

INFOWATCH

# InfoWatch Traffic Monitor 7.0

## User Guide

01/11/2021

© JSC “InfoWatch”

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

http://www.infowatch.com

# TABLE OF CONTENTS


1 InfoWatch Traffic Monitor Overview ..... 11
1.1 Objects Interception ..... 13
1.2 Object Analysis and Verdict ..... 14
1.3 Retrospective Data Analysis, User Decision on an Object ..... 17
1.4 InfoWatch Traffic Monitor Transport Modes ..... 18
1.5 Uploading Object to Database ..... 19
1.6 Specific Features of Blocking HTTP-queries and Messages Sent through Web Services 19
1.7 InfoWatch Device Monitor Functions ..... 20
1.7.1 Operation in Safe Mode ..... 21
2 Traffic Monitor Management Console: General Information ..... 23
2.1 System Operation Before Configuring ..... 24
2.2 Configuring the System ..... 24
2.3 Displaying Actual Data in Management Console ..... 26
3 Interface of Traffic Monitor Management Console ..... 28
3.1 Dashboard Section ..... 30
3.1.1 Dashboard Widgets ..... 31
3.1.1.1 Dynamics of Violations over the Period ..... 32
3.1.1.2 Top Violators ..... 32
3.1.1.3 Quantity of Violations over Period ..... 33
3.1.1.4 Selection ..... 34
3.1.1.5 Dynamics of Statuses ..... 35
3.1.1.6 Policy Statistics ..... 35
3.1.1.7 Statistics on Protected Objects ..... 36
3.1.1.8 Statistics on Catalogues of Protected Objects ..... 37
3.1.2 Dashboard Report ..... 38
3.2 Events Section ..... 39
3.2.1 Queries ..... 40
3.2.1.1 Standard Mode of Creating Queries ..... 42
3.2.1.2 Advanced Mode ..... 50
3.2.1.3 Search on the Event Text ..... 50
3.2.2 Object Interception ..... 52
3.2.2.1 Event Tile ..... 54
3.2.2.2 Brief Event Viewing Form ..... 55
3.2.2.3 Detailed Event Viewing Form ..... 57

3.2.3 Contact Identification in Event ..... 59
3.3 Reports Section ..... 60
3.3.1 Report Creation Form ..... 62
3.3.2 Widgets of Reports ..... 63
3.3.3 Queries ..... 65
3.4 Technologies Section ..... 66
3.4.1 Categories and Terms ..... 67
3.4.1.1 Categories ..... 68
3.4.1.2 Terms ..... 68
3.4.2 Text Objects ..... 69
3.4.2.1 Text Objects Patterns ..... 70
3.4.3 Sample Documents ..... 72
3.4.4 Blanks ..... 73
3.4.5 Stamps ..... 75
3.4.6 Database Unloadings ..... 75
3.4.6.1 Automatically Updated Database Unloadings ..... 77
3.4.7 Graphical Objects ..... 78
3.5 Protected Objects Section ..... 80
3.5.1 Elements of Technologies ..... 81
3.5.2 Detection Conditions ..... 82
3.6 Persons Section ..... 84
3.6.1 Persons ..... 85
3.6.2 Computers ..... 86
3.6.3 Screenshots ..... 87
3.7 Policies Section ..... 88
3.7.1 Rules and their Viewing Form ..... 89
3.7.1.1 Rule of Transfer ..... 91
3.7.1.2 Rule of Copying ..... 93
3.7.1.3 Rule of Placement ..... 94
3.7.1.4 Clipboard Rule ..... 95
3.7.1.5 Person Control Rule ..... 95
3.7.1.6 File Operations Rule ..... 96
3.8 Lists Section ..... 96
3.8.1 Tags ..... 97
3.8.2 Web Resources ..... 97
3.8.3 Statuses ..... 98
3.8.4 Perimeters ..... 99
3.8.5 File Types ..... 101
3.9 Administration Section ..... 102
3.10 Crawler Section ..... 102
3.10.1 Scanner ..... 104

3.10.2 Scan Job ... 106

4 Cases Solving in Traffic Monitor Management Console ... 111

4.1 Typical Actions ... 111
4.1.1 Login to the Management Console ... 112
4.1.2 Applying System Configuration ... 112
4.1.3 Editing Element ... 113
4.1.4 Deleting Element ... 113
4.1.5 Pages Navigation ... 114
4.1.6 Changing User Password ... 114
4.1.7 Selecting Interface Language ... 115
4.1.8 Calling Help File ... 115
4.1.9 Viewing Information on System ... 116

4.2 Managing Persons and Computers ... 116
4.2.1 Creating Group of Persons or Computers ... 117
4.2.2 Creating Persons and Computers ... 118
4.2.3 Configuring Person's Card ... 119
4.2.3.1 Adding Contact to Person ... 119
4.2.3.2 Adding Computer to Person ... 120
4.2.3.3 Adding Person to Group ... 120
4.2.4 Configuring Computer Card ... 121
4.2.4.1 Adding Contact to Computer ... 121
4.2.4.2 Adding Person to Computer ... 122
4.2.4.3 Adding Computer to Group ... 122
4.2.5 Adding Status to Persons ... 123
4.2.6 Viewing Screenshots ... 123

4.3 Managing Catalogues ... 125
4.3.1 Managing Tags ... 126
4.3.2 Managing Web Resources ... 126
4.3.3 Managing Statuses ... 127
4.3.4 Managing Perimeters ... 128

4.4 Managing Base of Technologies ... 131
4.4.1 Defining the Confidential Information ... 131
4.4.1.1 Managing Categories and Terms ... 133
4.4.1.2 Managing Text Objects ... 135
4.4.1.3 Managing Sample Documents ... 137
4.4.1.4 Managing Blanks ... 139
4.4.1.5 Managing Stamps ... 141
4.4.1.6 Managing DB Unloadings ... 143
4.4.1.7 Managing Graphical Objects ... 146
4.4.2 Exporting and Importing the Base of Technologies ... 148

4.5 Managing Protected Objects ... 149

4.5.1 Creating a Catalogue of Protected Objects ... 150
4.5.2 Creating a Protected Object ... 151
4.5.3 Adding Elements of Technologies ... 154
4.5.4 Adding Detection Conditions ... 155
4.5.5 Creating Policies for Protected Objects and Their Catalogues ... 156
4.5.6 Importing and Exporting Protected Objects ... 157
4.5.7 Activating and Deactivating Protected Objects ... 158
4.6 Managing Crawler Subsystem ... 158
4.6.1 Configuring Scanner ... 159
4.6.2 Creating Job ... 160
4.6.3 Clearing Hash Base ... 163
4.7 Managing Interception Objects ... 164
4.7.1 Viewing Summary on Violations/Violators ... 164
4.7.1.1 Creating Dashboard ... 166
4.7.1.2 Creating and Configuring Widget ... 166
4.7.1.3 Creating Dashboard Report ... 168
4.7.1.4 Viewing Dashboard Report ... 169
4.7.2 Viewing Events ... 170
4.7.2.1 Creating Queries ... 171
4.7.2.2 Choosing Event Fields of View ... 183
4.7.2.3 Viewing Brief Event Form ... 183
4.7.2.4 Viewing Detailed Event Form ... 184
4.7.3 Making Decision on Object ... 185
4.7.4 Adding and Deleting Tags ... 186
4.7.5 Saving Events (for SMTP mail) ... 186
4.7.6 Event Export ... 186
4.7.7 Dispatching a Quarantined Event ... 189
4.8 Configuring System Response ... 190
4.8.1 General Information on Policies ... 191
4.8.2 Preset Policies ... 198
4.8.2.1 Data Protection Policy ... 198
4.8.2.2 Person Control Policy ... 199
4.8.2.3 Policy that Regulates Transferring Password-Protected Data ... 200
4.8.2.4 Policies that Regulate Visiting Web Resources ... 200
4.8.2.5 Policy that Excludes Mailing Lists from Interception ... 203
4.8.3 Creating Data Protection Policy ... 203
4.8.3.1 Examples of Using Data Protection Policy ... 204
4.8.4 Creating Data Protection Policy on Agents ... 208
4.8.5 Creating Person Control Policy ... 210
4.8.6 Creating Rules ... 212
4.8.7 Determining System Response to Policy Violations ... 213
4.8.8 Configuring Notifications in Rules ... 215
4.8.9 Determining System Default Response ... 216

4.8.10 Filtering the List of Policies ... 217
4.8.11 On Data Protection Policy on Agents ... 218
4.8.12 On Data Protection Policy ... 218
4.8.13 On Person Control Policy ... 219
4.9 Managing Reports ... 220
4.9.1 Creating and Viewing Reports ... 220
4.9.1.1 Creating Folder with Reports ... 222
4.9.1.2 Creating Report ... 223
4.9.1.3 Creating and Configuring Widget ... 225
4.9.1.4 Viewing Ready Reports ... 227
4.9.2 Examples of Using Reports ... 228
4.10 Administrating the System ... 233
4.10.1 Managing Integration with LDAP Catalogues ... 234
4.10.1.1 Creating Connection to Server ... 234
4.10.1.2 Editing Connection to Server ... 237
4.10.1.3 Deleting Connection to Server ... 237
4.10.1.4 Running Synchronization with Server Manually ... 237
4.10.2 Managing System Users and their Roles ... 238
4.10.2.1 Users ... 238
4.10.2.2 Roles ... 242
4.10.2.3 Visibility Scopes ... 244
4.10.3 Managing Licenses ... 247
4.10.3.1 Checking License Validity ... 248
4.10.3.2 Installing a License ... 248
4.10.3.3 Deleting License ... 249
4.10.3.4 Requesting a License ... 249
4.10.4 Healthcheck ... 249
4.10.4.1 Configure Notifications ... 251
4.10.5 Managing Services ... 251
4.10.5.1 Running Service ... 251
4.10.5.2 Stopping Service ... 251
4.10.5.3 Restarting Service ... 252
4.10.5.4 Saving Service Logs ... 252
4.10.6 Collecting Diagnostic Data ... 252
4.10.6.1 Collecting the Diagnostic Data in Normal Mode ... 253
4.10.6.2 Collecting the Diagnostic Data in Extended Mode ... 254
4.10.7 User Actions Audit ... 254
4.10.7.1 Audit Events ... 255
4.10.7.2 Filtering by User ... 256
4.10.7.3 Filtering by Action ... 256
4.10.7.4 Filtering by Object ... 256
4.10.7.5 Filtering by Date ... 256

4.10.8 Integrity Monitoring ... 256
4.10.8.1 Manual Integrity Monitoring ... 257
4.10.8.2 Automatic Integrity Monitoring ... 257
4.10.8.3 Accepting Result as Standard ... 257
4.10.9 Plugins ... 257
4.10.9.1 Adding Plugin ... 260
4.10.9.2 Deleting Plugin ... 260
4.10.9.3 Working with Tokens ... 260
4.10.10 Configuring Connection to Mail Server ... 262
4.10.11 Configuring Notifications ... 262
4.10.11.1 Creating Notification ... 263
4.10.11.2 Testing Notification ... 265
4.10.11.3 Preset Notifications ... 265

5 Using Device Monitor Management Console ... 267

5.1 Management Console (DM) Overview ... 267
5.1.1 Authorization and Connecting to InfoWatch Device Monitor Server ... 267
5.1.2 Management Console (DM) Main Screen ... 268
5.1.2.1 Configuring Management Console (DM) Main Screen Elements ... 270
5.1.3 Management Console (DM) Sections ... 270

5.2 Managing Console (DM) Accounts ... 271
5.2.1 Viewing Management Console (DM) Account Details ... 273
5.2.1.1 Adding New Management Console (DM) Account ... 274
5.2.1.2 Editing Management Console (DM) Account ... 277
5.2.1.3 Locking or Unlocking Management Console (DM) Account ... 277
5.2.1.4 Deleting Management Console (DM) Account ... 278
5.2.2 Roles of DM Console Users ... 278
5.2.2.1 Adding Role of the Management Console (DM) User ... 279
5.2.2.2 Editing Role of DM Console User ... 282
5.2.2.3 Deleting Role of DM Console User ... 283
5.2.3 Management Console (DM) Security Schema Operation Activity Log ... 283
5.2.3.1 Viewing Audit Log ... 283
5.2.3.2 Log Records Filtering ... 286
5.2.3.3 Deleting Records from Log ... 290
5.2.3.4 Exporting Log Records ... 290
5.2.3.5 Analyzing Log Records in Microsoft Excel ... 290

5.3 General System Settings ... 291
5.3.1 Common Settings for Agents ... 291
5.3.2 Corporate Network Control ... 294
5.3.3 Messengers Control ... 296
5.3.4 Network Traffic Control ... 297
5.3.4.1 Adding Servers to Exclusions ... 299

5.3.5 Device Monitor Server Settings. Connecting to Traffic Monitor Server ... 301
5.3.6 Active Directory Connecting and Synchronizing ... 304
5.3.7 Employee Notifications about Policy (DM) Violations ... 308
5.3.8 Exclusion of Application from Interception ... 310
5.3.9 Application Control and screenshots ... 313
5.3.10 Event Storage ... 314
5.3.11 Synchronization of Traffic Monitor Policies ... 315
5.3.12 InfoWatch Device Monitor Server Manager ... 316
5.3.13 Stopping and Starting Device Monitor Agent ... 318
5.3.13.1 Stopping agent remotely/starting agent ... 318
5.3.13.2 Stopping/starting agent locally ... 319
5.3.14 Control of Keyboard Input ... 319
5.4 Managing Security Schema ... 320
5.4.1 Security Schema Organization ... 321
5.4.1.1 Security Policies and Rules (DM) ... 321
5.4.1.2 Employees and Employee Groups ... 323
5.4.1.3 Computers and Computer Groups ... 323
5.4.1.4 Uploading Security Scheme to Managed Computers ... 324
5.4.2 Security Scheme Overview ... 324
5.4.2.1 Viewing Active Security Scheme ... 324
5.4.2.2 Viewing Old Security Scheme ... 325
5.4.2.3 Security Scheme Comments ... 327
5.4.2.4 Editing Security Scheme ... 328
5.4.2.5 Updating Security Scheme ... 329
5.4.2.6 Exporting/Importing Security Scheme ... 330
5.4.3 Security Schema Setup ... 331
5.4.3.1 Security Policies (DM) ... 332
5.4.3.2 Rules (DM) ... 336
5.4.3.3 Employees ... 371
5.4.3.4 Computers ... 379
5.4.3.5 White Lists ... 389
5.4.3.6 Signatures ... 396
5.4.3.7 Application Protocol ... 398
5.4.4 Temporary Employee Access to Network ... 403
5.4.5 Temporary Employee Access to Devices ... 404
5.5 Viewing DM Events ... 406
5.5.1 Event Filters ... 414
5.5.2 Deleting Events ... 416
5.6 Agent Remote Installation, Updating and Uninstallation ... 417
5.6.1 Viewing Tasks ... 417
5.6.2 Preparing Primary Agent Installation. Distribution Agent ... 420
5.6.2.1 Enabling Shared Administrative Resources ... 421

5.6.2.2 Firewall Settings ... 421
5.6.3 Creating Primary Distribution Task ... 422
5.6.4 Creating Update Task ... 425
5.6.5 Creating Uninstallation Password Reset Task ... 427
5.6.6 Creating Uninstallation Task ... 428
5.6.7 Launching, Pausing, Editing, and Deleting Tasks ... 429
5.6.8 Agent Installation Errors ... 430
5.6.9 Creating Installation Package ... 431
5.7 Additional Features ... 434
5.7.1 Filter Table Contents ... 434
5.7.1.1 Filtering by Date ... 434
5.7.1.2 Applying Standard Filters ... 435
5.7.1.3 Custom Filter ... 435
5.7.1.4 Editing Filters ... 436
5.7.1.5 Removing a Filter ... 437
5.7.2 Grouping or Sorting Entries ... 437
5.7.3 Hotkeys ... 438
6 Licensing Information ... 442
6.1 User License Agreement ... 442
7 Glossary ... 445

# 1 InfoWatch Traffic Monitor Overview

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

Main functions of InfoWatch Traffic Monitor are listed below.

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

**InfoWatch Traffic Monitor Main Features:**

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

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

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

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

- Reviewing the files located in the corporative network (open network folders, workstation local discs, and SharePoint 2007/2010/2013 file storage) by 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, IMAP, Outlook; uploading data to cloud storages through HTTPS protocol, controlling data exchange via Jabber (XMPP protocol), Telegram (desktop version). Voice messages in Skype can also be intercepted. These data is intercepted by InfoWatch Device Monitor system.
- Intercepting and analyzing MS Lync objects via IW Lync Adapter installed on MS Lync server.
- Analyzing the contents of the intercepted traffic in order to detect violations of the corporate security policy.
- Filtering the intercepted traffic by allowing or blocking the delivery of certain data.

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

**InfoWatch Traffic Monitor Components:**

| InfoWatch Traffic Monitor Component | Purpose |
|---|---|
| Traffic Monitor Server | Interceptors: **IW_SNIFFER**, **IW_ICAP,** and **IW_SMTPD**.<br>**Analysis subsystem** receives event context and checks if the events contain technology elements and correspond to protected objects.<br>**Policy applying subsystem** implements actions defined by the user according to the corporate security policy. |
| Database | Storage of information associated with the System operations (intercepted data and results of their analysis). |
| Device Monitor | Interaction with workstations. Controlling user access to the peripherals, monitoring operations (data copying from/to removable storages and FTP, sending data to printing, using messengers) and intercepting the traffic from instant messengers. |
| 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 Objects Interception

The System objects are the following:

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

**Warning!**

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

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

It is also recommended to get acquainted with the differences of Traffic Monitor and Device Monitor functionality according to OS used. The articles are available in the knowlege base.

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

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

| | |
|---|---|
| Outlook | The System receives a copy of traffic from InfoWatch Device Monitor |
| 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.<br>When ICQ connects through HTTP, the System intercepts ICQ traffic in the same way as HTTP traffic. |
| Messages from messengers | The System receives a copy of Skype (including voice messages), Telegram (desktop version), Facebook, VK 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 |

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),<br>HTTP Processing module (copy mode),<br>ICQ Processing module (copy mode),<br>Shadow Copies Processing module,<br>SMTP Processing module (blocking mode),<br>HTTP Processing module (blocking mode). | Extracting significant data and 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.

> **Note:**
>
> Spliced files policy false positive may happen when detecting files of **xls**, **pdf**, **jpg**, **docx** format. See details in the article "Intercepted files are incorrectly marked as spliced" in the knowlege base.

## 1.3 Retrospective Data Analysis, User Decision on an Object

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

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

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

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

## 1.4 InfoWatch Traffic Monitor Transport Modes

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

> **Warning!**
>
> The transport mode can be specified only once for each object.

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

**Table 1**

| Transport mode | Description |
|---|---|
| **Blocking** | InfoWatch Traffic Monitor intercepts, analyses, and transports objects. In this mode, the verdict defines if the object will be delivered to recipients. Besides, in some cases, the delivery status of the SMTP messages can be changed after changing the user decision (see "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 object analysis only. As the System analyses the copy of objects, the verdict, and the analysis-based user decision do not impact the object delivery to recipients. |

**Table 2**

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

| | | |
|---|---|---|
| Shadow copy of a file | No | Yes |

## 1.5 Uploading Object to Database

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

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

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

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

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

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

Supported Web resources:

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

| | | |
|---|---|---|
| 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 is a system for controlling access to computer peripherals. Besides, InfoWatch Device Monitor allows you to monitor transferring data to removable devices, over a network or printing data. Monitoring result are then sent to InfoWatch Traffic Monitor for analysis.

The main functions of InfoWatch Device Monitor:

- Real-time control of managed workstations, automatic screenshots making (see "ScreenShot Monitor Rule (DM)")
- Control of employee access to peripherals (see "Device Monitor Rule (DM)")
- Monitoring print operations (see "Print Monitor Rule (DM)")
- Control of instant messengers: Skype, Telegram (desktop version), Facebook, VK, Jabber (XMPP protocol), MMP protocol (see "IM Client Monitor Rule (DM)")
- Control of traffic sent via FTP and FTPS (see "FTP Monitor Rule (DM)")
- Control of traffic sent via HTTP and HTTPS (see "HTTPS Monitor Rule (DM)")
- Control of transferring data through network connections outside the corporate network (see "Network Monitor Rule (DM)")
- Control of mail protocols (SMTP, IMAP, POP3, Outlook, HTTPS) (see "Mail Monitor Rule (DM)")
- Control of connection via Microsoft RDP or Citrix ICA (see "Device Monitor Rule (DM)")
- Control of copying files from/to removable devices and network resources (see "File Monitor Rule (DM)")
- Cloud storage control (see "Cloud Storage Monitor Rule (DM)")
- Control of taking screenshots (see "ScreenShot Control Monitor Rule (DM)")
- Control of applications (see "Application Monitor Rule (DM)")
- Control of employee access to the clipboard (see "Configuring Clipboard Monitor Rule")
- Control of keyboard input (see "Keyboard Monitor Rule (DM)")
- Gathering data received from controlled computers
- Data transfer into InfoWatch Traffic Monitor for analysis
- Configuring event storage (see "Event Storage")

**Warning!**

Only the following control functions are available for workstations on Astra Linux OS:

- Control of mail protocols SMTP, POP3, IMAP, and HTTPS (see "Mail Monitor Rule (DM)")
- Control of copying files from/to removable devices and network resources (see "File Monitor Rule (DM)")
- Cloud storage control (see "Cloud Storage Monitor Rule (DM)")
- Control of traffic sent via FTP and FTPS (see "FTP Monitor Rule (DM)")
- Monitoring print operations (see "Print Monitor Rule (DM)")
- Control of instant messengers: Facebook, VK, Jabber (XMPP protocol) (see "IM Client Monitor Rule (DM)")
- Control of traffic sent via HTTP and HTTPS (see "HTTPS Monitor Rule (DM)")

**Note:**

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

Actions of employees are controlled on managed computers. For this, agent modules are installed on the controlled computer. The agent 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, ScreenShot Monitor, Keyboard Monitor, Photo Monitor**. For more information on interceptors, see "Rules (DM)".

**Note:**

The work of interceptors is supported in restricted mode on workstations on Astra Linux OS (for details about specifics of interceptors work on different OS, see the rules description).

Intercepted data is analyzed on Device Monitor agents with the following detection technologies:

- Files formats
- Text objects
- Terms/ content filtering base

### 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<br>Safe Mode with Networking |

| | |
|---|---|
| Write control on removable devices | Safe Mode<br>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:**
>
> The administrator's tasks are partly described in "Administrating the System". For other information on the initial configuration of the System, see "*Infowatch Traffic Monitor. Administration Guide*".

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

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

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

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

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

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

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

**Warning!**

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

## 2.1 System Operation Before Configuring

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

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

  **Warning**

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

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

## 2.2 Configuring the System

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

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

**Warning!**

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

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




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

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

**The configuration process includes:**

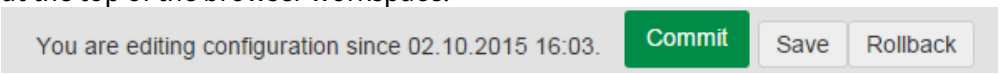
- Creating the base of technologies (see "Managing the Base of Technologies"):
  - Selecting terms to be detected - only when using **Linguistic Analysis technology** (see "Terms");
  - Selecting text object types to be detected - only when using **Detecting Text Objects technology** (see "Text objects");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

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

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

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

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




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

**Warning!**

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

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

- **Apply configuration** (see "Applying System Configuration") - the updated configuration becomes active on the server.
- **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.

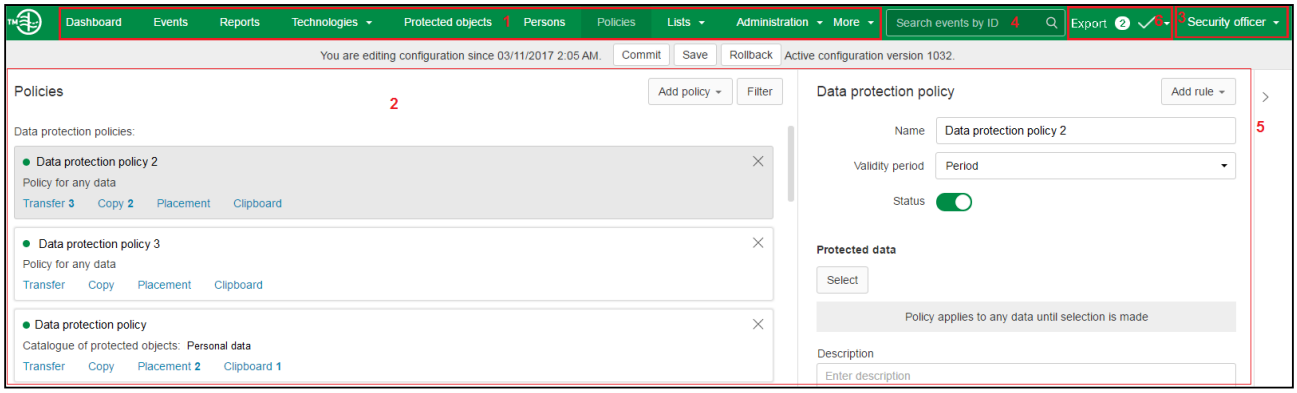
You can also update data manually in any section of the Management Console. To do this, use the standard browser refresh tool: by default the page is refreshed when you press the function key F5).

**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.<br>Click the section button to go to the selected section of the Management Console. |
| 2 | Working area | Displays elements of a selected Management Console section; is used for managing elements of the selected section. |
| 3 | User menu button | Displays the user name.<br>Click to open a drop-down list where you can:<br>• Change the password for your account (see "Changing User Password")<br>• Change the interface language (see "Selecting Interface Language")<br>• Call Help for system (see "Calling Help File")<br>• Get information on the System (see "Viewing Information on System")<br>• Log out of the Management Console (see "Login and logout of the Management Console") |
| 4 | Field for searching events by ID | Is displayed in all sections of the Console. Allows you to find required events by their ID. If you are searching events not from the "Events" section, you will be redirected to the "Events" section where the search results are displayed. 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. |
| 6 | Button for viewing information on export files | Is displayed in the System contains dashboard reports or event export files or if the event export is in progress. Click the button to view information on ready dashboard reports and event export files as well as export files being created at the moment. For details, see "Viewing Dashboard Report" and "Event Export". |

You can work in the Management Console in the sections:

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

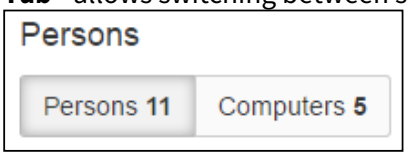
You can go to a specific section by clicking the section button.




**Events** section button

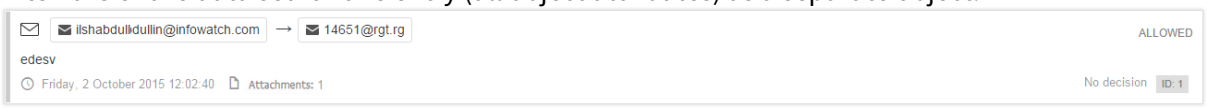
The following interface elements are used in the Management Console:

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




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

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




**Events** section, the event tile

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

**Note:**

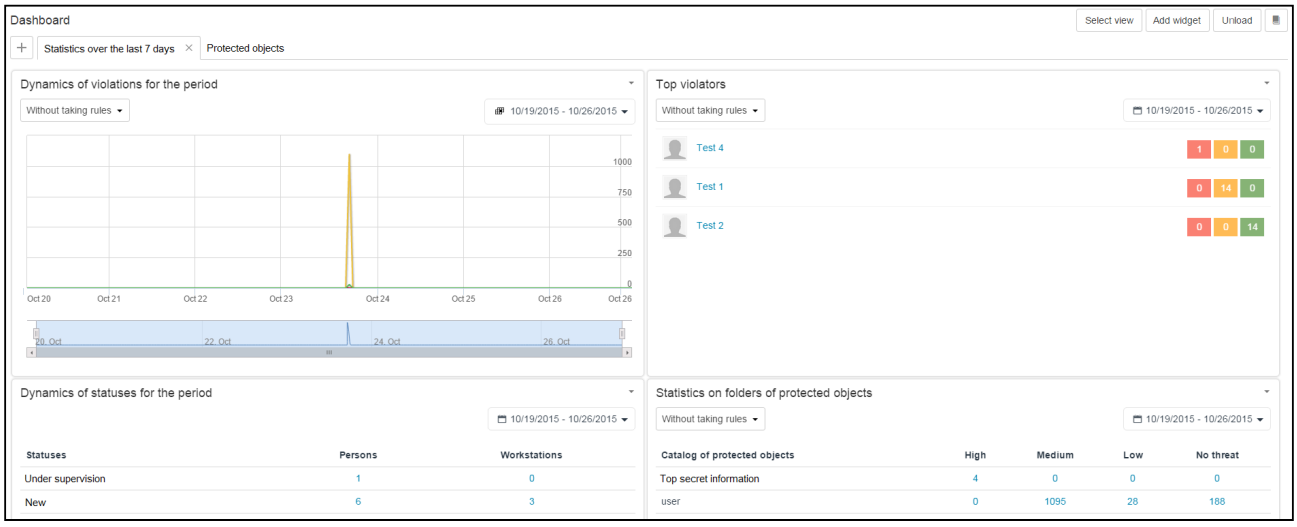
While downloading the requested data, the System may display the icon or an informational message.

## 3.1 Dashboard Section

**About the section:**

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

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




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

- splitting into 3 equal parts

- splitting in a ratio of 2:1

 - splitting into 2 equal parts

 - splitting in a ratio of 1:2

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

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

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

**User's target actions:**

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

### 3.1.1 Dashboard Widgets

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

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

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

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

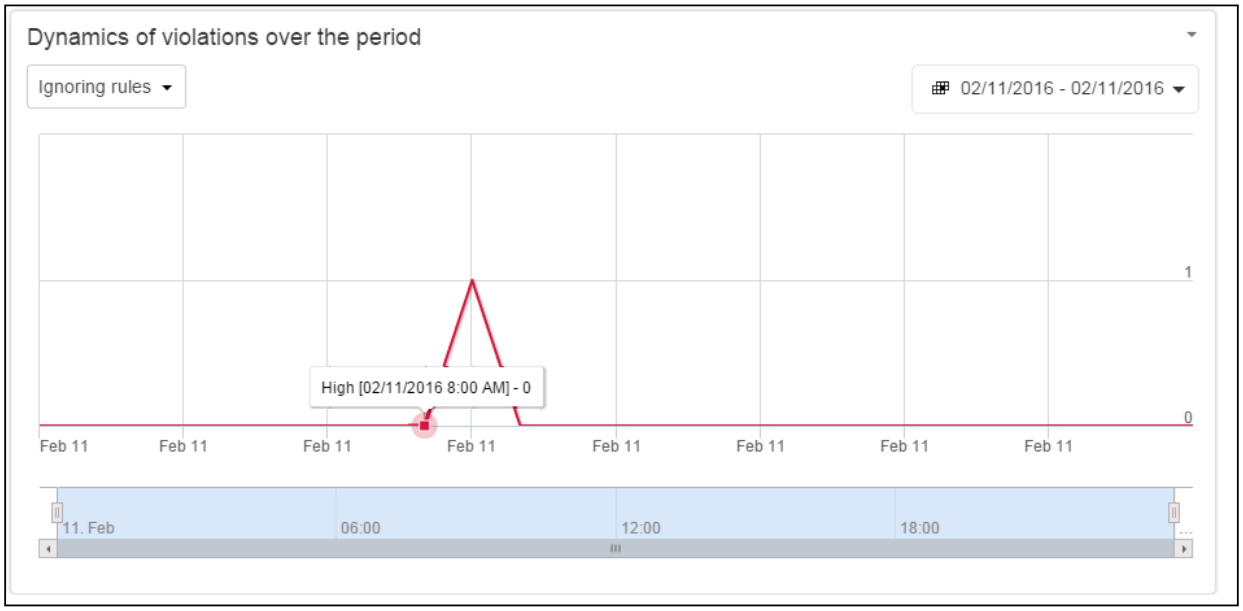
| | |
|---|---|
| Statistics on catalogs of protected objects | The number of violations per catalogs of protected objects broken down by levels of violations over the selected time period |

**User's target actions:**

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

## Dynamics of Violations over the Period

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




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

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

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

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

## Top Violators

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

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




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

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

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

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

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

You can edit the following parameters:

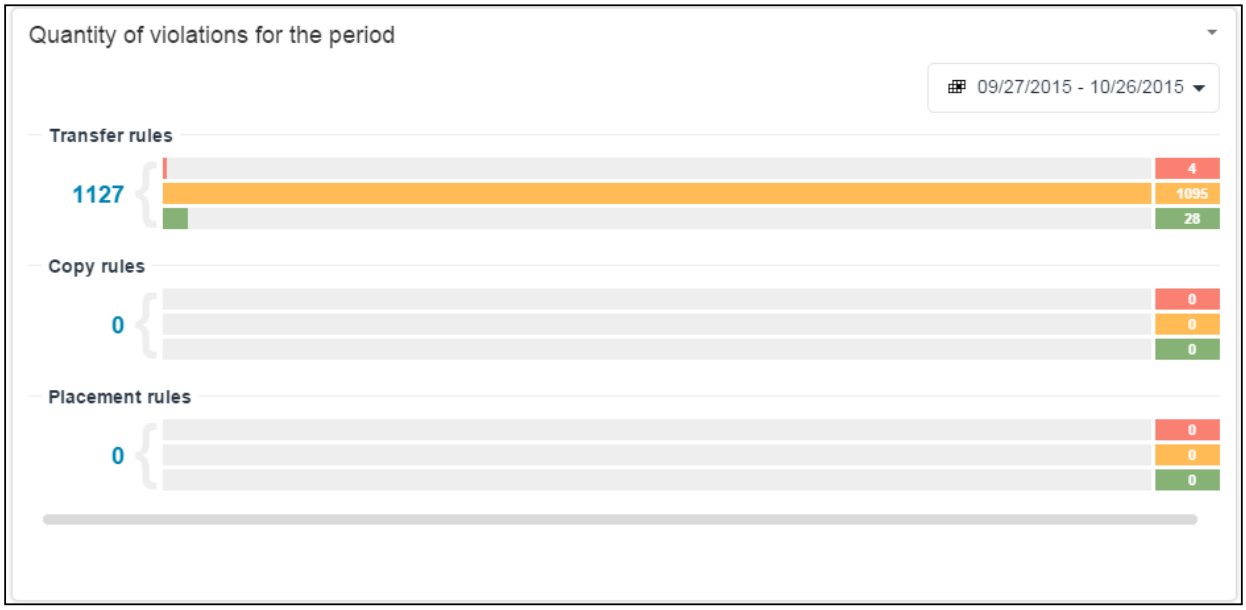
- **Name**;
- **Update interval** for data on the widget;
- **Quantity of violators** for which statistics will be displayed;
- **Groups** to which violation can belong. Statistics on the selected groups will be displayed in the widget. Start typing the group name or click + and select desired groups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

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

## Quantity of Violations over Period

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

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




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

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

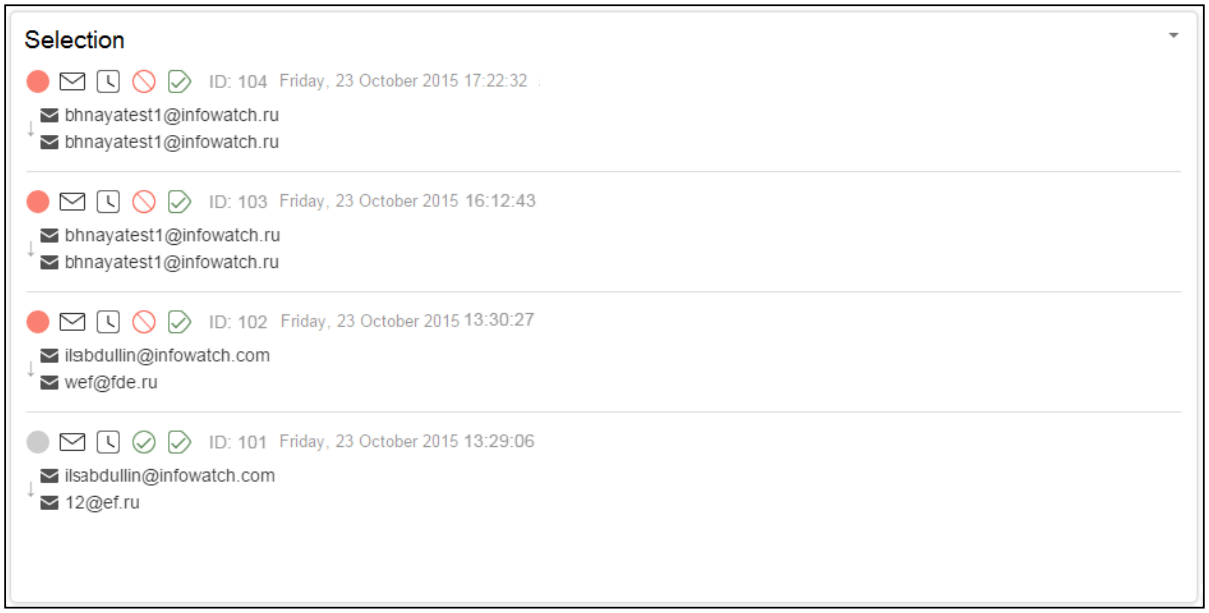
You can edit the following parameters:

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

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

## Selection

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




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

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

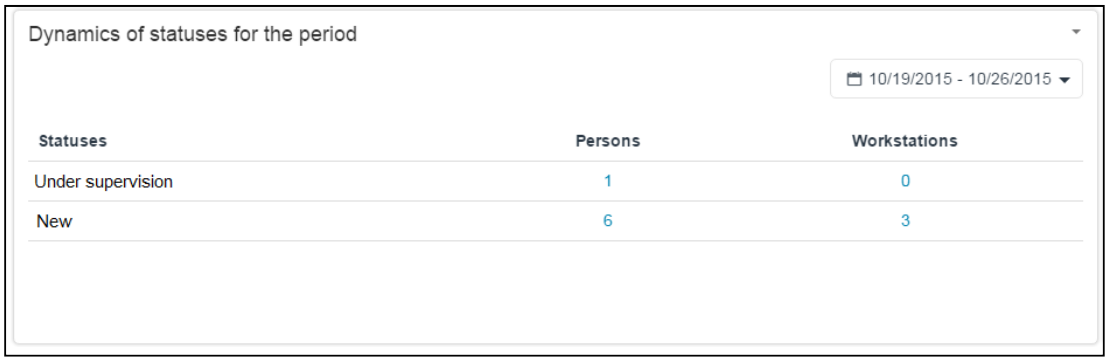
You can edit the following parameters:

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

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

## Dynamics of Statuses

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



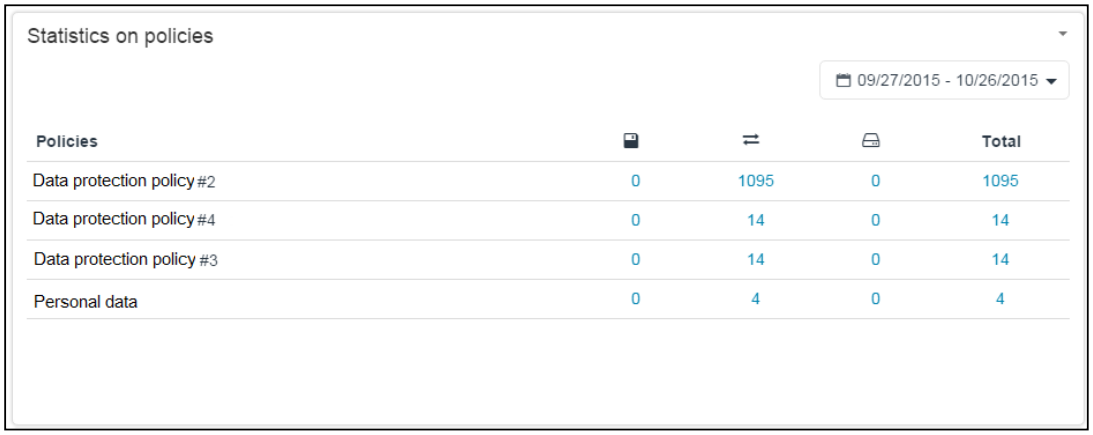

Clicking the number of persons or computers (highlighted in blue) opens the "Persons" section (the **Persons** or **Computers** tab respectively), where you can view the list of persons (or computers) that meet the conditions specified in the widget properties.

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

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

## Policy Statistics

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




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

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

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

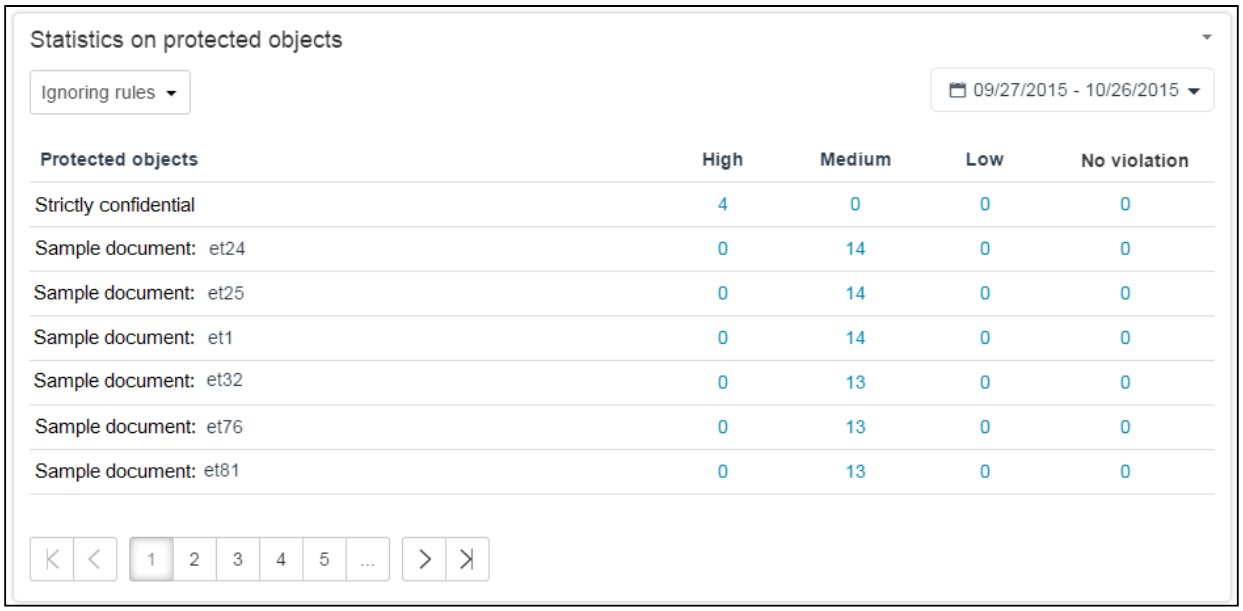
You can edit the following parameters:

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

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

## Statistics on Protected Objects

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



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

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

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

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

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

You can edit the following parameters:

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

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

## Statistics on Catalogues of Protected Objects

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




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

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

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

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

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

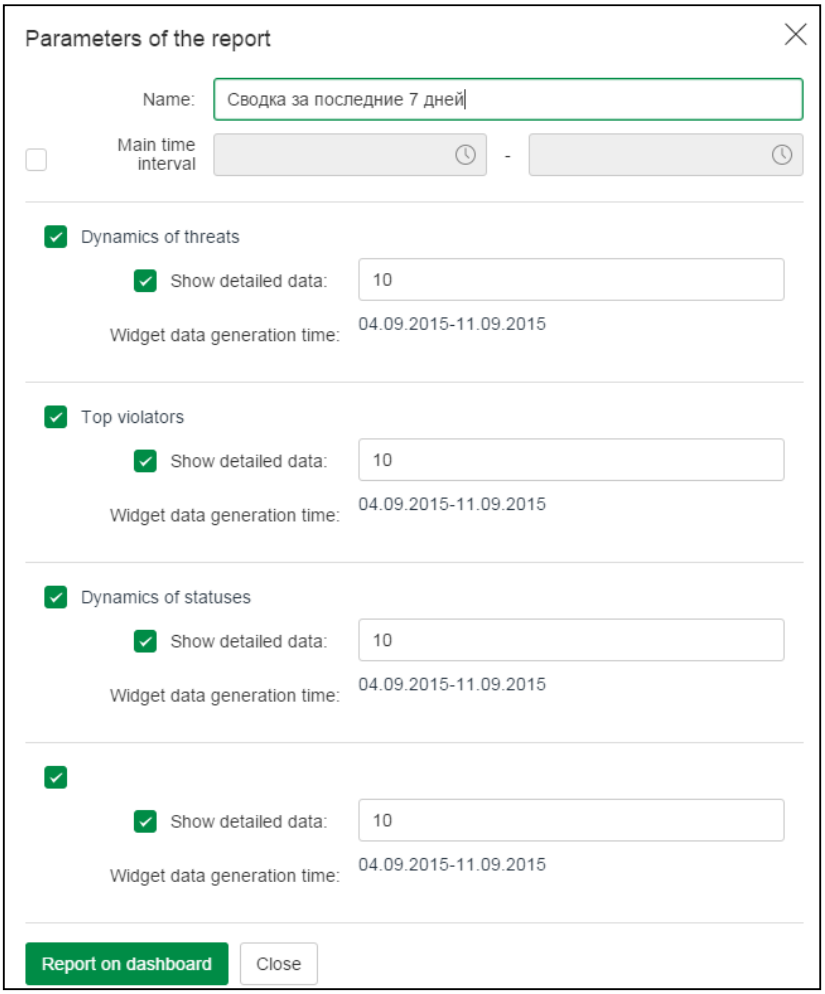
You can edit the following parameters:

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

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

## 3.1.2 Dashboard Report

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




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

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

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

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

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

**User's target actions:**

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

## 3.2 Events Section

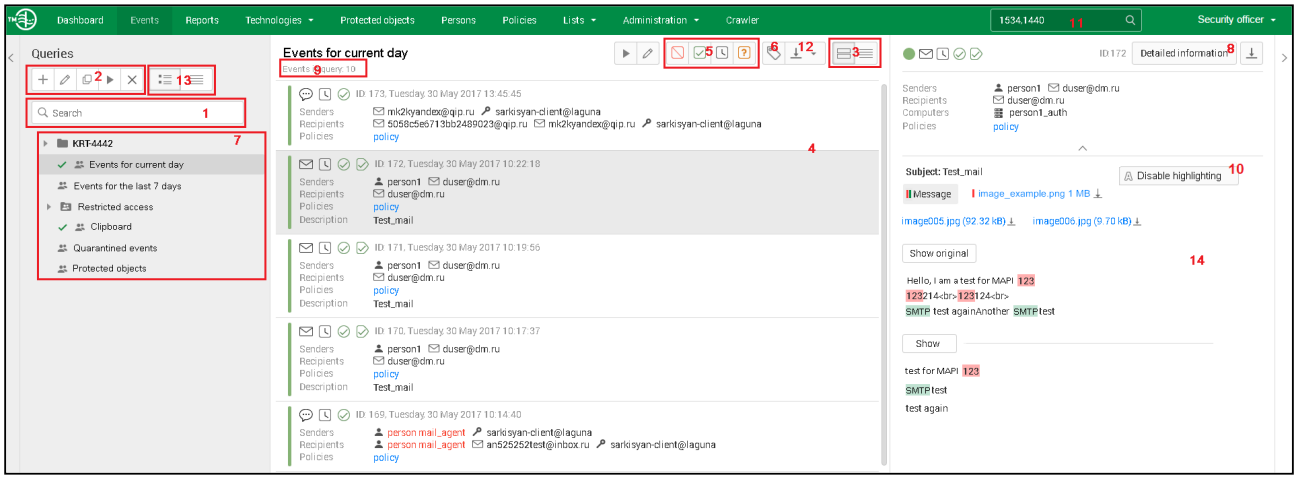
**Reference information:**
The event is the interception object of network traffic.

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

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

**About the section:**

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




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

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

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

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

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

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

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

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

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

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

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

-  - as tiles;
-  - as a table.

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

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

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

- 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:**

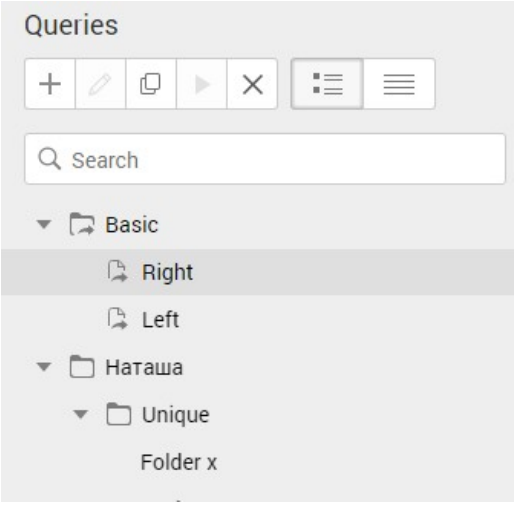
- Filtering events (see "Creating Queries")
- Viewing event details (see "Viewing Brief Event Form" and "Viewing Detailed Event Form")
- Making decision on the event (see "Making Decision on Object")
- Adding/removing tags (see "Adding and Deleting Tags")
- Saving the event (see "Saving Events (for SMTP 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 the System are stored in the database. To view information about these objects in the Management Console, you need to create and execute a query.

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

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




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

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

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

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

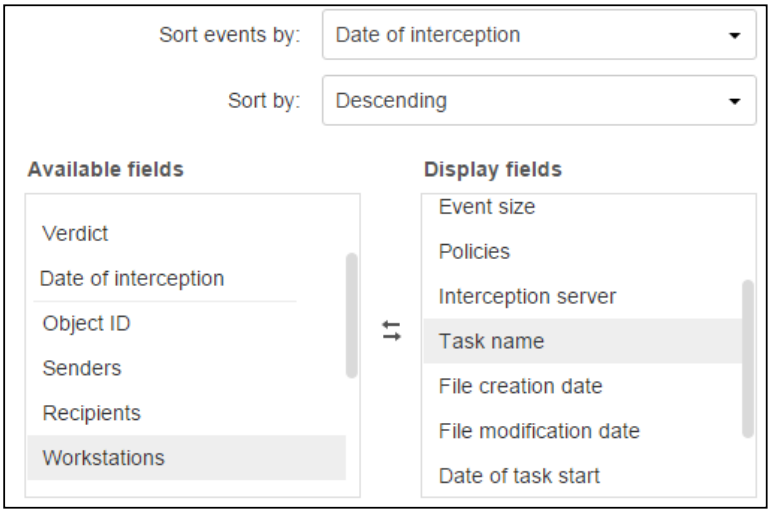
If the query is being executed at the moment, the icon is displayed next to its name. For queries whose execution failed, the icon is displayed.

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

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

The query creation form contains the following tabs:

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




If no attributes selected, the table form and the export file will include all the attributes.
You can also select the field to sort the list by and specify the sorting direction.

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

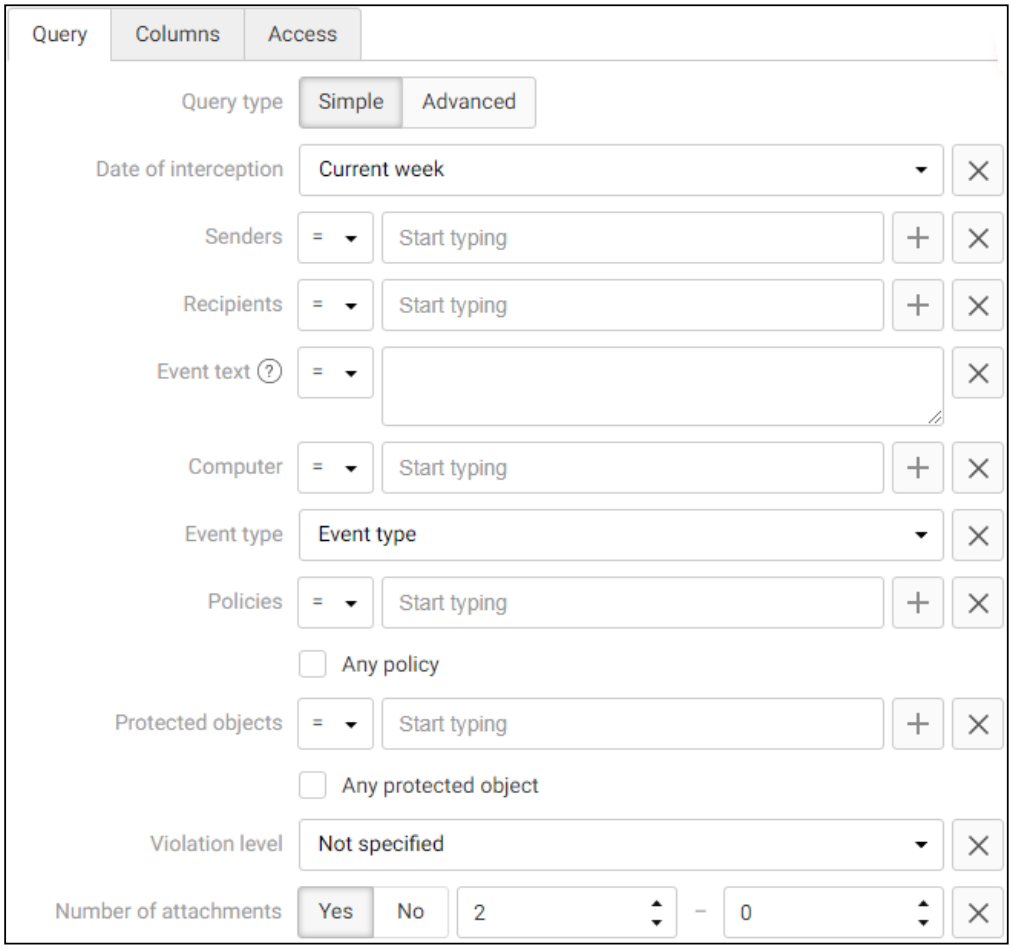
**User's target actions:**

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

## Standard Mode of Creating Queries

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

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




By default, most commonly used conditions are displayed.

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

The full list of available conditions:

| **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 are displayed.<br>Possible values:<br>▪ All time<br>▪ From<br>▪ To<br>▪ Current day/week/month<br>▪ Last several hours/days<br>▪ Last 3/7/30 days<br>▪ Period (from a calendar) |

| | |
|---|---|
| Event type | Specifies that the event belongs to a particular interceptor.<br>Event types are grouped by category. When selecting a category, all event types of this category will be displayed. Possible values:<br>• Application activity:<br>- Working in applications<br>- Clipboard<br>- Keylogger<br>• Internet activity:<br>- Web message<br>• File sharing:<br>- FTP<br>- Removable devices<br>- Cloud storage<br>- Terminal session<br>- Network resources<br>• Printers and MFPs<br>- Print<br>• Storage<br>- Crawler<br>• Email<br>- Mail on Client<br>- Mail in Browser<br>• Messenger<br>- Telegram<br>- Facebook<br>- VKontakte<br>- MS Lync<br>- ICQ<br>- XMPP<br>- MMP<br>- Skype<br>- Kribrum<br>• File operations:<br>- Read file<br>- Write file |
| Interceptor | Interceptor by which the event was received. Possible values:<br>• ICAP<br>• DM<br>• Adapter<br>• SMTPD<br>• Sniffer<br>• PushAPI<br>• Crawler |

| | |
|---|---|
| Protocol | Protocol over which the traffic was transferred. Possible values:<br>• FTP<br>• HTTP<br>• HTTPS<br>• IMAP<br>• MAPI<br>• MMP<br>• NRPC<br>• OSCAR<br>• POP3<br>• SIP<br>• Skype<br>• SMTP/ ESMTP<br>• XMPP |
| Copy sources and receivers | Sources and receivers, copy is performed from/to.<br>Configuration options:<br>• Copy receiver:<br>- Computer<br>- Removable device<br>- Network resource<br>- Terminal session<br>- FTP<br>- Cloud storage<br>• Copy source:<br>- Computer<br>- Removable device<br>- Network resource<br>- Terminal session<br>• Route direction:<br>- One direction<br>- Both directions<br>You may specify Path to a file or address, Device name, Device ID.<br>The value can be specified using wildcards:<br>• "?" - to replace a single character in the beginning or at the end of the string;<br>• "*" - to replace any number of characters in the beginning or at the end of the string.<br>**Note:**<br>Depending on the selected type of the copy source/receiver, there can be different recommendations on how to fill in the **Path to file or address** field (see "Recommendations on how to fill in the Path to file or Address field"). |
| Mandate level | Mandate level of confidentiality. It is recognized by Traffic Monitor, starting from version 6.10.10 on Astra Linux OS. |

| | |
|---|---|
| *Recipients* | |
| Senders | The list of object senders. May include persons, person groups, statuses, or contact values (except SID). For contacts, a value can be specified using wildcards:<br>• "?" - to replace a single character in the beginning or at the end of the string;<br>• "*" - to replace any number of characters in the beginning or at the end of the string. |
| Recipients | The list of object recipients. May include persons, person groups, statuses, or contact values. For contacts, a value can be specified using wildcards:<br>• "?" - to replace a single character in the beginning or at the end of the string;<br>• "*" - to replace any number of characters in the beginning or at the end of the string. |
| Number of recipients | The number of object recipients |
| Entered perimeters | Perimeter the object recipient belongs to |
| Left perimeters | Perimeter the object sender belongs to |
| Computer | The computer from which the object was sent. You can specify a computer name or an IP address. The value can be specified using wildcards:<br>• "?" - to replace a single character in the beginning or at the end of the string;<br>• "*" - to replace any number of characters in the beginning or at the end of the string. |
| Computer type | Type of computer from which the object was sent. Possible values:<br>• workstation<br>• 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.<br>The value can be specified using wildcards:<br>• "?" - to replace a single character;<br>• "*" - to replace any number of characters.<br>**Note**: If you want to specify a particular resource, choose icon (for example, facebook.com) |
| *Working in applications* | |
| Source application | Application from which data has been copied |

| | |
|---|---|
| Receiver application | Application to which data has been pasted from the clipboard |
| *Analysis results* | |
| Violation level | The level of violation of the corporate security policy. Possible values: *High*, *Medium*, *Low*, *No violation*. |
| Tags | Tags assigned to the object (see "Tags") |
| Policy | List of policies triggered on the object |
| Violation type | Type of rule that was violated. Possible values:<br>▪ *Violation of transfer*<br>▪ *Violation of copy*<br>▪ *Violation of placement* |
| User decision | A decision the user made for the object. Possible values:<br>▪ *Violation*<br>▪ *No violation*<br>▪ *No decision*<br>▪ *Requires additional processing* |
| Verdict | The verdict passed by the System on the object. Possible values:<br>▪ *Allowed*<br>▪ *Blocked*<br>▪ *Quarantine* |
| Technologies | Elements of technologies included in protected objects that were triggered on events.<br>If you add a text object, you can specify its value. If you add a text object and apply negation to the attribute, then the query results will not include events that contain the selected text object with the specified value. See also "Examples of Using Queries", *Example 6*.<br>**Note:** If the System has been updated to version 6.9, then the analysis results may omit system text objects from events that were intercepted before the update. |
| Protected objects | List of triggered protected objects.<br>You can select separate protected objects as well as catalogues. |
| *Crawler* | |
| Task name | Name of the scanning task. You can specify the value using wildcards:<br>• "?" - to replace a single character in the beginning or at the end of the string;<br>• "*" - to replace any number of characters in the beginning or at the end of the string. |

| | |
|---|---|
| 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:<br>• Shared network resources<br>• Local drives of workstations<br>• SharePoint file storage |
| File creation date | A date when the file was created on a disk or resource |
| File modification date | A date when the file was modified on a disk or resource |
| *Event content* | |
| Number of attachments | Using **Yes**/**No** switcher, specify if the event contains attachments. For events with attachments, specify the minimum and the maximum number of attachments the event may include. If you click **Yes** and do not set the number of attachments, the query results will include all events with attachments. |
| Attachment name | The name of the object attachment. Both file name and extension must be specified. You can specify the value using wildcards:<br>• "?" - to replace a single character in the beginning or at the end of the string;<br>• "*" - to replace any number of characters in the beginning or at the end of the string.<br>**Note**: If the attachment name contains a comma, the comma must be screened with \. For example, the 'test1,2.txt' attachment name should be specified as 'test1\,2.txt'.<br>See also the "How to find the event by its attachment" knowledge base article. |
| Attachment format | Attachment format. You can select multiple values from the list. |
| Path to file | File source. You can specify the value using wildcards:<br>• "?" - to replace a single character in the beginning or at the end of the string;<br>• "*" - to replace any number of characters in the beginning or at the end of the string. |
| 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.<br><br>When the condition is denied, events whose text contains all specified words will be excluded from search results.<br><br>**Note:** Search results will contain only those events that have already been indexed at the moment of the query execution. Events are indexed every ten minutes, however, under a heavy load on the server, this interval may increase. |
| *User attributes* | |
| | Attributes which can be added into the System via plugins, registered in Traffic Monitor (see Plugins). Thus increasing the amount of information to be processed and transmitted via adding attributes of third-party systems that are events sources. User attributes can be used in the rules of data protection policies.<br><br>Examples of possible user attributes:<br><br>• conversation duration;<br>• event identificator in initial system;<br>• hyperlink to event in initial system;<br>• type of action in network media. |

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

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

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

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

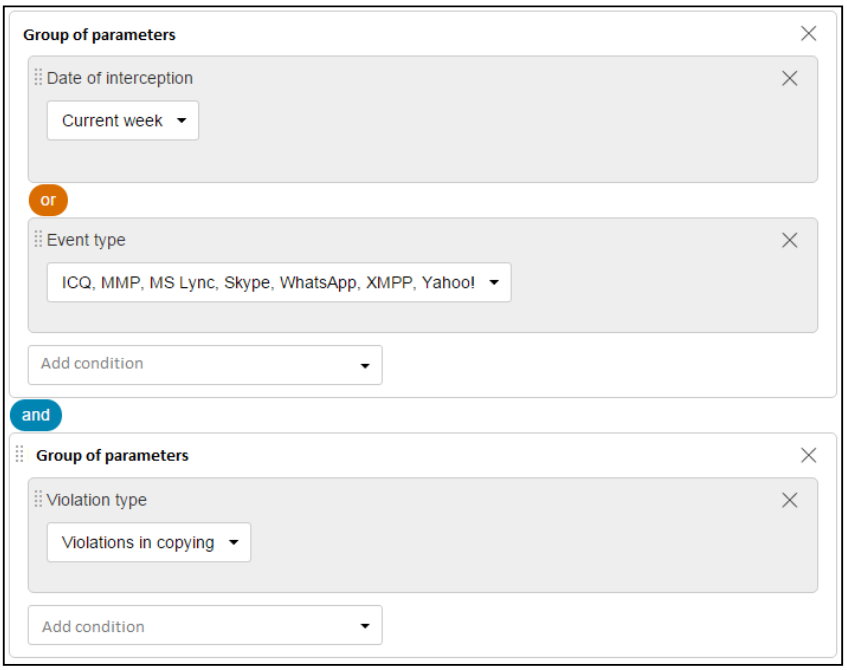
If a negation parameter is applied to an attribute with multiple values, then events that contain specified values will be excluded from search results. For example, if `user1@example.com` and `user2@example.com` users are specified as Senders, then events with the sender `user1@example.com` or `user2@example.com`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

**User's target actions:**

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

## Advanced Mode

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




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

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

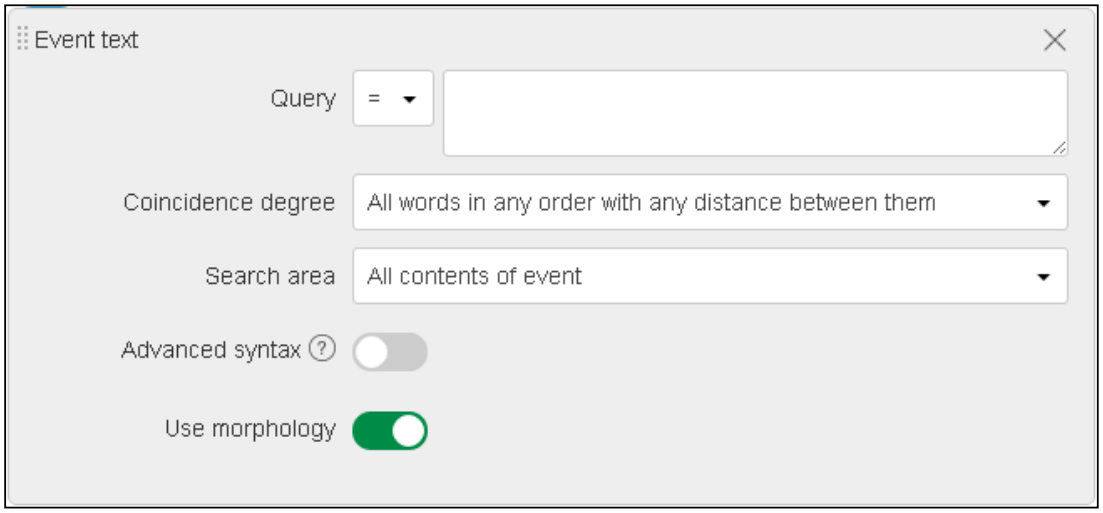
In the advanced mode, you can also perform a flexible search on the text of events.

**User's target actions:**

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

## Search on the Event Text

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




Full-text search parameters:

| Parameter | Description |
|---|---|
| Query | The text which the event contains or does not contain (if negation ≠ is applied to the attribute) |
| Coincidence degree | Specify the required coincidence degree:<br>• **All words following each other in specified order** - search results will include events whose text contains all listed words arranged in the specified order.<br>If the condition is negated, search results will include events whose text does not contain listed words arranged in the specified order.<br>• **All words following each other in any order** - search results will include events whose text contains all listed words in any order.<br>If the condition is negated, search results will include events whose text does not contain listed words irrespective of their order.<br>• **All words in any order with any distance between words** - search results will include events whose text contains all listed words irrespective of their order and distance between words.<br>If the condition is negated, search results will include events whose text does not contain listed words or contains not all of them.<br>• **At least one of the words** - search results will include events whose text contains, at least, one of the listed words.<br>If the condition is negated, search results will include events whose text does not contain any specified word. |
| Search area | Specify the area in which the search will be performed:<br>• **All contents of event** - search on all contents of the event will be performed.<br>• **Message body** - search on the message text and message subject will be performed.<br>• **Message subject** - search on the message subject will be performed.<br>• **Attachment** - search on the attachments text and file names will be performed.<br>• **File name** - search on the attachment file names will be performed. |

| | |
|---|---|
| Advanced syntax | Enable this setting if you want to specify the sought-for text using boolean operators. For details, see "Using advanced syntax". |
| Use morphology | If this setting is disabled, search results will include only those events which contain the sought-for words in a specified grammar form.<br>**Note:** 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.
- Hyphen ("-") is not taken into account while searching. Search is performed by each word, which is a part of a word with hyphen used.

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

**User's target actions:**

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

### 3.2.2 Object Interception

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

Information on the event is presented in following ways:

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

Event attributes:

| Element | Description |
|---|---|
| Object ID | Event unique identifier in the System |
| User decision | Decision the user made for the event. Possible choices:<br>• *No decision*<br>• *Violation*<br>• *No violation*<br>• *Requires additional proceeding* |

| | |
|---|---|
| Event type | The source of actions which led to the event creation. Possible choices:<br>•  - Internet activity (post requests to Web resources)<br>•  - File exchange (copying files to an external device or to a shared folder, transfer via FTP)<br>•  - Printer and MFP (sending files to print)<br>•  - Recording media (sending or receiving photos)<br>•  - Email (sending and receiving data via mail on client or mail in browser)<br>•  - Messenger (sending or receiving messages through Skype, MS Lync, ICQ(OSCAR), XMPP, Telegram)<br>•  - File storage (in SharePoint 2007/2010/2013 file storage, shared network resources and on local drives of workstations) |
| Sending date | Date and time when a mail server received the mail (only for e-mails) |
| Senders | The list of traffic senders |
| The sender's computer | The name of the computer from which traffic was sent |
| Recipients | The list of traffic recipients |
| Policies | List of policies triggered on analysis of this event |
| Categories | List of categories assigned to this event |
| Protected objects | List of protected objects triggered for this event |
| Elements of analysis | The list of elements of analysis contained in the triggered protected object |
| Website topic | Type of inappropriate resources visited by the employee |
| Tags | List of tags assigned to this object |
| Date of interception | Date and time when traffic was intercepted by the System |
| Insert date | Date and time when the event was saved into the Database |
| Size | Size of the event (in bytes) |

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

See also:

- "Event Tile" - on presenting the event and its attributes.
- "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 is displayed when you select an event in the list:



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

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

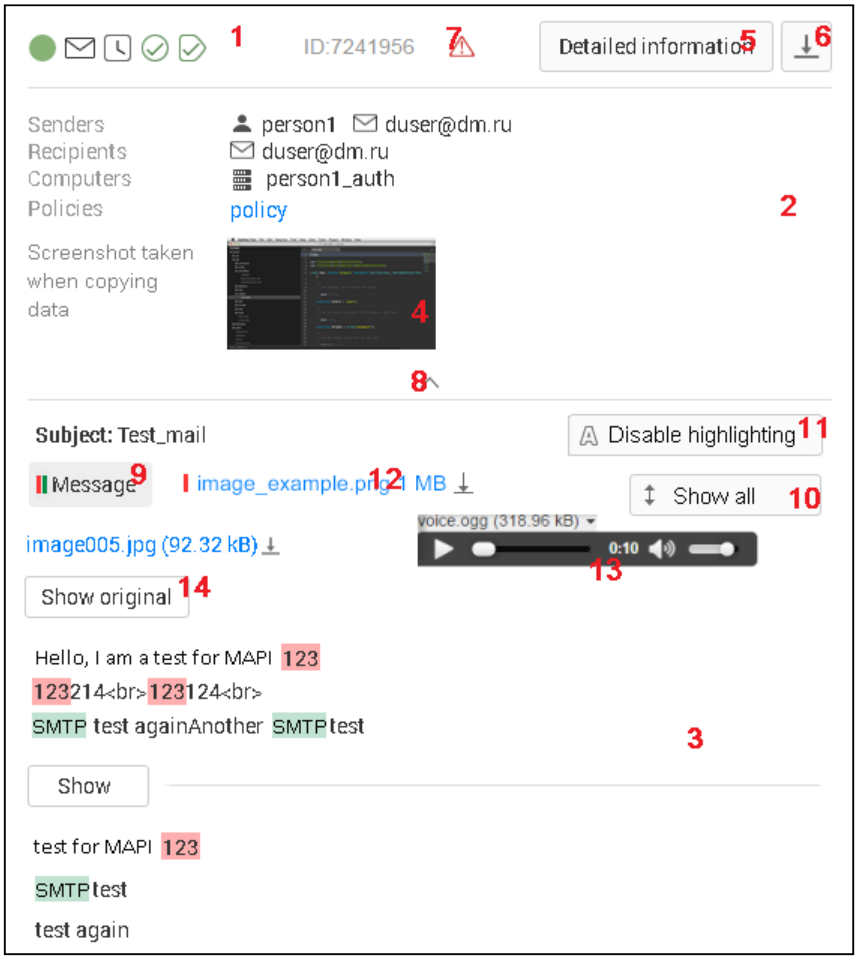
> **Note:**
>
> The set of displayed attributes depends on the event type.

1. The colour of the violation level. Possible values: *High*, *Medium*, *Low*, *No violation*.
2. The event type. Possible values: *Crawler, Clipboard, Keyboard input, Web message, Facebook, ICQ, MS Lync, Mail.ru Agent, Skype, Telegram, XMPP, Vkontakte, Cribrum, Mail on Client, Mail in Browser, FTP, Removable device, Cloud storage, Network resource, Terminal session, Print*.
3. The user desicion. Possible values: *Violation*, *No violation*, *No decision*, *Requires additional processing*.
4. The verdict. Possible values: *Allowed*, *Blocked*, *Quarantine*.
5. The sending status. Possible values: *Sent, Not sent, Waiting for sending.*
6. The list of triggered policies.
7. Tags assigned to the event. For details, see "Tags".
8. The screenshot indicator. Is displayed if a screenshot has been created for a person or computer.
9. The attachment indicator. If the event contains attachments, an indicator with the number of attachments is displayed.

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

## Brief Event Viewing Form

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




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

1. The upper part of the form (№ 1in the screenshot) where you can see:
   - event ID;
   - indicators of the following event attributes: the violation level, the event type, the user decision, the verdict, a delivery status (for possible attribute values, see "Event Tile");
   - the **Detailed** button (№ 5 in the screenshot), clicking which opens the detailed event viewing form (see "Detailed Event Viewing Form");
   - button (№ 6 in the screenshot) which allows you to save a shadow copy of the event (see "Saving Events (for SMTP mail)"). The button is displayed for SMTP messages only;
   - the indicator of processing errors (№ 7 in the screenshot). Is displayed if errors occurred during processing. You can see more details on the errors in the detailed event viewing form.
2. The area for viewing the event parameters (№ 2 in the screenshot).
   In the viewing area, you can see information on senders, recipients, triggered policies, and protected objects. Protected objects and policies that have been removed from the System are marked in red. For clipboard events, a thumbnail of the screenshot is displayed (№ 4 in the screenshot) if a screenshot has been taken during data copying/pasting.

   To hide the area with the event parameters, click (№8 in the screenshot). To restore the area, click .

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

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

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

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

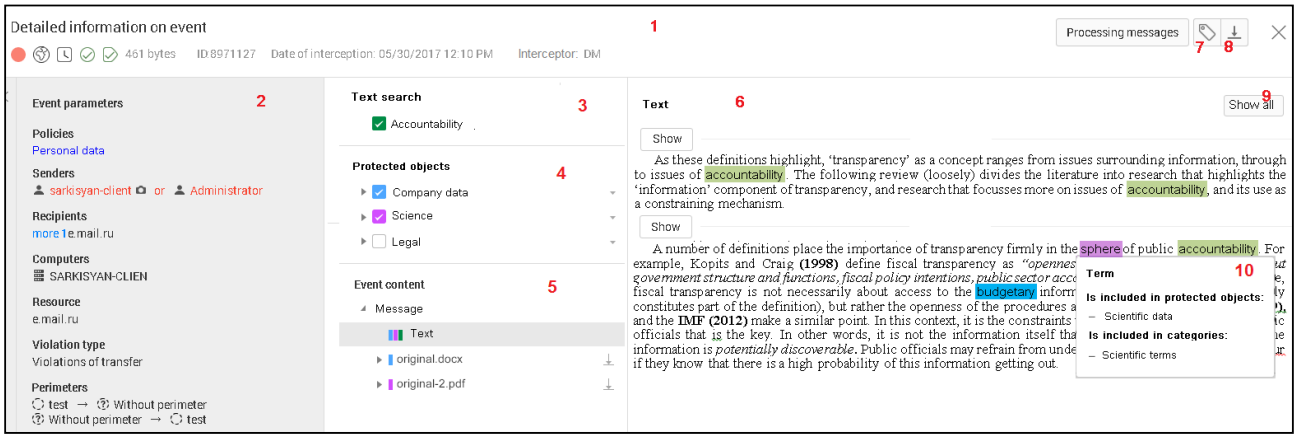
   To save an attachment to your computer, click (№ 12 in the screenshot) next to the attachment name.

**User's target actions:**

- Viewing Brief Event Form

## Detailed Event Viewing Form

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



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

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

   The  button next to the attachment name allows you to save a selected file to your computer.
6. The viewing area (№ 5 in the screenshot). Allows you to view the message text and the text extracted from attachments.

Be default, in the viewing area (№ 5 in the screenshot), the text is displayed as snippets which contain triggered protected objects or the found text.

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

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

- for each protected object, a separate colour is used; all triggered elements of technologies related to these protected objects are highlighted in the same colour;

  > **Note:**
  >
  > If a part of the text belongs to several elements of technologies, this part is highlighted in gray.

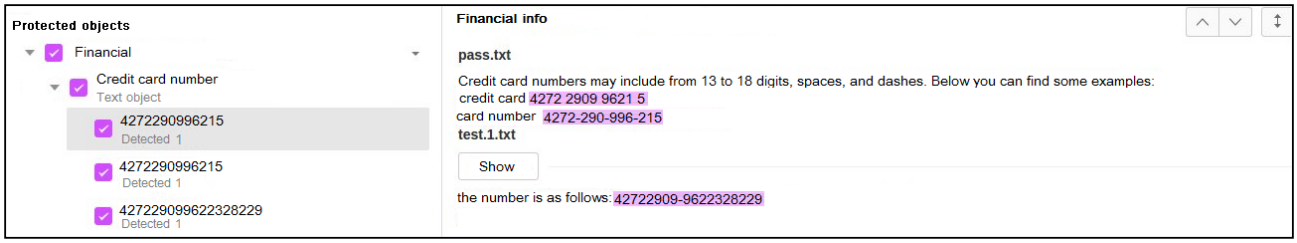
- results of a search by the event text are highlighted in green.

**Important!**

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

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

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




**Note:**

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

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

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

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

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

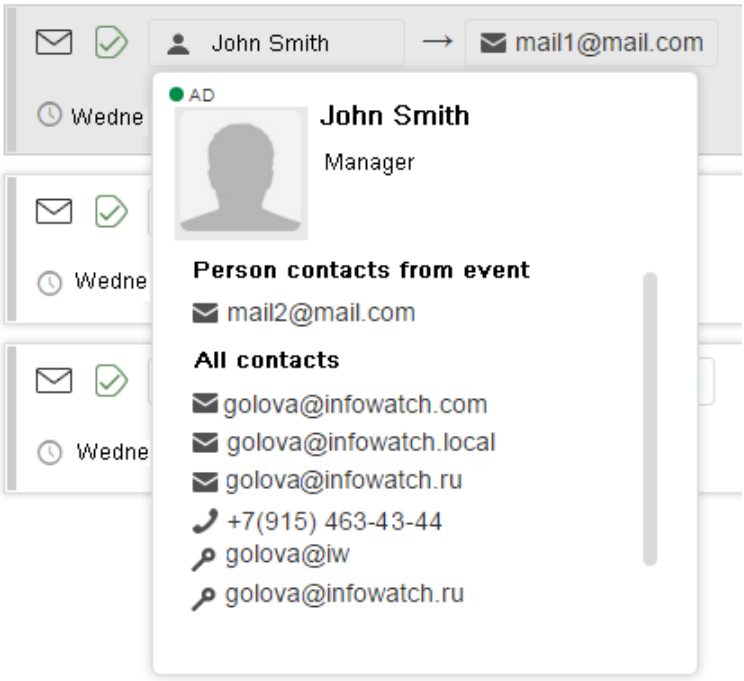
- for `original.docx` attachment - the *Company data* protected object;
- for `original-2.pdf` attachment - the *Science* protected object;
- for the event text - the *Company data* and *Science* protected objects; besides, the search text is found.

**User's target actions:**

- Viewing Detailed Event Form

## 3.2.3 Contact Identification in Event

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




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

**Note:**

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

**Note:**

For the following resources, post identification is not supported:

- odnoklassniki.ru
- gmail.com

**Note:**

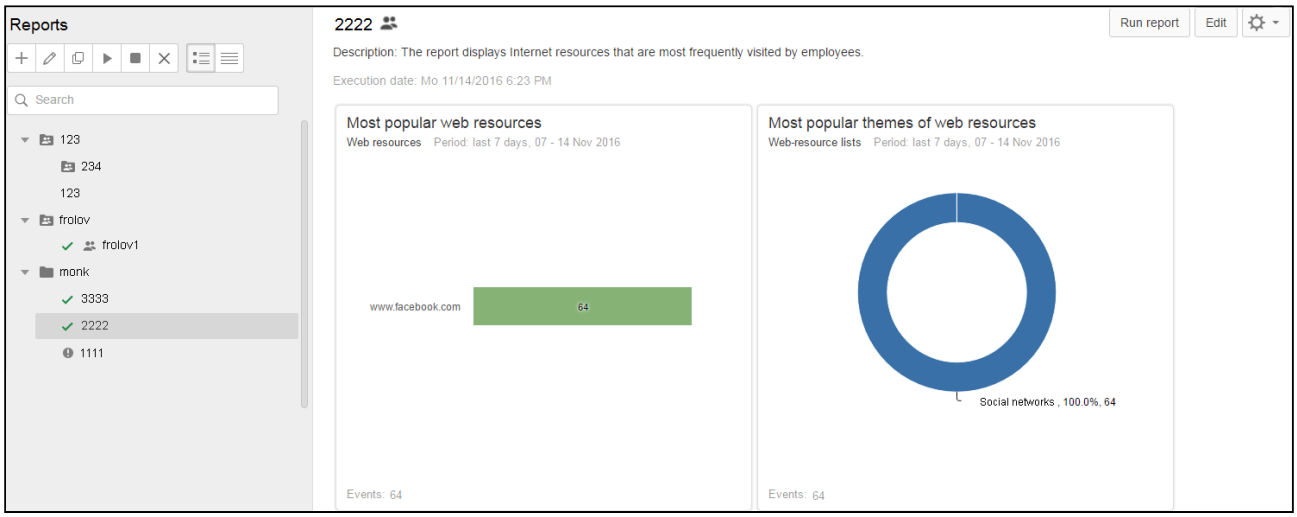
It can happen that personal cards of different users who work on different computers may contain the same accounts in messengers (e.g., Skype) as their contacts. This can happen if those users have logged into different computers under the same domain name or if they have logged into the same computer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

## 3.3 Reports Section

**About the section:**

Contains a list of reports and tools for managing them.

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




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

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

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

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

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

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

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

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

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

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

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

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

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

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

**User's target actions:**

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

### 3.3.1 Report Creation Form

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




You can specify the following settings:

- **Name**;
- **Description** (optional parameter);
- **Use common interception date** - select this option if you want all queries that are used in the report widgets to be generated for the same period. When selecting this option, a drop-down list is displayed where you can specify the desired period. By default, the option is disabled and, for each widget, the interception date is specified independently in the query parameters.
- **Widgets** - click **Add widget** button on the **Widgets** tab to add widgets on which required statistics will be displayed (for details, see "Widgets of Reports").
- **Access** - on the **Access** tab, specify access rights for the report. Possible choices:
    - If you create a report within a folder and the **Apply rights for related reports** option is selected, then access rights for the report will be the same as access rights specified for the folder. Editing access rights to the report is unavailable.

- If you create a report within a folder and the **Apply rights for related reports** option is not selected, or you create a report in the root, then you can specify access rights for the report. By default, the report is available only to the owner. To provide access to the report to other users, select required users in the list and set checkboxes next to their names in a field with the required access level (**View and execute access** or **Full access**).

