

INFOWATCH

InfoWatch Traffic Monitor 6.7

User Guide

10/01/2018

© JSC “InfoWatch”

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

http://www.infowatch.com

TABLE OF CONTENTS

1 InfoWatch Traffic Monitor Overview 10
1.1 Object Interception 12
1.2 Object Analysis and Verdict 13
1.3 Retrospective Data Analysis, User Decision on an Object 16
1.4 InfoWatch Traffic Monitor Transport Modes 16
1.5 Uploading Object to Database 17
1.6 Specific Features of Blocking HTTP-queries and Messages Sent through Web Services. 17
1.7 InfoWatch Device Monitor Functions 18
1.7.1 Operation in Safe Mode 20
2 Traffic Monitor Management Console: General Information 22
2.1 System Operation Before Configuring 23
2.2 Configuring the System 23
2.3 Displaying Actual Data in Management Console 25
3 Interface of Traffic Monitor Management Console 27
3.1 Dashboard Section 29
3.1.1 Dashboard widgets 30
3.1.1.1 Dynamics of violations over the period 31
3.1.1.2 Top violators 31
3.1.1.3 Quantity of violations over period 32
3.1.1.4 Selection 33
3.1.1.5 Dynamics of statuses 34
3.1.1.6 Policy statistics 34
3.1.1.7 Statistics on protected objects 35
3.1.1.8 Statistics on catalogues of protected objects 36
3.1.2 Dashboard report 37
3.2 Events Section 38
3.2.1 Queries 39
3.2.1.1 Standard Mode of Creating Queries 40
3.2.1.2 Advanced Mode 45
3.2.1.3 Search on the Event Text 46
3.2.2 Object Interception 48
3.2.2.1 Event tile 50
3.2.2.2 Brief Event Viewing Form 51
3.2.2.3 Detailed Event Viewing Form 53

3.2.3 Contact Identification in Event 55
3.3 Reports Section 56
3.3.1 Report Creation Form 58
3.3.2 Widgets of Reports 58
3.3.3 Queries 60
3.4 Technologies section 62
3.4.1 Categories and terms 62
3.4.1.1 Categories 63
3.4.1.2 Terms 63
3.4.2 Text Objects 64
3.4.2.1 Text objects patterns 65
3.4.3 Sample Documents 67
3.4.4 Blanks 68
3.4.5 Stamps 69
3.4.6 Database Unloadings 70
3.4.6.1 Automatically Updated Database Unloadings 71
3.4.7 Graphical Objects 73
3.5 Protected Objects Section 74
3.5.1 Elements of Technologies 75
3.5.2 Detection Conditions 76
3.6 Persons Section 77
3.6.1 Persons 78
3.6.2 Computers 80
3.6.3 Screenshots 80
3.7 Policies Section 81
3.7.1 Rules and their Viewing Form 82
3.7.1.1 Rule of Transfer 85
3.7.1.2 Rule of Copying 87
3.7.1.3 Rule of Placement 89
3.7.1.4 Clipboard Rule 90
3.7.1.5 Person Control Rule 92
3.8 Lists Section 93
3.8.1 Tags 93
3.8.2 Web Resources 94
3.8.3 Statuses 95
3.8.4 Perimeters 95
3.8.5 File Types 97
3.9 Crawler Section 98
3.9.1 Scanner 100
3.9.2 Scanning Job 101
4 Cases Solving in Traffic Monitor Management Console 106

4.1 Typical Actions 106
4.1.1 Login to the Management Console 107
4.1.2 Applying System Configuration 107
4.1.3 Editing Element 108
4.1.4 Deleting Element 108
4.1.5 Pages Navigation 109
4.1.6 Changing User Password 109
4.1.7 Selecting Interface Language 110
4.1.8 Calling Help File 110
4.1.9 Viewing Information on System 111
4.2 Managing Persons and Computers 111
4.2.1 Creating Group of Persons or Computers 112
4.2.2 Creating Persons and Computers 113
4.2.3 Configuring Person's Card 114
4.2.3.1 Adding Contact to Person 114
4.2.3.2 Adding Computer to Person 115
4.2.3.3 Adding Person to Group 115
4.2.4 Configuring Computer Card 116
4.2.4.1 Adding Contact to Computer 116
4.2.4.2 Adding Person to Computer 116
4.2.4.3 Adding Computer to Group 117
4.2.5 Adding Status to Persons 117
4.2.6 Viewing Screenshots 118
4.3 Managing Catalogs 120
4.3.1 Managing Tags 121
4.3.2 Managing Web Resources 121
4.3.3 Managing Statuses 122
4.3.4 Managing Perimeters 123
4.4 Managing Base of Technologies 126
4.4.1 Defining the Confidential Information 126
4.4.1.1 Managing Categories and Terms 128
4.4.1.2 Managing Text Objects 130
4.4.1.3 Managing Sample Documents 132
4.4.1.4 Managing Blanks 134
4.4.1.5 Managing Stamps 136
4.4.1.6 Managing DB Unloadings 137
4.4.2 Exporting and Importing the Base of Technologies 141
4.5 Managing Protected Objects 142
4.5.1 Creating a Catalog of Protected Objects 143
4.5.2 Creating a Protected Object 144
4.5.3 Adding Elements of Technologies 147
4.5.4 Adding Detection Conditions 148

4.5.5 Creating Policies for Protected Objects and Their Catalogs ... 149
4.5.6 Import and Export of Protected Objects ... 150
4.5.7 Activating and Deactivating Protected Objects ... 151
4.6 Managing Crawler Subsystem ... 151
4.6.1 Configuring Scanner ... 152
4.6.2 Creating a Job ... 153
4.6.3 Launching and Stopping the Job ... 154
4.6.4 Editing the Job ... 154
4.6.5 Cleaning the Hash Base ... 154
4.6.6 Viewing Launch History ... 155
4.6.7 Saving Scan Report ... 156
4.7 Managing Interception Objects ... 156
4.7.1 Viewing summary on violations/violators ... 157
4.7.1.1 Creating Dashboard ... 158
4.7.1.2 Creating and configuring widget ... 158
4.7.1.3 Creating dashboard report ... 160
4.7.1.4 Viewing dashboard report ... 161
4.7.2 Viewing Events ... 162
4.7.2.1 Creating queries ... 162
4.7.2.2 Choosing Event Fields of View ... 168
4.7.2.3 Viewing Brief Event Form ... 169
4.7.2.4 Viewing Detailed Event Form ... 170
4.7.3 Making Decision on Object ... 170
4.7.4 Adding and Deleting Tags ... 171
4.7.5 Saving Events (for SMTP mail) ... 171
4.7.6 Event Export ... 171
4.7.7 Dispatching a Quarantined Event ... 172
4.8 Configuring System Response ... 173
4.8.1 General Information on Policies ... 174
4.8.2 Preset Policies ... 181
4.8.2.1 Data Protection Policy ... 181
4.8.2.2 Person Control Policy ... 182
4.8.2.3 Policy that Regulates Transferring Password-Protected Data ... 183
4.8.2.4 Policies that Regulate Visiting Web Resources ... 183
4.8.2.5 Policy that Excludes Mailing Lists from Interception ... 186
4.8.3 Creating Data Protection Policy ... 186
4.8.3.1 Examples of using data protection policy ... 187
4.8.4 Creating Data Protection Policy on Agents ... 191
4.8.5 Creating Person Control Policy ... 192
4.8.6 Editing Policy ... 194
4.8.7 Creating Rules ... 194
4.8.8 Editing Rules ... 196
4.8.9 Determining System Response to Policy Violations ... 196

4.8.10 Determining System Default Response ... 198
4.8.11 Filtering the List of Policies ... 199
4.8.12 Sending Notifications on Responded Rule ... 200
4.8.13 On Data Protection Policy on Agents ... 201
4.8.14 On Data Protection Policy ... 201
4.8.15 On Person Control Policy ... 202
4.9 Managing Reports ... 202
4.9.1 Examples of using reports ... 203
5 Using Device Monitor Management Console ... 208
5.1 Management Console (DM) Overview ... 208
5.1.1 Authorization and Connecting to InfoWatch Device Monitor Server ... 208
5.1.2 Management Console (DM) Main Screen ... 209
5.1.2.1 Configuring Management Console (DM) Main Screen Elements ... 211
5.1.3 Management Console (DM) Sections ... 211
5.2 Managing Console (DM) Accounts ... 212
5.2.1 Viewing Management Console (DM) account details ... 214
5.2.1.1 Adding New Management Console (DM) Account ... 215
5.2.1.2 Editing Management Console (DM) Account ... 218
5.2.1.3 Locking or Unlocking Management Console (DM) Account ... 218
5.2.1.4 Deleting Management Console (DM) Account ... 219
5.2.2 Roles of DM Console users ... 219
5.2.2.1 Adding role of the Management Console (DM) user ... 220
5.2.2.2 Editing role of DM Console user ... 223
5.2.2.3 Deleting role of DM Console user ... 224
5.2.3 Management Console (DM) Security Schema Operation Activity Log ... 224
5.2.3.1 Viewing Audit Log ... 224
5.2.3.2 Log Records Filtering ... 227
5.2.3.3 Deleting Records from Log ... 231
5.2.3.4 Exporting Log Records ... 231
5.2.3.5 Analyzing Log Records in Microsoft Excel ... 231
5.3 General System Settings ... 232
5.3.1 Common Settings for Agents ... 232
5.3.2 Settings of Corporate Network ... 235
5.3.3 Network Traffic Control ... 237
5.3.3.1 Processing Addresses Added to Exclusions ... 239
5.3.4 Device Monitor Server Settings. Connecting to Traffic Monitor Server ... 241
5.3.5 Connecting to LDAP Server and synchronization with Active Directory and Astra Linux Directory ... 242
5.3.6 Employee Notifications about Policy (DM) Violations ... 246
5.3.7 Exclusion of Application from Interception ... 248
5.3.8 Application Control ... 251
5.3.9 Event Storage ... 252
5.3.10 Synchronization of Traffic Monitor Policies ... 253

5.3.11 InfoWatch Device Monitor Server Manager 254
5.3.12 Stopping and Starting Device Monitor Agent 255
5.3.12.1 Stopping agent remotely/starting agent 256
5.3.12.2 Stopping/starting agent locally 257
5.4 Managing Security Schema 257
5.4.1 Security Schema Organization 258
5.4.1.1 Security Policies (DM) and Rules (DM) 258
5.4.1.2 Employees and Employee Groups 260
5.4.1.3 Computers and computer groups 260
5.4.1.4 Uploading security scheme to managed computers 261
5.4.2 Security Scheme Overview 261
5.4.2.1 Viewing Active Security Scheme 261
5.4.2.2 Viewing Old Security Scheme 262
5.4.2.3 Security Scheme Comments 264
5.4.2.4 Editing Security Scheme 265
5.4.2.5 Updating Security Scheme 266
5.4.2.6 Exporting/Importing Security Scheme 267
5.4.3 Security Schema Setup 268
5.4.3.1 Security Policies (DM) 269
5.4.3.2 Rules (DM) 273
5.4.3.3 Employees 306
5.4.3.4 Computers 314
5.4.3.5 Mobile Devices 324
5.4.3.6 White Lists 332
5.4.3.7 Signatures 339
5.4.3.8 Application Protocol 341
5.4.4 Temporary employee access to network 346
5.4.5 Temporary Employee Access to Devices 347
5.5 Viewing DM Events 349
5.5.1 Event Filters 357
5.5.2 Deleting Events 359
5.6 Agent Remote Installation, Updating and Uninstallation 359
5.6.1 Viewing Tasks 360
5.6.2 Preparing Primary Agent Installation. Distribution Agent 363
5.6.2.1 Enabling Shared Administrative Resources 363
5.6.2.2 Firewall Settings 364
5.6.3 Creating Primary Distribution Task 365
5.6.4 Creating Update Task 368
5.6.5 Creating Uninstallation Password Reset Task 370
5.6.6 Creating Uninstallation Task 371
5.6.7 Launching, Pausing, Editing, and Deleting Tasks 372
5.6.8 Agent Installation Errors 373

5.6.9 Creating Installation Package 374
5.7 Additional Features 376
5.7.1 Filter Table Contents 376
5.7.1.1 Filtering by Date 376
5.7.1.2 Applying Standard Filters 377
5.7.1.3 Custom Filter 378
5.7.1.4 Editing Filters 379
5.7.1.5 Removing a Filter 380
5.7.2 Grouping or Sorting Entries 380
5.7.3 Hotkeys 380
6 Licensing Information 384
6.1 End-User License Agreement 384
6.1.1 License Agreement 384
6.2 Third-Party Licenses 386
7 Glossary 388

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 (RHEL or Astra Linux).

InfoWatch Traffic Monitor Main Features:

- Interception of SMTP, IMAP and POP3 traffic. It is possible to intercept traffic (or the copy of traffic) passed by a mail relay server or the copy of the traffic that passes through the hardware with the CISCO SPAN.
- Interception of the HTTP and HTTPS traffic. It is possible to intercept either traffic passed through an ICAP-supporting proxy server or the copy of traffic that goes through the CISCO SPAN-enabled equipment.

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

- Intercepting a copy of ICQ traffic (the OSCAR protocol) passing through the equipment that supports the CISCO SPAN technology. When ICQ connects through HTTP, the System intercepts ICQ traffic similar to HTTP traffic.

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

- Reviewing files located in the corporative network (open network folders, workstation local discs, and SharePoint 2007/2010/2013 file storage) with the Crawler subsystem.
- Analyzing Skype traffic, shadow copies of files, print jobs, traffic transferred by HTTP, HTTPS and FTP protocols; receiving and transmitting mail via SMTP, POP3 and IMAP using MAPI interface, controlling data exchange via Jabber (XMPP protocol), WhatsApp (WhatsApp protocol) and SMS. Voice messages in Skype can also be intercepted. Interception of listed data is performed by InfoWatch Device Monitor system.
- Analyzing shadow copies of files intercepted by DeviceLock version 6.3 or higher (provided by SmartLine, Inc.).
- Intercepting and analyzing MS Lync objects via IW Lync Adapter installed on MS Lync server.
- Analyzing the contents of the intercepted traffic in order to detect violations of the corporate security policy.
- Filtering the intercepted traffic by allowing or blocking the delivery of certain data.

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

InfoWatch Traffic Monitor Components:

InfoWatch Traffic Monitor Component	Purpose
Traffic Monitor Server	Interceptors: **IW_SNIFFER**, **IW_ICAP,** and **IW_SMTPD**. **Analysis subsystem** receives event context and checks if the events contain technology elements and correspond to protected objects. **Policy applying subsystem** implements actions defined by the user according to the corporate security policy.
Database	Storage of information associated with the System operations (intercepted data and results of their analysis).
Device Monitor	Controlling user access to the peripherals, monitoring operations (data copying to removable storages and FTP, sending data to printing, using messengers) and intercepting the traffic from instant messengers.
Crawler	Checking files from the corporate network (open network folders, local disks of workstations, and SharePoint 2007/2010/2013 file storage).
Connectors	Integration with external systems, generating events.
Web Management Console	Configuring rules for analyzing and filtering traffic, analysis of intercepted data.

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

1.1 Object Interception

The System objects are the following:

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

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

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

MS Lync	The System receives a copy of traffic from IW Lync Adapter installed on MS Lync server
Files located in the corporate network	The System receives copies of files from the Crawler subsystem
Shadow copies of files and print jobs received from InfoWatch Device Monitor	The System receives a copy of traffic. Blocking user actions (print jobs, access to devices) can be performed only by means of InfoWatch Device Monitor
Shadow copies of files received from DeviceLock	The System receives a copy of traffic. Blocking user actions (access to devices) can be performed only by means of DeviceLock

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

1.2 Object Analysis and Verdict

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

IW TM subsystem	Subsystem modules	Subsystem/module features
Processing subsystem	SMTP and POP3 Processing module (copy mode), HTTP Processing module (copy mode), ICQ Processing module (copy mode), Shadow Copies Processing module, SMTP Processing module (blocking mode), HTTP Processing module (blocking mode).	Extracting significant data and enclosures from the object, defining the enclosure format, and forwarding the extracted texts to the Analysis subsystem.
Analysis subsystem	Linguistic Analysis module	Checking if the object text corresponds to any categories
	Text Objects Detecting module	Searching through the object text for specific text objects (e.g. credit card numbers)

	Digital Prints Detecting module	Searching through the object text for quotes from sample documents
	Blanks Detecting module	Searching through the object text for completed forms
	Stamps Detecting module	Searching through the object text for stamp images
	Database Unloadings Detecting module	Searching through the object text for quotes from a database
	Graphic Objects Detecting module	Searching through the object text and enclosures for images of particular classes
Policies Application subsystem	Active Directory, Domino Directory, and Astra Linux Directory Integration module	Providing the initial import and periodical synchronization of Active Directory, Domino Directory, and Astra Linux Directory structure with a list of users and workstations in Traffic Monitor for further binding this information with data from the intercepted objects.
	Decision-Making module	Ensuring corporate security policies by employing policy rules to the intercepted objects

The object analysis is performed in the following order:

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

> **Note:**
>
> For MS Office 2007 and 2010 document, the System also analyzes metadata specified in document properties (in the **Description** block of the **Details** tab).

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

Content analysis technology	**Technology description**

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

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

1.3 Retrospective Data Analysis, User Decision on an Object

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

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

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

Note:

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

1.4 InfoWatch Traffic Monitor Transport Modes

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

Warning!

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

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

Table 1

Transport mode	Description
Blocking	InfoWatch Traffic Monitor intercepts, analyses, and transports objects. In this mode, the verdict defines if the object will be delivered to recipients. Besides, in some cases, the delivery status of the SMTP messages can be changed after changing the user decision (see "Specific Features of Blocking HTTP-queries and Messages Sent through Web Services").

Copy	In this mode, the System receives copies of objects. The difference from the blocking mode is that the System does not participate in object transporting. Thus, the System performs the object analysis only. As the System analyses the copy of objects, the verdict and the analysis-based user decision do not impact the object delivery to recipients.

Table 2

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

1.5 Uploading Object to Database

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

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

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

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

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

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

Supported Web resources:

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

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

- blogspot,
- 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.

1.7 InfoWatch Device Monitor Functions

InfoWatch Device Monitor (further referred to as InfoWatch Device Monitor or the System) is a mean of managing access to your computer peripherals. Moreover, the System lets you monitor data that is being transferred from computer to removable devices, sent to a printer or over the network. Resulting data is analyzed by InfoWatch Traffic Monitor.

The main functions of InfoWatch Device Monitor System:

- realtime monitoring of managed computers (workstations and mobile devices)
- managing employee access to system peripherals (see "Configuring Device Monitor Rule (DM)")
- monitoring computer print operations (see "Configuring Photo Monitor Rule (DM)")
- supervising Instant Messengers: Skype, WhatsApp, Jabber (XMPP protocol) (see "Configuring IM Client Monitor Rule (DM)")
- supervising SMS of mobile communication (see "Configuring IM Client Monitor Rule (DM)")
- supervising traffic transferred by FTP and FTPS (see "Configuring FTP Monitor Rule (DM)")
- supervising traffic transferred by HTTP and HTTPS (see "Configuring HTTPS Monitor Rule (DM)")
- supervising data transferred by network connections beyond corporate network (see "Configuring Network Monitor Rule (DM)")
- supervising emails transferred by protocols (SMTP, POP3, IMAP, MAPI) (see "Configuring Mail Monitor Rule (DM)")
- supervising photographs made by cameras of mobile devices (see "Configuring Photo Monitor Rule (DM)")
- retrieving data from managed computers (workstations and mobile devices) (see "Configuring Device Monitor Rule (DM)")
- controlling files that are copied to network resources (see "Configuring File Monitor Rule (DM)")
- transferring retrieved data for InfoWatch Traffic Monitor analysis
- Microsoft RDP and Citrix ICA client control (see "Configuring Device Monitor Rule (DM)")
- cloud storage control (see "Configuring Cloud Storage Monitor Rule (DM)")
- screenshot control (see "Configuring ScreenShot Control Monitor Rule (DM)")
- application control (see "Configuring Application Monitor Rule (DM)")
- clipboard control (see "Configuring Clipboard Monitor Rule")
- event storage management (see "Events")

Note:

For workstations installed on Astra Linux, only the following control functions are available:

- controlling emails sent via SMTP and POP3 protocols (see "Configuring Mail Monitor Rule (DM)")
- controlling files that are copied to removable devices (see "Configuring File Monitor Rule (DM)")
- controlling traffic sent through HTTP and HTTPS (see "Configuring HTTPS Monitor Rule (DM)")

Note:

Some functions are available in both regular and safe mode of your operating system (see "Operating in Safe Mode").

User (employee) actions are observed and controlled on managed computers.
Managed computer is a workspace (workstation or mobile device) that gives you access to controlled files and peripherals.

Controlled files are files that must be monitored according to corporate security policy.

Monitored peripherals are system devices controlled by InfoWatch Device Monitor.

To monitor and control computers you need a Client module installed. Client module includes the following interceptors: **File Monitor, Print Monitor, Device Monitor, IM Client Monitor, FTP Monitor, HTTP(S) Monitor, Network Monitor, Mail Monitor, Application Monitor, Cloud Storage Monitor, ScreenShot Control Monitor, Photo Monitor**.

File Monitor controls writing operations on removable devices and registers successful operations. This lets you monitor the following actions:

- creating/editing files on removable devices;
- copying/moving files to removable devices. This tracks files copied/moved from managed computers, removable devices, or over network.

See more information on configuring interceptor rule in "Configuring File Monitor Rule (DM)" section.

Device Monitor controls access to system peripherals. Possible access levels depend on device type. See more information on configuring interceptor rule in "Configuring Device Monitor Rule (DM)" section.

Print Monitor enables monitoring printing operations on local and network printers. It creates a copy of print job and sends it to InfoWatch Traffic Monitor for analysis. See more details in "Configuring Print Monitor Rule (DM)" section.

IM Client Monitor controls access to instant messengers: Skype, Jabber (XMPP protocol). You can completely deny application usage or just make chat copy. Also, you can create shadow copies of transferred files, messages, and chats. See more details in "Network Traffic Control" and "Configuring IM Client Monitor Rule (DM)" sections.

FTP Monitor controls data exchange through FTP/FTPS protocol. You can restrict or completely deny the usage of FTP/FTPS protocol and create shadow copies of transferred files. See more details in "Configuring FTP Monitor Rule" section.

HTTP(S) Monitor controls data exchange through HTTPS protocol. The System is able to create shadow copies of transferred files. See more details in "Configuring HTTP(S) Monitor Rule" section.

Network Monitor enables deny of data transferring by any network connections except corporate ones or connections with specified allowed servers. See more details in "Network Traffic Control" and "Configuring Network Monitor Rule" sections.

Mail Monitor controls receiving and sending emails. The System allows you to completely deny sending and receiving emails or accept the receiving emails only or completely accept sending and receiving emails. See "Configuring HTTP(S) Monitor Rule"

Application Monitor controls employees access to applications launched on computers. See "Configuring Application Monitor Rule".

Cloud Storage Monitor controls data transfer through cloud storages web-clients. See "Configuring Cloud Storage Monitor Rule".

Clipboard Monitor control access of employees to the clipboard. See "Configuring Clipboard Monitor Rule (DM)".

ScreenShot Control Monitor controls screenshots on the client side. See "Configuring ScreenShot Control Monitor Rule".

Photo Monitor enables shadow copies of photos made by cameras of controlled mobile devices. See "Configuring Photo Monitor Rule".

All the created file copies are not stored in InfoWatch Device Monitor but transferred to InfoWatch Traffic Monitor for analysis.

1.7.1 Operation in Safe Mode

Some of InfoWatch features are still available in safe mode (with network features or without them). The following table lists the features available in safe mode.

InfoWatch Device Monitor Feature	Operating system mode
Managing access to peripherals (except devices that are unavailable in safe mode)	Safe Mode Safe Mode with Networking
Write control on removable devices	Safe Mode Safe Mode with Networking
Monitoring managed computers	Safe Mode with Networking
Managing access to instant messengers: Skype, Jabber (XMPP protocol) and Mail.Ru Agent (MMP protocol)	Safe Mode with Networking
Managing data exchange through FTP/FTPS protocol	Safe Mode with Networking
Managing data transfer by network connections beyond corporate network	Safe Mode with Networking

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:**
>
> This guide does not describe the administration process. For this information, please see "*Infowatch Traffic Monitor. Administration Guide*".

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 System response to employees' actions that violate the corporate security policy

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

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

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

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

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

Warning!

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

2.1 System Operation Before Configuring

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

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

  Warning

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

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

2.2 Configuring the System

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

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

Warning!

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

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



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

> **Note:**
>
> The configuration version that is used in Device Monitor is displayed in Device Monitor Console (see "Synchronization of Traffic Monitor Policies"). 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 a technology database (see "Managing the Base of Technologies"):
  - Selecting terms to be detected - *only when using Linguistic Analysis technology (see "Terms")*;
  - Selecting text object types to be detected - *only when using Detecting Text Objects technology (see "Text objects")*;
  - Selecting sample documents to be detected - *only when using Detecting Sample Documents technology (see "Sample Documents")*;
  - Selecting blanks to be detected - *only when using Detecting Blanks technology (see "Blanks")*;
  - Selecting stamps to be detected - *only when using Detecting Stamps technology (see "Stamps")*;
  - Selecting database unloadings to be detected - *only when using Detecting Database Unloadings technology (see "Database Unloadings")*;
  - Selecting graphical object types to be detected - *only when using Detecting Graphic Objects technology (see "Graphical objects").*
- Creating protected objects based on the elements of the base of technologies *(see "Protected objects")*.
- Creating catalogues of:
  - Persons and computers *(see "Managing Persons and Computers")*;
  - Tags *(see "Managing Tags")*;
  - Web resources *(see "Managing Resources Lists")*;
  - Statuses *(see "Managing Statuses")*;
  - Perimeters *(see "Managing perimeters")*;
- Creating policies according to which objects on the Traffic Monitor Server are checked *(see "Configuring System Response")*

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

- Protected objects that contain only categories and text objects

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

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



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

Warning!

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

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

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

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

Note:

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

2.3 Displaying Actual Data in Management Console

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

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

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

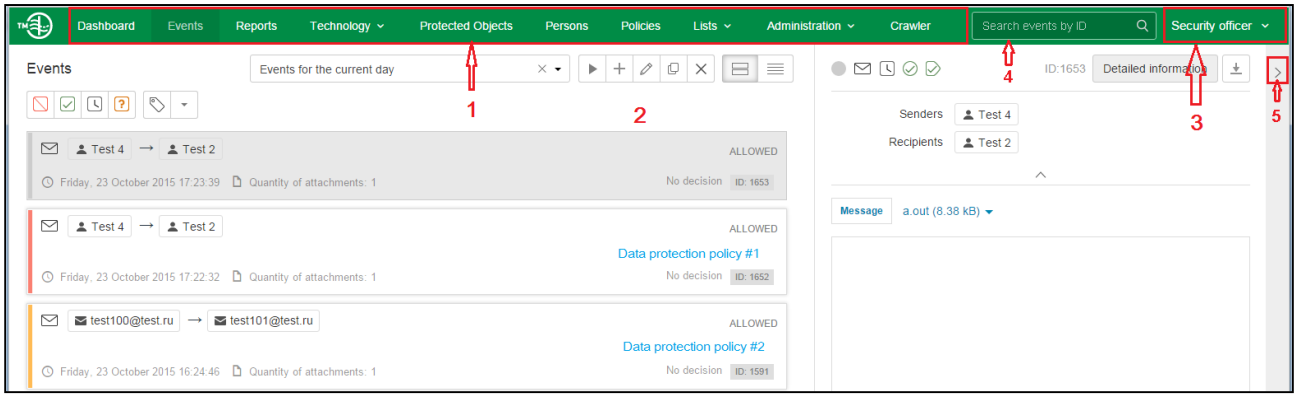
You can also update data manually in any section of the Management Console. To do this, use the standard browser refresh tool: by default the page is refreshed when you press the function key F5).

Note:

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

3 Interface of Traffic Monitor Management Console

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



Window elements of the Management Console:

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

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.

Operating the Management Console is performed in thematic sections:

Section	Purpose
Dashboard	Contains statistical information on violations/violators
Events	Contains a list of intercepted objects and tools for managing them
Reports	Contains a sampling of statistical data on intercepted objects
Technologies	Contains a description of analysis technologies being used (categories and terms, text objects, sample documents, etc.)
Protected objects	Contains a list of protected objects and tools for managing them
Persons	Contains a catalog of persons and workstations of the company IT system, and external contacts.
Policies	Contains the list of the alleged actions of employees and algorithm of the System responses
Lists	Contains editable catalogs of tags, statuses, and perimeters.
Administration	Operations performed in this section are described in *«Infowatch Traffic Monitor. Administration Guide»*
Crawler	Contains tools for creating, editing, and running jobs for the Crawler subsystem.

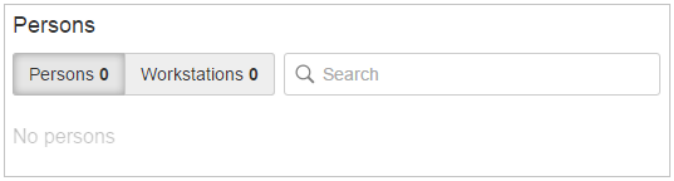
You can go to a specific section by clicking the section button.



Events section button

The following interface elements are used in the Management Console:

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



Persons section, **Persons** and **Workstations** tabs

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

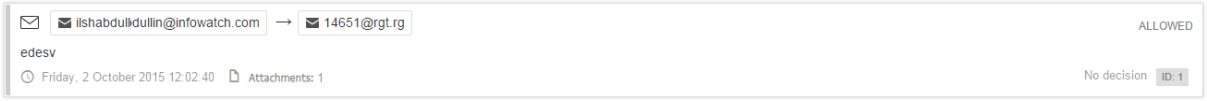
Note:

In the System, the *Panel* also refers to the entity of the Dashboard section (see “Раздел "Сводка"").



Toolbar

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



Events section, event tile

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

Note:

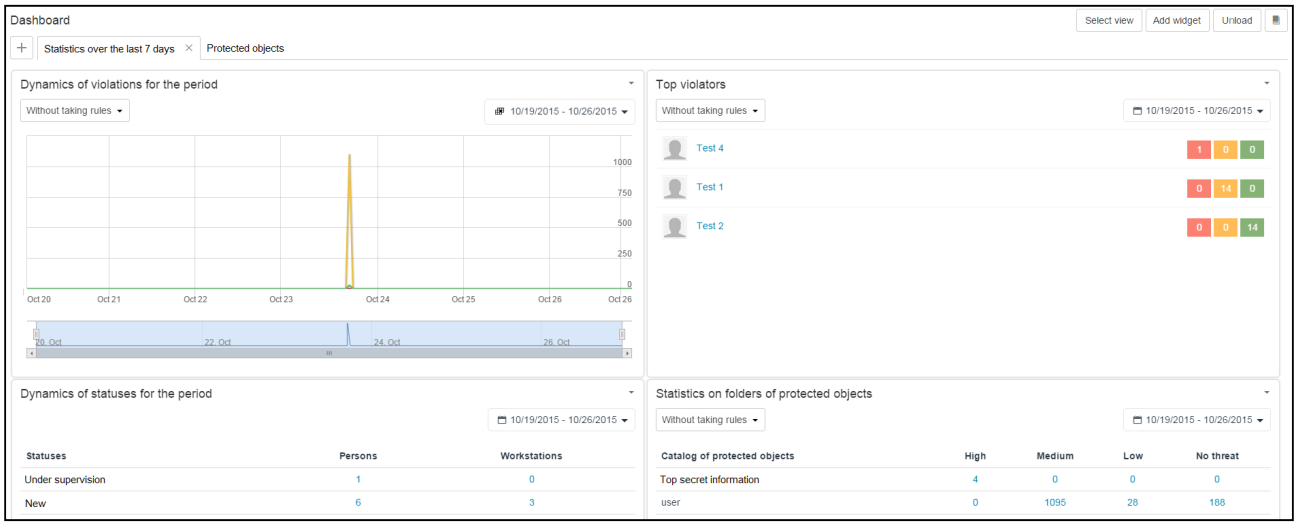
While downloading the requested data, the System may display a symbol like  or informational message.

3.1 Dashboard Section

About the section:

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

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



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

 - splitting into 3 equal parts

 - splitting in a ratio of 2:1

 - splitting into 2 equal parts

 - splitting in a ratio of 1:2

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

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

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

User's target actions:

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

3.1.1 Dashboard widgets

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

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

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

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

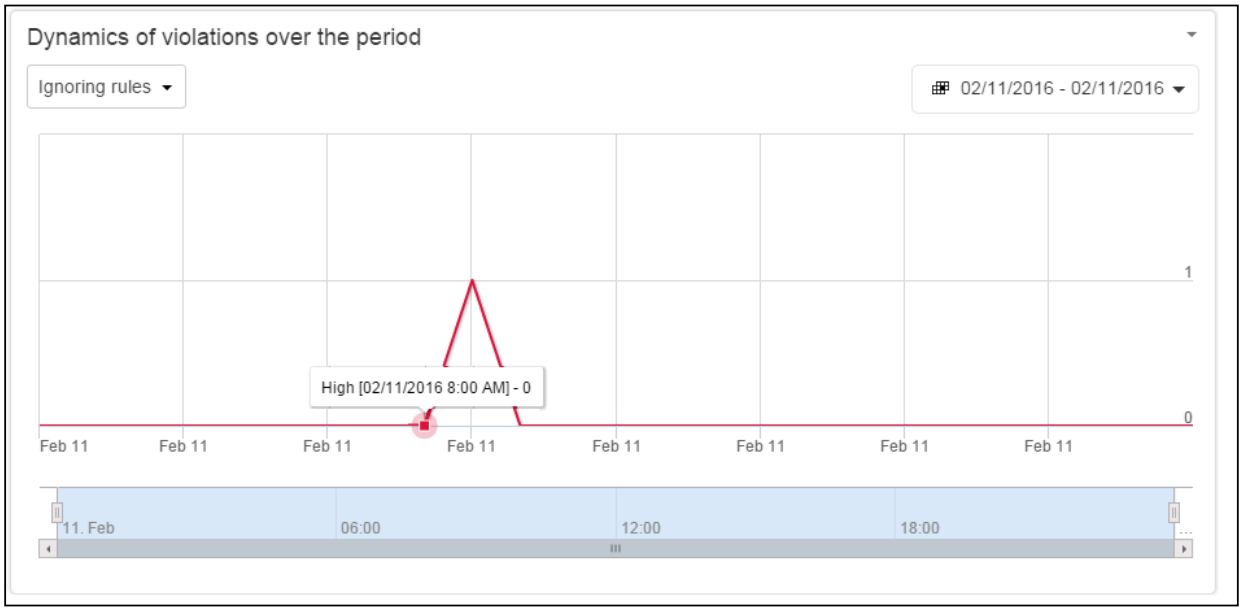
Statistics on protected objects	The number of violations per protected objects broken down by levels of violations over the selected time period
Statistics on catalogs of protected objects	The number of violations per catalogs of protected objects broken down by levels of violations over the selected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

User's target actions:

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

Dynamics of violations over the period

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



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

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

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

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

Top violators

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

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



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

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

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

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

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

You can edit the following parameters:

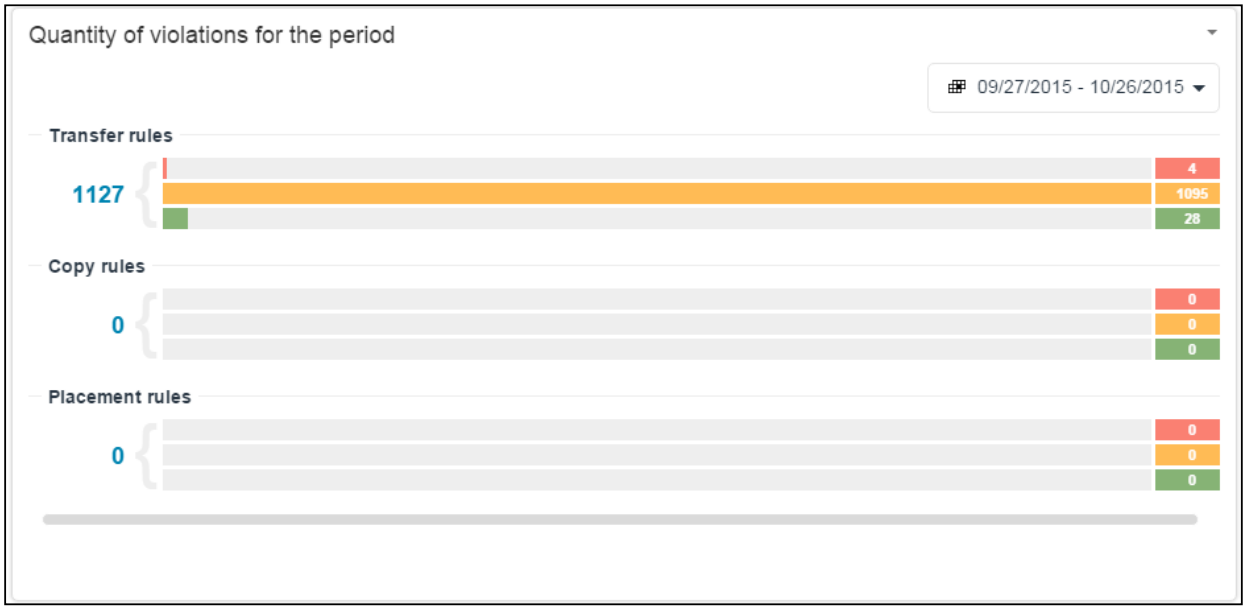
- **Name**;
- **Update interval** for data on the widget;
- **Quantity of violators** for which statistics will be displayed;
- **Groups** to which violation can belong. Statistics on the selected groups will be displayed in the widget. Start typing the group name or click + and select desired groups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

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

Quantity of violations over period

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

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



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

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

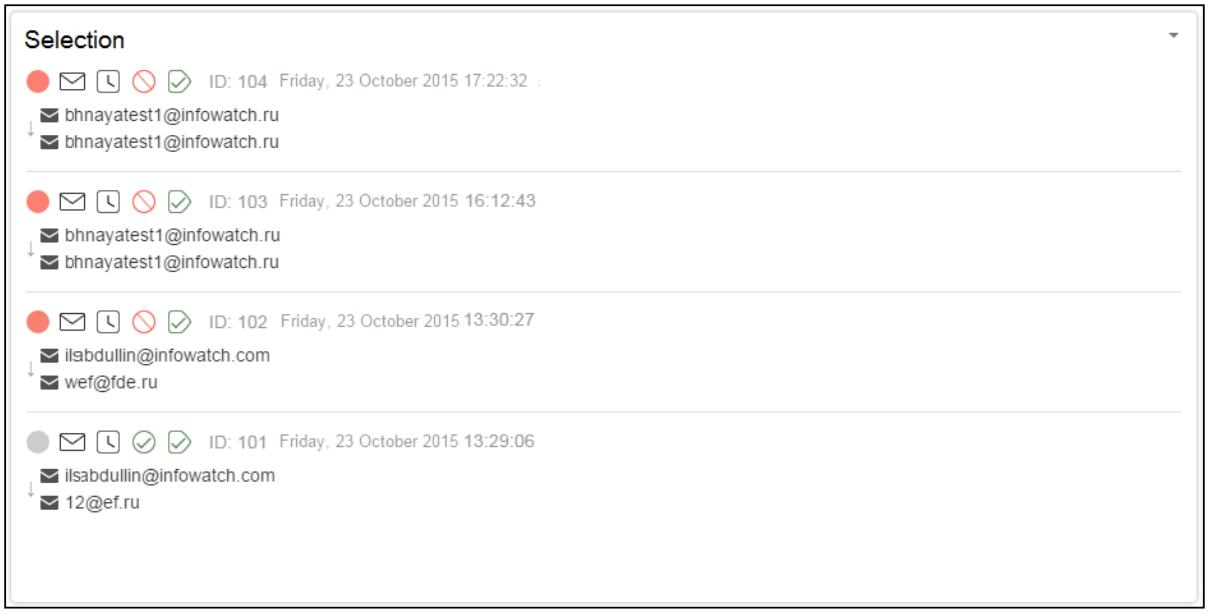
You can edit the following parameters:

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

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

Selection

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



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

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

You can edit the following parameters:

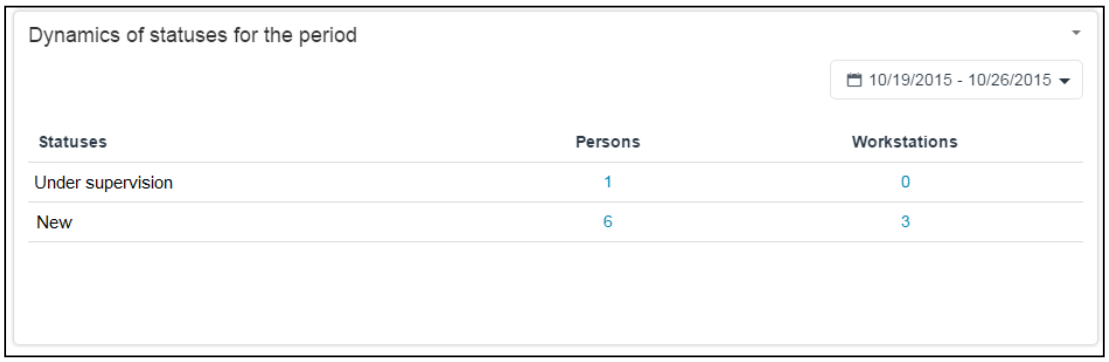
- **Name**
- **Update interval** for data on the widget
- **Selection** - a query that will be used for selection. Select a required request from the drop-down list (for details, see "Queries")
- **Events per page** - the number of events displayed on the page

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

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

Dynamics of statuses

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



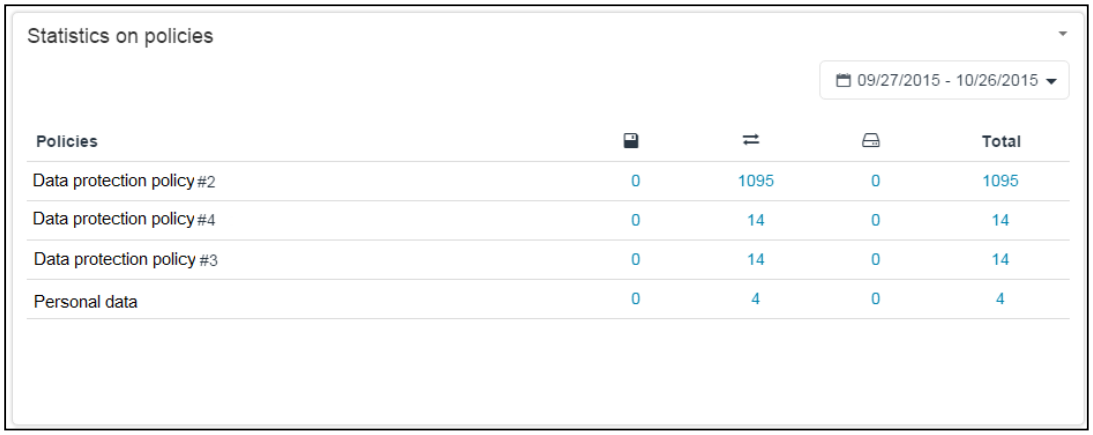
Clicking the number of persons or computers (highlighted in blue) opens the "Persons" section (the **Persons** or **Computers** tab respectively), where you can view the list of persons (or computers) that meet the conditions specified in the widget properties.

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**.

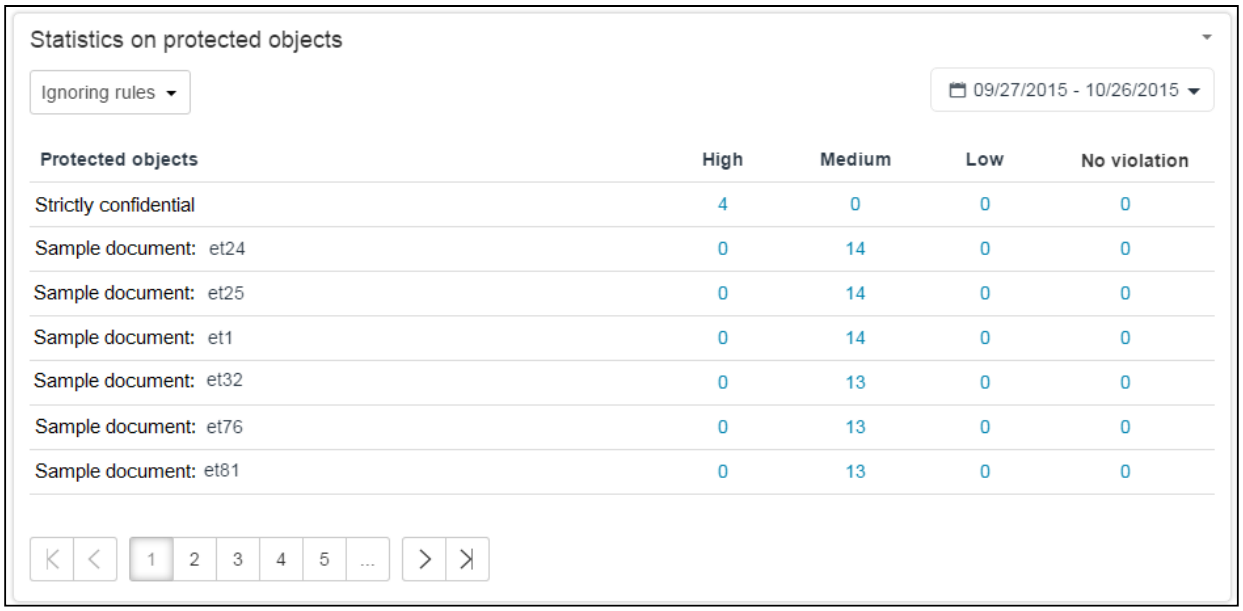
You can edit the following parameters:

- **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;
- **Catalog of protected objects** - catalogs 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**.

Statistics on catalogues of protected objects

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



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

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

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

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

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

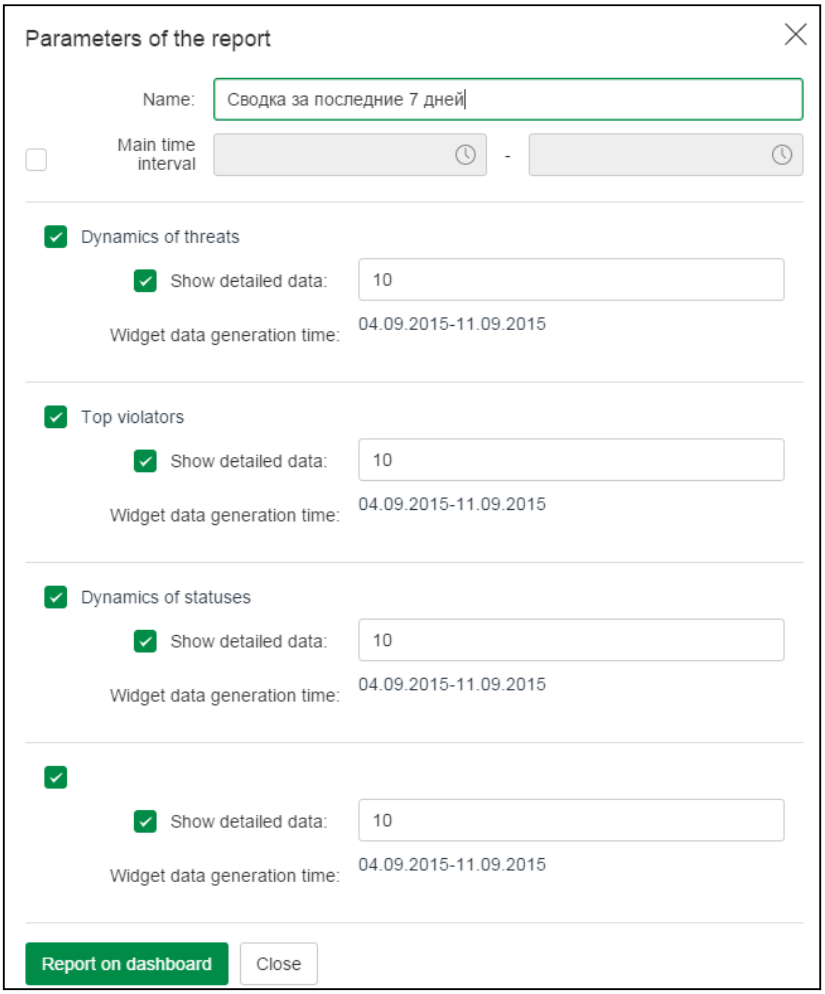
You can edit the following parameters:

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

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

3.1.2 Dashboard report

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



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

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

Important!

The report does not include data from the "Selection" widget.

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

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

Note:

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

User's target actions:

- Creating a dashboard report (see "Creating dashboard report").

3.2 Events Section

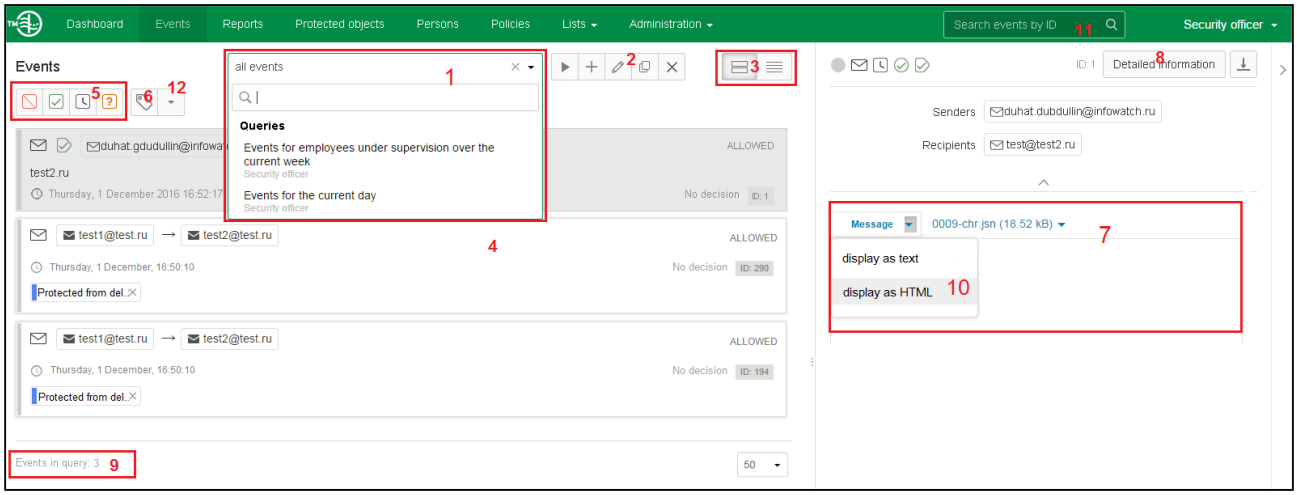
Reference information:
Event is the interception object of network traffic.

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

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

About the section:

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



To search for required events, select a query in the list (№1 in the screenshot) or create a new query using buttons on the toolbar (№2 in the screenshot).

You can also use a field for searching events by their IDs (№11 in the screenshot).

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

As a result of executing a query or searching events by IDs, a list of found events is displayed (№4 in the screenshot). At the bottom of the page, a total number of found events is displayed (№9 in the screenshot).

You can choose how events in the list should be displayed (№3 in the screenshot):

-  - displaying events as tiles
-  - displaying events as a table

In the right part of the workspace, a brief event viewing form is displayed (№7 in the screenshot). To switch to a detailed event viewing form, click the **Detailed information** button (№8 in the screenshot).

> **Note:**
>
> For emails with HTML markup, a button for choosing the viewing mode is displayed (№10 in the screenshot). Possible values:
>
> - **display as text** - is used for displaying the email text without formatting. Allows viewing hidden text (for example, white text on a white background or text contained in the picture name)
> - **display as HTML** - allows viewing pictures, tables, and the text markup

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

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

User's target actions:

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

3.2.1 Queries

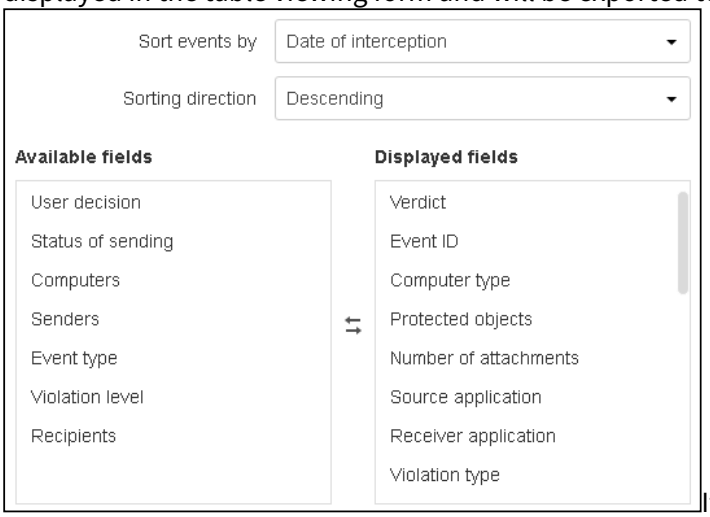
Objects checked by System are stored in the database To view information about these objects in the Management Console, you need to create and execute the query.

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

There are two query creation modes: standard (allows you to select desired conditions from the list) and advanced (enabled 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 that will be displayed for events. The **Available fields** list contains all event attributes and the **Displayed fields** list contains attributes that will be displayed in the table viewing form and will be exported to a file in XSLS format.



If no attributes are selected, then the table form and the export file will include all attributes.
You can also choose by what field the list must be sorted and specify the sorting direction.

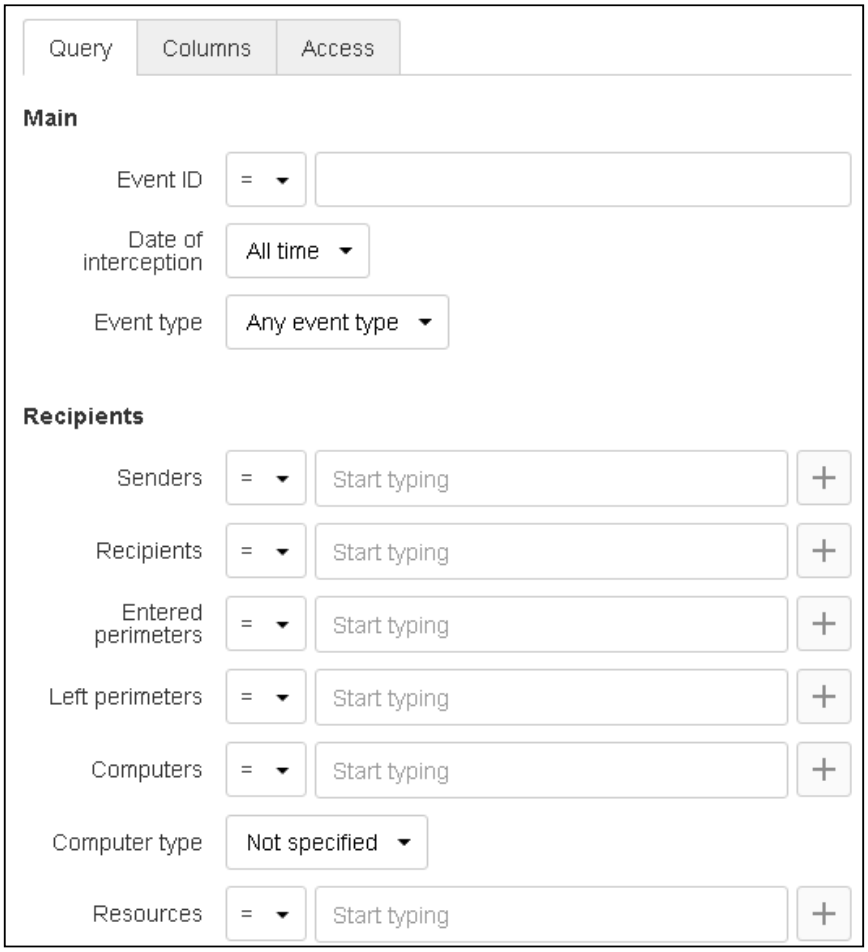
- **Access**. On this tab, you can configure access to the query. To provide access for viewing and editing the query to other users, deselect the **The query is available only to its owner** option and click **Save** (by default, the option is selected).

User's target actions:

- 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 **Condition** tab.



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

Query attributes:

Parameter	**Description**
Main	
Event ID	A unique identifier of the event. Multiple values may be specified, separated by commas.
Date of interception	The date when the event was created. By default events for the current week will be displayed.

Event type	Specifies that the event belongs to a particular interceptor. Event types are grouped by category. When selecting a category, all event types of this category will be displayed. Possible values: • Internet activity: - Web-message • File sharing: - FTP - External device (copying files to network resources also belongs to this event type) • Printers and MFPs - Print • Multimedia recording - Photography • Storage - Crawler • Email - Mail on Client - Mail in Browser • Messenger WhatsApp -MS Lync - ICQ - XMPP - MMP - Skype • Cellular communication - SMS
Recipients	
Senders	The list of object senders
Recipients	The list of object recipients
Entered perimeters	Perimeter the object recipient belongs to
Left perimeters	Perimeter the object sender belongs to
Computer	The computer from which the object was sent
Computer type	Type of computer from which the object was sent. Possible values: • computer • mobile device • terminal server

Resources	Internet resource or a group of resources (see "List of resources"). Start typing and choose the desired resource or group from the list of suggestions. **Note**: If you want to specify a particular resource, choose  icon (for example,  facebook.com)
Clipboard	
Source application	Application from which data has been copied
Receiver application	Application to which data has been pasted from the clipboard
Policies	
Violation level	The level of violation of the corporate security policy. Possible values: *High*, *Medium*, *Low*, *No violation*.
Tags	Tagsassigned to the object (see "Tags")
Policy	List of policies triggered on the object
Violation type	Type of rule that was violated. Possible values: ▪ *Violation of transfer* ▪ *Violation of copy* ▪ *Violation of placement*
User decision	Decision the user made for the object. Possible values: ▪ *Violation* ▪ *No violation* ▪ *No decision* ▪ *Requires additional processing*
Verdict	The verdict passed by the System on the object. Possible values: ▪ *Allowed* ▪ *Blocked* ▪ *Quarantine*
Crawler tasks	
Task name	Name of the scanning task
Date of task start	The date when the task was started

Type of scanning source	Type of the location where the object was found. Possible values: • Shared network resources • Local drives of workstations • SharePoint file storage
Event content	
Attachment name	The name of the object attachment. Both file name and extension must be specified. **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'.
Attachment format	Attachment format. You can select multiple values from the list.
Encrypted file	Whether the attachment is encrypted or not
Path to file	File source
File creation date	Attachment creation date
File modification date	Attachment modification date
Attachment size	Size of the attached file. You can specify a minimum or maximum file size or both parameters.
Event text	Specify the search text. Search results will include events whose text contains all listed words regardless of their location and order, letter case and morphology. Search is performed through all the event contents. Wildcards ("*", "?") are not supported. When the condition is denied, events whose text contains all specified words will be excluded from search results. **Note:** Search results will contain only those events that have already been indexed at the moment of the query execution. Indexing of events is performed every ten minutes, however under a heavy load on the server, this interval may increase.
Analysisresults	Elements of technologies included in protected objects that were triggered on events
Protected objects	List of triggered protected objects
Event context	

Interceptor	Interceptor by which the event was received. Possible values: • ICAP • DM • DM Mobile • Adapter • SMTPD • Sniffer • PushAPI • Crawler
Protocol	Protocolover which the traffic was transferred

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

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

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

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

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

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

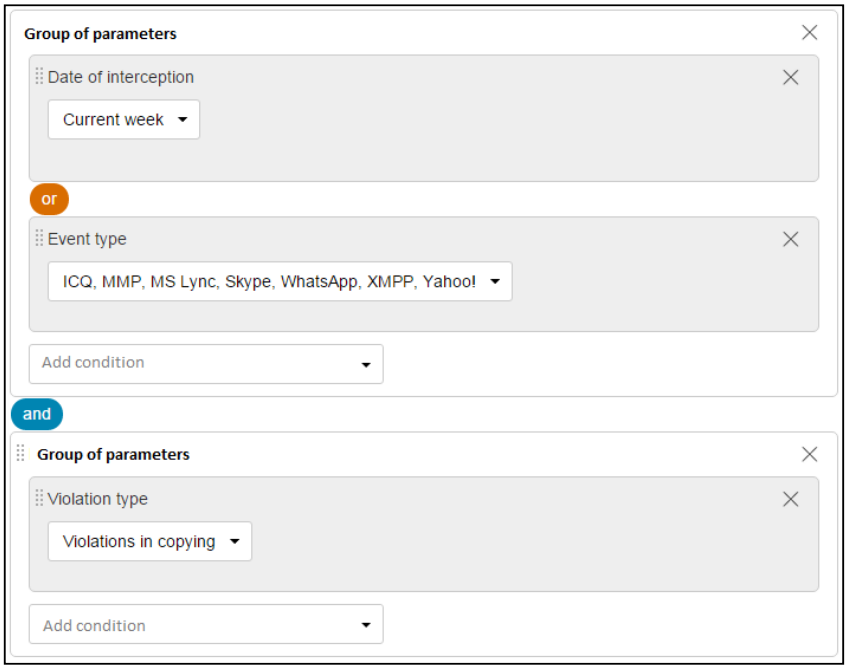
- ? - for a separate character
- * - for a number of characters.

User's target actions:

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

Advanced Mode

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



The following elements are used for creating a query:

- A list of event attributes. This is a set of attributes assigned to the intercepted object
- *Group of parameters* element. This is a container intended for a logical separation of query parts
- = – a parameter of attribute equality. Indicates, that events will be filtered with respect to the presence of the attributes to which this parameter is assigned;
- ≠ – a parameter of attribute negation. Indicates that search results will not contain events to which this parameter is assigned.

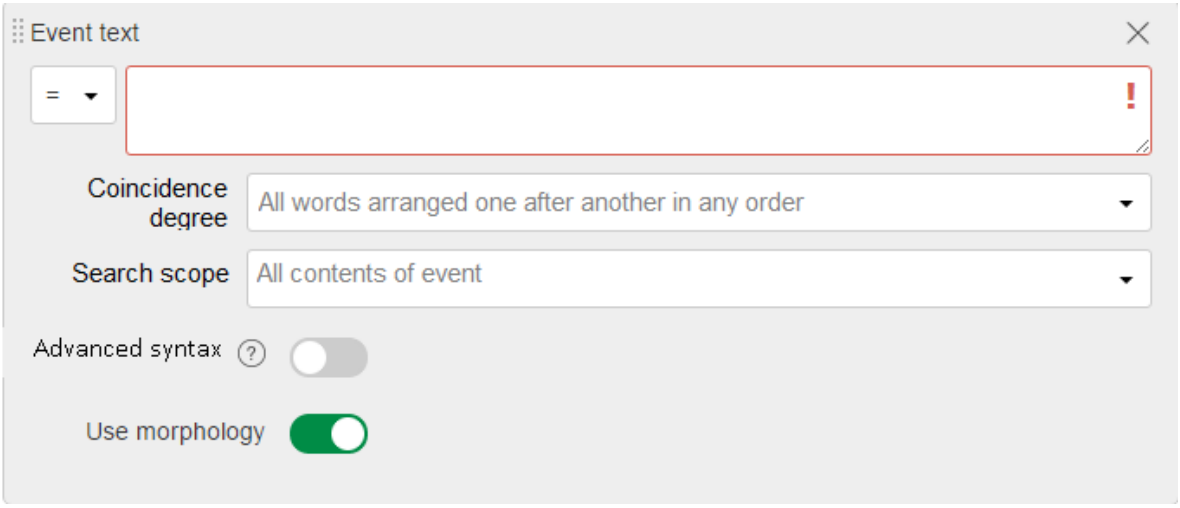
In the advanced mode, you can also perform a flexible search on the text of events.

User's target actions:

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

Search on the Event Text

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



Full-text search parameters:

Parameter	Description
Condition	Parameter of attribute equality. Possible values: = - indicates that filtering results will contain events with attributes for which this parameter has been assigned; ≠ - indicates that events with attributes for which this parameter has been assigned will be excluded from search results.
Coincidence degree	Specify the required coincidence degree: • **All words arranged one after another in a specified order** - search results will include events whose text contains all listed words arranged in the specified order. If the condition is negated, search results will include events whose text does not contain listed words arranged in the specified order. • **All words arranged one after another in any order** - search results will include events whose text contains all listed words in any order. If the condition is negated, search results will include events whose text does not contain listed words irrespective of their order. • **All words irrespective of their order and distance between words** - search results will include events whose text contains all listed words irrespective of their order and distance between words. If the condition is negated, search results will include events whose text does not contain listed words or contains not all of them. • **At least one of specified words** - search results will include events whose text contains, at least, one of the listed words. If the condition is negated, search results will include events whose text does not contain any specified word.

Search area	Specify the area in which the search will be performed: • **All contents of event** - search on all contents of the event will be performed. • **Message text** - search on the message text and message subject will be performed. • **Message subject** - search on the message subject will be performed. • **Attachment** - search on the attachments text and file names will be performed. • **File name** - search on the attachment file names will be performed.
Advanced syntax	Enable this setting if you want to specify the sought-for text using boolean operators. For details, see "Using advanced syntax".
Use morphology	If this setting is disabled, search results will include only those events which contain the sought-for words in a specified grammar form. **Note:** The **Use morphology** option is available only if the construction of the morphological index is enabled in database settings. For detailed information on this setting, please see the document *"Traffic Monitor. Administration Guide".*

Please note that:

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

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

User's target actions:

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

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;
- the short form viewing event displays the most commonly required information;
- the detailed event viewing form displays complete information about the interception object.

Event attributes:

Element	Description
Object ID	Event unique identifier in the System

User decision	Decision the user made for the event. Possible choices: • *No decision*; • *Violation*; • *No violation*; • *Requires additional proceeding*.
Event type	The source of actions which led to the event creation. Possible choices: •  - Internet activity (post requests to Web resources); •  - File exchange (copying files to an external device or to a shared folder, transfer via FTP); •  - Printer and MFP (sending files to print); •  - Recording media (sending or receiving photos); •  - Email (sending and receiving data via mail on client or mail in browser); •  - Messenger (sending or receiving messages through Skype, MS Lync, ICQ(OSCAR), XMPP, WhatsApp); •  - Cellular communication (sending or receiving messages via SMS); •  - File storage (in SharePoint 2007/2010/2013 file storage, shared network resources and on local drives of workstations).
Sending date	Date and time when a mail server received the mail (only for e-mails)
Senders	The list of traffic senders
The sender's computer	The name of the computer from which traffic was sent.
Recipients	The list of traffic recipients
Policies	List of policies triggered on analysis of this event
Categories	List of categories assigned to this event
Protected objects	List of protected objects triggered for this event
Elements of analysis	The list of elements of analysis contained in the triggered protected object
Website topic	Type of inappropriate resources visited by the employee
Tags	List of tags assigned to this object

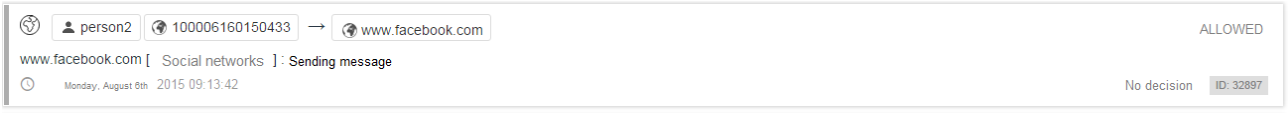
Date of interception	Date and time when traffic was intercepted by the System
Insert date	Date and time when the event was saved into the Database
Size	Size of event (in bytes)
Violation level	Characteristics of the violation assigned to the event. Possible choices: • *None* - is marked with a gray (■) color on the tile; • *High* - is marked with a red (■) color on the tile; • *Medium* - is marked with an orange (■) color on the tile; • *Low* - is marked with a green (■) color on the tile
Delivery status	Indication of whether the message was delivered (only for SMTP messages when the System operates in the "inline" mode. See the document "*Infowatch Traffic Monitor. Installation Guide*"). Possible choices: ▪ *Pending*; ▪ *Successfully delivered*; ▪ *Failed*; ▪ *Delivery Attempt Failed*; ▪ *Blocked*
Verdict	The conclusion which the System assigned to the object as a result of analysis (see "Object analysis and verdict"). Possible choices: • *Allowed* ( ) • *Blocked* ( ) • *Quarantined* ( ) **Note:** Events with *Deleted* verdict are deleted from the System and are not displayed in the Management Console.
Interception server	The name of the server which intercepted the object.

See also:

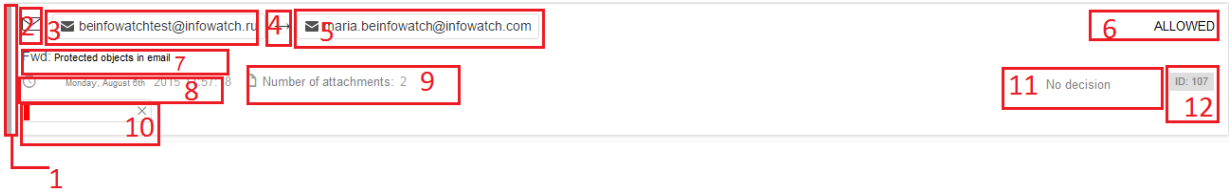
- "Event Tile" - on presenting the event and its attributes.
- "Brief Event Viewing Form" - on displaying general information about the event.
- "Detailed Event Viewing Form" - on displaying advanced information about the event.

Event tile

The event tile looks like this:



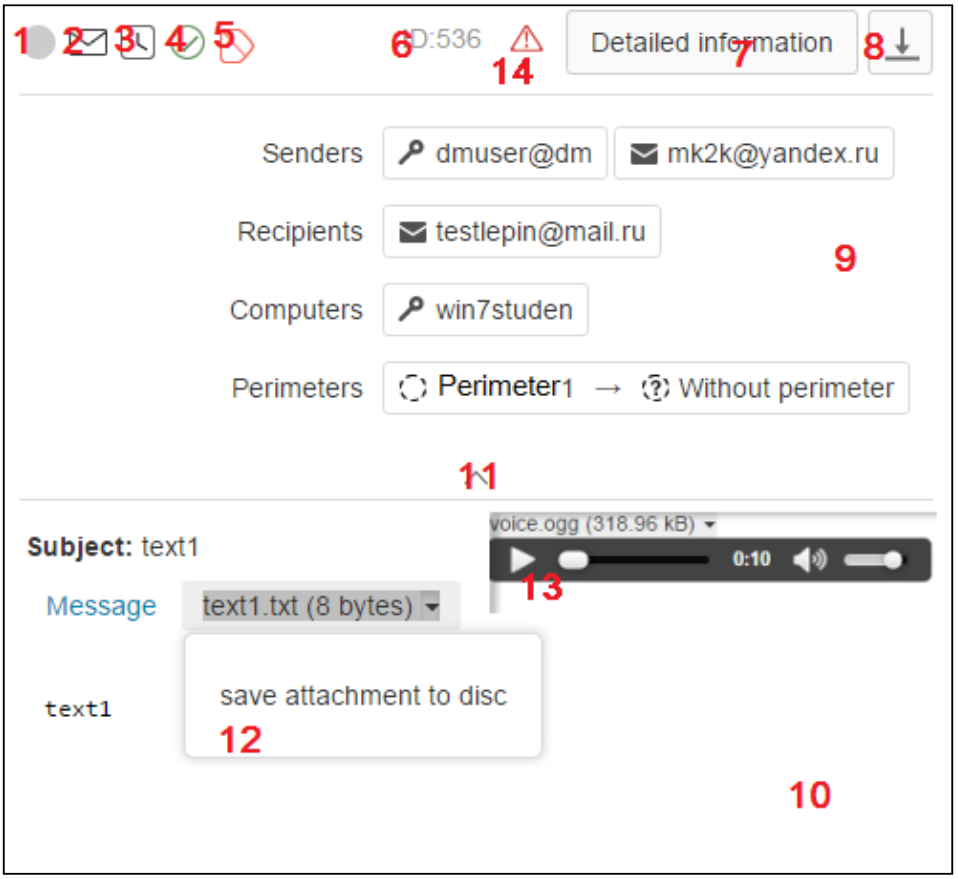
It consists of the following elements:



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

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.



Events section, a brief viewing form for a selected event

A brief event viewing form contains the following entities:

№ on scheme	Entity	Description
1	Violation level	Displays a color indicator for the **Violation level** attribute. Possible values: *High*, *Medium*, *Low*, *No violation*.
2	Icon of event type	Displays an icon of the event type. Possible values: *Web message*, *FTP*, *External device*, *Print*, *Photo*, *Crawler*, *Mail on Client*, *Mail in Browser*, *WhatsApp*, *MS Lync*, *ICQ*, *XMPP*, *MMP*, *Skype*, *SMS*.
3	User decision	Displays the value of the **User decision** attribute. Possible violations: *Violation*, *No violation*, *No decision*, *Additional processing is required*
4	Verdict	Displays the value of the **Verdict** attribute. Possible values: *Allowed*, *Blocked*, *Quarantine*.
5	Sending status	Displays the value of the **Sending status** attribute. Possible values: *Sent*, *Not sent*, *Waiting for sending*.
6	Object ID	Displays the value of the **Object ID** attribute

7	Button for opening a detailed event viewing form	Allows you to view additional information on the event
8	Button for saving event	Button that allows you to save the event to disk (see "Saving Events"). The button is displayed for SMTP messages only.
9	Area with event parameters	Shows event parameters such as *Senders*, *Recipients*, *Computers*, *Perimeters*, etc. **Note**: The set of parameters may vary depending on the event type.
10	Area with event contents	Displays the contents of the event: email texts, attachments, voice messages.
11	Button that shows/hides event parameters	Allows you to hide the area with event parameters. To restore the area, click 
12	**Save attachment to disk** command	Allows you to save attachments to your computer
13	Tools for working with intercepted voice messages in Skype	Allows you to listen to the intercepted voice message and save the file to your computer. To save the file, click  **save attachment to disc**
14	Indicator of errors	Is displayed if some errors occurred while processing the event. You can view detailed information on the errors in the detailed event viewing form.

Note:

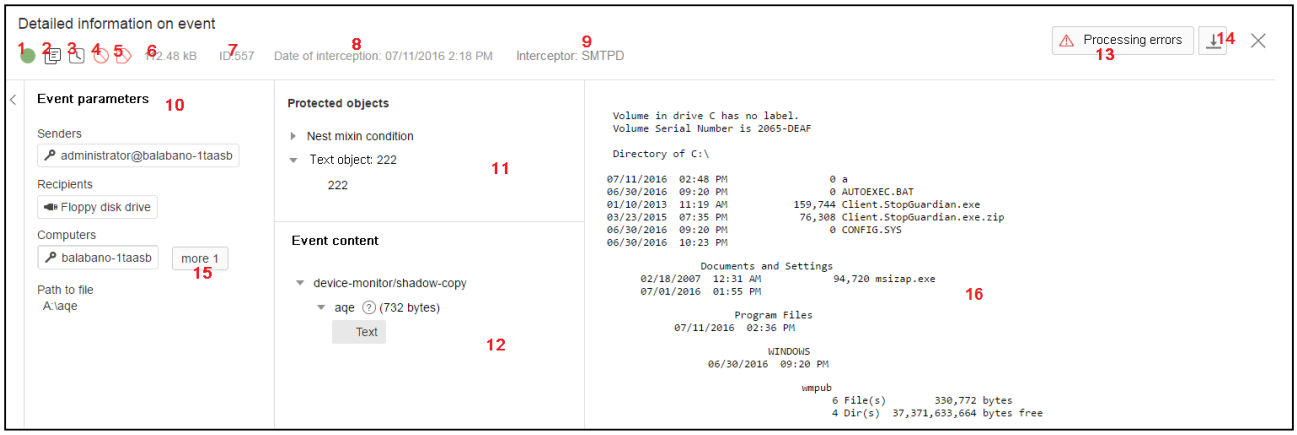
The set of objects in the brief event viewing form may vary depending on extracted attributes.

User's target actions:

- Getting acquainted with general information on the event (see "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").



Events section, a detailed viewing form of the selected event

The detailed event viewing form contains the following information on the event:

№ on scheme	Form element	Description
1	Violation level	Displays a color designation of the **Violation level** attribute. Possible values: *High*, *Medium*, *Low*, *No violation*.
2	Event type	Displays the value of the **Event type** attribute. Possible values: *Web message*, *FTP*, *External device*, *Print*, *Photo*, *Crawler*, *Mail on Client*, *Mail in Browser*, *WhatsApp*, *MS Lync*, *ICQ*, *XMPP*, *MMP*, *Skype*, *SMS*.
3	User decision	Displays the value of the **User decision** attribute. Possible values: *Violation*, *No violation*, *No decision*, *Additional processing is required*.
4	Verdict	Displays the value of the **Verdict** attribute. Possible values: *Allowed*, *Blocked*, *Quarantine*.
5	Sending status	Displays the value of the **Sending status** attribute. Possible values: *Sent*, *Not sent*, *Waiting for sending*.
6	Size of event	Displays the value of the **Size of event** attribute
7	Object ID	Displays the value of the **Object ID** attribute
8	Interception date	Date and time of object interception
9	Interceptor	Interceptor by means of which the event was received

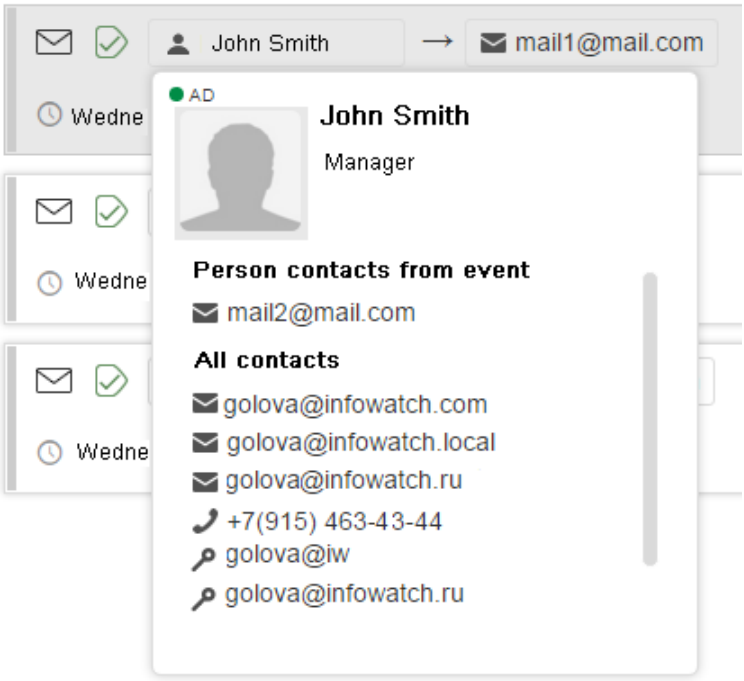
10	**Event parameters** block	Includes such event parameters as *Senders*, *Recipients*, *Computers*, *Perimeters*, etc. **Note**: The set of parameters may vary depending on the event type.
11	**Protected objects** block	The list of triggered protected objects and elements of technologies that are included in these protected objects. Click the protected object or the element of technologies to view detailed information in the right part of the form (№ 12 in the picture). The following information is displayed: • the number of detected elements of technologies; • a catalog the protected object belonged to at the moment of interception (clicking the catalog name opens the catalog in the "Protected Objects" section).
12	**Event content** block	Displaes the event content: email text, attachments, voice messages. To view detailed information, click the desired element. The detailed information is displayed in the right part of the form (№ 12 in the picture). For example, for the *Mail on Client* type of event, you can view message text or attached images.
13	**Processing errors** button	Clicking this button opens the **Processing messages** window with system messages on the stages of object processing and errors that occurred during the processing
14	Button for saving a shadow copy	Button that allows you to save the event to disk (see "Saving Events"). The button is displayed for SMTP messages only.
15	Button for expanding the list	The button appears if there are few elements in the list. Click this button to view the whole list. To collapse the list, click (is displayed when you expand the list).
16	Viewing area	Displays additional information when you select a protected object or an element of technologies in the **Protected objects** block (№ 10 in the picture) or select an element in the **Event content** block (№ 11 in the picture).

User's target actions:

- Getting acquainted with detailed information about the event (see "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 during 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) and social networks can be added to the person card.

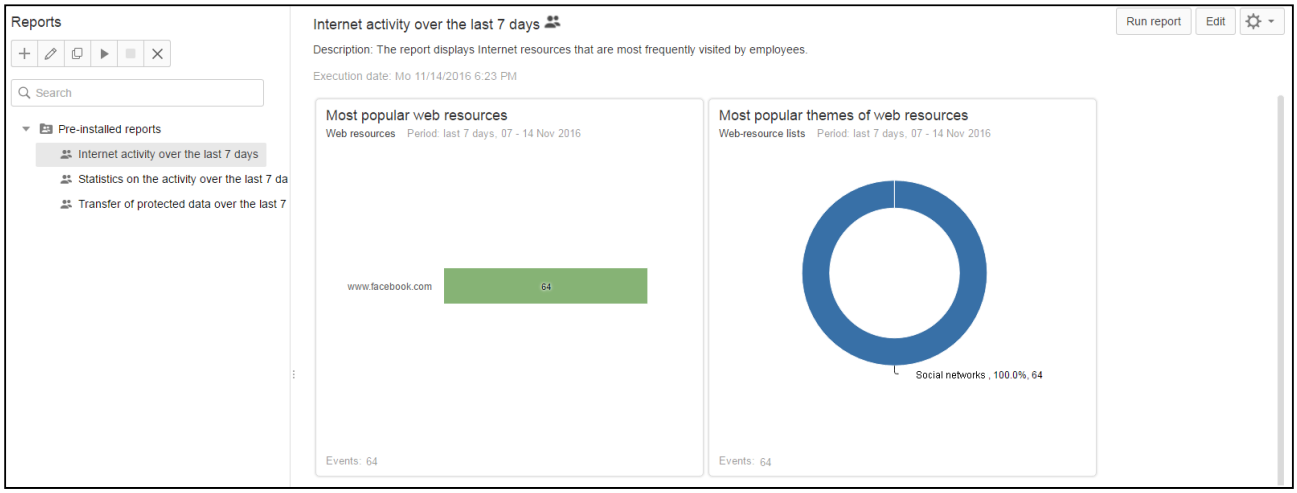
> **Note:**
>
> Post identification applies to traffic senders only. Contacts of traffic recipients are not identified.

3.3 Reports Section

About the section:

Contains a sampling of statistical data on intercepted objects.

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



The list of reports and tools for working with reports are located in the left part of the workspace. You can create top-level reports or group reports in folders.

Folders make it possible to inherit permissions and copy selected groups of reports. On how to create a folder, see "Creating Folder with Reports".

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

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

In the right part of the workspace, you can view parameters of the selected report and widgets with results of the last execution of the report. Widget types that can be used in reports are described in "Widgets of Reports" article.

When creating or editing a report, the report creation/editing form is displayed in the right part of the workspace (see "Report Creation Form").

To start the report execution, click on the toolbar or use the **Run report** button in the right upper corner of the workspace.

In the right upper corner of the workspace, there is also button. Clicking this button opens a drop-down list, where you can choos
:

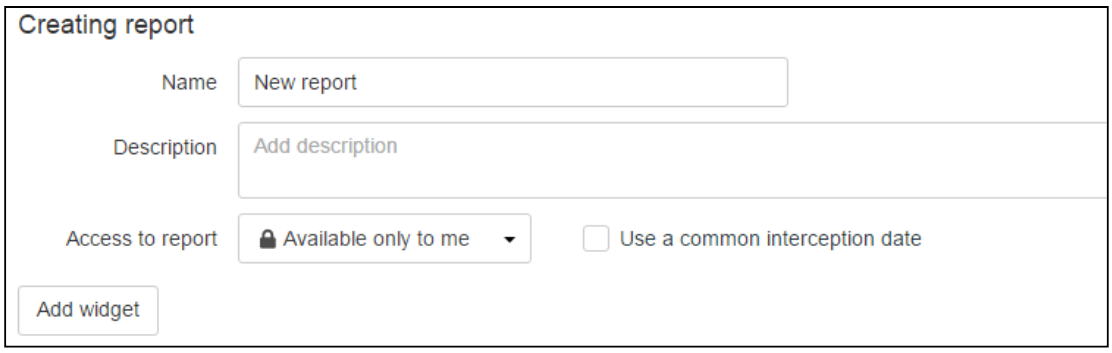
- open the report execution history;
- copy the report;
- delete the report;
- save the report as a file in one of supported formats.

User's target actions:

- Creating report
- Creating and configuring widget
- Creating folder with reports
- 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:

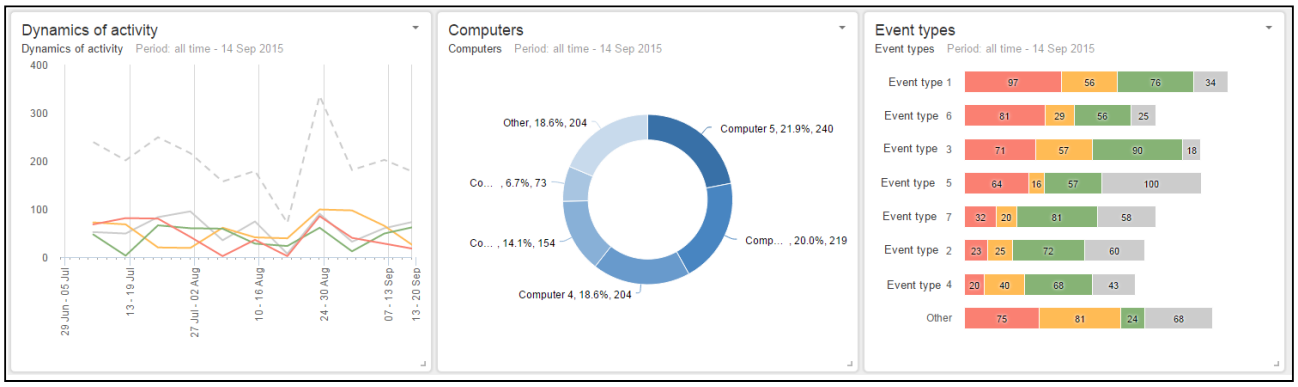
- **Name**;
- **Description**;
- **Access to report** - specify if the report is available only to the owner or to all users.
  This option is available only to reports of the first level. When creating a report within a folder, the access level specified for the folder defines the access level for the report.
- **Use common interception date** - select this 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.

User's target actions:

- Creating report

3.3.2 Widgets of Reports

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



Widgets of the **Reports** section

Widgets are designed to display statistical information on intercepted objects for a specified period of time.

Widgets can be created for the following data:

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

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

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

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

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

Parameter	Description
Violation levels	Events with a specified violation level will be added to the widget. Select checkboxes next to desired values.

Grouping period	Specify a period for which events will be grouped. Possible values: • minute; • hour; • day; • week; • month; • quarter; • year.

Widget parameters for other types of statistics:

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

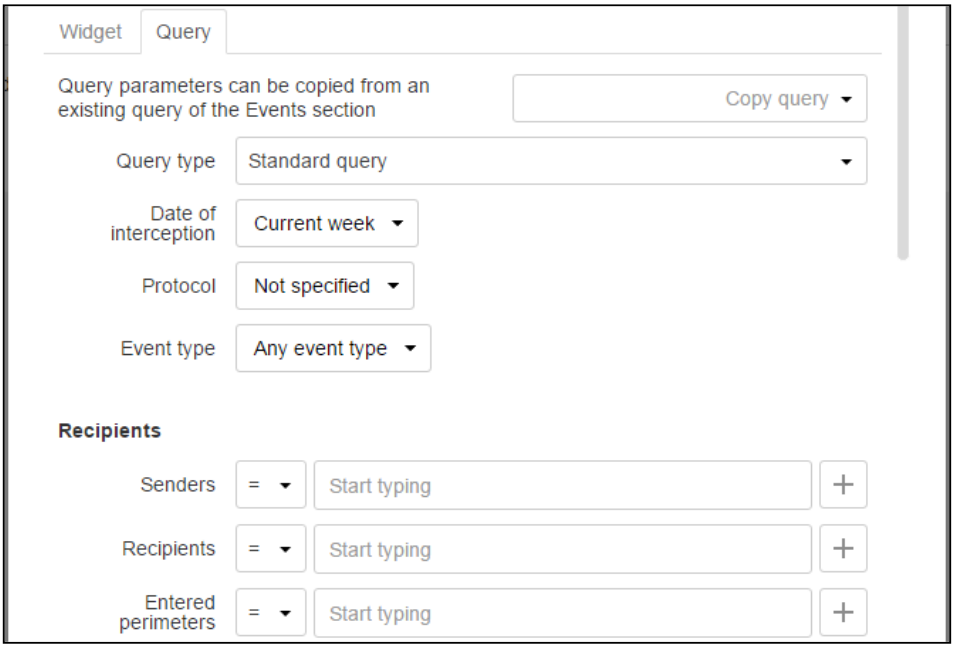
User’s target actions:

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

3.3.3 Queries

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

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



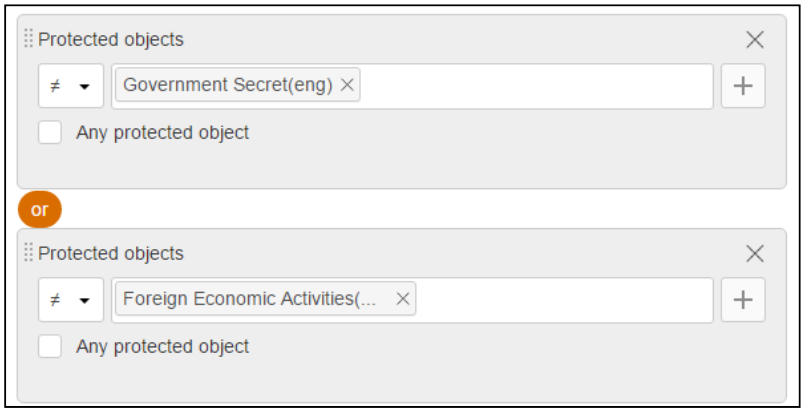
The **Query** tab in the widget creation window

You can create a query in one of the following modes:

- *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".

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 any of the specified elements.



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

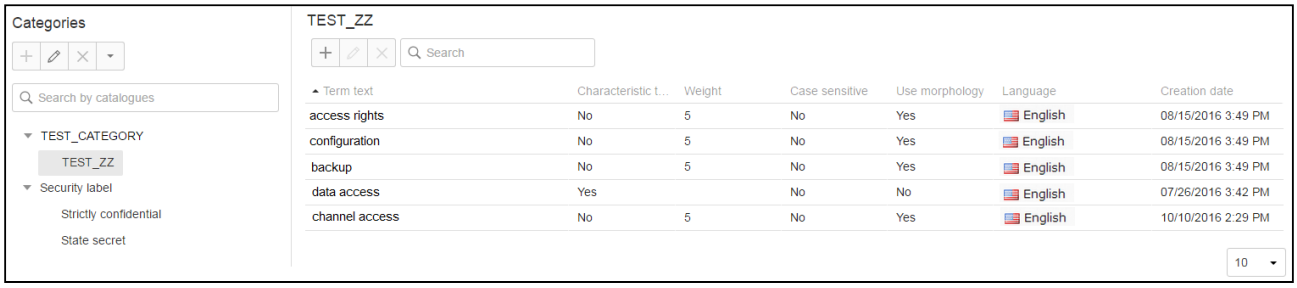
User's target actions:

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

3.4 Technologies section

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

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



Technologies section, **Categories and terms** subsection

User's target actions:

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

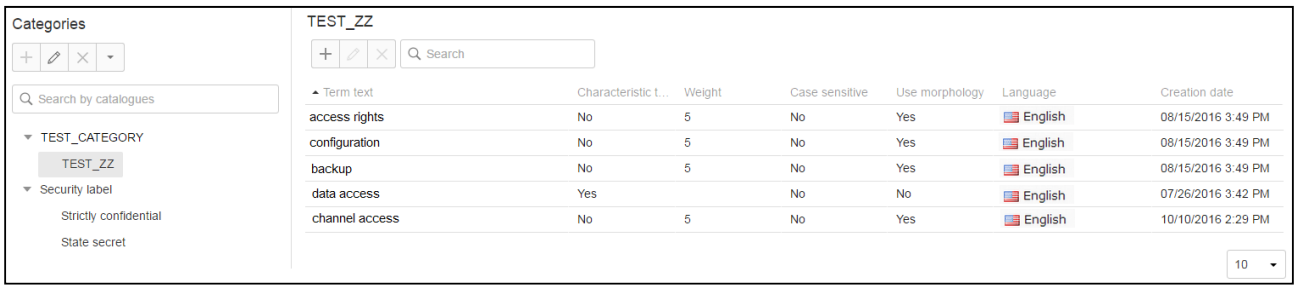
3.4.1 Categories and terms

Reference information:

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

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

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



User's target actions:

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

- Adding categories to protected objects (“Creating a Protected Object")

Categories

Reference information:

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

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

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

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

- Weight - a value specified by default for all terms of the category as the **Weight** attribute;
- Language - the language of category terms;
- Use morphology - if this option is selected, analysis is performed with respect to all morphological forms of the term;
- Case sensitive - if this option is selected, the analysis is performed with respect to the letter case.

