policy operation, the policy becomes inactive and has the "**Policy is damaged**" status in the Management Console. In this case, you can see the warning message in the upper part of the workspace.

**Example:**

*Data protection policy 1* contains the transfer rule. In this rule, *Employee 1* is specified, among others, in the list of senders. This employee leaves the company, and his account is deleted. As a result, *Data protection policy 1* is damaged.

To restore the policy work, edit the policy and apply the configuration.

**See also:**

- Policies Section - on the section where you can manage policies

## 4.7.1 General Information on Policies

The section describes how the System policies are configured (a set of rules according to which objects are analyzed and processed) are applied to events (intercepted objects of network traffic).

The System policies are divided into three groups:

- Data Protection Policies - allow you to set up rules of transfer, copying, placement, and using clipboard
- Data Protection Policies on Agents - allow you to set up transfer and copy rules that apply directly on Device Monitor agents
- Person Control Policies - allow you to set up rules for monitoring actions of individual persons and groups

The System applies policies to events in the following order:

1. The System checks if the event conforms to any active data protection policy on agents.
2. If the event has triggered a policy, the sub-events are considered.
3. For each sub-event, the matching rules are selected (rules triggering to this sub-event).
4. Triggered rules are divided into sub-rules.
5. From sub-rules corresponding to the event, the ones with the highest priority are selected.
6. The actions specified in triggered sub-rules of the highest priority apply to the interception object.
7. If there are sub-events without matching rules, default actions are executed (if they are specified for this type of rules).

Then steps 2-7 are repeated for all active data protection policies and then for all active person control policies.

For more information about accompanying processes, see:

1. Dividing events into sub-events
2. Dividing rules into sub-rules and choosing matching rules

3. Determining the priority sub-rule
4. Order of applying actions according to selected priority rules

The article also includes an *example of applying a policy*.

**1. Dividing events to sub-events**

During processing the event, the System divides it into sub-events:

1. For events related to transfer rules: by a pair of keys "Sender" - "Recipient".
2. For events related to copy rules: by the key "Sender".
3. For events related to clipboard rules: by the key "Persons".
4. For events related to storage rules: by a pair of keys "File owners" - "Who has access to file".

If any attribute of the event gets multiple values (for example, multiple recipients of SMTP messages), the System treats this event as a combination of several sub-events with unique attribute values.

For example, if an intercepted event has the following attributes:

| Sender | Recipient | Event type | Date |
|---|---|---|---|
| Person: Smith, Person: Johns | Person: Williams, Person: Johns, Person: Smith | Skype | 09:23 |

then the System divides it into the following sub-events:

| Sender | Recipient | Event type | Date |
|---|---|---|---|
| Person: Smith | Person: Williams | Skype | 09:23 |
| Person: Smith | Person: Johns | Skype | 09:23 |
| Person: Smith | Person: Smith | Skype | 09:23 |
| Person: Johns | Person: Williams | Skype | 09:23 |
| Person: Johns | Person: Johns | Skype | 09:23 |
| Person: Johns | Person: Smith | Skype | 09:23 |

**2. Dividing rules to sub-rules and choosing appropriate sub-rules**

Each rule of opearting policy is divided into sub-rules by the following keys:

1. For transfer rules: by a pair of keys "Sender" - "Recipient".

   > **Note:**
   >
   > If the **Direction of route** parameter has **In both directions** value, then a pair of keys "Recipient" - "Sender" will be added.

2. For copy rules: by the key "Sender".
3. For clipboard rules: by the key "Persons".

4. For storage rules: by a pair of keys "File owners" - "Who has access to file".

For example, the following rules:

| Sender | Direction | Recipient | Event type | Date | Reaction |
|---|---|---|---|---|---|
| Group: Lawyers, The<br>Person: Smith,<br>Person: Johns | -> | Group: Marketing,<br>Person: Williams | Email | 08:00-20:00 | Notify: Thomas<br>Violation level: Low |
| Group: Logistics | -> | Group: Sales,<br>Group: Delivery | Skype | 10:00-19:00 | Notify: Johns<br>Violation level: Medium |
| Group: Financial | -><br><- | Group: Lawyers,<br>Group: Sales | | | Notify: Miller<br>Violation level: High |

are divided into the following sub-rules:

| Sender | Direction | Recipient | Event type | Date | Reaction |
|---|---|---|---|---|---|
| Group: Lawyers | -> | Group: Marketing | Email | 08:00-20:00 | Notify: Thomas<br>Violation level: Low |
| Group: Lawyers | -> | Person: Williams | Email | 08:00-20:00 | Notify: Thomas<br>Violation level: Low |
| Person: Smith | -> | Group: Marketing | Email | 08:00-20:00 | Notify: Thomas<br>Violation level: Low |
| Person: Smith | -> | Person: Williams | Email | 08:00-20:00 | Notify: Thomas<br>Violation level: Low |
| Person: Johns | -> | Group: Marketing | Email | 08:00-20:00 | Notify: Thomas<br>Violation level: Low |
| Person: Johns | -> | Person: Williams | Email | 08:00-20:00 | Notify: Thomas<br>Violation level: Low |
| Group: Logistics | -> | Group: Sales | Skype | 10:00-19:00 | Notify: Johns<br>Violation level: Medium |
| Group: Logistics | -> | Group: Delivery | Skype | 10:00-19:00 | Notify: Johns<br>Violation level: Medium |

| Sender | Direction | Recipient | Event type | Date | Reaction |
|---|---|---|---|---|---|
| Group: Financial | -> | Group: Lawyers | | | Notify: Miller<br>Violation level: High |
| Group: Financial | -> | Group: Sales | | | Notify: Miller<br>Violation level: High |
| Group: Lawyers | -> | Group: Financial | | | Notify: Miller<br>Violation level: High |
| Group: Sales | -> | Group: Financial | | | Notify: Miller<br>Violation level: High |

Then, for each sub-event, the System chooses sub-rules whose conditions match the sub-event (for more details on rule attributes, see *Rule of Transfer*, *Rule of Copying*, *Rule of Placement* and *Application activity rule*).

**3. Determining the priority sub-rule**

For sub-rules that match the sub-event, a rule with the maximum weight is selected. The weight of a sub-rule is determined as the sum of weights of all matching conditions according to the table below:

| Sender/Recipient | Weight (if the attribute is enabled) | Weight (if the attribute is disabled) |
|---|---|---|
| Contact | 10000 | 3 |
| Person | 5000 | 7 |
| Group | 2500 | 15 |
| Domain | 1250 | 35 |
| URL | 600 | 75 |
| List of resources | 300 | 150 |
| Perimeter (for data protection policies) | Mimimum weight of the perimeter element | Maximum weight of the perimeter element |
| Perimeter (for data protection policies on agents) | 300 | 150 |
| Device ID | 50 | 25 |

| Sender/Recipient | Weight (if the attribute is enabled) | Weight (if the attribute is disabled) |
|---|---|---|
| Cloud storage address | 50 | does not apply |
| Address and path to file | 20 | |
| Device name | 10 | 5 |
| Source type/receiver type | 1 | does not apply |
| Storage | 1,25 | |
| Computer | 1,25 | does not apply |
| Source-application / Reciever-application | 0,415 | 0,1 |
| Terminal session = Enabled | 0,83 | does not apply |
| Days of the week | 0,15 | does not apply |
| Time (interval when the rule is active) | 0,15 | does not apply |
| Event type | 0,1 | does not apply |
| User attribute | 1 | 0,5 |
| If the attribute is not filled:<br>• Sender (for transfer and copy rules)<br>• Recipient (for transfer rules)<br>• Person (for application activity rules, file operations)<br>• File owners/Who has access to file (for placement rules) | 1 | does not apply |
| If the attribute is not filled:<br>• Event type (for all rules)<br>• Day of the week (for transfer, copy, and application activity rules)<br>• Time (for transfer, copy, and application activity rules) | 0 | does not apply |

| Sender/Recipient | Weight (if the attribute is enabled) | Weight (if the attribute is disabled) |
|---|---|---|
| • Computer (for transfer, copy, application activity rules and file operations)<br>• Storage (for placement rules)<br>• Terminal session (for application activity rules)<br>• Source-application/Reciever-application (for application activity rules and file operations)<br>• Copy source/Copy reciever (for copy rules)<br>• User attribute | | |

For example, the rule with a condition of forwarding from any sender to a specific contact (10000 + 1 = 10001) has a higher priority than the rule with a condition of forwarding from a particular person to a group of persons (5000 + 2500 = 7500).
If for the same sub-event, there are two or more sub-rules with the same priority, the several rules with the highest priority are selected.
If a sub-event has no matching rules, then a default rule is selected (see *Determining System Default Response*).

**4. The order of applying actions according to selected priority rules**

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

1. If the **Delete event** option is selected, then the actions specified in the rule are not executed and the event is not saved to the database.
2. The event is assigned a verdict with the highest priority from priorities in the selected rules. Verdicts have the following priorities:
   - for **Block** verdict, the priority is 2;
   - for **Quarantine** verdict, the priority is 1;
   - for **Allow** verdict, the priority is 0.

   > **Note:**
   >
   > A verdict assigned to the event as a result of applying a data protection policy on agents is not replaced with a verdict specified in rules of data protection policies and person control policies.
   >
   > A verdict assigned to the event as a result of applying a data protection policy is not replaced with a verdict specified in rules of a person control policy.

3. The event is assigned the highest violation level from violation levels in the selected rules.
4. Tags specified in the selected rules are added to existing tags.
5. For identified senders, statuses specified in the selected rules are added to existing statuses.
6. Persons specified in the selected rules are notified.

**Example:**

Let the System have two policies:

| Policy №1 | | | | | |
|---|---|---|---|---|---|
| Catalogue of protected objects: Accounts | | | | | |
| Rule number | Sender | Recipient | Date | **Event type** | Reaction |
| 1.1 | Group: Sales Department | Group: Accounts Department | 08:00-20:00 | Email | Violation: None |
| 1.2 | Smith | Group: Accounts Department | | Email | Violation: None |
| 1.3 | Smith | <>Perimeter: Company | | | Violation: Medium |
| 1.4 | Default: | | | | Violation: High |

| Policy №2 | | | | | |
|---|---|---|---|---|---|
| Catalogue of protected objects: Contract | | | | | |
| Rule number | Sender | Recipient | Date | **Event type** | Reaction |
| 2.1 | Group: Sales Department | <>Perimeter: Company | 08:00-20:00 | Email | Violation: None |
| 2.2 | Smith | <>Perimeter: Company | | Email | Violation: None |
| 2.3 | Default: | | | | Violation: None |

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

| Data | Sender | Recipient | Date | **Event type** |
|---|---|---|---|---|
| Protected objects: Accounting, Contract | Smith | Johns, williams@mail.com | 19:00 | Email |

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

**1. Check for conformance to policy №1.**

The event confirms to the policy №1 as it contains a *Group of protected objects - Accounts*.
The "Smith->Johns" sub-event is considered:

| Sender | Recipient | Date | **Event type** |
|---|---|---|---|
| Smith | Johns | 19:00 | Email |

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

| Sender | Recipient | Date | **Event type** |
|---|---|---|---|
| Smith | williams@mail.com | 19:00 | Email |

This sub-event confirms to the sub-rule №1.3 only. Therefore, the rule №1.3 is selected

**2. Check for conformance to policy №2.**

The event confirms to the policy №2 as it contains a *Group of protected objects Contract.*

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

| Sender | Recipient | Date | **Event type** |
|---|---|---|---|
| Smith | Johns | 19:00 | Email |

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

| Sender | Recipient | Date | **Event type** |
|---|---|---|---|
| Smith | williams@mail.com | 19:00 | Email |

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

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

> **Important!**
>
> Data interception on policies on agents configured works on each event's element. E.g., in case of sending an e-mail containing few attachments of different files, the analysis and policies can be applied separately to each element, each attachment. E-mail subject and e-mail body are to be analysed separately as well.

## 4.7.2 Preset Policies

There are the following preset policies in the System:

- Data protection policies for confidential data
- Person control policy
- Policy that regulates transferring of password-protected data
- Policies that regulate visiting web resources
- Policy that excludes mailing lists from interception
- Competitors Control Policy

- Clipboard Control Pollicy

Set of data protection policies for confidential data depends on classification base languages selected when installing Traffic Monitor. Set of other policies depends on the preset configuration language selected when installing Traffic Monitor. For details, see *InfoWatch Traffic Monitor*. *Installation Guide. Installing Traffic Monitor Server and Database* subsection.

**Note:**

When deleting the database scheme (see *InfoWatch Traffic Monitor. User Guide. Deleting the Database Scheme* article), policies (including preset ones) are also deleted from the System.

To redeploy the preset policies, do the following:

1. Create **/opt/iw/tm5/www/backend/protected/runtime/first_run** file on behalf of **iwtm** user;
2. Restart **iw_kicker** process:
   `iwtm restart kicker`

Then you need to create other policies anew (see *Creating Data Protection Policy*, *Creating Data Protection Policy on Agents*, and *Creating Person Control Policy*). You can import them as well. For details, see *Exporting and Importing policies*.

## Data Protection Policy

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

Default policies have the following attribute values:

| Attribute | Value |
|---|---|
| Policy name | <Name of the catalogue of protected objects> |
| Status | Active |
| Validity period | All time |
| Type of objects of research | <Name of the catalogue of protected objects> |

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

Each policy contains the following rules:

**Rules of transfer**

1. *A rule that regulates transferring confidential data outside the company perimeter*.
   **If** an employee sends traffic of any type outside the company perimeter any day of the week,
   **Then** the System performs the following actions:
   - sets the *Allowed* value to the *Verdict* attribute of the event;
   - sets one of the following values to the *Violation level* attribute of the event:
     - *High* - for the following catalogues of protected objects: Security label, Personal data;
     - *Low* - for the following catalogues of protected objects: Law, HR, IT;
     - *Medium* - for all other catalogues of protected objects;

    - sets the *None* value to the *Status* attribute of the person who sends the traffic.
2. *A rule regulating the transfer of confidential data by heads of the company*.
   **If** an employee from the VIP group sends traffic of any type to any recipient any day of the week,
   **Then** the System performs the following actions:
    - sets the *Allowed* value to the *Verdict* attribute of the event;
    - sets the *None* value to the *Violation level* attribute of the event;
    - sets the *VIP* tag to the event.

**Rules of copying**

*A rule that regulates copying confidential data to removable devices*.

**If** an employee copies confidential data related to any category to the removable device (including one within terminal session), cloud storages, or using FTP protocol any day of the week,
**Then** the System performs the following actions:

- sets one of the following values to the *Violation level* attribute of the event:
    - *High* - for the following catalogues of protected objects: Security label, Personal data;
    - *Low* - for the following catalogues of protected objects: Law, HR, IT;
    - *Medium* - for all other catalogues of protected objects;
- sets the *None* value to the *Status* attribute of the person who sends the traffic.

**Rules of placement**

*A rule that regulates storing confidential data. The rule is added only for the policies with the following protected data: Security Label or Personal Data catalogues of protected objects.*

**If** a person stores protected data in any location,
**Then** the System performs the following actions:

- sets the *High* value to the *Violation level* attribute of the event*;*
- sets the *None* value to the *Status* attribute of the person who owns the data*.*

## Person Control Policy

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

| Attribute | Value |
|---|---|
| Policy name | Persons under supervision |
| Status | Active |
| Validity period | All time |
| Statuses | Under supervision |

Policy Rules

*The rule that regulates transferring data by persons with Under Supervision status.*

**If** a person with the *Under supervision* status sends traffic of any type to any recipient,
**Then** the System sets:

- the *Allow* value to the *Verdict* attribute of the event;
- the *For consideration* value to the *Tag* attribute of the event.

## Policy that Regulates Transferring Password-Protected Data

By default, the System has a policy that regulates transferring password-protected data.

The default policy has the following attribute values:

| Attribute | Value |
|---|---|
| Policy type | Data protection policy |
| Policy name | Password-protected data |
| Status | Active |
| Validity period | All time |
| Protected data | Encrypted files of all formats |

Policy rules

*The rule that regulates transferring password-protected data outside the company perimeter.*

**If** a person sends traffic of any type outside the company perimeter any day of the week,
**Then** the System performs the following actions:

- sets the *Allow* value to the *Verdict* attribute of the event;
- sets the *Medium* value to the *Violation level* attribute of the event;
- assigns the *For consideration* tag to the event.

## Policies that Regulate Visiting Web Resources

By default, the System has the following data protection policies that control visiting web resources by the company employees:

- Using personal mail;
- File sharing services;
- Sending to free email domains;
- Disloyal Employees;
- Social networks, messengers and video conferencing;
- Artificial intelligence;
- Converters.

Using personal mail

By default, the System has a preset policy that controls usage of personal web email by employees.

The default policy has the following attribute values:

| **Attribute** | **Value** |
|---|---|
| Policy type | Data protection policy |

| Attribute | Value |
|---|---|
| Name | Using personal mail |
| Status | Active |
| Validity period | All time |
| Protected data | Any data |

The policy contains the following rule:

**Transfer rule**

*The rule that controls email transfer using web email.*

**If** a person sends or receives an email via web email,
**Then** the System will perform the following actions:

- assign the value *Allow* to the event attribute *Verdict*;
- assign the value *Low* to the event attribute *Violation level.*

File sharing services

By default, the System has a preset policy that controls usage of file sharing services.

The default policy has the following attribute values:

| Attribute | Value |
|---|---|
| Policy type | Data protection policy |
| Name | File sharing services |
| Status | Active |
| Validity period | All time |
| Protected data | All file formats, except JSON and XML |

The policy contains the following rule:

**Transfer rule**

*The rule that controls sending requests to file sharing services.*

**If** a person from the company perimeter sends request to a web resource from the list of "File sharing services" (for details, see *Web Resources*).
**Then** the System will perform the following actions:

- assign the value *Allow* to the event attribute *Verdict*;
- assign the value *Low* to the event attribute *Violation level.*

**Copy rules**

*The rule that controls cloud storage usage*.

**If** a person copies confidential data to cloud storage,
**Then** the System will perform the following actions:

- assign the value *Allow* to the event attribute *Verdict*;
- assign the value *Low* to the event attribute *Violation level.*

**File operation rule**

1. *The rule that controls file operations when file sharing services applications are used.*
   **If** a person reads a file using the application of file sharing services: GoogleDriveFS, MEGAsync, nextcloud, OneDrive, YandexDisk2,
   **Then** the System will perform the following actions:
   - assign the value *Allow* to the event attribute *Verdict*;
   - assign the value *Low* to the event attribute *Violation level.*
2. *The rule that controls file operations with file sharing services in browser.*
3. **If** a person reads a file using the file sharing service in browser,

   **Then** the System will perform the following actions:

   - assign the value *Allow* to the event attribute *Verdict*;
   - assign the value *Low* to the event attribute *Violation level.*

Sending to free email domains

By default the System has a preinstalled policy to control email sending to free email domains.

The preinstalled policy has the following attributes' values:

| Attribute | Value |
|---|---|
| Name | Sending to free email domains |
| Status | Active |
| Validity period | All time |
| Protected data | Any data |

**Policy rules:**

*The rule to control data transfer to free email domains outside the company perimeter*.

**If** a person transfers traffic of any type from the company perimeter to the "Free email domains" perimeter on any day of the week,
**Then,** the System will perform the following actions:

- assign the value *Allow* to the attribute of event *Verdict*;
- assign the value "No" to the attribute of event *Violation level*;
- assign Web-email tag to event.

Disloyal Employees

By default, the System has a preset policy that monitors actions of disloyal employees.

The default policy has the following attribute values:

| Attribute | Value |
|---|---|
| Policy type | Data protection policy |
| Policy name | Disloyal employees |
| Status | Active |
| Validity period | All time |
| Protected data | Any data |

**Policy rules**

*The rule of transfer that regulates sending requests to resources related to job search.*

**If** a person sends a request to a web resource included in the "Job search" list (for more details, see *Web Resources*) any day of the week,
**Then** the System performs the following actions:

- sets the *Allow* value to the *Verdict* attribute of the event;
- sets the *Low* value to the *Violation level* attribute of the event.

Artificial intelligence

By default, the System has a preset policy that controls the usage of artificial intelligence resources by company employees.

The default policy has the following attribute values:

| Attribute | Value |
|---|---|
| Policy type | Data protection policy |
| Name | Artificial intelligence |
| Status | Active |
| Validity period | All time |
| Protected data | Any data |

The policy contains the following rule:

**Transfer rule**

*The rule that controls data transfer when using artificial intelligence.*

**If** a person sends a web-message when using an artificial intelligence,

**Then** the System will perform the following actions:

- assign the value *Allow* to the event attribute *Verdict*;
- assign the value *Low* to the event attribute *Violation level.*

**File operations rule**

1. *The rule that controls file operations when using artificial intelligence in browser.*
2. **If** a person reads a file using the artificial intelligence service in browser,
   **Then** the System will perform the following actions:
   - assign the value *Allow* to the event attribute *Verdict*;
   - assign the value *Low* to the event attribute *Violation level.*

Social networks, messengers and video conferencing

By default the System has a policy that controls visiting web resources by the company employees.

The default policy has the following attribute values:

| Attribute | Value |
|---|---|
| Policy type | Data protection policy |
| Policy name | Social networks, messengers and video conferencing |
| Status | Active |
| Validity period | All time |
| Protected data | Any data |

**Policy rules**

*The rule of transfer that regulates sending requests to entertaining resources.*

**If** a person sends a request to a one of the following web resources included in "Social networks" list: Facebook, Skype, Telegram, WhatsApp, XMPP, VKontakte, Yandex messenger, (for more details, see "Web Resources") any day of the week,
**Then** the System performs the following actions:

- sets the *Allow* value to the *Verdict* attribute of the event
- sets the *Low* value to the *Violation level* attribute of the event.

**File operations rules**

1. *The rule that controls the file operations in case the messenger applications are used.*
   **If** a person reads or writes a file using the application WhatsApp, Telegram, Viber, Zoom, Slack, Webex,
   **Then** the System performs the following actions:
   - sets the *Allow* value to the *Verdict* attribute of the event
   - sets the *Low* value to the *Violation level* attribute of the event.
2. *The rule that controls the file operations in social networks and messengers applications in case a browser is used.*

1. **If** a person reads a file in social networks or messengers using a browser,

   **Then** the System performs the following actions:

   - sets the *Allow* value to the *Verdict* attribute of the event
   - sets the *Low* value to the *Violation level* attribute of the event.

Converters

By default, the System has a preset policy that controls the usage of converters by company employees.

The default policy has the following attribute values:

| Attribute | Value |
|---|---|
| Policy type | Data protection policy |
| Name | Converters |
| Status | Active |
| Validity period | All time |
| Protected data | All file formats |

The policy contains the following rule:

**Transfer rule**

*The rule that controls data transfer when using converters.*

**If** a person transfers data when using web resources relating to converters,

**Then** the System will perform the following actions:

- assign the value *Allow* to the event attribute *Verdict*;
- assign the value *Low* to the event attribute *Violation level.*

## Policy that Excludes Mailing Lists from Interception

By default, the System has a preset policy that excludes mailing lists from interception.

The default policy has the following attribute values:

| Attribute | Value |
|---|---|
| Policy type | Data protection policy |
| Policy name | Exclude from interception |
| Status | Active |
| Validity period | All time |
| Protected data | Any data |

Policy rules

*Rule that regulates sending data by persons from the "Exclude from Interception" perimeter*

**If** a person who belongs to the *Exclude from interception* perimeter (see *Perimeters*) sends traffic to any recipient any day of the week,
**Then** the System deletes the event.

## Competitors Control Policy

By default, the System has a preset policy that controls the data transfer to competitors by company employees.

The default policy has the following attribute values:

| Attribute | Value |
|---|---|
| Policy type | Data protection policy |
| Name | Competitors |
| Status | Active |
| Validity period | All time |
| Protected data | Any data |

The policy contains the following rule:

**Transfer rule**

*The rule that controls data transfer to competitors.*

**If** a person sends data to competitors,

**Then** the System will perform the following actions:

- assign the value *Allow* to the event attribute *Verdict*;
- assign the value *High* to the event attribute *Violation level.*

## Clipboard Control Pollicy

By default, the System has a preset policy that controls employees' access to the clipboard.