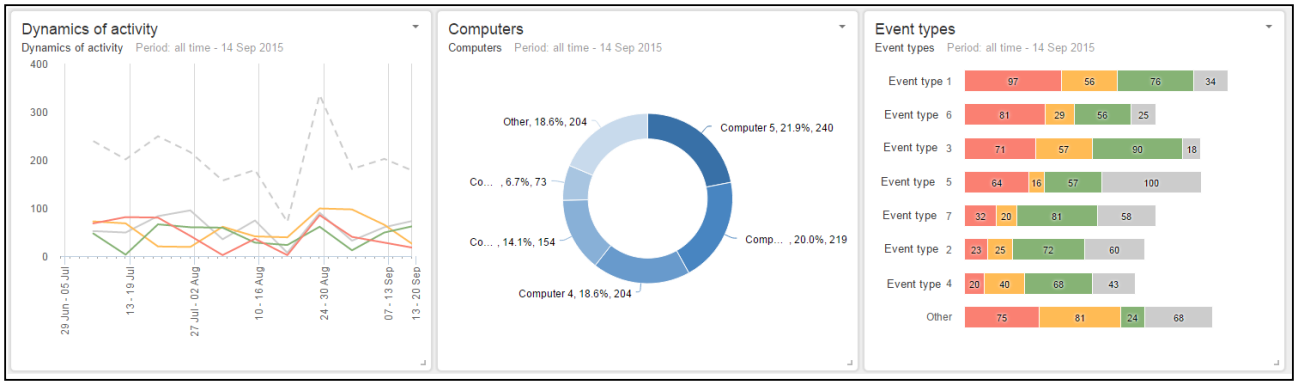
**User's target actions:**

- Creating report

## 3.3.2 Widgets of Reports

Widgets are designed to display statistical information in reports.

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




Widgets can be created for the following data:

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

| | |
|---|---|
| User decisions | Statistics on the decisions which the security officer made for events intercepted by the System |
| Web resource lists | Web resources to which the company employees sent requests most frequently |
| Event types | Distribution of the number of events into types (mail, Skype, external devices, etc.) |

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

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

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

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

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

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

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

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

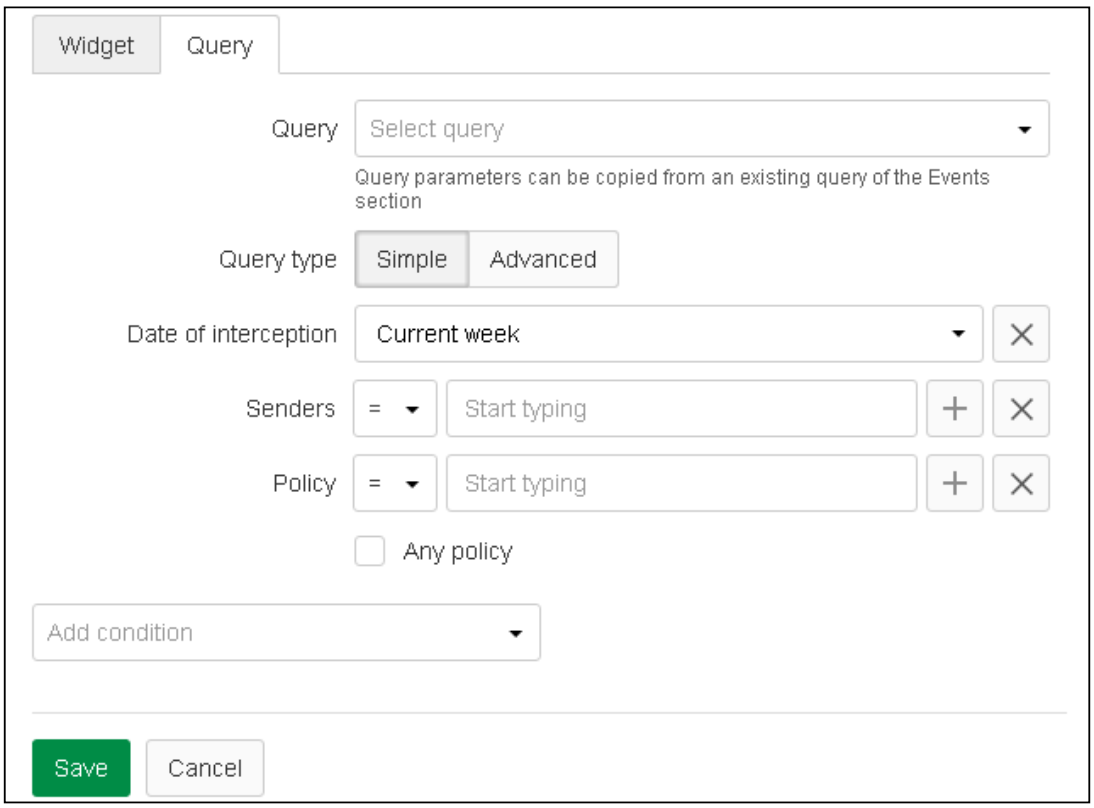
**User’s target actions:**

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

### 3.3.3 Queries

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

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




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

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

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

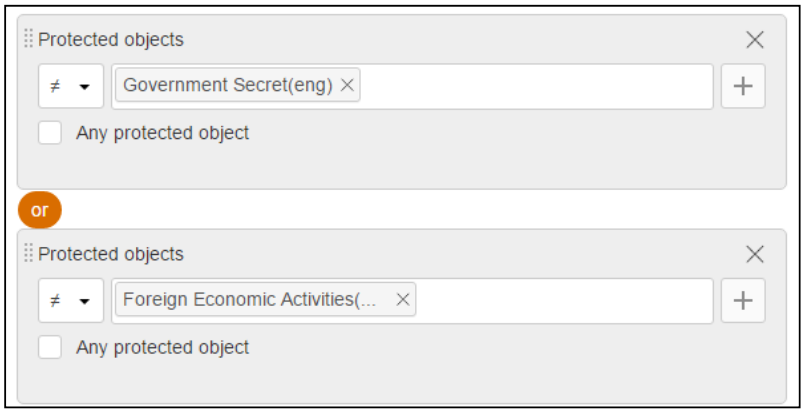
- *Standard mode* - allows you to specify parameter values and, if necessary, apply the negation ≠ to the parameter. All conditions are joined by the conjunction (logical "AND"). For details, see "Condition".
- *Advanced mode* - allows you to perform more flexible configuration of the query conditions using the conjunction (logical "AND") and disjunction (logical "OR"). For details, see "Advanced mode".

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

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

**Example of using the disjunction:**

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




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

**User's target actions:**

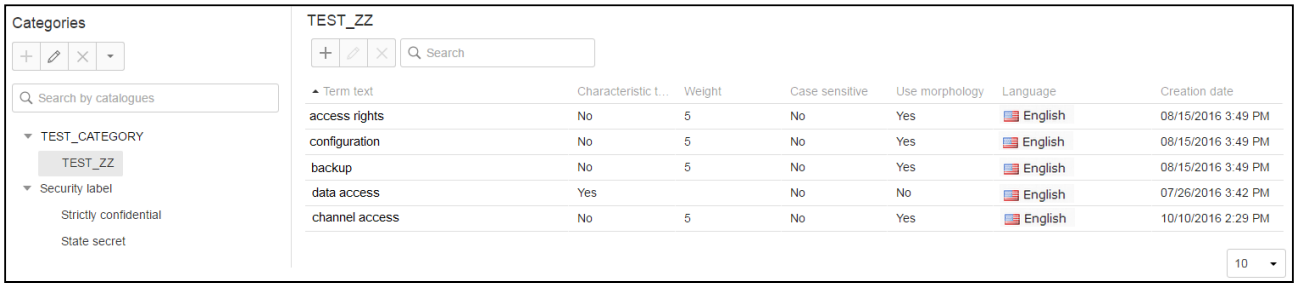
- creating a query (see "Query Creation in Standard Mode" and "Query Creation in Advanced Mode").

## 3.4 Technologies Section

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

**About the section:**
The section contains:

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




**Technologies** section, **Categories and terms** subsection

**User's target actions:**

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

## 3.4.1 Categories and Terms

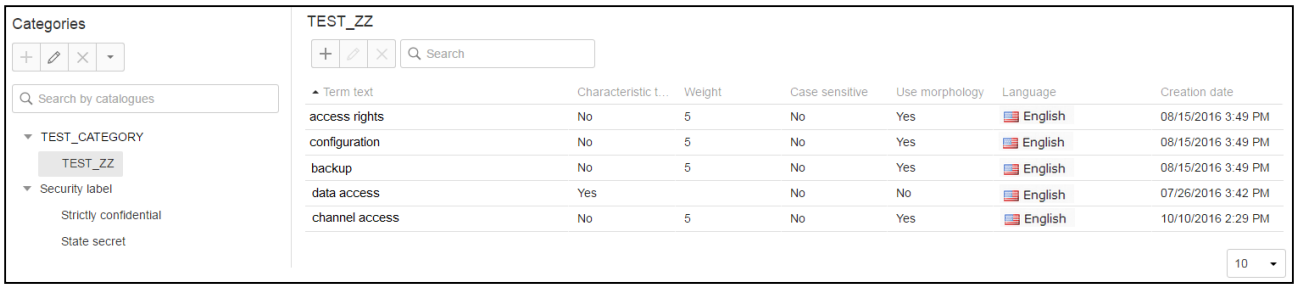
**Reference information:**

***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.

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




**User's target actions:**

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

## Categories

**Reference information:**

The ***category*** is a set of elements corresponding to a specific topic (for example, *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.

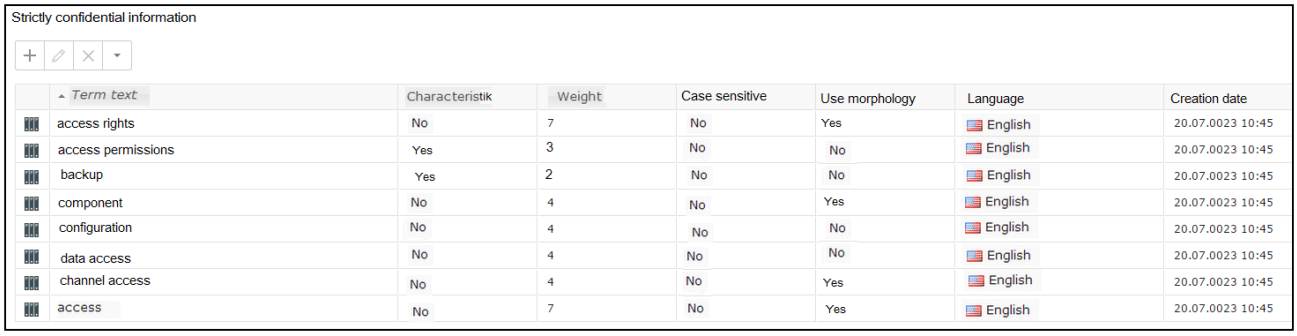
For the category to be detected in intercepted data, it must be included in protected objects.

**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:**

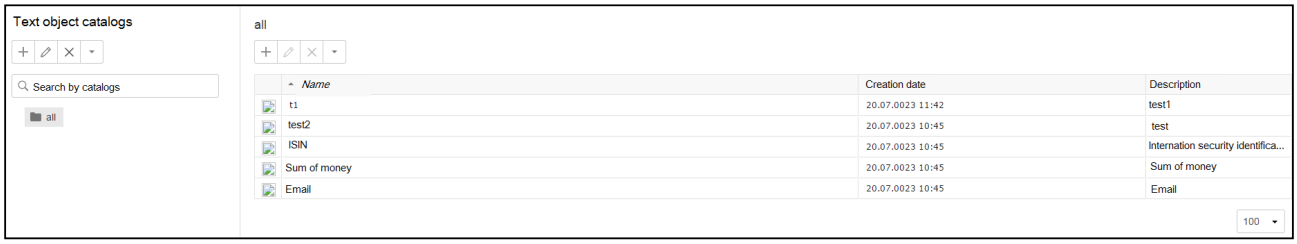
The **Case sensitive** and **Use morphology** parameters are set by default when specifying these parameters for the category. Parameters of the term can be then edited and saved. In this case, when editing case and morphology settings of the category, these changes will not apply to the terms.

**User's target actions:**

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

## 3.4.2 Text Objects

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




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

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

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

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

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

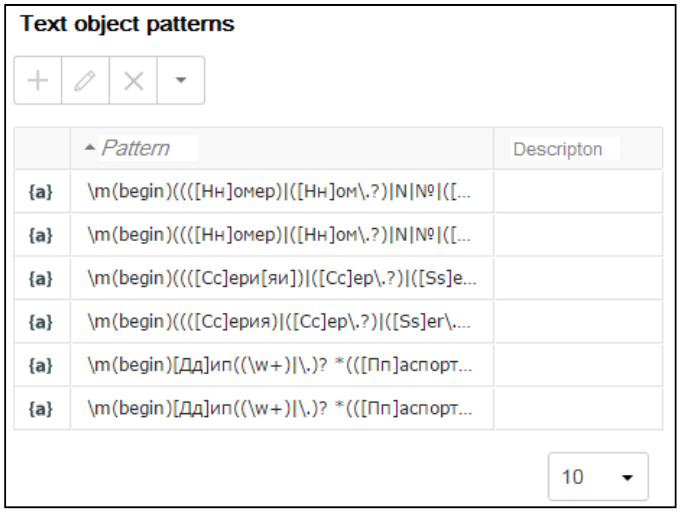
**User's target actions:**

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

## Text Objects Patterns

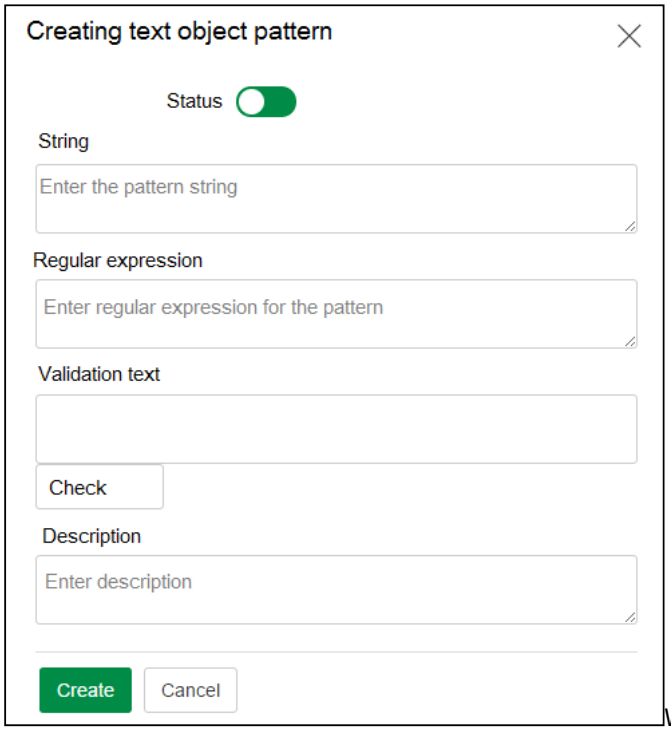
**Reference information:**
The *text object pattern* is a value of the text object set in a form of the exact sequence of characters or with a regular expression.Patterns allow you to specify one or several values for each text object.

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*.<br>The exact value of the text object specified as a sequence of characters.<br>*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*.<br>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*.<br>An example of a text for finding the regular expression. Enter the verification text and click **Check**. |
| Description | If necessary, add a description |

**User's target actions:**

- Creating a text object

## 3.4.3 Sample Documents

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

**Warning!**

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

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

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

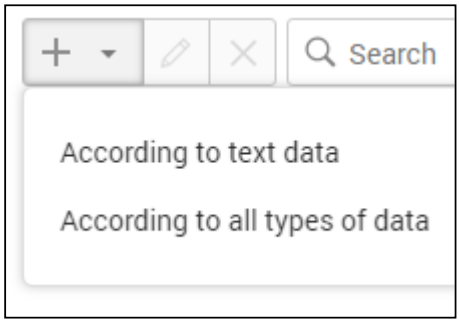
List of sample documents within the selected catalogue and tools for operations with sample documents (create, edit, delete and cross-cutting search within catalogues) are located on the right side of the working area. A cross-cutting search is performed in accordance with the name of sample document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




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

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

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




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

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

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

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

**User's target actions:**

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

### 3.4.4 Blanks

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

**Warning!**

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

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

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

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

**Warning!**

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

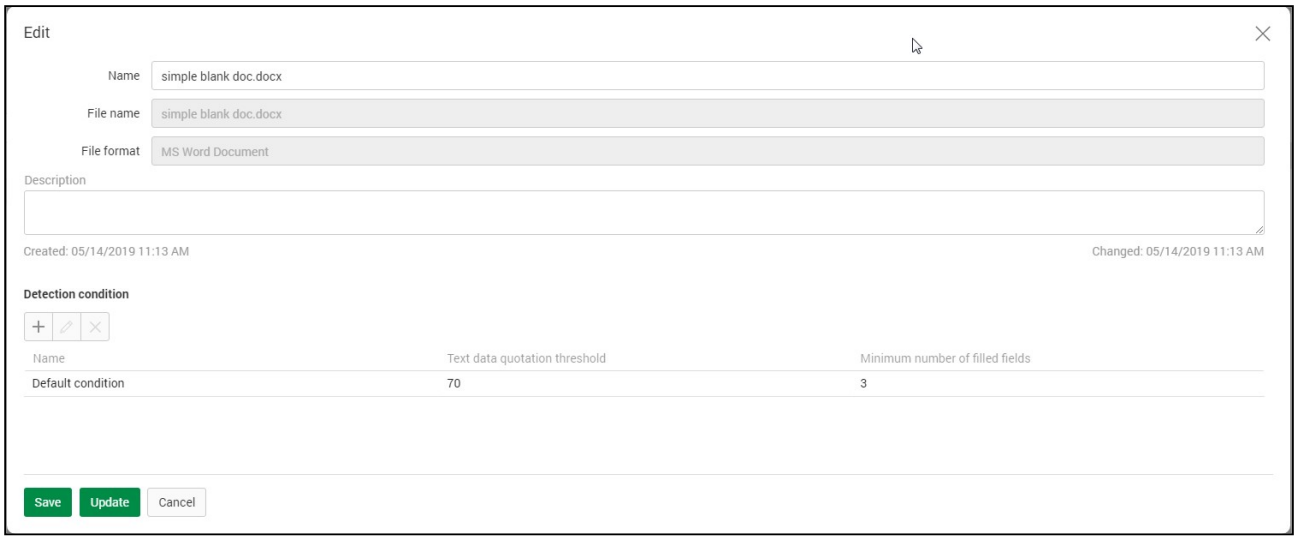
- the object text contains, at least, one field from blank;
- if the number of fields detected in the object text is more than one, then the fields should be in the same order as in the digital print uploaded to the System;
- if detection of filled blanks is set up, then, at least, one character should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

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




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

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



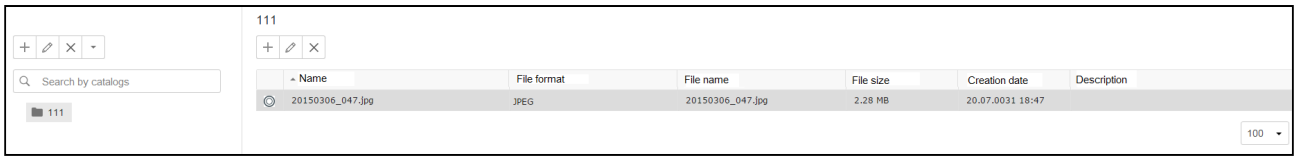

**User's target actions:**

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

## 3.4.5 Stamps

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

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




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

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

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

**User's target actions:**

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

## 3.4.6 Database Unloadings

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

**Warning!**

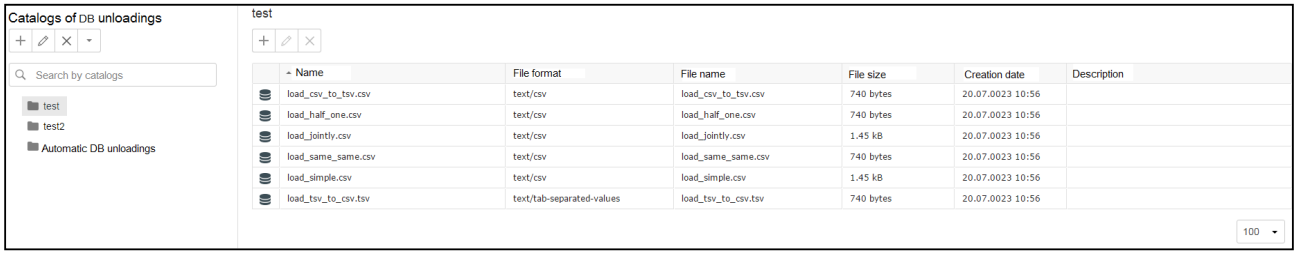
For correct operation in the System, the database unloading should have the following characteristics:

- file size - from 128 bytes to 2 Gb;
- number of columns is no more than 32;
- number of words in one cell is no more than 256;

- number of rows is no more than 1 million (for 8 GB RAM server) or no more than 3.5 million (for 16 GB RAM server);
- unloading size maximum of 1 Gb in case Postgre SQL is used.

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

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



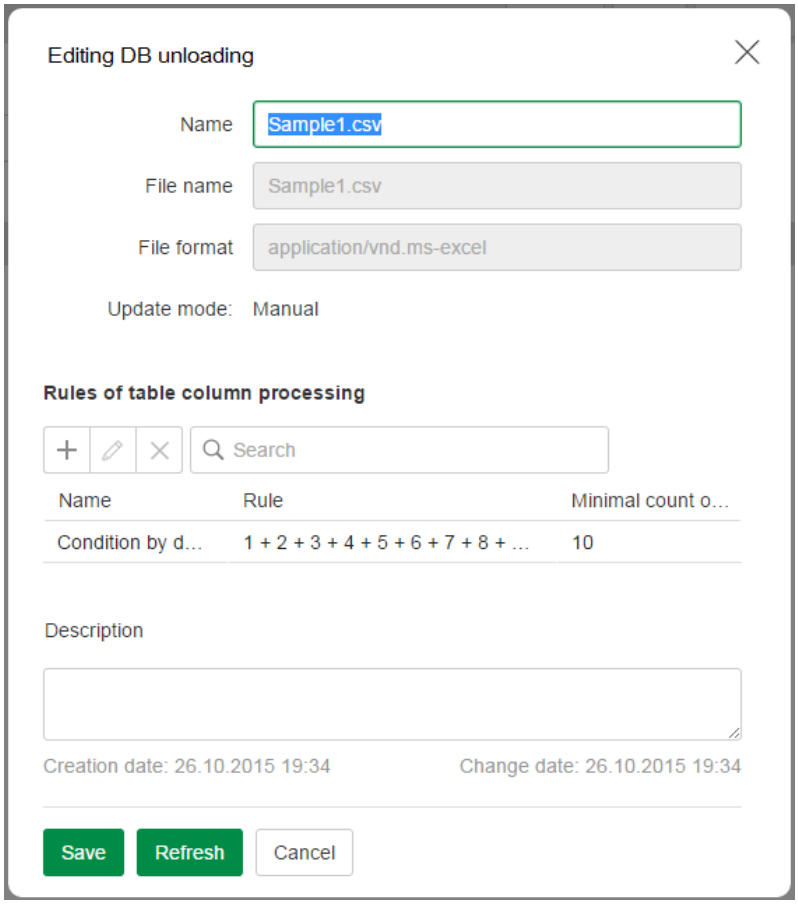

The preinstalled catalogue **Automatic DB unloadings** contains unloadings received from external systems (for further details, see "Automatically Updated Database Unloadings").

**Note:**

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

In the edit mode, the detection conditions for the unloading are displayed. Detection conditions define logical relationships between table columns 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 catalogues (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 "Automatically Updated Database Unloadings")
- Add DB unloadings to protected objects (see "Creating a Protected Object")

## Automatically Updated Database Unloadings

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

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

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

**Note:**

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

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`<br>For example:<br>If the number of columns is`3`, the condition will be as follows:<br>`1+2+3`, and the minimum number of columns is `10`. |

You can also add unloadings to the **Automatic DB unloadings** catalogue 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 catalogue can be edited or deleted. These operations are performed using buttons on the toolbar in the right part of the workspace.

**Warning!**

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

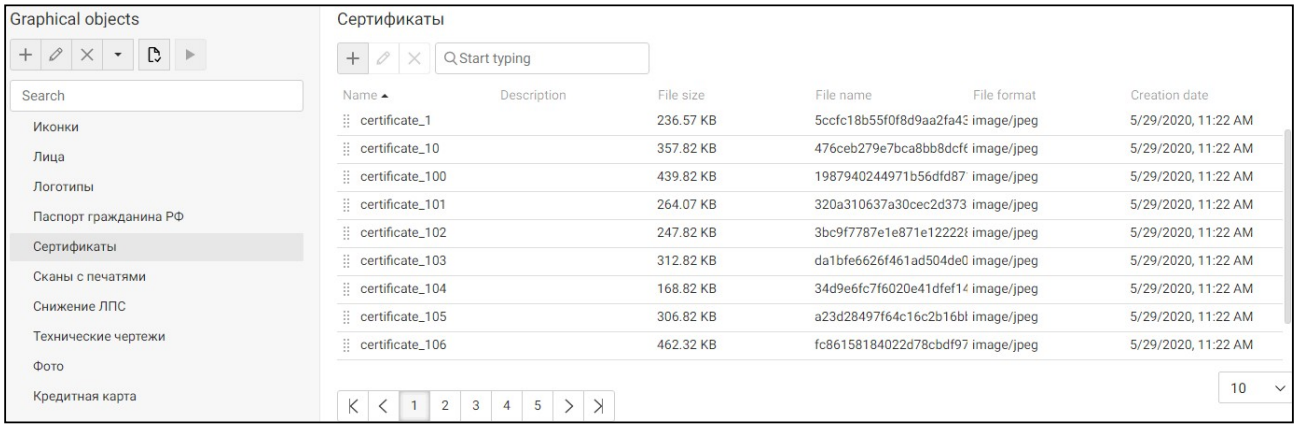
For automatic unloading to be detected in intercepted data, it must be included in a protected object.

## 3.4.7 Graphical Objects

**Reference information:**

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

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




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

- Passport of a citizen of the Russian Federation
- Technical drawings
- Geographic maps
- Certificates
- Faces
- Photos
- Scans with stamps
- Icons
- Logos
- Decreasing false-positives
  and uneditable graphical objects:

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

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

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

**User's target actions:**

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

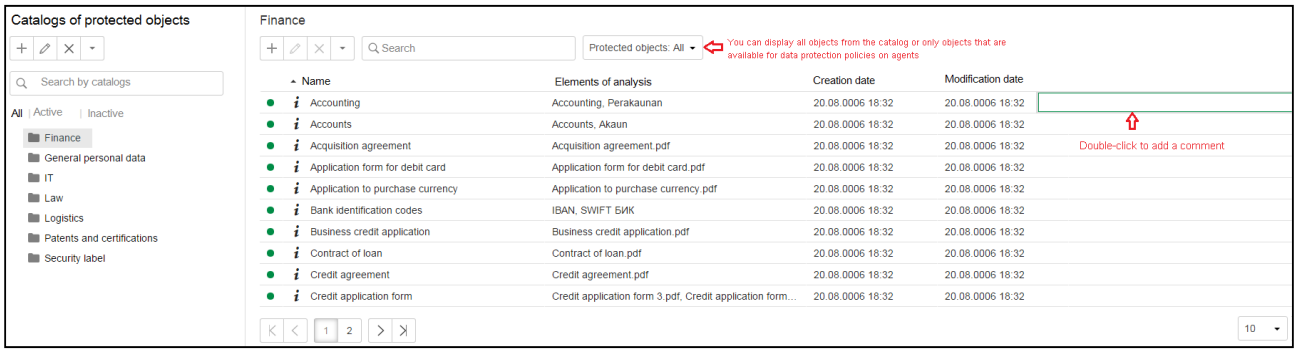
## 3.5 Protected Objects Section

**Reference information:**

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

**About the section:**

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




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

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

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

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

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

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

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

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

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

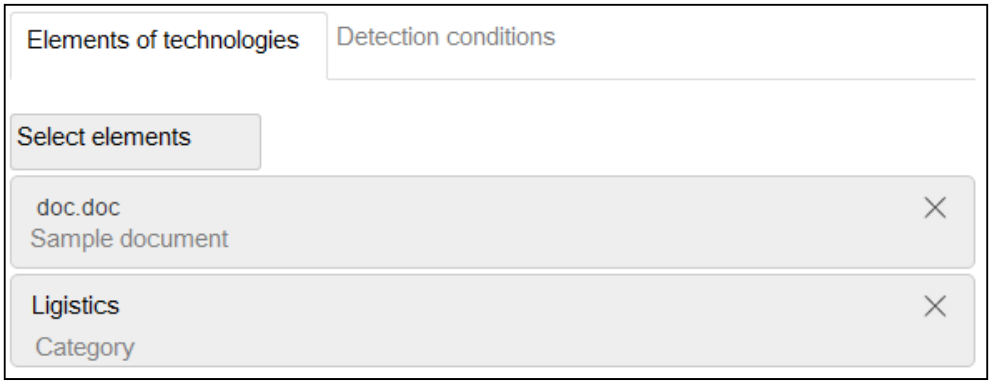
In the edit mode of the protected object, you can change the list of elements of technologies and specify detection conditions.

**User's target actions:**

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

## 3.5.1 Elements of Technologies

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




**Elements of technologies** tab for a protected object

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

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

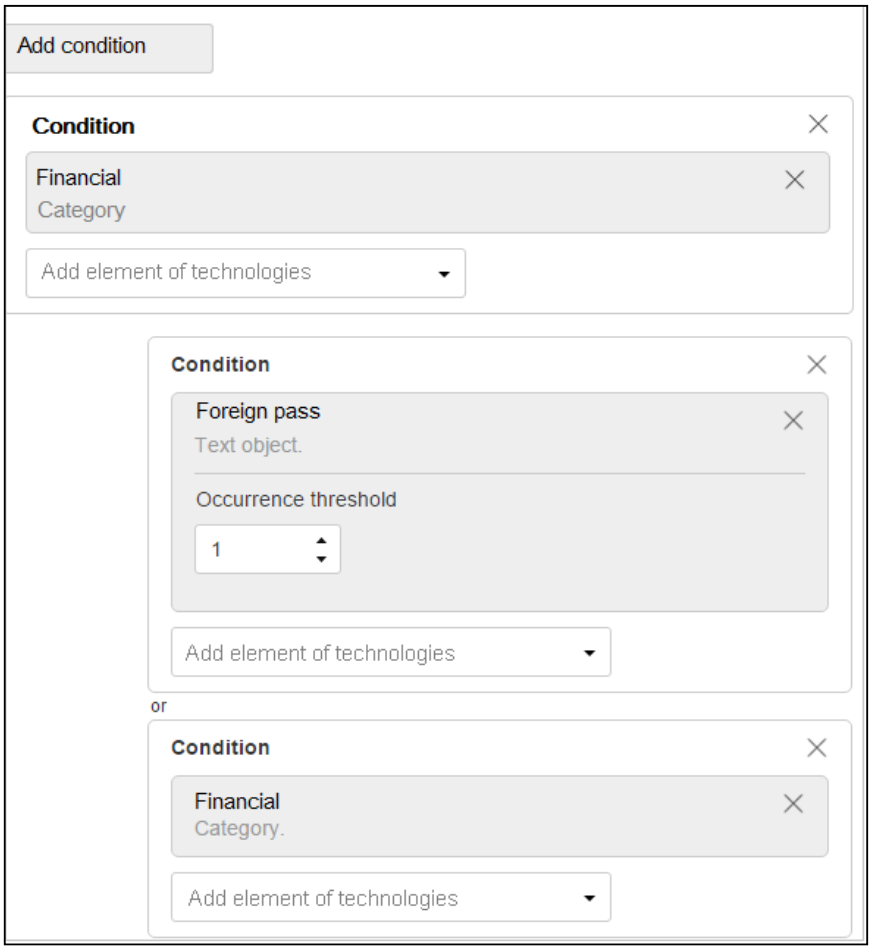
You can specify detection conditions for added elements of technologies on the **Detection conditions** tab.

**User's target actions:**

- Adding elements of technologies

## 3.5.2 Detection Conditions

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



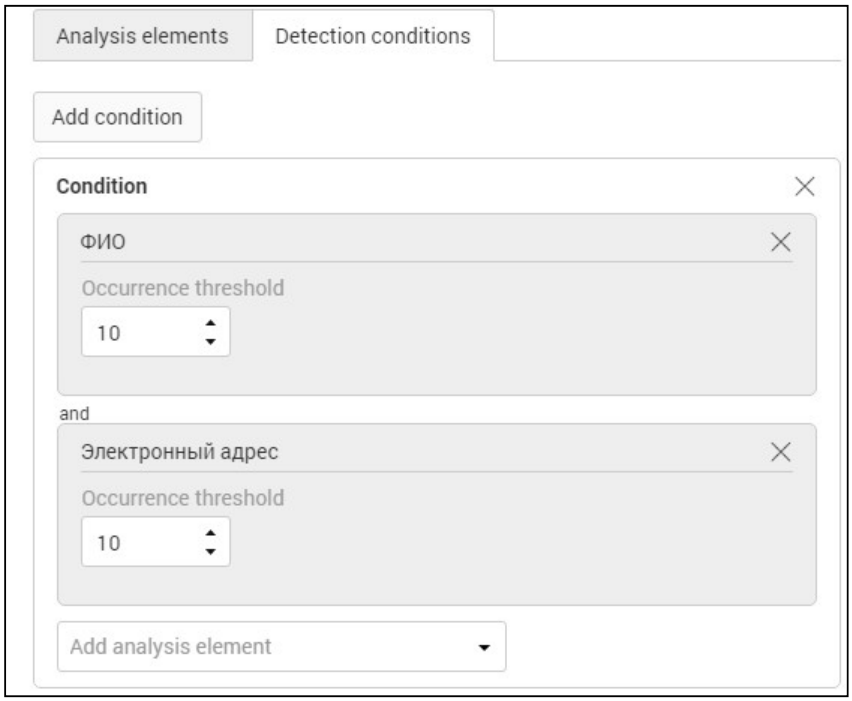

You can specify detection conditions when creating a protected object after the desired elements are selected in the window of adding elements of technologies or when switching to the edit mode of a previously created protected object.

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

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

Detection conditions for the elements of technologies are as follows:

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

| | |
|---|---|
| Text object | Checks whether the interception object contains a specified text object. Additional detection condition is a occurrence threshold. It determines the least number of times the text object must be present in the interception object. The default value is 1. The maximum value is 20000.<br><br>Depending on the pattern type, the number of occurrences of the text object is calculated as follows:<br><br>• if the text object pattern is specified as a regular expression, then one pattern value is counted as one occurrence even if it is detected several times within a document<br>• if the text object pattern is specified as a string, all its occurrences are counted.<br><br>Catalogue also has a quotation threshold defined. Text objects which are a part of this parameter will be detected in accordance with its detection condition. |
| Blank | Checks whether the interception object contains at least one of the specified blanks. Additional detection condition - blank detection condition. It is used when editing the blank and includes the fiollowing:<br><br>• text data quotation threshold - per cent of matching between intercepted blank and sample one. The default condition value is 70%;<br>• minimum number of filled fields. The default condition value is 3.<br><br>To be detected the intercepted blank should meet both conditions above.<br><br>Always specify one detection condition.<br><br>In case the technology element is a catalogue of blanks, one of the following conditions should be selected:<br><br>• **Default condition** - the blanks inside the catalogue will have its default conditions applied;<br>• **All conditions from catalogue as per OR** - for each blank within the catalogue any detection condition from it will be applied.<br><br> |
| 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<br>At least one detection condition should be selected always.<br>In case you've selected DB unloadings catalogue, you should select one as follows:<br>**Default condition** - for blanks within the catalogue its default conditions will be applied.<br>**All conditions from catalogue as per OR** - for each unloading within the catalogue any its condition will be applied. |

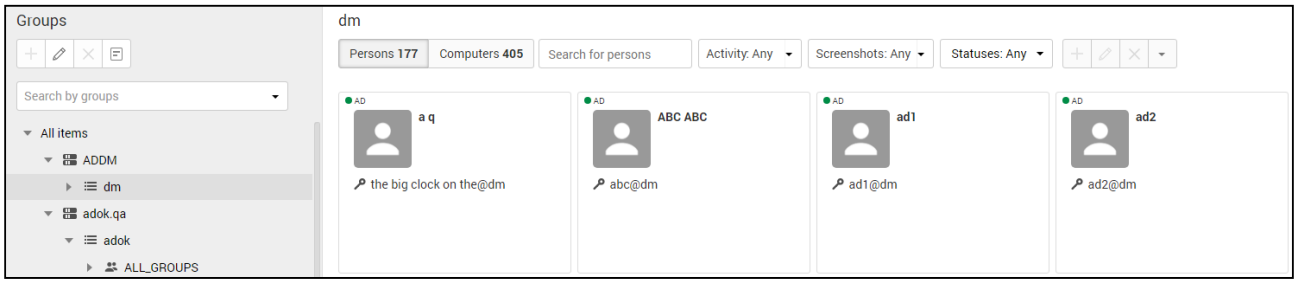
See also: Elements of technologies

**User's target actions:**

- Adding detection conditions

## 3.6 Persons Section

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




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

You can add groups of persons and computers from Active Directory, Domino Directory or Astra Linux Directory or create them in Traffic Monitor (see "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 use thy fields **Search by persons** and **Search by computers**. To switch to another field you should switch the tabs **Persons** or **Computers**. A cross-cutting search is performed in accordance with the name and surname of selected person, computer name and contatcs details and it is

performed within selected catalogue or enclosed ones. To perform the search through all the section's categories, select the root catalogue. Mask search is supported (e.g., `*name`).

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

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:**

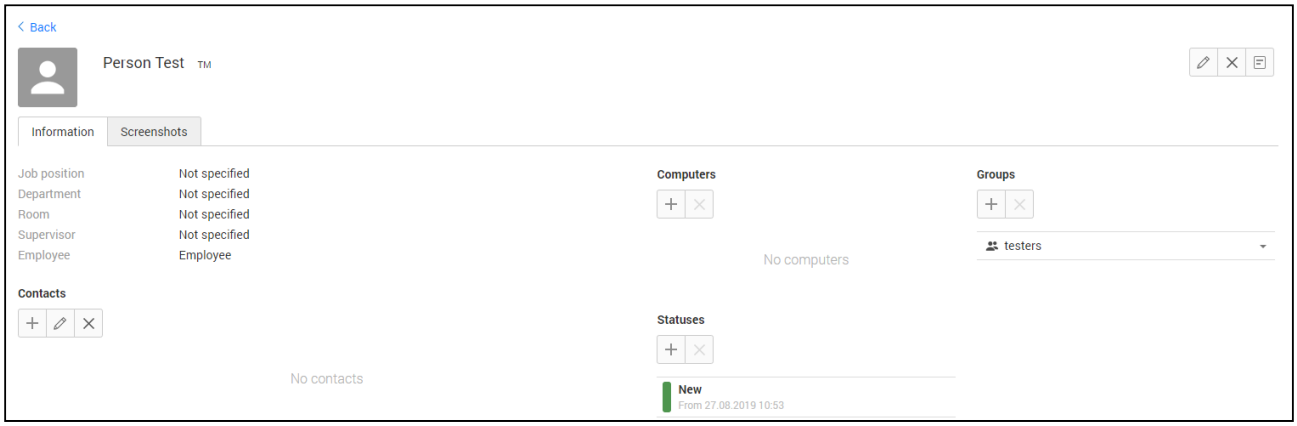
- Creating a group of persons and computers (see "Creating Group of Persons and Computers")
- Creating a list of persons and computers (see "Creating List of Persons and Computers")
- Viewing widgets with information on persons and computers (see "Viewing Summary on Person or Computer")
- Creating a 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 colour indicator appears in the upper left corner of the profile photo:
>
>  - for active employees, including employees whose accounts in AD/ALD have expired;
>
>  - 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
- Supervisor
- Employee
- Contacts (you can specify personal or working contacts of the person including email, phone number, Skype login, ICQ or web address on the Internet, social networks and messengers account)
- Computers (computers linked with the person account)
- Statuses (statuses assigned to the person)
- Groups (groups which include the person)

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

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

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

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

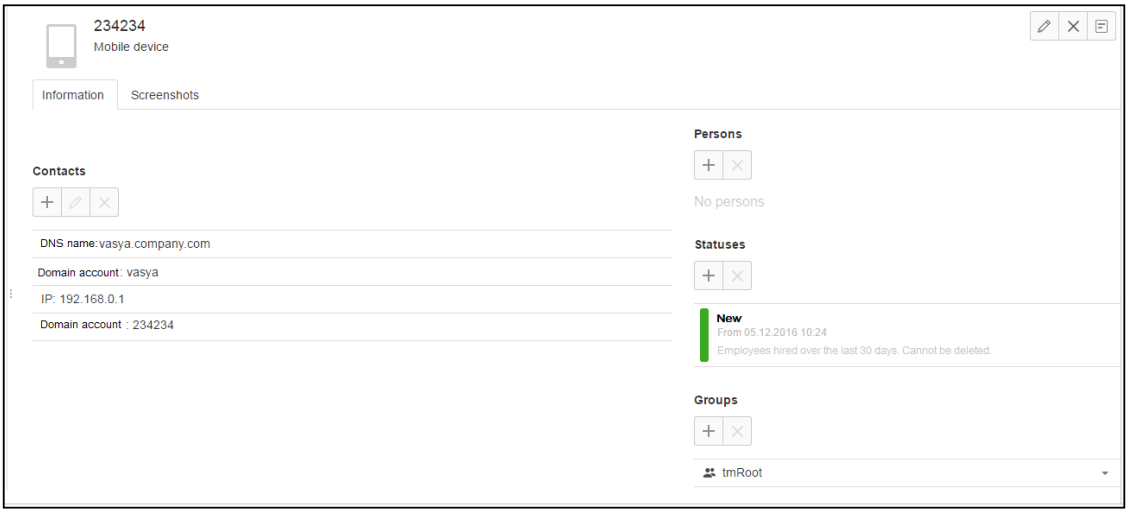
**User's target actions:**

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

## 3.6.2 Computers

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

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




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

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

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

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

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

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

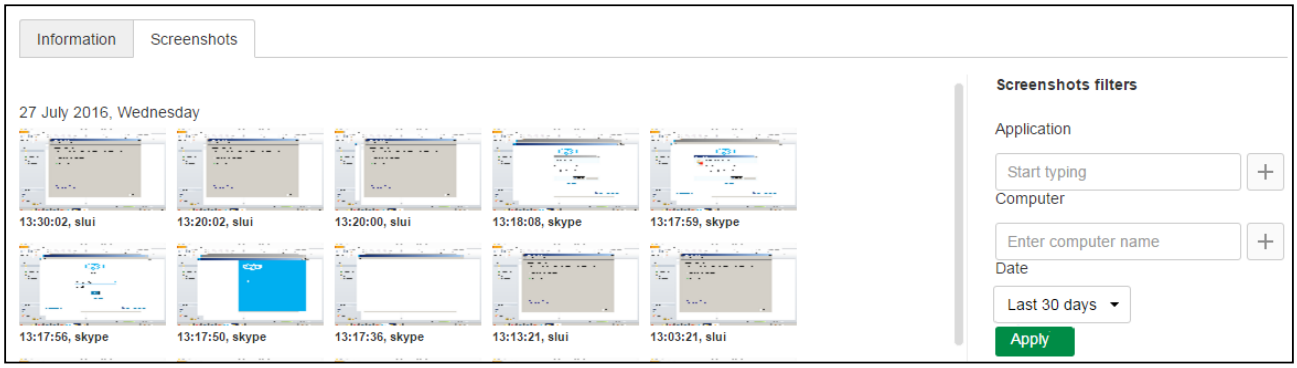
**User's target actions:**

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

## 3.6.3 Screenshots

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

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




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

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

Clicking a screenshot opens its enlarged image and attributes:

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

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

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

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

**User's target actions:**

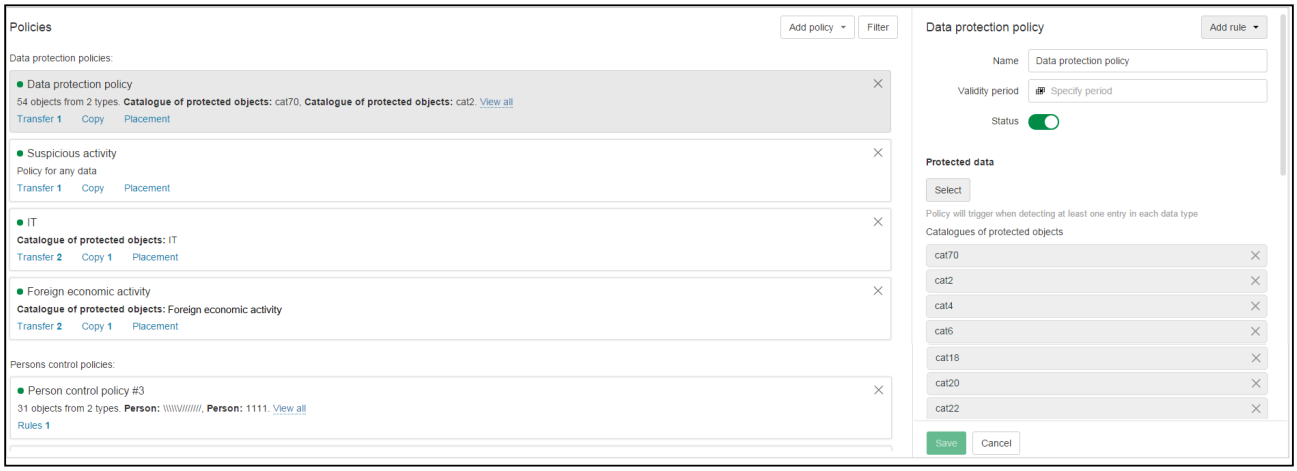
- Viewing Screenshots

## 3.7 Policies Section

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

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

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




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

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

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

In the policy viewing form, you can:

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

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

**User's target actions:**

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

## 3.7.1 Rules and their Viewing Form

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




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

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

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

- Transfer rule - regulates sending and receiving protected data.
- Copy rule - regulates copying and printing protected data;
- Placement rule - regulates storing protected data;
- Clipboard rule - regulates using the clipboard;
- File Operations Rule - regulates if an application can read a file or write to it.

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

- Transfer rule
- Copy rule

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

Also, for *Sender* and *Recipient*, you can specify the following 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:<br> - ICQ account. Integer number from 10000 to 999999999999;<br> - Skype account. String from 6 to 32 characters long, must begin with a letter; may contain only letters, digits, and the characters ".", ",", "-", "_";<br> - mobile phone number. String no less than three characters, can contain only numbers, space and symbols"-","_", "( )","+",".");<br> - landline phone number.String of 3 or more characters,can contain only digits, space, and the characters:"-","_", "( )","+",".");<br> - E-mail address. Address (in RFC format);<br> - 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) ;<br> - identifier on a web resource. A string of 3 or more characters when entering data in the input field, or string of 1 or more characters when entering data in the Senders window (opens when clicking the  button) . |
| Groups | Specify groups whose members can be traffic senders/recipients. |
| Persons | Specify persons who can be traffic senders/recipients. |
| Domains | Specify domains whose members can be traffic senders/recipients. |
| Perimeters | Specify perimeters whose elements can be traffic senders/recipients. |

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

**User's target actions:**

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

## Rule of Transfer

For the transfer rule, the following parameters are specified:

- **Direction of route**. Possible values:
  - **In single direction** - the rule is triggered only when traffic is passed from senders to recipients;

    - **In both directions** - the rule is triggered when traffic is passed both from senders to recipients and from recipients to senders.

- **Event type** - the type of traffic passing which triggers the rule. Possible values:
    - **Internet activity**
      - *Web message*
    - **Messenger** (for data protection policies only)
      - *ICQ*
      - *Mail.Ru Agent*
      - *MS Lync*
      - *Skype*
      - *Telegram*
      - *XMPP*
      - *Facebook*
      - *Vkontakte*
      - *Kribrum*
    - **Mail**
      - *Mail on Client*
      - *Mail in Browser*

- **Computers** - computers from which data has been sent.
- **Senders** - if persons or computers from this list send traffic (or traffic leaves specified domains and perimeters), it triggers the rule;
- **Recipients** - if persons, computers, domains or perimeters from this list receive traffic, it triggers the rule;

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

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

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

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

**User's target actions:**

- Creating Rule
- Configuring Notifications in Rules

### Rule of Copying

For the copy rule, the following parameters are specified:

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

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

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

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

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

> **Important!**
>
> Selected conditions are joined by the "logical AND" operation. With a condition, values are joined as follows:

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

**Important!**

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

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

**User's target actions:**

- Creating Rules
- Configuring Notifications in Rules

### Rule of Placement

For the placement rule, the following parameters are specified:

- **Event type** - the type of traffic placement of which triggers the rule. Possible values:
  - **Crawler**
- **Storage** - storing secured data in these storages triggers 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 field:
    - 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*

  Once you have specified all required storages, click **Save**.
- **File owners** - the rule is triggered when specified persons, groups or perimeters are detected among file owners.
- **Who has access to file** - the rule is triggered if specified persons, groups, and perimeters have access to the file.

**Important!**

Selected conditions are joined by logical "AND". Within a condition, values are joined as follows:

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

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

**User's target actions:**

- Creating Rules
- Configuring Notifications in Rules

### Clipboard Rule

For the clipboard rule, the following parameters are specified:

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

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

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

**User's target actions:**

- Creating Rules
- Configuring Notifications in Rules

### Person Control Rule

For the person control rule, the following parameters are specified

- **Violation level** - The System will intercept events with the specified violation level;

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

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

**User's target actions:**

- Creating Rules
- Configuring Notifications in Rules

### File Operations Rule

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

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

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

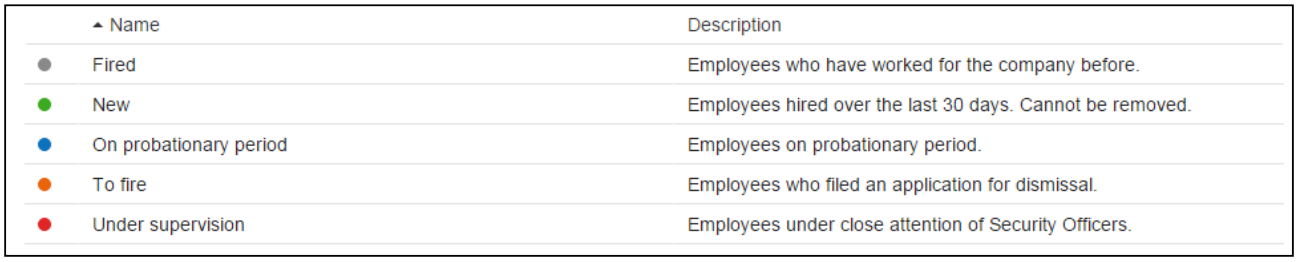
In the **Actions when the rule is triggered** area, specify the required actions (for details, see "Determining System Response to Policy Violations").

> **Important!**
>
> To enable operation of this rule, you should configure the **File Operations Monitor** rule in the Device Monitor Management Console (see "File Operations Monitor Rule (DM)").

## 3.8 Lists Section

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

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



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

**Lists** section, the list of statuses

The section contains the following catalogues:

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

**User's target actions:**

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

## 3.8.1 Tags

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

There are the following preset tags in the System:

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

**User's target actions:**

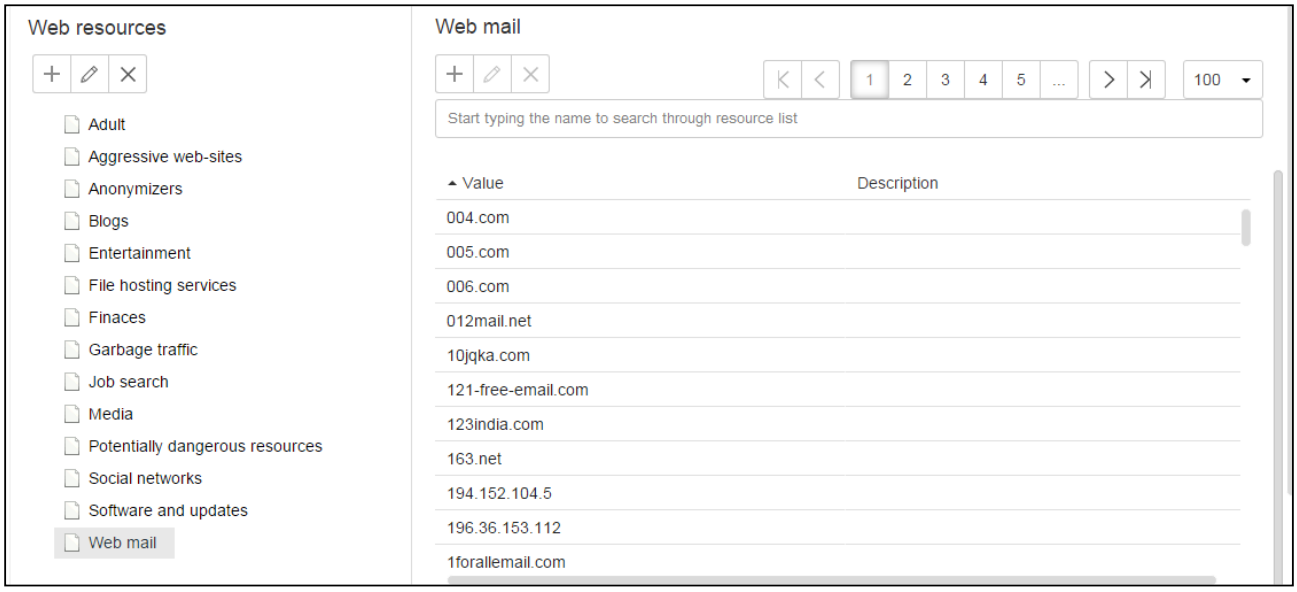
- Creating a list of tags (see "Managing Tags")

## 3.8.2 Web Resources

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

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

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




The System includes the following preset lists of web resources:

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

**User's target actions:**

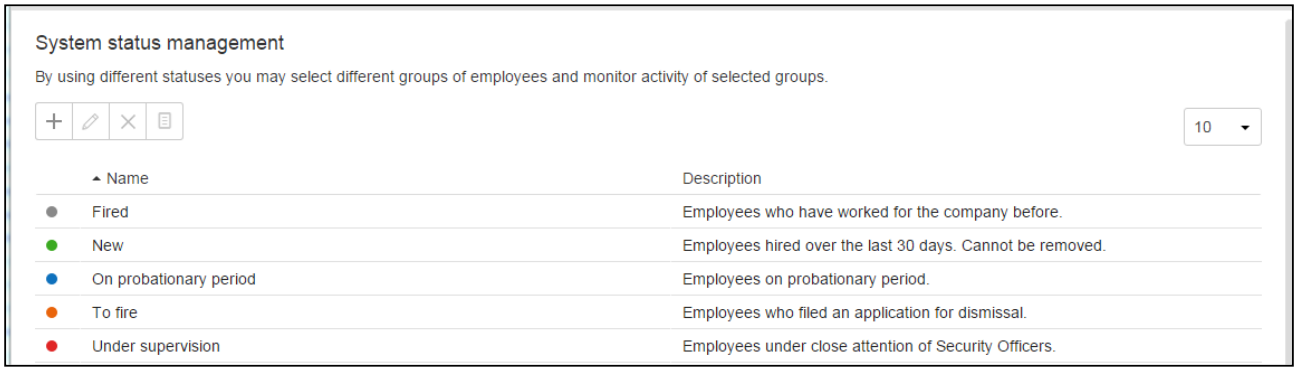
- Creating a list of resources (see "Managing Web Resources")

## 3.8.3 Statuses

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

- automatically assigned to a person according to the status of a user or a computer imported from Active Directory, 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 colour mark is set.




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

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

**User's target actions:**

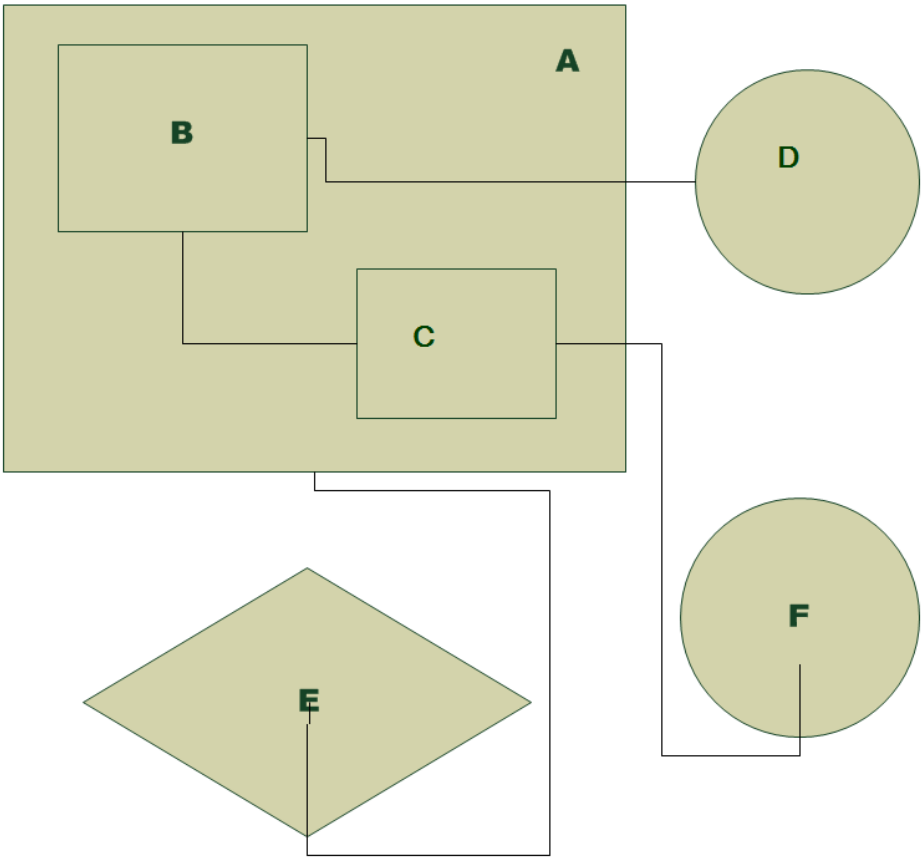
- Creating a list of statuses (see "Managing statuses")
- Manual assigning status to a person or workstation to monitor its activities or to visually distinguish them (see "Adding a Status to Person or Workstation")
- Automatic assigning status to a sender when the rule is triggered (see "Rules and their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

## 3.8.4 Perimeters

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

**For example:**

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




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

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

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

The System includes the following preset perimeters:

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

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

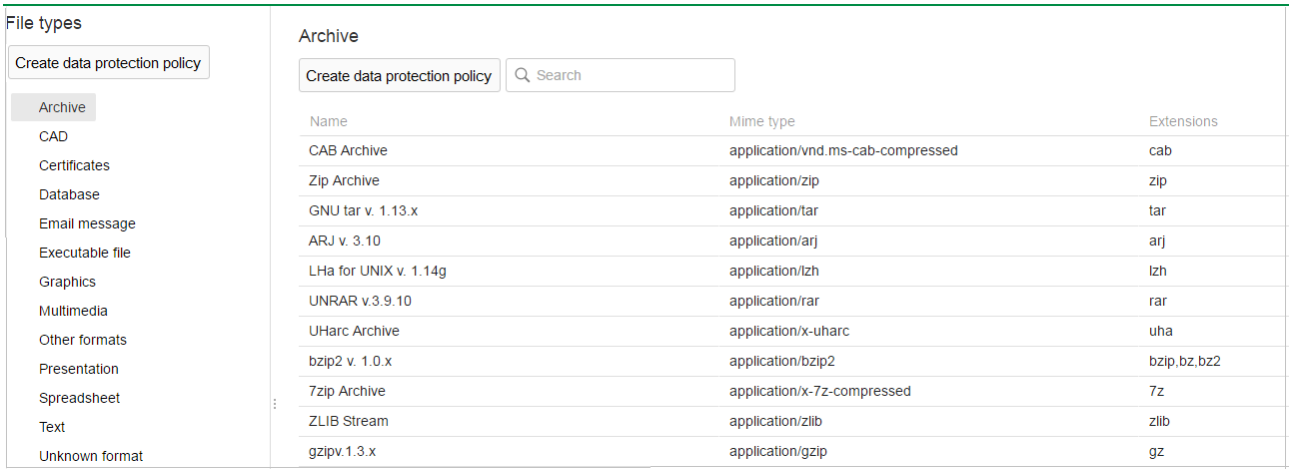
**User's target actions:**

- Building perimeters (see "Managing perimeters")

## 3.8.5 File Types

**Reference information:**

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




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

The tab contains the following elements:

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

**Warning!**

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

**User's target actions:**

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

## 3.9 Administration Section

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

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

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

## 3.10 Crawler Section

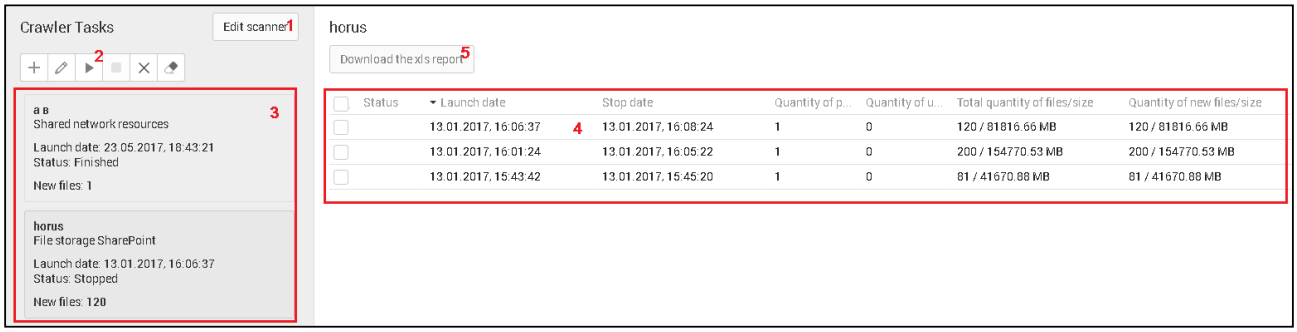
**Reference information:**
The Crawler subsystem of InfoWatch Traffic Monitor allows you to check files in the corporate network for violations of the corporate security policies. Files are checked by a *scanner* - a special module which scans data storage.

Crawler features

- Scanning network folders open for remote access via SMB protocol.
- Scanning local drives of workstations under Windows OS.
- Scanning SharePoint file storage. Checks documents stored in Microsoft SharePoint 2007/2010/2013 database. Only actual file versions are checked: the change log is not investigated.
- Fine-tuning scan job where you can specify:
    - folders and network nodes to be scanned;
    - masks of processed files;
    - size limit for processed files;
    - scanning schedule (you can also start jobs manually).
- Sending files to Traffic Monitor server for analysis. Only new or modified files are sent to the server; already processed file are not re-sent.
- Saving files according to the policy settings (by default, only files violating the security policy are saved)
- Scanning results are available in the Management Console: you can view them using queries and reports (including preset ones).

Crawler does not delete, move, rename, encrypt, or perform any other action with files - even if a file is considered a potential violation. Crawler only informs the security officer about the incident.  In the Management Console, the security officer can view files which are potential violations, with detailed information on their location and users who can access these files.

**About the section:**
The section contains a list of scan jobs and tools for managing them.




The left part of the workspace includes the following elements:

- the **Edit scanner** button (№1 in the screenshot) which allows you to configure the scanner (see "Configuring Scanner");
- a toolbar for managing scan jobs (№2 in the screenshot);
- the list of scan jobs (№3 in the screenshot).

To create a new job, use the  button on the toolbar (see "Creating Job").

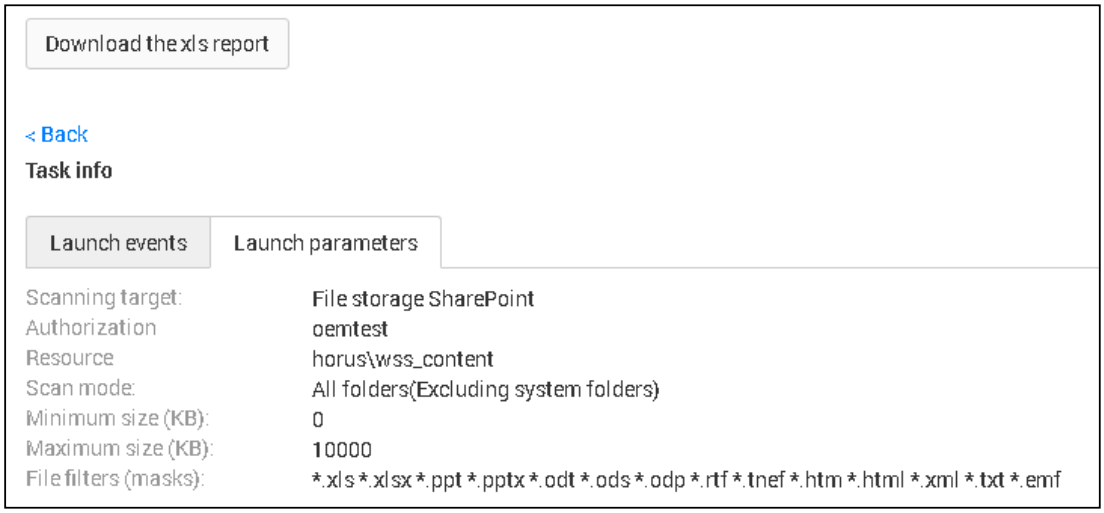
When you select a job in the list, then the  **Edit job**,  **Launch job**,  **Delete job**, and  **Clear job hashes** buttons become available and the job launch history is displayed in the right part of the workspace (№4 in the screenshot).

If the job is running, you can stop it by clicking  on the toolbar.

The job launch history (№4 in the screenshot) includes the following brief information on job launches:

- Status;
- Дата запуска и остановки задачи;
- The number of processed and unprocessed computers;
- The number and size of processed files;
- The number and size of new files processed by the job.

To view detailed information on the selected launch, double-click the selected row in the launch history. Information on the launch is displayed in the right part of the workspace in the following tabs: **Launch events** and **Launch parameters**.




To save a report in MS Excel format for a selected job version, click **Download the xls report**.

To return to the job launch history, click **<Back**.

You can also save reports in Excel format for several job versions at the same time. For this, select check-boxes next to required versions in the launch history and click **Download the xls report** (№5 in the screenshot).

> **Note:**
>
> If necessary, you can clear the history of task launches (see the KB article "Crawler. Scanning service is suspended and drop out from interface").

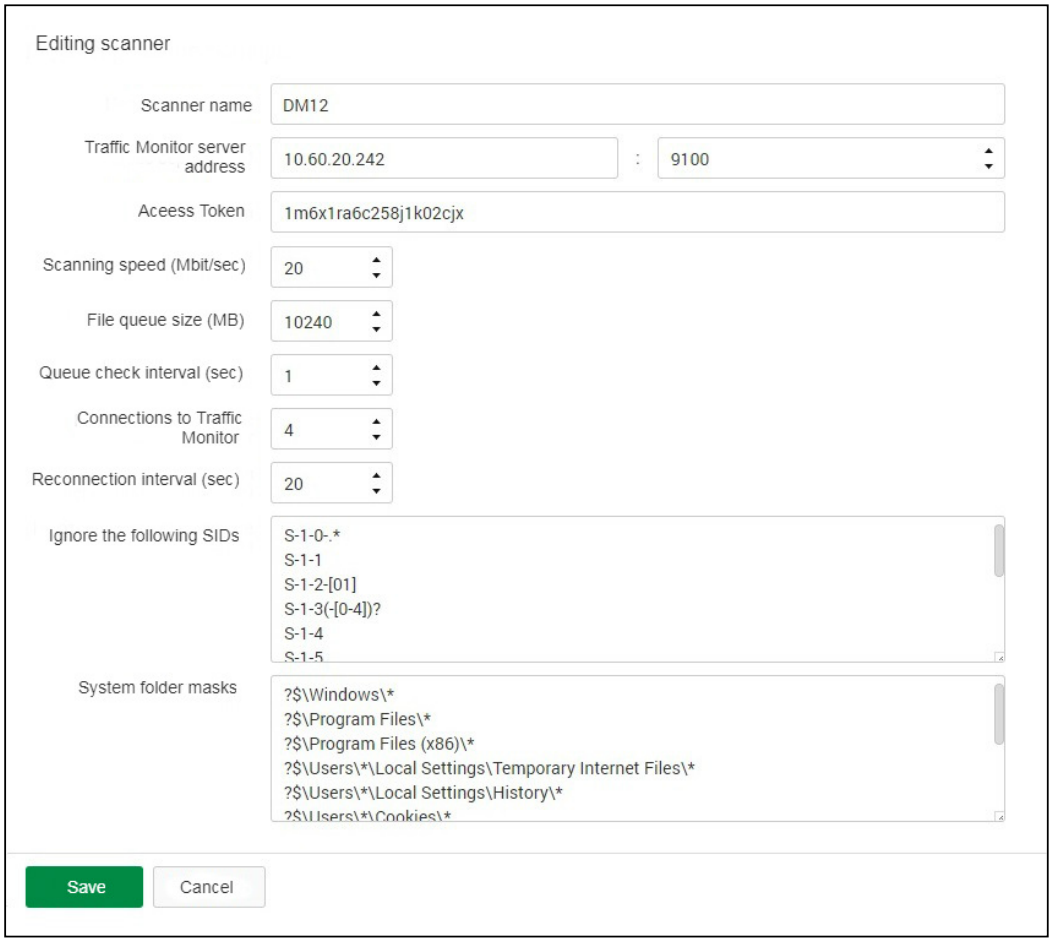
**User's target actions:**

- Configuring Scanner
- Creating a Job
- Cleaning the Hash Base

## 3.10.1 Scanner

**Reference information:**
The *scanner* is a module of Crawler subsystem which scans data storages (Microsoft SharePoint 2007/2010/2013 storage, workstation local drives, and shared network resources) defined by the user in scan jobs.

> **Note:**
>
> If you want to scan a Sharepoint storage, make sure that the scanner and the Sharepoint storage are the same domain.




Scanner attributes:

| Parameter | Description |
|---|---|
| Scanner name | Name of the scanner |
| Traffic Monitor server address | IP-address of the Traffic Monitor server, where `iw_xapi` is operating and service hosting port |
| Access Token | Access token to Traffic Monitor server for Crawler plugin |
| Scanning speed (Mbits/sec) | The maximum speed of uploading files from scanned resources to temporary storage (Mbits/sec)<br>Allows reducing the load on the workstation being scanned |
| File queue size (MB) | The maximum total size of the queue that stores detected files before sending them to the Traffic Monitor server, MB<br>**Warning!**<br>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. |

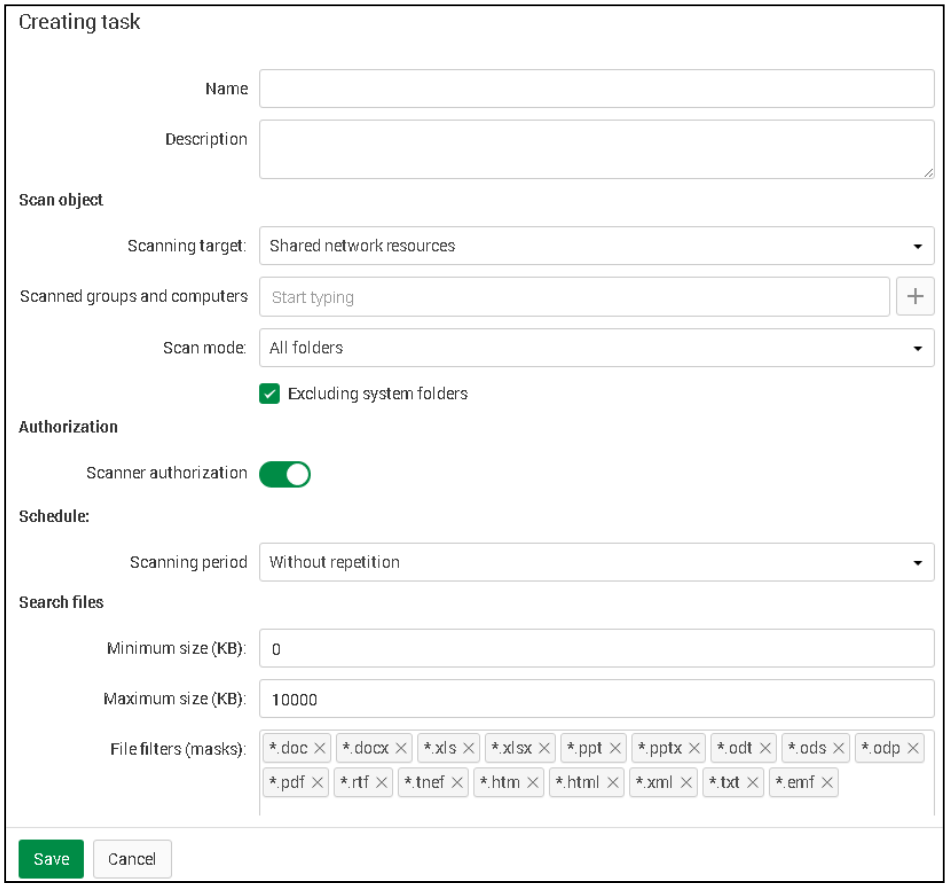
| | |
|---|---|
| Queue check interval (sec) | Interval (in seconds) at which the Crawler server checks for objects in the queue to upload them to the Traffic Monitor server. If there is at least one object in the queue, it is passed to the Traffic Monitor server |
| Connections to Traffic Monitor | The maximum number of simultaneous 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 |
| Ignore the following SIDs | Allows you to configure a filter of persons |
| System folder masks | Masks of folders that will not be scanned |

**User's target actions:**

Configuring Scanner

## 3.10.2 Scan Job

**Reference information:**
A *scan job* is a single or repeated operation that checks specified storages (Microsoft SharePoint 2007/2010/2013 storage, workstation local drives, shared network resources) for confidential data (on how to specify confidential data, see "Defining the confidential information"). When you create or edit a job, a dialog box appears where you can specify parameters of the job.




Job attributes:

| Parameter | Description |
|---|---|
| Name | Name of the job. A required parameter |
| Description | Jobdescription |

| | |
|---|---|
| Scanning target | Type of the scan job:<br>• **Shared network resources**<br><br>**Warning!**<br><br>Crawler does not support using more than one Astra Linux domain to scan shared network resources.<br><br>• **Local drives of workstations**<br>• **SharePoint file storage**<br>Depending on SharePoint version, specify the following parameters:<br>**For SharePoint 2007 and 2010:**<br>• **SharePoint version** - SharePoint version: 2007 or 2010;<br>• **Address of DB resource** - enter address of SharePoint database server, e.g., `sharepoint-test`;<br>• **Name of DB resource** - enter the name of SharePoint database instance, e.g., `wss_content`.<br><br>**For SharePoint 2013:**<br>• **SharePoint version** - SharePoint version: 2013;<br>• **SharePoint server address** - enter address of SharePoint database server with the protocol (http:// or https://). |
| Scanned groups and computers | You can specify individual computers, computer groups, and IP addresses. Enter the required values manually or click tp + select values from the list.<br><br>A required parameter. |

| | |
|---|---|
| Scan mode | **All folders** - scans all folders on the workstation<br>**All folders except** - scans all folders on the workstation except the specified ones<br>**Only folders** - only scans folders specified by the user<br>**Note:**<br>If you want to scan all folders including system folders, clear the check box **Exclude system folders**. By default, system folders are not scanned.<br>**To specify scanning paths, you can use the following symbols:**<br>`*`- any characters (0 and more)<br>`?`- any single character<br>`$`- a character that is used by Windows to indicate the hidden folder<br>**Warning!**<br>The scanning path should end with ***** or ****. For example, the path can look like: "C?\folder*" or "C?\folder\".<br>**When scanning the shared network resources or SharePoint storage you can use the following queries:**<br>`Docs*` - will scan the Docs folder and all its subfolders.<br>`text_example` - will search for “text_example” in the path.<br>`.file_format` - will scan files of specified format (.txt)<br>**When scanning local discs and folders, you can use the following queries:**<br>`C$\Docs*` - will scan the Docs folder and all its subfolders on C:\ drive<br>`*\Docs*` - will scan the Docs folder and its subfolders, regardless of their location.<br>`?$\Docs*` - will scan any folder whose name has 1 character and the Docs folder with all subfolders. (C$\Docs\, D$\Docs)<br>`\Docs????*` - will scan any folder that has Docs in its name with 4 additional characters (Docs1234)<br>**Warning!**<br>In the **All folders** scanning mode, only workstation local drives are 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.<br>**Warning!**<br>To scan a SharePoint storage, specify the user of the MS SQL Server that hosts the target database.<br>**Warning!**<br>Crawler uses access to the domain controller to receive information about users or groups by a unique identifier (SID). To enable access, use the domain account with read access for the resource you want to scan. |
| Scanning period | Scanning schedule<br>**Warning!**<br>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. A required parameter.<br>You can select extensions from the drop-down list or enter the value manually and press **Enter**. To delete a value, click ✕ next to the selected extension.<br>**Note:**<br>If you want to scan all files, then use * as the parameter value. |

**User's target actions:**

Creating a Job

# 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
- Administrating the System

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

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

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

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

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

5. Click **Login**.

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

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

### 4.1.2 Applying System Configuration

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

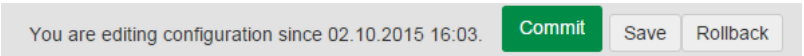
- Technologies
- Protected objects
- Persons
- Policies
- Lists

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

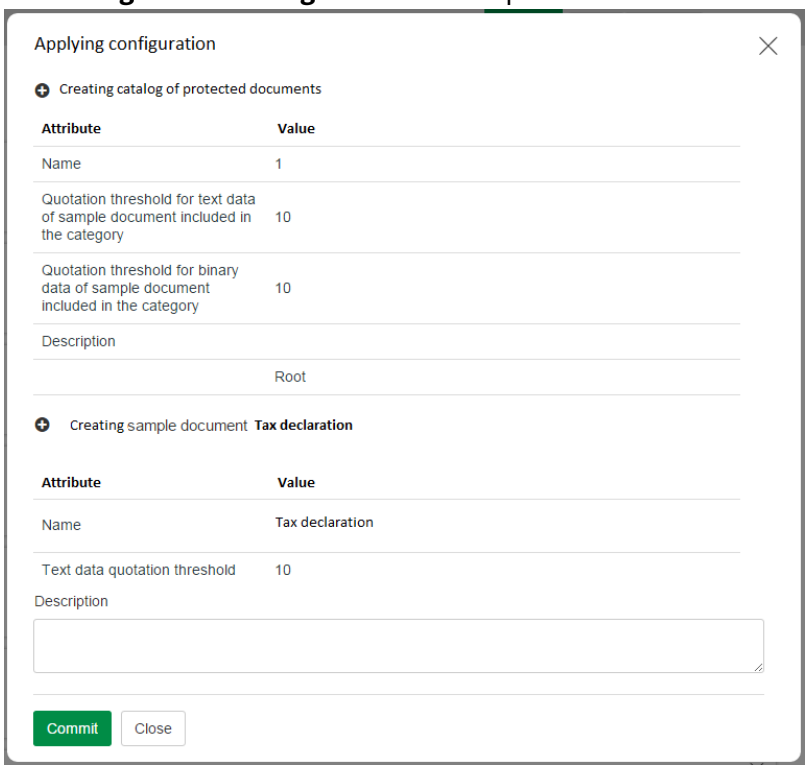
**Purpose:**
Apply the System configuration.

**Solution:**

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

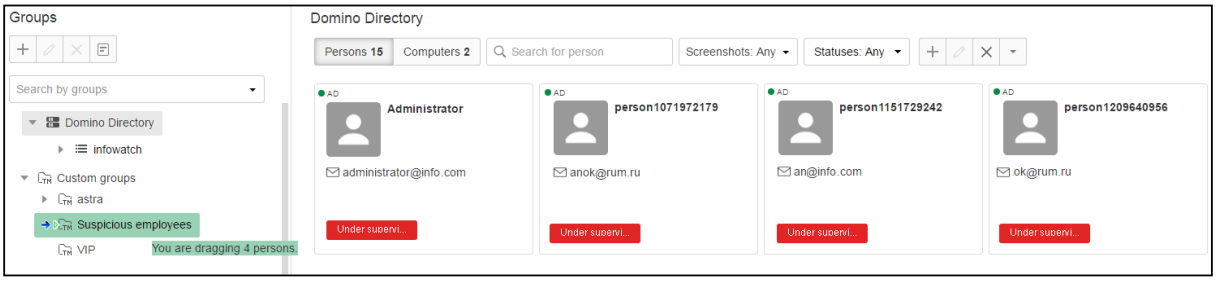
You need to add suspicious employees to a separate group. For this:

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**.

**To add a person from the contact in event:**

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

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

- Editing Element
- Deleting Element

## 4.2.3 Configuring Person's Card

**Purpose:**

Fill the card of person with data.

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

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

### Adding Contact to Person

**Purpose:**
Add or edit contact information for the person.

**Solution:**

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

**Note:**

Contact values must be specified in the following format:

- - mobile phone (string of 3 or more characters; may contain only digits, space, and the characters: "-","_", "( )","+");

- - landline phone (string of 3 or more characters; may contain only digits, space, and the characters: “-”,”_”, “( )”,”+”);
- - e-mail (e-mail address in RFC format);
- - Lotus e-mail (e-mail address in RFC format).
- - domain account (e-mail address in RFC format);
- - Skype contact (string of 1 or more characters);
- - ICQ contact (string of 1 or more characters);
- - Facebook account (string of 1 or more characters);
- - VK account (string of 1 or more characters);
- - Telegram account (string of 1 or more characters);
- - other Web-account (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**.

To add new contact from the event to the person:

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

## Adding Computer to Person

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

**Solution:**

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

## Adding Person to Group

**Purpose:**
Add a person to an existing group.

**Solution:**

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

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

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

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

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

### 4.2.4 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!**

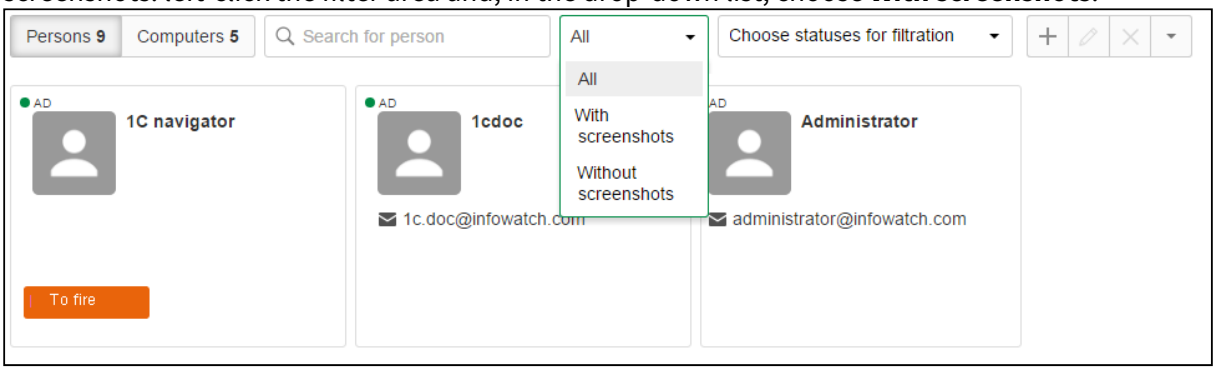
It is necessary to perform specified actions prior to creating a Device Monitor rule (see "ScreenShot Monitor Rule (DM)") and deploying the Device Monitor policy, which includes this rule, to workstations. Otherwise, the System will not display screenshots.