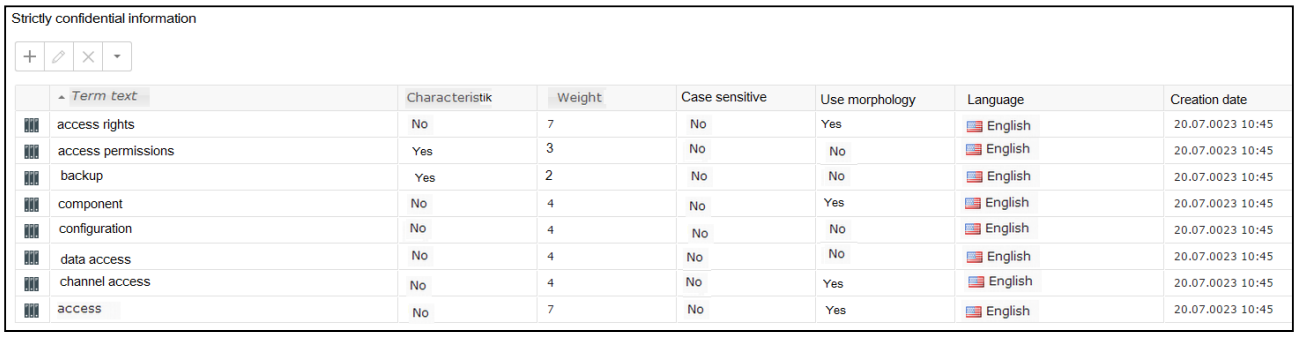
For the category to be detected in intercepted data, it must be included in protected objects.

User’s target actions:

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

Terms

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



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

Term attributes:

Parameter	Description
Term text	A word or phrase which (if found in the analyzed text) increases the degree of conformity of the text to the term category
Characteristic	If this attribute is enabled, then finding the term in traffic certainly assigns the term category to the object
Weight	Indicator of the term significance
Case sensitive	Indicates if the case is matched in traffic analysis
Use morphology	Indicates if morphology is used in traffic analysis
Language	The language of the term

Note:

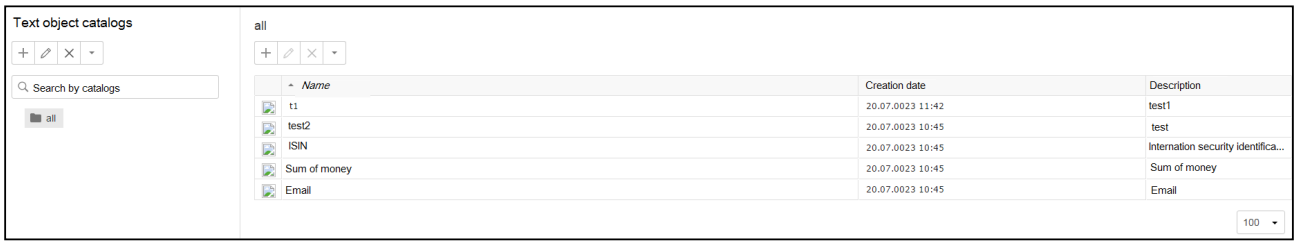
The **Case sensitive** and **Use morphology** parameters are set by default when specifying these parameters for the category. Parameters of the term can be then edited and saved. In this case, when editing case and morphology settings of the category, these changes will not apply to the terms.

User's target actions:

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

3.4.2 Text Objects

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



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

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

Warning!

When deleting a system text objects from a catalog, user templates created for this object are also deleted.

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

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

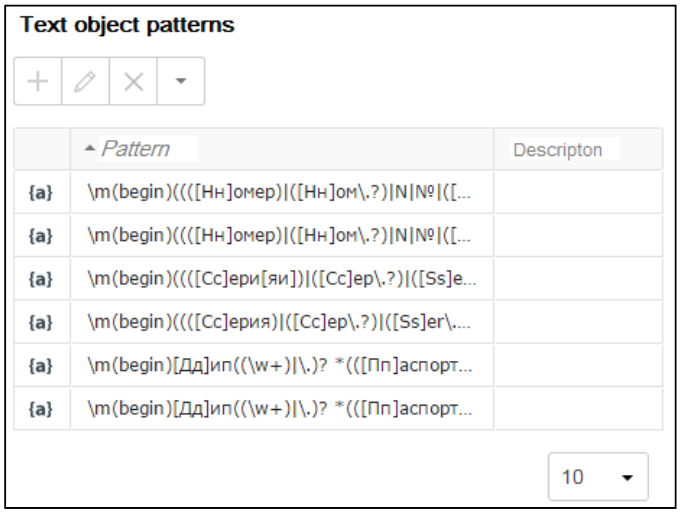
User's target actions:

- Creating text objects and their catalogs (see "Managing Text Objects")
- Adding system text object to a selected catalog (see "Managing Text Objects")
- Importing and exporting text objects as a part of technologies base (see "Exporting and Importing the Technologies Database")
- Adding text objects to protected objects (see "Creating a Protected Object")

Text objects patterns

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

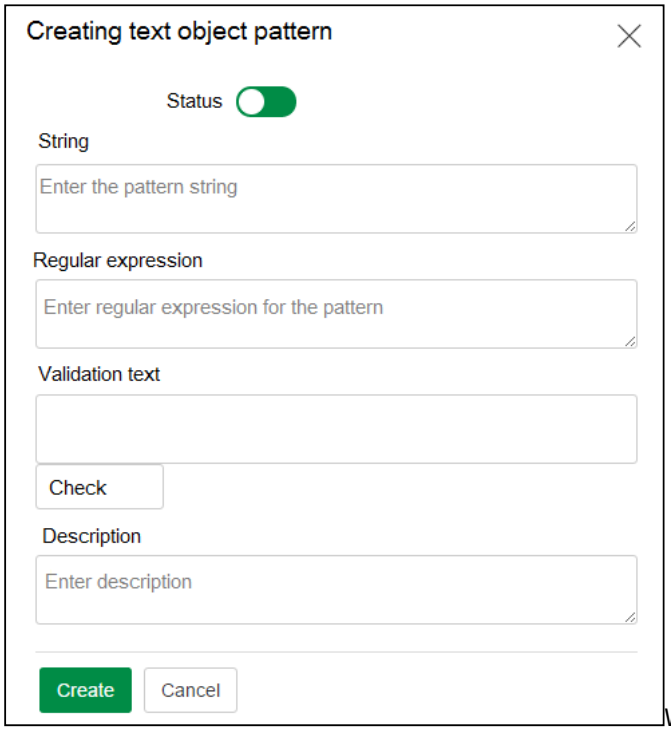
Patterns for a selected text object are displayed when switching to the edit mode of the text object.



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

Warning!

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



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

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

User's target actions:

- Creating a text object

3.4.3 Sample Documents

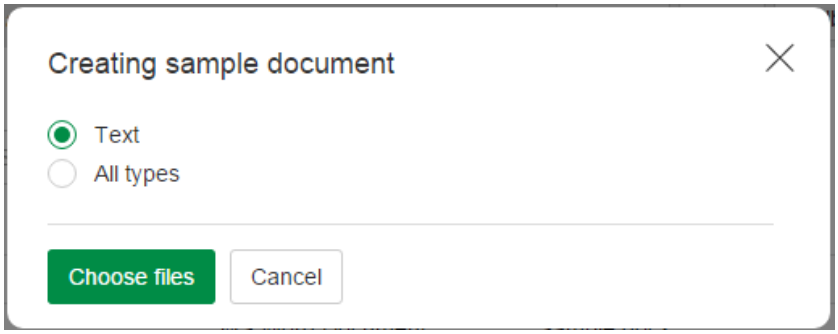
Reference information:
The *sample document* is a document containing quotes for text analysis. Memos, financial reports, contracts, and other sensitive documents can all be used as sample documents. Sample documents are stored in the system as digital prints, their text is not available to either users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



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

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

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



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

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

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

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

User's target actions:

- Creating Sample Documents and their Catalogs (see "Managing sample documents")

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

3.4.4 Blanks

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

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

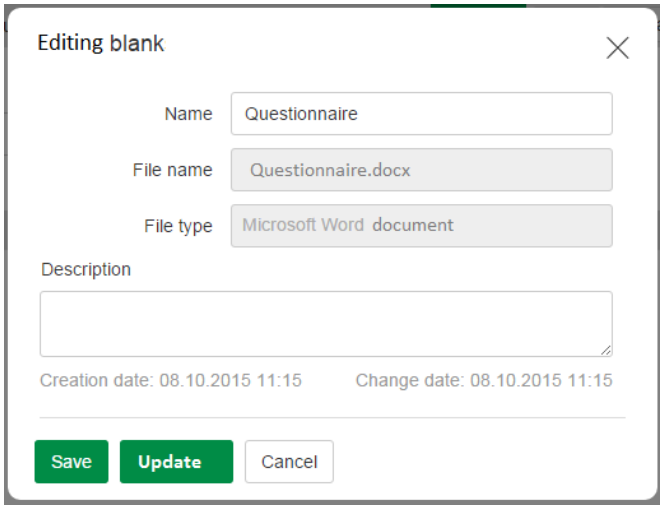
For the blank to be detected in intercepted data, it must be included in a protected object.

> **Warning!**
>
> To match an interception object with the protected object which contains a blank, the following requirements must be met:
>
> - the object text contains, at least, one field from the blank;
> - if the number of fields detected in the object text is more than one, then fields should be in the same order as in the digital print uploaded to the System;
> - if the **Detect only filled blanks** option is selected, then, at least, one character should be placed between the adjacent rows.

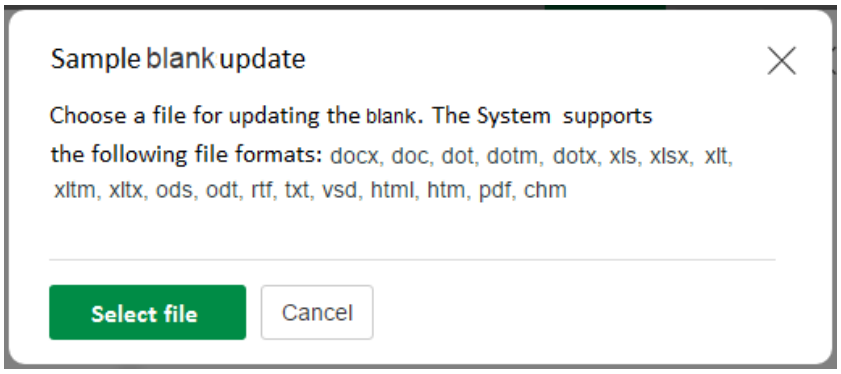
Blanks are created within catalogs. For operations with catalogs (creating, editing or deleting a catalog; search by catalogs), tools on the left side of the working area are used. Blanks of a selected catalog and tools for operations with blanks are located on the right side of the working area.



The list of blanks within a catalog and tools for working with blanks are located iin the right part of the working area. In the edit mode, you can view and, if necessary, change attributes of the selected blank. You can also switch to updating the selected blank by clicking the **Update** button.



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



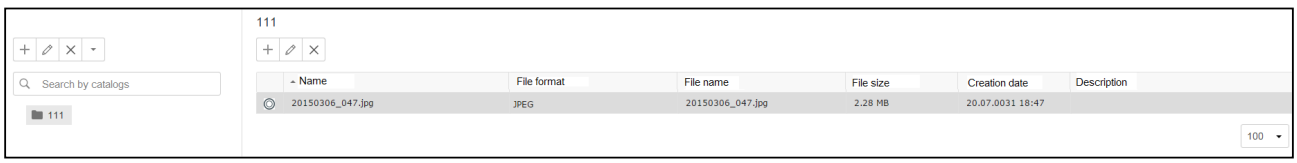
User's target actions:

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

3.4.5 Stamps

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

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



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

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

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

User's target actions:

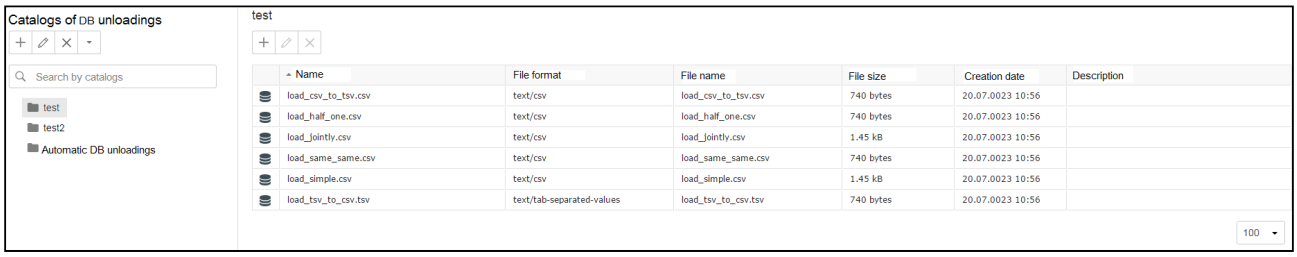
- Creating stamps and their catalogs (see "Managing Stamps")
- Adding stamps to protected objects (see "Creating a Protected Object")
- Importing and exporting stamps as a part of the technologies base (see "Exporting and Importing the Technologies Database")

3.4.6 Database Unloadings

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

> **Warning!**
>
> For correct operation in the System, the database unloading should have the following characteristics:
>
> - the number of columns is no more than 32;
> - the number of words in one cell is no more than 256;
> - the number of rows is no more than 1 million (for 8 GB RAM server) or no more than 3.5 million (for 16 GB RAM server);
> - unloading size maximum of 1 Gb in case Postgre SQL is used.

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



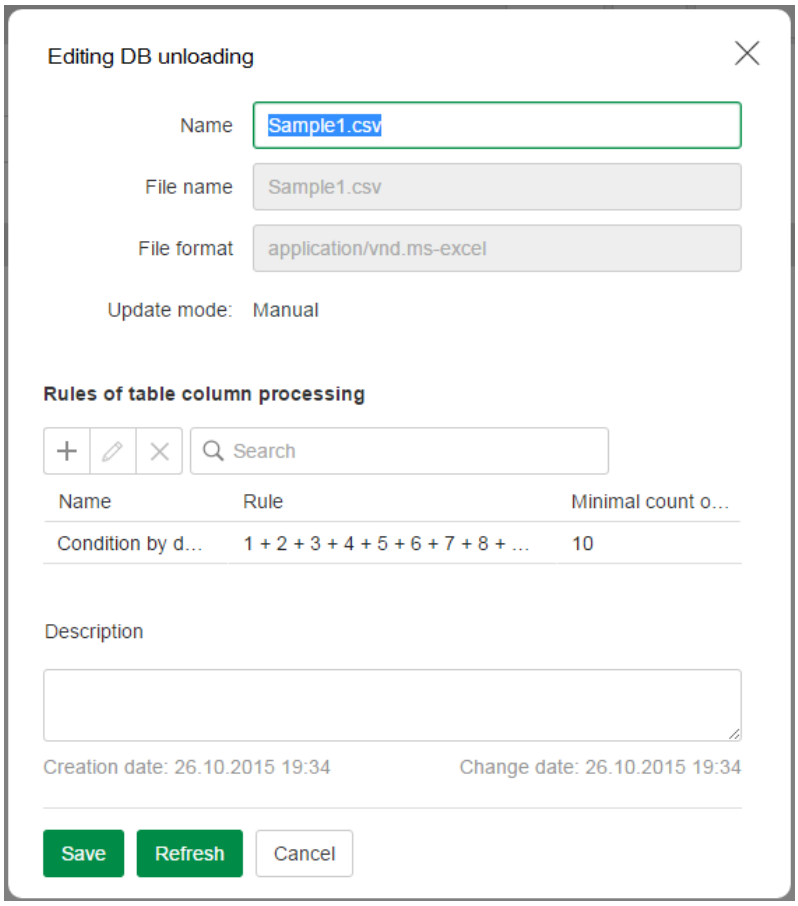
The preinstalled catalog **Automatic DB unloadings** contains unloadings received from external systems (for further details, see "Automatically Updated Database Unloadings").

Note:

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

In the edit mode, the detection conditions for the unloading are displayed. Detection conditions define logical relationships between table columns and the minimum number of non-empty rows this is required for triggering the unloading.

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



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

User's target actions:

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

Automatically Updated Database Unloadings

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

Warning!

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

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

Note:

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

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

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

You can also add unloadings to the **Automatic DB unloadings** catalog manually. For manually added unloadings, the update will be performed in a standard way (see "Managing DB Unloadings").

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.

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

Warning!

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

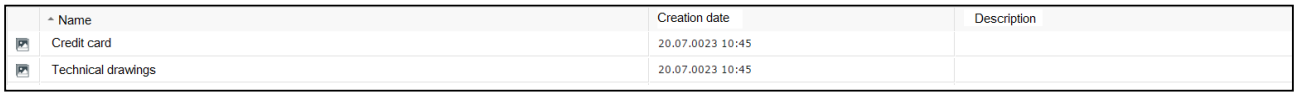
For automatic unloading to be detected in intercepted data, it must be included in a protected object.

3.4.7 Graphical Objects

Reference information:

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

Graphical objects are used when creating protected objects.



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

Name	Description
Credit card	Front side image of a VISA, Visa Electron, MasterCard, Maestro or Mir credit card. Is included in the **Personal data** preset protected object (or in the **Credit card information** preset protected object for the Malaysian version).
Topographic maps	A topographic map or its part
Technical drawings	Technical drawings in a form of black lines against a white background
Identification card of a citizen of Malaysia	Is available for the Malaysian version only. A group of identification documents of the citizens of Malaysia including: • `MyKad` – a general card for citizens of Malaysia over 12 years old (front side) • `MyKid` – a card for children under 12 (front side) • `MyPR` – a card for residents of Malaysia who received a residence permit (front side) • `MyTentera` – a card for those who serve in the army (front side) Is included in the **Personal ID** preinstalled protected object.

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

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

User's target actions:

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

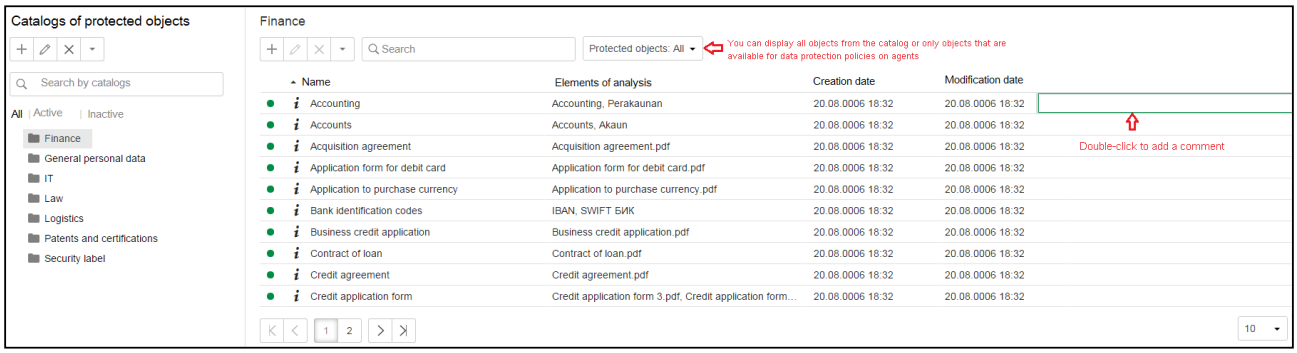
3.5 Protected Objects Section

Reference information:

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

About the section:

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



The catalog list includes both custom and preset protected objects.

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

In the right part of the workspace, protected objects for the selected catalog are displayed. For each protected object, the following attributes are displayed: status (*Active* or *Inactive*), name, elements of technologies included in the protected object, creation and modification dates, description.

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

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

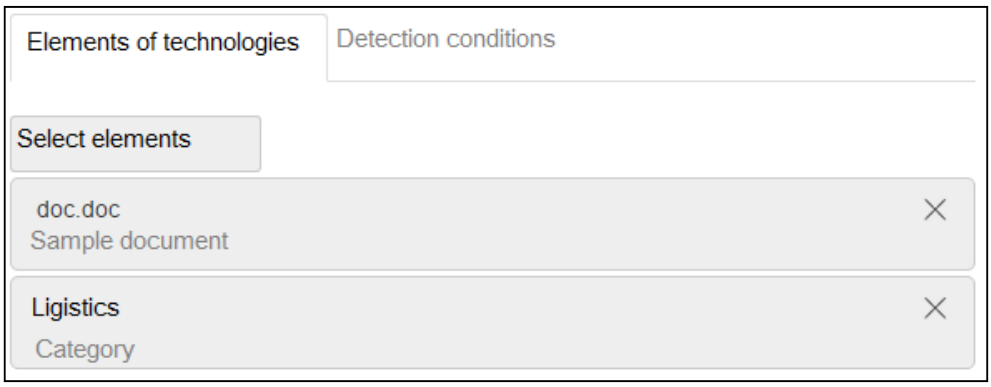
In the edit mode of the protected object, you can change the list of elements of technologies and specify detection conditions.

User's target actions:

- Creating a Catalog of Protected Objects
- Creating a Protected Object
- Adding Elements of Technologies
- Creating Policies for Protected Objects and Their Catalogs
- Import and Export of Protected Objects

3.5.1 Elements of Technologies

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



Elements of technologies tab for a protected object

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

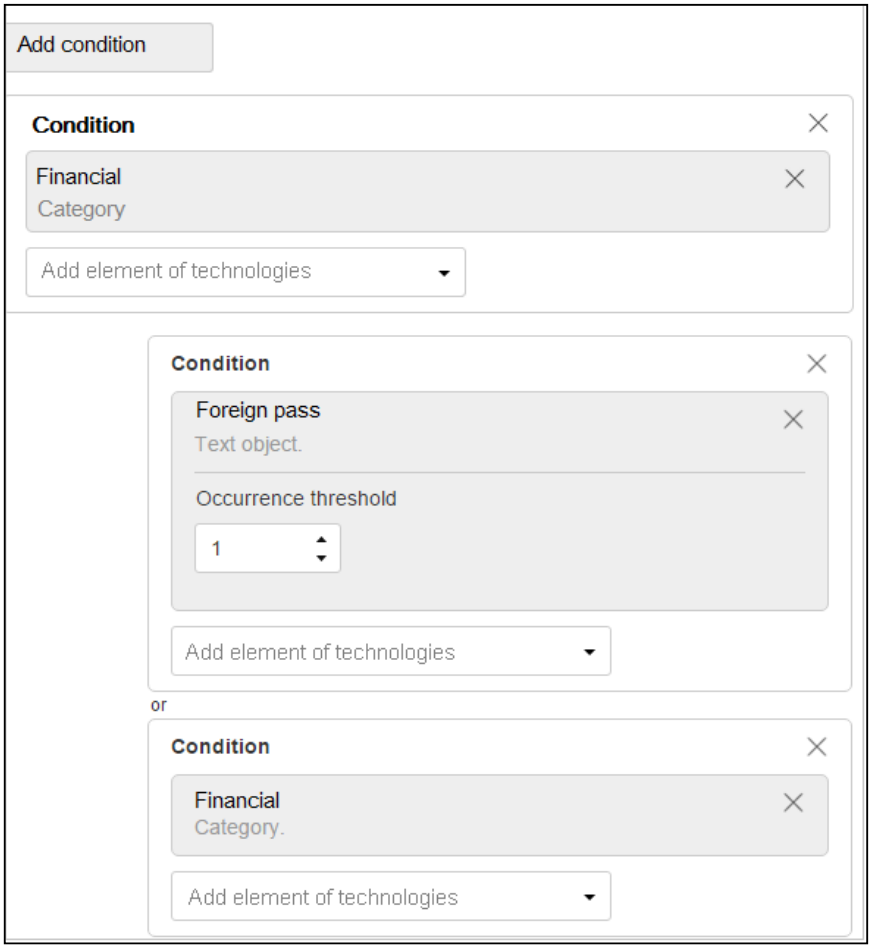
On the **Elements of technologies** tab, you can add more elements of technologies to a protected object (the **Select elements** button) or delete elements of technologies (the X button in the upper right corner of the element panel).

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

User's target actions:

- Adding elements of technologies

3.5.2 Detection Conditions



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

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

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

Detection conditions for the elements of technologies:

Element name	Detection condition
Sample document	Checks whether the interception object contains a specified sample document
Category	Checks whether the interception object matches the specified categories. For categories that contain sub-categories, checks if the interception object matches any subcategory

Text object	Checks whether the interception object contains a specified text object. Additional detection condition is a occurrence threshold. It determines the least number of times the text object must be present in the interception object. The default value is 1. Depending on the pattern type, the number of occurrences of the text object is calculated as follows: • if the text object pattern is specified as a regular expression, then one pattern value is counted as one occurrence even if it is detected several times within a document • if the text object pattern is specified as a string, all its occurrences are counted.
Blank	Checks whether the interception object contains at least one of the specified blanks. Additional detection conditions: • search through filled and unfilled blanks. If you want all blanks to be detected, select the **Filled and unfilled** checkbox. By default only filled blanks are detected; • a minimum number of matching entries. The default value is 3.
Stamp	Checks whether the interception object contains a specified stamp
Graphical object	Checks whether the interception object contains a specified graphical object
Database unloading	Checks whether the interception object contains a specified unloading.You must select one of the representations of unloading

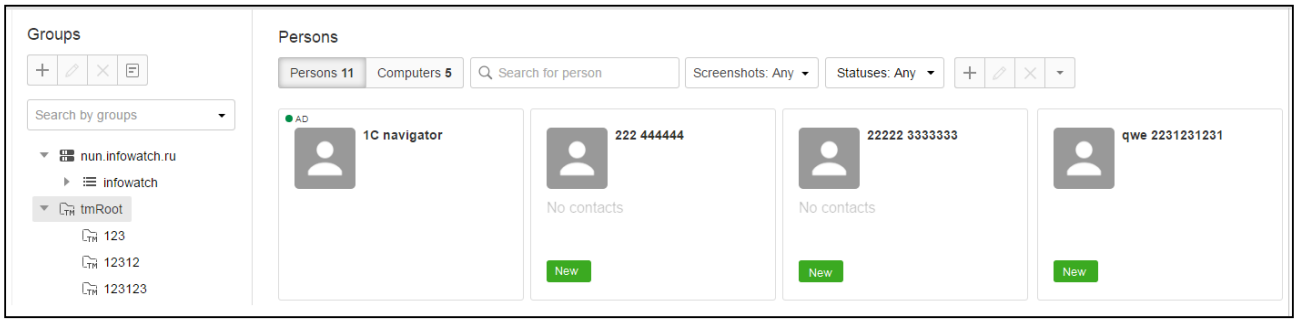
See also: Elements of technologies

User's target actions:

- Adding detection conditions

3.6 Persons Section

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



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

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

Note:

Groups synchronized with Active Directory are marked with . Groups synchronized with Domino Directory are marked with . Groups synchronized with Astra Linux Directory are marked with .

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

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

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

To search for desired persons or computers by the name or IP address, use **Search for person** field.

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

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

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

User's target actions:

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

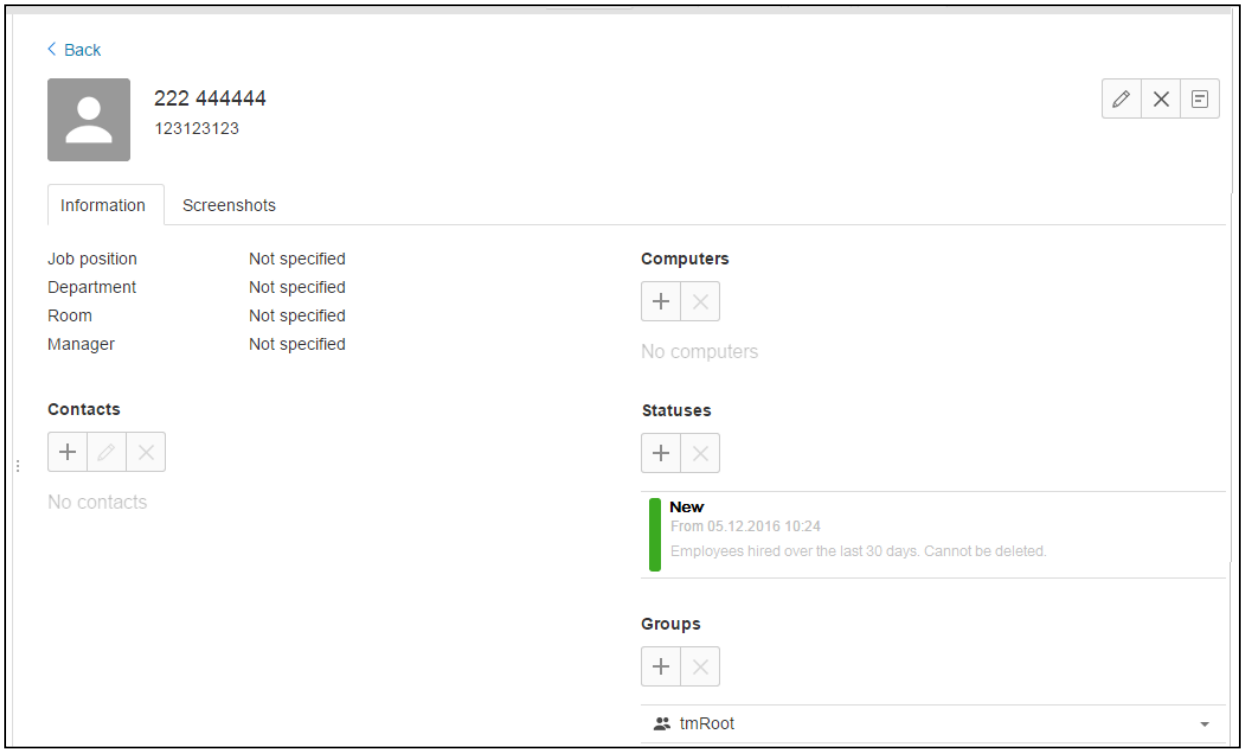
3.6.1 Persons

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

Note:

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

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



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

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

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

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

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

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

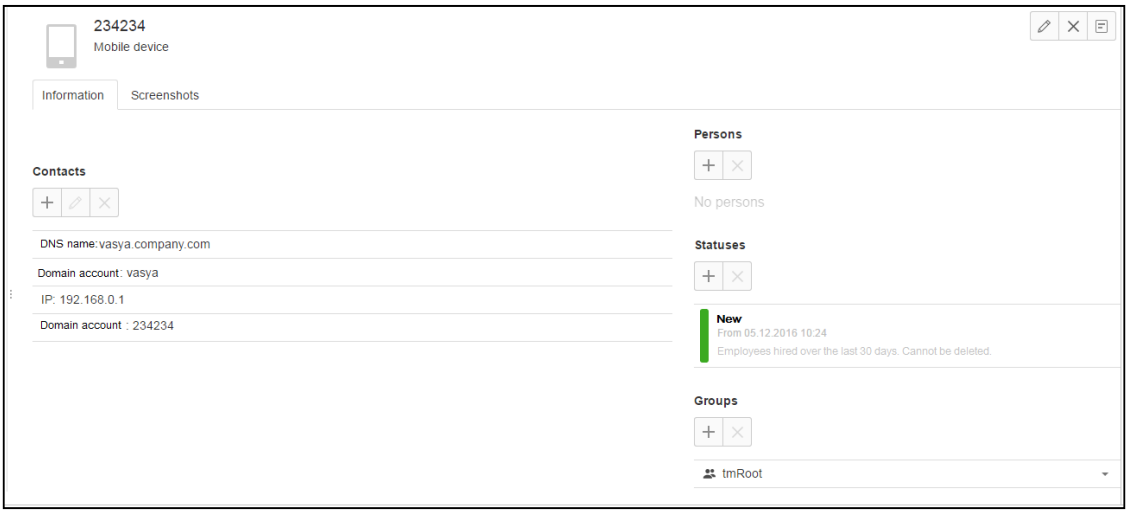
User's target actions:

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

3.6.2 Computers

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

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



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

- Contacts (you can specify DNS name, IP address, and domain account)
- Persons (persons to whose accounts the computer is linked)
- Statuses (statuses assigned to the computer)
- Groups (groups which include the computer)

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

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

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

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

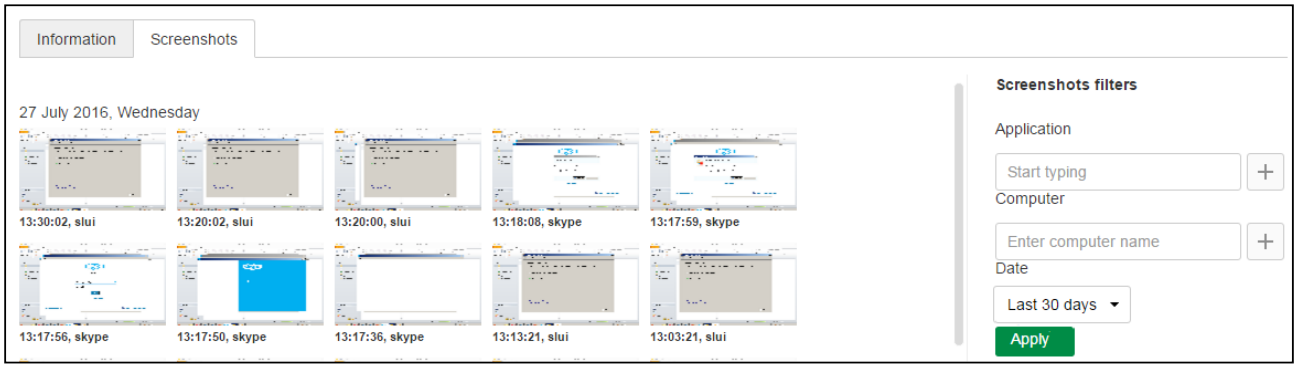
User's target actions:

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

3.6.3 Screenshots

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

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



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

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

Clicking a screenshot opens its enlarged image and attributes:

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

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

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

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

User's target actions:

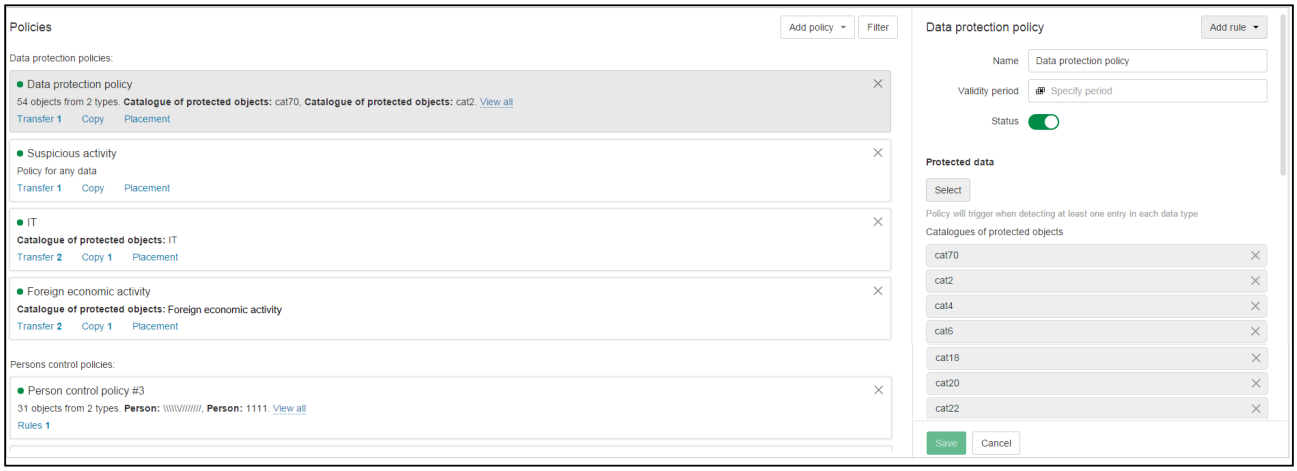
- Viewing Screenshots

3.7 Policies Section

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

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

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



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

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

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

In the policy viewing form, you can:

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

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

User's target actions:

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

3.7.1 Rules and their Viewing Form

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



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

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

There are four categories of rules for the **data protection policy**:

The rule	Description
Transfer rule	The rule that regulates sending and receiving protected data
Copy rule	The rule that regulates copying, printing and photographing protected data
Placement rule	The rule that regulates storing protected data
Clipboard rule	The rule that regulates using of clipboard

Note:

For the data protection policy on agents, only transfer and copy rules are available.

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

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

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

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

User's target actions:

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

Rule of Transfer

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.

Attributes of the rule of transfer:

Parameter	Description
Direction of route	There may be two types of directions: → In single direction - the rule is triggered only when traffic is passed from senders to recipients ⇌ In both directions - the rule is triggered when traffic is passed both from senders to recipients and from recipients to senders
Event type	The type of traffic that triggers the rule provided that other conditions are satisfied. Possible values: ▪ Internet activity ▪ Messenger (for data protection policies only) ▪ Mail ▪ Cellular (for data protection policies only)
Computers	Computers of the sender
Senders	If persons or computers from this list send traffic (or traffic leaves specified domains and perimeters), it will (provided that other conditions are satisfied) = ▾ - trigger the rule ≠ ▾ - do not trigger the rule

Parameter	Description
Recipients	If persons, computers, domains or perimeters from this list receive traffic, it will (provided that other conditions are satisfied) = - trigger the rule ≠ - do not trigger the rule **Note:** If you select a protected object based on a graphical object as policy protected data and specify the **Mail in Browser** event type, then the policy can be triggered only if no persons are specified in the **Recipients** field. This restriction is due to the fact that for webmail events, a recipient of enclosures is not an email, but a domain. For example, if a message with enclosures is sent to the `user1@example.com` email address, the enclosure recipient will be the `example.com` domain. Thus, if particular persons are specified as recipients, events with enclosed graphical objects will not be covered by the policy.
Rule validity days	The list of days of the week on which the rule can be triggered
Rule validity time	The time interval during the day when the rule can be triggered
Notify	List of user of the Console who will be notified when the rule is triggered **Note:** If after the rule is created, the user or the user 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 user.
Inform initiators	Enable this setting if you want to send notifications to traffic senders when the rule is triggered. By default, this setting is disabled.
Assign verdict to event	A verdict which will be assigned to the object when the rule is triggered. Possible values: *Allow*, *Block*, *Quarantine*.

Parameter	Description
Assign violation level to event	A violation level that will be assigned to the object when the rule is triggered. Possible values: *High*, *Medium*, *Low*, *No violation*.
Assign tags to event	The list of tags which will be assigned to the object when the rule is triggered (see "Tags")
Assign status to initiators	A status that will be assigned to senders when the rule is triggered (see "Statuses")
Delete event	If this option is selected, then the event will not be saved to the database and the actions specified in the rule will not be performed. By default, this setting is disabled. **Note:** In data protection policies on agents, events cannot be deleted.

User's target actions:

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

Rule of Copying

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.

Attributes of the rule of copying:

Parameter	Description
Event type	The type of traffic copying which triggers the rule provided that other conditions are met. Possible choices: • External device • FTP • Print (for data protection policies only) • Photography (for data protection policies only)
Computers	The list of computers copying the traffic who (provided that other conditions are met) trigger the rule
Senders	The list of persons and workstations copying the traffic who (provided that other conditions are met)  - trigger the rule  - do not trigger the rule
Rule validity days	The list of days of the week on which the rule can be triggered
Rule validity time	The time interval during the day when the rule can be triggered
Notify	List of user of the Console who will be notified when the rule is triggered **Note:** If after the rule is created, the user or his e-mail are deleted from the System (on managing user accounts, see *"Administration Guide"*, section "Users"), a notification will not be sent to this user.
Assign verdict to the event	A verdict which will be assigned to the object when the rule is triggered. Possible values: *Allow*, *Block*, *Quarantine*. **Note:** This option is available in data protection policies on agents only.
Assign violation level to event	The violation level which will be assigned to the object when the rule is triggered. Possible values: *High*, *Medium*, *Low*, *No violation*.
Assign tags to event	The list of tags which will be assigned to the object when the rule is triggered (see "Tags")
Assign status to initiators	The status which will be assigned to senders when the rule is triggered (see "Statuses")
Delete event	If this option is selected, then the event will not be saved to the database and actions specified in the rule will not be performed. By default, this setting is disabled. **Note:** In data protection policies on agents, events cannot be deleted.

User's target actions:

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

Rule of Placement

> **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.

Attributes of the rule of placement:

Parameter	Description
Event type	The type of traffic the placement of which triggers the rule provided that other conditions are met. Possible choices: • Crawler
Storage	Storing secured data in these storages will:  - trigger the rule  - do not trigger the rule To specify a storage, click  and in the dialog 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 fields: - in the **Enter network resource** field, enter a full name of the computer; - in the **Enter path** field, enter the path to the resource in the following format: `<directory>\<subdirectory>` (using wildcards such as ? or * is not supported). For example, *share|123* • **File storages**. To add a SharePoint file storage, enter the following values in the fields: - in the **Enter a source** field, enter IP address or a full DNS name of the file storage; - in the **Enter a path to storage** field, enter the path to the storage in the format: `<directory> /<subdirectory>` (using wildcards such as ? or * is not supported). For example, *Lib/Project documentation* When you specify all required storages, click **Save**.

Parameter	Description
File owners	The rule is triggered when specified persons, groups or elements of perimeters are detected among file owners. If the attribute is denied, the rule is triggered when persons, groups or elements of perimeters not included in the list are detected among file owners.
Who has access to file	The rule is triggered if specified persons, groups, and elements of perimeters have access to the file. If the attribute is denied, the rule is triggered when persons, groups or elements of perimeters not included in the list have access to the file.
Notify	List of the Console users who will be notified when the rule is triggered **Note:** If after the rule is created, the user or his e-mail are deleted from the System (on managing user accounts, see *"Administration Guide"*, section "Users"), a notification will not be sent to this user.
Assign violation level to event	A violation level which will be assigned to the object when the rule is triggered. Possible values: *High*, *Medium*, *Low*, *No violation*.
Assign tags to event	The list of tags which will be assigned to object when the rule is triggered (see "Tags")
Assign status to senders	A status which will be assigned to senders when the rule is triggered (see "Statuses")
Delete event	If this option is selected, then the event will not be saved to the database and actions specified in the rule will not be performed. By default, this setting is disabled.

User's target actions:

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

Clipboard Rule

> **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.

Attributes of the clipboard control rule:

Parameter	Description
Persons	List of persons, their groups, and perimeters. When traffic is sent by specified persons or groups or leaves specified perimeters, it will (provided that other conditions are met): - trigger the rule;  - not trigger the rule.
Computers	When traffic is sent from specified computers, it triggers the rule
Terminal session only	Selecting this option means that the receiver application for the event should be a terminal session. If the option is selected, choosing the receiver application manually is unavailable.
Source application	When copying data from specified applications to the clipboard (provided that other conditions are met), it will: - trigger the rule;  - not trigger the rule
Receiver application	When pasting data from the clipboard to specified applications (provided that other conditions are met), it will: - trigger the rule;  - not trigger the rule **Note**: if **Terminal session only** parameter is enabled, selecting the receiver application is unavailable.
Rule validity days	Days of the week when the rule can be triggered
Rule validity time	Time interval during the day when the rule can be triggered
Notify	List of the Console users who will be notified when the rule is triggered **Note:** If, after the rule is created, the user or user e-mail are deleted from the System (on managing user accounts, see *"InfoWatch Traffic Monitor. Administration Guide"*, "Users" section), this user will get a notification.
Assign violation level to event	A violation level assigned to the object when the rule is triggered. Possible values: *High*, *Medium*, *Low*, *No violation*.

Parameter	Description
Assign tags to event	The list of tags assigned to the object when the rule is triggered (see "Tags")
Assign status to senders	The list of tags assigned to the object when the rule is triggered (see "Tags")
Delete event	If this option is selected, then the event is not saved to the database and actions specified in the rule are not performed. By default, this setting is disabled.

User's target actions:

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

Person Control Rule

Attributes of the person control rule:

Parameter	Description
Violation level	Events with a specified violation level will be intercepted
Connect with policy	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)
Notify	List of the Console users who will be notified when the rule is triggered **Note:** If, after the rule is created, the user or user email are deleted from the System (on managing user accounts, see *"Administration Guide"*, "Users" section), a notification will not be sent to this user.
Assign verdict to event	A verdict which will be assigned to the object when the rule is triggered. Possible values: *Allow*, *Block*, *Quarantine*.
Assign violation level to event	A violation level which will be assigned to the object when the rule is triggered. Possible values: *High*, *Medium*, *Low*, *No violation*.
Assign tags to event	The list of tags which will be assigned to the object when the rule is triggered (see "Tags")
Assign status to senders	A status that will be assigned to initiators of the event when the rule is triggered (see "Statuses")

Parameter	Description
Delete event	If this option is selected, then the event will not be saved to the database and actions specified in the rule will not be performed. By default, this option is disabled.

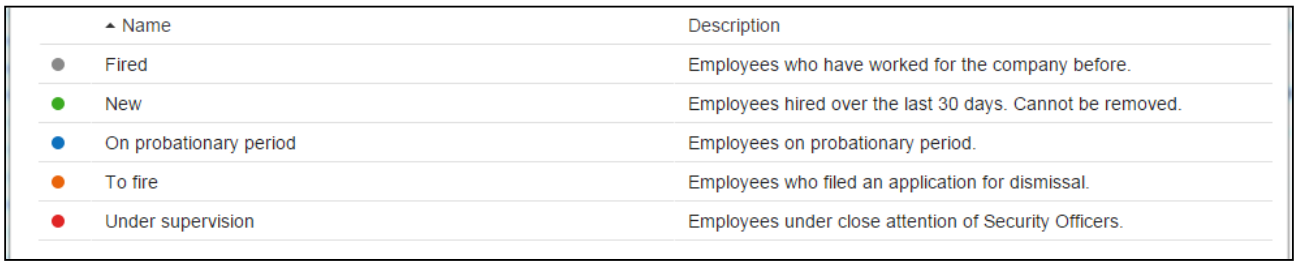
User's target actions:

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

3.8 Lists Section

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

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



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

Lists section, the list of statuses

The section contains the following catalogs:

- Tags
- Web resources
- Statuses
- Perimeters
- List of files

User's target actions:

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

3.8.1 Tags

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

There are the following preset tags in the System:

- **Under supervision** - events that indicate persons' suspicious activity

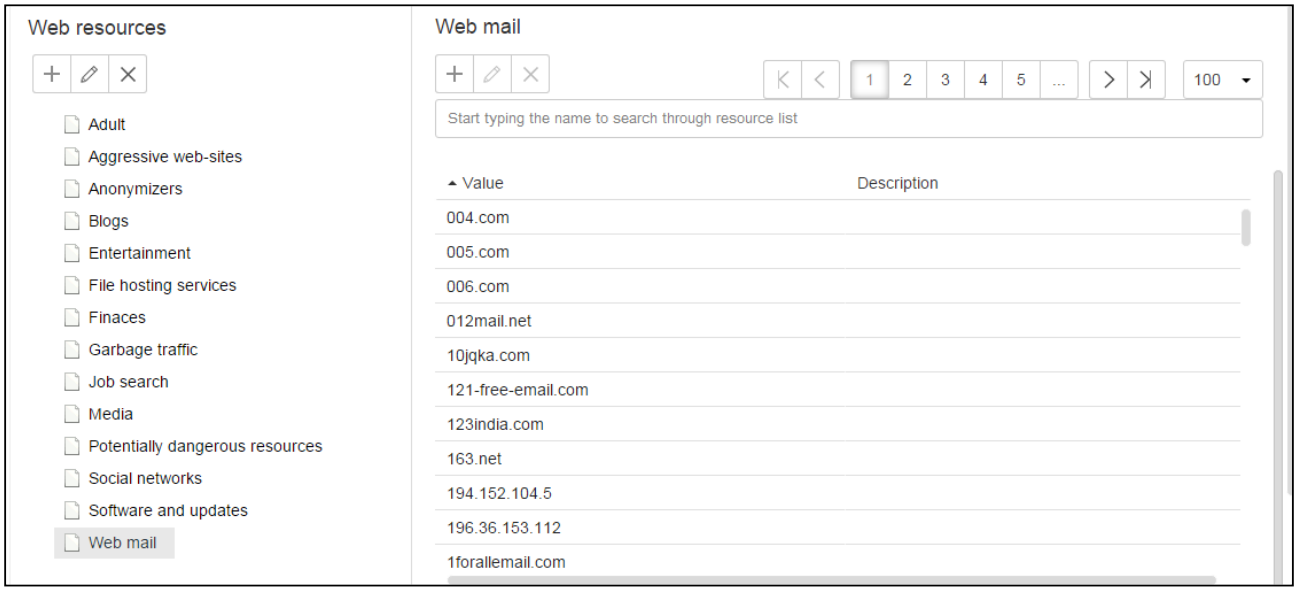
- **VIP** - events from persons who belong to the company authorities

User's target actions:

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

3.8.2 Web Resources

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



The System includes the following preset lists of web resources:

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

User's target actions:

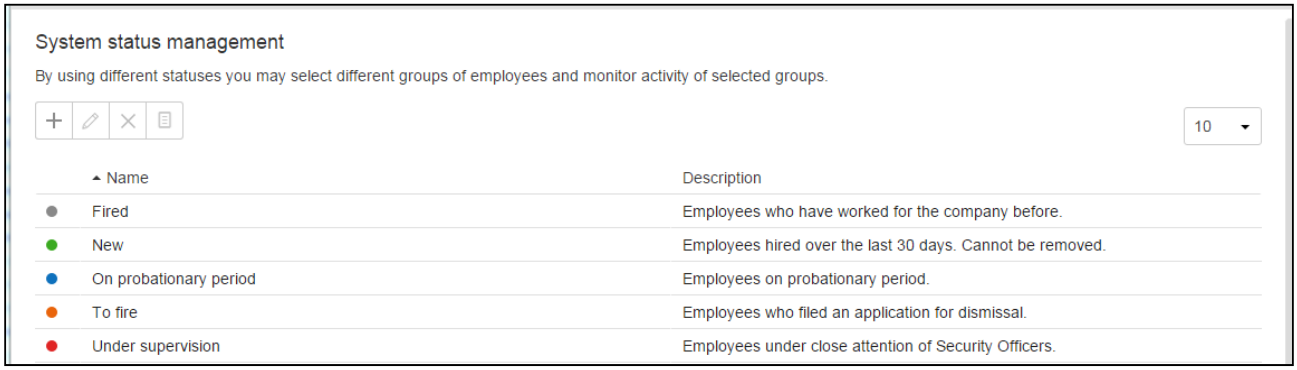
- Creating a list of resources (see "Managing Web Resources")

3.8.3 Statuses

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

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

For each status, a color mark is set.



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

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

User's target actions:

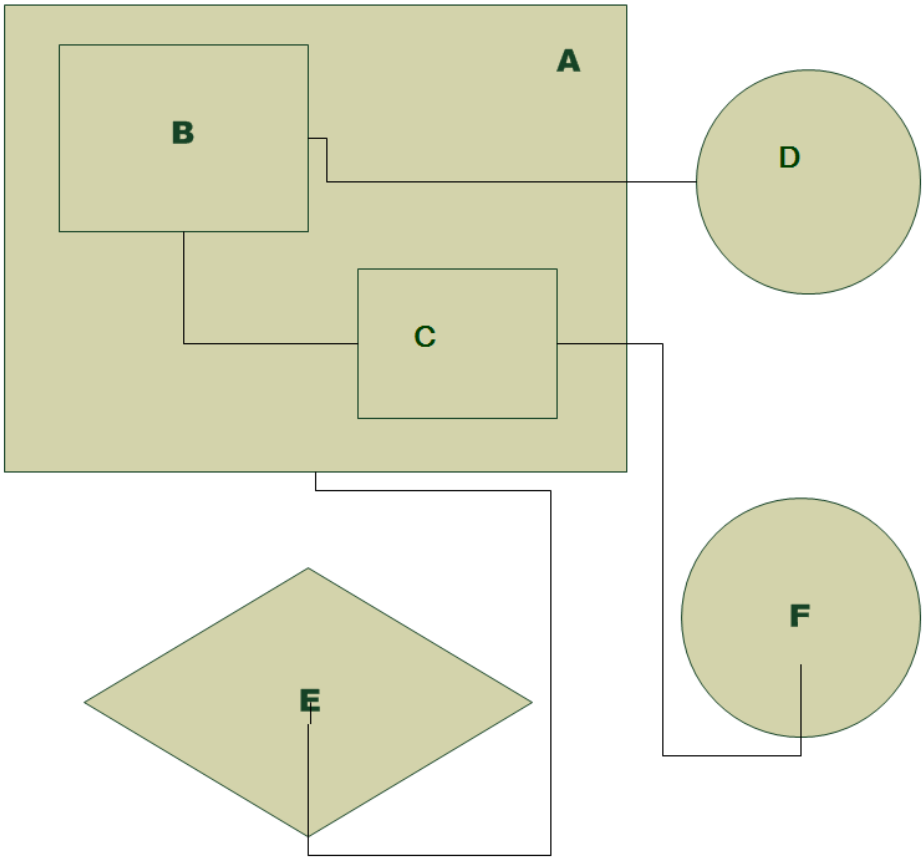
- Creating a list of statuses (see "Managing statuses")
- Manual assigning status to a person or workstation to monitor its activities or to visually distinguish them (see "Adding a Status to Person or Workstation")
- Automatic assigning status to a sender when the rule is triggered (see "Rules and their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

3.8.4 Perimeters

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

For example:

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



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

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

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

The System includes the following preset perimeters:

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

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

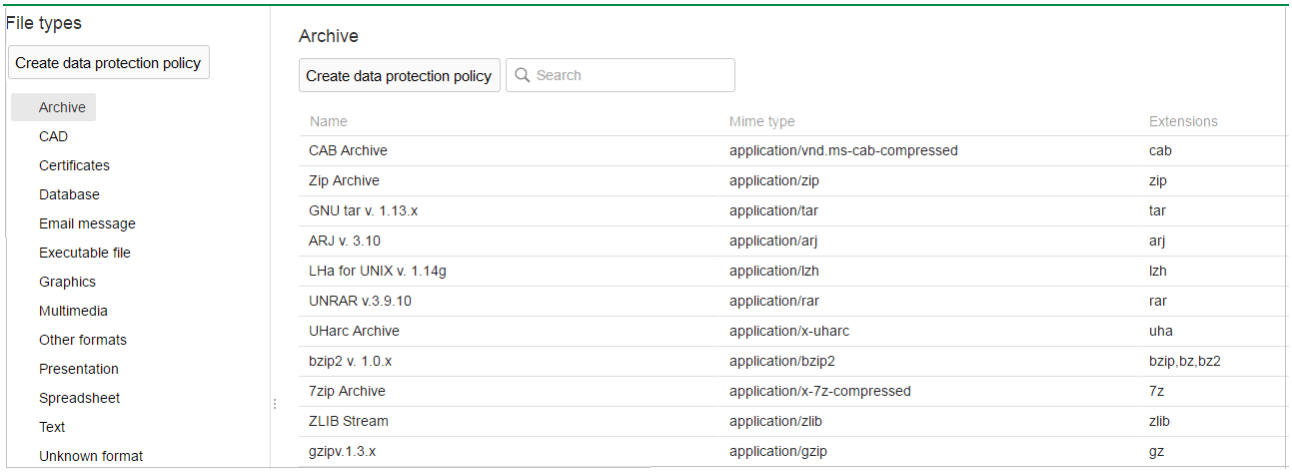
User's target actions:

- Building perimeters (see "Managing perimeters")

3.8.5 File Types

Reference information:

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



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

The tab contains the following elements:

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

Warning!

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

User's target actions:

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

3.9 Crawler Section

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

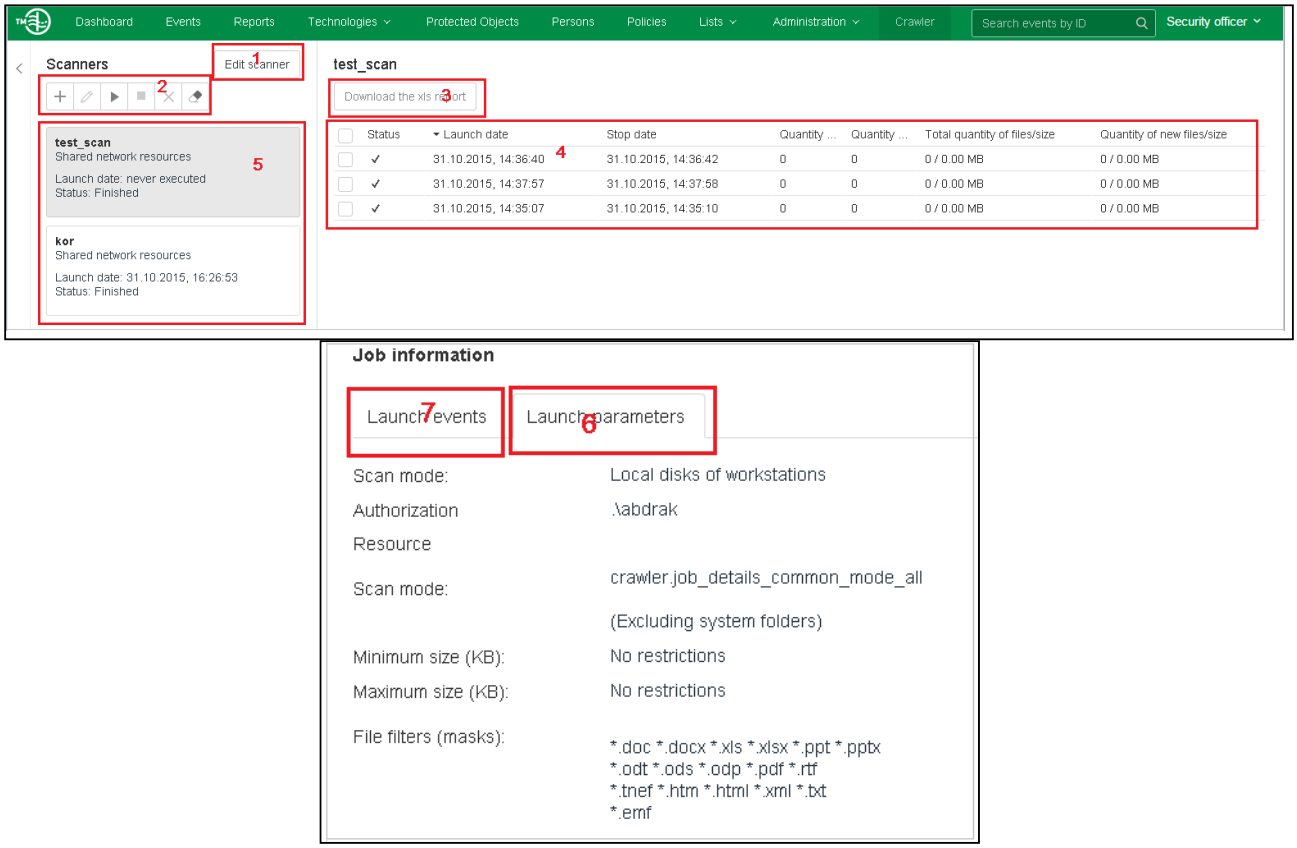
InfoWatch Crawler provides the following functions:

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

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

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

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



The section contains the following elements:

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

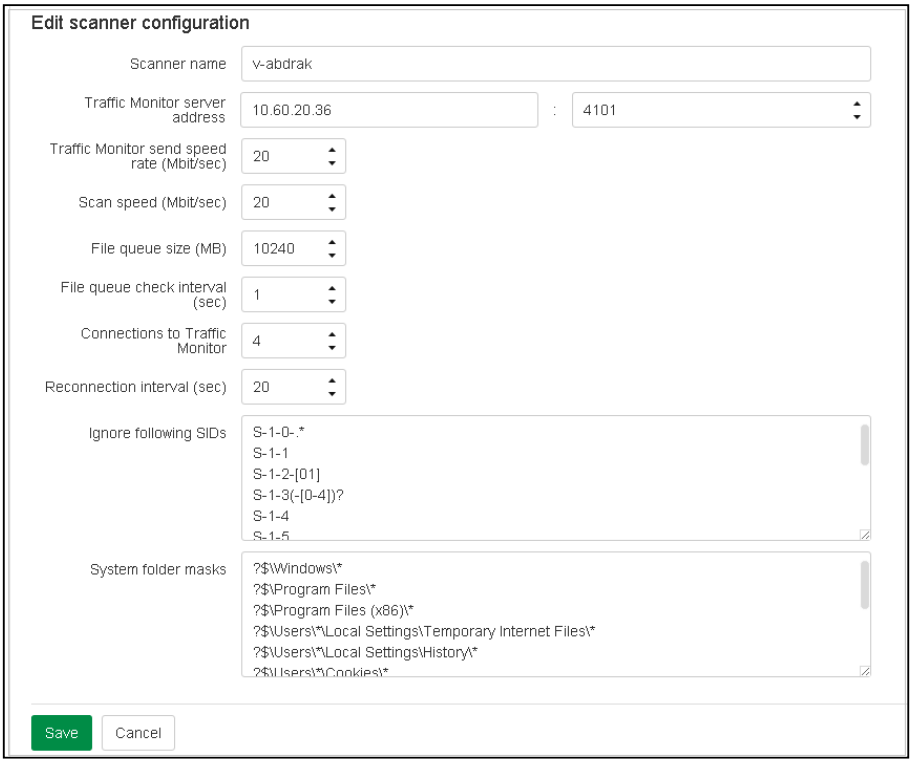
User's target actions:

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

3.9.1 Scanner

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

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



Scanner attributes:

Parameter	Description
Scanner name	Name of the scanner

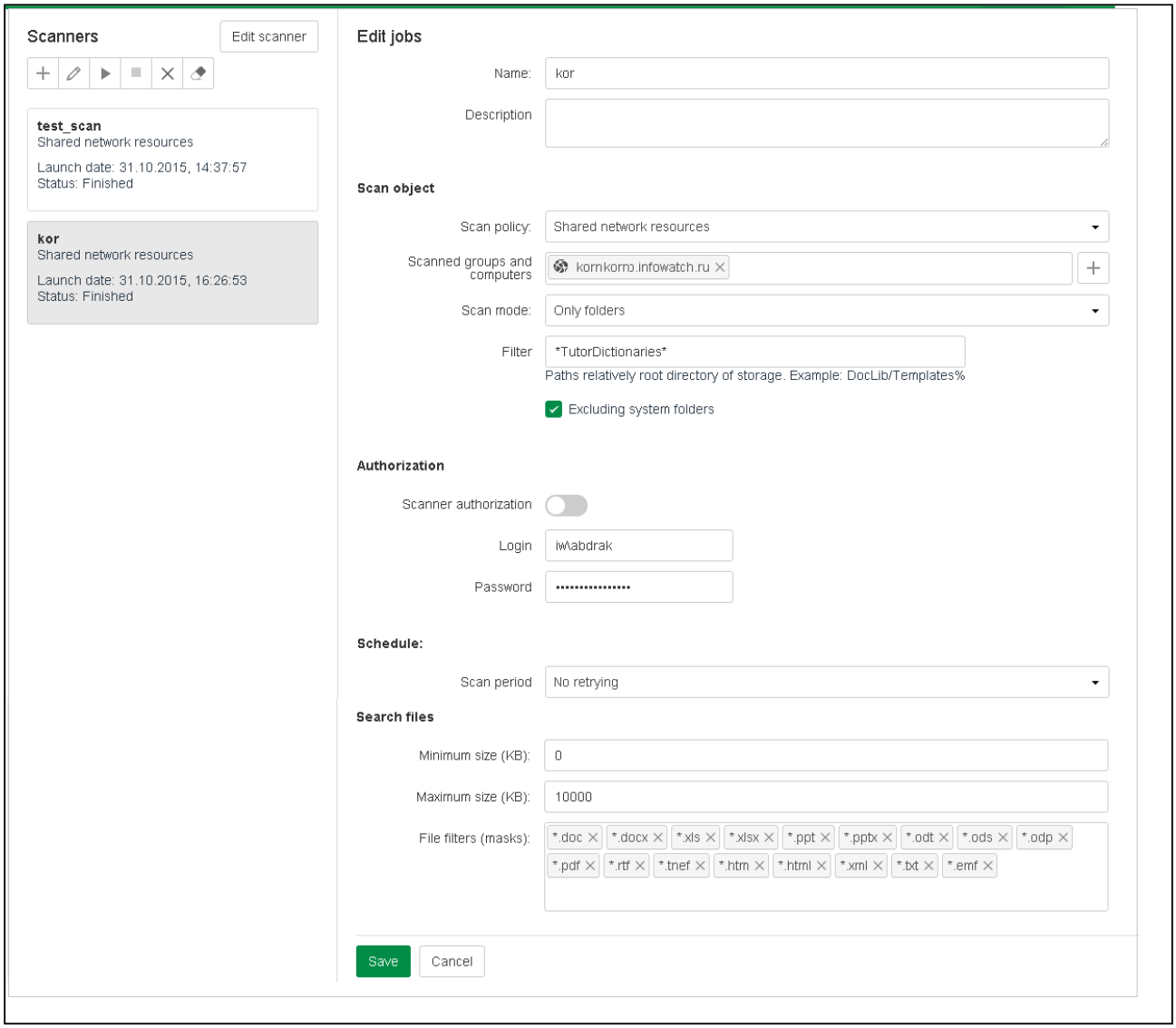
TM server address	The IP-address of the Traffic Monitor server hosting `iw_expressd`
Traffic Monitor sending speed (Mbit/s)	Maximum speed of uploading files to the Traffic Monitor server, Mbit/s Allows reducing the load on the Traffic Monitor server if the number of transmitted files is large
Scanning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

User's target actions:

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

3.9.2 Scanning Job

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



Job attributes:

Parameter	Description
Name	Name of the job
Description	Job description

Scan policy	Type of scan job: • **Shared network resources** **Warning!** Crawler does not support using more than one Astra Linux domain to scan shared network resources. • **Local drives of workstations** When using the **Local drives of workstations** policy, the **Use simple file sharing** option must be disabled on workstations where Windows XP is installed (**Control Panel** -> **Folder Options**, **View** tab) • **SharePoint file storage** Depending on SharePoint version, specify the following parameters: **For SharePoint 2007 and 2010:** • **SharePoint version** - SharePoint version: 2007 or 2010; • **Address of DB resource** - enter address of SharePoint database server, e.g. `sharepoint-test`; • **Name of DB resource** - enter the name of SharePoint database instance, e.g. `wss_content`. **For SharePoint 2013:** • **SharePoint version** - SharePoint version: 2013; • **SharePoint server address** - enter address of SharePoint database server with the protocol (http:// or https://).
Scanned groups and computers	Group of persons and workstations to be scanned

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

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

User's target actions:

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

4 Cases Solving in Traffic Monitor Management Console

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

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

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

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

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

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

4.1 Typical Actions

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

Typical actions include the following:

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

4.1.1 Login to the Management Console

Purpose:

Log into the Management Console.

Solution:

To log into the Management Console:

1. Open the browser Google Chrome of actual version (if the browser is not installed, you can download it by clicking on the link).
2. Open the address provided by the system administrator. The browser window will display the Management Console start page.
3. In the **Login** field, specify the username.
4. In the **Password** field, specify the password.

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

5. Click **Login**.

To log out of the Management Console:

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

4.1.2 Applying System Configuration

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

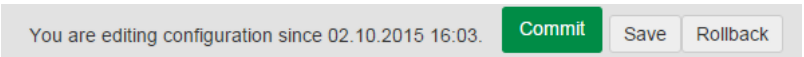
- Technologies
- Protected objects
- Persons
- Policies
- Lists

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

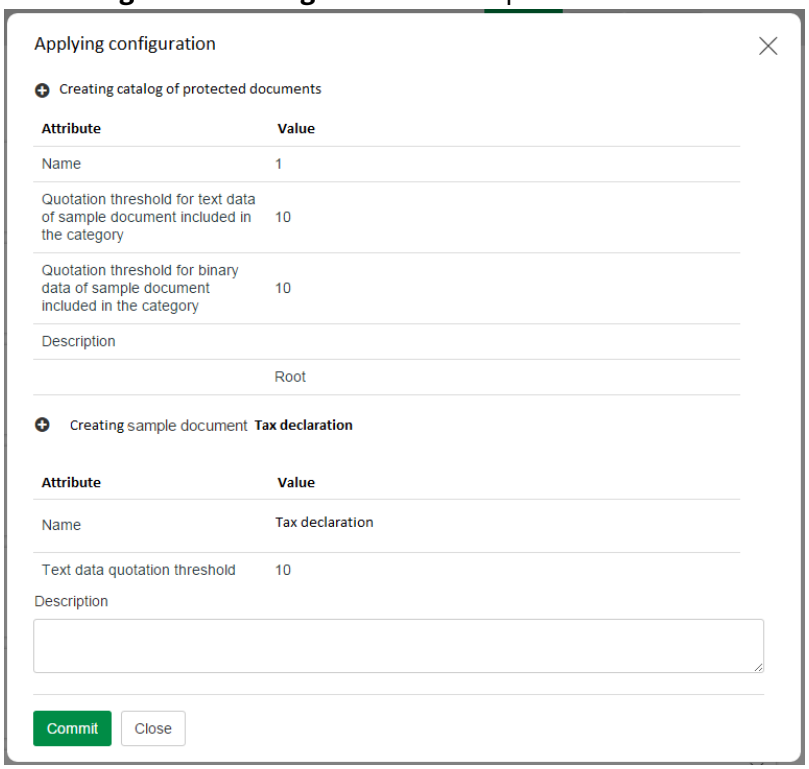
Purpose:
Apply the System configuration.

Solution:

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



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



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

4.1.3 Editing Element

Purpose:
Change attributes of an earlier created element.

Solution:

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

4.1.4 Deleting Element

Purpose:
Delete an element.

Solution:

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

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

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

4.1.5 Pages Navigation

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



Pages navigation panel

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

Solution:

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

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

4.1.6 Changing User Password

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

Purpose:
To change the password.

Solution:

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

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

3. Click **Save**.

4.1.7 Selecting Interface Language

Purpose:
Change the interface language of the Management Console.

Solution:

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

Do the same steps to revert English language if necessary.

4.1.8 Calling Help File

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

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

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

4.1.9 Viewing Information on System

Purpose:
Get general information about the System.

Solution:

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

4.2 Managing Persons and Computers

Why do you need persons and computers:

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

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

Creating lists of persons and computers include the following steps:

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

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

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

See also:

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

4.2.1 Creating Group of Persons or Computers

Purpose:
Create a group of persons or computers.

Solution:

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

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

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

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

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

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

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

Example:

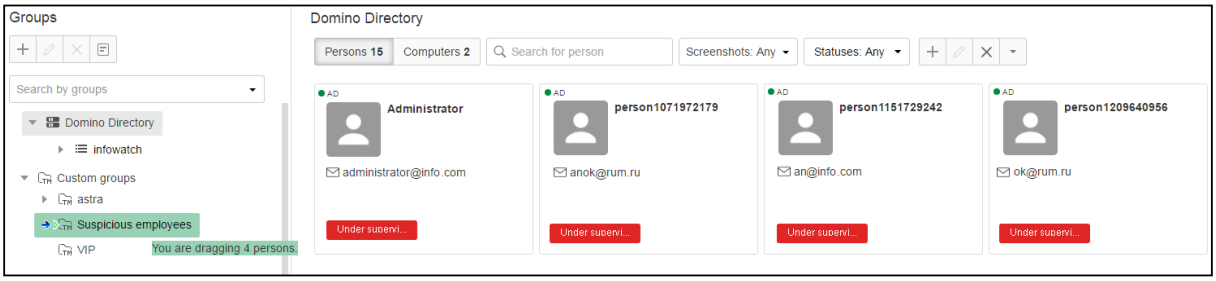
You need to add suspicious employees to a separate group. For this:

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

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

3. Add the found persons to the group.

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



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

Additional information:

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

- Editing Element
- Deleting Element

4.2.2 Creating Persons and Computers

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

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

Purpose:
To fill a group of persons and computers.

Solution:

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

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

- Editing Element
- Deleting Element

4.2.3 Configuring Person's Card

Purpose:

Fill the card of person with data.

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

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

Adding Contact to Person

Purpose:
Add or edit contact information for the person.

Solution:

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

Note:

Contact values must be specified in the following format:

- - mobile phone (string of 3 or more characters; may contain only digits, space, and the characters: "-","_", "( )","+");
- - landline phone (string of 3 or more characters; may contain only digits, space, and the characters: "-","_", "( )","+");
- - e-mail (e-mail address in RFC format);
- - Skype contact (string of 1 or more characters);
-  - Skype contact (string of 1 or more characters);

-  - WEB-identifier, for example, a profile on a social network (string of 1 or more characters);
-  - Lotus e-mail (string of 1 or more characters).

To edit previously specified contact details:

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

Adding Computer to Person

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

Solution:

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

Adding Person to Group

Purpose:
Add a person to an existing group.

Solution:

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

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

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

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

4.2.4 Configuring Computer Card

Purpose:
Add data to a computer card.

Configuring a computer card consists of the following actions:

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

Adding Contact to Computer

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

Solution:

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

Adding Person to Computer

Purpose:
Add a computer linked to a person.

Solution:

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

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

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

Adding Computer to Group

Purpose:
Add computer to an existing group.

Solution:

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

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

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

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

4.2.5 Adding Status to Persons

Purpose:
To add status to a person or computer.

Solution:

1. Go to the **Persons** section.
2. On the left part of the workspace, left-click the target group.
3. On the right part of the workspace, click on the tab:
   - **Persons** - to add status to a person;
   - **Computers** - to add status to a computer.
4. Select the target user or the target computer.

5. On the toolbar in the right part of the workspace, click ▾ and, in the drop-down list, select **Set status**.
6. In the dialog box that appears, specify the desired status and, if necessary, enter a description.
7. Click **Save**.

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

See also:

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

4.2.6 Viewing Screenshots

Preliminary settings:

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

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

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

   > **Примечание:**
   >
   > On workstations with Astra Linux OS, screenshots are not created.

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

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

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

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

Important!

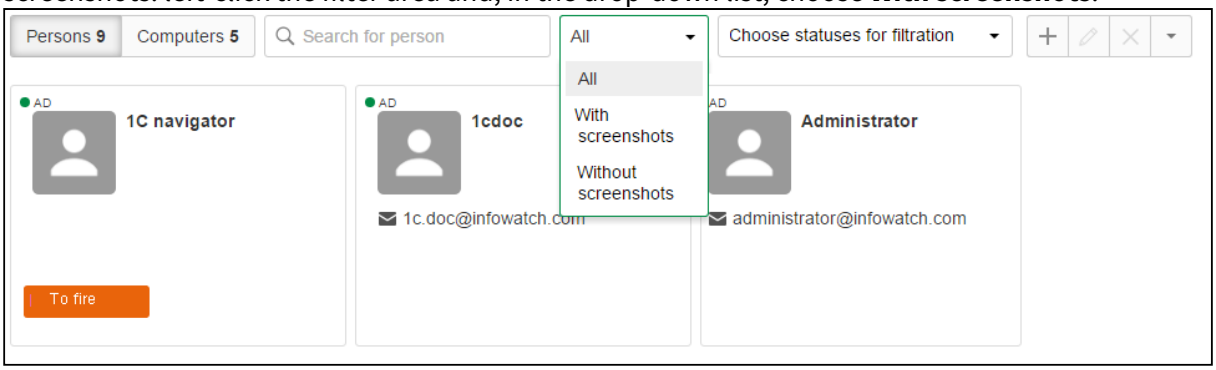
It is necessary to perform specified actions prior to creating a Device Monitor rule (see "Configuring ScreenShot Monitor Rule (DM)") and deploying the Device Monitor policy, which includes this rule, to workstations. Otherwise, the System will not display screenshots.

Purpose:

View intercepted screenshots for a person or a computer.

Solution:

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



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

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

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

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

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

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

4.3 Managing Catalogs

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

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

Managing catalogs includes the following actions:

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

See also:

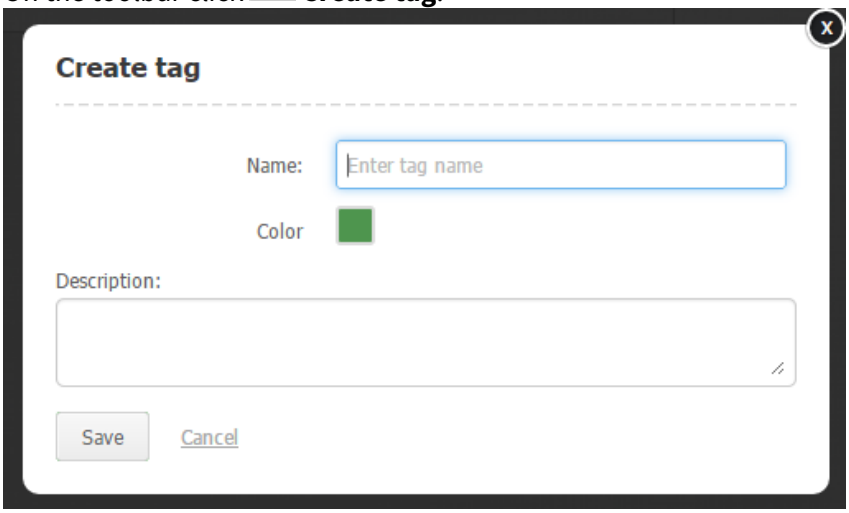
- "Lists Section" - on the section where you can manage catalogs

4.3.1 Managing Tags

Purpose:
To create a tag.

Solution:

1. Go to the **Lists** section, subsection **Tags**.
2. On the toolbar click + **Create tag**.



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

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

- Editing Element;
- Deleting Element.

4.3.2 Managing Web Resources

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

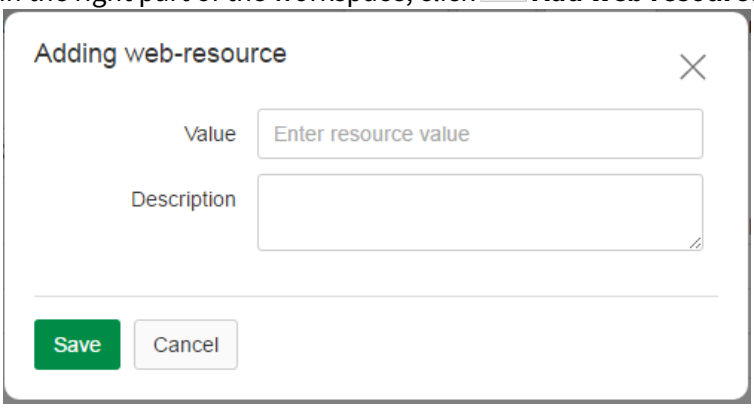
1. Create a list of web resources.
2. Add resources to the list.

Solution:

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

b. In the left part of the workspace, left-click the target resource list.

c. On the toolbar in the right part of the workspace, click + **Add web resource**.



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

e. Click **Save**.

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

Additional information:

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

- Editing Element
- Deleting Element

4.3.3 Managing Statuses

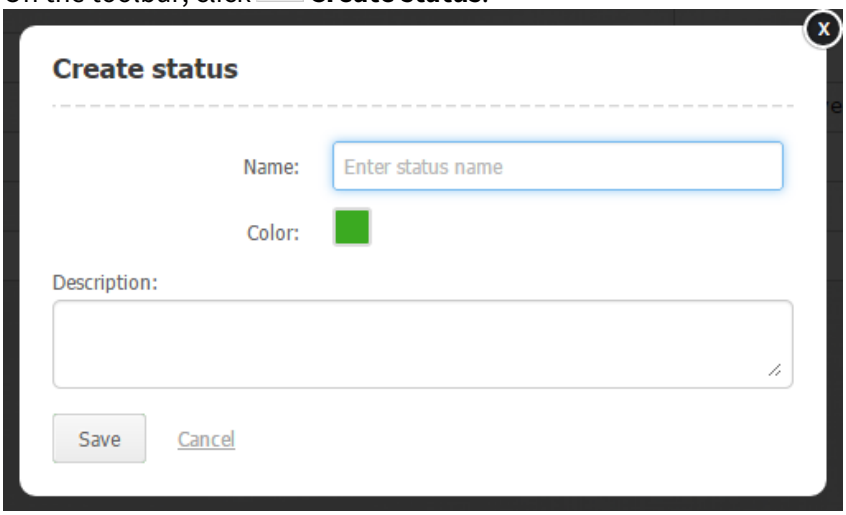
Purposes::

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

To create a new status:

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

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



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

To create a person control policy directly from Statuses subsection:

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

Additional information:

Statuses can be edited and deleted by standard means:

- Editing Element
- Deleting Element

4.3.4 Managing Perimeters

Reference information:

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

By default, the System includes the following perimeters:

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

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

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

- Email address
- Web resource
- Phone
- Skype contact
- ICQ contact

- Domain
- Lotus contact
- Person
- Person group

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

Purpose:

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

Solution:

1. Creating a perimeter.
   a. Go to the **Lists** section, **Perimeters** subsection.
   b. In the left part of the workspace, click + **Create perimeter**.
   c. In the window that opens, in the **Name** field, specify the name of the perimeter.
   d. In the **Description** field, enter a description (optional).
   e. Click **Save**.
2. To add an element to the perimeter.
   a. Go to the **Lists** section, **Perimeters** subsection.
   b. In the left part of the workspace, left-click the target perimeter in the list of perimeters.
   c. In the right part of the workspace, click **Add element to perimeter** and, in the drop-down list, select the desired element type.
   d. In the field that appears, specify one or more elements doing one of the following:
      - For *Persons*, *Group of persons* or *Resource type*:
        - start typing the name of the item in the field and select the desired entry from the drop-down list;
        - click + **Add** to the right of the field and, in the dialog window that opens, select desired elements. Then click **Save**.
      - For *E-mail address*, *Web-resource*, *Phone*, *Skype*, *ICQ*, *Domain,* and *Lotus contact* - enter the name (for example, of a web resource) or value (for example, of an IP address) in the field and click **Enter** on the keyboard.

> **Note:**
>
> If you specify a domain name of the first level, domains of nested levels will also not be included in the perimeter. For example, when you add the `domain.com` domain in the perimeter, the `basic.domain.com` domain of the nested level will also be considered.

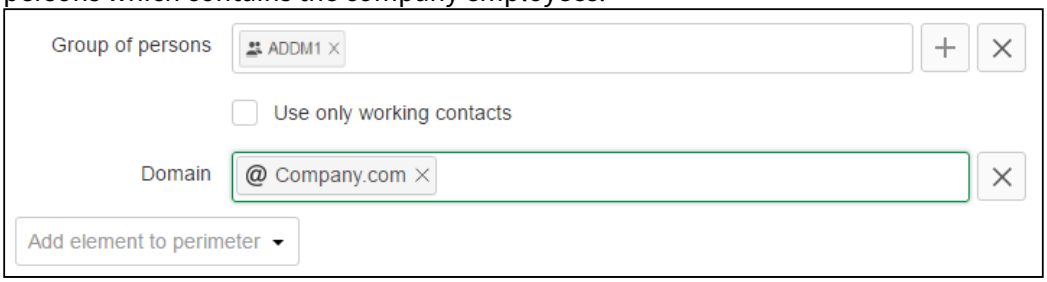
e. Entered values will be added to the list of elements. To remove a single element from the list, click ✕ next to the element name. To delete the entire list of elements of a particular type, click the ✕ button next to the line with a list of elements.



Example:

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

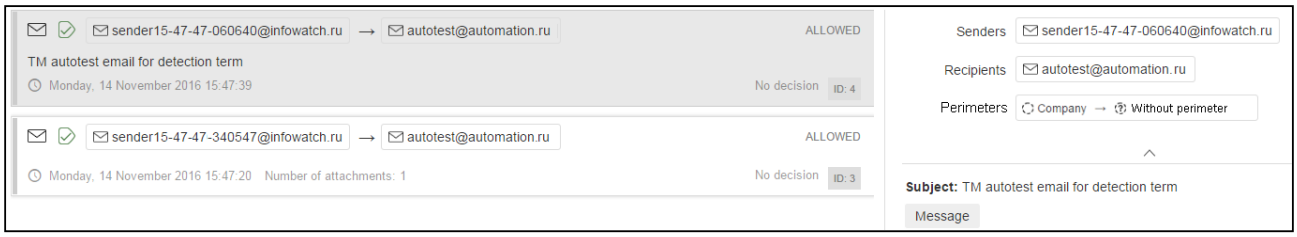
1. Create a *Company* perimeter (if the System already includes the *Company* perimeter, skip this step).
2. Add the following elements to the perimeter: `@company.com` mail domain and a group of AD persons which contains the company employees.



3. Save the perimeter.

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

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



Additional information:

Perimeters can be edited and deleted by standard means:

- Editing Element
- Deleting Element

4.4 Managing Base of Technologies

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

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

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

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

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

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

See also:

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

4.4.1 Defining the Confidential Information

Purpose:

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

Solution:

1. Go to a subsection of the **Technologies** section (**Categories and terms**, **Text objects**, **Sample Documents**, **Blanks**, **Stamps** or **Database Unloadings**).

Note:

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

2. Create a new category in the **Categories and terms** subsection or a new catalog in other subsections.
3. Fill the created category (or created catalog) with examples of confidential data that will indicate violations of the security policy if found in traffic.
4. If necessary, repeat steps 2 and 3.

Warning!

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

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

Technology name	Technology description	Action
Categories and terms	A set of terms and their categories. The term is a word or phrase which (if found in the analyzed text) increases the degree of conformity of the text to the category of the found term.	Creating terms and their categories
Text objects	Text information extracted from the object body and its attachments. Contains no formatting or markup. Applies and solving analysis tasks and search.	Creating text objects
Sample documents	Document quotes from which are searched in the analyzed text. Memos, financial reports, contracts, and other sensitive documents can all be used as sample documents. Sample documents are stored in the system as digital prints, their text is not available to either users or System administrators	Creating Sample Documents
Blanks	Blank whose version is searched for in the network traffic. Blanks may be different questionnaires, receipts, etc. Blanks are stored in the System as digital fingerprints, their text is not available for viewing either by users or by the System administrators.	Creating Forms
Stamps	Stamp image that is searched in the network traffic. Stamps can be images of round impressions used in organizations.	Creating Stamps
Database unloadings	A part of a database quotes from which are searched in the analyzed text. Database unloadings can be lists of salaries, other personal data, etc.	Creating Database Unloadings

Graphical objects	Image of particular type that is searched in the network traffic. Graphical objects can be images of credit cards or technical drawings.	The System contains only preset graphical objects. Creating or editing graphical objects is unavailable.

See also:

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

Managing Categories and Terms

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

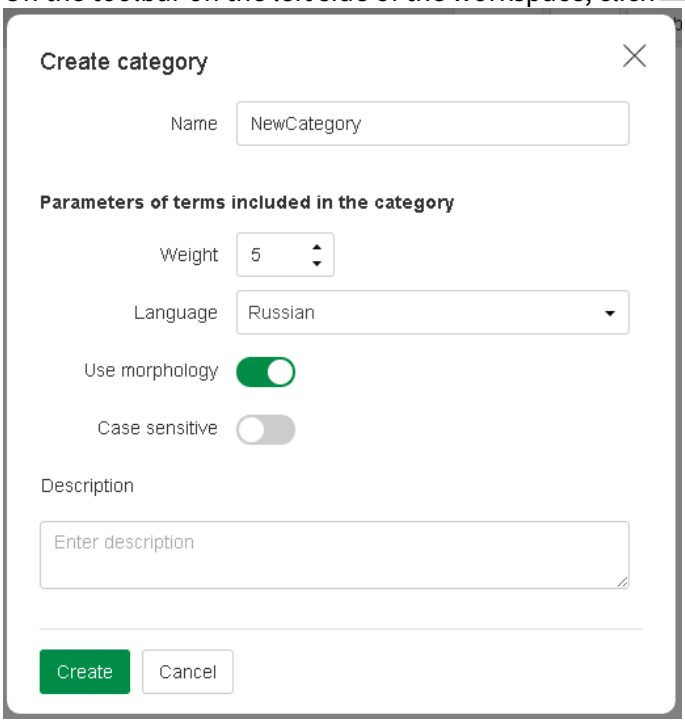
Purposes:

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

Solution:

1. To create a category.

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



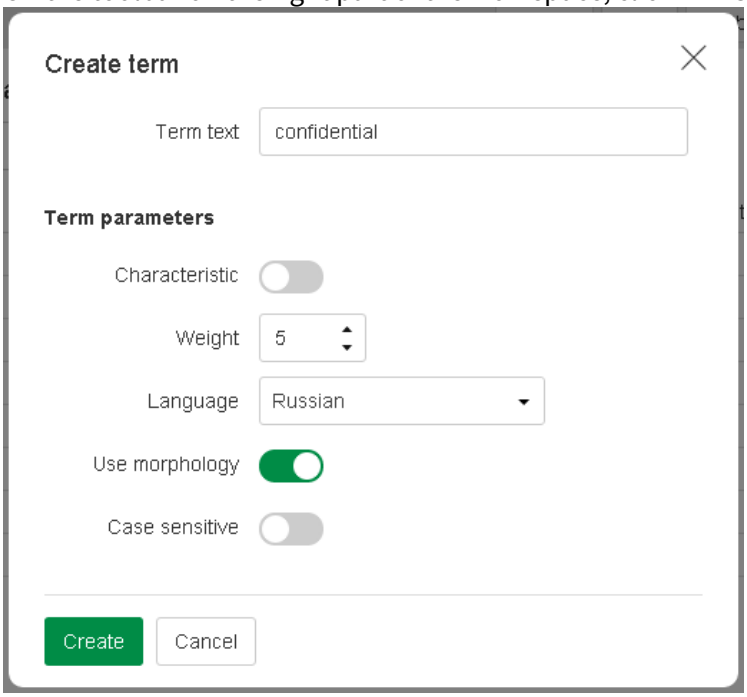
c. Specify required attributes for the category (see "Categories").
d. Click **Create**.

2. Creating a term.

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

> **Note:**
>
> For terms adding only those categories that do not include other nested categories are available.

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



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

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

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

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

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

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

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

Warning!

The interception object receives only the category that contains the actuated element (term, sample document, etc.).
For example:
Category A contains category B. Category B includes the term C. During the event analysis, the System detected the presence of the term C in the event body.
In this case, only the term C and category B will be assigned to the interception object.

Additional information:

Editing and deleting terms are performed by standard means:

- Editing Element;
- Deleting Element.

Managing Text Objects

Purposes:

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

Solution:

1. Create a catalog of text objects.

a. Go to the section **Technologies** -> **Text objects**.
b. On the toolbar on the left side of the workspace, click  **Create a catalog of text objects**.
c. In the window that opens, type a name and description for the catalog.
d. Click **Save**.

