

INFOWATCH

InfoWatch Traffic Monitor 4.1

User Guide

INFOWATCH TRAFFIC MONITOR 4.1

User Guide

© ZAO “InfoWatch”
Tel. +7 (495) 2290022 • Fax +7 (495) 2290022
http://www.infowatch.com
Last edited September 20014

Contents

Part I Introduction 11

1.1 Glossary 12

1.2 Additional Documentation 16

Part II InfoWatch Traffic Monitor Overview 16

2.1 InfoWatch Traffic Monitor Standard and InfoWatch Traffic Monitor Enterprise 17

2.2 Object Interception and Analysis 18

2.2.1 Object Interception 18

2.2.2 InfoWatch Traffic Monitor Transport Modes 19

2.2.3 Object Analysis and Verdict 20

2.2.4 Uploading Object into Database 22

2.2.5 Retrospective Data Analysis, User Decision on an Object 22

2.2.6 Specific Features of Blocking HTTP-queries and Messages Sent Through Web-services 22

2.2.7 Using the System without an Objects Analysis Script 23

Part III Management Console: General Information 24

3.1 Running the Management Console and Connecting to the Database Server 24

3.1.1 Configuring Connection List 26

3.2 Management Console Interface 27

3.2.1 Management Console Main Window 28

3.2.2 Menagement Console Sections 29

3.2.3 Management Console Hotkeys 31

3.3 Refreshing Data in Management Console 33

3.4 Changing the User's Password 34

Part IV Management Console Administration 35

4.1 Management Console Access Control 35

4.1.1 Management Console User Roles 36

4.1.1.1 Privilege List 36

4.1.1.2 Creating and Editing a Role 40

4.1.1.3 Deleting a Role 43

4.1.2 Controlling the Access to the Objects Content 43
4.1.3 Management Console Accounts 44
4.1.3.1 User Name and Password Recommendations 45
4.1.3.2 Creating and Editing a User Account 46
4.1.3.3 Locking/Unlocking a User Account 49
4.1.3.4 Deleting a User Account 50
4.2 Configuring Sending/Receiving Reports on Objects 50
4.2.1 Configuring the Mail Server for Sending Reports 51
4.3 Configuring the Violation Notifications 52
4.4 Configuring a Query on Exit from the Management Console 53
4.5 Working with Hosts 53
4.5.1 Adding Comments to the Host 55
4.5.2 Deleting a Host 56
4.6 Viewing the Database Usage Statistics 57
Part V Persons and Workstations Directory 58
5.1 Configuring Connection and Synchronization with Active Directory 58
5.2 Persons Directory 61
5.2.1 Creating and Editing a Person Record 62
5.2.2 Deleting and Restoring a Person Record 65
5.2.3 Viewing and Filtering Persons Entries 66
5.3 Workstations Directory 67
5.3.1 Editing a Workstation Record 67
5.3.2 Viewing and Filtering Workstations Entries 69
5.4 Groups Directory 70
5.4.1 Creating, Viewing, and Editing a Group 71
5.4.2 Adding Members to a TM Group 73
5.4.3 Deleting Members from a TM Group 74
5.4.4 Deleting and Restoring a TM Group 74
5.5 Uploading Directories to the Host 75
Part VI Crawler 75
6.1 Crawler's Work Scheme 77

6.2 Connecting the Management Console to the Crawler Sever 79
6.3 Configuring the Crawler Scanner General Settings 80
6.4 Creating and Editing the Scanning Job 83
6.4.1 Scanning the Network File Shares 84
6.4.2 Scanning the Workstation's Local Disks 90
6.4.3 Scanning the SharePoint File Storage 95
6.5 Deleting the Scan Job 100
6.6 Running and Stopping the Job 100
6.7 Cleaning the Hash Base 102
Part VII Configuring Objects Analysis 102
7.1 Configuration Management 102
7.1.1 Configuration versions 103
7.1.1.1 Viewing the Configuration Information 104
7.1.1.2 Adding Comments to the Configuration Version 105
7.1.1.3 Comparing Two Configuration Versions 105
7.1.1.4 Uploading Configuration to the Hosts 107
7.1.1.5 Rolling Back to a Previous Configuration Version 107
7.1.1.6 Deleting a Configuration Version 108
7.1.2 Classification 108
7.1.2.1 Main Principles for Creating a Classification 110
7.1.2.2 Creating a Category 111
7.1.2.3 Adding a Term to the Category 112
7.1.2.3.1Creating a Term 112
7.1.2.3.2Importing Terms from a File 113
7.1.2.3.3Moving a Term from Another Category 114
7.1.2.4 Editing Categories 114
7.1.2.5 Changing the Level of a Category 116
7.1.2.6 Configuring Term Settings 116
7.1.2.7 Searching for a Term 118
7.1.2.8 Deleting a Category 119
7.1.2.9 Exporting/Importing the Classification 119
7.1.3 Lists 120

7.1.3.1 Creating a List Group 121
7.1.3.2 Creating a List 122
7.1.3.3 Creating a List Item 123
7.1.3.4 Editing a List or a List Group 124
7.1.3.5 Viewing and Filtering List Items 125
7.1.3.6 Deleting a List or a List Group 126
7.1.4 Object Analysis Script 126
7.1.4.1 Creating a Script 127
7.1.4.2 Loading a Script from a File 129
7.1.4.3 Editing a Script 129
7.1.4.4 Activating a Script 129
7.1.4.5 Saving a Script to a File 130
7.1.4.6 Deleting a Script 130
7.1.5 Text Objects 130
7.1.5.1 Uploading Standard Text Objects from XML-files 132
7.1.5.2 Creating and Editing a User Text Object 133
7.1.5.3 Adding a Values of User Text Object 135
7.1.5.4 Enabling and Disabling a Text Object and its Values 136
7.1.5.5 Deleting a User Text Object and its Values 138
7.1.5.6 Groupping and Filtration of Records 138
7.1.6 Sample Document Database 139
7.1.6.1 Creation the Sample Documents Database 140
7.1.6.2 Editing Sample Document Information 141
7.1.6.3 Deleting a Sample Document 142
7.1.6.4 Grouping of Records 142
7.1.7 Responsibility Zones: objects access differentiation 143
7.1.7.1 Creating and Editing a Responsibility Zone 143
7.1.7.2 Changing Responsibility Zone Priorities 146
7.1.7.3 Deleting a Responsibility Zone 146
7.2 Directories 147
7.2.1 Tags 147
7.2.1.1 Creating a Tag Group 148