**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 Catalogues

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

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

**Managing catalogs includes the following actions:**

- Managing Tags

- Managing Web Resources
- Managing Statuses
- Managing Perimeters

**See also:**

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

### 4.3.1 Managing Tags

**Purpose:**
To create a tag.

**Solution:**

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




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

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

- Editing Element;
- Deleting Element.

### 4.3.2 Managing Web Resources

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

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

**Solution:**

1. Creating a group of resources
    a. Go to the **Lists** section, the **Web resources** subsection.

b. In the left part of the workspace, click + **Create web resource list.**
c. In the window that opens, type a name and description of the resource list.
d. Click **Save**.

2. Adding a resource
   a. Go to the **Lists** section, **Web resources** subsection.
   b. In the left part of the workspace, left-click the target resource list.
   c. On the toolbar in the right part of the workspace, click + **Add web resource**.




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

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

**Additional information:**

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

- Editing Element
- Deleting Element

### 4.3.3 Managing Statuses

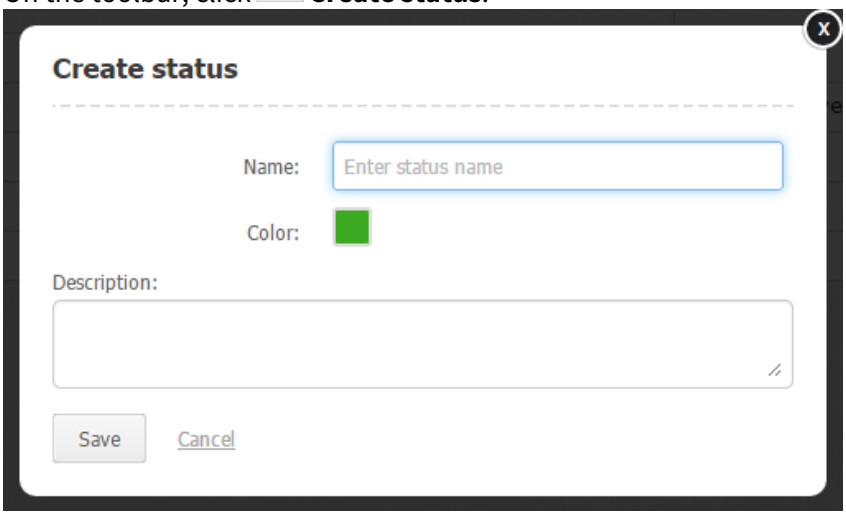
**Purposes:**:

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

**To create a new status:**

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

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




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

**To create a person control policy directly from Statuses subsection**:

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

**Additional information:**

Statuses can be edited and deleted by standard means:

- Editing Element
- Deleting Element

## 4.3.4 Managing Perimeters

**Reference information:**

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

By default, the System includes the following perimeters:

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

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

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

- 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.

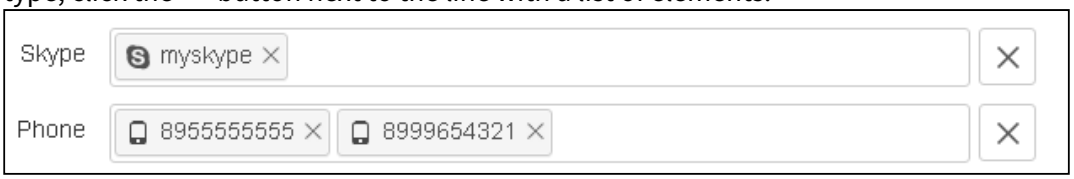
**Solution:**

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 or value in the field and press **Enter**he 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.

> **Note:**
>
> The web resource value can be a DNS name or an IP address (v4, v6) and the contact type should be URL.

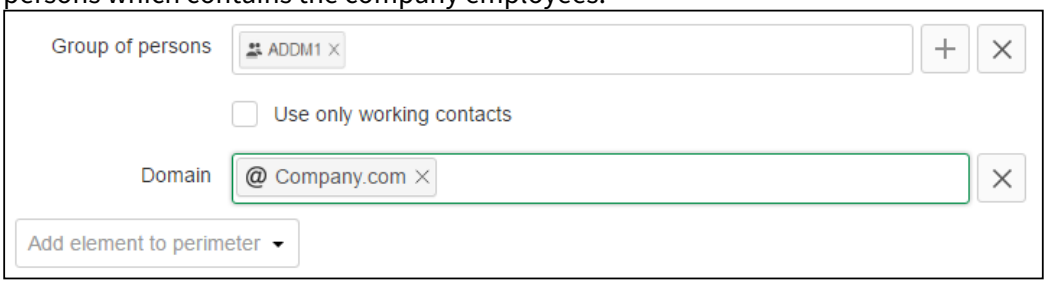
e. Entered values will be added to the list of elements. To remove a single element from the list, click ✕ next to the element name. To delete the entire list of elements of a particular type, click the ✕ button next to the line with a list of elements.




***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:

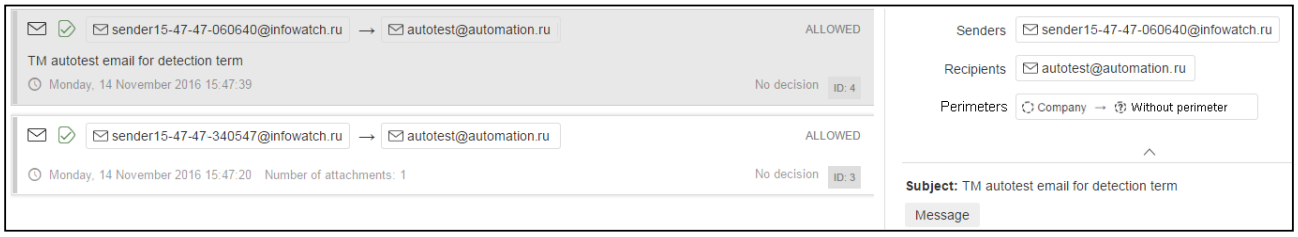
1. Create a *Company* perimeter (if the System already includes the *Company* perimeter, skip this step).
2. Add the following elements to the perimeter: `@company.com` mail domain and a group of AD persons which contains the company employees.




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.<br>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.<br>Contains no formatting or markup.<br>Applies and solving analysis tasks and search. | Creating text objects |
| Sample documents | Document quotes from which are searched in the analyzed text.<br>Memos, financial reports, contracts, and other sensitive documents can all be used as sample documents.<br>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.<br>Blanks may be different questionnaires, receipts, etc.<br>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.<br>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.<br>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.

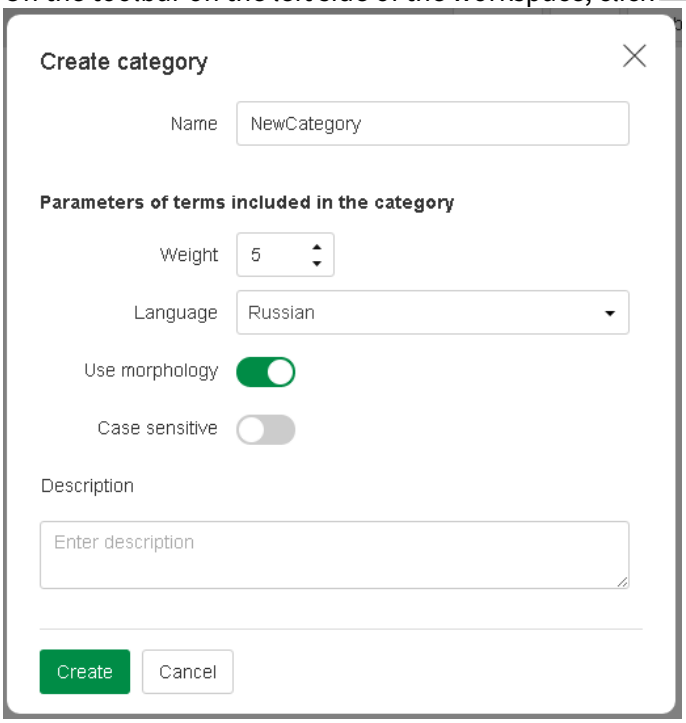
**Purposes:**

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**.



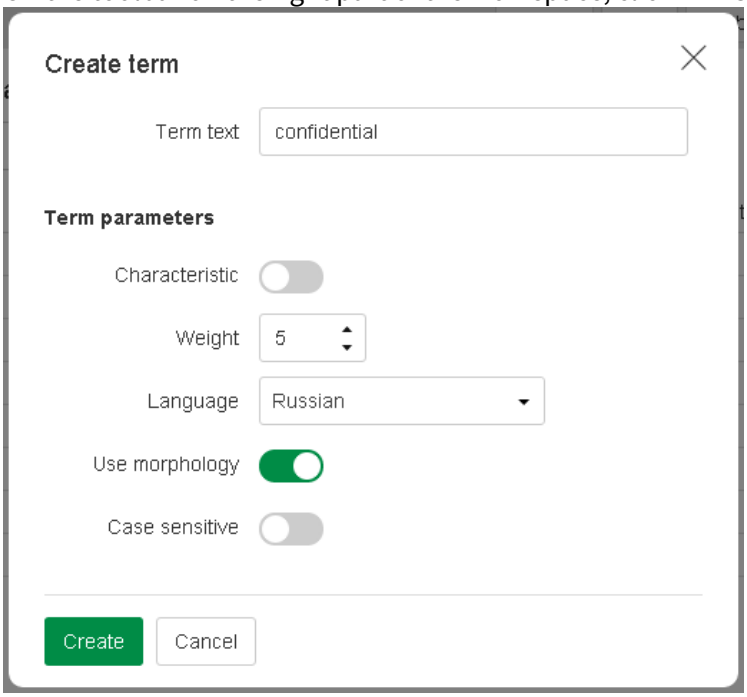

c. Specify required attributes for the category (see "Categories").
d. Click **Create**.

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

**Solution:**

**1. Create a catalogue of text objects.**

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

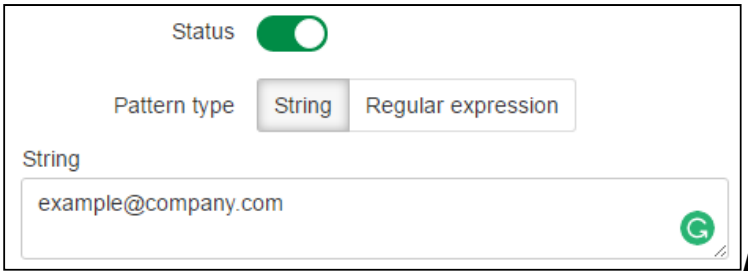
**2. Create a text object and specify its value.**

a. Go to the **Technologies** -> **Text objects** section.
b. On the left part of the workspace, select a catalogue 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  **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*.

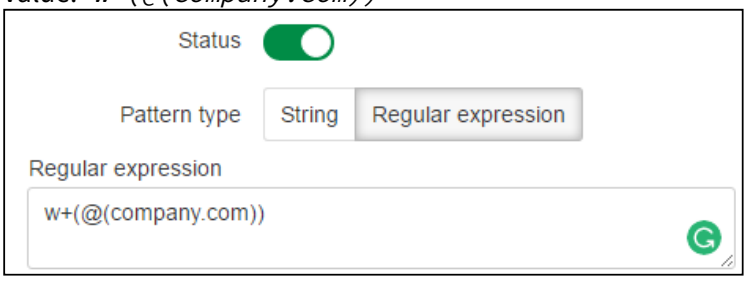
2. Select the object and switch to the edit mode.
3. Create a new active template for the text object and specify the following string as the template value:`example@company.com`:




***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 catalogue.**

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

**Note:**

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

e. Click **Add**.

**Additional information:**
Text objects, their templates, and catalogue

s are edited and deleted by standard means:

- Editing Element;
- Deleting Element.

## Managing Sample Documents

**Purposes:**

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

**Solution:**

**1. Create a catalogue of sample documents**

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

**2. To create a sample document**

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

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

**Warning!**

Requirements for file size:

- Maximum size of binary data - 128 MB;
- Maximum size of text data - 30 MB;
- Minimal size of binary and text data – 128 bytes;
- Minimal plain text size of text data - 10 characters;
- Minimal image size - 100 pixels on one side;
- Minimal size of vector data - 300 KB (about 800 primitives)
- Permissible sides ratio - not bigger than 5 : 1.

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

**3 Update a sample document**

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

**Note:**

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

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

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

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

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

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

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

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

- Editing Element;
- Deleting Element.

## Managing Blanks

**Purpose:**

1. Create a catalogue of blanks.
2. Create a blank.
3. Create a detection condition.
4. Update a blank.

**Solution:**

**1. Create a catalogue of blanks**

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

**2. Create a blank**

a. Go to the **Technologies**->**Blanks** section.
b. On the left part of the workspace by clicking the left mouse button, select a catalogue inside which you want to create a blank.
c. On the toolbar for managing blanks which is located on the right part of the workspace, click + **Add**.

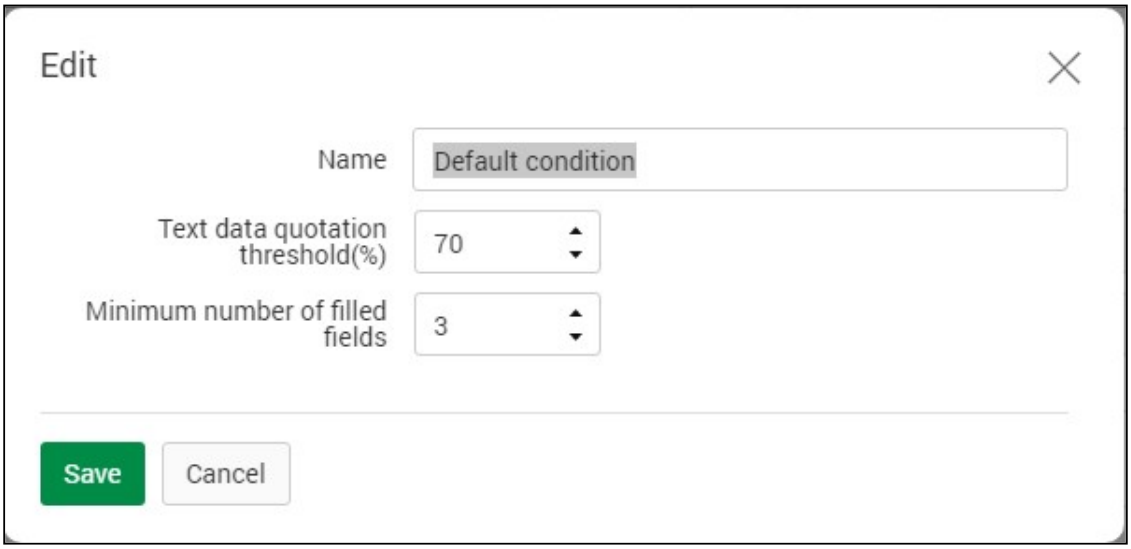
d. In the dialog window that opens, select a document that will be used as a blank and click **Open**. You can upload a document in one of the following formats: DOC, DOCX, DOT, DOTM, DOTX, XLS, XLSX, XLT, XLTM, XLTX, ODS, ODT, RTF, TXT, VSD, HTML, HTM, PDF, CHM.
e. When the download is finished, the blank will be added to the catalogue

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

f. . All necessary attributes are assigned to a newly created blank by default.
g. To change attributes of the blank specified by the System, click **Edit** on the toolbar and change required attributes (see “Blanks").

**3. Create a detection condition**

a. Go to the **Technologies**->**Blanks** section.
b. On the left side of the workspace, select the desired catalogue.
c. In the list on the right part of the workspace, select the blank you want the detection condition to be set.
d. Click **Edit**.
e. On the right part of the workspace click **Create**.
f. In the dialog window that opens, enter the name and specify the parameters of detection conditions:
Text data quotation threshold
Minimum number of filled fields




g. After data input click **Save**.
h. To add few detection conditions, repeat ection e-g.

> **Note:**
>
> It is recommended to create **no more than 20** detection conditions per one blank.

i. Click**Save**.

**4. Update a blank**

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

**Example:**

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

1. Create *RECRUITMENT_CHECKLIST* blank.
2. Load the document file “Recruitment checklist” as a blank.
3. Create a detection condition with **Minimum number of filled fields = 0**. Also you may edit the default condition which is created in accordance with the blank.
4. Create a protected object based on the *RECRUITMENT_CHECKLIST* blank and specify the detection condition you require.

**Additional information:**
Editing and deleting detection conditions, blanks and its catalogues are performed by standard means:

- Editing Element;
- Deleting Element.

## Managing Stamps

**Purposes:**

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

**Solution:**

**1. Create a catalogue of stamps.**

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

d. Click **Create**.

**2. Create a stamp**

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

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

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

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

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

> **Note:**
>
> For more details on creating stamps, see the Knowledge Base article "Stamps".

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

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

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

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

- Editing Element;
- Deleting Element.

## Managing DB Unloadings

**Purpose:**

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

**Solution:**

**1. Create a catalogue of unloadings**

a. Go to the **Technologies**->**DB Unloadings** section.
b. On the toolbar on the left side of the workspace, click  **Create catalogue of DB unloadings**.
c. In the window that opens, type a name and description for the catalogue.
d. 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 catalogue.
3. In the list in the right part of the workspace, select the unloading you want to update.
4. Click **Edit**.
5. In the edit window that opens, 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 catalogues are performed by standard means:

- Editing Element;
- Deleting Element.

Detection Conditions for Unloading

**Reference information:**

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

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.

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

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

Logical relations are defined using the following symbols:

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

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

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

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

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

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

***Minimal quantity of rows.***

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

For example, if a condition like 1+(2|3) is specified and the minimal quantity of rows is set to 10, then for triggering the 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

## Managing Graphical Objects

To configure an automatic classifier of graphical objects:

1. Create a category of text objects:
   a. Go to the **Technologies**->**Graphical objects** section.
   b. On the toolbar in the left part of the working area, click .
   c. Specify the name and description of the new category.
   d. Click **Save**.
2. Upload images:
   a. In the left part of the working area, click the category to which you want to add images
   b. On the toolbar in the right part of the working area, click 
   c. Select one or more files on a disk and click **Open**. Choose files from which graphical data can be extracted.
   d. Make sure that the selected files have been successfully added to the category. A pop-up window on the right displays the process status.

3. Learn the classifier:
    a. Create at least two categories that contain one or more images.
    b. Click  and wait until the end of the learning process. The process can take several minutes. After the learning, there can be errors inn some categories. In this case, delete all images from such a category, add new images and learn the classifier again.
    c. In the upper part of the working area, click **Apply**.
    d. In the **Applying configuration** window, check out the new configuration and click **Apply**. The new configuration will become the active one on the server.

**Note:**

For the technology to work correctly, follow these recommendations:

- There should be a lot of images in the collection. Images should be divided into categories. Each category should include at least 50 images.
- Images in a category should not be of different subjects. Each category should only those images that are related to its subject
- The sizes of different categories should be close.
- Learning time and System performance depend on the number of uploaded images.
- The minimum image size is 150 pixels on one side.
- The maximum image resolution is 10,000 by 10,000 pixels.
- The maximum image aspect ratio is 8:1.
- Allowed image rotation is 90+-10, 180+-10, 270+-10 degrees.
- Supported image types: `bmp, gif, jpeg, jp2, pbm, pgm, png, ppm, ras, tiff`. При этом:
    - If the file is an unencrypted archive, then a separate document is created from each file. All created documents are placed to the category that was selected when creating the document.
    - If the file is an encrypted archive, the document is not created or is created with an error.

To check individual files with the already learned classifier:

1. In the left part of the working area, click .
2. Click **Start new check**.
3. Select one or more files and click **Open**. Do not select archives to be checked.
4. Wait until the check is complete and read the results. The classifier will detect categories of graphical objects to which the images belong. You can add these images to specified categories and learn the classifier anew.

**Note!**

Images check to match any graphical object is run only for the graphical objects which can be edited. For more details, please see "Graphical Objects").

If you are not satisfied with the results of document processing (for example: for some files, categories are not defined; not all images are detected by the classifier or they are detected incorrectly), upload additional files to the category or delete earlier added files. Then learn the classifier anew.

### 4.4.2 Exporting and Importing the Base of Technologies

**Purpose:**

- Save the archive containing the base of technologies to a hard drive of the computer;
- Load the base of technologies, which is stored on your computer as an archive with `.cfb` extension, for using in the InfoWatch Traffic Monitor management console.

> **Note:**
>
> 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**, **Database Unloadings**, or **Graphical Objects**).
2. On the toolbar on the left part of the workspace, click ▾ and, in the drop-down list, select **Export**.
3. Preparing the base of technologies export will start. After the preparation is finished, an archive with `.cfb` extension will be loaded to your computer. This file contains the following elements:
   - categories and terms;
   - text objects, including pre-installed ones;
   - sample documents;
   - blanks;
   - stamps;
   - database unloadings;
   - graphical objects.
4. The structure of catalogues is preserved for all elements.

> **Warning!**
>
> As a result, the whole base of technologies will be exported, not a selected section only. The base of technologies from the last applied configuration is exported (see “Configuring the System").

**To import the base of technologies which is stored on your computer as an archive with `.cfb` extension:**

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

**Note:**

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

**Features of merging data during import:**

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

   **Note:**

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

4. To add sectoral and customized categories and terms into the System, you should use XML files that are compatible with InfoWatch Traffic Monitor System. After this XML file has been uploaded into the System, all appropriate categories and terms are to be automatically added to the System's management console, **Technologies** section (**Categories and terms**, **Text objects**, **Sample Documents**, **Blanks**, **Stamps**, **Database Unloadings, or Graphical Objects**).

   **Note:**

   Sectoral and customized categories and terms used for InfoWatch Traffic Monitor are unique and they cannot be imported to other DLP systems at present.

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

## 4.5 Managing Protected Objects

**Warning!**

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

**What are protected objects needed for:**

Protected objects make it possible to check if intercepted data contain all specified elements of analysis: for example, a sample document, a text object, and a database unloading. 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 Catalogue of Protected Objects | Creating a catalogue to which protected objects will be added |
| Creating a Protected Object | Creating a protected object and specifying its parameters |
| Adding Elements of Technologies | Adding elements of analysis to a protected object |
| Adding Detection Conditions | Specifying conditions for detecting added elements of analysis |
| Creating Policies for Protected Objects and Their Catalogues | Creating a data protection policy for selected protected objects and their catalogues |
| Importing and Exporting Protected Objects | Importing and exporting catalogue structure, protected objects included in these catalogues and elements of analysis used in these protected objects |
| Activating and Deactivating Protected Objects | Changing status of protected objects and their catalogues |

**See also:**

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

## 4.5.1 Creating a Catalogue of Protected Objects

**Purpose:**
Create a catalogue that will contain protected objects.

**Solution:**

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

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

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

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

**Note:**

The catalogue will be moved with all nested elements including subcatalogues and protected objects. When you move a catalogue, its status changes to the status of the catalogue to which you are moving it.

**Additional information:**

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

- Editing Element;
- Deleting Element.

### 4.5.2 Creating a Protected Object

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

**Solution:**

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

As a result, a protected object is created in the selected catalogue (if you have selected the **Create a protected object for each selected item** option, several protected objects are created).

You can move the created protected object to another catalogue.
To do this, select the required protected object in the list, press the left mouse button and move the protected object to the desired catalogue holding the left mouse button pressed. Then release the mouse button.

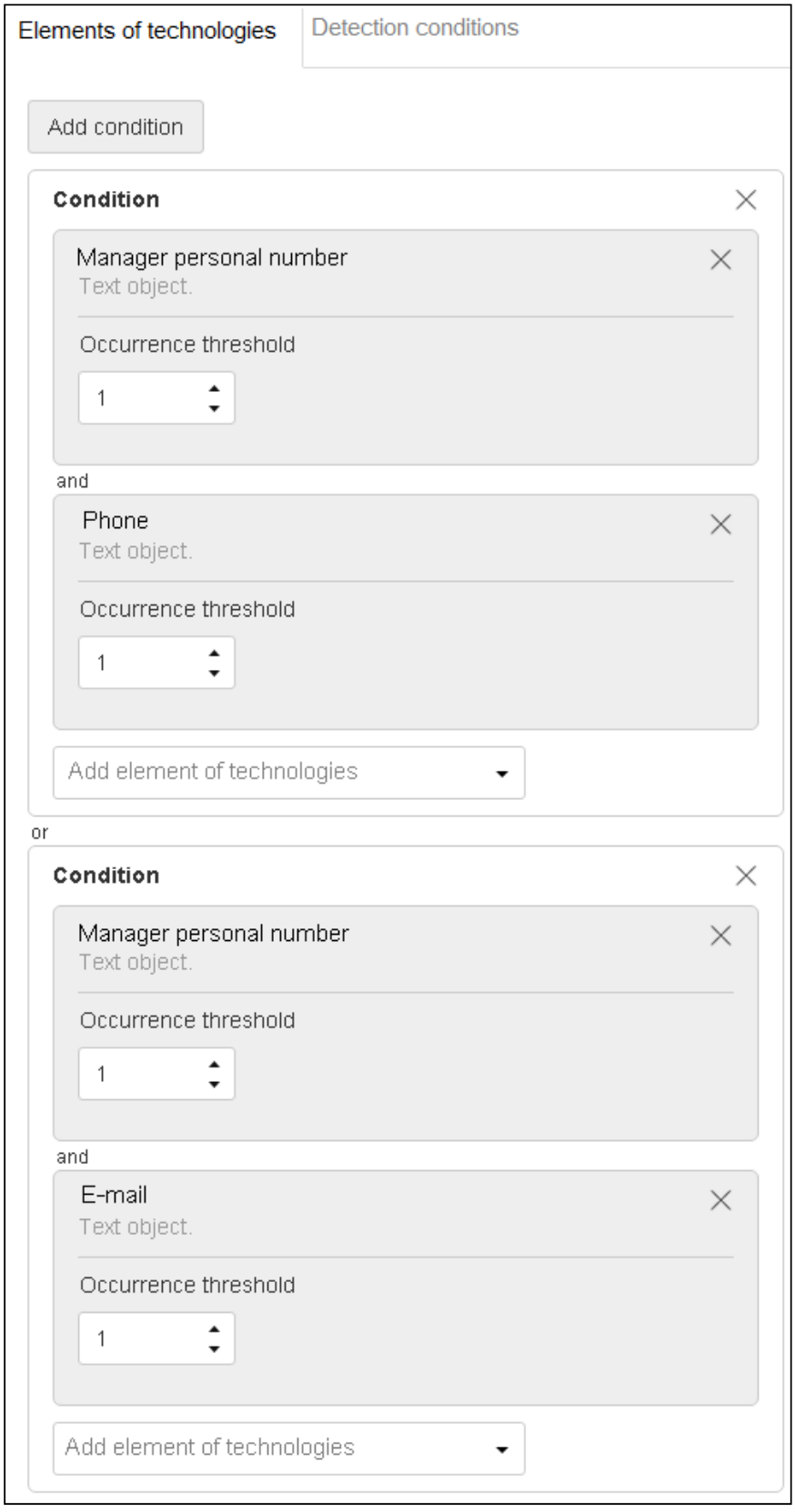
***Example:***

**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.
> This can be used when selecting catalogues and sub-catalogues.
> Adding catalogue as protected object is possible for sample documents, stamps, text objects, blanks and DB unloadings.
> When adding a catalogue to protected objects, all elements of technologies which are a part of the catalogue will be included as well.
> If new elements of technologies will be added after the protected object was created within the working catalogue, they will also let detecting the protected object within the intercepted traffic.
> If you delete elements of technologies from the catalogue that was added into protected object the detection by deleted elements will be finished.

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

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

**If you are editing an earlier created protected object:**

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

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

4. Click **Save**.

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

### 4.5.4 Adding Detection Conditions

**Reference information:**

A protected object can be detected in the event if:

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

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

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

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

**Purpose:**

Add detection conditions for a protected object.

**Solution:**

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

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

To add detection conditions for a protected object:

1. On the **Detection Conditions** tab, in the **Add element of technologies** field, click and, in the drop-down list, select the desired element.
2. The selected element will be added to the list of conditions. For some elements of technologies, you can specify additional detection conditions (see "Detection conditions").
3. If there are several elements of technologies in the protected object, you can add detection conditions for the other elements in one of the following ways:

- If you need conditions to be combined with a conjunction (logical "AND"), add conditions as described in step 1.
  In this case, all added conditions will be placed in the same **Condition** block and combined with a conjunction.
- If you need conditions (or groups of conditions) to be combined with a disjunction (logical “OR"), click the **Add condition** button.
  A new **Condition** block will be added. In this block, you can add conditions as described in step 1.
  In this case, all the **Condition** blocks will be combined with each other with a disjunction, and conditions within a single block will be combined with a conjunction.

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

**Additional information:**

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

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

### 4.5.5 Creating Policies for Protected Objects and Their Catalogues

**Purpose:**

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

**To create a policy for a catalogue of protected objects:**

1. Go to the **Protected objects** section.
2. In the **Catalogues of protected objects** list on the left side of the workspace, select the desired catalogue.
3. On the toolbar in the left part of the workspace, click and, in the drop-down list, select one of the following items:
   - **Create data protection policy**
   - **Create policy on agent**
4. In the policy creation form that opens, specify the required settings (for more information, see "Policies Section").
5. Click **Save**.

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

**To create a policy for selected protected objects:**

1. Go to the **Protected objects** section.
2. In the **Catalogues of protected objects** list in the left part of the workspace, select the desired catalogue.
3. In the right part of the workspace, a list of protected objects included in the selected catalogue will be displayed. Left-click the desired protected object. To select multiple objects, use the Shift or Ctrl key.
4. On the toolbar in the right part of the workspace, click and, in the drop-down list, select one of the following items:

- **Create data protection policy**
- **Create policy on agent**

5. In the policy creation form that opens, specify the required settings (for more information, see "Раздел "Политики"").
6. Click **Save**.

The created policy will be triggered when detecting at least one of the selected protected objects.

### 4.5.6 Importing and Exporting Protected Objects

**Purpose:**

- export to a file catalogue structure containing protected objects and elements of analysis used in them;
- load from file an earlier created catalogue 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** and select a catalogue.
2. On the toolbar in the left part of the workspace, click and in the drop-down list select **Export**.
3. Preparing the loading will start; then the archive will be saved on the computer.

The saved archive contains the xml files that store information about the protected objects and elements of analysis used in them. The structure of catalogues 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 catalogue name in the import file matches the catalogue name in the System, but paths to a catalogue differ, then the catalogue from the import file will not be added. If the catalogue name in the import file matches the catalogue name in the System, and paths to catalogue also match, then data from the import file will be merged with the data containing in the System.

**Features of merging data when importing:**

1. For catalogues, the following items missing in the System are added:
   a) child catalogues of protected objects;
   b) protected objects.

2. For protected objects, the following items missing in the System are added:
   a) elements of 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**.

**Note:**

If a protected object is selected as a result of end-to-end catalogue search, you cannot change its status when editing it or using **Activate**/**Deactivate** buttons. To change the protected object status, choose it in the catalogue.

This limitation is due to the fact that a protected object can belong to different catalogues including inactive ones.

**Warning!**

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

## 4.6 Managing Crawler Subsystem

**What do you need the Crawler subsystem for?**

The Crawler subsystem allows you to check if sensitive information is stored in the following 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 gets access to a scanner. Before operating the scanner, the user can configure it |
| Creating a Job | To scan resources, you need to create a job |
| Cleaning the Hash Base | Discarding file checksums saved in the System |

**See also:**

- "Crawler Section" - on the section where you can manage the Crawler subsystem

### 4.6.1 Configuring Scanner

**Purpose:**
To configure the scanner of the Crawler subsystem.

**Solution:**

1. Go to the **Crawler** section **Crawler**.
2. On the left part of the workspace, click the **Edit scanner** button.
3. In the window that opens, edit required parameters (see "Scanner").
4. Click **Save** to save your changes, or **Cancel** to exit the editing mode without saving changes.

> **Note:**
>
> When you edit the scanner, a message appears indicating that the scanner is locked. At this time, jobs for the scanner are not performed.
>
> When you exit the editing mode, a message appears indicating that the scanner is unlocked. It means that scanning jobs for this scanner can be performed.

**Additional information:**

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

> **Warning!**
>
> To define correctly the usernames and SIDs, Crawler scanner and a workstation or a SharePoint storage which are being scanned should be in the same domain.

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

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

*Invalid 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 - begins 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 begin with "S-1-5-21-".

**Note:**

For more information on the regular expression language, see in the article "Regular Expression Language".

## 4.6.2 Creating Job

**Purpose:**
Add a scan job.

**Solution:**

1. Go to the **Crawler** section.
2. On the toolbar, click **Create job**.
3. In the **Create job** form, specify required parameters (see “Scanning Job").
4. Click **Save**.

To edit an earlier created job, select it in the list and click on the toolbar.

To delete the selected task, click .

An example of scan job for shared network resources (e.g. when using SMB protocol)

There is a **`lv_426`** folder on **`PC_lv_426`** workstation. Access to the folder is open via SMB protocol. This folder has two subfolders: **`work_files_sec`** and **`work_files_not`**.

We need to scan the entire contents of the folder at `\\PC_lv_426\lv_426\work_files_sec\`. For this:

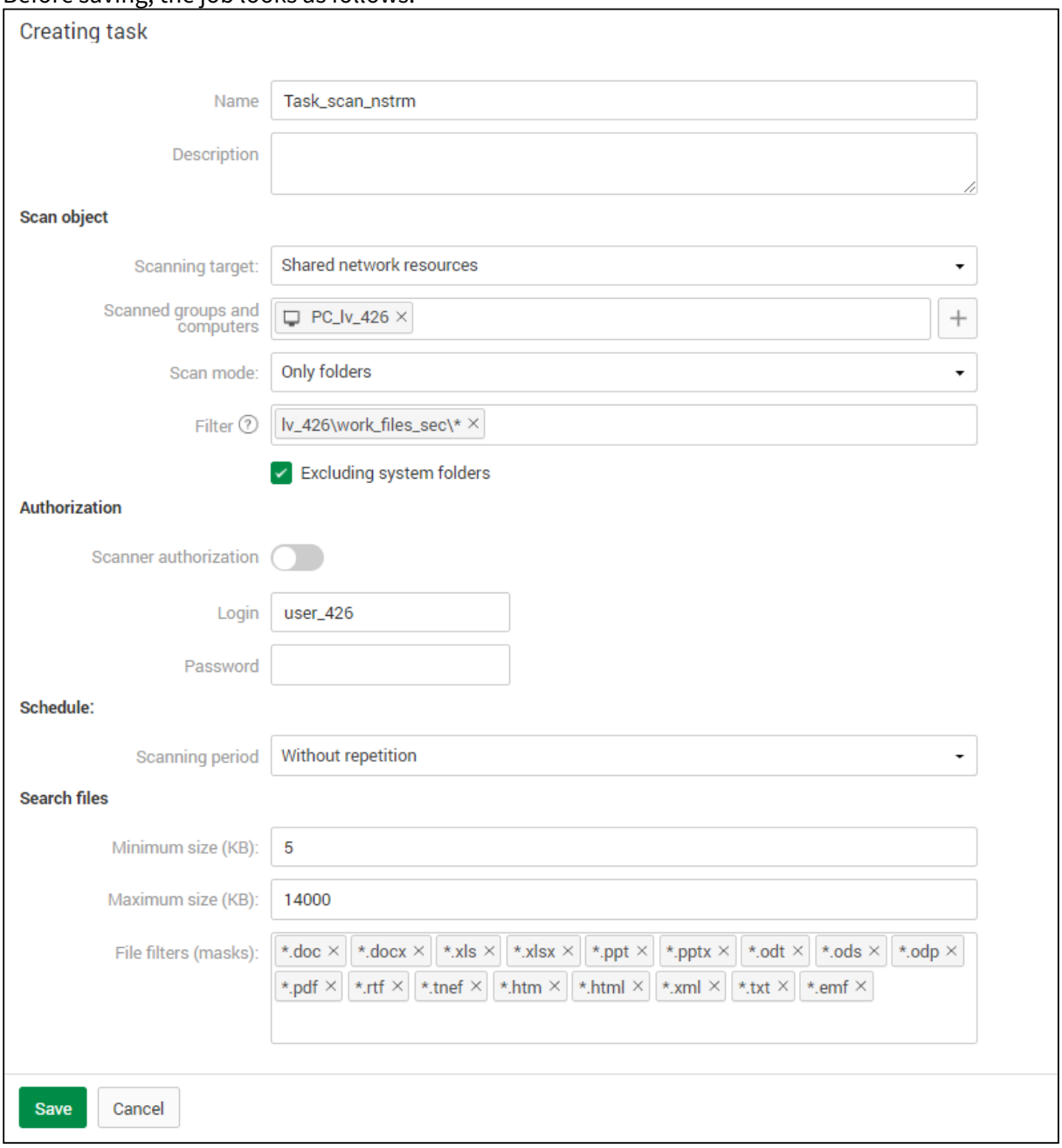
1. Create a scan job.
2. Fill in the **Name** field (required) and the **Description** field.
3. In the **Scanning target** field, select **Shared network resources**.
4. In the **Scanned groups and computers** field, specify the computer that stores the folder you want to scan.
   Here: `PC_lv_426.`
5. In the **Scan mode** field, select **Only folders**.
6. In the **Filter** field, specify the scanning path.
   Here:

`lv_426\work_files_sec\*` - the entire contents of the `work_files_sec` folder will be scanned, including subfolders. The path is specified relative to the folder to which access is provided.

> **Note:**
>
> Additional examples:
> - `lv_426\work_files*` - both `work_files_sec` and `work_files_not` folders will be scanned, including their entire contents;
> - `lv_426\` - будут only files in the `lv_426` folder will be scanned, the contents of the `work_files_sec` and `work_files_not` folders will not be scanned.

7. Leave the **Scanner authorization** option active if the account on behalf of which the scanner will be launched has access to the lv_426 folder. Otherwise, deselect the **Scanner authorization** option and specify suitable account details.
8. As we need to scan the folder only once, in the **Scanning period** field, select **Without repetition**.
9. If necessary, specify the minimum and maximum file sizes.
10. Specify extensions of scanned files.

11. Before saving, the job looks as follows:




**Important!**

Before running the scan job, check that the specified account can connect to scanning resources via the required protocol.

An example of using a scan job in the System

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

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, specify *SharePoint* as a scanning target, and specify the following attribute values:
    - **Address of DB resource** attribute - *SharePointRepo* value;
    - **Name of DB resource** attribute - *CorporateDataBase* value.
5. Create a policy and add a placement rule to it.
6. Specify the following parameters of the rule:
    - **Storage** - *File storage*; attributes have the following values:
        - **Enter source** attribute - *SharePointRepo* value;
        - **Enter path to storage** attribute - *CorporateDataBase* value;
    - **Assign tags** - *Printed circuit board* tag.