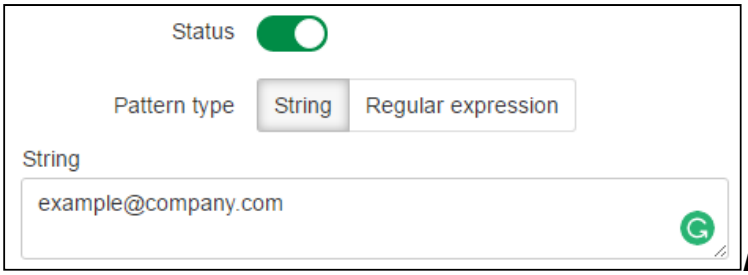
2. Create a text object and specify its value.

a. Go to the section **Technologies** -> **Text objects**.
b. On the left part of the workspace by clicking the left mouse button, select the catalog inside which you want to create a text object.
c. On the toolbar for working with text objects located on the right side of the workspace, click  **Create a text object**.
d. Enter the name and description of the text object.
e. Click **Create**. The new text object will be added to the list.
f. Select the text object in the list and click  **Edit**.
g. Create a template for the text object and specify its parameters (see "Text objects patterns").
h. Click **Save**.

Example 2:
If you want the System to determine the presence of the email address "example@company.com" in traffic and define it as a text object EXAMPLE_MAIL, then:

1. Create an active text object *EXAMPLE_MAIL*.

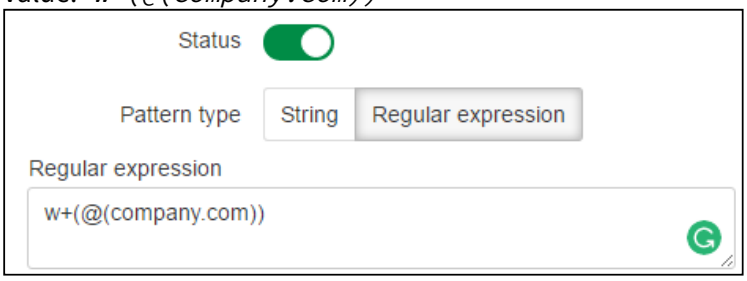
2. Select the object and switch to the edit mode.
3. Create a new active template for the text object and specify the following string as the template value:`example@company.com`:



Example 1:

If you want the System to determine the presence of email address with the domain “company.com” in traffic and define it as a text object*COMPANY_MAIL*, then:

1. Create an active text object 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:

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

3 Add a system text object to the catalog.

a. Go to the section **Technologies** -> **Text objects**. On the left part of the workspace left-click the target category.
b. On the left part of the workspace by clicking the left mouse button, select the catalog to which you want to add a text object.
c. On the toolbar for working with text objects located on the right side of the workspace, click ▾ and in the drop-down list select **Add system text object**.
d. In the window that opens, select check boxes next to the text objects you want to add.

Note:

To find required text objects in the list, enter the text in the **Search** string.

e. Click **Add**.

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

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

- Editing Element;
- Deleting Element.

Managing Sample Documents

Purposes:

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

Solution:

1. Create a catalog of sample documents

a. Go to the section **Technologies**->**Sample Documents**.
b. On the toolbar in the left part of the workspace click + **Create catalog of sample documents** .
c. In the window that opens, specify parameters for the new catalog (see "Sample Documents").
d. Click **Create**.

2. To create a sample document

a. Go to the section **Technologies**->**Sample Documents**.
b. On the left part of the workspace by clicking the left mouse button, select the catalog inside which you want to create a sample document.
c. On the toolbar for working with sample documents located on the right side of the workspace, click + **Add**.
d. In the dialog window that opens, select type of the data a sample document may contain: **Text** or **All types** (may contain text, images, and binary data).
e. Click **Choose files** and in the window that opens, specify the document which you want to use for creating a digital print. Click **Open**.
Choose a text file, an image or an archive to be uploaded according to the data type specified in step **d**. The following rules apply when uploading files:
    - If the format of the selected file is not supported by the System, the digital fingerprint will be uploaded as binary data.
    - If you upload an archive, then files from this archive will be added as sample documents.

- When the uploading is finished, the sample document will be added to the catalog. All necessary attributes are assigned to a newly created sample document by default.

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

> **Warning!**
>
> Requirements for file size:
> - Maximum size for binary data - 128 Mb;
> - Maximum size for text data - 30 Mb;
> - Minimal size for binary and text data – 128 байт;
> - Minimal plain text size for text data - 10 symbols;
> - Minimal image size - 100 pixels on one side;
> - Allowable aspect ratio - not bigger than 5 : 1.

a. To change the sample document attributes specified by the System, on the toolbar click **Edit** and change the required parameters (see “Sample Documents").

3 Update a sample document

a. Go to the section **Technologies**->**Sample Documents**.
b. On the left side of the workspace, select the desired catalog.
c. In the list in right part of the workspace, select the sample document you want to update.
d. Click **Edit**.
e. In the edit window that opens, click **Update**.
f. Click **Choose file**.
g. In the dialog window that opens, select a document that will be used for update, and click **Open**.
h. The file download will begin.After the download is finished, the sample document will be supplemented with new data in accordance with the selected update mode. If the System cannot perform an update, the download window will display an error message.

> **Note:**
>
> When updating a sample document, the System replaces data of the document being updated with the data from the update file.

Example 1:
If you need the System to react to transferring the "Internal regulations of the company” document if the traffic contains at least 30% of text from this document, then:

1. Select a catalog of sample documents or create a new one.
2. Add a new document to this catalog and specify the **Text** data type, as the document does not contain images or drawings.
3. Upload the "Internal rules of the company" file as a sample document.
4. Specify the sample document name, e.g., *INTERNAL_COMPANY_RULES.*
5. For the **Text data quotation threshold** attribute, specify the **30** value.

> **Note:**
>
> The quotation threshold is configured depending on the type of the protected document. Here, a low quotation threshold is specified, as the document consists of many pages and can be transferred in parts.

Example 2:
If you need the System to react to transferring the "Setup.exe" executable file if the traffic contains at least 10% of the binary content from this file, then:

1. Select a catalog of sample documents or create a new one.
2. Add a new document to this catalog and specify the **All data** type.
3. Upload the "Setup.exe" file as a sample document.
4. Specify the sample document name, e.g., *SETUP_EXE.*
5. For the **Text data quotation threshold** attribute, specify the **10** value.

For the System to track the presence of sample documents in the traffic, they must be included in protected objects.

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

- Editing Element;
- Deleting Element.

Managing Blanks

Purpose:

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

Solution:

1. Create a catalog of blanks

a. Go to the **Technologies**->**Blanks** section.
b. On the toolbar on the left part of the workspace, click + **Create a catalog of forms.**
c. In the window that opens, type a name and description of the catalog.
d. Click **Create**.

2. Create a blank

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

b. On the left part of the workspace by clicking the left mouse button, select a catalog inside which you want to create a blank.
c. On the toolbar for managing blanks which is located on the right part of the workspace, click **Add**.
d. In the dialog window that opens, select a document that will be used as a blank and click **Open**. You can upload a document in one of the following formats: DOC, DOCX, DOT, DOTM, DOTX, XLS, XLSX, XLT, XLTM, XLTX, ODS, ODT, RTF, TXT, VSD, HTML, HTM, PDF, CHM.
e. When the download is finished, the blank will be added to the catalog. All necessary attributes are assigned to a newly created blank by default.

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

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

3 Update a blank

a. Go to the **Technologies**->**Blanks** section.
b. On the left side of the workspace, select the desired catalog.
c. In the list on the right part of the workspace, select the blank you want to update.
d. Click **Edit**.
e. In the edit window that opens, click **Update**.
f. Click **Choose file**.
g. In the dialog window that opens, select a file that will be used for update, and click **Open**. The file download will begin.
h. Data of the blank will be replaced with data from the update file.
If the System cannot perform an update, the download window will display an error message.

Example:

If you need the System to mark the interception object as RECRUITMENT_CHECKLIST if the traffic contains fragments of the questionnaire "Recruitment checklist" (filled or not):

1. Create *RECRUITMENT_CHECKLIST* blank.
2. Load the document file “Recruitment checklist” as a blank.
3. Create a protected object based on the *RECRUITMENT_CHECKLIST* blank.
4. In detection conditions, select **Filled and unfilled** checkbox.

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

- Editing Element;
- Deleting Element.

Managing Stamps

Purposes:

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

Solution:

1. Create a catalog of stamps.

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

2. Create a stamp

a. Go to the section **Technologies**->**Stamps**.
b. On the left part of the workspace by clicking the left mouse button, select the catalog inside which you want to create a stamp.
c. On the toolbar in the right part of the workspace, click  **Add**.

> **Warning!**
>
> The uploaded file must contain only one stamp image.

d. In the dialog window that opens, select a document that will be used as a stamp and click **Open**.
e. When the download is finished, the stamp will be added to the catalog. All necessary attributes are assigned to a newly created stamp by default.

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

f. To change the stamp attributes specified by the System, on the toolbar click  **Edit** and change the required attributes.

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

Example:
If you need to protect legal documents sealed with a company stamp, then:

1. Prepare a file with the image of the company stamp.
2. In the **Technologies**->**Stamps** section, select the required catalog or create a new one.
3. Create a new stamp in the catalog and upload the prepared file with the stamp image.

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

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

- Editing Element;
- Deleting Element.

Managing DB Unloadings

Purpose:

1. Create a catalog of unloadings.
2. Create a database unloading.
3. Update the unloading.

Solution:

1. Create a catalog of unloadings

a. Go to the **Technologies**->**DB Unloadings** section.
b. On the toolbar on the left side of the workspace, click  **Create catalog of DB unloadings**.
c. In the window that opens, type a name and description for the catalog.
d. Click **Create**.

2. Create a database unloading

a. Go to the **Technologies**->**DB Unloadings** section.
b. In the left side of the workspace, select the group to which you want to add the unloading.
c. On the toolbar in the right part of the workspace, click  **Add**.
d. In the dialog window that opens, select a file in CSV or TSV format that you want to upload and click **Open**.

> **Note:**
>
> The uploaded file is then compiled. The amount of RAM consumed during compilation can be approximately calculated by the following formula: `Memory(GB) = 0.05 * unique_words(M) * cells(M)`, where M stands for million.
> For example, 10 million cells can fit in a table with 2 columns and 5 million rows, or in a table with 4 columns and 2.5 million rows.

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

e. When the file is uploaded:
   - click **Configure DB unloading** - to customize the unloading, or
   - close the **Creating DB unloading** window - to exit without additional configuration.

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

3 Update the unloading

1. Go to the **Technologies**->**DB Unloadings** section.
2. On the left side of the workspace, select the desired catalog.
3. In the list in the right part of the workspace, select the unloading you want to update.
4. Click **Edit**.
5. In the edit window that opens, click **Update**.
6. Specify the desired update mode: **Adding new records** or **Removing old records and adding new ones**.
7. Click **Choose file**.
8. In the dialog window that opens, select a file that will be used for update, and click **Open**. The file download will begin.
9. After the download is finished, the unloading will be supplemented with new data in accordance with the selected update mode. If the System cannot perform an update, the download window will display an error message.

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

- Editing Element;
- Deleting Element.

Detection Conditions for Unloading

Reference information:

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

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

Purpose:

Add a detection condition for an unloading.

Solution:

1. Go to the **Technologies**->**Database Unloadings** section.
2. In the left part of the working area, select the desired catalog.

3. In the right part of the working area, select a desired unloading from the list and click **Edit**. The unloading edit form will open.
4. On the toolbar under the **Conditions of unloading detection** caption, click **Add**.
5. In the dialog window that opens, specify the following parameters (you can find a detailed description of these parameters below):
   a. **Condition name**;
   b. **Minimal quantity of rows**;
   c. **Detection rule**.
6. Click **Create**.

When editing detection condition parameters, consider the following recommendations:

Detection rule.

The detection rule contains column numbers and logical relations between them. If the analyzed interception object contains data from specified cells, given the set relations, then this row is considered triggered.

> **Note:**
>
> To avoid false positives, the System uses stop-words: numbers, letters. and words, whose presence in cells results in not triggering these cells. You can find the whole list of stop-words in the InfoWatch Knowledge Base article "List of stop-words for database unloadings".

The **Available columns in selection** list contains columns that can be used for creating conditions.
The **Search** field allows you to find a required column by its name.

Logical relations are defined using the following symbols:

1. "+" - conjunction of cells (logical "AND");
2. "|" - disjunction of cells (logical "OR");

   > **Note:**
   >
   > A condition like (1|3) should be in parentheses.

3. "()" - a grouping of conditions. For example, a condition like 1+(2|3) means that the row is considered to be triggered if its first cell and either its second or its third cell are triggered.
   A condition like (1|3)+(5|4) means that the row is considered to be triggered if both the first or the third cells and the fifth or the fourth cells are triggered.

   > **Warning!**
   >
   > The "|" cannot be used to divide groups in parentheses. Thus, a condition like (1+8+11*)|(2+3*) should be specified as two separate conditions: 1+8+11* and 2+3*.

4. "*" - the asterisk symbol allows you to consider blank cells as well. For example, a condition like 1+2* means that the row is considered to be triggered if its first and second cells are triggered, wherein the second cell may be unfilled.

> **Warning!**
>
> The analysis technology does not consider special characters, so if the column contains an email address, then it is recommended that you should specify an additional column (e.g., Full name) in order to reduce false positives.

Minimal quantity of rows.

The minimal number of rows that must be detected to trigger the condition.

For example, if a condition like 1+(2|3) is specified and the minimal quantity of rows is set to 10, then for triggering the rule it is required that the analyzed text should contain at least 10 different rows that satisfy the condition 1+(2|3).

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

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

1. Save the table in CSV or TSV format and upload this file to the System.
2. Configure the detection rule:
   - in the **Detection rule** field, specify **1+4**
   - in the **Minimal quantity of rows** field, specify **7**
3. Create a protected object "PHONE_NUMBERS" based on the created DB unloading.

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

Additional information:
Editing and deleting detection conditions for the unloading are performed in a standard way:

- Editing Element
- Deleting Element

4.4.2 Exporting and Importing the Base of Technologies

Purpose:

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

> **Note:**
>
> While editing the System configuration, export and import of technologies are unavailable. In this case, an error message is displayed.

To export the technologies base:

1. Go to a subsection of the **Technologies** section (**Categories and terms**, **Text objects**, **Sample Documents**, **Blanks**, **Stamps** or **Database Unloadings**).
2. On the toolbar on the left part of the workspace, click and, in the drop-down list, select **Export**.
3. In the **Save as** window that opens, specify the location on disk where to save an XML file.
4. Click **Save**. The XML file will be saved to your computer. This file contains the following elements:
   - categories and terms;
   - text objects, including pre-installed ones;
   - sample documents;
   - blanks;
   - stamps;
   - database unloadings;
   - graphical objects.

   The structure of catalogs is preserved for all elements.

   > **Warning!**
   >
   > 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 XML document:

1. Go to a subsection of the **Technologies** section (**Categories and terms**, **Text objects**, **Sample Documents**, **Blanks**, **Stamps** or **Database Unloadings)** .
2. On the toolbar on the left part of the workspace, click and in the drop-down list select **Import**.
3. In the **Open** dialog window, select XML file that you want to load.
4. Click **Open** and wait till the data is loaded into the System.

Note:

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

Features of merging data during import:

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

   Note:

   The verifying functions that are present in the System will be replaced by functions from the file.

4. For a DB unloading, representations of the sample unloading will be added, if the contents of unloading in the System and the file are the same.

4.5 Managing Protected Objects

Important!

For the changes described in this section to be used in the System, apply the configuration: see "Configuring the System" and "Applying System Configuration".

What are protected objects needed for:

Protected objects make it possible to check if intercepted data contain all specified elements of analysis: for example, a sample document, a text object, and a database unloading. Thus, you can configure the System so that it could detect certain business documents: for example, a vehicle registration certificate or a declaration of insurance payment.

Working with protected objects includes the following actions:

Action	Description
Creating a catalog of protected objects	Creating a catalog to which protected objects will be added
Creating a protected object	Creating a protected object and specifying its parameters
Adding elements of analysis	Adding elements of analysis to a protected object

Adding detection conditions	Specifying conditions for detecting added elements of analysis
Creating policies for protected objects and their catalogs	Creating a data protection policy for selected protected objects and their catalogs
Import and export of protected objects	Importing and exporting catalog structure, protected objects included in these catalogs and elements of analysis used in these protected objects
Activating and deactivating protected objects	Changing status of protected objects and their catalogs

See also:

- "Protected Objects Section" - on the section where you can manage protected objects

4.5.1 Creating a Catalog of Protected Objects

Purpose:
Create a catalog that will contain protected objects.

Solution:

1. Go to the **Protected objects** section.
2. On the toolbar in the left part of the workspace, click + **Create catalog of protected objects**.

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

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

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

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

Additional information:

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

- Editing Element;
- Deleting Element.

4.5.2 Creating a Protected Object

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

Solution:

1. Go to the **Protected objects** section.
2. On the left side of the workspace, select a catalog to which you want to add a new protected object, or create a new catalog (see "Creating Catalog of Protected Objects").
3. On the toolbar in the right part of the workspace, click  **Create Protected Object**.
4. In the window that opens, select elements based on which the protected object will be created (see "Adding Elements of Technologies").
5. Determine whether selected items should be included in one protected object, or a separate protected object should be created for each element:
    - If **Create a protected object for each selected item** option is selected, a set of protected objects for each selected element of technologies will be created. Attributes of the created protected objects are generated automatically. Object names are generated based on the name technology and the element name, for example: "*Text object: Credit card number*".
    - If **Create a protected object for each selected item** option is not selected, then clicking **Create** opens an additional window where you can specify settings for the protected object: see step 7.
6. Click **Create**.
7. If **Create a protected object for each selected item** option has not been selected at step 5, the **Creating a protected object** window will open. In this window:
    a. Enter the name of protected object.
    b. On the **Elements of technologies** tab, that contains the selected items (see "Elements of Technologies"), you can add additional elements of technologies (for this, click **Select elements**) or remove elements from the list: for this, click ' x ' button in the row of the selected element.
    c. On the **Detection conditions** tab, specify conditions under which protected objects should be detected in intercepted data (for details, see "Adding Detection Conditions").
    d. If necessary, enter a description in the **Description** field.
    e. Click **Create**.

As a result, a protected object is created in the selected catalog (if you have selected the **Create a protected object for each selected item** option, several protected objects are created).
You can move the created protected object to another catalog.
To do this, select the required protected object in the list, press the left mouse button and move the protected object to the desired catalog holding the left mouse button pressed. Then release the mouse button.

Example:
If you need to create a protected object *"Manager Personal Number"* that should be detected in the System when one of the following conditions is fulfilled:

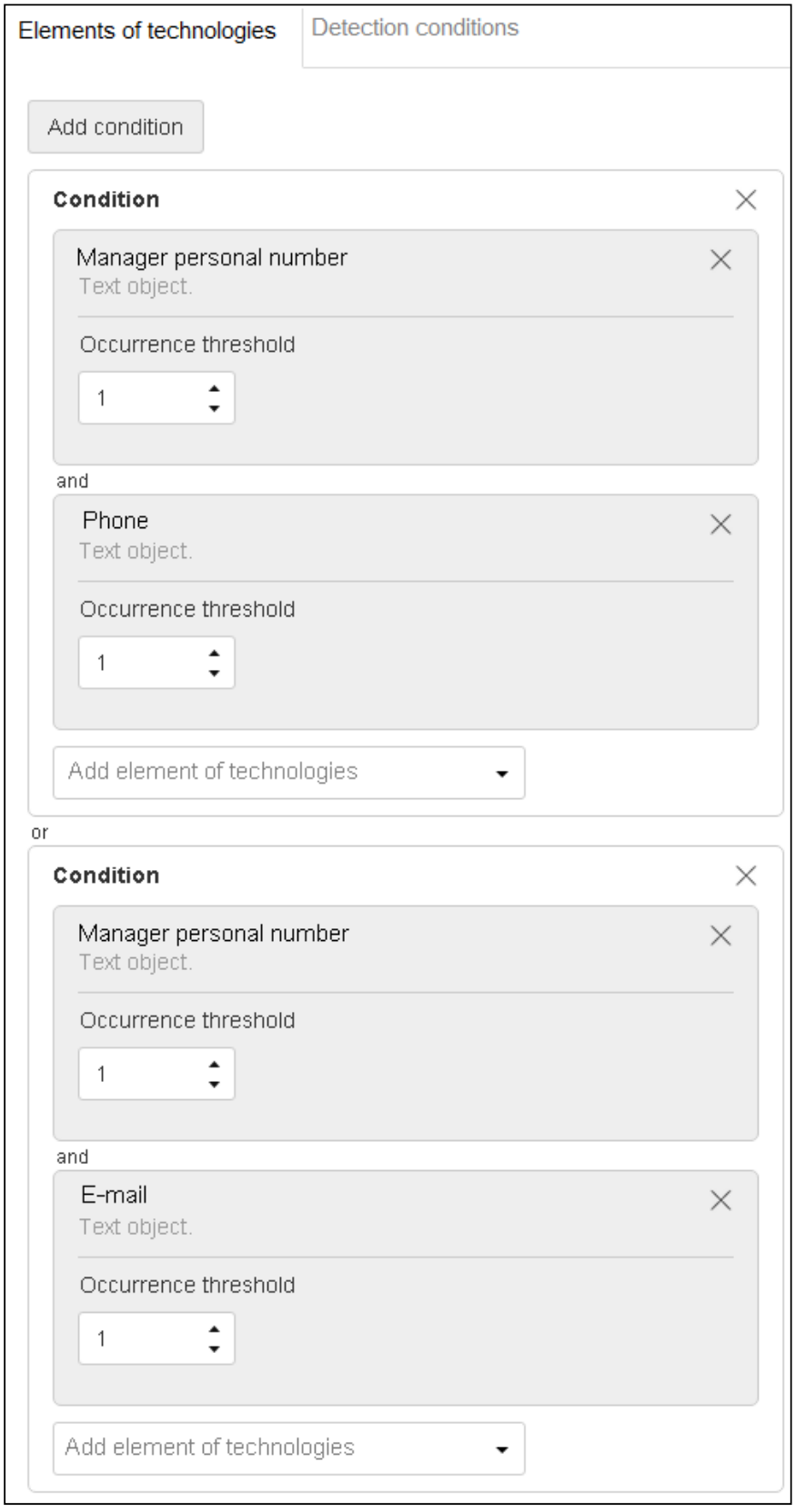
- the interception object contains a personal number of the manager and an email;
- the interception object contains a personal number of the manager and a phone number.

Then:

1. Create a new protected object and add the following elements of technologies:
    - a text object *"Manager Personal Number"*

- a text object *“E-mail”*
- a text object *"Phone"*

2. Specify the following detection conditions for the elements of technologies:



Additional information:

Protected objects can be edited and deleted by standard means:

- Editing Element
- Deleting Element

4.5.3 Adding Elements of Technologies

Purpose:
Add elements of technologies to a protected object.

Solution:

You can add elements of technologies when creating a new protected object or when editing an earlier created protected object (see "Creating Protected Objects").

If you are creating a new protected object:

1. In the **Create Protected Object** window, open a tab with desired elements.
2. From the list of available elements, select elements, you want to add.

> **Note:**
>
> When you select a category that contains subcategories (the **Category** tab), all subcategories will also be selected. If you want to add particular subcategories, click on the arrow to the left of the category name, and, from the drop-down list, select check boxes in required fields.

3. To create a protected object based on several technologies, repeat steps 1-2 until you add all desired elements.
4. Click **Create**.

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

If you are editing an earlier created protected object:

1. In the **Edit Protected Object** window, click **Select elements**.
2. In the **Select elements of technologies** window that opens, open a tab with desired elements.
3. From the list of available elements, select elements, you want to add.

> **Note:**
>
> If the protected object is included in a data protection policy on agents (see "Creating Data Protection Policy on Agents"), then you can only add categories and text objects to this protected object.

4. Click **Save**.

You can delete added elements of technologies. For this, on the **Elements of technologies** tab, click on the cross to the opposite of the desired element.

4.5.4 Adding Detection Conditions

Reference information:

A protected object can be detected in the event if:

1. The protected object status is **Active**.
2. The event contains elements of technologies included in the protected object with respect to specified detection conditions.

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

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

> **Note:**
>
> When exporting a protected object (see "Import and Export of Protected Objects"), the protected object includes only those elements of technologies for which detection conditions are specified.

Purpose:

Add detection conditions for a protected object.

Solution:

Detection conditions are added when creating protected objects. After you add selected elements of technologies to the protected object (see "Adding Elements of Technologies"), you need to specify detection conditions.

> **Note:**
>
> You can also add detection conditions when editing an earlier created protected object.

To add detection conditions for a protected object:

1. On the **Detection Conditions** tab, in the **Add element of technologies** field, click and, in the drop-down list, select the desired element.
2. The selected element will be added to the list of conditions. For some elements of technologies, you can specify additional detection conditions (see "Detection conditions").
3. If there are several elements of technologies in the protected object, you can add detection conditions for the other elements in one of the following ways:
   - If you need conditions to be combined with a conjunction (logical "AND"), add conditions as described in step 1.
     In this case, all added conditions will be placed in the same **Condition** block and combined with a conjunction.
   - If you need conditions (or groups of conditions) to be combined with a disjunction (logical “OR"), click the **Add condition** button.
     A new **Condition** block will be added. In this block, you can add conditions as described in step 1.

In this case, all the **Condition** blocks will be combined with each other with a disjunction, and conditions within a single block will be combined with a conjunction.

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

Additional information:

If you need to delete conditions, do either of the following:

- to delete a single condition, click x in the upper right corner of the panel with the required condition;
- to delete a block that contains conditions, click x in the upper right corner of the block.

4.5.5 Creating Policies for Protected Objects and Their Catalogs

Purpose:

Create a policy for protected objects and their catalogs directly from the "Protected objects" section.

To create a policy for a catalog of protected objects:

1. Go to the **Protected objects** section.
2. In the **Catalogs of protected objects** list on the left side of the workspace, select the desired catalog.
3. On the toolbar in the left part of the workspace, click and, in the drop-down list, select one of the following items:
   - **Create data protection policy**
   - **Create policy on agent**
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 catalog.

To create a policy for selected protected objects:

1. Go to the **Protected objects** section.
2. In the **Catalogs of protected objects** list in the left part of the workspace, select the desired catalog.
3. In the right part of the workspace, a list of protected objects included in the selected catalog will be displayed. Left-click the desired protected object. To select multiple objects, use the Shift or Ctrl key.
4. On the toolbar in the right part of the workspace, click and, in the drop-down list, select one of the following items:
   - **Create data protection policy**
   - **Create policy on agent**
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 Import and Export of Protected Objects

Purpose:

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

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

To export protected objects:

1. Go to the section **Protected objects**.
2. On the toolbar in the left part of the workspace, click and in the drop-down list select **Export**.
3. In the window that opens, specify where you want to save the created archive.

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

To import protected objects:

1. Go to the section **Protected objects**.
2. On the toolbar in the left part of the workspace, click and in the drop-down list select **Import**.
3. In the window that opens, select a previously exported file that you want to download.
4. Wait till the protected objects are loaded into the System.

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

Features of merging data when importing:

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

4.5.7 Activating and Deactivating Protected Objects

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

To deactivate a catalog of protected objects:

1. On the toolbar in the left part of the workspace, click and, in the drop-down list, select **Deactivate**.
2. The catalog status will change to *Inactive* (icon).

If you need to reactivate a deactivated catalog, click and, in the drop-down list, select **Activate**.

To deactivate a selected protected object:

1. On the left part of the workspace, select the desired catalog.
2. On the left part of the workspace, left-click the desired protected object in the list.
3. On the toolbar in the right part of the workspace, click and, in the drop-down list, select **Deactivate**.
4. The status of the protected object will change to *Inactive* (icon).

If you need to reactivate a deactivated protected object, click and, in the drop-down list, select **Activate**.

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

4.6 Managing Crawler Subsystem

What do you need the Crawler subsystem for?

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

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

Managing the Crawler subsystem includes the following actions:

Action	Description
Configuring Scanner	After the administrator installs and configures the System, the user will get access to a scanner. To work with the scanner, the user can configure it
Creating a Job	To scan resources, you need to create a job

Launching and Stopping the Job	Running the job starts the scanning of the target file storages; when the job is finished, the scanning stops
Editing the Job	Changing job settings
Cleaning the Hash Base	Discarding file checksums saved in the System
Viewing Launch History	Viewing system information during the job progress
Saving Scan Report	Copying a report to a hard disk of your computer

See also:

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

4.6.1 Configuring Scanner

Purpose:
To configure the scanner of the Crawler subsystem.

Solution:

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

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

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

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

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

Not matching SIDs:
`1S-1-5-21-12345-ABCDEF-498` - does not start with "S-1-5-21-"
`S-1-5-21-527`- S-1-5-21 - starts with "S-527-" but ends with "527" rather than " -527"

`S-1-5-21-ABCDEF-100-` does not end with " -498" or " -502" or " -517" or " -527".
`S-1-5-21-ABCDEF-502-`- does not end with " -498" or " -502" or " -517" or " -527".
`S-1-6-21-ABCDEF-502` - does not start with "S-1-5-21-".

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

4.6.2 Creating a Job

Purpose:
Add a scan job.

Solution:

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

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

1. Create a term with the text “printed circuit board” (see "Creating Terms").
2. Create *Printed circuit board* tag (see "Managing Tags“).
3. Apply the configuration (see “Applying System Configuration").
4. Create a scan job, select *SharePoint* as a scanning policy, and specify the following values of the attributes:
   - attribute **Address of DB resource** - *SharePointRepo* value;
   - attribute **Name of DB resource** - *CorporateDataBase* value.
5. Create a policy and a placement rule.
6. Specify the following parameters of the rule:
   - **Storage** - *File storage*; attributes have following values:
     - attribute **Enter a source** - *SharePointRepo* value;
     - attribute **Enter a path to storage** - *CorporateDataBase* value;
   - **Tags** - *Printed circuit board* tag.

> **Warning!**
>
> While the job runs even with domain administrator rights, you may receive the error:

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

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

4.6.3 Launching and Stopping the Job

Purposes:

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

Solution:

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

4.6.4 Editing the Job

Purpose:
To edit the scan job.

Solution:

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

4.6.5 Cleaning the Hash Base

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

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

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

Purpose:
To clear the hash base.

Solution:

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

4.6.6 Viewing Launch History

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

Purpose:
View the history of job launches.

Solution:

1. Go to the **Crawler** section.
2. Left-click the required job from the list.
3. View the summary in the right part of the workspace. The summary includes the following parameters:
    - **Status** - job status identifier (- *Started*, - *Stopped*, - *Completed*);
    - **Launch date**;
    - **Stop date**;
    - **Quantity of workstations proceeded** - the number of target workstations processed while the job was running;
    - **Quantity of workstations not proceeded** - the number of which were not process while the job was running;
    - **Total quantity of files/size** - the number and total size of files on target workstations processed while the job was running;
    - **Quantity of new files/size** - the number and total size of files which were not previously processed on target workstations.
4. To view more information about the job and on the launch settings, left-click the necessary launch’s entry in the list.
   Extended information is presented in the following tabs:
    - **Launch events** - the tab contains system information about the launch of scanning job

- **Launch parameters** - the tab contains the list of attributes of scanning job (see "Scanning Job")

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

4.6.7 Saving Scan Report

Purpose:
To save a report on scanning.

Solution:

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

4.7 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
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

4.7.1 Viewing summary on violations/violators

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

Purpose:
View a summary on violations/violators.

Solution:

1. Go to the **Dashboard** section.
2. Configure a dashboard where widgets will be added (see “Creating a Dashboard").
3. Add and configure the desired widget (see "Creating and configuring widget").
4. Examine the summary in the widget.

You can export a report with the summary as PDF or HTML page (see "Creating dashboard report").

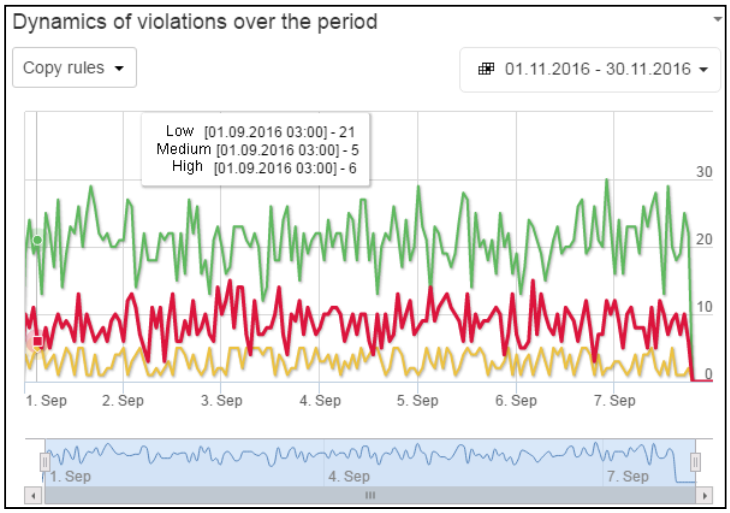
All generated reports are stored in the System. You can view the required report or delete reports which you do not need to store (see "Viewing dashboard report").

Example 1:
It is required to track dynamics of copying files which contain confidential data (see the list of actions that are considered data copying in "Rule of Copying").

For this:

1. Create a new dashboard or open an earlier created one.
2. Add "Dynamics of violations over the period" widget (for details on configuring this widget, see "Dynamics of violations over the period").
3. In the right upper corner of the widget, choose *Current month* as a period.
4. In the left upper corner of the widget, choose *Copy rules* from the list of rules.

The widget will display charts that show the dynamics of violating copy rules for the current month.



To view events for a particular date and hour, click the point where the timeline intersects the violation number curve.

Example 2:
It is required to display all interception objects for the current week where John Smith is either a sender or a recipient (it is supposed that John Smith person has already been created in the **Persons** section).

For this:

1. Create a new dashboard or open an earlier created one.
2. Add "Selection" widget (for details on configuring this widget, see "Selection").
3. Switch to the widget edit mode and for the Selection parameter, specify an earlier created *Smith* query (see Example 2 in "Examples of using queries").
4. Save the widget.

.

Creating Dashboard

Purpose:
Create a dashboard that will contain widgets.

Solution:

1. Go to the **Dashboard** section.
2. In the left part of the workspace, click + **Add**.
3. Specify the name of a new dashboard.
4. Click **Save**.

Additional information:

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

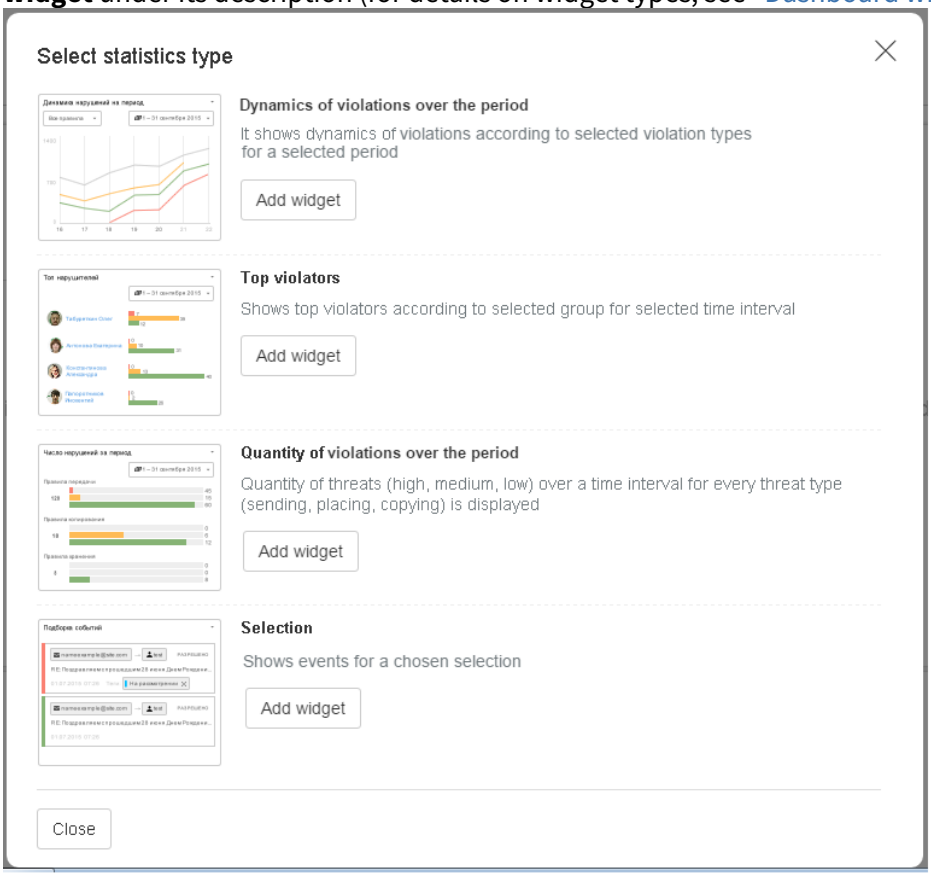
Creating and configuring widget

Purpose:
Create a widget in the dashboard pane.

Solution:

1. Go to the **Dashboard** section.
2. Select the dashboard, to which you want to add a widget, or create a new dashboard (see "Creating Dashboard").
3. Click **Add widget**.

4. In the **Select statistics type** window that opens, select the desired widget and click **Add widget** under its description (for details on widget types, see "Dashboard widgets").



> **Note:**
>
> You can add several widgets in succession. To do this, click **Add widget** under other widgets you want to add: selected widgets will be added to the dashboard.

> **Tip**
>
> You can add multiple widgets of the same type, and then configure them to display different types of data: for example, several widgets of **Summary** type to display events based on results of queries (for details on queries, see "Creating queries").

5. Click **Close** or use ✕ button in the upper right corner of the window.
6. Configure added widgets to display required data (parameters of different widgets are listed in the "Dashboard widgets" subsection).

Additional information:

1. You can move widget tiles to place them in a convenient order. To do this:
   a) Hover the mouse pointer over the tile header so that a standard cursor changed to a four-way arrow key.

b) Hold down the left mouse button and, keeping it pressed, move the tile over the workspace until the target position of the tile is displayed as a dotted line.
c) Release the left mouse button.

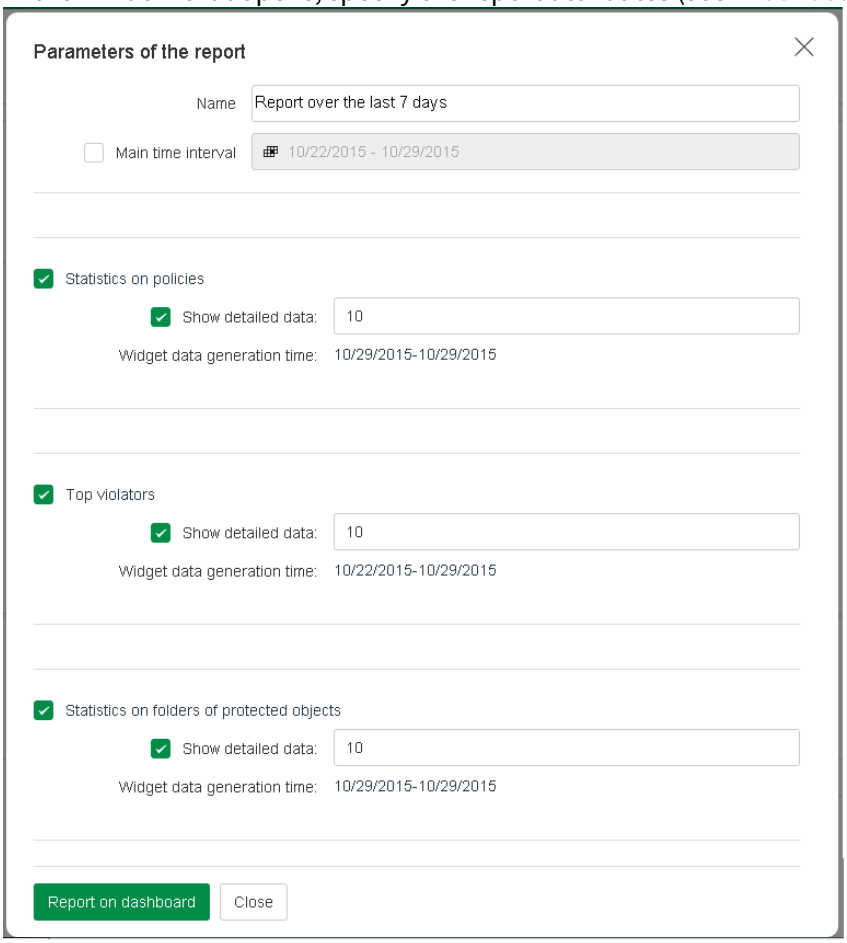
2. To edit a widget, in the right upper corner, click and, from the drop-down list, select **Edit**. In the **General widget settings** window that opens, change the required settings, then click **Save**.
3. To delete a widget, in the right upper corner, click and, from the drop-down list, select **Delete**. In the confirmation window, click **Yes**.

Creating dashboard report

Purpose:
To create a report on a dashboard with the summary on intercepted objects.

Solution:

1. Go to the **Dashboard** section.
2. Open the dashboard for which you want to generate a report.
3. In the right upper corner, click **Unload**.
4. In the window that opens, specify the report attributes (see "Dashboard report").



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

> **Note:**
>
> The dashboard report does not include data from the "Selection" widget.

6. If you want to manually specify the period, for which the report will be generated, select the **Common period** check box and enter the start and the end date. If this option is deselected, then, for each widget, the report will be generated for the period specified in the widget properties.
7. Click **Report on dashboard**.

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

Once the report is generated, you will be prompted to open it in PDF or HTML format.

All created reports are stored in the System and are available by clicking **Show list of reports** in the right upper corner of the workspace. For details, see "Viewing dashboard report".

> **Note:**
>
> If you remove or modify a widget which is included in the report, then the already created report will not be changed.

Viewing dashboard report

Purpose:
View a report on intercepted objects.

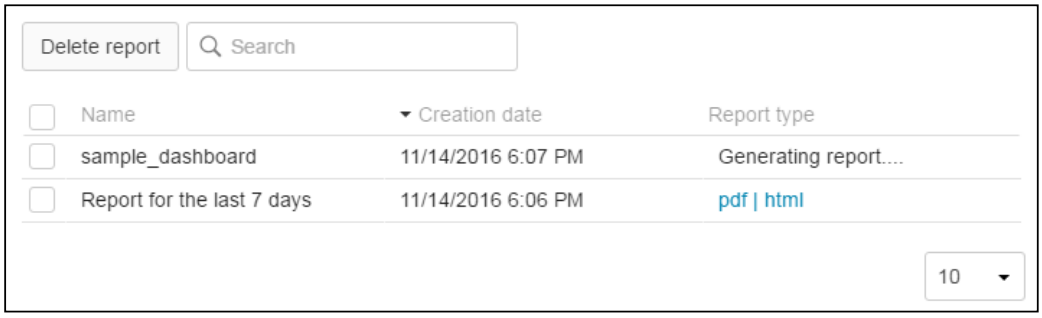
Solution:
When the report generation is complete, a message is displayed in the right upper corner of the workspace. In this message, you are offered to open the report in PDF or HTML format.



Click on the **pdf** or **html** link to open the report in a new browser window. You can also save, send or print the created report by standard means of your browser and operating system.
All created reports are stored in the System.

To view the list of generated reports, in the right upper corner, click the **Show list of reports** button. The **Reports** window will open where you can view information on the reports.

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



To view a selected report, in the **Report type** column, next to the desired report, click:

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

A new browser tab will display the selected report.

To delete selected reports:

1. Select checkboxes next to the reports you want to delete. To select all rows, select the checkbox in the header.
2. Click **Delete report**.

4.7.2 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. Select a query from the drop-down list in the upper part of the workspace or create a new query in a standard or advanced mode.

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

> **Note:**
>
> To hide the query results, click  next to the query name in the list of queries.

See also:

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

Query creation in standard mode

Purpose:
Create a query to search for events which satisfy specified conditions.

Solution:

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

> **Note:**
>
> For more flexible configuration of search conditions, you can use the advanced mode.

The "Examples of using queries" article contains an example of creating a simple query.

Additional information:

Queries can be edited and deleted by standard means:

- Editing Element
- Deleting Element

Query Creation in Advanced Mode

Purpose:
Configure search conditions for events more clearly.

Solution:

1. Go to the **Events** section.
2. On the toolbar, click + **Add query**.
3. In the drop-down list, select **Advanced query**. A query creation window will open.
4. In the **Name** field, specify the query name.
5. On the **Condition** tab, in the **Add condition** drop-down list, specify the search parameters.
6. By default, added attributes are joined by conjunction (logical AND). To change the operation type, left-click the and icon. The icon will change to or that stands for the disjunction (logical OR).
7. Use **Group of parameters** element to separate attributes joined by the conjunction (logical AND) from attributes joined by the disjunction (logical OR) (see "Advanced mode").
8. On the **Display fields** tab, select attributes whose values will be displayed for found events.
9. To allow other users to view and edit the query, on the **Access parameters** tab, clear **The query is available only to the owner** check box (by default, the check box is selected).
10. Click **Save**.

The "Examples of using queries" article contains examples of creating advanced queries.

Additional information:
Parameters can be edited and deleted by standard means:

- Editing Element
- Deleting Element

Using Advanced Syntax

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

Solution:

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

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

Example:

If you want that the event text:

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

create the following query using advanced syntax:

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

Examples of using queries

Example 1:

It is required 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:

It is required to find events:

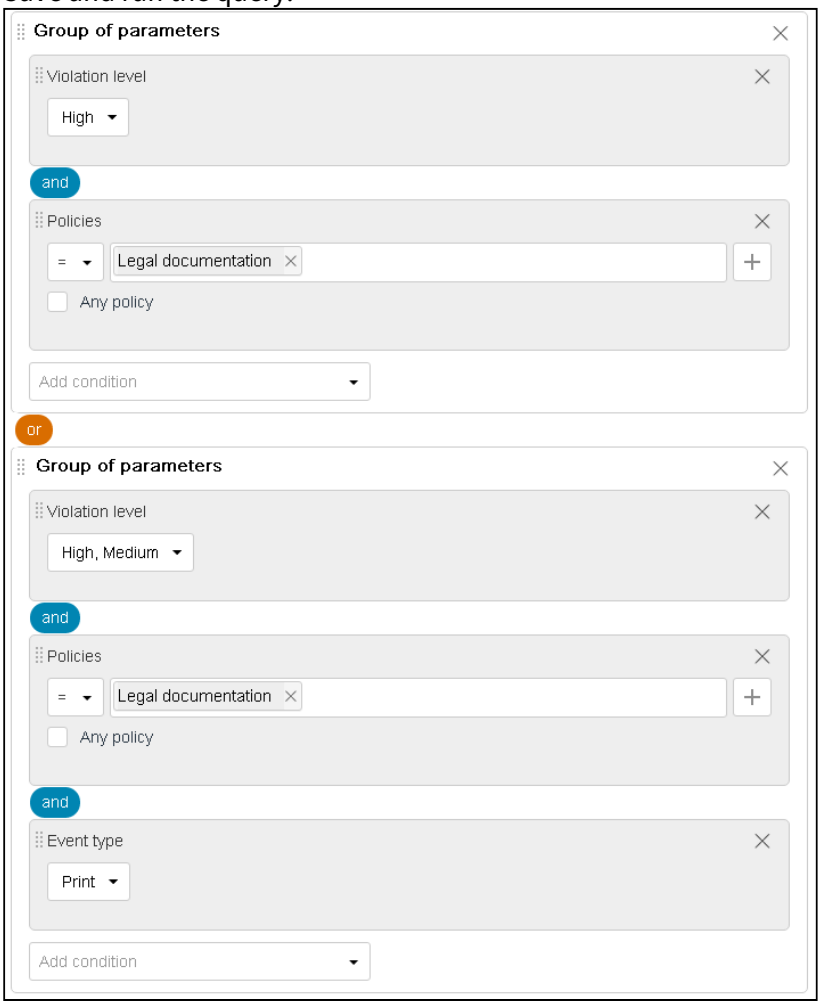
- with *High* violation level and the *Legal documentation* policy;
- with *High* and *Medium* violation levels, the *Legal documentation* policy, and the *Stamp* event type:

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.*

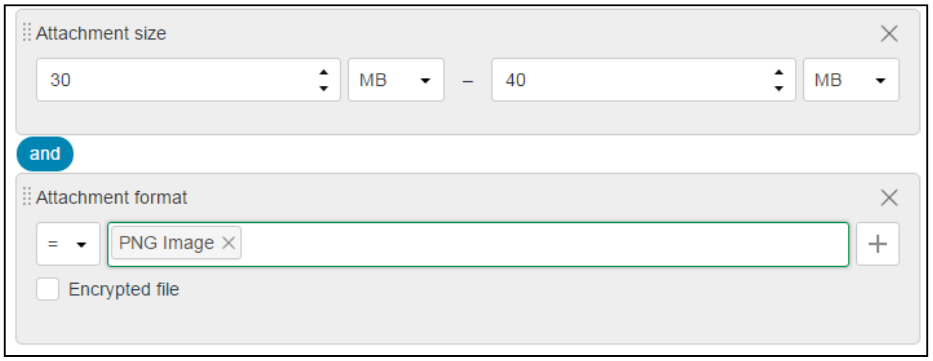
4. Within the second group, add the following attributes joined by logical AND:
   - **Violation level** - *High* and *Medium*;
   - **Policy** - *Legal documentation*;
   - **Event type** - *Print.*
5. Save and run the query.



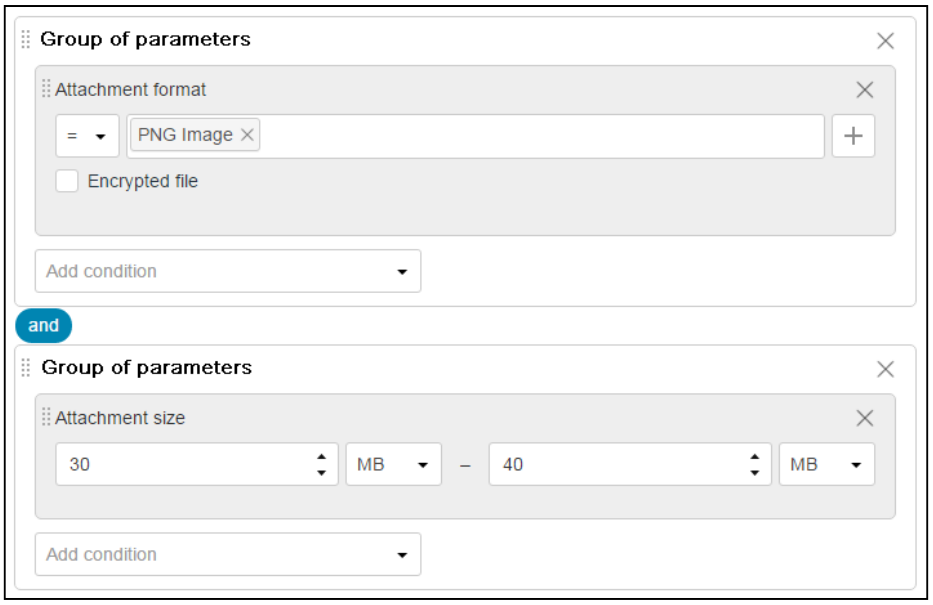
Example 4:

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.



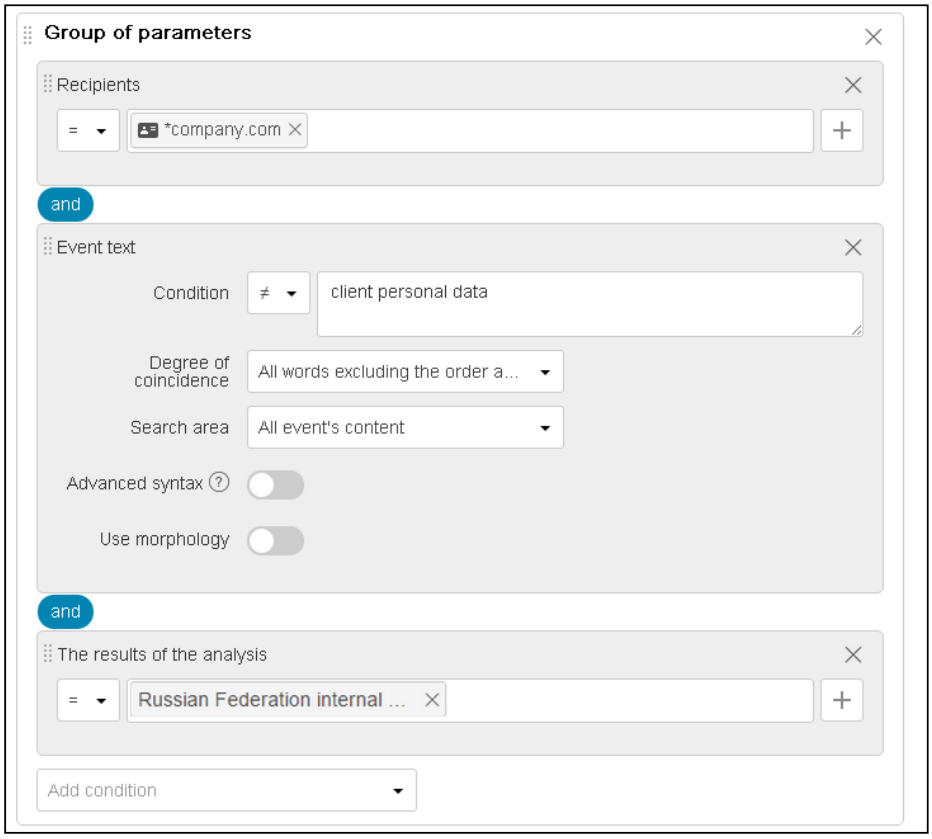
Example 5:

It is required to find events that:

- are sent within the company;
- do not contain *Client personal data* words in the event text;
- contain pass numbers.

For this:

1. Create an advanced query and specify its name.
2. Add *Group of parameters* element.
3. Within the group of parameters, add the following attributes joined by logical AND:
    - `Recipients` - **company.com*;
    - `Event text` - *“Client personal data”*; the search is performed in the *All words irrespective of their order and distance between words* mode and the negation is applied to the attribute;
    - `Search area` - *"All contents of event"*;
    - `Results of analysis` - *"Pass number"* text object.
4. Save and run the query.



Choosing Event Fields of View

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

Purpose:
To select attributes of interception objects that will be displayed.

Solution:

1. Go to the **Events** section.
2. Do either of the following:
    - Edit an existing query. For this, click **Edit query**;
    - Create a new query.

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

3. On the right part of the workspace select the **Display fields** tab.
4. Move all target attributes to the right field and all unwanted ones - to the left:
    - Left-click on the entry in the left field to move it to the right field;
    - Left-click on the entry in the right field to move it to the left field.

5. Click:
   - **Save** - to save a query.
   - **Save and execute** - to save and apply the changed query.

Viewing Brief Event Form

Purpose:
Viewing brief information on interception objects.

Solution:

1. Go to the **Events** section.
2. Create a query or run an earlier created query (see "Creating Queries").
3. Select the tile of the target event in the list (or a raw of the target event in the event table).
4. View the summary in the right part of the workspace. In the upper part of the form, you can view the event parameters; in the lower part, the event contents is displayed.
5. To view information on senders, recipients or computers, click the desired value. A card for the selected person or computer will be displayed.
   To view data on senders, recipients or computers, click the desired value. A card for selected person or computer will be displayed.
   When viewing the card, you can:
   a. Assign a status to a person/computer. For this, click Set status link and, in the **Adding status** window, select desired statuses. Then click **Save**.
   b. View detailed information on a person/computer in "Persons" section. For this, click Person profile link (for persons) or Go to computer link (for computers).
   c. View screenshot for a person/computer (if there are screenshots for a person, then icon is displayed next to the person name). For this, click Screenshots link. The **Screenshots** tab for the selected person or computer will open.

> **Note:**
>
> If there are screenshots taken within an hour before or after the event, the Screenshots near the event link is displayed for persons. Clicking this link opens the **Screenshots** tab with the screenshot whose creation time is closest to the event.

6. To view information about the triggered policy in the "Policies" section, click the name of the triggered policy.
7. If the event has attachments, you can save the attachment to your computer. For this, click next to the attachment name and select **save attachment to disk** command.
8. To get detailed information on the event, in the right upper corner of the form, click **Detailed information**.

See also:

- "Brief Event Viewing Form" - on the form with general information about the event.
- "Viewing Detailed Event Form" - on displaying detailed information about the event.
- "Viewing Screenshots" - on viewing screenshots for persons or computers

Viewing Detailed Event Form

Purpose:
To view a detailed information on the interception object.

Solution:

1. Go to the **Events** section.
2. Create a query or run an earlier created query (see “Creating Queries").
3. Select a tile of target event from the list (or a string of target event from the table). The right part of the workspace will display a brief event viewing form.
4. To open the detailed viewing form, click **Detailed information**.
5. In the **Detailed information on event** window that appears, view the required information. Information on the event is presented in the following blocks: **General information**, **Protected objects**, and **Event content** (see "Detailed Event Viewing Form“).
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

4.7.3 Making Decision on Object

Purpose:
To make a decision on the object.

Solution:

1. Go to the **Events** section.
2. Left-click the target event to select it.
3. On the toolbar, click
   -  **Violation** - for events that violate the corporate security policy. For events with *Quarantine* verdict, the verdict value will change to *Blocked*.
   -  **No violation** - for events that do not violate the corporate security policy. For events with *Quarantine* verdict, the verdict value will change to *Allowed*.

     > **Warning!**
     >
     > If the *Block* mode is used in the System, then as a result of this decision, SMTP messages quarantined by the System will be dispatched and the message sender will be notified via email. For details, see “Dispatching Blocked Event".

   -  **No decision** - if for now the user has not decidede a decision whether the event violates the corporate security policy.

-  **Requires additional proceeding** - if additional actions are needed to make a decision.

See also:

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

4.7.4 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 catalog

4.7.5 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.

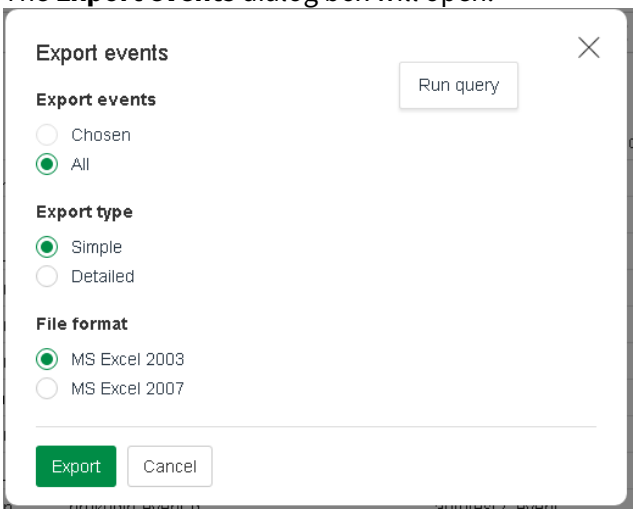
4.7.6 Event Export

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

Solution:

1. Go to the **Events** section.
2. Click the table viewing form icon .
3. Run the query to retrieve objects.

4. Select the event you want to export. To select multiple events, use the Shift or Ctrl key. If you want to generate unloading for all available events, skip this item.
5. On the toolbar click and in the drop-down list select **Export event**. The **Export events** dialog box will open.



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

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

4.7.7 Dispatching a Quarantined Event

Reference information:
If the System (in the *Blocking* transport mode) recognizes a transferred SMTP-letter as a potential violation and moves it to quarantine, the security officer can then review the decision of the System and allow sending this letter. In this case, the System dispatches the letter and notifies the person who has sent it.

Purpose:
Send a quarantined letter to the addressee.

Solution:

> **Warning!**
>
> You can dispatch the object with a *Quarantine* verdict. Objects with a *Blocked* verdict cannot be dispatched.

1. Go to the **Events** section.
2. Left-click the target event.
3. On the toolbar in the left part of the workspace, click **No violation**.

See also:

- "Retrospective Data Analysis, User Decision on an Object" - general information on making decisions
- "Making Decision on Event" - on how to make a decision on the object

4.8 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 Management Console users;
- assign a verdict to the interception object;
- assign a violation level, statuses, and tags to the interception object.

Configuring the System response includes:

Action	Description
Creating data protection policies	Data protection policy is a set of rules that regulate data transfer, copying, placement, and usage of the clipboard. Allows you to specify actions that may trigger policy rules.
Creating data protection policies on agents	Data protection policy on agents is a set of transfer and copy rules that apply directly on Device Monitor agents. Allows you to specify actions that may trigger policy rules.
Creating person control policies	Allows you to specify the list of controlled persons whose actions may trigger policy rules
Creating rules	Defining what is a violation of policy rules, and what actions will be done in the event of violation
Notifications on responded rule	If the rule is triggered, the System sends notification to specified Console users

Note:

If there are a lot of policies in the Management Console, you can filter the policy list by specified criteria (for details, see “Filtering the List of Policies").

See also:

- "Policies Section" - on the section where you can manage policies

4.8.1 General Information on Policies

The section describes how configured System policies (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

Каждое правило действующей политики разбивается на суб-правила по следующим ключам:

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 rules:

Sender	Direction	Recipient	Event type	Date	Reaction
Group: Lawyers, The Person: Smith, Person: Johns	->	Group: Marketing, Person: Williams	Mail on Client	08:00-20:00	Notify: Thomas Violation level: Low
Group: Logistics	->	Group: Sales, Group: Delivery	Skype	10:00-19:00	Notify: Johns Violation level: Medium
Group: Financial	-> <-	Group: Lawyers, Group: Sales			Notify: Miller Violation level: High

are divided into the following sub-rules:

Sender	Direction	Recipient	Event type	Date	Reaction
Group: Lawyers	->	Group: Marketing	Mail on Client	08:00-20:00	Notify: Thomas Violation level: Low
Group: Lawyers	->	Person: Williams	Mail on Client	08:00-20:00	Notify: Thomas Violation level: Low
Person: Smith	->	Group: Marketing	Mail on Client	08:00-20:00	Notify: Thomas Violation level: Low
Person: Smith	->	Person: Williams	Mail on Client	08:00-20:00	Notify: Thomas Violation level: Low
Person: Johns	->	Group: Marketing	Mail on Client	08:00-20:00	Notify: Thomas Violation level: Low
Person: Johns	->	Person: Williams	Mail on Client	08:00-20:00	Notify: Thomas Violation level: Low
Group: Logistics	->	Group: Sales	Skype	10:00-19:00	Notify: Johns Violation level: Medium
Group: Logistics	->	Group: Delivery	Skype	10:00-19:00	Notify: Johns Violation level: Medium
Group: Financial	->	Group: Lawyers			Notify: Miller Violation level: High

Group: Financial	->	Group: Sales			Notify: Miller Violation level: High
Group: Lawyers	->	Group: Financial			Notify: Miller Violation level: High
Group: Sales	->	Group: Financial			Notify: Miller Violation level: High

Then, for each sub-event, the System chooses sub-rules whose conditions match the sub-event (for more details on rule attributes, see "Rule of Transfer", "Rule of Copying", "Rule of Placement", and "Clipboard 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
Storage	1,25	0,25
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
If the attribute is not filled: • Sender (for transfer and copy rules) • Recipient (for transfer rules) • Person (for clipboard rules) • File owners/Who has access to file (for placement rules)	1	does not apply
If the attribute is not filled: • Event type (for all rules) • Day of the week (for transfer, copy, and clipboard rules) • Time (for transfer, copy, and clipboard rules) • Computer (for transfer, copy, and clipboard rules) • Storage (for placement rules) • Terminal session (for clipboard rules) • Source-application/Reciever-application (for clipboard rules)	0	does not apply

For example, the rule with a condition of forwarding from any sender to a specific contact (10000 + 1 = 10001) has a higher priority than the rule with a condition of forwarding from a particular person to a group of persons (5000 + 2500 = 7500).
If for the same sub-event, there are two or more sub-rules with the same priority, the several rules with the highest priority are selected.
If a sub-event has no matching rules, then a default rule is selected (see "Determining System Default Response").

4. The order of applying actions according to selected priority rules

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

1. If the **Delete event** option is selected, then the actions specified in the rule are not executed and the event is not saved to the database.
2. The event is assigned a verdict with the highest priority from priorities in the selected rules. Verdicts have the following priorities:
    - for **Block** verdict, the priority is 2;
    - for **Quarantine** verdict, the priority is 1;
    - for **Allow** verdict, the priority is 0.

Note:

A verdict assigned to the event as a result of applying a data protection policy on agents is not replaced with a verdict specified in rules of data protection policies and person control policies.
A verdict assigned to the event as a result of applying a data protection policy is not replaced with a verdict specified in rules of a person control policy.

3. The event is assigned the highest violation level from violation levels in the selected rules.
4. Tags specified in the selected rules are added to existing tags.
5. For identified senders, statuses specified in the selected rules are added to existing statuses.
6. Persons specified in the selected rules are notified.

Example:

Let the System have two policies:

Policy №1					
Catalogue of protected objects: Accounts					
Rule number	**Sender**	**Recipient**	**Date**	**Event type**	**Reaction**
1.1	Group: Sales Department	Group: Accounts Department	08:00-20:00	Mail on Client	Violation: None
1.2	Smith	Group: Accounts Department		Mail on Client	Violation: None
1.3	Smith	<>Perimeter: Company			Violation: Medium
1.4	Default:				Violation: High

Policy №2					
Catalogue of protected objects: Contract					
Rule number	**Sender**	**Recipient**	**Date**	**Event type**	**Reaction**
2.1	Group: Sales Department	<>Perimeter: Company	08:00-20:00	Mail on Client	Violation: None

2.2	Smith	<>Perimeter: Company		Mail on Client	Violation: None
2.3	Default:				Violation: None

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

Data	Sender	Recipient	Date	Event type
Protected objects: Accounting, Contract	Smith	Johns, williams@mail.com	19:00	Mail on Client

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

1. Check for conformance to policy №1.

The event confirms to the policy №1 as it contains a *Group of protected objects - Accounts*.
The "Smith->Johns" sub-event is considered:

Sender	Recipient	Date	Event type
Smith	Johns	19:00	Mail on Client

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

Sender	Recipient	Date	Event type
Smith	williams@mail.com	19:00	Mail on Client

This sub-event confirms to the sub-rule №1.3 only. Therefore, the rule №1.3 is selected

2. Check for conformance to policy №2.

The event confirms to the policy №2 as it contains a *Group of protected objects Contract.*

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

Sender	Recipient	Date	Event type
Smith	Johns	19:00	Mail on Client

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

Sender	Recipient	Date	Event type
Smith	williams@mail.com	19:00	Mail on Client

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

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

4.8.2 Preset Policies

There are the following preset policies in the System:

- Data protection policies for confidential data
- Person control policy
- Policy regulating transfer of password-protected data
- Policy regulating visiting web resources
- Policy that excludes mailing lists from interception

> **Note:**
>
> When deleting the database scheme (see "*Infowatch Traffic Monitor. User Guide*", "Deleting the Database Scheme" article), policies (including preset ones) are also deleted from the System.
>
> To redeploy the preset policies, do the following:
>
> 1. Create **/opt/iw/tm5/www/backend/protected/runtime/first_run** file on behalf of **iwtm** user;
> 2. Restart **iw_kicker** process:
>
> ```
> service iwtm restart kicker
> ```
>
> Then you need to create other policies anew (see "Creating Data Protection Policy", "Creating Data Protection Policy on Agents", and "Creating Person Control Policy").

Data Protection Policy

By default, the System contains one data protection policy for each preinstalled catalog of protected objects (for the list of preinstalled catalogs, see "Protected Objects").

Default policies have the following attribute values:

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

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

Each policy contains the following rules:

Rules of transfer

1. *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 catalogs of protected objects: Security label, Personal data;
     - *Low* - for the following catalogs of protected objects: Law, HR, IT;
     - *Medium* - for all other catalogs 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 a removable device 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 catalogs of protected objects: Security label, Personal data;
  - *Low* - for the following catalogs of protected objects: Law, HR, IT;
  - *Medium* - for all other catalogs 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 catalogs of protected objects.

If a person stores protected data in any location,
Then the System performs the following actions:

- sets the *High* value to the *Violation level* attribute of the event*;*
- sets the *None* value to the *Status* attribute of the person who owns the data*.*

Person Control Policy

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

Attribute	Value
Policy name	Persons under supervision

Status	Active
Period of activity	Not limited
Statuses	Under supervision

Policy Rules

The rule that regulates transferring data by persons with Under Supervision status.

If a person with the *Under supervision* status sends traffic of any type to any recipient,
Then the System sets:

- the *Allow* value to the *Verdict* attribute of the event;
- the *For consideration* value to the *Tag* attribute of the event.

Policy that Regulates Transferring Password-Protected Data

By default, the System has a policy that regulates transferring password-protected data.

The default policy has the following attribute values:

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

Policy rules

The rule that regulates transferring password-protected data outside the company perimeter.

If a person sends traffic of any type outside the company perimeter any day of the week,
Then the System performs the following actions:

- sets the *Allowed* value to the *Verdict* attribute of the event;
- sets the *Medium* value to the *Violation level* attribute of the event;
- assigns the *For consideration* tag to the event.

Policies that Regulate Visiting Web Resources

By default the System has the following data protection policies that control visiting web resources by the company employees:

- Inappropriate Use of Resources

- Disloyal Employees
- Concealing Employees' Actions
- Suspicious Activity

Inappropriate Use of Resources

By default the System has a policy that controls visiting web resources by the company employees.

The default policy has the following attribute values:

Attribute	Value
Policy type	Data protection policy
Policy name	Inappropriate use of resources
Status	Active
Period of activity	Not limited
Protected data	Any data

Policy rules

The rule of transfer that regulates sending requests to entertaining resources.

If a person sends a request to a web resource included in the "Media", "Blogs", "Entertaining" or "Social networks" groups (for more details, see "Web Resources") any day of the week,
Then the System performs the following actions:

- sets the *Allowed* value to the *Verdict* attribute of the event
- sets the *Low* value to the *Violation level* attribute of the event.

Disloyal Employees

By default, the System has a preset policy that monitors actions of disloyal employees.

The default policy has the following attribute values:

Attribute	**Value**
Policy type	Data protection policy
Policy name	Disloyal employees
Status	Active
Period of activity	Not limited
Protected data	Any data

Policy rules

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

If a person sends a request to a web resource included in the "Job search" group (for more details, see "Web Resources") any day of the week,
Then the System performs the following actions:

- sets the *Allowed* value to the *Verdict* attribute of the event;
- sets the *Low* value to the *Violation level* attribute of the event.

Concealing Employees' Actions

By default, the System contains a policy that monitors attempts of employees to conceal their actions or bypass access restrictions.

The default policy has the following attribute values:

Attribute	Value
Policy type	Data protection policy
Policy name	Concealing employees' actions
Status	Active
Period of activity	Not limited
Protected data	Any data

Policy rules

The rule of transfer that regulates sending requests to anonymizers.

If a person sends a request to a web resource included in the "Anonymizers" group (for more details, see "List of Resources") any day of the week,
Then the System performs the following actions:

- sets the *Allowed* value to the *Verdict* attribute of the event;
- sets the *Low* value to the *Violation level* attribute of the event.

Suspicious Activity

By default, the System has a preset policy that controls suspicious activities of employees on the Internet.

The default policy has the following attribute values:

Attribute	Value
Policy type	Data protection policy
Policy name	Suspicious activity
Status	Active
Period of activity	Not limited
Protected data	Any data

Policy rules

The rule of transfer that regulates sending requests to potentially dangerous resources.

If a person sends a request to a web resource included in the "Potentially dangerous resources", "Sites of aggressive orientation" or "Sites for adults" group (for details, see "Web Resources") any day of the week,
Then the System performs the following actions:

- sets the *Allowed* value to the *Verdict* attribute of the event;
- sets the *Low* value to the *Violation level* attribute of the event;
- set the *For consideration* tag to the event.

Policy that Excludes Mailing Lists from Interception

By default, the System has a preset policy that excludes mailing lists from interception.

The default policy has the following attribute values:

Attribute	Value
Policy type	Data protection policy
Policy name	Exclude from interception
Status	Disabled
Period of activity	Not limited
Protected data	Any data

Policy rules

Rule that regulates sending data by persons from the "Exclude from Interception" perimeter

If a person who belongs to the *Exclude from interception* perimeter (see "Perimeters") sends traffic to any recipient any day of the week,
Then the System deletes the event.

4.8.3 Creating Data Protection Policy

Purpose:
Create a policy that determines the System reaction to actions with data.

Solution:

1. Go to the **Policies** section.
2. In the left part of the workspace, click **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. 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.

4. In the window that appears, set the check boxes next to desired values. Protected data may include protected objects, their catalogs, and file formats.

> **Warning!**
>
> If protected data of several types are specified for the policy, then for triggering the policy rules (see "Rules and their Viewing Form"), it is necessary that the intercepted event should contain violations of each type.
> For example, a catalog of protected objects and several file formats are specified as protected data for the policy. In this case, for the policy to be triggered it is necessary that intercepted data should contain at least one protected object from the specified catalog and at least one file of the specified format.

5. After you have selected protected data, click **Save**.
6. In the right part of the workspace, fill the required fields 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.

Examples of tasks where a data protection policy can be used are given in the "Examples of using data protection policy" article.

Additional information:

- Policy editing is described in "Editing Policy".
- To delete the policy, in the upper right corner of the policy tile, click, ✖ and, in the window that opens, confirm the deletion.

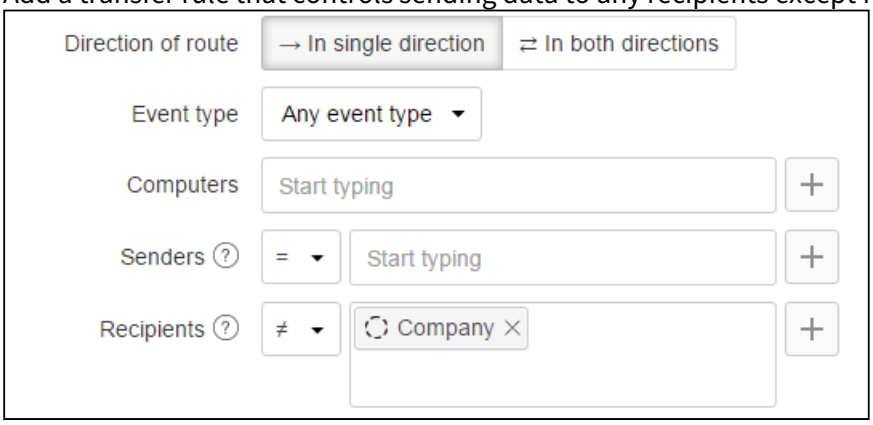
Examples of using data protection policy

Example 1:

It is required to control transferring the company statute outside the company which includes sending the document by email or copying it to removable devices. For this:

1. Create a data protection policy and name it *Protection of transferring company statute*.
2. Specify the *Company statute* protected object as protected data.

3. Add a transfer rule that controls sending data to any recipients except for the *Company* perimeter.



4. Specify what actions to perform if the rule is triggered (e.g., assign *Low* violation level to the event).
5. If in addition, you want to control employees under the supervision, add one more transfer rule and specify the *Employees under supervision* group as senders (see "Creating Group of Persons or Computers").
6. Specify what actions to perform if the rule is triggered (e.g., assign *Medium* violation level and *For consideration* tag to the event).
7. To control copying the document to a removable device, add a copy rule to the policy.

The System will detect a violation of the data protection policy when:

- an email whose body or attachment contains data related to the *Company statute* protected object is sent outside the *Company* perimeter;
- a file with information on the *Company statute* protected object is copied to a removable device.

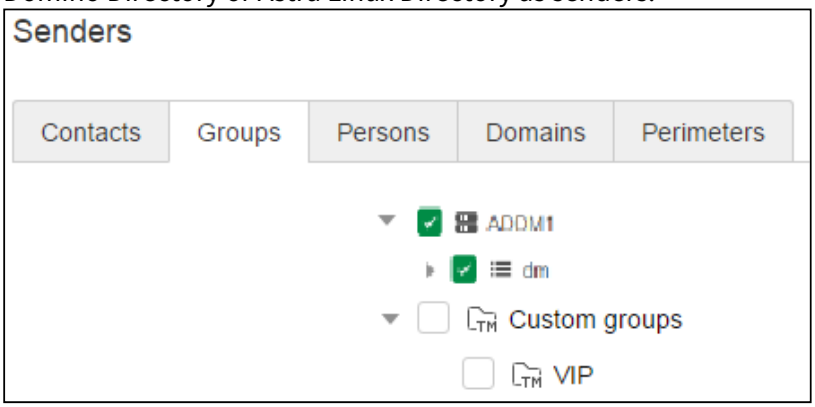
Example 2:

It is required to identify employees who visit job search sited. For this:

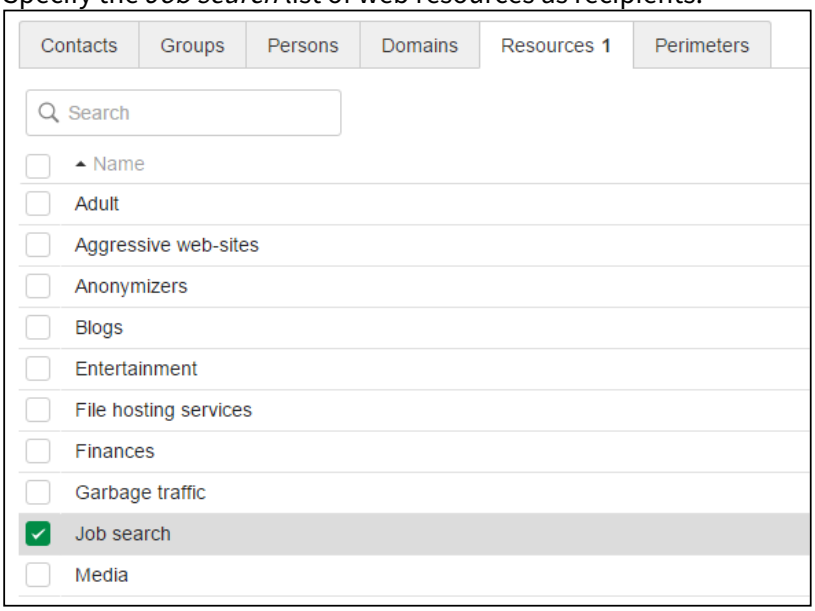
1. Create a data protection policy and name it *Identifying disloyal employees*.

> **Tip**
>
> Add the policy description to easily identify it in the policy list. For example, "Identifying employees who send requests to job search sites".

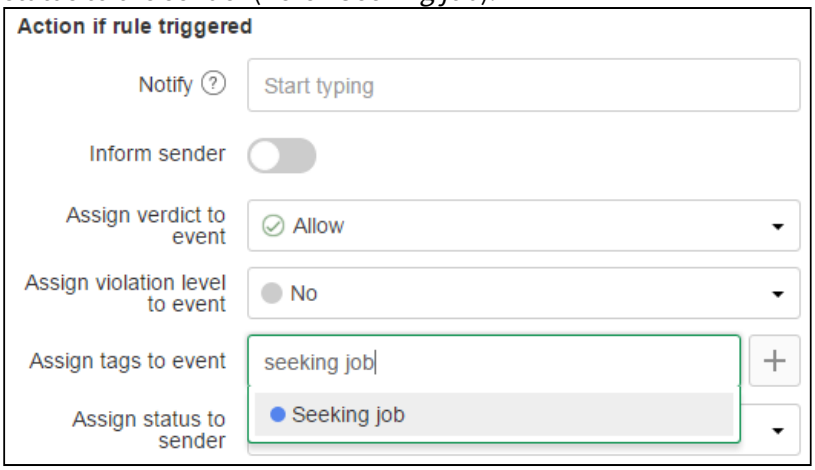
2. Add a transfer rule and specify the group of company employees imported from Active Directory, Domino Directory or Astra Linux Directory as senders.



3. Specify the *Job search* list of web resources as recipients.



4. Specify what actions to perform if the rule is triggered. For example, you can assign a specific status to the sender (here - *Seeking job*).



5. Save the rule and apply the changes of configuration.

Now, if an employee sends a request to a job search site, the System will assign the "Seeking job" status to the employee.

If necessary, you can find all such events. For this, create a query and specify on of the following search conditions:

- *Identifying disloyal employees* policy;
- senders with the *Seeking job* status.

Example 3:
It is required to identify employees who communicate with undesired destinations, i.e., fired employees, competitors, etc.

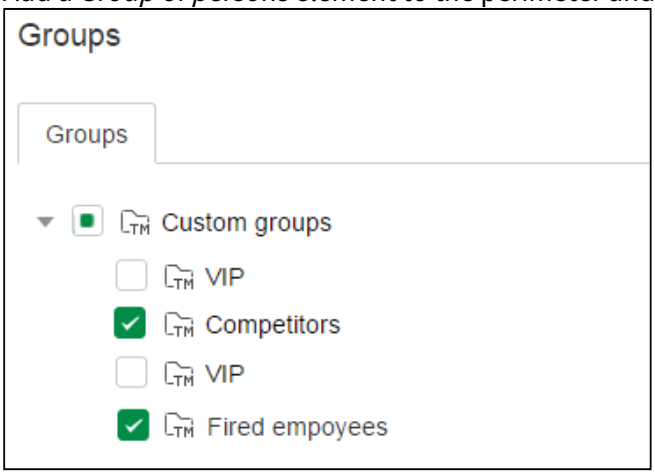
For this, you need to create a perimeter that will include fired employees, competitors, etc. and then create a data protection policy that tracks sending data to this perimeter.

Note:

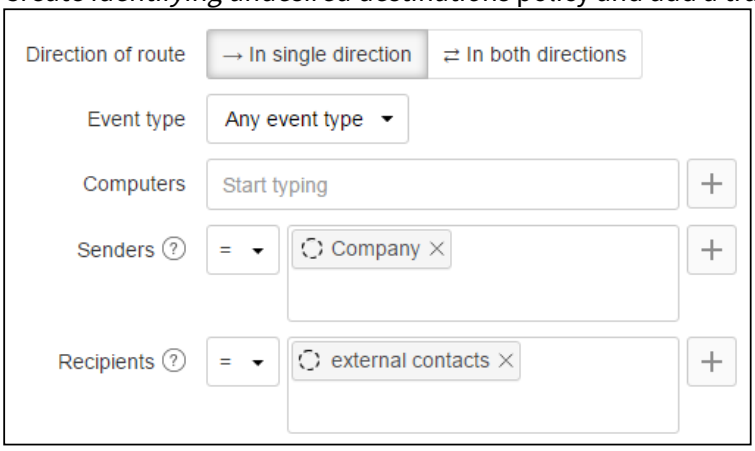
You can add separate person contacts or create user groups, e.g., *Fired employees* and *Competitors*. This example illustrates creating a perimeter based on user groups.

Perform the following steps:

1. Create *Fired employees* group and fill it in one of the following ways:
   - create cards for fired employees manually;
   - import persons from Active Directory, Domino Directory or Astra Linux Directory (if the person card is not deleted from the Directory Service when a person is fired).
2. Create *Competitors* group and fill it in one of the following ways:
   - create a separate card for each person in the group, e.g., John Williams from "New company";
   - create a card for each competitor company and add contacts of the company employees to this card.
3. If necessary, create groups for other undesired destinations.
4. Create a perimeter that will include the created groups and name it, for example, *External contacts*.
5. Add a *Group of persons* element to the perimeter and choose the created groups.



6. Create *Identifying undesired destinations* policy and add a transfer rule to it.



7. Specify what actions to perform if the rule is triggered, e.g., assign *Medium* violation level to the event.
8. Apply the configuration to put the configured policy in action.

If an email is sent to a fired employee or a competitor, the System will determine the policy violation.

If necessary, you can find all such events: for this, create a query and specify the *Identifying undesired destinations* policy in search conditions.

4.8.4 Creating Data Protection Policy on Agents

Purpose:

Create a policy that determines the System reaction to actions with data and applies directly on Device Monitor agents. This policy allows you to operatively prevent data leaks on computers where Device Monitor agents are installed.

> **Note:**
>
> On Device Monitor agents installed on OC Astra Linux, data protection policies on agents are not supported.

Solution:

1. Go to the **Policies** section.
2. In the left part of the workspace click **Add policy** and, in the drop-down list, select **Data Protection Policy on Agents**.
   A new policy will be added to the **Data protection policies on agents** group, and, in the right part of the workspace, a policy adding form will be displayed.
3. 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.

4. In the **Choose protected data** window that appears, set check boxes next to desired values. Protected data may include:
   - **Protected objects**
     You can select protected objects that contain only categories and text objects.
   - **Catalogs of protected objects**
     From selected catalogs, the policy will use only those protected objects that are based on categories and text objects.
   - **File formats**
     For file formats, you can also set an additional restriction on the file size and specify if the policy should apply to all files or only to files with an extraction error. If **With extraction error** option is selected, then the policy is triggered only if an error has occurred while extracting data from files of specified formats (for example, if the file is encrypted or the System failed to determine the file format).

Important!

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 catalog of protected objects and several file formats are specified as protected data for a policy. In this case, for the policy to be triggered, it is necessary that intercepted data should contain at least one protected object from the specified catalog and at least one specified file format.

5. After you have selected protected data, click **Save**.
6. In the right part of the workspace, fill the required fields (see “Раздел "Политики"”), 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 Device Monitor agent. If the local time of interception does not fall within the specified range, the policy does not apply to the event.

Additional information:

- Policy editing is described in "Editing Policy".
- To delete the policy, in the upper right corner of the policy tile, click, ✖ and, in the window that opens, confirm the deletion.

4.8.5 Creating Person Control Policy

Purpose:
Create a policy that determines the System reaction to actions of certain persons. The policy applies only to actions of traffic senders.

Solution:

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

> **Note:**
>
> If elements of different types are selected (for example, persons and statuses), then the policy is triggered when at least one object of each type is detected.

4. A new policy is added to the **Person Control Policies** group, and, in the right part of the workspace, a policy viewing form is displayed.
5. In the policy form, fill in the required fields (see "Policies and their Viewing Form") and click **Save**.

> **Important!**
>
> When you fill the **Validity period** attribute, consider the possible time zone difference between branches of your organization. The time of interception for the event is the local time on the server which intercepts data. If the local time of interception does not fall within the specified range, the policy does not apply to the event.

You can also add person control policies directly from **Persons** (see "Persons") and **Statuses** (see "Statuses") sections.

To add a policy for a group of persons or computers:

1. Go to the **Persons** section.
2. Select the desired group in the list.
3. On the toolbar in the left part of the workspace, click .

To add a policy for selected persons or computers:

1. Go to the **Persons** section.
2. Select the desired person or computer. To select multiple elements, use Shift or Ctrl keys.
3. On the toolbar in the right part of the workspace, click and, in the drop-down list, select **Create policy**.

To add a policy for a selected status:

1. Go to **Lists**->**Statuses** section.
2. Select the desired status from the list.
3. On the toolbar, click .

Example:

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

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 notification** - *example@company.com* value (for details, see “Sending Notifications on Responded Rule");
- attribute **Assign verdict** - *Allow* value;
- attribute **Set status** - *Under supervision* value.

3. Save the policy.

Additional information:

- Rules editing is described in "Editing Policy".
- To delete a policy, click ✕ button located in the upper right corner of the tile and, in the window that opens, confirm the deletion.

4.8.6 Editing Policy

Purpose:
Change attributes of the created policy.

Solution:

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

4.8.7 Creating Rules

Reference information:

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

- Data Transfer
- Data Copy
- Data Placement
- Clipboard

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

- Data Transfer
- Data Copy

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 each other, 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 each other, 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").

For each **person control policy**, you can configure rules for intercepting events with the specified violation level. You can also link the rule with existing data protection policies and data protection policies on agents.

> **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 fully performed.

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

Solution:

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

Example:

When somebody 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.

Additional information:

- Editing rules is described in "Editing Rules".
- To delete the rule, click × button in the upper right corner of the tile and, in the window that opens, confirm the deletion.

4.8.8 Editing Rules

Purpose:
Edit a previously created rule.

Solution:

1. Go to the **Policies** section.
2. On the left side of the workspace, left-click the target policy.
3. In a policy tile, select a target group of rules:
   - **Transfer**, **Copy**, **Placement** or **Clipboard** tabs - for a data protection policy;
   - **Transfer** or **Copy** tabs - for a data protection policy on agent;
   - **Rules** tab - for a person control policy.
4. The policy tile will display the list of policy rules of the selected group. Left-click the desired rule in the list.
5. On the right part of the workspace, the rule editing form will open. Edit the required fields (see "Rules and their Viewing Form") and click **Save**.

4.8.9 Determining System Response to Policy Violations

Reference information:
For each policy, you can specify actions, the System performs in case of rule violation (on how to specify the actions, see "Creating Rule").
Available actions are determined by the rule type:

Action	Data protection policies				Data protection policies on agents		Person control policies
	Transfer rule	Copy rule	Placement rule	Clipboard rule	Transfer rule	Copy rule	Person control rule
Send notification	Available	Available	Available	Available	Available	Available	Available
Notify sender	Available for the "Mail on Client" event type only	Not available	Not available	Not available	Available for the "Mail on Client" event type only	Not available	Not available
Assign verdict to event	Available	Not available	Not available	Not available	Available	Available	Available
Assign violation level to event	Available	Available	Available	Available	Available	Available	Available

Action	Data protection policies				Data protection policies on agents		Person control policies
	Transfer rule	Copy rule	Placement rule	Clipboard rule	Transfer rule	Copy rule	Person control rule
Assign tags to event	Available	Available	Available	Available	Available	Available	Available
Assign status to senders	Available	Available	Available	Available	Available	Available	Available
Delete event	Available	Available	Available	Available	Not available	Not available	Available

A detailed description of actions:

Action	Description
Send notification	Specified Console users will be notified via email. The list may contain users or their email addresses.
Notify sender	The sender of the intercepted email message will receive a notification
Assign verdict to event	The event is assigned a verdict which is a preliminary System decision concerning possible violation of the security policy. Possible values: • **Allow** - the object is not a potential violation and can be delivered to senders. • **Block** - the object is a potential violation. In the "Block" mode, the object delivery is blocked. • **Quarantine** (for data protection policies on agents, this verdict is unavailable) - the user should make a decision whether the object is a violation or not. In the "Block" mode, the object delivery is postponed until the user decision is made. Depending on the user decision, the verdict value will change either to **Allowed** (in this case, the message is delivered) or to **Blocked** (for details, see "Making Decision on Object"). Dispatching messages is available only for SMTP letters when the System operates in the inline mode (for details see the document "*Infowatch Traffic Monitor. Installation and Configuration Guide*".

Action	Description
Assign violation level to event	A violation level will be assigned to the event. Possible values: **High**, **Medium**, **Low**, **No violation**.
Assign tags to event	The event will be assigned tags, for example, **Under supervision**. For details, see "Tags".
Assign status to senders	The security policy violators will be assigned a specified status, for example, **Under supervision**. For details, see "Statuses".
Delete event	The event will not be saved to a database and actions specified in the rule will not be performed either.

See also:

- "Creating Rule" - how to create rules
- "Editing Rules"- how to modify earlier created rules

4.8.10 Determining System Default Response

Reference information:
If after applying the policy, there are sub-events with no matching rules, the System performs default actions (on dividing events into sub-events, see "General Information on Policies"). Default actions are specified by the user.

> **Note:**
> If default actions are not specified and none of the rules is triggered on the interception object, the policy is not triggered on this interception object either.

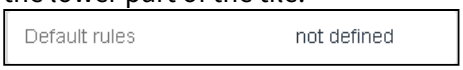
Purpose:

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

> **Note:**
>
> Default actions can only be specified for data protection policies and data protection policies on agents.

Solution:

1. Go to the **Policies** section.
2. On the left side of the workspace, left-click the target policy.
3. In the policy tile, select the target tab (**transfer**, **copying**, **placement** or **clipboard**) and left-click the lower part of the tile:



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

Additional information:

For *Web message* and *Mail in Browser* event types, a default rule can be false triggered. Such a situation may arise when:

The System contains a rule that regulates data transfer from person A to person B. If person A sends data to person B via a website, the System creates an event which is divided into two sub-events:

Sender	Recipient	Protocol
Person A	Person B	HTTP
Person B	Website domain	HTTP

Since the route **Person A**->**Website domain** is not specified in the policy rules, the default actions are executed.