7.2.1.2 Creating a Tag 149
7.2.1.3 Editing Tags and Tag Groups 149
7.2.1.4 Deleting a Tag Group 151
7.2.2 Colors 151
7.2.2.1 Creating and Editing a Color 151
7.2.2.2 Deleting a Color 152
7.3 Configuring Object Analysis Scripts (LUA) 153
7.3.1 Specifics of Creating LUA Scripts 153
7.3.2 InfoWatch Traffic Monitor Data Model 155
7.3.3 Data Types 155
7.3.3.1 The root element 156
7.3.3.2 Object envelope (Envelope) 156
7.3.3.3 Object content and content analysis results (Object) 158
7.3.3.4 Object headers (ObjectHeaders) 159
7.3.3.5 Object headers names (ObjectHeader) 159
7.3.3.6 Content analysis results (ObjectProcessing) 160
7.3.3.7 List of attachments (Objects) 160
7.3.3.8 Object processing results (Processing) 161
7.3.4 Operators 162
7.3.4.1 Assignment operator 163
7.3.4.2 Comparison operator 163
7.3.4.3 Condition operator 163
7.3.4.4 Cycle operator 164
7.3.5 Methods 164
7.3.5.1 Adding a message 165
7.3.5.2 Adding a tag 166
7.3.5.3 Search for a string in a list 166
7.3.5.4 Search for a string in a list group 167
7.3.5.5 Search by XML context elements 167
7.3.5.6 Search for a sender in a group 168
7.3.5.7 Search for a recipient in a group 168
7.3.5.8 Search for a workstation in a group 168

7.3.5.9 Search for list elements in a text 169
7.3.6 Helper Function Library 169
7.3.6.1 Categories Detection 170
7.3.6.2 Categories from List Detection 170
7.3.6.3 Quotes from Sample Documents Detection 171
7.3.6.4 Text Objects Detection 171
7.3.6.5 Text Object Relating to Specified Sector Detection 171
7.3.6.6 Attachments of Unknown Format Detection 171
7.3.6.7 Encrypted Attachments Detection 172
7.3.6.8 Object Processing Errors Detection 172
7.3.6.9 Attachment Processing Errors Detection 172
7.3.6.10 Content Analysis Errors Detection 172
7.3.6.11 Checking Garbage Traffic 172
7.3.6.12 First Node Searching 173
7.3.6.13 Identification Errors Detection 173
7.3.6.14 Sending Notice to Security Officer 173
7.3.6.15 Sending Notice to Violator 174
7.3.6.16 Several Tags Detection 174
7.3.7 Script Example 174

Part VIII Analyzing Intercepted Objects 182

8.1 Generation of Queries by Objects 182
8.1.1 Query Optimization Rules 183
8.1.1.1 General Object Attributes 183
8.1.1.2 Envelope Headers and Object Headers 185
8.1.2 Features of Searching in the Text 188
8.1.2.1 Indexing in Oracle Text 188
8.1.2.2 Syntax in Query Conditions 189
8.1.2.3 Examples 190
8.1.3 Creating and Editing a Query 194
8.1.3.1 General Query Settings (General tab) 196
8.1.3.2 Selecting Fields to View (View tab) 198
8.1.3.3 Configuring Query Conditions (Conditions tab) 199

8.1.3.3.1Creating a Query Condition 199
8.1.3.3.2Condition Settings 202
8.1.3.3.3Editing Query Conditions 204
8.1.3.4 Configuring Sorting Conditions (Sorting tab) 206
8.1.3.5 Configuring Grouping (Grouping tab) 207
8.1.3.6 Setting Permissions for Handling a Query (Allowed Users tab) 208
8.1.4 Copying a Query 209
8.1.5 Deleting a Query 209
8.2 Working with Objects 209
8.2.1 Object Custom Analysis 210
8.2.1.1 Configuring the Object Content Preview Mode 211
8.2.1.2 Setting the Size Limits for Downloaded SMTP Messages and Print Jobs 212
8.2.1.3 Configuring Object Info Pane 212
8.2.1.4 Running Object Queries 213
8.2.1.5 Query Autoupdate 214
8.2.1.6 Query Manager 215
8.2.1.7 Viewing Objects Information 216
8.2.1.7.1Viewing the General Object Information 216
8.2.1.7.2Detailed View of an Object 219
8.2.1.7.3Configuring Search for Object Headers 222
8.2.1.7.4Viewing the Object Log 223
8.2.1.8 Processing the Sender, Recipient, and Workstation Data 223
8.2.1.9 Making the Decision about an Object 225
8.2.1.10 Putting under Control 226
8.2.2 Moving Object to Another Responsibility Zone 229
8.2.3 Sending an Object Report 229
8.2.4 Assigning Tags to an Object 231
8.2.5 Highlighting Objects with Color 232
8.2.6 Adding a Comment to an Object 232
8.2.7 Downloading Attachments, Messages, and XML Context 233
8.2.7.1 Downloading the Attachments of an Object 233
8.2.7.2 Downloading SMTP Messages 234

8.2.7.3 Downloading XML Context 234
8.3 Generating Object Reports 235
8.3.1 Report Types 236
8.3.2 Creating and Editing a Report 240
8.3.3 Viewing the Report Results 242
8.3.4 Rebuilding a Report 242
8.3.5 Printing a Report 243
8.3.6 Copying a Report 243
8.3.7 Exporting a Report 243
8.3.8 Deleting a Report 244
8.4 Managing the Queries and Reports Folders 244
8.4.1 Creating and Editing a Folder 244
8.4.2 Moving Queries and Reports between Folders 246
8.4.3 Copying a Folder 246
8.4.4 Deleting a Folder 247
Part IX Licensing information 247
9.1 End-User License Agreement 247
9.2 Third-Party Licenses 250

1 Introduction

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

The Management Console application is a part of the InfoWatch Traffic Monitor system, it allows to configure the system settings and to monitor the System.

This guide explains how to use the System (configuring settings, analyzing information objects, etc.) using the Management Console.

The guide is intended for users with basic knowledge of Microsoft Windows. In order to create object analysis scripts it is required to use LUA programming language.

To set up context search using Oracle Text it is necessary to know how to use Oracle Text (see Oracle Text Reference, Version 11g).