**Warning!**

When a job is running (even with domain administrator rights), you may receive the following error message:

```
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.
Such an error may occur, for example, if the folder owner has forbidden access to the folder.

### 4.6.3 Clearing Hash Base

**Reference information:**
To optimize the performance, Crawler stores **hashes** - checksums of files. If during the previous job session, the hash of a file was saved and during the next session of the same job, the hash of this file was not changed, this means that the file is not changed 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; besides, identical events for each session of a scanning job are not duplicated.

Features of storing the hash base:

- The hash base is stored separately for each scanning job. So, if a file has already been processed by a scanning job, then a newly created scanning job can process this file anew.
- Hash sums for each workstation are stored separately. So, if the same file is located on several workstations, then a scanning job will process it on each workstation anew.

We recommend clearing the hash base from time to time, for example, when you modify Traffic Monitor configuration. As the configuration changes may include changes in policies, terms, etc., then the algorithm of detecting violation may change as well. When you clear the hash database, all data concerning already processed objects is deleted and Crawler will send to Traffic Monitor all files which meet the job conditions.

**Purpose:**
To clear the hash base.

**Solution:**

1. Go to the **Crawler** section.
2. Select the desired job in the list.

3. On the toolbar, click  **Clear hashes**.

## 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").

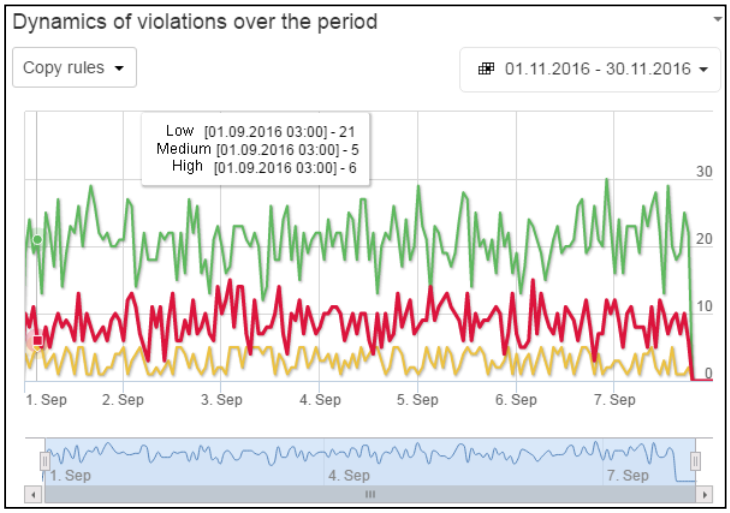
All generated reports are stored in the System. You can view the required report or delete reports which you do not need to store (see "Viewing Dashboard Report").

***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**.

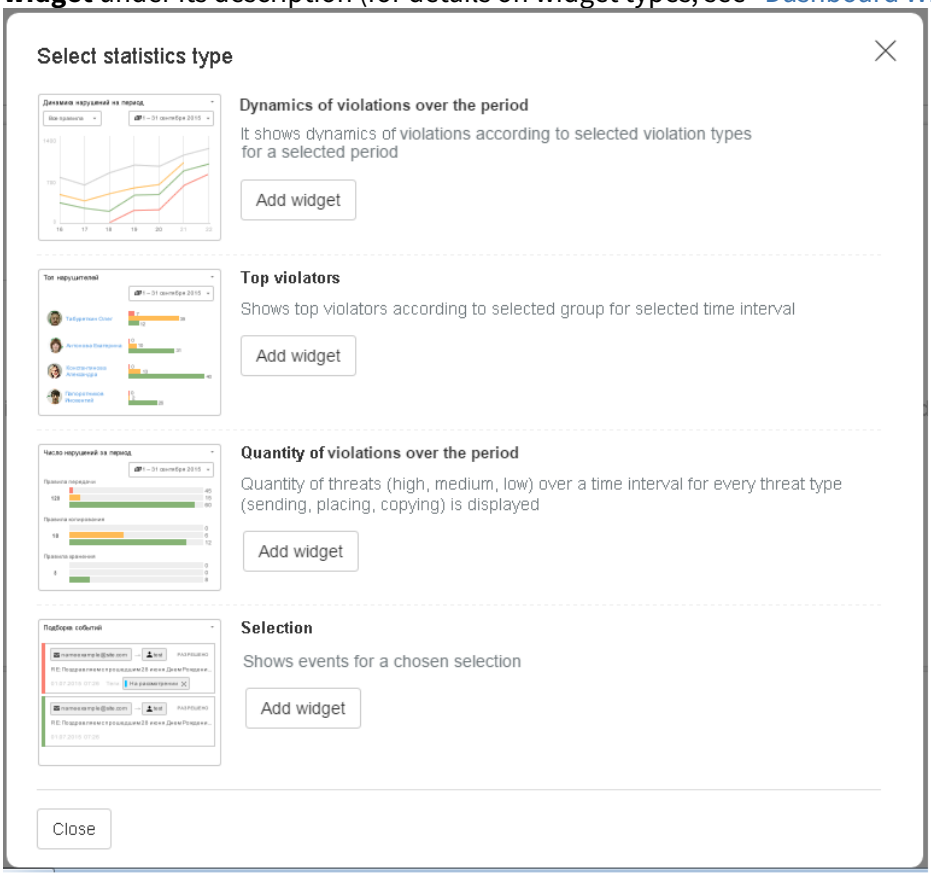
## Creating and Configuring Widget

**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.

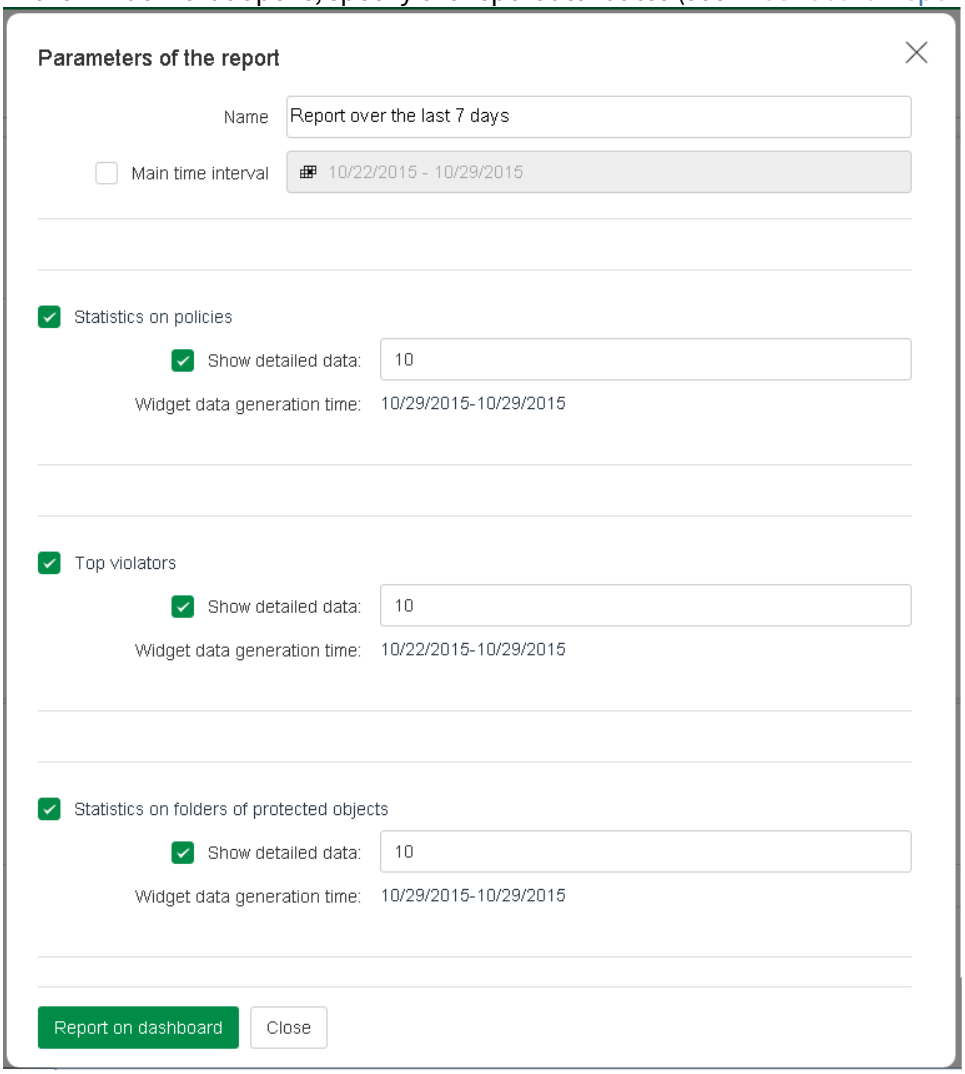
2. To edit a widget, in the right upper corner, click and, from the drop-down list, select **Edit**. In the **General widget settings** window that opens, change the required settings, then click **Save**.
3. To delete a widget, in the right upper corner, click and, from the drop-down list, select **Delete**. 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.
6. If you want to manually specify the period, for which the report will be generated, select the **Common period** check box and enter the start and the end date. If this option is deselected, then, for each widget, the report will be generated for the period specified in the widget properties.
7. Click **Report on dashboard**.

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

Once the report is generated, you will be prompted to open it in PDF or HTML format.

All created reports are stored in the System and are available by clicking **Show list of reports** in the right upper corner of the workspace. For details, see “Viewing Dashboard Report".

You can also view information about created reports from any section of the Management Console by clicking the **Export** button on the navigation panel (see "Interface of Traffic Monitor Management Console", №6 in the screenshot).

> **Note:**
>
> If you remove or modify a widget which is included in the report, then the already created report will not be changed.

## Viewing Dashboard Report

**Purpose:**
View a report on intercepted objects.

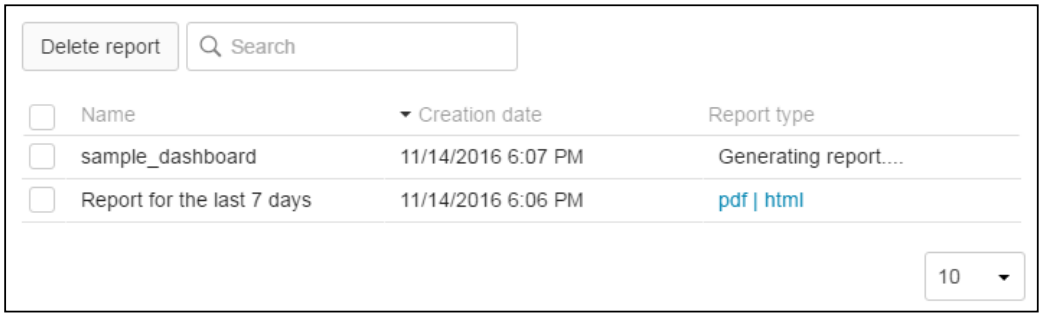
**Solution:**
When the report generation is complete, a message is displayed in the right upper corner of the workspace. In this message, you are offered to open the report in PDF or HTML format.




Click on the **pdf** or **html** link to open the report in a new browser window. You can also save, send or print the created report by standard means of your browser and operating system.
All created reports are stored in the System.

**To view the list of generated reports**, in the right upper corner, click the **Show list of reports** button. The **Reports** window will open where you can view information on the reports.

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




**To view a selected report**, in the **Report type** column, next to the desired report, click:

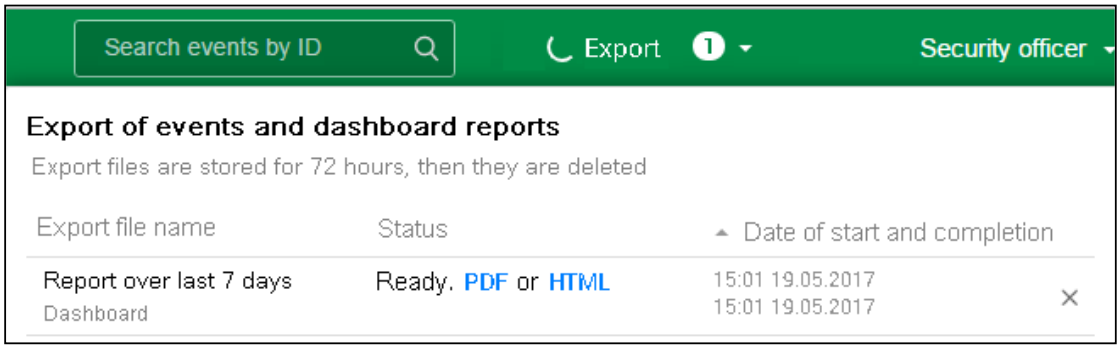
- **PDF** - if you want to display the report in PDF format;
- **HTML** - if you want to display the report in HTML format.

A new browser tab will display the selected report.

**To delete selected reports**:

1. Select checkboxes next to the reports you want to delete. To select all rows, select the checkbox in the header.
2. Click **Delete report**.

You can also view the list of reports from any section of the Management Console. For this, click the **Export** button in the Navigation page.




For each report, the list displays its name, status, date of start and completion, and links to PDF and HTML files. To open the report in a new browser tab, click the selected format.

To remove the report data from the list, click ✕ in the row of the selected report.

## 4.7.2 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. If you want to create a query within a folder, select a folder in the list or create a new folder (see "Creating Folder with Queries").
3. Create a query in a standard or advanced mode. You can create a query in a folder or in the root.
4. To run the query, select it in the list and click  **Run query** on the toolbar (or you can use **Save and run** button in the query creation form).

If necessary, you can copy or move an earlier created folder or query.

**To copy a folder** and its queries:

1. Select the folder in the list.
2. On the toolbar in the left part of the workspace, click  **Copy**.

If you are trying to copy a subfolder and you have full access to the parent folder, then the copy will be added to the same folder as the copied folder. If you don't have full access to the parent folder or you are copying a top-level folder, then the copy will be added to the root of the folder tree.

**To copy a query:**

1. Select the query in the list.
2. On the toolbar in the left part of the workspace, click  **Copy**.

If you are copying a query inside a folder and you have full access to the folder, then the copy will be added to the same folder as the copied query. If you don't have full access to the folder or you are copying a top-level query, then the copy will be added to the root of the folder tree.

**To move a folder**, select it in the list and holding the left mouse button move it to the desired location, then release the mouse button.

**Note:**

To move a folder, you need to have full access both to the folder you are moving and to the destination folder. If the folder includes queries, then you also need full access to the queries. For details, see the table below.

**To move a query**, select it in the list and holding the left mouse button move it to the desired location, then release the mouse button.

**Note:**

To move a query, you need to have full access both to the query and to the destination folder. For details, see the table below.

The table below shows what access rights are needed to manage queries:

| Action | Access rights | | | |
|---|---|---|---|---|
| | View and execute folder | Full access to folder | View and execute query | Full access to query |
| View the folder | + | | | |
| Edit the folder attributes (name, description, access rights) | + | + | | |
| Copy the folder | + | | | |
| Create a new item (a query or a subfolder) in the folder | + | + | | |
| Move an empty folder to a different folder | + | + | | |
| Move a folder which includes at least one query | + | + | + | + |
| Delete an empty folder | + | + | | |
| Delete a folder which includes at least one query | + | + | + | + |
| View and run the query | + | | + | |
| Edit the query parameters (including access rights) | + | | + | + |
| Copy the query | + | | + | |
| Move the query to a different folder | + | | + | + |

| | | | | |
|---|---|---|---|---|
| Delete the query | + | | + | + |

**Note:**

If after editing access rights, a query/folder becomes unavailable to any user of the System, then full access to the query/folder is automatically provided to the current user.

**See also:**

- Creating Folder with Queries
- Query Creation in Standard Mode
- Query Creation in Extended Mode
- Examples of Using Queries

Creating Folder with Queries

**Purpose:**
Create a folder where queries will be grouped.

**Solution:**

1. Go to the **Events** section.
2. In the list of folders and queries in the left part of the workspace, choose where to create a folder. You can create a folder in the root or inside an existing folder with queries.

   **Note:**

   If you do not have sufficient rights to create items within a selected folder, a warning will be displayed. In this case, you should create a folder at a different place.

3. Click + and, in the drop-down list, choose **Create query folder**.
4. In the form that opens, enter the folder name.
5. Specify if access rights to the folder should be inherited for subfolders and queries. By default, the **Apply rights for related queries** option is deselected.

   **Note:**

   If you create a folder inside a folder with the **Apply rights for related queries** option enabled, then actions described in steps 5-6 are unavailable.

6. Specify who can access the folder and define access rights. For this:
   a. Find required users in the list.

> **Tip.**
>
> To find required users, use the **Search** field.

b. Next to the user name, set the checkbox in one of the fields:
   - **View and execute access** - to provide access for viewing and copying the folder. Access rights to queries in the folder are specified when you create a query;
   - **Full access** - to provide full access to the folder.

> **Note:**
>
> To provide access to the folder to all users of the System, set a checkbox in the field with the required access level next to the **All users** value.

7. Click **Save**.

To edit the folder, click the button on the toolbar.

To delete the folder, click .

> **Note:**
> To edit or delete a folder, full access to the folder is required. If you can only view and execute the folder, then instead of button, button is displayed, and button is unavailable.

Query Creation in Standard Mode

**Purpose:**
Create a query to search for events which satisfy specified conditions.

**Solution:**

1. Go to the **Events** section.
2. In the list of folders and queries in the left part of the workspace, choose where to create a query. You can create a query in the root or inside an existing folder with queries.

> **Note:**
>
> If you do not have sufficient rights to create items within a selected folder, a warning will be displayed. In this case, you should choose another location for the query.

3. Click and, in the drop-down list, choose **Create standard query**.
4. In the form that opens, enter the query name and, if necessary, add a description.

5. On the **Query** tab, edit the query parameters. By default, the most commonly used parameters are displayed. For parameters that you need, specify the required values in the entry fields. To remove parameters that you do not want to use in the query, click
   ×
   in the right upper corner of the selected parameter.
6. To add a parameter, in the **Add condition** drop-down list, choose the required parameter (for the whole list of available parameters, see "Condition").
7. On the **Columns** tab, select attributes whose values will be displayed for the found events.
8. On the **Access** tab, specify who can access the query and define the access permissions.

   **Important!**

   If you create a query in a folder with the **Apply rights for related queries** option enabled, then access rights for the query will be the same as for the folder. In this case, editing access right to the query is unavailable.

   To specify access rights to the query:
   a. Find the required users in the list.

      **Tip.**

      To find users in the list, use the **Search** field.

   b. Next to the user name, set the checkbox in one of the fields:
      - **View and execute access** - to provide the user access for viewing, copying, and executing the query;
      - **Full access** - to provide the user full access to the query.

   **Note:**

   To provide access to the query to all users of the System, set a checkbox in the field with the required access level next to the **All users** value.

9. Click:
   - **Save** - to save the query;
   - **Save and execute** - to save and run the query.

**Tip.**

If while creating a query, you find out that you need to specify more flexible conditions, you can use the advanced mode. For this, in the **Query type** field, click **Advanced**. The advance query creation mode will open. All specified parameters of the query will be saved.

To edit the query, click  on the toolbar.

To delete the query, click  .

> **Note:**
> To edit, move, or delete a query, full access to the query is required. If you can only view and execute the query, then instead of  button,  button is displayed, and  button is unavailable.

The "Examples of using queries" article contains an example of creating a simple query.

Query Creation in Advanced Mode

**Purpose:**
To flexibly configure search conditions for events.

**Solution:**

1. Go to the **Events** section.
2. In the list of folders and queries in the left part of the workspace, choose where to create a query. You can create a query in the root or inside an existing folder with queries.

   > **Note:**
   > If you do not have sufficient rights to create items within a selected folder, a warning will be displayed. In this case, you should choose another location for the query.

3. On the toolbar, click  and, in the drop-down list, choose **Create advanced query**.
4. In the form that opens, enter the query name and, if necessary, add a description.
5. On the **Query** tab, in the **Add condition** drop-down list, specify the search parameters. By default, the most commonly used parameters are displayed. For parameters that you need, specify the required values in the entry fields. To remove parameters that you do not want to use in the query, click  in the right upper corner of the selected parameter.
6. To add a parameter, in the **Add condition** drop-down list, choose the required parameter.
7. By default, added parameters are joined by the logical AND. To change the operation type, left-click the  icon. The icon will change to  that indicates logical OR.
8. Use **Group of parameters** element to separate attributes joined by the logical AND from attributes joined by the logical OR (see "Advanced mode").
9. On the **Display fields** tab, select attributes whose values will be displayed for found events.
10. On the **Access** tab, specify who can access the query and define the access rights.

**Important!**

If you create a query in a folder with the **Apply rights for related queries** option enabled, then access rights for the query will be the same as for the folder. In this case, editing access right to the query is unavailable.

To specify access rights to the query:

a. Find the required users in the list.

**Tip.**

To find users in the list, use the **Search** field.

b. Next to the user name, set the checkbox in one of the fields:
   - **View and execute access** - to provide the user access for viewing, copying, and executing the query;
   - **Full access** - to provide the user full access to the query.

**Note:**

To provide access to the query to all users of the System, set a checkbox in the field with the required access level next to the **All users** value.

11. Click:
    - **Save** - to save the query;
    - **Save and execute** - to save and run the query.

**Note:**

If while creating a query, you want to switch to the standard mode, then, in the **Query type** field, click **Standard**. The standard query creation mode will open. All specified parameters of the query will be saved. However, if already specified conditions can be implemented in the advanced mode only, then switching to the standard mode is unavailable.

To edit the query, click on the toolbar.

To delete the query, click .

**Note:**

To edit, move, or delete a query, full access to the query is required. If you can only view and execute the query, then instead of button, button is displayed, and button is unavailable.

The "Examples of Using Queries" article contains examples of creating advanced queries.

Using Advanced Syntax

**Purpose:**
Configure full-text search through the event text by using extended syntax.

**Solution:**

1. Switch to the advanced mode of the query creation.
2. On the **Query** tab, in the **Add condition** drop-down list, select the **Event text** parameter.
3. Select **Advanced syntax**.
4. In the **Query** field, enter text using logical operators:"|","-", "!", "()", etc.

   **Note:**

   When **Advanced syntax** is enabled, search for special characters can be performed via shielding. To shield the special character, use '\' character placed before the character to be shielded.

5. Specify other parameters of the query (for details, see "Query Creation in Advanced Mode").
6. Click **Save**.

You can find detailed information on using logical operators for creating queries in the Internet article.

**Note:**

Please, not that the search area is defined explicitly in the **Search area** field (see "Search on the Event Text"), so you needn't specify the search area with Sphinx operators.

***Example:***

If you want to find the event whose text:

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

create the following query using the advanced syntax:

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

Examples of Using Queries

***Example 1:***

You need to view all email messages for the current day sent by employees under the supervision. For this:

1. Create a simple query and specify its name.

2. Specify the following query parameters:
    - **Interception date** - *Current day*;
    - **Event type** - *Email*.
3. In the **Senders** field, specify the *Employees under supervision* group (see how to create such a group in "Creating Group of Persons or Computers").
4. Save and run the query.

> **Tip**
>
> If there is a lot of traffic in your company and it takes much time to execute the query, you can continue working with other tasks while the query is running in the background. As soon as the query execution is complete, the System will notify you with a balloon tip.

***Example 2:***

An employee John Smith is suspected of misusing of confidential information. The incident has happened this week. To investigate the incident, you need to find events for John Smith.

For this:

1. Create an advanced query and specify its name - *Smith*.
2. Add the following conditions:




3. Save and run the query.

***Example 3:***

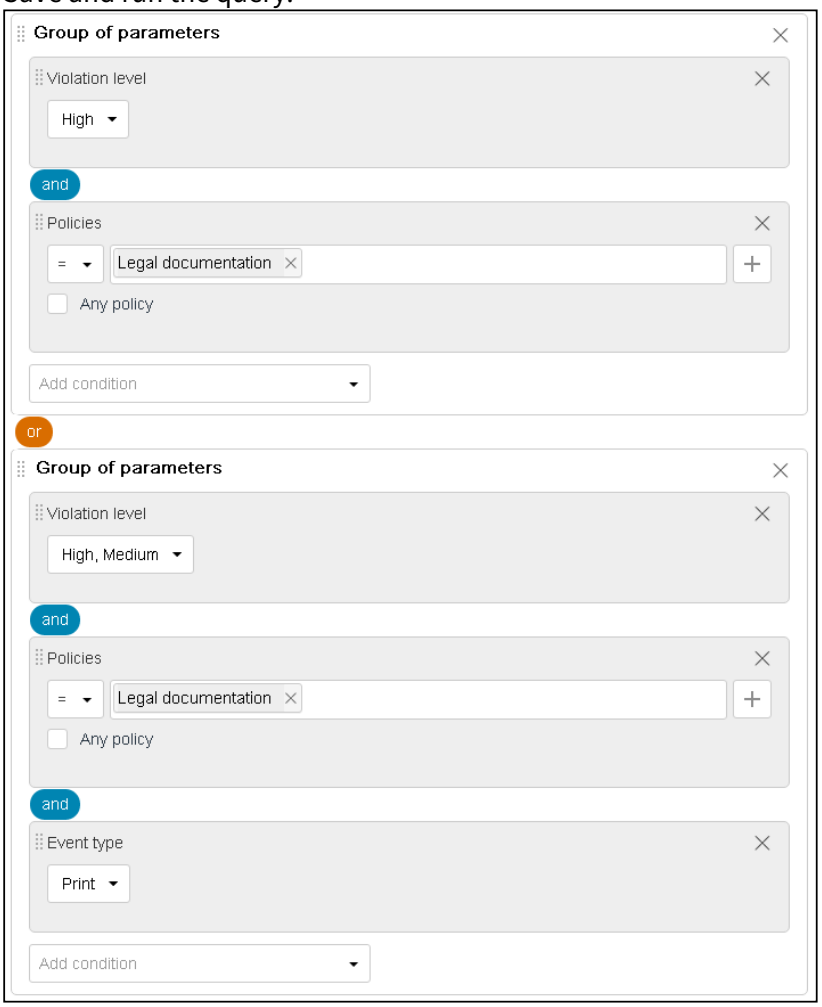
You need to find events:

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

For this:

1. Create an advanced query and specify its name.
2. Add two *Group of parameters* elements, joined by logical OR.
3. Within the first group, add the following attributes joined by logical AND:
    - **Violation level** - *High*;
    - **Policy** - *Legal documentation.*

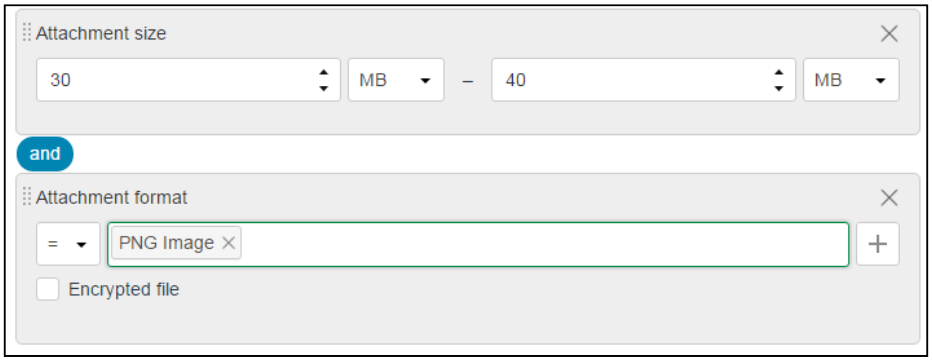
4. Within the second group, add the following attributes joined by logical AND:
    - **Violation level** - *High* and *Medium*;
    - **Policy** - *Legal documentation*;
    - **Event type** - *Print.*
5. Save and run the query.



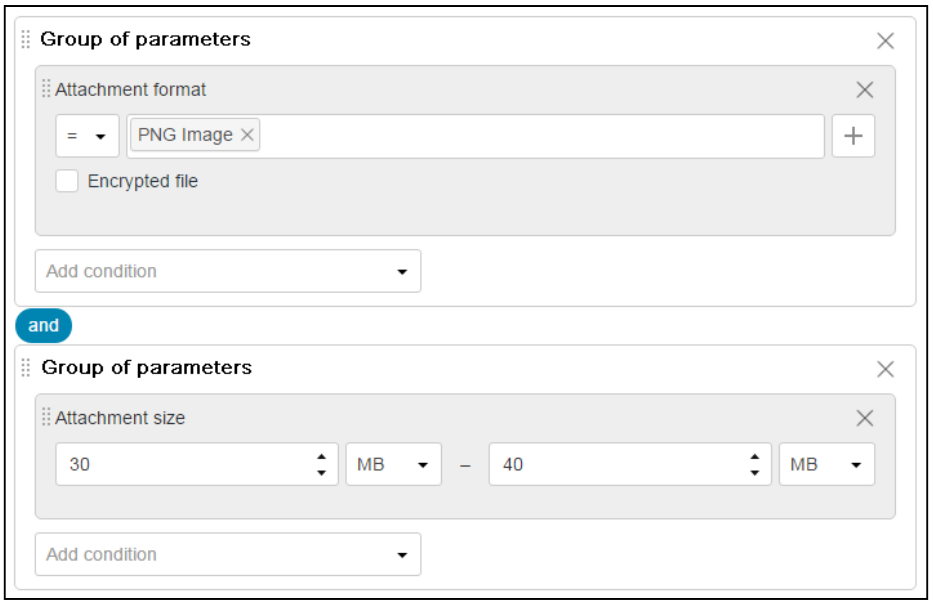

***Example 4:***

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

1. If several conditions within a group of parameters are combined by the operation of the logical “AND”, then query results will contain objects with at least one attachment that satisfies all specified conditions. In the example below, the query results will display objects with at least one attachment of PNG format whose size is between 30 and 40 MB.




2. If each condition is in a separate group of parameters and groups are combined by the operation of the logical “AND”, then query results will contain objects, for which all conditions are satisfied, but not necessarily for the same attachment. In the example below, the query results will display objects with at least one attachment of PNG format and at least one attachment whose size is between 30 and 40 MB.



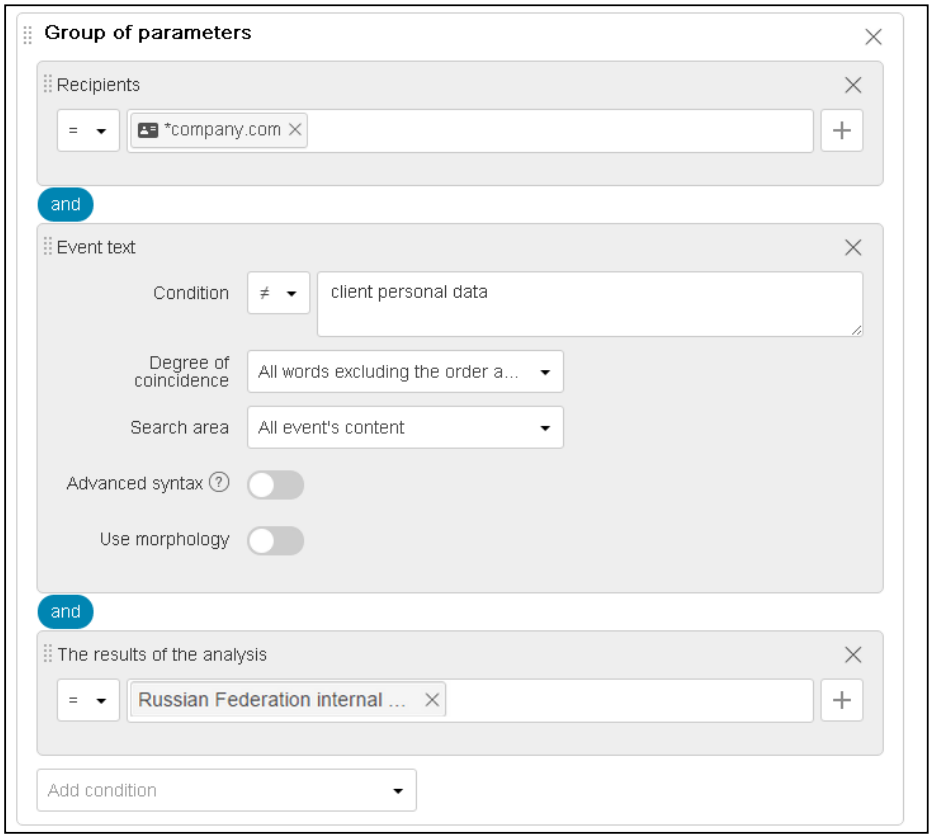

***Example 5:***

You need to find events which:

- 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 the *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.

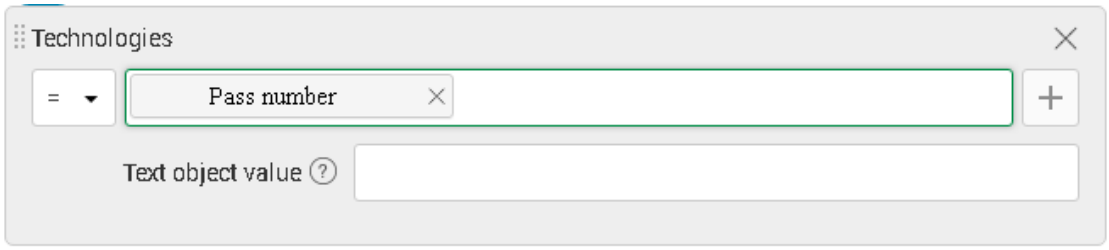



***Example 6:***

You need to find events which do not include the *"Pass number"* text object.

For this:

1. Create a query and specify its name.
2. Add the *Technologies* element.
3. As the element value, choose the "*Pass number*" text object and apply negation to the element.
4. Save and run the query.




The query results will include events:

- which do not contain triggered protected objects;
- where triggered protected objects do not contain the *Pass number* text object.

If you specify the text object value (e.g., 123456), then the query results will include events:

- which do not contain triggered protected objects;
- where triggered protected objects do not contain the *Pass number* text object with "123456" value.

## 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.

> **Note:**
>
> You can adjust the data representation in the viewing area. By default, the event content is displayed as snippets where all triggered protected objects and results of the text search are highlighted.

5. To view information on senders, recipients or computers, click the desired value. A card for the selected person or computer will be displayed.
   To view data on senders, recipients or computers, click the desired value. A card for selected person or computer will be displayed.
   When viewing the card, you can:
   a. Assign a status to a person/computer. For this, click Set status link and, in the **Adding status** window, select desired statuses. Then click **Save**.
   b. View detailed information on a person/computer in "Persons" section. For this, click Person profile link (for persons) or Go to computer link (for computers).
   c. View screenshot for a person/computer (if there are screenshots for a person, then icon is displayed next to the person name). For this, click Screenshots link. The **Screenshots** tab for the selected person or computer will open.

> **Note:**
>
> If there are screenshots taken within an hour before or after the event, the Screenshots near the event link is displayed for persons. Clicking this link opens the **Screenshots** tab with the screenshot whose creation time is closest to the event.

6. To view information about the triggered policy in the "Policies" section, click the name of the triggered policy.
7. If the event has attachments, you can save them to your computer. For this, click next to the attachment name.
8. To get detailed information on the event, in the right upper corner of the form, click **Detailed information**.

**See also:**

- "Brief Event Viewing Form" - on the form with general information about the event.
- "Viewing Detailed Event Form" - on displaying detailed information about the event.
- "Viewing Screenshots" - on viewing screenshots for persons or computers

## Viewing Detailed Event Form

**Purpose:**
To view a detailed information on the interception object.

**Solution:**

1. Go to the **Events** section.
2. Create a query or run an earlier created query (see “Creating Queries").
3. Select a tile of the target event in the list (or a row of the target event in the table). The right part of the workspace will display a brief event viewing form.
4. To open the detailed viewing form, click **Detailed information**.
5. In the **Detailed information on event** window that appears, view the needed information. Information on the event is presented in the following blocks: **General information**, **Text search**, **Protected objects**, and **Event content** (see "Detailed Event Viewing Form“).

> **Note:**
>
> You can adjust the data representation in the viewing area. By default, the event content is displayed as snippets where all triggered protected objects and results of the text search are highlighted.

6. When viewing the event parameters, you can get additional information about persons, computers, and policies of the event (see "Viewing Brief Event Form“, i. 5-6).
7. To close the detailed form, click ✕ in the upper right corner of the window.

**See also:**

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

### 4.7.3 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 catalogue

### 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.

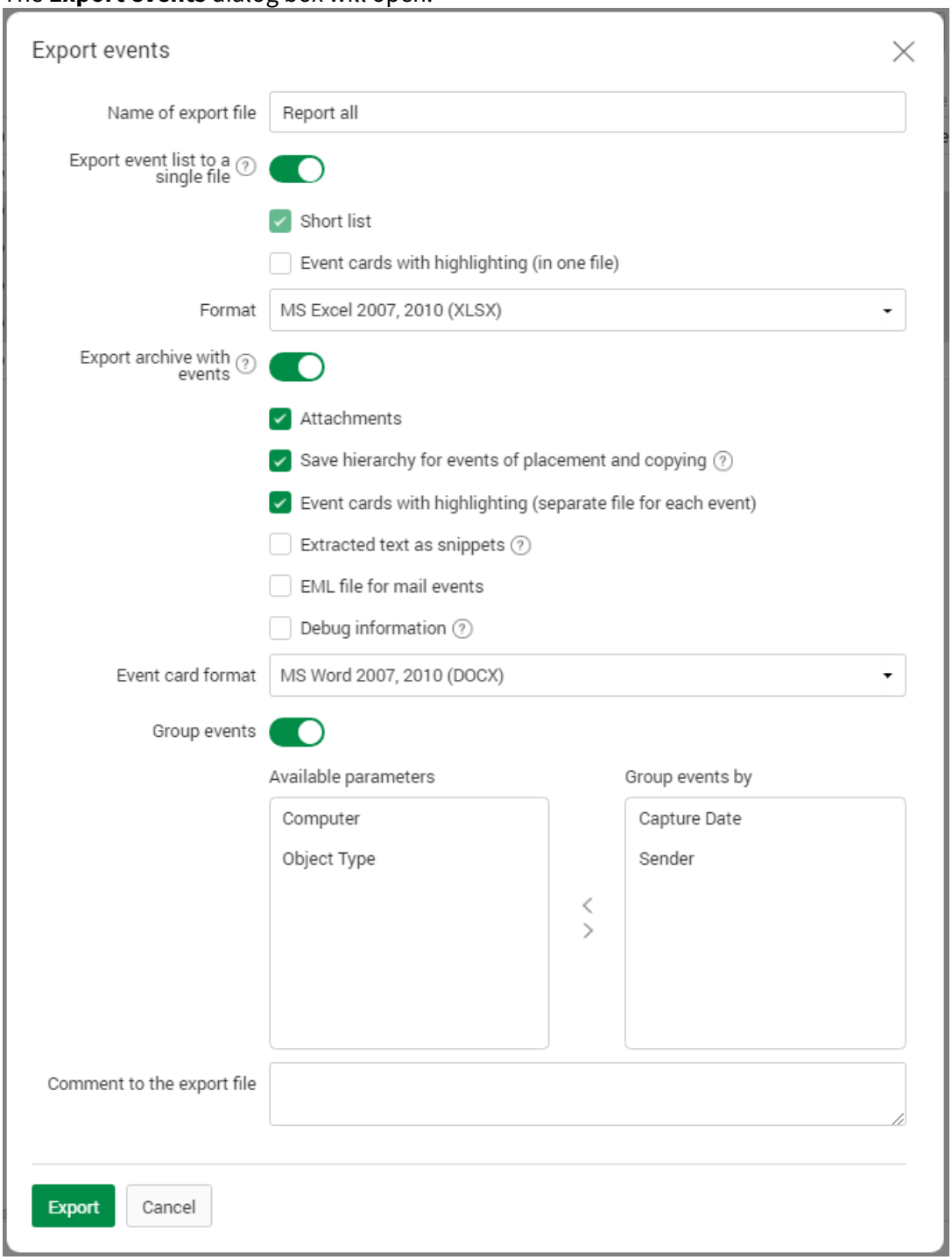
### 4.7.6 Event Export

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

**Solution:**

1. Go to the **Events** section.
2. Choose a query from the list and run it or create a new query (see "Creating Queries").
3. Select the event you want to export. To select multiple events, use the **Shift** or **Ctrl** key.

4. On the toolbar, click  and in the drop-down list select **Export events** or **Export all events**. The **Export events** dialog box will open.




5. If you have selected more than one event, specify how they should be exported (otherwise, go to step 7).
   You can choose one option or both:
   - **Export event list to a single file** - a file with data on all selected events will be created;
   - **Export archive with events** - an archive with a separate folder for each event will be created.

6. If you have chosen **Export event list to a single file**:

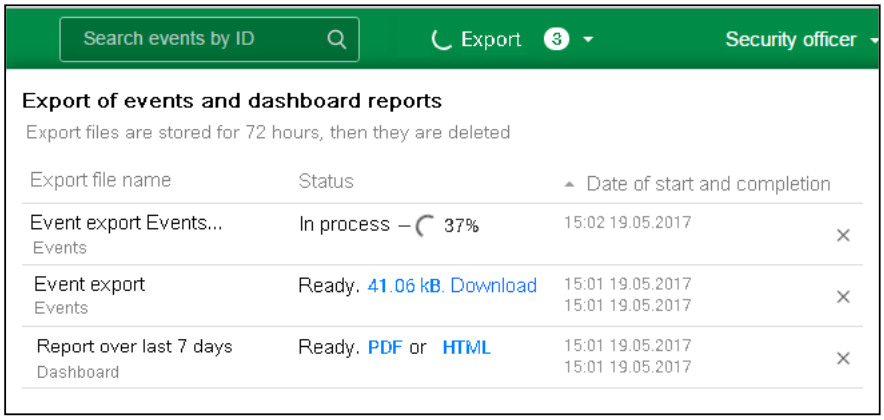
a. Choose the list view. You can choose one option or both:
   - **Short list** - for each event, a list of its main parameters is exported;
   - **Event card with highlighting** - for each event, a list of its parameters is exported. Besides, the export file includes the event text and the text extracted from attachments where all triggered protected objects are highlighted.

b. Choose the export format. The following formats are available:
   - MS Excel 2007, 2010 (XLSX) - unavailable if the **Event card with highlighting** view is selected;
   - MS Excel 2003 (XLS) - unavailable if the **Event card with highlighting** view is selected;
   - MS Word 2007, 2010 (DOCX);
   - Adobe Acrobat (PDF).

7. If you have chosen **Export archive with events** or the export file includes only one event, specify the following settings:
   - **Attachments** - original attachment files will be exported.
     By default the option is disabled to reduce RAM usage;
   - **Save hierarchy for events of placement or copying** - is displayed if the **Attachments** option is selected. Events of the same type will be saved to the "External device", "FTP", or "Crawler" folder depending on the event type;
   - **Event card with highlighting** - a file in DOCX format is created for the event; the file includes a list of the event parameters, the event text and the text extracted from attachments in which all triggered protected objects are highlighted;
   - **Extracted text as snippets** - is displayed if the **Event card with highlighting** option is selected. Text extracted from attachments will be exported in the form of snippets with triggered protected objects;
   - **EML file for mail events** - an EML file of the form [Event ID]_[Email subject] will be exported;
   - **Debug information** - for each exported file, debug information is added to the archive.
8. If you have chosen **Export archive with events**, you can specify additional settings:
   - **Group events** - select this option if you want to group events in the archive and add required parameter from the **Available parameters** field to the **Group events by** field. Events can be grouped by the following parameters: *Computer, Event type, Interception date, Sender.*
   - **Comment to the export file** - the added comment in DOCX format will be exported to the root folder
9. When you have specified all needed parameters, click **Create**.

When the operation is completed, in the upper right corner you will see a notification. To view the export file, click **download** and save it to your computer.

You can monitor the export progress by clicking the **Export** button on the navigation pane.




For each export process, you can view its name, status, start date and time. For already created files, the System also displays their size, creation date and time, and the **Download** link clicking which allows you to save the export file to your computer.

For export files that are being created at the moment, the progress in a percent format is displayed. If you want to cancel the export file generation (e.g., if the process takes a long time), click ✕ in the row of the selected file. The file generation will be canceled.

Besides event export files, the list also displays information on created dashboard reports (see "Viewing Dashboard Report").

The **Export** button is available from all sections of the Management Console.

## 4.7.7 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 security officer and other interested persons;
- assign a verdict to the interception object;
- assign a violation level, statuses, and tags to the interception object.

**Configuring the System response includes:**

| Action | Description |
|---|---|
| Creating data protection policies | Data protection policy is a set of rules that regulate data transfer, copying, placement, and usage of the clipboard.<br>Allows you to specify actions that may trigger policy rules. |
| Creating data protection policies on agents | Data protection policy on agents is a set of transfer and copy rules that apply directly on Device Monitor agents.<br>Allows you to specify actions that may trigger policy rules. |
| Creating person control policies | Allows you to specify the list of controlled persons whose actions may trigger policy rules |
| Creating rules | Defining what is a violation of policy rules, and what actions will be done in the event of violation |
| Configuring Notifications in Rules | If the rule is triggered, the System sends notification to specified recipients |

**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 the System policies are configured (a set of rules according to which objects are analyzed and processed) are applied to events (intercepted objects of network traffic).

The System policies are divided into three groups:

- Data Protection Policies - allow you to set up rules of transfer, copying, placement, and using clipboard
- Data Protection Policies on Agents - allow you to set up transfer and copy rules that apply directly on Device Monitor agents
- Person Control Policies - allow you to set up rules for monitoring actions of individual persons and groups

The System applies policies to events in the following order:

1. The System checks if the event conforms to any active data protection policy on agents.
2. If the event has triggered a policy, the sub-events are considered.
3. For each sub-event, the matching rules are selected (rules triggering to this sub-event).
4. Triggered rules are divided into sub-rules.
5. From sub-rules corresponding to the event, the ones with the highest priority are selected.
6. The actions specified in triggered sub-rules of the highest priority apply to the interception object.
7. If there are sub-events without matching rules, default actions are executed (if they are specified for this type of rules).

Then steps 2-7 are repeated for all active data protection policies and then for all active person control policies.

For more information about accompanying processes, see:

1. Dividing events into sub-events
2. Dividing rules into sub-rules and choosing matching rules
3. Determining the priority sub-rule
4. Order of applying actions according to selected priority rules

The article also includes an example of applying a policy.

**1. Dividing events to sub-events**

During processing the event, the System divides it into sub-events:

1. For events related to transfer rules: by a pair of keys "Sender" - "Recipient".
2. For events related to copy rules: by the key "Sender".
3. For events related to clipboard rules: by the key "Persons".
4. For events related to storage rules: by a pair of keys "File owners" - "Who has access to file".

If any attribute of the event gets multiple values (for example, multiple recipients of SMTP messages), the System treats this event as a combination of several sub-events with unique attribute values.

For example, if an intercepted event has the following attributes:

| Sender | Recipient | Event type | Date |
|---|---|---|---|
| Person: Smith, Person: Johns | Person: Williams, Person: Johns, Person: Smith | Skype | 09:23 |

then the System divides it into the following sub-events:

| Sender | Recipient | Event type | Date |
|---|---|---|---|
| Person: Smith | Person: Williams | Skype | 09:23 |
| Person: Smith | Person: Johns | Skype | 09:23 |
| Person: Smith | Person: Smith | Skype | 09:23 |
| Person: Johns | Person: Williams | Skype | 09:23 |
| Person: Johns | Person: Johns | Skype | 09:23 |
| Person: Johns | Person: Smith | Skype | 09:23 |

**2. Dividing rules to sub-rules and choosing appropriate sub-rules**

Each rule of opearting policy is divided into sub-rules by the following keys:

1. For transfer rules: by a pair of keys "Sender" - "Recipient".

   > **Note:**
   >
   > If the **Direction of route** parameter has **In both directions** value, then a pair of keys "Recipient" - "Sender" will be added.

2. For copy rules: by the key "Sender".
3. For clipboard rules: by the key "Persons".
4. For storage rules: by a pair of keys "File owners" - "Who has access to file".

For example, the following rules:

| Sender | Direction | Recipient | Event type | Date | Reaction |
|---|---|---|---|---|---|
| Group: Lawyers, The Person: Smith, Person: Johns | -> | Group: Marketing, Person: Williams | Mail on Client | 08:00-20:00 | Notify: Thomas<br>Violation level: Low |
| Group: Logistics | -> | Group: Sales, Group: Delivery | Skype | 10:00-19:00 | Notify: Johns<br>Violation level: Medium |
| Group: Financial | -><br><- | Group: Lawyers, Group: Sales | | | Notify: Miller<br>Violation level: High |

are divided into the following sub-rules:

| Sender | Direction | Recipient | Event type | Date | Reaction |
|---|---|---|---|---|---|
| Group: Lawyers | -> | Group: Marketing | Mail on Client | 08:00-20:00 | Notify: Thomas<br>Violation level: Low |
| Group: Lawyers | -> | Person: Williams | Mail on Client | 08:00-20:00 | Notify: Thomas<br>Violation level: Low |
| Person: Smith | -> | Group: Marketing | Mail on Client | 08:00-20:00 | Notify: Thomas<br>Violation level: Low |
| Person: Smith | -> | Person: Williams | Mail on Client | 08:00-20:00 | Notify: Thomas<br>Violation level: Low |
| Person: Johns | -> | Group: Marketing | Mail on Client | 08:00-20:00 | Notify: Thomas<br>Violation level: Low |
| Person: Johns | -> | Person: Williams | Mail on Client | 08:00-20:00 | Notify: Thomas<br>Violation level: Low |
| Group: Logistics | -> | Group: Sales | Skype | 10:00-19:00 | Notify: Johns<br>Violation level: Medium |
| Group: Logistics | -> | Group: Delivery | Skype | 10:00-19:00 | Notify: Johns<br>Violation level: Medium |
| Group: Financial | -> | Group: Lawyers | | | Notify: Miller<br>Violation level: High |

| | | | | | |
|---|---|---|---|---|---|
| Group: Financial | -> | Group: Sales | | | Notify: Miller<br>Violation level: High |
| Group: Lawyers | -> | Group: Financial | | | Notify: Miller<br>Violation level: High |
| Group: Sales | -> | Group: Financial | | | Notify: Miller<br>Violation level: High |

Then, for each sub-event, the System chooses sub-rules whose conditions match the sub-event (for more details on rule attributes, see "Rule of Transfer", "Rule of Copying", "Rule of Placement", and "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:<br>• Sender (for transfer and copy rules)<br>• Recipient (for transfer rules)<br>• Person (for clipboard rules)<br>• File owners/Who has access to file (for placement rules) | 1 | does not apply |
| If the attribute is not filled:<br>• Event type (for all rules)<br>• Day of the week (for transfer, copy, and clipboard rules)<br>• Time (for transfer, copy, and clipboard rules)<br>• Computer (for transfer, copy, and clipboard rules)<br>• Storage (for placement rules)<br>• Terminal session (for clipboard rules)<br>• Source-application/Reciever-application (for clipboard rules)<br>• Resource (for copy 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:
>
> ```
> iwtm restart kicker
> ```
>
> Then you need to create other policies anew (see "Creating Data Protection Policy", "Creating Data Protection Policy on Agents", and "Creating Person Control Policy").

### Data Protection Policy

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

Default policies have the following attribute values:

| Attribute | Value |
|---|---|
| Policy name | <Name of the catalogue of protected objects> |
| Status | Active |
| Period of activity | Not limited |
| Type of objects of research | <Name of the catalogue of protected objects> |

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

Each policy contains the following rules:

**Rules of transfer**

1. *A rule that regulates transferring confidential data outside the company perimeter.*
   **If** an employee sends traffic of any type outside the company perimeter any day of the week,
   **Then** the System performs the following actions:

- sets the *Allowed* value to the *Verdict* attribute of the event;
- sets one of the following values to the *Violation level* attribute of the event:
    - *High* - for the following catalogues of protected objects: Security label, Personal data;
    - *Low* - for the following catalogues of protected objects: Law, HR, IT;
    - *Medium* - for all other catalogues of protected objects;
- sets the *None* value to the *Status* attribute of the person who sends the traffic.

2. *A rule regulating the transfer of confidential data by heads of the company*.
   **If** an employee from the VIP group sends traffic of any type to any recipient any day of the week,
   **Then** the System performs the following actions:
    - sets the *Allowed* value to the *Verdict* attribute of the event;
    - sets the *None* value to the *Violation level* attribute of the event;
    - sets the *VIP* tag to the event.

**Rules of copying**

*A rule that regulates copying confidential data to removable devices*.

**If** an employee copies confidential data related to any category to 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 catalogues of protected objects: Security label, Personal data;
    - *Low* - for the following catalogues of protected objects: Law, HR, IT;
    - *Medium* - for all other catalogues of protected objects;
- sets the *None* value to the *Status* attribute of the person who sends the traffic.

**Rules of placement**

*A rule that regulates storing confidential data. The rule is added only for the policies with the following protected data: Security Label or Personal Data catalogues of protected objects.*

**If** a person stores protected data in any location,
**Then** the System performs the following actions:

- sets the *High* value to the *Violation level* attribute of the event*;*
- sets the *None* value to the *Status* attribute of the person who owns the data*.*

## Person Control Policy

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

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

Policy Rules

*The rule that regulates transferring data by persons with Under Supervision status.*

**If** a person with the *Under supervision* status sends traffic of any type to any recipient,
**Then** the System sets:

- the *Allow* value to the *Verdict* attribute of the event;
- the *For consideration* value to the *Tag* attribute of the event.

## Policy that Regulates Transferring Password-Protected Data

By default, the System has a policy that regulates transferring password-protected data.

The default policy has the following attribute values:

| Attribute | Value |
|---|---|
| Policy type | Data protection policy |
| Policy name | Password-protected data |
| Status | Active |
| Period of activity | Not limited |
| 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. Specify the policy attributes:
   - Name;
   - Description;
   - Status;
   - Period of action.

> **Important!**
>
> When you fill the **Validity period** attribute, consider the possible time zone difference between branches of your organization. The time of interception for the event is the local

time on the server which intercepts data. If the local time of interception does not fall within the specified range, the policy does not apply to the event.

4. To add protected data to the policy, click **Select**.

> **Note:**
>
> If you do not select any protected data, then the policy will apply to any data.

5. In the window that appears, set the check boxes next to desired values. Protected data may include protected objects, their catalogs, and file formats.
   For file formats, you can also set an additional restriction on the file size (in bytes) and specify the signs as follows:
   - encrypted;
   - merged;
   - signature and extension are incompatible.

> **Warning!**
>
> If protected data of several types are specified for the policy, then for triggering the policy rules (see "Rules and their Viewing Form"), it is necessary that the intercepted event should contain violations of each type.
> For example, a catalog of protected objects 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.

6. After you have selected protected data, click **Save**.
7. Add rules to the policy (see "Creating Rules").
8. To save the new policy, in the policy creation form, click **Save**.

**To edit the policy:**

1. Select the desired policy in the list.
2. In the right part of the workspace, edit the necessary parameters.
3. To change the protected data, in the **Protected data block**, click **Select** and then click **Save**.
4. Click **Save** in the policy edit form.

**To delete the policy**, in the right upper corner of the policy, click ✖ and confirm the action in the confirmation window.

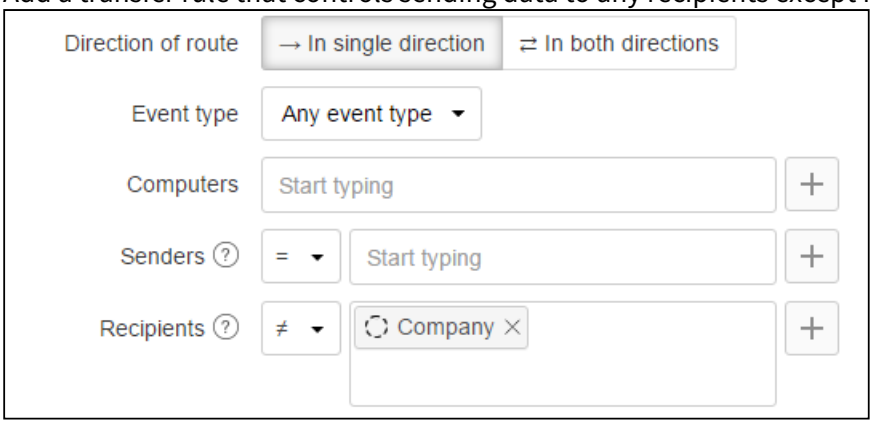
Examples of tasks where a data protection policy can be used are given in the "Examples of Using Data Protection Policy" article.

## Examples of Using Data Protection Policy

***Example 1:***

It is required to control transferring the company statute outside the company which includes sending the document by email or copying it to removable devices. For this:

1. Create a data protection policy and name it *Protection of transferring company statute*.
2. Specify the *Company statute* protected object as protected data.
3. Add a transfer rule that controls sending data to any recipients except for the *Company* perimeter.




4. Specify what actions to perform if the rule is triggered (e.g., assign *Low* violation level to the event).
5. If in addition, you want to control employees under the supervision, add one more transfer rule and specify the *Employees under supervision* group as senders (see "Creating Group of Persons or Computers").
6. Specify what actions to perform if the rule is triggered (e.g., assign *Medium* violation level and *For consideration* tag to the event).
7. To control copying the document to a removable device, add a copy rule to the policy.

The System will detect a violation of the data protection policy when:

- an email whose body or attachment contains data related to the *Company statute* protected object is sent outside the *Company* perimeter;
- a file with information on the *Company statute* protected object is copied to a removable device.

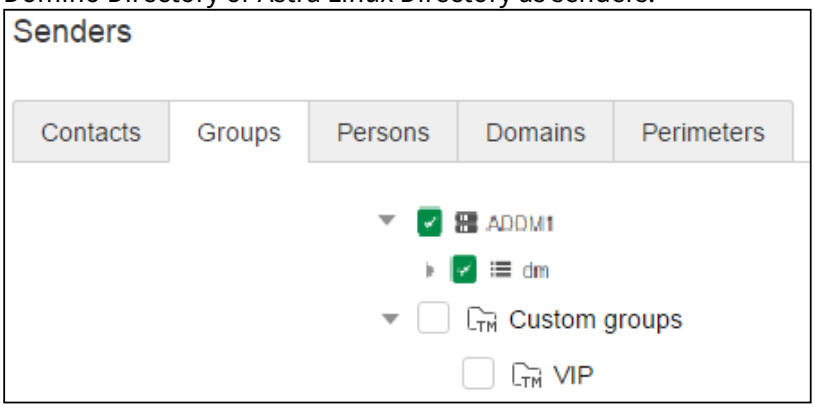
***Example 2:***

It is required to identify employees who visit job search sited. For this:

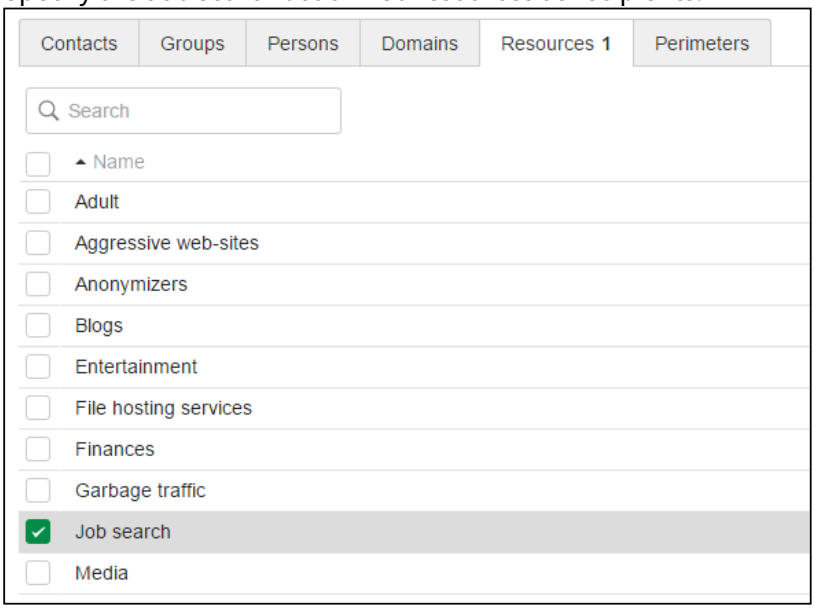
1. Create a data protection policy and name it *Identifying disloyal employees*.

> **Tip**
>
> Add the policy description to easily identify it in the policy list. For example, "Identifying employees who send requests to job search sites".

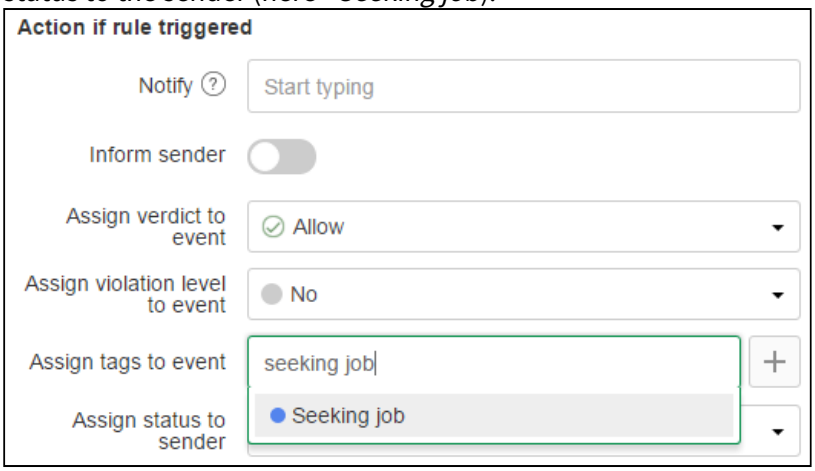
2. Add a transfer rule and specify the group of company employees imported from Active Directory, Domino Directory or Astra Linux Directory as senders.




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.

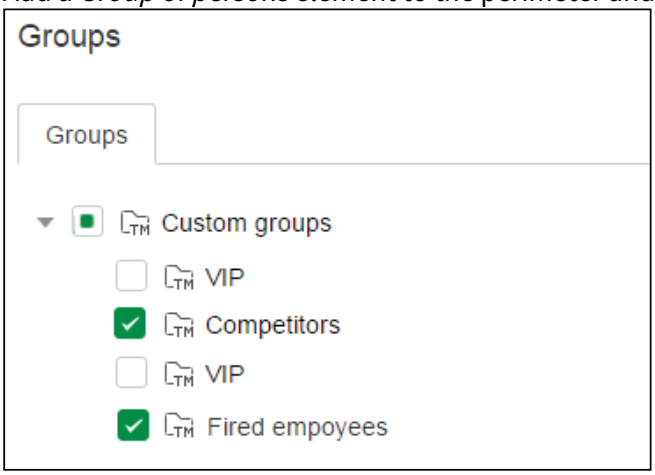
***Example 3:***
It is required to identify employees who communicate with undesired destinations, i.e., fired employees, competitors, etc.

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.

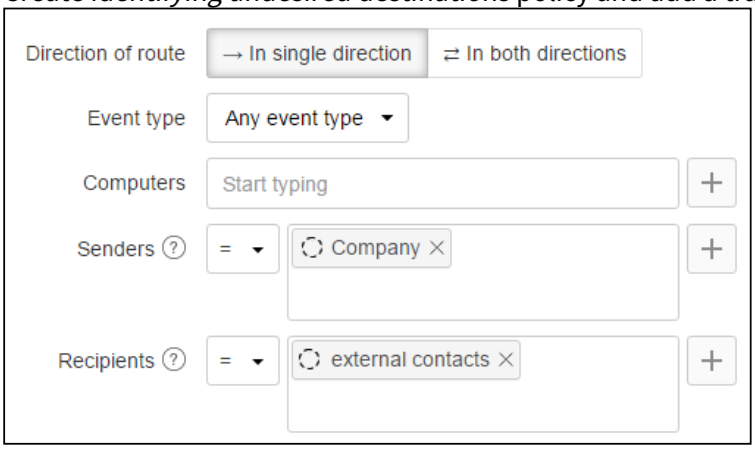
> **Note:**
>
> You can add separate person contacts or create user groups, e.g., *Fired employees* and *Competitors*. This example illustrates creating a perimeter based on user groups.

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. Specify the policy attributes:
   - Name;
   - Description;
   - Status;
   - Period of action.

**Warning!**

When you fill the **Validity period** attribute, consider the possible time zone difference between branches of your organization. The time of interception for the event is the local time on Device Monitor agent. If the local time of interception does not fall within the specified range, the policy does not apply to the event.

4. To add protected data to the policy, click **Select**.

**Note:**

If you do not select any protected data, then the policy will apply to any data.

5. In the **Choose protected data** window that appears, set checkboxes next to desired values. Protected data may include:
   - **Protected objects**
     You can select protected objects that contain only categories and text objects.
   - **Catalogues of protected objects**
     From selected catalogues, 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 (in bytes) and specify if the policy should apply to all files or in accordance with signs as follows:
   - encrypted;
   - file signature and extension do not match.
     If **Encrypted** option is selected, then the policy is triggered only if a file is encrypted or the System failed to determine the file format.

**Warning!**

If protected data of several types are specified for the policy, then for triggering the policy rules (see "Rules and their Viewing Form"), it is required that the intercepted object should contain violations of each type.
For example, a catalogue of protected objects and several file formats are specified as protected data for a policy. In this case, for the policy to be triggered, it is necessary that intercepted data should contain at least one protected object from the specified catalogue and at least one specified file format.

6. After you have selected protected data, click **Save**.
7. Add rules to the policy (see "Creating Rules").
8. To save the new policy, in the policy creation form, click **Save**.

**To edit the policy:**

1. Select the desired policy in the list.
2. In the right part of the workspace, edit the necessary parameters.

3. To change the protected data, in the **Protected data block**, click **Select** and then click **Save**.
4. Click **Save** in the policy edit form.

**To delete the policy**, in the right upper corner of the policy, click  and confirm the action in the confirmation window.

***Example:***

If you want the System to assign the *Block* verdict and the *Medium* violation level to the event in case of uploading data to cloud storages, take the following steps:

1. Create a data protection policy on agents.
2. Add a copy rule (see "Creating Rules").
3. In the rule attributes (see "Rule of Copying"), set the value of the **Event type** attribute to *Cloud storage*.
4. In the **Resource** field, specify cloud storages uploading data to which should be blocked.
5. In the **Actions when the rule is triggered** block, set the following values to the attributes:
   - to the **Assign verdict to the event** attribute - the *Block* value;
   - to the **Assign violation level to event** attribute - the *Medium* value.

For details about policy creating specifics, see "Intercepting Features and Restrictions when Copying Files (Data Protection Policy on Agents)".

## 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.

**To edit the policy:**

1. Select the desired policy in the list.
2. In the right part of the workspace, edit the necessary parameters.
3. To change the protected data, in the **Protected data block**, click **Select** and then click **Save**.
4. Click **Save** in the policy edit form.

**To delete the policy**, in the right upper corner of the policy, click and confirm the action in the confirmation window.

You can also add person control policies directly from **Persons** (see "Persons") and **Statuses** (see "Statuses") sections.

**To add a policy for a group of persons or computers**:

1. Go to the **Persons** section.
2. Select the desired group in the list.
3. On the toolbar in the left part of the workspace, click .

**To add a policy for selected persons or computers**:

1. Go to the **Persons** section.
2. Select the desired person or computer. To select multiple elements, use Shift or Ctrl keys.
3. On the toolbar in the right part of the workspace, click and, in the drop-down list, select **Create policy**.

**To add a policy for a selected status:**

1. Go to **Lists**->**Statuses** section.
2. Select the desired status from the list.
3. On the toolbar, click .

***Example:***

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

1. Go to the **Policies** section and create a person control policy named *Smith*.
2. Create a rule for the policy *Smith* and set the following values to the attributes:
   - attribute **Intercept with the violation level** - *High* value;
   - attribute **Send notifications** - *example@company.com* value (for details, see “Configuring Notifications in Rules");
   - attribute **Assign verdict** - *Allow* value;

- attribute **Set status** - *Under supervision* value.

3. Save the policy.

### 4.8.6 Creating Rules

**Reference information:**

Each policy can include one or more rules.

If the policy is triggered on the interception object, then, depending on the number of triggered rules, the following variants are possible:

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

> **Note:**
>
> If the interception object triggers multiple policies, and each policy has its own rules, then the System chooses the action with the highest priority and performs it (on the order of selecting priorities, see "General Information on Policies"). Actions that do not contradict other actions are performed in full.

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

**Solution:**

1. Go to the **Policies** section.
2. Select the required policy in the list or create a new policy (see "Creating Data Protection Policy", "Creating Data Protection Policy on Agents", and "Creating Person Control Policy").
3. Add a rule in one of the following ways:
   - on the tab of the selected rule group, click **Add rule**.
   - in the right upper corner of the form, click **Add rule**, and, from the drop-down list, select the desired rule.
4. Configure the rule using a form on the right part of the workspace (see “Rules and their Viewing Form").
5. In the **Actions when the rule is triggered** block, specify what actions the System should perform when the rule is triggered (see "Determining System Response to Policy Violations").
6. Click **Save**.

**To edit the rule:**

1. Select the required policy in the list.
2. In the policy tile, select the required rule group. Rules are grouped on the following tabs:
   - **Transfer**, **Copy**, **Placement**, **Application activity, and File operations** - for data protection policies;
   - **Transfer, Copy** - for data protection policies on agents;

- **Rules** - for person control policies.

3. The policy tile will display the list of rules of the selected group. Left-click the desired rule in the list.
4. The rule edit form will open in the right part of the workspace. Edit the necessary fields, then click **Save**.

**To delete the rule**, in the right upper corner of the rule tile, click ✕ and confirm the action in the confirmation window.

***Example:***

If a person transfers files included in the *Strictly confidential* protected object on Saturdays and Sundays, the System should assign the *Sending confidential data on weekends* tag to the event and set the *Medium* violation level:
For this:

1. Create the *Sending confidential data on weekends* tag (see "Managing Tags").
2. Create a data protection policy for the *Strictly confidential* protected object (see "Creating Data Protection Policy").
3. Add a transfer rule and assign the *Saturday* and *Sunday* values to the **Days of rule activity** attribute.
4. In the **Actions when the rule is triggered** block, assign the following values to attributes:
   - **Set violation level** attribute - *Medium* value;
   - **Tags** attribute - *Sending confidential data on weekends* value.

## 4.8.7 Determining System Response to Policy Violations

**Reference information:**
For each policy, you can specify actions the System performs in case of the rule violation. For this, choose actions in the **Actions when the rule is triggered** area while creating or editing the rule (see "Creating Rule").
Available actions are determined by the rule type:

| **Action** | **Data protection policies** | | | | **Data protection policies on agents** | | **Person control policies** |
|---|---|---|---|---|---|---|---|
| | **Transfer rule** | **Copy rule** | **Placement rule** | **Clipboard rule** | **Transfer rule** | **Copy rule** | **Person control rule** |
| Send notification | Available | Available | Available | Available | Available | Available | Available |
| Assign verdict to event | Available | Not available | Not available | Not available | Available | Available | Available |
| Assign violation level to event | Available | Available | Available | Available | Available | Available | Available |
| Assign tags to event | Available | Available | Available | Available | Available | Available | Available |