To avoid false triggering of the default rule for *Web message* and *Mail in Browser* event types, do either of the following:

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

Example:

You want the System to assign the *Under supervision* status to the card of the person who copies data if:

- the copied data from a *State secret* protected object, and
- no copy rules are triggered.

For this:

1. Create a data protection policy for the *State secret* protected object (see "Creating Data Protection Policy").
2. Start configuring default policy actions.
3. In the only **Actions** block, set the *Under supervision* value to the **Set status** attribute.

4.8.11 Filtering the List of Policies

Purpose:
Filter the list of policies in case of a large number of policies.

Solution:

1. Go to the **Policies** section.
2. In the left part of the workspace, click **Filter**.
3. In the **Filter settings** area, specify filtering criteria in one of the fields or in both of them:
   - **Filter by policy name** - start typing and select the name of the needed policy (repeat to select several policies)
   - **Filter by objects of research** - start typing and select the name of needed object (repeat to select several objects)
     For data protection policies and data protection policies on agents, you can specify the following objects of research:
     - catalog of protected objects;
     - protected object;
     - file format.

     For person control policies, you can specify the following objects of research:
     - person;
     - group of persons;
     - status.
4. Click **Apply**.

4.8.12 Sending Notifications on Responded Rule

Purpose:
Configure sending automatic notification about responded rule to some users.

> **Warning!**
>
> To send notifications, you can only use e-mail addresses. When you choose existing contacts, select user entries with specified e-mail address only.

Solution:

1. Go to the **Policies** section.
2. On the left side of the workspace, left-click the target policy.
3. In the policy tile, select the desired tab (**transfer**, **copying**, **placement** or **clipboard**) and left-click the target rule in the rule list.
4. The policy tile will display the list of rules of the selected group. By clicking the left mouse button select the desired rule in the list.
5. In the right part of the workspace, in the **Send notification** field, specify a contact of the Management Console user. To do this, start typing the contact details and select the desired entry from the drop-down list.

> **Note:**
>
> If, after the rule is created, the user or user's e-mail are deleted from the System (on managing user accounts, see *“Administration Guide”*, “Users" section), notifications will not be sent to this user.

4.8.13 On Data Protection Policy on Agents

Why do you need data protection policies?

Policies of this type apply first and directly on DM agents. They are used to control activity on workstations and prevent leaks of confidential data.

The policy controls such actions as data transfer (Internet activity, Mail on Client, Mail in Browser) and data copy (FTP, external storage).

How the policy works:

1. The security officer creates and configures the policy. The created policy is then deployed on workstations.
2. A person performs illegitimate actions (e.g., sends confidential data via the mail in browser).
3. DM agent on the workstation analyzes the transferred data.
4. If the policy is triggered, the DM agent performs actions specified in the policy (e.g. blocks sending if *Block* verdict is specified in the rule; in this case, the message is not sent).
5. TM gets the event and analyzes it.
6. The security officer sees the event and its analysis results in the Console and can take necessary actions.

What do you need to create a policy?

- Add policy rules. The following rules can be added: transfer rule, copy rule.
- Choose protected data. If no protected data is selected, the policy is applied to actions with any data.
- Specify a period during which the policy will apply.

4.8.14 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, SMS
- Photo, screenshots, printing
- Crawler
- Clipboard

How the policy works:

1. The security officer creates and configures the policy.
2. A person performs illegitimate actions (e.g., sends SMS 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).
5. The security officer can see the event in the console.
6. The security officer analyses received information and can take necessary actions.

What do you need to create a policy?

- Add policy rules. The following rules can be added: transfer rule, copy rule, placement rule, and clipboard rule (see "Rules and their Viewing Form").

- Choose protected data. If no protected data is selected, the policy is applied to actions with any data.
- Specify a period during which the policy will apply.

4.8.15 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.

4.9 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" contains examples of using reports for monitoring user activities and investigating incidents.

See also:

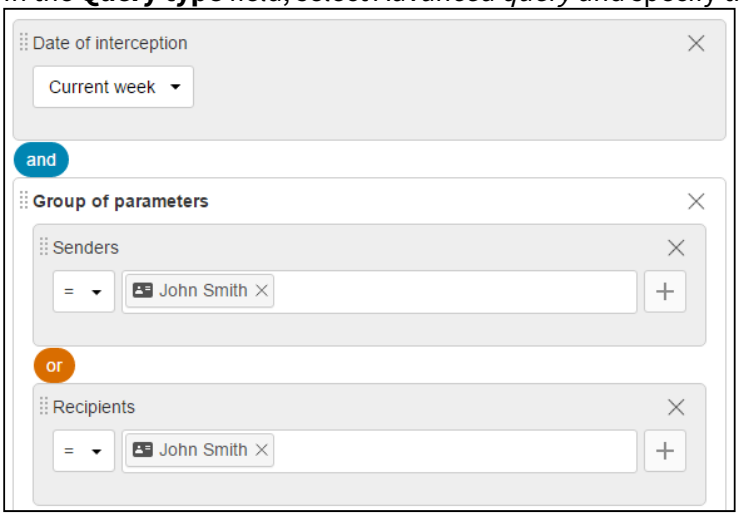
- "Reports Section" - on the section where managing reports is performed

4.9.1 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.

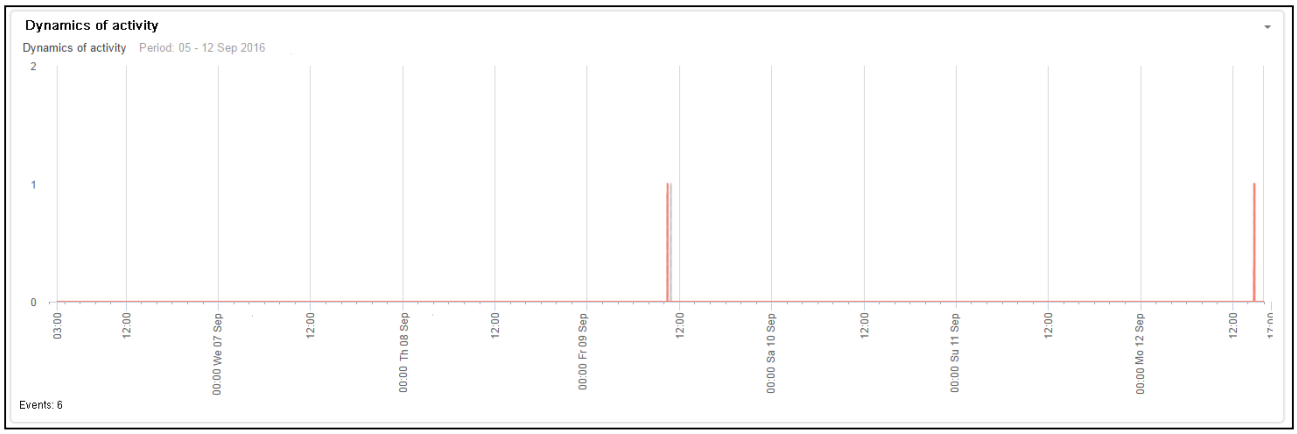
Step 1. Get information about the dynamics of violations. For this:

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.

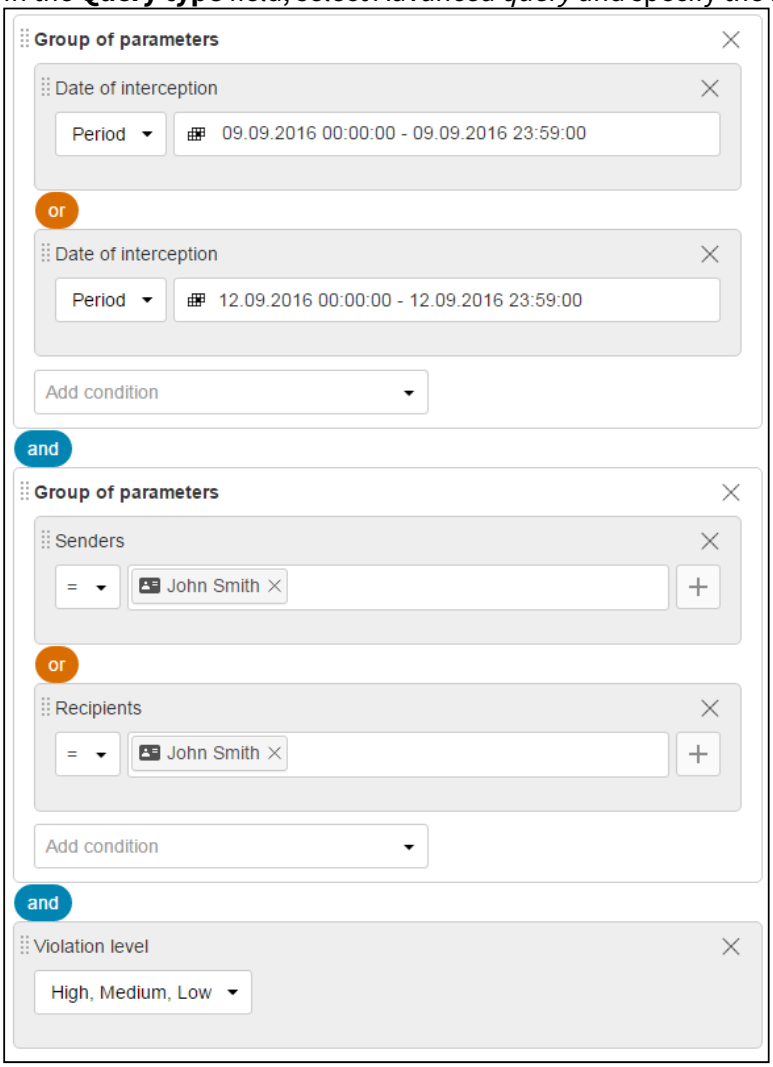
On the chart, you can see that the employee committed most violations on 09.09 and 12.09.



Step 2. Determine the channels through which the data was leaked. For this:

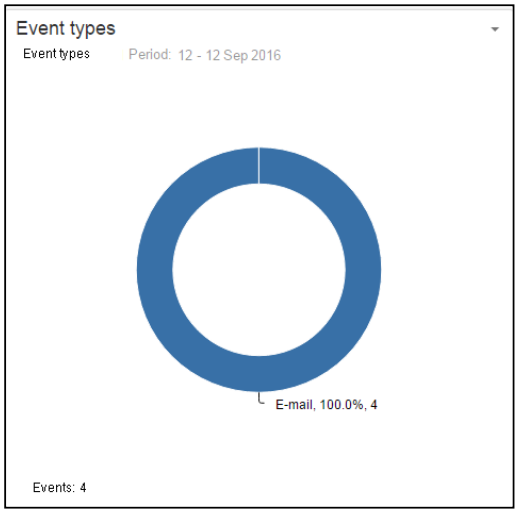
1. Add *Event types* widget to the created report.
2. Open the **Query** tab of the widget.

3. In the **Query type** field, select *Advanced query* and specify the following conditions:



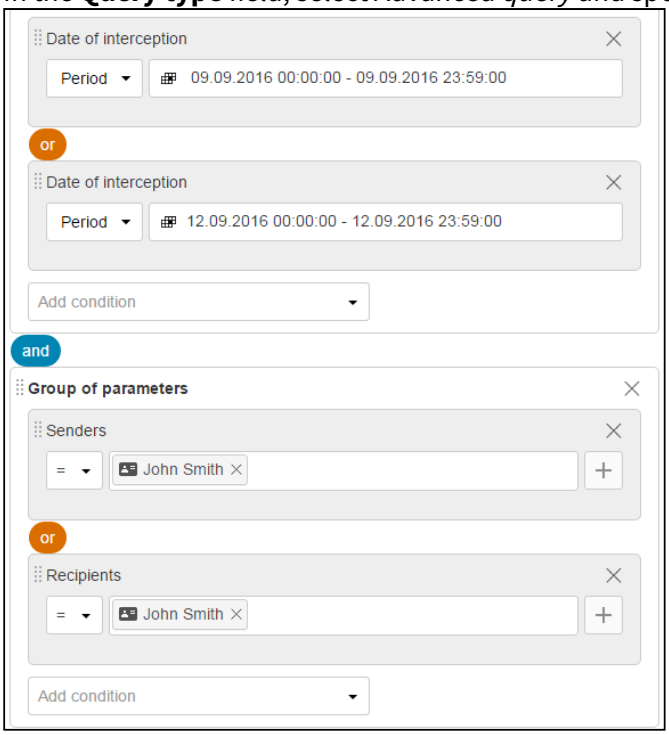
4. Save and run the report.

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.

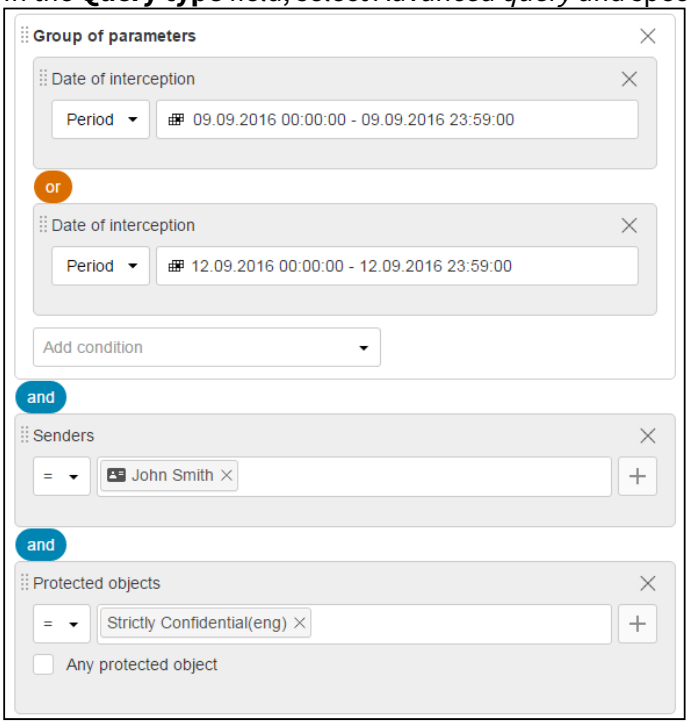
In the report, you can see, that the employee emailed documents included in the *Strictly confidential information* protected object.



Step 4. Determine, to whom John Smith sent confidential data. For this:

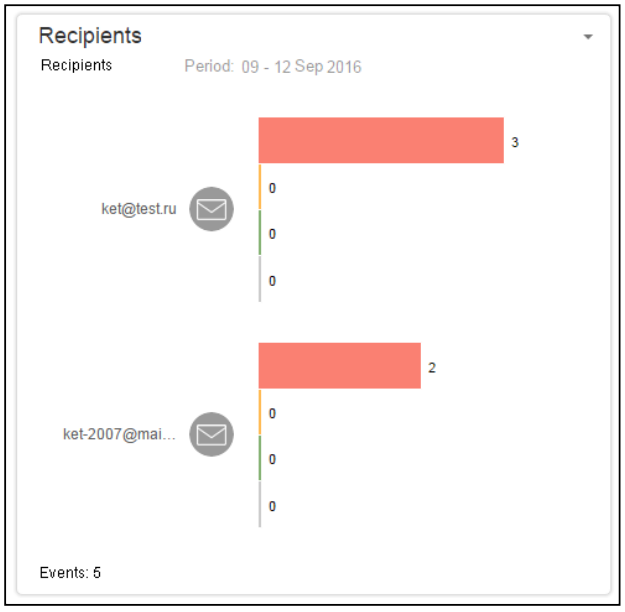
1. Add *Recipients* widget to the created report.
2. Open the **Query** tab of the widget.

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.



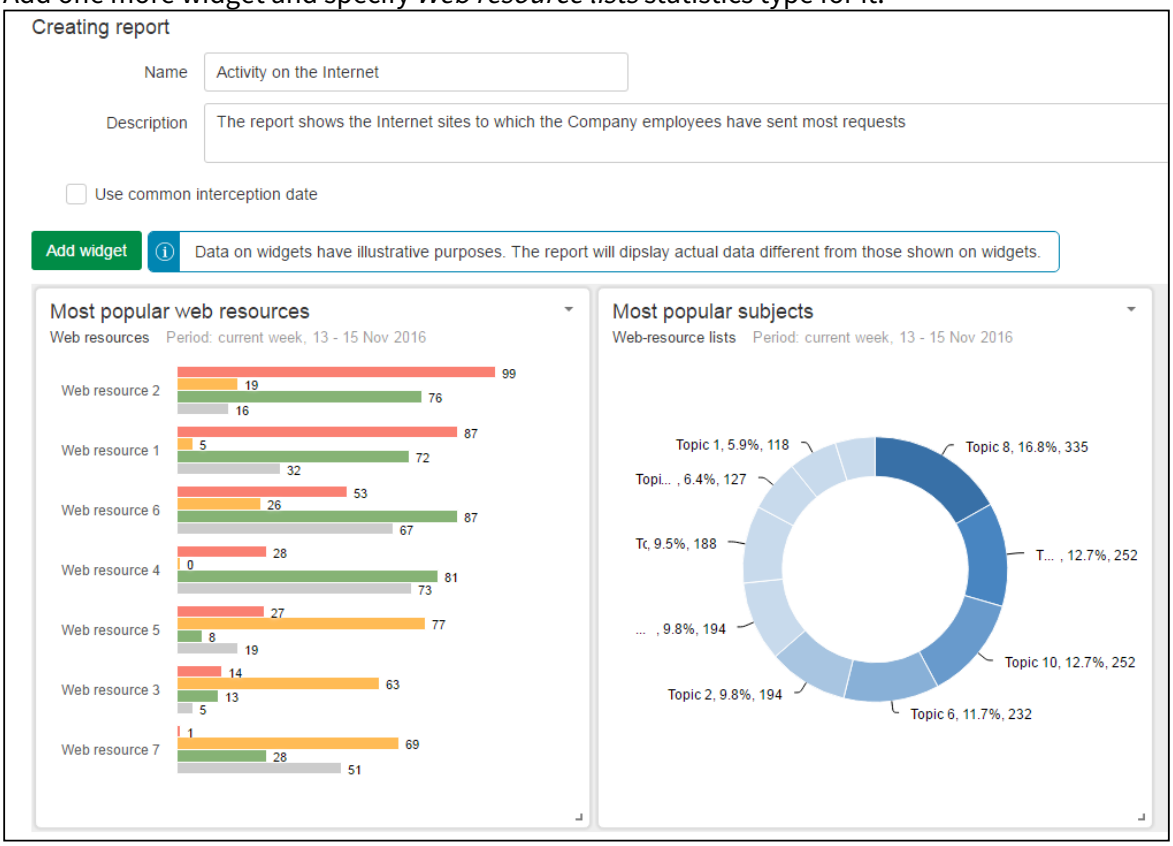
As a result of the investigation, you have determined when, through which channels, and to what recipients the violator leaked confidential data. Now you can easily find the needed events: for this, create a query and specify already known parameters in it (see "Creating queries"). In the found events, 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.

5 Using Device Monitor Management Console

The Management Console (DM) is designed to address the following tasks:

- InfoWatch Device Monitor access and management;
- configuring computers monitoring system;
- computers access control.

To use Management Console (DM) you have to be familiar with Microsoft Windows OS basics.
For more information on Management Console (DM) workflow, see:

- Management Console (DM) Overview. InfoWatch Device Monitor general actions (startup, interface configuration).
- Managing Console (DM) Accounts. How to perform InfoWatch Device Monitor administration tasks: managing InfoWatch Device Monitor Management Console (DM) accounts, working with log, etc.
- General System Settings. Defining global settings which are common for all rules (DM) and policies (DM).
- Managing Security Schema. How to use security schema and configure security settings.
- Viewing DM Events. Viewing information on managed devices and channels of data transfer on the managed computers.
- Agent Remote Installation, Updating and Uninstallation. InfoWatch Device Monitor Agent installation and configuring via Management console (DM).
- Additional Features. Secondary functions enhancing InfoWatch Device Monitor Management Console (DM) user experience: records filtering, grouping and sorting, Management Console (DM) shortcuts.

5.1 Management Console (DM) Overview

Management Console (DM) basics are available in the following subsections:

- Authorization and Connecting to InfoWatch Device Monitor Server;
- Management Console (DM) Main Screen;
- Management Console (DM) Sections.

5.1.1 Authorization and Connecting to InfoWatch Device Monitor Server

When working with DM Management Console, you need a permanent connection with Device Monitor Server. For this, you need to go through **authorization**, during which user permissions to start the Management Console are defined.

When you first start DM Management Console, the System uses the data (username and password) of the account with the **Superuser** role (the Superuser role is created during installation of the server, for details, see "*Traffic Monitor. Installation Guide*", "Server End Installation Procedure" article").

To start working with DM Management Console:

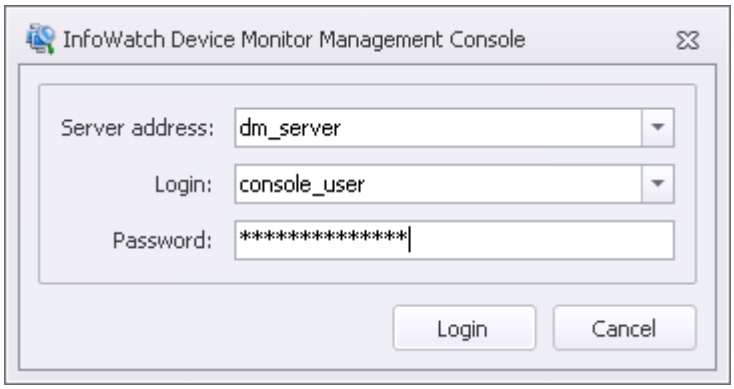
1. Start the Management Console (DM). For this, in the **Start** menu, choose **Programs** > **InfoWatch** > **Device Monitor** > **Management Console** or use the desktop shortcut (created by default during installation)..
2. Perform the authorization procedure as described below.

For successful authorization, the following conditions should be met:

- the database contains a user account with specified parameters;
- a role is assigned to the user account;

- the user account is active (not active);
- the user account is not blocked.

Enter the data for authorization in the connection dialog box.



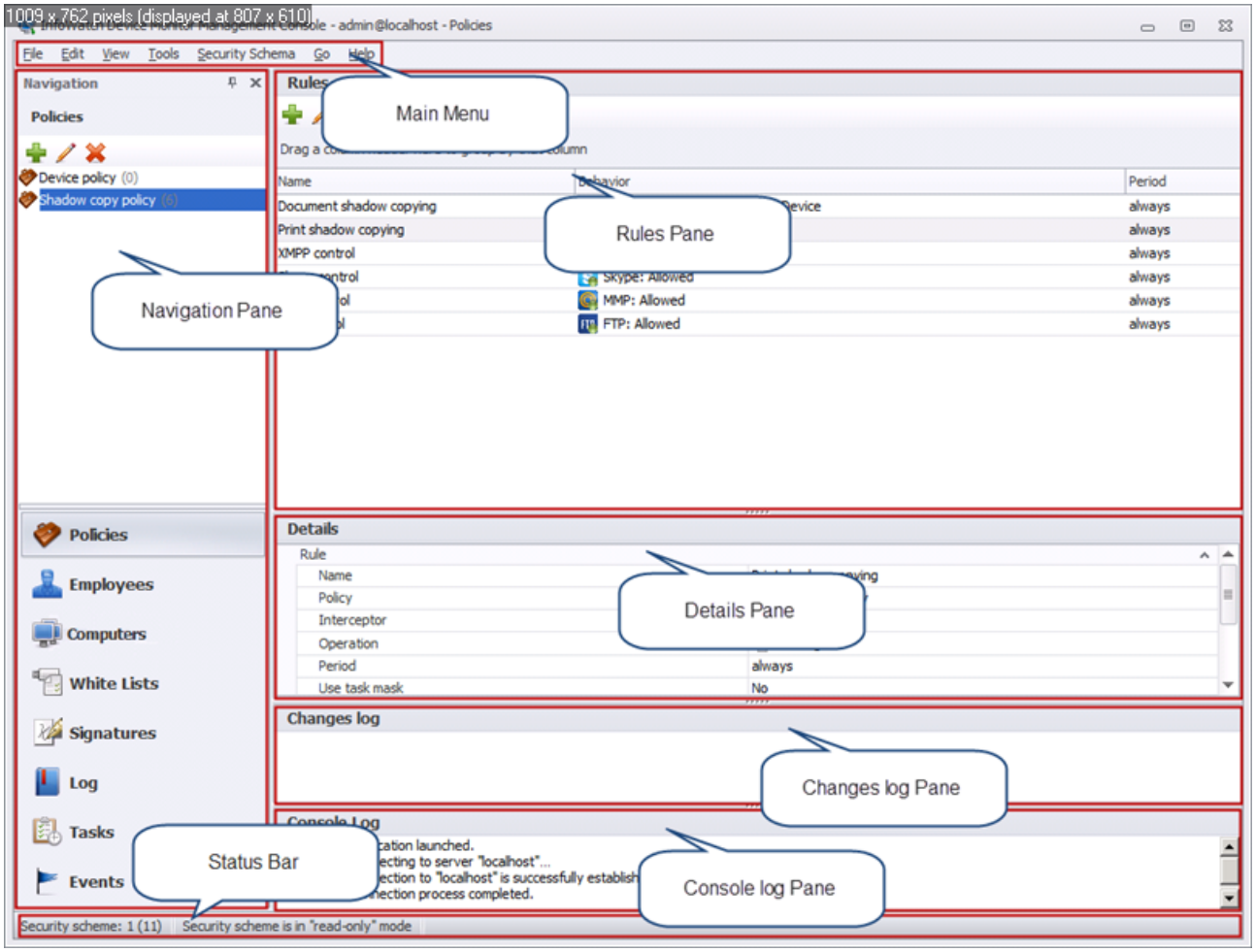
Parameter	Description
Server address	FQDN of the server, the Management Console is connecting to. Th default port for communication between the server and Management Console is 15003. If this port has been changed, enter the server address as follows: `dm_server:port`
Login	Name of the user account
Password	User password. Check the keyboard layout before entering your credentials.

At the first launch of DM Management Console, logon dialog fields are empty. Later, **Server address** and **Login** fields will contain the credentials entered during the previous authorization attempt. You must fill the **Password** field each time you are trying to log in.
You can track the status of connection with the server via system messages on the **Console log** panel (see "DM Management Console Main Screen").

If you need, you can open the authorization box and change the entered parameters to connect to the same or a different server using the same or a different account. To do this, in the Main Menu select **File** > **Connect**, then connect to the Server as described above.

5.1.2 Management Console (DM) Main Screen

After successful authorization in Management Console (DM), the main window is displayed on the screen:



For information on main screen customization see "Configuring Management Console (DM) Main Screen Elements".

The main screen contains elements required for working with the Management Console (DM):

- The **main menu** contains commands that give you access to all Management Console (DM) essential features.
- The **navigation** pane allows you to switch between different section of the Management Console (DM) and manage elements of the selected section.
- The **main screen workspace** allows you to view elements of the selected group and perform operations with these elements.
- The **toolbars** contain buttons for quick access to some functions of the Console (DM). The toolbars are located on the Navigation page (for elements of the selected section) and in the workspace (for the selected element).
- The **Details** pane displayed extended information about properties of the selected element.
- The **Changes log** pane displays all changes made by the current user and not saved in the security scheme.
- The **Console log** pane displays system messages.

If you are working with a single object, most commands are available from the context menu. To open the context menu, right-click the object.

General information on the current status is displayed on the status bar at the bottom of the main screen. In particular, the following information is displayed:

- number of the security scheme current version;
- mode of the security scheme;

- versions of control elements - in the **Computer groups** section.

Configuring Management Console (DM) Main Screen Elements

You can customize the appearance and location of Navigation, Details, Console log panes.

Action	Steps
Hide pane	Click View in the Main Menu and click on the bar title you want to hide. To open the pane again, repeat this step. **Note:** To delete the Navigation pane, you can also use button in the upper right corner of the pane.
Enable/disable pane automatic collapse	Click in the upper right corner of the pane.
Change pane location	Click on the pane name and drag the pane to a new location. Release the button to place the pane.
Return the pane to its original position	Double-click the title bar
Change panel size	Move the pointer to the edge of the panel. When the pointer turns into a double arrow, click and hold to drag the margin into the right direction. Release the button when the size is right.

b panel displays individual element properties. You can collapse or expand property table for any item.

To customize Details panel,
double-click properties table title bar or use the double-arrow button in the right part of the properties table header.

To hide/display toolbar or Status panel,
right-click on toolbar or status panel. In the context menu, flag the elements that will be displayed (by default, only status pane is flagged).

5.1.3 Management Console (DM) Sections

Management Console (DM) includes the following sections: **Policies, Employees, Computers, White Lists, Signatures, Log, Tasks** and **Events**. Each section corresponds to similar Navigation panel area.
To go to the section, do any of the following:

- in the Main Menu select **Go**. In drop-down menu, click on the section title;
- use Navigation panel buttons.

Sections **Policies, Employees, Computers, White Lists** and **Signatures** designed for managing the security scheme, **Applications** section is for controlling the launching of applications, **Log** section is for monitoring security schema management, **Tasks** is for managing Agent installation and uninstallation tasks, **Events** is for viewing the events on managed computers. Detailed description of section functions is available in the following table:

Section icon and name	Section assignment
Policies	Security policy management: creating security policies, setting policy rules
Employees	Employee management: creating employee groups, adding employees to groups
Computers	Computers management: creating computer groups, adding managed computers to groups
Whitelists	Managing white lists of fully accessed devices
Signatures	View and manage signature categories that assign File Monitor rules to certain file formats.
Applications	Application protocol and creating application lists to permit or forbid applications start.
Log	Security schema management activity log (logging administrating responsibility zones and configuring security schema)
Tasks	InfoWatch Device Monitor Agents centralized installation, updating, and uninstallation on computers
Events	Viewing information on employee activities at managed computers using controlled means

5.2 Managing Console (DM) Accounts

For each user who manages the security scheme, an account is created in the Management Console (DM). The account details are used for the authorization in the System and define permission for particular actions.

The Management Console (DM) contains a pre-installed user - **Superuser**, who has permissions for all operations in the Console. This user is intended not for everyday operations, but for initial configuration of the Management Console (DM), creating the Administrator account and then only in case of emergency.

To define privileges of users working in the Management Console (DM), roles are used. One user can have several roles for different groups. For each role, a set of privileges is defined.

The Management Console (DM) has the following preset roles:

- **Administrator** - a role for Console (DM) administrator who manages other Console accounts.
- **Security officer** - a role of Console (DM) end user who manages the security scheme and server settings.
- **Security officer of the group** - a role of Console (DM) end user who manages groups of employees and computers. сотрудников или компьютеров.

You can add custom roles based on preset ones and specify required settings for them (see "Adding role of the Management Console (DM) user").

The list of available actions for preset roles:

Action	Administrator	Security officer	Security officer of the group
Viewing audit log		+	

Action	Administrator	Security officer	Security officer of the group
Export audit log records		+	
Deleting audit log entries			
View Management Console accounts information	+	+	
Add, edit, delete Management Console (DM) accounts	+		
Assign/delete Management Console account roles	+		
Block/unblock Management Console accounts	+		
Viewing Device Monitor Server settings. Configuring connection to Traffic Monitor server		+	
View security schema versions		+	
Edit security schema		+	
Import/export security policies and rules		+	
Viewing events		+	
Agents Remote Installation, Updating and Uninstallation		+	
Temporary Employee Access to Network		+	
Temporary Employee Access to Devices		+	
Creating group			+
Viewing and managing employee groups, Viewing and managing computer groups, Viewing events for a group			+
Viewing and managing whitelists			+
Managing agents		+	+

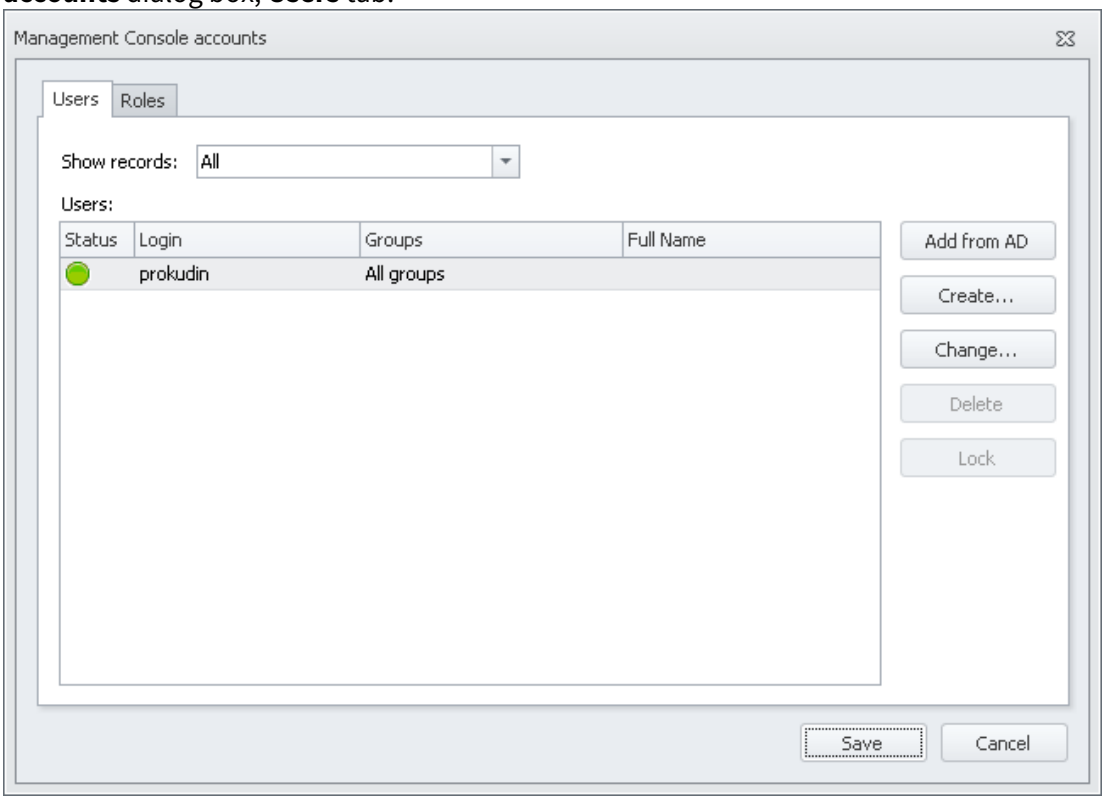
For more information on Management Console (DM) accounts management, see:

- Viewing Management Console (DM) account details;
- Adding New Management Console (DM) Account;
- Locking or Unlocking Management Console (DM) Account;
- Editing Management Console (DM) Account;
- Deleting Management Console (DM) Account;
- Management Console (DM) Security Schema Operation Activity Log.

5.2.1 Viewing Management Console (DM) account details

To view information on the Management Console accounts:

1. In the Main Menu, click **Tools > Console users and roles**. This opens **Management Console accounts** dialog box, **Users** tab.



2. There is **Show records** field at the top of the dialog box. Select displayed accounts type in from the drop-down list:
   - **All**. All accounts regardless of their status.
   - **Active**. List of all active accounts.
   - **Blocked**. List of blocked accounts which can be unblocked (see "Locking or Unlocking Management Console (DM) Account").
   - **Deleted**. List of deleted accounts which cannot be restored. However, the System saves information about actions those users performed.

> **Note:**
>
> Management Console (DM) can be only operated by accounts from the **Active** list. Deleted accounts can only be viewed.

For each entry, the following attributes are displayed:

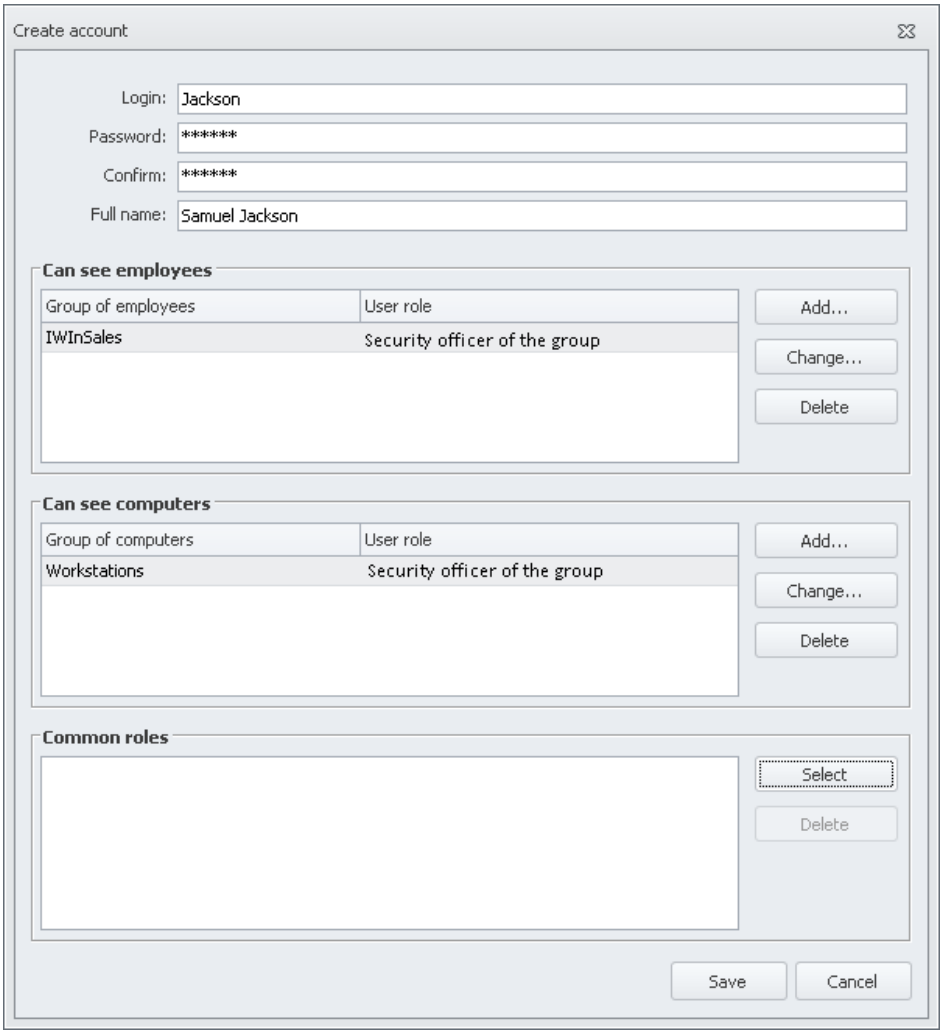
- **Status**. Indicates if the account is active (), blocked () or deleted ().
- **Login**. Name of the user account.
- **Groups**. Groups available to the user.
- **Full Name**. User's personal data.

Login, password, role, and status are mandatory attributes. For a detailed description of roles, see "Roles of DM Console users".

Adding New Management Console (DM) Account

To add a new Management Console account:

1. In the Main Menu, click **Tools > Console Accounts and Roles**.
2. Click **Create** at the right of **Management Console Accounts** dialog box.
3. Specify account settings in the **Create account** dialog box:
   - **Login**. Name of the user account.
   - **Password**, **Confirm**. Account password.
   - **Full name**. User's first and last name.



4. Specify visibility of employees and computers for the user (see "Assigning roles to user").
   - **Can see employees**. The list of employee groups available to the user and their roles;
   - **Can see computers**. The list of computer groups available to the user and their roles.
   - **Common roles**. The list of additional user roles.

Important!

At least one role of any type and a role for each available group must be assigned to the user.

5. Click **Save**.
   The **Create account** dialog box will close. Details of the new account will be displayed in the **Management Console Accounts** dialog box.

Note:

The new account status is active. You can lock the account, if necessary (see "Locking or Unlocking Management Console (DM) Accountt").

To add a user from Active Directory or ALD:

1. In the main menu, select **Tools > Console Accounts and Roles**.
2. Click **Add from AD** button.
3. In the **Adding user from AD** dialog box, select a user from a group (or use the search field).
4. Assign roles to the added user (for details, see "Assigning roles to user").
5. Click **Save**.

Note:

The login and full name that are displayed in the **Management Console Accounts** dialog box for the imported user will be filled automatically. The password matches the user password in AD.

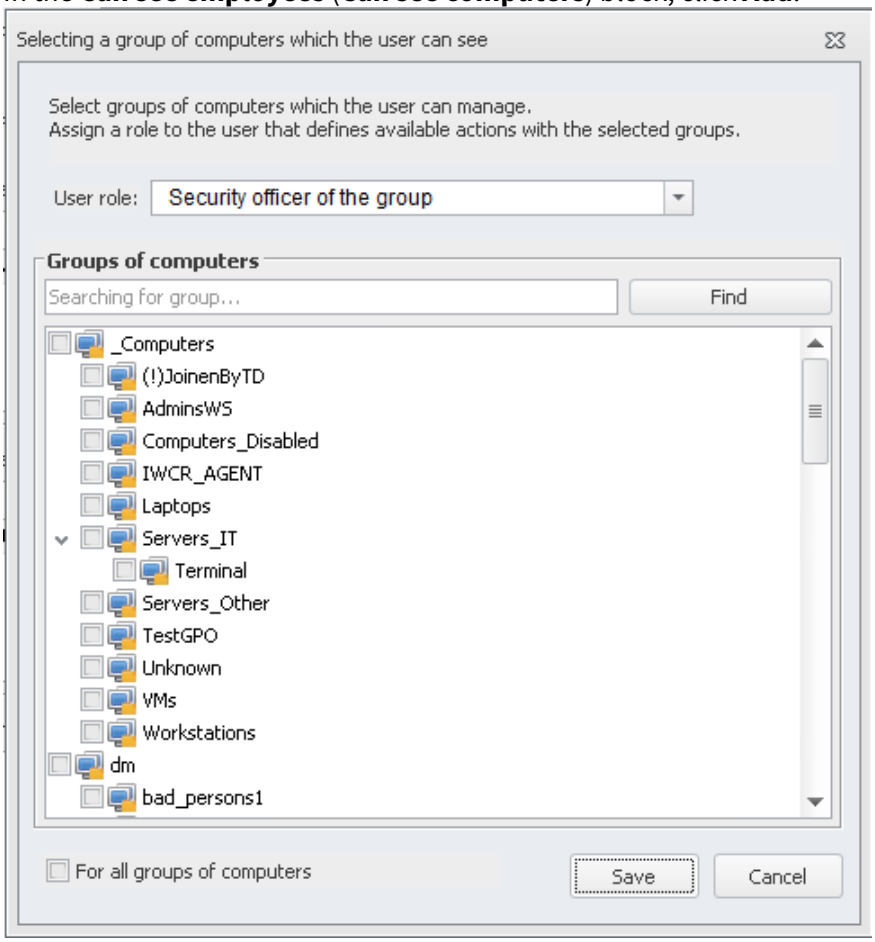
Assigning roles to user

Adding a user role for groups of employees (computers)

To add a group of employees to the user's visibility scope:

1. Open the **Creating user** (or **Editing user**) dialog box.

2. In the **Can see employees** (**Can see computers**) block, click **Add**.



3. In the window that opens:
   - Specify **User role**;
   - Select one or more groups of employees (or computers) from the tree structure or use the search field. Select **For all user groups** (**For all computer groups**) if you need to add all groups.
   - Click **Save**.
4. In the **Editing user** window, click **Save**.

Editing a user role for groups of employees (computers)

To change access permissions to the user's visibility scope:

1. Open the **Editing user** dialog box**.**
2. In the **Can see employees** (**Can see computers**) block, select the required group.
3. Click **Edit**.
4. In the window that opens, assign a role that defines user actions with the group. Further actions with employees (computers) will be performed according to the role privileges.
5. Click **Save**.

To remove a user role:

1. Open the **Editing user** dialog box.
2. In the **Can see employees** (**Can see computers**) block, select the required group.
3. Click **Delete.**
4. Click **Yes** for confirmation. The selected role will be removed from the user.

Configuring user common roles

To assign common roles to the user:

1. Open the **Creating user** (or **Editing user**) dialog box.
2. In the **Common roles** block, click **Select**.
3. In the window that opens, select roles that determine actions available to the user.
4. Click **Save**.

To remove common user roles:

1. Open the **Editing user** dialog box.
2. In the **Common roles** block, select the role you want to remove.
3. In the window that opens, click **Delete**. The common role will be removed from the user.

Editing Management Console (DM) Account

> **Warning!**
>
> If you edit a role that is currently authorized in the Management Console (DM), then after saving changes, connection with the server is automatically terminated. Then the user has to be authorized with new parameters. All unsaved changes will be lost.

To edit parameters of the Management Console account:

1. In the Main Menu, click **Tools > Management Console accounts**. This opens **Management Console Accounts** dialog box.
2. Select a row that contains the name of the account you want to edit.
3. Click **Change** or double-click the selected row.
4. In the **Change account** dialog box, edit the account parameters (the parameters are described in "Adding New Management Console (DM) Account").
5. After all necessary settings have been configured, click **Save**.
6. To apply changes, click **Save** in the **Management Console Accounts** dialog box.

> **Important!**
>
> For pre-installed users, you can only change a password.

Locking or Unlocking Management Console (DM) Account

Information about locked accounts is displayed in the **Management Console Accounts** dialog box.

> **Warning!**
>
> You can lock any account except Superuser and the account you are logged in with.
>
> You cannot log in with a locked account.

To lock/unlock Management Console account:

1. In the Main Menu, click **Tools > Management Console Accounts and Roles**. The **Management Console Accounts** dialog box will open.
2. Select a row that contains the account name.
3. Change the locking status:

- if the account is locked (state), click **Unlock**.
- if the account is unlocked (state), click **Lock**.

- Click **Save** to apply changes.

Deleting Management Console (DM) Account

After deletion, the account is moved to the list of deleted accounts. The account information remains in the database. You can view deleted accounts in **Management Console Accounts** dialog box. To do this, select **Obsolete** in the **Accounts** drop-down list.

> **Warning!**
>
> Accounts for Superuser and preset users cannot be deleted.
> Deleted accounts cannot be restored.

To delete Management Console account:

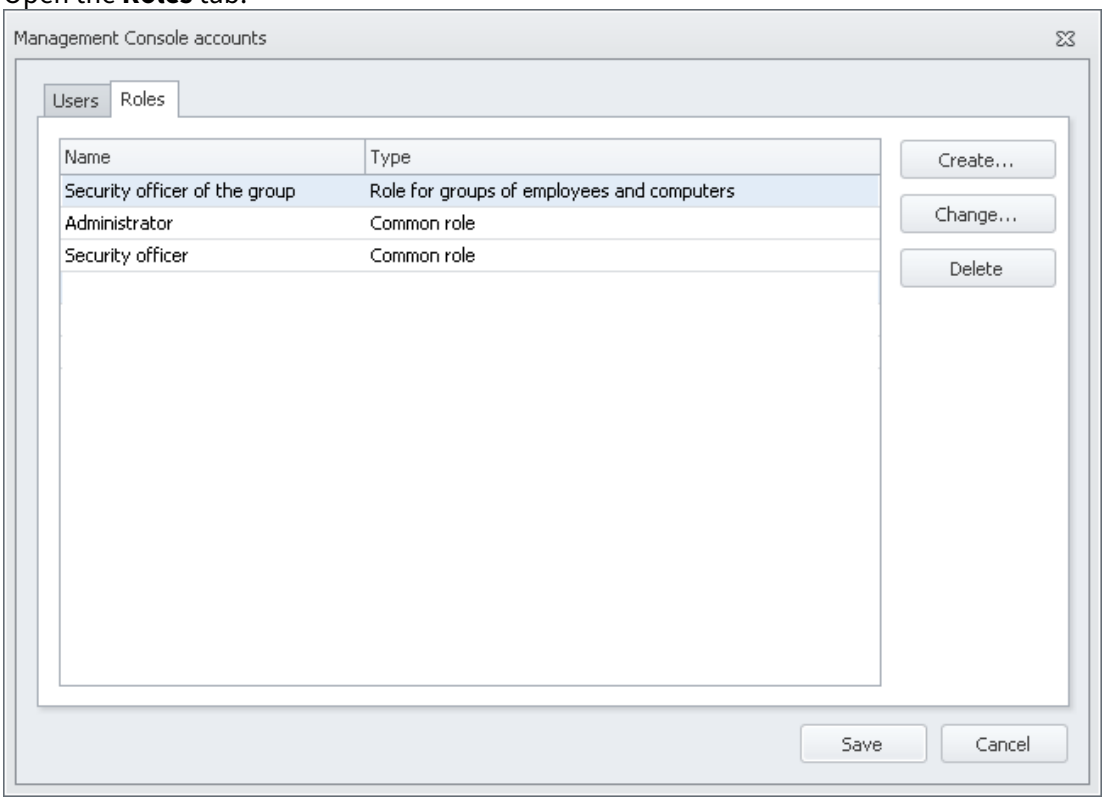
1. In the Main Menu, click **Tools > Console users and roles**. This opens **Management Console Accounts** dialog box.
2. Select a row that contains the account you want to delete.
3. Click **Delete** in the right part of the dialog box.
4. In the confirmation dialog, click **Yes**.
5. To apply changes, click **Save** in the **Management Console Accounts** dialog box.

5.2.2 Roles of DM Console users

To view information about role of Console users:

1. In the main menu, select **Tools** > **Console users and roles**. The **Management Console accounts** dialog box will open.

2. Open the **Roles** tab.



3. The tab contains a table with information on roles with the following attributes:
   - **Name**.
   - **Type**. Possible values:
     - **Role for groups of empoyees and computers** - includes permissions (privileges) for actions with groups of employees or computers.
     - **Common role** - includes permissions (privileges) for common actions in the Console.

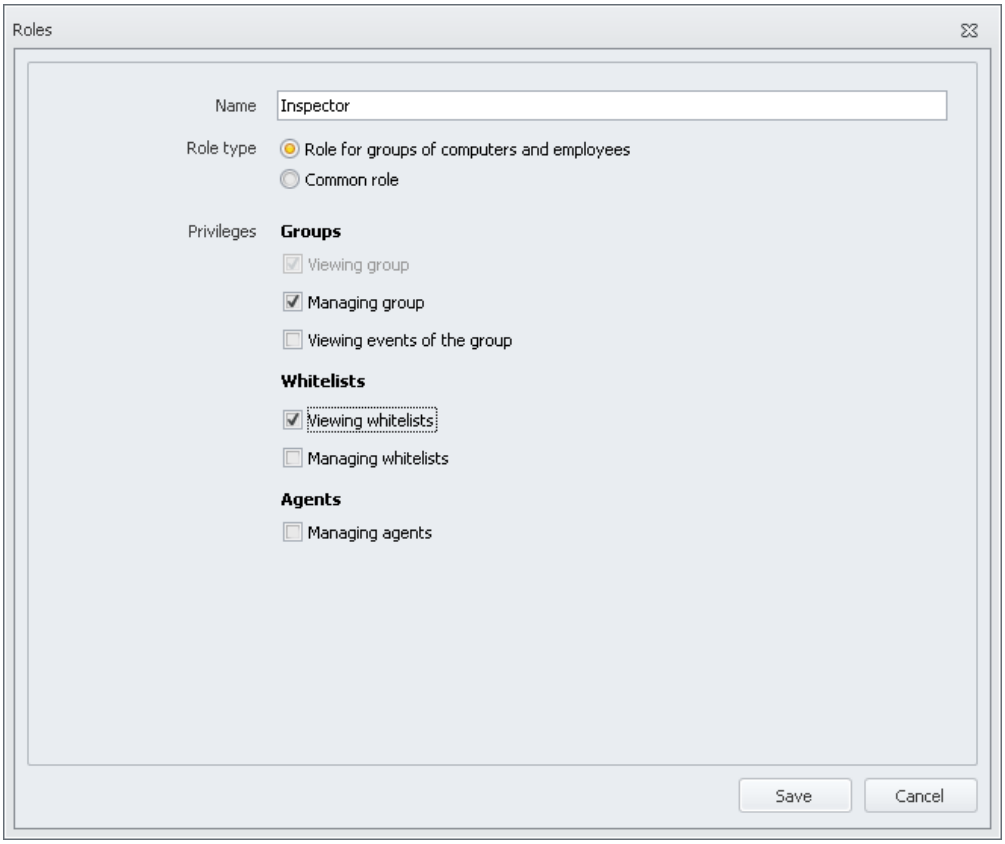
For a detailed description of privileges, see "Adding role of the Management Console (DM) user".

Adding role of the Management Console (DM) user

To add a role for the Management Console user:

1. In the main menu, choose **Tools** > **Console Users and roles**.
2. Open the **Roles** tab.
3. Click **Create**.
4. In the window that opens, specify parameters of the role:
   - **Name**
   - **Role type**
   - **Privileges**

> **Note:**
>
> A set of available privileges depends on the role type.



5. Click **Save**.
6. The **Creating role** dialog box will close. Information on the new role will appear on the **Roles** tab of the **Management Console Accounts** dialog box.

User privileges

In Device Monitor Management Console, privileges are actions that the user can perform with:

- a group of employees or computers;
- the whole System (common privileges).

Privileges for groups of employees/computers

Privilege	Available actions
Groups	
View group	• View the group in the list of groups • View the group parameters • View the list of computers/employees included in the group • View the effective policy for the computer/employee • View all subgroups of the group

Manage group	• Edit group parameters (including the policy assigned to the group; the policy should be available to the user for reading or editing) • Add/delete computers/employees of the group • Copy computers, employees or subgroups of the group • Manage all subgroups of the group • Delete groups **Note:** adding this privilege enables the **View group** privilege.
View group events	View events received from workstations/employees of the group and its subgroups. **Note:** adding this privilege enables the **View group** privilege.
Whitelists	
View whitelists	View whitelists related to the group and its subgroups
Manage whitelists	Create/edit/delete whitelists for the group and for computers/employees included in the group and its subgroups. **Note:** adding this privilege enables the **View whitelists** privilege.
Agents	
Manage agents	Add workstations from the group and its subgroups to the tasks to updating/deleting agents or changing the uninstallation password. **Note:** adding this privilege enables the **View group** privilege.

Common privileges

Privilege	Available actions
Policies	
View all policies	View all System policies available for reading and editing and their rules
Manage all policies	• Edit all System policies (irrespective of the policy owner and access level) and their rules • Create new policy • Delete policy (available only to the owner)
Manage available policies	• Edit policies that are available to the user (policies owned by the user and policies that are available for editing to all users) • Create new policy • Delete policy (available only to the owner)
Other privileges	
View audit log	Access to the "Log" section

Delete log entries	Delete entries from the audit log, clear the audit log. **Note:** adding this privilege enables the **View audit log** privilege.
Manage users	▪ View Console users and roles ▪ Create Console users and roles ▪ Edit Console users and roles ▪ Delete Console users and roles
Create groups	Create new groups of computers or employees. A new group is automatically added to the list of groups available to the user. The predefined role *Security officer of the group* is assigned to the group. **Note:** adding this privilege enables the **View all policies** privilege.
Manage agents on separate computers	• Add computers from the network environment and through connection to AD or ALD in the agent distribution task • Add computers through the file import or by name/IP • Create installation package • Delete agent from a mobile device
Manage settings	Manage global DM settings (except "Integration with AD" section in **Tools** -> **Settings** menu)
Sync with AD	Configure synchronization of workstations and employees with AD or ALD ("Integration with AD" section in **Tools** -> **Settings** menu)
Import/export of configuration	Import and export the security scheme and settings **Important!** This privilege allows the Console user to import and export the configuration regardless of the user permissions for imported/exported objects
Provide temporary access	Provide temporary access to the network or devices on the employee request

Editing role of DM Console user

> **Important!**
>
> If you edit a role that is currently authorized in the Management Console (DM), then after saving changes, connection with the server is automatically terminated. Then the user has to be authorized with new parameters. All unsaved changes will be lost.

To edit parameters of the Console user role:

1. In the main menu, choose **Tools** > **Console users and role**. The **Management Console Accounts** dialog box will open.
2. On the **Roles** tab, select a row with the role you want to edit.

3. Click **Edit** or double-click the selected row.
4. In the **Roles** window that opens, edit the role parameters (the parameters are described in "Adding role of the Management Console (DM) user"). The role type cannot be changed.
5. Click **Save**.
6. To apply changes, click **Save** in the **Management Console Accounts** dialog box.

> **Important!**
>
> Pre-installed roles (Administrator, Security officer, and Security Officer of the group) cannot be edited.

Deleting role of DM Console user

To delete a role of the Console user:

1. In the main menu, choose **Tools** > **Console users and role**. The **Management Console Accounts** dialog box will open.
2. On the **Roles** tab, select a row with the role you want to delete.
3. Click **Delete** in the right part of the window.
4. In the confirmation window, click **OK**.

> **Important!**
>
> A role assigned to a user cannot be deleted. To delete the role, you should remove it from all users.

5. To apply changes, click **Save** in the **Management Console Accounts** dialog box.

5.2.3 Management Console (DM) Security Schema Operation Activity Log

Management Console (DM) operation involves various security schema managing activities. Records related to activities that change database information (security schema customization, System administration) are stored in the Audit Log.
For information on Audit Log see:

- Viewing Log;
- Log Records Filtering;
- Deleting Records from Log;
- Exporting Log Records;
- Analyzing Log Records in Microsoft Excel.

Viewing Audit Log

You can manage audit log of Management Console (DM) user activities in the **Log** section. To go to this section, click **Log** button on Navigation pane.
Security schema management activities are performed as transactions. Transactions appear as a set of records in the audit log. Each record contains information on one basic action (transaction step). The transaction may only contain one step and will be represented by a single record in the audit log.

Configure filters to select records that meet certain criteria (for information on filters see "Log Records Filtering"). Filter list is displayed in **Log** area of Navigation pane. Records for selected filter are displayed in the main screen workspace.

> **Note:**
>
> Use additional options to adjust audit log records display (see "Additional Features").

To view a full list of audit log records, click **Show All Records** at the top of Navigation Pane.

To view filtered records, click the filter name in the filter list.

Log information is displayed in a tabular list where each row contains a single record. Columns contain basic properties of log entries. Extended information on each record is available in **Details** panel.

To view advanced information for a particular record, select the row that contains the record name in the main screen workspace.

Details panel displays properties table containing the following information for selected entry:

Property	Description
Transaction number (#)	Transaction number
Step	Basic action number within selected transaction
Date occurred	Action date and time
Object	Target object name
Action	Activity type
Object selector	Contains information that helps identify the target object. Selector values interpretation see in "Selector Values".
Field name	Object attribute changed by the action
Old value	Previous value of the attribute
New value	New value of the attribute
User	Name of Management Console (DM) account that initiated the transaction
Windows account	Account with credentials for Windows authorization
Computer	Name of the computer that initiated the action
Sequence number	Record number in the database

Some information from the **Details** panel is duplicated in the main screen workspace.
Number of transaction steps (and, therefore, number of log records) varies depending on the object and actions performed.

For example:
The image contains a few log records referring to different transactions.

#	Step	Date and Time ...	Object	Action	Object Selector	Field Name	Old Value	New Value	User	Seq...
10	1	5/29/2012 10:17...	Rule	Add	4/Device policy/Floppy control	Active since		1/1/1753 12:00:00 AM	1	38
10	2	5/29/2012 10:17...	Rule	Add	4/Device policy/Floppy control	Active until		12/31/9999 11:59:59 PM	1	39
10	3	5/29/2012 10:17...	Rule	Add	4/Device policy/Floppy control	Operation		Floppy: Full Access	1	40
10	4	5/29/2012 10:17...	Rule	Add	4/Device policy/Floppy control	Allow only to en...		No	1	41
10	5	5/29/2012 10:17...	Securit...	Add	4/Floppy read-only for Device Policy	Comment		Floppy read-only for Device P...	1	42
9	1	5/29/2012 9:54:...	Log	Export	Object in (Rule, Policy)				1	37
8	1	5/29/2012 9:49:...	Rule	Change	3/Device policy/CD/DVD Access	Operation	CD/DVD: Full Ac...	CD/DVD: Read Only	1	35
8	2	5/29/2012 9:49:...	Securit...	Add	3/CD/DVD read-only for Device Policy	Comment		CD/DVD read-only for Device ...	1	36

Transaction number 3 is associated with adding a comment to security schema.
Transaction number 4 corresponds to one change applied to a security schema. This was done in 9 steps. Steps 1-3 changed rule (DM) named "New IM client rule" in "Test Policy" security policy (DM). Each step configures a single rule (DM) parameter: for example, in step 1 an operation was defined, in step 2-3 an action period was set. Steps 4-7 added a new rule (DM), step 8 deleted another one. In step 9 a comment was added to saving security schema version.
Transaction number 5 is associated with Audit Log records export. This transaction includes one step.

Selector Values

Selector parameter contains instructions for target object search. **Selector** parameter value depends on particular object and performed actions. Each object has a different set of **Selector** values.
Edited security schema version is displayed for modified security schema settings followed by "/" and name of modified parameter.
When editing an object (action **Modify**) **Selector** value contains object name before modification.
The following are sample interpretations of *Selector* values.

Example 1
Audit Log includes the following record:

#	Step	Date and Time Occurred	Object	Action	Object Selector	Field Name	Old Value	New Value	User	Sequence ...
7	1	5/28/2012 3:42:42 PM	Policy	Add	2/New Policy	Policy		New Policy	1	17

This record indicates that a rule was changed in your security schema.
Selector value interpretation
Transaction took place while version 10 of security schema was active. A rule named "New IM client rule" was changed in policy named "test(new)": Skype access was denied.

Example 2
Audit Log includes the following record:

#	Step	Date and Time Occurred	Object	Action	Object Selector	Field Name	Old Value	New Value	U...	Sequence...
8	1	5/29/2012 9:49:22 AM	Rule	Change	3/Device policy/CD/DVD Access	Operation	CD/DVD: Full Access	CD/DVD: Read Only	1	35

This record is a step of transaction which adds a computer group to the security schema.
Selector value interpretation
Transaction took place while version 3 of security schema was active. The "*Device*" policy was assigned to new computer group.

Example 3
Audit Log includes the following record:

#	Step	Date and Time Occurred	Object	Action	Object Selector	Field Name	Old Value	New Value	User	Sequence Number
9	1	5/29/2012 9:54:04 AM	Log	Export	Object in (Rule, Policy)				1	37

This record indicates that audit log records were exported.
Selector value interpretation
All records for operation on policy and rules were exported during this transaction.

Log Records Filtering

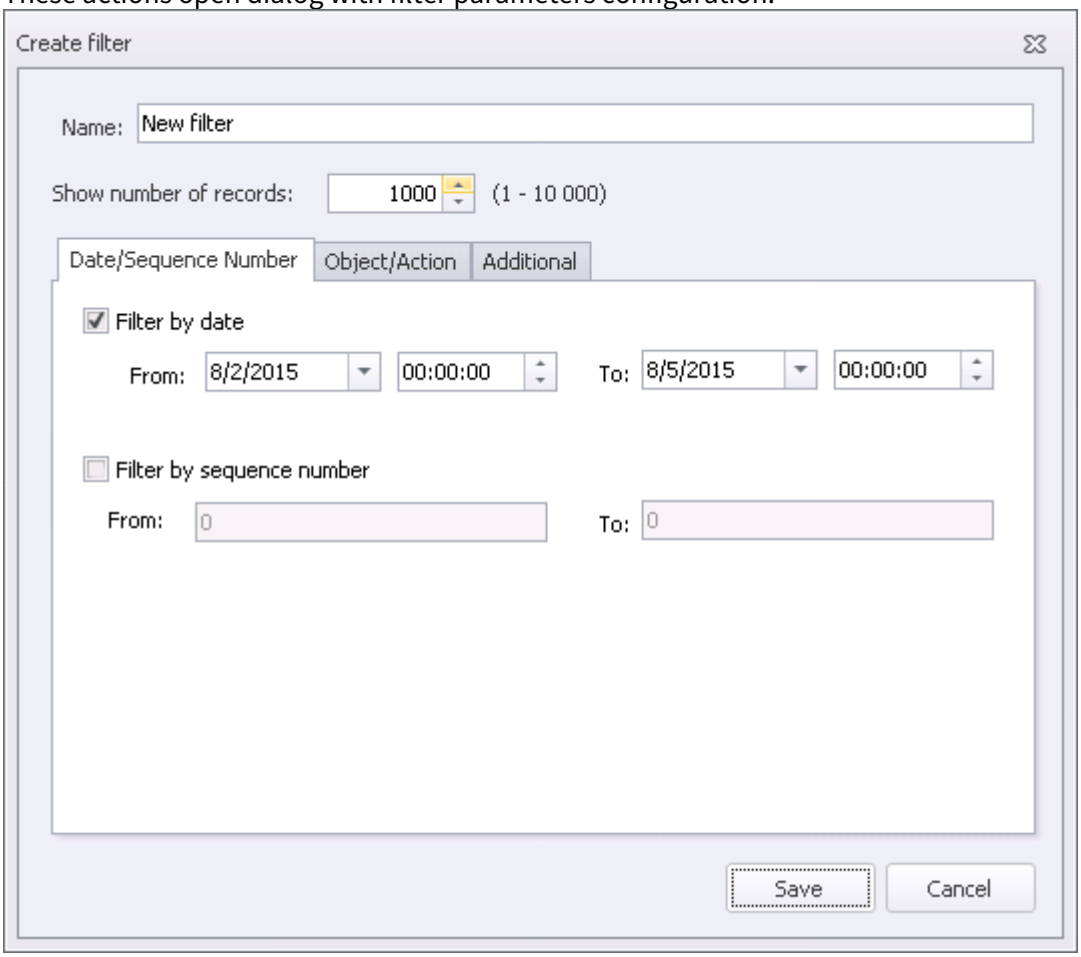
To access audit log records that meet certain criteria, you can use filters.

To create a new filter or modify an existing one:

1. Go to **Log** section.
2. Perform the following steps:

Action	Steps
Creating filter	• in Main Menu, select **Edit > Create Filter**; • click **Create filter** at the top of Navigation pane; • right-click in the **Log** area and choose **Create Filter** from the context menu; • press Ctrl+N.
Editing filter	a. In **Log** area of Navigation pane, select the name of the filter you want to edit. b. Take one of the following steps: • In Main Menu, click **Edit > Edit filter**; • click **Edit Filter** at the top of Navigation pane. • double-click with the left mouse button on the name of the chosen filter; • right-click the selected filter and choose **Edit** from the context menu; • press Ctrl+E.

These actions open dialog with filter parameters configuration.



3. Specify general filter options in filter parameters configuration dialog:
   - **Name**.
   - **Show number of records**. Limit on the number of entries displayed in Management Console (DM) workspace (1000 records by default).
4. Specify filtration criteria. Filtration configuration is performed on several tabs and is described in the following articles:
   - Date/Sequence Number Tab;
   - Object/Action Tab;
   - Additional Tab.

> **Warning!**
>
> If no condition is specified in filter parameters configuration dialog, filtering parameters are disabled. When this filter is applied, all records from the Audit Log will be displayed.

5. Click **Save**.

To remove filter:

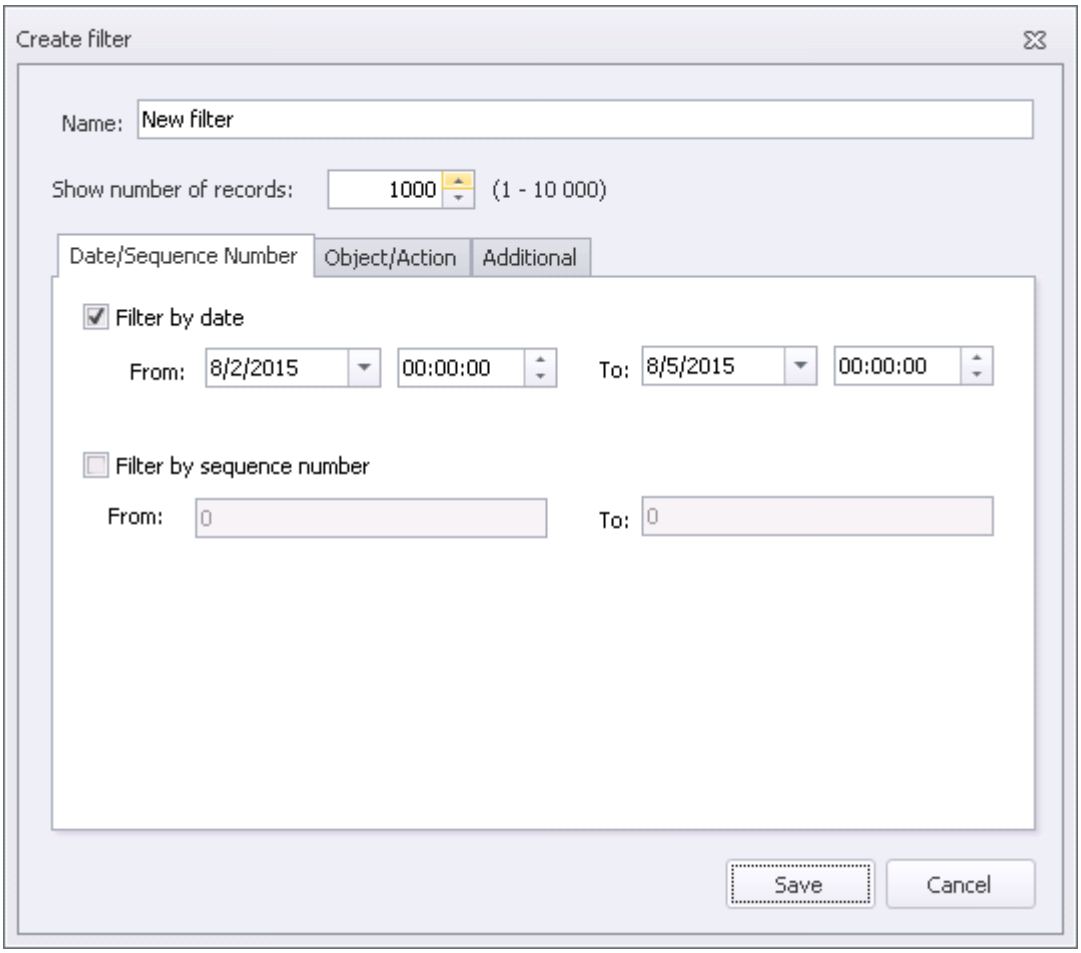
1. Go to **Log** section.
2. In the **Log** area of Navigation pane, select the name of the filter you want to remove.

3. Take one of the following steps:
    - in the Main Menu, select **Edit > Delete Filter**;
    - click **Delete Filter** at the top of Navigation pane;
    - right-click the selected filter and choose **Delete** from the context menu;
    - press Ctrl+D.
4. In the confirmation dialog, select **Yes** to confirm the deletion.

Date/Sequence Number Tab

Configure the following criteria on **Date/Sequence Number** tab:

- date and time the action took place;
- record number in the database.



To specify date and time criteria:

1. Flag **Filter by date** check box.
2. Specify the desired period.
   Starting and ending time is specified in **From** and **To** fields respectively. Set the date and time in right and left field respectively.

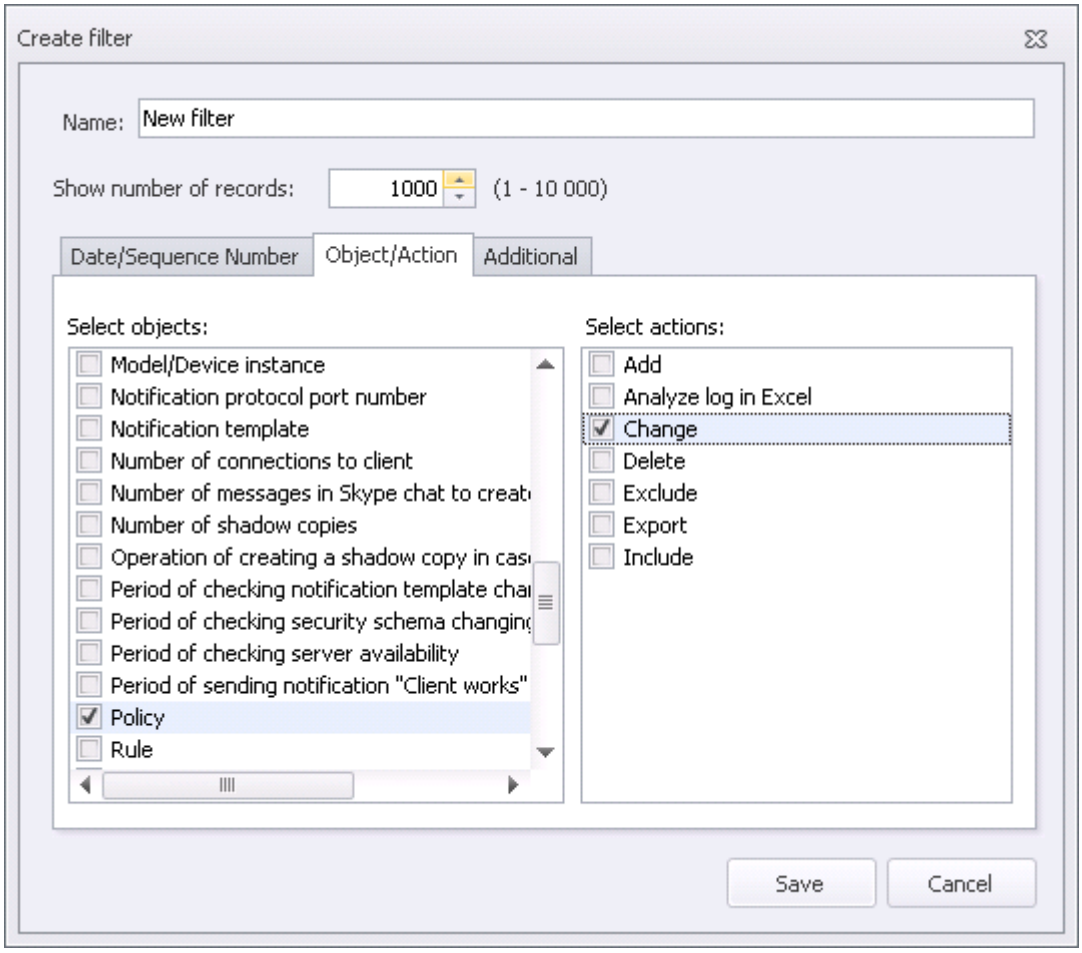
To filter by number:

1. Flag **Filter by sequence number** check box.
2. Specify range of numbers in **From** and To fields respectively.
   Database record numbers start from 1.

Object/Action Tab

Use **Object/Action** tab to specify the following filtering criteria:

- target object;
- action performed with an object.



To specify filtering criteria:

1. Set object filtering criteria: in the left list, flag the objects you want to filter out.
2. Set action filtering criteria: in the right list, flag the actions you want to filter out.

Additional Tab

You can use **Additional** tab to configure additional filter settings. These settings include:

- **Object Selector**. Filter records using Selector values.
- **Field Name**. Filter records using one of the rule's (DM) attributes (for example, Operation, Action , etc.)
- **Old Value**. Filter records using the rule's (DM) previous attribute value.
- **New Value**. Filter records using the rule's (DM) modified attribute value.
- **User**. Display user's actions list.
- **Windows Account**. Display list of actions performed on behalf of selected Windows account.
- **Computer**. Display selected computer activity records.

To configure additional filtering parameters, enter their values in the appropriate filed.

Note:

Additional filtering values are not case-insensitive.

Deleting Records from Log

Warning!

Log records can be deleted only by Superuser.

To delete log records:

1. In Main Menu click **Edit > Delete log entries**.
2. Enter transaction number in **Delete** dialog.

   Warning!

   Note that audit log records relating to selected transaction or previous transactions will be deleted.

3. Click **OK**.

Exporting Log Records

You can export log records to XLS, HTM, or TXT files. Later you will be able to view exported records with applications associated with appropriate file formats.

To export audit log records:

1. Go to **Log**.
2. Take one of the following steps:
   - To export records selected by the filter, click the filter on Navigation pane.
   - To export the whole log, click **Show All Records** at the top of Navigation pane.
3. Take one of the following steps:
   - click **Export Log** button in the top of **Records** area;
   - in Main Menu click **Edit > Export Log**;
   - right-click in the **Records** area and choose **Export Log** from the context menu.
4. In the next dialog, specify the target file name, type, and directory.
5. Click **Save**.

Now, the audit log records are exported to the selected file.

Analyzing Log Records in Microsoft Excel

To enable audit log analysis in Microsoft Excel, you must install the application on the computer that will be used to run the operation.

To view Audit Log records in Excel:

1. Go to **Log**.
2. Take one of the following steps:
    - To view records selected by the filter, click the filter on Navigation pane.
    - To view the whole log, click **Show All Records** at the top of Navigation pane.
3. In the Main Menu click **Edit > Analyze Log in Excel**.

This opens selected log in Microsoft Excel.

5.3 General System Settings

The System has a set of global settings that should be general for all active policies and rules in Device Monitor system. You can configure these settings from **Tools > Settings** menu. For more information, see the following articles:

- Common Settings for Agents
- Settings of Corporate Network
- Network Traffic Control
- Device Monitor Server Settings. Connecting to Traffic Monitor Server
- Connecting to LDAP Server
- Employee Notifications about Policy Violations
- Exclusion of Application from Interception
- Application control
- Event Storage
- InfoWatch Device Monitor Server Manager

Warning!

Modified settings will apply on controlled computers after Agents at every computer receive notification from the Server (when checking server availability or when checking security scheme changing or when checking notification templates changing) and then Agents will be updated.

5.3.1 Common Settings for Agents

In order to provide efficient operation of Device Monitor Agent applications, you need to specify a set of common settings.

To configure common settings for Device Monitor agents operation:

1. In the Main Menu select **Tools > Settings**.
2. At the left panel select **Common** node.
3. Change needed settings:

Parameter	Description
Connection	

Period of sending notification "Agent works" to the server	Interval (sec) with which the Agent sends data to Server
Period of checking server availability	Interval (sec) with which the Agent checks Server availability.
Period of checking security schema changing for active agent only	If a Agent is in active mode (i.e. computer could not open UDP-port for receiving Server notifications) then the Agent surveys Server itself to receive data on changing security schema. This parameter sets a survey period (sec).
Period of checking notification template changing for active agent only	If a Agent is in active mode (i.e. computer could not open UDP-port for receiving Server notifications) then the Agent surveys Server itself to receive data on changing notification templates (see "Employee Notifications about Policy (DM) Violations"). This parameter sets a survey period (sec).
Agent's disk space control	
Free agents' disk space	Minimal size of free disk space (%) of managed computer: when it is reached, shadow copies would not be created. I.e. if when a shadow copy is created, free disk space at the agent computer is less then parameter value, then neither shadow copy nor its part won't be created. See details in "Creating Shadow Copies and Blocking Operations Due to Free Space Shortage"
If there is not enough space for events	The managed computer dedicates space for storing 30000 events at the hard drive where Device Monitor Agent is installed. If Device Monitor Agent did not have connections with Device Monitor Server so that there is stored more than 30000 events controlled by rules (DM) defined for employee/ computer, then any actions controlled by security schema could be denied. **To deny**, select Operation will be blocked. To allow all actions performed without a control, select **Operation will be permitted**.
Speed of sending data from agent	
Limit the speed of sending data	If the channel is narrow you can prevent its excessively uploading by adjusting the speed of shadow copies sending to the Server. To do this check the setting and specify the upper-speed limit (Kbps) in **Maximum speed of sending** data field.

Events	
Log events of device and cloud storage interceptors	Level of detailing when saving information about working with external devices received by Device Monitor and Cloud Storage Monitor interceptors: see details in "Configuring Device Monitor Rule (DM)", "Configuring Cloud Storage Monitor Rule (DM)", "Viewing Events". The following options are available: • **None** - do not save events • **In case access denied** - events are created only if security policy (DM) violation is attempted - i.e. when device usage was denied, including blocking attempts of access level exceeding. The using of external devices which are not forbidden by policies, is not logged • **All** - all actions are logged (connection/usage of any devices, even from white lists)
Log connections outside of corporate network	Level of detailing when saving information about data transfer by network connections received by Network Monitor interceptor: see details in "Configuring Network Monitor Rule (DM)". The following options are available: • **None** - do not save events • **In case access denied** - events are created only if security policy (DM) violation is attempted - i.e. when connection attempt was denied.
Agent activity on computer	
Show employee notifications	Indicates if employee attempting to perform action forbidden by security policy (DM), would receive a warning message. See details in "Employee Notifications about Policy (DM) Violations"
Hide Agent presence	Indicates if Windows system tray of managed computer hides Agent presence on the computer. If this option is not selected, the Windows system tray of the computer where the Agent is installed will display  icon. Clicking this icon displays information on DM Agent operation and the list of currently controlled devices. **Warning**! If there is an antivirus protection enabled on the managed computer then the antivirus program can reveal the operation of Device Monitor: for example, in the list of processes running on the managed computer or in the list of programs that initiate a control.
Code generating key	
Update	Click Update to make the System generate a new key used to make codes of removing network connections or devices access prohibition. See details on codes in "Temporary Employee Access to Network" and "Temporary Employee Access to Devices", Request code and Confirmation code settings. The frequent key refreshment is not recommended.

4. To apply changes click **Apply**.

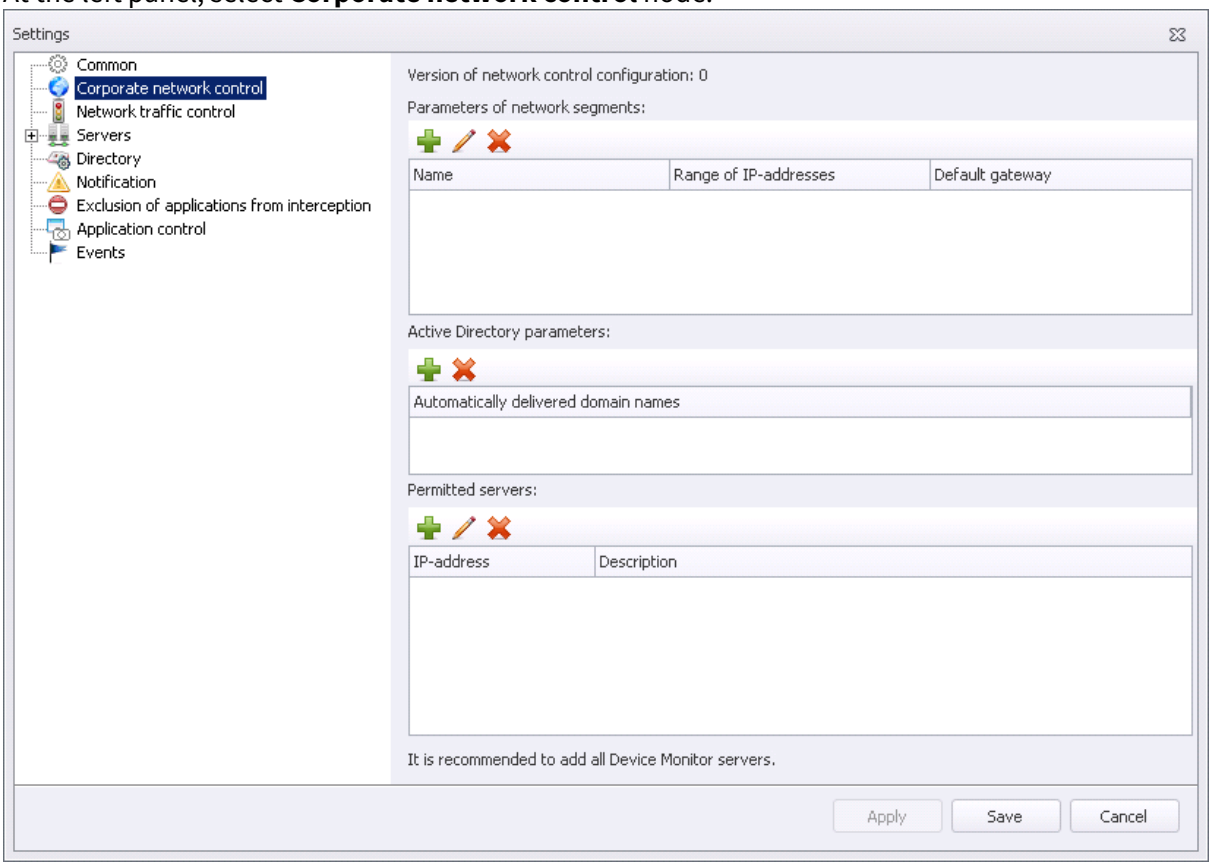
5.3.2 Settings of Corporate Network

In order to provide control of data transfer by network connections with **Network Monitor** (information on configuring the rule (DM) see in "Configuring Network Monitor Rule (DM)") you should specify, which network segments are considered as a corporate network and which external addresses are permitted.

> **Note:**
>
> Permitting the external addresses may be necessary to provide work with external resources when the Agent is outside corporate network: for example with VPN server or corporate network.

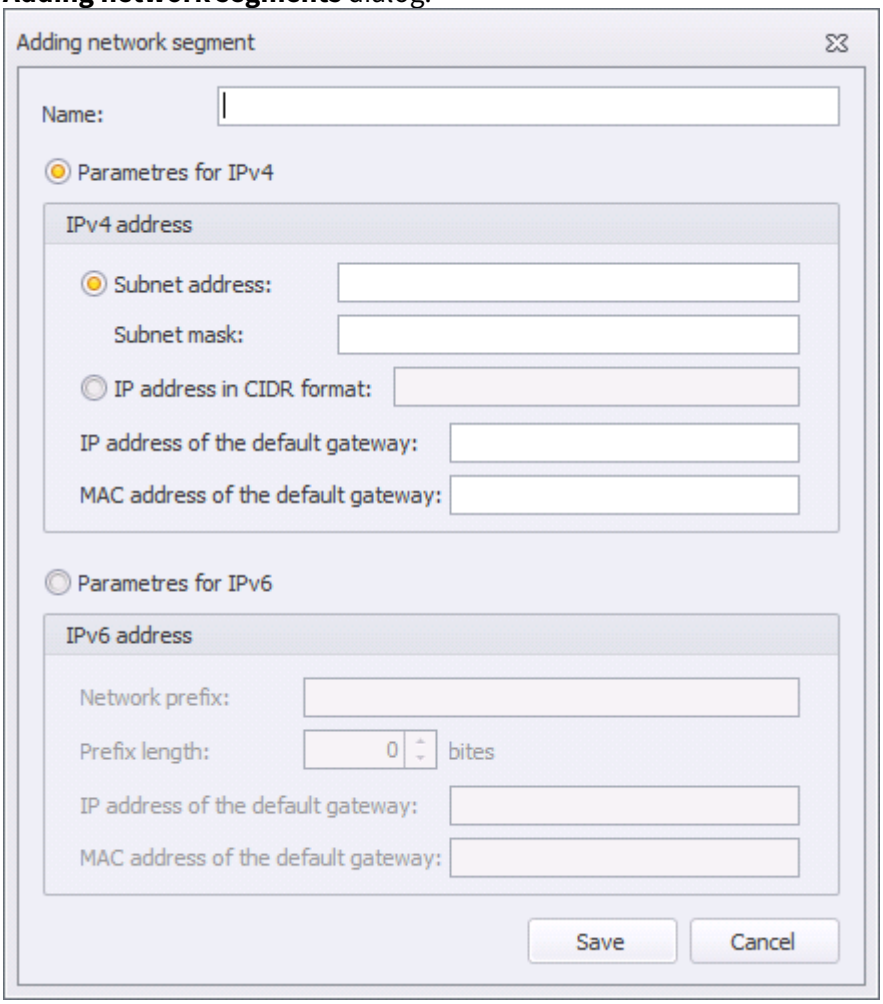
To configure corporate network settings:

1. In the Main Menu, select **Tools > Settings**.
2. At the left panel, select **Corporate network control** node.



3. To configure network segments:

a. In **Parameters of network segments** area click (or press Ctrl+Shift+S). This opens **Adding network segments** dialog.



b. Specify segment's name (description).
c. Select protocol in use: **IPv4** or **IPv6**.
   If you selected **Parameters for IPv4**, then select address format (CIDR or address and mask) and specify required parameters. Also, specify IP address and MAC address of the default gateway.
   If you selected **Parameters for IPv6**, then select network prefix and its length. Also, specify IP address and MAC address of the default gateway.
d. Click **Save**.
e. Repeat to add other segments.
   To change segment parameters, select it from the list in **Parameters of network segments** area and click (or press Ctrl+E).
   To delete a segment from the list, select it, click (or press **Delete**), then click **Yes** in the confirmation dialog.

> **Warning!**
>
> When configuring the corporate network connections you should keep in mind that domain setting takes precedence over the network segments settings.

4. To define Active Directory parameters, click . Then the System automatically defines a name and GUID of a domain where Device Monitor server is deployed.
5. To set a list of servers to permit connection with:
   a. In **Permitted servers** area click .
   b. In **Add permitted server** dialog specify DNS name or IP address of a server and server description.
   c. Click **Save**.
   d. Repeat for other permitted addresses.
   To change server parameters, select it from the list and click  (or press Ctrl+E).
   To delete a server from the list of permitted ones, select it, click  (or press **Delete**), then click **Yes** in the confirmation dialog.
6. To apply changes, click **Apply**.

5.3.3 Network Traffic Control

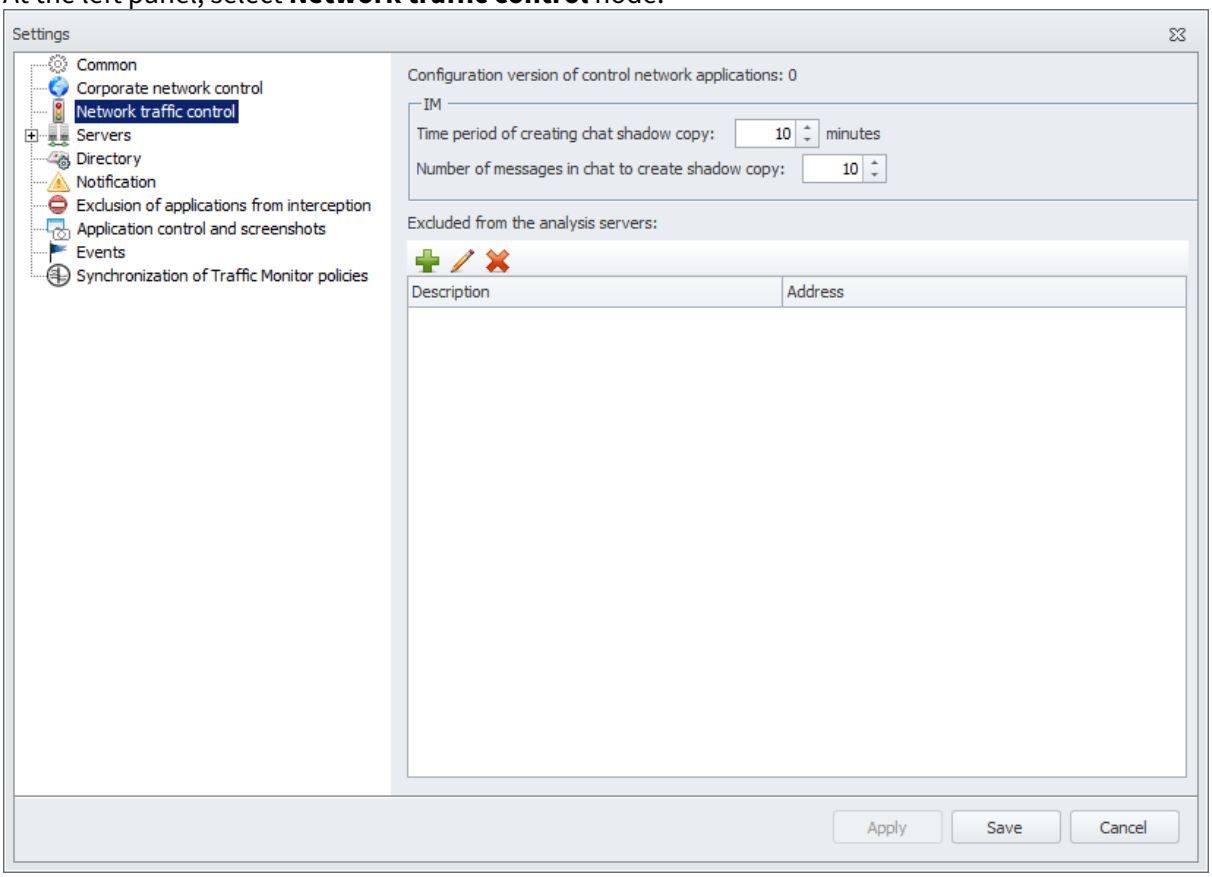
In order to provide control of network traffic, Device Monitor Agent acts as a transparent proxy server, to which all the connections are redirected irrespective of the protocol. Then Device Monitor Agent parses the protocol and defines if this protocol is a subject of interception. Controlled protocols are FTP, FTPS, POP3, SMTP, IMAP, HTTP, HTTPS, XMPP, and MMP. If a data stream is protected with TLS\SSL protocol, then the proxy server decrypts the traffic and defines if this stream should be controlled.