This guide contains the following sections:

- InfoWatch Traffic Monitor Overview – General description of the System, methods of checking the data. Describes how to start Management Console and how to log in. Contains introductory information about Management Console (user interface overview, user interface setup, updating data).
- Management Console Administration – This section covers the system administration (user accounts management, assigning roles, etc.), configuring the object reports settings, and working with hosts. It also describes how to get database usage statistics, and how the persons and workstations information (acquired from Active Directory and created using the System) is managed.
- Configuring objects analysis options – Describes how to configure the settings and rules for checking intercepted data, for data monitoring and analysis. Describes additional analysis settings (tags, responsibility zones, colors), also describes how to create scripts to analyze various objects (emails, s, etc.)
- Analyzing objects – Describes how to create and configure queries for data selection and getting statistics for the intercepted data. Contains the information on how the intercepted objects are being analyzed.

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

- If you have purchased the product from a partner of InfoWatch, you should contact the Technical Support Service of this partner company.
- If you purchased the product directly from InfoWatch, you can contact our Technical Support Service at support@infowatch.com.

  The representatives of our Technical Support Service are available to assist you Monday through Friday from 7AM to 9PM (Moscow time), except weekends and Russian public holidays.

Before contacting Technical Support it is advised to refer to our *Knowledge Base*: http://cp.infowatch.com/kb. The Knowledge Base may already contain the answer to your question or a description of the problem you are experiencing.

1.1 Glossary

Term	Definition
Active Directory	LDAP-compatible Microsoft directory services for the operating systems of the Windows NT family
Active Script	A script to be included into a configuration that is uploaded to a host. See also: *Script*
Administrator	A preset role and user account in Management Console. An Administrator can modify other accounts and their rights. Also - a system user who installs, configures and maintains the System. See also: *User Roles*, *Security Officer*
Attachment	File attached to the intercepted object (at any level). See also: *Object*
Autolinguist	The InfoWatch Autolinguist software. This software allows to create categories and terms based on a collection of texts, and then use these categories and terms in a Classification. See also: *Linguistic Analysis*, *Classification*
Category	A Classification element that corresponds to a certain area (e.g. security labels or project terms). Contains subcategories or terms. See also: *Term*, *Classification*
Case Sensitivity	A setting that defines if the term search is case-sensitive (uppercase and lowercase letters are considered different) or not. See also: *Term*
Characteristic Term	Term setting: If a text contains a characteristic term that referrers to a certain category, the text is classified as referring to this category. See also: *Term*
Citation Index	How close the sample document matches the text of the document being analyzed. See also: *Sample document*
Classification	Referencing of the analyzed text to any category of the Classification. See also: Classification, *Object context*
Classification	A set of data required to perform the linguistic analysis of a text. Contains the list of various security policy violation categories. If the text that contains a term from a certain category, it is matched with this category. Also - assigning a certain classification category for the text. See also: *Category*, *Term*, *Linguistic Analysis*, *Object context*
Configuration	A group of settings required to check objects, to monitor and analyze data. See also: *Classification*; *Script*, *Lists*, *Text object*
Configuration Version	A fixed state of the configuration designed to monitor changed settings of the object analysis. A configuration version is committed after uploading to a host. A configuration version can be Active (currently used), Editable (the last version with up-to-date modification) and Archive (obsolete). See also: *Configuration*
Copy mode	One of the transport modes of InfoWatch Traffic Monitor. In this mode the actual traffic bypasses the System. A copy of traffic is analyzed. In this mode the traffic cannot be filtered by the System. See also: *Transport Mode*
Color	Object attribute assigned by the decision engine or by the Management Console user. Defines the color to paint the object when displayed in Management Console. See also: *Object attributes*
Corporate Security Policy	A set of technical, organizational, administrative, legal and physical measures, methods, rules and guidelines that cover all the security aspects in a company.
Data Interception	A process of acquiring, parsing, categorizing and converting data (or a copy) into context. It is possible to intercept data transferred using the following protocols: SMTP, HTTP, ICQ/ OSCAR, Skype, IXP, XMPP, MMP, FTP. See also: *Monitor*, *Object context*
Data interception channel	A data interception environment that include technical appliances, software tools and communication protocols. The System supports the following data interception channels: email (SMTP), Web (HTTP), instant messaging services (ICQ and Skype), shadow copies of

	files, connected/disconnected workstation events, and print jobs.
Delivery Status	Object attribute that specifies if an object will be delivered to recipients after analysis. If the object is approved for delivery, the value of this attribute will match the delivery state (delivered/blocked). See also: *Object attributes*
Detecting Text Objects	A technology that searches for text objects (such as credit card numbers) in the text. See also: *Text object*, *Text object template*
Detecting Digital Fingerprints	A technology that searches for sample document quotes in the text. See also: *Sample document*, *Quote*
Device Monitor	InfoWatch Device Monitor: a software and hardware appliance designed to control the access to the peripherals and to monitor the data being copied to removable media and FTP, sent to printing and to monitor messengers.
DeviceLock Adapter	A Device Monitor interceptor that integrates with DeviceLock (by Smart Line, Inc.), intercepts the shadow copies of the files being copied to the removable devices. See also: *Device Monitor*, *Shadow copy of a file*
Digital Fingerprint	A method of storing a sample document in a database in the form of a set of quotes. See also: *Sample document*, *Quote*
Envelope headers	Predefined set of headers for all types of objects. The envelope header format is defined according to the context. See also: *Object attributes*
File Signature	A constant integer value that uniquely identifies a file of a certain type
Group	Groups of users and workstations. Groups are stored in the system directories. The groups are divided into AD Groups (imported from Active Directory) and TM Groups (created using InfoWatch Traffic Monitor). See also: *Persons, workstations, and groups directories*
Host profile	A group of settings related to the tasks performed by the given host. See also: *Host setting*
Host setting	A group of settings related to the tasks performed by the given host. See also: *Host profile*
HTTP	HyperText Transfer Protocol, an application-tier protocol used to transfer the data in the text format
HTTP request	A request formed according to the HTTP standards (POST requests, GET requests etc.) See also: *HTTP*, *Object*
ICAP	(Internet Content Adaptation Protocol), a protocol that allows to control the incoming and outgoing HTTP traffic. It also makes possible to modify the content of the HTTP requests (InfoWatch Traffic Monitor controls only outgoing traffic).
ICQ	An Internet instant messaging service, currently owned by Digital Sky Technologies
ICQ message	A message sent using the ICQ-OSCAR protocol. See also: *Object*
Identification Error	A situation when one value of the Sender, Recipients, or Workstation attribute have several matches in the persons and workstations directory. See also: *Persons, workstations, and groups directories*
InfoWatch Traffic Monitor	The InfoWatch Traffic Monitor software suite (IW TM). Designed to control various types of traffic (SMTP, HTTP, ICQ) and shadow copies of the data being copied to the removable media and sent to printing.
Linguistic Analysis	A text classification technology that works by matching this text with certain categories. See also: *Classification*, *Category*
Interceptor	Also: Sniffer, Network Traffic Analyzer, Monitor. An InfoWatch Traffic Monitor component that receives data (SMTP, HTTP, ICQ traffic) from external clients, prepares the data for further analysis and sends them to Traffic Monitor Server.
Lists	Lists of the data of the same type, generated by Management Console to use in the object analysis scripts. See also: *Configuration*, *Script*
Management	Graphic user interface. Designed to manage InfoWatch Traffic Monitor (system