| 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 status to senders | Available | Available | Available | Available | Available | Available | Available |
| Delete event | Available | Available | Available | Available | Not available | Not available | Available |

A detailed description of actions:

| Action | Description |
|---|---|
| Send notification | Allows you to specify which notifications to send if the rule is triggered. To configure sending notifications, click + next to the field. In the dialog box that opens, choose a notification from the list or create a new one. For details, see "Configuring Notifications in Rules".<br>A selected notification template should match the verdict specified in the rule.<br>**Note:** If after the rule is created, the person or the person's e-mail are deleted from the System (on managing user accounts, see *"InfoWatch Traffic Monitor. Administration Guide"*, "Users" section), a notification will not be sent to this person. |
| Assign verdict to event | The event is assigned a verdict which is a preliminary System decision concerning possible violation of the security policy. Possible values:<br>• **Allow** - the object is not a potential violation and can be delivered to senders.<br>• **Block** - the object is a potential violation. In the "Block" mode, the object delivery is blocked.<br>• **Quarantine** (for data protection policies on agents, this verdict is unavailable) - the user should make a decision whether the object is a violation or not. In the "Block" mode, the object delivery is postponed until the user decision is made. Depending on the user decision, the verdict value will change either to **Allowed** (in this case, the message is delivered) or to **Blocked** (for details, see "Making Decision on Object"). Dispatching messages is available only for SMTP letters when the System operates in the inline mode (for details see the document "*Infowatch Traffic Monitor. Installation Guid*e". |
| Assign violation level to event | A violation level will be assigned to the event. Possible values: **High**, **Medium**, **Low**, **No violation**. |

| Action | Description |
|---|---|
| Assign tags to event | The event will be assigned tags, for example, **Under supervision**. For details, see "Tags". |
| Assign status to senders | The security policy violators will be assigned a specified status, for example, **Under supervision**. For details, see "Statuses". |
| Delete event | The event will not be saved to a database and actions specified in the rule will not be performed either. |

**See also:**

- Creating Rule
- Configuring Notifications in Rules

## 4.8.8 Configuring Notifications in Rules

When you create or edit a rule, you can specify who should receive notifications if the rule is triggered.

For this:

1. In the **Actions when the rule is triggered** area, in the **Send notifications** field, click .
2. In the **Choosing mail notifications** dialog box, set checkboxes next to selected notifications. You can choose several notifications to be sent to different recipients.

   > **Note:**
   >
   > If there are no notifications in the System, a corresponding message is displayed. In this case, you can create a notification by clicking **Create notification** in the message window.

3. If there is no appropriate notification in the list, you can create a new notification. For this, click **Create a new one** in the left upper corner of the window.

   > **Note:**
   >
   > To edit a notification from the list, click the notification name.

> **Note:**
>
> You can also create notifications from the **Administration** -> **Notifications** section (see "Configuring Notifications").

4. In the notification create/edit form, specify the notification parameters as described in "Creating Notification".
5. To return to the notification list, click **Back to notifications** in the left upper corner of the form.
6. When you have chosen all required notifications, click **Save**.

> **Important!**
>
> A verdict in the notification should match the verdict in the rule. Otherwise, the notification will not be sent.

### 4.8.9 Determining System Default Response

**Reference information:**
If after applying the policy, there are sub-events with no matching rules, the System performs default actions (on dividing events into sub-events, see "General Information on Policies"). Default actions are specified by the user.

> **Note:**
>
> If default actions are not specified and none of the rules is triggered on the interception object, the policy is not triggered on this interception object either.

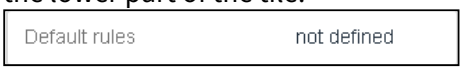
**Purpose:**

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

> **Note:**
>
> Default actions can only be specified for data protection policies and data protection policies on agents.

**Solution:**

1. Go to the **Policies** section.
2. On the left side of the workspace, left-click the target policy.
3. In the policy tile, select the target tab (**transfer**, **copying**, **placement** or **clipboard**) and left-click the lower part of the tile:



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

**Additional information:**

For *Web message* and *Mail in Browser* event types, a default rule can be false triggered. Such a situation may arise when:

The System contains a rule that regulates data transfer from person A to person B. If person A sends data to person B via a website, the System creates an event which is divided into two sub-events:

| Sender | Recipient | Protocol |
|---|---|---|
| Person A | Person B | HTTP |
| Person B | Website domain | HTTP |

Since the route **Person A**->**Website domain** is not specified in the policy rules, the default actions are executed.

To avoid false triggering of the default rule for *Web message* and *Mail in Browser* event types, do either of the following:

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

***Example:***

You want the System to assign the *Under supervision* status to the card of the person who copies data if:

- the copied data from a *State secret* protected object, and
- no copy rules are triggered.

For this:

1. Create a data protection policy for the *State secret* protected object (see "Creating Data Protection Policy").
2. Start configuring default policy actions.
3. In the only **Actions** block, set the *Under supervision* value to the **Set status** attribute.

## 4.8.10 Filtering the List of Policies

**Purpose:**
Filter the list of policies in case of a large number of policies.

**Solution:**

1. Go to the **Policies** section.
2. In the left part of the workspace, click **Filter**.
3. In the **Filter settings** area, specify filtering criteria in one of the fields or in both of them:
    - **Filter by policy name** - start typing and select the name of the needed policy (repeat to select several policies)
    - **Filter by objects of research** - start typing and select the name of needed object (repeat to select several objects)
      For data protection policies and data protection policies on agents, you can specify the following objects of research:
        - catalogue of protected objects;

- protected object;
- file format.

For person control policies, you can specify the following objects of research:

- person;
- group of persons;
- status.

4. Click **Apply**.

## 4.8.11 On Data Protection Policy on Agents

**Why do you need data protection policies?**

Policies of this type apply first and directly on DM agents. It does not apply on TM. The policy is a tool of a security officer who is using it to control activity on workstations and prevent leaks of confidential data.

The policy controls such actions as data transfer (Internet activity, Mail on Client, Mail in Browser) and data copy (FTP, cloud storages, external storages).

**How the policy works:**

1. To control traffic on workstations the security officer creates and configures the policy in TM console. The policy is then deployed on workstations.
2. A person performs illegitimate actions (e.g., sends confidential data via email in a browser).
3. DM agent on the workstation analyzes the data being transferred.
4. If the policy is triggered, DM agent performs actions specified in the policy (e.g. blocks sending if Block verdict is specified in the rule). Then DM sends the event and its analysis to TM, and the user gets the following message (if configured) «According to security policy the data transfer is blocked as confidential information has been detected in the data». The action or process initialized by the user is not complete.
5. TM receives the event, processes and analyzes it.
6. In the console, the security officer sees the intercepted event and its analysis results got from DM agent and TM server.
7. The security officer analyzes the information and takes necessary actions.

**What do you need to create a policy?**

- Add policy rules.
- Select protected data. This can be:
  - protected objects containing text objects, categories and terms and catalogues of protected objects;
  - file formats.
    If no protected data is selected, the policy is applied to actions with any data.
- Specify a period during which the policy will apply (can be unlimited or have defined dates).

The following rules can be added: transfer rule, copy rule.

For details see Rules and their Viewing Form, Rule of Transfer, Rule of Copying.

## 4.8.12 On Data Protection Policy

**Why do you need data protection policies?**

Policies of this type apply in TM after data protection policies on agents. They allow you to monitor the following channels of data leaks:

- Messengers, SMS
- 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., tries to print a file with confidential data).
3. TM analyses received data.
4. If the policy is triggered (policy rules are violated), an event is created. The message is sent to the recipient (its shadow copy is created in TM).
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.

### 4.8.13 On Person Control Policy

**Why do you need data protection policies?**

Policies of this type can be used if the security officer needs to monitor actions of a particular person.

**How the policy works:**

1. The security officer configures a person control policy and specifies the controlled person.
2. If actions of this person trigger the policy rules, information about these actions is sent to TM.
3. TM analyses the received information.
4. The security officer sees the event with analysis results and takes necessary actions.

**What do you need to create a policy?**

- Add person control rule (see "Person Control Rule").
- Specify controlled objects (they can be persons, person groups, or statuses).

> **Note:**
>
> The policy applies to event initiators only. Traffic recipients are not controlled by this policy.

## 4.9 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" article contains examples of using reports for monitoring user activities and investigating incidents.

**See also:**

- "Reports Section" - on the section where you can manage reports

### 4.9.1 Creating and Viewing Reports

**Purpose:**
Create a report to view statistics on interception objects.

**Solution:**

1. Go to the **Reports** section (see "Reports Section").
2. If you want to create a report within a folder, select a folder in the list or create a new folder (see "Creating Folder with Reports").
3. Create a report within a selected folder or in the root (see "Creating Report").
4. Add widgets to the report (see "Creating and Configuring Widget").
5. To run the report execution, select the report in the list and click  on the toolbar or the **Run report** button in the report viewing form (or you can use **Save and run** button in the report creation form).
6. To view results of an earlier executed report, select the report in the list in the left part of the workspace. Besides, you can view results of the report execution for different dates and save selected report versions to your computer (for details, see "Viewing Ready Reports").

If necessary, you can copy or move an earlier created folder or report.

**To copy a folder** and its reports:

1. Select the folder in the list.
2. On the toolbar in the left part of the workspace, click  **Copy**.

If you are trying to copy a subfolder and you have full access to the parent folder, then the copy will be added to the same folder as the copied folder. If you don't have full access to the parent folder or you are copying a top-level folder, then the copy will be added to the root of the folder tree.

**To copy a report:**

1. Select the report in the list.
2. On the toolbar in the left part of the workspace, click  **Copy**.

If you are copying a report inside a folder and you have full access to the folder, then the copy will be added to the same folder as the copied report. If you don't have full access to the folder or you are copying a top-level report, then the copy will be added to the root of the folder tree.

**To move a folder**, select it in the list and holding the left mouse button move it to the desired location, then release the mouse button.

> **Note:**
>
> To move a folder, you need to have full access both to the folder you are moving and to the destination folder. If the folder includes reports, then you also need full access to the reports. For details, see the table below.

**To move a report**, select it in the list and holding the left mouse button move it to the desired location, then release the mouse button.

> **Note:**
>
> To move a report, you need to have full access both to the report and to the destination folder. For details, see the table below.

The table below shows what access rights are needed to manage reports:

| Action | Access rights | | | |
|---|---|---|---|---|
| | View and execute folder | Full access to folder | View and execute report | Full access to report |
| View the folder | + | | | |
| Edit the folder attributes (name, description, access rights) | + | + | | |
| Copy the folder | + | | | |
| Create a new item (a report or a subfolder) in the folder | + | + | | |
| Move an empty folder to a different folder | + | + | | |
| Move a folder which includes at least one report | + | + | + | + |

| | | | | |
|---|---|---|---|---|
| Delete an empty folder | + | + | | |
| Delete a folder which includes at least one report | + | + | + | + |
| View and run the report | + | | + | |
| Edit the report parameters (including access rights) | + | | + | + |
| Copy the report | + | | + | |
| Move the report to a different folder | + | | + | + |
| Delete the report | + | | + | + |

**See also:**

- Creating Folder with Reports
- Creating Report
- Examples of Using Reports

## Creating Folder with Reports

**Purpose:**
Create a folder for grouping reports with a common theme.

**Solution:**

1. Go to the **Reports** section.
2. In the list of folders and reports in the left part of the workspace, choose where to create a folder. You can create a folder in the root or inside an existing folder.

> **Note:**
>
> If you do not have sufficient rights to create items within a selected folder, a warning will be displayed. In this case, you should find a different location for your folder.

3. Click + and, in the drop-down list, select **Create folder**.
4. In the form that opens, enter the folder name.
5. Specify if access rights to the folder should be inherited for subfolders and reports. By default, the **Apply rights for related reports** option is deselected.

> **Note:**
>
> If you create a folder inside a folder with the **Apply rights for related reports** option enabled, then actions described in steps 5-6 are unavailable.

6. Specify who can access the folder and define access rights. For this:

a. Find required users in the list.

> **Tip.**
>
> To find required users, use the **Search** field.

b. Next to the user name, set the checkbox in one of the fields:
   - **View and execute access** - to provide access for viewing and copying the folder. Access rights to reports in the folder are specified when you create a query;
   - **Full access** - to provide full access to the folder.

> **Note:**
>
> To provide access to the folder to all users of the System, set a checkbox in the field with the required access level next to the **All users** value.

7. Click **Save folder**.

To edit the folder, click the button on the toolbar.

To delete the folder, click .

> **Note:**
> To edit or delete a folder, full access to the folder is required. If you can only view and execute the folder, then instead of button, button is displayed, and button is unavailable.

## Creating Report

**Purpose:**
Create a report that contains statistical data on interception objects.

**Solution:**

1. Go to the **Reports** section.
2. In the list of folders and reports in the left part of the workspace, choose where to create a report. You can create a report in the root or inside an existing folder.

> **Note:**
>
> If you do not have sufficient rights to create items within a selected folder, a warning will be displayed. In this case, you should choose a different location for the report.

3. Click and, in the drop-down list, choose **Create report**.

4. In the form that appears, specify required parameters (for more information, see "Report Creation Window").
5. On the **Widgets** tab, click **Add widget**.
6. In the **Widget Creation** window that opens, specify the widget parameters (for details, see "Managing widgets of reports") and click **Save**.
7. If necessary, add more widgets as described at step 6. When you are done, close the **Adding widget** window by clicking ✕ in the right upper corner.
8. Open the **Access** tab to specify who can access the report and define the access rights.

> **Important!**
>
> If you create a report in a folder with the **Apply rights for related reports** option enabled, then access rights for the report will be the same as for the folder. In this case, editing access right to the report is unavailable.

For this:

a. Find required users in the list.

> **Tip.**
>
> To find required users, use the **Search** field.

b. Next to the user name, set the checkbox in one of the fields:
   - **View and execute access** - to provide the user access to viewing, copying, and executing the report;
   - **Full access** - to provide the full access to the report.

> **Note:**
>
> To provide access to the report to all users of the System, set a checkbox in the field with the required access level next to the **All users** value.

9. Click:
   - **Save** - to save the report.
   - **Save and execute** - to save and execute the report.

You can also copy a previously created report. To do this:

1. Select a report in the list using the left mouse button.
2. On the toolbar in the left part of the workspace, click **Copy** (or click ⚙ in the right part of the workspace and, in the drop-down list, select **Copy**).

The copy will be added to the report structure at the same level as the report you have copied.

You can change the location of the report using drag-and-drop. To do this, select the required report in the list, press the left mouse button and move the report to the desired location holding the left mouse button pressed. Then release the mouse button.

**Warning!**

When moving a report to a folder, access parameters specified for the folder will be applied to the report being moved.

To edit the report, click  on the toolbar.

To delete the report, click  .

**Note:**

To edit, move, or delete a report, full access to the report is required. If you can only view and execute the report, then instead of  button,  button is displayed, and  button is unavailable.

## Creating and Configuring Widget

**Purpose:**
Create a widget for displaying statistics.

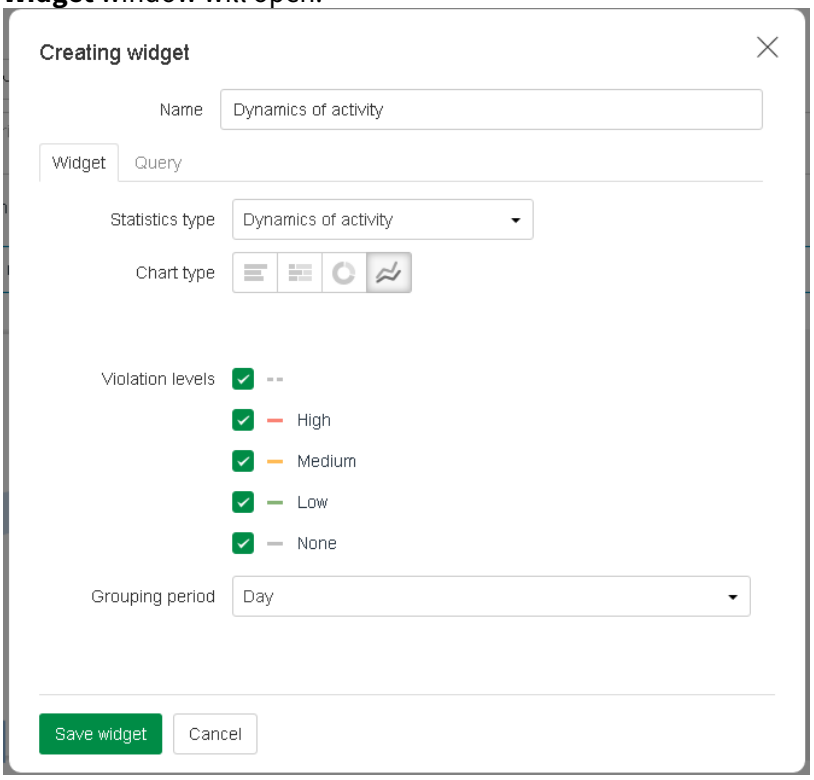
**Solution:**

1. Go to the **Reports** section.
2. In the left part of the workspace, select a report to which you want to add a widget or create a new report (see "Creating a report").

   **Note:**

   To add a widget to an earlier created report, switch to the report edit mode.

3. In the form that appears, open the **Widgets** tab and click **Add widget**. The **Creating Widget** window will open.




4. Fill in the required fields:
   a. In the **Name** field, enter the name of the widget.
   b. On the **Widget** tab, choose the type of statistics. Other settings (a chart type, the number of records, the grouping period, etc.) are available depending on the chosen type of statistics (for more details on the types of statistics, see "Widgets").
   c. On the **Query** tab, specify the parameters based on which events will be filtered (for more information about available settings, see "Queries").
5. Click **Save Widget**.

You can duplicate an earlier created widget to a different report. For this:

1. Switch to the edit mode of a report with the required widget.
2. In the upper-right corner of the desired widget, click and in the drop-down list select **Duplicate**.
3. In the report list in the left part of the workspace, select the report to which you want to duplicate the widget.

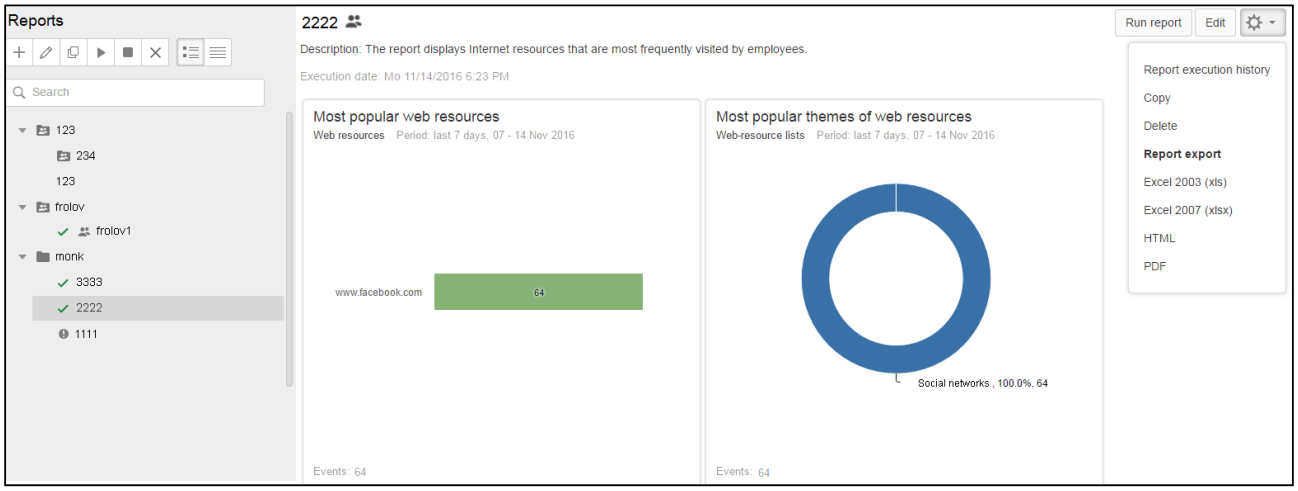
**Additional information:**

To edit or delete a widget, switch to the report edit mode and select the desired widget. Then:

- To edit the widget, in the upper-right corner of the widget, click and, in the drop-down list, choose **Edit**.
- To delete the widget, in the upper-right corner of the widget, click and, in the drop-down list, choose **Delete**.

## Viewing Ready Reports

**To view the last executed version of the report**, choose the required report in the list. Widgets for the selected report will be displayed in the right part of the workspace. Date and time of the report execution are displayed above the widgets.



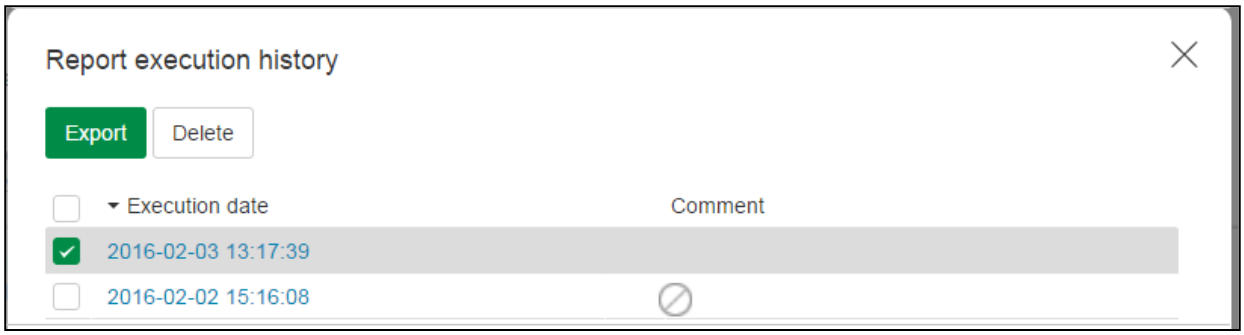

If you want to view events information about which is displayed in the widget, in the right upper corner, click and from the drop-down list, select **Go to events**. You will switch to the list of events in the "Events".

You can save the report as a file in one of the following formats:

- Excel 2003
- Excel 2007
- HTML
- PDF

**To export the report**, in the right upper corner, click and, in the drop-down list under the **Report export** caption, choose the desired format. A report in the selected format will be saved to you computer.

**To view report versions for other dates**, open the report execution history. For this, in the right upper corner, click and, in the drop-down list, choose **Report execution history**. In the window that opens, you can view information about the report execution.




For each report version, you can view the execution date and time and a comment field. To add a comment to a report version, double-click the field next to the selected version.

If the report execution was cancelled, icon is displayed next to the report version.

You can view required report versions, delete versions that are no longer needed, or save selected versions to a file.

**To view a report version**, click the row with the date and time of the report execution. Widgets for the selected report version will be displayed.

**To delete selected report versions:**

1. Select check boxes for the versions which you want to delete. To select all rows, select the check box in the header field.
2. Click **Delete**.

**To export selected report versions:**

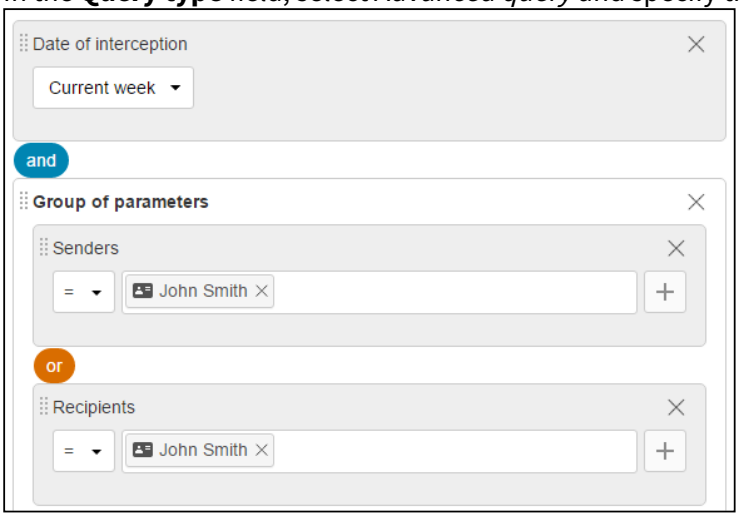
1. Select check boxes for the versions which you want to save as a file. To select all rows, select the check box in the header field.
2. Click **Export** and, in the drop-down list, choose the required format.: Excel 2007, Excel 2003, HTML, or PDF. A file in the specified format will be saved to your computer.

## 4.9.2 Examples of Using Reports

***Example 1:***
The employee John Smith is in the list of the most active violators of the week (statistics on the most active violators in displayed in the "Top Violators" widget). An investigation is required to get detailed information on activities of this employee. The investigation can be carried out in several steps.

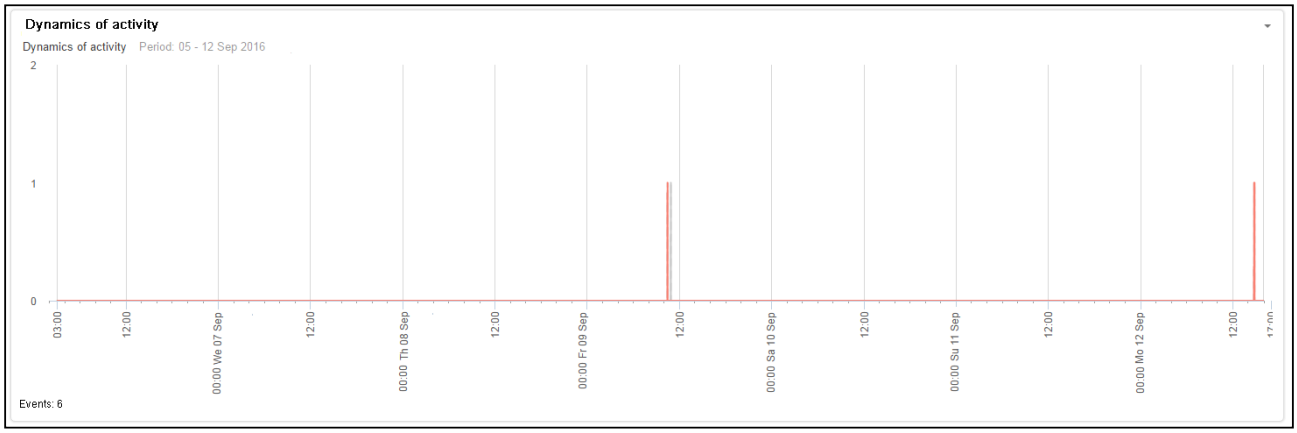
**Step 1**. Get information about the dynamics of violations. For this:

1. Create a report and add *Dynamics of activity* widget to it.
2. Open the **Query** tab of the widget.
3. In the **Query type** field, select *Advanced query* and specify the following conditions:



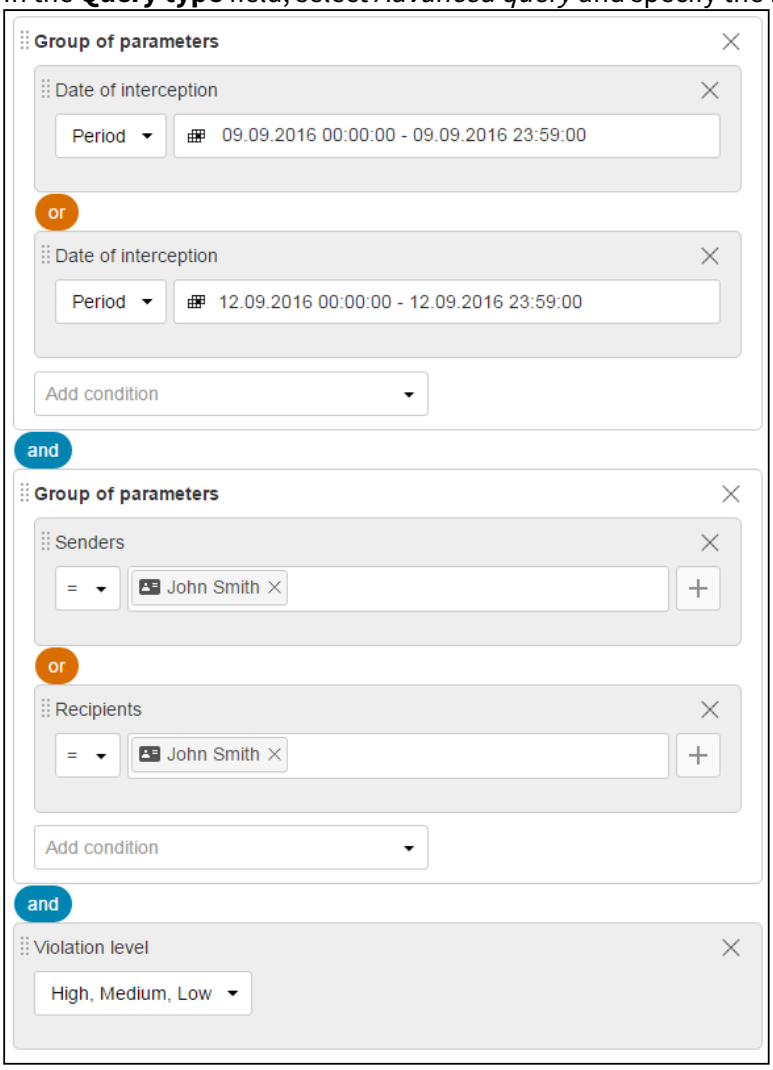

4. Save and run the report.

On the chart, you can see that the employee committed most violations on 09.09 and 12.09.



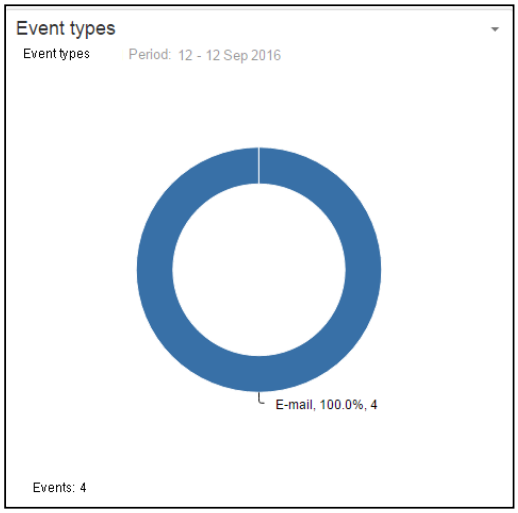

**Step 2**. Determine the channels through which the data was leaked. For this:

1. Add *Event types* widget to the created report.
2. Open the **Query** tab of the widget.
3. In the **Query type** field, select *Advanced query* and specify the following conditions:



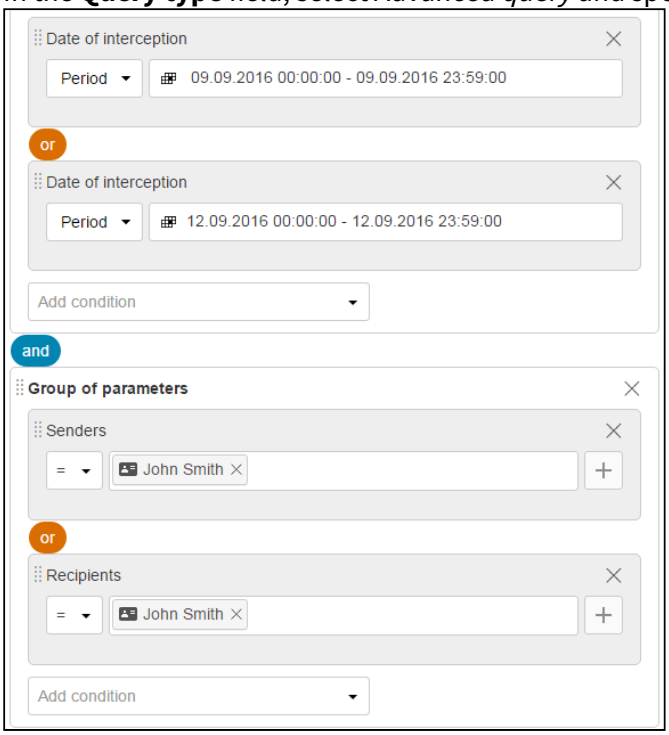

4. Save and run the report.

In the report, you can see, that most violations are related to sending data via email.




**Step 3**. Determine what protected objects were leaked. For this:

1. Add *Protected objects* widget to the created report.
2. Open the **Query** tab of the widget.
3. In the **Query type** field, select *Advanced query* and specify the following conditions:



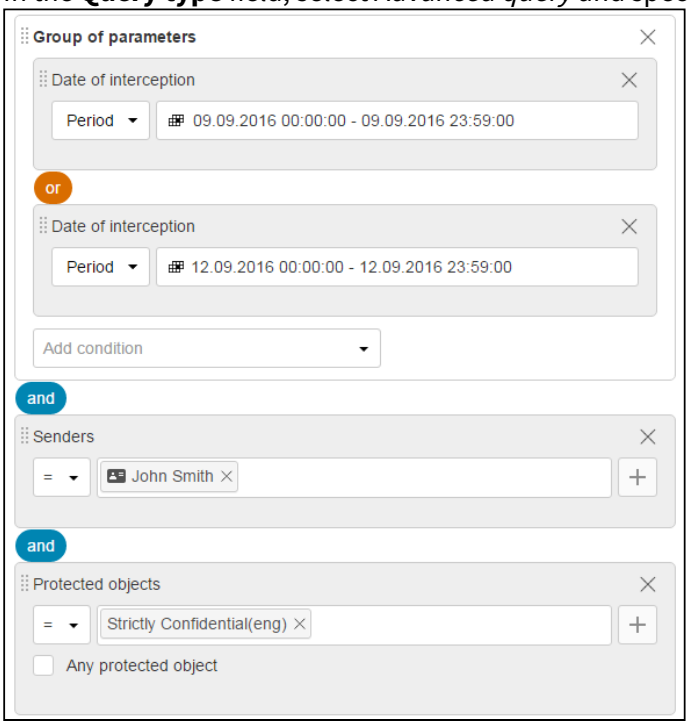

4. Save and run the report.

In the report, you can see, that the employee emailed documents included in the *Strictly confidential information* protected object.



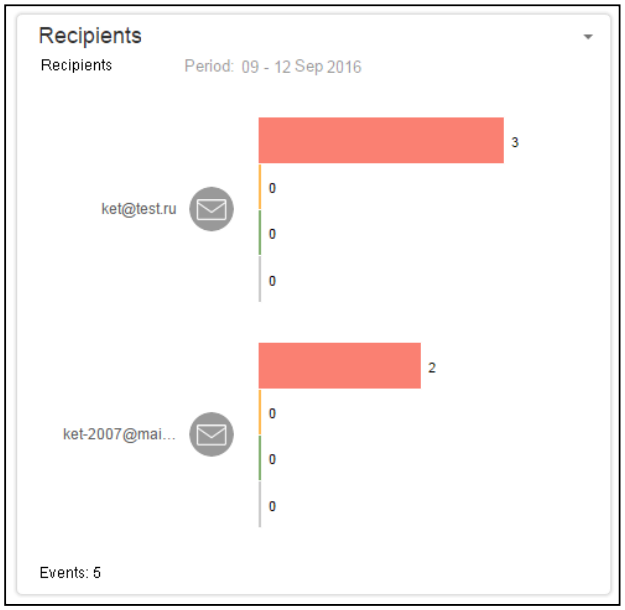

**Step 4**. Determine, to whom John Smith sent confidential data. For this:

1. Add *Recipients* widget to the created report.
2. Open the **Query** tab of the widget.
3. In the **Query type** field, select *Advanced query* and specify the following conditions:




4. Save and run the report.

In the report, you can see the emails to which confidential data was sent.



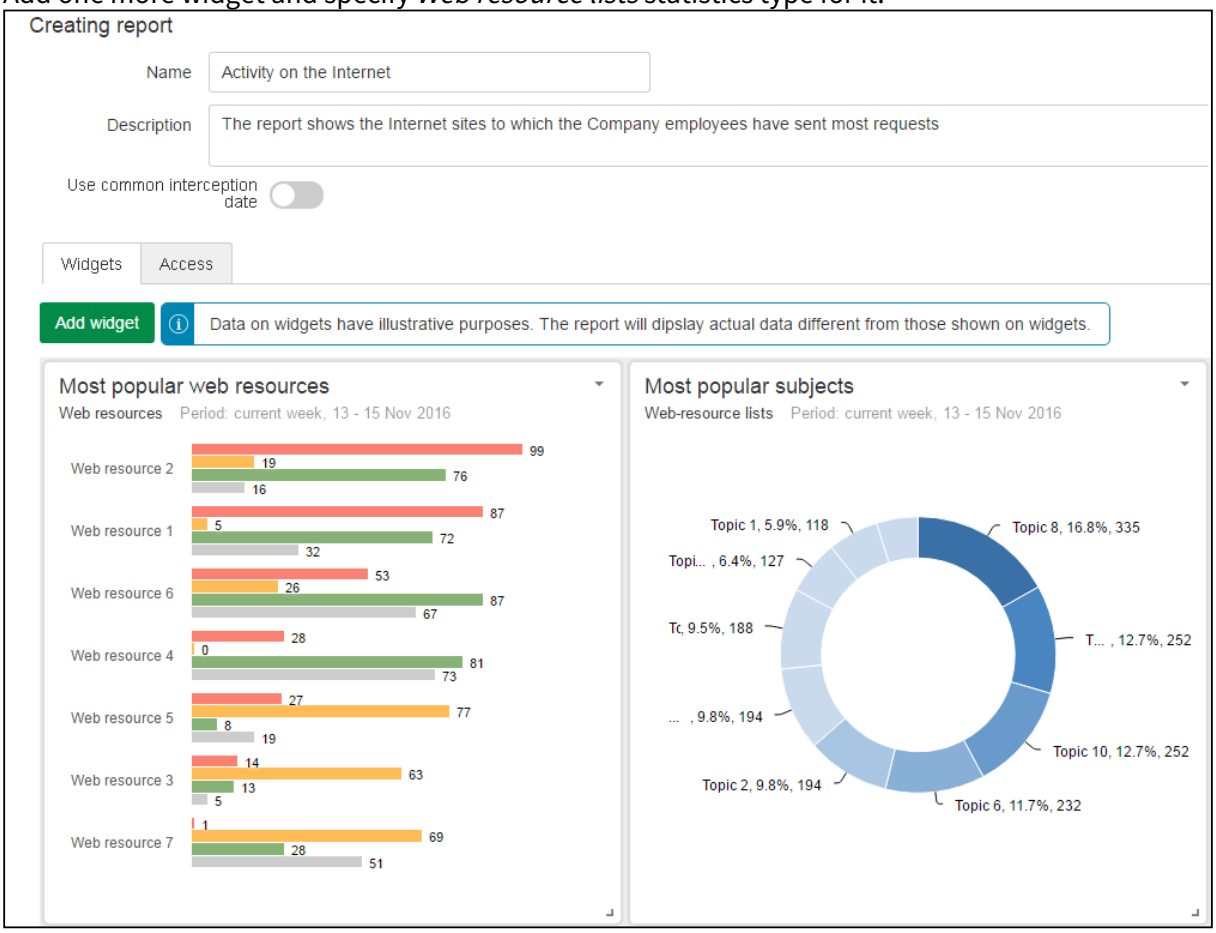

As a result of the investigation, you have determined when, through which channels, and to what recipients the violator leaked confidential data. Now you can easily find the needed events: for this, create a query and specify already known parameters in it (see "Creating Queries"). In the found events, you can see what exactly the violator leaked.

***Example 2:***

It is required to track the dynamics of attending web resources and the most popular subjects. For this:

1. Create *Activity on the Internet* report.
2. Add a widget and specify *Web resources* statistics type for it.

3. Add one more widget and specify *Web resource lists* statistics type for it.




4. On the **Query** tab, select the required period for each widget and specify additional parameters if necessary.
5. Save and run the report.

## 4.10 Administrating the System

The section is configured by the System administrator, except for the "Audit" and "Mail notifications" subsection operated by the security officer.

Administrating the System includes the following actions:

- Managing Integration with LDAP Catalogs
- Managing Licenses
- Managing System Users and their Roles
- Healthcheck
- Managing Services and Collecting Diagnostic Data
- Plugins
- User Actions Audit
- Integrity Monitoring
- Configuring Connection to Mail Server
- Configuring Notifications

## 4.10.1 Managing Integration with LDAP Catalogues

Configuring the synchronization with LDAP catalogues is performed in **Administration -> LDAP Synchronization** section.

> **Warning!**
>
> If you have Adblock Plus installed for the browser then you should disable this extension to provide correct operation of this web console section.

The toolbar is located in the left part of the **LDAP server** workspace.
Above the toolbar, you can find the list of servers for which synchronization with LDAP catalogues has been configured.
The toolbar contains a set of tools for working with the connection.
In the central part of the workspace, parameters for the selected connection, status and synchronization schedule are displayed:

Configuring integration with LDAP catalogues is described below:

- Creating Connection to Server
- Editing Connection to Server
- Deleting Connection to Server
- Running Synchronization with Server Manually

### Creating Connection to Server

**To create a connection to the server:**

1. Go to **Administration** -> **LDAP Synchronization**.
2. On the toolbar, click  **Create**.
3. Specify parameters for a new connection:

| Parameter | Description |
|---|---|
| **General parameters** | |
| Server name | Connection identifier used in the Management console<br>**Warning!** It is not allowed to change the server name between the last synchronization and System update |
| Server type | Indicates what kind of server is used: *Active Directory* or *Domino Directory* |
| Synchronization | • *Manual* - user starts synchronization manually<br>• *Automatic* - synchronization is performed according to schedule<br>**Important!** We recommend that the frequency of automatic synchronization with the Domino Directory server should be 10 minutes or more.<br>We recommend not running manual synchronization more ofter than once every 10 minutes. |

| Parameter | Description |
|---|---|
| Synchronization period | Type of synchronization repeating<br>• *Every N minutes*<br>• *Every N hours*<br>• *Every N days*<br>• *Every N weeks* |
| Retry parameters | Value of synchronization repeating period if *Automatic synchronization* is selected<br>***For example***, with the following values:<br>• *Synchronization period* – `Every N minutes`<br>• *Retry parameters* – `60 minutes`<br>the synchronization will be performed every 60 minutes |
| **Configuring connection** | |
| LDAP server | The IP address of the server whose LDAP catalogues are synchronized |
| Connection type | Selecting connection type with AD, DD or ALD that will be configured:<br>• Unsecured connection (LDAP)<br>• Secured connection using LDAP + StartTLS protocol<br>• Secured connection LDAPS (SSL)<br>**Warning!** Connection without using a certificate is not secure. When installing a secure connection, you can additionally load a file containing the certificate in .pfx format.<br>**Warning!** If the file that is being loaded contains several user certificates, the System will operate with the first of them and its private key. Correct work requires creating a file with one user certificate.<br>**Warning!** Synchronization using the secure connection is supported only for ActiveDirectory |
| Server certificate | Loading a certificate file in PEM format. |
| User certificate | Loading a certificate file in PEM format. When using a user certificate, it is necessary that you additionally load a file containing a private key of the user certificate |
| Private key of user certificate | Loading a file containing a key in PEM format.<br>**Note:** For details, see "Getting Client Certificate and Server Certificate". |
| Use Kerberos protocol | Indicates if Kerberos protocol is used for authentication (protocol of client and server mutual identification). For details, see "Specifics of LDAPS connection and synchronization using Kerberos protocol". |
| Global LDAP port | A port for connecting the global LDAP catalogue.<br>**Note:** This setting is available for Active Directory only. |
| LDAP port | Port for connecting a domain catalogue |

| Parameter | Description |
|---|---|
| Use global catalogue | Indicates if the global LDAP catalogue is used for synchronization<br>**Note:** This parameter is only available for Active Directory. |
| LDAP request | **Note:** the setting is required only for Active Directory.<br>Filtering attributes which are the full path to the specified catalogue. You can specify only one catalogue in the Active Directory or Domino Directory organizational structure.<br>To improve the AD search, you can use separate hierarchy levels of the base:<br>`C- countryName`<br>`O- organizationName`<br>`OU- organizationalUnitName`<br>`DC- domainComponent`<br>`CN- commonName`<br>**Example for AD**: to use the `Users` branch located in the company domain as the search base, enter:<br>`cn=users,dc=company,dc=com`<br>**Example for DD:** a request may contain one or several values: `o=company,ou=department,ou=group`<br>**Important!** To enable a partial synchronization using an LDAP request, you should firth sync with the entire LDAP catalogue (`dc=company,dc=ru`) and then run synchronization using a narrower LDAP request. To update information about groups/persons/computers for this synchronization, you should run complete synchronization with the entire LDAP catalogue and then a partial synchronization using an LDAP request. |
| Use user certificate for authentification | Whether is it allowed to use a client certificate for secure connection types instead of entering a password |
| Anonymous access | Indicates if the connection to the LDAP server is performed on behalf of an anonymous user |
| Login | Login to access the synchronization server |
| Password | Password to access the synchronization server |

4. Click **Check connection**, to perform control check of connection to the server.

5. Click **Save**.

> **Important!**
>
> To enable LDAP operation over a secure connection through port 389, you should edit the **/etc/openldap/ldap.conf** configuration file. For this, add the following entry to the file and save changes: `TLS_REQCERT never`. Without this entry, synchronization with AD will be declined.

**Encrypted connection support**

You can send data over a secure connection for synchronization with LDAP servers only if you choose the following connection types:

- LDAP with StartTLS function, which allows you to establish a secure connection over an existing unsecured one on ports 389 or 3268 if the global catalogue is used. In this case, both synchronization with AD using Kerberos protocol and anonymous access are supported.
- LDAPS, where data is sent over a secured channel: on ports 636 or 3269 if the global catalogue is used.

## Editing Connection to Server

**To edit connection to server:**

1. Go to **Administration -> LDAP Synchronization**.
2. By left-click select required server.
3. On the toolbar click  **Edit**.
4. Change connection parameters (see "Creating Connection to Server").
5. Click **Check connection**, to perform control check of connection to server.
6. Click **Save**.

## Deleting Connection to Server

**To delete existing Server connection:**

1. Go to **Administration -> LDAP Synchronization**.
2. By left-click select required server.
3. On the toolbar click  **Delete**.

   **Note:**

   To delete several connections at a time, highlight them (for example, holding **<SHIFT>** or **<CTRL>** ) and click **Delete** .

4. In the opened window click **Yes**.

## Running Synchronization with Server Manually

**To run synchronization with Server manually:**

1. Go to **Administration -> LDAP synchronization**.
2. Left-click at the target server on the left.
3. Click  **Starting synchronization** button located on the toolbar.

Information on the synchronization results will be displayed in *Last synchronization, Status of the synchronization, Next synchronization status* strings.

**Note:**

If the ***Synchronize*** connection attribute has *Every N minutes*, *Every N hours, Every N days* or *Every N week* values, then the automatic synchronization will be performed with specified frequency after last manual running.

**Warning!**

Synchronization will be performed according to Traffic Monitor server time. If management console is located in different time zone, then specifying synchronization time is required to be done considering difference between time zones of server and management console.

It is required to check connection with LDAP servers after updating from previous versions. To do this, take the following steps:

1. Left-click at the target server.
2. Click on **Check connection.**

Information on the synchronization results will be displayed in a message. If error occurs, set connection parameters.

### 4.10.2 Managing System Users and their Roles

To manage System users the following entities are used:

- *User* – user's account (see "Users");
- *Role* – a set of rights which can be assigned to User (see "Roles");
- *Visibility scope* – a set of attributes of interception objects: the objects with those attributes will be available to specified users only (see "Visibility Scopes").

#### Users

Configuring the System users list is performed in the **Administration -> Users and Roles** section, the **Users** tab.

In the work area the list of System users, toolbar and a drop-down menu (defining a number of users displayed at the page) are located.

Account attributes are listed in the following table:

| Parameter | Description |
|---|---|
| *Login* | Name of user account |
| *Full name* | User's first name and second name |
| *Email* | User's e-mail address |
| Roles | List of roles assigned to the user |
| *Scopes* | List of visibility scopes available for the user |

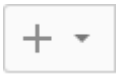
| | |
|---|---|
| *Description* | Note to the account |
| Status | Indicates whether user role is active or passive |

You can perform the following actions while managing users:

- Creating User Account
- Editing User Account
- Deleting User Account
- Changing User Account Password
- Changing User Account State
- Importing User Account from Active Directory
- Assigning Role to a User
- Creating Visibility Scope to User

Creating User Account

**To create user account:**

1. Go to the **Administration** -> **Users and roles** section.
2. Go to the **Users** tab.
3. On the toolbar click  **Create User**.
4. In the opened window specify account parameters.

| Parameter | Description |
|---|---|
| *Login* | User account name |
| *Status* | Indicates if the user account is active or passive |
| *Interface language* | Language, which will be assigned to the interface of selected user account |
| *Password* | User account password |
| *Confirm password* | User account password |
| *Email* | User email address |
| *Full name* | Full name of the user |
| *Description* | User account notes |

5. Click **Save**.

### Editing User Account

**To change existing user account parameters:**

1. Go to the **Administration** -> **Users and roles** section.
2. Go to the **Users** tab.
3. In the users list left-click at the target account.
4. Click  **Edit user** on a toolbar.
5. In the opened window change account attributes (see "Users").
6. Click **Save**.

### Deleting User Account

**To delete user account:**

1. Go to the **Administration -> Users and roles** section.
2. Go to the **Users** tab.
3. In the users list left-click at the target account.
4. On the toolbar click  **Delete user**.

> **Note:**
>
> To delete several accounts in one action, select them from the list (for example, by pressing **<SHIFT>** or **<CTRL>** ) and click **Delete user** .

5. In the opened window click **Yes**.

### Changing User Account Password

**To change user account password:**

1. Go to the **Administration** -> **Users and roles** section.
2. Go to the **Users** tab.
3. In the users list left-click at the target account.
4. On the toolbar click  **Change password**.
5. In the opened window enter a new password to **Password** and **Confirm password** fields.
6. Click **Save**.

### Changing User Account State

**To change account state:**

1. Go to the **Administration -> Users and roles** section.
2. Go to the **Users** tab.
3. In the users list left-click at the target account.
4. On the toolbar click  and choose **Activate user** or **Deactivate user**.

**Note:**

You can change a status of any account except of **Administrator**.

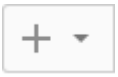
### Importing User Account from Active Directory

You can easily create users by importing their accounts from Active Directory or Domino Directory.

**Important!**

If AdBlock extension is used in your browser, then disable this extension before importing user accounts, as AdBlock blocks the import.

**To import user account:**

1. Go to the **Administration -> Users and roles** section.
2. Go to the **Users** tab.
3. On the toolbar click  **Import users from LDAP**.
4. In the opened window, specify LDAP server which stores the required account.

   **Note:**

   You can enter a part of login name to the **Search** field and click **Search**.

5. Flag required user accounts.
6. Click **Save**.

### Assigning Role to a User

**To assign role to a user:**

1. Go to the **Administration -> Users and roles** section.
2. Go to the **Users** tab.
3. In the users list left-click at the target account.
4. Click  on the toolbar.
5. Choose **Set role** in the list (see "Roles").
6. Click **Save**.

### Creating Visibility Scope to User

**To create visibility scope to user:**

1. Go to the **Administration** -> **Users and roles** section.
2. Go to **Users** tab.
3. In the users list left-click at the target account.
4. On the toolbar click .

5. Choose from Set visibility scope the list (see "Visibility Scopes").
6. Click **Save**.

## Roles

To control redundant access to system settings, policies of different structural departments, interception objects and other important information, there is role system of access rights differentiation in InfoWatch Traffic Monitor.

Role is a set of rights which can be assigned to user. Assigning a role to user is described in "Assigning Role to a User".

Initially, there are two predefined roles and the two preset user – roles **Adminitrator** and **Security officer**, which are accordingly assigned to Administrator and Officer users.

**Administrator** role provides an opportunity to carry out the initial configuration of the system (Managing users, roles, visibility scopes, licenses and LDAP synchronization).

**Security officer** role has all rights except for initial setup.

Configuring the roles list is performed in **Administration -> Users and Roles** section, **Roles** tab.

In the work area the list of System users, toolbar and a drop-down menu (defining a number of roles displayed on the page) are located.

Role attributes are listed in the following table:

| Attribute | Description |
|---|---|
| *Name* | Role name |
| *Users* | First name and second name of the user |
| *Description* | Comment to a role |

You can perform the following actions while managing roles:

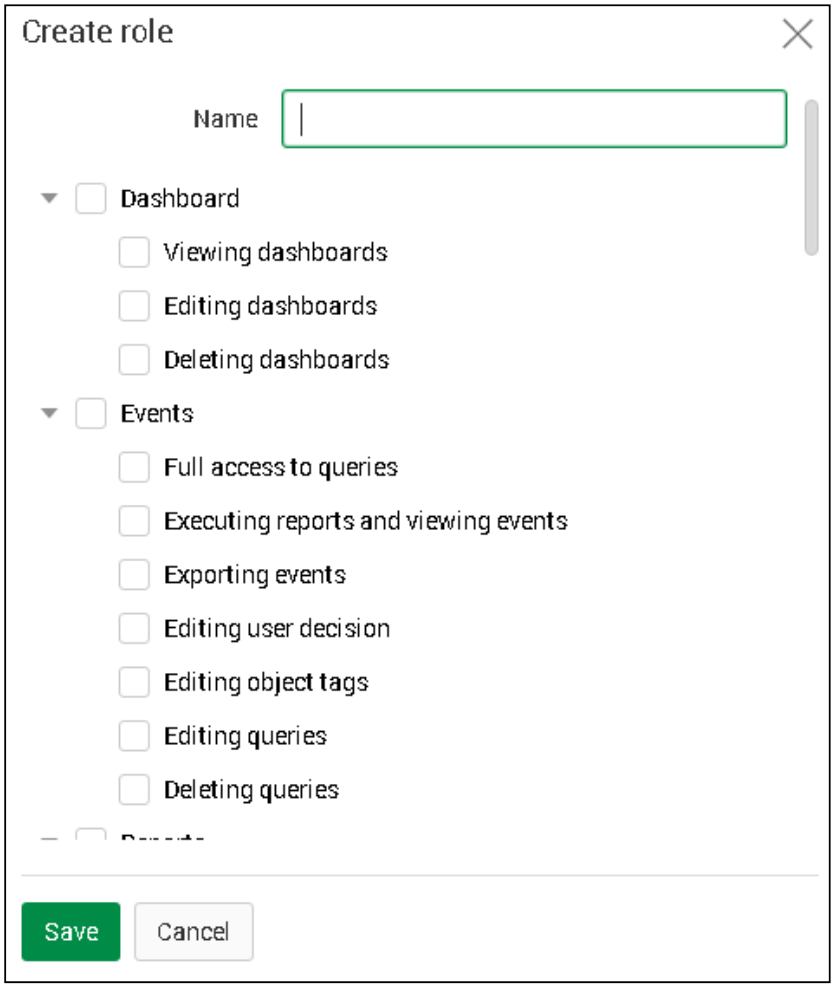
- Creating a Role
- Editing a Role
- Deleting a Role

### Creating a Role

**To create a new role, follow the steps below:**

1. Go to section the **Administration** -> **Users and roles**.
2. Go to the **Roles** tab.
3. On the toolbar, click  **Create role**.
4. In the opened window specify role attributes. Flag the privileges you want to assign to the role.

> **Note:**
>
> To expand/collapse privileges list, click ▶ or ◢ respectively.




**Note:**

**Viewing roles** and **Viewing visibility scopes** privileges are available by default when selecting **Roles** and **Visibility scopes**.

5. Click **Save**.

Editing a Role

**To change parameters of an existing role, follow the steps below:**

1. Go to the **Administration -> Users and roles** section.
2. Go to the **Roles** tab.
3. In the users list left-click at the target role.
4. Click  **Edit role**.
5. In the opened window change role attributes. Flag (unflag) the privileges you want to assign (unassign) to the role.

> **Note:**
>
> To expand / collapse privileges list, click ▶ or ◢ accordingly.

> **Note:**
>
> **Viewing roles** and **Viewing visibility scopes** privileges are available by default when selecting **Roles** and **Visibility scopes**.

6. Click **Save**.

Deleting a Role

**To delete role:**

1. Go to the **Administration -> Users and roles** section.
2. Go to the **Roles** tab.
3. In the users list left-click at the target role.
4. Click  **Delete role**.

> **Note:**
>
> To delete several roles at a time, select them in the list (for example, by holding **<SHIFT>** or **<CTRL>** ) and click **Delete role**.

5. In the opened window click **Yes**.

> **Note:**
>
> You can change any role except for **Administrator** and **Security officer**.

## Visibility Scopes

Visibility scope allows you to perform additional access control to intercepted objects. Visibility scope is created from intercepted objects attributes. User will only see those events, which attributes match the attributes, configured in visibility scope.

For example,

User officer 1 has visibility scope with Person Ivan and Tag 1. In this case user officer 1 can only view events with the participation of Ivan and tagged 1.

**Note:**

There can be several scopes for one user.

Assigning visibility scope to user is described in "Creating Visibility Scope to User".

Configuring the visibility scopes list is performed in **Administration** -> **Users and Roles** section, **Scopes** tab.

In the working area there is a list of scopes, toolbar and drop-down menu.

In the list of scopes, user scopes are displayed.

Toolbar contains set of tools to work with visibility scopes.

Drop-down menu defines number of scopes to be displayed on the page.

Visibility scope attributes are listed in the following table:

| Attribute | Description |
|---|---|
| *Name* | Name of the visibility scope |
| *Description* | Note for visibility scope |

You can perform the following actions while managing visibility scopes:

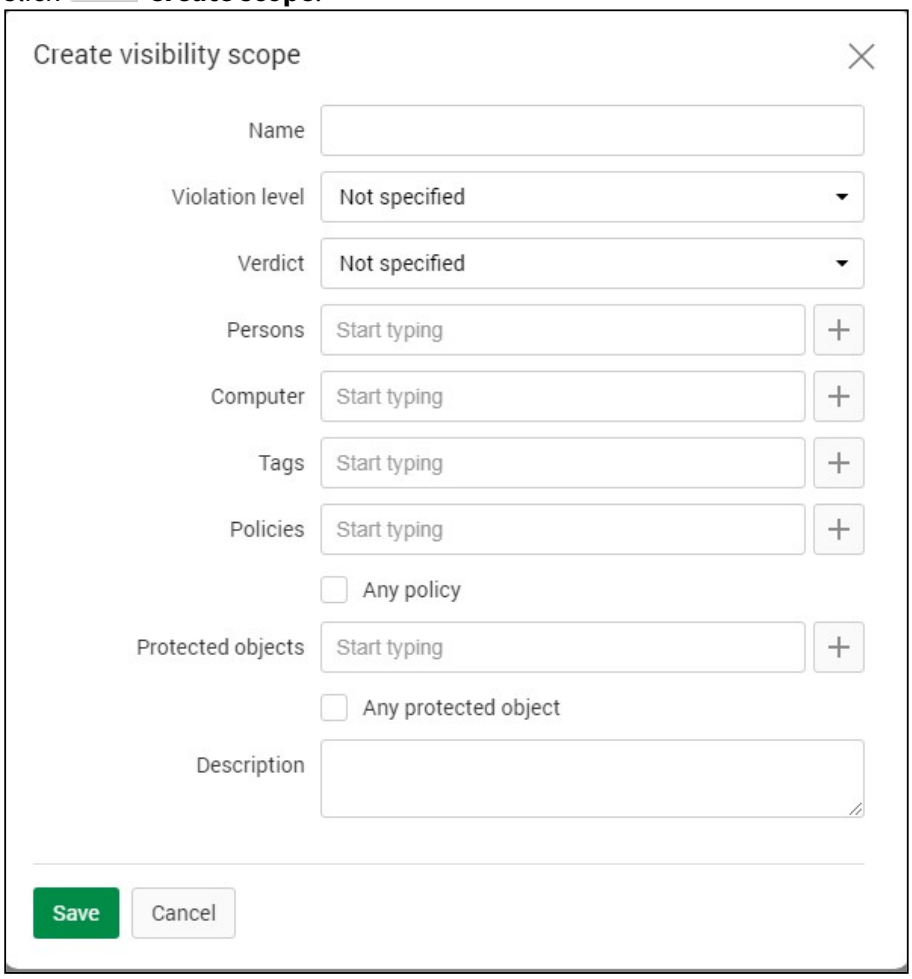
- Creating Visibility scope
- Editing Visibility scope
- Deleting Visibility Scope

Creating Visibility scope

To create a visibility scope:

1. Go to the **Administration** -> **Users and Roles** section, and open the **Scopes** tab.

2. Click  **Create scope**.




3. In the opened window, specify parameters of the visibility scope:
   a. *Name* - enter name in the field.
   b. *Violation level* - choose from drop-down menu.
   c. *Verdict* - choose from drop-down menu.
   d. *Persons*:
      enter first symbols of user name and choose required value from drop-down menu
      or
      press  and set flag for the required users in the user list. Click **Add**.
   e. *Workstations* – as in item d.
   f. *Tags* - as in item d.
   g. *Policy* – as in item d.
   h. *Protected objects* – as in item d.
   i. *Any protected object* - choose option.
   j. *Description* - enter description text in the filed.
4. Click **Save**.

Editing Visibility scope

**To edit visibility scope:**

1. Go to the **Administration -> Users and roles** section.
2. Go to the **Scopes** tab.
3. Click  **Edit scope**.
4. In the opened window change visibility scope attributes like when creating the scope (see 'Creating visibility scope').
5. Click **Save**.

Deleting Visibility Scope

**To delete a visibility scope:**

1. Go to section the **Administration** -> **Users and roles** section.
2. Go to the **Visibility scopes** tab.
3. On the toolbar, click  **Delete scope**.

   > **Note:**
   >
   > To delete several visibility scopes at a time, select them in the list (for example, by holding **<SHIFT>** or **<CTRL>**) and click **Delete**.

4. In the opened window click **Yes**.

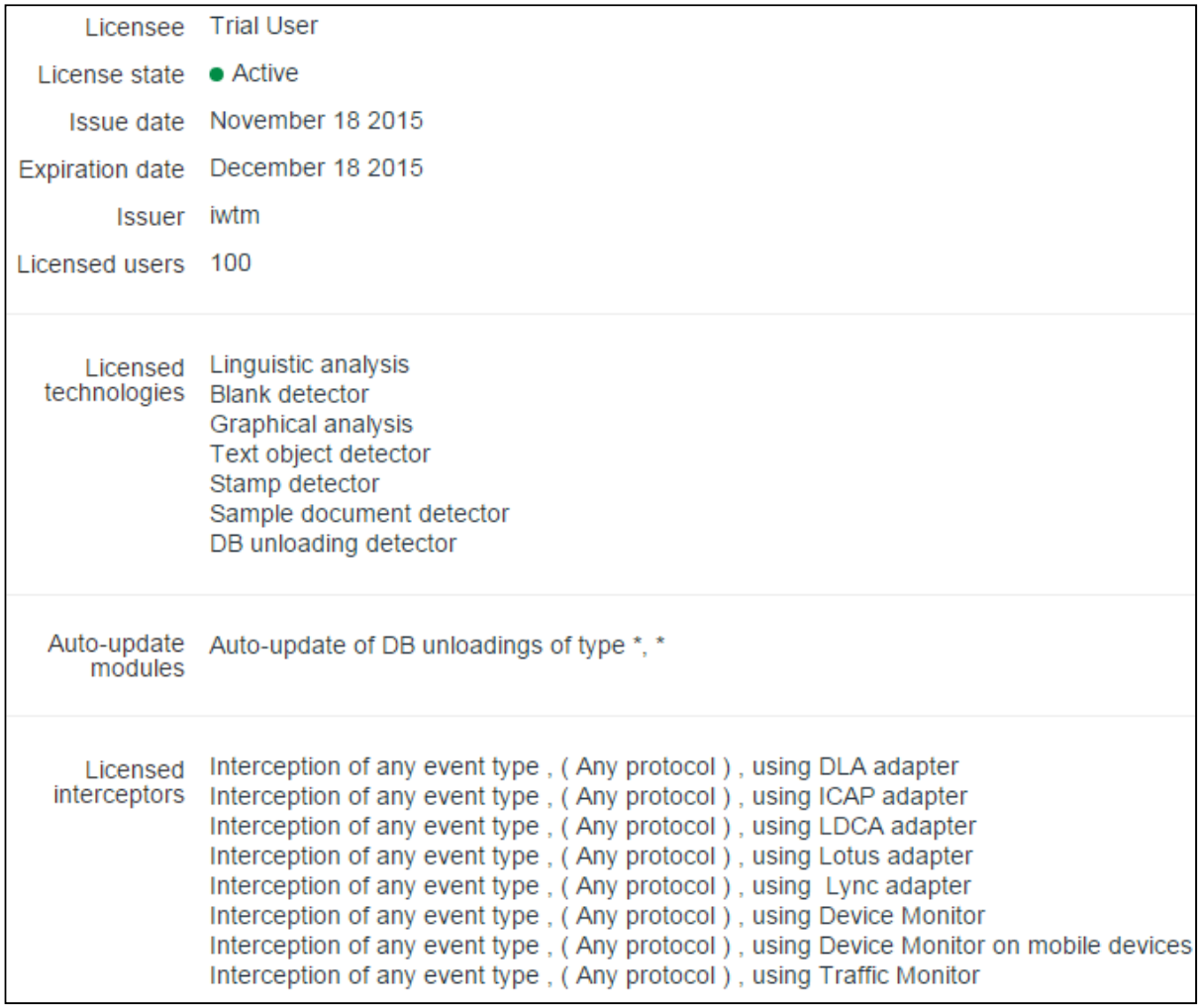
## 4.10.3 Managing Licenses

> **Warning!**
>
> The System licensing is described in the document "InfoWatch Traffic Monitor. Administration Guide", "Licensing" article.

Licenses are managed in the Management Console, the **Administration** –> **Licenses** section:

- In the left part of the working area, you can see the list of licenses and a toolbar.
- In the right side of the working area, you can see information on the selected license.

> **Note:**
>
> Editing licenses is unavailable. You can only upload a new license or delete an earlier created license.




You can perform the following actions with licenses:

- Installing a License
- Deleting License
- Requesting a License

## Checking License Validity

Information about licensed technologies and interceptors, state, expiration date and number of licensed users, are available in **Administration –> Licenses**.

**To check license validity:**

1. Go to **Administration -> Licenses**.
2. Make sure, that **Expiration date** contains future date.
3. Make sure, that **Licensee** field value matches Licensee parameter of **license.conf** configuration file, located in `/opt/iw/tm5/etc` directory.

## Installing a License

**To install a license:**

1. Go to **Administration -> Licenses**.

2. Click  **Add license** on the toolbar.
3. Click **Upload** in the pop-up menu.
4. Choose required license.lic file and click **Open** in the dialog box.
   Information about licenses and licensed technologies and interceptors will be shown in the **License adding** pop-up window.
5. Click **Add**.
6. Click **Yes** in the dialog box.

Browser page will be refreshed and new license will be added to the list. You may leave or remove the expired licenses at your option.

### Deleting License

**To delete license:**

1. Choose the target license from the list.
2. On the toolbar click  **Delete**.

   > **Note:**
   >
   > To delete several several licenses at a time, select them in the list (for example, by holding **<SHIFT>** or **<CTRL>** ) and click **Delete** .

3. In the opened windows press **Yes**.

### Requesting a License

**To request a license:**

1. Go to **Administration** - **Licenses**;
2. On the toolbar, press  **Request license**.
3. Send an automatically formed email, adding description, if necessary.

## 4.10.4 Healthcheck

You can monitor the state of each server on which the System is deployed in **Administration**->**System state** section of the Management Console.

For each server that is used in the System, indicators are listed in the table:

| | Parameter | Details |
|---|---|---|
| ● | Current System load | OK - load average: 0.21, 0.15, 0.19 |
| ● | Number of active users | USERS OK - 3 users currently logged in |
| ● | State of local mail server | SMTP OK - 0.013 sec. response time |
| ● | System time deviation | NTP OK: Offset -0.01090276241 secs |
| ● | Errors in the alert log. | OK - no errors found in log |
| ● | Size of database alert log. | OK - size of PostgresSQL system log is 9047 bytes |
| ● | State of PostgreSQL database. | OK - database postgres (0.003083 sec.) |
| ● | Server availability | PING OK - Packet loss = 0%, RTA = 0.06 ms |
| ● | Free space in root partition | DISK OK - free space: / 96362 MB (71% inode=98%): |
| ● | State of time syncronization service | OK - ntpd (pid 2491) is running... |
| ● | State of Syslog service | OK - 'rsyslogd' is running |
| ● | Server availability via SSH | SSH OK - OpenSSH_5.3 (protocol 2.0) |
| ● | Swap usage | SWAP OK - 77% free (6145 MB out of 8015 MB) |
| ● | Queue of processing actions specified in policies applied to the events. | OK - Blackboard queue: 0 item(s), 0.000 MBytes |
| ● | Number of errors occurred when processing actions from policies applied to events. | OK - Blackboard-errors queue: 0 item(s), 0.000 MBytes |
| ● | Presense of memory dumps | OK |
| ● | State of System components | OK |
| ● | Number of errors occurred when indexing events by INDEXER service. | OK - index_error queue: 0 item(s) |
| ● | TM_PG_INDEXER_QUEUE | OK - index_queue queue: 0 item(s) |
| ● | Queue for loading to storage | OK - DB queue: 0 item(s), 0.000 MBytes |
| ● | Queue processing errors | OK - Errors queue: 0 item(s), 0.000 MBytes |
| ● | Queue processing mail traffic | OK - SMTP queue: 0 item(s), 0.000 MBytes |
| ● | Number of errors occurred when processing events by IW_LOADER and IW_XML2LIR... | OK - XML2LIRO-errors queue: 0 item(s), 0.000 MBytes |
| ● | Number of running processes | PROCS OK: 283 processes with STATE = RSZDT |
| ● | Free space in /var partition | DISK OK - free space: / 96361 MB (71% inode=98%): |

For each indicator, the following information is displayed:

- **State** – the current value of the indicator:
  - 🔴 – CRITICAL, the parameter value is higher than the critical threshold;
  - 🟡 – WARNING, the parameter value is a warning zone (if this zone exists);
  - 🟢 – OK, the parameter value is normal.
- **Parameter** – indicator name.
- **Details** – detailed information on healthcheck results.

> **Warning!**
>
> If the indicator value cannot be obtained, it is assumed, that the current value is higher than a critical threshold.

Values are refreshed:

- Every 5 minutes – for parameters:
  - DB Alert Log Errors
  - Swap usage
  - DB Alert log Size
- Every 10 minutes – for parameters:
  - SSH availability
  - Database Status
  - Oracle TNS Status
- Every 360 minutes – for **NTP time deviation** parameter
- Every 30 minutes – for all other parameters

To refresh the values manually, click **Refresh**.

### Configure Notifications

To configure the System condition notifications:

1. Go to **Administration** - **System condition**;
2. Click the button "**Configure notifications**";
3. Enable the option "**Enable notifications**".
4. Specify the values for the following parameters:

| Parameter | Description |
|---|---|
| *Mail prefix* | Mail prefix is used to sort out the e-mail messages from different monitoring systems. The value you've entered is to be added in the beginning of the line "Subject" of the messages to be sent. The default value is: `IWTM` |
| *Recipients* | Email of recipient/recipients. The default value is: `nagios@localhost` |

5. Click *Send text message* to check if the settings are correct.
6. Click **Save**.

## 4.10.5 Managing Services

System Administrator can manage services without using Linux command line.

The following actions with services are possible:

- Running Service
- Stopping Service
- Restarting Service
- Saving Service Logs

### Running Service

**o start service**:

1. Go to **Administration - Services**.
2. Set flag in the field of the service you want to start.
3. Click button.

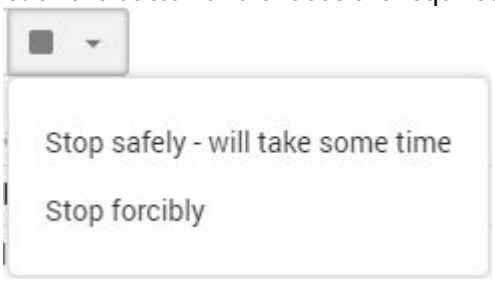
> **Information:**
>
> To restart several services at a time, set flag opposite each of them.

### Stopping Service

**To stop service**:

1. Go to **Administration - Services**.

2. Set flag in the field of the service you want to stop.
3. Click the button and choose the required option:




**Stop safely** - the System waits until the service operation is complete and then stops the service with no loss of data being processed;

**Stop forcibly** - quick stop of services. Loss of data may occur.

> **Note:**
>
> To stop several services at a time, set flag opposite each of them.

### Restarting Service

**To restart service**:

1. Go to **Administration - Services**.
2. Set flag in the field of the service you want to restart.
3. Click button.

> **Note:**
>
> To restart several services at a time, set flag opposite each of them.

### Saving Service Logs

To save service logs:

1. Go to **Adminitration - Services**.