The default policy has the following attribute values:

| Attribute | Value |
|---|---|
| Policy type | Data protection policy |
| Name | Clipboard |
| Status | Active |
| Validity period | All time |
| Protected data | Any data |

The policy contains the following rule:

**Application activity rule**

*The rule that controls data copying and pasting from/to applications when clipboard is used.*

**If** a person uses specified applications when copying or pasting text data to/from the clipboard,

**Then** the System will perform the following actions:

- assign the value *Allow* to the event attribute *Verdict*;
- assign the value *Low* to the event attribute *Violation level.*

### 4.7.3 Creating Data Protection Policy

**Purpose:**
Create a policy that determines the System reaction to actions with data.

**Solution:**

1. Go to the **Policies** section.
2. In the left part of the workspace, click **Add policy** and, in the drop-down list, select **Data Protection Policy**.
   A new policy will be added to the **Data protection policies** group, and, on the right side of the workspace, a policy adding form will be displayed.
3. Specify the policy attributes:
   - Name;
   - Description;
   - Status;
   - Period of action.

   **Important!**

   When you fill the **Validity period** attribute, consider the possible time zone difference between branches of your organization. The time of interception for the event is the local time on the server which intercepts data. If the local time of interception does not fall within the specified range, the policy does not apply to the event.

4. To add protected data to the policy, click **Select**.

   **Note:**

   If you do not select any protected data, then the policy will apply to any data.

5. In the window that appears, set the check boxes next to desired values. Protected data may include protected objects, their catalogs, and file formats.
   For file formats, you can also set an additional restriction on the file size (in bytes) and specify the signs as follows:
   - encrypted;
   - merged;
   - signature and extension are incompatible.

> **Note:**
>
> Attachments with ZIP and RAR multi-volume archives may have the following signs: *merged* and *signature and extension are incompatible*.

> **Warning!**
>
> If protected data of several types are specified for the policy, then for triggering the policy rules (see *Rules and their Viewing Form*), it is necessary that the intercepted event should contain violations of each type.
>
> For example, a catalog of protected objects, several file formats and several attributes are specified as protected data for the policy. In this case, for the policy to be triggered, it is necessary that intercepted data contain at least one protected object from the specified catalog, at least one file of the specified format and all specified attributes.

6. After you have selected protected data, click **Save**.
7. Add rules to the policy (see *Creating Rules*).
8. To save the new policy, in the policy creation form, click **Save**.

**To edit the policy:**

1. Select the desired policy in the list.
2. In the right part of the workspace, edit the necessary parameters.
3. To change the protected data, in the **Protected data block**, click **Select** and then click **Save**.
4. Click **Save** in the policy edit form.

**To delete the policy**, in the right upper corner of the policy, click  and confirm the action in the confirmation window.

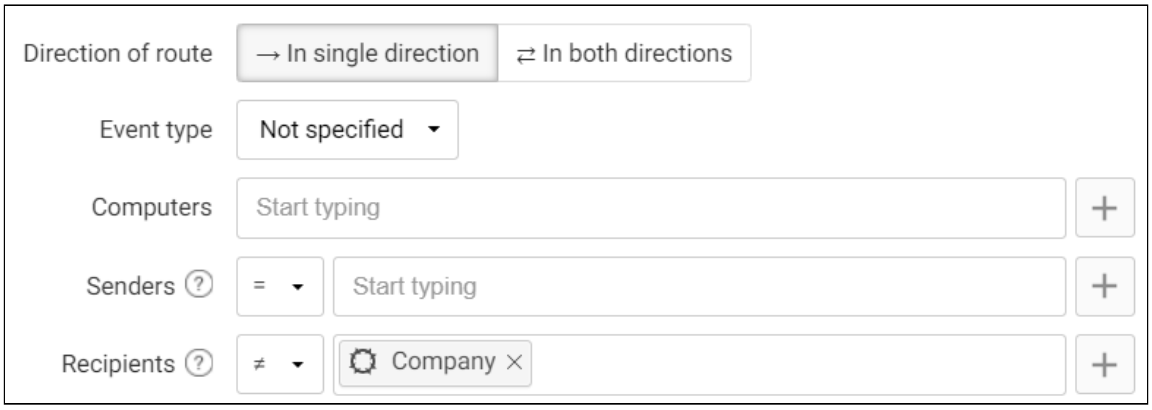
Examples of tasks where a data protection policy can be used are given in the *Examples of Using Data Protection Policy* article.

## Examples of Using Data Protection Policy

***Example 1:***

It is required to control transferring the company statute outside the company which includes sending the document by email or copying it to removable devices. For this:

1. Create a data protection policy and name it *Protection of transferring company statute*.
2. Specify the *Company statute* protected object as protected data.
3. Add a transfer rule that controls sending data to any recipients except for the *Company* perimeter.




4. Specify what actions to perform if the rule is triggered (e.g., assign *Low* violation level to the event).
5. If in addition, you want to control employees under the supervision, add one more transfer rule and specify the *Employees under supervision* group as senders (see *Creating Group of Persons or Computers*).
6. Specify what actions to perform if the rule is triggered (e.g., assign *Medium* violation level and *For consideration* tag to the event).
7. To control copying the document to a removable device, add a copy rule to the policy.

The System will detect a violation of the data protection policy when:

- An email whose body or attachment contains data related to the *Company statute* protected object is sent outside the *Company* perimeter;
- A file with information on the *Company statute* protected object is copied to a removable device.

***Example 2:***

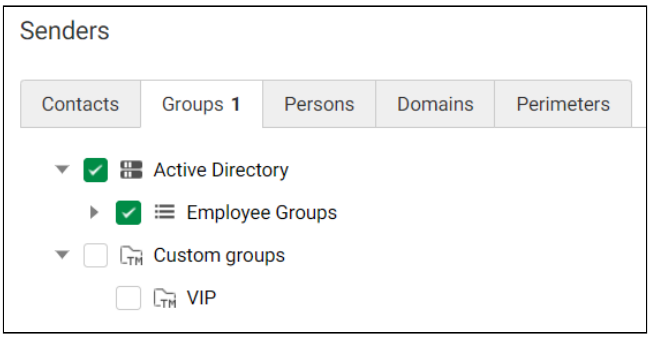
It is required to identify employees who visit job search sites. For this:

1. Create a data protection policy and name it *Identifying disloyal employees*.

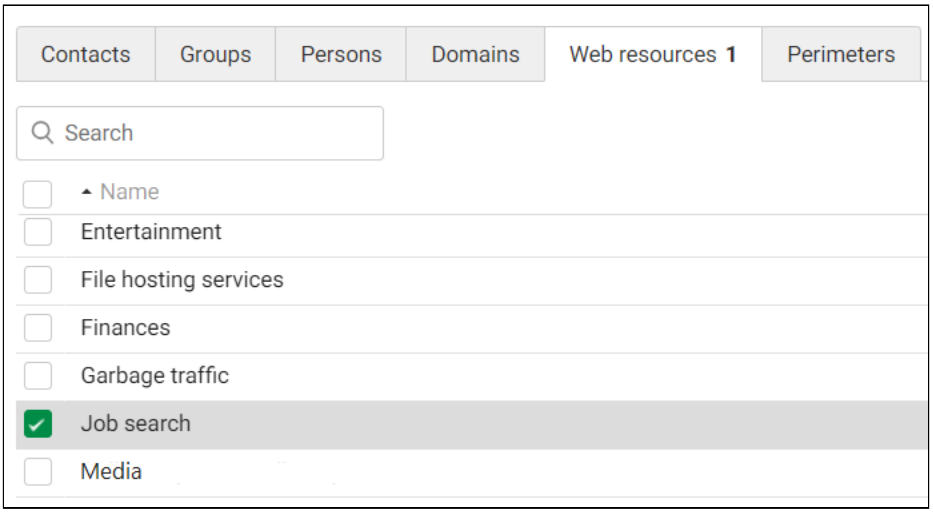
   **Tip:**

   Add the policy description to easily identify it in the policy list. For example, "Identifying employees who send requests to job search sites".

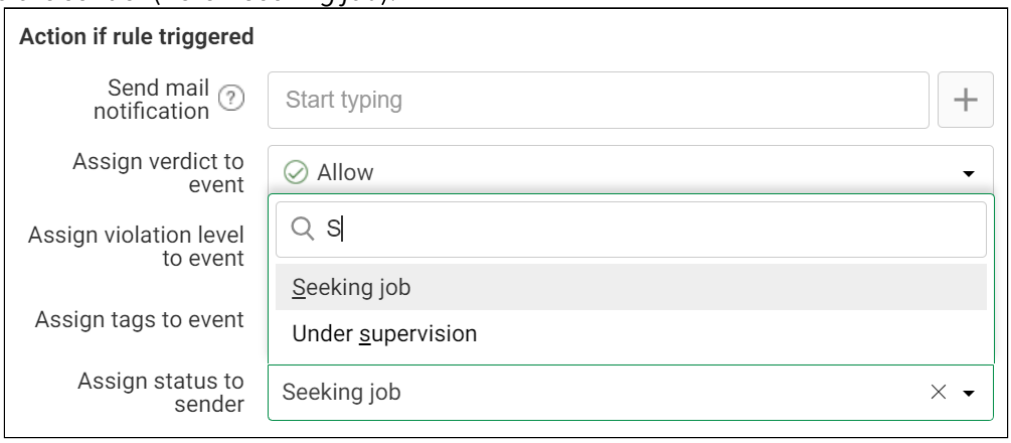
2. Add a transfer rule and specify the group of company employees imported from the Directory Service as senders.




3. Specify the *Job search* list of web resources as recipients.




4. Specify what actions to perform if the rule is triggered. For example, you can assign a specific status to the sender (here – *Seeking job*).




5. Save the rule and apply the changes of configuration.

Now, if an employee sends a request to a job search site, the System will assign the *Seeking job* status to the employee.

If necessary, you can find all such events. For this, create a query and specify one of the following search conditions:

- *Identifying disloyal employees* policy;
- senders with the *Seeking job* status.

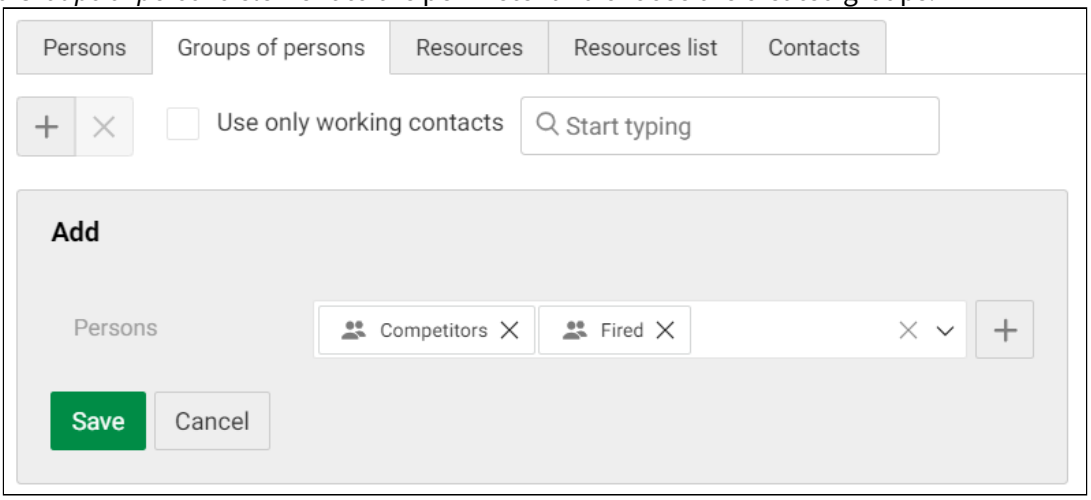
***Example 3:***
It is required to identify employees who communicate with undesired destinations, i.e., fired employees, competitors, etc.

For this, you need to create a perimeter that will include fired employees, competitors, etc. and then create a data protection policy that tracks sending data to this perimeter.

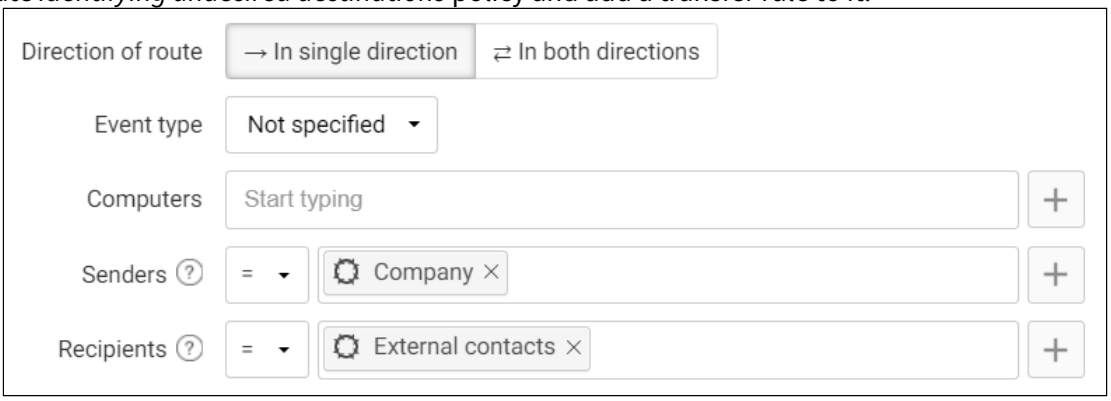
> **Note:**
>
> You can add separate person contacts or create user groups, e.g., *Fired employees* and *Competitors*. This example illustrates creating a perimeter based on user groups.

Perform the following steps:

1. Create *Fired employees* group and fill it in one of the following ways:
    - Create cards for fired employees manually;
    - Import persons from the Directory Service (if the person card is not deleted from the Directory Service when a person is fired).
2. Create *Competitors* group and fill it in one of the following ways:
    - Create a separate card for each person in the group, e.g., John Williams from "New company";
    - Create a card for each competitor company and add contacts of the company employees to this card.
3. If necessary, create groups for other undesired destinations.
4. Create a perimeter that will include the created groups and name it, for example, *External contacts*.
5. Add a *Groups of persons* element to the perimeter and choose the created groups.




6. Create *Identifying undesired destinations* policy and add a transfer rule to it.




7. Specify what actions to perform if the rule is triggered, e.g., assign *Medium* violation level to the event.
8. Apply the configuration to put the configured policy in action.

If an email is sent to a fired employee or a competitor, the System will determine the policy violation.

If necessary, you can find all such events: for this, create a query and specify the *Identifying undesired destinations* policy in search conditions.

## 4.7.4 Creating Data Protection Policy on Agents

**Purpose:**

Create a policy that determines the System reaction to actions with data and applies directly on Device Monitor Agents. This policy allows you to operatively prevent data leaks on computers where Device Monitor Agents are installed.

**Note:**

If Device Monitor Agent is installed directly on a computer running Windows, it can block:

- HTTP(S) traffic (text and files);
- Outgoing webmail as well as SMTP and MAPI traffic;
- Copying of files:
  - From/to removable devices;
  - From/to resources connected via a terminal session;
  - From/to network resources;
  - To cloud storage services according to Device Monitor rule;
  - To FTP servers;
  - From terminal session applications (available when working with Device Monitor server running Windows OS);
- Copying of text from/to a terminal session via the clipboard;
- Printing of documents, if text has been extracted from a webpage or a file sent to print.

If Device Monitor Agent is installed directly on a computer running a Linux-family OS, it can block:

- HTTP(s) traffic (text only);
- Outgoing web email and SMTP traffic;
- Copying of files from/to removable devices connected via the file system;
- Copying of files from/to network resources connected via the file system and with standard file explorers, built-in and third-party utilities.

On Device Monitor Agents of version 12 and earlier installed on workstations running Astra Linux or Alt Linux OS, data protection policies on Agents are not supported.

**Solution:**

1. Go to the **Policies** section.
2. In the left part of the workspace, click **Add policy** and, in the drop-down list, select **Data Protection Policy on Agents**.
   A new policy will be added to the **Data protection policies on agents** group, and, in the right part of the workspace, a policy adding form will be displayed.
3. Specify the policy attributes:
   - Name;
   - Description;
   - Status;
   - Period of action.

**Warning!**

When you fill the **Validity period** attribute, consider the possible time zone difference between branches of your organization. The time of interception for the event is the local time on Device Monitor agent. If the local time of interception does not fall within the specified range, the policy does not apply to the event.

4. To add protected data to the policy, click **Select**.

> **Note:**
>
> If you do not select any protected data, then the policy will apply to any data.

5. In the **Choose protected data** window that appears, set checkboxes next to desired values. Protected data[1] may include:
   - **Protected objects**
     You can select protected objects that contain only categories and text objects and for which detection within the event element is not enabled.[2]
   - **Catalogues of protected objects**
     From selected catalogues, the policy will use only those protected objects that are based on categories and text objects, and for which detection within the event element is not enabled.[2]
   - **File formats**
     For file formats, you can specify:
     - encrypted;
     - file signature and extension do not match.
       If the **Encrypted** option is selected, then the policy is triggered only if a file is encrypted or the System failed to determine the file format.
   - restriction on the file size (in bytes);
   - if the policy should apply to all files or in accordance with the following file signs:
   - if the policy should apply only when detecting violations in files of the specified formats.
     If the **Apply to selected file formats only** option is selected, then protected objects specified in the policy will be detected only in attachments. The attachments should have formats specified in the policy.

> **Note:**
>
> By default, detecting violations only in files of the specified formats is disabled. To enable it, first you should select a protected object or a catalogue of protected objects, as well as a file format.
>
> The option applies only for events with the **Email** type.

> **Warning!**
>
> [1] If protected data of several types are specified for the policy, then for triggering the policy rules (see *Rules and their Viewing Form*), it is required that the intercepted object should contain violations of each type.
>
> For example, a catalogue of protected objects and several file formats are specified as protected data for a policy. In this case, for the policy to be triggered, it is necessary that intercepted data should contain at least one protected object from the specified catalogue and at least one specified file format.

[2] In case of Device Monitor version 7.9 and earlier, protected objects with enabled negation are not triggered.

When you select the protected data, the following catalogues and protected objects will have the icon :

- The protected objects where negation is enabled. When pointing on the icon  the text explaining that for this protected object the negation is enabled, which is not supported on agents installed on OS Linux, will appear;
- The catalogues containing the protected objects with enabled negation;
- The catalogues containing the protected objects with technologies unsupported on agents (for example, Graphical objects). When pointing on the icon  the tip explaining that this catalogue contains the protected objects which are not supported on agents, will appear.

6. After you have selected protected data, click **Save**.
7. Add rules to the policy (see *Creating Rules*).
8. To save the new policy, in the policy creation form, click **Save**.

**To edit the policy:**

1. Select the desired policy in the list.
2. In the right part of the workspace, edit the necessary parameters.
3. To change the protected data, in the **Protected data block**, click **Select** and then click **Save**.
4. Click **Save** in the policy edit form.

**To delete the policy**, in the right upper corner of the policy, click  and confirm the action in the confirmation window.

***Example 1:***

If you want the System to assign the *Block* verdict and the *Medium* violation level to the event in case of uploading data to cloud storages, take the following steps:

1. Create a data protection policy on agents.
2. Add a copy rule (see *Creating Rules*).
3. In the rule attributes (see *Rule of Copying*), set the value of the **Event type** attribute to *Cloud storage*.
4. In the **Copy receiver** field, specify cloud storages uploading data to which should be blocked.
5. In the **Actions when the rule is triggered** block, set the following values to the attributes:
   - To the **Assign verdict to the event** attribute – the *Block* value;
   - To the **Assign violation level to event** attribute – the *Medium* value.

***Example 2:***

If you want the System to block data transfer via terminal session using clipboard, send notification to Security officer and assign the status *Under supervision* to violator, take the following steps:

1. Create data protection policy on Agents.
2. While creating the policy, specify the protected data the transfer of which, if detected, will be blocked by the System.
3. Add the Clipboard rule (see *Creating Rules*).
4. As the rule attributes (see *Application activity rule*) specify **Persons** and **Computers**, for which the policy will work, and also rule validity days and time.
5. In the block **Actions when the rule is triggered** specify the values to the attributes as follows:

a. **Send notification** – specify notification template. For example, select the default template **Notification to security officer**.
b. **Assign verdict to event** – the value *Block*;
c. **Assign status to senders** – select the default status **Under supervision**.

After applying the configuration, the created policy will be sent through Device Monitor server to Agents. If the protected data will be detected in transferred text data, the transfer will be blocked and the clipboard will be cleared. Also, the event will be created, Security officer will receive a notification about it, and the violator will get a status "Under supervision" in the System.

For details on creating policies, see the KB article *Intercepting Features and Restrictions when Copying Files (Data Protection Policy on Agents)*.

### 4.7.5 Creating Person Control Policy

**Purpose:**
Create a policy that determines the System reaction to actions of certain persons. The policy applies only to actions of traffic senders.

**Solution:**

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

   > **Note:**
   >
   > If elements of different types are selected (for example, persons and statuses), then the policy is triggered when at least one object of each type is detected.

4. A new policy is added to the **Person Control Policies** group, and, in the right part of the workspace, a policy viewing form is displayed.
5. In the policy form, fill in the required fields (see *Policies Section*) and click **Save**.

   > **Important!**
   >
   > When you fill the **Validity period** attribute, consider the possible time zone difference between branches of your organization. The time of interception for the event is the local time on the server which intercepts data. If the local time of interception does not fall within the specified range, the policy does not apply to the event.

**To edit the policy:**

1. Select the desired policy in the list.
2. In the right part of the workspace, edit the necessary parameters.
3. To change the protected data, in the **Protected data block**, click **Select** and then click **Save**.
4. Click **Save** in the policy edit form.

**To delete the policy**, in the right upper corner of the policy, click  and confirm the action in the confirmation window.

You can also add person control policies directly from **Persons** (see *Persons Section*) and **Statuses** (see *Statuses*) sections.

**To add a policy for a group of persons or computers**:

1. Go to the **Persons** section.
2. Select the desired group in the list.
3. On the toolbar in the left part of the workspace, click .

**To add a policy for selected persons or computers**:

1. Go to the **Persons** section.
2. Select the desired person or computer. To select multiple elements, use Shift or Ctrl keys.
3. On the toolbar in the right part of the workspace, click  and, in the drop-down list, select **Create policy**.

**To add a policy for a selected status:**

1. Go to **Lists** -> **Statuses** section.
2. Select the desired status from the list.
3. On the toolbar, click .

***Example:***

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

1. Go to the **Policies** section and create a person control policy named *Smith*.
2. Create a rule for the policy *Smith* and set the following values to the attributes:
    - attribute **Intercept with the violation level** - *High* value;
    - attribute **Send notifications** - *example@company.com* value (for details, see *Configuring Notifications in Rules*);
    - attribute **Assign verdict** - *Allow* value;
    - attribute **Set status** - *Under supervision* value.
3. Save the policy.

## 4.7.6 Creating Rules

**Reference information:**

Each policy can include one or more rules.

If the policy is triggered on the interception object, then, depending on the number of triggered rules, the following variants are possible:

- If one rule is triggered, the System performs actions specified in this rule.
- If several rules are triggered and
    - their actions contradict, then the System chooses the priority action and performs it (on the order of selecting priorities, see *General Information on Policies*);
    - their actions do not contradict, then the System performs all specified actions.

- If no rule is triggered or rules are not specified, then the System performs the actions specified in the default rule (see *Determining System Default Response*).

> **Note:**
>
> If the interception object triggers multiple policies, and each policy has its own rules, then the System chooses the action with the highest priority and performs it (on the order of selecting priorities, see *General Information on Policies*). Actions that do not contradict other actions are performed in full.

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

**Solution:**

1. Go to the **Policies** section.
2. Select the required policy in the list or create a new policy (see *Creating Data Protection Policy*, *Creating Data Protection Policy on Agents*, and *Creating Person Control Policy*).
3. Add a rule in one of the following ways:
   - on the tab of the selected rule group, click **Add rule**.
   - in the right upper corner of the form, click **Add rule**, and, from the drop-down list, select the desired rule.
4. Configure the rule using a form on the right part of the workspace (see *Rules and their Viewing Form*).
5. In the **Actions when the rule is triggered** block, specify what actions the System should perform when the rule is triggered (see *Determining System Response to Policy Violations*).
6. Click **Save**.

**To edit the rule:**

1. Select the required policy in the list.
2. In the policy tile, select the required rule group. Rules are grouped on the following tabs:
   - **Transfer**, **Copy**, **Placement**, **Application activity, and File operations** - for data protection policies;
   - **Transfer, Copy** - for data protection policies on agents;
   - **Rules** - for person control policies.
3. The policy tile will display the list of rules of the selected group. Left-click the desired rule in the list.
4. The rule edit form will open in the right part of the workspace. Edit the necessary fields, then click **Save**.

**To delete the rule**, in the right upper corner of the rule tile, click  and confirm the action in the confirmation window.

***Example 1:***

If a person transfers files included in the *Strictly confidential* protected object on Saturdays and Sundays, the System should assign the *Sending confidential data on weekends* tag to the event and set the *Medium* violation level. For this:

1. Create the *Sending confidential data on weekends* tag (see *Managing Tags*).
2. Create a data protection policy for the *Strictly confidential* protected object (see *Creating Data Protection Policy*).