Console	administration, configuring settings, object analysis etc.)
Morphology	Term setting: if morphology is used, the text search will detect all word forms of this term. See also: *Term*
Monitor	See: Interceptor
Normal transport mode	A traffic analysis and filtering mode. In this mode it's possible to block the illegal traffic. See also: *Transport Mode*
Object	Traffic objects (SMTP e-mails, HTTP requests, ICQ messages, Skype messages), shadow copies of files and print jobs.
Object analysis	The procedure of processing the attributes, attached files and text of the intercepted objects, assignment additional attributes. See also: *Script*, *Object attributes*
Object attributes	Structured data extracted from the intercepted objects and assigned based on the processing results. See also: *Script*, *Verdict*, *Solution*, *Transport Mode*, *Color*, *Tag*
Object Context	An internal representation of an intercepted object. XML data (attributes, text) extracted from the object and its attachments. After processing, the analysis results and the decision are added to the context. See also: *Object*
Object Headers	An arbitrary, dynamically updated set of headers. See also: *Object attributes*
Object Body	An object without its attached files. See also: *Object*
Object Text	Text information extracted from the object body and attachments. Does not contain formatting or markup. Used for search and analysis purposes. See also: *Object*
Query	Management Console database query to get the updated data. See also: *Management Console*
Oracle Text	A text search technology by Oracle. See also: *Object*
Persons, workstations, and groups directories	Information about users, workstations, groups of users, and groups of workstations, imported from Active Directory and created using Management Console. Used to make it easier to work with the intercepted objects information
Privilege	An entity that defines the actions (or sets of actions) available for a user to work with the System
Quote	A quote from the sample document database, found in the intercepted object text. See also: *Sample document*
Sample document	Quotes from these documents are searched in the text being analyzed. Memos, financial reports, contracts and other sensitive documents can all be used as sample documents. Sample documents are stored as digital fingerprints. The text cannot be viewed by users or administrators. See also: *Detecting Text Objects*, *Digital Fingerprint*, *Quote*
Sample Document Database	Storage of digital fingerprints captured from sample documents. Required to search for quotes in the texts being analyzed. See also: *Sample document*, *Detecting Digital Fingerprints*, *Digital Fingerprint*, *Quote*
Report	An e-mail sent using Management Console to notify other Management Console users about one or more intercepted objects. Contains the numbers of the selected objects and the corresponding message. Also - a selection of the statistics about the intercepted objects. See also: *Management Console*
Responsibility Zone	A way to separate the intercepted objects to restrict the user access from Management Console. The objects belonging to a certain responsibility zone are visible to the users who belong to this responsibility zone (provided that the user has privileges to view or/and handle the objects). See also: *Privilege*
Script	Set of rules used to analyze and process objects. A rule consists of a set of conditions for analyzing objects and actions to be performed when the specified conditions are met/not

	met. See also: *Active script*
Security Officer	A preset role and user account in Management Console, has all privileges except managing users and roles. See also: *User Roles*, *Administrator*
Shadow copy of a file	A copy of the file creating on a removable storage media. The copy is created only if the file is successfully saved on the removable storage device. The shadow copies of files are analyzed by InfoWatch Traffic Monitor
SMTP	Simple Mail Transfer Protocol, a networking protocol used to send the email in TCP/IP networks
SMTP e-mail	An e-mail formed according to SMTP standards. See also: *SMTP*, *Object*
Solution	A decision made by the user: whether or not the intercepted object violates the corporate security policy. Possible values: `No Decision`, `Violation`, and `No Violation`. See also: *Verdict*, *Object attributes*
SPAN	Switched Port Analyzer, 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. A copy of the traffic is sent to Traffic Monitor Server for analysis. See also: *SPAN*
Tag	A text markup that defines the intercepted object. See also: *Object attributes*
Term	Word of phrase that increases the matching rate if found in the text. See also: *Category*
Term Weight	How characteristic is the term for the given category. If a term with a higher weight is detected in a text, then this text will be more likely associated with the category of this term. In the Management Console – an integer between 1 and 10. See also: *Term*
Text Index	List of words generated by Oracle Text from the text and attachments of intercepted objects. Contains links to the objects. Used to search in objects text and attachments, and when running database queries. See also: *Query*, *Oracle Text*
Text Object	The data from the analyzed text that were considered matching the pattern by the text object detection module. See also: *Text object template*, *Detecting Text Objects*
Text Object Template	Unified description of all possible text objects with a typical structure: passport numbers, credit card numbers, phone numbers, medical codes etc. See also: *Detecting Text Objects*
Transparent Transport Mode	The mode of transferring the traffic without being filtered. The System only analyzes the intercepted traffic. See also: *Transport Mode*
Transport Mode	Object attribute that defines the level of control when the object is delivered to the recipients. Assigned by the analysis and decision engine during the object analysis. Together with the "Verdict" attribute, determines if the object can be delivered further on. See also: *Verdict*, *Copy mode*, *Normal transport mode*, *Transparent transport mode*, *Delivery Status*, *Object attributes*
Verdict	An object attribute with the conclusion about the presence (or absence) of violations in an object. Together with the Transport Mode attribute, determines if the object can be delivered further on. This is a mandatory attribute of an object. See also: *Transport Mode*, *Delivery Status*, *Object Attributes*
Verdict Reason	Object attribute that describes the reason why a certain verdict was assigned to the object: *Verdict*
Violation	The value of the `Decision` attribute; means that the corporate security policy has been violated. See also: *Solution*, *Corporate Security Policy*
User role	A set of privileges that define the actions available for the user. See also: *Administrator*, *Security Officer*, *Management Console*, *Privilege*

1.2 Additional Documentation

For more information see the following documents:

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

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

2 InfoWatch Traffic Monitor Overview

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

InfoWatch Traffic Monitor Main Features:

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

  Note

  When integrated with a Blue Coat proxy server, the System can only intercept the HTTPS traffic if the proxy server processes the HTTPS traffic as the HTTP traffic.
- Interception of the copy of the ICQ traffic (using OSCAR protocol) that passes through CISCO SPAN-enabled hardware. When ICQ connects through HTTP, the System intercepts the ICQ traffic similarly to HTTP traffic.