When configuring the traffic control, you can specify additional parameters for instant messanger (for more information about configuring rules (DM) for this control type, see "Configuring IM Client Monitor Rule (DM)"), mail systems (see "Configuring Mail Monitor Rule (DM)"), and FTP/FTPS taffic (see "Configuring FTP Monitor Rule (DM)"). Besides, you can define servers excluded from interception: traffic sent to these servers should not be controlled.

To configure network traffic control settings:

1. In the main menu, select **Tools > Settings**.

2. At the left panel, select **Network traffic control** node.



3. Specify control parameters for messengers: set a period of creating a chat shadow copy to send to Traffic Monitor. You can set a time period in minutes (**Time period of creating chat shadow copy** option) or a number of messages (**Number of messages in chat to create shadow copy** option) as criteria: the first actuated condition will be applied. If a file is be sent in a chat, the shadow copy is formed instantly, without accessing specified criteria.
For details, see "Configuring IM Client Monitor Rule (DM)".
4. You can specify a list of server IP addresses which protocols won't be controlled - i.e. traffic sent to those servers won't be redirected to the internal proxy server.

> **Note:**
>
> Permitting external addresses can be needed for providing work with external resources and updating installed programs, for example:
> - Firefox automatic update needs *.mozilla.com and *.mozilla.net in the list of permitted servers
> - Filezilla requires update.filezilla-project.org
> - Dropbox needs *.dropbox.com
> - Yandex Disk requires:
>   - oauth.yandex.ru
>   - webdav.yandex.ru
>   - clck.yandex.ru

- push.xmpp.yandex.ru
- etc.

Note:

For agents installed on Astra Linux, only traffic sent to the server through SSL protocol is excluded from analysis.

5. To set a list of servers excluded from analysis:
   a. In **Excluded from the analysis servers** area, click .
   b. In **Add server to the list of excluded from the analysis** dialog, specify DNS name or IP address of a server and server description. For more information on addresses that can be added, see "Processing Addresses Added to Exclusions".
   c. Click **Save**.
   d. Repeat for other permitted addresses.
   e. To change the server parameters, select it in the list and click .
   f. To delete a server from the list of excluded ones, select it, click , then click **Yes** in the confirmation dialog.
6. When all changes are made, click **Apply**.

Processing Addresses Added to Exclusions

When you exclude a server from analysis (see "Network Traffic Control"), you need to specify the server IP address or DNS name. To exclude from analysis a specific port or address range or, conversely, explicitly enable interception for a specific port, specify the value in the following format:

- to exclude a specific port from interception, use the following format: `address:port` (e.g., `10.128.0.2:80`)
- to exclude from interception a server address, use the following format: *hostname
- to exclude from interception all traffic sent to the address `10.128.0.2` except for the traffic sent on port `8080`, add two exceptions: `10.128.0.2` and `!~10.128.0.2:8080`
- to exclude from interception a range of addresses, use `#` character: `#192.168.0.1-192.168.0.255`
- to exclude from interception a range of addresses except one separate address, use the following format: `#192.168.0.1-192.168.0.255!192.168.0.5`
- to explicitly enable interception for a specific port, use the following format: `!~address:port`

Note:

Do not use the following template:`FQDN:port`. Instead of this, you require adding all possible IP addresses (`IP:port`) to exclusion list. For example: `10.128.0.2:8080`

Example: Notation `*server.com` will add to exclusion list `wiki.server.com, info.server.com`.

Note:

'*' character can be used only with hostname. Using '*' with IP-address is not allowed.

Each line is processed according to the following algorithm:

Step 1. The System looks for a position of '#' character. If '#' character is found, then the following actions are performed (otherwise, go to step 2):

1. The System looks for a position of '!' character, and then checks the relative position of '#' and '!' characters.
2. In the place where '!' character is located, the string is divided into two parts. The part to the left of '!' contains addresses to be excluded from interception, the part to the right of '!' contains addresses for which interception should be explicitly enabled (explicitly enabled interception has a higher priority than any added exclusions).
3. In each part of the string, the System looks for ',' character. This character delimiters separate addresses or address ranges (substrings).
4. In each address or address range (substring) defined at step 3, the System looks for '-' character.
5. If '-' character is not found, then the substring is considered a separate IP address (not FQDN).
6. If '-' character is found, then the substring is considered a range of addresses IP1-IP2.
7. When all substrings are processed, obtained addresses or address ranges are added either as addresses to be excluded from interception or as addresses for which interception should be explicitly enabled.

Example: `#192.168.1.1-192.168.255.255,10.10.0.0-10.10.255.255!192.168.1.5-192.168.1.0,10.10.10.10`. This string contains two address ranges to be excluded from interception, and a range of addresses with an address for which interception should be enabled.

Note:

The System does not check if specified address regions intersect or if addresses for which interception is explicitly enabled are in the list of addresses excluded from interception.

Step 2. The System looks for a position of '~' character. If '~' character is found, then the following actions are performed (otherwise, go to step 3):

1. The System looks for positions of '~', '!', ':' characters and checks the relative position of these characters. If their relative position is incorrect, the further check is not performed.
2. If '!' character is not found, then the string in `address:port` format will be excluded from interception (e.g., `~192.168.1.1:5122`). Requests sent to this address and port will not be redirected to the proxy server.
3. If '!' character is found, then for the string in `address:port` format, interception will be explicitly enabled (e.g., `!~192.168.1.1:5122`). Requests sent to this address and port will be redirected to the proxy server even if this server and port have been excluded from interception.

Step 3. The System looks for a position '*' character. If '*' character is found, the address is considered a template one and is excluded from SSL interception. Requests sent to this address will not be redirected to the proxy server. If '*' character is not found, go to step 4.

Step 4. If neither of the '#', '~', '*' characters is found, then the address excluded from interception is considered a common address or FQDN. By means of OS functions, such an address is converted to IP address and added to the list of addresses excluded from interception (e.g., `192.168.1.1`, example`.infowatch.ru`). Requests sent to this address will not be redirected to the proxy server.

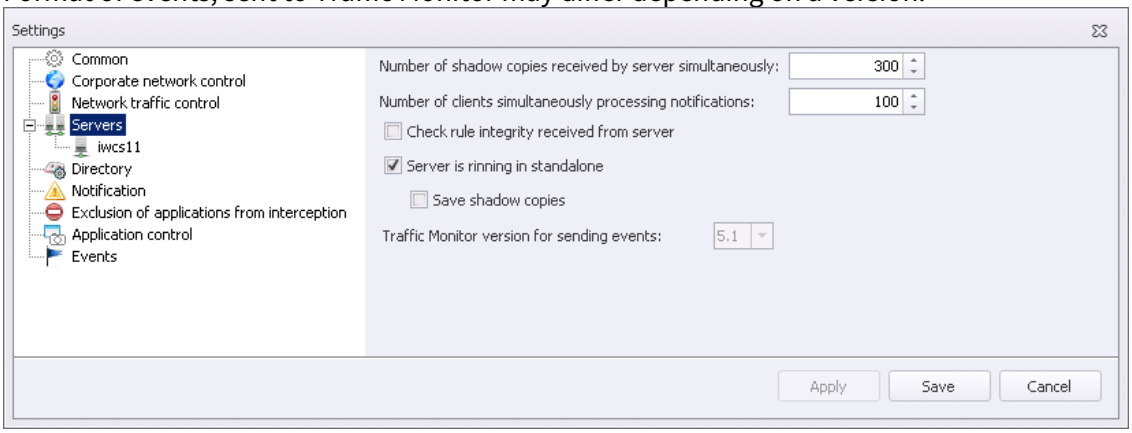
5.3.4 Device Monitor Server Settings. Connecting to Traffic Monitor Server

You need to set up connection parameters to be able to send events to Traffic Monitor.

> **Note:**
>
> Changing server role (General or Secondary) and attribute Notification protocol port number and Main protocol port number is being executed with InfoWatch Device Monitor Server Manager (see "InfoWatch Device Monitor Server Manager").

To view and set up Traffic Monitor connection parameters:

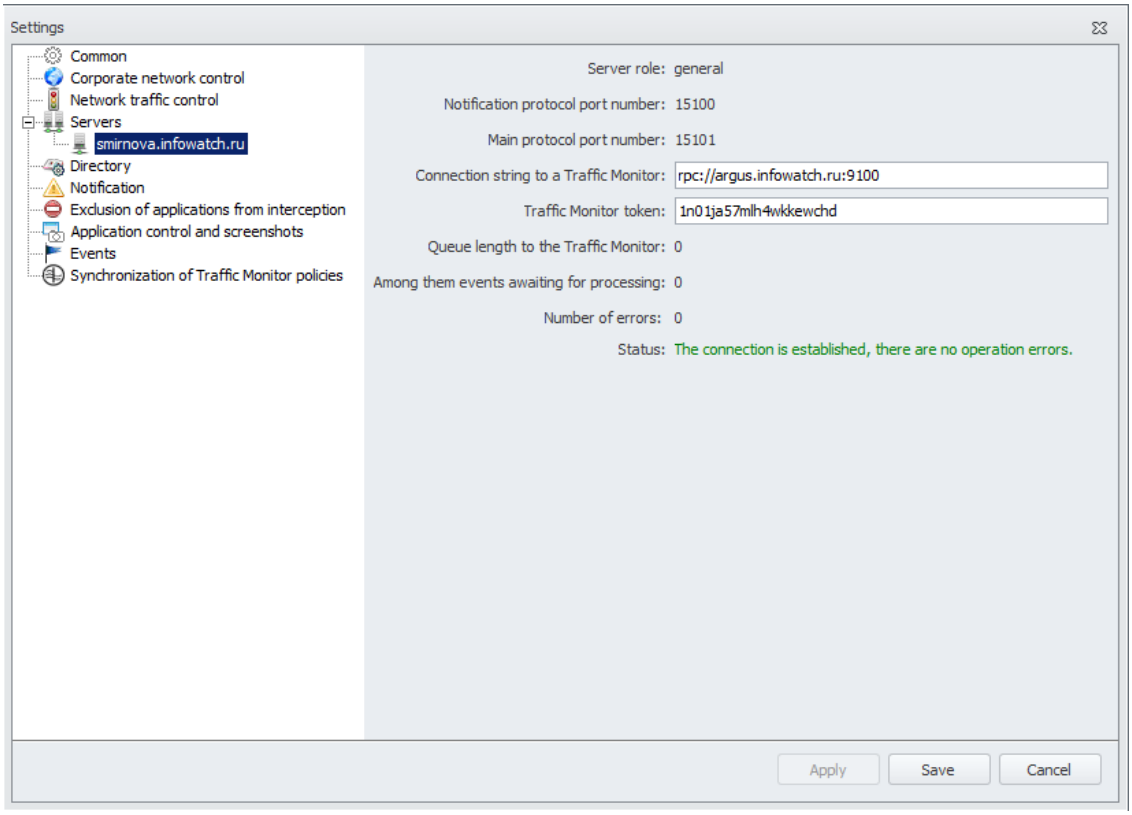
1. In main menu choose **Tools -> Settings**.
2. In **Servers** node set up the following parameters:
   - **Number of shadow copies received by server simultaneously**: - determine the number of copies which can be sent to Traffic Monitor Server simultaneously.
   - **Number of clients simultaneously processing notifications**: determines the number of agents, which can receive notifications (security schema) from server at a time
   - **Check rule integrity received from server** - compares rules (DM) on server and agent to avoid management on agent side.
   - **Server is running in standalone** - server is running without integration with Traffic Monitor.
     - **Save shadow copies** - shadow copies are being saved locally in `ShadowCopyTempDir`.
   - **Traffic Monitor version for sending events** - current version of used Traffic Monitor. Format of events, sent to Traffic Monitor may differ depending on a version.



3. When selecting the server name, you will receive information on the following connection parameters:
   - **Server role** – server role (primary or secondary), assigned to this server during installation: see "*InfoWatch Traffic Monitor. Installation Guide*", article "InfoWatch Device Monitor Server End Installation Procedure".
   - **Notification protocol port number**.
   - **Main protocol port number**.
   - **Connection string to a Traffic Monitor** – InfoWatch Traffic Monitor server address that will receive events. Address must be entered in the following format:

`xml://host:port` - for Traffic Monitor v. 6.0 or higher.
`rcp://host:port` - for Traffic Monitor versions under 6.0.
host parameter should contain domain name or IP address of InfoWatch Traffic Monitor server. The server address is the standard URL address (Uniform Resource Identifier) with its formal syntax described in RFC 3986 http://tools.ietf.org/html/rfc3986.
port parameter contains InfoWatch Traffic Monitor server port that delivers events. InfoWatch Traffic Monitor default server port is 9100.

- **Traffic Monitor token** – the token to connect to API. Required for Traffic Monitor v. 6.0 or higher. You can get the actual token from your Traffic Monitor administrator.
- **Queue length to the Traffic Monitor** - number of events pending submission to InfoWatch Traffic Monitor.
- **Among them events awaiting for processing** – number of events pending processing before sending to InfoWatch Traffic Monitor.
- **Errors number** – number of events in the errors queue.
- **Status** – information on Traffic Monitor connection state.



4. When all changes are made, click **Apply**.
5. Click **Save**.

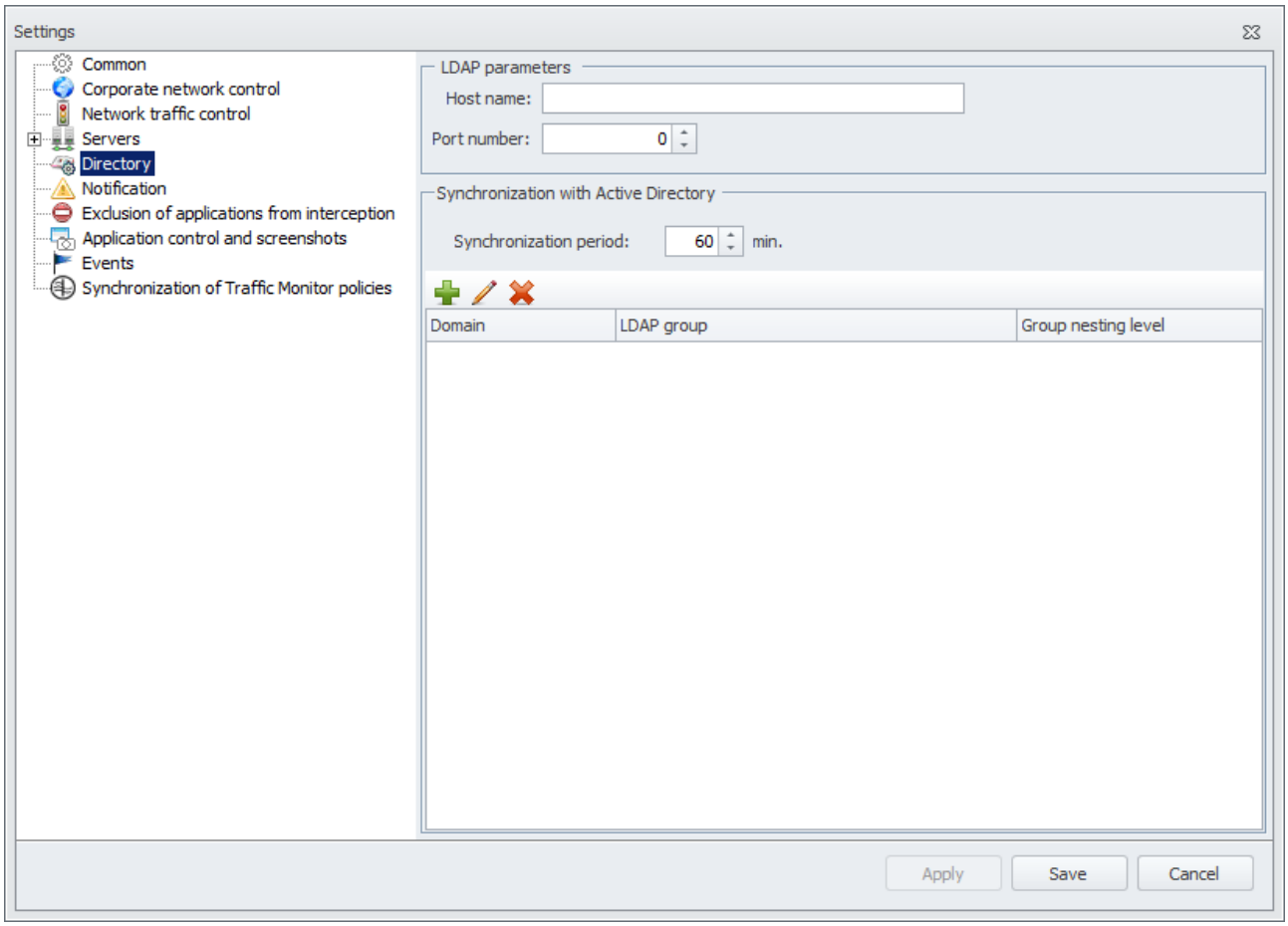
5.3.5 Connecting to LDAP Server and synchronization with Active Directory and Astra Linux Directory

Configuring parameters of connection with LDAP server

In order to receive information on computers and employees from directory services, configure parameters of connection with LDAP server.

To view and configure LDAP connection settings:

1. In the Main Menu, select **Tools > Settings**.
2. Select **Integration with Active Directory** node.
3. In the **Host name** field, specify a domain name or IP-address of LDAP server.
4. If needed, specify a port to redirect requests when the default port (**389**) is unavailable.
5. Click **Save**.



Note:

Connection to LDAP server is performed in an anonymous mode.

Adding synchronization settings

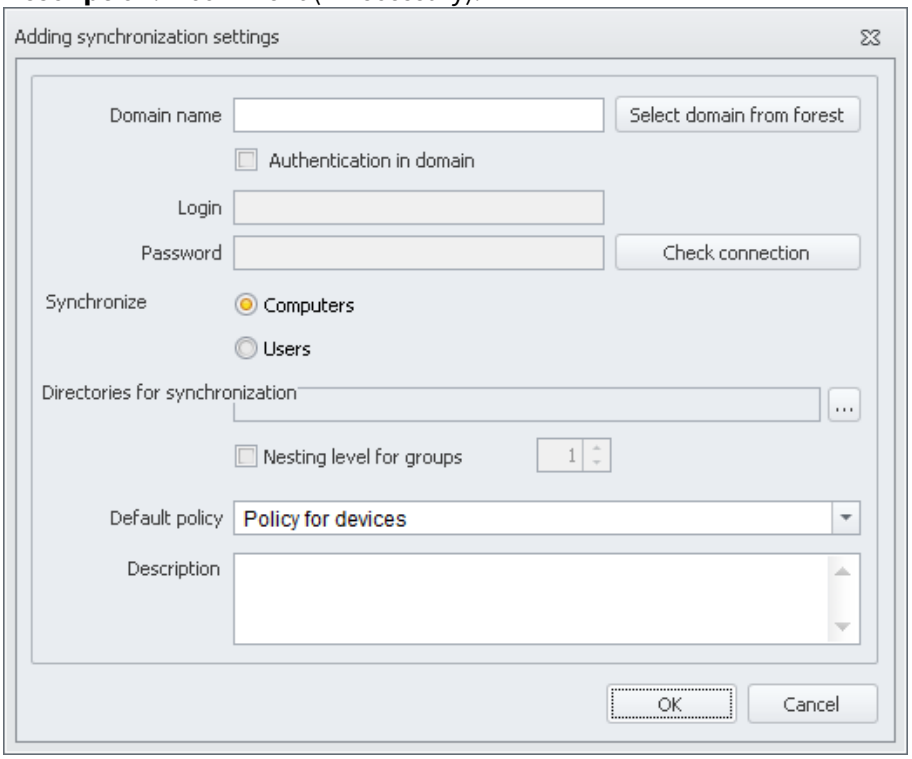
To add a synchronization setting with Active Directory or Astra Linux Directory:

1. In **Synchronization with Active Directory** area, click .
2. In a dialog window, specify synchronization settings:

- **Domain name.** Name of the domain with which you want to synchronize (you can type the name manually or choose it from the domain forest).

> **Note:**
>
> The domain name is an IP address or a DNS name. A DNS name must be registered in the network.

- **Login.** To authenticate to the domain (if **Authentication in domain** option is selected).
- **Password.** To authenticate to the domain (if **Authentication in domain** option is selected).
- **Synchronize**. Synchronization objects - **Computers** or **Users**.
- **Directories for synchronization**. Directories in Active Directory that must be synchronized. For synchronization:
  1. Click ... .
  2. In the tree, specify directories for synchronization.
  3. Click **Select**.
- **Nesting level for groups** (if necessary). The maximum nesting level is 100.
- **Default policy**. A policy that will apply to synchronized groups after the first synchronization.
- **Description**. A comment (if necessary).



- If the **Authentication in domain** option is selected, click **Check connection** to check connection with the domain.
- If the connection is successful, click **OK**.
- To apply changes, click **Apply** in the **Settings** window.

> **Note:**
>
> **Domain name** and **Directories for synchronization** fields are required.

The table in the **Settings** window contains data on the synchronization settings and results:

Parameter	Description
Domain	IP address of DNS name of the server
Synchronize	Object of synchronization: computers or users
Directories	Folders and groups for synchronization
Synchronization status	Possible values: • **Is running** (the synchronization process is in progress) • **Successfully** (the synchronization process is complete), • **Failed** (the synchronization process has failed).
Synchronization time	Date and time of the last synchronization

Note:

For users and computers, the synchronization is configured separately. You can add several synchronization settings for the same domain.

Launching/editing/disabling synchronization

To launch synchronization with Active Directory or Astra Linux Directory:

1. In the **Synchronization with Active Directory** area, select the required row in the table.
2. Click (to launch synchronization manually).
3. To update the synchronization status, select **View** > **Refresh** or press **F5**.

Note:

You can launch the synchronization automatically in specified periods. For this, specify the synchronization period and click **Apply**.

To edit synchronization settings:

1. In the **Synchronization with Active Directory** area, choose the desired row.
2. Click .
3. Edit synchronization settings.
4. Click **OK**.

To disable synchronization with Active Directory or Astra Linux Directory:

1. In the **Synchronization with Active Directory** area, choose the desired row.
2. Click .
3. In the confirmation window, click **Yes**.

Important!

When deleting a synchronization setting, all groups of computers or employees associated with this setting will also be deleted.

5.3.6 Employee Notifications about Policy (DM) Violations

When an employee working at managed computer tries to perform an action forbidden by security policy (DM), the notification is displayed. Notifications are displayed in following cases:

- **Access to device denied** – Device Monitor rule which denies reading and writing to the device (see "Configuring Device Monitor Rule (DM)") was actuated.
- **Writing to device denied** – Device Monitor rule which denies writing to the device (see "Configuring Device Monitor Rule (DM)") was actuated.
- **Writing to open area denied** – Device Monitor rule which denies writing to unencrypted floppy drives and detachable devices (see "Configuring Device Monitor Rule (DM)") was actuated.
- **Copying/printing file denied if there is not enough space for incidents** – if Device Monitor Agent did not have connections with Device Monitor Server so that there is out of dedicated space for storing information on events controlled by rules (DM) (30000 events) and common settings have Operation is blocked option selected (see in "Common Settings for Agents") then any operations controlled by current security policy (DM) are forbidden.
- **Data transfer via network protocols denied** – Ftp Monitor or IM Agent Monitor rule (DM) which denies data transfer through FTP/FTPS/SMTP/POP3/MAPI/XMPP/MMP/YMSG/Skype (see "Configuring FTP Monitor Rule (DM)" and "Configuring IM Client Monitor Rule (DM)") was actuated.
- **Data transfer via network protocols denied if there is not enough space for incidents** – if Device Monitor Agent did not have connections with Device Monitor Server so that there is out of dedicated space for storing information on events controlled by rules (DM) (30000 events) and common settings have Operation is blocked option selected (see in "Common Settings for Agents") then any operations controlled by current security policy (DM) are forbidden.
- **Pasting from clipboard is denied if there is not enough space for incidents** – the «Forbid operation if there is no free space for incidents» option was triggered, there is no space for incidents and the operation of pasting data from clipboard to an application is performed.
- **Access to clipboard in applications is forbidden** – the rule (DM) which prohibits applications to access the clipboard at the attempt to paste/copy data in the application was triggered.
- **Printing in applications is forbidden** – the rule (DM) which prohibits printing for applications at the attempt to print from the application was triggered.
- **Copying file is forbidden when a data protection policy is triggered** – is displayed if the file copying is blocked because of applying a data protection policy (DM).
- **Passing data via network protocols is forbidden when a data protection policy is triggered** – is displayed when sending data via mail protocols, FTP or HTTP(S) is forbidden because of applying a data protection policy (DM).
- **Passing data via network protocols is forbidden if there is not enough space for events** – if Device Monitor Agent has not connected with the server for a long time and has run out of space for storing information on events (30000 events), and **Forbid operaton** option is selected in general settings (for details, see. "Common Settings for Agents"), then all operations controlled by the current security policy (DM) are forbidden.
- **Network connection forbidden** – Network Monitor rule (DM) which denies data transfer through any network connections except corporate network and specified permitted servers (see "Configuring Network Monitor Rule (DM)" and "Settings of Corporate Network") was actuated.
- **Network connection forbidden and request of temporary network access** – Network Monitor which denies data transfer through any network connections except corporate network and specified permitted servers was actuated. In this notification employee can request for temporary access to external connections (see "Configuring Network Monitor Rule (DM)", "Settings of Corporate Network" and "Temporary Employee Access").

- **Request of temporary access to the device by phone** – text displayed when user selected Request access command in InfoWatch Device Monitor Agent interface, Device list tab (see "Temporary Employee Access to Devices").
- **Request of temporary access to the device by mail** – text displayed when user selected Request access command in InfoWatch Device Monitor Agent interface, Device list tab (see "Temporary Employee Access to Devices").
- **Prohibition of access to cloud storage** – Cloud Storage Monitor rule (DM) which controls cloud storages agent usage (see "Configuring Cloud Storage Monitor Rule (DM)", Access Denied option) was actuated.
- **Prohibition of writing to cloud storage** – Cloud Storage Monitor rule (DM) which controls cloud storages agent usage (see "Configuring Cloud Storage Monitor Rule (DM)", Only download option) was actuated.
- **Prohibition of running application** – Application Monitor rule (DM) which controls user access to applications by means of white lists and black lists (see "Configuring Application Monitor Rule (DM)") was actuated.
- **Prohibition of making screenshot** – ScreenShot Control Monitor rule (DM) which controls making screenshots (see "Configuring ScreenShot Control Monitor Rule (DM)") was actuated.
- **Prohibition of pasting data** - Clipboard Monitor rule (DM) which controls data paste from clipboard (see "Configuring Clipboard Monitor Rule") was actuated.

To disable showing notifications for employees entirely or to enable it back:

1. In the Main Menu select **Tools > Settings**.
2. At the left panel select **Common** node.
3. Deselect **Show notification** to disable showing notifications for employees, or flag it to enable notifications.
4. Click **Apply**.

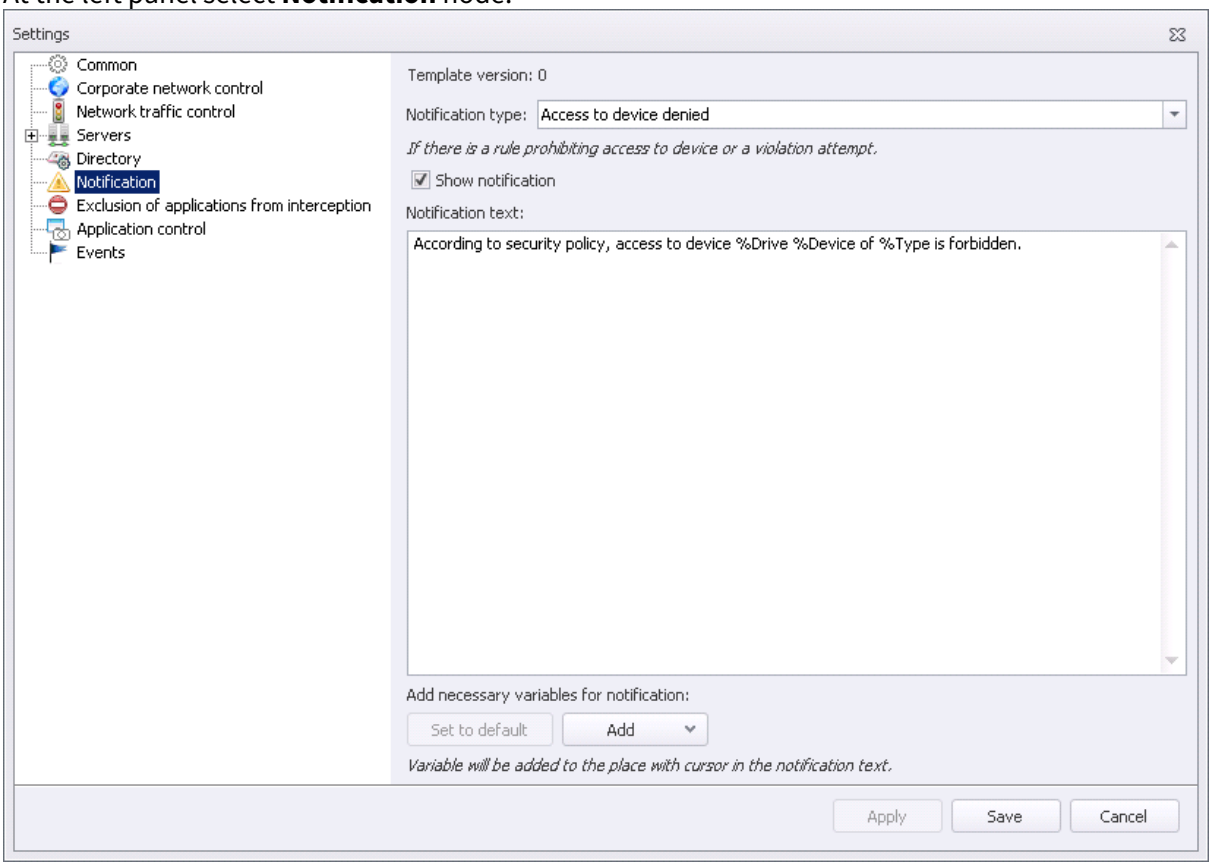
If needed, you can change notification text or disable showing of any certain notification type or enable it back.

> **Warning!**
>
> If you disabled notifications using the method described above, then notifications enabled using the method described below won't displayed yet.

To change notification text or enable\disable certain notifications:

1. In the Main Menu select **Tools > Settings**.

2. At the left panel select **Notification** node.



3. From **Notification type** list, select a notification type.
4. To enable (disable) displaying notification of chosen type, select (deselect) **Show notification**.
5. Enter notification text.
   You can use variables which would be transformed to actual data when displayed to employee: for example, type of blocked device or IP address of permitted host. To do this, set the cursor at the required place of text, then click **Add** below textbox and select required variable from the list. To cancel changes and set default settings back, click **Set to default**.
6. Click **Apply**. If needed, change settings for other notifications by repeating steps 2-5.
7. When all changes are made, click **Save**.

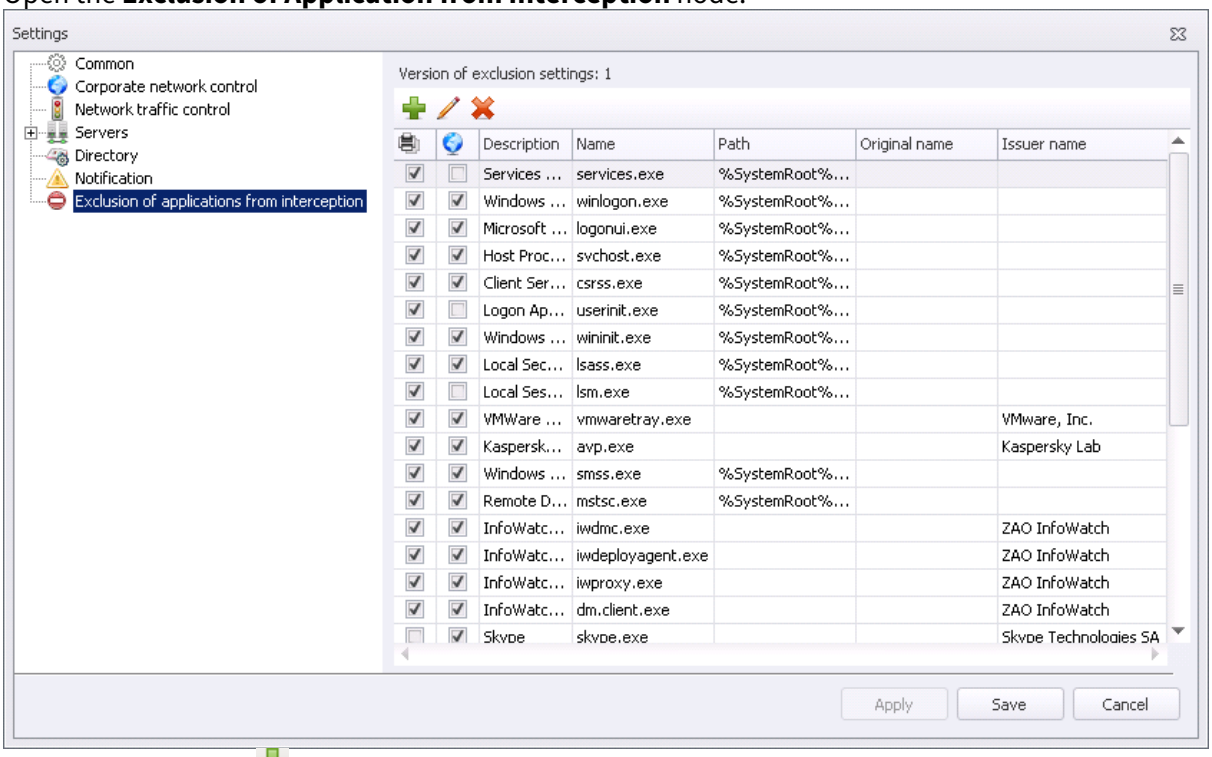
5.3.7 Exclusion of Application from Interception

You can configure parameters of applications that will be excluded from interception. These exceptional activities will become operative when Device Monitor policies are deployed over computers.

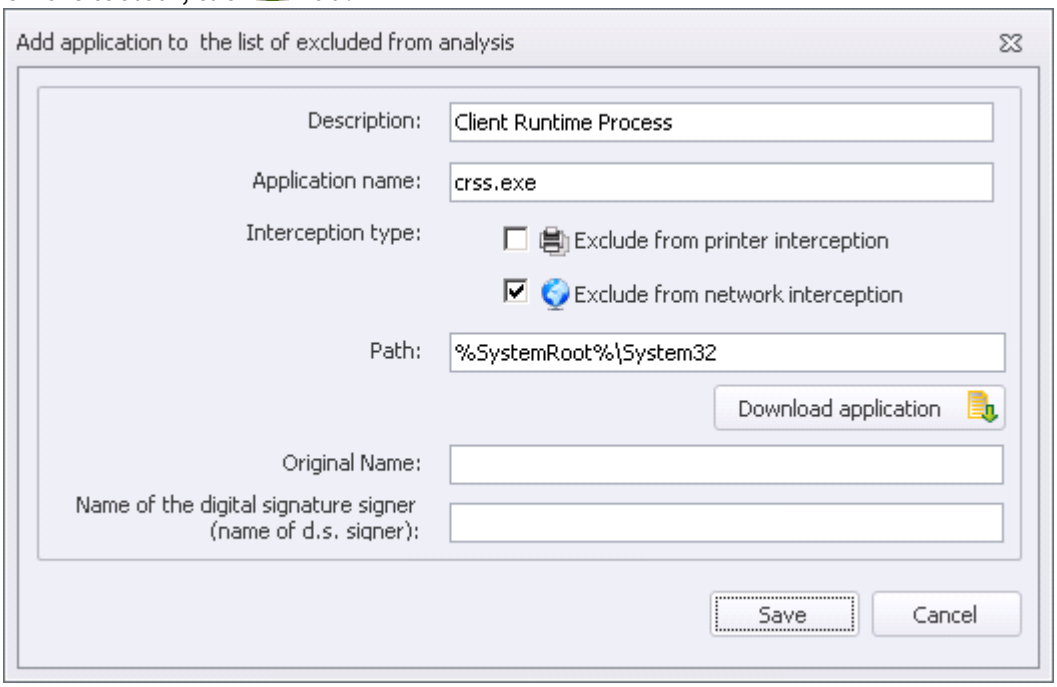
To view and configure parameters of excluding applications:

1. In the Main Menu, select **Tools** > **Settings**.

2. Open the **Exclusion of Application from Interception** node.



3. On the toolbar, click **Add**.



4. In the **Description** field, add a description of the application. This is a required field.
5. In the **Application name** field, enter the name of the application executable file. The exclusion is performed by the file name. A field is required and not case sensitive.

> **Note:**
>
> Instead of the application name, you can enter *. In this case, all applications with the specified path or specified digital signature (see i. 7) will be excluded from interception.

6. In the **Interception type** field, select:
   - **Exclude from printer interception** - neither events nor shadow copies will be created when you print data from the application;
   - **Exclude from network interception** - network activity of the application will be excluded from interception (see "Network Traffic Control").

     > **Note:**
     >
     > At least, one interception type must be selected.

7. You can specify the application file parameters manually or automatically:
   - To specify the file parameters manually:
     a. In the **Path** field, specify a folder on the Agent that contains the application executable file or an upper-level folder (you can use system variables). The path to the file must begin with the specified string. For example, if you set an exclusion as: «`*» + %Programm Files%\Citrix`, then all applications in *.exe format located in the Citrix folder or any its subfolder will be excluded from interception.
     b. In the **Original Name** field, specify the application name (in the file shortcut menu, choose **Properties**, **Details** tab, **Original filename** attribute).
     c. In the **Name of the digital signature signer (name of d.s. singer)** field, enter the value specified in the application properties (in the file shortcut menu, choose **Properties**, **Digital signatures** tab, **Name of signer** attribute). You can specify the whole name or its part. For example, if you set an exclusion as: «`*» + Kaspersky`, then all applications whose digital signature contains "Kaspersky" substring will be excluded from interception.

     > **Note:**
     >
     > The **Path** and **Original Name** fields are not case sensitive. The **Name of the digital signature signer (name of d.s. singer)** field is case sensitive.

   - To specify file parameters automatically, click **Download application** button and select the needed file. Fields **Path**, **Original Name**, **Name of the digital signature signer** will be filled automatically.

> **Note:**
>
> By filling the **Original Name** and **Name of the digital signature signer (name of d.s. singer)** fields, you can prevent, for example, the user's unapproved attempt to rename the application to make its name look like the name of application excluded from interception.

8. Click **Save**.

5.3.8 Application Control

The System allows to control applications running of managed computers by allowing or forbidding some applications. For this purpose there are two operation modes provided:

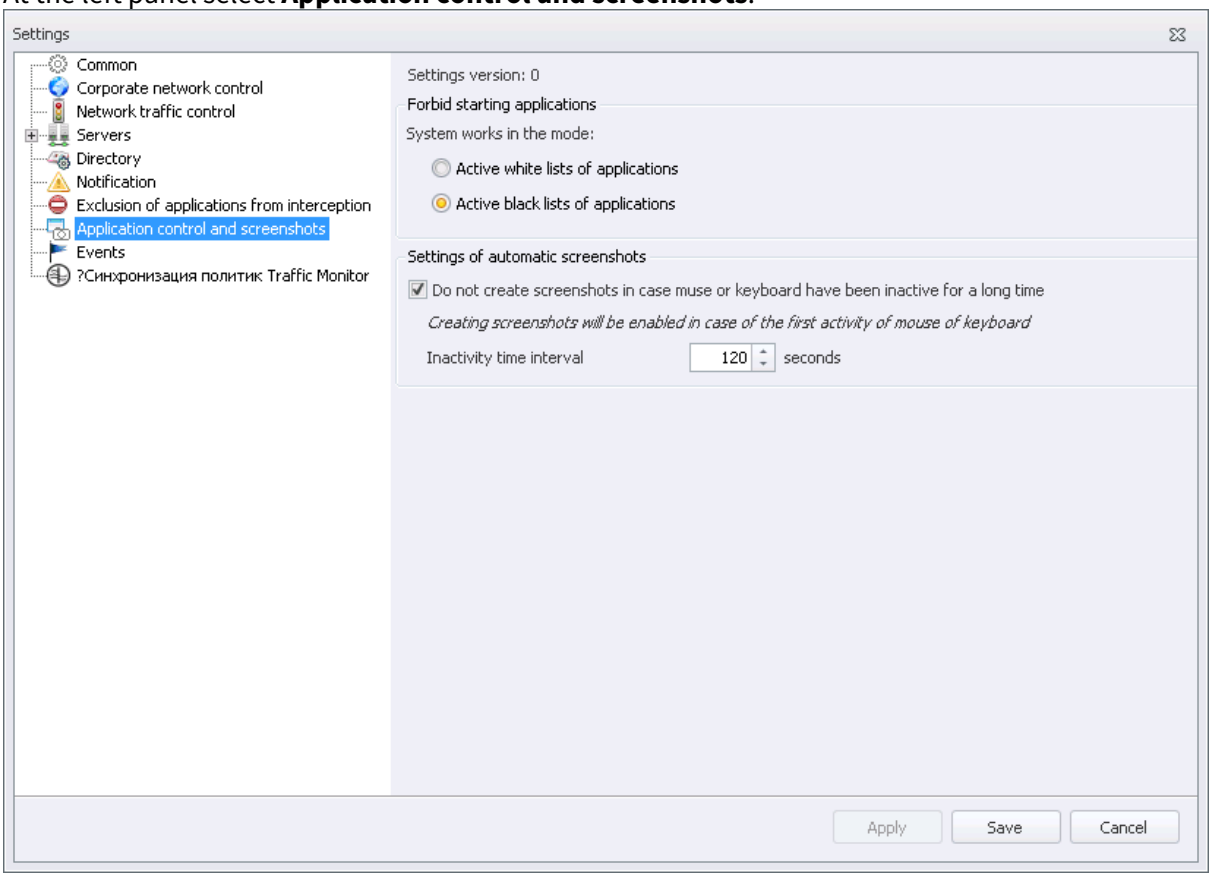
- **Active white lists of application**s - all applications from the lists selected in the Application Monitor rule from the resulting policy are allowed. Other applications are forbidden.
- **Active black lists of applications** - all applications from the lists selected in the Application Monitor rule from the resulting policy are forbidden. Other applications are allowed.

See details on forming application lists in "Application Protocol".
See details on applying lists in rules (DM) regulating application access in "Configuring Application Monitor Rule".
See details on resulting policy (DM) viewing in "Viewing Resultant Policy (DM) and Resultant White List for an employee" and "Viewing Resultant Policy (DM) and Resultant White List for Computer".

To set System mode for application control:

1. In the Main Menu select **Tools > Settings**.

2. At the left panel select **Application control and screenshots**.



3. Change mode if needed.
4. Click **Save**.

In **Application control and screenshots** section you can specify, whether it is necessary to create screenshots if there is no activity on the controlled computer.

In case **Do not create screenshots in case mouse or keyboard have been inactive for a long time** option is enabled, screenshot creation will be stopped until value in **Inactivity time interval** field is reached and renewed at first keyboard or mouse activity.

More information on how to configure automatic screenshots creation, see "Configuring ScreenShot Monitor Rule (DM)".

New version of applications and screenshots settings will ne applied to controlled computers after the next restart.

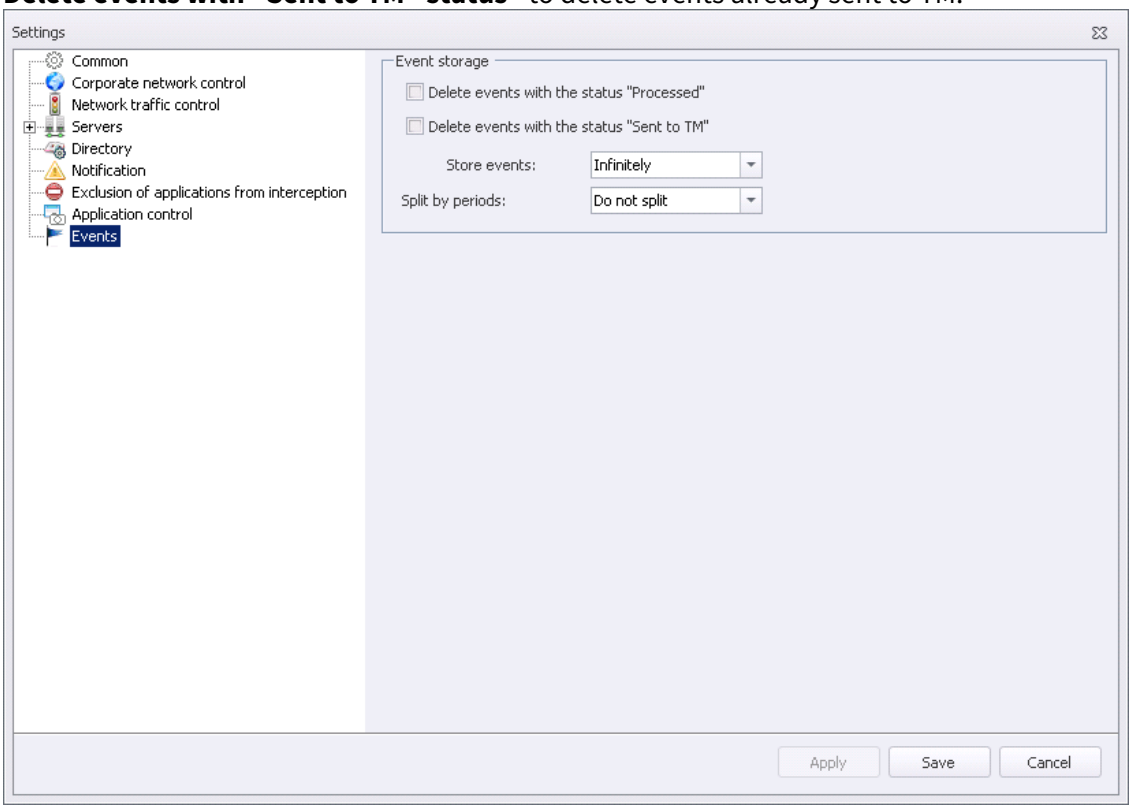
5.3.9 Event Storage

In the **Events** tab, you can set the parameters of automatic event storage and deletion.

To set up event storage:

1. In the Main Menu select **Tools > Settings**.
2. At the left panel select **Events** node.
3. Mark the following boxes:
    - **Delete events with "Processed" status** - to delete processed Device Monitor events or events of a standalone server;

- **Delete events with "Sent to TM" status** - to delete events already sent to TM.



4. From drop-down lists select:
   - **Store events** - to set up the time for event to be stored in DB and be displayed in the console (DM);
   - **Split by periods** - splitting events into blocks depending on the time it has been created to speed up connection process.

> **Note:**
>
> When **Delete events with the status "Processed"** and **Delete events with the status "Sent to TM"** options are chosen simultaneously, **Store events** becomes automatically disabled.

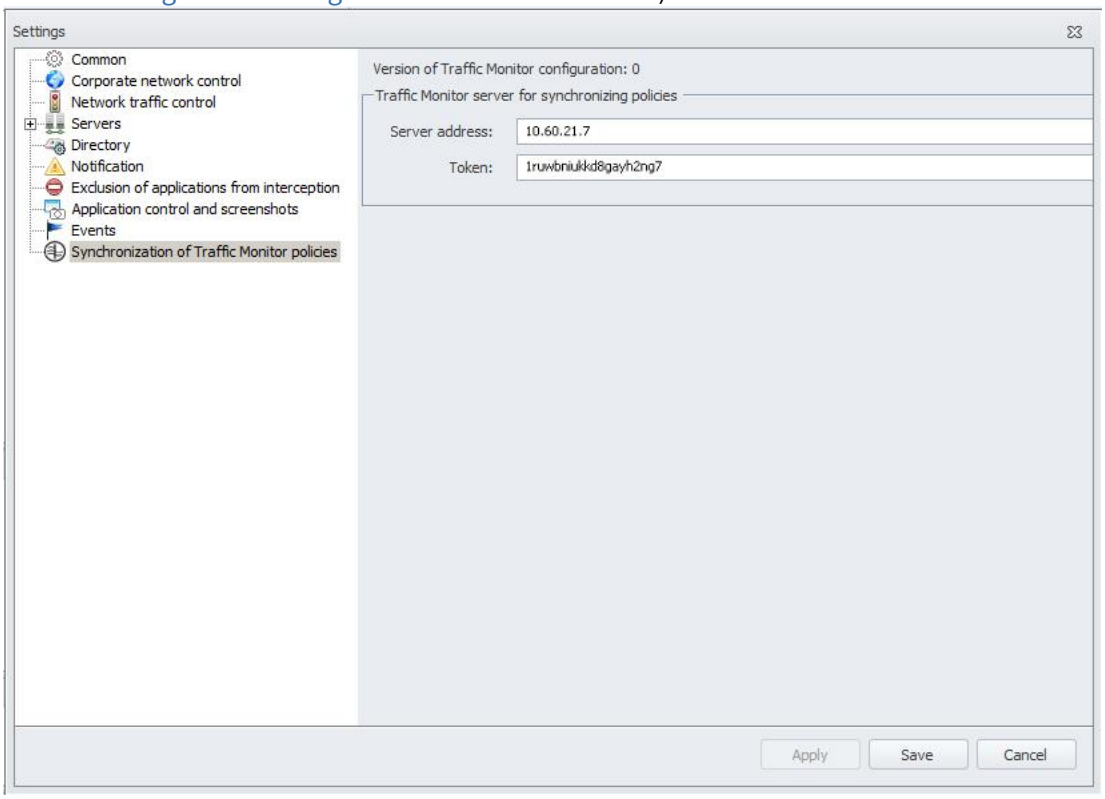
5.3.10 Synchronization of Traffic Monitor Policies

In the **Synchronization of Traffic Monitor policies** node, specify Traffic Monitor server from which Device Monitor will receive a configuration version. This configuration version is then deployed to Device Monitor agents.

> **Note:**
>
> The configuration version that is used in Traffic Monitor is displayed in TM console (see "Configuring the System"). If necessary, you can compare version numbers in Traffic Monitor and Device Monitor to make sure that Device Monitor uses an actual version.

To synchronize policies in TM:

1. From Console (DM) main menu, choose **Tools** > **Settings**.
2. Open **Synchronization of Traffic Monitor Policies** node.
3. Make sure that the server address (host) matches earlier specified settings (see "Device Monitor Server Settings. Connecting to Traffic Monitor Server").



4. Click **Apply**.
5. Click **Save**.

5.3.11 InfoWatch Device Monitor Server Manager

InfoWatch Device Monitor Server Manager is being used to define roles and change server settings.

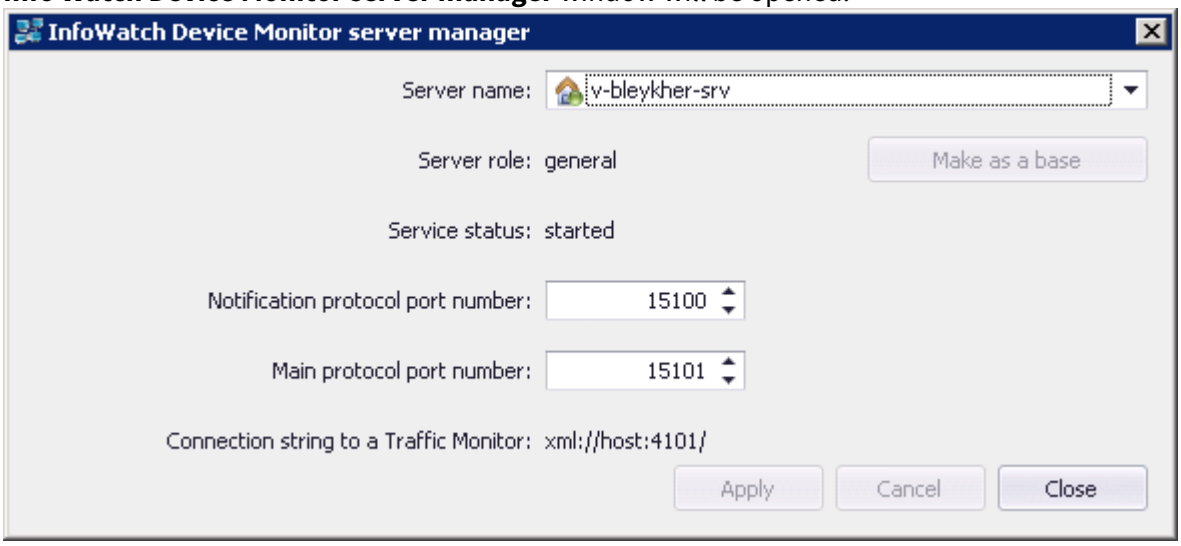
Warning!

There are following requirements to run the InfoWatch Device Monitor Server Manager utility:

- the computer where utility will run, must be included to the domain
- the user on behalf of which the utility will run, must have Administrator role at each of the servers to be changed
- there must be FQDN access granted to the servers (to check use ping `<server_name>.<domain_name>`)
- the utility must be run on behalf of the Administrator (use the option in the drop-down menu opened by clicking the right mouse button on the utility icon); or User Access Control must be disabled the computer.

To assign the main role to the server, proceed with the following steps:

1. Go to **Start -> All programs -> InfoWatch -> Device Monitor -> InfoWatch Device Monitor Server Manager**.
Info Watch Device Monitor server manager window will be opened.



2. From **Server name** drop-down menu, pick the necessary server.
3. Click **Make as a base**.

> **Note:**
>
> Specifying one of the servers as the main one automatically makes other servers secondary.

4. Click **Apply**.
5. Click **Close**.

To set up server ports, proceed with following steps:

1. Open **Info Watch Device Monitor server manager** window.
2. From **Server name** drop-down menu, pick the necessary server.
3. Edit fields **Notification protocol port number** and **Main protocol port number**.
4. Click **Apply**.
5. Click **Close**.

5.3.12 Stopping and Starting Device Monitor Agent

When there are conflicts with third-party programs as well as in critical situations, user can stop Device Monitor agent running on a workstation. One can do it locally or remotely

> **Note:**
>
> Some restrictions:
> - When you stop the DM agent, Self Protection module is not disabled.
> - The Diagnostics menu is unavailable during collecting logging results) .
> - In case stopped agent has been updated, it will be started after the update.

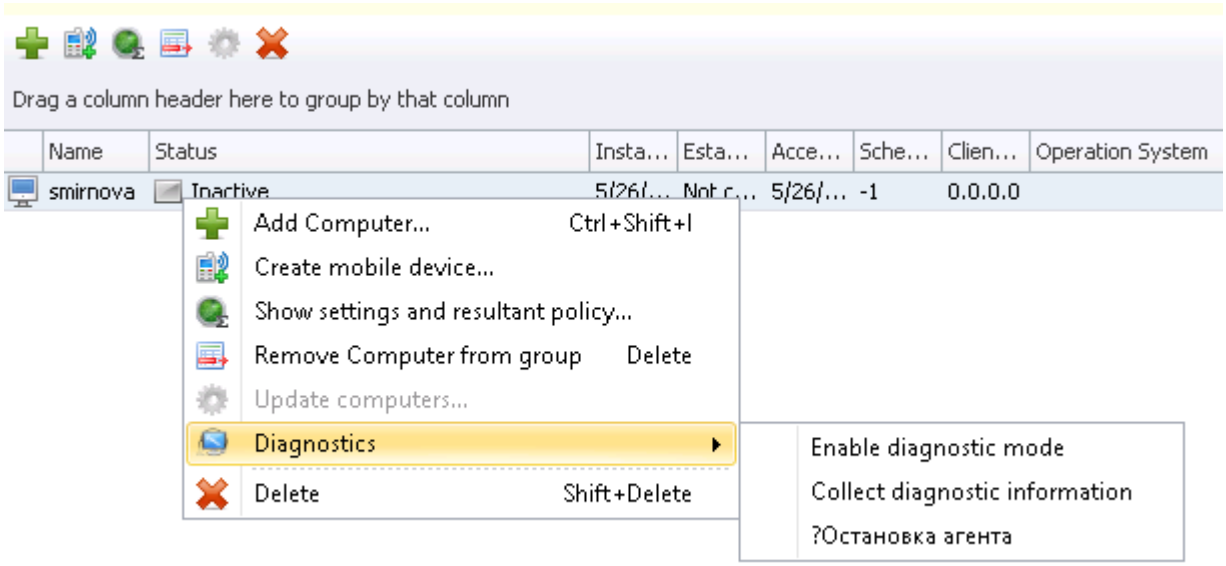
- In case agent is hidden, it cannot be stopped locally.

Important!

To avoid network failure, before you stop DM agent, please make sure that antivirus self-protect function is disabled on computers with antivirus software installed.

Stopping agent remotely/starting agent

Stopping a remote DM agent is performed from DM Management Console. To stop the agent, right-click on a Workstation and choose **Diagnostics -> Stop agent** (in case agent is already started on a Workstation).



When choosing **Stop Agent**, its operation will be suspended and status of the workstation will change to " Inactive".

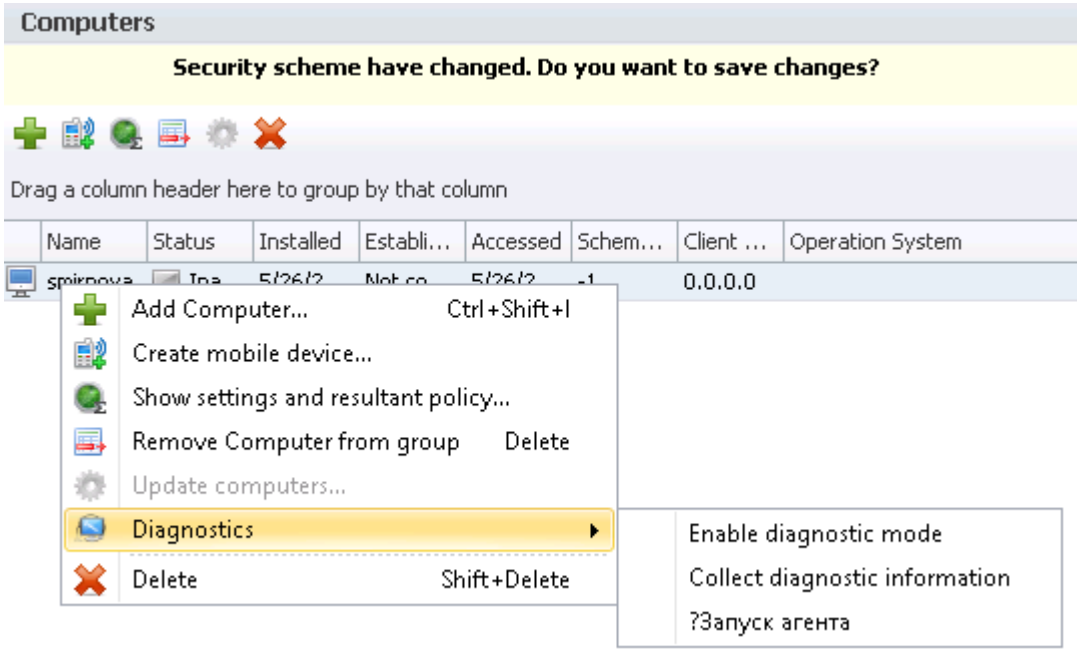
Note:

Stopped agent is available for update or deletion, but stopping is unavailable during update/deletion. In case there is no connection with the agent, stop/start are unavailable.

After the Agent has been stopped:

- events are not intercepted;
- actions are forbidden;
- notifications and DM icon on the toolbar are not dosplayed.

To start DM agent remotely, right-click on a Workstation and choose **Diagnostics -> Start agent** (in case agent is stopped).



Afte choosing agent Start option, its work will be resumed and Workstation status will go back to "Working normally".

Stopping/starting agent locally

Agent can be stopped/started using Windows command prompt. Run **rmtdiag.exe**, specifying the full path to it on the workstation (by default, C:\Program Files\InfoWatch\DeviceMonitor\Client) with the required parameter. For example:

- **C:\Program Files\InfoWatch\DeviceMonitor\Client\rmtdiag.exe /cle** - to start agent;
- **C:\Program Files\InfoWatch\DeviceMonitor\Client\rmtdiag.exe /cld** - to stop agent.

> **Warning!**
>
> To stop the agent, you need to enter DM agent uninstallation password. The password should be entered after **/cld** key and a space. To start the agent, the password is not required.
> For more information on uninstallation password, see "Creating Uninstallation Password Reset Task".

5.4 Managing Security Schema

Security schema description and operation procedures for its managing are provided in the following sections:

- Security Schema Organization;
- Common Actions in Managing Security Schema;
- Security Schema Setup;
- Temporary Employee Access to Network;
- Temporary Employee Access to Devices.

5.4.1 Security Schema Organization

Security schema of InfoWatch Device Monitor is a set of configuration parameters for managing employee controlled by InfoWatch Device Monitor. Security schema is created during server installation and is stored in the database.
Security schema includes the following parameters:

- **Security polices** with a set of rules specified for each security policy (DM).
- **Employee groups** registered in Device Monitor. Each employee group must have a security policy (DM).
- **Computer groups**. Each computer group must have a security policy (DM).
- **White lists** of fully accessed devices.
- **Signature categories** that apply File Monitor rules (DM) to certain file formats.

> **Note:**
>
> To make sure all computers and accounts are covered by security policy (DM), the default employee group and default computer group are provided in the System.

Security schema can be edited multiple times. Updated security schema will be saved as a new version of the existing one. Old security schemas are stored in the database. Using DM Management Console you may see the policies and rules contained therein of any security scheme version.

This topic also contains:

- Security Policies and Rules;
- Employees and Employee Groups;
- Computers and Computer Groups;
- Loading Security Schema to Managed Computers.

Security Policies (DM) and Rules (DM)

Security policy (DM) is a set of rules (DM) used for monitoring operations of data transfer to removable devices, sending documents to print and network activity; it also defines access level to managed peripherals.

The security policy (DM) is assigned to employee group or computer group according to the following principles:

- Each employee group and each computer group must have a security policy (DM).
  You can't add a new employee group or computer group without assigning a security policy (DM). The security policy (DM) for employee group or computer group is selected from available policies (DM). Therefore, security policy (DM) must be created before you add a group.
- You can't assign more than one security policy (DM) to employee group or computer group.
- One security policy (DM) can be assigned to several employee groups or computer groups. However, it is recommended that you assign an individual security policy (DM) to each group.

> **Note:**
>
> You can't remove a security policy (DM) from security scheme if it is assigned to at least one employee group or computer group.

Controlled files and devices access level is defined by security policies (DM) assigned to:

- employee group which the employee belongs to;
- computer group which includes the computer used by the employee.

If an employee was registered with Device Monitor for the first time, his account is automatically added to Default employee group. Therefore, each new employee's access level is initially defined by default employee group security policy (DM) and employee's computer group security policies (DM). You can change access level later by adding the employee to various employee groups.

> **Warning!**
>
> In case of a multiuser access to the workstation and when it is not possible to identify the initiator of the process (event), it is important to configure interception rights not only for employees, but for the computer as well.

Rules are restrictions and conditions that monitor data transfer to removable devices, network activity, sending documents to print, and control access to managed peripherals. A new set of rules (DM) is created for each security policy (DM).

Each rule (DM) has a validity period and is disabled after its expiry.

Rule (DM) types include:

- **Application Monitor Rule** provides application access control via black and white lists.
- **Cloud Storage Monitor Rule** provides web-client control.
- **Clipboard Monitor Rule** provides control of data paste from clipboard. You can prohibit data paste to specified applications or to all applications of a terminal session.
- **Device Monitor Rule**. Lets you control employee access to selected type of peripherals.
- **File Monitor Rule**. Monitors data transfer and editing on removable devices. Rule (DM) can be configured to create file shadow copy and send it to InfoWatch Traffic Monitor when attempting to save a file to a removable device.
- **FTP Monitor Rule**. Both complete deny and partially restrict are available for FTP/FTPS protocol usage: for example, you can allow downloading only. Also, you can set creating shadow copies of transferred files to send them to the InfoWatch Traffic Monitor for further analysis.
- **HTTP(S) Monitor Rule** controls data exchange through HTTP and HTTPS protocol. The System allows you to create shadow copies of transferred files.
- **IM Client Monitor Rule**. Allows to control employee access to instant messengers: Skype, WhatsApp, XMPP, and mobile SMS. The rule can block access to the application or just make copies of transferred files, messages, and chats. InfoWatch Device Monitor sends shadow copies of files and chat sessions to InfoWatch Traffic Monitor without saving them.
- **Mail Monitor Rule**. Provides full control of incoming and outgoing e-mail. Lets you deny of sending and receiving e-mail completely or to allow receiving only or to allow both sending and receiving e-mail completely. The creating of shadow copies transferred to InfoWatch Traffic Monitor for analysis is available too.
- **Network Monitor Rule**. Lets you deny data transferring by any network connections except corporate ones or connections with specified allowed servers. The System has a global setting of which network segments are corporate network and which external addresses are allowed.
- **Photo Monitor Rule**. Lets you set creating of shadow copies of photos made by cameras of controlled mobile devices.
- **Print Monitor Rule**. Lets you to monitor printing activity. Rule (DM) can be configured to create shadow copies of print jobs, which will be sent for InfoWatch Traffic Monitor analysis.
- **ScreenShot Control Monitor Rule** allows you to control screen shots on the agent side.

For each rule, there is a list of operating systems where the rule can apply. The way how the rule applies also depends on the OS. For more information on applying rules, see the "Rules (DM)" subsection.

Employees and Employee Groups

Registration of controlled users (employees) is done according to the following rules:

1. Each employee belongs to at least one employee group (default group). The reason for this requirement is that security policy (DM) can only be assigned to employee groups.
   Default group includes all accounts that have not been added to other groups (employees newly registered in Device Monitor or employees excluded from all other groups).
   You can exclude an employee from "*Default*" group, if the account is added to at least one employee group besides the Default group.
2. After System installed, the "*Shadow copy policy*" is assigned to "*Default*" employee group. The "*Shadow copy policy*" contains following rules:

- **Document shadow copying**. File Monitor rule which sets creating shadow copies of all files written to removable devices.
- **Print shadow copying**. Print Monitor rule which sets creating shadow copies of all print jobs.
- **Skype control**, **XMPP control**, **MMP control**. IM Client Monitor rules which allow instant messengers and set creating shadow copies of all messages, chats and outgoing files.
- **FTP control**. FTP Monitor rule which allows FTP/FTPS protocol and set creating shadow copies of all files sent by FTP/FTPS.
- **HTTPS control**. HTTPS Monitor rule, which creates a post-event, without any dependence on its size, in case transfer is being performed via encrypted channel. Shadow copy is being created, in case request size, transferred via encrypted channel is not smaller than 40 B and not bigger than 40 MB.
- **Mailing subsystem control**. Mail Monitor, which allows incoming and outgoing mail and creates shadow copies for email, sent via encrypted channel, when its size is not bigger than 40 MB.

Computers and computer groups

A computer registered in Device Monitor should be included in at least one computer group (the "default" group). The reason for this requirement is that the security policy (DM) can only be assigned to a computer group.

The default group includes all computers that do not belong to other computer groups (computers that are newly registered in Device Monitor or computers excluded from all other groups). The "*Device policy*" is assigned to the default computer group after the System installation. This policy (DM) does not contain any rule.

You can remove a computer from the default group only if it is added to at least one computer group besides the default group.

You can also add mobile devices to the security scheme, connect them to an employee and install Device Monitor Agent on the mobile device. You can add the mobile device in two ways:

- from a computer group: in this case, you should specify the employee who has been earlier created in the System or added from LDAP;
- from a group of employees: in this case, you should specify the computer group to which you want to add the mobile device.

Uploading security scheme to managed computers

The security scheme of managed computers must be up to date. This is ensured by Agent-Server interaction on managed computers.
Server transmits security scheme to managed computers automatically in the following cases:

- when you save a new or edited security scheme;
- if the employee was registered which's access level is unidentified. Such employee is automatically added to default employee group, and security schema is updated.

If the managed computer is disconnected from the network where InfoWatch Device Monitor is deployed, the policies (DM) will still be active, but they won't be updated and shadow copies will be stored on the hard drive. After the managed computer has connected to InfoWatch Device Monitor server, it automatically updates policies (DM) and sends shadow copies to the server.

5.4.2 Security Scheme Overview

For information on operation of the security scheme, see the sections:

- Viewing Active Security Scheme
- Viewing Old Security Scheme
- Security Scheme Comments
- Editing Security Scheme
- Updating Security Scheme
- Exporting/Importing Security Scheme

For general information on the security scheme, see "Security Schema Organization".
For information on the security scheme configuration, see "Security Schema Setup".

Viewing Active Security Scheme

By default, the Management Console (DM) displays a security scheme which is currently active.

Information on the security scheme configuration is displayed in **Policies**, **Employees**, **Workstations**, **White Lists**, and **Signatures** sections (see "Management Console (DM) Sections").

The security scheme configuration is displayed as groups of elements. Element groups of the selected section are displayed in Navigation pane. Each group of elements has its icon (see the table below).

Icon	Elements group
	Default workstation group
	Workstation group
	Default employee group
	Employee group
	Default signature category
	Signature category
	Devices white list for employee

	Devices white list for employee group
	Devices white list for workstation
	Devices white list for a group of workstations
	Audit log filter
	Security policy

To view information about a security scheme section:

1. Open the required section (see "Management Console (DM) Sections"). The Navigation pane will display the element groups of the selected section.
2. On Navigation pane, select the element group you want to view. This will display all elements of the group in the main screen workspace.
3. To view detailed information on individual elements, click a row with the element name. This opens a table with element properties table on **Details** panel.

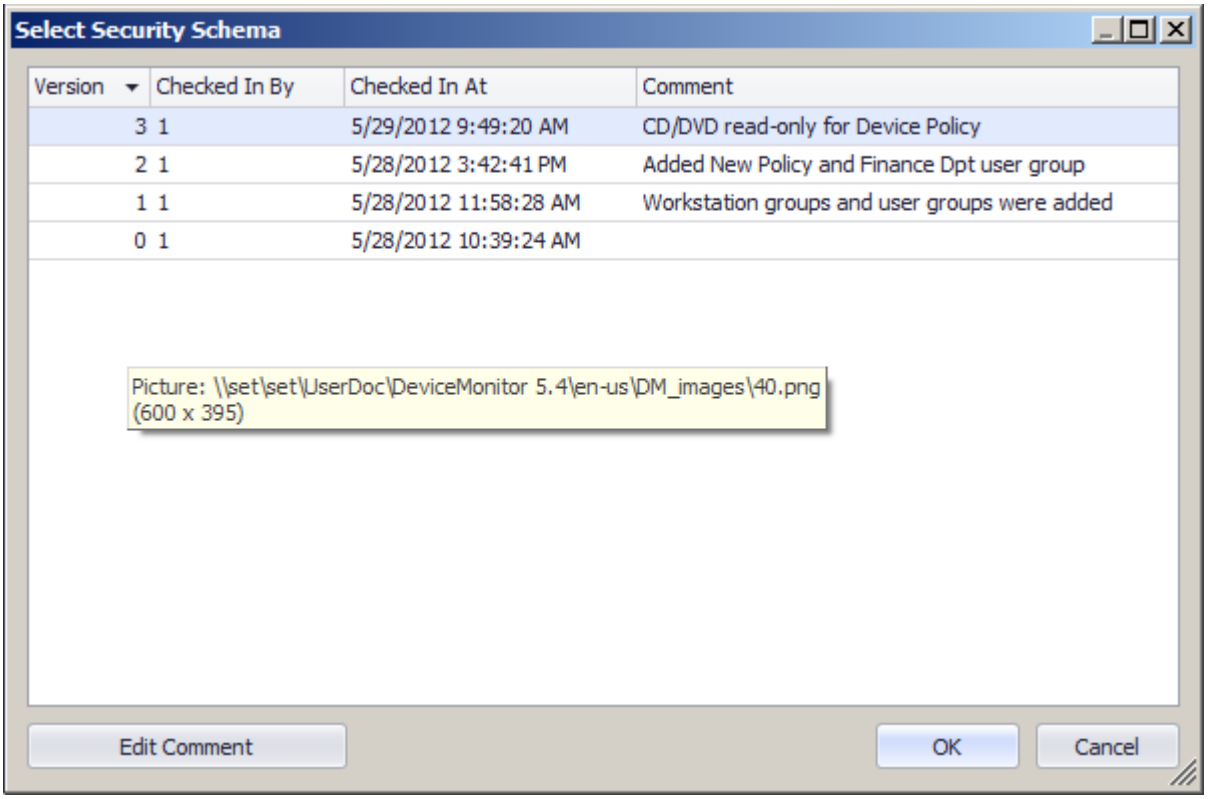
> **Note:**
>
> You can customize the main screen appearance (see "Main screen customization").

Viewing Old Security Scheme

> **Note:**
>
> If you view previous security schemes in editing mode, your recent changes will be discarded.

To view older security schema:

1. In Main Menu select **Security Schema > View Old Security Schema**.
   This opens **Select security schema** dialog.



Each security scheme features the following information:

- **Version**. Security scheme version number.
- **Checked in by**. Name of the version owner.
- **Checked in at**. Last saved version date and time.
- **Comment**. Additional information.

> **Note:**
>
> You can edit comments to any version on this screen (see "Security Schema Comments").
> Information on current Management Console (DM) security scheme (version number and comment) is displayed on the status bar.

2. In **Select security scheme** dialog, select a row that contains the version number of the security scheme you want to view.
3. Click **OK**.

After you click **OK** the selected security schema version will be loaded into Management Console (DM). When working with an old version, the state bar displays: "*Old security schema*".

To return to preview and active security schema, open **Security Schema > View Latest Security schema** in the Main Menu

Security Scheme Comments

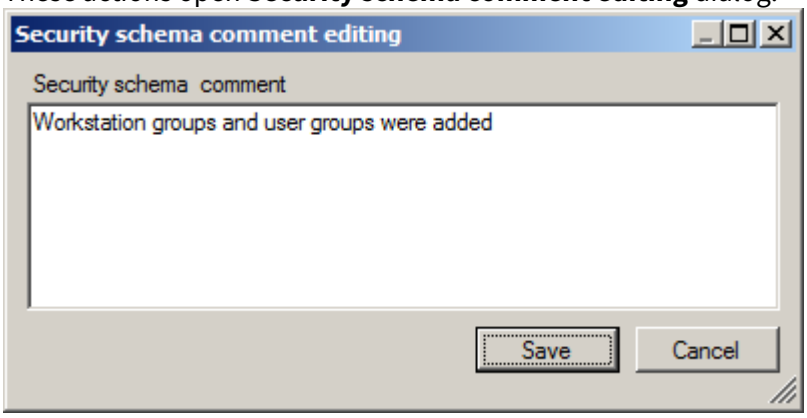
You can specify additional information on your security scheme as a comment. You can add comments to each version of the security scheme.
Comments on current security scheme are displayed in brackets to the right of the scheme version number on the status panel.
You can view comments for all security scheme versions in the **Select Security Schema** dialog (see "Viewing Old Security Schemas").

> **Note:**
>
> You can add comments to security schema regardless of its state (whether it is in editing mode or not).

To add/edit security scheme comment:

1. Take one of the following steps:
   - (*For the current security scheme only*). In Main Menu select **Security Schema > Edit Current Security Schema Comment**.
   - (*For any security schema version except the current one*). In the Main Menu, select **Security schema > View Old Security Schema**. This opens **Select Security Schema** dialog. In this dialog, select the row containing the right security schema version. Then click **Edit Comment**.

   These actions open **Security schema comment editing** dialog.



2. Enter your comment in the dialog box. The maximum comment length is 512 characters.

   > **Note:**
   >
   > For line break, press **<ENTER>** or **<CTRL>+<ENTER>**.

3. Click **Save**.

Editing Security Scheme

> **Warning!**
>
> Security scheme can be edited only by one user at a time. If the security scheme is being edited, information about the user who is editing the scheme and the computer where editing is performed is displayed at red-highlighted string at the top of the main screen. See details in "Awaiting Editing Ends. Unlocking Security Scheme".

All changes are implemented in security scheme editing mode. This mode protects existing security scheme from potential editing errors. The System automatically switches to editing mode just after any Console (DM) user makes any change of security scheme parameters. Changes are saved only by **Save** command.

> **Warning!**
>
> If the server connection terminates during the security scheme editing process, all unsaved changes will be lost.

To edit security scheme:

1. Take one of the following steps:
   - in the Main Menu select **Security Scheme > Edit**
   - click **Edit** on Toolbar
   - make any change of security scheme parameters (security policies (DM), computers, employee accounts, device white lists, signature categories).
     These actions open security scheme editing mode.

     > **Note:**
     >
     > You can edit only the latest version of the security scheme. Thus, Save command is not available when viewing previous versions. To open current security scheme version, open **Security scheme** > **View Latest Security Scheme** from the main menu.
     > Information on security scheme currently used by Management Console (DM) is displayed on the status bar.

2. Edit security scheme parameters:
   - security policies (see "Security Policies");
   - workstation groups (see "Workstations");
   - employee accounts lists (see "Employees");
   - device white lists (see "White Lists");
   - file signature categories (see "Signatures").
3. When all changes are made, save your security scheme. To do this, follow these steps:
   - click **Save** at the top string of main screen workspace where "*Security Scheme have changed. Save changes?*" message is displayed
   - in the Main Menu, select **Security scheme > Save**

- click **Save** on Toolbar.
  These actions save the changes and close security scheme editing mode.

> **Note:**
>
> To discard changes, select **Security Scheme** > **Undo editing** or click **Undo editing** button on the toolbar. This closes scheme editing mode discarding all changes.

Awaiting Editing Ends. Unlocking Security Scheme

The security scheme can be edited only by one user at a time. Changes are applied only after you have saved your security scheme.
If security scheme is being edited, information about the user who is editing it and the computer where editing is performed is displayed at red-highlighted string at the top of the main screen.
If you try to edit any parameters of security scheme (security policies (DM), workstations, employee accounts, device white lists, signature categories) while security scheme is being edited by another user:

1. Management Console (DM) displays warning message.
2. When another user saves changes (or cancel them) Windows system tray displays a notification: "***Security schema is in "read-only" mode***".

Information about the user who is currently editing the scheme is displayed at the string at the top of the main screen and in the status bar.

Security schema might be blocked even if it is not being edited. This may occur if the last editing operation wasn't properly completed (i.e. due to disconnection from the server).
When a user who blocked a scheme connects the server again, the security scheme is automatically unlocked and all unsaved changes made by this user are lost.
There is also a special function that targets the blocking issue - security scheme unblock.

> **Warning!**
>
> Security scheme can be unblocked only by Superuser.

To unblock security schema, in the Main Menu click **Security Schema > Unlock**. All unsaved changes will be lost.

Updating Security Scheme

The system can be simultaneously operated by multiple users. To keep security scheme details in Management Console (DM) up-to-date, run updates regularly. The scheme update security is automatically (in the process of connecting to the server) or manually (when working with the Microsoft Management Console).

You might need to upgrade your security scheme in the following cases:

- registering a new workstation;
- registering an unknown employee;
- modifying your security scheme.

To update security scheme manually, do one of the following:

- select **View > Refresh** in the Main Menu;
- click **Update** on the toolbar;
- press F5.

Exporting/Importing Security Scheme

You might need to save existing settings of a security scheme. You might want to do this if you need to configure Device Monitor server after reinstalling it or when deploying new Device Monitor servers.

When exporting the configuration, a file in .dmc format is saved to your computer. The file contains the current version of the security scheme including:

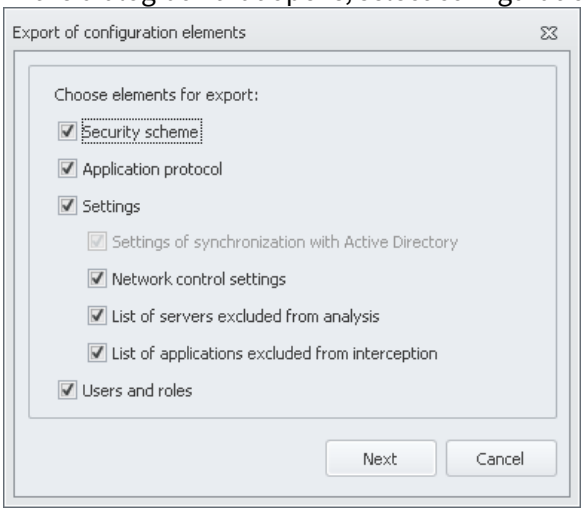
- **Security scheme** (including security policies with rules, groups of employees and computers, categories of signatures) (see "Managing Security Schema")
- **Applicaiton protocol** (see "Application Protocol")
- **Network control settings** (see "Settings of Corporate Network")
- **Servers included from analysis** (see "Network Traffic Control")
- **Applications excluded from interception** (see "Exclusion of Application from Interception")
- **User and roles** (see "Managing Console (DM) Accounts")

> **Important!**
>
> Device Monitor version 6.0 or later does not support importing a configuration file that was exported from earlier versions.

Saved settings can be then imported to a new security scheme.

To export the System configuration:

1. In the main menu, select **Tools** > **Export configuration**.
2. In the dialog box that opens, select configuration elements you want to export.

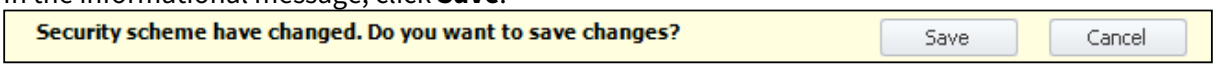


3. Click **Next**.
4. Specify the export file name and select a folder where the file will be saved. Click **Save**.

To import the System configuration:

1. In the main menu, select **Tools** > **Import configuration**.
2. In the dialog box that opens, choose a file in *.dmc format which stores the saved configuration.
3. Click **Open**.
4. In the **Import of configuration elements** dialog box, select elements you want to import.
5. Click **Next**.
6. In the confirmation window, click **OK**.

7. In the informational message, click **Save**.



The saved settings of the security scheme will be imported to the active scheme. If the active scheme contains items with similar names, then **1** will be added to the names of imported items.

5.4.3 Security Schema Setup

After system installation, you must configure your security schema. Security schema is configured as follows:

1. Configure "*Default*" employee group and "*Default*" workstation group.
2. Configuring the rest of security settings.

Security schema configuration principles:

- A security policy (DM) must be created before you create an employee group or workstation group the policy (DM) will be assigned to.
- It is recommended that you assign an individual security policy (DM) for each employee group and workstation group.
- Each security policy (DM) assigned to a group must have a specific set of rules (DM).

Adding workstations to security schema
There are two ways to add a managed workstation:

- add a new workstation automatically during registration;
- add workstation manually via Management Console (DM).

In case of automatic registration, a workstation is added to "*Default*" group. Later you can move it to other groups. If you add it manually, you can select the group immediately.

Adding employee accounts to security schema
You can add new account information manually or automatically. You can register a new employee while editing your security schema. However, if an unknown employee is registered on a workstation, the account will automatically be added to security schema ("*Default*" employee group).

Adding white lists to security schema
Before you create a white list, add device models and instances to the database. Then a whitelist is created for a specific employee/employee group/workstation/workstation group. These employees/workstations have access to whitelisted device models and instances regardless the policy (DM). When a white list record expires, access rights are distributed according to the policies (DM).
Security schema configuration details are available in the following subsections:

- Security Policies (DM);
- Rules (DM);
- Workstations;
- Employees;
- White Lists;
- Signatures;
- Temporary Employee Access to Network;
- Temporary Employee Access to Devices;
- Awaiting Editing Ends. Unlocking Security Scheme.

Security Policies (DM)

On Device Monitor agents, policies apply in the following order:

1. Prohibiting policies (DM).
2. Data protection policies on agents created in TM.
3. Policy of shadow copying (DM).

> **Note:**
>
> For recomendations on configuring the security policy (DM), see "Security Policies (DM) and Rules (DM)".

Each security policy (DM) is a set of rules (DM) that define employees' level of access to controlled files and devices.

Security policies (DM) are assigned to **employee groups** and **computer groups**. The security policy (DM) assigned to the employee group applies to all employees included in this group. The security policy (DM) assigned to a group of computers applies to all employees who work at managed computers included in this group.

Security policies (DM) are managed in the **Policies** section. To go to this section, click **Policies** button in Navigation pane or select **Go > Policies** in in the Main Menu.

For information on working with security policies (DM), see:

- Viewing Security Policies (DM)
- Adding and Configuring New Security Policy (DM)
- Edit Security Policy (DM)
- Deleting Security Policy (DM)

Viewing Security Policies (DM)

Policies area of Navigation pane displays a list of security scheme policies (DM). Main screen workspace displays the list of security policy rules (DM).

> **Note:**
>
> Use additional options to adjust list display (see "Additional Features").

To view security policy rules, select security policy (DM) name in **Policies** area of Navigation pane.

Rules are displayed in a form of a table where each row contains a rule. Columns contain general rule properties. Each rule (DM) has an icon depicting the rule's (DM) coverage and a color mark depicting if a rule (DM) is an allowing one (green), forbidding (red) or partially restricting (yellow).

Extended information on each rule (DM) is displayed on **Details** panel.

For you each rule, you can view general information and additional and additional attributes which depend on the rule type.

To view all rule properties, select the row that contains the rule (DM) name in the main screen workspace. This opens a table containing rule (DM) information on **Details** panel.

General information:

- **Name**. Rule (DM) name.
- **Policy**. Name of the security policy (DM) that includes the rule (DM).
- **Interceptor**. Interceptor type assigned to the rule (DM).

- **Operation**. The operation controlled by the rule (DM).
- **Period**. Rule starting and expiry time.

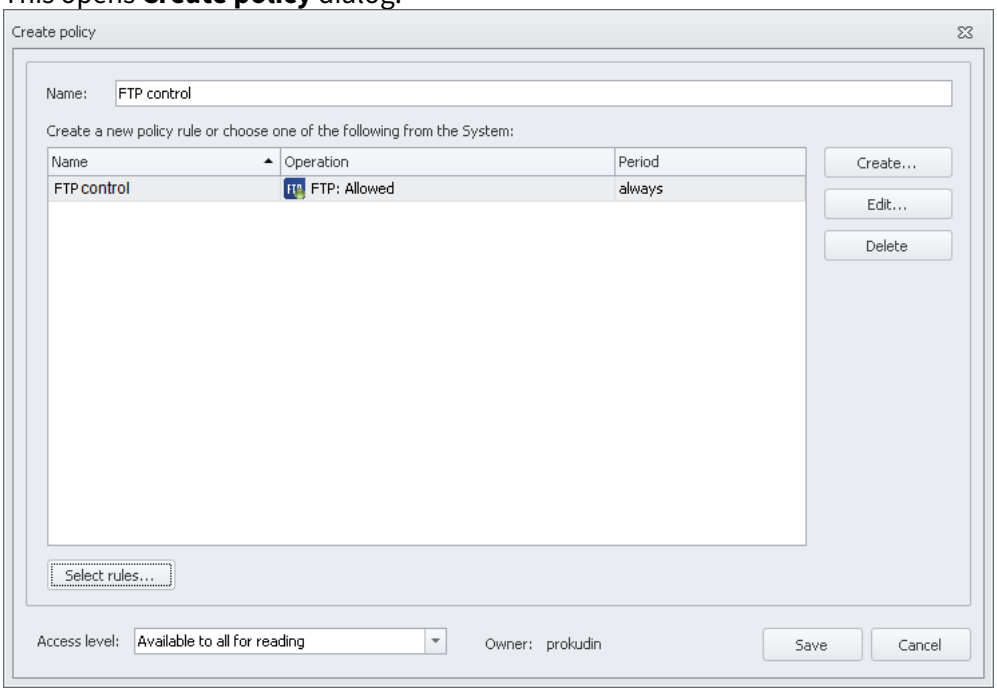
> **Note:**
>
> Information for some attributes is duplicated on the main screen.

Adding and Configuring New Security Policy (DM)

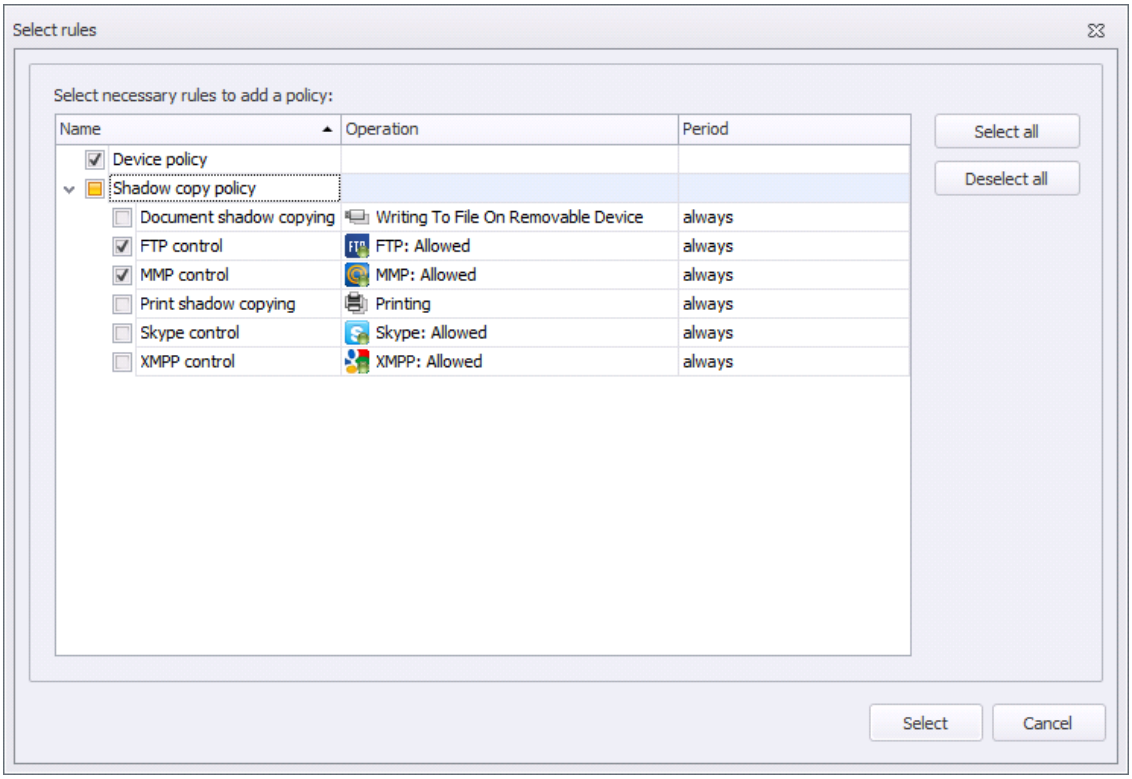
To create and configure security policy:

1. Go to **Policies**.
2. Take one of the following steps:
   - click **Create Policy** at the top of Navigation panel;
   - in Main Menu, select **Edit > Create Policy**.
   - Use **Ctrl+N** shortcut on a keyboard.

   This opens **Create policy** dialog.



3. In **Name field**, enter new security policy (DM) name.
4. Make a list of rules (DM) for new security policy (DM):
   - To copy rule (DM) from another policy (DM) click **Select rules**. In new dialog flag the rules (DM) you want to copy to a new security policy (DM).