3. Add a transfer rule and assign the *Saturday* and *Sunday* values to the **Days of rule activity** attribute.
4. In the **Actions when the rule is triggered** block, assign the following values to attributes:
   - **Set violation level** attribute - *Medium* value;
   - **Tags** attribute - *Sending confidential data on weekends* value.
5. Click **Save**.

***Example 2:***

If a person copies confidential files from the *Confidential_information* folder on the *www.company.ru* network resource, the System should assign the *Copying confidential information* tag to the event and set the *Low* violation level.
For this:

1. Create the *Copying confidential information* tag (see *Managing Tags*).
2. Create a data protection policy for the *Confidential information* protected object (see *Creating Data Protection Policy*).
3. Add a copy rule and assign the *In single direction* value to the **Direction of route** attribute.
4. In the **Copy source** attribute, click . Then in the window that opens, select *Network resource* as the **Source type** field and enter the value *www.company.ru/Confidential_information/** in the **Path to file or address** field.
5. In the **Actions when the rule is triggered** block, assign the following values to attributes:
   - **Set violation level** attribute - *Low* value;
   - **Tags** attribute - *Copying confidential information* value.
6. Click **Save**.

***Example 3:***

If a person stores personal data in a *Lib/Personal/user_storage.ru* file storage, the System should set the *High* violation level.
For this:

1. Create a scanning task in Data Discovery (see *InfoWatch Data Discovery. User Guide. Scanning Task*).
2. Create a data protection policy for the *Personal data* protected object (see *Creating Data Protection Policy*).
3. Add a placement rule and assign the *Data Discovery* value to the **Event type** attribute.
4. In the **Storage** attribute, click .
5. In the window that opens, on the **File storages** tab enter the *user_storage.ru* server value and the *Lib/Personal* path value. Click **Save**.
6. After entering the information in the **Storage** window, click **Save**.
7. In the **Actions when the rule is triggered** block, assign the *High* value to the **Set violation level** attribute.
8. Click **Save**.

***Example 4:***

If a person forwards copied text data from the *CRM-system* to the *Google Chrome* browser, the System should set the *Low* violation level.
For this:

1. Create a data protection policy for the *Clipboard control* protected object (see *Creating Data Protection Policy*).
2. Add an application activity rule and assign the *Clipboard* value to the **Event type** attribute.

3. Enter the **CRM-system** value in the field of the **Source application** attribute or click  and select the required value from the list.
4. Enter the **Google Chrome** value in the field of the **Source application** attribute or click  and select the required value from the list.
5. In the **Actions when the rule is triggered** block, assign the *Low* value to the **Set violation level** attribute.
6. Click **Save**.

Example 5:

If a person uploads a file to the *example.com* website, the System should assign the *Read file* tag to the event and set the *Low* violation level.
For this:

1. Create the *Read file* tag (see *Managing Tags*).
2. Create a data protection policy for the *Read file* protected object (see *Creating Data Protection Policy*).
3. Add a file operation rule and assign the *Read file* value to the **Event type** attribute.
4. Enter the **example.com** value in the field of the **Browser tab address** attribute.
5. In the **Actions when the rule is triggered** block, assign the following values to attributes:
   - **Set violation level** attribute - *Low* value;
   - **Tags** attribute - *Read file* value.
6. Click **Save**.

## 4.7.7 Determining System Response to Policy Violations

**Reference information:**
For each policy, you can specify actions the System performs in case of the rule violation. For this, choose actions in the **Action when rule triggered** area while creating or editing the rule (see *Creating Rule*).

**Available actions** are determined by the rule type:

<table>
<tr><th colspan="2"></th><th colspan="6">Action</th></tr>
<tr><th>Policy</th><th>Rule</th><th>Send notification</th><th>Assign verdict to event</th><th>Assign violation level to event</th><th>Assign tags to event</th><th>Assign status to sender</th><th>Delete event</th></tr>
<tr><td rowspan="5">Data protection policies</td><td>Transfer</td><td rowspan="5">Available</td><td>Available</td><td rowspan="5">Available</td><td rowspan="5">Available</td><td rowspan="5">Available</td><td rowspan="5">Available</td></tr>
<tr><td>Copy</td><td>Available*</td></tr>
<tr><td>Placement</td><td rowspan="3">Not available</td></tr>
<tr><td>Application activity</td></tr>
<tr><td>File operations</td></tr>
</table>

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Data protection policies on agents | Transfer | Available | Available | Available | Available | Available | Not available |
| | Copy | | | | | | |
| | Application activity | | | | | | |
| Person control policies | Person control | Available | Available | Available | Available | Available | Available |

* By default, assigning verdict to events is unavailable for Copy rules, but you can manually enable verdict management. For details, see *InfoWatch Traffic Monitor. Administration Guide. Configuring Verdict Management* article.

**A detailed description of actions:**

| Action | Description |
|---|---|
| Send notification | Allows you to specify which notifications to send if the rule is triggered. To configure sending notifications, click + next to the field. In the dialogue box that opens, choose a notification from the list or create a new one. For details, see *Configuring Notifications in Rules*.<br>A selected notification template should match the verdict specified in the rule.<br>**Note:** If after the rule is created, the person or the person's e-mail are deleted from the System (on managing user accounts, see *InfoWatch Traffic Monitor. Administration Guide. Users* section), a notification will not be sent to this person. |
| Assign verdict to event | The event is assigned a verdict which is a preliminary System decision concerning possible violation of the security policy. Possible values:<br>• **Allow** – the object is not a potential violation and can be delivered to senders.<br>• **Block** – the object is a potential violation. In the *Block* mode, the object delivery is blocked.<br>• **Quarantine** (for data protection policies on agents, this verdict is unavailable) – the user should make a decision whether the object is a violation or not. In the *Block* mode, the object delivery is postponed until the user decision is made. Depending on the user decision, the verdict value will change either to **Allowed** (in this case, the message is delivered) or to **Blocked** (for details, see *Making Decision on Object*). Dispatching messages is available only for SMTP letters when the System operates in the inline mode (for details see the |

| Action | Description |
| --- | --- |
| | document *InfoWatch Traffic Monitor. Administration Guide*. |
| Assign violation level to event | A violation level will be assigned to the event. Possible values: **High**, **Medium**, **Low**, **No**. |
| Assign tags to event | The event will be assigned tags, for example, **Under supervision**. For details, see *Tags*. |
| Assign status to senders | The security policy violators will be assigned a specified status, for example, **Under supervision**. For details, see *Statuses*. |
| Delete | Select an option:<br>• **Attachments only**<br>• **Attachments and extracted text**<br>• **Entire event** (the option selection makes all other actions with events unavailable)<br>In case **Entire event** option is selected, then the event will not be saved to a database and actions specified in the rule will not be performed either.<br>In case you have Data Analysis Service installed and selected **Attachments only**, the System will search for analogues of text contents. If you selected **Attachments and extracted text**, the search will not be performed. For more information, see *Search for Analogues*.<br>**Note:** Available for the Data protection policy and the Person control policy. |

**See also:**

- Creating Rule;
- Configuring Notifications in Rules.

## 4.7.8 Configuring Notifications in Rules

When you create or edit a rule, you can specify who should receive notifications if the rule is triggered.

For this:

1. In the **Actions when the rule is triggered** area, in the **Send notifications** field, click .
2. In the **Choosing mail notifications** dialog box, set checkboxes next to selected notifications. You can choose several notifications to be sent to different recipients.

> **Note:**

If there are no notifications in the System, a corresponding message is displayed. In this case, you can create a notification by clicking **Create notification** in the message window.

3. If there is no appropriate notification in the list, you can create a new notification. For this, click **Create a new one** in the left upper corner of the window.

> **Note:**
>
> To edit a notification from the list, click the notification name.

> **Note:**
>
> You can also create notifications from the **Administration** -> **Notifications** section (see *Configuring Notifications*).

4. In the notification create/edit form, specify the notification parameters as described in *Creating Notification*.
5. To return to the notification list, click **Back to notifications** in the left upper corner of the form.
6. When you have chosen all required notifications, click **Save**.

> **Important!**
>
> A verdict in the notification should match the verdict in the rule. Otherwise, the notification will not be sent.

### 4.7.9 Determining System Default Response

**Reference information:**
If after applying the policy, there are sub-events with no matching rules, the System performs default actions (on dividing events into sub-events, see *General Information on Policies*). Default actions are specified by the user.

> **Note:**
>
> If default actions are not specified and none of the rules is triggered on the interception object, the policy is not triggered on this interception object either.

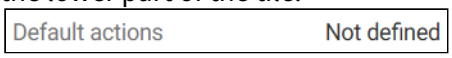
**Purpose:**

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

> **Note:**
>
> Default actions can only be specified for data protection policies and data protection policies on agents.

**Solution:**

1. Go to the **Policies** section.
2. On the left side of the workspace, left-click the target policy.
3. In the policy tile, select the target tab (**transfer**, **copying**, **placement** or **clipboard**) and left-click the lower part of the tile:

4. In the right part of the workspace, specify required actions in the single **Actions** block (see *Rules and their Viewing Form*) and click **Save**.

**Additional information:**

For *Web message* and *Web Email* event types, a default rule can be false triggered. Such a situation may arise when:

The System contains a rule that regulates data transfer from person A to person B. If person A sends data to person B via a website, the System creates an event which is divided into two sub-events:

| Sender | Recipient | Protocol |
|---|---|---|
| Person A | Person B | HTTP |
| Person B | Website domain | HTTP |

Since the route **Person A**->**Website domain** is not specified in the policy rules, the default actions are executed.

To avoid false triggering of the default rule for *Web message* and *Web Email* event types, do either of the following:

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

***Example:***

You want the System to assign the *Under supervision* status to the card of the person who copies data if:

- the copied data from a *Protected government information* protected object, and
- no copy rules are triggered.

For this:

1. Create a data protection policy for the P*rotected government information* protected object (see *Creating Data Protection Policy*).
2. Start configuring default policy actions.
3. In the only **Actions** block, set the *Under supervision* value to the **Set status** attribute.

## 4.7.10 Filtering the List of Policies

**Purpose:**

Filter the list of policies in case of a large number of policies.

**Solution:**

1. Go to the **Policies** section.
2. In the left part of the workspace, click **Filter**.
3. In the **Filter settings** area, specify filtering criteria in one of the fields or in both of them:
   - **Filter by policy name** – start typing and select the name of the needed policy (repeat to select several policies)

- **Filter by protected objects** – start typing and select the name of needed object, file format, person etc (repeat to select several objects)
  For data protection policies and data protection policies on agents, you can specify the following controlled data:
    - catalogue of protected objects;
    - protected object;
    - file format.

  For person control policies, you can specify the following controlled data:
    - person;
    - group of persons;
    - status.

4. Click **Apply**.

## 4.7.11 On Data Protection Policy on Agents

**Why do you need data protection policies?**

Policies of this type apply first and only on DM Agents. In Traffic Monitor, this policy does not apply. The policy allows the Security Officer to control employees' activity on workstations and prevent leaks of confidential data.

The policy allows you to restrict such actions as:

- Data transfer:
  - Outgoing emails via SMTP and MAPI protocols on email
  - Outgoing emails via web email in a browser
  - Internet activity (HTTP(S) requests )
- Data copy:
  - From and to removable devices, network resources, applications connected through a terminal session
  - To FTP, media devices (via MTP protocol), cloud storage
- Work in applications (copying text using the clipboard through a terminal session)

**How the policy works:**

1. To control traffic on workstations, the Security Officer creates and configures the policy in the TM console. The policy is then deployed on workstations.
2. A person performs illegitimate actions (e.g., sends confidential data via web email).
3. DM agent on the workstation analyzes the data being transferred.
4. If the policy is triggered, DM agent performs actions specified in the policy (e.g. blocks data sending if the *Block* verdict is set in the rule). Then DM sends the event and its analysis to TM, and the user gets the following message (if configured): «According to security policy the data transfer is blocked as confidential information has been detected in the data». The action or process started by the user is not complete.
5. TM receives the event, processes and analyzes it.
6. In the console, the Security Officer sees the intercepted event and its analysis results got from DM Agent and TM server.
7. The security officer analyzes the information and takes necessary actions.

**What do you need to create a policy?**

- Add policy rules
- Select protected data. This can be:
  - protected objects containing text objects, categories and terms and catalogues of protected objects

    - file formats
      If no protected data is selected, the policy is applied to actions with any data
- Specify a period during which the policy will apply (can be unlimited or have defined dates).

The following rules can be added: transfer rule, copy rule, application activity rule.

For details see *Rules and their Viewing Form*, *Rule of Transfer*, *Rule of Copying*, *Application activity rule*.

## 4.7.12 On Data Protection Policy

**Why do you need data protection policies?**

Policies of this type apply in TM after data protection policies on agents. They allow you to monitor the following channels of data leaks:

- Messengers
- Screenshots, printing
- File operations
- Clipboard
- Keyboard input

**How the policy works:**

1. The security officer creates and configures the policy for extended control of data protection. The channels listed above are to be controlled..
2. A person performs illegitimate actions (e.g., tries to print a file with confidential data).
3. TM analyses received data.
4. If the policy is triggered (policy rules are violated), an event is created. The message is sent to the recipient (its shadow copy is created in TM) or sending is blocked (if *Blocked* verdict is applied according to the rule). An event is created.
5. In the console, the security officer can see the event and the results of its analysis received after processing the event on TM server.
6. The security officer analyses the information and can take necessary actions.

**What do you need to create a policy?**

- Add policy rules.
- Choose protected data. This can be any combinations of protected objects, catalogues of protected objects, file formats. If no protected data is selected, the policy is applied to actions with any data.
- Specify a period during which the policy will apply (can be unlimited or have defined dates).

The following rules can be added: transfer rule, copy rule, rule of placement, clipboard rule.

For details see *Rules and their Viewing Form*, *Rule of Transfer*, *Rule of Copying*, *Rule of Placement*, *Application activity rule*, *File Operations Rule*.

## 4.7.13 On Person Control Policy

**Why do you need data protection policies?**

Policies of this type can be used if the security officer needs to monitor actions of a particular person.

**How the policy works:**

1. The security officer configures a person control policy and specifies the controlled person.
2. If actions of this person trigger the policy rules, information about these actions is sent to TM.
3. TM analyses the received information.

4. The security officer sees the event with analysis results and takes necessary actions.

**What do you need to create a policy?**

- Add person control rule (see *Person Control Rule*).
- Specify controlled objects (they can be persons, person groups, or statuses).

> **Note:**
>
> The policy applies to event initiators only. Traffic recipients are not controlled by this policy.

## 4.7.14 Exporting and Importing policies

**Purpose:**

- export policies with their attributes and elements of technologies used in them to a file;
- load from the file earlier saved policies.

Possibility to export and import policies makes it easier to move the configuration to another server. Also it allows you to back up the configuration before its large-scale change or before updating the system.

### Exporting policies

Before the export, make sure that Traffic Monitor configuration is not being edited and the user has the **Import and export policies** privilege.
All policies with their attributes and elements of technologies used in policies, e.g. protected objects perimeters, persons, etc. are to be exported.

**To export policies:**

1. Go to the **Policies** section.
2. In the upper part of the workspace, click **Export**.
3. The System will prepare policies to be exported, the progress will be displayed in the lower right corner.
   As a result, a ZIP archive containing XML files with a description of configuration elements will be saved to the computer. The archive name includes the date of the export. Example of the archive name: `iwtm-policy-20250821_203503.zip`.
   You can use the archive to import configuration elements.

### Importing policies

Before the import, make sure that Traffic Monitor configuration has been applied and the user has the **Import and export policies** privilege.
Make sure that, on the current server, LDAP synchronization has been carried out and it is the same as on the server where export was performed.

**To import policies:**

1. Go to the **Policies** section.
2. In the upper part of the workspace, click **Import**.
3. In the window that opens, select an earlier exported ZIP archive with a description of policies.
   Importing policies will start, the progress will be displayed in the lower right corner.

4. Refresh the page by clicking **Refresh** in the window that opens. Added policies will be displayed in the Traffic Monitor Management Console.
5. To finish importing, apply the configuration for changes to take effect.

## Features of exporting and importing policies

**General features:**

1. Features of exporting/importing protected objects are the same as described in the *Importing and Exporting Protected Objects* article.
2. All catalogues of protected objects and all included in them protected objects and technology elements are exported and imported whether they are used in policies or not.
3. All persons/computers are exported with no dependence of whether they have attributes and contacts added to them. Other features of exporting/importing persons and computers are the same as described in the *Exporting and Importing Persons* article, except for the feature: "Only entities that have been created or edited in Traffic Monitor can be exported. When exporting contacts and attributes, they are linked to persons". This exporting feature has no relation to the policies.
4. If a group of persons or computers is specified in policy then both the group itself with elements included in it and its subgroups with their elements will be exported. Also, its relationships with parent groups will be exported for maintaining hierarchy. Similarly, relationships with parent groups for single persons and computers will be exported.
5. Relationships between persons and computers are not exported and not imported.

**Features of import:**

1. Policy that contains user's file format will be imported as damaged if, on the server, there is no file format with the same identifier (ID).
2. If an LDAP object (group/person/computer) is imported and its identifier (ID) is absent on the server then policy will be damaged after import.
3. If, on the server, there is no mail notification with the identifier (ID) that is specified in an imported policy then the policy is imported without that notification. This policy will not be damaged.
4. Rules that contain event types or user attributes created with plugins will not be imported as part of policies if, on the server, there are no the same event types and user attributes registered with plugins.
5. During import, the following operations with matching objects will be performed:

| Object | Matching characteristic | Operation with an original object in the System |
|---|---|---|
| **Match on an identifier (ID)** | | |
| Policy | ID | • The policy and rules with their attributes and elements are replaced from the file |
| Perimeter | ID | • Attributes are replaced from the file<br>• Added new elements |
| Traffic Monitor group | ID | • Attributes are replaced from the file<br>• Added new contacts |

| Object | Matching characteristic | Operation with an original object in the System |
|---|---|---|
| Traffic Monitor person | | |
| Traffic Monitor computer | | |
| LDAP group | ID | • Attributes are replaced from the file if they have been modified in Traffic Monitor where export was performed<br>• Added new contacts |
| LDAP person | | |
| LDAP computer | | |
| List of web resources | ID | • Attributes are replaced from the file<br>• Added new object elements |
| Contact | ID | • Attributes are replaced from the file |
| Web resource | ID | • Attributes are replaced from the file |
| Status | ID | • Attributes are replaced from the file |
| Tag | ID | • Attributes are replaced from the file |
| **Match on a value** | | |
| Policy | Name | • The existing object is not modified<br>• The object from the file is added as a new object with the modified unique name |
| Perimeter | Name | • The existing object is not modified<br>• The object from the file is added as a new object with the modified unique name |
| Traffic Monitor group | Name | • The existing object is not modified<br>• The object from the file is added as a new object with the modified unique name |
| Traffic Monitor computer | | |

| Object | Matching characteristic | Operation with an original object in the System |
|---|---|---|
| Traffic Monitor person | Name and last name (displayname) | • The existing object is not modified<br>• The object from the file is added as a new object with the unique value of the displayname parameter |
| LDAP group | Name | The policy will be damaged because, for LDAP objects, only identifiers and modified in Traffic Monitor attributes are exported, not the object itself. |
| LDAP person | Name and last name (displayname) | |
| LDAP computer | Name | |
| List of web resources | Name | • The existing object is not modified<br>• The object from the file is added as a new object with the modified unique name |
| Contact | Type + Value | • Attributes are not modified |
| Web resource | Value | • Attributes are not modified |
| Status | Name | • The existing object is not modified<br>• The object from the file is added as a new object with the modified unique name |
| Tag | Name | • The existing object is not modified<br>• The object from the file is added as a new object with the modified unique name |

## 4.8 Managing Reports

**What for do you need reports?**

Reports are used for monitoring user activities and investigating incidents and allow you to get statistics on required parameters.

Reports are convenient when you need to flexibly configure parameters, while widgets in the *Dashboard* section contain fewer conditions and provide you with timely statistics.

Tools in the "Reports" section also allow you to create printed reports based on results of monitoring or investigations.

**Working with reports includes the following actions:**

- Creating Folder with Reports;

- Creating a report;
- Creating and Configuring Widget;
- Managing ready reports.

The *Examples of Using Reports* article contains examples of using reports for monitoring user activities and investigating incidents.

**See also:**

- Reports Section - on the section where you can manage reports.

## 4.8.1 Creating and Viewing Reports

**Purpose:**
Create a report to view statistics on interception objects.

**Solution:**

1. Go to the **Reports** section (see *Reports Section*).
2. If you want to create a report within a folder, select a folder in the list or create a new folder (see *Creating Folder with Reports*).
3. Create a report within a selected folder or in the root (see *Creating Report*).
4. Add widgets to the report (see *Creating and Configuring Widget*).
5. To run the report execution, select the report in the list and click  on the toolbar or the **Run report** button in the report viewing form (or you can use **Save and run** button in the report creation form).
6. To view results of an earlier executed report, select the report in the list in the left part of the workspace. Besides, you can view results of the report execution for different dates and save selected report versions to your computer (for details, see *Viewing Ready Reports*).

If necessary, you can copy or move an earlier created folder or report.

**To copy a folder** and its reports:

1. Select the folder in the list.
2. On the toolbar in the left part of the workspace, click  **Copy**.

If you are trying to copy a subfolder and you have full access to the parent folder, then the copy will be added to the same folder as the copied folder. If you don't have full access to the parent folder or you are copying a top-level folder, then the copy will be added to the root of the folder tree.

**To copy a report:**

1. Select the report in the list.
2. On the toolbar in the left part of the workspace, click  **Copy**.

If you are copying a report inside a folder and you have full access to the folder, then the copy will be added to the same folder as the copied report. If you don't have full access to the folder or you are copying a top-level report, then the copy will be added to the root of the folder tree.

**To move a folder**, select it in the list and holding the left mouse button move it to the desired location, then release the mouse button.

**Note:**

To move a folder, you need to have full access both to the folder you are moving and to the destination folder. If the folder includes reports, then you also need full access to the reports. For details, see the table below.

**To move a report**, select it in the list and holding the left mouse button move it to the desired location, then release the mouse button.

**Note:**

To move a report, you need to have full access both to the report and to the destination folder. For details, see the table below.

The table below shows what access rights are needed to manage reports:

| **Action** | **Access rights** | | | |
|---|---|---|---|---|
| | View and execute folder | Full access to folder | View and execute report | Full access to report |
| View the folder | + | | | |
| Edit the folder attributes (name, description, access rights) | + | + | | |
| Copy the folder | + | | | |
| Create a new item (a report or a subfolder) in the folder | + | + | | |
| Move an empty folder to a different folder | + | + | | |
| Move a folder which includes at least one report | + | + | + | + |
| Delete an empty folder | + | + | | |
| Delete a folder which includes at least one report | + | + | + | + |
| View and run the report | + | | + | |
| Edit the report parameters (including access rights) | + | | + | + |
| Copy the report | + | | + | |

| | | | | |
|---|---|---|---|---|
| Move the report to a different folder | + | | + | + |
| Delete the report | + | | + | + |

**See also:**

- Creating Folder with Reports;
- Creating Report;
- Examples of Using Reports.

## Creating Folder with Reports

**Purpose:**
Create a folder for grouping reports with a common theme.

**Solution:**

1. Go to the **Reports** section.
2. In the list of folders and reports in the left part of the workspace, choose where to create a folder. You can create a folder in the root or inside an existing folder.

> **Note:**
>
> If you do not have sufficient rights to create items within a selected folder, a warning will be displayed. In this case, you should find a different location for your folder.

3. Click  and, in the drop-down list, select **Create folder**.
4. In the form that opens, enter the folder name.
5. Specify if access rights to the folder should be inherited for subfolders and reports. By default, the **Apply rights for related reports** option is deselected.

> **Note:**
>
> If you create a folder inside a folder with the **Apply rights for related reports** option enabled, then actions described in steps 5-6 are unavailable.

6. Specify who can access the folder and define access rights. For this:
   a. Find required users in the list.

> **Tip.**
>
> To find required users, use the **Search** field.

   b. Next to the user name, set the checkbox in one of the fields:
      - **View and execute access** - to provide access for viewing and copying the folder. Access rights to reports in the folder are specified when you create a query;
      - **Full access** - to provide full access to the folder.

> **Note:**
>
> To provide access to the folder to all users of the System, set a checkbox in the field with the required access level next to the **All users** value.

7. Click **Save folder**.

To edit the folder, click the  button on the toolbar.

To delete the folder, click .