  Important!

  Interception and analysis of the encrypted ICQ traffic, including SSL, is not supported.
- Analyze the contents of the intercepted traffic to detect the violations of the corporate security policy
- Filtering the intercepted traffic by allowing or blocking delivery of certain data

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

- Analyze the Skype traffic, shadow copies of files and print jobs intercepted by InfoWatch Device Monitor system to detect the violations of the corporate security policy.
- Analyze the file shadow copies intercepted by DeviceLock version 6.3 or higher (provided by SmartLine, Inc.) to detect the violations of the corporate security policy.

InfoWatch Traffic Monitor Components

InfoWatch Traffic Monitor component	Purpose
Server end	Traffic Monitor Server: intercepts, analyzes and filters the traffic, and analyzes the data received from InfoWatch Device Monitor and DeviceLock. Sniffer: intercepts a copy of traffic which goes through the SPAN port of a switch and transfers it for analysis. The IW ICAP module: intercepts, analyzes and filters the HTTP traffic transmitted over the ICAP protocol. The remote database management module: transmits data for storage to a remote database over narrow-band connections
Database	Stores the information provided by the System running (intercepted data, results of the analysis)
Management Console	Configures the rules for traffic analyzing and filtering, analysis of the incoming data

2.1 InfoWatch Traffic Monitor Standard and InfoWatch Traffic Monitor Enterprise

Starting with InfoWatch Traffic Monitor 3.5, there are two editions of the software: Traffic Monitor Standard and Traffic Monitor Enterprise.

InfoWatch Traffic Monitor Standard has lower system requirements (for more details see "*InfoWatch Traffic Monitor. Installation and Configuration Guide*") and has limited functionality:

- The objects are intercepted only in the copy mode (for more information about modes see "Objects Interception ");
- If the objects in the database exceed certain size, the objects periodically are deleted from the database. It's possible to prevent objects from being deleted in such a way using a special tag (see "Assigning Tags to an Object").

InfoWatch Traffic Monitor Enterprise provides the full functionality (see "InfoWatch Traffic Monitor Overview").

2.2 Object Interception and Analysis

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

- Object Interception
- InfoWatch Traffic Monitor Transport Modes
- Object Analysis and Verdict
- Uploading Object into Database
- Retrospective Data Analysis, User Decision on an Object
- Specific Features of Blocking HTTP-queries and Messages Sent Through Web-services
- Using the System without an Objects Analysis Script

2.2.1 Object Interception

The system *objects* are the following:

- traffic objects (SMTP e-mails, HTTP-requests, ICQ messages, Skype messages);
- shadow copies of files;
- print jobs.

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

Object type	Object interception options
SMTP	• The System intercepts and delivers the SMTP traffic. There is a possibility of filtering the intercepted objects (the delivery can be allowed or blocked). *Only for InfoWatch Traffic Monitor Enterprise.* • The System receives a copy of SMTP traffic from the corporate mail relay server. The System does not take part in traffic delivery. • The System receives a copy of SMTP traffic that goes through the switches with a SPAN port. The copy is intercepted using Sniffer. The System does not take part in traffic delivery.
HTTP	• The System intercepts the HTTP using the ICAP server integration. There is a possibility of filtering the intercepted objects (the delivery can be allowed or blocked). *Only for InfoWatch Traffic Monitor Enterprise.* • The System receives a copy of the HTTP traffic that passes through a switch with a SPAN port. The copy is intercepted using Sniffer. The System does not take part in traffic delivery.
ICQ	• The System receives a copy of the ICQ traffic that passes through a switch with a SPAN port. The copy is intercepted using Sniffer. The System does not take part in traffic delivery. • When ICQ connects through HTTP, the System intercepts the ICQ traffic in the same way as the HTTP traffic.
Skype messages, GTalk messages or Mail.Ru Agent messages	The System receives a copy of traffic from InfoWatch Device Monitor.
Files located in corporate network	The System receives a copies of files from Crawler subsystem.

Object type	Object interception options
Shadow copies of files and print jobs received from InfoWatch Device Monitor	The System receives a copy of traffic. Blocking user actions (printing, access to the devices) is possible only using InfoWatch Device Monitor
Shadow copies of files received from DeviceLock	The System receives a copy of traffic. Blocking user actions (access to the devices) is possible only using DeviceLock

The interception options and the following delivery of the objects depend on the InfoWatch Traffic Monitor transport mode (see "InfoWatch Traffic Monitor Transport Modes").

2.2.2 InfoWatch Traffic Monitor Transport Modes

InfoWatch Traffic Monitor supports three transport modes: *normal*, *transparent*, and *copy*. The conditions that specify the transport mode for different objects are defined in the object analysis script. A transport mode is assigned to the object when the object is analyzed in Traffic Monitor Server (see "Object analysis and verdict"). The selected transport mode defines further delivery of the object.



Important!

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

The difference between modes consists in the feature of objects delivery (see the table below).

Transport Mode	Description
Normal	InfoWatch Traffic Monitor intercepts, analyses, and forwards objects. In this mode the verdict defines if the object will be delivered to recipients. Moreover, in some cases the delivery status of the SMTP messages can be changed after changing the user decision (see "Specific features of blocking HTTP-queries and messages sent through web-services"). *Only for InfoWatch Traffic Monitor Enterprise*
Transparent	This mode differs from the previous one in one thing: the object is always delivered regardless of the verdict. In the transparent mode the change of the user's decision have no impact on the delivery of the object. *Only for InfoWatch Traffic Monitor Enterprise*
Copy	In this mode the System receives copies of objects. The difference of this mode is that the objects are transported without using the System. In this way, the System performs the object analysis only. Since the copies of the objects are analyzed, the verdict and the analysis-based user decision do not impact on the object delivery to the recipients.