2. Click **Save** in **Logs** column opposite the service which logs you want to save.

## 4.10.6 Collecting Diagnostic Data

Collecting diagnostic data is performed in **Administration** -> **Services** section.

| Data collection mode | Description |
|---|---|
| Normal | Information about System logs, configuration and initial installation. |

| | |
|---|---|
| Extended | Information about System logs, configuration, initial installation and information about processes of System emergency stop. |

Diagnostic information is to be collected from the following sources:

| Data type | Path to files |
|---|---|
| Logs | `/var/log/infowatch/*.log`<br>`/var/log/nagios/nagios.log`<br>`/root/iwsetup-install-logs/*`<br>`/var/log/nagios/status.dat`<br>`/home/oracle/addm/logs/*` – If Oracle DBMS is installed<br>`/u01/app/oracle/diag/rdbms/iwtm/iwtm/trace/alert_iwtm.log` – If Oracle DBMS is installed<br>`/u01/postgres/pg_log/*` – If PostgreSQL DBMS is installed |
| Configuration information | `/opt/iw/tm5/etc/*.conf`<br>`/opt/iw/tm5/etc/scripts/*.lua`<br>`/opt/iw/tm5/etc/config/lua/vademecums/*.info`<br>`/opt/iw/tm5/etc/config/lua/vademecums/vademecum.list`<br>`/etc/nagios/*`<br>`/etc/nagios/objects/*` |
| Logs and scripts of initial installation of the System | `/root/iw*` |

**To download a report with results of the last diagnostics:**

1. Go to **Administration** -> **Services** section.
2. Click the **Results of the latest diagnostics are available** link to download the archive in `dd-mm-yyyy_hh-mm-ss` format.

> **Warning!**
>
> If diagnostics has not been performed earlier, downloading the diagnostics results is unavailable.

Diagnostics data can be collected in the following ways:

- Collecting the Diagnostic Data in Normal Mode
- Collecting the Diagnostic Data in Extended Mode

## Collecting the Diagnostic Data in Normal Mode

**To collect the diagnostic data in extended mode**:

1. Go to **Administration - Services**.

2. Press Collect data.
3. Mark the **Normal** filed.
4. Click Run button.
5. Wait till completion of diagnostic information collection.
6. In pop-up window click **Result of the last data collection** is available in `dd-mm-yyyy_hh-mm-ss` format.

### Collecting the Diagnostic Data in Extended Mode

**To collect the diagnostic data in extended mode**:

1. Go to **Administration - Collecting the diagnostic data**.
2. Click Collect data button.
3. Set marker in **Extended** field.
4. Press Run.
5. Wait till completion of diagnostic information collection.
6. Download archive by clicking **Result of the last data collection is available** in `dd-mm-yyyy_hh-mm-ss format`.

## 4.10.7 User Actions Audit

The system provides the ability to monitor user actions in Management Console.

Audit events and searching filters review is performed in **Administration -> Audit**.

The system records and displays the following information:

- logging in the System and out of the system;
- access control objects management (Users, Roles, Visibility Scope);
- user actions concerning system objects (queries, reports, policies, classifier elements and so on).

> **Note:**
>
> Changing elements through configuration cancellation is not being tracked in audit events. In this case, only configuration cancellation event will be created.

**To set storing period for audit events**:

1. Go to **Administration -> Audit**;
2. Specify number of days to store audit events in **During storage of audit events (days)** area;

Working with audit events is described in the following subsections:

- Audit Events
- Filtering by User
- Filtering by Action
- Filtering by Object
- Filtering by Date

## Audit Events

Audit Events area is located in **Administration - Audit**.

**Audit Events** area displays **Search filters** results and represents list of audit events panels with the following attributes:

| Attribute | Description |
|---|---|
| *User* | Name of the user, which performed an action |
| *Object* | Name of an object, connected with an action |
| *Action* | Type of action, performed by user |
| *Action date and time* | Date/time of user registered action |
| *More info* | Additional information on audit event |




**Picture 1. Audit event panel**

**To filter audit events by date:**

1. Go to **Administration - Audit**;
2. In the upper left corner click **Sorting** 

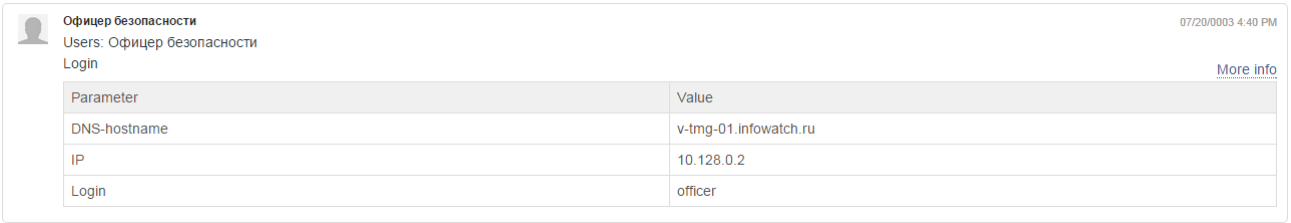
.

More Info

**More info** will be displayed depending on the *Object* and *Action* registered in the System.

For example, logging out of the System, one will see the following Audit parameters:

- **DNS-hostname** - name of the computer, logging out of the System;
- **IP** - IP-address of logging out computer;
- **Login** - name of the user logging out of the System.




**Picture 2. More info**

**Warning!**

Audit events parameters can be different depending on *Object* and *Action*.

**To view more information about audit event:**

1. Go to **Administration - Audit**.
2. On event panel click **More info**.

### Filtering by User

**To filter events by user:**

1. Go to **Administration** - **Audit**;
2. In **Search filters** area choose user from **User** drop-down list (see "Managing System Users and their Roles").

For more filtering options, use *Action*, *Object* and *Date* parameters.

### Filtering by Action

**To filter events by action:**

1. Go to **Administration** - **Audit**;
2. In **Search filters** area choose action from **Action** drop-down list.

For more filtering options, use *User*, *Object* and *Date* parameters.

### Filtering by Object

**To filter events by Object**:

1. Go to **Administration** - **Audit**;
2. In **Search filters** area choose object from **Object** drop-down list.

For more filtering options, use *User*, *Action* and *Date* parameter.

### Filtering by Date

**To filrer events by date:**

1. Go to **Administration** - **Audit**;
2. In **Search filters** area click on **Date** field.
3. In calendar specify dates of period.
4. Click **Apply**.
5. Click **Clear** to cancel filering by date.

For more filtering options, use *User*, *Action* and *Object* parameter.

## 4.10.8 Integrity Monitoring

Integrity monitoring is intended to monitor system foles state. Primary reference amount is automatically generated by the System.

System files integrity monitoring is described in the following sections:

- Manual Integrity Monitoring
- Automatic Integrity Monitoring
- Accepting Result as Standard

### Manual Integrity Monitoring

**To check system files integrity:**

1. Go to **Administration - Integrity monitoring**;
2. In the central part of the working area click **Scan files**.

> **Note:**
>
> In the process of integrity check the **Integrity check is being performed** message is being displayed. Upon check completion, you will see the message with date and time of the last check.

### Automatic Integrity Monitoring

**To configure system files automatic integrity monitoring:**

1. Go to **Administration - Integrity monitoring**;
2. In the central part of the working area enable **Automatic check** setting.
3. In the **Schedule** field set the time of integrity check using **up** and **down** arrows.
4. Click **Save**.

### Accepting Result as Standard

**To accept result of integrity check as standard:**

1. Go to **Administation - Integrity monitoring**;
2. In the central part of the working area click **Accept result as standard**.

## 4.10.9 Plugins

The System uses plugins to connect additional interceptors. The extension makes it possible to receive events from external interceptors, add user attributes of events, automatically update sample unloadings and provide data to external systems.

Any API/Public API connectors of external systems must be registered in TM by adding a new plugin.

A plugin is an archive in a ZIP format, which contains:

- **licenses** folder with license files;
- **icon** folder with icons for registered contacts and event types;
- **manifest.json** file with information about the plugin. For plugins that are used for receiving events and plugins used for updating sample unloadings, the file structure is different.

> **Note:**
>
> Names of files in the plugin should contain only Latin characters and/or numbers.
>
> Folders **licenses** and **icon** are optional. License files and files with pictograms can be located in the root folder.

Default plugins **InfoWatch Device Monitor**, **InfoWatch Sample documents Autoupdate Adapter**, **InfoWatch Crawler** will be displayed in Traffic Monitor management console in case the System contains the active license installed (see "Managing Licenses").

For external systems which are the sources of events the file **manifest.json** should contain the following information:

| Name | Compulsory | Description |
|---|---|---|
| Version | Yes | Plugin version |
| Developer company ID | Yes | Matches the company name in the license |
| Used preinstalled event types, contacts and protocols | No | List of preinstalled event type and protocols intercepted by this plugin |
| Name | Yes | Plugin unique name |
| Description | No | Plugin description |
| "Preinstalled" attribute | No | Whether it is included in the System |
| Registered event types, contacts, and protocols | No | Contains the following data:<br>• Type of registered events with specifying the service type<br>• Protocols<br>• Actions<br>• Code of interceptor type for InfoWatch plugins<br>• Event type names localization at least in one language<br>• Types of registered contacts and their localization at least in one language<br>• Files with icons of registered contacts and event types |
| Unique identifier | Yes | Unique 128-bit identifier (UUID) of the plugin |

For external systems which are the sources of events the file **manifest.json** should contain the following information:

| Name | Compulsory | Description |
|---|---|---|
| Version | Yes | Plugin version |
| Developer company ID | Yes | Matches the company name in the license |
| Name | Yes | Plugin unique name |

| Name | Compulsory | Description |
|---|---|---|
| Data receiving systems | Yes | List of identifiers for systems receiving data from TM that are registered in the plugin |
| Description | Yes | Plugin description |
| "Preinstalled" attribute | No | Whether it is included in the System |
| Unique identifier | Yes | Unique 128-bit identifier (UUID) of the plugin |

For external systems receiving data from TM, the **manifest.json** file should contain the following information:

| Name | Compulsory | Description |
|---|---|---|
| Version | Yes | Plugin version |
| Developer company ID | Yes | Matches the company name in the license |
| Name | Yes | Plugin unique name |
| Data receiving systems | Yes | List of identifiers for systems receiving data from TM that are registered in the plugin |
| Description | Yes | Plugin description |
| "Preinstalled" attribute | No | Whether it is included in the System |
| Unique identifier | Yes | Unique 128-bit identifier (UUID) of the plugin |

In **Plugins** sections, you can perform the following actions:

- Adding Plugin
- Deleting Plugin
- Working with Tokens

**Warning!**

Plugins and tokens are deleted from the System when deleting the DB schema (see "*Infowatch Traffic Monitor. Installation Guide*", "Deleting the Database Schema" article). To restore the Device Monitor plugin:

1. Create the file **/opt/iw/tm5/www/backend/protected/runtime/first_run** on behalf of **iwtm** user.
2. Restart **iw_kicker** process:
   ```
   iwtm restart kicker
   ```

Other plugins should be added manually (see "Adding Plugin").

## Adding Plugin

**To add plugin:**

1. Go to **Administration - Plugins**;
2. In **Plugins** are press .
3. Press **Add**.
4. Review plugin's description and press **Install**.

**Note:**

To update plugin, add renewed version.

## Deleting Plugin

**To delete plugin:**

1. Go to **Administration - Plugins**;
2. In **Plugins** area press .
3. Press **Yes** to confirm deletion.

**Warning!**

Preset plugins cannot be deleted.

## Working with Tokens

Tokens are designed for authorizing an external which uses Push API (sending events from third-party interceptors to TM) and Public API (loading external unloadings from DB to TM and access to TM data for external systems). When the plugin is added, a token is created automatically. (see "Adding Plugin").

For InfoWatch Device Monitor, a token is created automatically and is available in **Administration** -> **Plugins** -> **Tokens** section of the Management Console.

The following actions with tokens are available:

- Adding Token
- Editing Token Data
- Updating Token Value
- Copying Token
- Deleting Token

Adding Token

**o add token:**

1. Go to **Administration** - **Plugins**;
2. Choose plugin in **Plugins** area;
3. Go to **Tokens** tab;
4. Press .

> **Note:**
>
> Token value is generated automatically upon token creation and can be defined by user.

Editing Token Data

**To edit token data:**

1. Go to Administration - Plugins;
2. Choose plugin in **Plugins** area;
3. Go to **Tokes** tab;
4. By double-clicking the left mouse button in the *Name* column or *Description* type in the neccesary data.

Updating Token Value

In case token is compromised or there is a likehood, that it leaks to third-parties, we need to generate a new token value.

**To update tokem value:**

1. Go to **Administration - Plugins**;
2. Choose plugin in **Plugin** area;
3. Go to **Tokens** tab;
4. Click .

Copying Token

**To copy token value to the clipboard:**

1. Go to **Administration - Plugins**;
2. Choose plugin in **Plugins** area;
3. Go to **Tokens** tab;
4. Click .

Deleting Token

**To delete token:**

1. Go to **Administration** - **Plugins**;

2. Choose plugin in **Plugins** area;
3. Go to **Tokens** tab;
4. Press  .

### 4.10.10 Configuring Connection to Mail Server

In the **Administration** -> **Connection to mail server** section, you can specify an SMTP server that will be used for sending notifications about triggered rules (see "Configuring Notifications") and the state of the System (see "Healthcheck").

To configure the connection:

1. In the **Sender's email address** field, specify the address that will be used for sending notifications.
2. Choose the server type. Possible choices:
   - **Embedded in Traffic Monitor** - select this option if you are using a local Traffic Monitor mail server with anonymous access;
   - **External** - select this option if you are using an external server. for example, if sending emails to external servers without authorization is prohibited in your company.
3. If an external server is used, specify the server parameters:
   - **SMTP server address**;
   - **Port**;
   - **Login** - optional parameter;
   - **Password** - optional parameter;
   - **Encryption** - optional parameter. If you select **Use**, then SSL/TLS encryption and NTLM authentication will be used for the connection.

   When you have specified all connection settings, click **Check connection**.
4. Click **Save**.

### 4.10.11 Configuring Notifications

In the **Administration** -> **Notifications** section, you can configure templates for emails which are sent when the security policy is triggered.

Notifications can be sent to:

- **An employee** who has violated a security policy. If a rule is triggered, the employee is notified that his/her actions violate the corporate security policy. If the System operates in the inline mode, employees also get timely notifications when:
  - their emails are blocked or quarantined and await a decision of the security officer;
  - the security officer has decided on the quarantined email (whether to block it or send it to the recipient).
- **A security officer**. Getting timely notifications about incidents makes it easier for the security officer to promptly respond to important incidents.
- **Other interested persons**, for example, the head of an employee who has violated a security policy.

To create a notification, click  on the toolbar to the left (see "Creating Notification"). Added notifications are used in policy rules: in the **Actions when the rule is triggered** area, **Send notification** field, click  and select the required notification (for details, see "Creating Rules").

**Note:**

If necessary, you can create or edit notifications when configuring a rule in the **Policies** section. Editing and deleting notifications is only available from the **Notifications** section.

To edit a notification, choose the required notification in the list and click on the toolbar.

While creating/editing a notification, you can test the resulting template (see "Testing Notification").

To copy an earlier created notification, choose it in the list and click on the toolbar. The notification copy will be added to the list.

To delete a notification, use button on the toolbar.

**Note:**

In this case, the notification is also deleted from all policies where it is used.

Besides user-created notifications, there are also preset notifications in the System (see "Preset Notifications").

## Creating Notification

**Purpose:**
Create a notification that can be sent when rules are violated.

**Solution:**

1. Go to the **Administration** -> **Notifications** section.
2. On the toolbar to the left, click .
3. In the form that opens, enter the notification name.
4. Choose notification recipients. Possible choices:
   - **Initiator of event** - select this field to create a template that will be sent to the event initiator;
   - **Custom recipients** - select this field and click to add recipients. In the window that opens, go to the required tab:
     - On the **Persons** and **Security officers** tabs, choose required values from the list. You can sort values in the list by the person/user name.
     - On the **Email** tab, you can enter email addresses of recipients who are not in the list of persons or security officers.
     - On the **Head** tab, enable the switch if you want to notify the head of the event initiator.

   Once you have specified all required recipients, click **Save**.
5. In the **Email template for different verdicts** open the tab with a verdict for which you want to create a template. The following tabs are available:
   - **Allowed** - the rule has the *Allowed* verdict, however, the employee should be informed that his/her actions violate the security policy;

- **Blocked** - the event is blocked by Traffic Monitor which operates in the inline mode or by Device Monitor agent as a result of applying a data protection policy on agents;
- **Quarantined** - SMTP email is quarantined by Traffic Monitor and awaits a decision of the security officer (only if the System operates in the inline mode);
- **Unblocked after quarantine** - the security officer has changed the verdict from *Quarantined* to *Allowed*, and the SMTP email is passed to an external server to be sent to recipients (only if the System operates in the inline mode).
- **Blocked after quarantine** - the security officer has changed the verdict from *Quarantined* to *Blocked* and forbidden sending the SMTP email (only if the System operates in the inline mode).

6. To create a template for the selected verdict, enable the **Send** switch on the selected tab.
7. In the form that opens, specify what items should be included in the email subject and body. By default, inputs fields are displayed where you can enter required text.
8. To add an item to the message subject or body, click **+Add** in the **Email subject** or **Email body** area respectively and choose the required item from the drop-down list. You can choose the following items:
    - **Event ID** - when you add the event ID to the message body, you can also add a link to view the event in the Management Console;
    - **Senders** and **Recipients** - from the drop-down list, choose what details on senders and recipients should be included in the message subject or body. By default, a name and a contact from the event are added;
    - **Policies** triggered in the event. When adding policies to the message body, you can specify what information about policies should be added: the policy name, a description, or both parameters;
    - **Attachments** - from the drop-down list, choose what details on attachments should be included in the message subject or body. By default, the file name and size are added.
    - **Sender's computer**;
    - **Interception date**;
    - **Event type**;
    - **Verdict**;
    - **Violation level**;
    - **Protected objects** triggered in the event;
    - **Message subject** for emails sent by employees;
    - **Source application and destination application**;
    - **Path to file**;
    - **Print task name**;
    - **Resource**.

    To delete an item, clickin the right upper corner of the selected item.
9. If you want to add the event card to the notification, enable the **Attach event card** switch. The notification email will include a file with the event text and the text extracted from attachments. Triggered protected objects are highlighted in the text.

**Important!**

A notification with the event card will be sent to all recipients specified in the **Custom recipients** field. You should see to it that sending event details to external emails should not lead to the leakage of confidential data.

10. Choose the card format: **Microsoft Word** or **PDF**.
11. Specify in what form the highlighted text should be included in the card. Possible choices:
    - **As snippets** - the event text will be exported as snippets which contain triggered protected objects;
    - **All text** - the whole event text will be exported.
12. When you have specified all required parameters, click **Save**.

**Note:**

While creating a notification, you can test the resulting template (see "Testing Notification").

## Testing Notification

While creating or editing a notification, you can test the resulting template. For this:

1. In the right lower corner of the workspace, click **Send test notification**.
2. In the window that opens, specify:
    - **Event ID** - enter an ID of the event which exists in the System;
    - **Recipient** - specify an email address to which a test message should be sent.
3. Click **Send notification**.

A test message with a notification created according to your template will be sent to the specified email address.

## Preset Notifications

There are the following preset notifications in the System:

1. *Notification to violator*. Includes templates that can be sent to the event initiator if the event is:
    - allowed;
    - blocked;
    - quarantined;
    - unblocked after quarantine;
    - blocked after quarantine.

    The notification includes a message on the current state of the event and information about senders, recipients, interception date and time, resources, and attachments.
2. *Notification to security officer*. Includes templates that can be sent to the security officer if the event is:
    - allowed;
    - blocked;

- quarantined.

The message subject includes information about the incident, its violation level, and the verdict. The message body includes the following data:

- event ID;
- interception date and time;
- event type;
- violation level;
- verdict;
- triggered policies;
- triggered protected objects;
- sender's computer;
- senders;
- recipients;
- resource;
- message subject;
- attachments.

# 5 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:

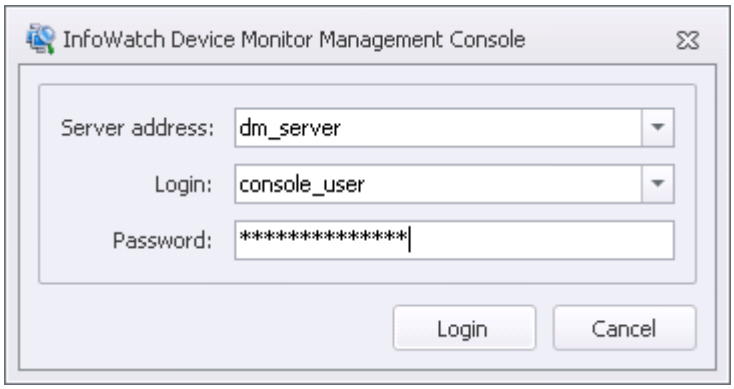
1. Start the Management Console (DM). For this, in the **Start** menu, choose **Programs** > **InfoWatch** > **Device Monitor** > **Management Console** or use the desktop shortcut (created by default during installation)..
2. Perform the authorization procedure as described below.

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.



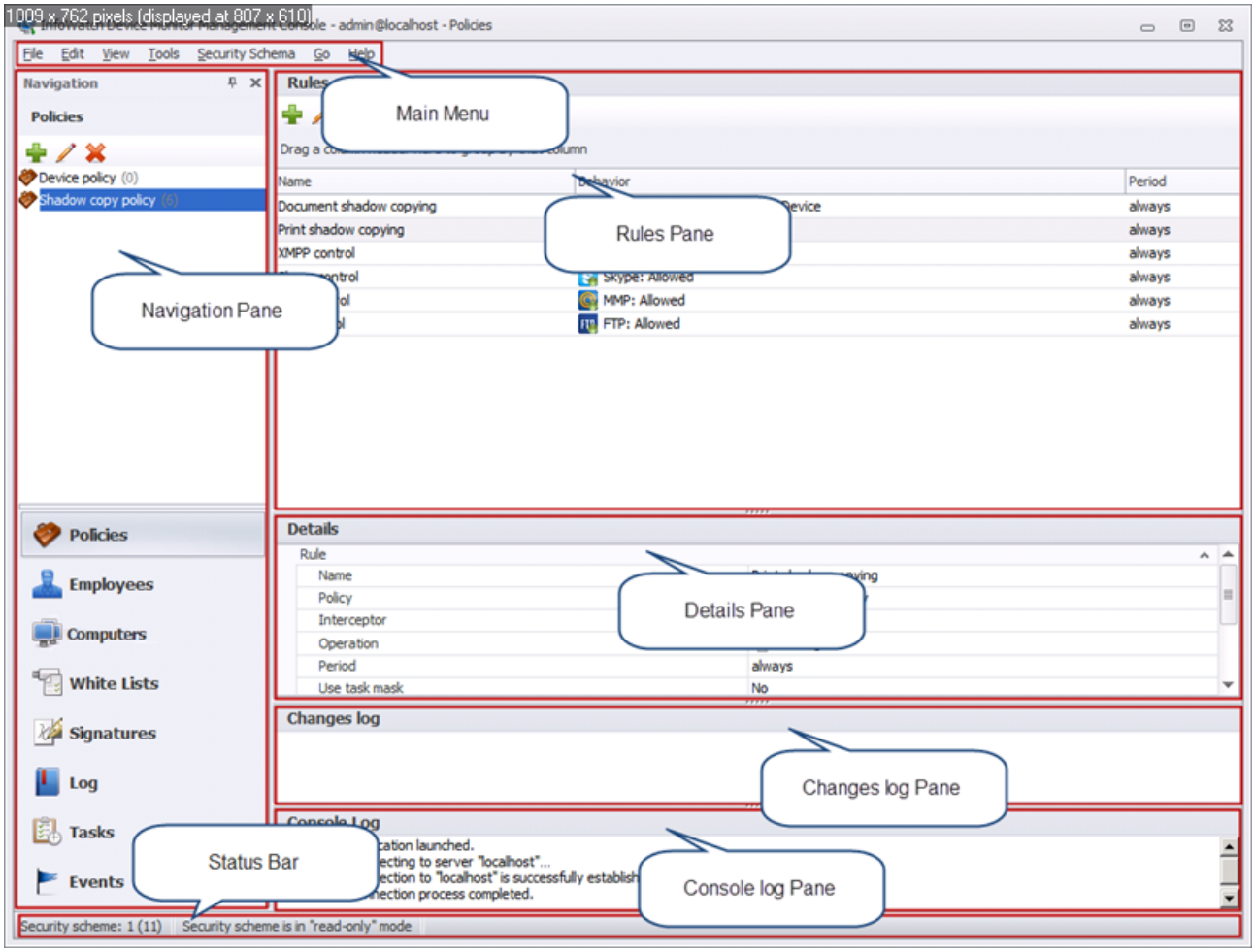

| Parameter | Description |
|---|---|
| Server address | FQDN of the server, the Management Console is connecting to.<br>Th default port for communication between the server and Management Console is 15003. If this port has been changed, enter the server address as follows: `dm_server:port` |
| Login | Name of the user account |
| Password | User password.<br>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.<br>**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. |
| Return to the initial interface settings | Click **View** in the Main Menu and click on **Reset interface options**. After that DM concole should be restarted.<br>**Note:** In this case the previously used columns order and grouping on the **Working area of the main window**<br>will be returned as well as the initial **Navigation pane** settings. |

**Details** 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 |
| White Lists | 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 | | + | |
| 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 | | + | + |

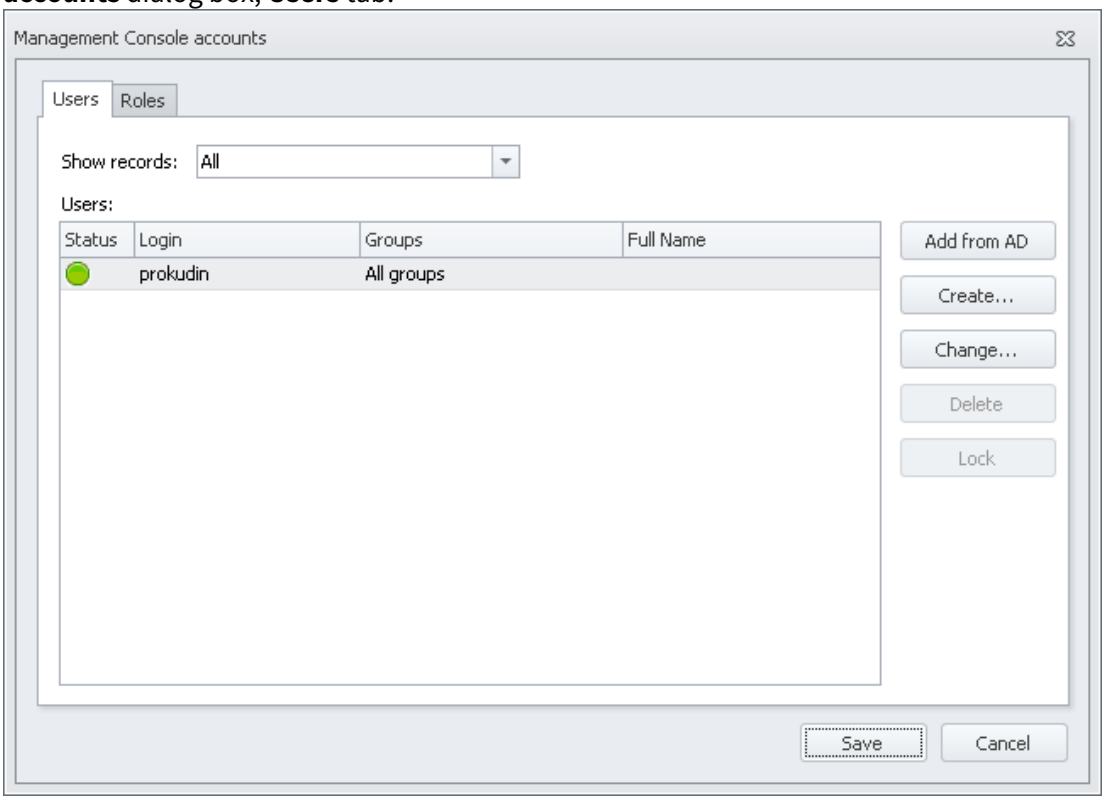
For more information on Management Console (DM) accounts management, see:

- 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:

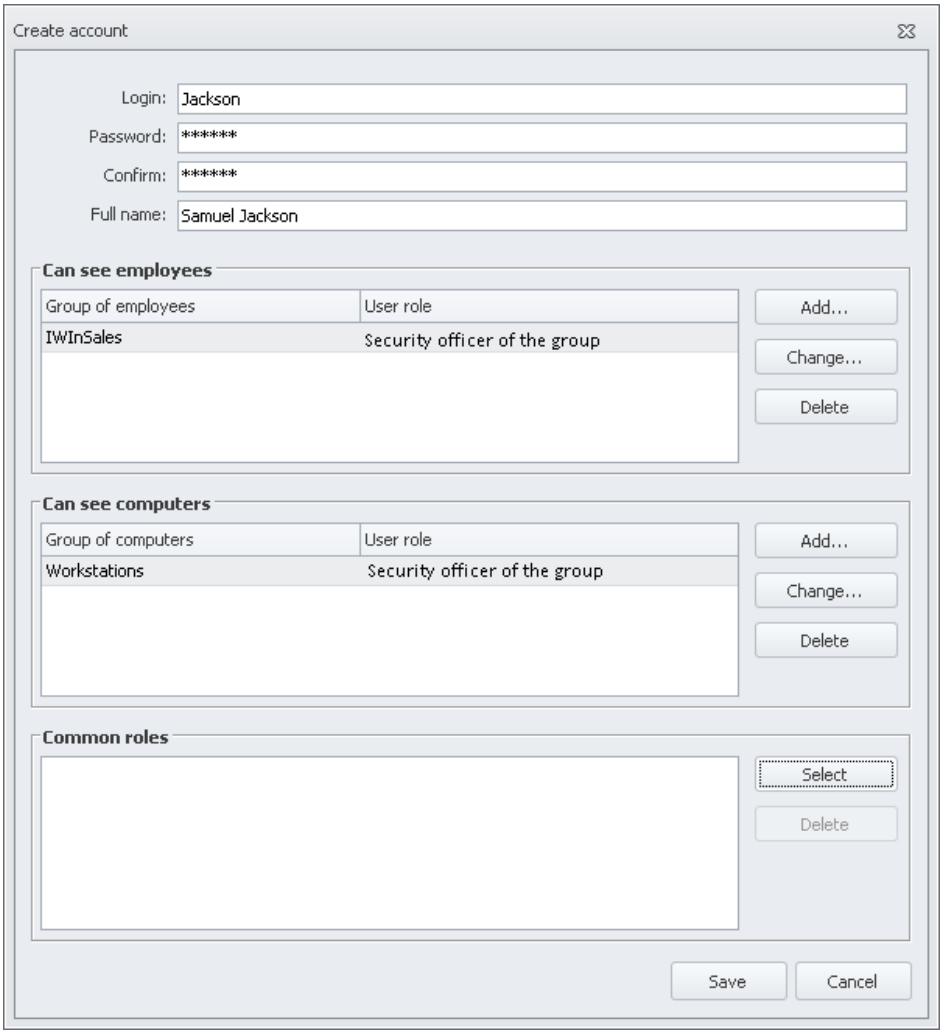
- **Status**. Indicates if the account is active (), blocked () or deleted ().
- **Login**. Name of the user account.
- **Groups**. Groups available to the user.
- **Full Name**. User's personal data.

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.

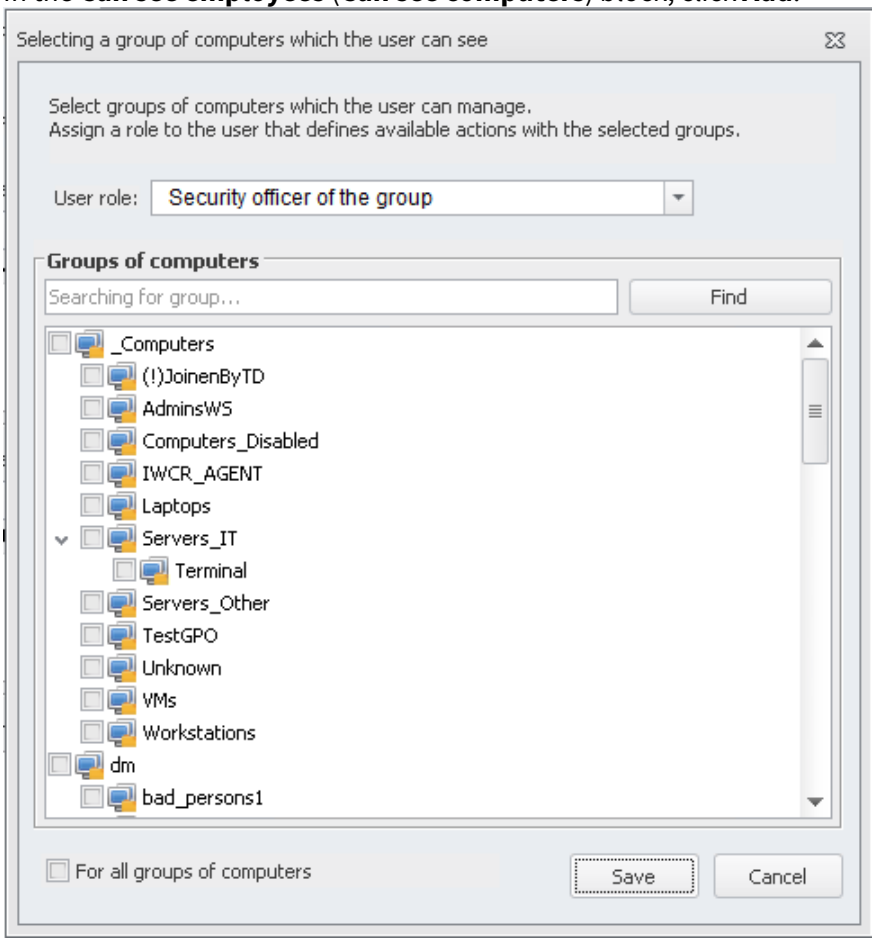
Assigning Roles to User

**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:**

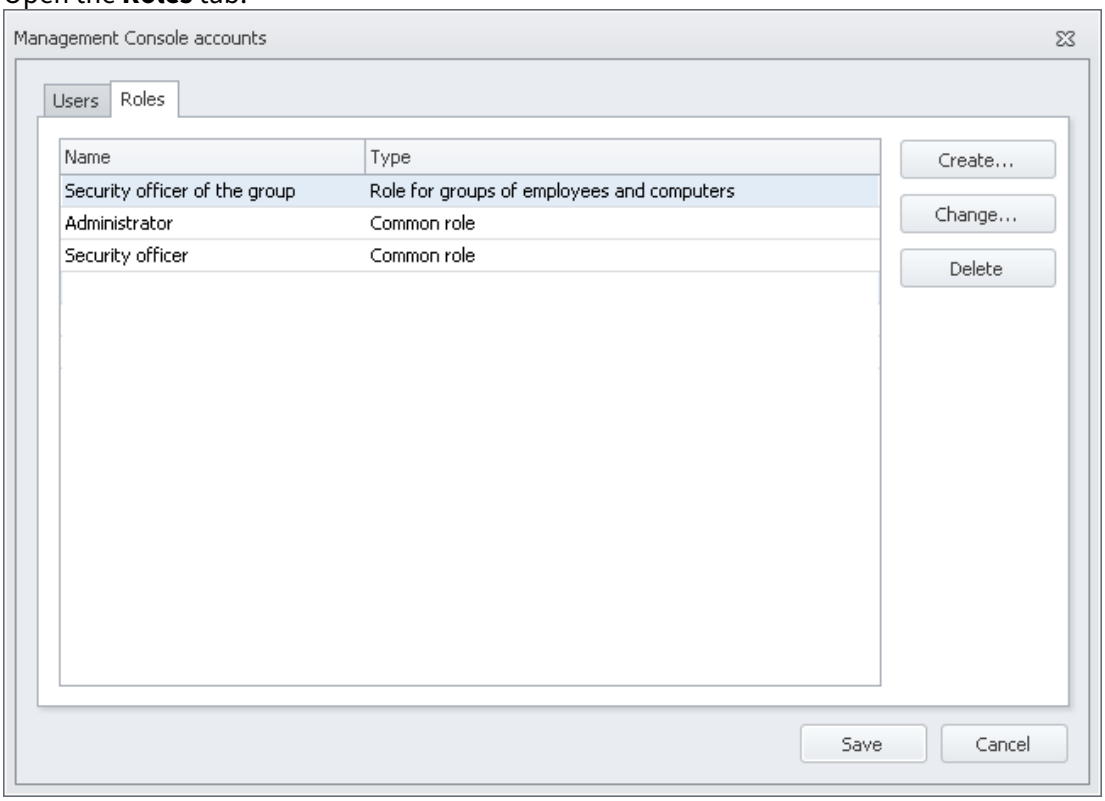
1. In the Main Menu, click **Tools > Console users and roles**. This opens **Management Console Accounts** dialog box.
2. Select a row that contains the account you want to delete.
3. Click **Delete** in the right part of the dialog box.
4. In the confirmation dialog, click **Yes**.
5. To apply changes, 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.

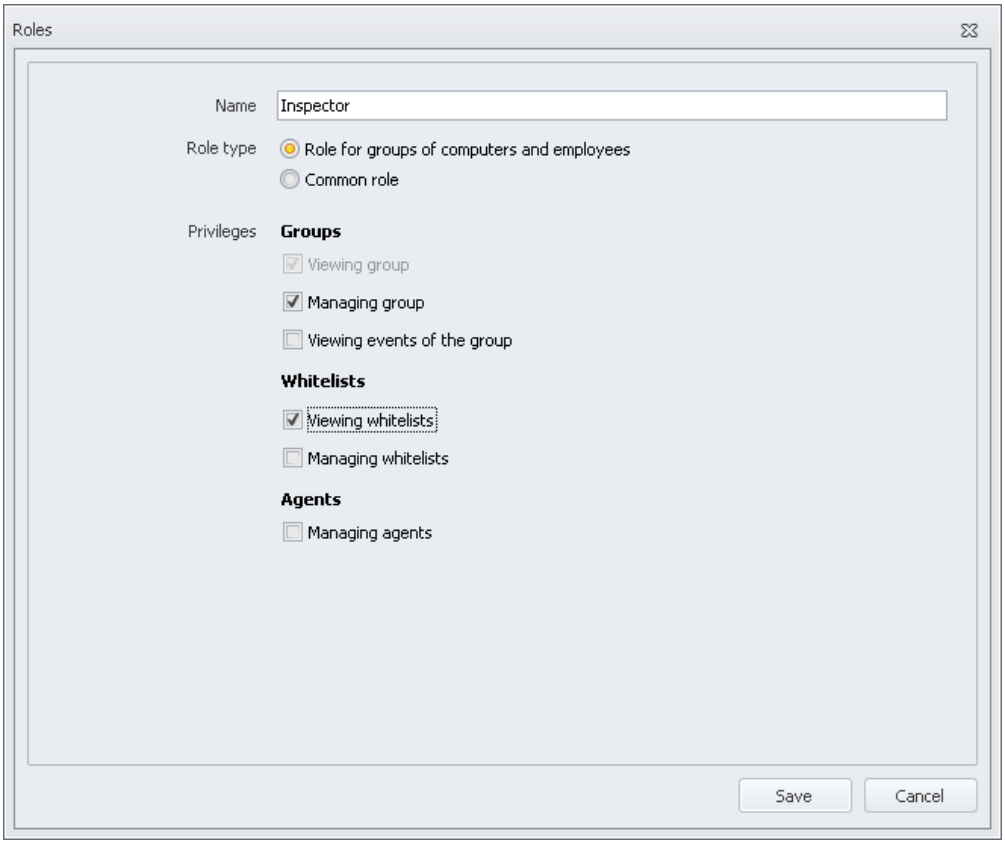
For a detailed description of privileges, see "Adding Role of the Management Console (DM) User".

## 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<br>• View the group parameters<br>• View the list of computers/employees included in the group<br>• View the effective policy for the computer/employee<br>• 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)<br>• Add/delete computers/employees of the group<br>• Copy computers, employees or subgroups of the group<br>• Manage all subgroups of the group<br>• Delete groups<br>**Note:** adding this privilege enables the **View group** privilege. |
| View group events | View events received from workstations/employees of the group and its subgroups.<br>**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.<br>**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.<br>**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<br>• Create new policy<br>• 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)<br>• Create new policy<br>• 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.<br>**Note:** adding this privilege enables the **View audit log** privilege. |
| Manage users | ▪ View Console users and roles<br>▪ Create Console users and roles<br>▪ Edit Console users and roles<br>▪ 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.<br>**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<br>• Add computers through the file import or by name/IP in the agent distribution task<br>• Create installation package<br>• 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<br>**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.<br>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

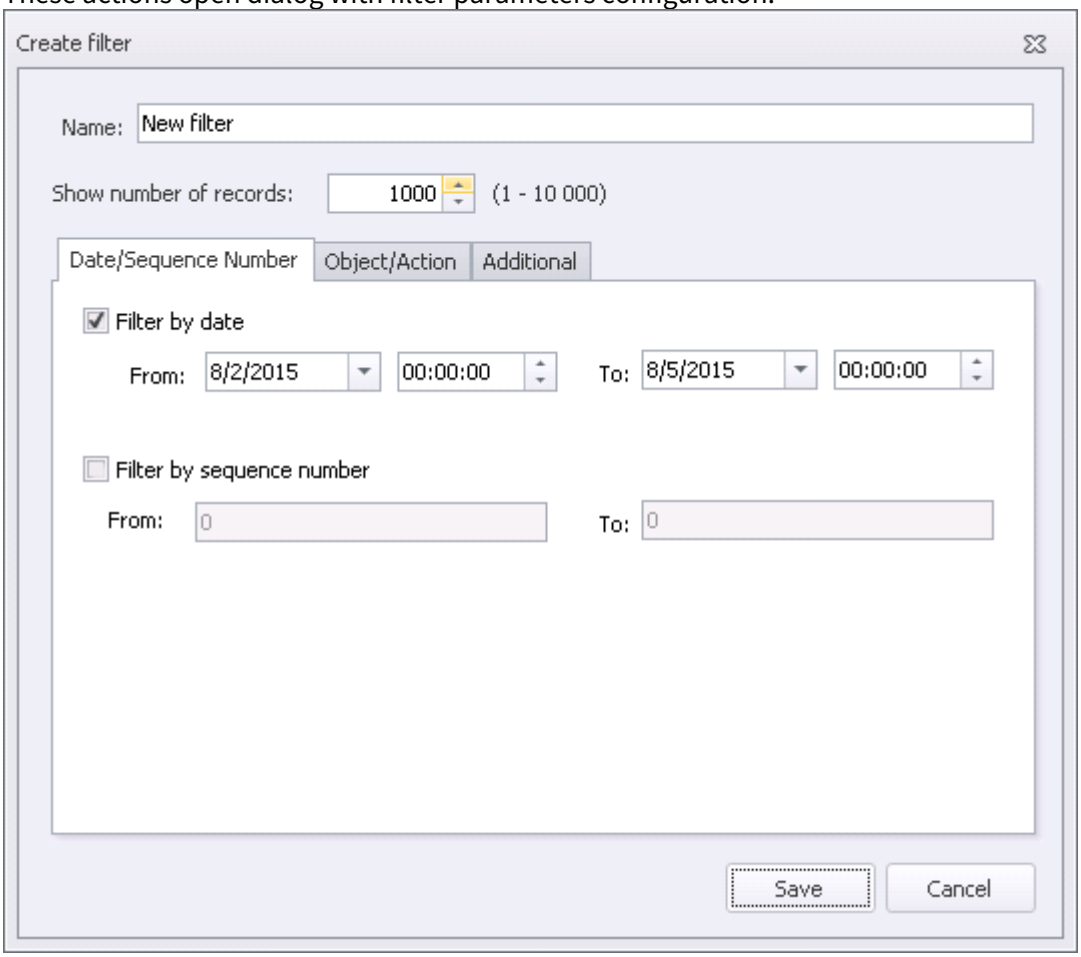
To access audit log records that meet certain criteria, you can use filters.

**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**;<br>• click **Create filter** at the top of Navigation pane;<br>• right-click in the **Log** area and choose **Create Filter** from the context menu;<br>• press Ctrl+N. |
| Editing filter | a. In **Log** area of Navigation pane, select the name of the filter you want to edit.<br>b. Take one of the following steps:<br>• In Main Menu, click **Edit > Edit filter**;<br>• click **Edit Filter** at the top of Navigation pane.<br>• double-click with the left mouse button on the name of the chosen filter;<br>• right-click the selected filter and choose **Edit** from the context menu;<br>• 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:**

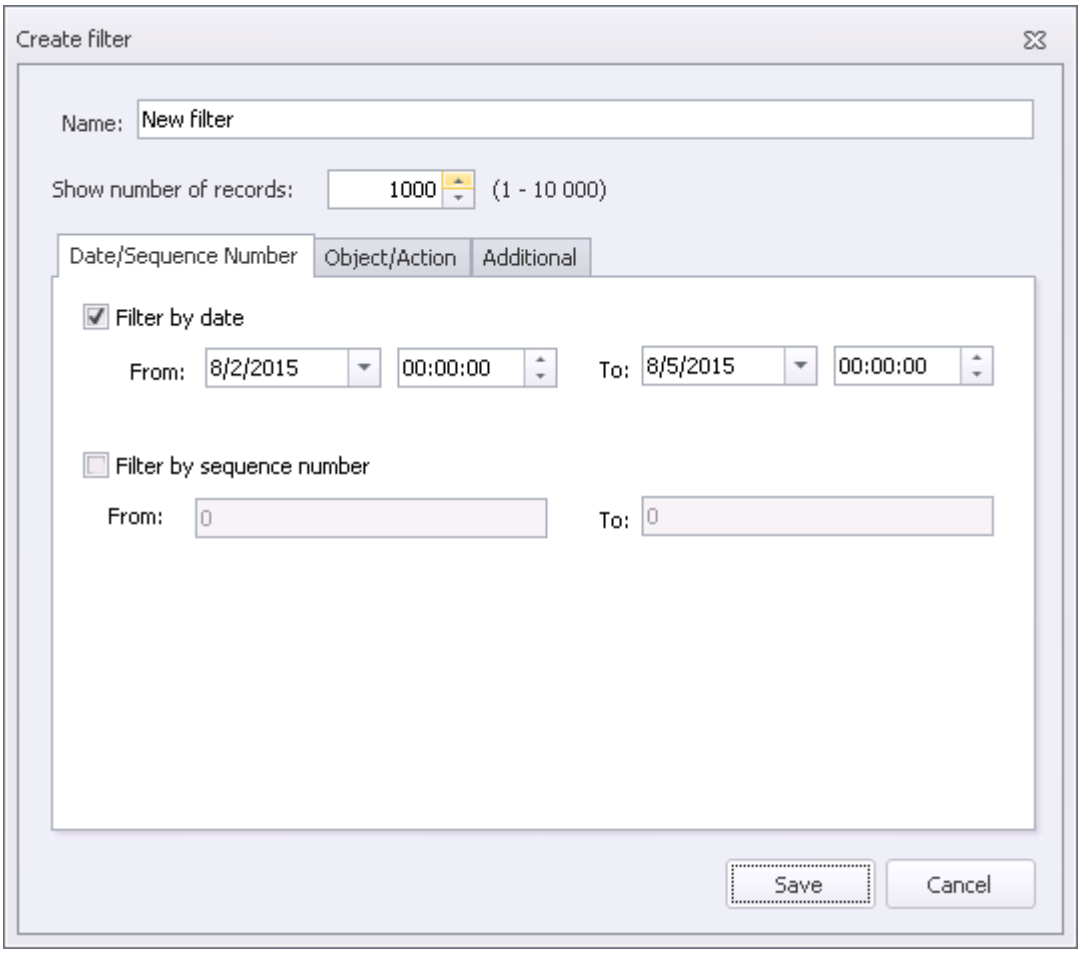
1. Go to **Log** section.
2. In the **Log** area of Navigation pane, select the name of the filter you want to remove.

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.

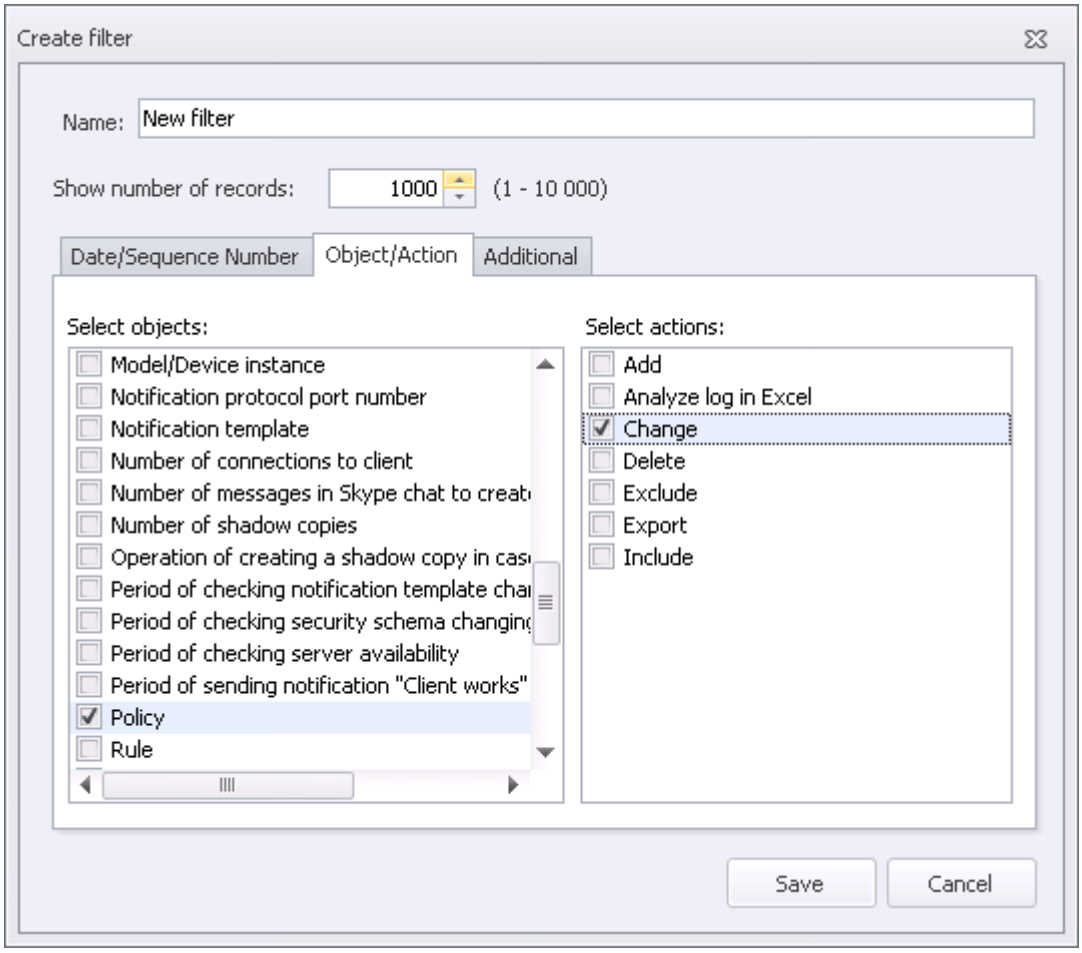
**To filter by number:**

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
- Corporate Network Control
- Messengers Control
- Network Traffic Control
- Device Monitor Server Settings. Connecting to Traffic Monitor Server
- Active Directory Connecting and Synchronizing
- Employee Notifications about Policy Violations
- Exclusion of Application from Interception
- Application control
- Event Storage
- Synchronization of Traffic Monitor Policies
- InfoWatch Device Monitor Server Manager
- Stopping and Starting Device Monitor Agent
- Control of Keyboard Input

**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. Default value – 600 seconds. |
| Period of checking server availability | Interval (sec) with which the Agent checks Server availability. Default value – 2400 seconds. |
| Period of checking security schema changing for active agent only | If the Agent operates in an active mode (the Agent itself polls the Server for security schema modification), then this parameter sets the polling frequency (in seconds). Default value – 600 seconds. |
| Period of checking notification template changing for active agent only | If the Agent operates in an active mode (the Agent itself polls the Server for modifications of notification templates), then this parameter sets the polling frequency (in seconds). Default value – 1800 seconds.<br>**Note**: For details on notification templates, see "Employee Notifications about Policy (DM) Violations"). |
| **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. Default value – 10%. 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 "Device Monitor Rule (DM)", "Cloud Storage Monitor Rule (DM)", "Viewing Events". The following options are available:<br>• **None** - do not save events<br>• **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<br>• **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 "Network Monitor Rule (DM)". The following options are available:<br>• **None** - do not save events<br>• **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.<br>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.<br>**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**.

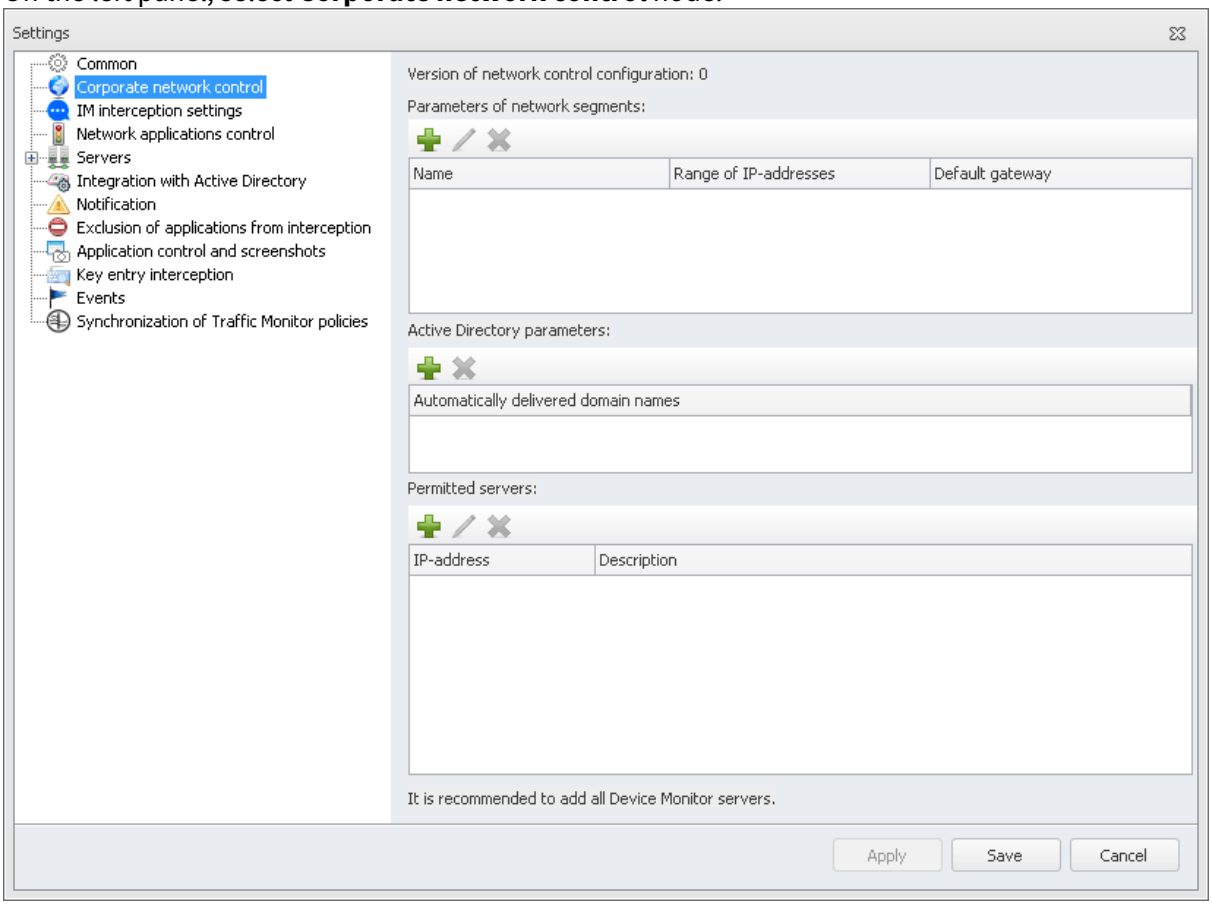
## 5.3.2 Corporate Network Control

To provide the data transfer control via network connections using **Network Monitor** (information on configuring the rule (DM) see in "Network Monitor Rule (DM)") you should specify the network segments to be considered the corporate network and which external addresses are permitted.

> **Note:**
>
> Permitting the external addresses can be required to provide the work with external resources when the Agent is outside the corporate network, such as VPN server or corporate network.

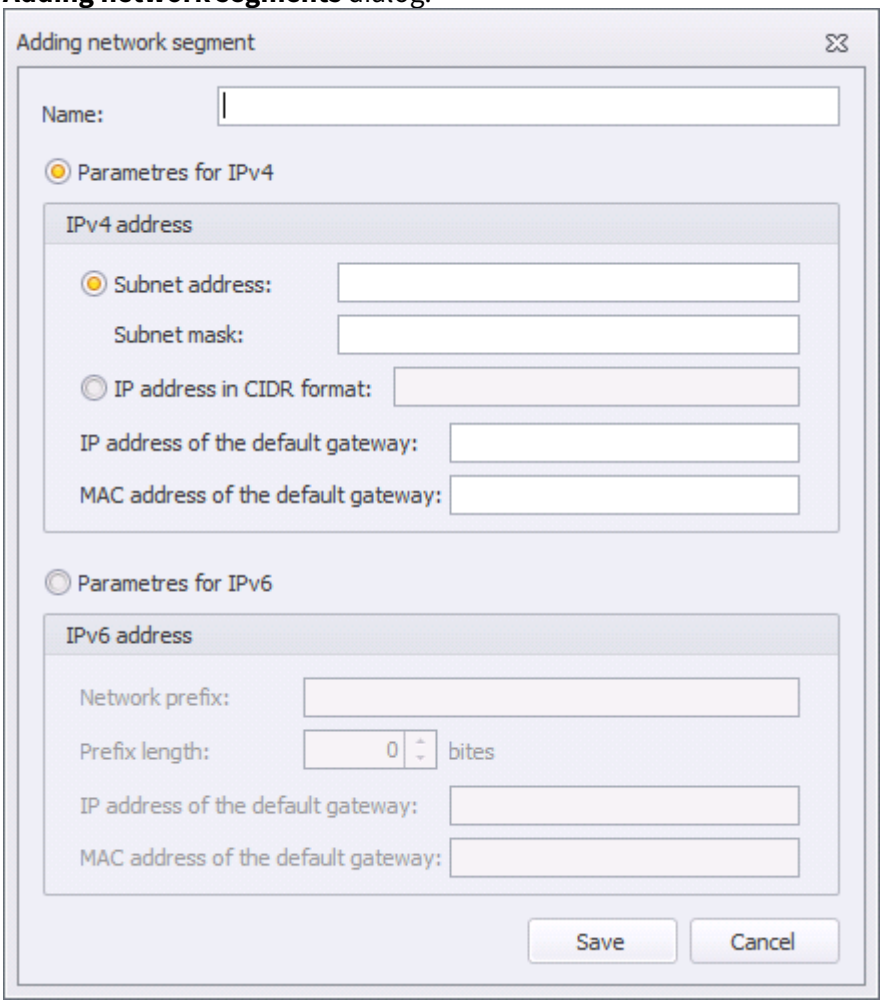
**To configure corporate network settings**:

1. In the Main Menu, select **Tools** > **Settings**.
2. On 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 have 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 have 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.

4. To define Active Directory parameters, click in the **Active Directory parameters** area. 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 **OK**.
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**.

**How the System detects connections to the corporate network for different cases:**

1. Only **Parameters of network segments** are specified. In this case, both domain and non-domain workstations are considered to be on the corporate network if:
   a. The IP address of the workstation is included in one of the specified segments.
   b. The IP address and MAC address of the default gateway correspond to the values specified for this segment.
2. Only **Active Directory parameters** are specified. In this case:
   a. A domain workstation is considered to be on the corporate network if:
      i. The network has a domain with the specified parameters.
      ii. It is possible to connect through a specific network adapter to a domain controller the workstation belongs to.
   b. A non-domain workstation is considered to be always on the corporate network.
3. Both **Parameters of network segments** and **Active Directory parameters** are specified. In this case:
   a. A non-domain workstation is considered to be on the corporate network if:
      i. The network has a domain with the specified parameters.
      ii. It is possible to connect through a specific network adapter to a domain controller the workstation belongs to.
   b. A domain workstation is considered to be on the corporate network if:
      i. The IP address of the workstation is included in one of the specified segments.
      ii. The IP address and MAC address of the default gateway correspond to the values specified for this segment.

   OR
      i. The network has a domain with the specified parameters.
      ii. It is possible to connect through a specific network adapter to a domain controller the workstation belongs to.

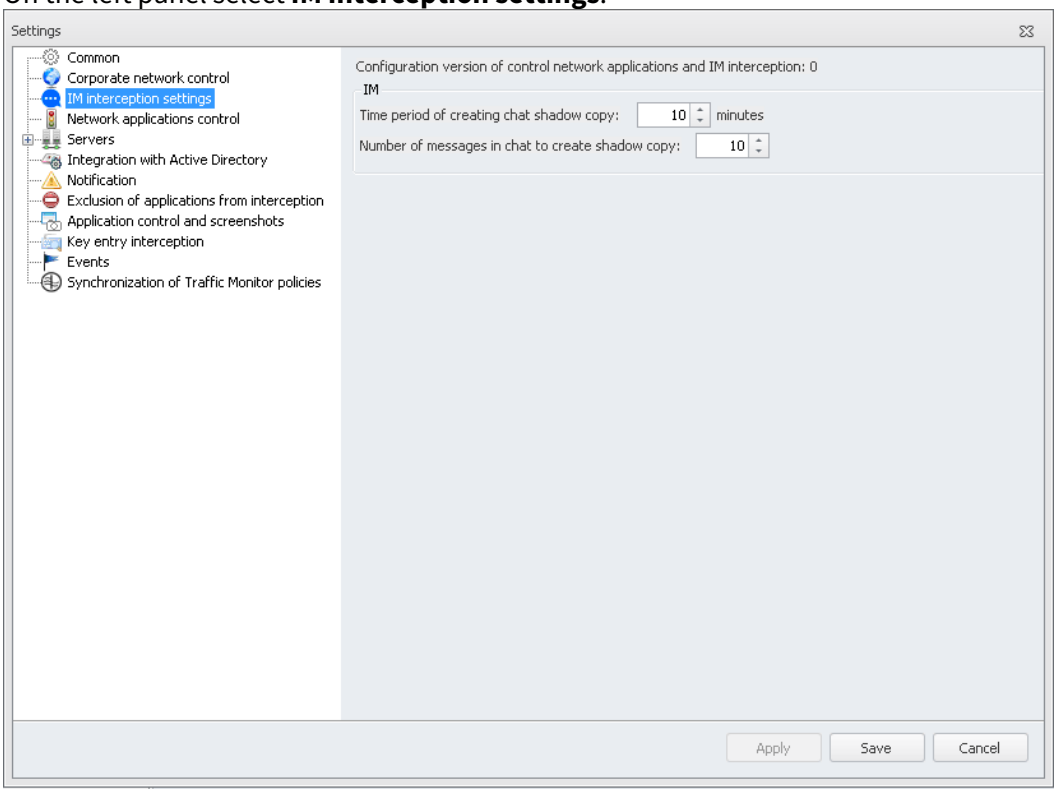
### 5.3.3 Messengers Control

When controlling the traffic, you can set additional settings for messengers (for more information on configuring this type of DM rules, please see IM Client Monitor Rule (DM)).

To configure the messengers control:

1. In the main menu select **Tools > Settings**.

2. On the left panel select **IM interception settings**.




3. Specify the messengers control settings: set the assembling frequency for chat shadow copy to be sent for analysis to Traffic Monitor. You can specify the time frame (minutes), after expiration of which the shadow copy should be assembled (**Time period of creating chat shadow copy**), the number of messages, beyond which the shadow copy should be assembled (**Number of messages in chat to create shadow copy**). If the file sending is being processed within the chat, the shadow copy can be assembled before the period specified.

### 5.3.4 Network Traffic Control

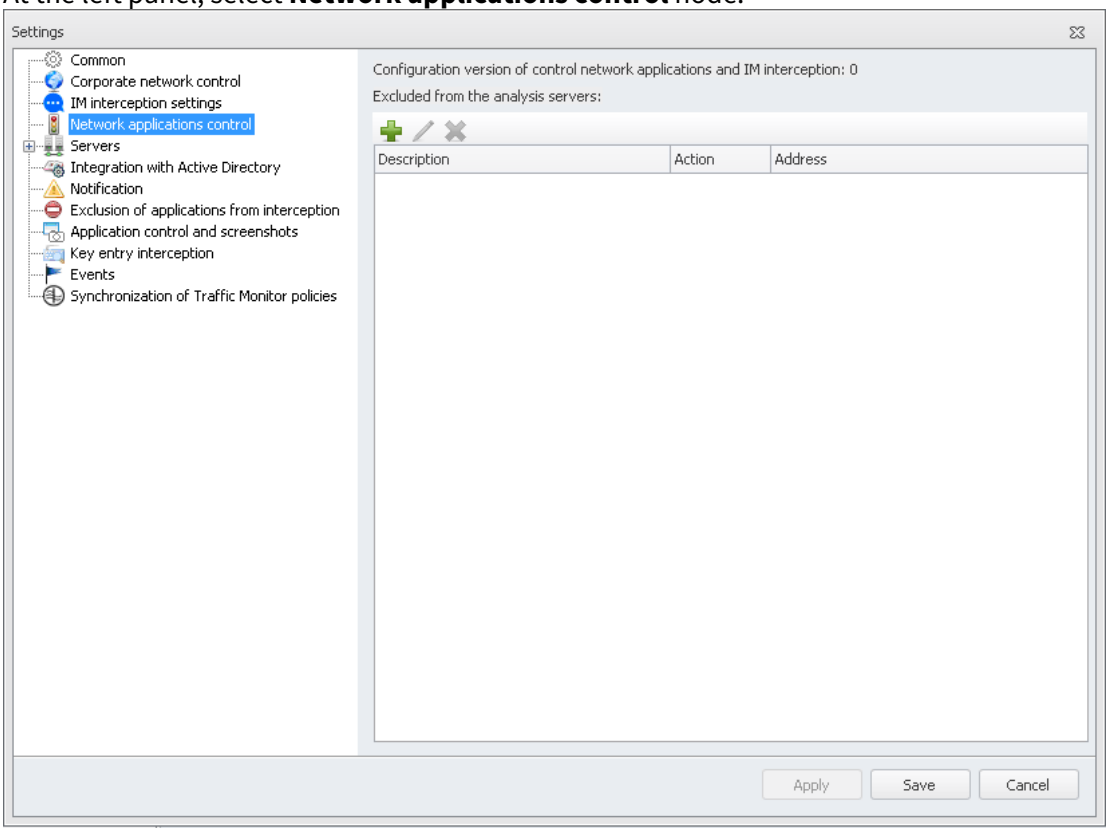
In order to provide control of network traffic, Device Monitor Agent acts as a transparent proxy server, to which all the connections are redirected irrespective of the protocol. Then Device Monitor Agent parses the protocol and defines if this protocol is a subject of interception. Controlled protocols are FTP, FTPS, POP3, SMTP, S/MIME, Outlook, 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 mail systems (see "Mail Monitor Rule (DM)"), and FTP/FTPS taffic (see "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 applications control** node.




3. You can specify a list of server IP addresses which protocols will not be controlled (i.e. traffic sent to those servers will not be redirected to internal proxy server) or will be compulsory controlled (to be redirected to internal proxy server).

> **Note:**
>
> Permitting external addresses can be required to provide work with external resources and update the programs installed, 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.

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, enter the server description. For more information on addresses that can be added, see "Processing Addresses Added to Exclusions".
c. Select an option: **Exclude from interception** или **Include into interception**.
d. Specify DNS name or IP address of a server and connection port.
e. If required, select **Address range** and set the spacing options between IP addresses.

> **Note:**
>
> When excluding server from interception, you can also select and enter **Domain from MiM interceptor**, which traffic is to be excluded from interception using SSL connection.

f. Click **OK**.
g. To change the server parameters, select it in the list and click .
h. To delete a server from the list of excluded ones, select it, click , then click **Yes** in the confirmation dialog.

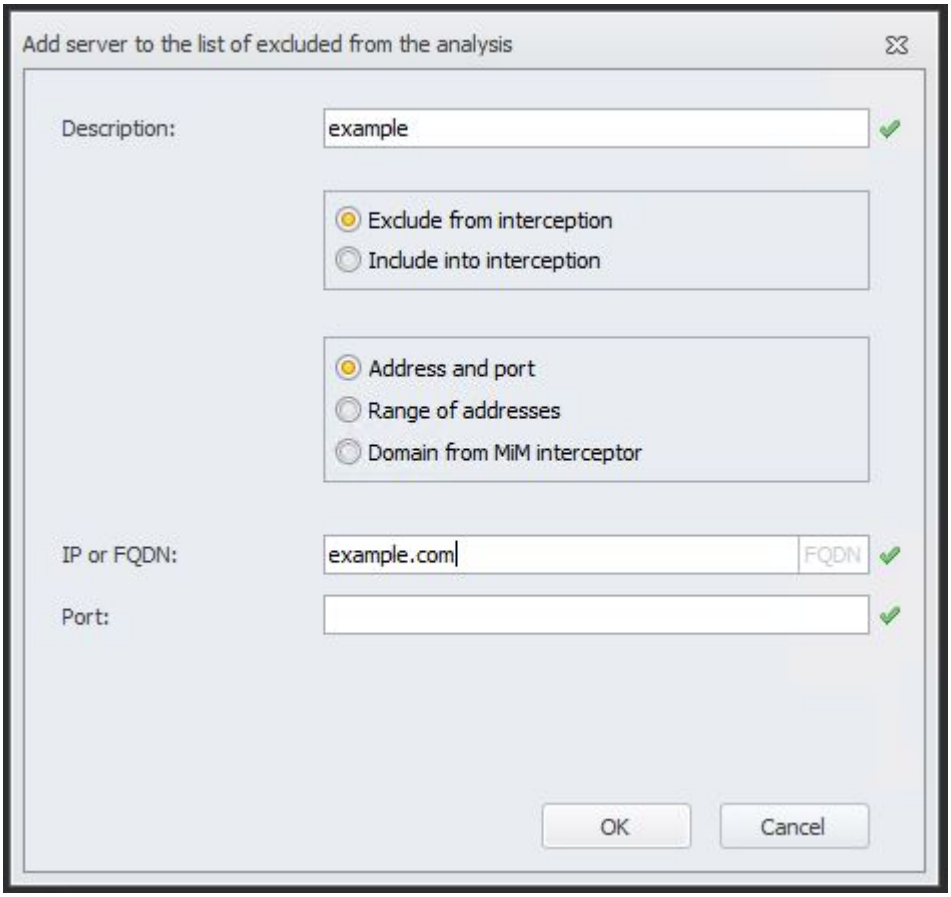
4. When all changes are made, click **Apply**.

## Adding Servers to Exclusions

Adding server address to exclusions, (see "Network Traffic Control") it is required to specify the server IP address or FQDN.

To set the list of servers, permitted or forbidden:

1. In **Servers excluded from analisys** area press .
   Then the window to add the server will open:



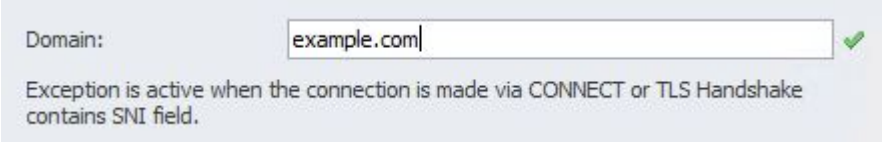

2. In the window **Add server to the list of excluded from analysis** enter the server description:
   - To add a separate server port:
     a. Select the required action: **Exclude from interception** or **Include into interception**;
     b. Select the check box in the field **Address and port**;
     c. Specify FQDN or server IP address (IPv4 or IPv6) and connection port;

   - To add the addresses range:
     a. Select the required action: **Exclude from interception** or **Include into interception**;
     b. Select the check box in the field **Range of addresses**;
     c. Specify server IP address (IPv4 or IPv6) in the required fields




   - To add the resources group exclusion from interception via SSL/TLS connection template:
     a. Select **Exclude from interception**;
     b. Select the check box in the field **Domain from MiM interceptor**;

c. Specify the domain




3. Click **OK**.

In the form of a text IPv4 address is speciified as nnn.nnn.nnn.nnn, where nnn has a value from 0 to 255 and each n letter means decimal figure. Zero with no value should not be specified.

In the form of a text IPv6 address is speciified as xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, where each x letter is a hexadecimal figure, meaning 4 bits. Zero with no value should not be specified.

**Note:**

Including into interception has higher priority than exclusion.

Exclusion template will operate in case the agent is connected via proxy server.

0.0.0.0 address is applied only together with a port, since it is a special address for all the exclusions with the port specified.

**Example 1:**

To exclude from interception the whole 10.128.0.2 traffic, except the one for port `8080`:

1. Exclude from interception the server with IP address `10.128.0.2` not specifying the port;
2. Include into interception the server with IP address `10.128.0.2`, specifying the port `8080`.

**Example 2:**

To exclude from interception range of addresses `192.168.0.1` - `192.168.0.255` except one specific address `192.168.0.5`:

1. Exclude from interception a range of addresses `192.168.0.1` - `192.168.0.255`;
2. Include into interception the server with IP address `192.168.0.5`.

**Example 3:**

To exclude from interception the port `8080` on all the servers, exclude from interception the server with IP address `0.0.0.0`, specifying the port `8080`.

To change server configuration, select it in the list and click .

To remove server from the list of permitted ones, sklect the one required and click , then cleck **Yes** to confirm thr removal.

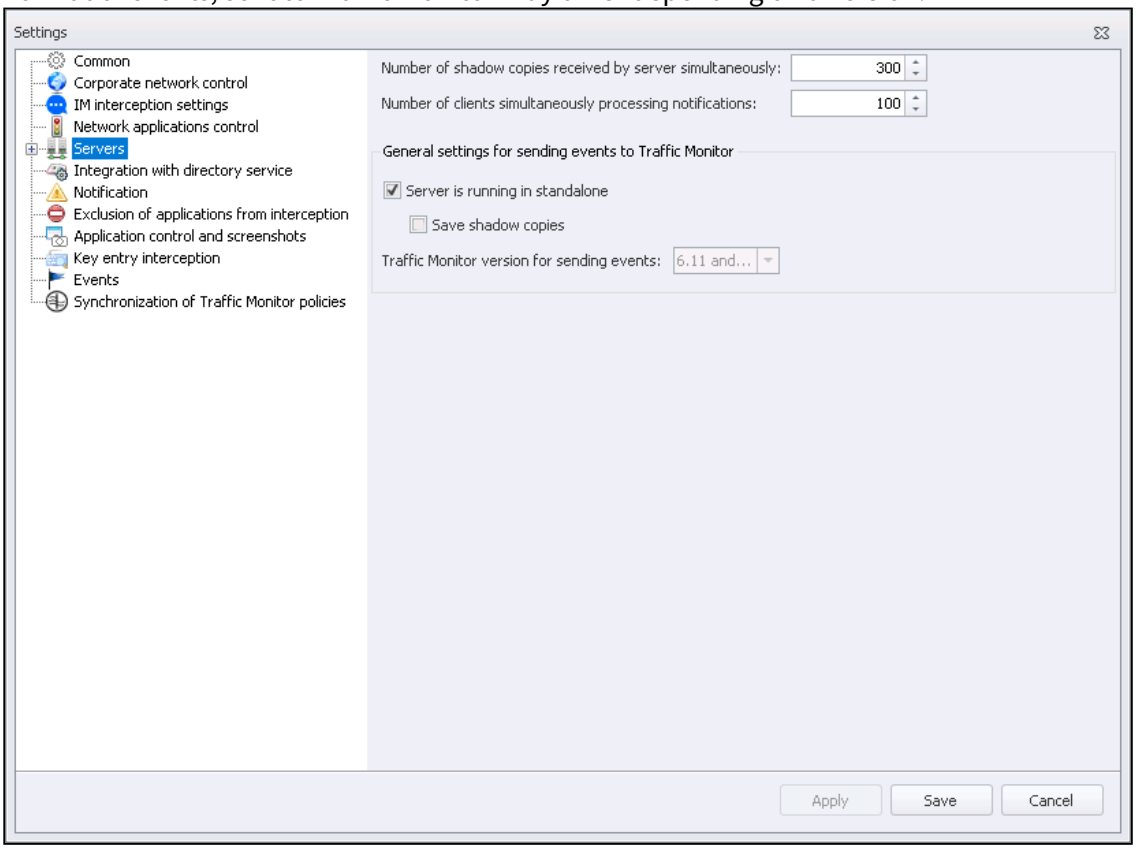
## 5.3.5 Device Monitor Server Settings. Connecting to Traffic Monitor Server

You need to set up connection parameters to be able to send events to Traffic Monitor.

**To view and set up Traffic Monitor connection parameters**:

1. In main menu select **Tools -> Settings**.
2. In the **Servers** node, set up the following parameters:

- **Number of shadow copies received by server simultaneously**: - determine the number of copies that 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 the server at a time
- **Server is running in standalone** - the 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.

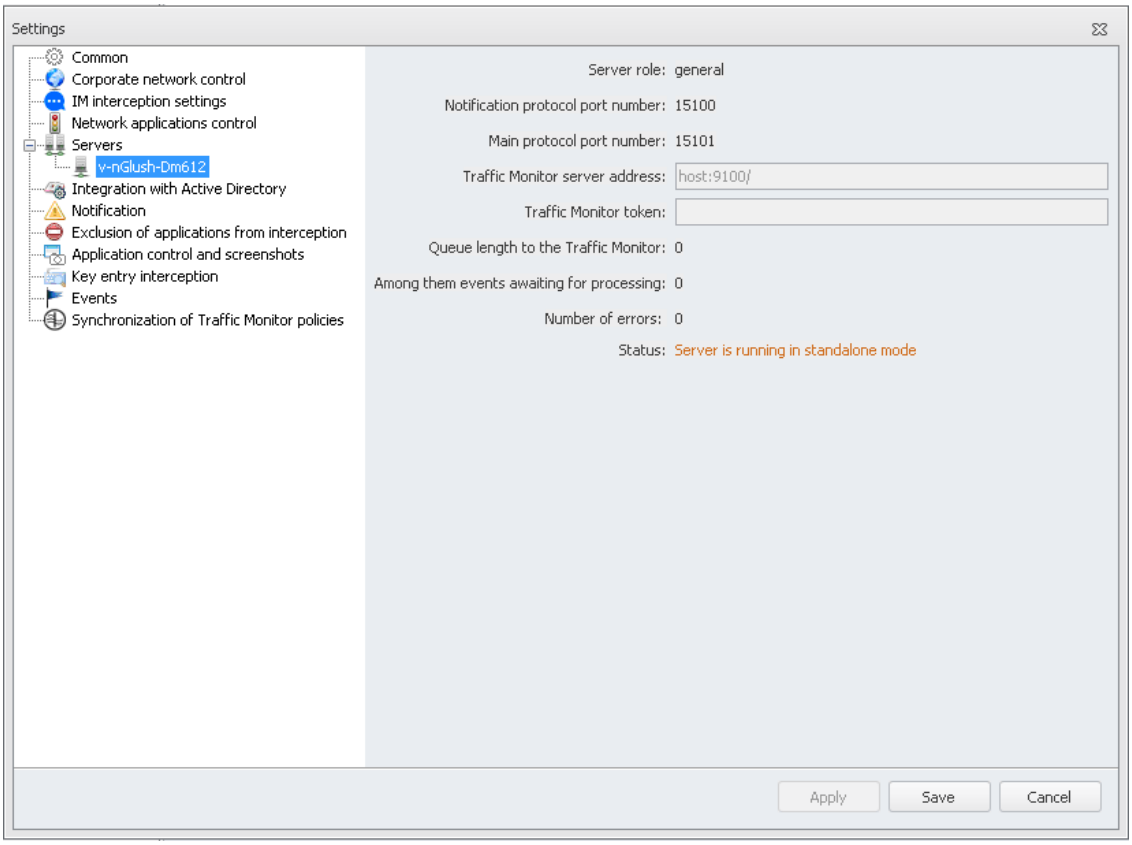



3. When selecting the server name, the information on the following connection parameters is available:
    - **Server role** – server role (primary or secondary), assigned to this server during installation: see "*InfoWatch Traffic Monitor. Installation Guide*", article "InfoWatch Device Monitor Server End Installation Procedure".
    - **Notification protocol port number**.
    - **Main protocol port number**.

> **Note:**
>
> Changing server role (General or Secondary) and attribute Notification protocol port number and Main protocol port number are being executed with InfoWatch Device Monitor Server Manager (see "InfoWatch Device Monitor Server Manager").

- **Connection string to a Traffic Monitor** – address of InfoWatch Traffic Monitor server to work in the Management Console. This server will receive events.
  Supported formats:
  - `host:port`
  - `protocol://host:port/`, where `protocol` should be `xml` for Traffic Monitor versions under 6.0 and `rcp` for Traffic Monitor versions 6.0 or higher
  - `host:port/`

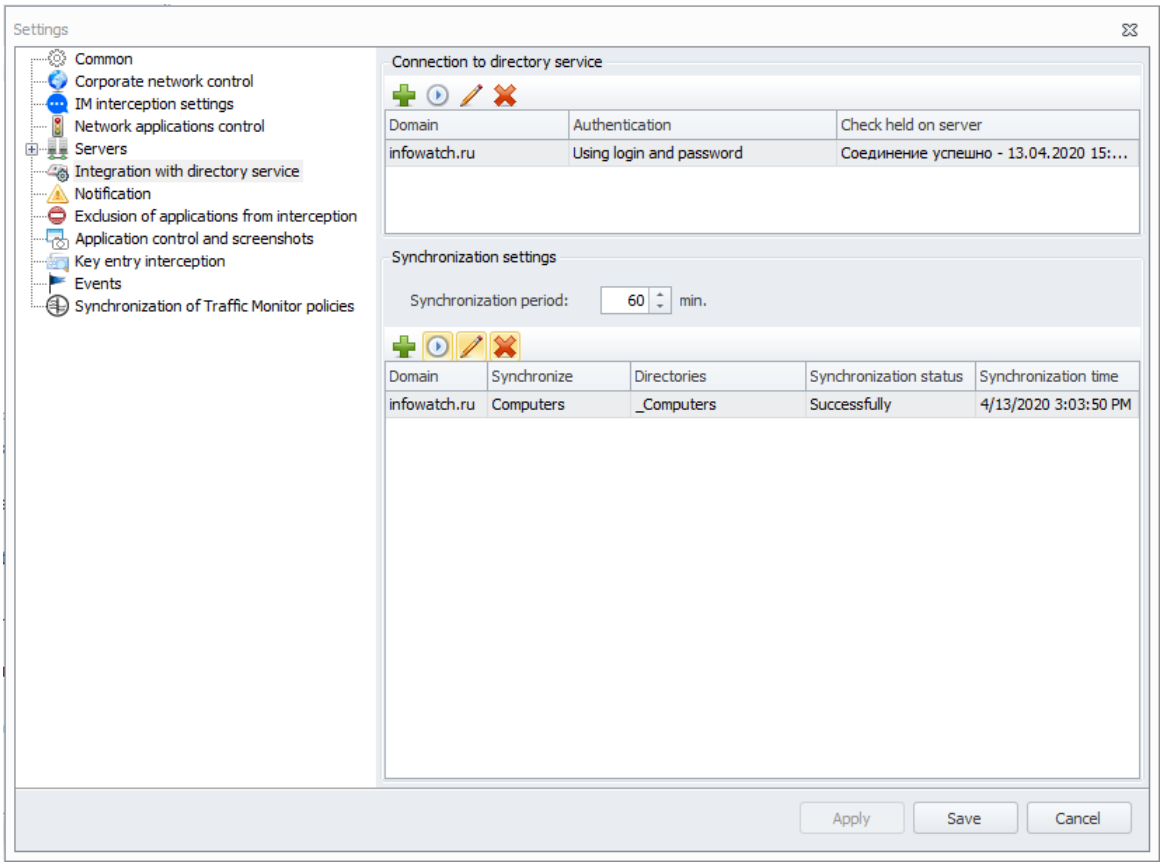
  The connection string should be in the URI (Uniform Resource Identifier) format whose formal syntax described in RFC 3986 http://tools.ietf.org/html/rfc3986.
  The *port* parameter contains InfoWatch Traffic Monitor server port that delivers events. InfoWatch Traffic Monitor default server port is 9100.
- **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** – the number of events in the error queue.
- **Status** – information on Traffic Monitor connection state.




4. When all changes are made, click **Apply**.
5. Click **Save**.

## 5.3.6 Active Directory Connecting and Synchronizing

You can specify all the attributes of synchronization and connection to directory service in settings. Indicate connection settings when connecting to LDAP using management console. To receive information about computers and employees from directory services, specify LDAP server connection parameters.



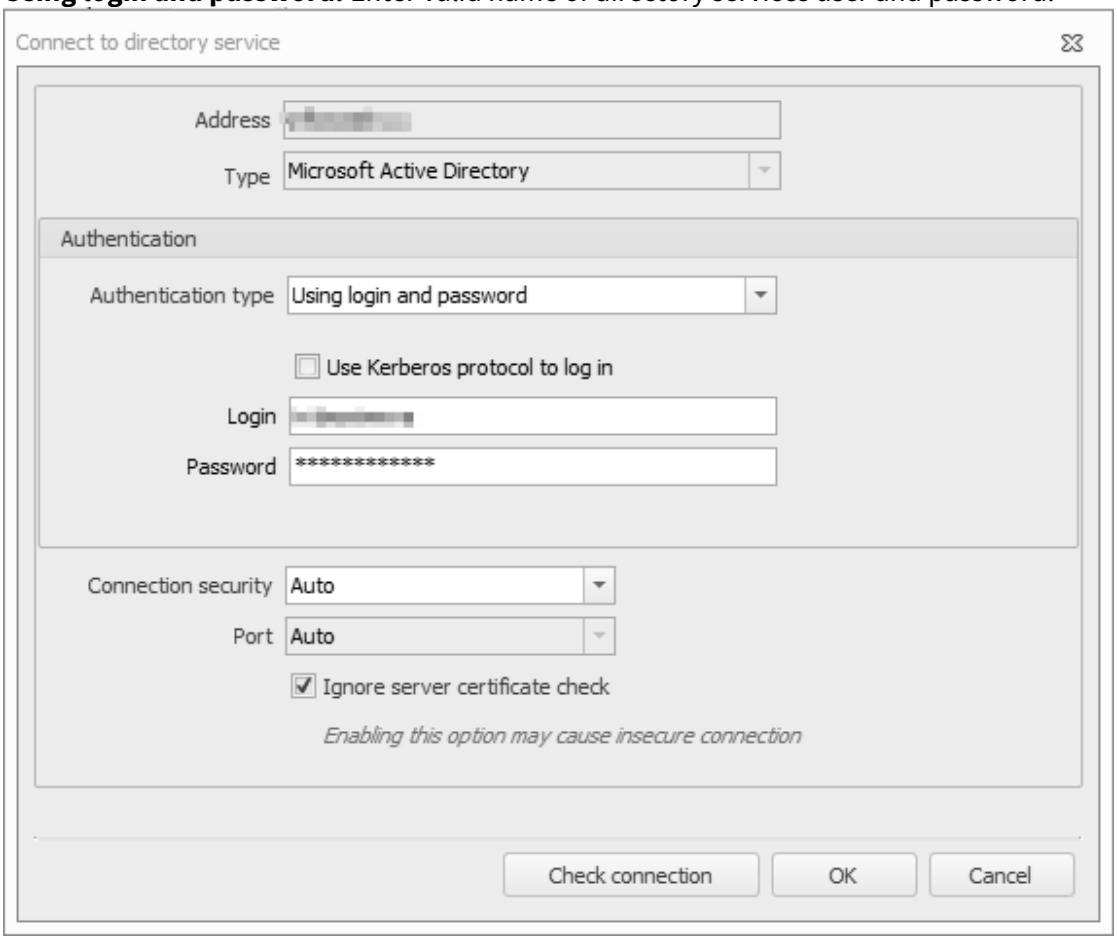

**To configure synchronization parameters with LDAP server:**

1. In main menu of management console (DM) select **Tools** > **Settings**.
2. Open **Integration with directory service**.
3. If you connect to directory service for the first time, click  in **Connection to directory service** section.
4. In **Address** field specify LDAP server domain name, IP address or click **Select domain from forest**. The forest should be selected in accordance with the user, who started the management console.
5. Specify directory service, if you know it or select **Auto**. After successful connection is confirmed, **Auto** type will be changed to this LDAP type.

   > **Warning!**
   >
   > Once the connection settings are saved, the type of directory service cannot be changed.

6. Specify Authorization details to connect to directory service:

- **Using login and password.** Enter valid name of directory services user and password.




- **User account.** Credentials of the current Windows session, that the System was started under, will be used for authorization.
- **Using client certificate.** Specify the full name of private key and certificate in `.p12` or `.pfx` format and the key password.
- **Anonymous.**

7. When selecting **User account** or **Using login and password**, you can also add Kerberos protocol support.
8. Click **Advanced** to establish secure connection and select from: **Auto**, **STARTTLS, LDAPS** or **Unprotected**. If you select Kerberos protocol support or **Using client certificate**, **Auto** will be applied.

> **Warning!**
>
> Synchronization using secure connection is supported for ActiveDirectory only.

9. Indicate the port, that will pespond to requests when the default port 389 is unavailable: **Auto**, **636**. If you select **Auto** or **Using client certificate**, or enable Kerberos protocol support, then **Auto** will be applied.
10. Enable the option **Ignore server certificate check**, if you don't need to check the certificate, that is sent from server while establishing secure connection.
11. Click **Check connection** and make sure that it is successfully established.

12. Click **OK**.

**To check connection to previously created synchronizations:**

1. In **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**.

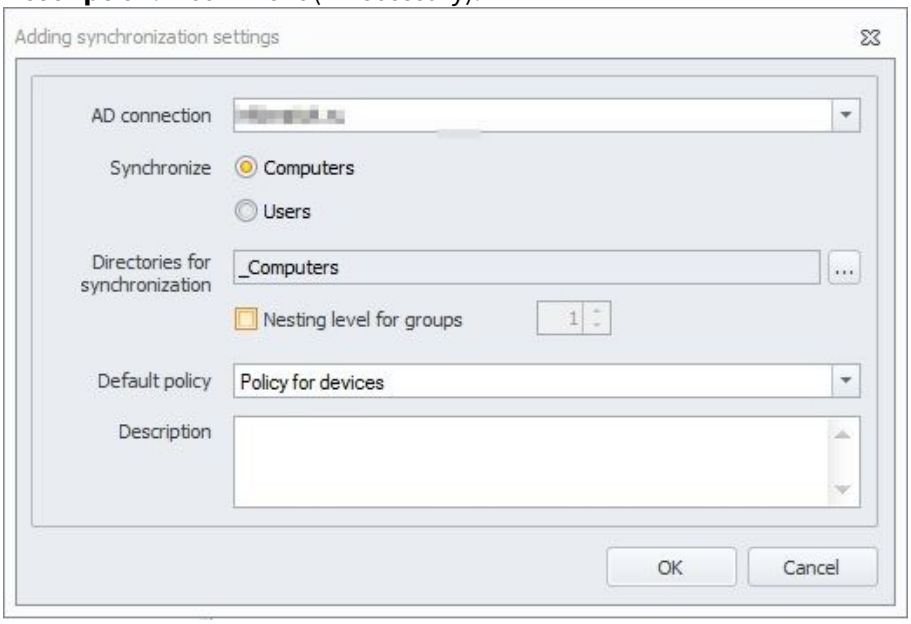
After configuring synchronization parameters, define what information directory services are required to provide and what policies are to be applied afterwards.

> **Note:**
>
> Synchronization is launched for Organizational units and Security groups of Active Directory

**To add synchronization settings with Active Directory:**

1. In **Synchronization settings** area, click .
2. In a dialog window, specify synchronization settings:

- **AD connection.** Name of the domain to which connection was installed before
- **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).




- Click **OK**.
- To apply changes, click **Apply** in the **Settings** window.
- Check the table with synchronization settings and results:

| Parameter | Description |
|---|---|
| Domain | IP address or DNS name of the server |
| Synchronize | Object of synchronization: computers or users |
| Directories | Folders and groups for synchronization |
| Synchronization status | Possible values:<br>• **Is running** (the synchronization process is in progress)<br>• **Successfully** (the synchronization process is complete),<br>• **Failed** (the synchronization process has failed). |
| Synchronization time | Date and time of the last synchronization |

**Note:**

For users and computers the synchronization is to be configured separately. You can add several synchronization settings for the same domain.

**To launch synchronization with Active Directory:**

1. In **Synchronization settings** 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 (every 1 hour by default) and click **Apply**.

**To edit Synchronization settings**:

1. In **Synchronization settings** area, choose the desired row.
2. Click .
3. Edit synchronization settings.
4. Click **OK**.

**To disable synchronization with Active Directory:**

1. In **Synchronization settings** area, choose the required row.
2. Click .
3. In the confirmation window, click **Yes**.

**Warning!**

When deleting synchronization settings, all groups of computers or user groups associated with this settings will be removed.

### 5.3.7 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 the following cases:

- **Access to device denied** – Device Monitor rule which denies reading and writing to the device (see "Device Monitor Rule (DM)") was actuated.
- **Writing to device denied** – Device Monitor rule which denies writing to the device (see "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 "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, Mail Monitor or IM Client Monitor rule (DM) which denies data transfer through FTP/FTPS/SMTP/S/MIME/POP3/Outlook/XMPP/MMP/YMSG/Skype (see "FTP Monitor Rule (DM)", "Mail Monitor Rule (DM)", and "IM Client Monitor Rule (DM)") was actuated.
- **Data transfer via network protocols denied if there is not enough space for events** – 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 "Network Monitor Rule (DM)" and "Corporate Network Control") was actuated.
- **Network connection forbidden and request for 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 "Network Monitor Rule (DM)", "Corporate Network Control" and "Temporary Employee Access").

- **Request for 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 for temporary access to the device by email** – 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 "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 "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 blacklists (see "Application Monitor Rule (DM)") was actuated.
- **Prohibition of making screenshot** – ScreenShot Control Monitor rule (DM) which controls making screenshots (see "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 notifications displaying 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**.

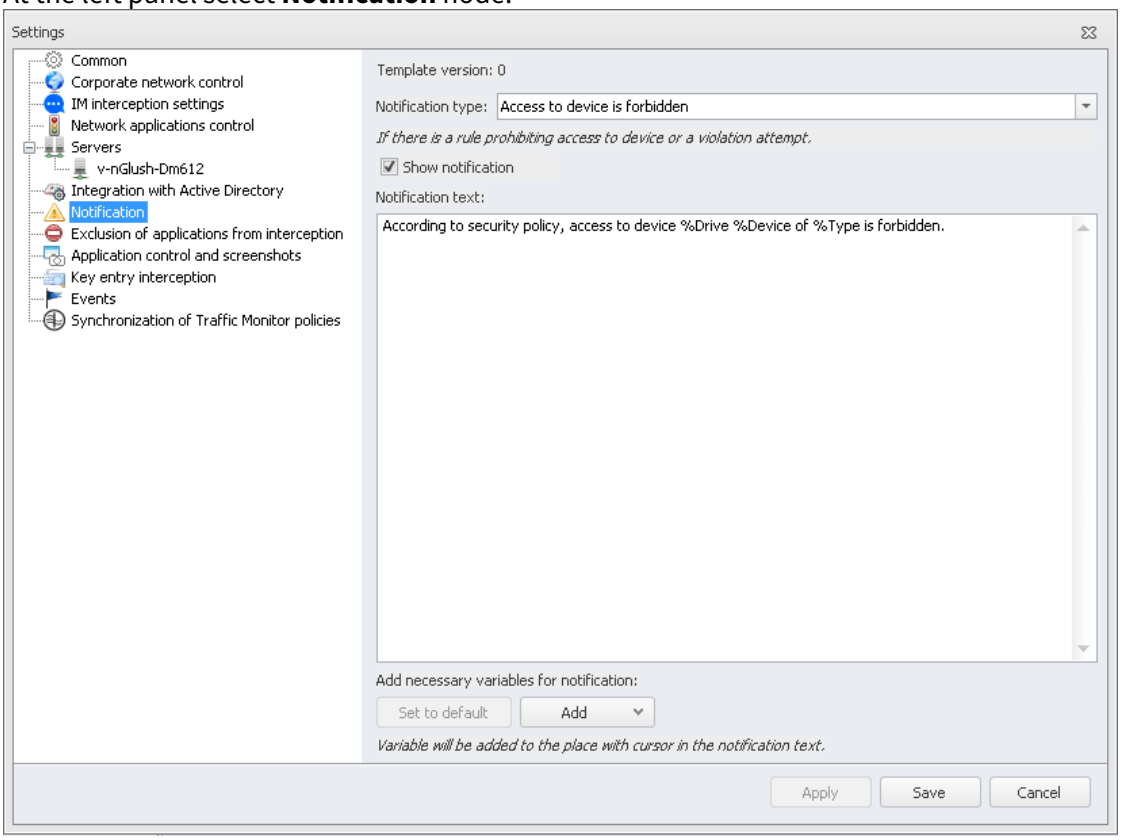
If required, you can change notification text or disable showing of any certain notification type or enable it back.

> **Warning!**
>
> If you have disabled notifications using the method described above, the notifications enabled using the method described below won't be 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**.

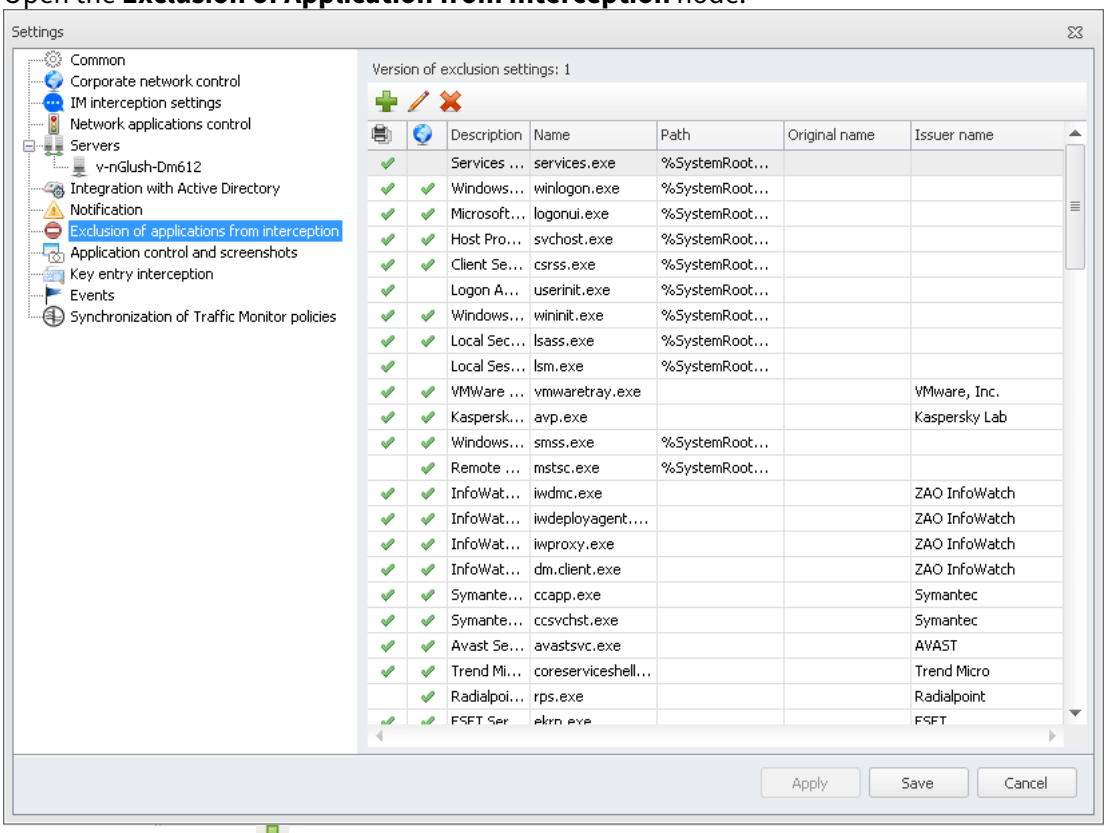
## 5.3.8 Exclusion of Application from Interception

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.

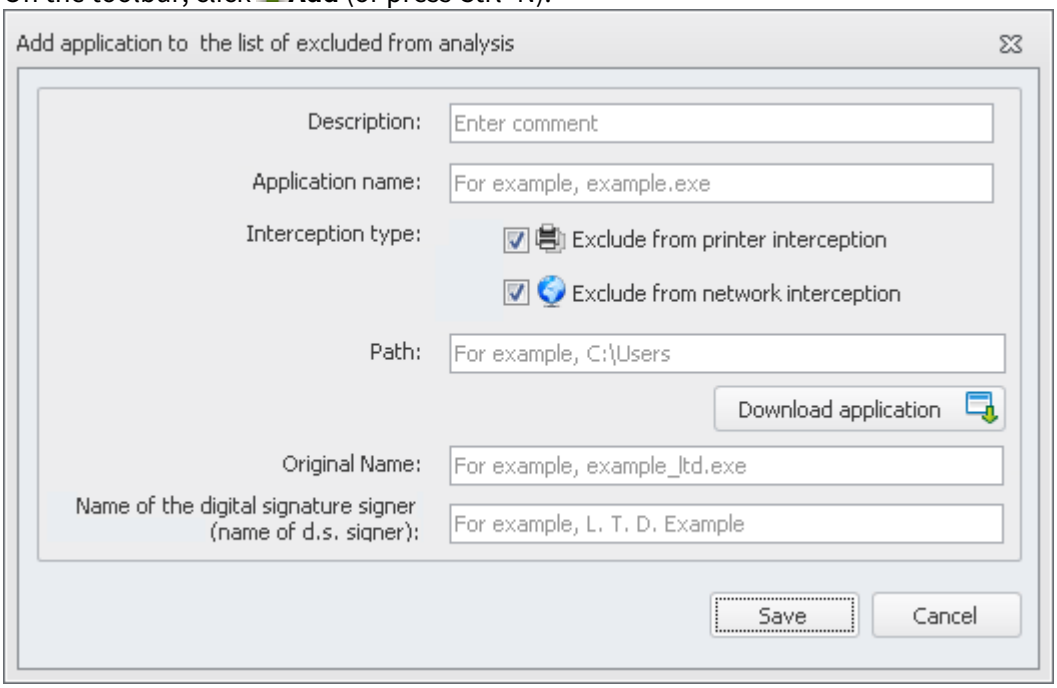
**To view and configure parameters of excluding applications**:

1. In the Main Menu, select **Tools** > **Settings**.

2. Open the **Exclusion of Application from Interception** node.




3. On the toolbar, click **Add** (or press Ctrl+N).




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 should be selected.

   > **Important!**
   >
   > Specifics of excluding **Outlook** from interception.
   > When excluding Outlook from printer interception:
   > - Intercepting Outlook mail (MAPI) will also be disabled. In this case, to intercept emails, configure rules for other protocols (see "Mail Monitor Rule (DM)").
   > - Checking Outlook mail will also be disabled according to policies that are configured in the Traffic Monitor Management Console.

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: `*%ProgramFiles%\Citrix`, then all applications in *.exe format located in the Citrix folder or any of its subfolders 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 file name** 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 the **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**. Excluding an application from interception, as well as canceling exclusion will be applied during the next run of the application. That is why you need to restart the application to apply the exclusions.

> **Note:**
>
> Applications with a built-in integrity check (e.g. SWIFT client) or the ones, containing debugger detections should be added to the printer interception exceptions list. Otherwise, they cannot be launched.

### 5.3.9 Application Control and screenshots

Device Monitor allows to control applications running on the managed computers via permitting or forbidding some applications. For this purpose there are two operation modes provided:

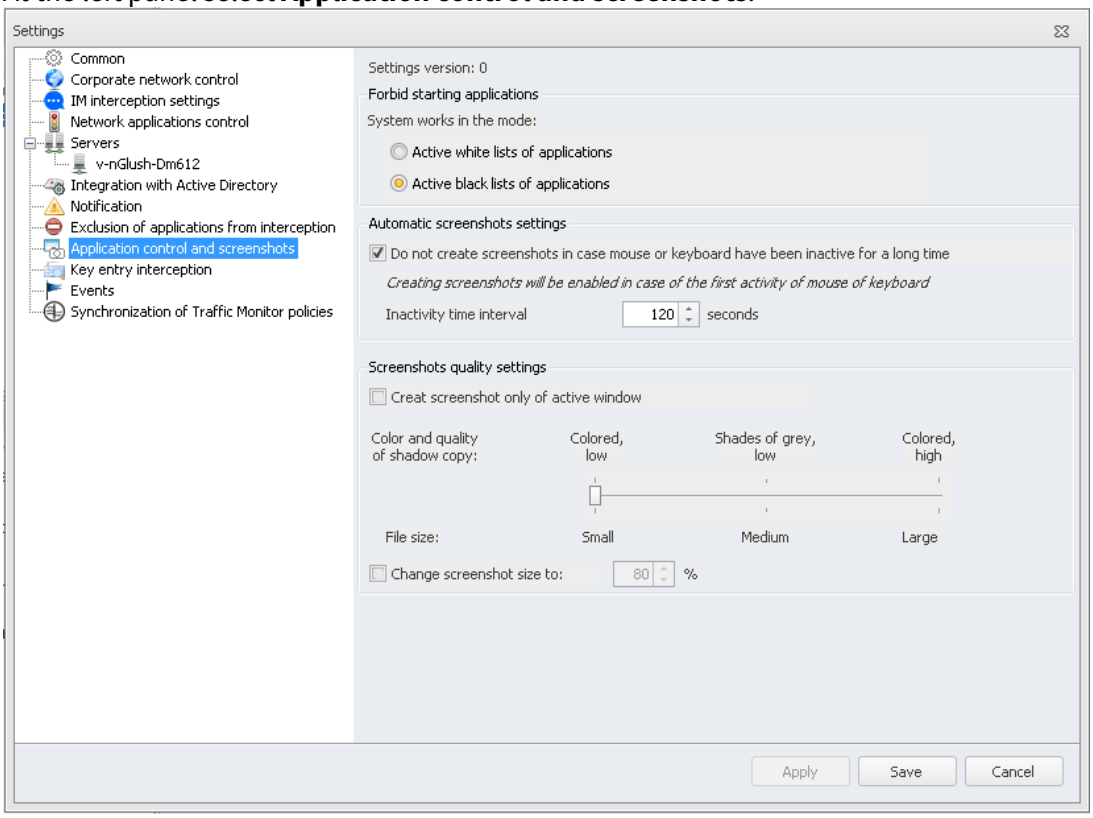
- **Active white lists of application**s - all applications from the lists selected in the Application Monitor rule from the resulting policy are allowed. Other applications are forbidden.
- **Active black lists of applications** - all applications from the lists selected in the Application Monitor rule 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 Settings, 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. 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 the value in **Inactivity time interval** field is reached and renewed at the first keyboard or mouse activity.
4. In **Screenshots quality settings** specify:
    - **Colour and quality of shadow copy.** The following colour modes are available:
    - **Colored, low**. A colored file in a low resolution to be saved. Use this mode, in case you need files of small size.
    - **Shades of gray, low**. A file in greyscale mode in a low resolution to be saved.
    - **Colored, high**. A colored file in a high resolution to be saved. Use this mode, when you need high-quality images regardless of their size.
    - **Change screenshot size to**. If you need to reduce the image size while saving, select this option and specify the value (per cent, to be calcuted in accordance with initial file).
5. Change the mode if required.
6. Click **Save**.

More information on how to configure automatic screenshots creation, see "ScreenShot Monitor Rule (DM)".

New version of applications and screenshots settings will ne applied to controlled computers after the next restart.

## 5.3.10 Event Storage

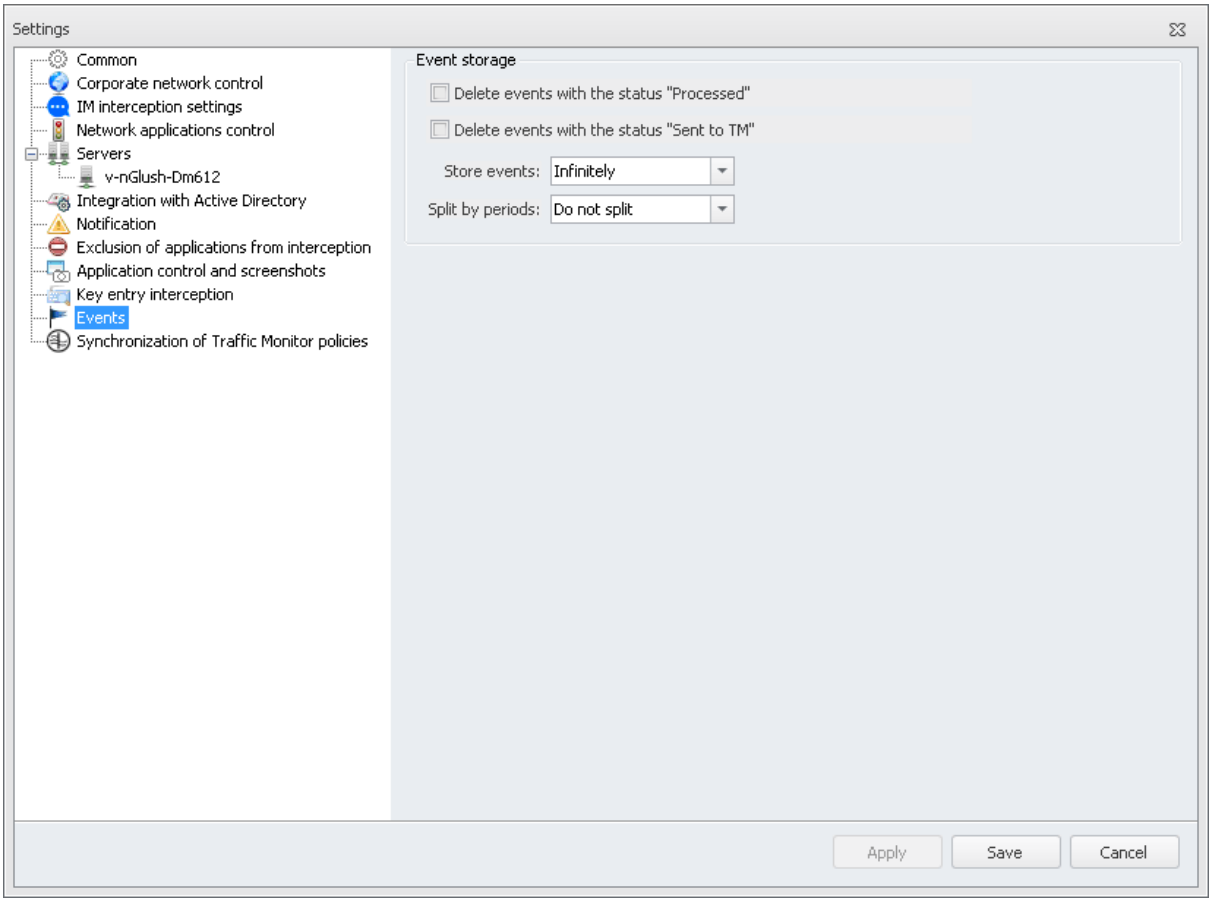
In the **Events** tab, you can set the parameters of automatic event storage and deletion.

**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.

> **Note:**
>
> If fields specifying immediate deletion are not marked, the events with status "**Processed**" and "**Sent to TM**" will be stored in accordance with "**Store events**" field.




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.

## 5.3.11 Synchronization of Traffic Monitor Policies

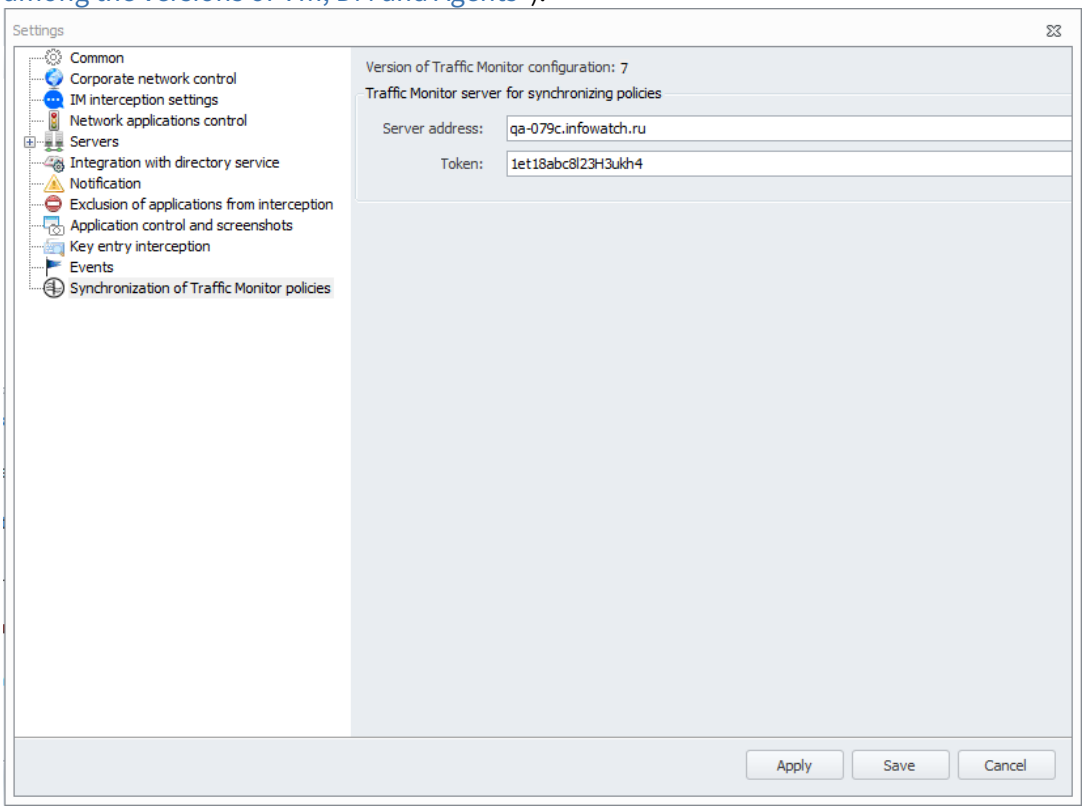
In the **Synchronization of Traffic Monitor policies** node, specify Traffic Monitor server from which Device Monitor will receive a configuration version. This configuration version is then deployed to Device Monitor agents.

**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 the Console (DM) main menu, choose **Tools** > **Settings**.
2. Open **Synchronization of Traffic Monitor Policies** node.
3. Enter the server address (host), on which you are going to work in the Management Console, and a token (see "Device Monitor Server Settings. Connecting to Traffic Monitor Server"). Make sure that you establish a connection with the Traffic Monitor server of the same version (see "Compatibility among the versions of TM, DM and Agents").




4. Click **Apply**.
5. Click **Save**.

## 5.3.12 InfoWatch Device Monitor Server Manager

InfoWatch Device Monitor Server Manager is being used to define roles and change server settings.

**Warning!**

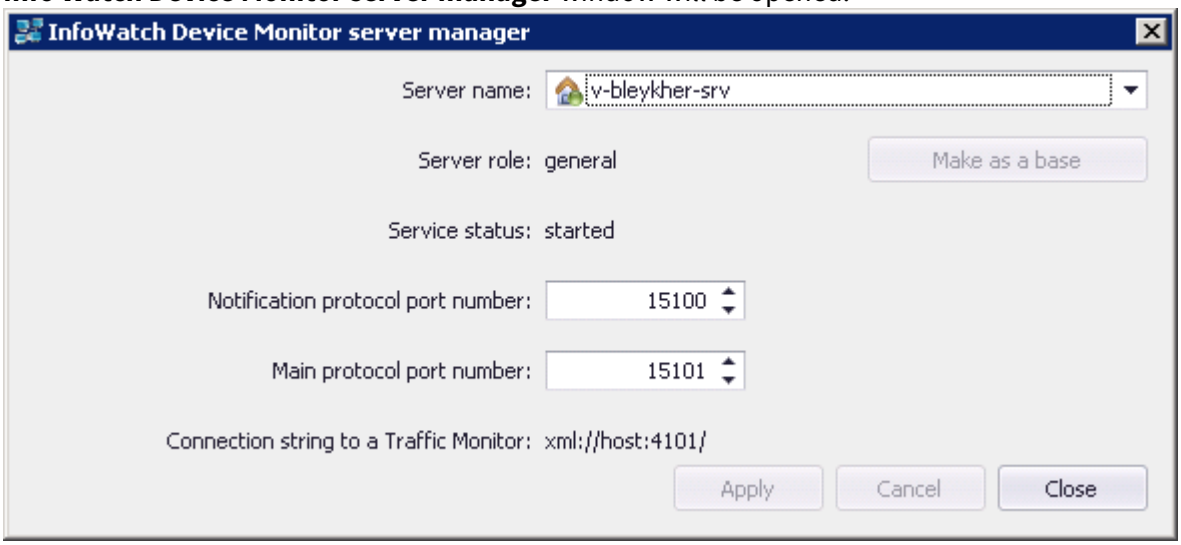
There are following requirements to run the InfoWatch Device Monitor Server Manager utility:

- 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
- server names must be successfully resolved through the customer's DNS service to the IP address (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**.

## 5.3.13 Stopping and Starting Device Monitor Agent

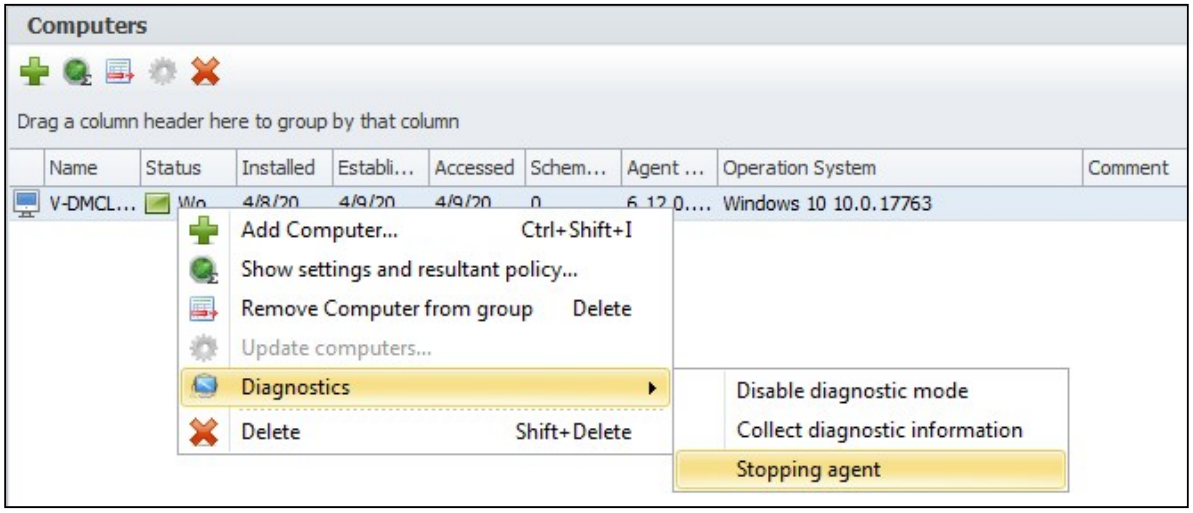
When there are conflicts with third-party programs as well as in critical situations, user can stop Device Monitor agent running on a workstation. One can do it locally or remotely

> **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.
>
> Restart computer after stopping/starting the agent.

### 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 -> Stopping agent** (in case agent is already started on a Workstation).



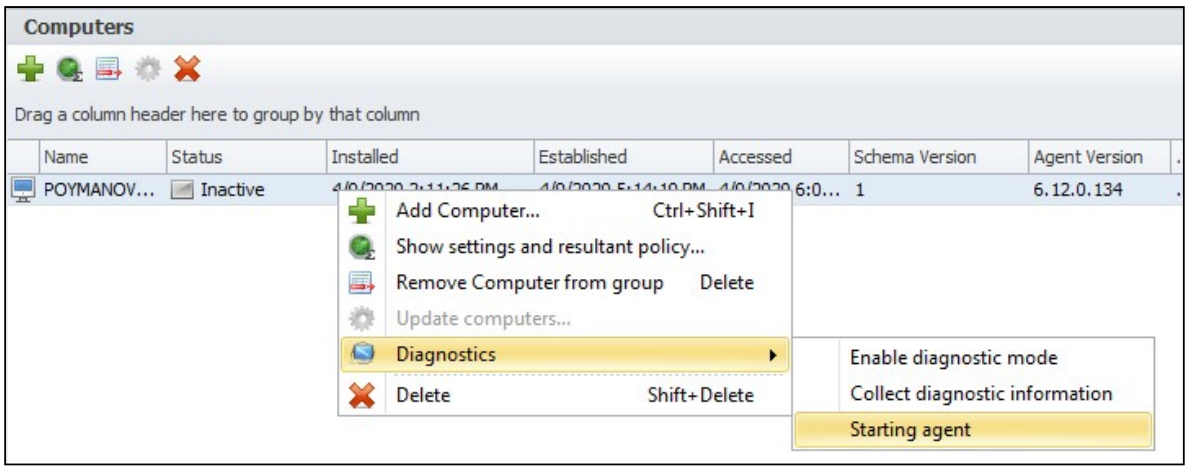

When choosing **Stopping agent**, its operation will be suspended and status of the workstation will change to " Inactive".

> **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 -> Starting agent** (in case agent is stopped).