> **Note:**
>
> To edit or delete a folder, full access to the folder is required. If you can only view and execute the folder, then instead of  button,  button is displayed, and  button is unavailable.

## Creating Report

**Purpose:**
Create a report that contains statistical data on interception objects.

**Solution:**

1. Go to the **Reports** section.
2. In the list of folders and reports in the left part of the workspace, choose where to create a report. You can create a report in the root or inside an existing folder.

> **Note:**
>
> If you do not have sufficient rights to create items within a selected folder, a warning will be displayed. In this case, you should choose a different location for the report.

3. Click  and, in the drop-down list, choose **Create report**.
4. In the form that appears, specify required parameters (for more information, see *Report Creation Window*).
5. On the **Widgets** tab, click **Add widget**.
6. In the **Widget Creation** window that opens, specify the widget parameters (for details, see *Managing widgets of reports*) and click **Save**.
7. If necessary, add more widgets as described at step 6. When you are done, close the **Adding widget** window by clicking  in the right upper corner.
8. Open the **Access** tab to specify who can access the report and define the access rights.

> **Important!**

If you create a report in a folder with the **Apply rights for related reports** option enabled, then access rights for the report will be the same as for the folder. In this case, editing access right to the report is unavailable.

For this:

a. Find required users in the list.

> **Tip.**
>
> To find required users, use the **Search** field.

b. Next to the user name, set the checkbox in one of the fields:
   - **View and execute access** - to provide the user access to viewing, copying, and executing the report;
   - **Full access** - to provide the full access to the report.

> **Note:**
>
> To provide access to the report to all users of the System, set a checkbox in the field with the required access level next to the **All users** value.

9. Click:
   - **Save** - to save the report.
   - **Save and execute** - to save and execute the report.

To edit the report, click  on the toolbar.

To delete the report, click .

> **Note:**
>
> To edit, move, or delete a report, full access to the report is required. If you can only view and execute the report, then instead of  button,  button is displayed, and  button is unavailable.

## Creating and Configuring Widget

**Purpose:**
Create a widget for displaying statistics.

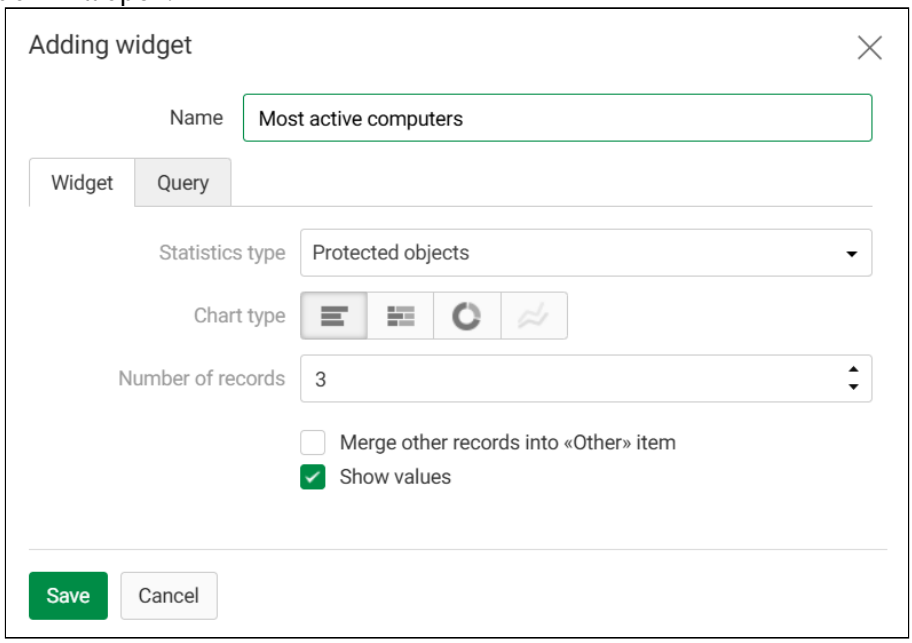
**Solution:**

1. Go to the **Reports** section.
2. In the left part of the workspace, select a report to which you want to add a widget or create a new report (see *Creating Report*).

**Note:**

To add a widget to an earlier created report, switch to the report edit mode.

3. In the form that appears, open the **Widgets** tab and click **Add widget**. The **Creating Widget** window will open.




4. Fill in the required fields:
   a. In the **Name** field, enter the name of the widget.
   b. On the **Widget** tab, choose the type of statistics. Other settings (a chart type, the number of records, the grouping period, etc.) are available depending on the chosen type of statistics (for more details on the types of statistics, see *Widgets of Reports*).
   c. On the **Query** tab, specify the parameters based on which events will be filtered (for more information about available settings, see *Queries*).
5. Click **Save Widget**.

You can duplicate an earlier created widget to a different report. For this:

1. Switch to the edit mode of a report with the required widget.
2. In the upper-right corner of the desired widget, click  and in the drop-down list select **Duplicate**.
3. In the report list in the left part of the workspace, select the report to which you want to duplicate the widget.

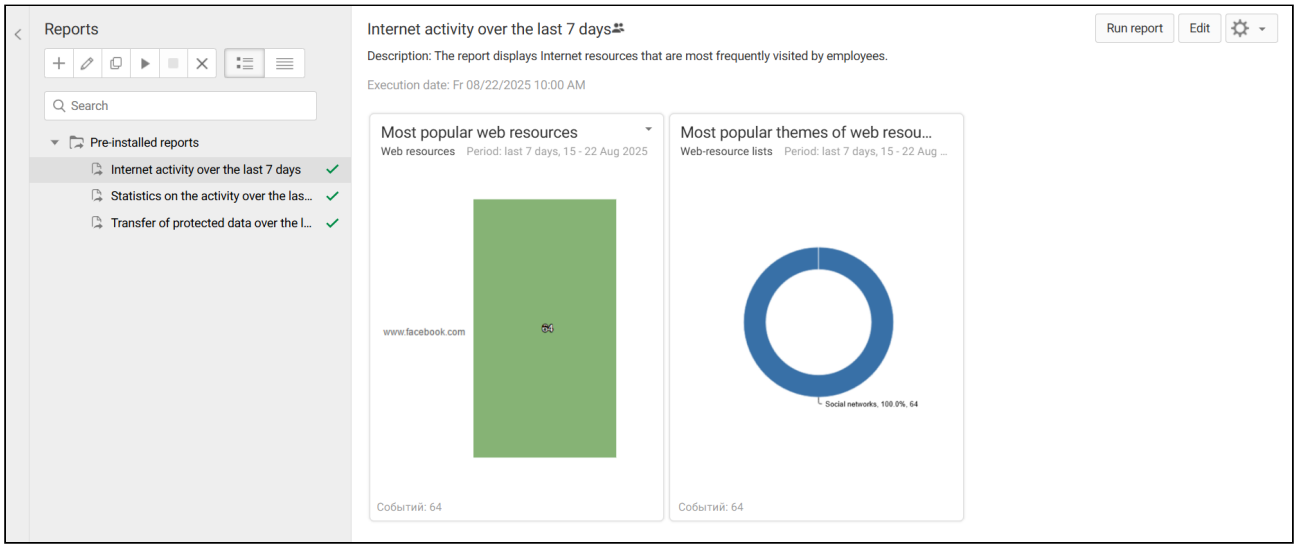
**Additional information:**

To edit or delete a widget, switch to the report edit mode and select the desired widget. Then:

- To edit the widget, in the upper-right corner of the widget, click  and, in the drop-down list, choose **Edit**.
- To delete the widget, in the upper-right corner of the widget, click  and, in the drop-down list, choose **Delete**.

## Viewing Ready Reports

**To view the last executed version of the report**, choose the required report in the list. Widgets for the selected report will be displayed in the right part of the workspace. Date and time of the report execution are displayed above the widgets.




If you want to view events information about which is displayed in the widget, in the right upper corner, click  and from the drop-down list, select **Go to events**. You will switch to the list of events in the *Events*.

You can save the report as a file in one of the following formats:

- Excel 2003;
- Excel 2007;
- HTML;
- PDF.

**To export the report**, in the right upper corner, click  and, in the drop-down list under the **Report export** caption, choose the desired format. A report in the selected format will be saved to you computer.

**To view report versions for other dates**, open the report execution history. For this, in the right upper corner, click  and, in the drop-down list, choose **Report execution history**. In the window that opens, you can view information about the report execution.




For each report version, you can view the execution date and time and a comment field. To add a comment to a report version, double-click the field next to the selected version.

If the report execution was cancelled,  icon is displayed next to the report version.

You can view required report versions, delete versions that are no longer needed, or save selected versions to a file.

**To view a report version**, click the row with the date and time of the report execution. Widgets for the selected report version will be displayed.

**To delete selected report versions:**

1. Select check boxes for the versions which you want to delete. To select all rows, select the check box in the header field.
2. Click **Delete**.

**To export selected report versions:**

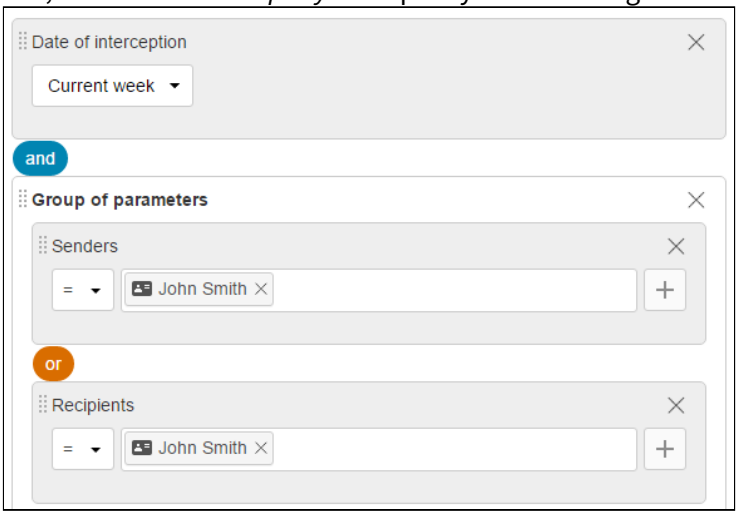
1. Select check boxes for the versions which you want to save as a file. To select all rows, select the check box in the header field.
2. Click **Export** and, in the drop-down list, choose the required format.: Excel 2007, Excel 2003, HTML, or PDF. A file in the specified format will be saved to your computer.

## 4.8.2 Examples of Using Reports

***Example 1:***
The employee John Smith is in the list of the most active violators of the week (statistics on the most active violators in displayed in the *Top Violators* widget). An investigation is required to get detailed information on activities of this employee. The investigation can be carried out in several steps.

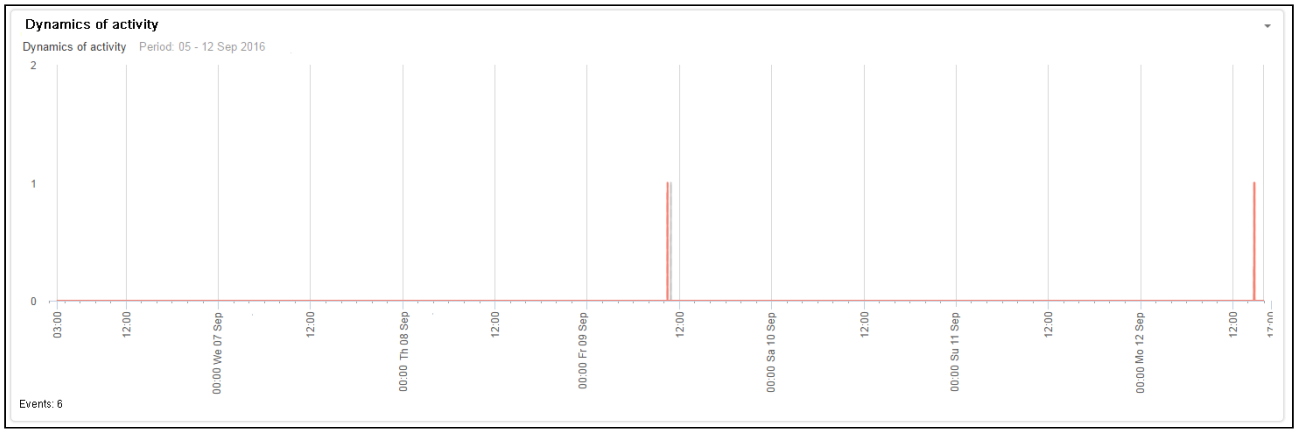
**Step 1**. Get information about the dynamics of violations. For this:

1. Create a report and add *Dynamics of activity* widget to it.
2. Open the **Query** tab of the widget.
3. In the **Query type** field, select *Advanced query* and specify the following conditions:



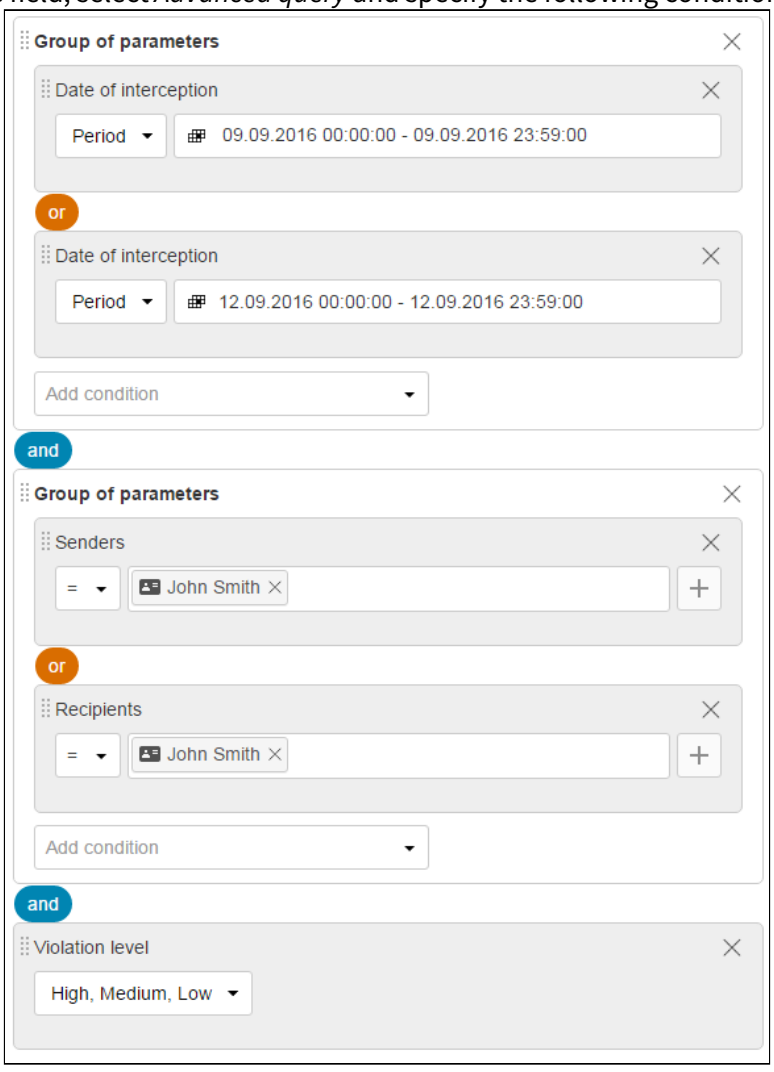

4. Save and run the report.

On the chart, you can see that the employee committed most violations on 09.09 and 12.09.



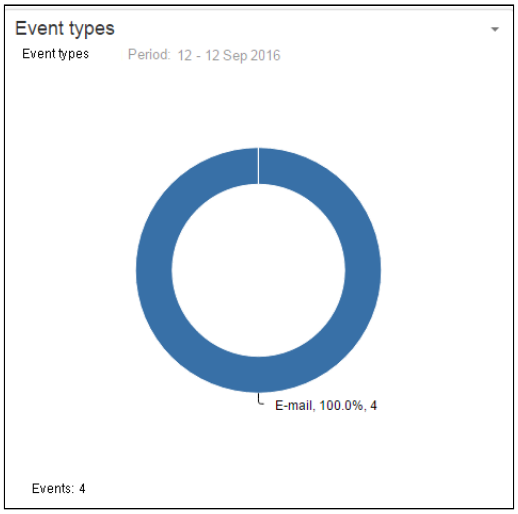

**Step 2**. Determine the channels through which the data was leaked. For this:

1. Add *Event types* widget to the created report.
2. Open the **Query** tab of the widget.
3. In the **Query type** field, select *Advanced query* and specify the following conditions:



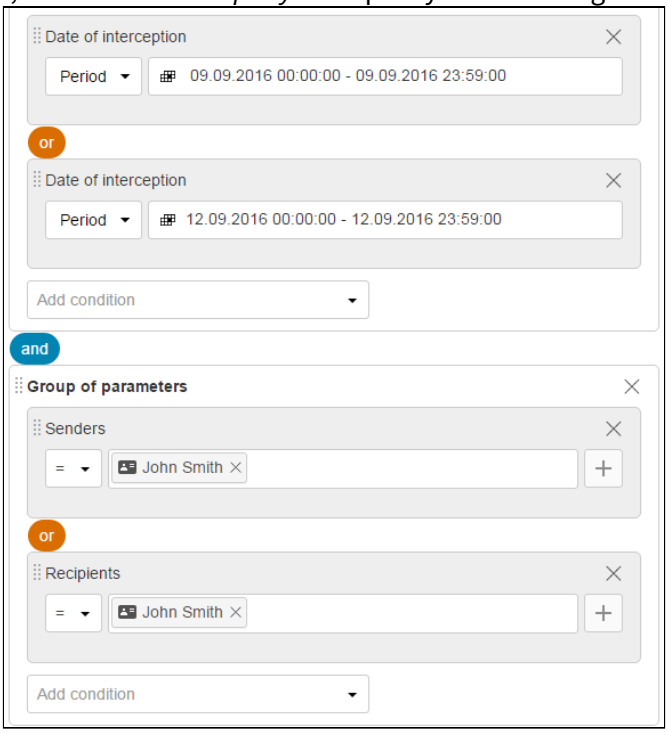

4. Save and run the report.

In the report, you can see, that most violations are related to sending data via email.




**Step 3**. Determine what protected objects were leaked. For this:

1. Add *Protected objects* widget to the created report.
2. Open the **Query** tab of the widget.
3. In the **Query type** field, select *Advanced query* and specify the following conditions:



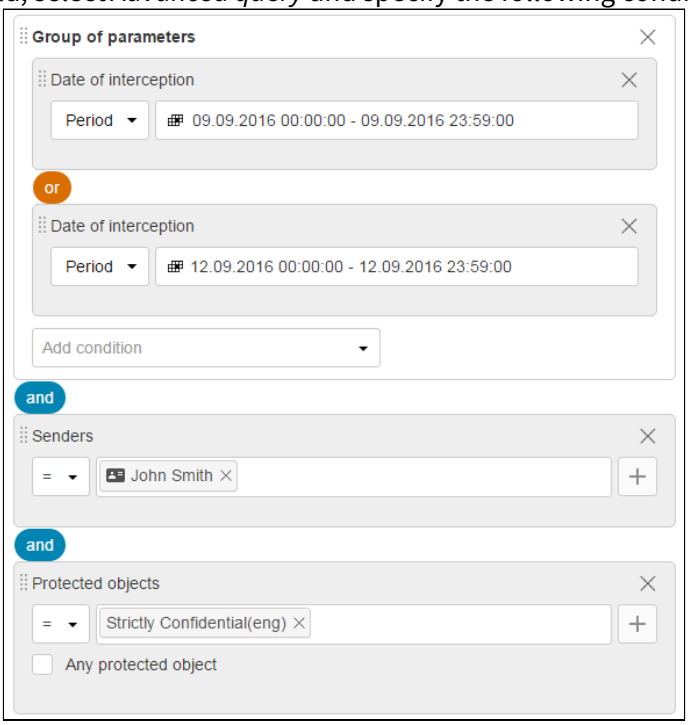

4. Save and run the report.

In the report, you can see, that the employee emailed documents included in the *Strictly confidential information* protected object.



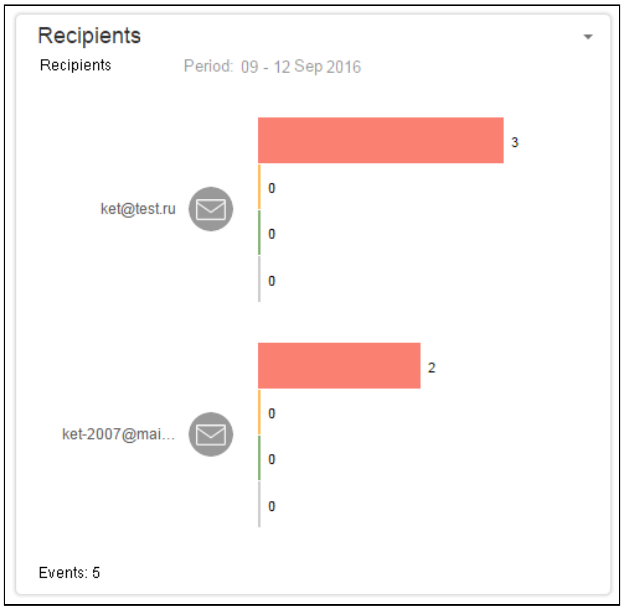

**Step 4**. Determine, to whom John Smith sent confidential data. For this:

1. Add *Recipients* widget to the created report.
2. Open the **Query** tab of the widget.
3. In the **Query type** field, select *Advanced query* and specify the following conditions:




4. Save and run the report.

In the report, you can see the emails to which confidential data was sent.

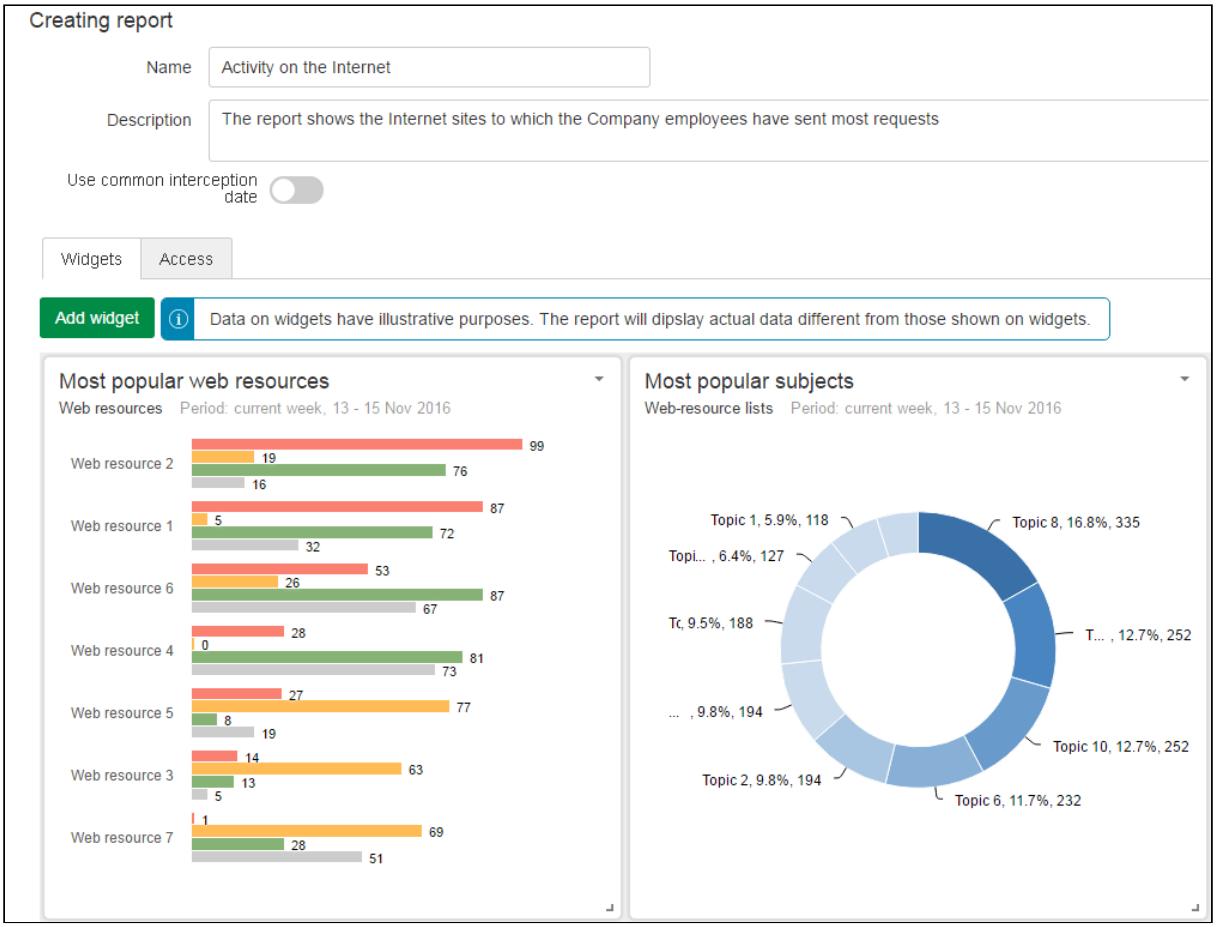



As a result of the investigation, you have determined when, through which channels, and to what recipients the violator leaked confidential data. Now you can easily find the needed events: for this, create a query and specify already known parameters in it (see *Creating Queries*). In the found events, you can see what exactly the violator leaked.