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

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

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

2.2.3 Object Analysis and Verdict

All intercepted items are delivered to the Traffic Monitor Server for analysis. The analysis of the objects is performed by the Traffic Monitor Server engines:

Traffic Monitor subsystem	Subsystem modules	System/subsystem features
Processing subsystem	SMTP Processing module (copy mode), HTTP Processing module (copy mode), ICQ Processing module (copy mode), Shadow Copies Processing module, SMTP Processing module (blocking mode), HTTP Processing module (blocking mode)	Extracting the valuable data and enclosures from the object, defining enclosures format and forwarding the extracted texts to the Analysis subsystem.
Analysis subsystem	Linguistic Analysis module	Text classification by searching if it corresponds to any categories
	Text Objects Detecting module	Searching in the object's text for text objects (credit card numbers for example)

Traffic Monitor subsystem	Subsystem modules	System/subsystem features
	Digital Fingerprints Detecting module	Searching in the object's text for quotes from sample documents
Policies Application subsystem	Active Directory Integration module	Providing the initial import and periodical synchronization of Active Directory structure with a Traffic Monitor persons and workstations directory for further binding this information with data from the intercepted objects
	Decision Making module	Providing application of information security policies by implementation object rules from the object processing script.

The object analysis is performed in the following order:

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

   The system supports three types of analysis:

Content analysis technology	Technology description
Linguistic Analysis	Determining the subject and content of a text based on the terms (words and phrases) found in this text. The search for the terms is performed using the Classification. The Classification includes the organization-specific terminology. All terms are divided into categories (each term can be correlated with one or more categories). Thus, the presence of a term belonging to a category allows to relate the text to this category. For example, the *Salary* term could be included in *Internal payments* and *Working conditions* categories. The presence of the term in the text means that the text can belong to the mentioned categories
Detecting Text Objects	Search for text objects matching the specified templates (like searching for credit card numbers in the intercepted objects)
Detecting Digital Fingerprints	Search for fragments of a text matching the predefined template documents (orders, financial reports, contracts, etc.)

4. Based on the results of the analysis, the Decision Making module assigns a **verdict** – a conclusion on the possible policy violation. The rules of taking a verdict are defined in the object analysis script. The following verdicts are provided:

- *Forbidden*. The object is qualified as violating the corporate security policy. In the normal transport mode this object is blocked and will not be delivered.
- *Allowed*. The object does not contain any violations of the corporate security policy. After being analyzed, the object will be delivered to the recipients if the normal transport mode is used.

2.2.4 Uploading Object into Database

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

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

2.2.5 Retrospective Data Analysis, User Decision on an Object

Objects in a database are available for analysis in the Management Console. When analyzing, the user can view the result of the analysis and make his/her own decision on the object (the *Decision* attribute).

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

- *Violation*. Based on the analysis results, the user found out that the object violates the corporate security policy.
- *No Violation*. The user has concluded that the object doesn't violate the corporate security policy.

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

Note

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

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

Important!

Object blocking allowed in InfoWatch Traffic Monitor Enterprise only.

If in the general transport mode (see "InfoWatch Traffic Monitor Transport Modes ") the System decides to block a HTTP-request or a message sent using a web service (such as Mail.RU), then the web-browser of the sender of the

request or of the message will display the blocking message.

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

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

- at the **Object Info** pane (see "Viewing the General Object Information") the *From*, *To*, *CC*, *Subject*, and *Sent* fields and attachments (if present) are displayed.
- if no aforementioned attributes can be found and no text can be extracted from headers, these POST requests may be deletes as a garbage traffic. For example, background status requests in social networks are such a garbage traffic. Information on using this feature see in "Checking Garbage Traffic" and "Script Example".

Web resource type	**Resources**	
	Without limitations	**With limitations**
Web-mail	mail.ru, yandex.ru, rambler.ru, pochta.ru, km.ru, newmail.ru, gmail.com, aim.com, gmx.com, yahoo.com, inbox.com, hotmail.com, hotmail.ru, mail.com	gmx.com, yahoo.com, mail.com, aol.com, aim.com Only the attachments are displayed
Blogs and social networks	livejournal.com (.ru), blogs.mail.ru, liveinternet.ru (li.ru), my.ya.ru, diary.ru, blogspot.com (blogger.com), loveplanet.ru/a-journal, myspace.com, mylivepage.com, privet.ru, perfspot.com, linkedin.com, odnoklassniki.ru, vkontakte.ru (vk.com), facebook.com, twitter.com, wordpress.com	myspace.com, facebook.com Only the attachments are displayed
Job search and CV posting sites		moikrug.ru, hh.ru, job.ru, rabota.ru, jobs.com, eurojobs.com Only the attachments are displayed. The text that has been entered during filling form does not appear (for example, when filling the online CVs)
Forums	forum.ru-board.com, sysadmins.ru, talk.mail.ru, dom.bankir.ru, forum.exler.ru, forum.ixbt.com, groups.google.ru (.com), biznet.ru	

2.2.7 Using the System without an Objects Analysis Script

There may be a situation when the Analysis and Decision Making subsystem won't be able to use the object analysis script (see "Configuring object analysis scripts"): for example, the script has not been created or has been deleted, or there was en error while running the script. The *Transport mode* or *Verdict* mandatory object attributes may also have incorrect values in the script or no values specified.. In this case, the following values of mandatory attributes are assigned to the objects:

- verdict: *Forbidden*;
- transport mode: *Copy*.

The *Verdict Reason* attribute is assigned the *No verdict from script*.

3 Management Console: General Information

This chapter covers the following topics:

- Management Console Main WindowManagement Console main window
- Management Console SectionsManagement Console sections
- Management Console Hotkeys

3.1 Running the Management Console and Connecting to the Database Server

Management Console needs a permanent connection to the database server. To connect to the database server you need to log in. The following conditions are checked during the logon process:

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

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

Note

Management Console is started for the first time with the user administrator's account (user name and password). This user account is added when the database schema is created (see "*InfoWatch Traffic Monitor. Installation and Configuration Guide*").

The connection to the database server is established at the startup of Management Console. You can also re-establish the connection to the database while working with Management Console. As a rule, the connection is re-established if you need to do the following:

- to restore the interrupted connection to the database server.
- to log on using another account.
- to connect to another database server.

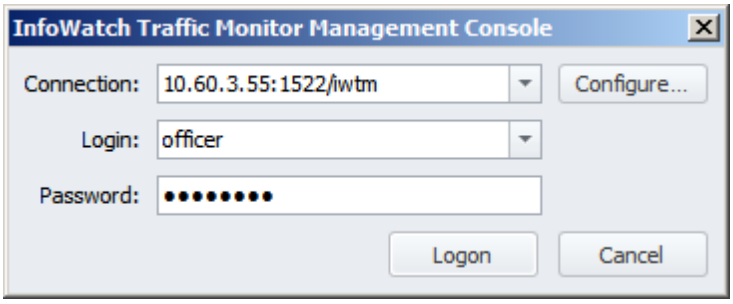
Note

The information about the current connection (*User@Server*) is displayed in the title bar of the main window and in the left side of the status bar.