When selecting the option **Starting agent**, its work will be resumed and the workstation status will go back to "Working ptoperly".

### 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".

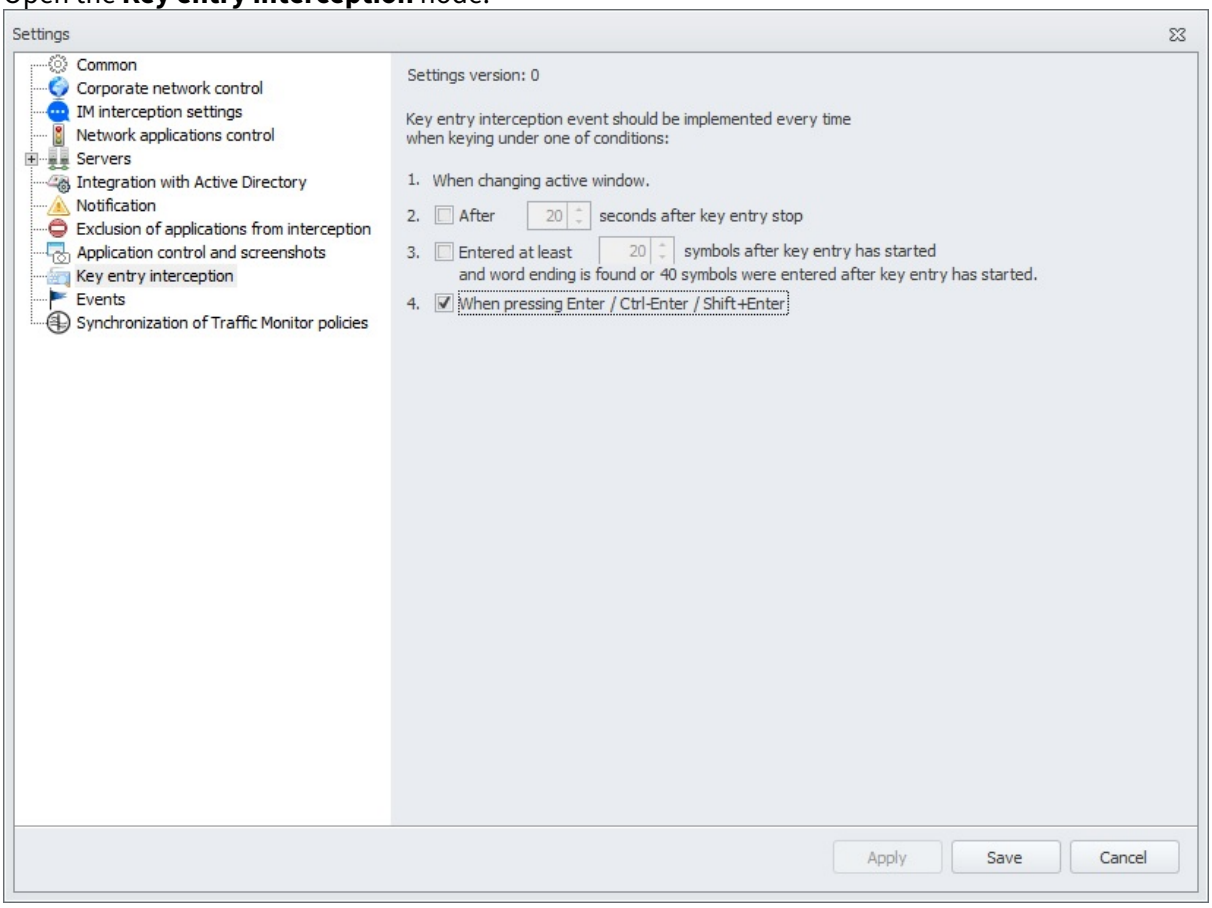
## 5.3.14 Control of Keyboard Input

On the **Key entry interception** tab, you can specify general conditions under which the rule is triggered.

For this:

1. In the main menu of the Management Console (DM), select **Tools** > **Settings**.

2. Open the **Key entry interception** node.




3. If necessary, specify conditions, under which a new event is created:
   - the number of seconds which should pass after the user stops typing;
   - the minimum number of entered characters;
   - pressing Enter/Ctrl+Enter/Shift+Enter.

> **Note:**
>
> An event is always created when an active window changes.

4. Click **Apply**, then click **Save**.

## 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.

The security schema can be edited multiple times. An updated security schema is then saved as a new version of the existing schema. Old security schemas are stored in the database. In DM Management Console, you may see policies and rules of any security schema 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 and Rules (DM)

A security policy (DM) is a set of rules (DM) which allow you to monitor transferring data to removable devices and network resources, sending documents to print, control network activity, and define access level to controlled peripherals.

When you assign a security policy (DM) to a group of employees or computers, please, mind the following:

- Each employee group and each computer group should have an assigned security policy (DM). You can't add a new group without assigning a security policy (DM) to it. The security policy (DM) is selected from available policies (DM). Therefore, a security policy (DM) should be created before adding a group.
- You can't assign more than one security policy (DM) to a group.
- The same security policy (DM) can be assigned to several groups. However, we recommend that you should 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 group.

Accounts that are newly registered with Device Monitor are automatically added to *Default* employee group. So, for a new employee, the access level is initially defined by the security policy which is assigned to the "default" group

of employees and the security policy which is assigned to the computer group to which the employee's computer belongs. You can change the access level later by adding the employee to a different group.

> **Warning!**
>
> In case of multi-user type of access to workstation and when it is impossible to define the process (event) initiator, the interceprion rules for employees cannot be taken into consideration. Only the interception rule for this specific workstation will be effective. In this case you should set up the interception rules for workstation with multi-user access, not only for employees.

**Rules** are restrictions and conditions according to which the System monitors data transfer to removable devices, network activity, sending documents to print and controls access to peripherals. A new set of rules (DM) is created for each security policy (DM).

Each rule (DM) has a validity period during which the rule applies.

InfoWatch Device Monitor includes the following rule types:

- **Application Monitor Rule** allows you to control access to applications by means of black and white lists.
- **Clipboard Monitor Rule** allows you to control pasting data from the clipboard. You can prohibit pasting data to specified applications or to all applications of a terminal session.
- **Cloud Storage Monitor Rule** allows you to control web clients of cloud storage.
- **Device Monitor Rule** allows you to control access of employees to selected peripherals.
- **File Monitor Rule** allows you to monitor the following actions with files on removable and network resources:
  - copying files to network resources using UNC (e.g., *Server**SharedFolder**Folder**File*);
  - creating a file directly on a removable device;
  - copying/moving a file to a removable device. The System controls copying/moving files from a controlled computer, another removable device, or a network resource.
- **File Operations Monitor Rule** allows you to control if applications read data from a file or write to file. With this rule, you can also create a file shadow copy and a screenshot.
- **FTP Monitor Rule** allows you to control data exchange through FTP/FTPS protocols. You can restrict or completely forbid using the protocol and create shadow copies of transferred files.
- **HTTP(S) Monitor Rule** allows you to control data exchange through HTTP and HTTPS protocol. The System allows you to create shadow copies of transferred files.
- **IM Client Monitor Rule** allows you to control employee access to instant messengers: Skype, Telegram, XMPP, MMP, Facebook, Vkontakte. The rule can block access to the application or just make copies of transferred files, messages, and chats (for Skype, voice messages can also be recorded). It is also possible to create shadow copies of transferred files messages.
- **Mail Monitor Rule** allows you to control incoming and outgoing mail. You can forbid or allow using email or allow only receiving emails. The System can also create shadow copies of transferred files.
- **Network Monitor Rule** allows you to forbid data transferring through any network connections except for the connection with the corporate network or with specified servers. You can specify the network segments that are considered the corporate network and create the list of allows external addresses.
- **Print Monitor Rule** allows you to monitor sending documents to local and network printers. It is also possible to create shadow copies of print jobs.
- **ScreenShot Monitor Rule** allows you to automatically create screenshots on controlled computers.

- **ScreenShot Control Monitor Rule** allows you to control screenshots on the agent side.

> **Important!**
>
> To enable correct interception of Google services (Gmail, Google Drive, etc.), we recommend disabling the use of experimental QUIC protocol in Google Chrome (for details, see the KB article "Disabling QUIC protocol in Google Chrome").

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 must belong to at least one employee group (the *default* group) as the security policy (DM) can not apply to individual employees.
   The *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 the "*Default*" group if the account is added to at least one employee group besides the Default group.
2. When the System is installed, the *Shadow copy policy* is assigned to the *default* employee group. The *Shadow copy policy* contains the 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**, **Telegram 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 an encrypted channel. Shadow copy is created, if the request size, transferred via an 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 an encrypted channel, when its size is not bigger than 40 MB.

### Computers and Computer Groups

A computer registered in Device Monitor must belong to at least one computer group (the "default" group) as the security policy (DM) can not apply to an individual computer.

> **Note:**
>
> Last time logged in user is displayed in the field **User** in the section **Computers**.

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.

### 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.

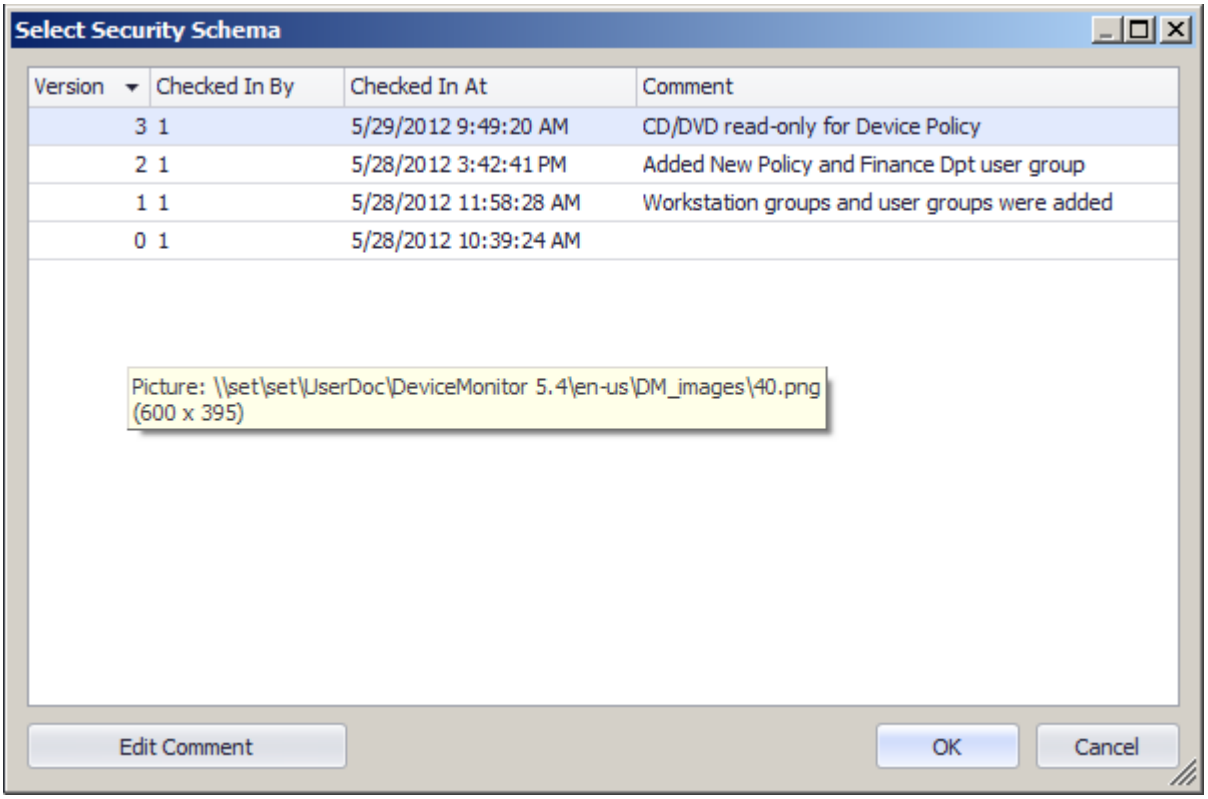
> **Note:**
>
> You can customize the main screen appearance (see "Main screen customization").

## 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**.

Policies of the selected security schema version and their rules will be loaded into Management Console (DM). When working with an old version, the "*Old security schema*" status is displayed.

**To return to preview and active security schema**, open **Security Schema > View Latest Security schema** in the Main Menu

## Security Scheme Comments

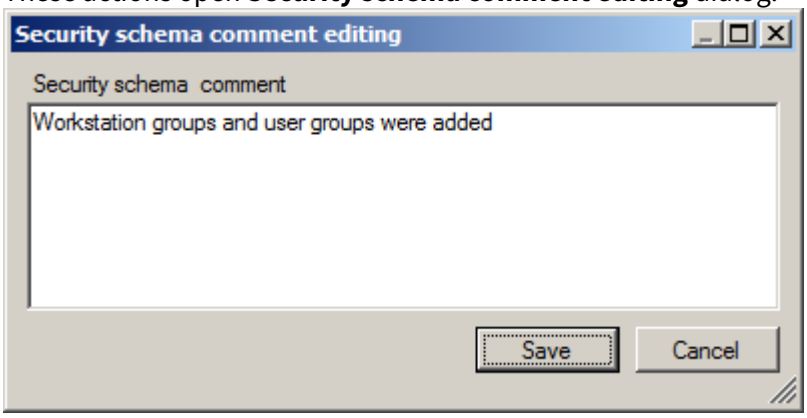
You can specify additional information on your security scheme as a comment. You can add comments to each version of the security scheme.
Comments on current security scheme are displayed in brackets to the right of the scheme version number on the status panel.
You can view comments for all security 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 the existing settings of a security scheme. You might want to do this if you need to configure the 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:

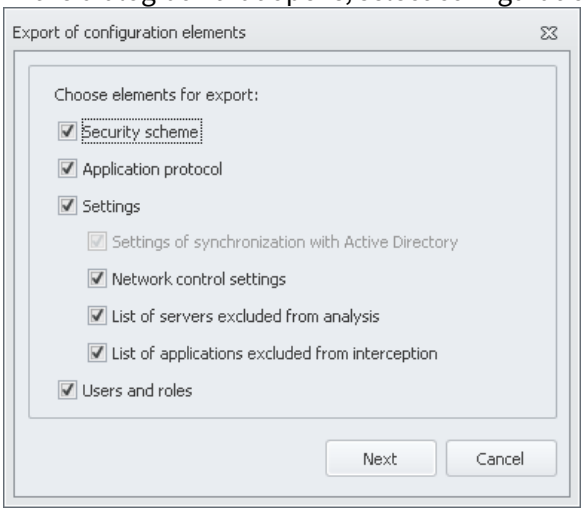
- **Security scheme** (including security policies with rules, groups of employees and computers, categories of signatures) (see "Managing Security Schema")
- **Applicaiton protocol** (see "Application Protocol")
- **Network control settings** (see "Corporate Network Control")
- **Servers included from analysis** (see "Network Traffic Control")
- **Applications excluded from interception** (see "Exclusion of Application from Interception")
- **User and roles** (see "Managing Console (DM) Accounts")

> **Important!**
>
> To Device Monitor version 7.0 you can import a configuration file of the same version only.

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.



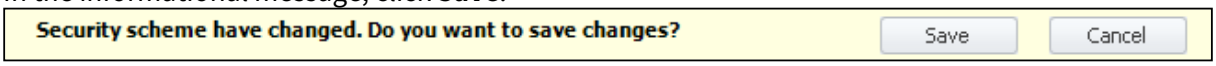

3. Click **Next**.
4. Specify the export file name and select a folder where the file will be saved. Click **Save**.

> **Important!**
>
> For a correct connection between roles and groups, the security scheme should be exported as well.

**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 and added to the existing settings. 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 the "*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 the 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 you should create a whitelist for a specific employee/employee group/workstation/workstation group and specify devices included in the list. These employees/workstations have access to whitelisted device models and instances regardless of 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 and Rules (DM)".

Each security policy (DM) is a set of rules (DM) which allow you to monitor operations related to data transfer to removable devices, sending documents to print and network activity as well as to define access level to controlled peripherals

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 colour 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:

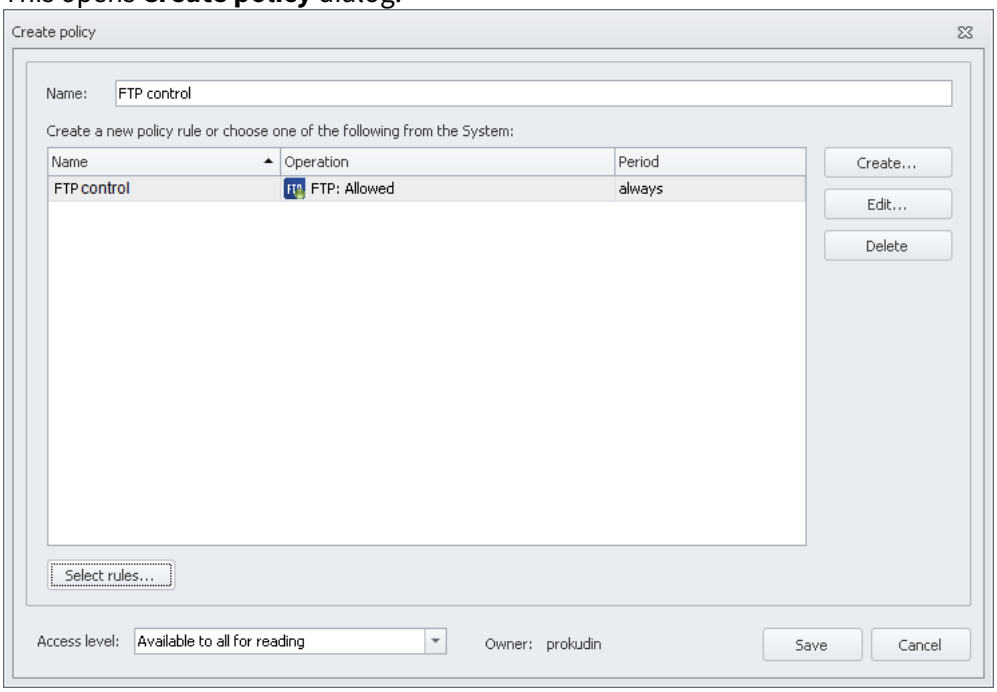
- **Name**. Rule (DM) name.
- **Policy**. Name of the security policy (DM) that includes the rule (DM).
- **Interceptor**. Interceptor type assigned to the rule (DM).
- **Operation**. The operation controlled by the rule (DM).
- **Period**. Rule starting and expiry time.

> **Note:**
>
> Information for some attributes is duplicated on the main screen.

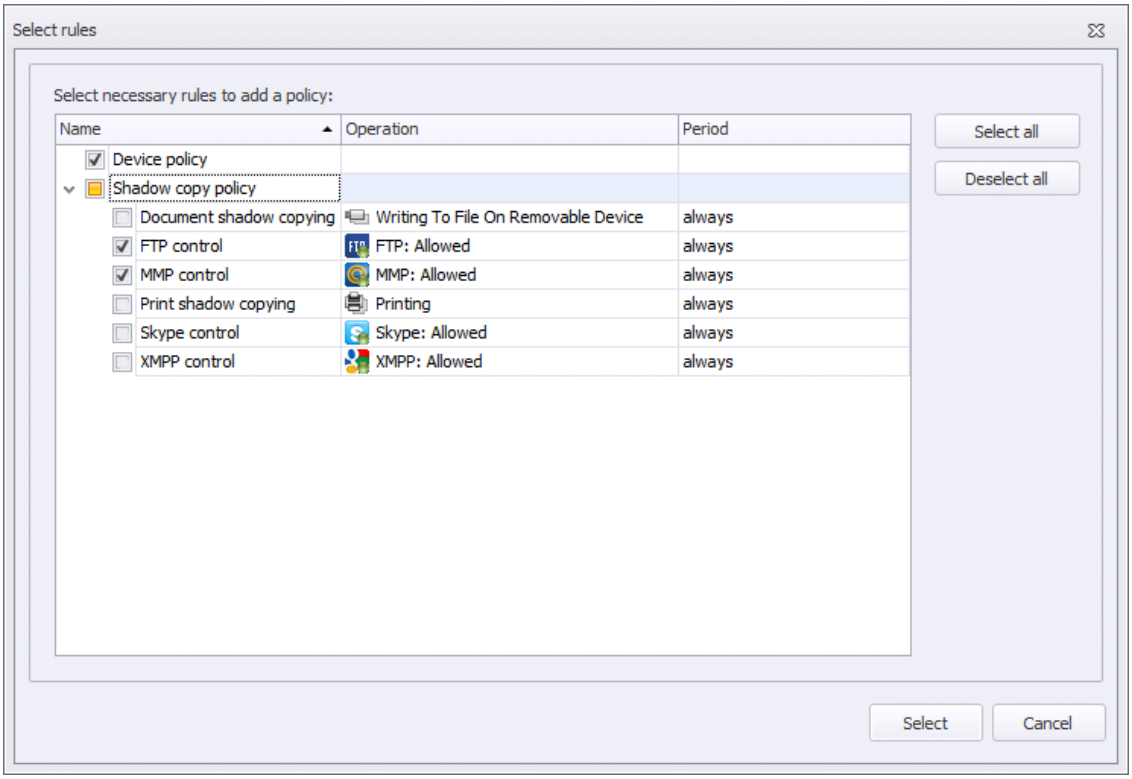
Adding and Configuring New Security Policy (DM)

**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:
  - Application Monitor Rule (DM);
  - Configuring Clipboard Monitor Rule;
  - Cloud Storage Monitor Rule (DM);
  - Device Monitor Rule (DM);
  - File Monitor Rule (DM);
  - FTP Monitor Rule (DM);
  - HTTPS Monitor Rule (DM);
  - IM Client Monitor Rule (DM);
  - Mail Monitor Rule (DM);
  - Network Monitor Rule (DM);
  - Print Monitor Rule (DM);
  - ScreenShot Control Monitor Rule (DM);
  - 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 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)

You can work with rules (DM) within the security policy (DM) in which they are created. Each security policy (DM) has an individual set of rules (DM).

You can find information on rules (DM) in the following subsections:

- Applying Rules (DM)
- Adding Rule (DM)

### Applying Rules (DM)

The event satisfies a rule (DM) if all conditions of the rule are satisfied.

If the event matches several rules (DM) at a time, then the rule priority is determined as follows:

1. An excluding rule (DM) (the **Exclude from interception option** is available for File Monitor rule) has the highest priority.
2. A full access rule (DM) overrides the forbidding one, while the forbidding rule overrides the permission to read-only and to access encrypted devices.
   *Example 1*. *Allowed to use* rule for Device Monitor overrides *No access* restriction, which overrides on its part the rule permitting *Read only*, the one that is accordingly more preferred than a rule with *Full access to encrypted devices* option.
3. *Example 2*. If there are several HTTP(S) Monitor rules, then a rule with the *Do not intercept requests to internal resources* is superior to the same rule without this option.
4. The rule where the **Create a shadow copy** option is selected overrides a rule without shadow copies.

See also:

- 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 based 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.

When the Agent is installed, controlled devices are fully accessible by default. Therefore, all forbidden operations with the device must be set explicitly as DM rules.

Each newly registered computer is added to the Default group. This group has a "Shadow copy policy" (DM) which contains no rules (DM). Rules (DM) regulating access to devices are not defined for employees by default. Thus, the System always allows access to all controlled devices after the installation.

**Example**:
There is a rule (DM) that prohibits writing to CD/DVD drive to members of *A* computer group. A computer *PC* belongs only to the group *A*. Employee Smith belongs only to the employee group *B* with no device rules (DM) and his computer belongs to the group *A*. Employee Smith tries to view a CD on the computer *PC*. In this case, the employee won't be able to view CD contents of the disk or write new data to it.

You can assign multiple rules (DM), in the same or in different policies (DM), with various access levels to the same device. In this case, a rule which is allowed to use is superior to other rules (see the table below).

| Device type | Access in descending order of priority |
|---|---|
| All devices, except CD/DVD, Floppy drives, and removable storage devices | 1. Allowed to use<br>2. Using is prohibited |
| CD/DVD | 1. Allowed to use<br>2. No access<br>3. Read-only |
| Floppy drives and removable storage devices | 1. Allowed to use<br>2. No access<br>3. Read-only<br>4. Full access to encrypted devices only |
| Cloud storages | 1. No access<br>2. Read-only<br>3. Allowed to use |

**Example**:

> There is a rule (DM) for the employee group *E* that allows read-only access to a removable storage device. There is a rule (DM) for the employee group *F* that grants full access only to encrypted removable storage devices. An employee Smith who belongs to both groups can only get read-only access to both encrypted and not encrypted devices (the rule with a lower priority is not applied at all).

For some types of devices controlled by Device Monitor interceptor, rules can overlap (see the table below). Please, keep it in mind when configuring access to a controlled device.

| Rule (DM) | Overlapping rules | Notes |
|---|---|---|
| Floppy | No | |
| CD/DVD | No | |
| Parallel port (LPT) | Local printer (LPT)<br>Imaging devices (LPT) | If there is no access to LPT port, the device connected to this port will be unavailable |

| | | |
|---|---|---|
| Serial port (COM) | Modem<br>Local printer (COM)<br>Imaging devices (COM) | A modem connected to COM port is only accessed basing on COM port rule<br>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)<br>Serial port (COM)<br>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)<br>Serial port (COM)<br>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)<br>Local printer (IEEE 1394)<br>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.<br>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 | MTP-compatible device | When a mobile device is connected to the computer, it can be treated either as an MTP device or as a USB network adapter |
| Pocket Computer (Windows Mobile and Palm OS pocket computers) | No | |

| | | |
|---|---|---|
| MTP-compatible device | USB Network Adapter | When a mobile device is connected to the computer, it can be treated either as an MTP device or as a USB network adapter |

Creating shadow copies and blocking operations due to space problems

**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.

> **Note:**
>
> 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").

> **Warning!**
>
> Shadow copies for printing files exceeding 512 Mb **cannot** be made.

If: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).

- 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 Rule (DM)

To add a rule to a security policy:

1. Go to the **Policies** section.
2. In the **Policy** area of Navigation pane, select a security policy (DM) to which you want to add the rule (DM).
3. Do either of the following:
   - in the main menu, click **Edit** > **Create Rule**;
   - click **Create Rule** at the top of the **Policies** area;
   - right-click in the **Policies** area and select **Create Rule** from the drop-down list;
   - press **Ctrl+Shift+N**.
4. In the dialog box that opens, choose the rule type and specify other setting of the rule. Available rule types:

- Application Monitor Rule (DM)
- Clipboard Monitor Rule (DM)
- Cloud Storage Monitor Rule (DM)
- Device Monitor Rule (DM)
- File Monitor Rule (DM)
- File Operations Monitor Rule (DM)
- FTP Monitor Rule (DM)
- HTTPS Monitor Rule (DM)
- IM Client Monitor Rule (DM)
- Mail Monitor Rule (DM)
- Network Monitor Rule (DM)
- Print Monitor Rule (DM)
- ScreenShot Control Monitor Rule (DM)
- ScreenShot Monitor Rule (DM)

5. Oncer you have set all necessary parameters, click **Save**.

**To edit the rule:**

1. In the list of the policy rules, select the rule you want to edit.
2. Do either of the following:
   - in the main menu, click **Edit** > **Edit Rule**;
   - double-click the selected rule;
   - right-click the selected rule and select **Edit rule** from the drop-down menu;
   - click  **Edit rule** in the upper part of the **Policies** area;
   - press **Ctrl+Shift+E**.
3. In the dialog box that opens, edit the necessary parameters, then click **Save**.

**To delete the rule:**

1. In the list of the policy rules, select the rule you want to delete.

   > **Note:**
   >
   > To select multiple rules, use Shift or Ctrl keys. To select all rules, press Ctrl+A.

2. Do either of the following:
   - in the main menu, click **Edit** > **Delete Rule**;
   - click  **Delete rule** in the upper part of the **Policies** area;
   - right-click the selected rule and select **Edit rule** from the drop-down menu;
   - press **Delete**.
3. In the confirmation window, click **Yes**.

**To copy the rule:**

1. In the list of the policy rules, select the rule you want to copy. If you want to copy more than one rule, select all required lines.
2. Click the selected rule and holding the left mouse button drag the rule to the **Policies** area in the Navigation pane. Hover the mouse over the security policy (DM) to which you want to add the rule. When you see a yellow arrow to the left of the policy name, release the mouse.
   The rule will be copied to the selected policy (DM).

You can also copy rules when editing the security policy (DM). For this:

1. Start editing the selected policy (DM).
2. Click **Select rules**. In the drop-down list, select rules (DM), you want to copy to the policy. You can select the whole policy - in this case, all rules of the selected policy will be added to the policy being edited.
3. When you select all required rules, click **Select**.
4. Click **Save**.

**Warning!**

To apply changes, you need to save the security scheme (see "Editing Security Scheme"). If you don't save the security scheme, all changes will be discarded.

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.

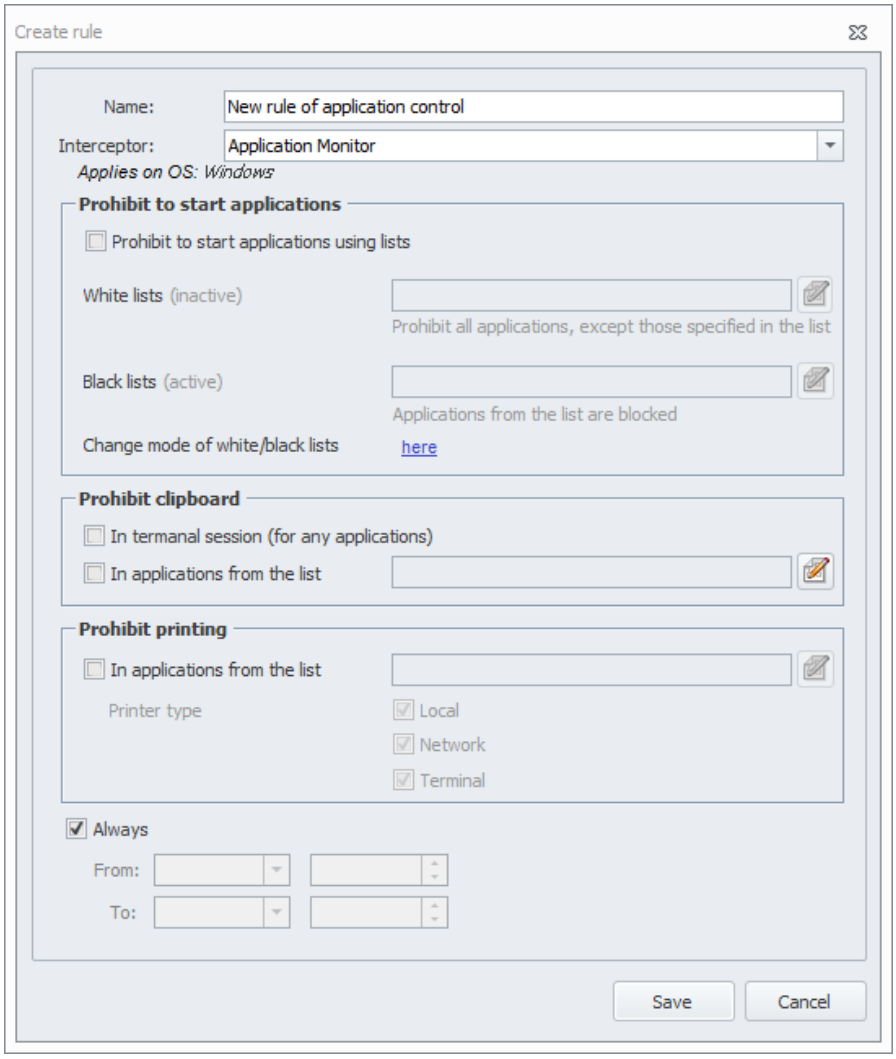
Application Monitor interceptor allows you to control employees' access to applications prohibiting the following actions:

- starting applications;
- using clipboard;
- printing.

These prohibitions can be activated both separately and together.

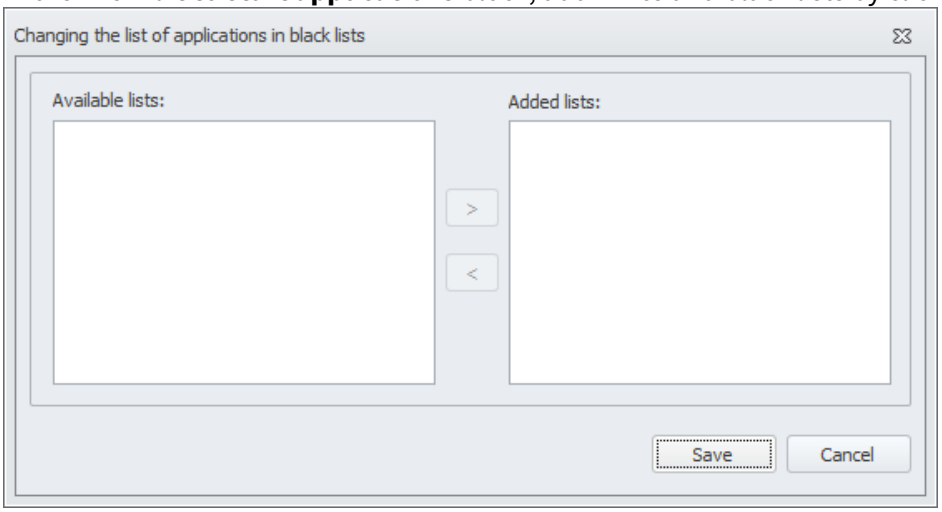
**Note:**

The rule applies on computers with Windows OS.




**To configure the rule:**

1. Open the **Create rule** window (see "Adding Rule (DM)") and in the **Name** field, specify the rule name.
2. In the **Interceptor** field, select **Application Monitor**.
3. In the **Prohibit to start applications** block, add white and black 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".

4. In the window that opens, choose necessary types of available lists and move them to **Added lists** area by pressing >.
5. Click **Save**.
6. In the **Prohibit clipboard** block, select check boxes next to the application groups for which data copying should be prohibited. Possible choices:
   - **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.

7. In the **Prohibit printing** block, specify applications for which printing should be prohibited and choose the printer type:
   - local;
   - network;
   - terminal.

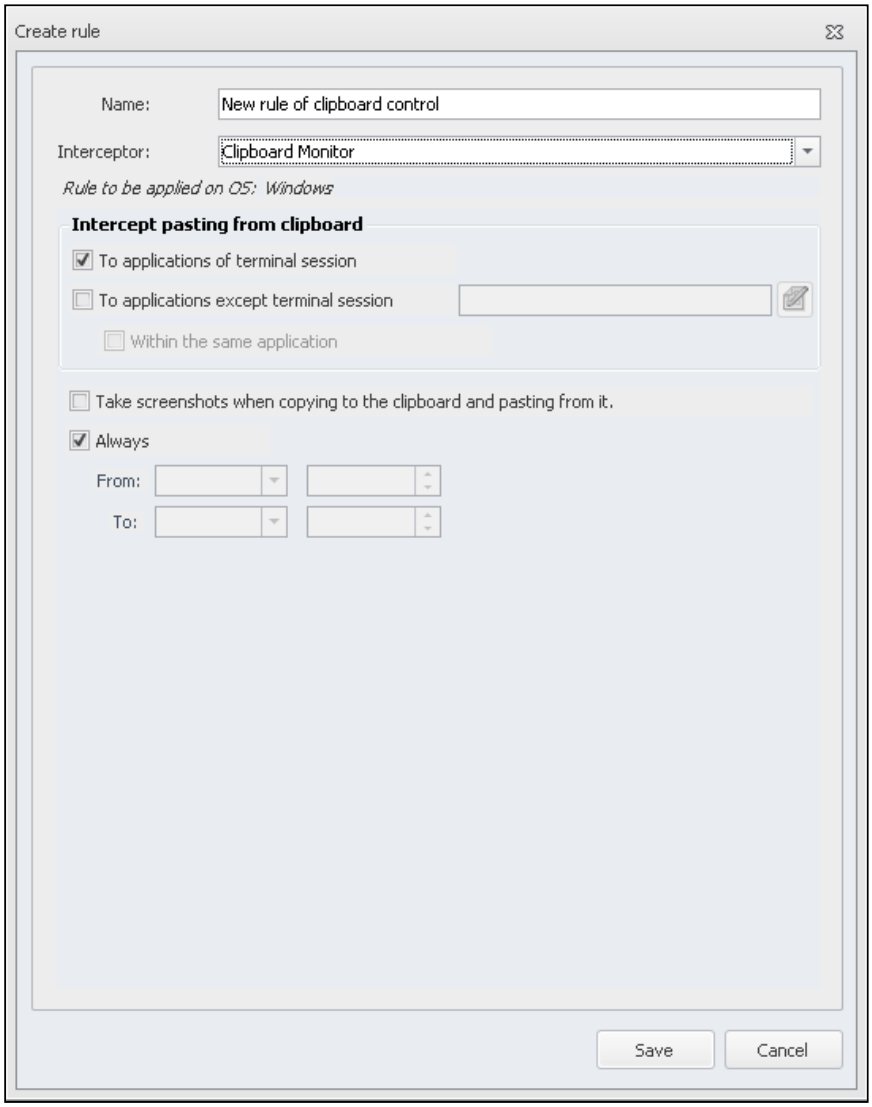
   The user will not be able to print data in specified applications. Choosing specified printer types is not available either.

8. 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.
9. When all parameters are configured, click **Save**.

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**:

1. Open the **Create rule** window (see "Adding Rule (DM)") and in the **Name** field specify the rule name.
2. In the **Interceptor** field, select **Clipboard Monitor**.
3. In the **Intercept pasting from clipboard** area, specify when the rule applies:
   - **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.
4. Set flag next to the field **Take screenshots when copying to the clipboard and pasting from it** to select the corresponding option.

5. 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.
6. When all parameters are configured, click **Save**.

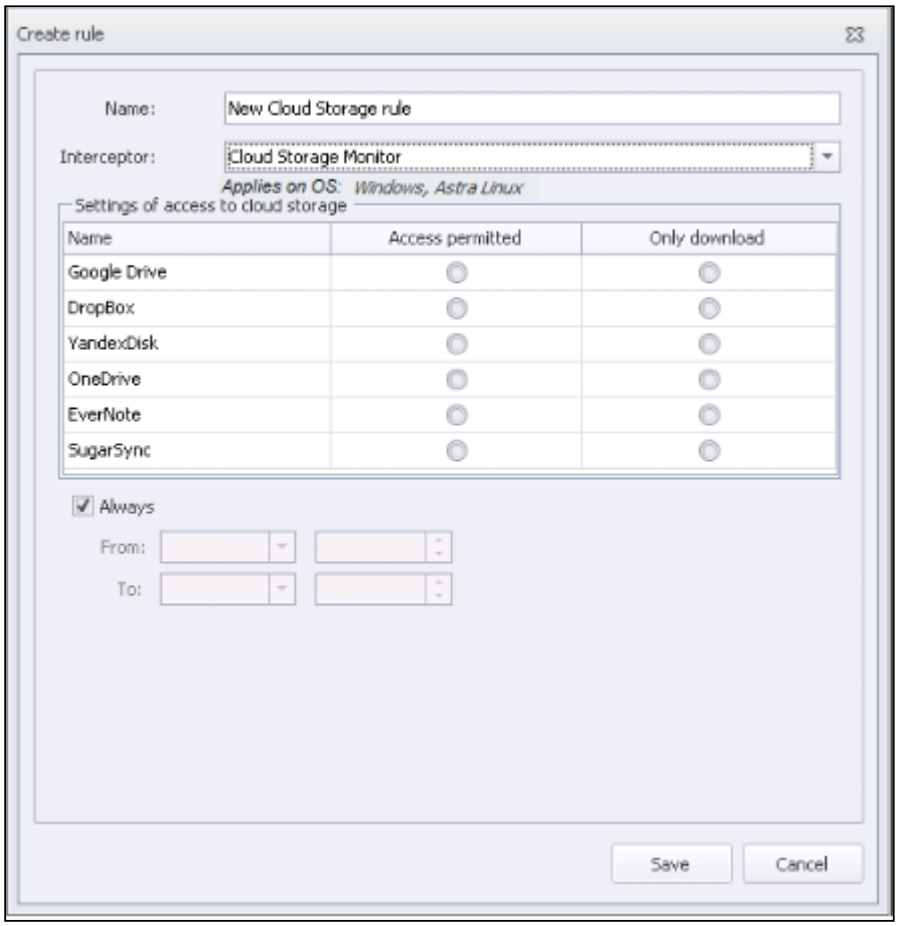
Cloud Storage Monitor Rule (DM)

The **Cloud Storage Monitor** interceptor allows you to control web clients of the following cloud storages:

- Google Drive
- DropBox
- YandexDisk
- OneDrive
- EverNote
- SugarSync

For all cloud storages, the following restriction modes are available: **Access Denied** and **Only download**.

> **Note:**
>
> The rule applies on computers with Windows and Astra Linux OS.




**To configure the rule**:

1. Open the **Create rule** window (see "Adding Rule (DM)") and in the **Name** field, specify the rule name.
2. In the **Interceptor** field, select **Cloud Storage Monitor**.
3. In the **Setting of access to cloud storage** area, mark the option for access limitation.
4. Define a period of the rule action. By default, the rule is always in effect (**Always** option is checked). To specify a period, clear **Always** checkbox and specify dates and time in **From** and **To** fields.
5. When all parameters are configured, click **Save**.

> **Important!**
>
> When the file was downloaded ever before on Yandex Disk by any person and was not completely removed (including the recycle bin), the shadow copy of this file cannot be made.

Device Monitor Rule (DM)

The **Device Monitor** interceptor allows you to control employee access to peripheral devices, mobile devices, and cameras connected to the computer as well as devices connected to thin and thick terminal clients.

> **Note:**
>
> The rule applies on computers with Windows OS.

You can configure appropriate control options for the following types of devices connected to the computer:

| Full access only to encrypted devices / Read only / No access / Allowed to use | Read only / No access / Allowed to use | No access / Allowed to use |
|---|---|---|
| • Floppy<br>• Removable storages (USB and IEEE 1394 devices) | • CD/DVD | • LPT port<br>• COM port<br>• Local Printer (with USB, IEEE 1394, SCSI connection, etc.)<br>• Image Editing Devices (cameras and scanners)<br>• Bluetooth Device<br>• IrDA Device<br>• Other USB Devices<br>• FireWire<br>• Modem<br>• Smart Card Reader<br>• Tape Drive<br>• Multifunctional Device<br>• PCMCI device<br>• USB Adapter<br>• Network printer<br>• Pocket Computer (Windows Mobile and Palm OS pocket computers)<br>• MTP-compatible device (connected via MTP or PTP) |

**Note:**

InfoWatch Device Monitor supports devices with information encrypted by InfoWatch CryptoStorage SOHO 2.1, InfoWatch CryptoStorage Enterprise 1.0, Kaspersky KryptoStorage 1.0 and TrueCrypt 7.1.

Mobile devices can be connected to the computer as:

- a removable storage;
- an MTP or PTP device;
- a USB network adapter.

Connection via MTP and PTP can be controlled for mobile phones on Android, iOS, Windows Phone/10 Mobile, and Blackberry 10 platforms.

A photo camera can be connected to the computer as:

- a removable device;
- a PTP device.

**Important!**

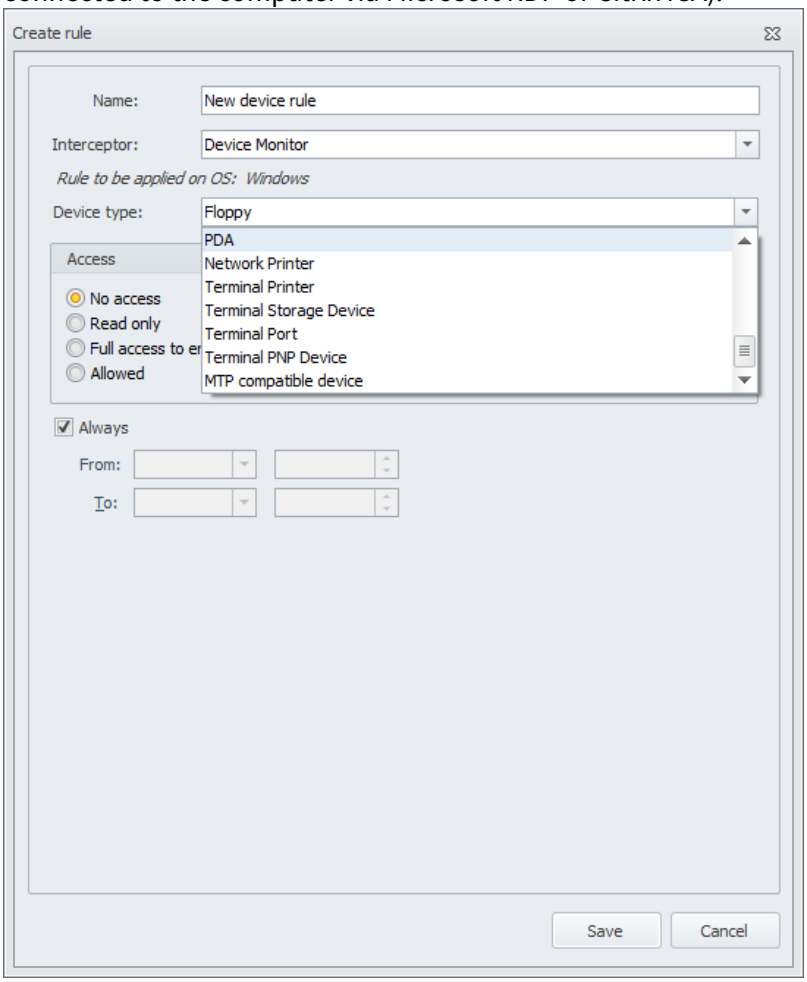
You can also use the File Monitor rule to control copying files to removable and MTP devices. Please note that the File Monitor rule allows you to monitor copying files, while the Device Monitor rule allows you to completely prohibit such operations. On how to solve conflicts if the event matches more than one rule, see "Applying Rules (DM)" and "Device Monitor Rules (DM) Application".

With this rule, you can also control the following types of devices which are connected via Microsoft RDP or Citrix ICA with the following restrictions:

| Read only / No access / Allowed to use | No access / Allowed to use |
|---|---|
| • Terminal storage | • Terminal printer<br>• Terminal port (thin client port)<br>• Terminal Plug and Play devices |

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).




**To configure the rule:**

1. Open the **Create rule** window (see "Adding Rule (DM)") and in the **Name** field, specify the rule name.
2. In the **Interceptor** field, select **Device Monitor**.
3. Select the device type controlled by this rule from the **Device type** drop-down list.
4. In the **Access** area, select the required access level. You can:
    - completely prohibit access to the device;
    - allow read-only access (only for **CD/DVD**, **MTP-compatible device**, **Floppy**, **Removable storage**, and **Terminal storage** types);

      > **Note:**
      >
      > For **MTP-compatible device** type, the read-only access level also enables deleting files from devices.

    - allow full access only to encrypted devices (only for **Floppy** and **Removable storage** types).
    - allow full access to the device;
5. Define a period of the rule 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.
6. When all parameters are configured, click **Save**.

**Specifics of applying the rule on particular devices:**

Mobile devices on BlackBerry 10 platform with "USB storage mode" setting enabled are treated by Device Monitor as two devices: *MTP-compatible device* and *Removable storage device*. To prevent copying data to the device, you should prohibit using *Removable storage device*.

File Monitor Rule (DM)

The **File Monitor** interceptor allows you to monitor the following operations: copying files from/to removable storages and network resources (including network volumes), writing to the file on a removable device. The System registers only successful operations.

> **Note:**
>
> The rule applies on computers with MS Windows and Astra Linux operating systems.

**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.

Using this rule, you can monitor the following actions of employees:

- Copying files to network resources using UNC (for example, *Server**SharedFolder**Folder**File*);
- Copying/moving files from/to a removable device. The System monitors operation of copying/moving from a controlled computer, another removable device or a network resource;
- Creating files directly on a removable device;

- Editing files directly on a removable device, including file renaming;
- Copying files to media devices connected via MTP;

> **Note:**
>
> The rule does not control operations of renaming files on media devices.

- Copying files to a terminal session application;
- Copying files to resources connected via terminal session (redirection for network folders and virtual devices is supported).

**Warning!**

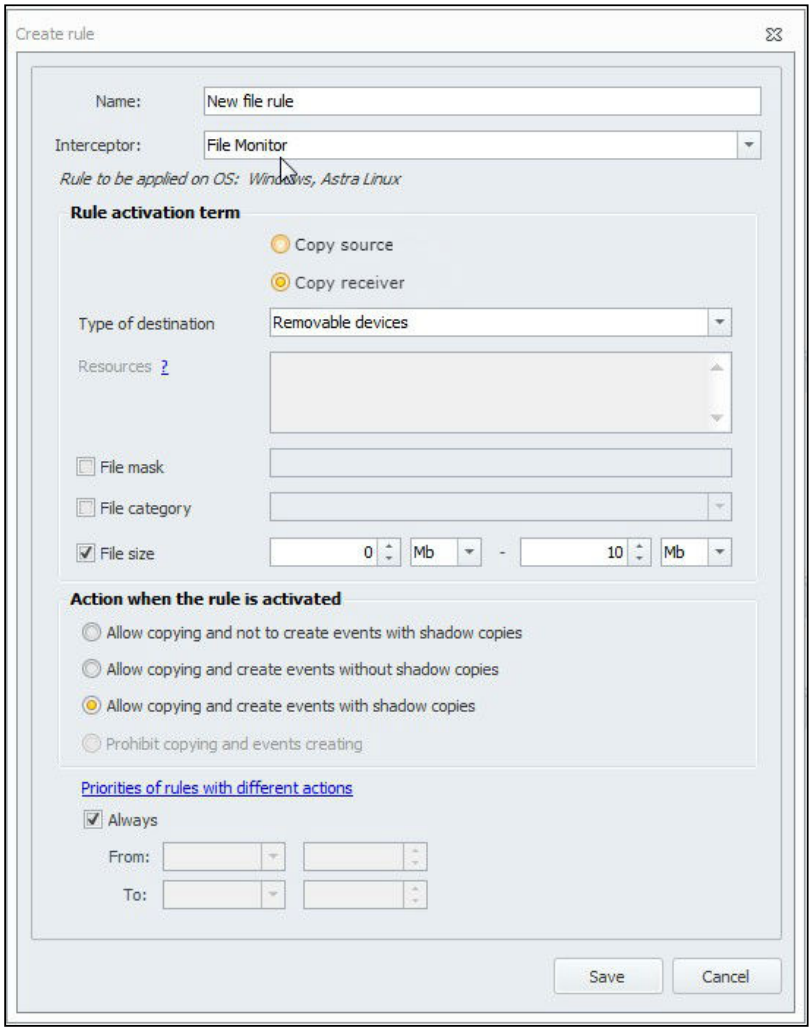
On computers with Astra Linux, the following operations are not controlled:

- copying/moving files to resources connected via terminal session;
- writing to CD/DVD disks including those connected via USB ports.

**Warning!**

You can also control access to removable and MTP-compatible devices with Device Monitor Rule (DM) which allows you to completely deny access to the device.

Information on cases when the rule matches several rules (DM), see in "Applying Rules (DM)".




**To configure the rule**:

1. Open the **Create rule** window (see "Adding Rule (DM)") and in the **Name** field, specify the rule name.
2. In the **Interceptor** field, select **File Monitor**.
3. Specify **Rule activation term:**
   a. set the intercepted copy direction: C*opy source* or C*opy receiver;*
   b. specify the type of destination: *Removable devices*, *Network resources*, or *Terminal session*;
   c. if required, specify the Network resources, setting its addresses.
4. If required, you may restrict the list of controlled files, setting the file mask. To do this, mark the field **File mask** and specify the mask: you may use «?» to replace one symbol or use «*» to replace the range of symbols. For example, *.doc. The backspace is interpreted as a part of a filename.

> **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 the mask.

> **Note:**
>
> Masks cannot be taken into consideration on the computers running under Astra Linux.

5. 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 the chosen signature type.

> **Note:**
>
> Signatures categories cannot be taken into consideration on the computers running under Astra Linux.

6. 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.
7. Select the option for the rule, you may:
   a. Allow copying and not to create events with shadow copies;
   b. Allow copying and create events without shadow copies;
   c. Allow copying and create events with shadow copies;
   d. Prohibit copying and events creating.

> **Warning!**
>
> If the File Monitor rule enables shadow copying, but there is less free space on the hard drive than required by the policy (DM) (see "Creating shadow copies and blocking operations due to space problems"), then the file will be saved without a shadow copy.

8. Define a period of the rule (DM) action. By default, the rule (DM) is always in effect (the **Always** option is checked). To specify a period, clear the **Always** check box and specify dates and time in **From** and **To** fields.
9. When all parameters are configured, click **Save**.

For details, see "Intercepting Features and Restrictions when Copying Files (Data Protection Policy on Agents)".

File Operations Monitor Rule (DM)

The **File Operations Monitor** interceptor allows you to control if applications read data from files or write to files. With this rule, you can also create file shadow copies and screenshots.

**Important!**

By default, the rule is unavailable. Only InfoWatch **engineers** can activate this feature.

For more information, please contact our technical support at support@infowatch.com.

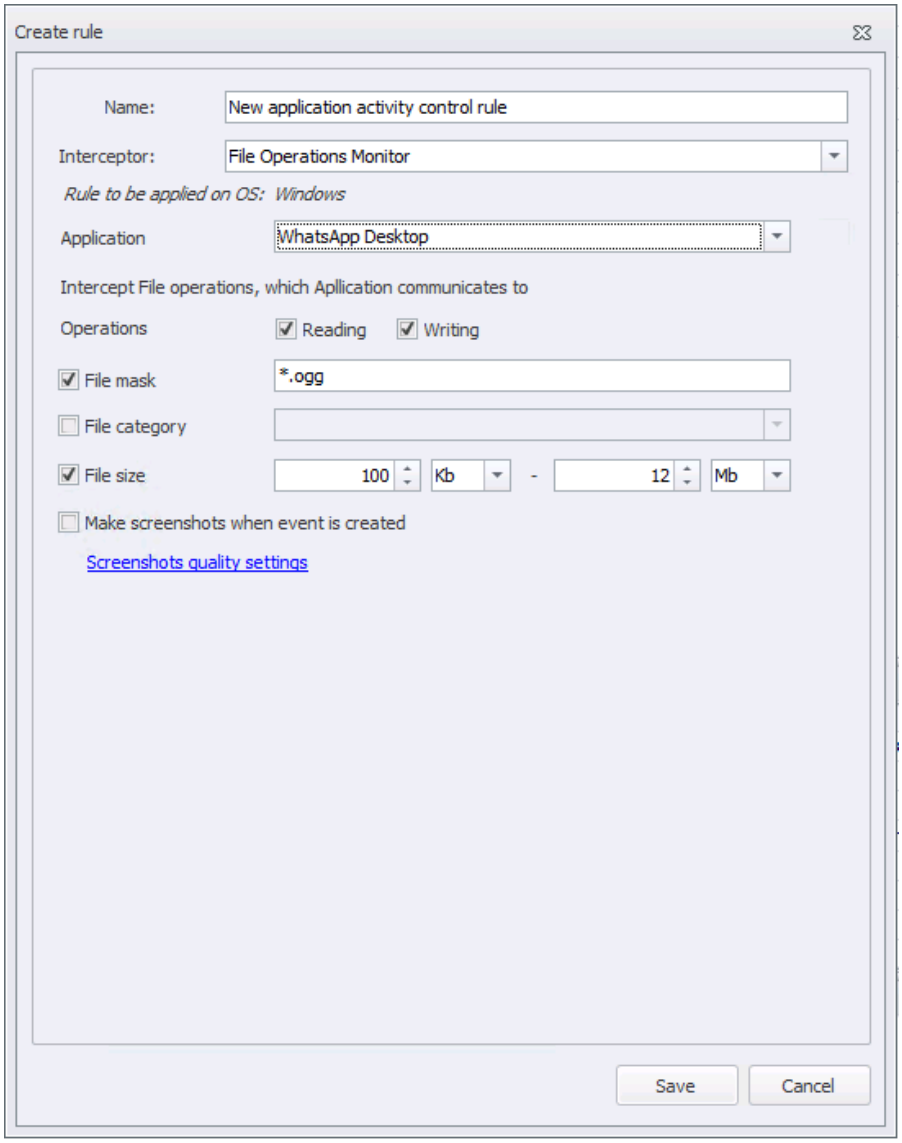
You can also visit the technical support section on our website: www.infowatch.com/support.

**Note:**

The rule applies on computers with MS Windows OS.

The rule provides advanced control of the following applications:

- Telegram Desktop
- WhatsApp Desktop
- Viber Desktop
- Google Chrome
- Microsoft Edge




**To configure the rule**:

1. Open the **Create rule** window (see "Adding Rule (DM)") and in the **Name** field, specify the rule name.
2. In the **Interceptor** field, select **File Operations Monitor**.
3. In the **Application** field, select the needed applications from the list of available applications.
4. In the **Operations** field, specify what operation you want to control:
    - Reading
    - Writing
5. If necessary, you can limit the set of controlled files using a file mask. For this, select the **File mask** option and specify the mask using the following characters:
    - «?» - to replace a single character;
    - «*» - to replace a set of characters. For example, *.doc;
    - The space is treated as a part of the file name.

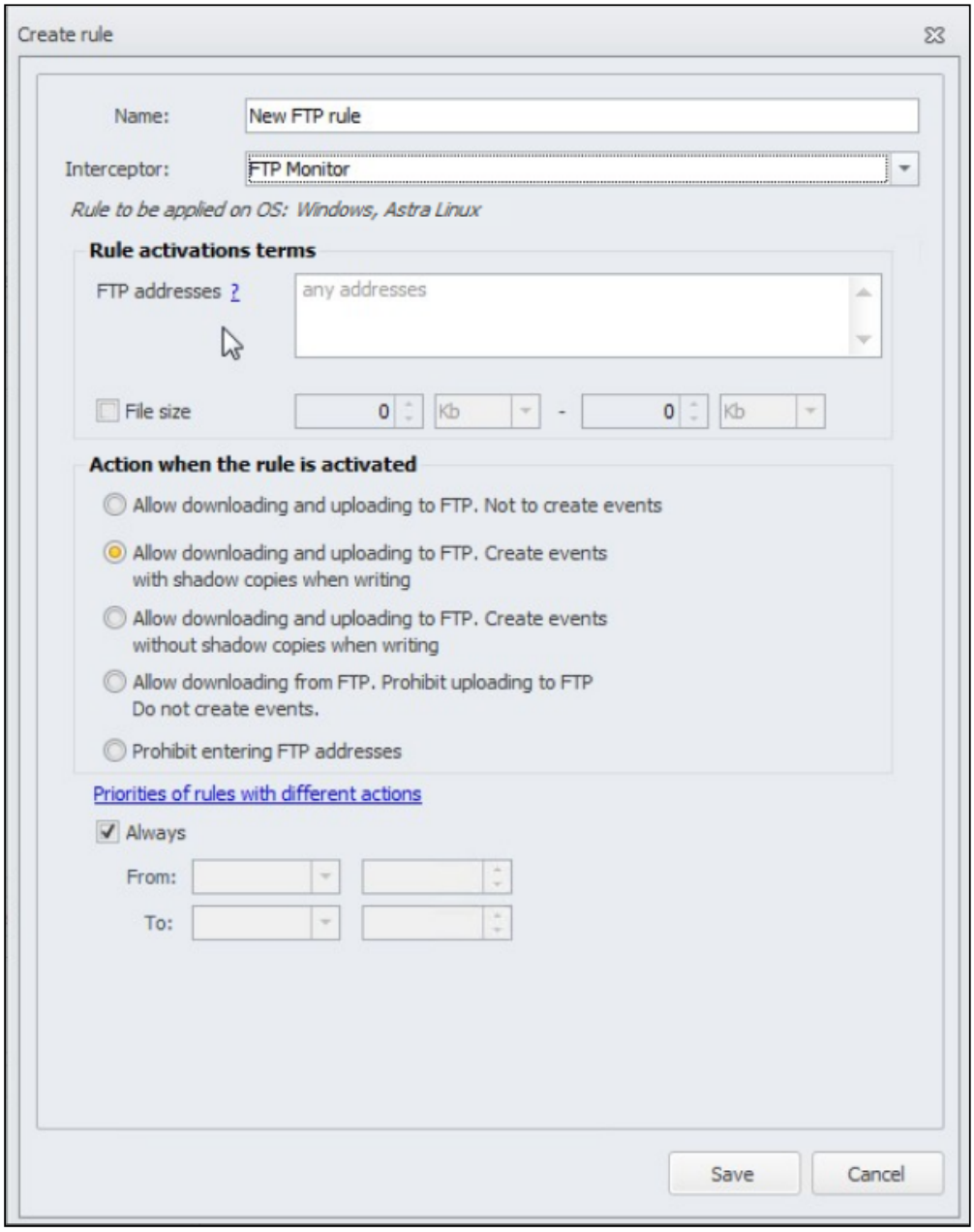
> **Important!**
>
> There can only be one mask for one rule (DM). If you need to add several masks, you should create a separate rule (DM) for each mask.

6. You can also limit the application of the rule (DM) with a signature category (see "Signatures"). For this, select the **Category** field and choose a category from a drop-down list: the rule (DM) will apply to files if their type matches the selected category of signatures.
7. To limit the size of controlled files, select the **File size** field and specify :
   - Minimum file size. If the field is filled, then the rule (DM) will only apply to files whose size is greater than or equal to the specified value.
   - Maximum file size. If the field is filled, then the rule (DM) will only apply to files whose size is less than or equal to the specified value.
8. To create screenshots, select the **Make screenshot when event is created** option.
9. If necessary, specify image quality settings: see "Application Control and screenshots".
10. When all parameters are configured, click **Save**.

FTP Monitor Rule (DM)

The **FTP Monitor** interceptor allows you to control data transfer through FTP/FTPS protocol.

> **Note:**
>
> The rule applies on computers with MS Windows and Astra Linux OS.




**To configure the rule**:

1. Open the **Create rule** window (see "Adding Rule (DM)") and in the **Name** field, specify the rule name.
2. In the **Interceptor** field, select **FTP Monitor**.
3. In **Rule activation terms** please specify **FTP addresses.** Clicking on **?** (question mark), you will know the details on how to fill in the field. You can also specify file size limitation, putting a check next to the File size tab. This parameter is available only when creating events with shadow copies and creating events without shadow copies when writing if there is less free space on the computer than it is required by the policy (DM) (see "Creating shadow copies and blocking operations due to space problems").
4. Select the control level for data exchange through the FTP protocol:
    - **Allow downloading and uploading to FTP. Not to create events**

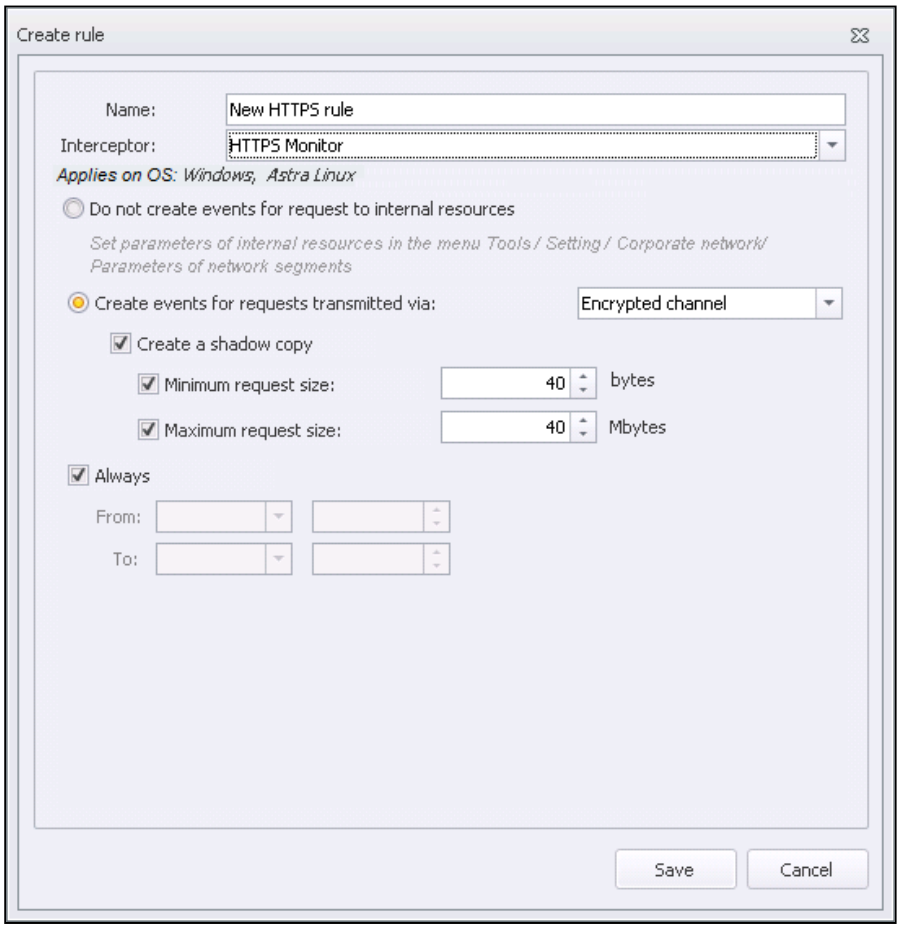
- **Allow downloading and uploading to FTP. Create events with shadow copies when writing**
- **Allow downloading and uploading to FTP. Create events without shadow copies when writing**
- **Allow downloading and uploading to FTP. Prohibit uploading to FTP. Do not create events**
- **Prohibit entering FTP addresses**

5. Define a period of rule (DM) action. By default, the rule (DM) is always in effect (the **Always** option is checked). To specify a period, clear the **Always** checkbox and specify dates and time in **From** and **To** fields.
6. When all parameters are configured, click **Save**.

HTTPS Monitor Rule (DM)

The **HTTPS Monitor** interceptor allows you to control data transfer through HTTP and HTTPS protocols.

> **Note:**
>
> The rule applies on computers with MS Windows and Astra Linux OS.




**To configure the rule**:

1. Open the **Create rule** window (see "Adding Rule (DM)") and in the **Name** field, specify the rule name.
2. In the **Interceptor** field, select **HTTPS Monitor**.
3. 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 "Corporate Network Control", **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.

   - 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 a specified size or larger.
     - **Maximum request size**. If the check box is selected, shadow copies will be enabled only for files of a specified size or smaller.

     **Important!**

     If there is less free space on the computer than it is required by the policy (see. "Creating shadow copies and blocking operations due to space problems"), then the event will be created without a shadow copy.

4. Define a period of the rule (DM) action. By default, the rule (DM) is always in effect (the **Always** option is checked). To specify rule (DM) duration, clear the **Always** check box and specify dates and time in **From** and **To** fields.
5. 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.

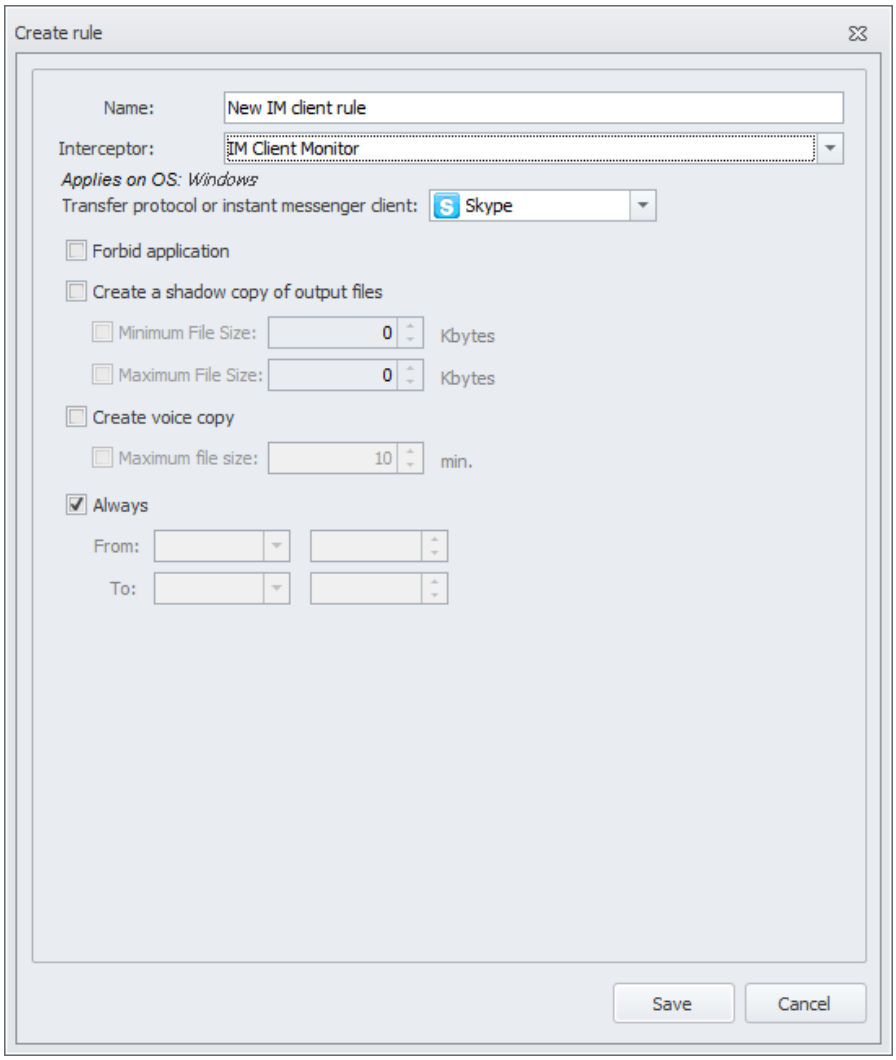
IM Client Monitor Rule (DM)

The **IM Client Monitor** interceptor allows you to control employee access to instant messengers: Skype, Telegram, Jabber (XMPP protocol), Facebook, VK (MMP protocol).

**Note:**

The rule applies on computers with the following operating systems:

- MS Windows and Astra Linux - for Facebook, Jabber (XMPP), VK (VKontakte);.
- MS Windows only - for Skype, MMP, Telegram.




**To configure the rule**:

1. Open the **Create rule** window (see "Adding Rule (DM)") and in the **Name** field, specify the rule name.
2. In the **Interceptor** field, select **IM Client Monitor**.
3. In **Transfer protocol or instant messenger client** field, select messenger type which is controlled by this rule (DM):
   - Skype - to control usage of Skype versions 7, 8 and Skype For Web

- XMPP - to control Jabber usage
- MMP - to control applications, using MMP protocol;
- Telegram - to control Telegram usage on mobile devices
- Facebook - to control Facebook usage
- VK - to control VK usage

4. If you need to intercept Skype voice messages, select the **Create shadow copy of output files** checkbox and, if necessary, specify file size (sound file will be saved in `*.ogg` format)
    - If the **Maximum File Size** option is selected, then several events with shadow copies will be created for talks, whose length exceeds the specified value.
5. If you want to completely prohibit using Client of this type, select the **Forbid application** checkbox (not available for **Telegram, Facebook, VK**).

> **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 prohibit using Telegram, Facebook, and VK, use Application Monitor Rule (DM) (see "Application Monitor Rule (DM)").

6. If you want to create shadow copies of transferred files and send them to Traffic Monitor, select the **Create shadow copy of output file** checkbox. In this case, you can also define additional parameters for shadow copies:
    - **Minimum File Size**. When checked, shadow copies will be created only for files of larger or equal size.
    - **Maximum File Size**. When checked, shadow copies will be created only for files of smaller or equal size.
7. If you want to create shadow copies of voice messages and send them to Traffic Monitor, select the **Create voice copy** option and specify the maximum length of a voice file. For this, in the **Maximum file size** field, specify the required value in minutes.
8. Define a period of the rule (DM) action. By default, the rule (DM) is always in effect (the **Always** option is checked). To specify the rule (DM) duration, clear the **Always** checkbox and specify dates and time in **From** and **To** fields.
9. When all parameters are configured, click **Save**.

> **Warning!**
>
> Values specified in the **Minimum File Size** and **Maximum File Size** fields apply only to creating shadow copied. If the file size is within the specified range, then the event will contain a shadow copy. Otherwise, the event will be created without a shadow copy. The event can be created without a shadow copy also in the case if there is less free space on the computer than it is required by the policy (DM) (see "Creating shadow copies and blocking operations due to space problems").

If there is an active IM Client Monitor rule (DM), then shadow copies for chats and messages are created regardless of the **Create shadow copy of output file** and **Create voice copy** settings. Shadow copies for chats and messages are configured in the "Network Traffic Control" section.

**Important!**

When sending messages to a Skype group chat, the list of recipients in the event includes also the chat ID.

If sending a file is the first message in the group chat, then the list of recipients in the event will contain only the chat ID.

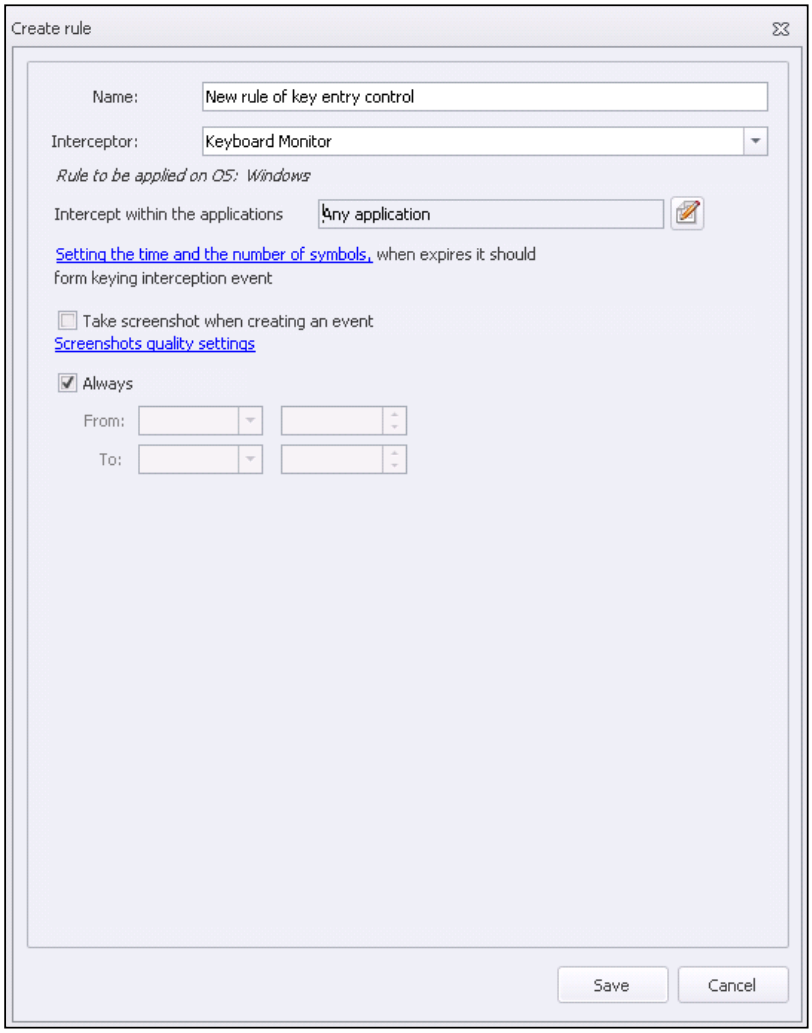
You can use the chat ID in queries to search for events (see "Creating Queries"). When entering the ID, use the mask *. For example: d57efb0b486c4*.

Keyboard Monitor Rule (DM)

The **Keyboard Monitor** interceptor allows you to intercept text which is entered from the keyboard on workstations. Events which are created from intercepted data are then sent to Traffic Monitor for analysis and further processing.

**Note:**

The rule applies on computers with MS Windows OS.




**To configure the rule:**

1. Open the **Create rule** window (see "Adding Rule (DM)") and in the **Name** field, specify the rule name.
2. In the **Interceptor** field, select **Keyboard Monitor**.
3. In the **Intercept within the applications** area, specify:
   - applications where the rule should apply. To choose applications, click : see "Application Protocol".
   - *Any application* - if you want to intercept keyboard input in all applications.
4. If required, specify additional conditions for creating events: see "Control of Keyboard Input".
5. Set flag next to the field **Take screenshot when creating event** to select the corresponding option.
6. If required, specify the screenshots quality settings: see "Application Control and screenshots".
7. Define the period of rule action. By default, the rule is always in effect (the **Always** option is checked). To specify the rule duration, clear the **Always** check box and specify dates and time in the **From** and **To** fields.
8. When all parameters are configured, click **Save**.

Mail Monitor Rule (DM)

The **Mail Monitor** interceptor allows you to control incoming and outgoing e-mail.

The Mail Monitor rule provides control of SMTP, IMAP, POP3, HTTPS protocols, and Outlook.

**Note:**

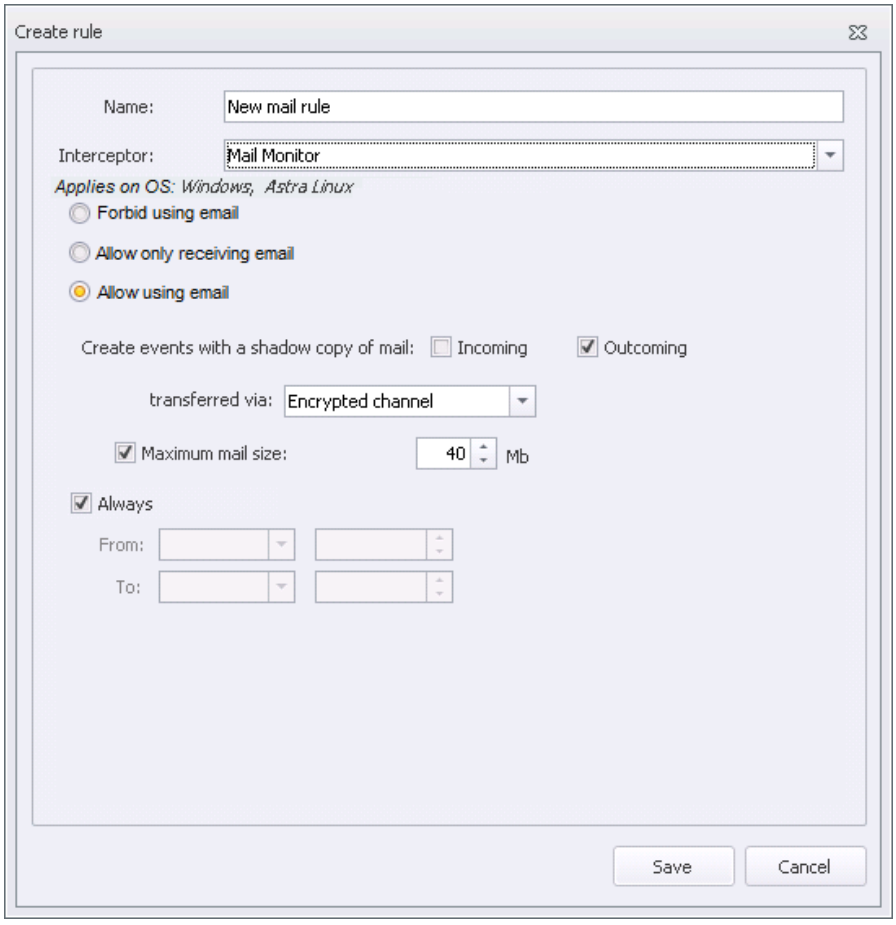
For HTTPS, the System controls emails sent via the following services:

- Gmail
- Yandex
- Mail.ru
- Yahoo
- Rambler
- Outlook.com

**Important!**

The rule applies on computers with MS Windows and Astra Linux OS.

On computers with Astra Linux, the rule controls only SMTP, POP3, IMAP, and HTTPS protocols.




**To configure the rule**:

1. Open the **Create rule** window (see "Adding Rule (DM)") and in the **Name** field, specify the rule name.
2. In the **Interceptor** field, select **Mail Monitor**.

3. In the **Protocol** field, choose the channel that will be controlled by the rule. Possible values:
   - **All channels**;
   - **SMTP** - only for outgoing mail;
   - **POP3** - only for incoming mail;
   - **Outlook** - both for incoming and for outgoing mail;
   - **IMAP** - only for incoming mail;
   - **HTTPS** - only for outgoing mail.
4. Choose what actions with mail are allowed for the user. Possible values:
   - **Forbid using email**;
   - **Allow only receiving mail** - is available only if *Outlook* or *All channels* value is selected in the **Protocol** field;
   - **Allow using email**.
5. In the **Create events with a shadow copy of mail** line, specify for what emails shadow copies should be created. Depending on the channel selected in step 6 the following values are available:
   - for **POP3** and **IMAP** channels - only the **Incoming** direction;
   - for **SMTP** and **HTTPS** - only the **Outgoing** direction;
   - for **Outlook** and **All channels** - both **Incoming** and **Outgoing** directions are available. You can choose one value or both.

   **Warning!**

   If the **Allow using email** 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:
   - In the **transferred via** field, specify if shadow copies should be created for emails sent via all channels or only via encrypted ones;

     **Note:**

     For HTTPS protocol, the **All channels** value is unavailable.

   - **Maximum mail size**. If the option is enabled, shadow copies will be created only for emails which 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 space problems"), a shadow copy will not be created.

6. Define a period of the rule action. By default, **Always** option is active. To specify the rule (DM) duration, clear **Always** checkbox and specify dates and time in **From** and **To** fields.
7. When all parameters are configured, click **Save**.

**Warning!**

If the rule has the following attributes:

- **Allow using mail**;
- **Create events with a shadow copy of mail: Incoming and Outcoming, transferred via: All channels**.

and the mail program is configured to store data on the server (e.g., in MS Outlook, the **Save sent items to the next folder on the server** option is enabled in the **Internet E-mail Settings** dialog box, **Sent** tab), then each mail sending event will generate two interception objects: one of the **Outcoming** type and the other one of the **Incoming** type. Depending on the mail program, the option name may differ.

**Example:**

To intercept Outlook emails via IMAP, SMTP, POP3 protocols at the network level:

1. Cancel excluding **Outlook** from network interception (for details, see "Exclusion of Application from Interception"). By default, this option is enabled.
2. Create a rule, activating interception for these protocols, as described above.
3. Delete the rule for Outlook/MAPI protocol.

**Important!**

When Outlook is included in network interception, operation with MS Exchange server may be incorrect.

Network Monitor Rule (DM)

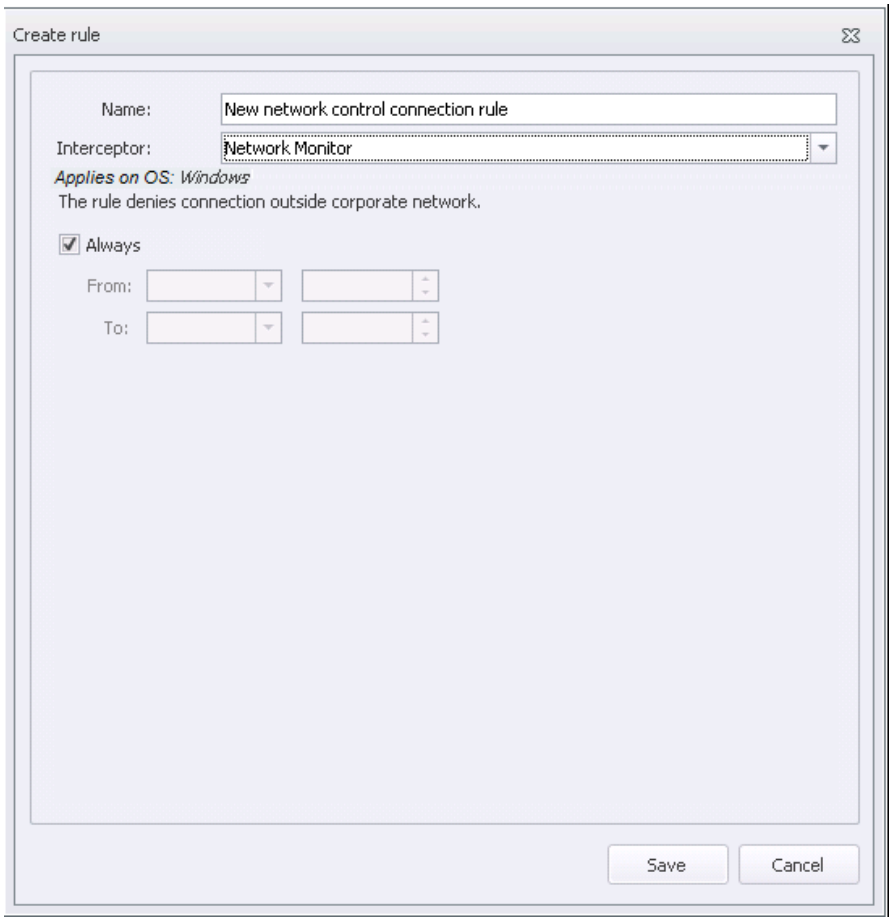
The **Network Monitor** interceptor allows you to prohibit data transfer over any network connections except connections with the corporate network or specified authorized servers. On how to define segments of the corporate network and authorized external addresses, see "Corporate Network Control".

**Note:**

The rule applies on computers with MS Windows OS.

**Warning!**

If there is at least one active Network Monitor rule, Device Monitor Agent installed on the computer tries to resolve the DNS names of Internet pages being opened. To avoid problems with external connections, you should configure forwarding servers on the corporate DNS server (for details, see the Internet article "Configure a DNS Server to Use Forwarders").



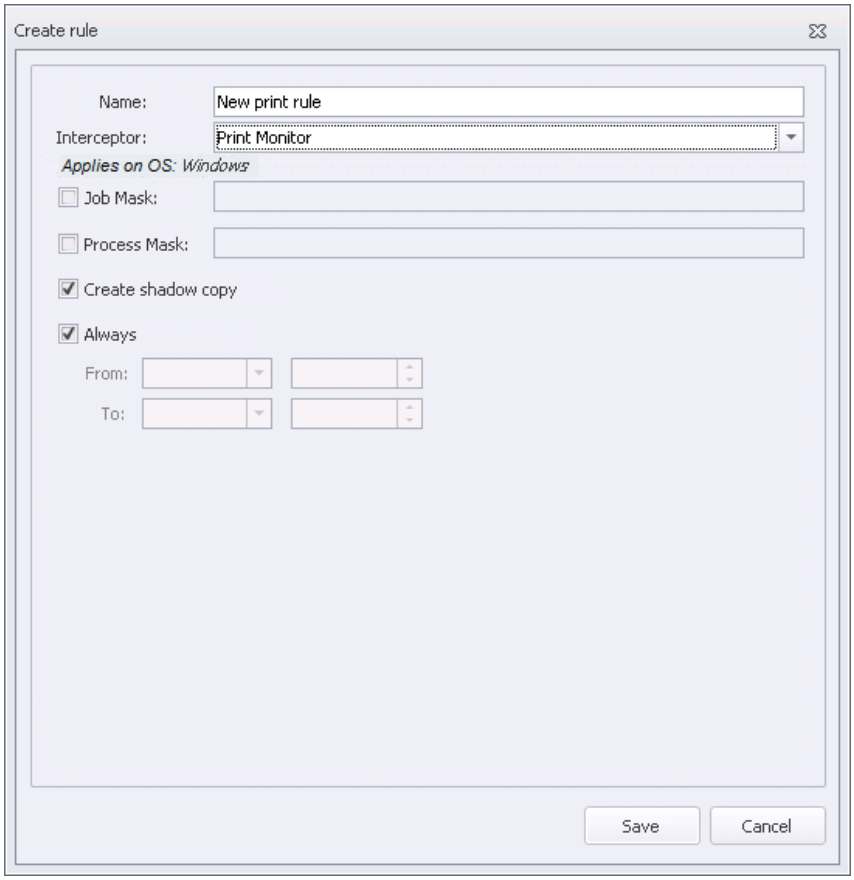

**To configure the rule**:

1. Open the **Create rule** window (see "Adding Rule (DM)") and in the **Name** field, specify the rule name.
2. In the **Interceptor** field, select **Network Monitor**.
3. Define a period of the rule (DM) action. By default, the rule (DM) is always in effect (the **Always** option is checked). To specify the rule (DM) duration, clear the **Always** check box and specify dates and time in **From** and **To** fields.
4. When all parameters are configured, click **Save**.

Print Monitor Rule (DM)

The **Print Monitor** interceptor allows you to monitor operations related to printing documents on local and network printers.

> **Note:**
>
> The rule applies on computers with MS Windows OS.




**To configure the rule**:

1. Open the **Create rule** window (see "Adding Rule (DM)") and in the **Name** field, specify the rule name.
2. In the **Interceptor** field, select **Print Monitor**.
3. If necessary, you can specify restrictions for 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 wildcards: «?» to replace one character or «*» to replace several characters. Spaces are treated as a part of the task name.

      **Important!**

      The title for printing task is being generated by the application, where from the document is sent for printing. That's why the title may be any tex and not the one that is a document title.

    - **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 wildcards: «?» to replace one character or «*» to replace character set. Spaces are treated as a part of the task name.

4. 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 space problems"), then the document will be printed without creating a shadow copy.

5. Define a period of the rule action. By default, the rule (DM) is always in effect (the **Always** option is checked). To specify the rule duration, clear the **Always** check box and specify dates and time in the **From** and **To** fields.
6. When all parameters are configured, click **Save**.

**Example:**

To intercept the printing task file with `.txt` extension, in `notepad.exe`:

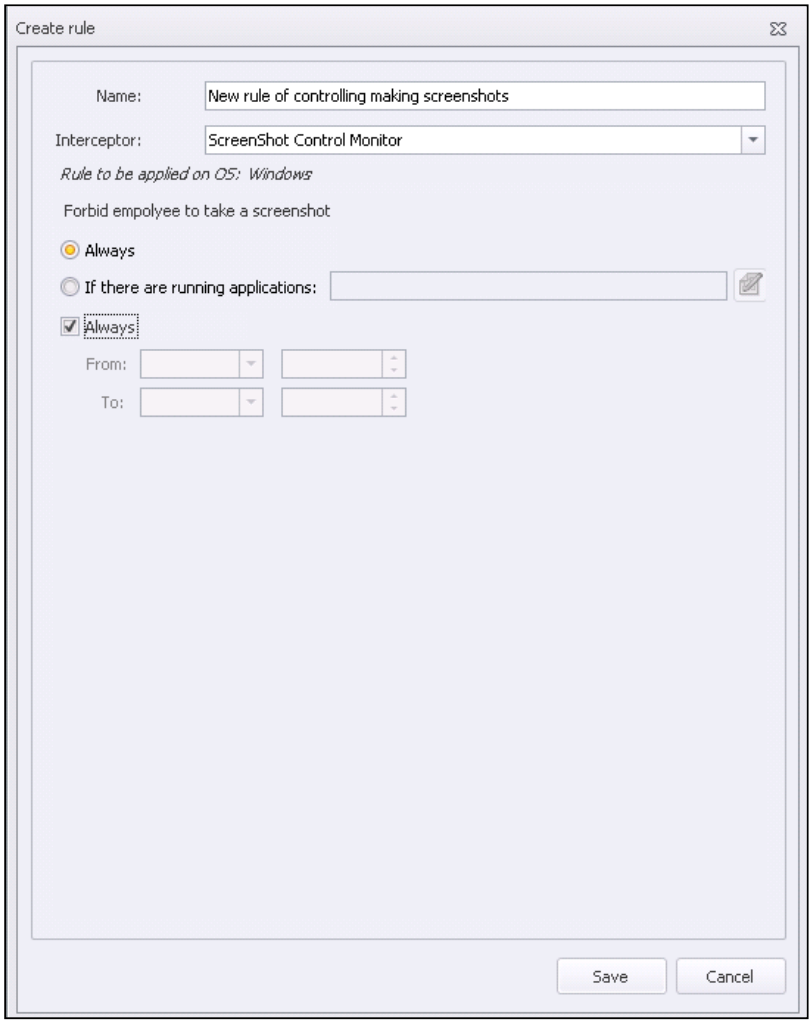
1. In Process Mask line enter *.txt*
2. In Process Mask line enter *nodepad.exe

> **Important!**
>
> The printing tasks are to be intercepted in case the user OS displays the files extension (In Folder options unmark **Hide extension for registered file types**).

ScreenShot Control Monitor Rule (DM)

The **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**:

1. Open the **Create rule** window (see "Adding Rule (DM)") and in the **Name** field, specify the rule name.
2. In the **Interceptor** field, select **ScreenShot Control Monitor**.
3. In the **Forbid employee to take a screenshot** area, specify the condition. Possible choices:
   - **Always**;
   - **If there are running applications**. If you select this option, click  to specify applications (see "Applications protocol").
4. Define a period of the rule action. By default, the rule is always in effect (the **Always** option is checked). To specify rule (DM) duration, clear the **Always** check box and specify dates and time in the **From** and **To** fields.
5. When all parameters are configured, click **Save**.

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.

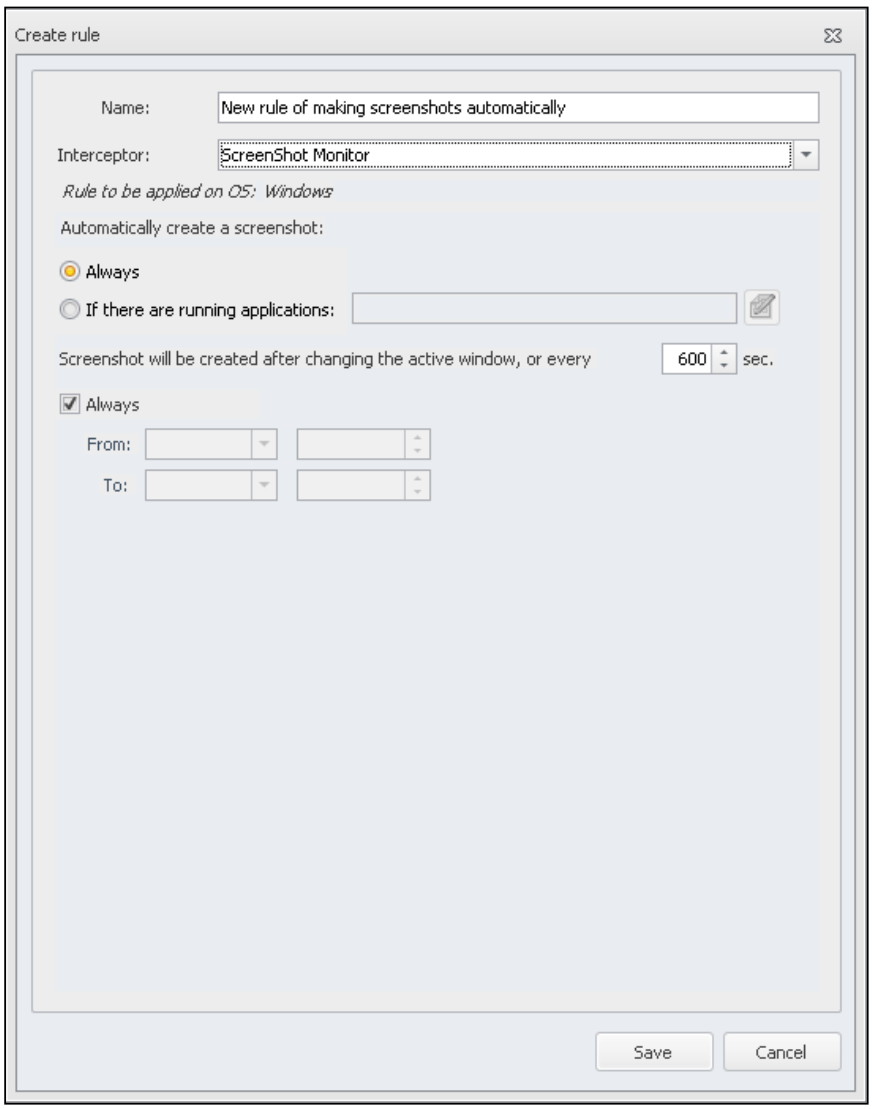
**Warning!**

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 "Application Control and screenshots").

**Important!**

To create screenshots when data is copied to the clipboard or pasted from the clipboard use the Clipboard Monitor rule (see "Clipboard Monitor Rule (DM)").

To create screenshots when intercepting text input from keyboard on workstations use the Keyboard Monitor rule (see "Keyboard Monitor Rule (DM)").



**To configure the rule**:

1. Open the **Create rule** window (see "Adding Rule (DM)") and in the **Name** field, specify the rule name.
2. In the **Interceptor** field, select **ScreenShot Monitor**.
3. In the **Automatically create a screenshot** area, define in which case the rule (DM) is valid. Possible choices:
   - **Always**;
   - **If there are running applications**. If you select this option, click  to specify applicaitons (see "Application protocol").
4. Specify the periodicity of screenshots creation (in seconds). The default value is 600. A screenshot is also created when the user switches to a different window.
5. Define the period of rule action. By default, the rule is always in effect (the **Always** option is checked). To specify the rule duration, clear the **Always** check box and specify dates and time in the **From** and **To** fields.
6. When all parameters are configured, click **Save**.

## 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.

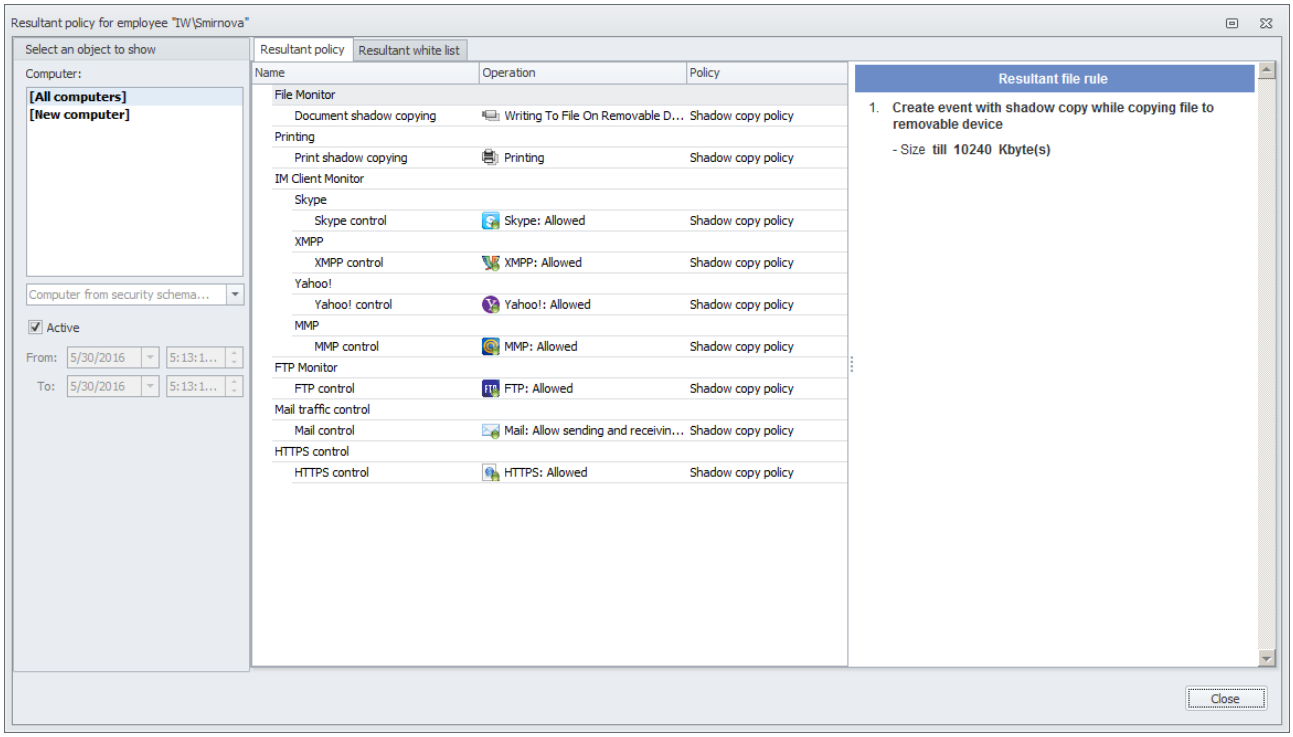
> **Note:**
>
> Some information on **Details** panel is duplicated in the main screen workspace.

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.

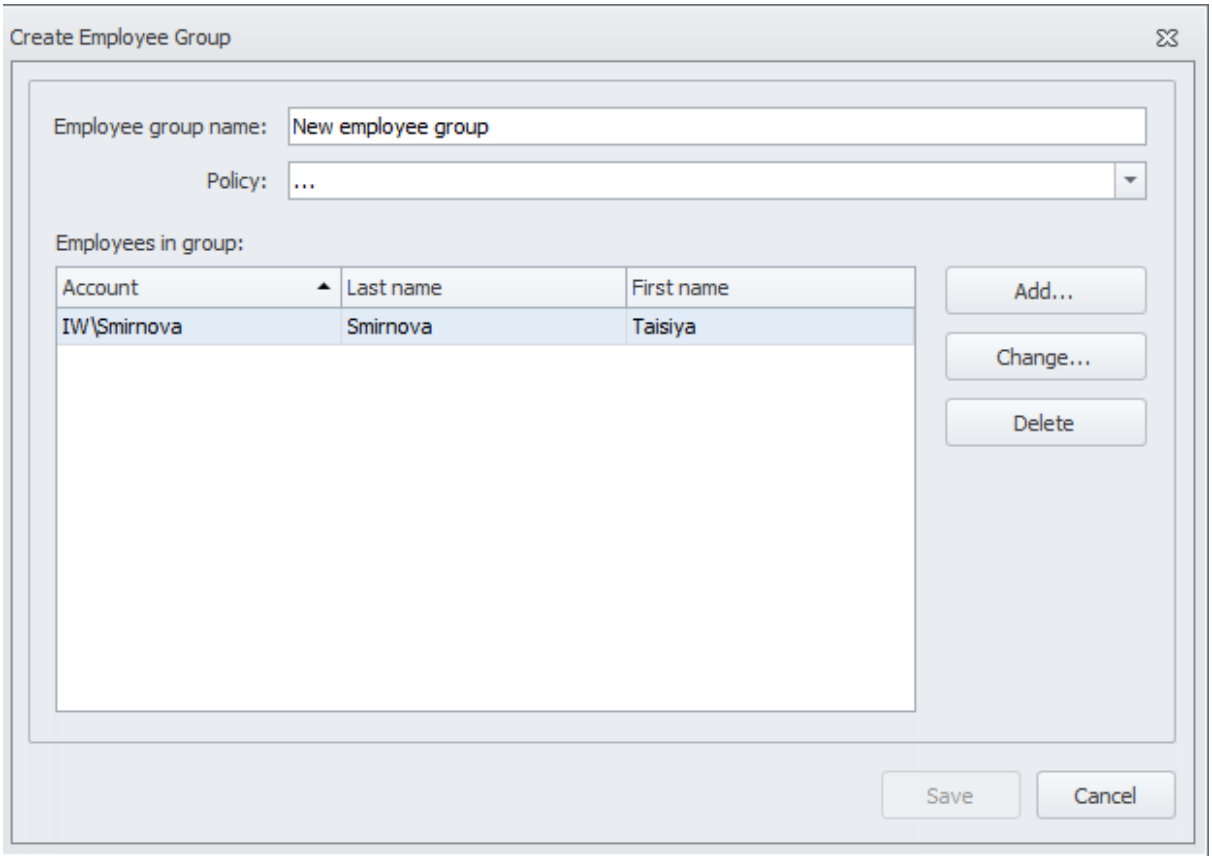
Adding and Editing an Employee Group

**To add or edit an employee group**:

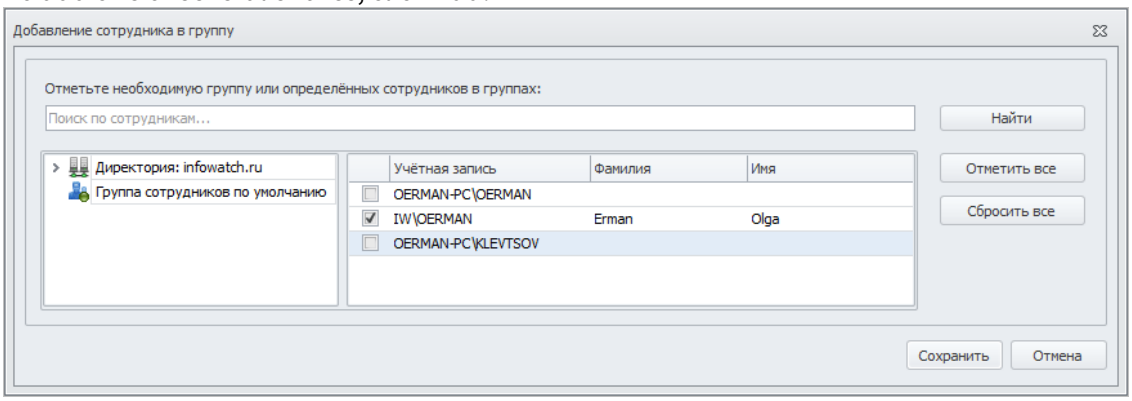
1. Go to **Employees** section.
2. Take one of the following steps:

| Action | Steps |
|---|---|
| Add employee group | • select **Edit > Create Employee Group** in the Main Menu;<br>• 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.<br>b. Take one of the following steps:<br>• in the Main Menu, click **Edit > Edit Employee Group**;<br>• click **Edit Employee Group** at the top of Navigation pane;<br>• 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 "Active Directory Connecting and Synchronizing") 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.

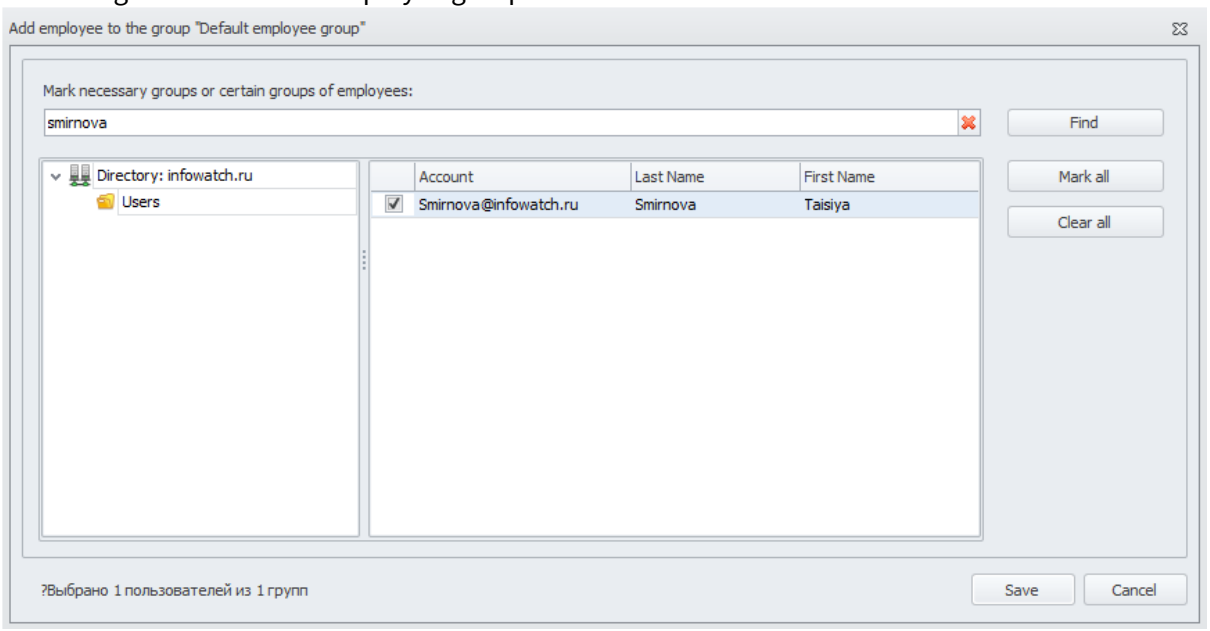
This adds an account to the selected group.

You can also manually import an information on the employee from directory service (see connection configuring description in "Active Directory Connecting and Synchronizing"). 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 "Active Directory Connecting and Synchronizing") 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!**

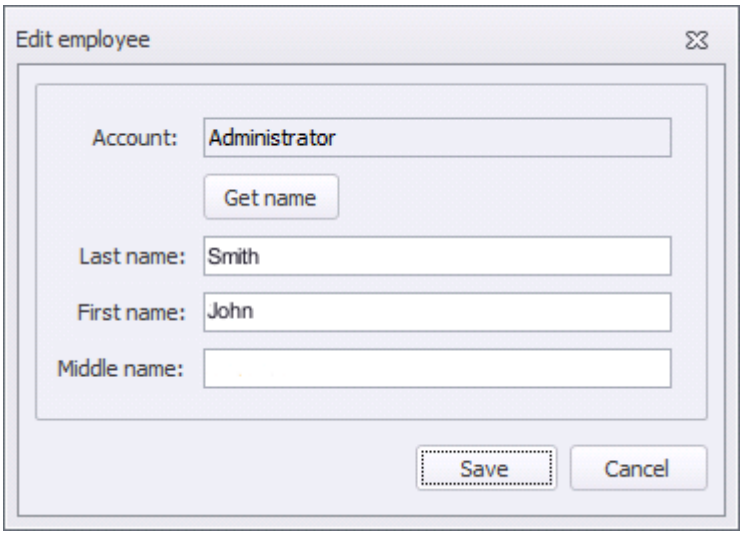
To apply changes you have to save current security scheme (see "Editing Security Scheme"). If you don't save your security schema, all changes will be discarded.

Editing Employee Account

Parameters of employee account can be 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 epy 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

### Viewing Computer Details

**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.

Information on computers is displayed as a table. The table columns contain basic properties of the computer. You can adjust the order of columns and hide columns you do not need.

The table 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 after the Agent is uninstalled from the 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.

**Note:**

Workstation comment is to be saved immediately while editing with no changes within security scheme. Thus, the following restrictions should be taken into consideration:

- changing workstation comment it is to be stored immediately in DB even when security scheme is being edited;
- changing comment of the workstation that was just added, the comment to be saved only when security scheme is saved.

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:

- **Settings**. Common security policy (DM) settings version number (see "General System Settings").
- **Template version**. Version of templates for notifications to be displayed to employees.
- **Version of network control settings**. Data transmission through network connections with the help of Network Monitor control version (see "Corporate Network Control").
- **Configuration version of network applications control**. Version of network traffic control configuration, using protocols YMSG,XMPP, MMP, FTP, FTPS, SMTP/S/MIME/Outlook/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.
- **Version of TM configuration**. The last version of TM configuration that was delivered to the workstation.