***Example 2:***

It is required to track the dynamics of attending web resources and the most popular subjects. For this:

1. Create *Activity on the Internet* report.
2. Add a widget and specify *Web resources* statistics type for it.
3. Add one more widget and specify *Web resource lists* statistics type for it.




4. On the **Query** tab, select the required period for each widget and specify additional parameters if necessary.
5. Save and run the report.

## 4.9 Managing the System

The section is configured by the System Administrator, except for the **Audit** and **Mail notifications** subsections operated by the Security Officer.

Managing the System includes the following actions:

- Managing Integration with LDAP Catalogs;
- Managing Licenses;
- Managing System Users and their Roles;
- Healthcheck;
- Collecting Diagnostic Data;
- Plugins;
- User Actions Audit;
- Integrity Monitoring;
- Configuring Connection to Mail Server;
- Configuring Notifications;
- Managing Tablespaces.

## 4.9.1 Managing Integration with LDAP Catalogues

Configuring the synchronization with LDAP catalogues is performed in **Administration -> LDAP Synchronization** section.

> **Warning!**
>
> If you have Adblock Plus installed for the browser then you should disable this extension to provide correct operation of this web console section.

The toolbar is located in the left part of the **LDAP server** workspace.
Above the toolbar, you can find the list of servers for which synchronization with LDAP catalogues has been configured.
The toolbar contains a set of tools for working with the connection.
In the central part of the workspace, parameters for the selected connection, status and synchronization schedule are displayed:

Configuring integration with LDAP catalogues is described below:

- Creating Connection to Server;
- Editing Connection to Server;
- Deleting Connection to Server;
- Running Synchronization with Server Manually.

### Creating Connection to Server

**To create a connection to the server:**

1. Go to **Administration** > **LDAP Synchronization**.
2. On the toolbar, click  **Create**.
3. Specify parameters for a new connection:

| Parameter | Description |
|---|---|
| **General parameters** | |
| Server name | Connection identifier used in the Management console<br>**Important!** It is not allowed to change the server name between the last synchronization and System update |
| Server type | Indicates what kind of server is used: *Active Directory, Samba DC, Domino Directory, Astra Linux Directory* (further also *ALD*) or *Astra Linux Directory Pro/Free IPA* |
| Synchronization | • *Manual* – user starts synchronization manually<br>• *Automatic* – synchronization is performed according to schedule |

| Parameter | Description |
|---|---|
| | **Important!** We recommend that the frequency of automatic synchronization with the Domino Directory server should be 10 minutes or more.<br>We recommend not running manual synchronization more often than once every 10 minutes |
| Synchronization period | Type of synchronization repeating<br>• *Every N minutes*<br>• *Every N hours*<br>• *Every N days*<br>• *Every N weeks* |
| Retry parameters | Value of synchronization repeating period if *Automatic synchronization* is selected<br>***For example***, with the following values:<br>• *Synchronization period – Every N minutes*<br>• *Retry parameters – 60 minutes*<br>the synchronization will be performed every 60 minutes |
| **Configuring connection** | |
| LDAP server | The IP address of the server whose LDAP catalogues are synchronized |
| Connection type | Selecting connection type with Active Directory, Samba DC, Domino Directory, ALD or ALD Pro/Free IPA that will be configured:<br>• Unsecured connection (LDAP)<br>• Secured connection using LDAP + StartTLS protocol<br>• Secured connection LDAPS (SSL)<br>**Important!** Connection without using a certificate is not secure. When installing a secure connection, you can additionally load a file containing the certificate in PFX format.<br>**Important!** If the file that is being loaded contains several user certificates, the System will operate with the first of them and its private key. Correct work requires creating a file with one user certificate.<br>**Note:** For Samba DC, using unsecured connection is not supported.<br>**Important!** Synchronization using the secure connection is supported only for Active Directory and Samba DC. For Samba DC, you can choose only secured connection using LDAP + StartTLS protocol |
| Server certificate | Loading a certificate file in PEM format. |

| Parameter | Description |
| --- | --- |
| | **Note:** For Samba DC, this option is unavailable |
| User certificate | Loading a certificate file in PEM format. When using a user certificate, it is necessary that you additionally load a file containing a private key of the user certificate.<br>**Note:** For Samba DC, this option is unavailable |
| Private key of user certificate | Loading a file containing a key in PEM format.<br>**Note:** For details, see *Getting Client Certificate and Server Certificate*.<br>**Note:** For Samba DC, this option is unavailable |
| Use Kerberos protocol | Indicates if Kerberos protocol is used for authentication (protocol of client and server mutual identification). For details, see *Specifics of LDAPS connection and synchronization using Kerberos protocol*.<br>**Important!** If Kerberos is used with LDAP connection, we recommend editing the configuration file.<br>**Important!** You should enable this only when **Use client certificate to authenticate** is disabled. These two principles are mutually exclusive and if you enable both of them, connection will not work |
| Global LDAP port | A port for connecting the global LDAP catalogue.<br>**Note:** This setting is available for Active Directory and Samba DC only |
| LDAP port | Port for connecting a domain catalogue |
| Use global catalogue | Indicates if the global LDAP catalogue is used for synchronization<br>**Note:** This parameter is only available for Active Directory and Samba DC |
| LDAP request | **Note:** the setting is required only Active Directory and Samba DC only.<br>Filtering attributes which are the full path to the specified catalogue. You can specify only one catalogue in the Active Directory, Samba DC, Domino Directory, Astra Linux Directory or Astra Linux Directory Pro/FreeIPA organizational structure.<br>To improve the AD search, you can use separate hierarchy levels of the base:<br>`C - countryName`<br>`O - organizationName`<br>`OU - organizationalUnitName` |

| Parameter | Description |
| --- | --- |
| | `DC - domainComponent`<br>`CN - commonName`<br>**Example for AD, Samba DC, ALD, ALD Pro/FreeIPA**:<br>To use the `Users` branch located in the company domain as the search base, enter:<br>`cn=users,dc=company,dc=com`<br>**Example for DD:**<br>A request may contain one or several values:<br>`o=company,ou=department,ou=group`<br>**Important!** To enable a partial synchronization using an LDAP request, you should firth sync with the entire LDAP catalogue ( `dc=company,dc=ru` ) and then run synchronization using a narrower LDAP request. To update information about groups/ persons/computers for this synchronization, you should run complete synchronization with the entire LDAP catalogue and then a partial synchronization using an LDAP request |
| Use user certificate for authentication | Whether is it allowed to use a client certificate for secure connection types instead of entering a password.<br>**Important!** You should use this option only if the **Use Kerberos protocol** option is disabled. These options are mutually exclusive and if you select both options, the connection will not work |
| Anonymous access | Indicates if the connection to the LDAP server is performed on behalf of an anonymous user.<br>**Note:** For Astra Linux Directory Pro and FreeIPA, the option is unavailable |
| Login | Login to access the synchronization server<br>**Important!** To connect to Astra Linux Directory Pro and FreeIPA, specify the login in `uid=login,cn=users,cn=accounts,dc=company,dc=com` format |
| Password | Password to access the synchronization server |

4. Click **Check connection**, to perform control check of connection to the server.

5. Click **Save**.

**Note:**

Starting from Traffic Monitor version 7.5, you do not need to fill in the `DnsRootDefault` and `NetbiosNameDefault` fields in the **adlibitum.conf** configuration file. AUTH contacts for persons will be automatically added during synchronization with ALD, ALD Pro or FreeIPA. Values of these parameters specified in earlier Traffic Monitor version will be ignored.

**Important!**

When synchronizing with ALD, we recommend enabling the **Use Kerberos protocol** option in LDAP server settings. If this option is disabled, synchronization with ALD will work only with the **Anonymous access** parameter enabled. In this case, authentication for users imported from ALD will not work.

#### Encrypted connection support

You can send data over a secure connection for synchronization with LDAP servers only if you choose the following connection types:

- LDAP with StartTLS function, which allows you to establish a secure connection over an existing unsecured one on ports 389 or 3268 if the global catalogue is used. You can synchronize with AD or Samba DC both using Kerberos protocol and anonymous access.
- LDAPS, where data is sent over a secured channel: on ports 636 or 3269 if the global catalogue is used.

Example of settings in Kerberos configuration file

To use Kerberos protocol with LDAP connection, specify all domain controllers in the `/etc/krb5.conf` file. The steps below illustrate settings for `example-company.com` domain.

1. To `[realms]` section, add the code:

```
EXAMPLE-COMPANY.COM = {
    kdc = dc1.example-company.com
    kdc = dc2.example-company.com
    admin_server = dc1.example-company.com
    default_domain = example-company.com }
```

2. Edit the `[domain_realm]` section so that it looks as follows:

```
[domain_realm]
.unix.example-company.com  = UNIX.EXAMPLE-COMPANY.COM
unix.example-company.com  = UNIX.EXAMPLE-COMPANY.COM
msk2-test-iwtm01.unix.example-company.com = UNIX.EXAMPLE-COMPANY.COM
.example-company.com = EXAMPLE-COMPANY.COM
example-company.com = EXAMPLE-COMPANY.COM
```

3. For `default_ccache_name` parameter, specify the value: `FILE:/tmp/krb5cc_%{uid}`.
4. Destroy the old ticket and get a new one. Use the commands:

```
kdestroy
```

```
kinit infowatch@EXAMPLE-COMPANY.COM
klist
```

## Editing Connection to Server

**To edit connection to server:**

1. Go to **Administration -> LDAP Synchronization**.
2. By left-click select required server.
3. On the toolbar click  **Edit**.
4. Change connection parameters (see *Creating Connection to Server*).
5. Click **Check connection**, to perform control check of connection to server.
6. Click **Save**.

## Deleting Connection to Server

**To delete existing Server connection:**

1. Go to **Administration -> LDAP Synchronization**.
2. By left-click select required server.
3. On the toolbar click  **Delete**.

> **Note:**
>
> To delete several connections at a time, highlight them (for example, holding **<SHIFT>** or **<CTRL>** ) and click **Delete** .

4. In the opened window click **Yes**.

## Running Synchronization with Server Manually

**To run synchronization with Server manually:**

1. Go to **Administration -> LDAP synchronization**.
2. Left-click at the target server on the left.
3. Click  **Starting synchronization** button located on the toolbar.

Information on the synchronization results will be displayed in *Last synchronization, Status of the synchronization, Next synchronization status* strings.

> **Note:**
>
> If the ***Synchronize*** connection attribute has *Every N minutes*, *Every N hours, Every N days* or *Every N week* values, then the automatic synchronization will be performed with specified frequency after last manual running.

**Warning!**

Synchronization will be performed according to Traffic Monitor server time. If management console is located in different time zone, then specifying synchronization time is required to be done considering difference between time zones of server and management console.

It is required to check connection with LDAP servers after updating from previous versions. To do this, take the following steps:

1. Left-click at the target server.
2. Click on **Check connection.**

Information on the synchronization results will be displayed in a message. If error occurs, set connection parameters.

## 4.9.2 Managing System Users and their Roles

To manage System users, the following entities are used:

- *User* – user's account (see *Users*);
- *Role* – a set of rights which can be assigned to the user (see *Assigning Role to a User*);
- *Visibility scope* – groups of persons and interception objects that are available to specified users only (see *Visibility Scopes*).

### Users

Configuring the System users list is performed in the **Administration -> Users and Roles** section, the **Users** tab.

In the work area the list of System users, toolbar and a drop-down menu (defining a number of users displayed at the page) are located.

Account attributes are listed in the following table:

| Parameter | **Description** |
|---|---|
| *Login* | Name of user account |
| *Full name* | User's first name and second name |
| *Email* | User's e-mail address |
| Roles | List of roles assigned to the user |
| *Scopes* | List of visibility scopes available for the user |
| *Description* | Note to the account |
| Status | Indicates whether user role is active or passive |

You can perform the following actions while managing users:

- Creating User Account;

- Editing User Account;
- Deleting User Account;
- Changing User Account Password;
- Changing User Account State;
- Importing User Account from Active Directory;
- Assigning Role to a User;
- Assigning Visibility Scope to a User.

Creating User Account

**To create user account:**

1. Go to the **Administration** -> **Users and roles** section.
2. Go to the **Users** tab.
3. On the toolbar click  **Create User**.
4. In the opened window specify account parameters.

| Parameter | Description |
|---|---|
| *Login* | User account name |
| *Status* | Indicates if the user account is active or passive |
| *Interface language* | Language, which will be assigned to the interface of selected user account |
| *Password* | User account password |
| *Confirm password* | User account password |
| *Email* | User email address |
| *Full name* | Full name of the user |
| *Description* | User account notes |

5. Click **Save**.

Editing User Account

**To change existing user account parameters:**

1. Go to the **Administration** -> **Users and roles** section.
2. Go to the **Users** tab.
3. In the users list left-click at the target account.
4. Click  **Edit user** on a toolbar.
5. In the opened window change account attributes (see *Users*).
6. Click **Save**.

Deleting User Account

**To delete user account:**

1. Go to the **Administration -> Users and roles** section.
2. Go to the **Users** tab.
3. In the users list left-click at the target account.
4. On the toolbar click  **Delete user**.

> **Note:**
>
> To delete several accounts in one action, select them from the list (for example, by pressing **<SHIFT>** or **<CTRL>** ) and click **Delete user** .

5. In the opened window click **Yes**.

Changing User Account Password

**To change user account password:**

1. Go to the **Administration** -> **Users and roles** section.
2. Go to the **Users** tab.
3. In the users list left-click at the target account.
4. On the toolbar click  **Change password**.
5. In the opened window enter a new password to **Password** and **Confirm password** fields. The password should contain:
   - uppercase letters of Latin alphabet (A-Z);
   - lowercase letters of Latin alphabet (a-z);
   - numbers (0-9);
   - symbols: !, $, #, %.
6. Click **Save**.

Changing User Account State

**To change account state:**

1. Go to the **Administration -> Users and roles** section.
2. Go to the **Users** tab.
3. In the users list left-click at the target account.
4. On the toolbar click  and choose **Activate user** or **Deactivate user**.

> **Note:**
>
> You can change a status of any account except of **Administrator**.

Importing User Account from Active Directory

You can easily create users by importing their accounts from the Directory Service.

**Important!**

If AdBlock extension is used in your browser, then disable this extension before importing user accounts, as AdBlock blocks the import.

**To import user account:**

1. Go to the **Administration -> Users and roles** section.
2. Go to the **Users** tab.
3. On the toolbar, click  **Import users from LDAP**.
4. In the opened window, specify LDAP server which stores the required account.

   **Note:**

   You can enter a part of login name to the **Search** field and click **Search**.

5. Flag required user accounts.
6. Click **Save**.

Assigning Role to a User

**To assign role to a user:**

1. Go to the **Administration -> Users and roles** section.
2. Go to the **Users** tab.
3. In the users list left-click at the target account.
4. Click  on the toolbar.
5. Choose **Set role** in the list (see *Roles*).
6. Click **Save**.

Assigning Visibility Scope to a User

**To assign a visibility scope to a user:**

1. Go to the **Administration** -> **Users and roles** section.
2. Open the **Users** tab.
3. Click the required account.
4. From the **Scopes** list (see *Visibility Scopes*), set a visibility scope for the user. The user will be able to view the events and screenshots that match their visibility scope. Herewith:
   a. If you do not specify any visibility scope for the user, then all interception events and screenshots will be unavailable for this user, and all groups will be available.
   b. If several visibility scopes set for the user, then their criteria will be joined by the logical OR.
   c. To grant the user access to all the events with any criteria, set a visibility scope **Full access**.
5. Click **Save**.

## Roles

To control redundant access to system settings, policies of different structural departments, interception objects and other important information, there is role system of access rights differentiation in InfoWatch Traffic Monitor.

Role is a set of rights which can be assigned to user. Assigning a role to user is described in *Assigning Role to a User*.

Initially, there are two predefined roles and the two preset user – roles **Adminitrator** and **Security officer**, which are accordingly assigned to Administrator and Officer users.

**Administrator** role provides an opportunity to carry out the initial configuration of the system (Managing users, roles, visibility scopes, licenses and LDAP synchronization).

**Security officer** role has all rights except for initial setup.

Configuring the roles list is performed in **Administration -> Users and Roles** section, **Roles** tab.

In the work area the list of System users, toolbar and a drop-down menu (defining a number of roles displayed on the page) are located.

Role attributes are listed in the following table:

| Attribute | Description |
|---|---|
| *Name* | Role name |
| *Users* | First name and second name of the user |
| *Description* | Comment to a role |

You can perform the following actions while managing roles:

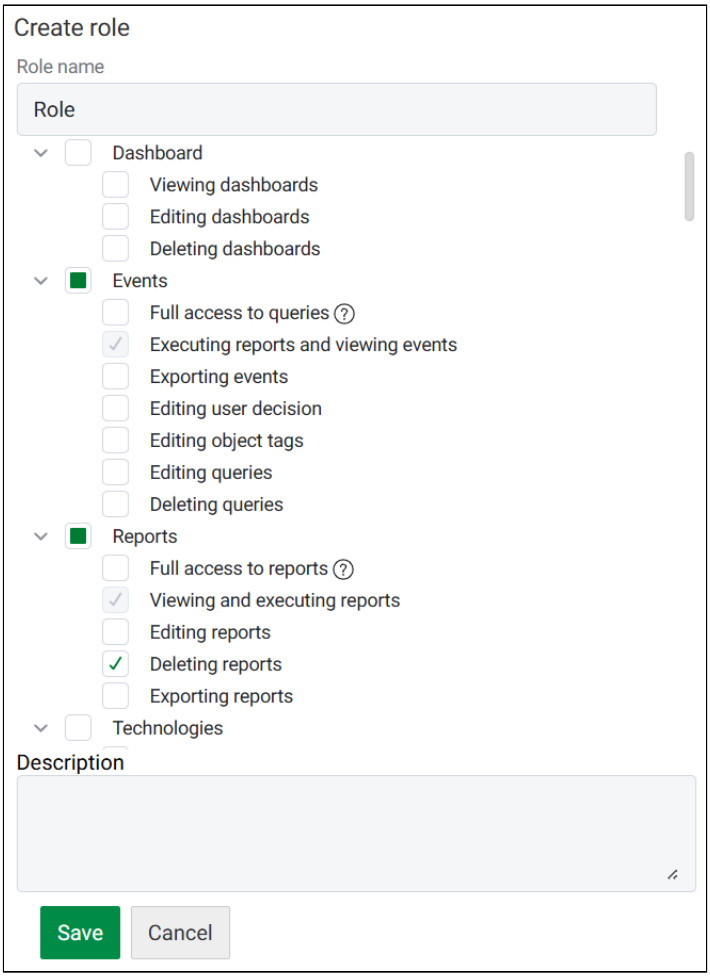
- Creating a Role;
- Editing a Role;
- Deleting a Role.

Creating a Role

**To create a new role, follow the steps below:**

1. Go to **Administration** -> **Users and roles** section.
2. Go to **Roles** tab.
3. On the toolbar, click  **Create role**.
4. In the opened window specify role attributes. Flag the privileges you want to assign to the role.

> **Note:**
>
> To expand/collapse privileges list, click  or  respectively.




> **Note:**
>
> **Viewing roles** and **Viewing visibility scopes** privileges are available by default when selecting **Roles** and **Visibility scopes**.

5. Click **Save**.

Editing a Role

**To change parameters of an existing role, follow the steps below:**

1. Go to **Administration -> Users and roles** section.
2. Go to **Roles** tab.
3. In the users list left-click at the target role.
4. On the toolbar, click  **Edit role**.
5. In the opened window change role attributes. Flag (unflag) the privileges you want to assign (unassign) to the role.

> **Note:**

To expand / collapse privileges list, click ▶ or ◢ accordingly.

> **Note:**
>
> **Viewing roles** and **Viewing visibility scopes** privileges are available by default when selecting **Roles** and **Visibility scopes**.

6. Click **Save**.

Deleting a Role

**To delete role:**

1. Go to **Administration -> Users and roles** section.
2. Go to **Roles** tab.
3. In the users list left-click at the target role.
4. Click ☒ **Delete role**.

> **Note:**
>
> To delete several roles at a time, select them in the list (for example, by holding **<SHIFT>** or **<CTRL>** ) and click **Delete role**.

5. In the opened window click **Yes**.

> **Note:**
>
> You can change any role except for **Administrator** and **Security officer**.

## Visibility Scopes

A visibility scope allows you to control access to groups of persons and intercepted objects.

In the visibility scope, you can specify groups of persons visible to the user:

- in the **Persons** section, the user:
  - can see persons specified in the visibility scope
  - can select the **Create policy** action only for visible persons
  - is not allowed to export and import groups of persons, if the user has restricted access to groups of persons in the visibility scope, regardless of their role and privileges
- in the **Events** section, when choosing senders and recipients in the query, the user can see:
  - only visible Groups of persons
  - all individual Persons

> **Note:**

When viewing information about a person not specified in the visibility scope, only a contact from the event will be shown. Viewing screenshots will not be available.

- in the **Policies** section, the user can add only visible Groups of persons and individual Persons to the data protection policy
- in the **Lists** -> **Perimeters** section, the user can see:
  - only visible Groups of persons
  - all individual Persons
- in the **Mail notifications** section, the user can choose only visible persons as recipients

**Important:**

In the **Audit** section, the events are displayed regardless of visibility scope. We recommend restricting access to the **Audit** section using roles and privileges.

**Important:**

In other Infowatch products, **all** persons and computers are visible to the user.

In the visibility scope, you can specify attributes of intercepted objects. The user will only see those events, whose attributes match the attributes configured in the visibility scope.

Several visibility scopes can be specified for one user.

**Example 1:**

The *officer* user has a visibility scope with a Group of persons *Department 11*. In the **Persons** section, the *officer* user can only view persons from the Department 11 and all its subdivisions.

**Example 2:**

The *officer* user has a visibility scope with a person *Smith* and a tag "1". In this case, the *officer* user can only view events with the participation of Smith and tagged "1".

Assigning visibility scopes to a user is described in *Assigning Visibility Scope to a User*.

To configure a list of visibility scopes, go to **Administration** -> **Users and Roles** section, **Scopes** tab.

In the working area, you can find a list of scopes, a toolbar, and a drop-down menu.

In the list of scopes, user scopes are displayed.

The toolbar contains a set of tools to work with visibility scopes:

-  - to create a new visibility scope. Double-click a visibility scope to edit it.
-  - to delete an earlier created visibility scope. Preset visibility scopes cannot be deleted.

The  drop-down menu defines the number of scopes to be displayed on the page.

Visibility scope attributes include the scope name and its short description.