To start using Management Console:

1. Do the following:

Action	Procedure
Start the Management Console and connect to the database server	Click **Start**, select **Programs > InfoWatch > Traffic Monitor > Management Console** or Run the program file from its folder
Connect to the database server from the Management Console	in the main menu, select **File > Connect**; or click **Connect** on the toolbar; or press `CTRL+SHIFT+C` on the keyboard.



2. In the **InfoWatch Traffic Monitor Management Console** dialog box, specify the logon settings:

Setting	Description
Connection	Alias of the database server used by the Management Console. To select a connection, click an arrow to the right of the field, and select a connection from the dropdown list. If the necessary connection is absent in the list, create it according to "Configuring Server Connection List" section
Login	User account name
Password	User password

Important!

If a user makes 10 consecutive attempts to log in with an incorrect password, this user will be locked out from Management Console for 24 hours (this is a default security measure of Oracle DBMS). To unlock the access to Management Console before this time expires, contact the database administrator.

Note

When Management Console is started for the first time, the **InfoWatch Traffic Monitor Management Console** dialog box will contain empty fields. The next time you start Management Console, the **Server** and **User** files will contain the details from the last successful logon. You have to enter the **Password** every time you attempt to log in.

If you have already logged in the system, you can select the required *User@Server* credentials using the ... button to the right of the **Server** field.

3. Click **Logon**.

If you log in successfully, you will have access to the main window of the Management Console. Otherwise, an error message will appear.

Important!

The maximum timeout of the connection to the database server is 15 seconds. If the connection could not be established, please try again.

Important!

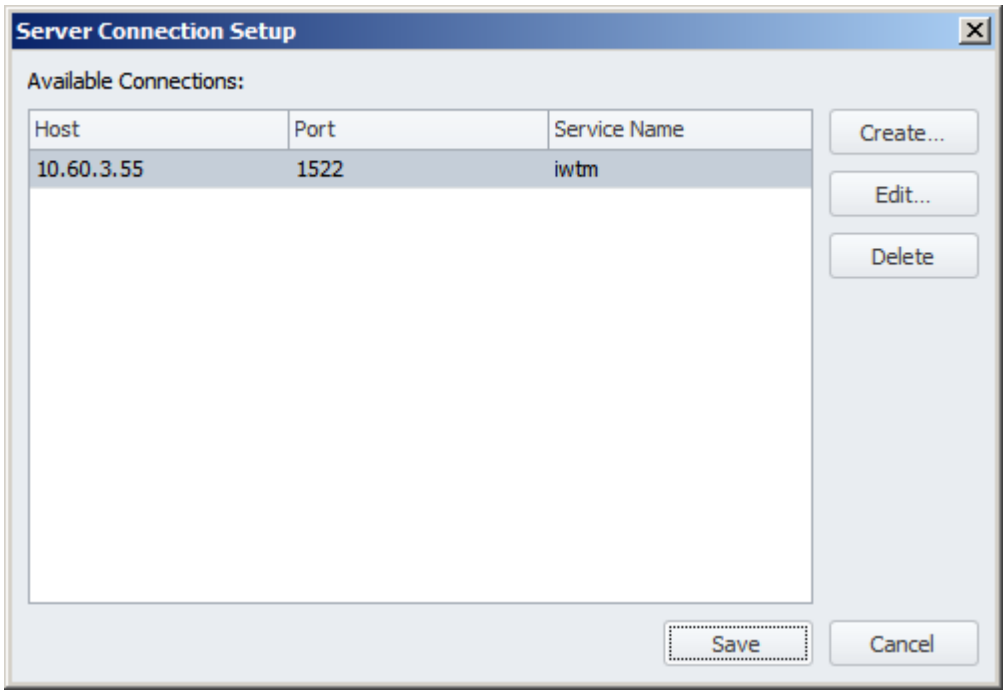
If you see a notice about lisence expiration, please address to Traffic Monitor administrator. You can read about installation details and lisence updating in document *«InfoWatch Traffic Monitor. Administration Guide»*.

3.1.1 Configuring Connection List

You can edit a list of Management Console connections to the Traffic Monitor database, if the necessary connection is absent in the field **Connection** of the logging dialog box (see "Running the Management Console and Connecting to the Database Server").

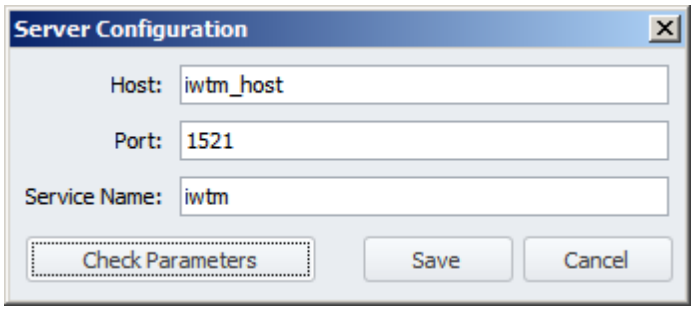
To add or change a connection entry:

1. In the logging dialog box click **Configure**.
2. In the **Server Connections Setup** dialog box do one of the following actions:
   - click **Create** to create new connection;
   - choose the connection string and click **Edit** to change its parameters.



3. In the dialog box appeared on the screen specify connection settings:
   - **Host** – name or IP-address of the computer where Traffic Monitor database operates;

- **Port** – database server port where the process of client connections listener is started;
- **Service Name** – name of the database service.



You can check the settings you've entered using the **Check Parameters** button. If the connection cannot be established, a message with the explanation will appear. Please check the settings or contact the system administrator. If the connection to the server is established, a "*Connection Successful*" message will appear.