You can also select the whole policy (DM) - then all rules (DM) it contains will be added to a new security policy (DM).
After you mark all rules (DM) click **Select**.

- To create a new rule (DM) click **Create** and specify rule (DM) parameters as described:
  - Configuring Application Monitor Rule (DM);
  - Configuring Clipboard Monitor Rule;
  - Configuring Cloud Storage Monitor Rule (DM);
  - Configuring Device Monitor Rule (DM);
  - Configuring File Monitor Rule (DM);
  - Configuring FTP Monitor Rule (DM);
  - Configuring HTTPS Monitor Rule (DM);
  - Configuring IM Client Monitor Rule (DM);
  - Configuring Mail Monitor Rule (DM);
  - Configuring Network Monitor Rule (DM);
  - Configuring Photo Monitor Rule (DM);
  - Configuring Print Monitor Rule (DM);
  - Configuring ScreenShot Control Monitor Rule (DM);
  - Configuring ScreenShot Monitor Rule (DM).

  You can also edit or delete policy (DM) rule (DM) by selecting it and clicking **Edit** or **Delete** appropriately.

5. In the **Access level** drop-down list, specify permissions for reading and editing the policy.
6. When all rules (DM) to be included in the policy (DM) are defined, click **Save**.

Warning!

To apply changes you have to save current security scheme (see "Editing Security Scheme"). If you don't save your security schema, all changes will be discarded.

Later you will be able to edit or remove security policies (DM): (see "Editing Security Policy", "Removing Security Policy"), as well as their rules (DM) (see "Adding a Rule (DM)", "Editing a Rule (DM)", "Deleting a Rule (DM)", "Copying a Rule (DM)").

Edit Security Policy (DM)

To edit security policy (DM):

1. Go to **Policies**.
2. In **Policies** area of Navigation pane, select security policy (DM) name.
3. Take one of the following steps:
   - in the Main Menu, select **Edit > Edit Policy**;
   - click  **Edit Policy** at the top of Navigation pane;
   - use **Ctrl+E** shortcut;
   - double-click selected security policy (DM) name;
   - right-click the policy name and choose **Edit** from the context menu.

   These actions open **Edit Policy** dialog.
4. In this dialog, edit security policy (DM) name by entering a new one in **Name** field.
5. Click **OK**.

Warning!

To apply changes, save current security scheme (see "Editing Security Scheme"). Otherwise, all changes will be discarded.

Deleting Security Policy (DM)

Warning!

The policy (DM) appointed at least one employee group or workstation groups, cannot be deleted. To delete security policy (DM) make sure that this policy (DM) is not apointed to any employee group (see "Viewing Employee Details") or workstation group (see "Viewing Workstation Details").

To delete security policy:

1. Go to **Policies**.
2. In **Policies** area of Navigation pane select security policy (DM) name.
3. Take one of the following steps:
   - in the Main Menu select **Edit > Delete Policy**
   - click  **Delete Policy** at the top of Navigation pane.
   - Use **Ctrl+D** shortcut.
4. In the following confirmation dialog select **Yes** to confirm that you want to remove security policy (DM).

Warning!

To apply changes you have to save current security schema (see "Editing Security Scheme"). If you don't save your security schema, all changes will be discarded.

Rules (DM)

Rules (DM) are used basing on the security policy (DM) they are assigned to. Each security policy (DM) has individual set of rules (DM). Information on rules (DM) is available in the following subsections:

- Applying Rules (DM)
- Adding a Rule (DM)
- Editing a Rule (DM)
- Deleting a Rule (DM)
- Copying a Rule (DM)

Applying Rules (DM)

To make a set of rules (DM) effective, keep in mind all possible instances of their application.

The event is considered as satisfying the rule (DM) if it meets all rule (DM) parameters (for example both event time is within rule (DM) time period and a size of outgoing document is not less than minimal file size and so on).

If the event meets several rules (DM) at the same time, then, in general, more limiting rule overrides the permissive one. In details:

1. The excluding rule (DM) (Exclude from interception option is selected: see "Configuring File Monitor Rule (DM)") has the highest priority.
2. The forbidding rule (DM) overrides the permitting one. For example, Device Monitor rule (DM) (see "Configuring Device Monitor Rule (DM)") with *No access limitation* overrides rule which permits *Read only*, and the last one overrides a rule (DM) with *Full access to encrypted devices*. Also, FTP Monitor rule (DM) (see "Configuring FTP Monitor Rule (DM)") with *Forbid using FTP-protocol* applies instead of the rule (DM) with *Full access to encrypted devices*, and the last one - instead of the rule with *Permit using FTP-protocol*. And so on.
3. The rule creating shadow copies (**Create a shadow copy option** is selected) overrides a rule without shadow copying.
4. For IM Client Monitor rules (DM) which make a copy of voice traffic (**Create voice copy** option is selected: see "Configuring IM Client Monitor Rule (DM)"), the rule (DM) which has a constraint of lesser recording duration overrides a rule (DM) with longer recording duration.

Other important information on applying rules (DM):

- Device Monitor Rules Application;
- Creating Shadow Copies and Blocking Operations Due to Free Space Shortage.

Device Monitor Rules (DM) Application

Access to all Device Monitor interceptor controlled peripherals is a collection of rules (DM) assigned to each device.

Employee access rights are defined basing on:

- rules (DM) applied to employee groups which an employee is included in;
- rules (DM) applied to workstation groups of the workstation using for device access;
- white lists.

During Agent installation controlled are fully accessible by default. Therefore, all forbidden operations with the device must be set explicitly (i.e., in form of a rule (DM)).

Initially, each newly registered workstation is added to the Default group. This group has a "Shadow copy policy" (DM) which contains no rules (DM). Device rules (DM) are nor applied to default employees. Thus, the System always allows access to all managed workstations after installation.

For example:
There is a rule (DM) that lets workstation group A write to CD/DVD drive. Workstation WS belongs only to workstation group A. Employee Smith belongs only to employee group B with no device rules (DM). Employee Smith tries to view a CD on workstation WS. In this case, the employee won't be able to view CD contents of a disk and write new data.

You can assign multiple rules (DM), in several policies (DM) either, with various access levels to the same device. This causes rule (DM) conflict. General conflict resolution principle: higher limit means higher priority (see the table for further details).

Device type	All devices, except CD/DVD, Floppy drives, and removable storage devices	CD/DVD	Floppy drives and removable storage devices
Access in descending order of priority	Banned from use	1. No access 2. Read-only	1. No access 2. Read-only 3. Full access to the encrypted devices only

Examples:

> **Example 1**. There is a rule (DM) for workstation group C that forbids an access to a removable storage device. There is a rule (DM) in employee group D policy (DM) that allows access to removable storage devices in read-only mode. Employee Smith belongs to employee group D and tries to access removable storage device from the workstation that belongs to workstation group C. Conflict is resolved in favor of more restrictive rule (DM), i.e. employee Smith cannot read from a removable storage device.
> **Example 2**. There is a rule (DM) in employee group E policy (DM) that allows read-only access to a removable storage device. There is a rule (DM) in employee group F that grants a full access only to encrypted removable storage devices. Employee Smith belongs to both groups. Conflict is resolved in favor of the more restrictive rule (DM): i.e. employee Smith can get a read-only access: both encrypted and not encrypted (less priority rule (DM) is not applied at all).

Rules (DM) for certain controlled device types may overlap (see the table). These rules (DM) should also be considered when banning access to controlled devices.

> **Note:**
>
> A list of controlled devices types and a set of matching operations are provided in "Configuring Device Monitor Rule (DM)".

Rule (DM)	Overlapping rules	Notes
Floppy	No	
CD/DVD	No	

Parallel port (LPT)	Local printer (LPT) Imaging devices (LPT)	If there is no access to LPT port, the device connected to this port will be unavailable
Serial port (COM)	Modem Local printer (COM) Imaging devices (COM)	A modem connected to COM port is only accessed basing on COM port rule If there is no access to COM port, the device connected to this port will be unavailable
Removable Storage (USB and IEEE 1394 devices)	FireWire (IEEE 1394)	If there is no access to FireWire (IEEE 1394) port, the device connected to this port will be unavailable
Local Printer (with USB, IEEE 1394, SCSI connection, etc.)	FireWire (IEEE 1394) Serial port (COM) Parallel port (LPT)	If there is no access to FireWire (IEEE 1394), COM, LPT port, the device connected to this port will be unavailable
Image-processing Devices (cameras, scanners)	FireWire (IEEE 1394) Serial port (COM) Parallel port (LPT)	If there is no access to FireWire (IEEE 1394), COM, LPT port, the device connected to this port will be unavailable
Bluetooth Device	No	
IrDA Device	No	
Other USB Devices	No	
FireWire	Removable storage device (IEEE 1394) Local printer (IEEE 1394) Imaging devices (IEEE 1394)	If there is no access to FireWire (IEEE 1394) port, the device connected to this port will be unavailable
Modem	Serial port (COM)	Modem access rules do not affect modems connected to COM port. A modem connected to COM port is only accessed basing on COM port rule
Smart Card Reader	No	
Tape Device	No	
Multifunctional Device	No	
PCMCI device	No	
USB Network Adapter	No	

Pocket Computer (Windows Mobile and Palm OS pocket computers)	No	

Creating Shadow Copies and Blocking Operations Due to Free Space Shortage

A shadow copy of a file, document, message or chat is created when the following conditions are met:

1. A rule (DM) which applies to the file enables creating shadow copies and the file size is within the specified range.
2. There is more free space on the controlled computer than the value specified in the **Free clients' disk space** parameter (see "Common Settings for Agents"). The default value is 10%.
3. There is more free space on the controlled computer than it is needed to create a shadow copy.

> **Warning!**
>
> If a rule (DM) enables shadow copying, but there is less free space on the computer than it is defined by the policy or than it is needed to save the file, then the event will be created without a shadow copy. Such events are displayed in the Management Console (DM) with the *Error of copy creating* state (see "Viewing Events").

Besides shadow copies, the computer temporary (until a connection with Device Monitor Server is established) stores information about events. For this purpose, the drive where Device Monitor Agent is installed has allocated space for storing up to 30000 events (about 300 MB).

If:

- Device Monitor Agent has not connected with Device Monitor Server for a long time and has than 30000 events
  and
- in common settings for agents the **If there is not enough disk space to save shadow copy, the operation will** parameter has the **Operation is blocked** value,

then any employee's actions controlled by the current security policy will be blocked.

Adding a Rule (DM)

To add a rule to security policy:

1. Go to **Policies**.
2. In **Policy** area of Navigation pane, select the name of the security policy (DM) you want to add the rule (DM) to.
3. Take one of the following steps:
   - in Main Menu, click **Edit > Create Rule**;
   - click **Create Rule** in the top of **Policies area**;
   - right-click in **Policies** area and select **Create Rule** from the drop-down list;
   - use **Ctrl+Shift+N** shortcut.
4. Specify the interceptor rule (DM):
   - Configuring Application Monitor Rule (DM)
   - Configuring Clipboard Monitor Rule (DM)
   - Configuring Cloud Storage Monitor Rule (DM)
   - Configuring Device Monitor Rule (DM)

- Configuring File Monitor Rule (DM)
- Configuring FTP Monitor Rule (DM)
- Configuring HTTPS Monitor Rule (DM)
- Configuring IM Client Monitor Rule (DM)
- Configuring Mail Monitor Rule (DM)
- Configuring Network Monitor Rule (DM)
- Configuring Photo Monitor Rule (DM)
- Configuring Print Monitor Rule (DM)
- Configuring ScreenShot Control Monitor Rule (DM)
- Configuring ScreenShot Monitor Rule (DM)

5. After you have set all necessary parameters, click **Save** in rule (DM) settings.

Warning!

To apply changes you have to save current security scheme (see "Editing Security Scheme"). If you don't save the security scheme, all changes will be discarded.

Configuring Application Monitor Rule (DM)

An employee can perform actions which can lead to the leakage of confidential information through third-party applications installed on a workstation and not controlled by InfoWatch Device Monitor.

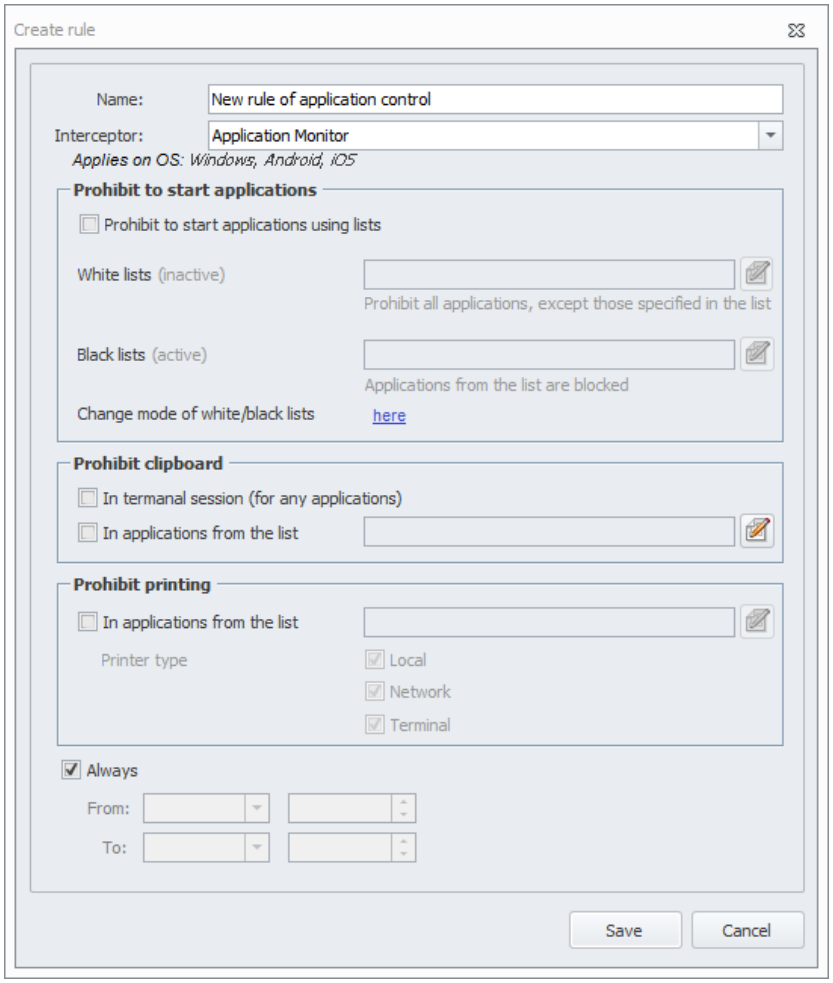
Application Monitor interceptor allows you to control employees' access to applications prohibiting the following actions:

- starting applications;
- using clipboard;
- printing.

These prohibitions can be activated both separately and together.

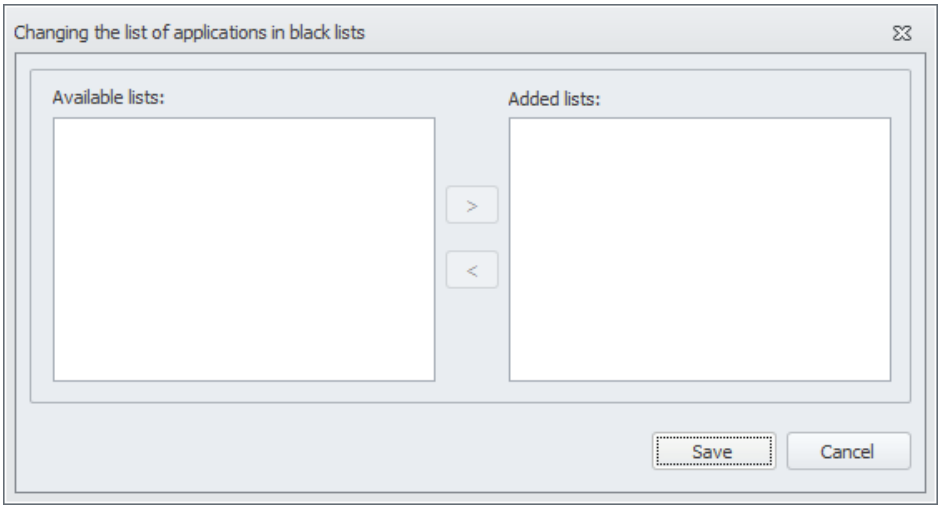
Note:

The rule applies on computers with Windows OS and mobile devices on Android and iOS platforms.



To configure the rule, perform the following steps:

1. Go to **Policies** section.
2. In **Policies** area at Navigation pane select a security policy (DM) which you want to add a rule (DM) to.
3. Take one of the following steps:
   - in the Main Menu select **Edit > Create rule**;
   - click **Create rule** at the top of **Policies** area;
   - right-click at the empty space in **Policies** area and select **Create rule** from the drop-down list;
   - click Ctrl+N.
4. In Create rule (DM) dialog in **Interceptor** field select **Application Monitor**.
5. Enter rule (DM) name to **Name field**.
6. In **Prohibit to start applications** block add white and black applications lists by clicking .



Note:

To switch between active black and white application lists, click the link here.
On creating the application list, see "Application protocol".

7. In the window that opens, choose necessary types of available lists and move them to **Added lists** area by pressing >.
8. Click **Save**.
9. In **Prohibit to start applications** block, select check boxes next to the application groups for which data copying should be prohibited:
   - In terminal session (for any applications);
   - In applications from the list (add lists by clicking).

Warning!

If using the clipboard is prohibited, the prohibition applies to all data types to both copying and pasting data, regardless of the black/white list mode.

10. In the **Prohibit printing** block, specify applications for which printing should be prohibited and the printer type:
    - local;
    - network;
    - terminal.

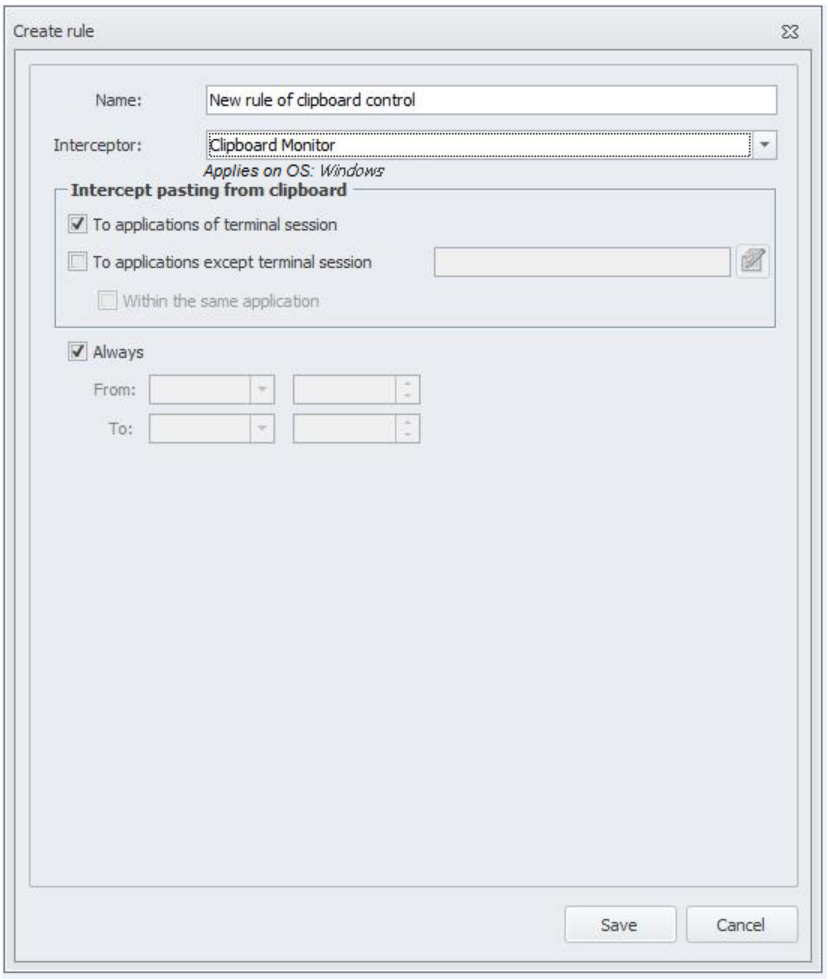
    The user will not be able to print data in specified applications. Choosing specified printer types is not available either.

11. Define a period when the rule applies. By default, the rule (DM) is always in effect (**Always** option is selected). To specify a period, clear the **Always** check box and specify dates and time in **From** and **To** fields.
12. When all parameters are configured, click **Save**.

Configuring Clipboard Monitor Rule (DM)

The Clipboard Monitor interceptor allows you to control access of employees to the clipboard.

> **Note:**
>
> The rule applies on computers with Windows OS.



To configure the rule, perform the following steps:

1. Go to **Policies** section.
2. In **Policies** area at Navigation pane, select a security policy (DM) to which you want to add a rule (DM).
3. Do either of the following:
   - in the main menu, select **Edit > Create rule**;
   - click **Create rule** at the top of **Policies** area;
   - right-click at the empty space in **Policies** area and select **Create rule** from the drop-down list;
   - press Ctrl+Shift+N.
4. In **Create rule** dialog in the **Interceptor** field, select **Clipboard Monitor**.
5. Enter rule (DM) name to **Name** field.

6. In **Intercept pasting from clipboard** area, define in which case the rule (DM) will trigger:
   - **To applications of terminal session**. If the option is selected, then the rule (DM) will trigger when data is pasted to applications of a terminal session. Pasting data within a terminal session does not trigger the rule.
   - **To applications except terminal session**. If the option is selected, then the rule (DM) will trigger only when data is pasted to specified applications. To choose applications, click  button (see "Application protocol"). The rule also applies to data copied from a terminal session
     If you need the rule to be trigger when data is pasted to the application from which it has been copied, select the **Within the same application** option.
7. Define a period of rule (DM) action. By default, the rule (DM) is always in effect (**Always** option is checked). To specify the period, clear the **Always** check box and specify dates and time in **From** and **To** fields.
8. When all parameters are configured, click **Save**.

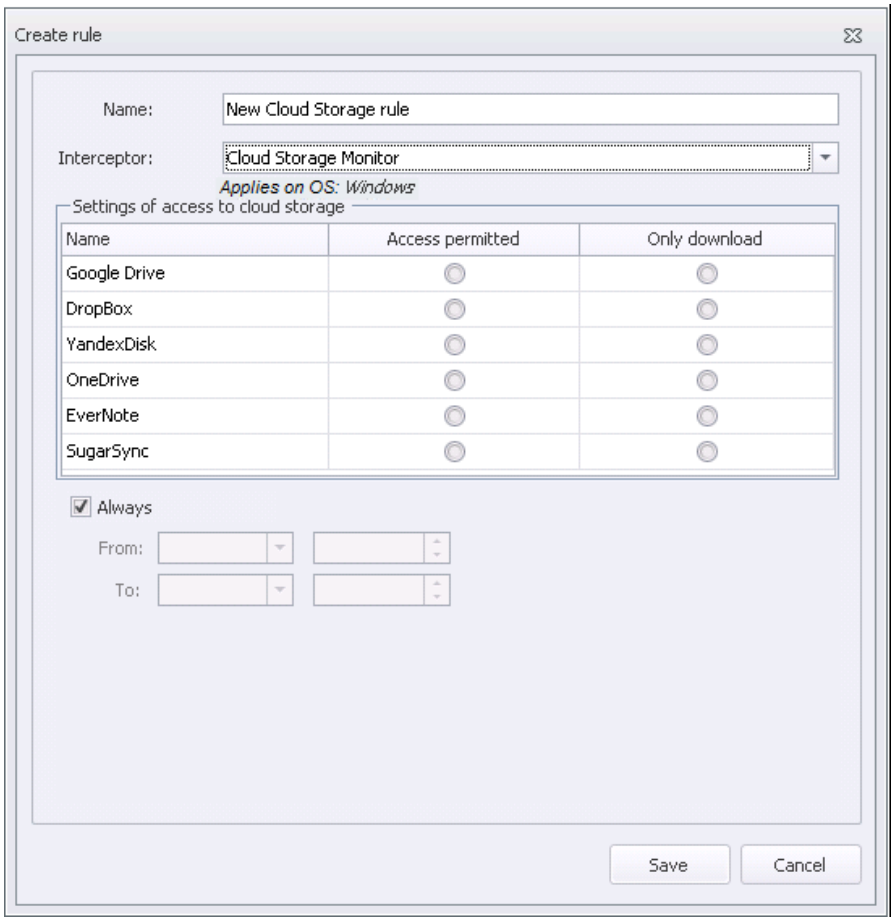
Configuring Cloud Storage Monitor Rule (DM)

Cloud Storage Monitor interceptor allows you to control web clients of the following cloud storages:

Storage name	Restriction options
Google Drive	Access Denied/Only download
DropBox	Access Denied/Only download
YandexDisk	Access Denied/Only download
OneDrive	Access Denied/Only download
EverNote	Access Denied/Only download
SugarSync	Access Denied/Only download

Note:

The rule applies on computers with Windows OS.



To configure the rule, perform the following steps:

1. Go to **Policies** section.
2. In **Policies** area at Navigation pane, select a security policy (DM) to which you want to add a rule (DM).
3. Take one of the following steps:
   - in the Main Menu select **Edit > Create rule**;
   - click **Create rule** at the top of **Policies** area;
   - right-click at the empty space in **Policies** area and select **Create rule** from the drop-down list;
   - press Ctrl+Shift+N.
4. In **Create rule** dialog in **Interceptor** field, select **Cloud Storage Monitor**.
5. Enter rule (DM) name to the **Name** field.
6. In **Setting of access to cloud storage** area, mark the option for access limitation (see table above).
7. Define a period of rule (DM) action. By default, the rule (DM) is always in effect (**Always** option is checked). To specify a period, clear **Always** check box and specify dates and time in **From** and **To** fields.
8. When all parameters are configured, click **Save**.

Configuring Device Monitor Rule (DM)

Device Monitor interceptor allows you to control employee access to peripheral devices and devices connected to thin and thick terminal clients.

Note:

The rule applies on computers with Windows OS.

Control of terminal clients connected via Microsoft RDP or Citrix ICA can be useful in the following cases:

1. A remote user connects to a computer with installed Device Monitor Agent from a terminal client.
2. There is a storage device or a printer connected to a terminal client.
3. A remote user tries to print/copy data from a computer (the terminal storage/printer must be connected to the computer via Microsoft RDP or Citrix ICA).

Name	Behavior
Floppy	Full access to encrypted devices only / Read only / Access denied
CD/DVD	Read only / Access denied
LPT port	Denied
COM port	Denied
Portable disk drives (USB and IEEE 1394 devices)	Full access to encrypted devices only / Read only / Access denied
Local Printer (with USB, IEEE 1394, SCSI connection, etc.)	Denied
Image Editing Devices (cameras and scanners)	Denied
Bluetooth Device	Denied
IrDA Device	Denied
Other USB Devices	Denied
FireWire	Denied
Modem	Denied
Smart Card Reader	Denied
Tape Drive	Denied
Multifunctional Device	Denied
PCMCI device	Denied
USB Adapter	Denied
Pocket Computer (Windows Mobile and Palm OS pocket computers)	Denied
Network printer	Denied

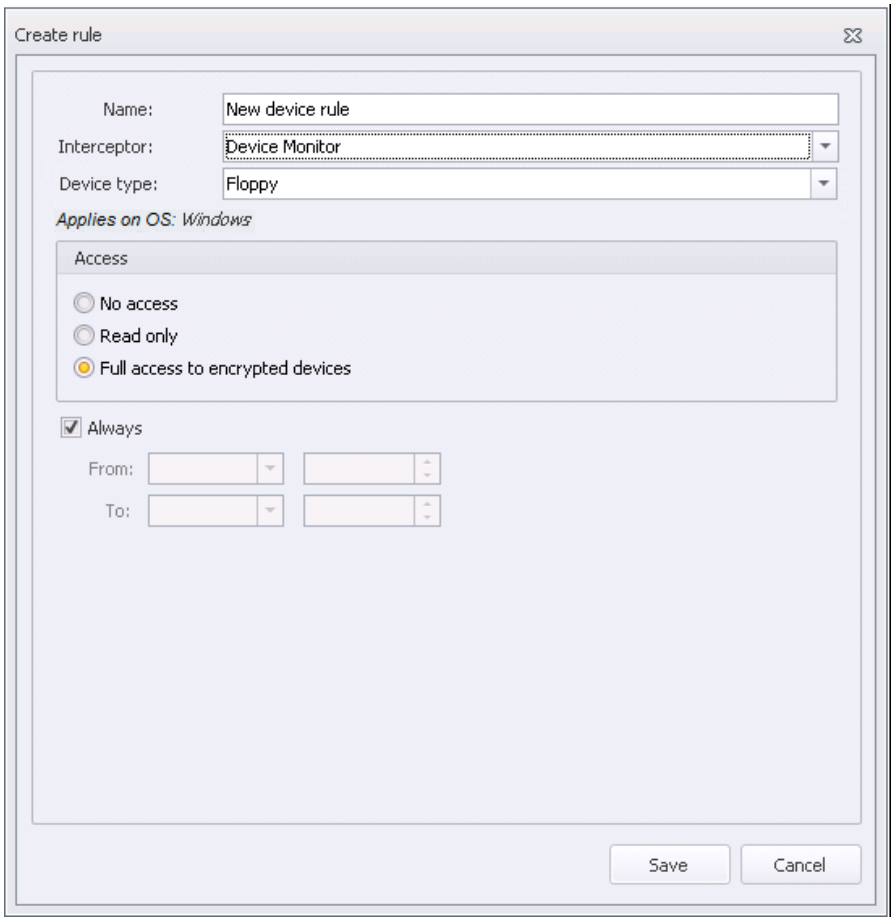
Microsoft RDP or Citrix ICA connection control	
Terminal printer	Denied
Terminal storage	Read only/Access denied
Terminal port (thin client port)	Denied
Terminal Plug and Play devices	Denied

Note:

InfoWatch Device Monitor supports devices encrypted by InfoWatch CryptoStorage SOHO 2.1, InfoWatch CryptoStorage Enterprise 1.0, Kaspersky KryptoStorage 1.0 and TrueCrypt 7.1.

Warning!

If event matches multiple rules (DM), see "Applying Rules (DM)" and "Device Monitor Rules (DM) Application".



To configure the rule, perform the following steps:

1. Go to **Policies** section.
2. In **Policies** area at Navigation pane select a security policy (DM) to which you want to add a rule.

3. Take one of the following steps:
    - in the Main Menu select **Edit > Create rule**;
    - click **Create rule** at the top of **Policies** area;
    - right-click at the empty space in **Policies** area and select **Create rule** from the drop-down list.
4. In **Create rule** dialog in **Interceptor** field, select **Device Monitor**.
5. Enter rule (DM) name to the **Name** field.
6. Select the device type controlled by this rule from **Device type** drop-down list.
7. In the **Access** area, select the required access level (see the table above).
8. Define a period of rule (DM) action. By default, the rule (DM) is always in effect (**Always** option is checked). To specify a period, clear **Always** check box and specify dates and time in **From** and **To** fields.
9. When all parameters are configured, click **Save**.

Configuring File Monitor Rule (DM)

File Monitor interceptor allows you to monitor the following operations: copying files to network resources and writing to the file on a removable device. The System registers only successful operations.

The following removable devices are supported:

- devices connected via USB and IEEE 1394 ports (FireWire, i-Link)
- floppy disk storage systems (floppy disk drive, ZIP drive)
- optical disks (CD, DVD, BD) in Live File System mode
- media devices
- external devices connected through a terminal session

The following network devices are supported:

- network resources
- network volumes

With this rule, you can monitor the following actions of employees:

- Copying a file to network resources using UNC (for example, *Server**SharedFolder**Folder**File*)
- Copying or moving files to a removable device. The System monitor operation of copying/moving from a controlled computer, another removable device or a network resource
- Creating a file directly on a removable device
- Editing a file directly on a removable device, including file renaming
- Copying a file to media devices connected via MTP

    Note:

    File renaming on media devices is not supported.

- Copying a file to a terminal session application
- Copying a file to resource connected via a terminal session (redirection for network folders and virtual devices is supported)

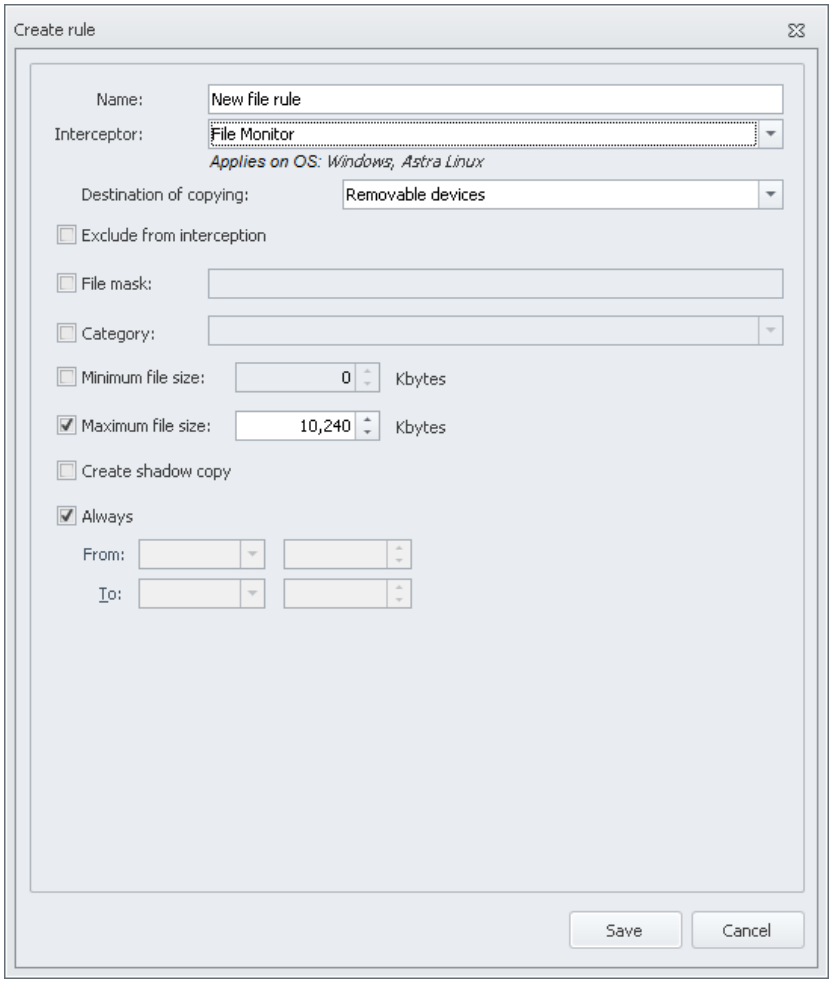
Warning!

The rule applies on computers with MS Windows and Astra Linux OS.

On computers with Astra Linux, the rule controls only copying/moving files to removable devices connected via USB and FireWire.

Warning!

Information about rule (DM) conflict resolving see in "Applying Rules (DM)".



To configure the rule, perform the following steps:

1. Go to **Policies** section.
2. In **Policies** area at Navigation pane, select a security policy (DM) to which you want to add a rule.
3. Do either of the following:
   - in the Main Menu select **Edit > Create rule**;
   - click **Create rule** at the top of **Policies** area;
   - right-click at the empty space in **Policies** area and select **Create rule** from the drop-down list;
   - press Ctrl+Shitf+N.

4. In **Create rule** dialog in **Interceptor** field, select **File Monitor**.
5. Enter rule (DM) name to the **Name** field.
6. In the **Destination of copying** field, specify objects whose copying will be intercepted. The can be removable devices or network volumes.
7. If you want to exclude specific files from interception, flag **Exclude from interception**. For operations satisfying this rule, no events or shadow copies will be created.

> **Warning!**
>
> If file record event is a subject of several rules (DM), the excluding rule (DM) has the highest priority.

8. You can constrain controlled files by mask. Flag **File mask** checkbox and specify a mask. You can use wildcard characters when specifying a file mask: «?» to replace a character or «*» to replace a character set. For example, *.doc. The space character is interpreted as a part of file name.

> **Warning!**
>
> There should be only one mask for one rule (DM). In case it is required to type in several masks, one should create a rule (DM) corresponding to mask.

> **Note:**
>
> On computers with Astra Linux, file masks are ignored.

9. You can constrain controlled files by signature category (see "Signatures"). Flag Category checkbox and select a category from a drop-down list: the rule (DM) will be applied to files with chosen signature type.

> **Note:**
>
> On computers with Astra Linux, signature categories are ignored.

10. To control files by size, specify:
    - **Minimum File Size**. When checked, rule (DM) will be applied only to files larger or of the specified size.
    - **Maximum File Size**. When checked, rule (DM) will be applied only to files smaller or of the specified size.
11. If you want to create shadow copies of outgoing files and then analyze them in Traffic Monitor, flag **Create a shadow copy**.

Warning!

If there is at least one valid rule (DM) for File Monitor that enables shadow copying, and there is less free space at the hard drive than required by the policy (DM) (see "Creating Shadow Copies and Blocking Operations Due to Free Space Shortage"), then file saving will be performed without shadow copy creating.

12. Define a period of rule (DM) action. By default, the rule (DM) is always in effect (**Always** option is checked). To specify a period, clear **Always** check box and specify dates and time in **From** and **To** fields.
13. When all parameters are configured, click **Save**.

Configuring FTP Monitor Rule (DM)

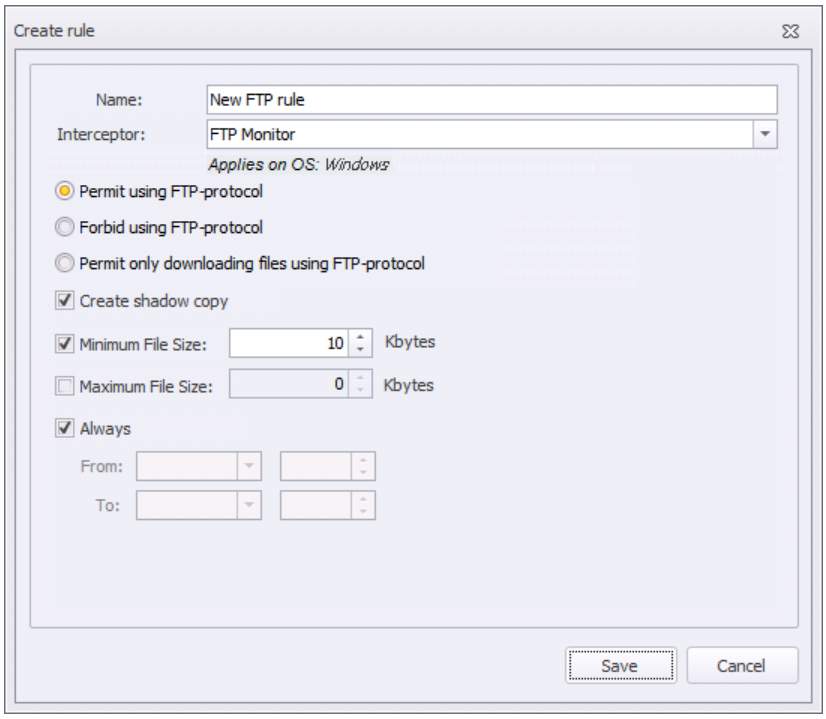
FTP Monitor interceptor allows you to control data transfer through FTP/FTPS protocol.

Note:

The rule applies on computers with Windows OS.

Warning!

The file is subject to **FTP Monitor** rule (DM) if **ALL** file parameters meet rule (DM) conditions **EXCEPT** maximum and minimum file size. **Maximum file size** and **Minimum file size** are taken into consideration only for shadow copying. So if the file size is within specified range, then file transfer event will contain a shadow copy; otherwise, an event will be created without shadow copy.



To configure the rule, perform the following steps:

1. Go to **Policies** section.
2. In **Policies** area at Navigation pane select a security policy (DM) which you want to add a rule (DM) to.
3. Take one of the following steps:
   - in the Main Menu, select **Edit > Create rule**;
   - click **Create rule** at the top of **Policies** area;
   - right-click at the empty space in **Policies** area and select **Create rule** from the drop-down list;
   - press Ctrl+Shift+N.
4. In **Create rule** dialog in **Interceptor** field, select **Ftp Monitor**.
5. Enter rule (DM) name to **Name** field.
6. Select inspection level for data transfer through FTP/FTPS protocol:
   - **Permit using FTP-protocol**
   - **Forbid using FTP-protocol**
   - **Permit only downloading files using FTP-protocol**
7. If you allowed using FTP/FTPS protocol then you can also configure creating of shadow copies of outgoing files. You can select **Create a shadow copy** check box and specify additional settings:
   - **Minimum File Size**. If the check box is selected, shadow copies will be enabled only for files of specified size or larger.
   - **Maximum File Size**. If the check box is selected, shadow copies will be enabled only for files of specified size or smaller.

   Warning!

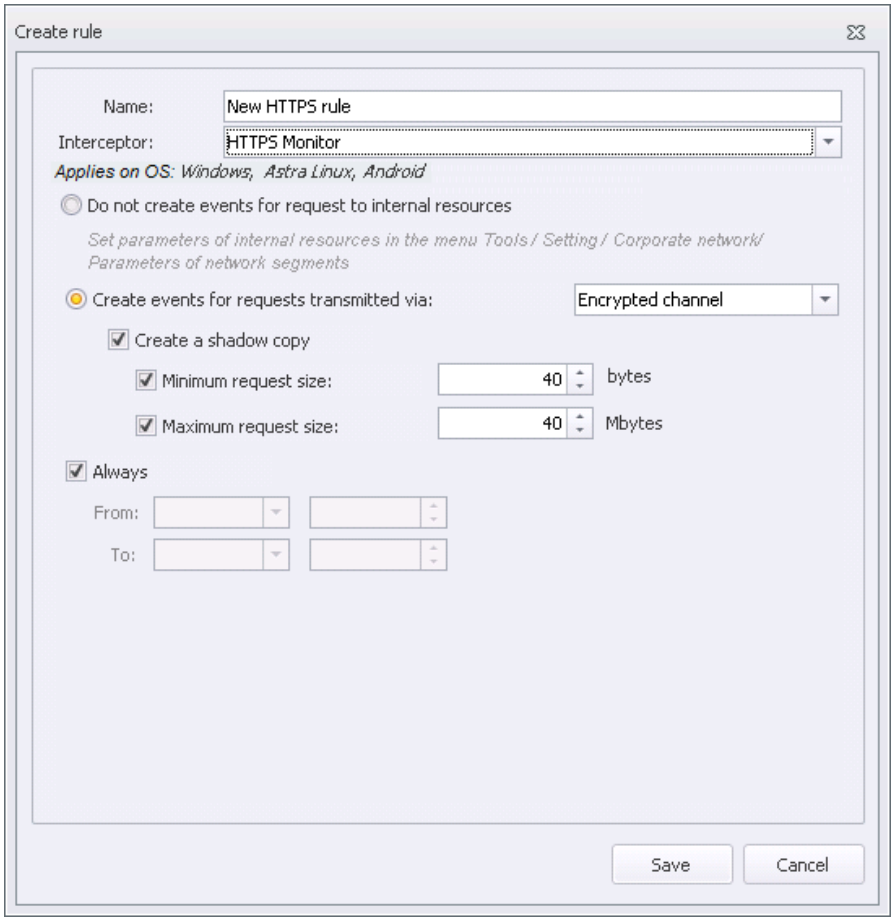
   If FTP Monitor rule (DM) should create a shadow copy of file but there is less free system drive space left than required by the policy (DM) (see "Creating Shadow Copies and Blocking Operations Due to Free Space Shortage") then shadow copies of messages still will be created but files will be sent without shadow copying.
8. Define a period of rule (DM) action. By default, the rule (DM) is always in effect (**Always** option is checked). To specify a period, clear **Always** check box and specify dates and time in **From** and **To** fields.
9. When all parameters are configured, click **Save**.

Configuring HTTPS Monitor Rule (DM)

HTTPS Monitor interceptor allows you to control data transfer through HTTP and HTTPS protocol.

Note:

The rule applies on computers with MS Windows and Astra Linux OS and mobile devices on Android platform.



To configure the rule, perform the following steps:

1. Go to **Policies** section.
2. In **Policies** area at Navigation pane, select a security policy (DM) which you want to add a rule (DM) to.
3. Take one of the following steps:
   - in the Main Menu, select **Edit > Create rule**;
   - click **Create rule** at the top of **Policies** area;
   - right-click at the empty space in **Policies** area and select **Create rule** from the drop-down list;
   - press Ctrl+Shift+N.
4. In **Create rule** dialog in **Interceptor** field, select **HTTPS Monitor**.
5. Enter rule (DM) name to the **Name** field.
6. Specify parameters of events which are created when traffic is intercepted. You can:
   - disable interception of events to internal resources. For this, select the **Do not create events for request to internal resources** option. Requests within the corporate network (on configuring network segments, see "Settings of Corporate Network", **Parameters of network segments** group) will not be intercepted.

Important!

If you select this mode, then creating a shadow copy in the rule will be unavailable. If you need to:
- not create events for requests to internal resources
and
- create shadow copies
then create two separate rules: a single rule for each requirement.

Important!

For mobile devices, traffic to internal resources cannot be excluded from interception.

- configure data interception via encrypted channels or via all channels. For this, select the **Create requests for events transmitted via** option and from the drop-down list select:
  - **All Channels**
  - **Encrypted channel**

  If you want to save shadow copies of sent files, select the **Create shadow copy** option. You can also specify additional settings for shadow copies:
  - **Minimum request size**. If the check box is selected, shadow copies will be enabled only for files of specified size or larger.
  - **Maximum request size**. If the check box is selected, shadow copies will be enabled only for files of specified size or smaller.

Important!

In case there is not enough space available on a Workstation (see. "Creating Shadow Copies and Blocking Operations Due to Free Space Shortage"), shadow copy will not be created.

7. Define a period of rule (DM) action. By default, the rule (DM) is always in effect (**Always** option is checked). To specify rule (DM) duration, clear **Always** check box and specify dates and time in **From** and **To** fields.
8. When all parameters are configured, click **Save**.

Specifics of applying the rule on computers with Astra Linux OS:

1. Connections via IPv6 protocol are not intercepted.
2. Requests related to webmail are intercepted similar to common HTTP requests.
3. Rules with the enabled setting **Do not create events for request to internal resources** are ignored.

Configuring IM Client Monitor Rule (DM)

IM Client Monitor interceptor lets to control employee access to instant messengers: Skype, WhatsApp, Jabber (XMPP protocol) and SMS.

Note:

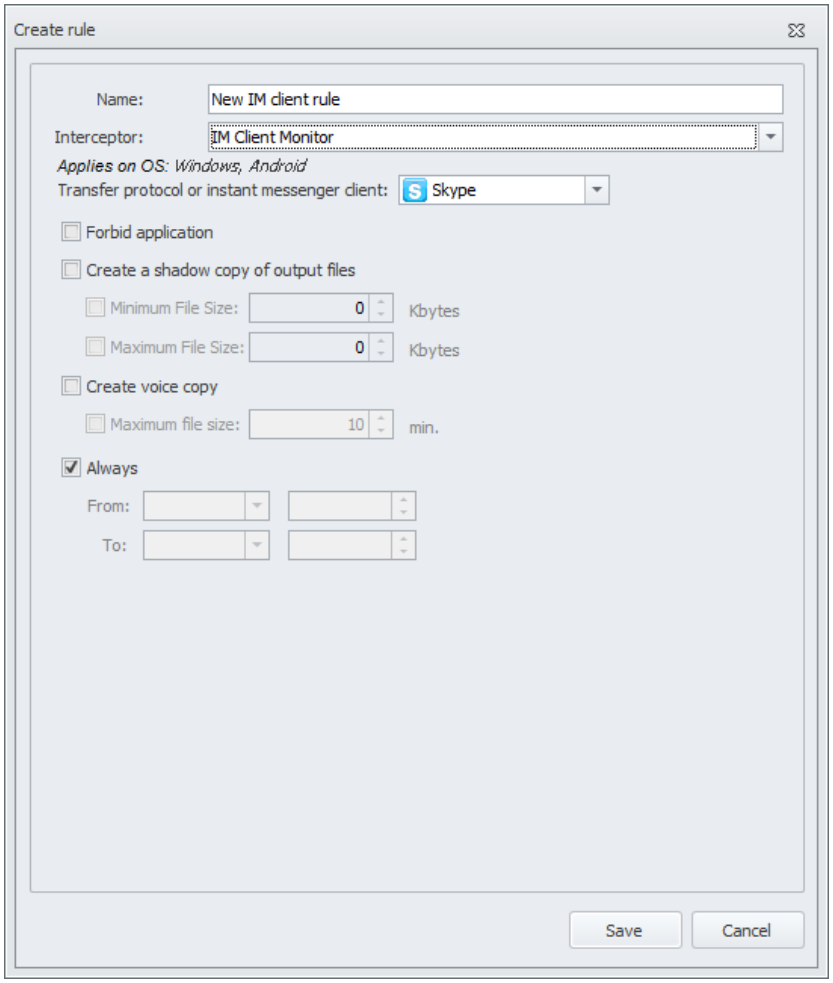
The rule applies on computers with MS Windows and mobile devices on Android platform.

Warning!

IM Client Monitor interceptor global settings (employee request to launch the interceptor, configuring chat shadow copying period) are configured along with general security policies (DM): see "Network Traffic Control".

Warning!

The file is subject to **IM Client Monitor** rule if **ALL** file parameters meet rule (DM) conditions **EXCEPT** maximum and minimum file size. **Maximum file size** and **Minimum file size** are taken into consideration only for shadow copying. So if the file size is within a specified range, then a file transfer event will contain a shadow copy; otherwise, the event will be created without a shadow copy.



To configure the rule, perform the following steps:

1. Go to **Policies** section.
2. In **Policies** area at Navigation pane select a security policy (DM) which you want to add a rule (DM) to.
3. Take one of the following steps:
   - in the Main Menu select **Edit > Create rule**;
   - click **Create rule (DM)** at the top of **Policies** area;
   - right-click at the empty space in **Policies** area and select **Create rule** from the drop-down list.
4. In **Create rule** dialog in Interceptor field select **IM Client Monitor**.
5. Enter rule (DM) name in the **Name** field.
6. In **Transfer protocol or instant messenger client** field, select messenger type which is controlled by this rule (DM):
   - Skype - to control Skype usage;
   - XMPP - to control Jabber usage;
   - SMS - to control mobile devices usage;
   - WhatsApp - to control WhatsApp usage on mobile devices.
7. In case it is required to intercept Skype voice messages, mark the **Create shadow copy of output files** checkbox and, if necessary, specify file size (sound file will be saved in *.ogg format)

- If **Maximum File Size** box is checked, then several events with shadow copies will be created for talks, whose length exceeds the specified value.

> **Note:**
>
> Voice traffic is not supported for a mobile version.

8. In case you want to entirely ban using Client of this type, mark the **Forbid application** checkbox (not available for **SMS of mobile connection** and **WhatsApp**).

> **Note:**
>
> To Skype, the setting applies as follows: the interceptor checks if the application is started and, if yes, forcibly closes it. The check is performed every minute.

> **Warning!**
>
> To forbid using WhatsApp and Skype mobile version, use Application Monitor Rule (DM) (see "Configuring Application Monitor Rule (DM)")

9. If you want to create and transfer shadow copies of transferred files to Traffic Monitor, mark the **Create shadow copy of output file** checkbox. In this case, you will be able to define additional parameters for these copies:
   - **Minimum File Size**. When checked, shadow copying will only be performed for files larger or equal in size.
   - **Maximum File Size**. When checked, shadow copying will only be performed for files smaller or equal in size.

> **Warning!**
>
> Shadow copy of chats and messages are always created (regardless of **Create shadow copy** setting), in case there is at least one **IM Client Monitor** active rule (DM) on the computer.
> The frequency of creating shadow copies from chats and messages (time period and the number of messages, which form a shadow copy) is described in the article "Network Traffic Control".

10. Define a period of rule (DM) action. By default, the rule (DM) is always in effect (**Always** option is checked). To specify rule (DM) duration, clear **Always** check box and specify dates and time in **From** and **To** fields.
11. When all parameters are configured, click **Save**.

Warning!

In case shadow copy of message or chat must be created in accordance with an active IM Client Monitor rule (DM), but there is less free space on a computer, than it was defined by a policy (DM) (see "Creating Shadow Copies and Blocking Operations Due to Free Space Shortage"), then shadow copies of the messages will be saved, but files will be transferred without shadow copy creation.

Configuring Mail Monitor Rule (DM)

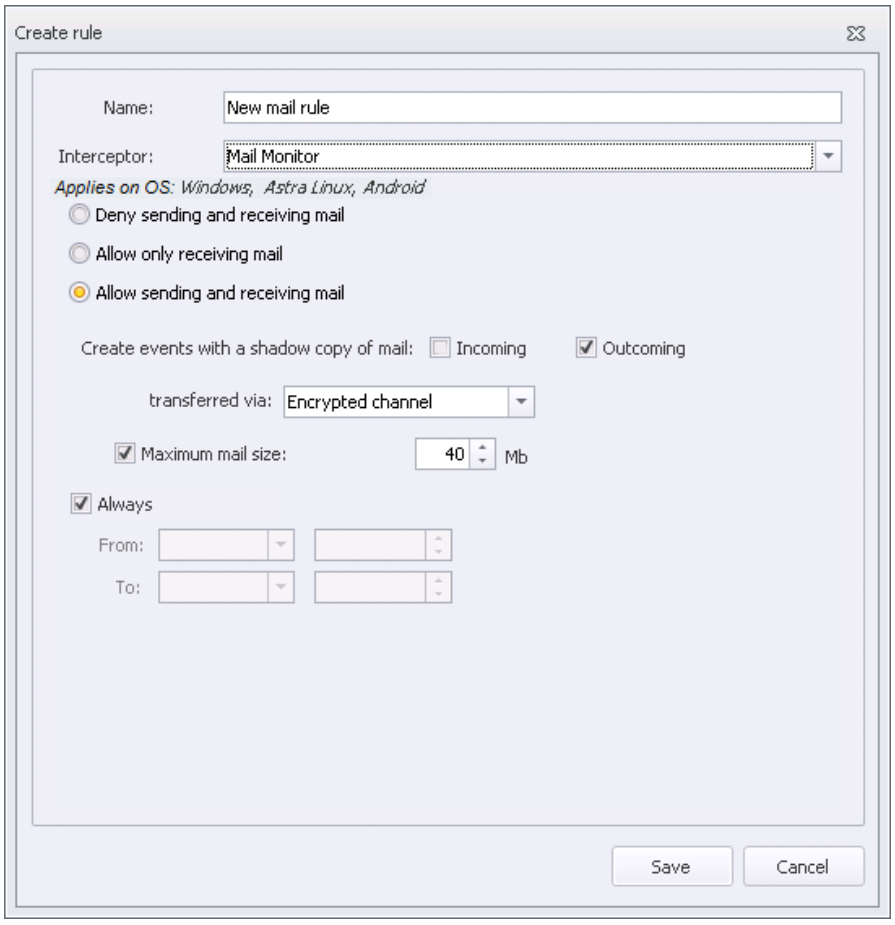
Mail Monitor interceptor provides full control of incoming and outgoing e-mail.

Mail Monitor allows control of SMTP, IMAP, POP3, MAPI mail protocols.

Important!

The rule applies on computers with MS Windows and Astra Linux OS and mobile devices on Android platform.

On computers with Astra Linux, the rule controls only SMTP, POP3, and IMAP protocols.



To configure the rule, perform the following steps:

1. Go to **Policies** section.
2. In **Policies** area at Navigation pane select a security policy (DM) which you want to add a rule (DM) to.

3. Take one of the following steps:
    - in the Main Menu select **Edit > Create rule**;
    - click **Create rule** at the top of **Policies** area;
    - right-click at the empty space in **Policies** area and select **Create rule** from the drop-down list;
    - press Ctrl+N.
4. In **Create rule** dialog in the **Interceptor** field, select **Mail Monitor**.
5. Enter the rule (DM) name to the **Name** field.
6. Choose the control level for sending and receiving emails:
    - **Deny sending and receiving mail**;
    - **Allow only receiving mail**;
    - **Allow sending and receiving mail**.

    > **Warning!**
    >
    > Depending on the outgoing and incoming mail control method, the following variants of shadow copy creation are possible:
    > - **Deny sending and receiving mail** -shadow copies are not being created;
    > - **Allow only receiving mail** - for incoming mail (for shadow copy creation, tick the **Incoming** box);
    > - **Allow sending and receiving mail** - for incoming and outgoing mail (for shadow copy creation, tick the **Incoming** and **Outcoming**).

7. Configure creation of shadow copies. Select the **Incoming** or **Outcoming** checkbox in the **Create events with a shadow copy of mail** line.

    > **Warning!**
    >
    > If the **Allow sending and receiving mail** option is enabled, then at least one mail direction (**Incoming** or **Outgoing**) should be selected, otherwise, the rule won't be saved.

    You can also define additional parameters of shadow copies:
    - **Transferred via**. Possible variants:
        - **All channels** - to create a shadow copy of emails sent through any channels;
        - **Encrypted channel** - to create a shadow copy of emails sent via encrypted channels.
    - **Maximum mail size**. If the option is enabled, shadow copies will be created only for emails whose size is smaller or equal to the specified one.

> **Warning!**
>
> If there is not enough free space on the workstation (see. "Creating Shadow Copies and Blocking Operations Due to Free Space Shortage"), a shadow copy will not be created.

8. Define a period of the rule (DM) action. By default, the rule (DM) is always in effect (**Always** option is checked). To specify the rule (DM) duration, clear **Always** check box and specify dates and time in **From** and **To** fields.
9. When all parameters are configured, click **Save**.

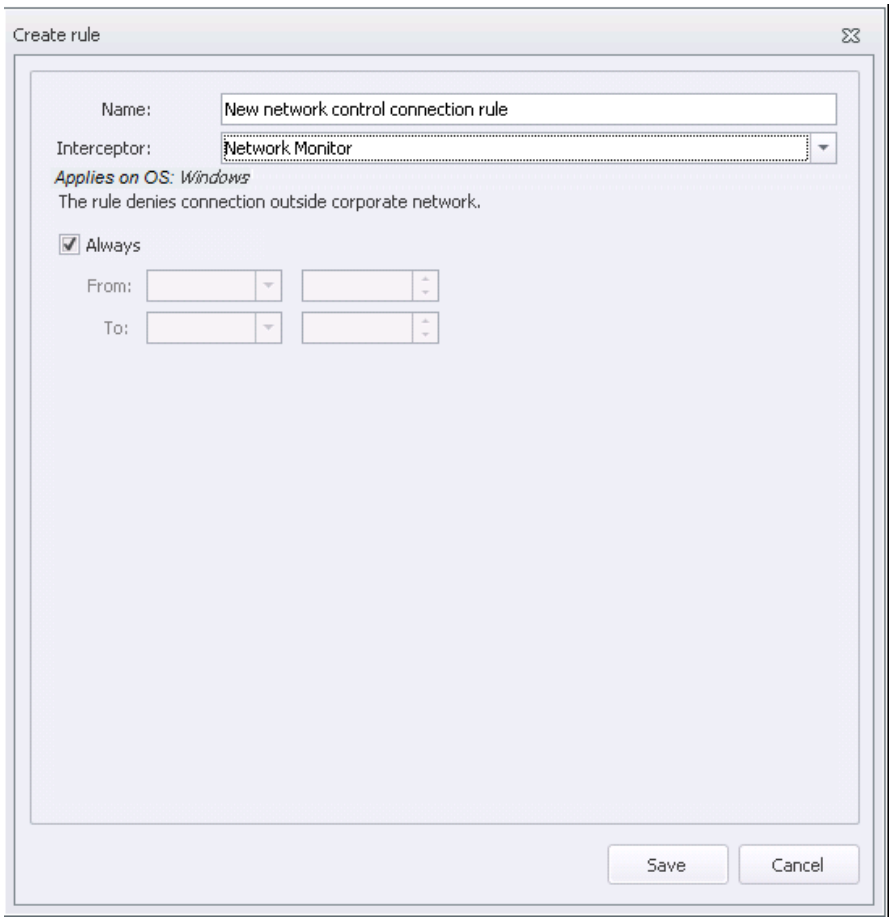
> **Warning!**
>
> In case existing rule (DM) has attributes:
>
> - **Allow sending and receiving mail**;
> - **Create events with a shadow copy of mail: Incoming and Outcoming, transferred via: All channels**
>
> and there is a saving mail on the mail server setting configured in the mailer, then each mail sending event will generate two interception objects: one of **Outcoming** type and other of **Incoming** type. The name of the mailer option might change depending on the program in use.

Configuring Network Monitor Rule (DM)

Network Monitor interceptor lets to deny transferring data by any network connections except connections with the corporate network or specified permitted servers. Configuring segments of the corporate network and permitted external addresses is performed as described in "Settings of Corporate Network".

> **Note:**
>
> The rule applies on computers with MS Windows OS.

> **Warning!**
>
> As at least one Network Monitor takes effect, Device Monitor Agent installed on the computer will try to approve DNS-names of opened internet pages. To prevent problems with external connections, it is required to configure forwarders usage on a corporate DNS-server (see internet article "Configure a DNS Server to Use Forwarders").



To configure the rule, perform the following steps:

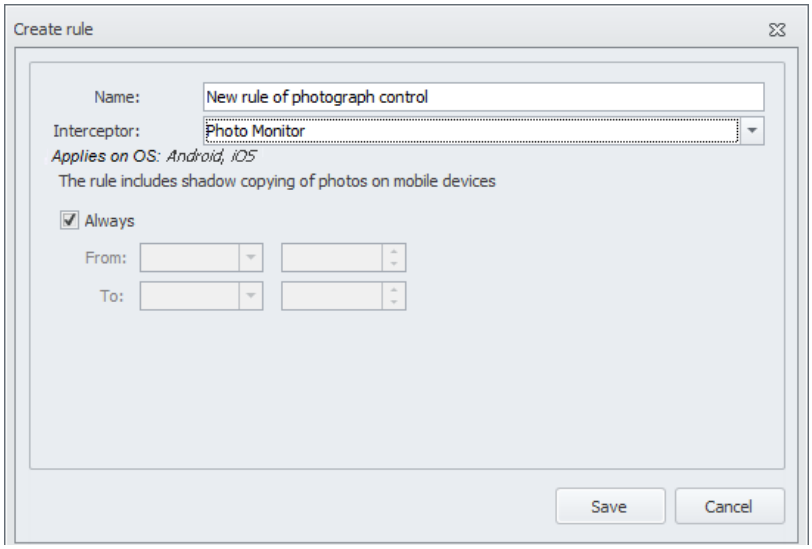
1. Go to **Policies** section.
2. In **Policies** area at Navigation pane select a security policy (DM) which you want to add a rule (DM) to.
3. Take one of the following steps:
   - in the Main Menu select **Edit > Create rule**;
   - click **Create rule** at the top of **Policies** area;
   - right-click at the empty space in **Policies** area and select **Create rule** from the drop-down list.
4. In **Create rule** dialog in Interceptor field select **Network Monitor**.
5. Enter rule (DM) name to **Name** field.
6. Define a period of rule (DM) action. By default, the rule (DM) is always in effect (**Always** option is checked). To specify rule (DM) duration, clear **Always** check box and specify dates and time in **From** and **To** fields.
7. When all parameters are configured, click **Save**.

Configuring Photo Monitor Rule (DM)

Photo Monitor interceptor allows you to perform shadow copying of photos taken with cameras of controlled mobile devices.

Note:

The rule applies on mobile devices on Android and iOS platforms.



To configure the rule, perform the following steps:

1. Go to the **Policies** section.
2. In **Policies** area at Navigation pane select a security policy (DM) which you want to add a rule (DM) to.
3. Take one of the following steps:
   - in the Main Menu select **Edit > Create rule**;
   - click **Create rule** at the top of **Policies** area;
   - right-click at the empty space in **Policies** area and select **Create rule** from the drop-down list;
   - press Ctrl+Shift+N.
4. In the **Create rule** dialog in the **Interceptor** field, select **Photo Monitor**.
5. Enter rule (DM) name to the **Name** field.

   Warning!

   If there is not enough free space on a workstation (see. "Creating Shadow Copies and Blocking Operations Due to Free Space Shortage"), a shadow copy will not be created.

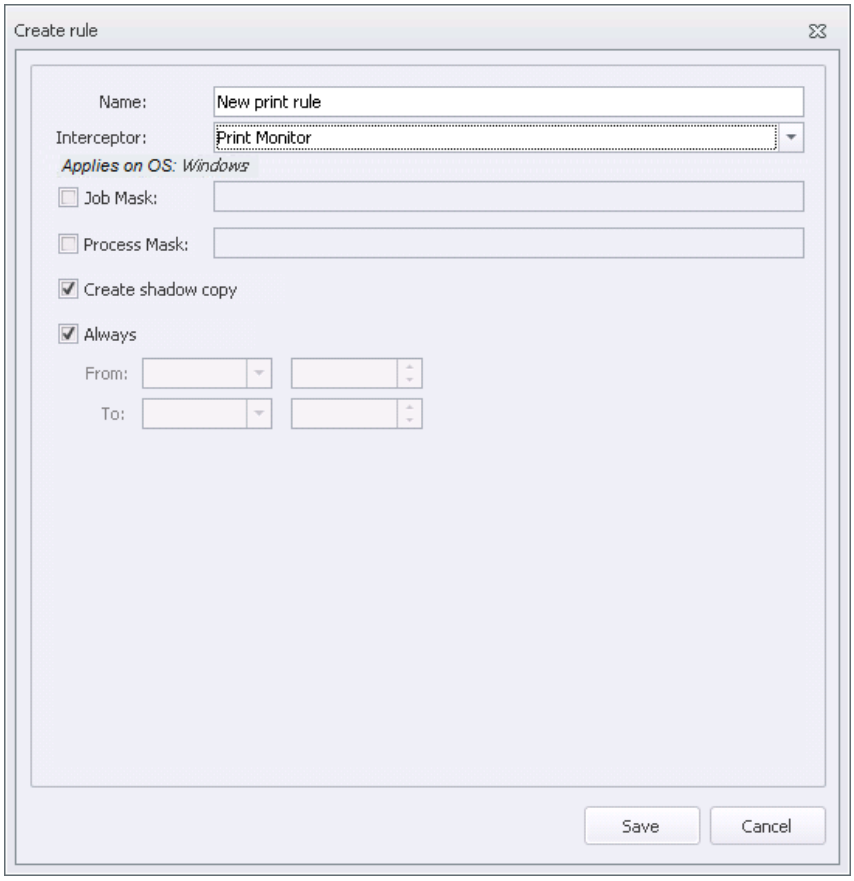
6. Define a period of rule (DM) action. By default, the rule (DM) is always in effect (**Always** option is checked). To specify rule (DM) duration, clear **Always** check box and specify dates and time in **From** and **To** fields.
7. When all parameters are configured, click **Save**.

Configuring Print Monitor Rule (DM)

Print Monitor interceptor allows you to perform monitoring of operations, which are connected with printing documents on local and network printers.

Note:

The rule applies on computers with MS Windows OS.



To configure the rule, perform the following steps:

1. Go to the **Policies** section.
2. In the **Policies** area at Navigation pane, select a security policy (DM) which you want to add a rule (DM) to.
3. Take one of the following steps:
   - in the Main Menu select **Edit > Create rule**;
   - click **Create rule** at the top of **Policies** area;
   - right-click at the empty space in **Policies** area and select **Create rule** from the drop-down list;
   - press Ctrl+Shift+N.
4. In the **Create rule** dialog in the **Interceptor** field, select **Print Monitor**.
5. Enter rule (DM) name to the **Name** field.
6. If necessary, you can limit controlled print tasks using masks:
   - **Job Mask**. A mask is used for a task (document) which is sent to print. If you want to set the mask, select the checkbox and specify the mask.
     The print task name is formed by the application, from which document is sent to print. So, the name can be any text, not necessarily related to the type of the document.
     In the mask, you can use substitution symbols: «?» to replace one character or «*» to replace several characters. Spaces are treated as a part of the task name.

- **Process Mask**. A mask is used for the process, which executes the print task. If you want to set a mask for a process, select the checkbox and specify the mask.
  The name (a full path) of the process is obtained for the process, in whose context rendering of the print task is performed. In some cases (local LPT- and COM-printers), printing subsystem can perform rendering in the context of the Print Spooler service. The path to the executable file of the service is `%SystemRoot%\system32\spoolsv.exe`.
  For the process name to be identified correctly, it is necessary to set the **Print directly to the printer** parameter in the printer properties (**Printer properties** > **Additionally**). Then, the task will be processed in the context of the application, from which the document is sent to print. However, in this case, printing will be synchronous, so you won't be able to work with the application until the document is printed.
  In the task mask, you can use substitution symbols: «?» to replace one character or «*» to replace character set. Spaces are treated as a part of the task name.

7. If you want to create shadow copies of printed documents and send them to Traffic Monitor, select the **Create shadow copy** checkbox.

   Warning!

   If there is less free space on the computer than required by the policy (DM) (see "Creating Shadow Copies and Blocking Operations Due to Free Space Shortage"), then the document will be printed without creating a shadow copy.

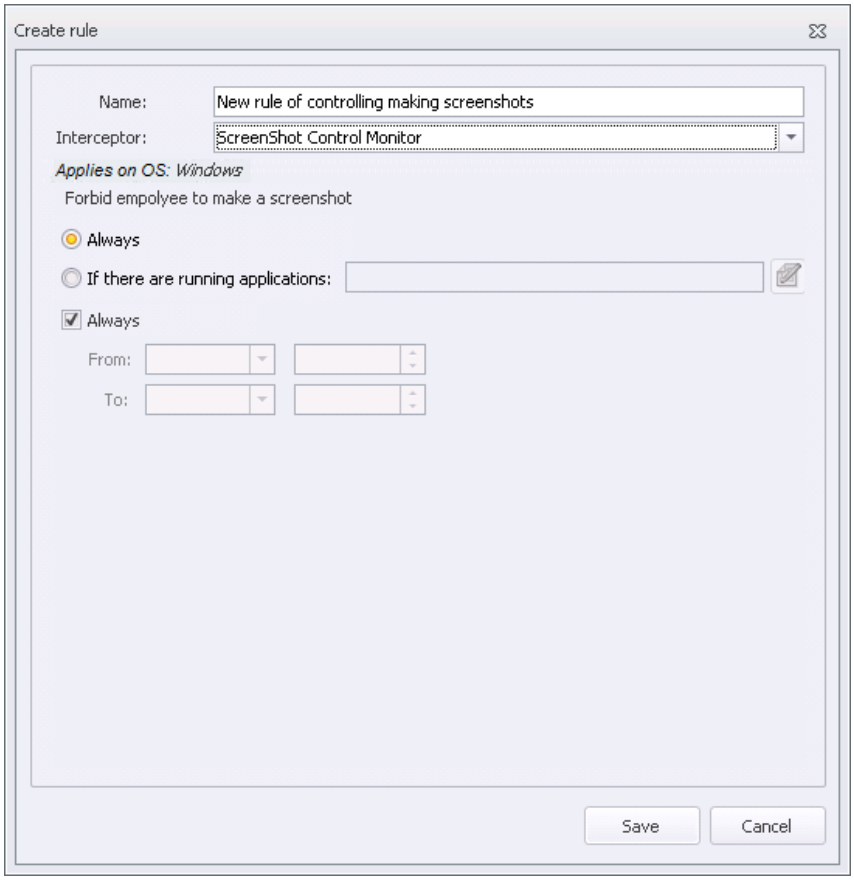
8. Define a period of rule (DM) action. By default, the rule (DM) is always in effect (**Always** option is checked). To specify rule (DM) duration, clear **Always** check box and specify dates and time in **From** and **To** fields.
9. When all parameters are configured, click **Save**.

Configuring ScreenShot Control Monitor Rule (DM)

ScreenShot Control Monitor interceptor allows you to control screenshots on the agent side.

Note:

The rule applies on computers with MS Windows OS.



To configure the rule, perform the following steps:

1. Go to **Policies** section.
2. In **Policies** area at Navigation pane, select a security policy (DM) which you want to add a rule (DM) to.
3. Take one of the following steps:
   - in the Main Menu, select **Edit > Create rule**;
   - click **Create rule** at the top of **Policies** area;
   - right-click at the empty space in **Policies** area and select **Create rule** from the drop-down list.
4. In **Create rule** dialog in **Interceptor** field, select **ScreenShot Control Monitor**.
5. Enter rule (DM) name to the **Name** field.
6. In **Forbid employee to make a screenshot** area, define a rule (DM) period::
   - **Always**. Has no time limit by default.
   - **If there are running applications**. Select this option to specify applications using button (see "Applications protocol").
7. Define a period of rule (DM) action. By default, the rule (DM) is always in effect (**Always** option is checked). To specify rule (DM) duration, clear **Always** check box and specify dates and time in **From** and **To** fields.
8. When all parameters are configured, click **Save**.

Configuring ScreenShot Monitor Rule (DM)

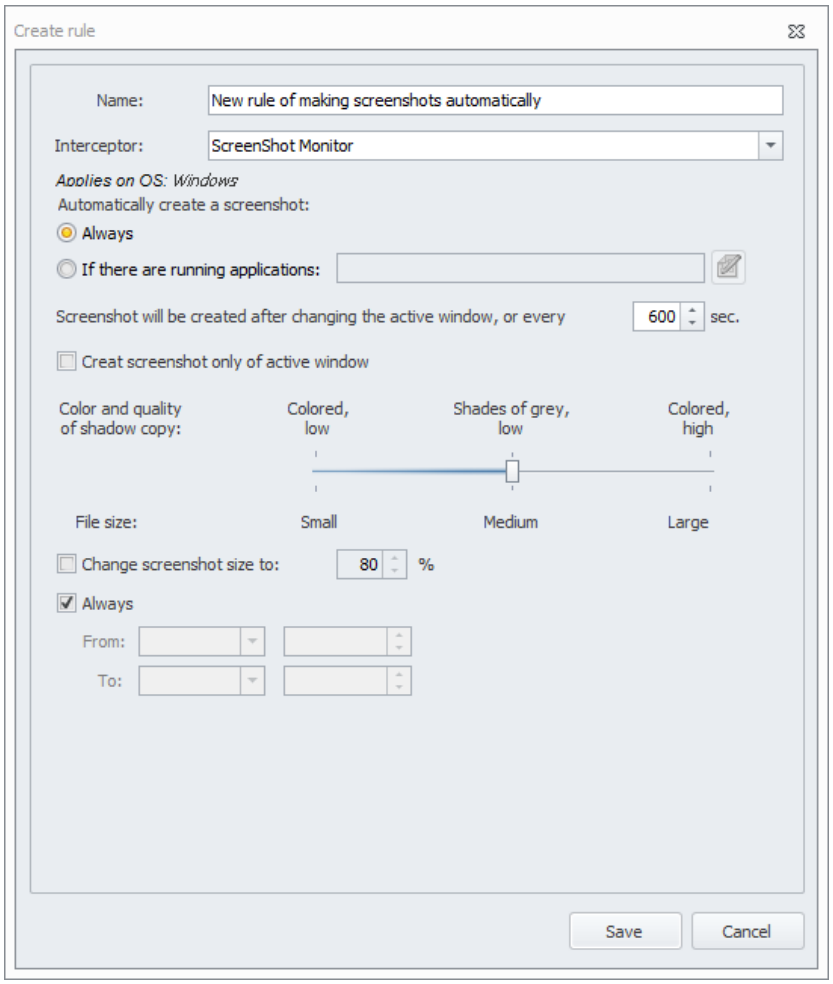
The **ScreenShot Monitor** interceptor allows you to automatically create screenshots on controlled computers.

Note:

The rule applies on computers with MS Windows OS.

Warning!

The **Do not create screenshots in case mouse or keyboard have been inactive for a long time** parameter, which defines how the rule works depending on the activity on controlled computers, is configured along with general security settings (see "Control of Applications and Screenshots").



To configure the rule, perform the following steps:

1. Go to **Policies** section.
2. In **Policies** area at Navigation pane, select a security policy (DM) to which you want to add a rule (DM).
3. Do either of the following:
   - in the main menu, select **Edit > Create rule**;
   - click **Create rule** at the top of **Policies** area;
   - right-click at the empty space in **Policies** area and select **Create rule** from the drop-down list.
4. In **Create rule** dialog in the **Interceptor** field, select **ScreenShot Monitor**.

5. Enter rule (DM) name to **Name** field.
6. In the **Automatically create a screenshot** area, define in which case the rule (DM) will be valid:
    - **Always**. Has no time limit by default.
    - **If there are running applications**. Pick a list of applications using  button (see "Application protocol").
7. Specify periodicity of screenshots creation (in seconds). The default value is 600. A screenshot is also created when the active window changes.
8. If necessary, mark the **Create screenshot only of active window** checkbox. By default, a picture of the whole screen is taken.
9. Choose the color mode and the quality of created copies. Available color modes:
    - **Colored, low**. A colored file in a low resolution. Use this mode, in case you need files of small size.
    - **Shades of gray, low**. A file in greyscale mode in a low resolution.
    - **Colored, high**. A colored file in a high resolution. Use this mode, when you need high-quality images regardless of their size .
10. If you need to decrease the file size while saving, mark the **Change screenshot size to** checkbox and specify the value in percent (the percentage is calculated from the original file size).
11. Define a period of rule (DM) action. By default, the rule (DM) is always in effect (**Always** option is checked). To specify the rule (DM) duration, clear **Always** check box and specify dates and time in **From** and **To** fields.
12. When all parameters are configured, click **Save**.

Editing a Rule (DM)

To edit a rule:

1. Go to **Policies**.
2. In **Policy** area of Navigation pane select the title of security policy (DM) that contains the rule (DM). The main window will display the full list of the policy (DM) rules (DM).
3. Select the row with the name of the rule (DM) you want to edit.
4. Take one of the following steps:
    - in Main Menu click **Edit > Edit Rule**;
    - double-click the selected row;
    - click  **Edit Rule** at the top of **Policy** area;
    - use **Ctrl+Shift+E** shortcut.
5. Edit rule (DM) parameters:
    - Configuring Application Monitor Rule (DM);
    - Configuring Clipboard Monitor Rule (DM);
    - Configuring Cloud Storage Monitor Rule (DM);
    - Configuring Device Monitor Rule (DM);
    - Configuring File Monitor Rule (DM);
    - Configuring FTP Monitor Rule (DM);
    - Configuring HTTPS Monitor Rule (DM);
    - Configuring IM Client Monitor Rule (DM);
    - Configuring Mail Monitor Rule (DM);
    - Configuring Network Monitor Rule (DM);
    - Configuring Photo Monitor Rule (DM);
    - Configuring Print Monitor Rule (DM);
    - Configuring ScreenShot Control Monitor Rule (DM);

- Configuring ScreenShot Monitor Rule (DM).

6. When all changes are made click **Save** in rule (DM) configuration dialog.

> **Warning!**
>
> To apply changes you have to save current security schema (see "Editing Security Scheme"). If you don't save your security schema, all changes will be discarded.

Deleting a Rule (DM)

To delete a rule:

1. Go to **Policies**.
2. In **Policy** area of Navigation panel select the name of security policy (DM) that contains the rule (DM). The main window will display the full list of the policy (DM) rules (DM).
3. Select the row that contains the rule (DM) you want to remove.

> **Note:**
>
> To delete multiple rules (DM) from a single security policy (DM), select the rows with the names of all rules (DM) you want to remove.

4. Take one of the following steps:
   - in Main Menu click **Edit > Delete Rule**;
   - use **Delete rule**, which is located in the upper part of **Policies** area;
   - click **Delete** button on a keyboard.
5. In request box select **Yes** to confirm that you want to remove the rule (DM).

> **Warning!**
>
> To apply changes you have to save current security schema (see "Editing Security Scheme"). If you don't save your security schema, all changes will be discarded.

Copying a Rule (DM)

Rules (DM) can be copied from one security policy to another.
To copy a rule:

1. Go to **Policies**.
2. In **Policy** area of Navigation pane, select the name of the security policy (DM) that contains the rule (DM) you want to copy.
3. In main screen workspace select the row that contains the name of the rule you want to copy. You can select multiple rows to copy group rules (DM) into a single security policy (DM).
4. Click and hold the selected row and drag the rule (DM) into **Policies** area of Navigation pane. Move the pointer over the title of security policy (DM) you are adding the rule (DM) to. Release the button when a yellow arrow appears next to the selected policy (DM).

This copies the rule (DM) to selected security policy (DM).

You can also copy rules (DM) from the dialog of editing the policy (DM) to which you want to add rules (DM) from other policies (DM).

To copy a rule while editing a policy:

1. Go to **Policies**.
2. In **Policy** area of Navigation pane, select the name of the security policy (DM) that you want to add a rule (DM) to.
3. Take one of the following steps:
    - in the Main Menu select **Edit > Edit Policy**;
    - click  **Edit Policy** at the top of Navigation pane;
    - press **Ctrl+E** on a keyboard;
    - double-click selected security policy (DM) name.
4. click **Select rules**. In new dialog flag the rules (DM) you want to copy to a new security policy (DM). You can select the whole policy (DM) - then all rules (DM) it contains will be added to editing security policy (DM).
5. After you mark all rules (DM) click **Select**.
6. Click **Save** to save policy (DM).

> **Warning!**
>
> To apply changes you have to save current security schema (see "Editing Security Scheme"). If you don't save your security schema, all changes will be discarded.

Employees

Employee and employee group management basics are available in "Employees and Employee Groups". Existing security policies (DM) can be assigned only to employee groups. Security policy (DM) for an employee is defined by including his/her account to the employee group.

> **Warning!**
>
> In addition to employee group security policy (DM), each employee is covered by workstation security policy (DM). Information about rule (DM) conflict resolving see in "Applying Rules (DM)".

To go to Console (DM) section designed for accounts management, click **Employees** button on Navigation pane.

Guidelines on account management is available in:

- Viewing Employee Details;
- Viewing Resultant Policy and Resultant White List for an employee;
- Adding and Editing an Employee Group;
- Deleting Employee Group;
- Adding Employee Account to a Group;
- Editing Employee Account;
- Removing Employee Account from Employee Group;
- Deleting Employee Account from Security Schema.

Viewing Employee and Employee Groups Details

Employees area of Navigation pane displays employee group list. Selected employee group employees are listed in the main window work pane.

> **Note:**
>
> Use additional features to adjust employee list view (see "Additional Features").

To view information for specific employee group,
select group name in employee group list.
To view all registered employees information,
click **Show All Employees** at the top of Navigation pane.
Employee account information is represented as tabular list. Each row in the list contains a single account. Columns contain accounts' general properties. Extended information on each account is available in **Details** panel.

To view account's detailed properties,
select the row that contains the account name.
Details panel displays table properties including the following information:

- **Account**. Account name.
- **Last Name**, **First Name**, **Middle Name**. Account owner's last, first and middle name.
- **SID**. Operating System internal ID.

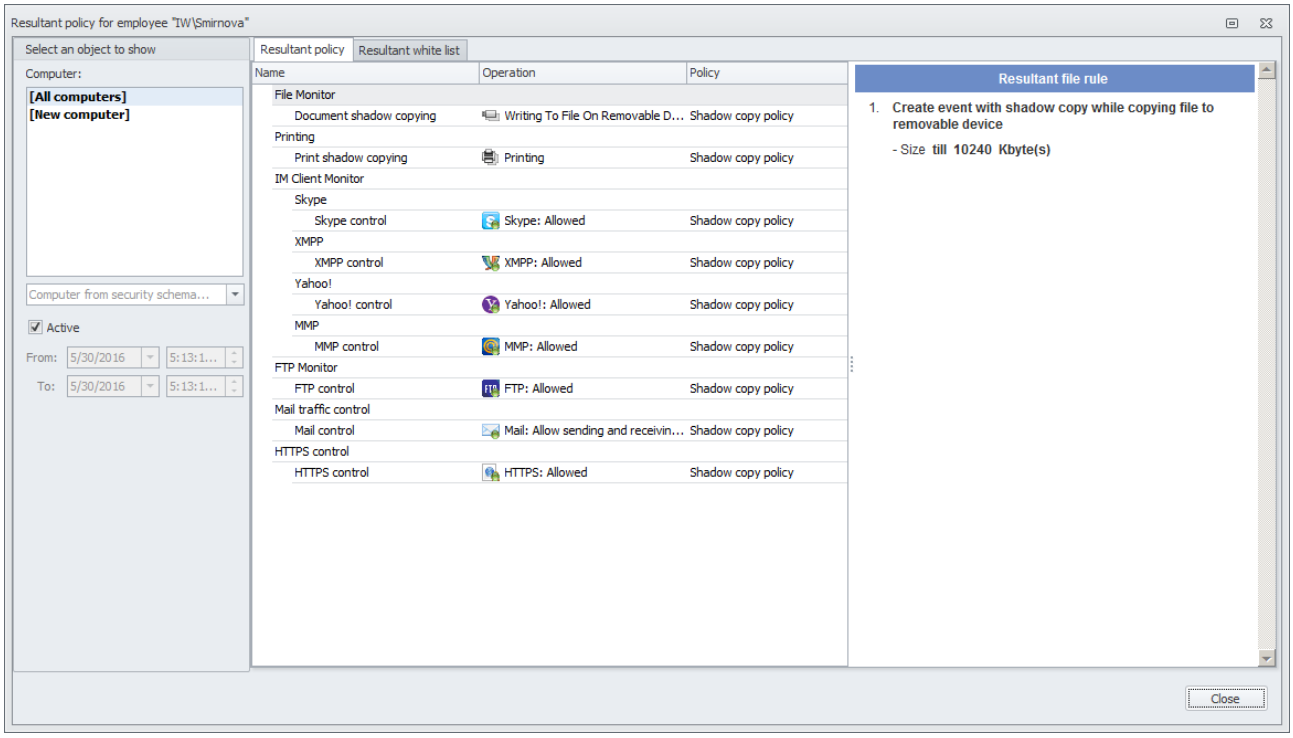
> **Note:**
>
> Some information on **Details** panel is duplicated in the main screen workspace.

Viewing Resultant Policy (DM) and Resultant White List for an employee

To view information about policy for an employee:

1. In the **Employee** list, pick an employee you want to view policy (DM) and white list for.
2. Proceed with one of the following actions:
    - in the Main Menu choose **Edit -> Show effective policy**.
    - on **Employees pane** click **Show effective policy**.

As a result, a window **Resulting policy for employee<employee name>** will be displayed**:** where by default all resulting policies (DM) for all employees on the chosen computer are displayed.



The main window **Resulting policy for employee<computer name>** area contains three tabs:

- **Resultant policy** - rules (DM) are displayed, that are resulting on a computer. Resulting policy (DM) folds from rules (DM), configured by default, rules (DM), applied for this computer and rules (DM) for computer's users (see "Device Monitor Rules (DM) Application"). To see detailed information about a rule (DM), select it from the list: detailed information will be displayed on the panel on the right.
- **Resultant white list** - displays devices, which are allowed for computer (see "White lists"). To see detailed information about device, select it from the list: detailed information will be displayed on the panel on the right.

On a Workstation pane:

- **All Workstations** - resulting policy (DM) for an employee account without attachment to a workstation.
  Note: to view resulting policy (DM) of an employee for a definite workstation, pick a workstation from Workstation pane or drop-down list Workstations from security schema.
- **New workstation** - resulting policy (DM) for an employee on a new workstation (it is not yet present in the security schema).
- To see resulting policy (DM) for chosen user on a definite computer:
  - from the **Computer** list, choose the name of the computer, on which chosen account is registered

  or
- from the **Computer from seciruty schema** drop-down list choose any account on computer, which is registered in the System (see "Computers").

You can choose time period for resulting policy/white list:

- Default setting is **Active** and current resulting policies (DM) and white list is displayed;
- To see resulting policy/white lists for chosen emloyee for defined period, untick the **Active** checkbox and specify time period.

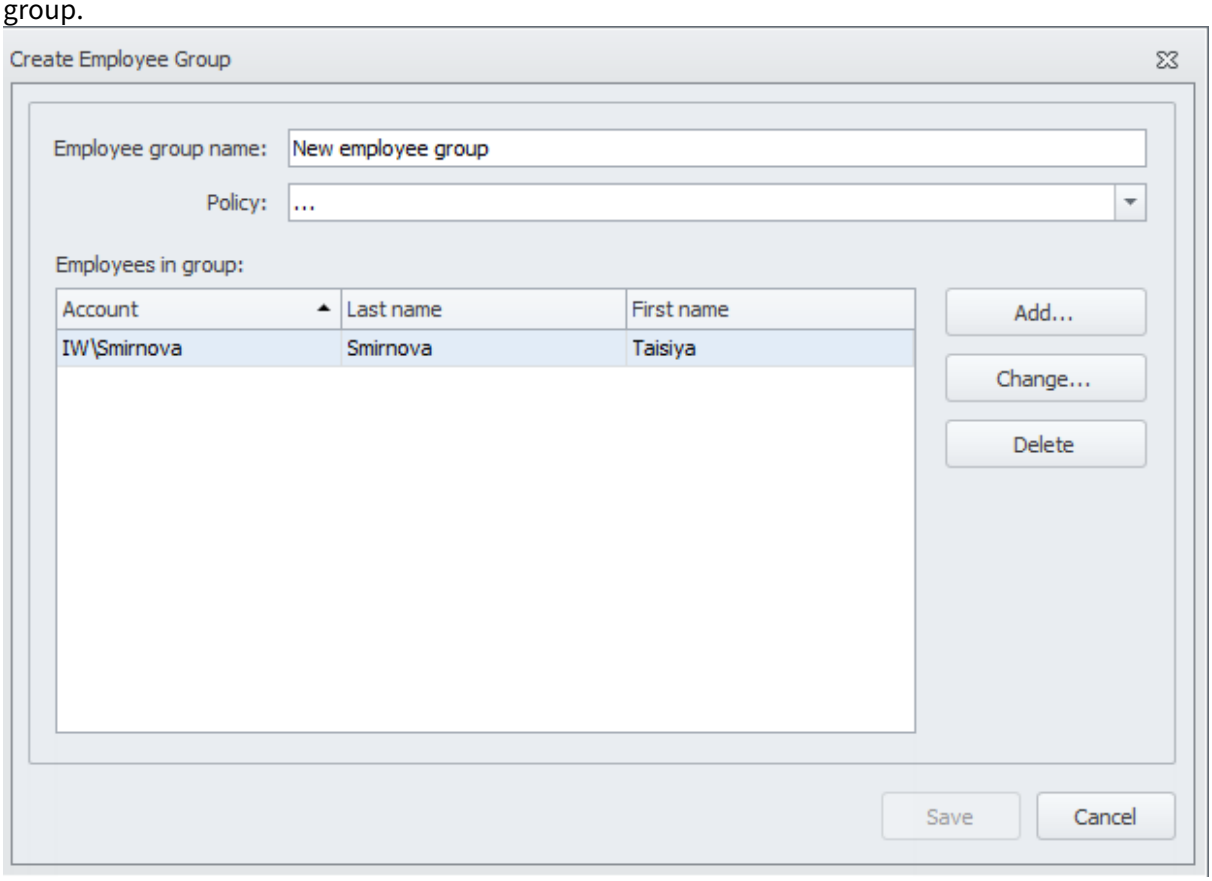
Adding and Editing an Employee Group

To add or edit an employee group:

1. Go to **Employees** section.
2. Take one of the following steps:

Action	Steps
Add employee group	• select **Edit > Create Employee Group** in the Main Menu; • click **Create Employee Group** at the top of the Navigation Pane.
Edit employee group	a. I**n Employees** area of Navigation Pane select the employee group name. b. Take one of the following steps: • in the Main Menu, click **Edit > Edit Employee Group**; • click **Edit Employee Group** at the top of Navigation pane; • double-click selected employee group name.