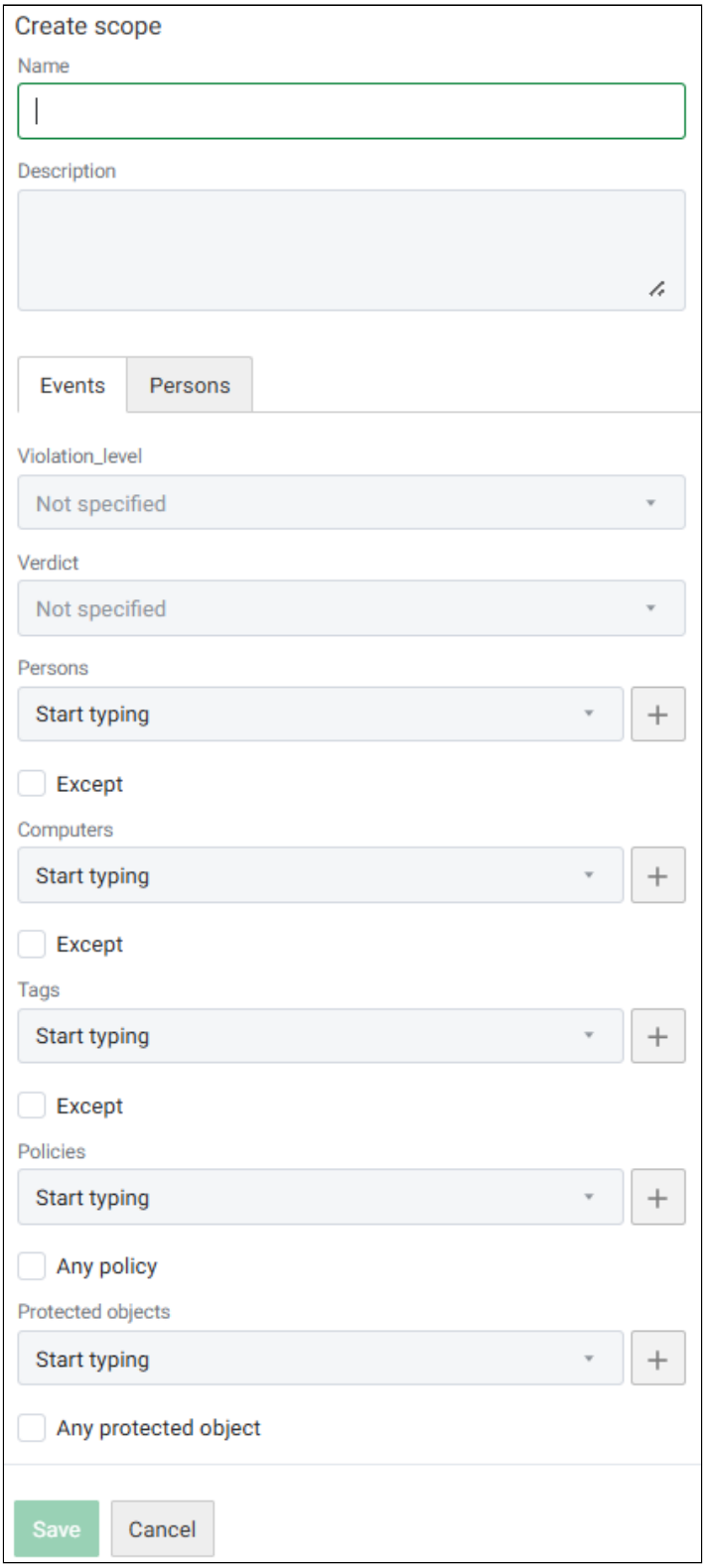
You can perform the following actions while managing visibility scopes:

- Creating Visibility scope;
- Editing Visibility Scope;
- Deleting Visibility Scope.

Creating Visibility scope

To create a visibility scope:

1. Go to the **Administration** -> **Users and Roles** section.
2. Open the **Scopes** tab.
3. On the toolbar, click .




4. In the **Create scope** window, enter the name of the visibility scope into the *Name* field.
5. If necessary, enter a short description into the *Description* field.
6. On the *Events* tab, specify the required parameters:
    a. *Violation level* - choose the level from a drop-down menu.

b. *Verdict* - choose from a drop-down menu.
c. *Persons* - choose either of the following:
   - enter the first characters of the username, group, or status and choose the required value from a drop-down list;
   - click  and in the window that opens, select required checkboxes on the **Persons**, **Groups**, and **Statuses** tabs. Click **Save**.

d. *Computers* – as described in item c.
e. *Tags* – choose either of the following:
   - enter the first characters of the tag name and and choose the required value from a drop-down list;
   - click  and in the window that opens, select required checkboxes in the list of tags. Click **Save**.

   If you want to exclude some persons, computers, or tags from the selection of events and screenshots, select the **Except** option. Fill in the field that appears as described in t item. If mutually exclusive rules are selected within the same visibility scope, then all events will be unavailable for the user.
f. *Policies* – as described in item e.
g. *Protected objects* – as described in item e.

7. On the *Persons* tab – choose either of the following:
   - enter the first characters of the group of persons and choose the required value from a drop-down list;
   - click  and in the window that opens, select required checkboxes. Click **Save**.

   > **Note:**
   >
   > Attributes of events, screenshots and persons specified on the tabs *Events* and *Persons* are joined by the logical AND, and the input values of the attributes by the logical OR.

8. Click **Save**.

> **Note:**
>
> If you do not select any value in a field of the visibility scope, then event filtering results will not take this field into account. So if you do not select any person, events of all persons will be available to the user.
>
> If you do not select any value in the *Person groups* field on the **Persons** tab, then in the **Persons** section of Traffic Monitor, all persons and computers will be available to the user.

Editing Visibility Scope

**To change the parameters of a visibility scope:**

1. Go to the **Administration -> Users and roles** section.
2. Open the **Scopes** tab.
3. Click the required visibility scope.
4. In the area that opens, edit the required parameters like when creating the scope (see *Creating Visibility scope*).
5. Click **Save**.

Deleting Visibility Scope

**To delete a visibility scope:**

1. Go to the **Administration** -> **Users and roles** section.
2. Open the **Visibility scopes** tab.
3. On the toolbar, click .

   > **Note:**
   >
   > To delete several visibility scopes at a time, select them in the list (for example, by holding **<SHIFT>** or **<CTRL>**) and click **Delete**.

4. In the window that opens, click **Yes**.

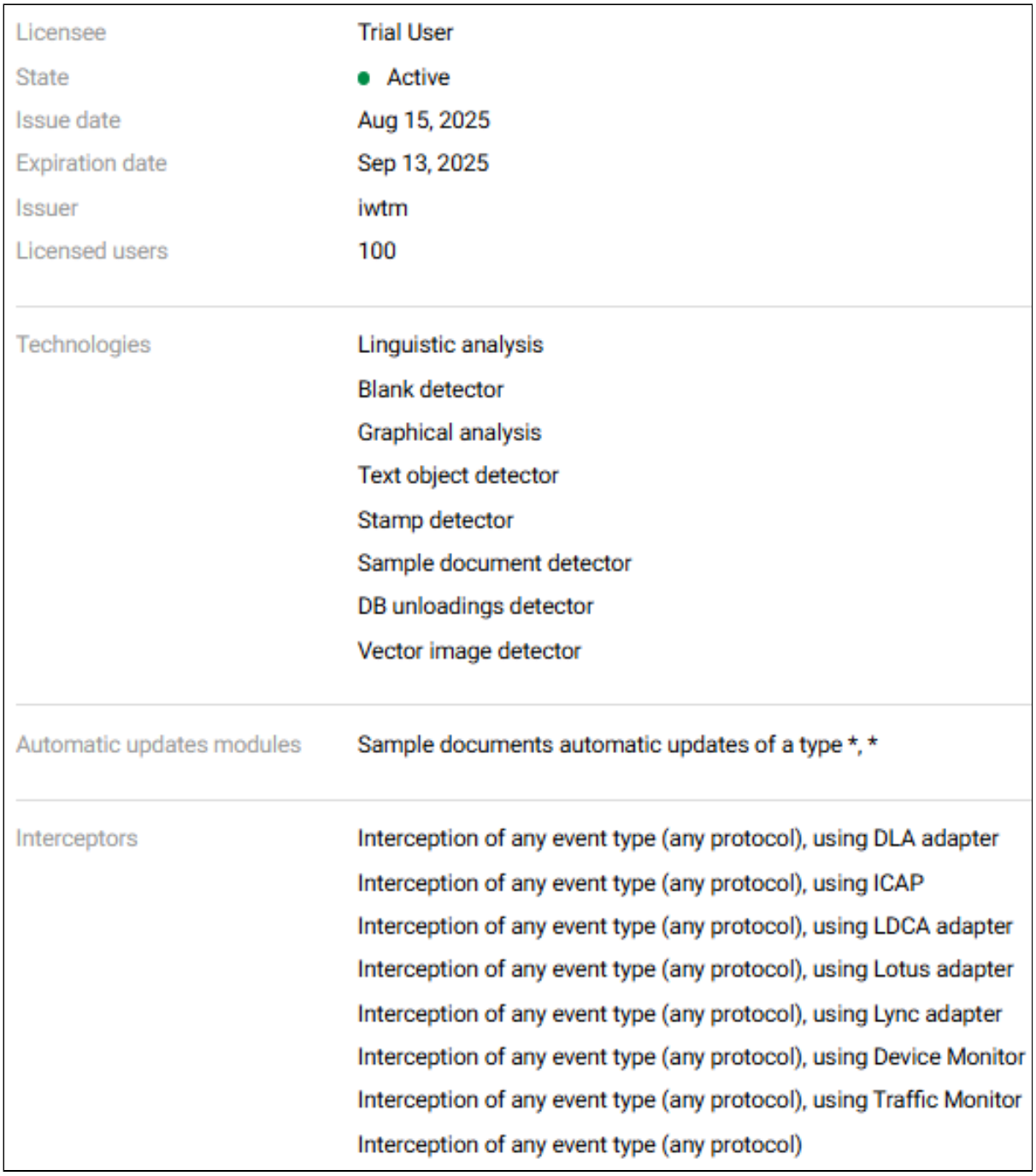
## 4.9.3 Managing Licenses

> **Warning!**
>
> The System licensing is described in the document *InfoWatch Traffic Monitor. Administration Guide. Licensing* article.

Licenses are managed in the Management Console, the **Administration** –> **Licenses** section:

- In the left part of the working area, you can see the list of licenses and a toolbar.
- In the right side of the working area, you can see information on the selected license.

> **Note:**
>
> Editing licenses is unavailable. You can only upload a new license or delete an earlier created license.




You can perform the following actions with licenses:

- Installing a License;
- Deleting License;
- Requesting License;
- Viewing License Usage Statistics.

## Checking License Validity

Information about licensed technologies and interceptors, state, expiration date and number of licensed users, are available in **Administration –> Licenses**.

**To check license validity:**

1. Go to **Administration -> Licenses**.
2. Make sure, that **Expiration date** contains future date.
3. Make sure, that **Licensee** field value matches Licensee parameter of **license.conf** configuration file, located in `/opt/iw/tm5/etc` directory.

## Installing a License

**To install a license:**

1. Go to **Administration -> Licenses**.
2. In the **Licenses** area, click  .
3. Choose required license.lic file and click **Open** in the dialog box.
   Information about licenses, licensed technologies and interceptors will be shown in the **Add license** pop-up window.
4. Click **Save**.
5. Click **Yes** in the dialog box.

Browser page will be refreshed and new license will be added to the list. You may leave or remove the expired licenses at your option.

## Deleting License

**To delete license:**

1. Choose the target license from the list.
2. On the toolbar click  **Delete**.

   > **Note:**
   >
   > To delete several licenses at a time, select them in the list (for example, by holding **<SHIFT>** or **<CTRL>** ) and click  **Delete**.

3. In the opened windows press **Yes**.

## Requesting License

**To request a license:**

1. Go to **Administration** - **Licenses**.
2. On the toolbar, click  **Request license**.
3. Send an automatically generated email. If necessary, add a description.

## Viewing License Usage Statistics

With license usage statistics you can estimate the number of used licenses.

**To view license usage statistics:**

1. Go to **Administration** -> **Licenses**.
2. Choose the required license.
3. In the lower left part of the working area, click **license usage statistics.**
   In the central part of the working area, you can view license usage statistics for the last month. On each intercept channel, you can see:
   - for Device Monitor intercept channels, the number of identified persons/groups of persons (for details, see *Contact Identification in Event*)
   - for Traffic Monitor intercept channels:
     - the number of all unique contacts
     - the number of identified persons/groups of persons

> **Note:**
>
> You can get license usage statistics for the month only after the third day of the next month because statistics will be calculated until then.

### 4.9.4 Healthcheck

You can monitor the state of each server on which the System is deployed in **Administration**->**System state** section of the Management Console.

For each server that is used in the System, indicators are listed in the table:

| | Parameter | Details |
|---|---|---|
| ● | /u02/arch | DISK OK - free space: / 124465 MiB (81.89% inode=100%): |
| ● | /u02/pgdata | DISK OK - free space: / 124465 MiB (81.89% inode=100%): |
| ● | /u02/pgdata1 | DISK OK - free space: / 124469 MiB (81.89% inode=100%): |
| ● | System load | OK - load average per CPU: 0.09, 0.06, 0.05 |
| ● | DB syslog errors | OK - '0' errors in iwtm.V_SYS_LOG |
| ● | Availability of built-in mail transfer agent | SMTP OK - 0.046 sec. response time |
| ● | NTP time deviation | NTP OK: Offset -0.000376701355 secs, stratum best:0 worst:3 |
| ● | Size of database alert log | OK - size of PostgresSQL system log is 695103 bytes |
| ● | PostgreSQL database status | OK - database postgres (0.003618 sec.) |
| ● | Free space in main DB catalogue | DISK OK - free space: / 124462 MiB (81.89% inode=100%): |
| ● | Server availability | PING OK - Packet loss = 0%, RTA = 0.06 ms |
| ● | Root Partition free space | DISK OK - free space: / 124465 MiB (81.89% inode=100%): |
| ● | NTP status | OK - Redirecting to /bin/systemctl status chronyd.service |
| ● | State of syslog service | OK - 'rsyslog' is running |
| ● | Server availability via SSH | SSH OK - OpenSSH_8.0 (protocol 2.0) |
| ● | Swap usage | SWAP CRITICAL - 0% free (0 MB out of 1023 MB) |
| ● | Applied policies actions processing queue | OK - Blackboard queue: 0 item(s), 0.000 MBytes |

For each indicator, the following information is displayed:

- **State** – the current value of the indicator:

    - 🔴 – CRITICAL, the parameter value is higher than the critical threshold;
    - 🟡 – WARNING, the parameter value is a warning zone (if this zone exists);
    - 🟢 – OK, the parameter value is normal.
- **Parameter** – indicator name.
- **Details** – detailed information on healthcheck results.

> **Warning!**
>
> If the indicator value cannot be obtained, it is assumed, that the current value is higher than a critical threshold.

Values are refreshed:

- Every 5 minutes – for parameters:
    - DB Alert Log Errors;
    - Swap usage;
    - DB Alert log Size.
- Every 10 minutes – for parameters:
    - SSH availability;
    - Database Status;
    - Oracle TNS Status.
- Every 360 minutes – for **NTP time deviation** parameter;
- Every 30 minutes – for all other parameters.

To refresh the values manually, click **Refresh**.

## Configure Notifications

To configurenotification about the System state:

1. Go to **Administration** - **System condition**.
2. Click **Configure notifications**.
3. Enable the **Enable notifications** option.
4. Specify values for the following parameters:

| Parameter | Description |
|---|---|
| *Mail prefix* | Mail prefix allows you to sort out the emails from different monitoring systems. The entered value will be added to the beginning of the line in the "Subject" field of messages being sent. The default value is: `IWTM` |
| *Recipients* | Email of recipient(s). The default value is: `nagios@localhost` |

5. Click *Send text message* to check if the settings are correct.
6. Click **Save**.

Notifications will contain the following information:

- Indicator name
- Name of the server where controlled indicator exceeds the threshold value
- IP address of this server
- Current status of the indicator
- Date and time when the indicator threshold value was exceeded

- System message from the source

**Important!**

Notifications from the monitoring subsystem will only be sent if you are using a mail server with the PLAIN authenticaion method.

### 4.9.5 Collecting Diagnostic Data

Collecting diagnostic data is performed in **Administration** -> **Services** section.

| Data collection mode | Description |
|---|---|
| Normal | Collecting information about System logs, configuration and initial installation. |
| Extended | Collecting detailed debug information, including errors, content of processes working memory and their emergency stop. |

Diagnostic information is to be collected from the following sources:

| Data type | Path to files |
|---|---|
| Logs | `/var/log/infowatch/*.log`<br>`/var/log/infowatch/nagios/nagios.log`<br>`/var/log/infowatch/nagios/status.dat`<br>`/var/log/infowatch/install/*`<br>`/var/log/infowatch/update/*`<br>`/var/log/infowatch/sphinx/*`<br>`/var/log/infowatch/iwtm-php-fpm/iwtm-php-fpm.log`<br>`/home/oracle/addm/logs/*` – If Oracle DBMS is installed<br>`/u01/app/oracle/diag/rdbms/iwtm/iwtm/trace/alert_iwtm.log` – If Oracle DBMS is installed<br>`/u01/postgres/pg_log/*` – If PostgreSQL DBMS is installed |
| Configuration information | `/opt/iw/tm5/etc/*.conf`<br>`/opt/iw/tm5/etc/scripts/*.lua`<br>`/opt/iw/tm5/etc/config/lua/vademecums/*.info` |

| Data type | Path to files |
|---|---|
| | `/opt/iw/tm5/etc/config/lua/vademecums/vademecum.list`<br>`/opt/iw/tm5/etc/nagios/*`<br>`/opt/iw/tm5/etc/nagios/objects/*` |
| Logs and scripts of initial installation of the System | `/var/log/infowatch/install/*` |

**To download a report with results of the last diagnostics:**

1. Go to **Administration** -> **Services** section.
2. On the left, select the TM server you need.
3. Click **Collect data**.
4. Select the mode by marking one of the fields: *Normal* or *Extended*.
5. Press **Run**.
6. Wait till completion of diagnostic information collection.
7. Click the **Result of the last data collection is available** link to download the archive in `dd-mm-yyyy_hh-mm-ss` format.

> **Warning!**
>
> If diagnostics has not been performed earlier, downloading the diagnostics results is unavailable.

**To download a report with logs of service:**

1. On the left, select the TM server you need.
2. Press **Save** in **Logs** column opposite one or several running services you need. Logs of stopped service cannot be downloaded.

> **Note:**
>
> When working on OS Microsoft Windows it is possible that the downloaded log will be empty. In this case it is recommended to install the program *UnZip* (for Windows) and use it to unzip the archive.

### 4.9.6 User Actions Audit

The System provides means to track user activity in Management Console.

To review audit events and apply search filters go to **Administration** -> **Audit**.

**Audit events** section contains the following information from the System:

- log in to System, logouts, switch between InfoWatch products, authorization temporary blocks;
- objects related to access control management (Users, Roles, Visibility Scope);
- user actions related to perimeter management;
- user interactions with organizational structure (persons, groups, computers);
- users interactions with System objects (queries, reports, email notifications, policies, rules, elements of technologies, etc.);
- modifications in System configuration (creation, editing, cancelling);

- modifications in System objects by external systems.

**Important!**

Audit events section does not contain:

- Information on configuration changes from rollbacks. In this case, only the event of cancelling will be created;
- Information on creation of groups, persons or computers in the process of synchronization with LDAP server, as well as their old values if changed by user;
- Information on any changes to report widget, except for the name change.

After updating to current version, audit events for actions with policy rules, persons, groups and computers that were registered in earlier versions of System will not be changed.

For more on working with audit events, see the following subsections:

- Audit Events;
- Extended Information;
- Filtering and search.

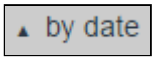
## Audit Events

The **Audit Events** area is located in the **Administration -> Audit** section.

The **Audit Events** area displays results of **Search filters**. This is a list of audit events in the form of panels with the following attributes:

- The name of the user who took an action;
- The name of the object the action applied to;
- The type of action that was taken by the user;
- Date ana time of the registered user action;
- Extended information on the audit event (the More info link).




To sort audit events by the creation date, click  in the left upper corner.


To display extended information for all the audit events in the list, click . To hide this information for all the events, click . If you switch the section or exit the System, the setting is saved.

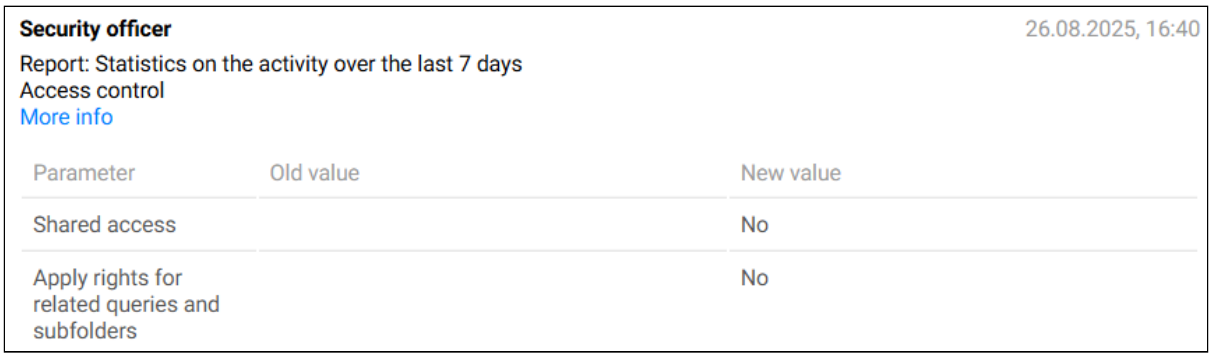

### Extended Information

The audit event may contain additional information: the list of modified parameters, their new and old values, modification data. To view this data, click **More info** on the desired panel.

For example, when a user logs into the System, the event has the following parameters:

- DNS-name of the computer from which the user logged into the System;
- The IP address of the computer from which the user logged into the System;

- The name of the user who logged into the System.




**Warning!**

Audit events data can be different depending on *Object* and *Action*.

You can enable displaying detailed information for all the audit events in the list (see *Audit Events*).

## Filtering and search

To view required audit events, you can use full-text search or filters in the **Search filters** area of the **Audit events** section:

1. In the search bar, type the full name of the desired object. The name should contain at least three letters. To find long word forms, you can type the first three letters of the name and then use the ***** character.
2. If necessary, select the user names from the **User** drop-down list (see *Managing System Users and their Roles*).
   If you select the **Select all** option, then all values from the drop-down list will be added to the filter.
3. If necessary, select the user actions from the **Action** drop-down list.
4. If necessary, select the objects in the System from the **Object** drop-down list.
5. If necessary, select the **Date** parameter and then select:
   a. **All time**, if you need the list of events created for all time,
   or
   b. **Period** to specify the start and end dates of the period. Audit events for the specified period will be displayed. Click **Apply**.

You can use both the search bar and filter parameters (some or all of them) at the same time. In this case, found audit events will satisfy both the specified attribute values and the search query.

To save free space in the database, you can set the **Audit events storage period (days)**, after which events will be deleted.

**Important!**

Audit events and Traffic Monitor events may have different storage periods. If audit events have a larger storage period, there can be audit events without related Traffic Monitor events, as related Traffic Monitor events may already be deleted.

## 4.9.7 Integrity Monitoring

Integrity monitoring is intended to monitor system files state. Primary reference amount is automatically generated by the System.

System files integrity monitoring is described in the following sections:

- Manual Integrity Monitoring;
- Automatic Integrity Monitoring;
- Accepting Result as Standard.

### Manual Integrity Monitoring

**To check system files integrity:**

1. Go to **Administration - Integrity monitoring**;
2. In the central part of the working area click **Scan files**.

> **Note:**
>
> In the process of integrity check the **Integrity check is being performed** message is being displayed. Upon check completion, you will see the message with date and time of the last check.

### Automatic Integrity Monitoring

**To configure system files automatic integrity monitoring:**

1. Go to **Administration - Integrity monitoring**;
2. In the central part of the working area enable **Automatic check** setting.
3. In the **Schedule** field set the time of integrity check using **up** and **down** arrows.
4. Click **Save**.

### Accepting Result as Standard

**To accept result of integrity check as standard:**

1. Go to **Administation - Integrity monitoring**;
2. In the central part of the working area click **Accept result as standard**.

## 4.9.8 Plugins

Using plugins you can add the following additional features to Traffic Monitor:

- Receiving events from external interceptors;
- Adding user attributes of events;
- Automatically updating of sample unloadings with data from external systems;
- Automatically updating of sample documents;
- Providing data to external systems.

## Default Plugins

After installing Traffic Monitor, the Management Console displays the **InfoWatch Investigation Centre** plugin.

To activate another default plugin, request the appropriate license and upload it to the Management Console (see *Managing Licenses*). The following plugins can be added:

- **InfoWatch Data Discovery**;
- **InfoWatch Device Monitor**;
- **InfoWatch Sample Documents Autoupdate Adapter**;
- **InfoWatch Password Disclosure Adapter**.

## Custom Plugins

Plugins for integration with Traffic Monitor an be developed by:

- the InfoWatch company. If you need to add an integration developed by InfoWatch to Traffic Monitor, request a plugin from technical support at *support@infowatch.com*. For more details about supported InfoWatch integrations, see the section *IW Traffic Monitor Integrations*;
- third-party developers. To add an integration created by third-party developers, request the corresponding plugin from them. For more details about the structure and types of plugins see the article *Plugin Types*.