- **Free disk space on computers**. Free space size on disks, where shadow copies are saved (also in percentages).

**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 space problems"), 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:

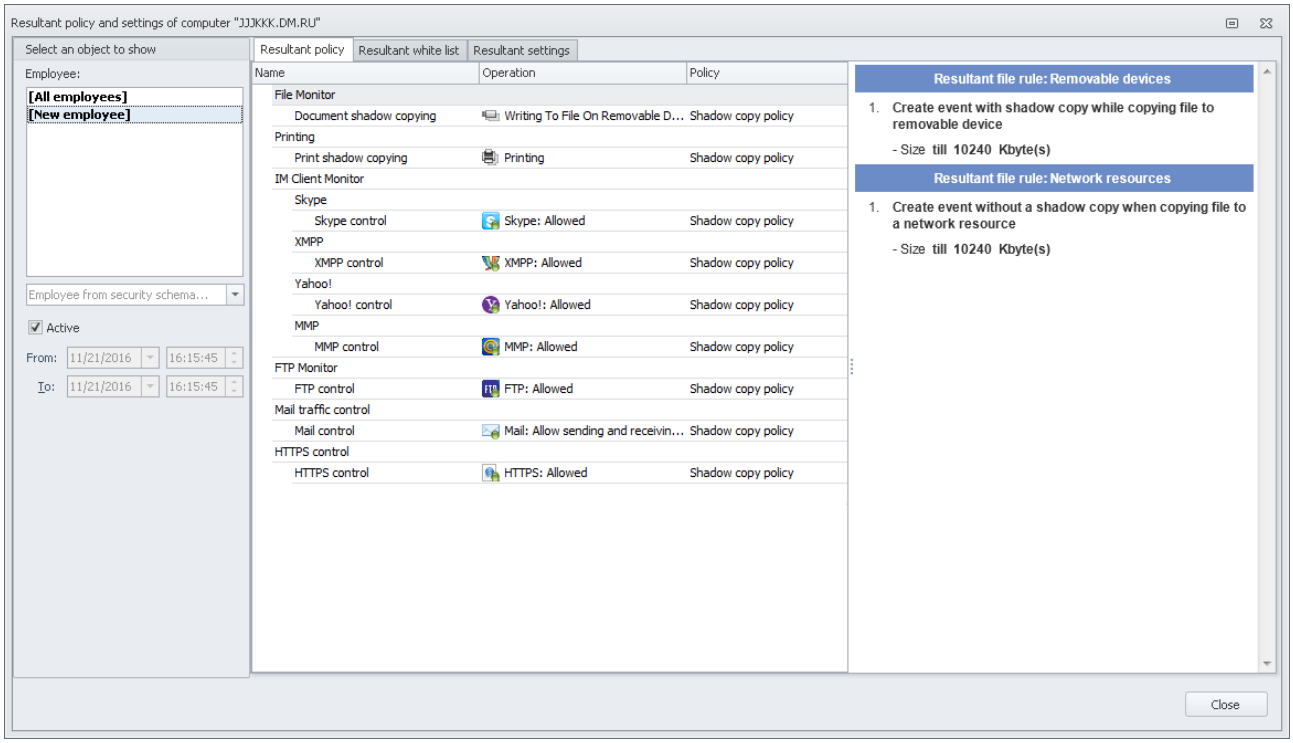
- manage computer groups:
  - add computer groups;
  - edit computer group parameters;
  - delete workstation groups.
- manage computers:
  - add computers' information to computer groups and thus define computer security policy;
  - remove computers from workstation group;
  - delete computer from security schema;
  - update Agents at managed computers.

Viewing Resultant Settings, Policy (DM) and Resultant White List for Computer

To view information about settings, policy (DM) and white list 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 resulting policy (DM) for all employees on the chosen computer is 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) consists of 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 a new employee (which is not yet registered in security scheme) are displayed.
- To view resulting policy\white list\settings for a specific 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:

- by default, **Active** setting is enabled, and current resultant policy/white list/settings for an employee are displayed;
- untick **Active** box and specify the period, to view resultant policy/white list/settings for the period.

**Warning!**

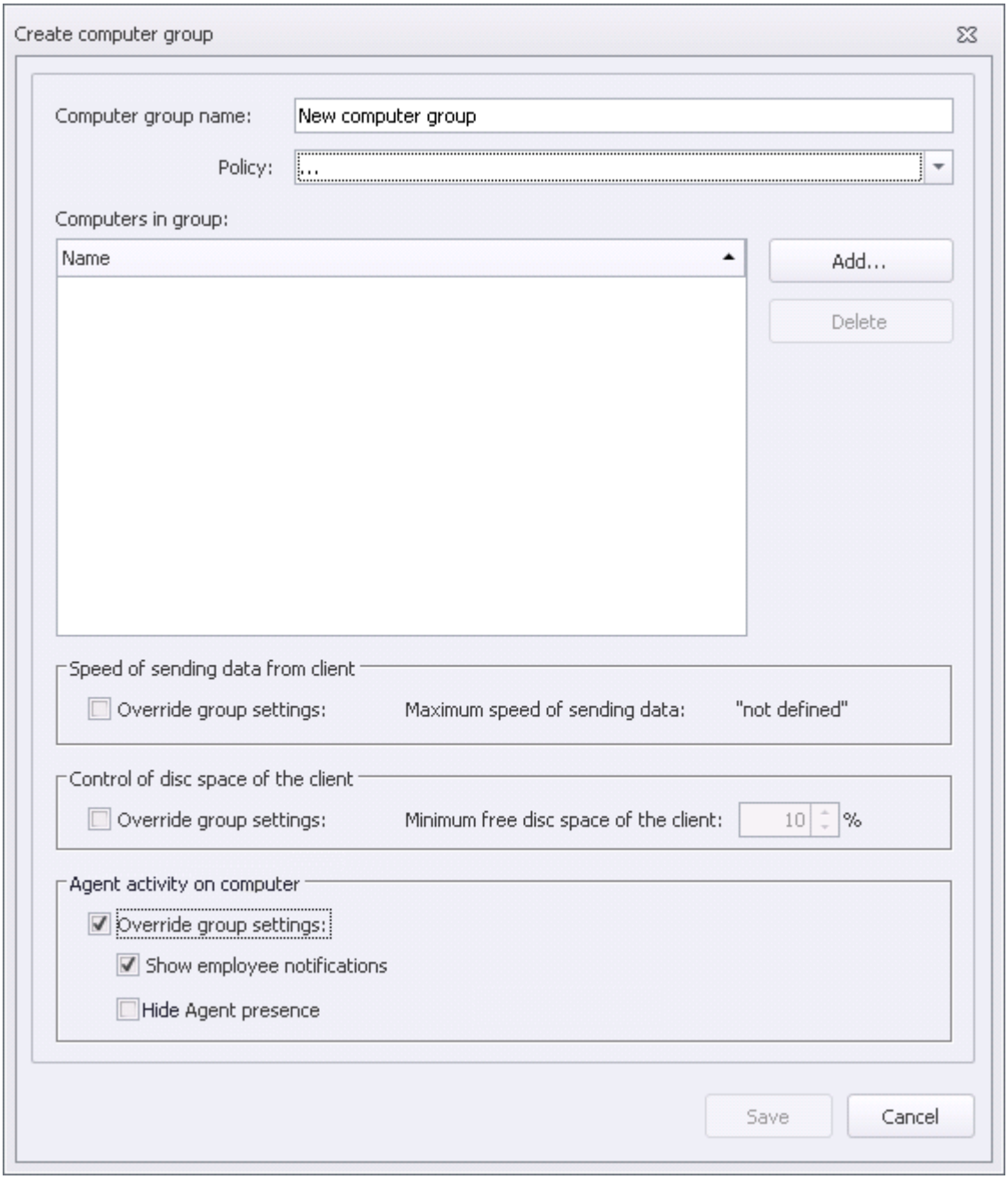
When you register a new computer, information on this computer is automatically added to the security scheme (to the "default" computer group).

**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**;<br>• click **Create Computer Group** at the top of Navigation pane. |
| Edit computer group | a. In **Computers** area of Navigation pane select workstation group name.<br>b. Take one of the following steps:<br>• in the Main Menu select **Edit > Edit**;<br>• click **Edit** at the top of Navigation pane;<br>• 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:
     - Microsoft Windows Network;
     - AD and/or ALD tree;
     - 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 a 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 "Active Directory Connecting and Synchronizing") 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.

**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 a 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:

- received from Microsoft Windows Network;
- from AD and/or ALD tree;
- among previously registered in the System. For this, type computer name in the search line and click **Search**.

> **Warning!**
>
> Connection or search of a computer is limited by connected directories (marked ).

4. Flag computers or computer groups ( ).
   a. Minimized groups are marked with an icon ; expanded - . Doubleclick a group, to expand or collapse it.
   b. You can also specify computer name in the line at the bottom of dialog box. When listing names, separate them with semicolons.
   c. Select **Connect all directories**. Herewith, all directories will be consistently connected after indicating authorization data.
5. Click **Save**.

This closes **Select computer** dialog and adds information on selected computers to the computer group.

> **Warning!**
>
> To apply changes you have to save the 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.

**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**.

## 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 Settings, 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.

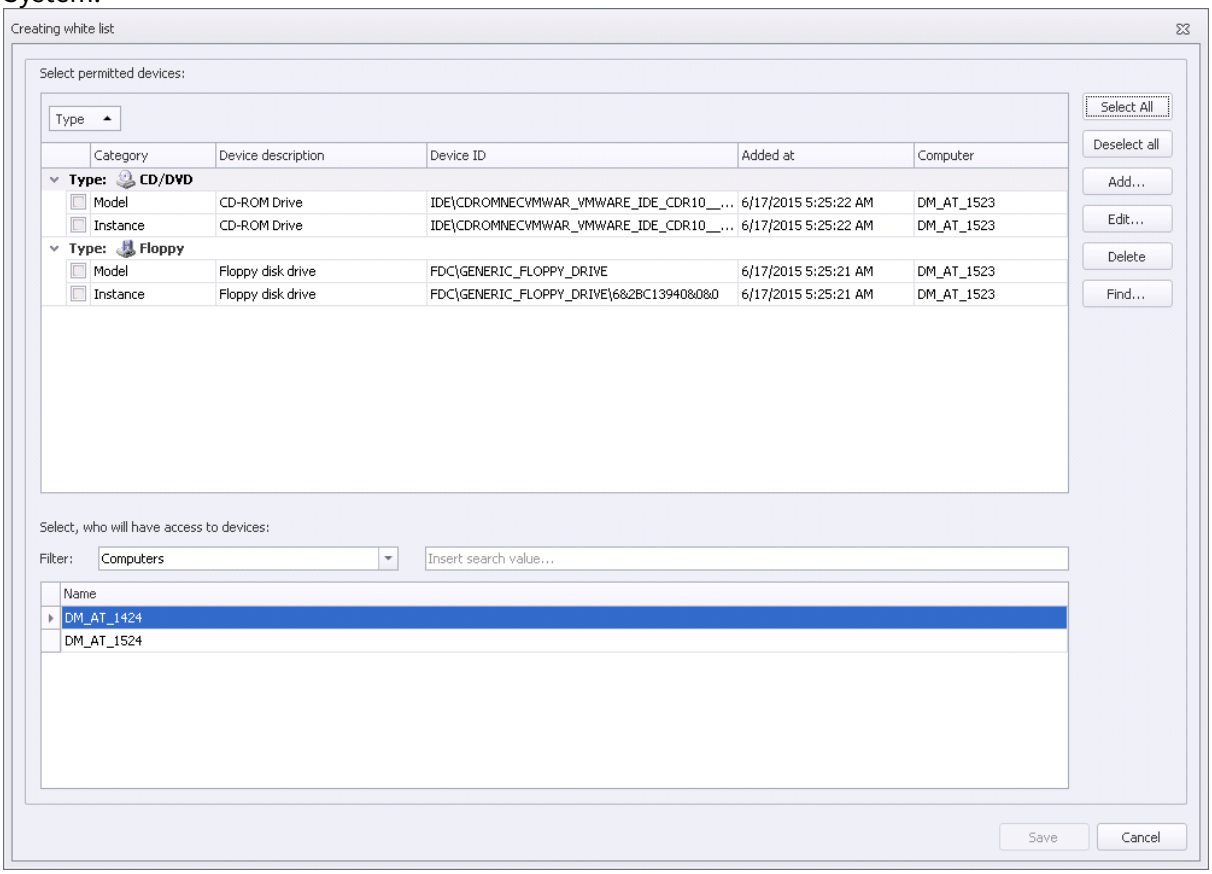
**Warning!**

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**.

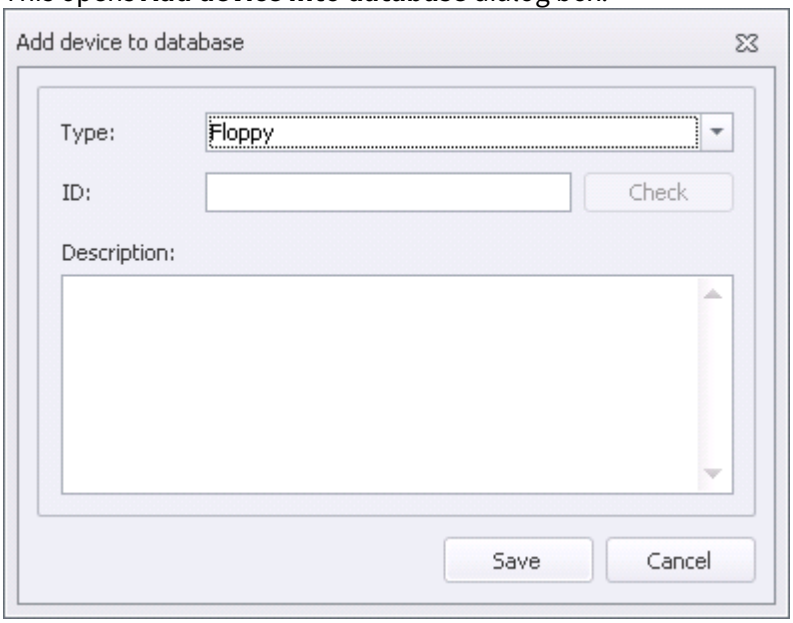
Adding Device Entry

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**.

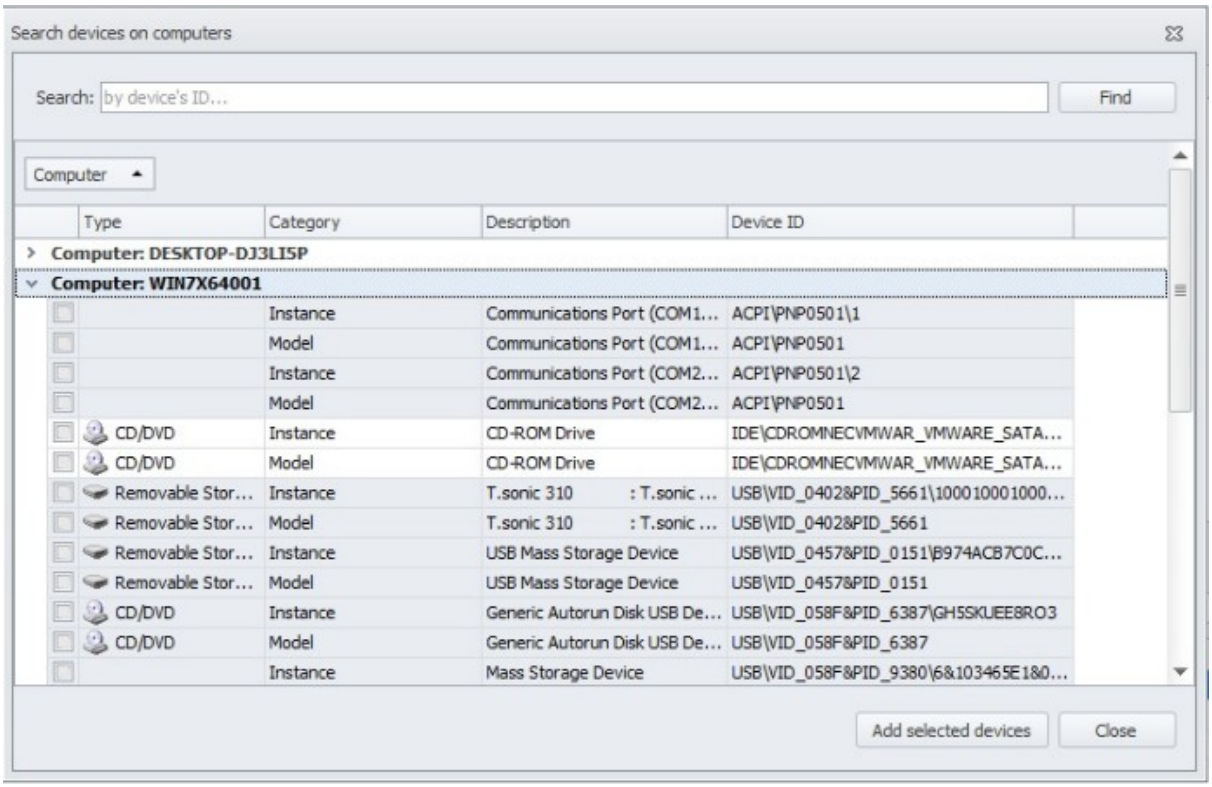
> **Warning!**
>
> When using instance code, take into account that some devices do not have unique ID: ID can be changed dynamically and differed even when connecting to different ports of the same computer.
> In such case using device model code is recommended.

- 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.

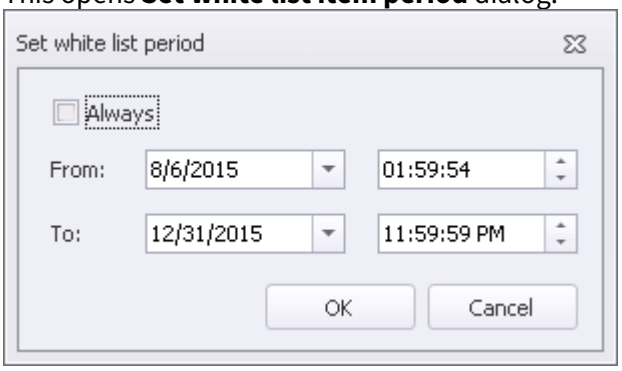
**To set white list entry period**:

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 catalogue 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:

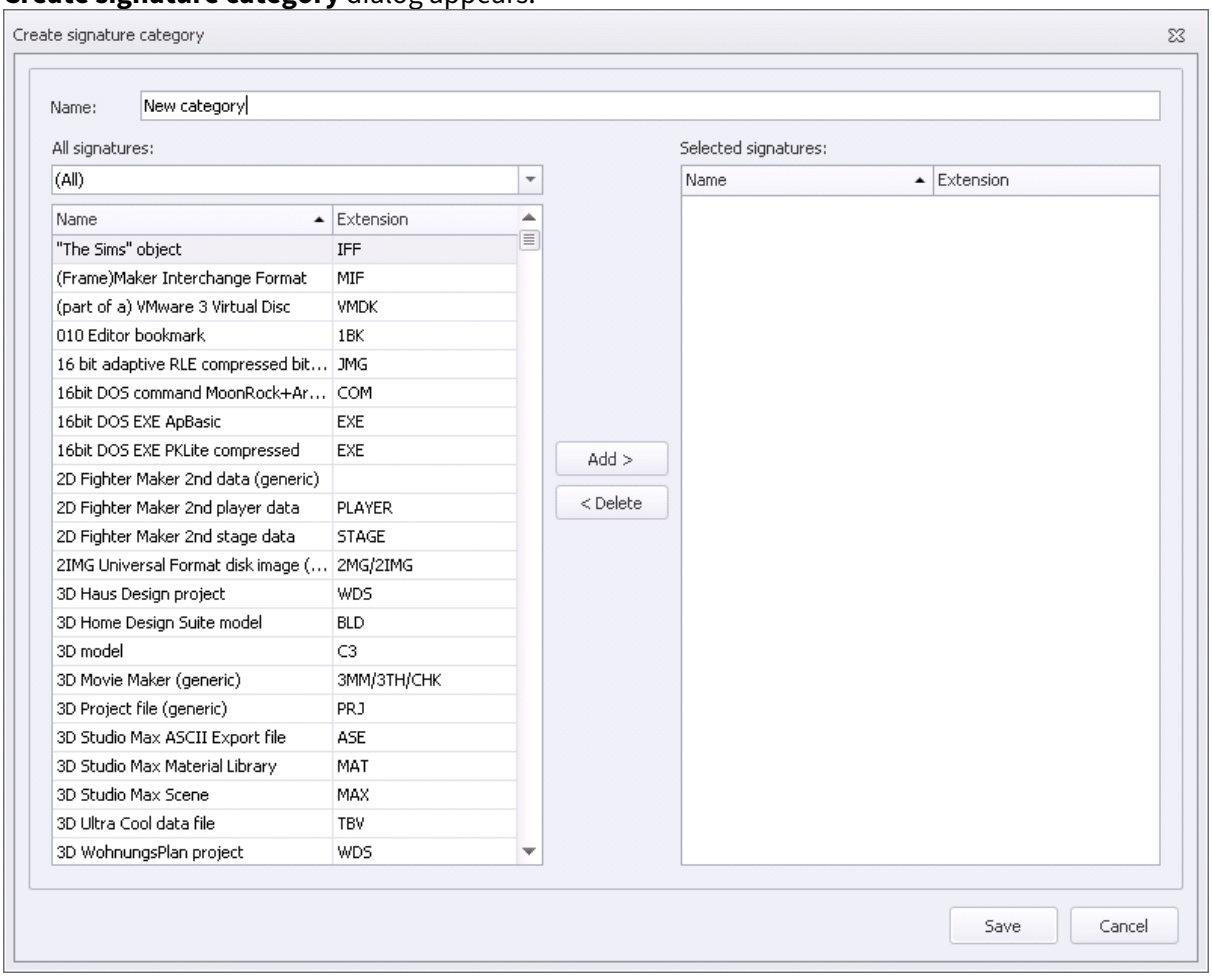
- create signature categories;
- fill created categories by copying predefined signatures;
- delete your signature categories, if they are not used by any rule.

### 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**
   **signature**s 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 a and the computer is rebooted, the System automatically starts to receive data on applications launched on managed workstations.

Data on all launches and installations produces an *application protocol*.

**Warning!**

Application protocol aim is that one can not forbid the application, which absence is obstructive for computer proper 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 "Application Monitor Rule (DM)".
  - forbid screenshots creating. See details in "ScreenShot Control Monitor Rule (DM)";
  - automatic creating the screenshots by the System. See details in "ScreenShot Monitor Rule (DM)".
- The **Applications Protocol** group is intended for creating filters showing data on all applications launched on managed workstations. 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

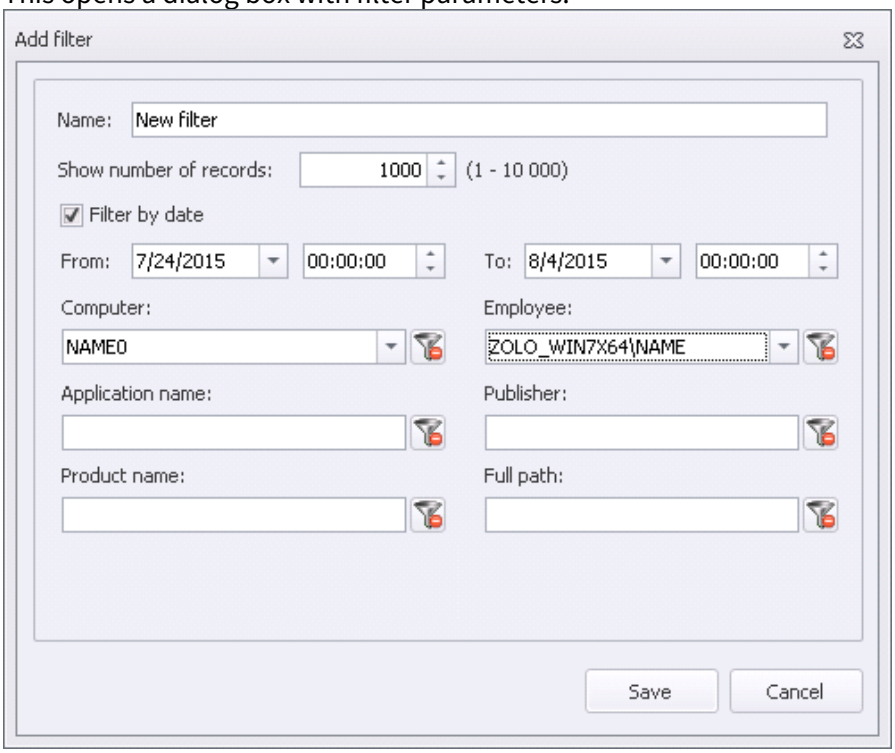
Filters allow you to configure the application protocol (see "Application protocol") to display information on applications that meet specified conditions.

> **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.

   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.

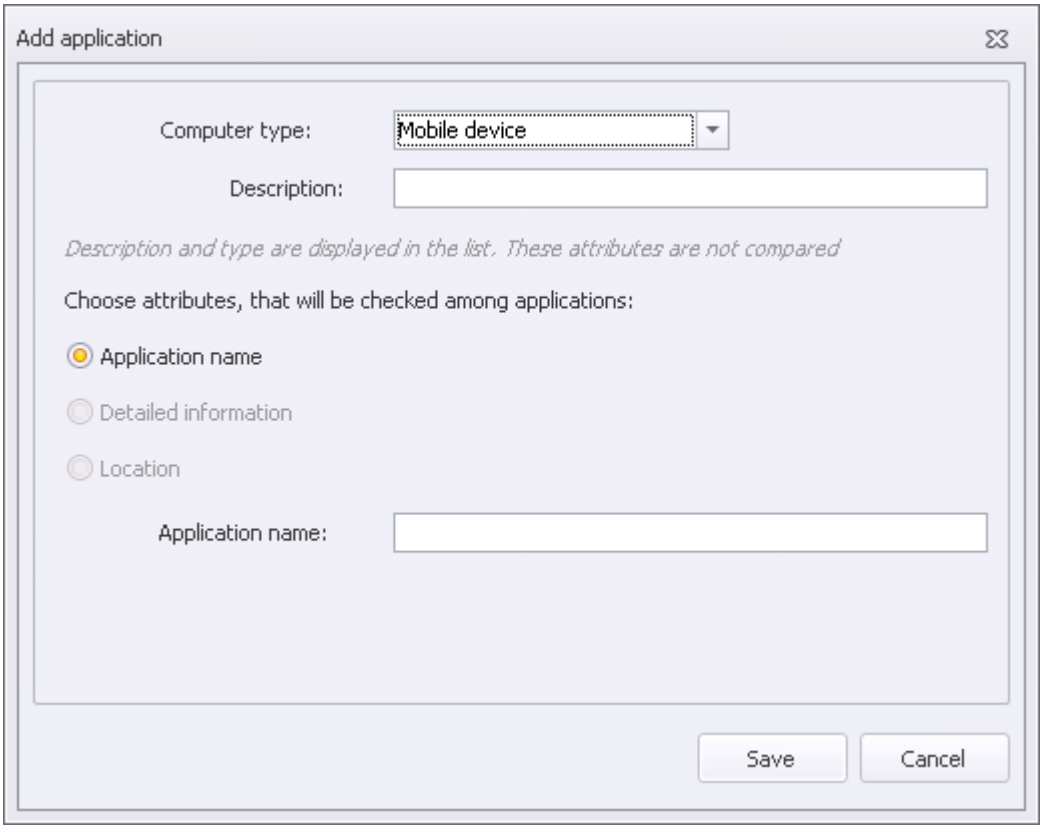
3. On the **Application protocol** pane select one or several entries. To select several entries click at them
   while pressing **Shift** or **Ctrl** button.
4. Take one of the following steps:
   - on the **Application protocol** pane click  A**dd application to list automatically**;
   - select **Edit > 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

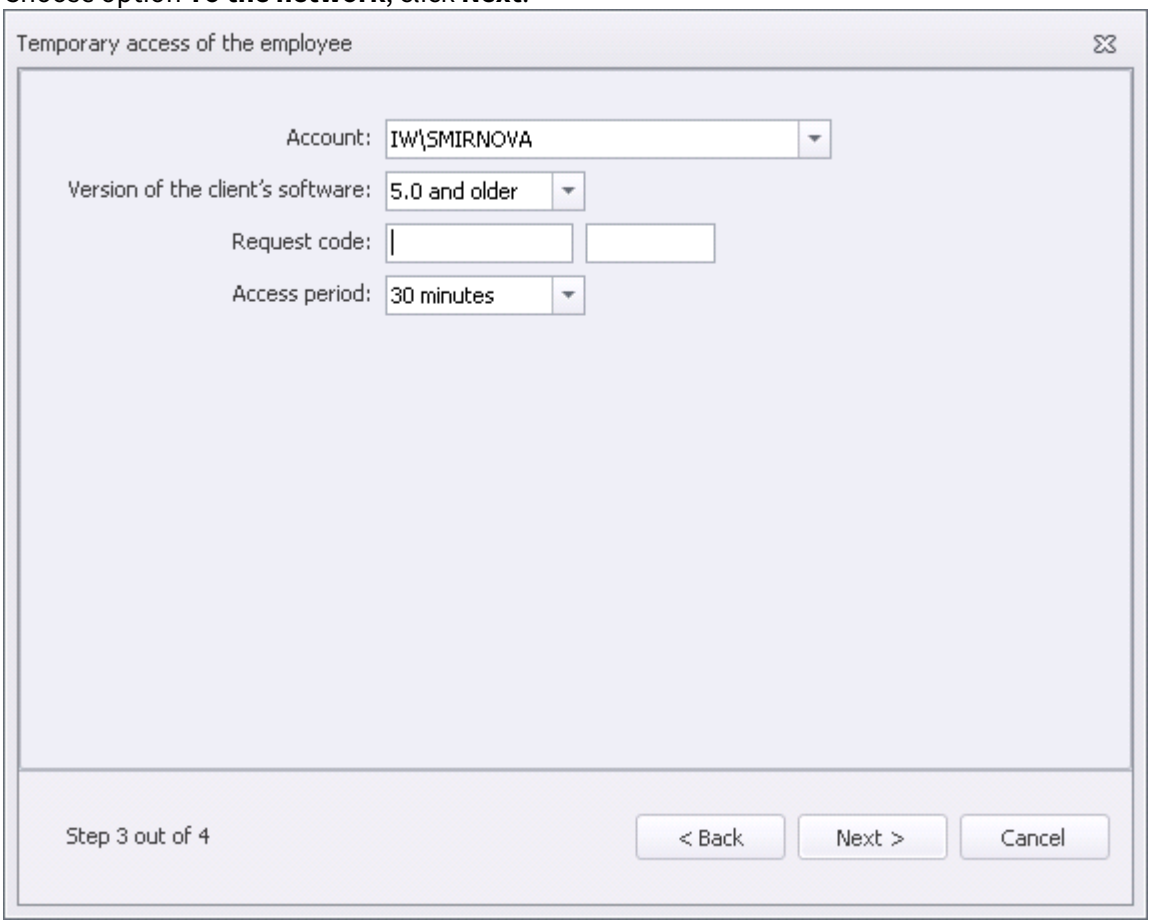
An employee for which a rule (DM) denying connections outside corporate network is active (see "Settings of Corporate Network" and "Network Monitor Rule (DM)"), can request temporary access to external connections from InfoWatch Device Monitor Agent menu, **Network control** command.

> **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!**

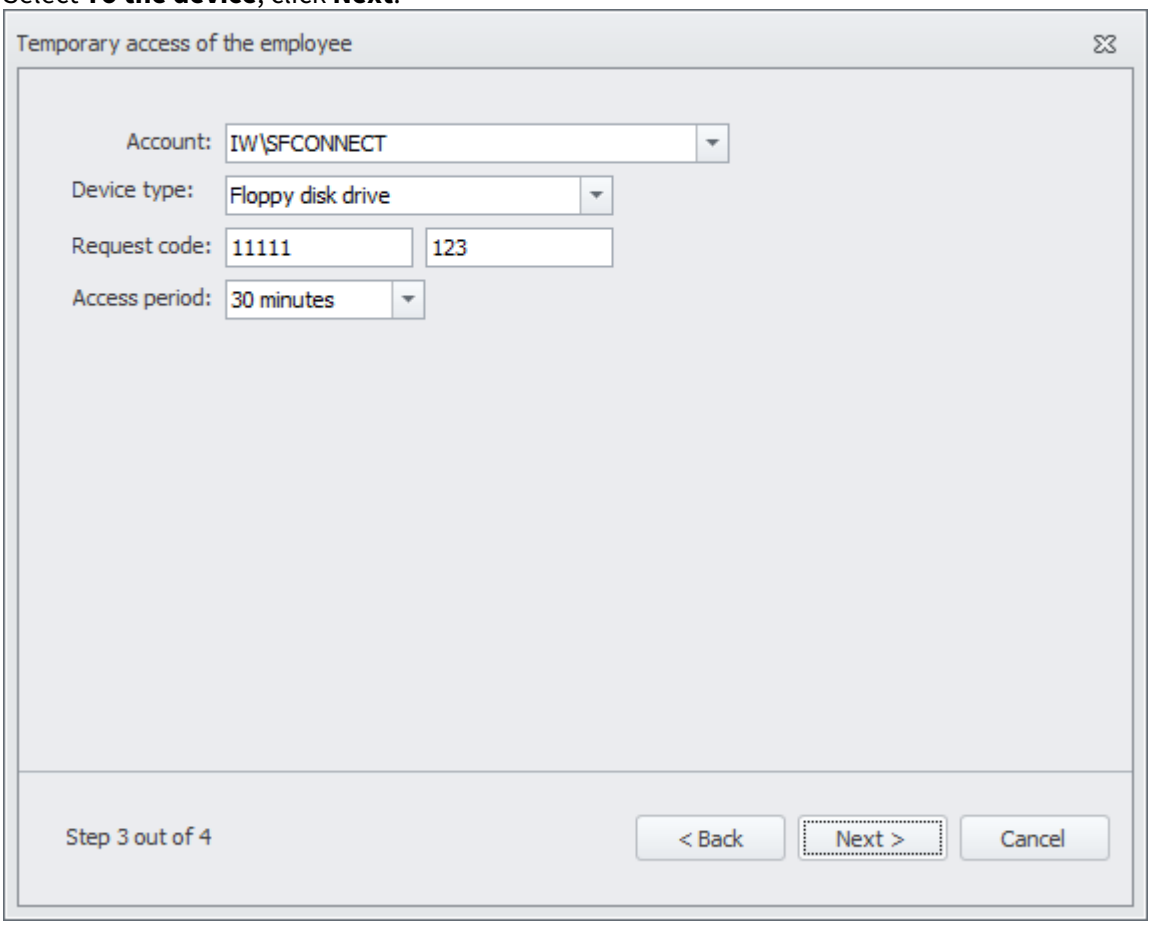
An employee can request access only if the **Show tray icon** option is selected (see "Common Settings for Agents"). On to configure the text displayed to the employee, see "Employee Notifications about DM Policy Violations", "**Access to device denied**" notification type.

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**:

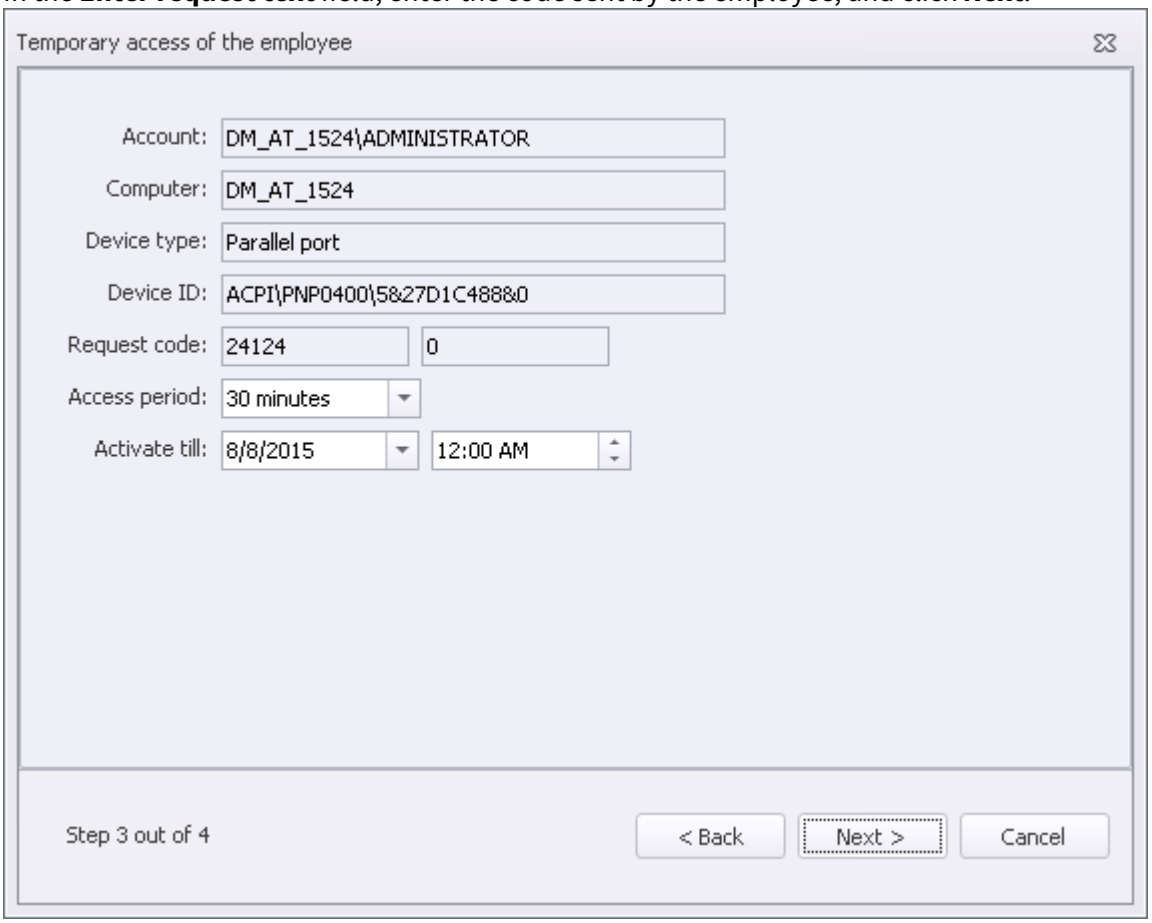
1. In Main Menu select **Tools > Temporary employee access**.
2. Select **Dictated by phone**, click **Next**.
3. Select **To the device**, click **Next**.




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

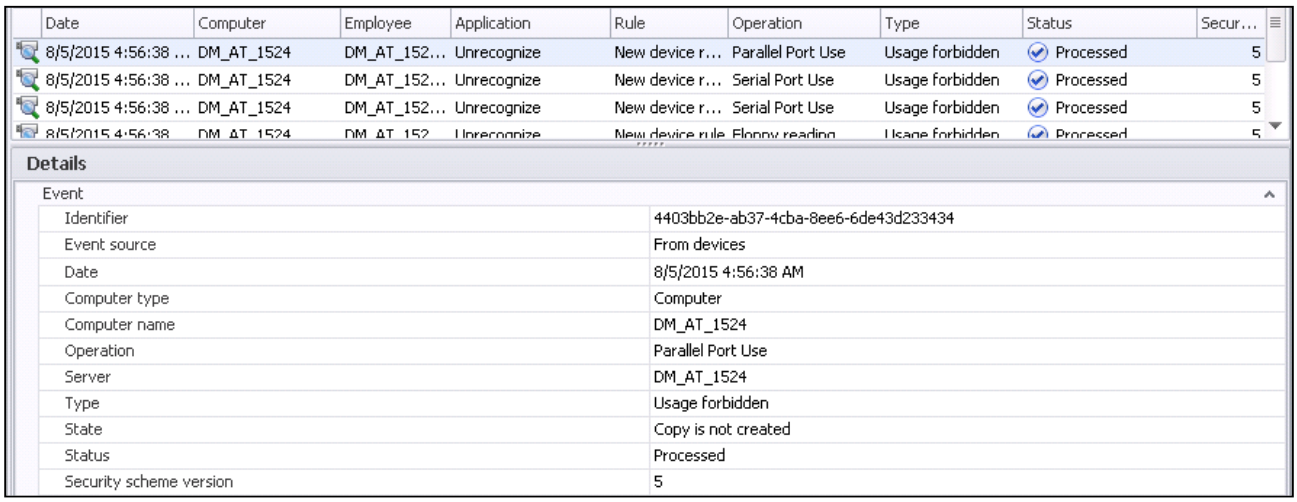
Data obtained by InfoWatch Device Monitor Agents on controlled computers are stored as **events** and transferred to InfoWatch Device Monitor servers along with shadow copies. Events (unlike shadow copies) are registered in InfoWatch Device Monitor database and are available from Management Console (DM).
You can define the logging level (save information on all attempts of access, on policy violations only or not save anything) in general settings of the security scheme: for details, see "Common Settings for Agents".

You can view events in **Events** section. To go to this section, click **Events** button on the Navigation pane.

**To view events**, choose the required filter in the list. You can choose a preset filter or create a new one as described in "Event Filters". Preset filters:

- **Last: 4 hours**
- **Today**

Event data is displayed as a table. Extended information on each record is available in the **Details** pane.




| Attribute name | Description | Available values |
|---|---|---|
| **Common attributes** | | |
| Identifier | Unique event number | |
| Event source | Interceptor-based event type | • **File** – File Monitor;<br>• **Devices** – Device Monitor;<br>• **Printer** – Print Monitor;<br>• **Skype, XMPP, MMP, Telegram** – IM Agent Monitor;<br>• **FTP/FTPS** – FTP Monitor;<br>• **HTTP/HTTPS** – HTTP(S) Monitor;<br>• **Cloud Storage** - Cloud Storage Monitor;<br>• **Mail** - Mail Monitor;<br>• **Network** – Network Monitor;<br>• **System** - event is created when the disk space for saving shadow copies is running out. *Such an 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 name | Name of the computer that registered the event | |
| Operation | Description of an action or an action attempt performed by the employee | |
| 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 an external device; sending files via messenger; sending print jobs to printer; sending data via FTP/FTPS.<br>• **Use** – connecting an external device that allows unmonitored read/write operations or sending messages;<br>• **Violation** – IM Agent interceptor user-initiated violation;<br>• **Warning** – user-initiated a ban or didn't give consent to use IM Agent plug-in, while monitoring is required by security policy (DM).<br>• **Usage forbidden** – attempt of sending data via forbidden channel. |
| Status | Status of event processing on the server and sending to Traffic Monitor server | • **New**<br>• **Awaiting for proceeding**<br>• **Awaiting for sending to TM**<br>• **Sent to TM**<br>**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**<br>• **Forbidden** – only for events from devices<br>• **Unprotected data copying is disabled** – only for events from devices<br>• **Allowed (in white list)** - for whitelisted events from devices |
| 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 | |
| **For events with *File, Devices, Printer, FTP/FTPS, HTTP/HTTPS, Cloud Storage, Network, System*** sources | | |
| 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<br>• **copy created** - shadow copy created successfully<br>• **no free space on disk** - if there is no free space on the agent<br>• **copying error** - if an error occurred while creating a copy |
| 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, Telegram*** | | |
| IM user ID | UIN of the user authorized in the messenger on the computer | |
| Object status | Shadow copy of transferred data | • **no copies created** - rule (DM) does not require shadow copying<br>• **copy created** - shadow copy created successfully<br>• **no free space on disk** - if there is no free space on the agent<br>• **copying error** - if an error occurred while creating a copy |
| 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 a transferred file | |
| File size | Transferred file size | |
| Shadow copy | File, message or chat shadow copy | • **No** - no shadow copy was created<br>• **Yes** - shadow copy created successfully |
| **For events with *Printer* source** | | |
| Document | Full name of the file sent to print | |

| | | |
|---|---|---|
| Printer | Name of a 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.<br>2. Shadow copy of print job was not created. The job contained no graphic or text data.<br>3. An error occurred while creating a shadow copy of print job.<br>4. Shadow copy of print job was successfully created. The job contained only graphic data.<br>5. The shadow copy should not have been created.<br>6. Shadow copy of print job was partially created. Graphic data were fully processed. Text data were partially processed.<br>7. Shadow copy of print job was partially created. Graphic data were partially processed. Text data were fully processed.<br>8. Shadow copy of print job was successfully created. The job contained only text data.<br>9. Shadow copy of print job was partially created. Graphic data were partially processed. The job contained no text data.<br>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<br>• **copy created** - shadow copy created successfully<br>• **no free space on disk** - if there is no free space on the agent<br>• **copying error** - if an error occurred while creating a copy |
| **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<br>• **copy created** - shadow copy created successfully<br>• **no free space on disk** - if there is no free space on the agent<br>• **copying error** - if an error occurred while creating a copy |
| 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 a 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<br>• **Yes** – shadow copy created successfully |
| **For events with *HTTP/HTTPS* source** | | |
| State | Result of creating shadow copy | • **no copies created** - rule (DM) does not require shadow copying<br>• **copy created** - shadow copy created successfully<br>• **no free space on disk** - if there is no free space on the agent<br>• **copying error** - if an error occurred while creating a copy |

| | | |
|---|---|---|
| Reciever DNS | DNS name of a computer | |
| Receiver 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 *Cloud storage* source** | | |
| Name of cloud storage | Name of the cloud storage where data is uploaded | • Google Drive<br>• DropBox<br>• YandexDisk<br>• SkyDrive<br>• EverNote<br>• SugarSync |
| File name | | |
| File size | | |
| **For events with *Terminal session* source** | | |
| Path | Short name of file being copied | |
| Device name | Device name, if detected | |
| Device ID | Device ID, if detected | |
| **For events with *Mail* source** | | |
| State | Result of creating shadow copy | • **no copies created** - rule (DM) does not require shadow copying<br>• **copy created** - shadow copy created successfully<br>• **no free space on disk** - if there is no free space on the agent<br>• **copying error** - if an error occurred while creating a copy |
| List of senders | 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). |
| 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. | |

If needed, you can free some space in the database by deleting 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.

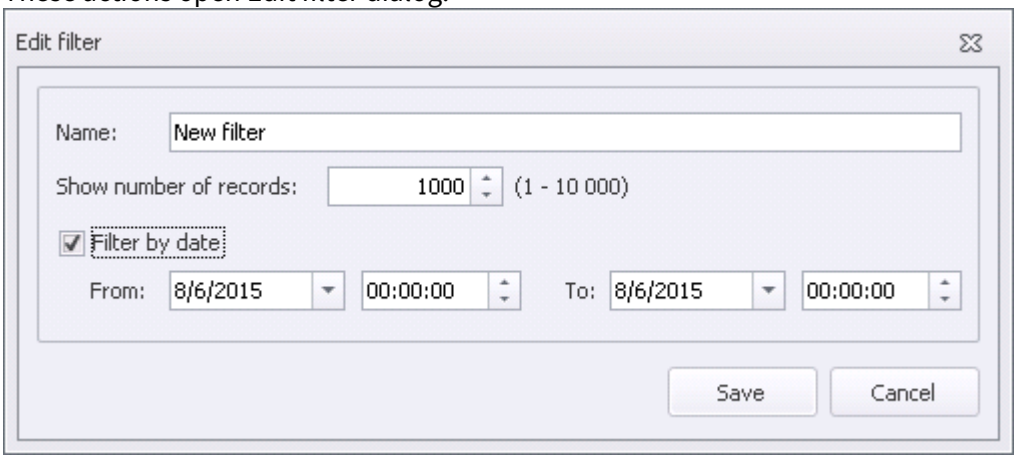
**To add or edit a filter**:

1. Go to **Events**.
2. Follow the necessary steps:

| Action | Steps |
|---|---|
| Creating filter | • in Main Menu select **Edit > Add Filter**;<br>• 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:<br>• in Main Menu click **Edit > Edit Filter**;<br>• click **Edit Filter** at the top of Navigation pane;<br>• 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.

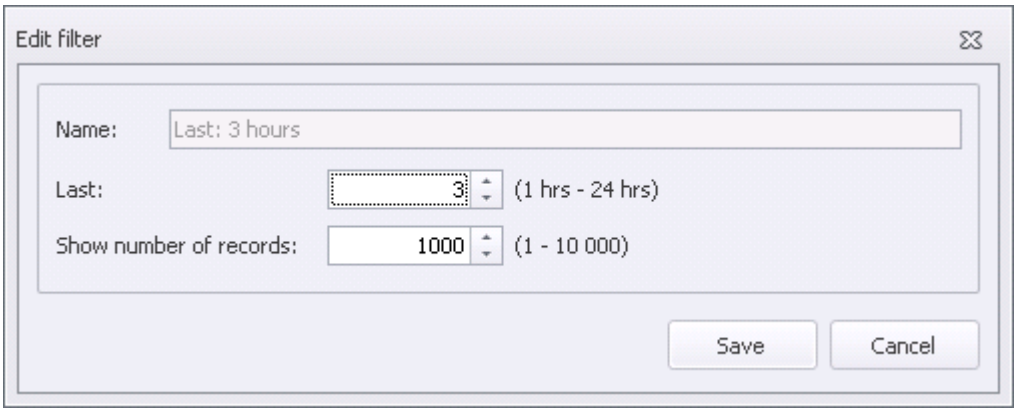
4. Click **Save**.

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;
- Agent 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:<br>• Primary distribution<br>• Change password<br>• Update<br>• Uninstall |
| Status | Current task status. Possible values:<br>• Executing<br>• Stopped<br>• 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.<br>**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:<br>• **Not running**<br>• **Prepare to start**<br>• **In progress**<br>• **Waiting for reboot** (only for installation and upgrade tasks)<br>• **Error** (for further details, see "Agent Installation Errors")<br>• **No access**<br>• **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 requirement is met:

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 DM Management Console) of InfoWatch Device Monitor Agent is performed using **installation agents**. The installation agent is an executable file. During the task execution, it is sent to workstations and starts automatically. The current agent version is received from the server.

> **Warning!**
>
> If the account under which the server is running doesn't have administrator rights on all target computers, then the primary Device Monitor Agent distribution will require credentials of an account with administrator rights for:
>
> - all target computers
> - a computer where Management Console (DM) is running
> - a computer where Device Monitor server is running
>
> If the password of Windows account is expiring (Windows displays a warning that the password expires in 3 days and needs 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 "*InfoWatch Traffic Monitor. Installation guide*", article "Creating Installation Package") and install it by other means (see "*InfoWatch Traffic Monitor. Installation guide*", article "Standard InfoWatch Device Monitor Agent Setup" and "Agent Setup via Software Distribution Tools").

> **Warning!**
>
> If Kaspersky Internet Security is installed on the workstation, then you need to disable its self-protection to install the InfoWatch Device Monitor Agent. For details, see the Internet article "How to enable/disable self-defense in Kaspersky Internet Security".

**To create a primary distribution task for InfoWatch Device Monitor Agent**:

1. Go to **Tasks**.
2. Take one of the following steps:
   - in the Main Menu, select **Edit** -> **Create Task**;
   - click **Create Task** at the top of the Navigation pane.

   The **Deployment task wizard** will open.
3. Enter the task name, select **Initial deployment task** and enter the task description, then click **Next**.
4. Create a list of computers to which you want to install Device Monitor Agent. To add a computer (or several computers):
   a. Click **Add**. You can select computers from:
      - a directory;
      - Microsoft Windows Network;
      - ALD tree;
      - computers that have already been registered (for example, after manual Agent installation) and belong to existing computer groups (**DM computer groups** node).

   b. Click **Connect to all the categories**, if you need to select computers from directories that are not connected yet.

c. Select computers or computer groups. Collapsed groups are marked with , expanded ones are marked with . 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
   - by clicking **Import** and downloading a text file with listed IP addresses or DNS names of computers. Each entry should begin with a new line; blank lines are not allowed

d. After you specify all computers you want to add, click **Select**. The dialog box will close and the **Task target computers list** area will display selected computers. To remove a computer from the list, select it and click **Remove**. When the list of computers is ready, click **Next**.

5. The **Deployment task wizard** displays servers registered in the System. You can change the Agent installation directory (by default, it is `%Program Files%\Infowatch\DeviceMonitor\Client`).

> **Warning!**
>
> Path to the catalogue may contain the following characters: 0-9, a-z, A-Z, ":", ".", "_", "-", "\", " ". If the path includes other characters, the agent will not be installed properly.

   Click **Next**.
6. A unique name of Device Monitor proxy server certificate (Issuer Distinguished name, Proxy Root Issuer DN) will be displayed. You can change it in accordance with X.509 standard, CN (Common Name) field is required, fields inside the name should be separated by commas. Click **Next**.
7. Configure Agent settings:
   - To prevent deleting Agents by employees, enter a password that is required to uninstall the Agent and confirm the password
   - **Hide agent's presence on computer until the configuration from DM server is received** - the System will hide the Agent's presence on the computer until a connection with the DM server is established

> **Warning!**
>
> The fact that you do not notify users about interceptors running on their computers may contradict the applicable laws of your country.

> **Warning!**
>
> Hiding/notifying settings apply on the Agent until the first call to the server. Once the workstation addresses the server, the Agent starts using settings of the workstation group it belongs to.

> **Warning!**
>
> If an antivirus system is enabled on the computer, it can reveal the presence of Device Monitor: for example, in the list of running processes or in the list of programs that initiate 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 interception** - installs **iw_proxy** component on the computer
  The component will not be installed if you leave the checkbox empty
- **Install the component of network control** - installs **Network Monitor** interceptor on the computer. The component will not be installed if you leave the checkbox empty

> **Warning!**
>
> We do not recommend installing the component of network perimeter control to the image that will be used as the base image of VDI framework under control of Citrix Provisioning Services, as it will affect the technology and the performance of the whole scheme.

- Specify task restart parameters: they will be used if the task wasn't launched at the first attempt. Specify the number of attempts and their intervals, in minutes. If the first launch ended with an error, the task will not be launched again
- To launch the task immediately after saving, select the **Run task immediately** option
- 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 the accounts that are used to launch tasks. If a new task is not launched immediately, you will need to enter the password the next time to launch the task from the Management console (DM).
> If a password of the Windows user account is expiring (Windows displays a warning that the password expires in 3 days and needs to be changed), then primary distribution task cannot run on behalf of this user.

Click **Next**.

8. Specify options of the computer reboot.

> **Note:**
>
> If at the previous step, you have selected the **Hide agent's presence on computer until the configuration from DM server is received** option, then these options are unavailable.

Possible values:

- **Wait for reboot without notifying the employee**. The Agent can:
  - start notifications immediately (*Do not wait* option),
  - start notifications after the specified time (*Wait for* option - specify the time after which to start notifications),
  - not show notifications at all (*Wait infinitely* option).
- **Notify the employee about reboot necessity and wait for reboot**. When waiting in the "silent" mode (the **Wait for reboot without notifying the employee** option) ends or immediately after the installation, Device Monitor Agent starts notifying the employee that reboot is required:
  - during a specified time period (*Notify within* option);
  - permanently (*Notify infinitely* option);
  - not show notifications at all (*Do not notify* option).

  If needed, change the duration and frequency of notifications and enter the message text that is displayed in the notification. The message can contain not more than 255 characters.
- **Show a warning before forced reboot**. If the option is selected, then the Agent displays a notification about forced reboot. The computer will be restarted in 5 minutes during which the employee can finish operations. If the option is not selected, then the forced reboot (if required according to settings) will be performed without notifying the employee.

  > **Warning!**
  >
  > Forced reboot is performed if neither the **Wait while employee is rebooting computer** setting, nor the **Show a warning before force reboot** option is selected, or if the waiting time has expired but the employee has not restarted the computer.

Click **Next**.

9. Look through the task summary. If you need to change anything, click **Back** to return. If all settings are correct, click **Finish**.

### 5.6.4 Creating Update Task

> **Important!**
>
> If you update DM to version 6.7, you should use a primary distribution task to update the agents (see the article "Creating Primary Distribution Task"), otherwise errors may occur. When updating to all other versions, follow the steps described below.

You should update Device Monitor Agents after you update InfoWatch Device Monitor server end: 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 use the automatic creation of update tasks for selected computers as described in the document "*InfoWatch Traffic Monitor. Installation guide*", "Updating Agents at Managed Computers" article.

**To create an update task for InfoWatch Device Monitor Agents**, go to **Tasks** and take one of the following steps:

- in the Main Menu, select **Edit** -> **Add Task**;
- click **Add Task** at the top of the Navigation pane.

In the **Deployment task wizard** that opens, take the following steps.

1. 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**.
2. Create a list of computers where Device Monitor Agents should be updated. To add a computer (or several computers):
   a. Click **Add**. The **Select computers** dialog, **DM server computers** node, will display the list of computers where Device Monitor Agent version does not match Device Monitor Server version and they can be automatically updated (agent software version should be 4.0.651 or higher).
   b. Select computers or computer groups. Collapsed groups are marked with , expanded ones are marked with . Double-click a group to expand or collapse it.
   c. You can also use the **Filter by computer name** field to find a computer. To start the search, click **Find**.
   d. After you specify the computers you want to add, click **OK**. The **Select computers** dialog will be closed and the **Task target computers list** area will display selected computers. To remove a computer from the list, select it and click **Remove**.

   When the list of computers is ready, click **Next**.
3. Specify parameters of restarting computers:
   - **Wait for reboot without notifying.** The Agent can**:**
     - notify the employee immediately (*Do not wait* parameter),
     - notify the employee after the specified time period (*Wait for hour(s)* parameter - you need to specify the time before notification),
     - not notify the employee (*Wait infinitely* parameter).
   - **Notify the employee about reboot necessity and wait for reboot.** When waiting in the "silent" mode (the **Wait for reboot without notifying the employee** option) ends or when the update process is complete, Device Monitor Agent starts notifying the employee that reboot is required during a specified time period (*Notify within hour(s) within: minutes* parameter) or infinitely (*Notify infinitely every x minutes*), or it does not notify the employee (*Do not notify*). If needed, change the duration and frequency of notifications and enter the message text that is displayed in the notification. The message can contain not more than 255 characters.
   - **Show a warning before reboot** - if the option is selected, then a notification about a forced reboot will be displayed (the employee can complete current tasks within 5 minutes before the forced reboot). Otherwise, a forced reboot will be performed without notifications.

**Important!**

If the **Hide Agent presence** option is enabled on the workstation, notifications are not displayed.

4. Specify the task retry parameters: they will be used if the task wasn't launched at the first attempt. Specify the number of attempts and their intervals, in minutes. If the first launch ended with an error, the task will not be launched again.
   If necessary, select the **Run task immediately** option to launch the task immediately after saving.
5. 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**.

**Warning!**

If the Kaspersky Internet Security is installed on the computer, then you need to disable its self-protection function before updating InfoWatch Device Monitor Agents.
See details in the 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 **ЫSelect**. 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;<br>• click **Perform task** located at the top of Navigation pane. |
| Stop task | • in the Main Menu select **Edit >Stop task**;<br>• 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**<br>• right-click computer row and select **Add computer** or **Exclude computer from task**.<br>**Warning!** You can't remove a computer if the task is running and not completed. |
| Edit task | • in the Main Menu select **Edit > Edit**;<br>• click **Edit** at the top of Navigation pane.<br>• right-click on task name and select **Edit**.<br>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**;<br>• click **Delete** at the top of Navigation Pane.<br>• right-click on task name and select **Delete**.<br>**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**<br>• 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".

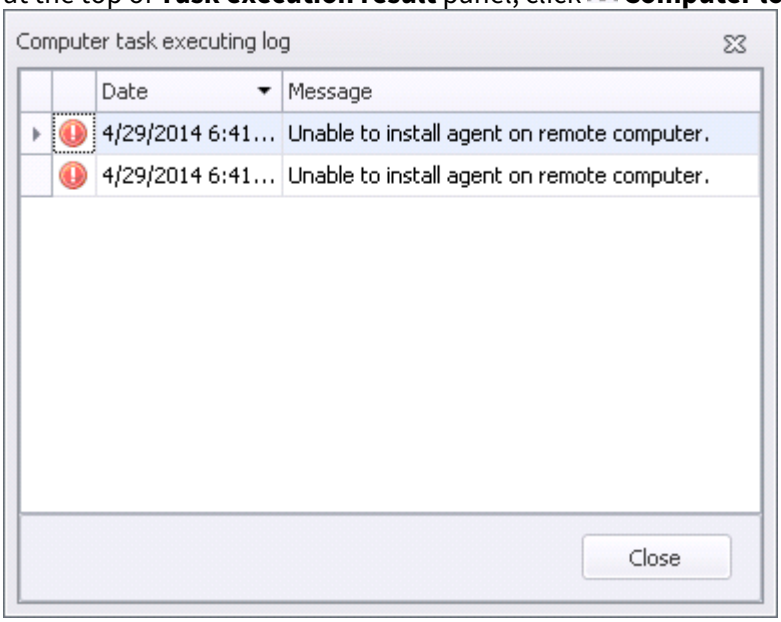
**To view task errors**:

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. The message can contain not more than 255 characters.
   - **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:

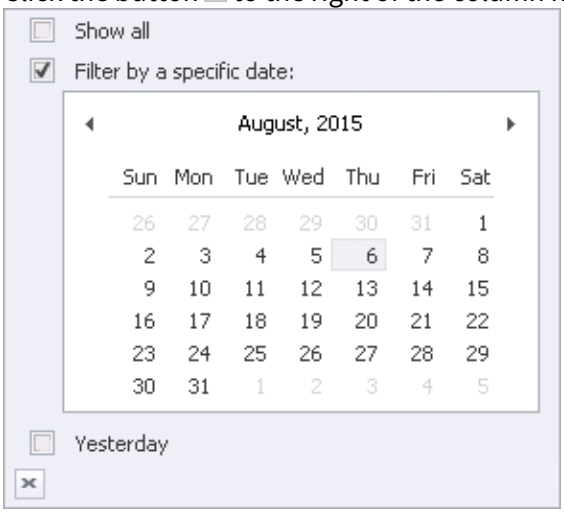
- Filter by Date;
- Applying Standard Filters;
- Custom Filter;
- Editing Filters;
- Removing a Filter.

#### 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").

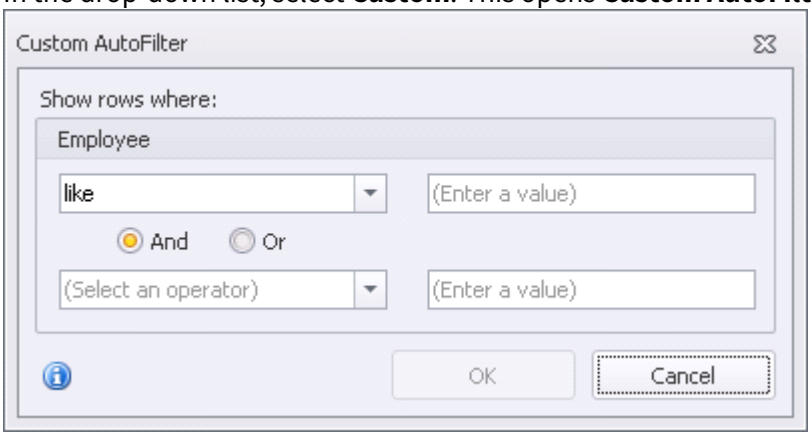
The table will only display filtered values.

**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.

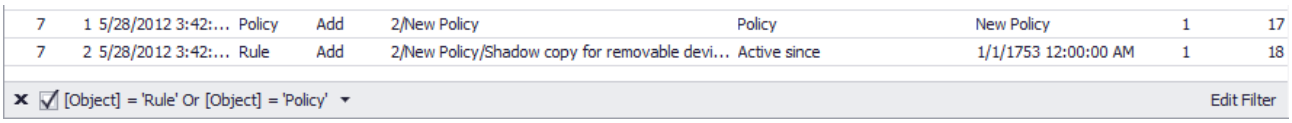
> **Note:**
>
> You can use comparison operators to limit filtering criteria: *equal, not equal, greater than, greater than*
> *or equal to, less than, less than or equal to; values empty (blank) and nonempty (non-blank field)*; or
> text filter with a mask. To get a text filter syntax tip, click .

- 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.

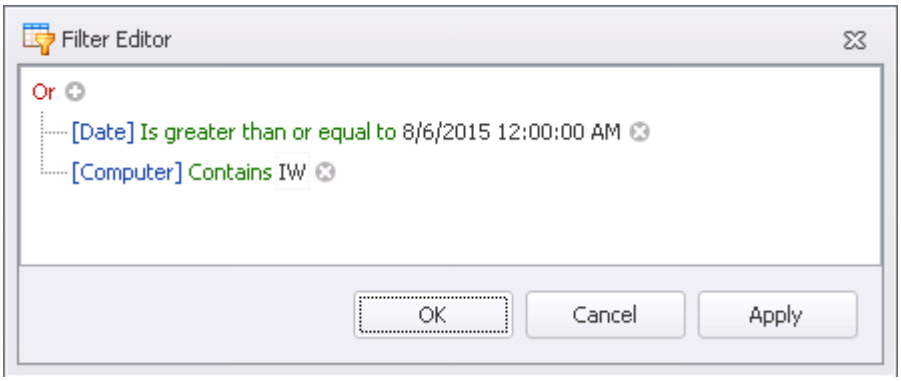



To remove filter and view all items, clear the check box in filter string. To apply the filter again, select the check box. To re-use a filter, click the filter string and select filter from drop-down filter history list. Custom filters are stored until you close the window with filtered content.

## 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<br>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<br>or<br>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<br>2. Select **Add Group** in the menu |
| Delete criteria group | 1. Click the name of operator criteria group<br>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 "User License Agreement" section.

## 6.1 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.**

**1. License granting**

1.1. You are granted a non-exclusive license to use the Software (the Software Rights Holder is InfoWatch, JSC) within the framework of the features described in the Software Documentation (User Manual, Administrator Manual, Installation Manual), provided that you comply with all the technical requirements described in the Software Documentation, as well as all the restrictions and terms of use of the Software specified in this Agreement and the Contract between you and your licensor.

1.2. If you have received, downloaded and/or installed the Software designed for educational purposes, you may only use the Software for educational purposes and during the trial period. Any use of the Software for other purposes or after the trial period shall be prohibited.

1.3. If you use different versions of the Software or Software versions for different languages, if you have received the Software on several media, if you have otherwise received several copies of the Software or have received the Software as a part of other software package, the total number of licenses you use shall not exceed their number specified by the Contract between you and your licensor.

1.4. You have the right to make a copy of the Software, provided that such a copy is only designed for archival purposes and for replacement of the copy legally purchased, if the original copy is lost, destroyed or is no longer usable. This copy may not be used for other purposes and must be destroyed if the possession of the Software copy ceases to be legitimate.

1.5. You shall be solely responsible and ensure compliance with the applicable export and import laws, as well as applicable trade sanctions and embargo with regard to the transfer of rights and use of the Software.

**2. Restrictions**

2.1. You may not decompile, disassemble, modify or perform derivative works based on the Software, in whole or in part, except as otherwise required by the applicable laws of the Russian Federation.

2.2. You are not allowed to transfer the right to use the Software to third parties.

2.3. It is prohibited to transfer or provide access to the license key to third parties, contrary to the provisions of this Agreement and the Contract between you and your licensor. The license key constitutes confidential information. The Rights Holder shall reserve the right to use authentication tools for the license key installed by you.

2.4. It is prohibited to lease, rent or assign for temporary use the Software, as well as to disclose the results of the Software bench tests.

2.5. The Rights Holder shall have the right to lock the license key if you breach the provisions of this Agreement or the Contract between you and your licensor.

2.6. Anyone who violates intellectual property rights to the Software shall bear civil, administrative or criminal liability for this under the law.

2.7. You may not use the Software for any purposes or in a manner restricted or prohibited by the applicable laws. You shall be solely responsible for unlawful use of the Software.

2.8. Should you breach any of the provisions of this Agreement or the Contract between you and your licensor, the Rights Holder or your licensor shall be entitled to terminate the Software license at any time without notice to you and without reimbursement of the cost of the Software or a part thereof.

**3. Limited guarantee and disclaimer**

3.1. The Rights Holder guarantees that the Software shall operate in line with the description set forth in the Software Documentation.

3.2. You agree that no Software shall be error free, and it is recommended that you regularly back up your files.

3.3. The Rights Holder does not guarantee the operability of the Software upon breach of the terms and conditions specified in the Software Documentation, as well as in case the user breaches the terms of this Agreement and the Contract between you and your licensor.

3.4. Except for the limited guarantee set forth in this paragraph, the Software shall be delivered on an "as is" basis. The Rights Holder shall provide no guarantees and bear no responsibility to you in case of any changes in third party software, occurring after installation/implementation of the Software and resulting in loss of the Software functionality (including but not limited to any change in data transfer protocol, data storage format, logic of third party software, software update that no longer supports work with the Software). The Rights Holder provides no guarantees, conditions, information or provisions (explicitly or implicitly) for everything, including without limitation any violation of rights of third parties, commercial quality, integration or suitability for specific purposes. The user shall agree that he or she is responsible for the Software selection to produce results, for installation and use of the Software, as well as for the results obtained with its use.

**4. Liability limitation**

To the fullest extent permitted by the laws of the Russian Federation, the Rights Holder shall not be liable for any loss, damage, regardless of its causes (including but not limited to particular, incidental or indirect damage, lost profits, losses associated with downtime or lost business, business information loss, negligence or any other losses), resulting from the use or inability to use the Software. The basis of the liability of the Rights Holder shall be guilt, and the loss shall be limited only to the actual damage proven in a court of law.

**5. Intellectual property rights**

5.1. You agree that exclusive rights to any objects of intellectual property embodied in the Software and/or any documentation provided to you belong to the Rights Holder. Nothing in this Agreement shall grant you any rights to the said objects of the intellectual property, other than those provided by the Contract between you and your licensor.

5.2. You agree that the source code, the license key for the Software shall be the property of the Rights Holder.

5.3. You may not remove or alter copyright notices or other proprietary notices on any Software copy.

**6. Rights to information, access to which has been obtained by you in the implementation of this Agreement.**

6.1. You agree that you have no rights to information which is not the object of the intellectual property pursuant to Section 6, access to which has been obtained by you in the implementation of this Agreement.

6.2. This information includes, but is not limited to, systems, working methods, other information.

6.3. You shall use the said information only to exercise the rights granted to you under a Software rights agreement, without the right to use this information for your own benefit and outside the scope of the Contract between you and your licensor.

**7. Third parties software**

You have been informed that all used of third parties are listed in licenses.inf file distributed within Software .

**8. Contact details of the Rights Holder of InfoWatch, JSC**

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

Commercial Department: sales@infowatch.com

Support Service: support@infowatch.com

Website: http://www.infowatch.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 actions fulfilled by Management Console users: creating and managing the security schema, System administrating. See also: Audit log, Management Console accounts |
| Blanks | Technology of searching the filled blanks of forms: questionnaires, receipts, etc. Blanks are stored in the System as digital prints, their text is not available for viewing to either users or System administrators. See also: Technologies, Technology element |
| Case sentive | Term setting: if the term is case-sensitive, the text search will detect only word forms which completely match upper- and lower-case letters defined in a term. See also: Term |
| Catalogs of persons, computers, and groups | Information about users, workstations, groups of users, and groups of computers imported from Active Directory, 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 terminal device. See also: Workstation, Terminal device |
| Configuration | A group of settings required to check events for data monitoring and analyzing. See also: Event, Technologies, Lists, Policy |
| Configuration version | A fixed state of the configuration designed to monitor changed settings of the event analysis. The configuration version is committed after uploading to a host. The configuration version can be active (currently used), editable (the last version with up-to-date modification) and saved (having changes and editable for users). See also: Configuration |

| | |
|---|---|
| Consul agent | Consul cluster member. It can be server or client. |
| Controlled persons | Set of persons, groups of persons and person's statuses which detection in the event results in associating this event to the person control policy which defines this set. See also: Persons, Person group, Person status, Person control policy |
| Copy mode | One of IW TM transport modes. In this mode, the actual traffic does not pass through the System. The copy of traffic is analyzed. In this mode, the traffic cannot be filtered by the System. See also: Transport mode |
| Copy rule | The rule that regulates copying and printing protected data. See also: Rule, Protected data, Data protection policy |
| Corporate security policy | A set of technical, organizational, administrative, legal, and physical measures, methods, rules, and guidelines that cover all security aspects in a company |
| Dashboard | Management console section that displays on widgets the statistical information on the violations and violators. See also: Management Console, Widget, Violation |
| Data interception | A process of acquiring, parsing, categorizing, and converting data (or a copy) into context. It is possible to intercept data transferred using the following protocols: SMTP, HTTP, ICQ/OSCAR, Skype, IXP, XMPP, MMP, FTP. See also: Interceptor, Event context |
| Data interception channel | A data interception environment that includes technical appliances, software tools, and communication protocols. The System supports the following data interception channels: email (SMTP, IMAP, and POP3), Web (HTTP), instant messaging services (ICQ and Skype), shadow copies of files, connected/disconnected workstation events, and print jobs. |
| Database | A collection of data stored in accordance with a data scheme. Contains all information needed for the System. |
| Database unloadings | Technology of searching the quotes the database. Database unloadings may be lists of salaries, other personal data, etc. See also: Technologies |
| Decision | The security officer’s conclusion on whether the event violates the corporate security policy or not. Possible values: “No decision“, “Violation:“ and “No violation“. See also: Security officer, Corporate security policy, Event, Event attributes, Violation, Policy, Verdict |
| Delivery status | Event attribute that specifies the possibility of event delivery to recipients after the analysis. If the event delivery has been allowed, then the attribute value represents the delivery tracking (completed or failed). See also: Event attributes |
| Digital print | A method of storing a sample document in the database in the form of a set of quotes. See also: Sample document, Quote |
| Document shadow copy | A copy of printed document received from the print job initiated on the managed computer. See also: InfoWatch Device Monitor |
| Domino Directory | IBM Lotus Domino Directory is a directory of information about users, servers, and groups. The Domino Directory is also a tool that administrators use to manage the Domino system. |

| | |
|---|---|
| Event | Objects of traffic interception (SMTP and IMAP and POP3 mail, HTTP requests, ICQ and Skype messages), shadow copies of files and print jobs. Generated by the System as a result of the data exchange between employees and others, including publication in media, copy to external devices and printing. |
| Event analysis | The procedure of processing of the attributes, attached files, and text of the intercepted events and of assigning additional attributes to the event. See also: Event, Policy, Event attributes |
| Event attributes | Structured data extracted from the events and assigned according to the processing results. See also: Event, Policy, Verdict, Decision, Transport mode |
| 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 you to control the incoming and outgoing HTTP traffic. It also makes it possible to modify the content of the HTTP requests. |

| | |
|---|---|
| ICQ | An Internet instant messaging service. Uses OSCAR protocol. |
| ICQ message | A message sent through the ICQ-OSCAR protocol. See also: Event |
| IMAP | Internet Message Access Protocol is a protocol for e-mail retrieval and storage |
| InfoWatch Device Monitor | IW DM is software appliance designed to control the user access to peripherals and to monitor operations (data either copied to removable media and network storages or sent to print, network activity, applications usage) and intercepting messengers traffic (Skype, Gtalk and Jabber) and so on. |
| InfoWatchTraffic Monitor | IW TM software suite is designed to control various types of traffic (SMTP, IMAP, POP3, HTTP, HTTPS, IMAP, XMPP, ICQ, NRPC) and shadow copies of the data copied to the removable media and sent to printing. |
| Initiators | A person whose actions led to the event creation |
| Inline mode | IW TM system deployment mode which may block mail outgoing from the perimeter, followed by dispatching. IW TM Server is used as a relay server. |
| IW Lync Adapter | Interceptor of data communication events through MS Lync servers installed in the company infrastructure. |
| Jabber | Messaging and information exchange system based on the open XMPP protocol. |
| LAN | Local Area Network |
| License | Right to the System usage. Gained when buying the System and defines available users number, used technologies and interceptors and so on. See also: Technologies, Interceptors |
| Lists | Lists the similar data generated by Management Console to be used in policies creating. See also: Configuration, Policy |
| Lotus Adapter | Interceptor installed on the IBM Lotus server to redirect emails to IW TM for analysis. See also: Interceptor |
| Lotus Domino | IBM mail server which messages are intercepted by Lotus Adapter. |
| Management Console | A graphical user interface. Designed to manage InfoWatch Traffic Monitor (administration, configuring settings, event analysis, etc.). |
| Management Console (DM) | GUI element. It is designed to control InfoWatch Device Monitor (system administration, security schema configuration, etc.) |
| Management Console user | User who manages the System. Each user has a role assigned basing on corporate security policy. |
| MAPI | Messaging Application Programming Interface is a messaging architecture and a Component object model based API for Microsoft Windows |
| Mask | A search pattern of characters and wildcards used to match folder and file names. |
| Monitor | See: Interceptor |

| | |
|---|---|
| Morphology | Term setting: if morphology is used, the text search will detect all word forms of this term. See also: Term |
| MS Lync | Microsoft instant messaging clients for corporate environments. |
| MTProto | A cryptographic protocol used in the messaging system to encrypt user correspondence |
| Normal transport mode | A traffic analysis and filtering mode. In this mode, it’s possible to block the traffic forbidden by the System can be blocked. See also: Transport mode, Inline mode |
| Notification | E-mail sent in case if the policy triggers on the event. Is sent via Management Console to notify Management Console users, employees or third parties. Contains a summary on the intercepted events and attached message. See also: Policy, Event |
| Occurrence threshold | A number of text objects found in the event enough to detect the protected object where this occurrence threshold is defined. See also: Event, Text objects, Protection object |
| Perimeter | A container of company infrastructure elements and contact information. The perimeter is used to logically divide a company into structural elements and track the traffic of every element. See also: Group of persons and computers |
| Person | Account of employee or external contact that is contained in System catalog and allows to process the data belonging to this account as a whole and to user-friendly display data referring to it. See also: Group of persons and computers |
| Persons control policy | A policy to add rules controlling persons, person groups, and person statuses. See also: Policy, Person control rule, Person,  Person status |
| Persons control rule | Rule that assigns attributes to the event of specified violation level and which senders or recipients contain persons specified in the policy which includes this rule. Allows to re-assign person's status and to send notifications. See also: Rule, Event attributes, Person, Violation level, Person status, Notification, Person control policy |
| Placement rule | The rule that regulates storing protected data. See also: Rule, Protected data, Data protection policy, 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 accepted the data enclosed in the request message body for storage. Often used for file downloading of filled web-form representing |
| Privilege | Entity defining user’s ability to perform some action (set of actions) when managing the System |

| | |
|---|---|
| Protected data | A set of protected objects, their catalogues and file formats which detection in the event allows to characterize this event as fallen under the data protection policy where this set is defined. See also: Protected object, File format, Data protection policy |
| Protected object | The set of technology elements whose presence in the event allows the System to determine that this event belongs to a particular type of business documents (catalogue of protected objects). Protected objects are used in defining of data protection policies. See also: Technology element, Data protection policy |
| Proxy Server | The service that allows indirect requests to other network services. Proxy forwards all requests of the client programs to the network, and, having received the reply, sends it back to the client. |
| Quotation threshold | A percent of the sample document found in the even as quotes, enough to associate the event with this sample document. See also: Event, Sample document, Quote |
| Quote | A quote from the sample document found in the event text. See also: Sample document |
| Reference hash sum | Unlike the current hash sum, keeps the representative state of System files. See also: Integrity control |
| Relay server | A server which allows anyone on the Internet to send e-mail through it, not just mail destined to or originating from known users. |
| Report | Selection providing a visual display of event statistic data. See also: Management Console, Event |
| Rule | Entity defining System's actions in the response to any actions which persons do with secured data.A rule is a set of conditions to test the event with and actions performed when those conditions are fulfilled or not. See also: Event, Policy, Protected object, Person control rule, Copy rule, Transfer rule, Placement rule |
| Rule (DM) | Set of restrictions and conditions that monitor file operations on removable devices, network activity, printing, configure access to managed peripherals etc. Each interceptor features a separate rule type. A rule can be only applied within its policy. See also: Policy (DM) |
| 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 which checks files in the corporate network 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. |
| S/MIME | A standard for public key encryption and signing of MIME data |
| SMTP mail | An e-mail formed according to SMTP standards. See also: SMTP, Event |
| SPAN | Switched Port Analyzer is a technology that allows to mirror the network traffic from one port to another |
| SPAN copy | A variety of the “Copy” transport mode. In this case the traffic passes through a CISCO switch. The copy of the traffic is sent to Traffic Monitor Server for analysis. See also: SPAN |
| SSL | Secure Sockets Layer is a cryptographic network protocol developed for transmitting private documents via the Internet. |
| Status | Characteristics of persons and computers allowing to divide them onto groups for convenient analysis and activity control and to display them on dashboards and reports with special colour indicating. See also: Persons, Computers, Dashboard, Report |
| Stop word | Numbers, letters and words, whose presence in cells do not trigger these cells. Stop words are used to eliminate false triggering. |
| Tag | The text label giving a brief description of the event. See also: Event attributes |
| 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. |
| Telegram | A messenger for smartphones which allows you to sent text messages, images, audio and video files; uses MTProto protocol |
| Term | One of the set of words and phrases together defining a topical area. See also: Category |
| Term Weight | How the term is characterized for the given category; an integer between 1 and 10. If a term with a higher weight is detected in event, then this event will be more likely associated with the category of this term. See also: Term |
| Text object pattern | Unified description of all possible text objects with the typical structure: passport numbers, credit card numbers, phone numbers, medical codes etc. See also: Text objects |

| | |
|---|---|
| Text objects | Technology of matching the data from the events' text with defined patterns (rules of generating bank card numbers) . See also: Technologies, Event, Technology element, Text object pattern |
| Transfer rule | The rule that regulates sending and receiving protected data. See also: Rule, Protected data, Data protection policy |
| Transport mode | Event attribute that defines the level of control when the object is delivered to the recipients. Assigned by the analysis and decision engine during the object analysis. Together with the "Verdict" attribute determines if the object can be delivered further on. See also: Event attributes, Verdict, Copy mode, Normal transport mode, Delivery status |
| User | IW TM users: administrator, security officer etc. See also: Administrator, Security officer, Person |
| User interface | The complex of tools and methods by means of whose the user interacts with the system. |
| User role | A set of privileges that define a set of actions available for the user. See also: Administrator, Security officer, Management Console, Privilege |
| Verdict | An event attribute with the conclusion about the presence (or absence) of violations in an event. Together with the Transport Mode attribute determines if the event can be delivered further on. See also: Event, Transport mode, Delivery status, Event attributes |
| Verdict reason | Event attribute that describes the reason why a certain verdict was assigned to the event. See also: Event attribute, Verdict |
| Violation | The value of the «Decision» attribute; means that the corporate security policy has been violated. See also: Decision, Corporate security policy |
| Violation level | Event attribute indicating (by the colour tag) the level of threat to corporate security policy. See also: Event, Event attributes, Violation |
| Visibility scope | The way to divide intercepted events to restrict Management console user access to them. Events satisfying criteria of some visibility scope will be visible to those users who have an access to this scope only (given that user has privileges to view or/and manage events). See also: Event, Privilege |
| Widget | Interface element in the form of an isolated area that displays the specified statistic information on violations and violators. See also: Management console, Violation, Violator |
| Workstation | Computer type: desktop or notebook with OS of Windows or Linux or Mac family. See also: Computer |
| XMPP | Extensible Messaging and Presence Protocol is a communications protocol for message-oriented middleware based on XML. |