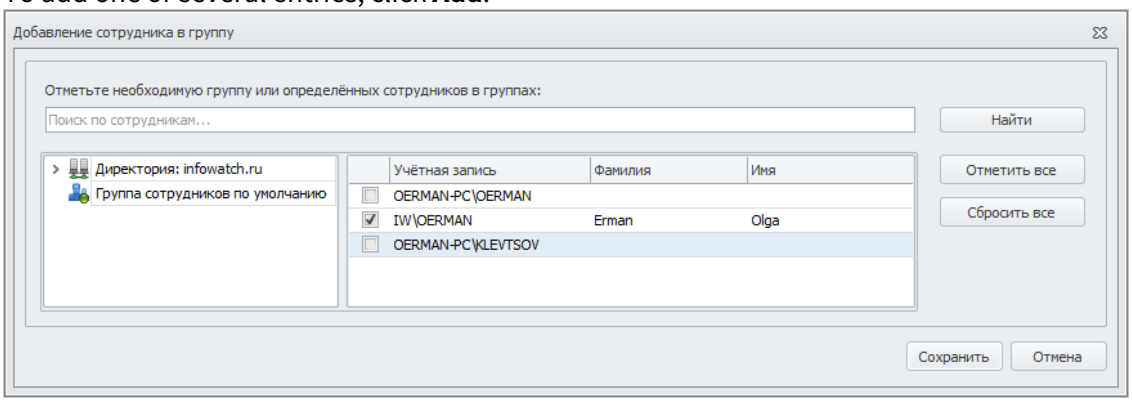
As a result of any of these actions, a dialog window will appear to define parameters of employees group.



3. Specify the following parameters:
   - **Employee group name**. Name of employees group.

- **Policy**. Choose security policy (DM) from the drop-down list, which will be applied to this employee group.

4. Determine the list of employees in the group:
   - To add one or several entries, click **Add**.



   The **Add employee to the group** dialog displays a list of accounts imported from the directory service (see "Connecting to LDAP Server and synchronization with Active Directory and Astra Linux Directory") and already registered in the System (for example, when Device Monitor Agent was installed to the workstation) and belonging to existing Device Monitor employee groups. To add an employee, in left pane select a node in groups tree, then flag accounts you want to add to the edited group. To flag all accounts of selected node, click Mark all. To clear selection, click Clear all.
   You can also make a search of account by all available elements: enter a part of account name to the field at the top and click Find. After you selected all needed accounts, click Save to close Add employee to the group dialog and return to a dialog box with group parameters. To edit account parameters, select it from the list of employees belonging to the group and click Change (see "Editing Employee Account").
   - To edit account parameters, select it from the list of employees belonging to the group and click **Change** (see "Editing Employee Account").
   - To delete an entry from the group, select it and click **Delete**.

5. Click **Save**.

> **Warning!**
>
> To apply changes you have to save current security scheme (see "Editing Security Scheme"). If you don't save your security schema, all changes will be discarded.

Deleting Employee Group

To delete employee group:

1. Go to **Employees** section.
2. Click the employee group you want to delete.
3. Take one of the following steps:
   - select **Edit > Delete Employee Group** in the Main Menu;
   - click **Delete Employee Group** at the top of **Navigation Pane**.
4. Click **Yes** in confirmation box to confirm that you want to remove employee group.

Warning!

To apply changes you have to save current security schema (see "Editing Security Scheme"). If you don't save your security schema, all changes will be discarded.

Adding Employee Account to a Group

After InfoWatch Device Monitor Agent is installed on the workstation (see document "*InfoWatch Traffic Monitor. Installation guide*" "InfoWatch Device Monitor Agent Setup" article), data on all employees registered at it is automatically added to the Device Monitor security scheme, "Default" employee group. Therefore the policy (DM) assigned to "Default" employee group will be applied to all newly registered employees. In prospect security policy (DM) for an employee is defined by including its account to different employee groups.

To move an employee account from one group to another:

1. Go to **Employees** section.
2. In **Employees area** of Navigation pane select a group containing employee's entry.
3. In **Employees** area of the main screen, select an account which you want to add to another group. Left-click and hold the selected row and drag it to **Employees** area of Navigation pane. Move the cursor over the name of the group you want to add an account to. When a yellow arrow appears at the left of selected group, release left mouse button.

This adds an account to the selected group.

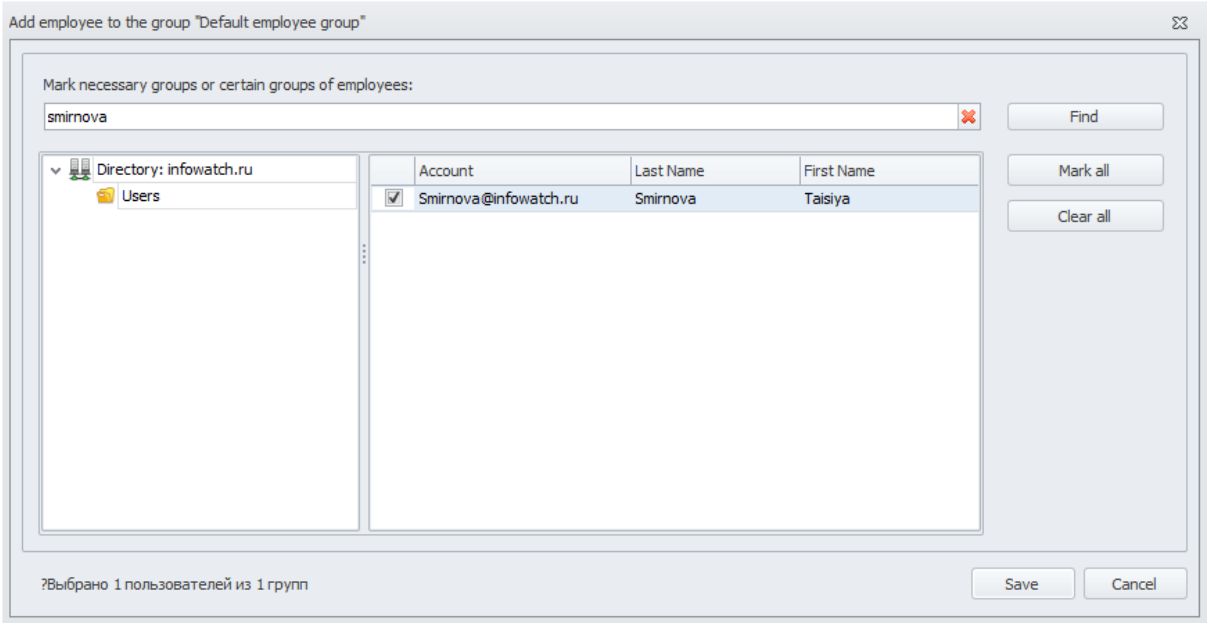
You can also manually import an information on the employee from directory service (see connection configuring description in "Connecting to LDAP Server and synchronization with Active Directory and Astra Linux Directory"). Then after this employee is registered at the workstation where InfoWatch Device Monitor Agent installed, this employee will be subject of policy (DM) of a group where the employee is added to.

To add one or several accounts to employee group:

1. Go to **Employees** section.
2. In **Employees** area of Navigation pane, select a group to which you want to add the employee's account.
3. Take one of the following steps:
   - in the Main Menu, click **Edit > Add Employee**;
   - click **Add Employee** at the top of **Employees** area;
   - right-click in Employees area and select **Add Employee** from the drop-down list;

   The **Add employee to the group** dialog displays a list of accounts imported from the directory service (see "Connecting to LDAP Server and synchronization with Active Directory and Astra Linux Directory") and already registered in the System (for example, when Device Monitor Agent was

installed on the workstation) and belonging to existing Device Monitor employee groups.



4. To add an employee, in left pane select a node in groups tree, then flag accounts you want to add to edited group.
   To flag all accounts of selected node, click **Mark all**. To clear selection, click **Clear all**.
   You can also search for the account by all available elements: enter a part of account name to the field at the top and click **Find**.
5. After you selected all needed accounts, click **Save** to close **Add employee to the group** dialog and return to a dialog box with group parameters.
6. Click **Save**.

> **Warning!**
>
> To apply changes you have to save current security scheme (see "Editing Security Scheme"). If you don't save your security schema, all changes will be discarded.

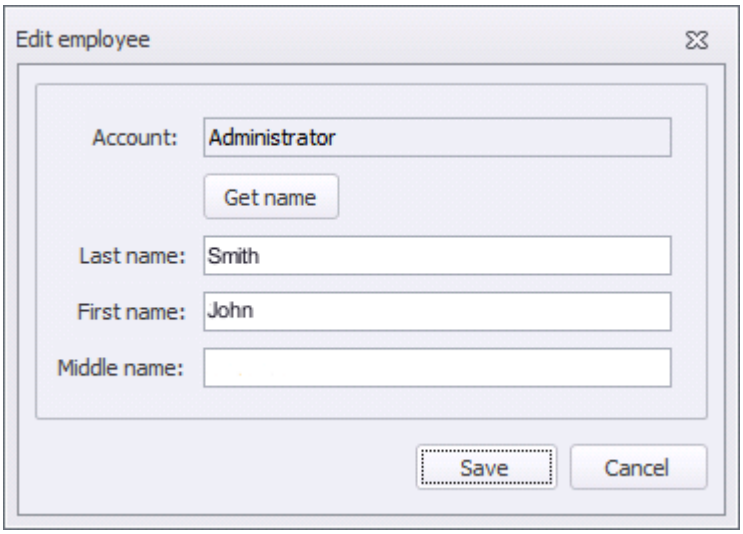
Editing Employee Account

Parameters of employee account are imported from directory service or while installing InfoWatch Device Monitor Management to the computer where this employee is registered. If you want to add some information, you can enter employee's personal data as described below.

To edit an employee account:

1. Go to **Employees** section.
2. In **Employees** area of Navigation pane, select the group the account belongs to.
3. Select the row that contains the name of the account you want to edit.
4. Take one of the following steps:
   - in the Main Menu, click **Edit > Edit Employee**;
   - click **Edit Employee** at the top of **Employees** area;

- double-click the selected row.



5. In the **Edit employee** dialog window, you can modify the following optional parameters: **Last Name**, **First Name**, and **Middle Name**. You can either enter new values into appropriate fields manually or import them from directory service with **Get name** button.
6. Click **Save**.

Warning!

To apply changes you have to save current security scheme (see "Editing Security Scheme"). If you don't save your security schema, all changes will be discarded.

Removing Employee Account from Employee Group

To remove an account from employee group:

1. Go to **Employees** section.
2. In **Employees** area of Navigation pane select employee group the account belongs to.
3. Select the row that contains the name of the account you want to remove from this group.

Note:

To remove multiple accounts from a group, select the rows with employee's accounts you want to exclude from this group.

4. Take one of the following steps:
   - In the Main Menu, click **Edit > Remove** employee from group;
   - click **Remove employee** from group at the top of **Employees** area;
   - press **Delete** keyboard button.

This removes employee account from selected employee group.

Note:

If employee account belongs to a single employee group, then after excluding it will be automatically added to default employee group.

Warning!

To apply changes you have to save current security schema (see "Editing Security Scheme"). If you don't save your security schema, all changes will be discarded.

Deleting Employee Account from Security Schema

To remove employee account from security schema:

1. Go to **Employees** section.
2. In **Employees** area of Navigation pane select employee group the account belongs to.
3. Select the row that contains the account you want to remove.

   Note:

   To remove multiple accounts from security schema, select all the rows that contain the accounts you want to remove.

4. Take one of the following steps:
   - In the Main Menu, click **Edit > Delete employee from security schema**;
   - click  **Delete employee from security schema** at the top of **Employees** area;
   - press **Shift+Delete** at the keyboard.
5. In the confirmation box click **Yes** to confirm that you want to remove the account.

Warning!

To apply changes you have to save current security schema (see "Editing Security Scheme"). If you don't save your security schema, all changes will be discarded.

Computers

In InfoWatch Device Monitor, a computer is a controlled computer where InfoWatch Device Monitor Agent is installed.

General principles of managing computers are described in "Computers and Computer Groups" section.

Active security policies (DM) can be applied only to a computer group. You can define a security policy (DM) for a certain computer by including it to a computer group.

Warning!

To each computer, both a security policy (DM) of the computer group and a security policy (DM) of the employee who is currently authorized on the computer apply. For information on resolving conflicts between rules (DM), see "Rules Application".

To go to Management Console (DM) section where you can manage computers, click **Computers** button on Navigation pane.

For more information on working with controlled computers, see:

- Viewing Computer Details
- Viewing Computer Effective Policy
- Adding and Editing a Computer Group
- Deleting Computer Group
- Adding Computer to a Group
- Removing Computer from a Group
- Deleting Computer from Security Schema
- Updating Agents on managed computers
- Diagnostics

On how to install the Agent on a mobile device or uninstall it, see "Mobile devices".

Viewing Computer Details

In **Computers** area of Navigation pane displays a list of computer groups. Main screen workspace displays the list of computers in selected computers group.

Note:

Use additional options to adjust computers list display (for details, see "Additional Features").

To view the list of computers that belong to a separate group, on the panel **Computers** choose the name of the required group: a list of computers included in the group will be displayed in the working area.

To view a full list of registered workstations, click **Show All Computers** at the top of Navigation pane.

Computer information is displayed in a tabular list. Each row in the list contains a computer (row starts with) or a mobile device (row starts with) . Columns contain basic computer properties.

Tabular list contains the following basic information:

- **Name.** Domain name of the computer.
- **Status**. Managed computer and Agent status. This parameter may have the following values:
  - **Works properly**. Managed computer is enabled, Agent is running.
  - **Inactive**. Managed computer is disabled or unavailable for a long time. The same status is displayed if the Agent is uninstalled from the managed computer.
- **Installed**. Date and time of computer Agent's first access to the server.
- **Established**. Date and time of Agent launch on the computer.
- **Accessed**. Date and time of computer Agent's last access to the Server.
- **Schema version**. Agent's current security schema version number.
- **Agent version**. Agent version number.

- **Operation system**. Operation system version.
- **Comment.** Field to type in a comment.
- **IP address**. IP address of the computer.
- **User.** The name of the user who logged to the computer last.

Extended information on each workstation is available in **Details** panel.

To view properties of a separate computer, choose a row with the description of the required computer in working area of the main window.
Details panel will display table of properties with the following workstation data:

- **Type.** Type of computer - displayed only for stationary or mobile computers.
- **Model name**. Model of mobile device - displayed for mobile devices only.
- **Settings**. Common security policy (DM) settings version number (see "General System Settings").
- **Version of network control settings**. Data transmission through network connections with the help of Network Monitor control version (see "Settings of Corporate Network").
- **Configuration version of network applications control**. Version of network traffic control configuration, using protocols YMSG,XMPP, MMP, FTP, FTPS, SMTP/MAPI/POP3, HTTPS (see "Settings of Corporate Network").
- **Configuration version of excluded applications control**. Version number of application exclusion settings (see "Exclusion of Application from Interception"). In brackets, the last application version number is specified.
- **Free disk space on computers**. Free space size on disks, where shadow copies are saved (i.e in percentages) and the minimum allowable size of this space.

Warning!

If there is at least one valid rule (DM) that allows shadow copying, and there is less free space on the host drive than specified by the policy (DM) (see "Creating Shadow Copies and Blocking Operations Due to Free Space Shortage"), no data will be printed or written to removable media: even if these steps aren't covered by any rule (DM).

Note:

Information retrieved from some attributes is duplicated in the main screen workspace.

Each registered workstation is automatically added to "default" workstation group. At the same time, "default" workstation group security policy (DM) is assigned to the new workstation.

You can do the following as you work:

- manage computer groups:
  - add computer groups;
  - edit computer group parameters;
  - delete workstation groups.
- manage computers:
  - add computers' information to computer groups and thus define computer security policy;
  - remove computers from workstation group;
  - delete computer from security schema;
  - update Agents at managed computers.

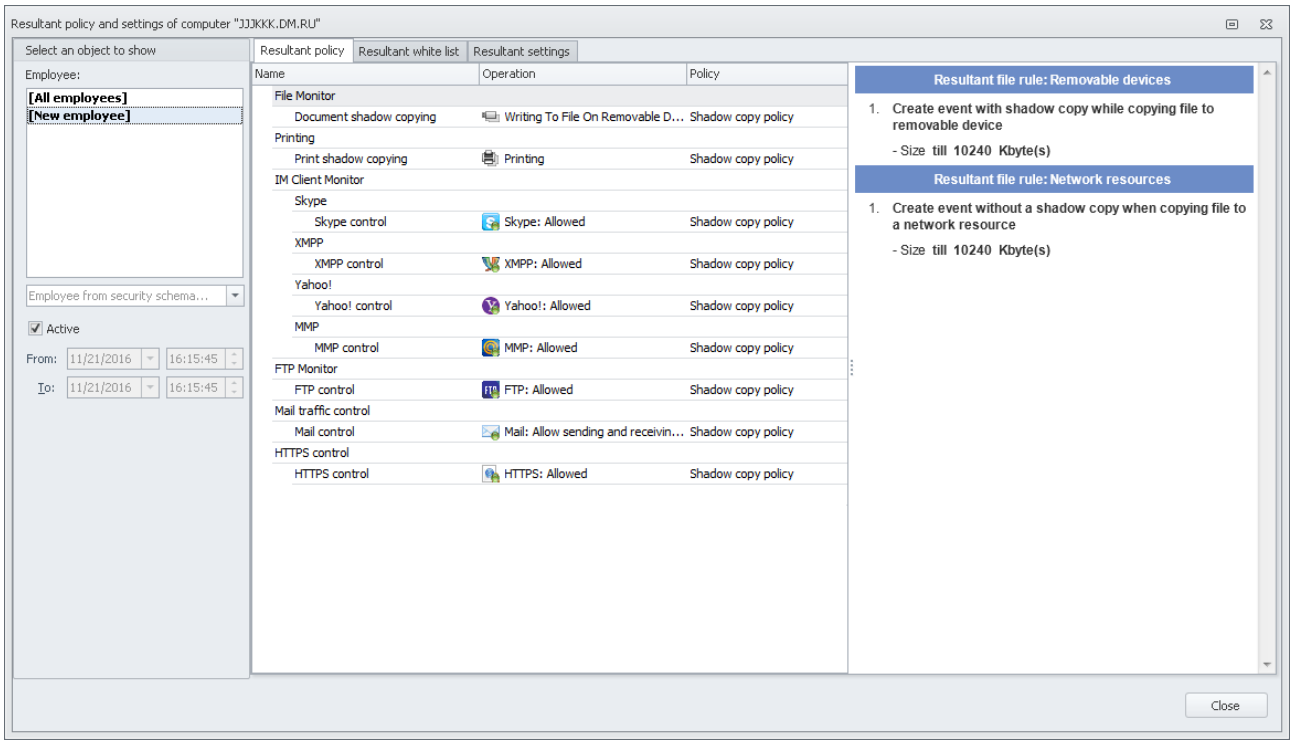
For more information on installing and deleting Agents for mobile devices see "Mobile devices".

Viewing Resultant Policy (DM) and Resultant White List for Computer

To view information about policy for computer:

1. In the **Computers** list, choose the required one:
2. Proceed with one of the following actions:
    - in the Main Menu choose **Edit -> Show settings and resultant policy**.
    - on **Computers** pane, click **Show settings and resultant policy**.

As a result, a window **Show settings and resultant policy <computer name>** will be displayed**:** where by default all resulting policies (DM) for all employees on the chosen computer are displayed.



The main window **Resulting policy for employee<computer name>** area contains three tabs:

- **Resultant policy** - rules (DM) are displayed, that are resulting on the computer. Resulting policy (DM) folds from rules (DM), configured by default, rules (DM), applied for this computer and rules (DM) for computer's users (see "Device Monitor Rules (DM) Application"). To see detailed information about a rule (DM), select it from the list: detailed information will be displayed on the panel on the right.
- **Resultant white list** - displays devices, which are allowed for the computer (see "White lists"). To see detailed information about the device, select it from the list: detailed information will be displayed on the panel on the right.
- **Resultant settings** - settings of Sending data to the agent speed and Control disk space on agent, which are resultant on the computer, are displayed. Resultant settings consist of default settings and settings for computer group, which includes the selected computer. (see "Common Settings for Agents" and "Adding and Editing an Employee Group").

On the **Employee** pane, you can choose object for review:

- **All Employees** - when chosen, resulting policy\white list\settings for all employees are displayed, regardless of who is logged on the selected computer.

- **New Employee** - when chosen, resulting policy\white list\settings for all employees are displayed for a new employee (which is not yet registered in security scheme).
- To view resulting policy\white list\settings for a definite user:
    - Choose the account name, registered on chosen computer from **Employee** list

  or
- From **Employee** drop-down list in the security scheme, choose any account, which is registered in the System (see "Employees").

You can, as well, choose period for resultant policy/white list/settings to be displayed:

- tick **Active** box, to view current resultant policy/white list/settings for an employee;
- untick **Active** box, to view resultant policy/white list/settings for a definite period.

Adding and Editing a Computer Group

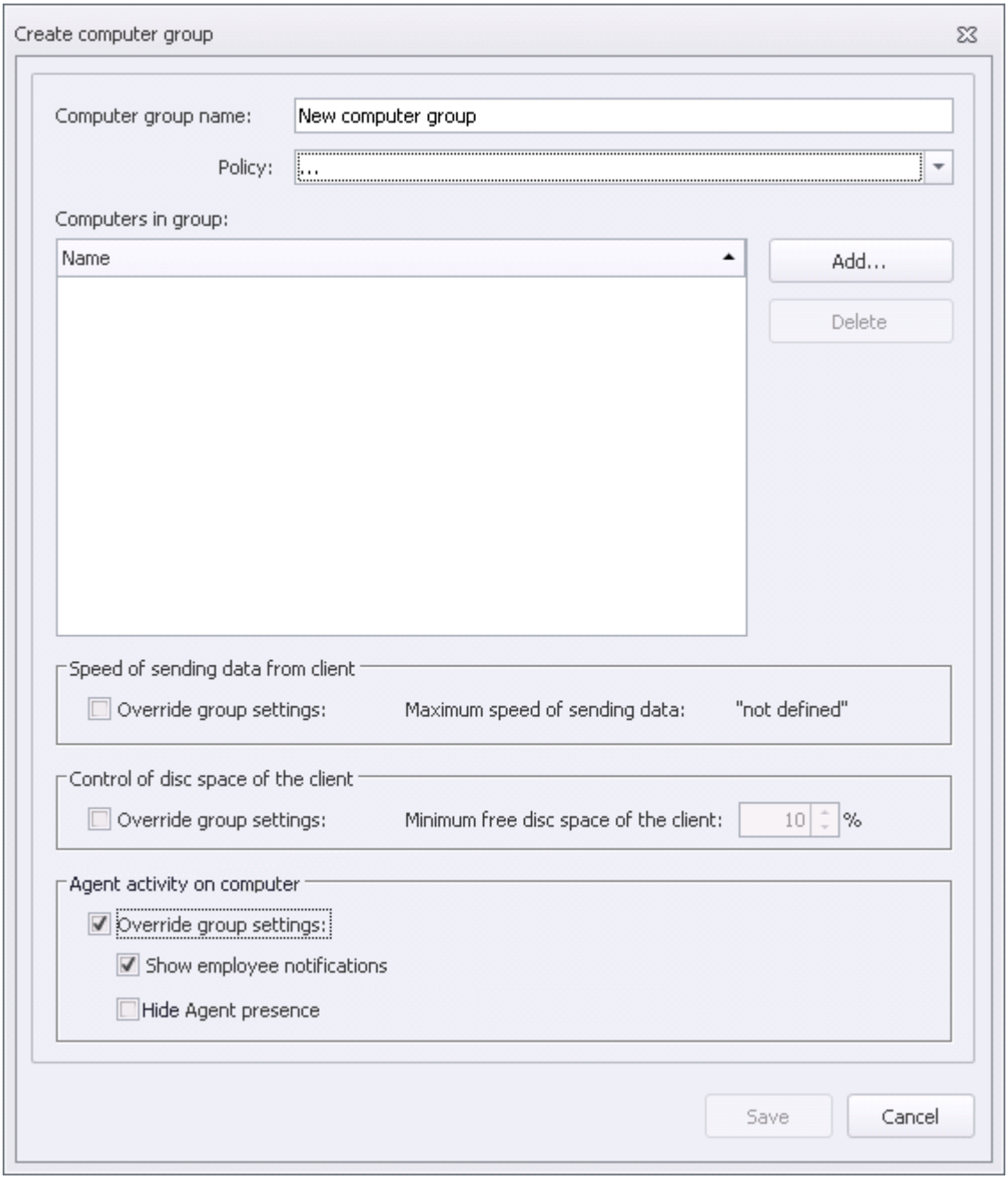
> **Important!**
>
> When you register a new computer, information on this computer is automatically added to the security scheme (to the "default" computer group).

To create computer group:

1. Go to **Computers** section.
2. Take one of the following steps:

Action	Steps
Add computer group	• in the Main Menu, click **Edit > Create workstation group**; • click **Create Computer Group** at the top of Navigation pane.
Edit computer group	a. In **Computers** area of Navigation pane select workstation group name. b. Take one of the following steps: • in the Main Menu select **Edit > Edit**; • click **Edit** at the top of Navigation pane; • double-click selected workstation group name.

This opens a dialog box with group parameters.



3. In this dialog, specify the following parameters:
   - **Workstation group name**.
   - **Policy (DM)**. From the drop-down list select security policy (DM) that will be assigned to this computer group.
4. Define a list of computers in a group:
   - To add one or several computers click **Add**. In the opened **Add computer to the group** dialog you can
     select computers from:
     - directory service (for example, Active Directory);
     - Microsoft Windows Network;
     - ones registered in System previously (for example, after manual Device Monitor Agent installation) and already belonging to other Device Monitor groups.

Select a node from a tree in left panel then flag computers which you want to add to the group.
You can also make a search of a computer in the directory. For this end enter a part or a computer name to the upper field and click **Find**.
When all needed computers are selected click **Save**: this closes the add window and returns you to configuring group settings.

- To delete a computer from the list select it and click **Delete**.

5. You can set particular speed of sending data from the Agents for computers belonging to the group (configuring of a common value is described in "Common Settings for Agents", **Limit the speed of sending data** setting). To do this:
   a. in the **Speed of sending data from agent** area select **Override group settings**;
   b. in the **Maximum speed of sending data** field, specify the needed value, Kbps.

   The setting is not selected by default.
6. You can set particular volume of a minimum free disk space (when it is reached on the managed computer, shadow copies would not be created) for computers belonging to the group (the configuring of a common value is described in "Common Settings for Agents", **Minimum free disc space of the agent** setting). To do this:
   a. in the **Control of disk space of the agent** area select **Override group settings**;
   b. in the **Minimum free disc space** of the agent field, specify the needed value, percent.

   The setting is not selected by default.
7. You can set a particular mode of Agent hiding for computers belonging to the group (the configuring of a common value is described in "Common Settings for Agents", **Agent activity on computer** setting group).
   To do this:
   a. in the **Agent activity on computer** area select **Override group settings**;
   b. select or deselect **Show employee notifications** and **Hide Agent presence** settings.

   The setting is not selected by default.
8. Click **Save**.

> **Warning!**
>
> To apply changes you have to save current security scheme (see "Editing Security Scheme"). If you don't save your security schema, all changes will be discarded.

Deleting Computer Group

To edit or delete computer group:

1. Go to **Computers**.
2. In Computers area of Navigation pane select computer group name.
3. Take one of the following steps:
   - in the Main Menu select **Edit > Delete**;
   - click **Delete** at the top of Navigation pane.
4. In the following confirmation dialog select **Yes** to confirm that you want to delete computer group.

Warning!

The group you are deleting may contain computers that don't belong to any other group. If you delete
the only group these computers belong to, they will be automatically added to "default" group

5. Click **OK**.

Warning!

To apply changes you have to save current security schema (see "Editing Security Scheme"). If you don't save
your security schema, all changes will be discarded.

Adding Computer to a Group

When installing InfoWatch Device Monitor Agent (see the document "*InfoWatch Traffic Monitor. Installation Guide*", "InfoWatch Device Monitor Agent Setup" article), the computer is added to "default" computer group. To all computers within the "default", the policy assigned to this group will apply. Further on, you can assign security policies (DM) to the computer by adding it to various computer groups.

To move a computer from one computer group to another:

1. Go to **Computers**.
2. In **Computers** area of Navigation pane, select computer group that contains the computer.
3. Select a row that contains the computer you want to add to another group. Click and hold the selected row and drag the computer to **Computers** area of Navigation pane. Move the pointer over the name of the computer group to which you want to add the computer. When a yellow arrow appears to the left of the selected group name, release the mouse button.
   This adds the computer to selected computer group.

You can also add information about computers without InfoWatch Device Monitor Agent manually.
Computer information is imported from directory service (connection configuring settings see in "Connecting to LDAP Server and synchronization with Active Directory and Astra Linux Directory") or your network environment. Then after InfoWatch Device Monitor installation this computer (see "Creating Primary Distribution Task") will be affected by the policy (DM) of the group it was added to.

The mobile devices do not allow this option.

Warning!

It is not recommended to add computers with similar names. These computers will be registered in InfoWatch Device Monitor system as a single computer, affected by the same policies (DM), and register the same events, etc.

To add computer to a group:

1. Go to **Computers**.
2. In **Computers** area of Navigation pane select computer group name. The main screen will display a list of all computers inside the group.

3. Take one of the following steps:
   - in the main menu select **Edit > Add computer**;
   - click **Add computer** located at the top of **Computers** area;
   - right-click in the workspace and select **Add computer** from the drop-down menu.

   In the opened dialog you can select computers:
   - imported from directory service (for example Active Directory);
   - received from Microsoft Windows Network;
   - from ALD tree;
   - among previously registered in the System.
4. Flag computers or computer groups. Minimized groups are marked with an icon; expanded - . Doubleclick a group, to expand or collapse it.
   You can also specify computer name in the line at the bottom of dialog box. When listing names, separate them with semicolons.
5. Click **OK**.

This closes **Select computer** dialog and adds information on selected computers to the computer group.

> **Warning!**
>
> To apply changes you have to save current security scheme (see "Editing Security Scheme"). If you don't save your security schema, all changes will be discarded.

Removing Computer from a Group

Computer is added to a group basing on needed security policies (DM). You might need to disable policy's (DM) action to the
computer. To perform this procedure, you must remove computer from computer group with this policy (DM).

> **Note:**
>
> If you remove a computer from a single group it belongs to, it will be automatically added to "default" group.

To exclude computer from computer group:

1. Go to **Computers**.
2. In **Computers** area of Navigation pane, select computer group that contains the computer. This displays a
   full list of computers that belong to selected group.
3. Select a row that contains the computer you want to remove from computer group.
4. Take one of the following steps:
   - in the main menu select **Edit > Remove Computer From Group**;
   - click **Remove Computer From Group** located at the top of Computers area;
   - press **Delete** keyboard button.

This removes computer from the group.

Warning!

To apply changes you have to save current security schema (see "Editing Security Scheme"). If you don't save
your security schema, all changes will be discarded.

Deleting computer from security schema

You can remove a computer from the list of registered computers (for example, computer discontinued operation). Computer information will not be deleted, but it will be marked as **Inactive** due to Agent deactivation.

If you don't want to save inactive computer information, you can delete its record.

To remove computer from the security scheme:

1. Go to **Computers**.
2. In **Computers** area of Navigation pane, select computer group that contains the computer.
3. In the Main screen workspace, select the row that contains the inactive computer you want to remove.
4. Take one of the following steps:
   - in the Main Menu, click **Edit** > **Delete Computer From Security Schema**;
   - click **Delete Computer From Security Schema** located at the top of **Computers** area;
   - right-click computer row and select **Delete Computer From Security Schema**;
   - press **Shift+Delete** at the keyboard.
5. In the following confirmation dialog select **Yes** to confirm that you want to remove the computer.

This removes computer information from all groups the computer was assigned to.

Warning!

To apply changes you have to save current security scheme (see "Editing Security Scheme"). If you don't save your security scheme, all changes will be discarded.

Updating Agents on managed computers

Device Monitor Agents at managed computers can be simply updated by the task (see task details in "Agent Remote Installation, Updating and Uninstallation" and "Creating Update Task").

To update Device Monitor Agents on all managed computers of the group:

1. Go to **Computers**.
2. In **Computers** area of Navigation pane, select computer group.
3. Click **Update All Computers** located at the top of Navigation pane.

To update Device Monitor Agents on selected computers:

1. Go to **Computers**.
2. In **Computers** area of Navigation pane, select computer group.
3. In the Main screen workspace, select the row(s) containing managed computer(s). To select several computers,use **Shift** or **Ctrl** button.
4. Click **Update Computers** located at the top of **Computers** area.

This creates and runs the update task for the selected computers.

Diagnostics of the Workstation

The System allows you to remotely collect diagnostic data from workstations.

> **Warning!**
>
> It is only possible to collect diagnostic data for workstations: for mobile devices, this feature is unavailable.

To start collecting diagnostic data on the computer:

1. Go to **Computers** section.
2. In **Computers** area of the Navigation pane, select the group which includes the required workstation.
3. In the computer list, right-click the desired workstation and select **Diagnostics > Enabling diagnostic mode**.

To stop diagnostic data collection on the computer:

1. Go to **Computers** section.
2. In **Computers** area of Navigation pane, select the group which includes the required workstation.
3. In the computer list, right-click the desired workstation and select **Diagnostics > Disabling diagnostic mode**.

To get the archive that contains all provided diagnostic data:

1. Go to **Computers** section.
2. In **Computers** area of Navigation pane, select the group which includes the required workstation.
3. In the computer list, right-click the desired workstation row and select **Diagnostics > Gathering diagnostic data**.
4. In the **Select path to save archive with diagnostic data** dialog, specify the folder and the archive name.
5. In the notification window that opens, click **OK**.

Mobile Devices

Besides workstations, InfoWatch Device Monitor allows you to control employees' mobile devices (smartphones and tablet PCs).

InfoWatch Device Monitor Agent supports mobile devices specified in the document "*InfoWatch Traffic Monitor. Installation Guide*", the page "Hardware and Software Requirements".

> **Note:**
>
> InfoWatch Device Monitor Mobile Lite application can be downloaded from Google Play and provides the following functionality:
>
> - Control of incoming and outgoing SMS messages;
> - Control of cloud storages: YandexDisk, Google Drive, DropBox;
> - Control of Skype text chats;
> - Control of photos;
> - Possibility to replace GPS coordinates.

Important!

Installing InfoWatch Device Monitor on iPhone or iPad is possible only if the device is jailbroken.

The System can associate several mobile devices with one employee, but a single mobile device can be associated with one employee only.

Warning!

To manage a mobile device entry and to install or uninstall InfoWatch Device Monitor Agent, the following requirements should be met:

- USB Debugging mode must be enabled on the mobile device and all required drivers should be installed (for devices on Android platform only);
- the Management Console (DM) should run on a physical workstation (using virtual machines or remote desktop connections is not recommended; Microsoft Windows XP is not supported);
- the mobile device directly must be connected via USBe to the computer where the Management Console (DM) is running.

See details in "Preparing a Mobile Device on Android Platform" and "Preparing a Mobile Device on iOS Platform".

Guidelines on Agent installation and uninstallation for mobile devices are available in:

- Preparing a Mobile Device on Android Platform
- Preparing a Mobile Device on iOS Platform
- Adding a Mobile Device to Computer Group
- Adding a Mobile Device through Appointment to Employee
- Deleting the Mobile Device

Preparing a Mobile Device on Android Platform

If you are using a mobile device on Android platform, then to install, update or delete InfoWatch Device Monitor Agent, you should:

1. Enable "**USB debugging**" mode on the device: see example below.
2. Via a USB-wire connect this device to the computer where Device Monitor Management Console is running.
3. If necessary (for example, for some builds of Samsung), install additional drivers.

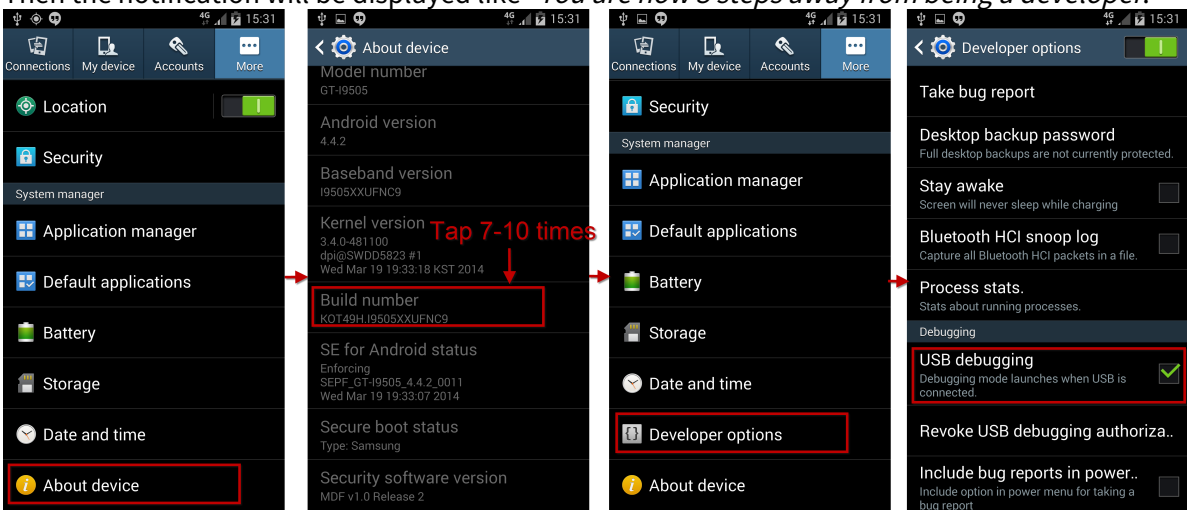
Step 1. Enabling "USB debugging" mode

The process of enabling the "USB debugging" mode can slightly vary for different models of mobile devices, different versions of OS and firmware.

Enabling the debugging mode for Samsung Galaxy S4 with Android 4.4.2:

1. Enable developer mode: **Settings -> About device -> Build number**; tap the build number several times (7-10).

2. Then the notification will be displayed like "*You are now 3 steps away from being a developer.*"



3. Continue tapping till successful mode enabling.
4. Return to the **Settings** menu. Select **Developer options** which appeared near **About device** section.
5. Select **USB debugging**.

You can disable the debugging mode when the installation, updating or deleting the InfoWatch Device Monitor Agent is successfully completed.

Huawei feature:
The Huawei models can automatically disable USB debugging mode if the connection with the computer is lost. Therefore the debugging mode should be enabled every time after connecting to the computer.

Step 2. Connecting to the computer

To install or update the InfoWatch Device Monitor Agent, you should connect the mobile device to the physical workstation where Device Monitor Management Console is running, via the USB-wire.

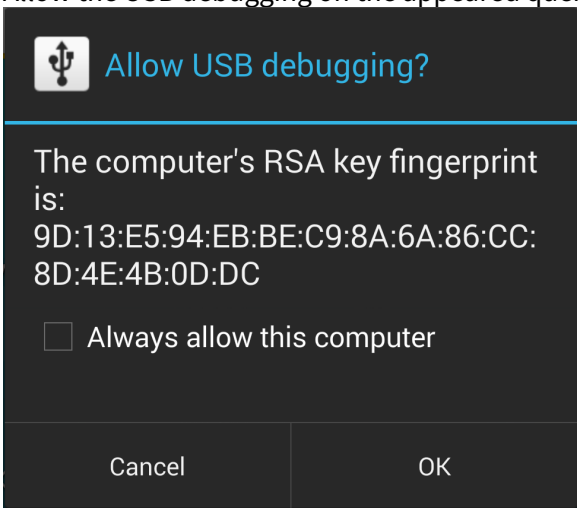
> **Warning!**
>
> If you are using a virtual machine or connection to a remote desktop, then the installation can fail due to increasing of the System response time. Therefore, we recommend that you should not use virtual machines or remote desktops.
>
> The System does not support installation of Device Monitor Agent to mobile devices if the Management Console (DM) is running on a computer with Microsoft Windows XP. Therefore, we do not recommend using Microsoft Windows XP either.

You can see if the connection was successful and control the further installation of drivers in Device Manager (**Control Panel -> Hardware and Sound -> Device Manager**).

Samsung feature:
If the phone is "clear" - for example, the build is just updated, - then you can need to perform additional actions:

1. On the phone slide down the notification panel.
2. Switch the device from the "**Multimedia**" connection mode to the "**Camera**" mode.

3. Allow the USB debugging on the appeared query.



Step 3. Drivers installation

In a first connecting of the mobile device to the computer where the Device Monitor server is working the automatic installation of the following drivers is performed:

- a driver for operation in a normal mode;
- the **libusb** driver for operation in the downloaded mode;

During installation of the drivers, the icon on the Device Monitor server's computer taskbar displays the process of drivers searching and installation.

> **Warning!**
>
> Do not disconnect the mobile device during drivers installation! Wait for installation completion.

When installation of a driver is completed successfully, the computer will display a notification that this driver is ready to use. In case of some errors in drivers installation, you can find solutions in InfoWatch Knowledge Base: "Mobile Device Driver Cannot Run Automatic Installation" or "Installing the Driver for Downloaded Mode" (libusb0)" for example.

Preparing a Mobile Device on iOS Platform

If you are using a mobile device on iOS platform, then to install, update or delete InfoWatch Device Monitor Agent, you should:

1. Jailbreak your mobile device (iPhone or iPad).
2. On the computer where Device Monitor Management Console is installed, install iTunes.
3. Connect the mobile device to the computer, where Device Monitor Management Console is installed, via a USB-wire.
4. Authorize the mobile device on the computer.

Step 1. Jailbreaking the mobile device

Installing InfoWatch Device Monitor Agent on iPhone or iPad is possible only if the device is jailbroken.

Note:

The supported versions of iPhone and iPad are 8.0 - 9.0.2.

Step 2. Installing iTunes

To install InfoWatch Device Monitor Agent on a mobile device, it is necessary that Apple Mobile Device Support application should be installed on the computer (it is installed together with iTunes).

Step 3. Connecting to the computer

To install or update InfoWatch Device Monitor Agent, you should connect the mobile device to the physical workstation where Device Monitor Management Console is running, via the USB-wire.

Warning!

If you are using a virtual machine or connection to a remote desktop, then the installation can fail due to increasing of the System response time. Therefore, we recommend that you should not use virtual machines or remote desktops.

The System does not support the installation of Device Monitor Agent to mobile devices if the Management Console (DM) is running on a computer with Microsoft Windows XP. Therefore, we do not recommend using Microsoft Windows XP either.

You can see, if the connection was successful, and control the further installation of drivers in Device Manager (**Control Panel -> Hardware and Sound -> Device Manager**).

Step 4. Authorizing the device on the computer

Once you have connected the device to your computer, you should authorize the device on this computer. For this:

1. Run iTunes on the computer.
2. In the message that appears on the device, confirm that this computer can be trusted.
3. On the computer, in the iTunes menu bar, select **Store -> Authorize this computer**.

Adding a Mobile Device to Computer Group

Mobile devices can be added to the security schema from the computer group with specifying the employee earlier created in the System or added from LDAP.

Warning!

To manage the mobile device account and to install or delete InfoWatch Device Monitor Agent, the following settings are required:

- USB Debugging or similar mode should be enabled on the mobile device and all required drivers should be installed (for devices on Android platform only);

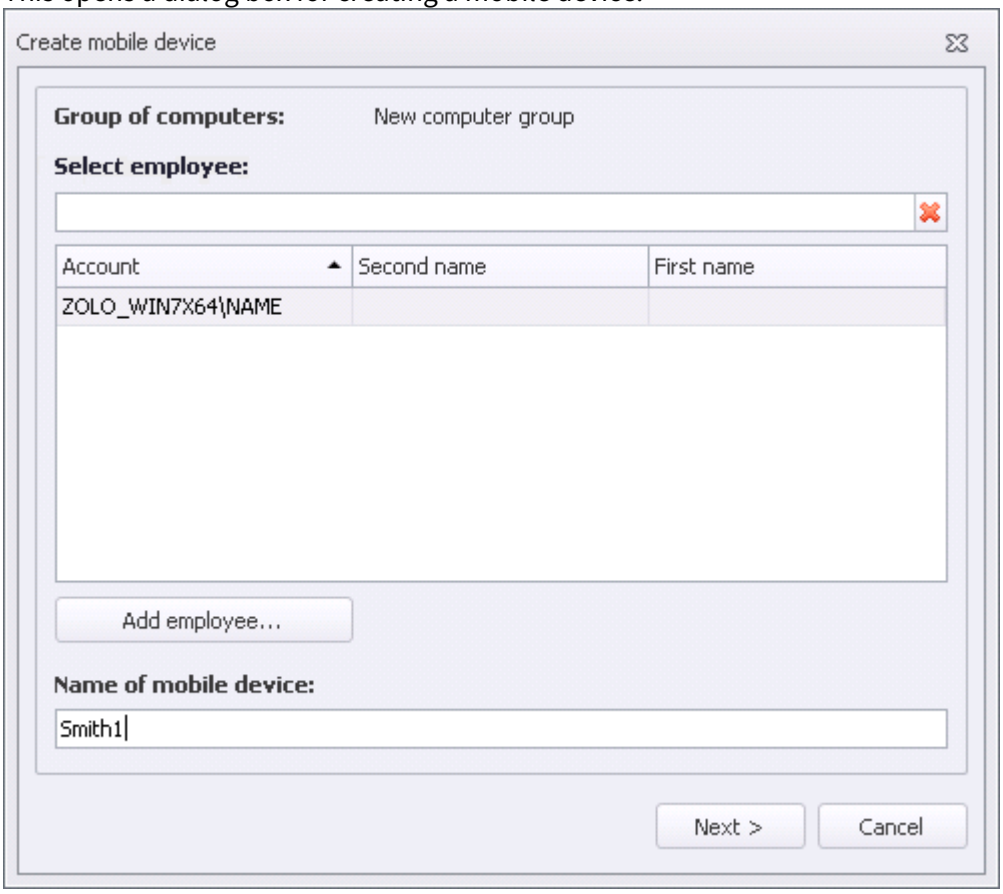
- the Management Console (DM) should be running on a physical workstation (using virtual machines or remote desktop connections is not recommended; using Microsoft Windows XP is not supported);
- the mobile device should be directly connected via USB wire to the computer where the Management Console (DM) is running.

Details see in "Preparing a Mobile Device" and "Preparing a Mobile Device on iOS Platform".

To add a mobile device to the computers group and install the InfoWatch Device Monitor Agent to it:

1. Go to the **Computers** section.
2. In the **Computers** area of Navigation pane, select the name of the group to which you want to add a mobile device.
3. Do either of the following:
   - in the main menu, select **Edit > Create mobile device**;
   - click **Create mobile device** button located in the upper part of the **Computers** area;
   - right-click the workspace and select **Create mobile device** from the shortcut menu.

   This opens a dialog box for creating a mobile device.



4. In the list of employees, select the required account.
   You can also start typing the account name in the entry field: the list will be filtered.
   If there is no needed account in the list, you can add it: click **Add employee**. On adding accounts, see "Adding Employee Account to a Group".
5. If necessary, change the entry name for the mobile device that was automatically created by the System.

6. Click **Next**.
7. In the installation wizard dialog box that opens, select the connected mobile device.
8. Click **Install**.
9. When the installation is complete, click **Finish**.

This will install InfoWatch Device Monitor Agent to the mobile device and add the entry of the new mobile device to the selected computer group of the security scheme. The new mobile device will be associated with the selected employee.

> **Warning!**
>
> Once the Agent is installed on the mobile device, a policy (DM) that is assigned to a default computer group will be deployed to this device. The policy (DM) assigned to the specified policy will be deployed on the mobile device after you save the security scheme.
> On how to save the security scheme, see "Editing Security Scheme".

Adding a Mobile Device through Appointment to Employee

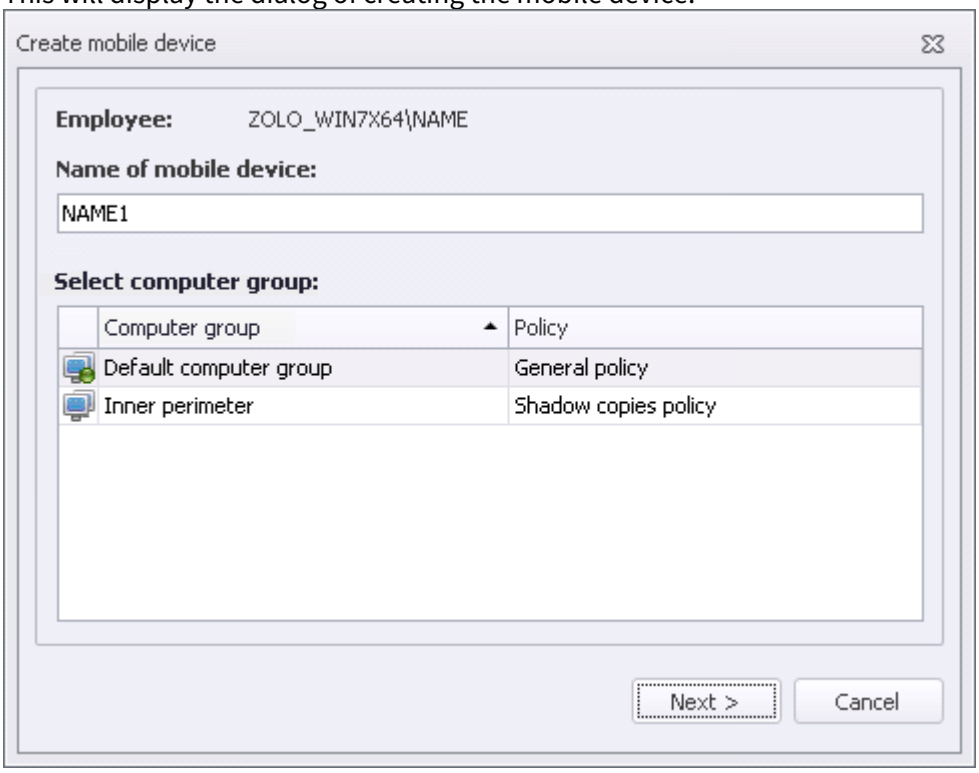
Mobile devices can be added to the security schema from the entry of the employee which you want to assign this mobile device.

> **Warning!**
>
> To install InfoWatch Device Monitor Agent, there should be:
>
> - USB Debugging mode enabled on the mobile device and all required drivers installed (for devices on Android platform only);
> - the Management Console (DM) running on the physical workstation (using virtual machines or remote desktop connections is not recommended; using of the Microsoft Windows XP is not supported);
> - mobile device directly connected via USB wire to the computer where the Management Console (DM) is running.
>
> Details see in "Preparing a Mobile Device" and "Preparing a Mobile Device on iOS Platform".

To add a mobile device to the security schema through the employee group and install the InfoWatch Device Monitor Agent to this device:

1. Go to the **Employees** section.
2. In the **Employees groups** area on the Navigation pane select the group which contains the needed employee.
3. Select the employee list which you want to assign a mobile device to.
4. Take one of the following steps:
   - in the main menu select **Edit > Create mobile device**;
   - click  **Create mobile device** button located in the upper part of the **Employees** area;
   - right-click on the workspace and select  **Create mobile device** from the context menu.

This will display the dialog of creating the mobile device.



5. If needed, change the name of the mobile device entry.
6. Select the needed computer group from the list.
7. Click **Next**.
8. In the opened installation dialog window select the connected mobile device.
9. Click **Install**.
10. When the installation is completed, click **Finish**.

This will install the InfoWatch Device Monitor Agent to the mobile device and add the entry of the new mobile device to the selected computer group of the security schema. The new mobile device will bó associated with the selected employee.

Warning!

Just after the Agent installed to the mobile device, this device will have a policy (DM) appointed to the default computer group, and only when the security schema will be saved, the device will have a policy (DM) appointed to the computer group specified on mobile device adding.

Information on saving the security schema see in "Editing Security Scheme".

Deleting the Mobile Device

The removing the mobile device from the security scheme without uninstalling the InfoWatch Device Monitor Agent is performed in the way common for all the computers: see "Deleting computer from security schema". For this action, no device connection is needed.

Warning!

To uninstall InfoWatch Device Monitor Agent, there should be:

- USB Debugging mode enabled on the mobile device and all required drivers installed (for devices on Android platform only);
- the Management Console (DM) running on the physical workstation (using virtual machines or remote desktop connections is not recommended; using of the Microsoft Windows XP is not supported);
- the mobile device directly connected via USB wire to the computer where the Management Console (DM) is running.

Details see in "Preparing a Mobile Device" and "Preparing a Mobile Device on iOS Platform".

To delete the mobile device from the security scheme and uninstall the InfoWatch Device Monitor Agent from this mobile device:

1. In the main menu select **Tools > Delete mobile device**.
2. In the opened installation dialog window select the connected mobile device.
3. Click **Uninstall**.
4. When the uninstallation is completed, click **Finish**.

This will uninstall the InfoWatch Device Monitor Agent from the mobile device and delete the entry of a new mobile device from the computer group and security scheme.

White Lists

You can manage lists of devices with full access from **White Lists** section. To go to this section, click **White Lists** button at Navigation pane.
For more information on white lists see:

- Viewing White List Details;
- Adding White List;
- Defining Entry Validity Period;
- Editing White List;
- Deleting White List.

You can view an information on acting white lists as described in "Viewing Resultant Policy (DM) and Resultant White List for an employee" and "Viewing Resultant Policy (DM) and Resultant White List for Computer".

Viewing White List Details

White Lists area of Navigation pane displays all white lists. Main screen work pane displays devices (models and instances) in selected white list.

Note:

You can make search in white list index: type the name of the list in the search box below the index on Navigation pane.
You can adjust the displaying of selected white list using additional features (see "Additional Features").

To view information for separate white list,
select white list title in the group.

White lists information is available as a list of devices grouped by their type. Each row in the list contains device model or instance. Columns contain devices' general properties. Extended information on device properties is displayed in **Details** panel.

To view detailed information on device properties,
select the row that contains device model or instance name.

Details panel displays properties table including the following information:

- **Device instance or model identifier**. Model code (VID - Vendor ID) or device instance serial number (PID-Product ID).
- **Device description**.
- **Device type**.
- **Category**. Model or instance.
- **Period**. Full access period starting and expiry date and time.
- **Detected on computer**. Name of computer where the device was detected.
- **Added to database at**. Date of device information submission to database (see "Adding Device to Database").

> **Note:**
>
> Some of the properties on **Details** panel are duplicated in the main screen workspace.

Adding White List

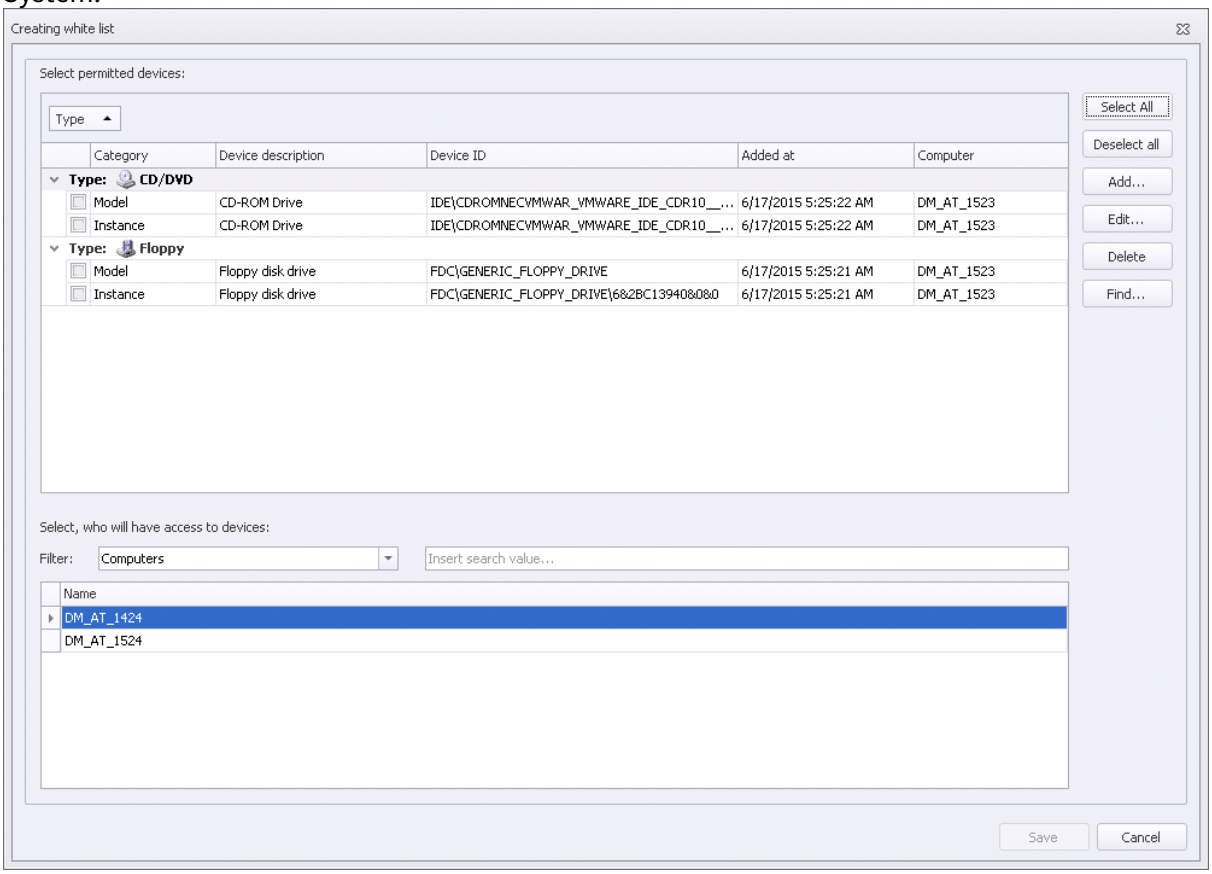
White list affects selected objects: employees, employee groups, computers or computer groups.

> **Warning!**
>
> A single object (employee, employee group, computer or computer group) can have only one white list assigned to.

To add white list:

1. Go to **White Lists** section.
2. Take one of the following steps:
    - select **Edit > Create White List** in the Main Menu;
    - click **Create White List** at the top of Navigation pane..

This opens **Creating White List** dialog displaying table containing all devices registered in the System.



3. In the table of devices select models and instances which should have full access to.

> **Warning!**
>
> Information on creating a list of registered device models and instances see in:
> Adding Device Entry;
> Deleting Device Entry.

4. In **Select, who will have access to devices** area select a filter: who will be affected to white list action:
   - employees
   - employee groups
   - computers
   - computer groups

   The list of entries will appear below.
   You can also use a search string by entering a name or its part.
5. Select employee / employee group / computer / computer group that will have full access to selected
   devices.
6. Click **Save**.

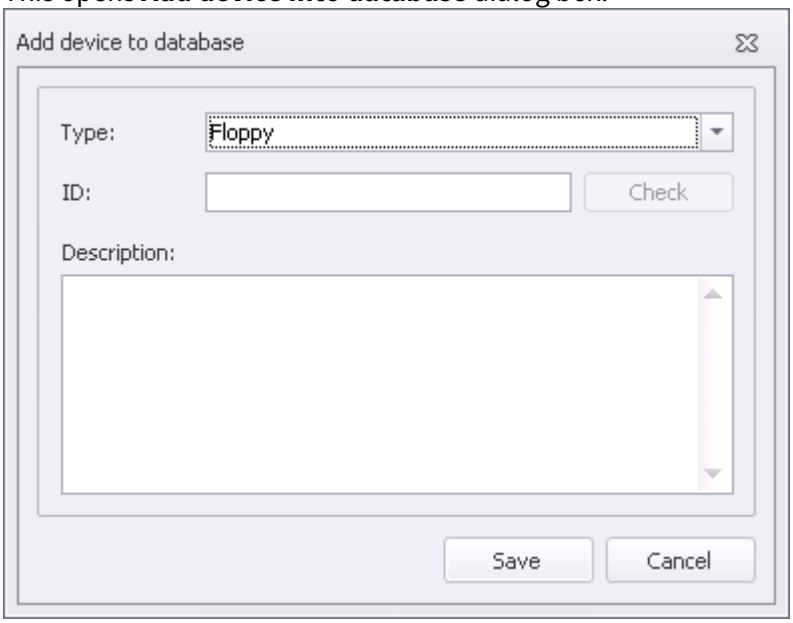
Adding Device Entry

You can add to white lists only device models and instances which were previously registered in the System. Device information is added in two ways:

- manually (if device ID is provided)
- via the search engine (if the device is connected to managed computer).

To add device information manually:

1. Open **Creating White List** dialog box (see "Adding White List").
2. Click **Add** button at the right of the window.
   This opens **Add device into database** dialog box.



3. Specify device parameters:
   - select device type from **Type** drop-down list;
   - enter the device instance or model identifier into **ID** box;

> **Note:**
>
> To retrieve device instance string, connect the device and use standard Windows tools (for example, **Device Manager**) to view its properties. Device instance string is displayed on Information tab.
> Device instance string is displayed as XXX\YYY\ZZZ where XXX is device type (usually, connection type, such as USB, IDE or ACPI), YYY is device model string (Vendor ID), and ZZZ is device instance string (Product ID).
> Model ID is displayed as XXX\YYY where XXX is device type and YYY is model ID string (VID).

   To make sure the ID is valid, click **Check**.

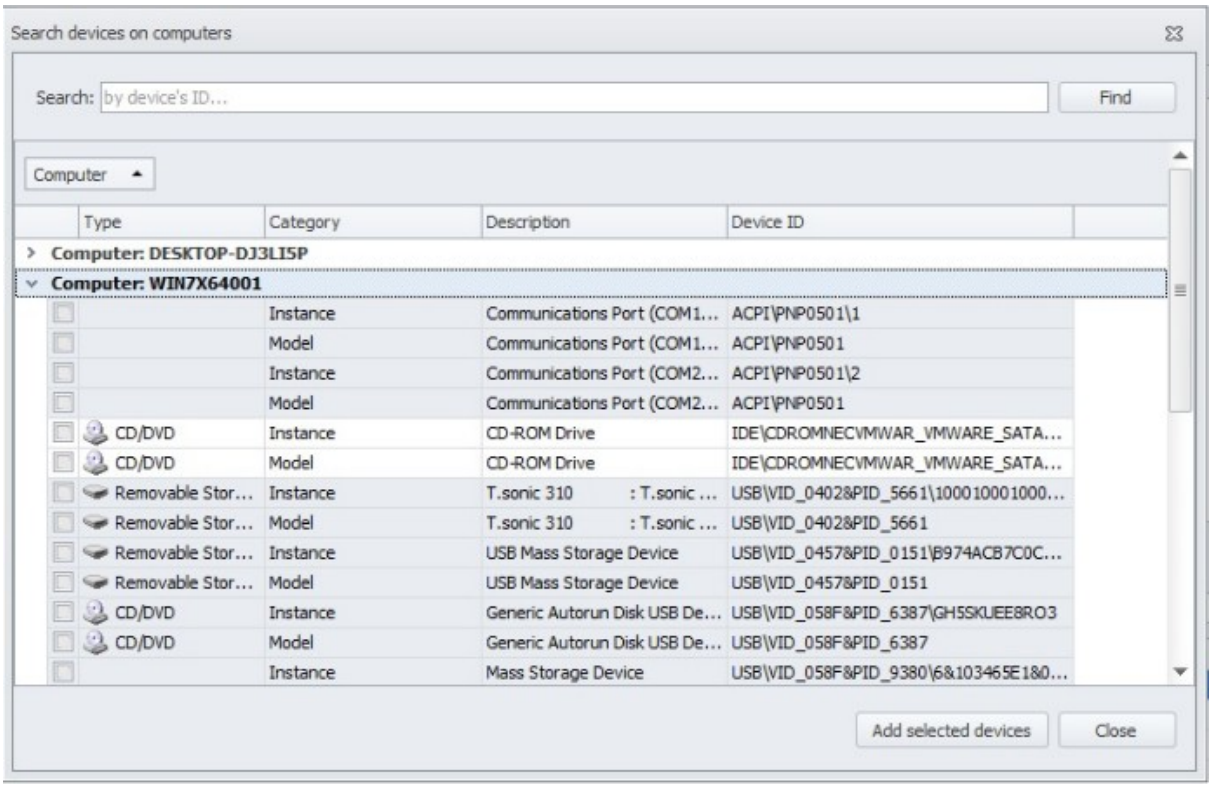
> **Warning!**
>
> When using instance code, take into account that some devices do not have unique ID: ID can be changed dynamically and differed even when connecting to different ports of the same computer.
> In such case using device model code is recommended.

- enter description into **Description** box.

4. Click **Add**.

To add device information via searching devices connected to managed computers:

1. Open **Creating White List** dialog (see "Adding White List").
2. Click **Find** at the right.
   This opens **Search devices on computers** dialog box.



3. Use one of the following ways to select a managed computer from the list:
   - click ▸ next to computer;
   - double-click computer name.

   You will see a list of devices which were connected to selected computer during all the time Device Monitor Agent was installed on the computer.

> **Note:**
>
> It is required to point out the devices connected to computer are highlighted with a white background, while the disabled devices are highlighted with grey.

4. Flag the devices you want to add.
5. Click **Add selected devices**.

Deleting Device Entry

To remove device entry from database:

1. Open **Creating White List** dialog (see "Adding white list").
2. Select and right-click device instance or model in device database table. In the drop-down menu, select **Delete device**.
3. In confirmation dialog click **OK**.

Defining Entry Validity Period

Each device instance or model from the white list has an access permission displayed separately. This item's (permission's) default validity period is practically infinite (from 01.01.1753 to 31.12.9999). You can limit full access period for this device. This device will be subject to general rules (DM) that apply to this device type before and after the
specified period.

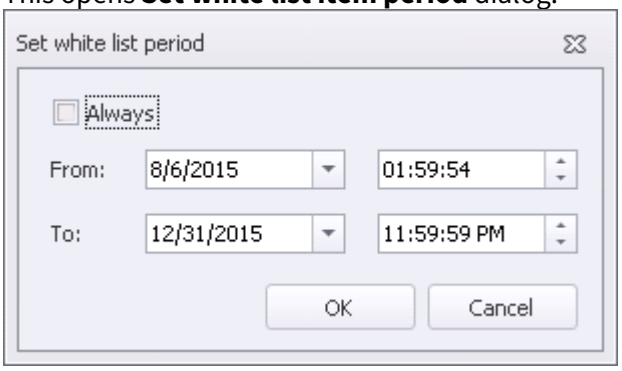
To set white list entry period:

1. Go to **White Lists**.
2. In **White Lists** area of Navigation pane select white list that contains the item.
3. If white list items are grouped in (for example, by the type of devices), expand them (see "Grouping Entries
").

> **Note:**
>
> If you set validity period for the entire group, the change will only take effect for the first item of the
> group.

4. Select the row that contains device instance or model you want to assign validity period to and take one of
the following steps:
   - select **Edit > Edit Item** in the Main Menu;
   - click **Edit Item** at the top of **Permitted devices** area;
   - double-click selected entry name;
   - right-click entry row and select **Edit Item** from drop-down menu.

This opens **Set white list item period** dialog.



5. Set item validity period and click **OK**.

Editing White List

To edit white list parameters:

1. Go to **White Lists**.
2. In **White Lists** area of Navigation pane select the name of white list.
3. Take one of the following steps:
   - in the Main Menu, click **Edit > Edit**;
   - click **Edit** at the top of Navigation pane;
   - double-click selected white list name.

   These actions open **Edit white list** dialog box. This dialog is similar to **Creating white list** dialog with the
   exception of **Select, who will have access to devices** area, which is unavailable.
4. You can add or remove devices from database, if needed (see "Adding Device to Database" and "Removing
   Device from Database").
   You can also change the description of previously registered device: to do this select the device in the index
   and click **Edit** button at the right of the window. In the opened window change the description text and click
   Save.
5. Add or remove flags in device database table to change the catalog of models and instances in the white
   list.
6. Click **Save**.

> **Warning!**
>
> To apply changes you have to save current security schema (see "Editing Security Scheme"). If you don't save
> your security schema, all changes will be discarded.

Deleting White List

To delete white list:

1. Go to **White Lists** section.

2. Click the white list you want to delete.
3. Take one of the following steps:
    - select **Edit > Delete** in the Main Menu;
    - click **Delete** at the top of Navigation pane..
4. In confirmation box click **Yes** to confirm that you want to remove the white list.

> **Warning!**
>
> To apply changes you have to save current security schema (see "Editing Security Scheme"). If you don't save
> your security schema, all changes will be discarded.

Signatures

File Monitor rules (DM) can be configured to affect only files of specific structure distinguishing defined file format. To do
this, InfoWatch Device Monitor defines file format basing on its signature.
Signatures section contains a list of signatures which the System can recognize. Signatures are conveniently grouped into **categories**.

To view available signatures:

1. Go to **Signatures** by clicking the Signatures button in Navigation pane or selecting in Main Menu Go > **Signatures**.
   Signatures area of Navigation pane displays a list of signature categories.
2. Select a signature category from the list.
   Main screen workspace will display a list of all signatures in the selected category.

> **Warning!**
>
> Predefined signature categories cannot be edited or deleted. You can't create new signatures.

You can do the following:

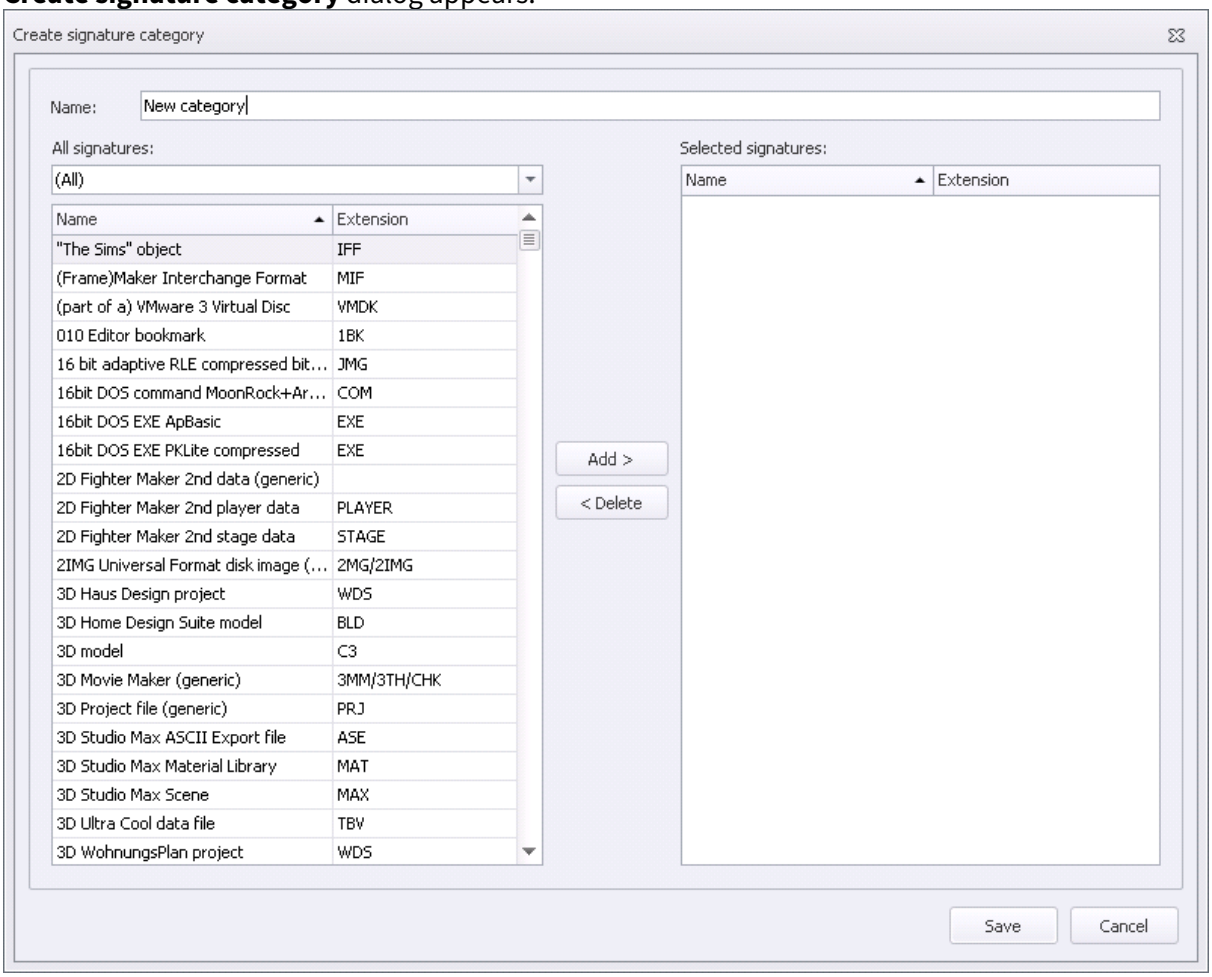
- create signature categories;
- fill created categories by copying predefined signatures;
- delete your signature categories, if they are not used by any rule.

Adding Signature Category

To add signature category:

1. Go to **Signatures**.
2. Take one of the following steps:
    - in the main menu select **Edit > Create signature category**;
    - click **Create signature category** at the top of Navigation pane..

Create signature category dialog appears.



3. Enter new category's name..
4. In **All signatures** area you can select one of preset categories from the list. All preset signatures are
   displayed by default.
5. In the left panel select signatures you want to add to a new category.
   To delete signatures from the list of included to a new category selected them at the right panel **Selected**
   signatures and click **Delete**.
   To select several signatures hold **Ctrl** or **Shift** button.
   To move selected signatures to a new category click **Add**.
   To delete signatures from the list of included to a new category selected them at the right panel **Selected**
   signatures and click **Delete**.
6. Click **Save**.

Editing Signature Category

After you have created a signature category (see "Adding Signature Category"), you can fill it. For this, do either of the following:

- in the signature category editing dialog (select a category and click **Edit > Edit** in the Main Menu or click **Edit** at the top of Navigation pane, or double-click the selected category name), define the list of signatures as described in "Adding Signature Category".

or

- copy signatures from other categories directly in the Console workspace.

To copy a signature from one category to another:

1. Go to **Signatures** section.
2. In **Signatures** area of the Navigation pane, select the name of a predefined category that contains the signature you want to copy.
3. In the main window workspace, select a row that contains the name of the signature you want to copy. You can select multiple signatures with **Ctrl** or **Shift**.
4. Click and hold the selected row, then drag the pointer to **Signatures** area of Navigation pane. Move the pointer over the category you created earlier where signatures will be added. Release the button when a yellow arrow appears next to the selected category.

As a result, the signature will be copied to the selected category.

To remove a signature from the category, select the signature and do either of the following:

- click  **Remove signature from category** at the top of **Signatures** area;
- right-click and select **Remove signature from category** in the drop-down menu;
- press **Delete** key.

Deleting Signature Category

> **Warning!**
>
> The following categories cannot be deleted:
>
> - signature categories used by any File Monitor rule (DM)
> - predefined signature categories.

To delete a signature category:

1. Go to **Signatures**.
2. Click the signature category name.
3. Take one of the following steps:
   - in the main menu select **Edit > Delete**;
   - click  **Delete** at the top of Navigation pane.
4. In the next confirmation dialog select Yes to confirm that you want to remove signature category.

> **Warning!**
>
> To apply changes you have to save current security schema (see "Editing Security Scheme"). If you don't save
> your security schema, all changes will be discarded.

Application Protocol

After the InfoWatch Device Monitor Agent is installed on the computer (computer or mobile device) and the computer is rebooted, the System automatically starts to receive data on applications launched on managed workstations and installed on managed mobile devices.

Data on all launches and installations produces an *application protocol*.

> **Warning!**
>
> Application protocol excludes system vital applications. One can not forbid application which absence is obstructive for computer properly operation.

Managing the application protocol is performed in the **Applications** section. To go to this section click **Applications** button located on the Navigation pane or select **Go > Applications** command in the main menu.

The Navigation pane is divided into two groups in this section: **List of applications** and **Applications Protocol**:

- The **List of applications** group contains lists used to control employee's access to applications:
  - forbid launching applications in one of two modes: white lists and black lists. See details in "Configuring Application Monitor Rule (DM)".
  - forbid screenshots creating. See details in "Configuring ScreenShot Control Monitor Rule (DM)";
  - automatic creating the screenshots by the System. See details in "Configuring ScreenShot Monitor Rule (DM)".
- The **Applications Protocol** group is intended for creating filters showing data on all applications launched on managed workstations and installed on managed mobile devices. In this group, you can add applications to lists.

One can find information about working with protocols and application lists in the following articles:

- Creating an application list and adding applications;
- Creating and editing the application protocol filter;
- Adding Application to List Automatically;
- Adding Application to List Manually;
- Exporting Application Protocol.

Creating an Application List and Adding Applications

To manage white and black application list, the System offers application lists creation from the **Application protocol** (see "Application protocol").
Lists are used to permit or forbid application usage on computers.

To create an empty application list:

1. Go to **Applications** section..
2. On the Navigation pane set the cursor on the **List of applications** group and take one of the following steps:
   - in **List of applications** group menu click **Create list of applications**;
   - select **Edit > Create list of applications** command in the main menu;
   - right-click in the **List of applications** group and select **Create list of applications** from the dropdown list.
3. In the **List Name** field enter a name for a list you create.
4. Click **Save**.

Details on filling lists and creating lists from application protocols see "Adding Application to List Automatically"

and "Adding Application to List Manually".

To select an application from the list:

1. Go to **Applications** section.
2. Set the cursor on the **List of applications** group.
3. Click in **List of applications** group menu.
4. Select application(s) from list(s) and click **Add applications to the list**.
5. From the drop-down list select **Add applications automatically** or **Add applications manually**.

To edit application in the list:

1. Click button on the **List of applications** group.
2. You can edit details which will be used to filter the application (see "Adding Application to List Manually").

To delete application from the list:

1. Click button on the **List of applications** group.
2. Click **Yes** to delete application from the security scheme.

in List of applications group menu click Create list of applications

Creating and Editing the Application Protocol Filter

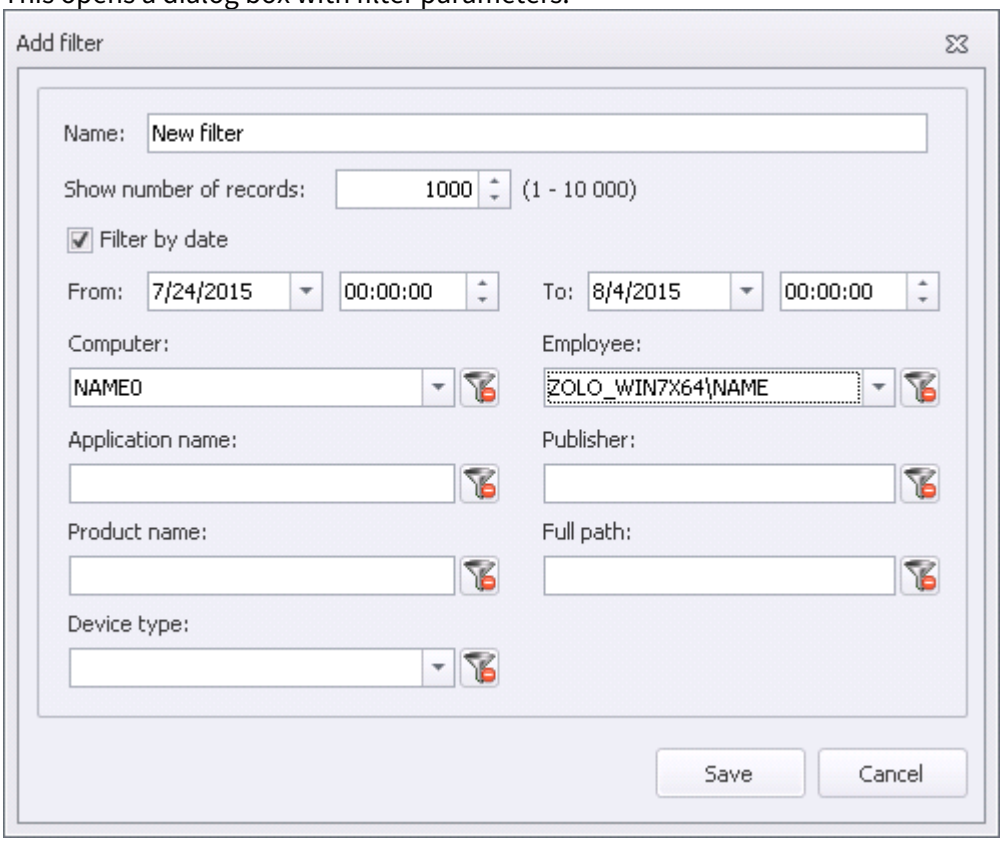
Filters allow you to configure the application protocol (see "Application protocol") to display information on applications that meet specified conditions.

> **Warning!**
>
> A preset **Today** filter shows applications which have been started on a particular day since initial installation of the Agent.
> The **All** filter shows applications which have been started right upon the Agent installation.

To create a new filter:

1. Go to **Applications** section.
2. On the Navigation pane set the cursor on the **Application Protocol** group and take one of the following
   steps:
   - in the click button in **Application Protocol** group on Navigation pane;
   - select **Edit > Create filter** command in the main menu;
   - right-click in the Application Protocol group and select **Create filter** from the drop-down list.

This opens a dialog box with filter parameters.



3. Enter the name of the filter in **Name** field.
4. In the **Show number of records** field, enter the number of records you want to see in the protocol.
5. To set up period for the records to be displayed flag the **Filter by date** option and specify parameters **From** and **To**.
6. If needed, specify additional filter conditions:
   - in **Computer** field select employee's computer which protocol you need to view;
   - in **Employee** field select account of an employee who launches applications;
   - in **Application name** field type in the name of the application you want to see information about;
   - in **Publisher** field type in the program publisher;
   - in **Product** name field pick the name of the product;
   - in **Full path** specify the path to the application location;
   - from **Device type** drop-down list, select whether the filter should display information on applications launched on computers or installed on mobile devices.

   Click button to delete the filter.
7. Click **Save**.

To edit filter:
Click button in **Application protocol** on Navigation pane or press **Ctrl+E**.

To delete filter:

1. Click button in **Application protocol** on Navigation pane or press **Ctrl+D**.
2. Click **OK** to confirm the deletion.

Adding Application to List Automatically

The System allows to fill application lists automatically using data received from the application protocol.

To add application to the list automatically:

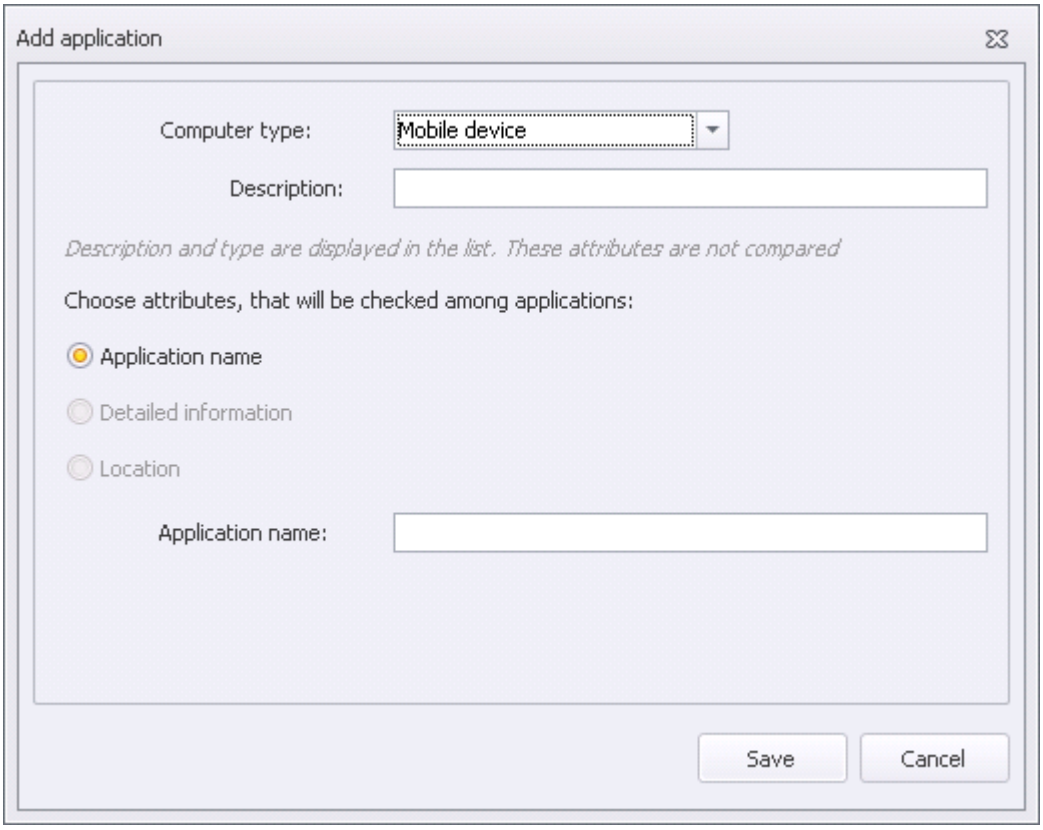
1. Go to **Applications** section.
2. On the Navigation pane select the needed filter in the **Application protocol** group.
3. On the **Application protocol** pane select one or several entries. To select several entries click at them
   while pressing **Shift** or **Ctrl** button.
4. Take one of the following steps:
   - on the **Application protocol** pane click  A**dd application to list automatically**;
   - select **Edit > Add application to list automatically** command in the main menu;
   - right-click in the **Application Protocol** pane and select  **Add application to list automatically**
     manually from the drop-down list.
5. In the appeared window:
   - select existing list

   or
6. click **Create new** then enter a list name to the **List name** field and click **Save**.
7. Click **Select**.
8. Click **OK**.

Adding Application to List Manually

To add application to the list manually:

1. Go to **Applications** section.
2. On the Navigation panel select the required filter in the **Application protocol** group.
3. On the **Application protocol** panel select one or several entries. To select several entries click on them
   while pressing **Shift** or **Ctrl** button.
4. Take one of the following actions:
   - on the **Application protocol** panel click  A**dd application to list manually**;
   - select **Edit > Add application to list manually** command in the main menu;
   - right-click in the **Application Protocol** panel and select **Add application to list manually**
     manually from the drop-down list.
5. In **Add application** window you can set parameters for application correspondence check:
   - **Application name**
     Enter the full name of the application file
   - **Detailed information**
     Filtering application by detailed information of Publisher, Product Name, Application Name.
   - **Location**
   - Filtering application by detailed information of **Location** (type in path to the file up to the folder), **Application name** (type in the file name).



6. Click **Save**.
7. If you have selected several entries, repeat steps 5 and 6 for other entries.
8. Click **OK**.

Exporting Application Protocol

To export the application protocol:

1. Go to **Applications** section.
2. On the Navigation pane, in the **List of applications** group, select the needed protocol.
3. In the **List of applications** group menu click **Export application protocol**.
4. Specify export location and click **Save**.

The protocol will be exported in .**xls** format.

5.4.4 Temporary employee access to network

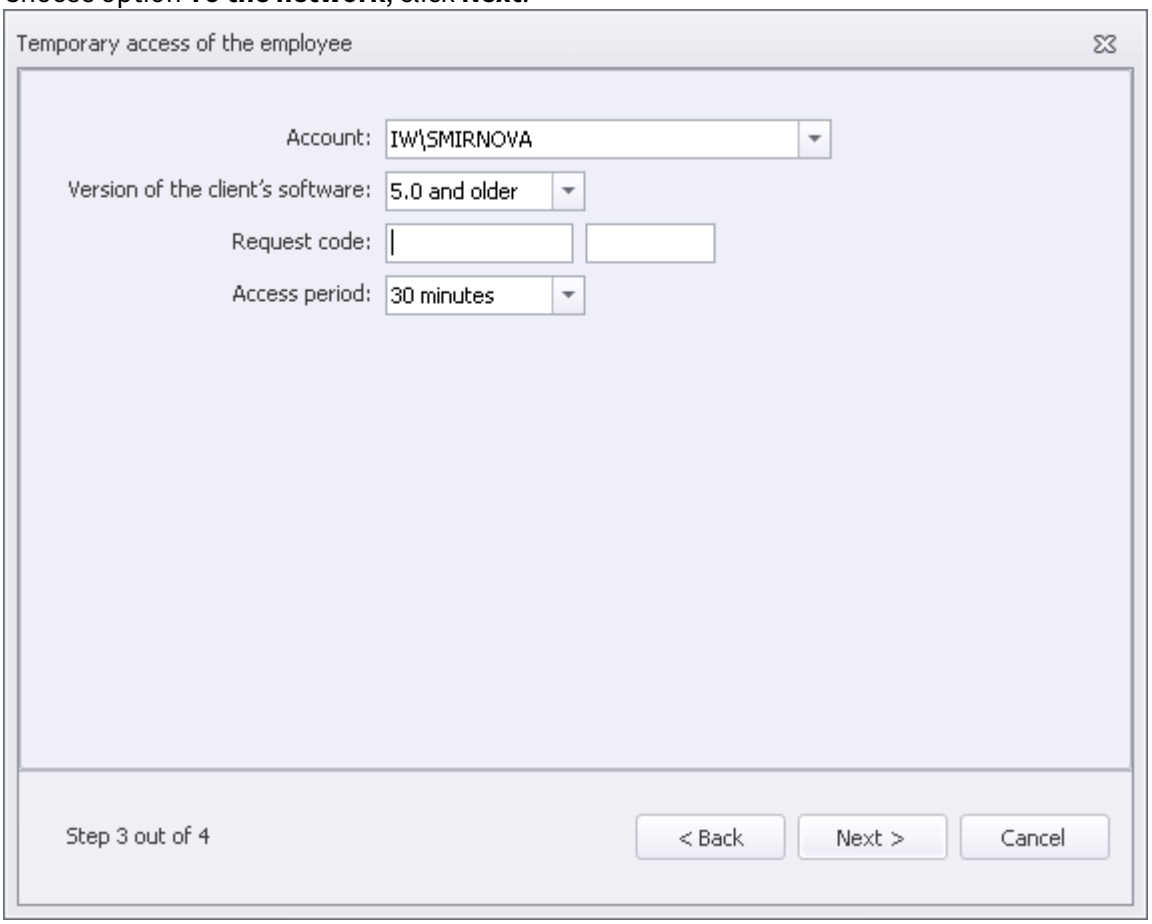
An employee for which a rule (DM) denying connections outside corporate network is active (see "Settings of Corporate Network" and "Configuring Network Monitor Rule (DM)"), can request temporary access to external connections from InfoWatch Device Monitor Agent menu, **Network control** command.

> **Warning!**
>
> An employee can request access only if the **Show tray icon** interface option is selected (see "Common Settings for Agents"). The way how to configure text displayed to an employee is described in "Employee Notifications about Policy (DM) Violations", **"Network connection forbidden. Detailed"** notification type.

An employee should send the received request code to the security officer.

To grant access to external connections for employee:

1. In main menu, select **Tools > Temporary employee access**.
2. In the dialog window, choose **Dictated by phone**, click **Next**:.
3. Choose option **To the network**, click **Next**.



4. From **Account** drop-down list, select an account of the employee to which a temporary access should be granted.
5. In **Version of client's software**, choose the version of Device Monitor Agent installed on employee's computer.
6. In **Request code** field, enter a code sent by the employee.
7. From **Access period** drop-down list, select the time period for which temporary access should be granted.
8. Click **Next**.
   The code which should be sent to the employee is displayed in **Response code** field.
9. Click **Close**.

5.4.5 Temporary Employee Access to Devices

An employee for which a rule (DM) denying using devices is active (see "Configuring Device Monitor Rule"), can request temporary access to a device from InfoWatch Device Monitor Agent menu, **Device list** tab.

Warning!