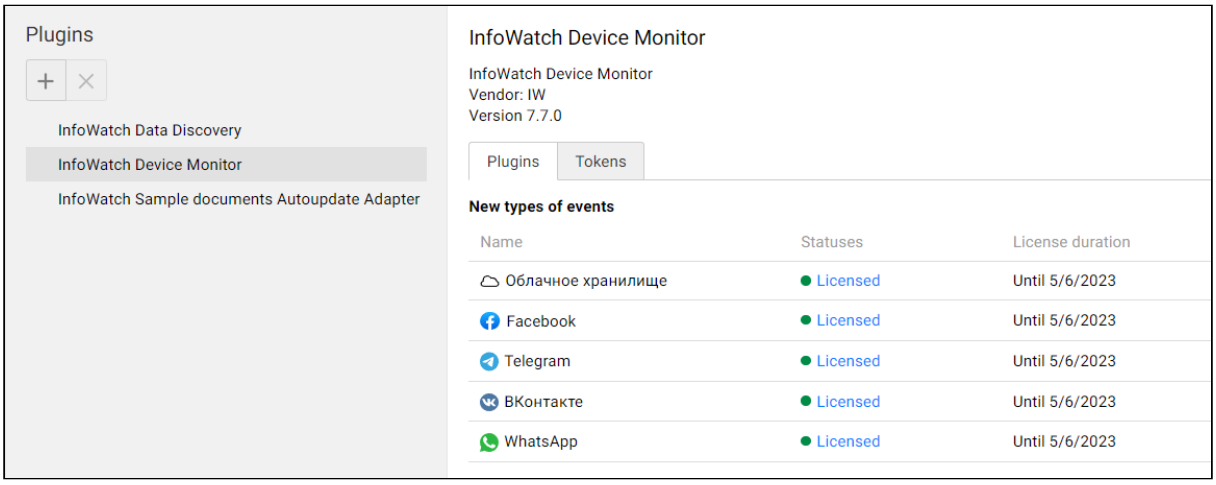
All integrations with external systems must be registered in Traffic Monitor by adding a new plugin. For more details about adding a plugin to Traffic Monitor, see *Adding Plugin*.

Each integration must be matched with a specific plugin.

## Work with Plugins in Traffic Monitor

You can work with plugins in the Management Console, the **Administration** –> **Plugins** section:

- In the left part of the working area, you can see the list of plugins and the toolbar
- In the central part of the working area, you can see information on the selected plugin. Also you can find here the **Tokens** tab




In **Plugins** sections, you can perform the following actions:

- Adding Plugin;
- Deleting Plugin;
- Working with Tokens.

**Warning!**

Plugins and tokens are deleted from the System when deleting the DB schema (see *InfoWatch Traffic Monitor. Installation Guide. Deleting the Database Schema* article). To restore the Device Monitor plugin:

1. Create the file **/opt/iw/tm5/www/backend/protected/runtime/first_run** on behalf of **iwtm** user.
2. Restart **iw_kicker** process:
   ```
   iwtm restart kicker
   ```

Other plugins should be added manually (see *Adding Plugin*).

## Plugin Types

A plugin is an archive in a ZIP format, which contains:

- **licenses** folder with license files;
- **icon** folder with icons for registered contacts and event types;
- **manifest.json** file with information about the plugin. For each type of plugins, the file structure is different.

**Note:**

Names of files in the plugin should contain only Latin characters and/or numbers.

Folders **licenses** and **icon** are optional. License files and files with pictograms can be located in the root folder.

To bind a plugin to a license, see the Knowledge Base article *Binding plugin and license*.

### Plugin Types

This section provides information for developers about the **manifest.json** file depending on the plugin type. See the file example in the articles *InfoWatch Traffic Monitor. Administration Guide. DataExport API third-party component registry file format*, *PushAPI SDK third-party component registry file format* and *REST API third-party component registry file format*.

Plugin types:

- Plugin for External Systems which are the Sources of Events;
- Plugin for External Systems which are the Sources of Sample Unloadings;
- Plugin for External Systems Receiving Data from Traffic Monitor.

#### Plugin for External Systems which are the Sources of Events

Using the plugin, you can register the following objects in Traffic Monitor:

- Event types;
- Protocols;
- Actions;
- Contact types;
- User attribute of events.

The **manifest.json** file should contain the following information:

- Unique identifier – unique 128-bit identifier (UUID) of the plugin;
- Name – plugin unique name;
- Description (optional element);
- Version;
- *Preinstalled* attribute (optional element) – whether it is included in the System;
- Developer company ID – matches the company name in the license.

Registered Events Types, Contacts, Protocols, etc.
Using plugin you can register new events types, protocols, actions and contacts.

To do this, add the following information to the **manifest.json** file:

- **Registered events type:**
- Service type which the registered event type belongs to;
- Protocols which the registered event type belongs to (optional element);
- Codes of interceptors types (origin) for InfoWatch Plugins (optional element);
- Localizations of event type names in at least one language;
- Files with icons of registered event types (optional element) – path to the icon file relative to the archive root (must not start with /).

- **Registered protocols:**
  - Localization of protocol names in at least one language.
- **Registered actions:**
  - Localization of action names in at least one language.
- **Registered contact types:**
  - Objects types which the registered contact belongs to;
  - Localizations of contact type names in at least one language;
  - Files with icons of registered contacts (optional element) – path to the icon file relative to the archive root (must not start with /);
  - Registered user attributes of events (optional element) – set of a custom event attributes that are registered by this plugin. The parameter list for each registered attributes see *below*.

Preinstalled Event Types and Protocols
When creating an event type, you can rely on an existing one.

To do this, add the following information to the **manifest.json** file:

- Event types;
- Service type which the preinstalled event type belongs to;
- Protocols which the preinstalled event type belongs to (optional element);
- Codes of interceptors types (origin) for InfoWatch Plugins (optional element).

Custom Attribute Parameters
To register required attributes for using them in Traffic Monitor, add the following information to the **manifest.json** file:

- Attribute name;
- Code – unique attribute code that is used in event headers and for identification in xAPI/PushAPI.;
- Service – service code. Several services can be specified;
- Use in policy – whether an attribute is used in rules of data protection policies;
- Display in policies by default (optional element) – displaying an attribute in the comon list in the corresponding rule when configuring data protection policies;
- Use in query – whether an attribute is used in Traffic Monitor query;

- Use in notifications – whether an attribute is used in Traffic Monitor email notifications;
- Display in tabular form of event preview – displaying an attribute in the event card;
- Display in brief form of event preview – displaying an event in brief preview form;
- Display in detailed form of event preview – displaying an event in detailed preview form;
- Value type – value type that the external system transmits;
- Possible values (optional element) – rules for validating user input in requests and policies;
- Multiple value – feature that allows to add several values to one attribute.

Plugin for External Systems which are the Sources of Sample Unloadings

The plugin helps to register updated data types in Traffic Monitor.

The **manifest.json** file should contain the following information:

- Unique identifier – unique 128-bit identifier (UUID) of the plugin;
- Name – plugin unique name;
- Description;
- Version;
- *Preinstalled* attribute (optional element) – whether it is included in the System;
- Developer company ID – matches the company name in the license;
- Data types list – list of identifiers for systems receiving data from Traffic Monitor that are registered in the plugin.

Plugin for External Systems Receiving Data from Traffic Monitor

The plugin helps to register systems receiving data in Traffic Monitor, which can recieve information aout Traffic Monitor objects using Public API.

The **manifest.json** file should contain the following information:

- Unique identifier – unique 128-bit identifier (UUID) of the plugin;
- Name – plugin unique name;
- Description;
- Version;
- *Preinstalled* attribute (optional element) – whether it is included in the System;
- Developer company ID – matches the company name in the license;
- Data receiving systems – list of identifiers for systems receiving data from TM that are registered in the plugin.

## Adding Plugin

**To add a plugin:**

1. Go to **Administration - Plugins**.
2. In **Plugins** area, click  **Add plugin**.
3. Click **Select file** and choose a plugin archive to be loaded into the System.

> **Note:**
>
> To update the plugin, add a new version.

### Deleting Plugin

**To delete a plugin:**

1. Go to **Administration - Plugins**.
2. In **Plugins** area, choose the plugin and click  **Delete plugin**.
3. Click **Yes** to confirm deletion.

> **Warning!**
>
> Preset plugins cannot be deleted.

## Working with Tokens

Tokens are designed for authorizing an external which uses Push API (sending events from third-party interceptors to TM) and Public API (loading external unloadings from DB to TM and access to TM data for external systems). When the plugin is added, a token is created automatically. (see *Adding Plugin*).

For InfoWatch Device Monitor, a token is created automatically and is available in **Administration** -> **Plugins** -> **Tokens** section of the Management Console.

The following actions with tokens are available:

- Adding Token;
- Editing Token Data;
- Updating Token Value;
- Copying Token;
- Deleting Token.

### Adding Token

**To add a token:**

1. Go to **Administration** - **Plugins**.
2. In the **Plugins** area, choose the plugin.
3. Go to the **Tokens** tab.
4. Click  **Create token**.

> **Note:**
>
> The token value is generated automatically upon the token creation and can not be defined by user.

### Editing Token Data

**To edit token data:**

1. Go to **Administration** - **Plugins**.
2. In the **Plugins** area, choose the plugin.
3. Go to the **Tokens** tab.

4. Choose the token and click  **Edit token**.
5. In the appeared form in the *Status* field choose the *Active* or *Inactive* value.
6. If necessary, change the *Name* and add the *Note.*
7. Click **Save**.

Updating Token Value

In case the token is compromised, we need to generate a new token value.

**To update a token value:**

1. Go to **Administration** - **Plugins**.
2. In the **Plugin** area, choose the plugin.
3. Go to the **Tokens** tab.
4. Choose the token and click  **Refresh token content**.

Copying Token

**To copy the token value to the clipboard:**

1. Go to **Administration - Plugins**.
2. In the **Plugins** area, choose the plugin.
3. Go to the **Tokens** tab.
4. Choose the token and click  **Copy token**.

Deleting Token

**To delete a token:**

1. Go to **Administration** - **Plugins**.
2. In the **Plugins** area, choose a plugin.
3. Go to the **Tokens** tab.
4. Choose the token and click  **Delete token**.

> **Note:**
>
> To delete several tokens at a time, select them in the list (for example, by holding **<SHIFT>** or **<CTRL>** ) and click  **Delete token**.

5. In the opened window click **Yes**.

## 4.9.9 Configuring Connection to Mail Server

In the **Administration** -> **Mail server** section, you can specify an SMTP server that will be used for sending notifications about triggered rules (see *Configuring Notifications*) and the state of the System (see *Healthcheck*).

To configure the connection:

1. In the **Sender's email address** field, specify the address that will be used for sending notifications.
2. Choose the server type. Possible choices:

- **Embedded in Traffic Monitor**. Select this option if you are using a local Traffic Monitor mail server with anonymous access;
- **External**. Select this option if you are using an external server. For example, if sending emails to external servers without authorization is prohibited in your company.

3. If an external server is used, specify the server parameters:
   - **SMTP server address**;
   - **Port**;
   - **Login**. Optional parameter;
   - **Password**. Optional parameter;
   - **Encryption**:
     - *Use STARTTLS*[1]. For encrypted connection, STARTTLS protocol and NTLM authentication will be used;
     - *Not use*. Connection without encryption.
4. When you have specified all connection settings, click **Check connection**.
5. Click **Save**.

**Important!**

[1] In case you configure a connection to an external mail server with encryption, notifications from Nagios monitoring system cannot be sent.

### 4.9.10 Configuring Notifications

In the **Administration** -> **Notifications** section, you can configure templates for emails which are sent when the security policy is triggered.

Notifications can be sent to:

- **An employee** who has violated a security policy. If a rule is triggered, the employee is notified that his/her actions violate the corporate security policy. If the System operates in the inline mode, employees also get timely notifications when:
  - their emails are blocked or quarantined and await a decision of the security officer;
  - the security officer has decided on the quarantined email (whether to block it or send it to the recipient).
- **A security officer**. Getting timely notifications about incidents makes it easier for the security officer to promptly respond to important incidents.
- **Other interested persons**, for example, the head of an employee who has violated a security policy.

To create a notification, click  on the toolbar to the left (see *Creating Notification*). Added notifications are used in policy rules: in the **Actions when the rule is triggered** area, **Send notification** field, click  and select the required notification (for details, see *Creating Rules*).

**Note:**

If necessary, you can create or edit notifications when configuring a rule in the **Policies** section. Editing and deleting notifications is only available from the **Notifications** section.

To edit a notification, choose the required notification in the list and click  on the toolbar.

While creating/editing a notification, you can test the resulting template (see *Testing Notification*).

To copy an earlier created notification, choose it in the list and click  on the toolbar. The notification copy will be added to the list.

To delete a notification, use  button on the toolbar.

> **Note:**
>
> In this case, the notification is also deleted from all policies where it is used.

Besides user-created notifications, there are also preset notifications in the System (see *Preset Notifications*).

## Creating Notification

**Purpose:**
Create a notification that can be sent when rules are violated.

**Solution:**

1. Go to the **Administration** -> **Notifications** section.
2. On the toolbar to the left, click .
3. In the form that opens, enter the notification name.
4. Choose notification recipients. Possible choices:
   - **Initiator of event** - select this field to create a template that will be sent to the event initiator;
   - **Custom recipients** - select this field and click  to add recipients. In the window that opens, go to the required tab:
     - On the **Persons** and **Security officers** tabs, choose required values from the list. You can sort values in the list by the person/user name.
     - On the **Email** tab, you can enter email addresses of recipients who are not in the list of persons or security officers.
     - On the **Head** tab, enable the switch if you want to notify the head of the event initiator.

   Once you have specified all required recipients, click **Save**.
5. In the **Email template for different verdicts** open the tab with a verdict for which you want to create a template. The following tabs are available:
   - **Allowed** - the rule has the *Allowed* verdict, however, the employee should be informed that his/her actions violate the security policy;
   - **Blocked** - the event is blocked by Traffic Monitor which operates in the inline mode or by Device Monitor agent as a result of applying a data protection policy on agents;
   - **Quarantined** - SMTP email is quarantined by Traffic Monitor and awaits a decision of the security officer (only if the System operates in the inline mode);
   - **Unblocked after quarantine** - the security officer has changed the verdict from *Quarantined* to *Allowed*, and the SMTP email is passed to an external server to be sent to recipients (only if the System operates in the inline mode).

- **Blocked after quarantine** - the security officer has changed the verdict from *Quarantined* to *Blocked* and forbidden sending the SMTP email (only if the System operates in the inline mode).

6. To create a template for the selected verdict, enable the **Send** switch on the selected tab.
7. In the form that opens, specify what items should be included in the email subject and body. By default, inputs fields are displayed where you can enter required text.
8. To add an item to the message subject or body, click **+Add** in the **Email subject** or **Email body** area respectively and choose the required item from the drop-down list. You can choose the following items:
   - **Event ID** - when you add the event ID to the message body, you can also add a link to view the event in the Management Console;
   - **Senders** and **Recipients** - from the drop-down list, choose what details on senders and recipients should be included in the message subject or body. By default, a name and a contact from the event are added;
   - **Policies** triggered in the event. When adding policies to the message body, you can specify what information about policies should be added: the policy name, a description, or both parameters;
   - **Attachments** - from the drop-down list, choose what details on attachments should be included in the message subject or body. By default, the file name and size are added.
   - **Sender's computer**;
   - **Interception date**;
   - **Event type**;
   - **Verdict**;
   - **Violation level**;
   - **Protected objects** triggered in the event;
   - **Message subject** for emails sent by employees;
   - **Source application and destination application**;
   - **Path to file**;
   - **Print task name**;
   - **Resource**;
   - **Perimeters**;
   - **Sending date**;
   - **Terminal session name**;
   - **Browser tab address**.

   To delete an item, click  in the right upper corner of the selected item.
9. If you want to add the event card to the notification, enable the **Attach event card** switch. The notification email will include a file with the event text and the text extracted from attachments. Triggered protected objects are highlighted in the text.

> **Important!**
>
> A notification with the event card will be sent to all recipients specified in the **Custom recipients** field. You should see to it that sending event details to external emails should not lead to the leakage of confidential data.

> **Important!**

In case if the event contains an archive where the number of attachments (contents) exceeds 2000, then:

- the event card will be missing in the email notification;
- the email will contain a note that the event card is not downloaded, as the number of the event contents is bigger than the allowed value.

10. Choose the card format: **Microsoft Word** or **PDF**.
11. Specify in what form the highlighted text should be included in the card. Possible choices:
    - **As snippets** - the event text will be exported as snippets which contain triggered protected objects;
    - **All text** - the whole event text will be exported.
12. When you have specified all required parameters, click **Save**.

**Note:**

While creating a notification, you can test the resulting template (see *Testing Notification*).

## Testing Notification

While creating or editing a notification, you can test the resulting template. For this:

1. In the right lower corner of the workspace, click **Send test notification**.
2. In the window that opens, specify:
    - **Event ID** - enter an ID of the event which exists in the System;
    - **Recipient** - specify an email address to which a test message should be sent.
3. Click **Send notification**.

A test message with a notification created according to your template will be sent to the specified email address.

## Preset Notifications

There are the following preset notifications in the System:

1. *Notification to violator*. Includes templates that can be sent to the event initiator if the event is:
    - allowed;
    - blocked;
    - quarantined;
    - unblocked after quarantine;
    - blocked after quarantine.

    The notification includes a message on the current state of the event and information about senders, recipients, interception date and time, resources, and attachments.
2. *Notification to security officer*. Includes templates that can be sent to the security officer if the event is:
    - allowed;
    - blocked;
    - quarantined.

    The message subject includes information about the incident, its violation level, and the verdict. The message body includes the following data:
    - event ID;

- interception date and time;
- event type;
- violation level;
- verdict;
- triggered policies;
- triggered protected objects;
- sender's computer;
- senders;
- recipients;
- resource;
- message subject;
- attachments.

## 4.9.11 Managing Tablespaces

The System stores events and intercepted data in the form of daily tablespaces. The System creates three types of daily tablespaces:

- Events with violations;
- Events without violations;
- Other (screenshots).

In the **Manage** -> **Tablespaces** section, you can see the list of daily tablespaces, which includes events and screenshots for each day. Daily tablespace status shows the current daily tablespace state and can have the following values:

- *Connected*;
- *Archived*;
- *Restored*.

In addition to the main values listed, statuses automatically get temporary values during tablespace state change. In case an error occured during temporary status change, then the status will have an icon . To view the error text, point the cursor on the icon. To copy the error text, click .

You can view the amount of disk space that a tablespace occupies in the following columns: “DB size”, “Storage size», and «Total size». «Storage size» shows how much space a tablespace occupies in the storage of binary data, Data Storage, if you use it. Otherwise, the value of this column equals zero.

To reduce the volume of processed data, archive daily tablespaces which are currently not in use. To do this:

1. Select a daily tablespace from the list. To select several daily tablespaces, use *Ctrl*.
2. Click , then click **Yes** in the confirmation window and wait for the end of the process.

As a result, the daily tablespace archive is stored on the hard drive.

To reconnect an archived daily tablespace to the System, select it, click  and wait for the process to finish. After this, the events in the archive are available for viewing and analyzing, including full-text search without reindexation required.

To remove an archived daily tablespace or a tablespace which is not in use, select it and click .

**Important!**

In Management Console, you cannot perform operations on tablespaces where date of event interception is greater than or coincides with today's date. Archiving, restoring and deleting such tablespaces is available via the database or `iw_space_manager` console utility using `--force` flag. For details, see document *InfoWatch Traffic Monitor. Administration Guide*. *Managing Daily Tablespaces* in section *Oracle* or *PostgreSQL*.

# 5 END-USER LICENSE AGREEMENT

**ATTENTION! Please read the terms and conditions of this End-User License Agreement (hereinafter referred to as the "Agreement") carefully before using the Software. Installation and/or use of the Software shall constitute your full and unconditional acceptance of all the terms and conditions of this Agreement.**

**If you do not accept to the terms and conditions of this Agreement, or if you enter into this Agreement on behalf of a legal entity, but you do not have such authority, you must interrupt the installation and/or stop using the Software and delete any copies of the same.**

**1. Grant of License**

1.1. This End-User License Agreement shall constitute a standard form contract entered into by and between the End User and Laboratory InfoWatch LLC, Taxpayer Identification Number (INN) 7734583888 (hereinafter referred to as the "Copyright Holder").

1.2. You shall be granted hereunder a personal, non-transferable and non-exclusive license granting you the rights to use the Copyright Holder's software (hereinafter referred to as the "Software"), namely the rights to download, install, backup and use the Software for its intended purpose, as set forth in the Software Documentation (User's Guide, Administrator's Guide, Installation Guide), this Agreement and your Licensing Agreement. The Software Documentation shall be an integral part hereof.

1.3. The Software is only for use in your current operational activities. If you have received, downloaded and/or installed the Software for information, you may use the Software only for informational purposes and only during the trial period. Any use of the Software for any other purposes or after the trial period shall be prohibited.

1.4. If you use different Software versions or Software versions for different languages, or if you receive the Software on several media, or if you otherwise receive several copies of the Software or receive the Software as part of a package of other software, the total number of your licenses shall not exceed the number specified in your Licensing Agreement.

1.5. You may make a copy of the Software, provided that such a copy is intended only for archival purposes or to replace a duly purchased copy in cases where the original is lost, destroyed or becomes unusable. This copy may not be used for any other purposes and shall be destroyed, if the possession of the Software copy ceases to be legitimate.

1.6. You shall be solely responsible and ensure compliance with the applicable export and import laws, as well as applicable trade sanctions and embargo with regard to the transfer of rights and use of the Software.

**2. Terms and Conditions of Use**

2.1. The Software is intended solely for use in analyzing and checking corporate information, and specifically for detecting and preventing unauthorized use of confidential data.

2.2. You shall use the Software exclusively in accordance with the applicable statutory requirements of the Russian Federation or any other countries, including but not limited to:

- legislation on personal data;
- legislation on trade secrets;
- legislation on combating the misuse of insider information;
- anti-corruption legislation;
- legislation on critical information infrastructure;
- legislation on state information systems;
- National Payment System data protection legislation;
- statutory provisions of the Labor Code of the Russian Federation;
- and any other applicable sources of law.

2.3. You may not use the Software for any purpose or in any manner that violates applicable law, this Agreement and/or any third-party rights. The Copyright holder shall not be liable for your breach of this Clause.

2.4. If you are not a resident of the Russian Federation, you shall use the Software in full compliance with applicable law, including laws and regulations on personal data and trade secrets.

2.5 In order to avoid your violation of Articles 138, 138.1 of the Criminal Code of the Russian Federation, Article 23 of the Constitution of the Russian Federation or any other legal regulations, before using the Software, you are recommended to inform your employees in writing that:

- this Software is used on the workstation computer, and you should inform your employees about the features of this Software and data that may be obtained as a result of using the same;
- the workstation computer and the communication channels used (e-mail, local corporate network, telephony and IP-telephony, etc.) are your property and are provided to such employees for temporary use so that they could perform their official duties;
- all information created on the workstation computer is your property and is subject to inspection and logging on a legal basis.

2.6. Please note that you need to obtain the consent of the persons whose data will be processed when using the Software to the relevant collection, storage, use, processing, distribution or any other form processing of such data.

2.7. We remind you that installing a program on another person's computer without prior authorization from such a person, obtaining personal data of any third party without his/her consent, violating privacy, breaching confidentiality of correspondence, telephone conversations, telegraphic or any other types of messages shall constitute a criminal offense and shall be prosecuted, as prescribed by the current legislation of the Russian Federation.

2.8. The Copyright Holder shall not have access to the data created and/or obtained as part of your use of the Software. You shall have exclusive access to such data. In view of the foregoing, the Copyright Holder shall not collect, or store, or use, or distribute such data.

2.9. You shall be held fully and solely liable if the information created and/or obtained as part of your use of the Software contains unethical and/or illegal data, computer viruses or programs (or links thereto) that may interrupt or disrupt the standard features of computer equipment, software or telecommunication facilities of any persons.

2.10. You shall not:

- fully or partially edit, change, adapt, translate, decompile, disassemble, reverse engineer, create or recreate source code, modernize, correct obvious errors, modify the Software and/or its components, whether in full or in part, or attempt to do so in respect to the Software and/or its components, or create derivative works based on the Software and/or Documentation;
- to use the Software in excess of the licensed number of accounts stipulated in the agreement with your direct licensor;
- integrate the Software into any third-party website or software product, except where such integration is expressly authorized by the Copyright Holder and the copyright holder of such a third-party website or software product. The Software may be integrated into a third-party software product only through the built-in API module within the features of such a module;
- remove or modify any notice of copyright, proprietary rights to the Software and/or its elements;
- to use the Software for the purpose of making a profit, let on lease, rent out or assign for temporary use, to provide a subscription to the Software, provide outsourcing services using the Software, sublicense, distribute the Software or otherwise grant any rights with respect to the Software and/or Documentation to any person or entity, or disclose the results of development testing of the Software, except as expressly permitted by this Agreement or by the written consent of the Copyright Holder;
- allow or provide a link to the distribution copy or a license key to any third party in violation of this Agreement and your Licensing Agreement;
- use the Software to create data or code intended for use by other Software products;
- independently install additional Software applications, replace Software components;
- collect, systematize, store or disseminate confidential and/or personal information in violation of law;

- use the Software for unauthorized remote access to any third-party computer, or changing the configuration of the computer so that such features can appear in third-party software;
- use the Software to collect, store, use, process or distribute any information or data that violates the applicable laws or the rights and legitimate interests of any third party.

2.11. The license key shall constitute confidential information, and its unauthorized transfer to third parties is prohibited. The Copyright Holder shall reserve the right to use the means to verify the authenticity of the license key you have installed.

**3. Disclaimer of Warranties and Liability of the Copyright Holder**

3.1. The Software shall be provided "AS IS" in accordance with generally accepted international business practice. The Copyright Holder shall not be responsible for any issues arising during the operation of the Software, including those related to compatibility with other software products (packages, drivers, etc.) or those arising from ambiguous interpretation of the Software Documentation, or for failure of the Software to meet your expectations, etc.).

3.2. You confirm that you are aware of the features of the Software licensed hereunder, and you shall be held fully and solely liable if the Software or the results of using the same do not meet your individual needs or expectations.

3.3. The Copyright Holder makes no warranties, whether expressed or implied, and hereby disclaims all warranties.

The Copyright Holder makes no representations or warranties regarding the fact that the Software is flawless, uninterrupted, fast or accurate, and shall not be responsible for any direct or indirect consequences of using the Software, including those arising from potential errors in the Software or typos in the Software and/or the Documentation attached thereto or further provided.

The Copyright Holder makes no representations or warranties and shall not be held liable in the event of any changes in a third-party software that occurred after the installation/deployment of the Software and resulted in a loss of the Software features (including, but not limited to, a change in the data transfer protocol, data storage format, logic of a third-party software, an update of a software that ceases to support the Software). The Copyright Holder makes no warranties or representations and sets no conditions or provisions (whether expressed or implied) in respect of any matters, including but not limited to infringement of third-party rights, merchantability, integration or fitness for a particular purpose.

3.4. Any data that becomes available in the course of using the Software, including any file, link, image or text, shall be the sole responsibility of a disclosing person or entity and shall be the property of such a person or entity. This Agreement shall not grant any rights to such data. You accept responsibility for any potential consequences, security risks or any losses caused by such data viewed or obtained by using the Software.

3.5. The Copyright Holder shall not be liable for any loss or damage, regardless of the reasons for such a loss or damage (including, but not limited to, direct or indirect damage, lost profits, interruption of commercial or business activities, loss of business information, negligence, or any other losses) arising from the use or failure to use the Software, even if the Copyright Holder has been notified of eventual losses. The Copyright Holder's liability shall be at any time limited to reimbursement for documented actual damage of up to Three thousand rubles (RUB 3,000). The Copyright Holder shall be held liable only for actions or omissions for which the Copyright Holder is at fault.

**4. Intellectual Property Rights**

4.1. You hereby agree that the exclusive rights to any intellectual property embodied in the Software and /or any documentation provided to you shall be vested in the Copyright Holder. The Software shall not be assigned or sold hereunder, but shall be granted under a limited non-exclusive license. Nothing in this Agreement grants you any rights to the said intellectual property other than those conferred under your Licensing Agreement.

4.2. You agree that the source code and the license key for the Software shall be the property of the Copyright Holder.

**5. Rights to Information Accessed in the Course of Performance of this Agreement**

5.1. You hereby agree that you do not have any rights to any information that is not subject to intellectual property, as set forth in Section 4, accessed by you in the course of performance hereof.

5.2. Such information may include, but shall not be limited to, any system, method of work or any other information.

5.3. You may use the above information only for the purpose of exercising the rights to the Software granted under this Agreement and the Licensing Agreement. You may not use this information for your own benefit or beyond the scope of this Agreement or the Licensing Agreement.

**6. Open Source Software**

**You are aware that the Software contains open source software distributed under certain licenses, available in the licenses.inf (license.info) file, provided together with the Software as part of the distribution kit.**

You agree that the Software components developed by third-party developers are provided without guarantees of access to updated versions of the components and to other programs, equipment, training certificates or services of third-party developers.

**7. Miscellaneous**

7.1. This Agreement shall come into force immediately upon installing the Software and shall be valid throughout the period of use.

7.2. In the event that you violate any of the provisions of this Agreement and/or your Licensing Agreement, or in the event that the performance of this Agreement and/or your Licensing Agreement violates or may result in violation of the applicable laws, the Copyright Holder shall have the right to repudiate and terminate this Agreement (including, but not limited to, by blocking the license key, terminating the grant of rights) at any time without prior notice. To the extent set forth above in this Clause, you shall not be reimbursed for the cost of the Software/the amount of the Software license fee, or any eventual losses arising under this Agreement and/or your Licensing Agreement.

7.3. Upon termination or expiration hereof, the End User shall destroy all copies of the Software installed.

7.4. You are hereby notified that when the usage statistics collection function is enabled in the Software, the Software may collect and record anonymized information on:

1. a) hardware, operating system of the device on which the Software is installed and operated, as well as other technical data containing information on the use of hardware, hardware load and processing speed of the Software;
2. b) end user's activities in the user interface of the Software.

The Copyright Holder may use the specified data to make decisions on the development of features and improvement of the operational characteristics of the Software.

The Copyright Holder shall ensure the confidentiality of the data obtained and shall not disclose or transfer such data to any third party.

7.5. This Agreement, as well as any disputes arising out of or in connection with this Agreement, shall be governed by and construed in accordance with the laws of the Russian Federation.

7.6. All disputes and disagreements arising during the performance hereof shall be resolved through negotiations, if possible. In case of failure to reach an agreement, disputes shall be settled in court in the Arbitration Court of Moscow.

7.7. This Agreement may be amended by the Copyright Holder at any time without prior notice. The amended Agreement shall enter into force once it is posted at the address specified below in this Clause. The current version of the Agreement is always available at *https://kb.infowatch.com/display/EULA/*. By continuing to use the Software, you accept the amendments and/or additions made to this Agreement. If you do not accept the terms and conditions of such amended Agreement, you shall immediately discontinue the use of the Software.

**8. Contact Details of the Copyright Holder**

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

Sales Department: sales@infowatch.com

Technical Support: support@infowatch.com

Web site: www.infowatch.ru

# 6 Glossary

| Term | Glossary |
|---|---|
| Active Directory | LDAP-compatible Microsoft directory services for the Windows NT operating systems family |
| Active policy | A policy included into a configuration that is uploaded to a host. See also: Policy, Host |
| Administrator | A preset role and user account in Management Console. An Administrator can modify other accounts and their rights. It is also a System user who installs, configures and maintains the System. See also: User role, Security officer, User |
| AJAX | Asynchronous JavaScript and XML is a group of interrelated Web development techniques used on the client-side to create asynchronous Web applications |
| Astra Linus Directory Pro | A software package based on the Astra Linux OS, designed for centralized management of objects of organizations of various sizes |
| Attachment | File attached to the intercepted event at any nesting level. See also: Event |
| Audit | Controlling of actions fulfilled by Management Console users: creating and managing the security schema, System administrating. See also: Audit log, Management Console accounts |
| Blanks | Technology of searching the filled blanks of forms: questionnaires, receipts, etc. Blanks are stored in the System as digital prints, their text is not available for viewing to either users or System administrators. See also: Technologies, Technology element |
| Case sentive | Term setting: if the term is case-sensitive, the text search will detect only word forms which completely match upper- and lower-case letters defined in a term. See also: Term |
| Catalogs of persons, computers, and groups | Information about users, workstations, groups of users, and groups of computers imported from the Directory Service or created using Management Console. Used to simplify work with the events information. |
| Categories and terms | Technology of searching the words and phrases in the event text. The event where the term is found is referred to the category which this term belongs to. Old synonyms: Classifier, CFB. See also: Event, Term, Category, Technologies, Protected object |

| Term | Glossary |
| --- | --- |
| Category | Named term group characterizing some theme. If the System detects any term from the category in the text of the intercepted event, it associates the event with this category. See also: Term |
| Citation index | A measure of how close the sample document matches the text of the document being analyzed. See also: Sample document, Quote |
| Computer | A managed computer: workstation or terminal device. See also: Workstation, Terminal device |
| Configuration | A group of settings required to check events for data monitoring and analyzing. See also: Event, Technologies, Lists, Policy |
| Configuration version | A fixed state of the configuration designed to monitor changed settings of the event analysis. The configuration version is committed after uploading to a host. The configuration version can be active (currently used), editable (the last version with up-to-date modification) and saved (having changes and editable for users). See also: Configuration |
| Consul agent | Consul cluster member. It can be server or client. |
| Controlled persons | Set of persons, groups of persons and person's statuses which detection in the event results in associating this event to the person control policy which defines this set. See also: Persons, Person group, Person status, Person control policy |
| Copy mode | One of IW TM transport modes. In this mode, the actual traffic does not pass through the System. The copy of traffic is analyzed. In this mode, the traffic cannot be filtered by the System. See also: Transport mode |
| Copy rule | The rule that regulates copying and printing protected data. See also: Rule, Protected data, Data protection policy |
| Corporate security policy | A set of technical, organizational, administrative, legal, and physical measures, methods, rules, and guidelines that cover all security aspects in a company |
| Dashboard | Management console section that displays on widgets the statistical information on the violations and violators. See also: Management Console, Widget, Violation |
| Data interception | A process of acquiring, parsing, categorizing, and converting data (or a copy) into context. It is possible to intercept data transferred using the following protocols: SMTP, HTTP, Skype, ICQ/OSCAR, IXP, XMPP, MMP, FTP. See also: Interceptor, Event context |

| Term | Glossary |
| --- | --- |
| Data interception channel | A data interception environment that includes technical appliances, software tools, and communication protocols. The System supports the following data interception channels: email (SMTP, IMAP, and POP3), Web (HTTP), instant messaging services (ICQ and Skype), shadow copies of files, connected/disconnected workstation events, and print jobs. |
| Database | A collection of data stored in accordance with a data scheme. Contains all information needed for the System. |
| Database unloadings | Technology of searching the quotes the database. Database unloadings may be lists of salaries, other personal data, etc. See also: Technologies |
| Decision | The security officer's conclusion on whether the event violates the corporate security policy or not. Possible values: "No decision", "Violation:" and "No violation". See also: Security officer, Corporate security policy, Event, Event attributes, Violation, Policy, Verdict |
| Delivery status | Event attribute that specifies the possibility of event delivery to recipients after the analysis. If the event delivery has been allowed, then the attribute value represents the delivery tracking (completed or failed). See also: Event attributes |
| Digital print | A method of storing a sample document in the database in the form of a set of quotes. See also: Sample document, Quote |
| Document shadow copy | A copy of printed document received from the print job initiated on the managed computer. See also: InfoWatch Device Monitor |
| Domino Directory | IBM Lotus Domino Directory is a directory of information about users, servers, and groups. The Domino Directory is also a tool that administrators use to manage the Domino system. |
| Event | Objects of traffic interception (SMTP and IMAP and POP3 mail, HTTP requests, ICQ and Skype messages), shadow copies of files and print jobs. Generated by the System as a result of the data exchange between employees and others, including publication in media, copy to external devices and printing. |
| Event analysis | The procedure of processing of the attributes, attached files, and text of the intercepted events and of assigning additional attributes to the event. See also: Event, Policy, Event attributes |
| Event attributes | Structured data extracted from the events and assigned according to the processing results. See also: Event, Policy, Verdict, Decision, Transport mode |

| Term | Glossary |
| --- | --- |
| Event context | Internal representation of an intercepted event in the System. XML data (attributes, text) extracted from the event and its attachments. After processing the analysis results and the decision are added to the context. See also: Event, Technologies, Decision |
| Event text | Text information extracted from the event body and its attachments. Contains no formatting or markup. Is used for analysis and search. See also: Event, Event body |
| File shadow copy | A copy of file recorded to a removable device.The copy is created only if the file is successfully saved on the removable storage device. See also: InfoWatch Device Monitor |
| File signature | A constant integer value that uniquely identifies a file of a certain type. |
| FreeIPA | An open-source set of components for centralized management of users, their groups, hosts, authentication and authorization in Linux systems |
| FTP | File Transfer Protocol is a network protocol used to transfer computer files from one host to another host over a TCP-based network, such as the Internet. |
| Graphical object | Technology of searching the images (passports, bank cards, etc) in the text and attachments of the intercepted events. See also: Technologies, Event, Protected object |
| Group of persons and computers | Group aggregating data on organization's users and computers and on external contacts. The groups can be AD Groups (imported from Active Directory), Samba DC groups (imported from Samba DC), DD groups (imported from Domino Directory), ALD groups (imported from Astra Linux Directory), ALD Pro groups (imported from Astra Linux Directory Pro), FreeIPA groups (imported from FreeIPA) or TM Groups (created using Traffic Monitor). See also: Person, Computer, Contact |
| GTalk | Google Talk is an instant messaging service that provides both text and voice communication. |
| Headers | Supplemental data placed at the beginning of a block of data being stored or transmitted. Used for creating the event entity in the System and for determining the attribute values of this event. See also: Event, Event attributes |
| HTTP | HyperText Transfer Protocol, an application-tier protocol used to transfer the data in the text format. See also: HTTPS, HTTP(S) Monitor |

| Term | Glossary |
| --- | --- |
| HTTP query | A request formed according to the HTTP standards (POST request, GET request etc.) See also: HTTP, Event |
| HTTPS | Hypertext Transfer Protocol Secure is a network protocol for secure communication over a computer network. See also: HTTP, HTTP(S) Monitor |
| ICAP | Internet Content Adaptation Protocol is a lightweight HTTP-like protocol that allows you to control the incoming and outgoing HTTP traffic. It also makes it possible to modify the content of the HTTP requests. |
| ICQ | An Internet instant messaging service. Uses OSCAR protocol. |
| ICQ message | A message sent through the ICQ-OSCAR protocol. See also: Event |
| IMAP | Internet Message Access Protocol is a protocol for e-mail retrieval and storage |
| InfoWatch Device Monitor | IW DM is software appliance designed to control the user access to peripherals and to monitor operations (data either copied to removable media and network storages or sent to print, network activity, applications usage) and intercepting messengers traffic (Skype, Gtalk and Jabber) and so on. |
| InfoWatchTraffic Monitor | IW TM software suite is designed to control various types of traffic (SMTP, IMAP, POP3, HTTP, HTTPS, IMAP, XMPP, ICQ, NRPC) and shadow copies of the data copied to the removable media and sent to printing. |
| Initiators | A person whose actions led to the event creation |
| Inline mode | IW TM system deployment mode which may block mail outgoing from the perimeter, followed by dispatching. IW TM Server is used as a relay server. |
| IW Lync Adapter | Interceptor of data communication events through MS Lync servers installed in the company infrastructure. |
| Jabber | Messaging and information exchange system based on the open XMPP protocol. |
| LAN | Local Area Network |

| Term | Glossary |
| --- | --- |
| License | Right to the System usage. Gained when buying the System and defines available users number, used technologies and interceptors and so on. See also: Technologies, Interceptors |
| Lists | Lists the similar data generated by Management Console to be used in policies creating. See also: Configuration, Policy |
| Lotus Adapter | Interceptor installed on the IBM Lotus server to redirect emails to IW TM for analysis. See also: Interceptor |
| Lotus Domino | IBM mail server which messages are intercepted by Lotus Adapter. |
| Management Console | A graphical user interface. Designed to manage InfoWatch Traffic Monitor (administration, configuring settings, event analysis, etc.). |
| Management Console (DM) | GUI element. It is designed to control InfoWatch Device Monitor (system administration, security schema configuration, etc.) |
| Management Console user | User who manages the System. Each user has a role assigned basing on corporate security policy. |
| MAPI | Messaging Application Programming Interface is a messaging architecture and a Component object model based API for Microsoft Windows |
| Mask | A search pattern of characters and wildcards used to match folder and file names. |
| Monitor | See: Interceptor |
| Morphology | Term setting: if morphology is used, the text search will detect all word forms of this term. See also: Term |
| MS Lync | Microsoft instant messaging clients for corporate environments. |
| MTProto | A cryptographic protocol used in the messaging system to encrypt user correspondence |
| Normal transport mode | A traffic analysis and filtering mode. In this mode, it’s possible to block the traffic forbidden by the System can be blocked. See also: Transport mode, Inline mode |
| Notification | E-mail sent in case if the policy triggers on the event. Is sent via Management Console to notify Management Console users, employees or third parties. Contains a summary on the intercepted events and attached message. See also: Policy, Event |

| Term | Glossary |
| --- | --- |
| Occurrence threshold | A number of text objects found in the event enough to detect the protected object where this occurrence threshold is defined. See also: Event, Text objects, Protection object |
| Perimeter | A container of company infrastructure elements and contact information. The perimeter is used to logically divide a company into structural elements and track the traffic of every element. See also: Group of persons and computers |
| Person | Account of employee or external contact that is contained in System catalog and allows to process the data belonging to this account as a whole and to user-friendly display data referring to it. See also: Group of persons and computers |
| Persons control policy | A policy to add rules controlling persons, person groups, and person statuses. See also: Policy, Person control rule, Person, Person status |
| Persons control rule | Rule that assigns attributes to the event of specified violation level and which senders or recipients contain persons specified in the policy which includes this rule. Allows to re-assign person's status and to send notifications. See also: Rule, Event attributes, Person, Violation level, Person status, Notification, Person control policy |
| Placement rule | The rule that regulates storing protected data. See also: Rule, Protected data, Data protection policy |
| Policy | A set of rules according to which the event analysis and processing facilities are performed. See also: Policy, Active policy, Rule |
| Policy (DM) | A set of file monitoring rules for removable devices, network activity, printing, configuring peripherals access level etc. You can only assign security policy to a group (of employee or workstations.) See also: Rule (DM) |
| POP3 | Post Office Protocol Version 3 is an application-layer network protocol used by local e-mail clients to retrieve e-mail from a remote server over a TCP/IP connection |
| POST query | A query method designed to request that a web server accepted the data enclosed in the request message body for storage. Often used for file downloading of filled web-form representing |
| Privilege | Entity defining user’s ability to perform some action (set of actions) when managing the System |

| Term | Glossary |
| --- | --- |
| Protected data | A set of protected objects, their catalogues and file formats which detection in the event allows to characterize this event as fallen under the data protection policy where this set is defined. See also: Protected object, File format, Data protection policy |
| Protected object | The set of technology elements whose presence in the event allows the System to determine that this event belongs to a particular type of business documents (catalogue of protected objects). Protected objects are used in defining of data protection policies. See also: Technology element, Data protection policy |
| Proxy Server | The service that allows indirect requests to other network services. Proxy forwards all requests of the client programs to the network, and, having received the reply, sends it back to the client. |
| Quotation threshold | A percent of the sample document found in the even as quotes, enough to associate the event with this sample document. See also: Event, Sample document, Quote |
| Quote | A quote from the sample document found in the event text. See also: Sample document |
| Reference hash sum | Unlike the current hash sum, keeps the representative state of System files. See also: Integrity control |
| Relay server | A server which allows anyone on the Internet to send e-mail through it, not just mail destined to or originating from known users. |
| Report | Selection providing a visual display of event statistic data. See also: Management Console, Event |
| Rule | Entity defining System’s actions in the response to any actions which persons do with secured data.A rule is a set of conditions to test the event with and actions performed when those conditions are fulfilled or not. See also: Event, Policy, Protected object, Person control rule, Copy rule, Transfer rule, Placement rule |
| Rule (DM) | Set of restrictions and conditions that monitor file operations on removable devices, network activity, printing, configure access to managed peripherals etc. Each interceptor features a separate rule type. A rule can be only applied within its policy. See also: Policy (DM) |
| Samba DC | Free software implementation of the SMB network protocol. Provides file and print services for various Microsoft Windows clients |

| Term | Glossary |
| --- | --- |
| Sample documents | Technology of searching the quotes from sensitive documents: memos, financial reports, contracts, and others. Sample documents are stored in the System as digital prints, their text is not available for viewing to either users or System administrators. See also: Technologies, Technology element, Digital print, Quote |
| Security officer | A basic user of the Management console. Also - pre-installed role of the Management Console user that has privileges for all the actions in the system except administrative. See also: Management Console, User, User role, Privilege, Administrator |
| Skype | A voice-over-IP service and instant messaging client |
| SMB | Server Message Block operates as an application-layer network protocol mainly used for providing shared access to files, printers, serial ports, and miscellaneous communications between nodes on a network. |
| SMTP | Simple Mail Transfer Protocol is a networking protocol used to send the email in TCP/IP networks. |
| S/MIME | A standard for public key encryption and signing of MIME data |
| SMTP mail | An e-mail formed according to SMTP standards. See also: SMTP, Event |
| SPAN | Switched Port Analyzer is a technology that allows to mirror the network traffic from one port to another |
| SPAN copy | A variety of the “Copy” transport mode. In this case the traffic passes through a CISCO switch. The copy of the traffic is sent to Traffic Monitor Server for analysis. See also: SPAN |
| SSL | Secure Sockets Layer is a cryptographic network protocol developed for transmitting private documents via the Internet. |
| Status | Characteristics of persons and computers allowing to divide them onto groups for convenient analysis and activity control and to display them on dashboards and reports with special colour indicating. See also: Persons, Computers, Dashboard, Report |
| Stop word | Numbers, letters and words, whose presence in cells do not trigger these cells. Stop words are used to eliminate false triggering. |
| Tag | The text label giving a brief description of the event. See also: Event attributes |

| Term | Glossary |
| --- | --- |
| Technologies | Set of analysis tools searching for defined elements in the events' context and adding characterizing attributes to the event. See also: Technology element, Event context, Categories, Terms, Sample documents, Blanks, Database unloadings, Text objects, Graphical objects |
| Technology element | A part of the System technologies settings. Samples of confidential data. Can be categories and terms, sample documents, blanks, database unloadings, text and graphical objects. See also: Technologies, Categories and terms, Sample documents, Blanks, Database unloadings, Text objects, Graphical objects, Protected object. |
| Telegram | A messenger for smartphones which allows you to sent text messages, images, audio and video files; uses MTProto protocol |
| Term | One of the set of words and phrases together defining a topical area. See also: Category |
| Term Weight | How the term is characterized for the given category; an integer between 1 and 10. If a term with a higher weight is detected in event, then this event will be more likely associated with the category of this term. See also: Term |
| Text object pattern | Unified description of all possible text objects with the typical structure: passport numbers, credit card numbers, phone numbers, medical codes etc. See also: Text objects |
| Text objects | Technology of matching the data from the events' text with defined patterns (rules of generating bank card numbers) . See also: Technologies, Event, Technology element, Text object pattern |
| Transfer rule | The rule that regulates sending and receiving protected data. See also: Rule, Protected data, Data protection policy |
| Transport mode | Event attribute that defines the level of control when the object is delivered to the recipients. Assigned by the analysis and decision engine during the object analysis. Together with the "Verdict" attribute determines if the object can be delivered further on. See also: Event attributes, Verdict, Copy mode, Normal transport mode, Delivery status |
| User | IW TM users: administrator, security officer etc. See also: Administrator, Security officer, Person |
| User interface | The complex of tools and methods by means of whose the user interacts with the system. |

| Term | Glossary |
| --- | --- |
| User role | A set of privileges that define a set of actions available for the user. See also: Administrator, Security officer, Management Console, Privilege |
| Verdict | An event attribute with the conclusion about the presence (or absence) of violations in an event. Together with the Transport Mode attribute determines if the event can be delivered further on. See also: Event, Transport mode, Delivery status, Event attributes |
| Verdict reason | Event attribute that describes the reason why a certain verdict was assigned to the event. See also: Event attribute, Verdict |
| Violation | The value of the «Decision» attribute; means that the corporate security policy has been violated. See also: Decision, Corporate security policy |
| Violation level | Event attribute indicating (by the colour tag) the level of threat to corporate security policy. See also: Event, Event attributes, Violation |
| Visibility scope | The way to divide intercepted events to restrict Management console user access to them. Events satisfying criteria of some visibility scope will be visible to those users who have an access to this scope only (given that user has privileges to view or/and manage events). See also: Event, Privilege |
| Widget | Interface element in the form of an isolated area that displays the specified statistic information on violations and violators. See also: Management console, Violation, Violator |
| WhatsApp | A messenger for smartphones which allows you to sent text messages, images, audio and video files; uses its own protocol |
| Workstation | Computer type: desktop or notebook with OS of Windows or Linux or Mac family. See also: Computer |
| XMPP | Extensible Messaging and Presence Protocol is a communications protocol for message-oriented middleware based on XML. |