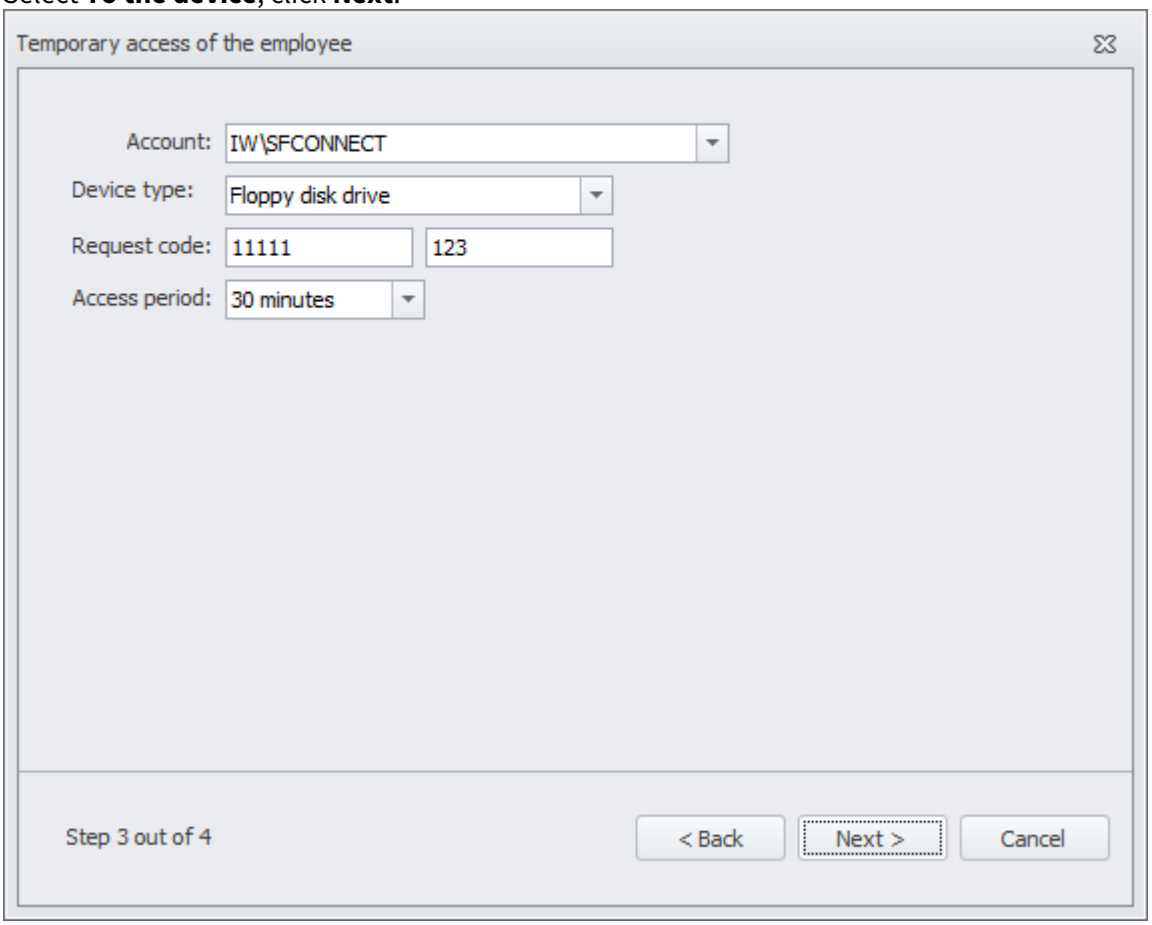
An employee can request access only if the **Show tray icon** option is selected (see "Common Settings for Agents"). On to configure the text displayed to the employee, see "Employee Notifications about DM Policy Violations", "**Access to device denied**" notification type.

The employee should send a received request code to the security officer.

You can communicate with the employee using phone or e-mail.

To grant temporary access to devices for an employee who called by phone:

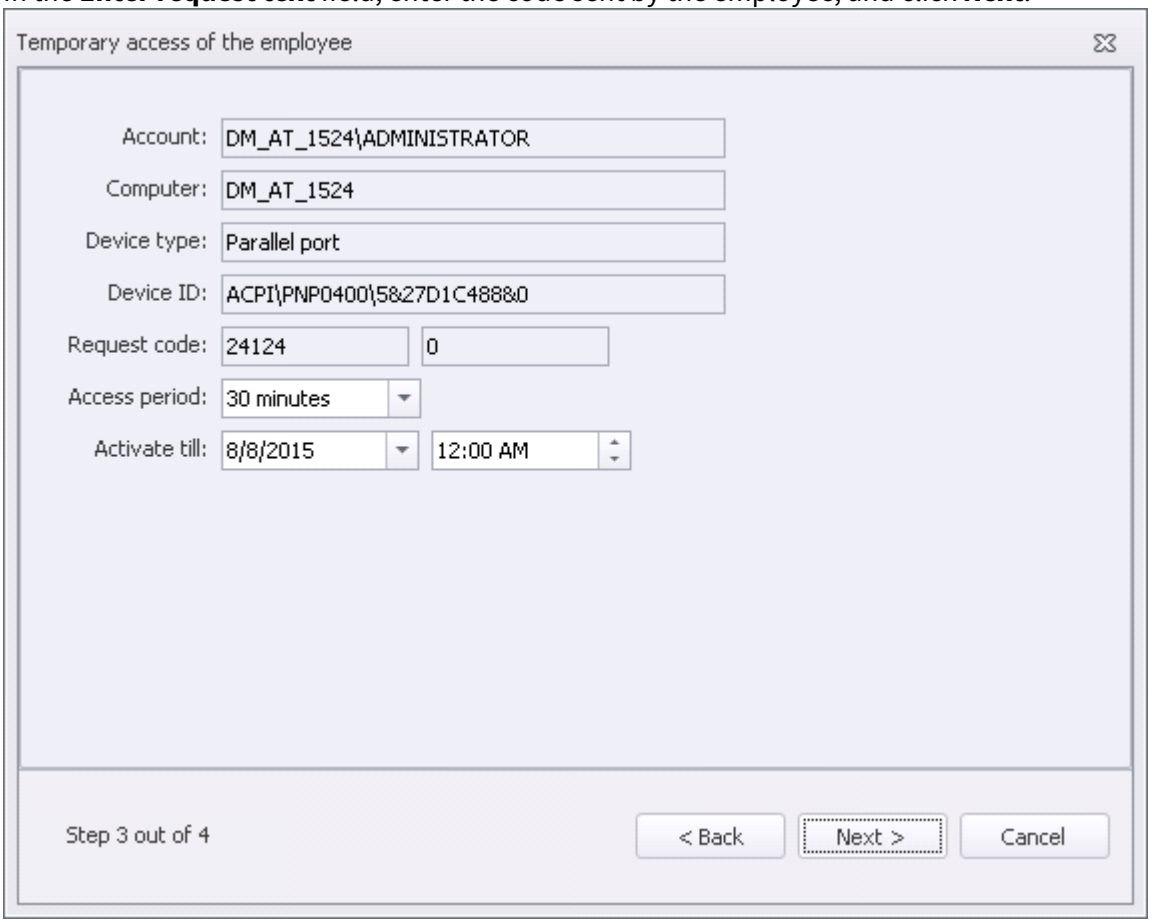
1. In Main Menu select **Tools > Temporary employee access**.
2. Select **Dictated by phone**, click **Next**.
3. Select **To the device**, click **Next**.



4. From the **Account** drop-down list, select an account of the employee to which temporary access should be granted.
5. From the **Device type** drop-down list, select the necessary device type.
6. In the **Request code** field, enter the code dictated by the employee.
7. From the **Access period** drop-down list, select the time period for which temporary access should be granted.
8. Click **Next**.
   The code you should provide to the employee is displayed in **Confirmation code** field.
9. Click **Finish**.

To grant access to devices for employee who sent an e-mail:

1. In Main Menu select **Tools > Temporary employee access**.
2. Select **Obtained via e-mail or other means of communication**, click **Next**.
3. In the **Enter request text** field, enter the code sent by the employee, and click **Next**.



4. From the **Access period** drop-down list, select the time period for which temporary access should be granted.
5. From **Activate till** drop-down lists, define the time period, when the employee can activate access to the device (after the activation, access will be provided for the time selected from **Access period** drop-down list).
6. Click **Next**.
   The code which should be sent to the employee is displayed in **Copy answer text to clipboard** field.
7. Click **Finish**.

5.5 Viewing DM Events

InfoWatch Device Monitor Agents installed on controlled computers provide keeping data on using external devices, transferring data via network connections and using instant messengers for data transfer. This information is stores as **events** and transferred to InfoWatch Device Monitor servers along with data of shadow copies. Events (unlike shadow copies) are registered in InfoWatch Device Monitor database and are available from Management Console (DM).
You can define the information logging level (keep all information on access attempts, policy (DM) violations only or save nothing) in general settings of your security schema: for further details see "Common Settings for Agents".

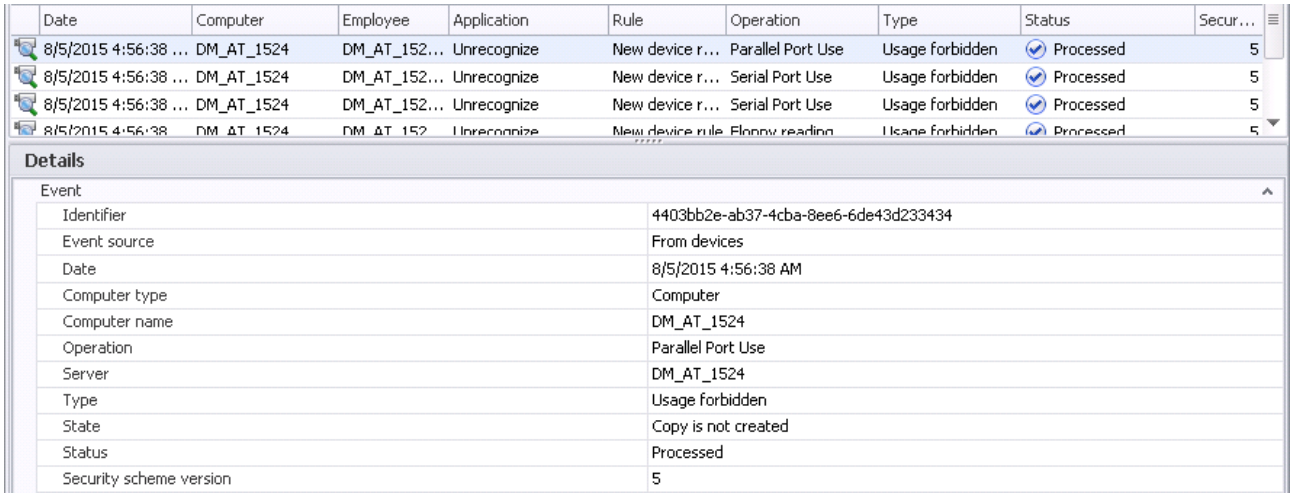
You can view events in **Events** section. To go to this section, click **Events** button on Navigation pane.

To view events,
click the filter name in the filter list.
There are two predefined filters:

- **Last: 4 hours**
- **Today**

You can create custom filters to view events, as described in "Event Filters".

Event information is displayed in a tabular list where each row contains a single record. Columns contain basic properties of log entries. Extended information on each record is available in **Details** panel.



Attribute name	Description	Available values
Common attributes		
Identifier	Unique event number	
Event source	Interceptor-based event type	• **File** – File Monitor; • **Devices** – Device Monitor; • **Printer** – Print Monitor; • **Skype, XMPP, MMP, WhatsApp, SMS** – IM Agent Monitor; • **FTP/FTPS** – FTP Monitor; • **HTTP/HTTPS** – HTTP(S) Monitor; • **Mail** - Mail Monitor; • **Network** – Network Monitor; • **Mobile device camera** - Photo Monitor; • **System** - event on ending disc space for shadow copy saving. *Such event is not transferred to Traffic Monitor.*

Date	Event date and time (in hours and minutes) registered on the computer. Device Monitor server keeps an event in UTC, and Management Console (DM) displays it according to the local time of a computer where Console (DM) installed	
Computer type	Indicates if the computer where the event arisen is the workstation or mobile device	• Workstation • Mobile device
Computer name	Name of the computer that registered the event	
Operation	Employee initiated action or attempt	
Server	Name of InfoWatch Device Monitor server the Agent transmits event information to	
Application	Executable file name and/or name of the process responsible for the action, if detected	
Type	Action-based event type	• **Record** – adding or changing data (including renaming) on external device; sending files via messenger; sending print jobs to printer; sending data via FTP/FTPS. • **Use** – connecting an external device that allows unmonitored read/write operations or sending messages; • **Violation** – IM Agent interceptor user-initiated violation; • **Warning** – user-initiated a ban or didn't give consent to use IM Agent plug-in, while monitoring is required by security policy (DM). • **Usage forbidden** – attempt of sending data via forbidden channel.
Status	Status of event processing on the server and sending to Traffic Monitor server	• **New** • **Awaiting for proceeding** • **Awaiting for sending to TM** • **Sent to TM** **Note**: If the Server is in standalone mode then the event has the **Processed** status only

Security schema version	Number of security schema version that was active on the computer when the event was registered	
Operation verdict	Attribute of allowed action. For Devices events (**Device Monitor** rule) the blocking is also available.	• **Allowed** • **Forbidden** – only for Devices events • **Unprotected data copying is disabled** – only for Devices events • **Allowed (in white list)** - for whitelisted device events
Employee	Name of the domain (computer name outside the domain) and user login used for event registration or operating system reference for events outside user sessions	
Rule (DM)	Name of policy (DM) rule (DM) managing the event	
Terminal agent	Terminal agent name, if detected	
Network address of a terminal agent	Terminal agent IP, if detected	
For events with *File* source		
Assign	Full target file name	
File size	Target file size	
Object status	Shadow copy of transferred data	• **no copies created** - rule (DM) does not require shadow copying • **copy created** - shadow copy created successfully • **copying error** - for example, if there is no free space on the agent
Device description	Target device instance or model ID	

For events with *Devices* source		
Device type	For supported device types list see "InfoWatch Device Monitor Functions"	
Device instance or model identifier	Model identifier (VID) and serial number (PID) of external device or printer used for the operation	
Device description	Device description received from OS of the computer where the Agent is installed	
For events with *Skype, XMPP, MMP, WhatsApp, SMS source*		
IM user ID	UIN of the user authorized in the messenger at computer	
Object status	Shadow copy of transferred data	• **no copies created** - rule (DM) does not require shadow copying • **copy created** - shadow copy created successfully • **copying error** - for example, if there is no free space on the agent
List of senders	UIN of IM users, who sent the message/file via messenger	
List of recipients	UIN of IM users, who received the message/file via messenger	
File name	Full name of transferred file	
File size	Transferred file size	
Shadow copy	File, message or chat shadow copy	• **No** - no shadow copy was created • **Yes** - shadow copy created successfully
For events with *Printer* source		
Document	Full name of the file sent to print	

Printer	Name of target network printer	
Object status	Result of creating a shadow copy of the print job	1. Shadow copy of print job was successfully created. The job contained graphic and text data. 2. Shadow copy of print job was not created. The job contained no graphic or text data. 3. An error occurred while creating a shadow copy of print job. 4. Shadow copy of print job was successfully created. The job contained only graphic data. 5. The shadow copy should not have been created. 6. Shadow copy of print job was partially created. Graphic data were fully processed. Text data were partially processed. 7. Shadow copy of print job was partially created. Graphic data were partially processed. Text data were fully processed. 8. Shadow copy of print job was successfully created. The job contained only text data. 9. Shadow copy of print job was partially created. Graphic data were partially processed. The job contained no text data. 10. Shadow copy of print job was partially created. The job contained no graphic data. Text data were partially processed.
Object status	Result of creating shadow copy of transferred data	• **no copies created** - rule (DM) does not require shadow copying • **copy created** - shadow copy created successfully • **copying error** - for example, if there is no free space on the agent
For events with *FTP/FTPS* source		

Object status	Result of creating shadow copy of transferred data	• **no copies created** - rule (DM) does not require shadow copying • **copy created** - shadow copy created successfully • **copying error** - for example, if there is no free space on the agent
Sender	Name used for employee authorization at FTP server	
FTP server	Name or IP address of FTP server	**Note**: When using the FTP via proxy server this field can contain proxy address instead of FTP.
Relative path	Directory at FTP server where to the file is transferred	
File name	Full name of transferred file	
Real file size	File size calculated after transfer	
Declared file size	File size according to data of application which performs a transfer to FTP server (browser for example)	
Starting point	When file is transferred by piecemeals, position which starts the of the current part transfer.	
Shadow copy	Result of creating file shadow copy	• **No** – shadow copy was not created • **Yes** – shadow copy created successfully
For events with *HTTP or HTTPS* source		
State	Result of creating shadow copy	• **no copies created** - rule (DM) does not require shadow copying • **copy created** - shadow copy created successfully • **no free space on disk** - agent does not have enough free space • **copying error** - for example, if there is no free space on the agent
Reciever DNS	DNS name of a computer	

Reciever IP	IP-address of a computer	
Request size	Size of a request in Kbps	
Rule (DM)	Name of policy (DM) rule (DM) managing the event	
For events with *Mail* source		
State	Result of creating shadow copy	• **no copies created** - rule (DM) does not require shadow copying • **copy created** - shadow copy created successfully • **no free space on disk** - agent does not have enough free space • **copying error** - for example, if there is no free space on the agent
Sender	DNS name of a sender computer	
List of recipients	Receiver addresses	**Note**: For events with a large number of senders you should remember that when Device Monitor Management Console can't display more than 1024 symbols in this field. However, if the shadow copy is set for this event then Traffic Monitor will receive and display the full list of recipients (under 4000 Bytes).
Subject	Mail Subject	
Transmission type	Used protocol	
Message type	Mail direction	• **Incoming** • **Outgoing**
Size, bite	Size in bites	
Channel type	Encrypted or not encrypted	• **All channels** • **Encrypted channel**
Rule (DM)	Name of policy (DM) rule (DM) managing the event	

For events with *Network* source		
Time of ban removal starts	For *Network* operations temporary ban removal operation - start of temporary access period. See details in "Temporary Employee Access".	
Time of ban removal ends	For *Network* operations temporary ban removal operation - end of temporary access period. See details in "Temporary Employee Access".	
Connection server	For *Connection forbidden* operation - address or name of forbidden server which was attempted to gain access to	
Port	For *Connection forbidden* operation - the port number used for connection attempts.	
For events with *Mobile* device camera source		
Photo size	Size of photo a shadow copy, in bytes	

If needed, you can free some space in the database by deleting all the information about already processed events (**Processed** or **Sent to Traffic Monitor** state). See details in "Deleting Events".

5.5.1 Event Filters

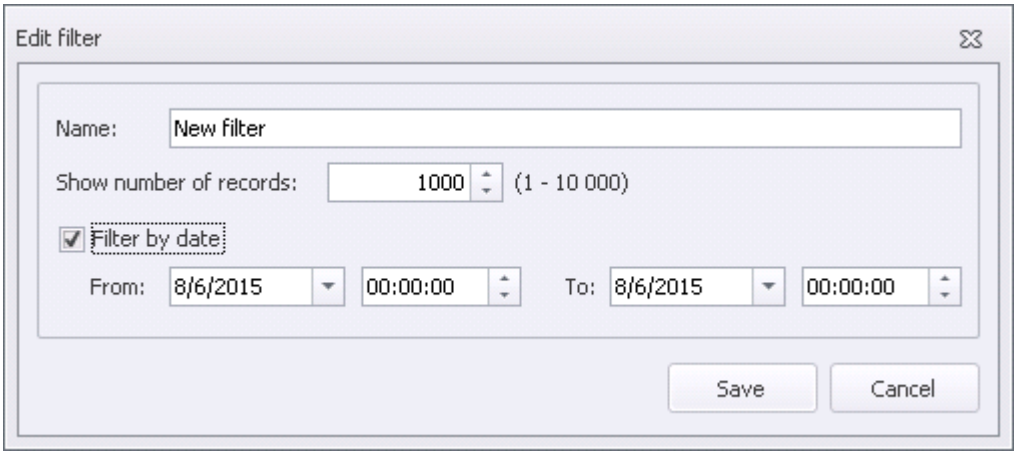
In addition to predefined filters you can create custom filters to view event information.

To add or edit a filter:

1. Go to **Events**.
2. Follow the necessary steps:

Action	Steps
Creating filter	• in Main Menu select **Edit > Add Filter**; • click **Add Filter** at the top of Navigation pane.
Editing filter	1. In **Events** area of Navigation pane, select the name of the filter you want to edit. 2.Take one of the following steps: • in Main Menu click **Edit > Edit Filter**; • click **Edit Filter** at the top of Navigation pane; • double-click selected filter name.

These actions open Edit filter dialog.



3. Specify filter options in **Edit Filter** dialog:
   - **Filter Name**.
   - **Show number of records**. Limit on the number of entries displayed in Management Console (DM) workspace (1000 records by default).
   - To filter by a date, flag **Filter by date** box and specify the desired period in From and To fields. Set the date and time in right and left field respectively.

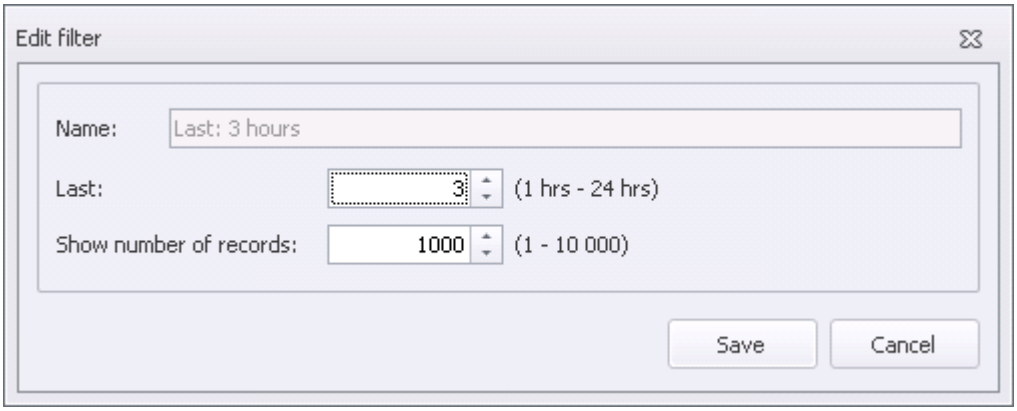
> **Note:**
>
> For the predefined filters **Filter Name** and **Filter by date** parameters cannot be edited.

4. Click **Save**.

The predefined filter **Last: 4 hours** has another editing interface and lets to make filters displaying events for last several hours.

To edit predefined filter to view events for the selected number of hours:

1. In **Events** area of Navigation pane, select the **Last: 4 hours** filter.
2. Take one of the following steps:
   - in Main Menu click **Edit > Edit Filter**;
   - click **Edit Filter** at the top of Navigation pane.
   - double-click the filter name.



3. Specify filter options in **Edit Filter** dialog:

- **Last**. Specify the number of hours, entries for which should be displayed in the Management Console (DM) workspace.
- **Show number of records**. Limit on the number of entries displayed (1000 records by default).

4. Click **Save**.

5.5.2 Deleting Events

The information about already processed events (**Processed** or **Sent to Traffic Monitor** state) can be deleted.

You can delete events:

- for certain time period;
- all matching certain filter.

To delete from the database an information about events for a period:

1. Go to **Events**.
2. Take one of the following steps:
   - click **Delete events** at the top of Navigation pane.
   - in Main Menu click **Edit > Delete events**.
3. In the opened dialog window **Deleting from database**, specify needed time period for which you want to delete events.
4. Click **Delete**.

Then a number of deleted events will be displayed.

To delete from the database an information about events matching certain filter:

1. Go to **Events**.
2. In the filter list select needed filter name.
3. Take one of the following steps:
   - click **Delete filter events**at the top of **Events** area.
   - in Main Menu click **Edit > Delete filter events**.
4. In request box select **Yes** to confirm.

Then a number of deleted events will be displayed.

5.6 Agent Remote Installation, Updating and Uninstallation

You can install, update, or delete InfoWatch Device Monitor Agents from a computer via InfoWatch Device Monitor Management Console (DM). These operations are performed through **tasks**. You can run tasks to install, update or remove agent software, change uninstallation password, or monitor these processes.

Remote agent management is carried out by special **Distribution Agent** transmitted onto agent workstations. The Agent requires the following:

- Target computers must meet hardware and software requirements: see the document "*InfoWatch Traffic Monitor. Installation guide*", "InfoWatch Device Monitor Agent Hardware and Software Requirements" article.
- Proactive virus protection for computers must be turned off at the time of installation (only for agents on MS Windows OS).
- Device Monitor server and target computers should resolve each other by domain names.

- On computers, where firewall, different from windows standard one, is installed, it should be disabled. Except for disabling, you can also allow any network connections for the following Device Monitor components: `IWDeployAgent.exe`, `iwdmc.exe`, `DM.Client.exe`, `IWProxy.exe`, `rmtlogctr.exe` (only for agents on MS Windows OS).

> **Note:**
>
> To install Agent on Windows 7 computer, go to **Control Panel -> Network and sharing center -> Change advanced sharing settings**. Enable file and printer sharing. Upon completion, **Distribution Agent** can be copied to the computer. The firewall will be automatically configured.

To go to Management Console (DM) task section, use **Tasks** button on Navigation pane.

Tasks management guidelines are available in:

- View Tasks;
- Preparing Primary Agent Installation;
- Creating Primary Distribution Task;
- Creating Update Task;
- Creating Uninstallation Password Reset Task;
- Creating Uninstallation Task;
- Launching, Pausing, Editing, and Deleting Tasks;
- ClienAgent Installation Errorst Installation Errors.

You can also install and upgrade your Agent with software distribution tools (for example, via Microsoft Active Directory group policies (DM)). For more information see the document "*InfoWatch Traffic Monitor. Installation guide*", "Agent Installation via Software Distribution Tools" article. To run these operations, use installation package that was created as described in "Creating Installation Package".

5.6.1 Viewing Tasks

Tasks area of Navigation pane displays a list of all created, executed and outstanding tasks. Main screen work pane displays a list of target computers for the selected task.

Details panel displays the following parameters for selected task:

Parameter	Description
Name	Original name of the task
Description	Original description of the task
Type	One of the following task types: • Primary distribution • Change password • Update • Uninstall

Status	Current task status. Possible values: • Executing • Stopped • Completed
Restart period, min	Intervals between task launches on the computer, if the previous attempt failed, in minutes. Counted from ending the last workstation proceeding in previous task launch. If the task fails, it won't be launched again.
Number of restart trials	The maximum number of retries to restart distribution task on the computer. If all attempts have been used, **Task status** parameter value will be set to **Error** (for further details, see "Agent Installation Errors").
For primary distribution tasks	
Show employee notifications	Indicates that employee's attempt to perform a banned action will trigger a warning. For further details, see "General System Settings", "Creating Installation Package" and "Employee Notifications about Policy (DM) Violations"
Hide presence of agent on workstation	Indicates if Windows system tray of managed computer hides Agent presence on the computer. Otherwise, Windows system tray of the computer where Agent installed will display  icon. By clicking this icon, information on DM Agent operation and list of currently controlled devices are displayed. **Warning!** If there is an antivirus protection enabled on the managed computer then the antivirus program can reveal the operation of Device Monitor: for example, in the list of processes running on the managed computer or in the list of programs that initiate a control.
Install the component of network connections control	Indicates if `iw_proxy` component is installed.
Install the component of network connections control	Indicates if Network Monitor interceptor is installed.
Uninstallation product password	Shows if the password requested from the employee who attempts to remove Device Monitor Agent.
Proxy Root Issuer DN	The unique name of Device Monitor proxy server certificate, issuer distinguished name.
For primary distribution and update tasks	
Installation directory	Installation directory for Device Monitor Agent at target computers.

Installation login	Name of the Console (DM) user that launches the task on computers.
Waiting fir restart duration, hours	Computer reboot waiting period (in hours); if the computer is not restarted manually during this period, the System will notify the employee (if notifications are enabled), and force operating system restart.
Duration of restart notifications, hours	Period of displaying requests for rebooting the computer, in hours.
Restart notifications rate, min	Time intervals between repeated reboot requests, in minutes.
Reboot messages	Text displayed to the employee in reboot request.
Show a warning before forced reboot	Indicates if a notification about forced reboot will be displayed when reboot wait durations are expired but the employee did not reboot the computer.
For change password tasks	
Uninstallation product password	Shows if the password requested from a user who attempts to remove Device Monitor Agent.

Each target computer's main screen workspace displays the following parameters:

Parameter	Description
Address	Computer IP address or domain name
Status	Current status of task for the relevant computer. Possible values: • **Not running** • **Prepare to start** • **In progress** • **Waiting for reboot** (only for installation and upgrade tasks) • **Error** (for further details, see "Agent Installation Errors") • **No access** • **Completed**
Agent version	Agent version currently installed on the computer.
Operation system	Computer operating system.

System type	Type of operating system on the computer: x64 or x32.
Connections count	Number of connection attempts to the unavailable computer.
Time	Date and time of the last connection to the computer.

5.6.2 Preparing Primary Agent Installation. Distribution Agent

Remote agent installation is carried out by InfoWatch Device Monitor special **Distribution Agent**.

For correct remote installation of agents, workstations should meet hardware and software requirements: see the document "*InfoWatch Traffic Monitor. Installation guide*", "InfoWatch Device Monitor Agent Hardware and Software Requirements" article.

Besides, for workstations installed on Windows OS, the following conditions should be met:

- Proactive virus protection for computers must be turned off.
- Computers with the firewall that differ from Windows firewall, that firewall:
  - should be disabled
    or
  - should have a permission for InfoWatch Device Monitor Distribution Agent
    or
  - should have **15505** port (default port by which the Distribution Agent waits for a connection) opened for incoming connections, if it was not changed in connection settings (see the document "*InfoWatch Traffic Monitor. Installation guide*", "<applicationSettings> section" article, **CommunicationPort** parameter).

Additional requirements vary depending on the distribution method:

Method 1:

Distribute `Setup.DeployAgent.msi` installation package (provided along with installation software) to target computers.

Method 2:

For workstations installed on Windows OS, perform actions required for transmitting the Distribution agent through shared administrative resources:

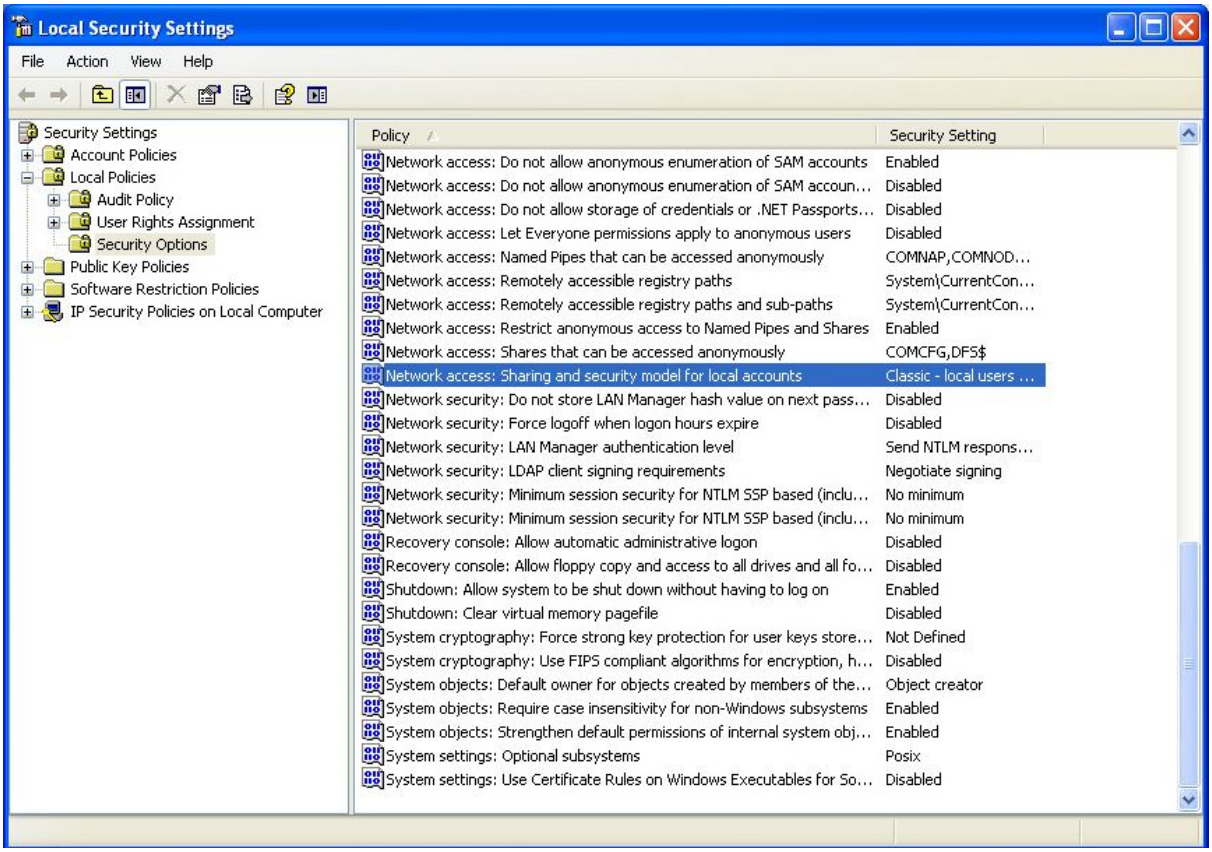
- Computer firewalls must be either turned off or required permissions must be provided: see "Firewall Settings".
- Specify settings for network access to shared resources: see "Enabling Shared Administrative Resources".

If all requirements are met, you can create and then start primary distribution tasks.

Enabling Shared Administrative Resources

To transfer InfoWatch Device Monitor distribution agent to target computers with Windows OS through shared administrative resources, make sure that the following requirements are met:

- If a workstation with Windows XP is outside the domain, in the local security policy settings (**Control Panel** -> **Administrative Tools** -> **Local Security Policy** -> **Security Options**) on this workstation, set the **Network access configuration parameter: Sharing and security model for local accounts** parameter value to `Classic`.



- Shared administrative resources (like `\\computername\admin$`) must be enabled on workstations (in Windows Vista and Windows 7, they are disabled by default). To enable them:
  1. Make sure that sharing of files and printers is enabled. In Control Panel, open **Network and sharing Center -> Change advanced sharing settings**. In the desired profile, enable file sharing and printer sharing.
  2. In the registry, in `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System` path, add **DWORD (32-bit)** parameter named **LocalAccountTokenFilterPolicy**. Set its value to **1**.

     > **Note:**
     >
     > After you add the parameter in the registry, you need to log into the System again.

Firewall Settings

Firewall settings requirements:

Application protocol	Transport protocol	Port
RPC	TCP	135
RPC over HTTPS	TCP	593

NetBIOS Datagram Service	UDP	138
NetBIOS Name Resolution	UDP	137
NetBIOS Session Service	TCP	139
SMB	TCP	445

For computer availability defining quickness the ICMP protocol should be permitted.
For Windows firewall the "**File printing and sharing**" preset rule should be permitted.

5.6.3 Creating Primary Distribution Task

Primary distribution (installation from Management Console (DM)) of InfoWatch Device Monitor Agent using installation **agents**. Installation agent is an executable file. It is passed on to computers and starts automatically during task execution, receiving Agent updates from the server.

> **Warning!**
>
> If server account doesn't have administrator rights on all target computers, primary Device Monitor Agent distribution will require credentials of an account having administrator rights at:
>
> - all target computers
> - a computer where Management Console (DM) is running
> - a computer where Device Monitor server is running
>
> If a password of used account is expiring (Windows warns that the password expires in 3 days and need to be changed) then primary distribution task cannot run on behalf of this user.
>
> If you are unable to enter administrator name and password, you can create your own InfoWatch Device Monitor Agent installation package (see "*Traffic Monitor. Installation guide*", article "Creating Installation Package") and install it by other means (see "*Traffic Monitor. Installation guide*", article "Standard InfoWatch Device Monitor Agent Setup" and "Agent Setup via Software Distribution Tools").

> **Warning!**
>
> If the workstation has Kaspersky Internet Security installed then you need to disable its self-protection to install the InfoWatch Device Monitor Agent. See internet article "How to enable/disable self-defense in Kaspersky Internet Security" internet article.

To create a primary InfoWatch Device Monitor agent application distribution task:

1. Go to **Tasks**.
2. Take one of the following steps:
   - in the Main Menu select **Edit > Add Task**;
   - click **Add Task** at the top of Navigation pane.

   These actions open **Deployment task wizard** dialog.
3. Enter the task name, select **Initial deployment task** (to install the agent on computers with Windows OS) or **Initial deployment task (Linux)** (to install the agent on computers with Astra Linux OS) and enter the task description, then click **Next**.
4. Create a list of computers which you need to install Device Monitor Agent to. To add a computer (or several computers):

a. Click **Add Select computer** dialog will display a list of computers from:
   - from a directory;
   - Microsoft Windows Network;
   - from ALD tree;
   - ones registered before (for example, after manual Agent installation) and belonging to computer groups (**DM server computers** node).

b. Flag computers or computer groups. Minimized groups are marked with an icon ; expanded - . Doubleclick a group, to expand or collapse it.
   You can also specify computer names or IP addresses:
   - in the line at the bottom of dialog box. When listing addresses, separate them with semicolons;
   - click **Import** and download text file where one entry should be placed in the each line; text should
     contain no blank lines.

c. After you specify the computers you want to add, click Select. The dialog will be closed and selected computers list will be displayed in **Task target computers list** area. To remove a computer from the list, select it and click **Remove**. When you make a full list of computers click **Next**.

5. Then InfoWatch Device Monitor servers currently registered in the System are displayed. You can change Agent installation directory (%Program Files%\Infowatch\DeviceMonitor\Agent is used by default).

   Important!

   Path to the catalogue may contain the following characters: 0-9, a-z, A-Z, ":", ".", "_", "-", "\", " ". If the path includes other characters, the agent installation will be incorrect.

   Click **Next**.
6. The unique name of Device Monitor proxy server certificate (Issuer Distinguished name, Proxy Root Issuer DN) will be displayed. You can change it with accordance to X.509 standard, CN (Common Name) field is mandatory, all fields comma-separated. Click **Next**.
7. Specify options of computer reboot:
   - **Wait for reboot without notifying the employee**. The Agent can:
     - start notifications immediately (*Do not wait* option),
     - start notifications in specified time (*Wait for option* - please specify the time period to start notifications),
     - or do not notify at all (*Wait infinitely* option).
   - **Notify the employee about reboot necessity and wait for reboot**. Upon completing reboot waiting in "silent" mode (see **Wait for reboot without notifying the employee** setting) or immediately after installation ends, Device Monitor Agent starts to notify employee on reboot necessity:
     - during specified time period (*Notify within option*);
     - permanently (*Notify infinitely* option);
     - do not notify at all (*Do not notify* option).

     If needed, change continuance and frequency of notifications appearance and enter the text of the message displaying in reboot notification.

- **Show a warning before forced reboot**. If this check box is flagged, then the Agent displays a notification about forced reboot and allows 5 minutes to end operations. Then the computer will be forced to reboot. If the option is not checked then the forced reboot (if it should be made according your settings) will be performed unexpectedly for the employee.

> **Warning!**
>
> Forced reboot is performed if neither **Wait while employee reboots computer** setting, nor **Show a warning before force reboot** setting is flagged, or their wait durations are expired but the employee did not reboot the computer.

Click **Next**.

8. Configure Agent settings:
   - To protect Agent application from deleting by an employee, enter the password that will be requested when trying to uninstall the Agent and confirm it.
   - **Show employee notifications** - if employee attempts to perform an action restricted by security policy (DM), a warning will be displayed. For further details, see "Employee Notifications about Policy (DM) Violations".
   - **Hide Agent presence** - indicates if Windows system tray of managed computer hides Agent presence on the computer.

> **Warning!**
>
> Not notifying the user about interceptor operation may contradict the applicable laws of your country.

> **Important!**
>
> Hiding/notifying settings apply on the Agent up to the first call to the server. On calling to the server, the Agent will start using settings of the group the workstation belongs to.

> **Warning!**
>
> If there is an antivirus protection enabled on the managed computer then the antivirus program can reveal the operation of Device Monitor: for example, in the list of processes running on the managed computer or in the list of programs that initiate a control.

If this option is not selected, the Windows system tray of the computer where the Agent is installed will display  icon. By clicking this icon, information on DM Agent operation and the list of currently controlled devices is displayed.

- **Install the component of network traffic interception** - installs **iw_proxy** component on a computer.
  The component will not be installed if you leave the checkbox empty.
- **Install the component of network connections control** - installs **Network Monitor** interceptor on a computer. The component will not be installed if you leave the checkbox empty.

> **Warning!**
>
> It is not recommended to install the component of network perimeter control to the image that would become the base image of VDI framework under control of Citrix Provisioning Services, since it would cause the technology breach and would break the whole scheme performance.

- Task run parameters: they will be used in case the task wasn't launched at the first attempt. Specify the number of attempts and their intervals, in minutes.
- To launch a task immediately after saving, flag **Run task immediately** check box.
- Enter the credentials for the account that launches the task.This account must have administrator rights on all target computers.

> **Warning!**
>
> The System does not save passwords for accounts used to launch tasks. If the new task is not launched immediately, you will have to use password next time to launch it from Management Console (DM).
> If a password of used account is expiring (Windows warns that the password expires in 3 days and need to be changed) then primary distribution task cannot run on behalf of this user.

Click **Next**.

9. Look through the task summary. If you need to change any settings click **Back** to return. If all settings are correct, click **Finish**.

5.6.4 Creating Update Task

> **Warning**
>
> You need to update agents with a primary distribution task (see. Article "Creating Primary Distribution Task") when updating the DM to version 6.7, otherwise errors may occur. When upgrading to all other versions, the procedure described in this article is used.

Updating InfoWatch Device Monitor Agents is required after updating InfoWatch Device Monitor server: for details, see the document "*InfoWatch Traffic Monitor. Installation guide*", "Updating InfoWatch Device Monitor Server End" article.

Note:

Besides the method described below, you can create the update task with a simplified function as described in the document "*InfoWatch Traffic Monitor. Installation guide*", "Updating Agents at Managed Computers" article.

To create and schedule an update task for InfoWatch Device Monitor Agents:

1. Go to **Tasks**.
2. Take one of the following steps:
   - in the Main Menu select **Edit > Add Task**;
   - click **Add Task** at the top of Navigation pane.

   These actions open **Deployment task wizard** dialog.
3. At step1, select **Update task** (to update computers with Windows OS) or **Update task (Linux)** (to update computers with Astra Linux OS), enter the task name and description and click **Next**.
4. At step 2, create a list of computers where Device Monitor Agents should be updated. To add a computer (or several workstations):
   a. Click **Add**. The **Select computers** dialog, **DM server computers** node, contains the list of computers where Device Monitor Agent version does not match Device Monitor Server version but can be automatically updated (agent software version should be 4.0.651 and higher).
   b. Flag computers or computer groups. Minimized groups are marked with an icon ; expanded - with . Double-click a group, to expand or collapse it.
   c. Use **Filter by computer name** field to specify computer. Click **Find**.
   d. After you specify the computers you want to add, click **OK**. **Select computers** dialog will be closed. Selected computers list will be displayed in **Task target computers list** area. To remove a computer from the list, select it and click **Remove**.

   When you make a full list of computer, click **Next**.
5. At step 3, specify parameters of restarting computers:
   - **Wait for reboot without notifying.** The Agent can**:**
     - Notify immediately (*Do not wait* parameter),
     - Notify after specified time period (*Wait for hour(s)* parameter - you need to specify the time before notification),
     - Do not notify the employee (*Wait infinitely* parameter).
   - **Notify the employee about reboot necessity and wait for reboot.** After "silent mode" wait to notify (see Wait for reboot without notifying setting), or right after update process completion, Device Monitor Agent will start to notify the employee about reboot necessity during specified time period (*Notify within hour(s) within: minutes* parameter) or infinitely (*Notify infinitely every x minutes*), or not notify (*Do not notify*). When necessary, change length and frequency and specify the text of the message, which will be displayed along with the notification.
   - **Show a warning before reboot** - is a parameter to specify whether forced reboot notification will be displayed (an employee can complete current tasks within 5 minutes before forced reboot) or forced reboot will be performed without any additional text.
6. At step 4, specify:
   - Task retry parameters: they will be used in case the task wasn't launched at the first attempt; if launching failed, the task won't be launched again. Specify the number of attempts and their intervals, in minutes.

- To launch a task immediately after saving, flag **Run task immediately** check box.

Click **Next**.

7. Look through the task summary. If you need to change any settings click **Back** to return. If all settings are correct, click **Finish**.

> **Warning!**
>
> If the computer has the Kaspersky Internet Security installed then you need to disable its self-protection function for successful InfoWatch Device Monitor Agent update.
> See details in internet article "How to enable/disable self-defense in Kaspersky Internet Security".

5.6.5 Creating Uninstallation Password Reset Task

To create and schedule InfoWatch Device Monitor agent update task:

1. Go to **Tasks**.
2. Take one of the following steps:
   - in the Main Menu select **Edit > Add Task**;
   - click **Add Task** at the top of Navigation pane.

   These actions open **Deployment task wizard** dialog.
3. Select **Change uninstall password task**, enter task name and description and click **Next**.
4. Create a list of computers that need their uninstallation passwords to be changed on **Deployment target computers** screen. To add a computer (or several computers):
   a. Click **Add**. The **Select computers** dialog, **DM server computers** node, contains the list of computers where Device Monitor Agent is installed.
   b. Flag computers or computer groups. Minimized groups are marked with an icon ; expanded -. Double-click a group to expand or collapse it. Use **Filter by computer name** field to specify the computer. Click **Find**.
   c. After you specify the computers you want to add, click **ЬISelect**. The **Select computers** dialog will be closed.
   Selected computers will be displayed in the **Task target computers list** area.
   To remove a computer from the list, select it and click **Remove**.

   When you specify all required computers, click **Next**.
5. Specify:
   - **Password** which is required to delete Device Monitor Agent. In the **Confirm** field, retype the password.
   - **Task running parameters**: they will be used in case the task wasn't launched at the first attempt; if launching failed, the task won't be launched again. Specify the number of attempts and their intervals, in minutes.
   - To launch a task immediately after saving, select the **Run task immediately** check box.

   Click **Next**.
6. Look through the task summary. If you need to change any settings, click **Back**. If all settings are correct, click **Finish**.

5.6.6 Creating Uninstallation Task

To create a centralized task that removes InfoWatch Device Monitor agents:

1. Go to **Tasks**.
2. Do either of the following:
   - from the main menu, choose **Edit** > **Add task**;
   - use **Add task** button which is located at the top of the **Tasks** section.

   The **Deployment task** wizard dialog box will appear.
3. At step 1, select **Uninstall task** (to delete the agent from a computer with Windows OS) or **Uninstall task (Linux)** (to delete the agent from a computer with Astra Linux OS), enter the task name and description, then click **Next**.
4. At step 2, create a list of computers, from which you want to uninstall Device Monitor Agent. To add computers:
   a. Click **Add**. The **Select computers** dialog box will open. The **DM server computers** node contains the list of computers, where Device Monitor Agent is installed. You can also use the search field **Filter by computer name**. Enter the computer name and click **Find**.
   b. Flag required computers or computer groups. Minimized groups are marked with ; expanded ones are marked with . To expand or collapse a group, double-click its name. You can also list computer names or IP addresses:
      - manually in the row at the bottom of the dialog box; items in the list should be separated by a semicolon;
      - by clicking **Import** and loading a text file with IP addresses or DNS names of computers: each entry should start with a new line; there should be no empty lines in the file.

   c. After you specify the computers you want to add, click **Select**. Selected computers list will be displayed in **Task target computers list** area.

   To remove a computer from the list, select its name and click **Remove**.
   If all required computers are present in the list, click **Next**.
5. At step 3, specify restart options for the task: they will be used if, for some reasons, the task was not started at the first attempt; if the task start failed with an error, the task will not be started again. Specify the number of attempts and the interval between attempts in minutes.
   To launch the task immediately after saving, select **Run task immediately** check box.
   Click **Next**.
6. View the task summary. If you need to change some settings, click **Back**. If all settings are specified correctly, click **Finish**.

> **Important!**
>
> If Kaspersky Internet Security is installed on a computer, then, before uninstalling InfoWatch Device Monitor Agent applications, you should disable self-defense in Kaspersky Internet Security.
> For more details, see "How to enable/disable self-defense in Kaspersky Internet Security".

5.6.7 Launching, Pausing, Editing, and Deleting Tasks

If you flagged **Launch task immediately** when creating a task, it will start immediately. Otherwise, you will need to launch the task manually. You may need this option if for some reason you had to stop the task and want to start it again.

For instructions, see the table below.

To perform any of these actions, you must first select a task from the list on the **Tasks** panel.

> **Important!**
>
> When you run a task of deploying/updating/deleting agents on Astra Linux, you need to enter a login and a password to get authorized on workstations. The user whose login and password are used for launching the task must be in the `sudo users` list on workstations specified in the task.

Action	Steps
Start task	• in the Main Menu select **Edit > Perform** task; • click **Perform task** located at the top of Navigation pane.
Stop task	• in the Main Menu select **Edit >Stop task**; • click **Stop task** at the top of Navigation pane.
Edit list of computers in task	• at the top of **Task execution result** panel click **Add computer** or **Exclude computer from task** • right-click computer row and select **Add computer** or **Exclude computer from task**. **Warning!** You can't remove a computer if the task is running and not completed.
Edit task	• in the Main Menu select **Edit > Edit**; • click **Edit** at the top of Navigation pane. • right-click on task name and select **Edit**. Specify new settings for the task like it is done for a new task (see "Creating Primary Distribution Task", "Creating Updating Task", "Creating Uninstallation Password Reset Task", "Creating Uninstallation Task")
Delete task	• in the Main Menu select **Edit > Delete**; • click **Delete** at the top of Navigation Pane. • right-click on task name and select **Delete**. **Warning!** You can't remove a task with computer that has a running task.
View computer error log	• at the top of **Task execution result** panel click **Computer log** • right click computer row and select **Computer log**

5.6.8 Agent Installation Errors

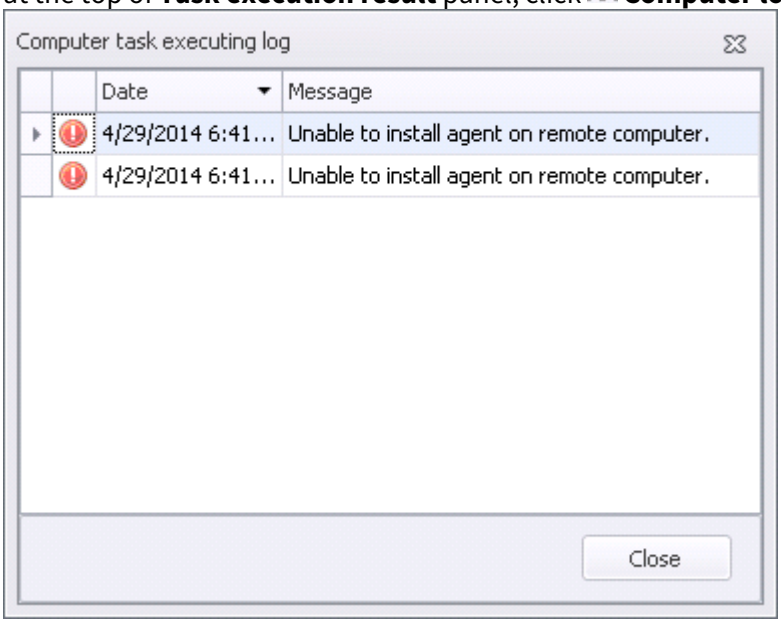
You may encounter problems during remote installation of InfoWatch Device Monitor agents to computers. This will be indicated by Task status value in the list of tasks: see "Viewing Tasks".

To view task errors:

1. Go to **Tasks**.
2. On **Tasks** panel select the task you want to review.
3. In **Status** column select filter value **Error** (for more information on filters see "Applying Standard Filters").

> **Note:**
>
> Status **No access** indicates that computer is not available (switched off or disconnected from network)

4. In the row of the target computer, do one of the following:
   - right-click the row and select **Computer Log;**
   - double-click the target computer row;
   - at the top of **Task execution result** panel, click **Computer log**.



5. To view detailed error information, click the row. This opens a screen with Windows error description.

For detailed information on the error see its description, error code, or log in error's description. In particular, the errors may be caused by the following things:

- the computer is not available (switched off or disconnected from the network);
- the installation process or reboot is blocked by another task or user (common description could be "*Other task is running*");
- target computer does not allow administrative resources;
- the account in use doesn't have enough rights on the target computer.

If all remote Agent installation conditions in "Preparing Primary Agent Installation. Distribution Agent" are met and the task is not blocked by the user, but the error persists, please contact InfoWatch technical support at support@infowatch.com and attach error description and log.

5.6.9 Creating Installation Package

Supplied InfoWatch Device Monitor Agent installation package contains the following default settings:

- Agent installation directory on computer system drive - `%Program Files%\Infowatch\DeviceMonitor\Client.`
- There is no uninstallation password.
- After installation Device Monitor Agent starts to remind an employee that a reboot is required. Message text - "*Please reboot your computer as soon as possible*". Reminders are displayed infinitely, with 10 min intervals.

To change these settings create your own installation package. When you run it, it will use the settings specified when installation package created: no other parameters are needed to specify.

To create InfoWatch Device Monitor Agent installation package:

1. In the Main Menu select **Tools > Create install package**.
   This opens distribution task manager dialog box.
2. The InfoWatch Device Monitor servers currently registered in the System are displayed. Agent will use them for primary installation.
   If necessary, change Agent installation directory at computers.
   Specify local or network directory where to the installation packages will be saved.
   Click **Next**.
3. The unique name of Device Monitor proxy server certificate (Issuer Distinguished name, Proxy Root Issuer DN) will be displayed. You can change it with accordance to X.509 standard, CN (Common Name) field is mandatory, all fields comma-separated. Click **Next**.
4. Specify options of computer reboot:
   - **Wait for reboot without notifying the employee**. The Agent can:
     - start notifications immediately (*Do not wait option*),
     - start notifications in specified time (*Wait for option* - please specify time period to start notifications),
     - do not notify at all (*Wait infinitely option*).
   - **Notify the employee about reboot necessity and wait for reboot**. Upon completing reboot waiting in "silent" mode (see **Wait for reboot without notifying the employee** setting) or immediately after installation ends, Device Monitor Agent starts to notify employee on reboot necessity:
     o during specified time period (*Notify within* option)
     o permanently (*Notify infinitely* option)
     o do not notify at all (*Do not notify* option).
     If needed, change continuance and frequency of notifications appearance and enter text of the message displaying in reboot notification.
   - **Show a warning before forced reboot**. If this check box is flagged, then the Agent displays a notification about forced reboot and allows 5 minutes to end operations. If the option is not checked then the forced reboot (if it should be made according your settings) will be performed unexpectedly for the employee.

> **Warning!**
>
> Forced reboot is performed in case when neither **Wait while employee reboots computer** setting no **Show a warning before force reboot** setting do not flagged, or their wait durations are expired but employee did not reboot the computer.

Click **Next**.

5. Define Agent settings before it connects to the server for the first time:
   - To protect Agent application from deleting by employee, enter the password that will be requested when trying to uninstall the Agent and confirm it.
   - **Show employee notifications** - if employee attempts to perform an action restricted by security policy (DM), a warning will be displayed. For further details, see "Employee Notifications about Policy (DM) Violations"
   - **Hide Agent presence** - indicates if Windows system tray of managed computer hides Agent presence on the computer.

     > **Warning!**
     >
     > Not notifying the user about interceptor operation may contradict the applicable laws of your country.

     > **Warning!**
     >
     > If there is an antivirus protection enabled on the managed computer then the antivirus program can reveal the operation of Device Monitor: for example, in the list of processes running on the managed computer or in the list of programs that initiate a control.

     > **Warning!**
     >
     > If "Hide Agent presence" is activated on the computer, notification about computer reboot will not be displayed.

     If this option is not selected, the Windows system tray of the computer where the Agent is installed will display icon. By clicking this icon, information on DM Agent operation and the list of currently controlled devices are displayed.
   - **Install the component of network interception** - installs **iw_proxy** component on a computer.
     Component will not be installed if you leave the checkbox empty.

- **Install the component of network control** - installs **Network Monitor** interceptor on a computer.
  Component will not be installed if you leave the checkbox empty.

  > **Warning!**
  >
  > You should not install the component of network control to the server with Citrix Provisioning Services: this can lead to the serious problems concerning server operation.

  Click **Next**.
6. Look through the task summary. If you need to change any settings click **Back** to return. If all settings are correct, click **Finish**.

Agent installation package will be saved in the folder you specified at the first step.

5.7 Additional Features

You can use the following functions to enhance your Management Console (DM) experience: filtering, grouping and sorting table entries.
Certain functions can be also accessed with hotkeys.

5.7.1 Filter Table Contents

You can filter table contents against one parameter or more with various filters. A filter makes a table display only the entries that comply with filtering conditions.
More information on filters is available in the following subsections:

- Filter by Date;
- Applying Standard Filters;
- Custom Filter;
- Editing Filters;
- Removing a Filter.

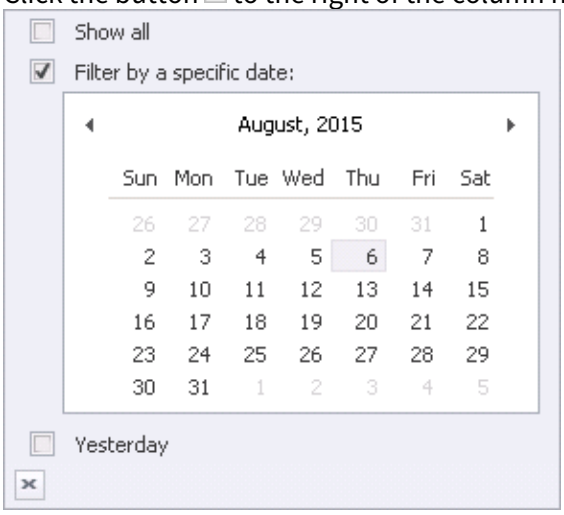
Filtering by Date

If the table shows temporary parameter characteristics (for example, Agent installation date and time, Console (DM) log
time, last computer access, registered event date, etc.), you can filter the column against the desired date or period.

To view the records for specific date or period:

1. Move the pointer over the time/date attribute in the column header.

2. Click the button to the right of the column header.



3. Select one of the following filters:
   - **Show all** - select this check box to view all records regardless the date.
   - **Filter by a specific date** - select the date in the calendar.
     To select a period, select it holding the mouse button.
     To go from date to month or year display, click the month/year.
     Use arrows to go forward or backward.
   - **Today; Yesterday; Last week; Earlier this week; Earlier this year** fields depend on column values: for
     example, if there are no records for the date, **Today** field won't be displayed. Check this box to display
     only the records inside specific date range.
4. Click to apply the filter and close the form.

Applying Standard Filters

To filter table entries against a single attribute:

1. Move the pointer over the time/date attribute in the column header.
2. To view filter list, click to the right of the column.
3. Select one of the following filters from the list:
   - **Blanks**. Display records with `<Is Null>` value (the field is empty).
   - **Non blanks**. Display records with `<Is Not Null>` value (i.e., the field contains attribute value).
   - `<attribute value>`. Display records that contain selected attribute.

> **Note:**
>
> **Custom** option lets you configure your filtering criteria (for more info see "Custom Filter").

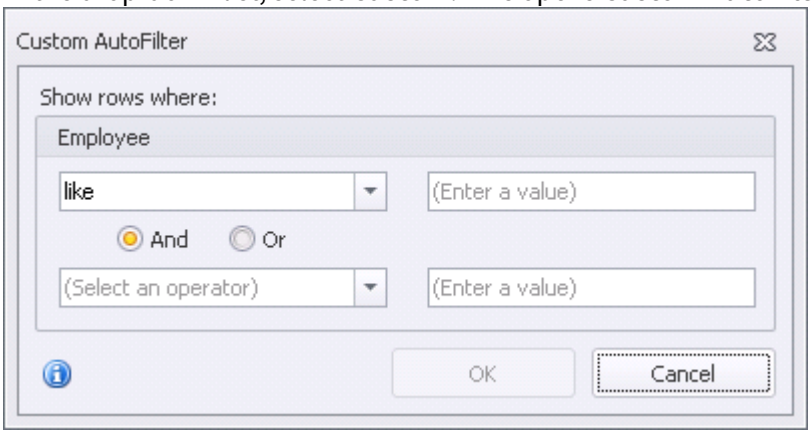
The table will only display filtered values.

To filter values against several attributes,
repeat simple filtering procedure against all filter attributes you want to apply.
Complex filter reduces the table contents to records filtered against several attributes.

Custom Filter

To specify your own filtering criteria for table entries:

1. Move the pointer over the column header that contains required attribute.
2. Expand filter list by clicking to the right of the column header.
3. In the drop-down list, select **Custom**. This opens **Custom AutoFilter** dialog.



4. In this box, specify filtering criteria:
   - Select conditions from the drop-down list in the upper-left box.

     Note:

     You can use comparison operators to limit filtering criteria: *equal, not equal, greater than, greater than or equal to, less than, less than or equal to; values empty (blank) and nonempty (non-blank field)*; or text filter with a mask. To get a text filter syntax tip, click .

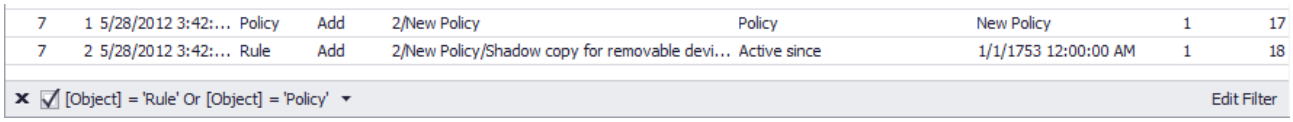
   - Enter condition value into the top right box.
   - Specify additional criteria, if needed, by selecting a logical operator for and entering the second condition at the bottom.

     Note:

     Choose logical operator **AND**, if you want the items that match both conditions at the same time.
     Select logical operator **OR** filters the items that match at least one condition.

5. Click **OK** to apply the filter.

Filtered table only displays the items that match filtering criteria. Filtering criteria string is at the bottom of the screen that contains filtered items.

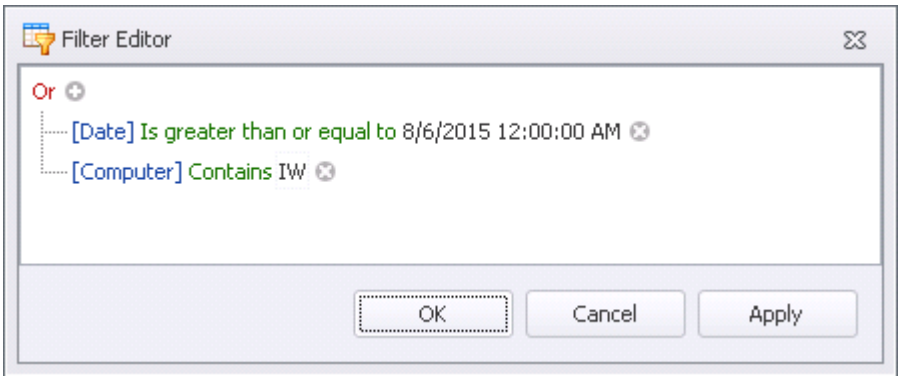


To remove filter and view all items, clear the check box in filter string. To apply the filter again, select the check box. To re-use a filter, click the filter string and select filter from drop-down filter history list. Custom filters are stored until you close the window with filtered content.

Editing Filters

To edit active filter:

1. Click **Edit Filter** at the end of the filtering conditions string. The following dialog box displays **Filter Editor**.



2. Edit filtering criteria. Available actions:

Action	Steps
Edit an attribute, attribute value or operator	1. Click attribute/value name of attribute/operator 2. Select the value from the drop-down list or enter the value to the field
Add a simple condition	Click the button ⊕ to the right of the logical operator or Click **Add Condition** in logical operator menu
Delete condition	Click the button ⊕ at the end of condition string
Add criteria group	1. Click the logical operator name 2. Select **Add Group** in the menu
Delete criteria group	1. Click the name of operator criteria group 2. Select **Delete Group** in the menu
Delete all criteria	Click **Clear All** in logical operator menu

3. Click **Apply** and view the filtered results without closing **Filter Editor** screen.
4. Click **OK**.

Removing a Filter

To remove a filter,
take one of the following steps:

- Click filtered column header and select **All** from the drop-down filter list.
  If you are using complex filter, repeat the step for every condition you want to remove.
- Remove the flag in filter conditions string.
- Click ✖ in filter conditions string. This closes filter conditions string.

5.7.2 Grouping or Sorting Entries

Grouping function is intended for managing table entries according to selected schema. Group scheme is displayed on the group panel over the column title row. Contents are grouped basing on a single attribute or more (table columns).

To group the contents basing on an attribute:

1. In table's title row, click the column title that corresponds to the attribute name.
2. Click and hold the title to drag it over the group panel. Name of the grouping attribute appears on the group panel.

To group the contents basing on multiple attributes, repeat steps 1-2 for all attributes participating in the process.

> **Note:**
>
> You can change the grouping procedure by changing the order of column titles in group scheme. The column with the title is at the top right of the group scheme is processed first.

Grouped entries appear collapsed. To view information for a specific entry, click ▸ on the left of the record you want to expand. To minimize entry, click ▾ to the entry's left. You can ungroup entries basing on one or more attributes, removing columns from the group scheme.

To ungroup entries basing on any attribute:

1. In group panel, click and hold the column title you want to remove from the group scheme and drag it into
   table title row. Column location is indicated with a rectangular frame.
2. Move column title over the title row to the desired position and release the button. This will move the column
   to specified location.

Use sorting feature to display table contents in ascending or descending order of any attribute.

To change attribute values sorting order of the in a column,
move the pointer over the column title you want to use for sorting. Click the selected title. This will sort all table contents in ascending/descending order of the attribute values.
To go back to the old sorting order,
click the selected header once again.

5.7.3 Hotkeys

The following table lists the keys and key combinations, used for quick access to various system functions.

Feature name	Hotkeys
Server connection	
Connect to server	F4
Exit Console	Alt+F4
Main screen customization	
Hide/show Navigation bar	Ctrl+Shift+1
Hide/show Details	Ctrl+Shift+2
Hide/show Console log	Ctrl+Shift+3
Management Console sections	
Go to Policies	Ctrl+1
Go to Employees	Ctrl+2
Go to Computers	Ctrl+3
Go to White Lists	Ctrl+4
Go to Signatures	Ctrl+5
Go to Applications	Ctrl+6
Go to Log	Ctrl+7
Go to Tasks	Ctrl+8
Go to Events	Ctrl+9
Manage security schema (overview)	
Go to security schema editing mode	F11
Save security schema	F12
Cancel saving security schema	Shift+F11
Unblock security schema (Superuser only)	Ctrl+Shift+U
Update security schema	F5
Go to the latest security schema version (when viewing an earlier version)	F9
Manage security policies	
Add security policy	Ctrl+N
Edit security policy	Ctrl+E

Delete security policy	Ctrl+D
Manage rules	
Add rule	Ctrl+Shift+N
Edit rule	Ctrl+Shift+E
Delete rule	Delete
Manage employee groups	
Add new employee group	Ctrl+N
Edit employee group	Ctrl+E
Delete employee group	Ctrl+D
Manage employee accounts	
Add employee account to a group	Ctrl+Shift+N
Edit employee account	Ctrl+Shift+E
Remove employee account from a group	Delete
Delete employee account from security schema	Shift+Delete
Manage computer groups	
Add new computer group	Ctrl+N
Edit computer group	Ctrl+E
Delete computer group	Ctrl+D
Manage computers	
Add computer	Ctrl+Shift+I
Remove computer from a group	Delete
Delete computer from security schema	Shift+Delete
Manage white lists	
Add white list	Ctrl+N
Edit white list	Ctrl+E
Delete white list	Ctrl+D
Edit white list entries	Ctrl+Shift+E
Manage signatures	

Add signature category	Ctrl+N
Edit signature category	Ctrl+E
Delete signature category	Ctrl+D
Remove signature from category	Delete
Configure filters for Audit Log and Event Viewer	
Add filter	Ctrl+N
Edit filter	Ctrl+E
Delete filter	Ctrl+D
Manage Agent remote installation and upgrade tasks	
Add task	Ctrl+N
Edit task	Ctrl+E
Delete task	Ctrl+D
Add computer to selected task	Ctrl+Shift+N
Remove computer from selected task	Delete
Display target computer error log	Ctrl+L

6 Licensing Information

The licensing information for the System is contained in the following topics:

- End-User License Agreement
- Third-Party Licenses

6.1 End-User License Agreement

IMPORTANT! Read this End-User License Agreement (EULA) carefully before using the Software.

Clicking the Accept button in the License Agreement box at installation time or any use of the installed Software will signify your irrevocable acceptance of the terms and conditions of this EULA. If you do not accept the terms and conditions of this EULA, You should terminate the installation process and/or the use of the Software.

6.1.1 License Agreement

This End-User Licence Agreement (“Agreement”) is a joinder agreement between InfoWatch (“Rightholder”) and you, a person or legal entity (“User”), legally possessing a copy of InfoWatch Traffic Monitor (“System”).
The System is designed for monitoring, filtering, and the prevention of leaks of data transferred beyond the company frontiers through Right holder, Internet or Internet pagers as well as for network and local printing. The System also allows you to control access to ports and monitor data copied to removable storage devices.

1. Definitions

1.1. “Software” means, in whole or in part, the System, the accompanying documentation, and optionally ordered updates to the System, copyrighted by “InfoWatch”.
1.2. Computer” means the hardware that the Software is designed for and where the System will be installed and/or used.
1.3. User (You) means a person or legal entity that installs the Software on its behalf and legally possesses a copy of the Software. If the Software has been downloaded or acquired on behalf of a legal entity, the term "User" (you) means the legal entity for which the Software was downloaded or acquired and that an authorized person accepts the terms and conditions of this Agreement on its behalf.
1.4. "Partners" means the organizations distributing the Software under the agreement with the Rightholder.
1.5. "System Documentation" means the accompanying printed and other materials, User Guide, Administrator Guide, reference book, help file, and similar System-related printed and electronic documents copyrighted by "InfoWatch".

2. Grant of License

2.1. The Rightholder grants you a non-exclusive license to use the Software within the functionality as described in the System Documentation provided that you meet all the technical requirements specified in the System Documentation, as well as all the restrictions and terms of use of the System specified in this Agreement.
2.2. Unless otherwise specified, if you have received, downloaded, or installed an evaluation version of the Software, you may use the Software only for evaluation purposes within one evaluation period starting with the software installation date. Any use of the Software for other purposes or after the evaluation period expires is prohibited.
2.3. Unless otherwise specified in the license agreement, if you are using different versions of the Software or versions for different languages, if you have received the Software on several media or otherwise possess several copies of the Software, or if you have received the Software as part of some other software, the total number of your computers where all the versions are installed and/or used must correspond to the number of licenses procured from the Rightholder. Each purchased license gives you the right to install and use the System on a certain number of computers or for a certain number of licensed objects, as set forth in Clause 2.2.

2.4. The User has the right to make a single copy of the Software, provided that this copy is only used for archive purposes or for the replacement of a duly purchased Software copy, should the original be lost, destroyed, or become unusable. This copy cannot be used for any other purposes and must be destroyed, if the User's right to use the Software becomes invalid.
2.5. Any legal transfer of rights for the use of the Software is only possible after entering this Agreement and upon prior consent of the Rightholder or its authorized Partner. The successor of the rights for the use of the Software then becomes a legal successor of the User, provided that the User under this Agreement is fully replaced.
2.6. You are fully responsible for compliance with all applicable export and import laws and regulations as well as trade sanctions and embargoes concerning the transfer of rights for the use of the Software.

3. Restrictions

3.1. You shall not decompile, disassemble, or modify the Software as well as produce derived works on its basis, in whole or in part, unless it is allowed by law.
3.2. You shall not transfer or assign your rights to use the Software to any third party except as set forth in Clause 2.6.
3.3. You shall not transfer or provide access to the license key to any third parties except for as set forth in Clause.2.6 of this Agreement. Any other transfer of rights will be considered a violation of this Agreement. A license key is considered confidential information. The Rightholder reserves the right to verify the validity of your license key with the available means.
3.4. You shall not rent, lease, or lend the Software to any third parties or disclose the results of the benchmark testing of the System.
3.5. The Rightholder has the right to block the license key, should the User breach any of the terms or conditions of this Agreement.
3.6. If you are using an evaluation version of the Software, you shall not transfer your copy of the Software to any third party.
3.7. Any violation of the intellectual property rights on the Software will result in civil, administrative, or criminal responsibility under the applicable law.
3.8. You shall not use the Software for any purposes or in any ways restricted or prohibited by the applicable law. You are fully responsible for any unauthorized use of the Software.
3.9. Should you violate any terms or conditions of this Agreement, the Rightholder has the right to terminate this Agreement for the use of the Software at any time without notice or any refund of the cost of the Software full or partial.

4. Limited Warranty and Disclaimer

4.1. The Rightholder guarantees that the Software will substantially perform according to the description in the System Documentation.
4.2. You agree that no software is free of errors and are recommended to back up your files regularly.
4.3. The Rightholder does not guarantee proper Software operation if any requirements described in the System Documentation or any terms and conditions of this Agreement are violated by the User.
4.4. EXCEPT AS SET FORTH IN THIS LIMITED WARRANTY, THE SOFTWARE IS PROVIDED "AS IS". THE RIGHTHOLDER OR ITS PARTNERS GIVE NO WARRANTY AS TO ITS USE OR PERFORMANCE. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE RIGHTHOLDER AND ITS PARTNERS MAKE NO WARRANTY, CONDITION, OR REPRESENTATION, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, NON-INFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABILITY, SATISFACTORY QUALITY, INTEGRATION, OR FITNESS FOR A PARTICULAR PURPOSE. YOU ASSUME FULL RESPONSIBILITY FOR SELECTING THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS FOR THE INSTALLATION AND USE OF THE SOFTWARE AND FOR THE RESULTS OBTAINED WITH THE SOFTWARE.

5. Limitation of Liability

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE RIGHTHOLDER AND/OR ITS PARTNERS BE LIABLE FOR ANY DAMAGES (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION, LOSS OF INFORMATION, ETC.) IN CONNECTION WITH THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF THE RIGHTHOLDER OR ITS PARTNERS WERE ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN ANY CASE, THE LIABILITY OF THE RIGHTHOLDER OR ITS PARTNERS IN

CONNECTION WITH ANY PROVISION OF THIS AGREEMENT IS LIMITED BY THE COST OF THE SOFTWARE, ACTUALLY PAID BY YOU. THESE RESTRICTIONS MAY NOT BE EXCLUDED OR LIMITED UNDER APPLICABLE LAW.

6. Software Products

6.1. Any third party technologies the use of which within the Software is necessary or reasonable are specified in the System Documentation. Such a technology is licensed to the end user on the terms and conditions of a license agreement with the third party, specified in the System Documentation. This license agreement with the third party is included in this Agreement by reference.
6.2. The software products making part of the System are only licensed for limited use within the System. When the license agreement for the use of the Software expires, the User must destroy all the copies of the Software.

7. Open Source (Free) Software

This product may contain programs that are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or other similar free software/open source licenses which among other rights permit the user to copy, modify, and redistribute certain programs, or portions thereof, and have access to the source code ("Open Source Software"). If such licenses require that for any software distributed in an executable binary format, the source code should also be made available to the user, such source code should be obtained by sending a query to the Rightholder or supplied with the product. If any Open Source Software licenses require that the Rightholder provide rights to use, copy, or modify an Open Source Software program beyond the rights granted in this Agreement, then such rights take precedence over the rights and restrictions in this Agreement.

8. Intellectual Property Rights

8.1. You agree that the Software, documentation, other copyright matter, any systems, ideas, methods of operation, documentation, and other information contained in the Software as well as the trademarks are the intellectual property of the Rightholder or its Partners. This Agreement does not grant you any rights to the intellectual property including any trademarks or service marks of the Rightholder or its Partners except for the rights provided by this Agreement.
8.2. You agree that the source code and the license key for the Software are the intellectual property of the Rightholder and its Partners.
8.3. You may not delete or modify any copyright or other proprietary notices on any copy of the Software.

9. Rightholder Contact Information

"InfoWatch"
Phone/fax:+7 (495) 229-00-22
Sales department:sales@infowatch.com
Technical support service:support@infowatch.com
Website:http://infowatch.com/

6.2 Third-Party Licenses

The system contains third-party components distributed under the MIT License (http://www.opensource.org/licenses/mit-license.html):

- Lua - http://www.lua.org/license.html
- LuaBind – http://www.rasterbar.com/products/luabind.html
- libxml2 – http://www.xmlsoft.org/

The system also contains software:

- distributed under the terms of the BSD Licenses (http://www.opensource.org/licenses/bsd-license.php):
  - Stringencoders – http://code.google.com/p/stringencoders/
- distributed under the GNU GENERAL PUBLIC LICENSE (http://www.gnu.org/licenses/gpl-2.0.html):

- Pdftotext – http://www.foolabs.com/xpdf/
- Tnef – http://sourceforge.net/projects/tnef/
- Unzip – http://www.info-zip.org/UnZip.html
- libcole.so – arturo@directmail.org; andy.scriven@research.natpower.co.uk
- libhtmltree.so – pauljlucas@mac.com

7 Glossary

Term	Glossary
Active Directory	LDAP-compatible Microsoft directory services for the Windows NT operating systems family
Active policy	A policy included into a configuration that is uploaded to a host. See also: Policy, Host
Administrator	A preset role and user account in Management Console. An Administrator can modify other accounts and their rights. It is also a System user who installs, configures and maintains the System. See also: User role, Security officer, User
AJAX	Asynchronous JavaScript and XML is a group of interrelated Web development techniques used on the client-side to create asynchronous Web applications
Attachment	File attached to the intercepted event at any nesting level. See also: Event
Audit	Controlling of acrions fulfilled by Management Console users: creating and managing the security schema, System administrating. See also: Audit log, Management Console accounts
Blanks	Technology of searching the filled blanks of forms: questionnaires, receipts, etc. Blanks are stored in the System as digital prints, their text is not available for viewing to either users or System administrators. See also: Technologies, Technology element
Case sentive	Term setting: if the term is case-sensitive, the text search will detect only word forms which completely match upper- and lower-case letters defined in a term. See also: Term
Catalogs of persons, computers, and groups	Information about users, workstations, groups of users, and groups of computers imported from Active Directory, Domino Directory or Astra Linux Directory 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
Category	Named term group characterizing some theme. If the System detects any term from the category in the text of the intercepted event, it associates the event with this category. See also: Term
Citation index	A measure of how close the sample document matches the text of the document being analyzed. See also: Sample document, Quote
Computer	A managed computer: workstation or mobile device or terminal device. See also: Workstation, Mobile device, Terminal device
Configuration	A group of settings required to check events for data monitoring and analyzing. See also: Event, 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
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, Persons group, Persons status, Person control policy
Copy mode	One of IW TM transport modes. In this mode the actual traffic does not pass through the System. The copy of traffic is analyzed. In this mode, the traffic cannot be filtered by the System. See also: Transport mode
Copy rule	The rule that regulates copying, printing and photographing protected data. See also: Rule, Protected data, Data protection policy
Corporate security policy	A set of technical, organizational, administrative, legal, and physical measures, methods, rules, and guidelines that cover all security aspects in a company
Dashboard	Management console section that displays on widgets the statistical information on the violations and violators. See also: Management Console, Widget, Violation
Data interception	A process of acquiring, parsing, categorizing, and converting data (or a copy) into context. It is possible to intercept data transferred using the following protocols: SMTP, HTTP, ICQ/OSCAR, Skype, IXP, XMPP, MMP, FTP. See also: Interceptor, Event context
Data interception channel	A data interception environment that includes technical appliances, software tools, and communication protocols. The System supports the following data interception channels: email (SMTP, IMAP, and POP3), Web (HTTP), instant messaging services (ICQ and Skype), shadow copies of files, connected/disconnected workstation events, and print jobs.
Database	A collection of data stored in accordance with a data scheme. Contains all information needed for the System.
Database unloadings	Technology of searching the quotes the database. Database unloadings may be lists of salaries, other personal data, etc. See also: Technologies
Decision	The security officer’s conclusion on whether the event violates the corporate security policy or not. Possible values: “No decision“, “Violation:“ and “No violation“. See also: Security officer, Corporate security policy, Event, Event attributes, Violation, Policy, Verdict
Delivery status	Event attribute that specifies the possibility of event delivery to recipients after the analysis. If the event delivery has been allowed, then the attribute value represents the delivery tracking (completed or failed). See also: Event attributes
DeviceLock	Data loss prevention (DLP) system providing endpoint device/port control and data leak prevention
DeviceLock Adapter	IW DM interceptor that integrates with DeviceLock; it intercepts the shadow copies of the files copied to the removable devices. See also: IW DM, Shadow copy of a file, Interceptor
Digital print	A method of storing a sample document in the database in the form of a set of quotes. See also: Sample document, Quote

Document shadow copy	A copy of printed document, received from the print job initiated on the managed computer. See also: InfoWatch Device Monitor
Domino Directory	IBM Lotus Domino Directory is a directory of information about users, servers, and groups. The Domino Directory is also a tool that administrators use to manage the Domino system.
Event	Objects of traffic interception (SMTP and IMAP and POP3 mail, HTTP requests, ICQ and Skype messages), shadow copies of files and print jobs. Generated by the System as a result of the data exchange between employees and others, including publication in media, copy to external devices and printing.
Event analysis	The procedure of processing of the attributes, attached files, and text of the intercepted events and of assigning additional attributes to the event. See also: Event, Policy, Event attributes
Event attributes	Structured data extracted from the events and assigned according to the processing results. See also: Event, Policy, Verdict, Decision, Transport mode
Event context	Internal representation of an intercepted event in the System. XML data (attributes, text) extracted from the event and its attachments. After processing the analysis results and the decision are added to the context. See also: Event, Technologies, Decision
Event text	Text information extracted from the event body and its attachments. Contains no formatting or markup. Is used for analysis and search. See also: Event, Event body
File shadow copy	A copy of file recorded to 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.
FTP	File Transfer Protocol is a network protocol used to transfer computer files from one host to another host over a TCP-based network, such as the Internet.
Graphical object	Technology of searching the images (passports, bank cards, etc) in the text and attachments of the intercepted events. See also: Technologies, Event, Protected object
Group of persons and computers	Group aggregating data on organization's users and computers and on external contacts. The groups can be AD Groups (imported from Active Directory) or TM Groups (created using IW TM). See also: Person, Computer, Contact
GTalk	Google Talk is an instant messaging service that provides both text and voice communication.
Headers	Supplemental data placed at the beginning of a block of data being stored or transmitted. Used for creating the event entity in the System and for determining the attribute values of this event. See also: Event, Event attributes
HTTP	HyperText Transfer Protocol, an application-tier protocol used to transfer the data in the text format. See also: HTTPS, HTTP(S) Monitor
HTTP query	A request formed according to the HTTP standards (POST request, GET request etc.) See also: HTTP, Event

HTTPS	Hypertext Transfer Protocol Secure is a network protocol for secure communication over a computer network. See also: HTTP, HTTP(S) Monitor
ICAP	Internet Content Adaptation Protocol is a lightweight HTTP-like protocol that allows to control the incoming and outgoing HTTP traffic. It also makes it possible to modify the content of the HTTP requests.
ICQ	An Internet instant messaging service. Uses OSCAR protocol.
ICQ message	A message sent through the ICQ-OSCAR protocol. See also: Event
IMAP	Internet Message Access Protocol is a protocol for e-mail retrieval and storage
InfoWatch Device Monitor	IW DM is software appliance designed to control the user access to peripherals and to monitor operations (data either copied to removable media and network storages or sent to print, network activity, applications usage, photo) and intercepting messengers traffic (Skype, Gtalk and Jabber) and so on.
InfoWatchTraffic Monitor	IW TM software suite is designed to control various types of traffic (SMTP, IMAP, POP3, HTTP, HTTPS, IMAP, XMPP, YMSG, ICQ, NRPC) and shadow copies of the data copied to the removable media and sent to printing.
Initiators	A person whose actions led to the events 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.
License	Right to the System usage. Gained when bying the System and defines available users number, used technolodies and interceptors and so on. See also: Technologies, Interceptors
Lists	Lists the similar data generated by Management Console to be used in policies creating. See also: Configuration, Policy
Lotus Adapter	Interceptor installed on the IBM Lotus server to redirect mails to IW TM for analysis. See also: Interceptor
Lotus Domino	IBM mail server which messages are intercepted by Lotus Adapter.
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.
Mobile device	Computer type: smartphone or tablet PC with OS of Android or Windows Phone or iOS family. See also: Computer
Monitor	See: Interceptor
Morphology	Term setting: if morphology is used, the text search will detect all word forms of this term. See also: Term
MS Lync	Microsoft instant messaging clients for corporate environments.
Normal transport mode	A traffic analysis and filtering mode. In this mode, it’s possible to block the traffic forbidden by the System can be blocked. See also: Transport mode, Inline mode
Notification	E-mail sent in case if the policy triggers on the event. Is sent via Management Console to notify Management Console users, employees or third parties. Contains a summary on the intercepted events and attached message. See also: Policy, Event
Occurrence threshold	A number of text objects found in the event enough to detect the protected object where this occurrence threshold is defined. See also: Event, Text objects, Protection object
Perimeter	A container of company infrastructure elements and contact information. The perimeter is used to logically divide a company into structural elements and track the traffic of every element. See also: Group of persons and computers
Person	Account of employee or external contact that is contained in System catalog and allows to process the data belonging to this account as a whole and to user-friendly display data referring to it. See also: Group of persons and computers
Persons control policy	A policy to add rules controlling persons, persons groups and person statuses. See also: Policy, Persons control rule, Person, Person status
Persons control rule	Rule that assigns attributes to the event of specified violation level and which senders or recepients contain persons specified in the policy which includes this rule. Allows to re-assign person's status and to send notifications. See also: Rule, Event attributes, Person, Violation level, Person status, Notification, Persons control policy
Placement rule	The rule that regulates storing protected data. See also: Rule, Protected data, Data protection policy, Crawler
Policy	A set of rules according to which the event analysis and processing facilities are performed. See also: Policy, Active policy, Rule
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 accept the data enclosed in the request message body for storage. Often used for file downloading of filled web-form representing
Privilege	Entity defining user's ability to perform some action (set of actions) when managing the System
Protected data	A set of protected objects, their catalogues and file formats which detection in the event allows to characterize this event as falled under the data protection policy where this set is defined. See also: Protected object, File format, Data protection policy
Protected object	The set of technology elements whose presence in the event allows the System to determine that this event belongs to a particular type of business documents (catalogue of protected objects). Protected objects are used in defining of data protection policies. See also: Technology element, Data protection policy
Proxy Server	The service that allows indirect requests to other network services. Proxy forwards all requests of the client programs to the network, and, having received the reply, sends it back to the client.
Quotation threshold	A procent of the sample document found in the even as quotes, enough to associate the event with this sample document. See also: Event, Sample document, Quote
Quote	A quote from the sample document found in the event text. See also: Sample document
Reference hash sum	Unlike the current hash sum, keeps the representative state of System files. See also: Integrity control
Relay server	A server which allows anyone on the Internet to send e-mail through it, not just mail destined to or originating from known users.
Report	Selection providing a visual display of event statistic data. See also: Management Console, Event
Rule	Entity defining System's actions in the response to any actions which persons do with secured data.A rule is a set of conditions to test the event with and actions performed when those conditions are fulfilled or not. See also: Event, Policy, Protected object, Persons control rule, Copy rule, Transfer rule, Placement rule
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)
Sample documents	Technology of searching the quotes from sensitive documents: memos, financial reports, contracts, and others. Sample documents are stored in the System as digital prints, their text is not available for viewing to either users or System administrators. See also: Technologies, Technology element, Digital print, Quote
Scan task	Operation (single or repeated) of checking target storage locations (Microsoft SharePoint storage, local drives of workstations, shared network resources) if they store technology elements. See also: Crawler, Scanner, Tecnology element

Scanner	Crawler service whicn checks files in the corporate nerwork if they violate the corporate security policy. See also: Crawler, Corporate security policy
Security officer	A basic user of the Management console. Also - pre-installed role of the Management Console user that has privileges for all the actions in the system except administrative. See also: Management Console, User, User role, Privilege, Administrator
Skype	A voice-over-IP service and instant messaging client
SMB	Server Message Block operates as an application-layer network protocol mainly used for providing shared access to files, printers, serial ports, and miscellaneous communications between nodes on a network.
SMTP	Simple Mail Transfer Protocol is a networking protocol used to send the email in TCP/IP networks.
SMTP mail	An e-mail formed according to SMTP standards. See also: SMTP, Event
SPAN	Switched Port Analyzer is a technology that allows to mirror the network traffic from one port to another
SPAN copy	A variety of the “Copy” transport mode. In this case the traffic passes through a CISCO switch. The copy of the traffic is sent to Traffic Monitor Server for analysis. See also: SPAN
SSL	Secure Sockets Layer is a cryptographic network protocol developed for transmitting private documents via the Internet.
Status	Characteristics of persons and computers allowing to divide them onto groups for convienent analysus and activity control and to display them on dasboards and reports with special color indicating. See also: Persons, Computers, Dasboard, Report
Stop word	Numbers, letters and words, whose presence in cells do not trigger these cells. Stop words are used to eliminate false triggering.
Tag	The text label giving a brief description of the event. See also: Event attributes
Task	See Scan task
Technologies	Set of analysis tools searching for defined elements in the events' context and adding characterizing attributes to the event. See also: Technology element, Event context, Categories, Terms, Sample documents, Blanks, Database unloadings, Text objects, Graphical objects
Technology element	A part of the System technologies settings. Samples of confidential data. Can be categories and terms, sample documents, blanks, database unloadings, text and graphical objects. See also: Technologies, Categories and terms, Sample documents, Blanks, Database unloadings, Text objects, Graphical objects, Protected object.
Term	One of the set of words and phrases together defining a topical area. See also: Category
Term Weight	How the term is characterized for the given category; an integer between 1 and 10. If a term with a higher weight is detected in event, then this event will be more likely associated with the category of this term. See also: Term

Text object pattern	Unified description of all possible text objects with the typical structure: passport numbers, credit card numbers, phone numbers, medical codes etc. See also: Text objects
Text objects	Technology of matching the data from the events' text with defined patterns (rules of generating bank cards numbers) . See also: Tecnologies, Event, Technology element, Text object pattern
Transfer rule	The rule that regulates sending and receiving protected data. See also: Rule, Protected data, Data protection policy
Transport mode	Event attribute that defines the level of control when the object is delivered to the recipients. Assigned by the analysis and decision engine during the object analysis. Together with the "Verdict" attribute determines if the object can be delivered further on. See also: Event attributes, Verdict, Copy mode, Normal transport mode, Delivery status
User	IW TM users: administrator, security officer etc. See also: Administrator, Security officer, Person
User interface	The complex of tools and methods by means of whose the user interacts with the system.
User role	A set of privileges that define a set of actions available for the user. See also: Administrator, Security officer, Management Console, Privilege
Verdict	An event attribute with the conclusion about the presence (or absence) of violations in an event. Together with the Transport Mode attribute determines if the event can be delivered further on. See also: Event, Transport mode, Delivery status, Event attributes
Verdict reason	Event attribute that describes the reason why a certain verdict was assigned to the event. See also: Event attribute, Verdict
Violation	The value of the «Decision» attribute; means that the corporate security policy has been violated. See also: Decision, Corporate security policy
Violation level	Event attribute indicating (by the color tag) the level of threat to corporate security policy. See also: Event, Event attributes, Violation
Visibility scope	The way to divide intercepted events to restrict Management console user access to them. Events satisfying criterias of some visibility scope will be visible to those users who have an access to this scope only (given that user has privileges to view or/and manage events). See also: Event, Privilege
WhatsApp	Messenger for smartphones that allows you to send text messages, images, audio and video files; as well as the protocol used in it.
Widget	Interface element in the form of an isolated area that displays the specified statistic information on violations and violators. See also: Management console, Violation, Violator
Workstation	Computer type: desktop or notebook with OS of Windows or Linux or Mac family. See also: Computer
XMPP	Extensible Messaging and Presence Protocol is a communications protocol for message-oriented middle-ware based on XML.