4. Click **Save** to save specified connection settings and return to the logging dialog box.

To delete a connection entry:

1. In the **Server Connections Setup** choose the connection string and click **Delete**.
2. Click **Save**.

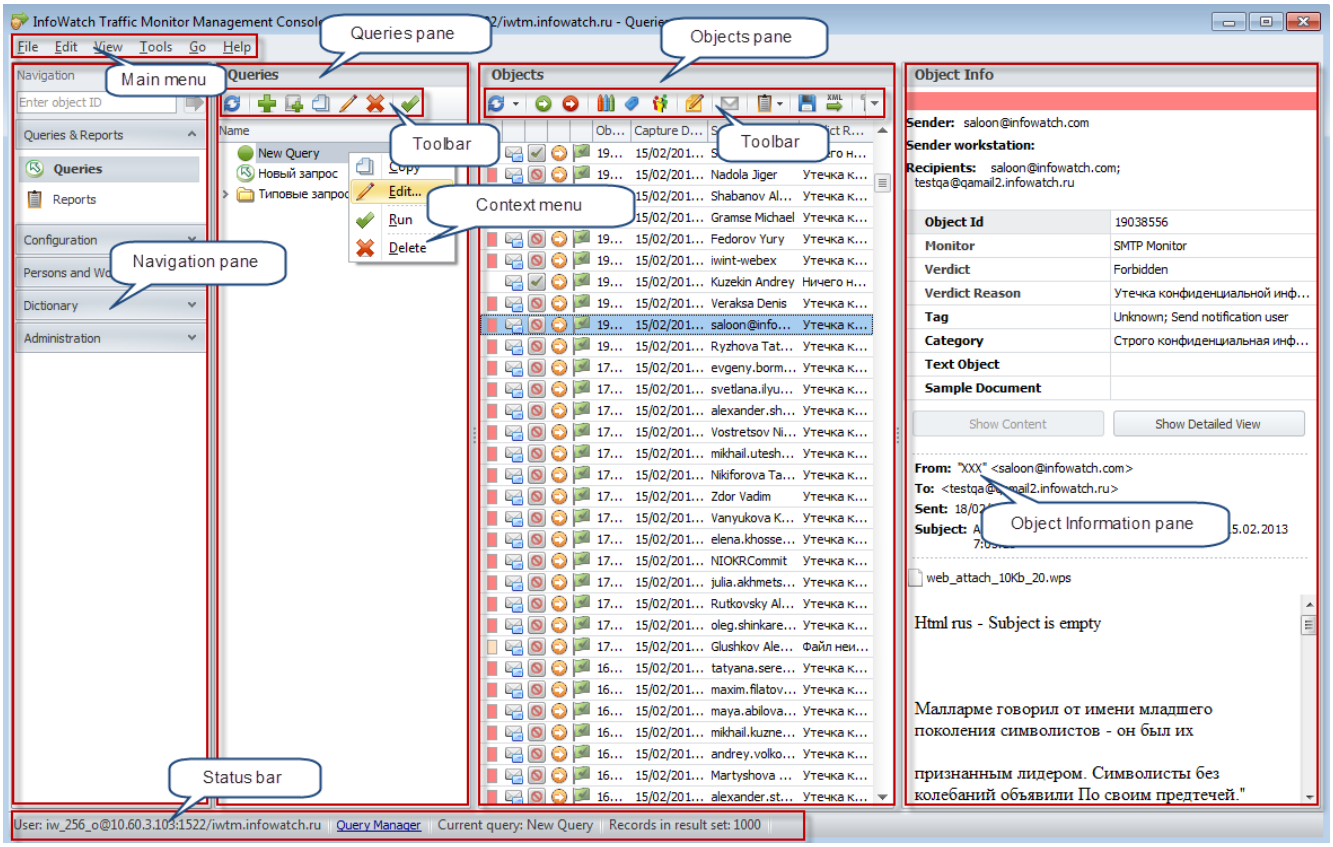
3.2 Management Console Interface

This chapter covers the following topics:

- Management Console Main WindowManagement Console main window
- Management Console SectionsManagement Console sections
- Management Console Hotkeys

3.2.1 Management Console Main Window

The following picture demonstrates the main window of InfoWatch Traffic Monitor Management Console.



Management Console main window

The main window items are listed in the following table.

Main window item	Purpose of the item
Main menu	Using basic Management Console features
Toolbar	Quick access to certain Management Console sections **Note:** Some sections contain additional toolbars
Context menu (right-click the required object)	Manage the selected object (repeats some of the main menu functions)
The **Navigation** pane	Navigating between the Management Console sections
The **Queries** pane (in the **Query** section)	View and configure queries to load objects from the database, query list management
The **Objects** pane (in the **Query** section)	Displaying the list of objects found by the query

Main window item	Purpose of the item
The **Object Info** pane (in the **Query** section)	Displaying information about an object (when working with queries)
The working area of the main window	Displaying the items of the selected section of the Management Console, working with the items of this section
Status bar	Displaying information about the current connection (*User@Server*) on the left side of the status bar. **Queries Manager** link When working with the Active Directory directories, also displays the Active Directory synchronization status and the status of uploading directories to Traffic Monitor Server. When working with queries, also displays the name of the current query, the number of loaded records etc.

You can configure the appearance and location of the **Navigation**, **Query List**, and **Object Info** panes.

To hide a pane,

In the main menu, select the **View** menu and click the name of the pane you want to hide. To display the pane again, repeat the operation.

To configure how the Navigation pane is displayed,

do one of the following:

- to enable the automatic minimization mode, click in the top right of the **Navigation** pane. To disable automatic minimization, click this button again.
- to hide the **Navigation** pane, click in the top right.
- to collapse the **Navigation** pane to the window mode, double click the pane header.

To move the Navigation pane,

click the header of the pane and drag it to the desired location on the screen. Then release the mouse button to lock the pane in its new position.

To resize a pane,

move the mouse pointer to the edge of the pane. When the mouse pointer turns into a double-headed arrow, click and hold the left mouse button. Drag the edge in the direction you need. When the pane reaches the desired size, release the mouse button.

3.2.2 Menagement Console Sections

The InfoWatch Traffic Monitor Management Console contains several sections. Each section is intended for certain management tasks. The sections are grouped on the **Navigation** pane by their purpose: **Queries & Reports**, **Configuration**, **Persons and workstations**, **Dictionary** and **Administration**.

To go to the required section,

do one of the following:

- In the main menu, select **Go** and click the name of the section you need.
- use the links on the **Navigation** pane.

The following table contains the description of the Management Console sections (the sections are grouped according to the **Navigation** pane sections).

Section Name	Section Icon	Section Description
Queries & Reports		
Queries		Displays current information about the data processed by the System. Working with the received data (allowing or blocking object delivery, sending a report, moving an object to another responsibility zone, assigning tags to an object, etc.)
Reports		Creates reports on the data processed by the System.
Configuration		
Configuration Versions		Manages the configuration versions (viewing and comparing different versions, changing current version, rolling back to a previous version). Uploading configuration to the hosts
Categories and Terms		Creating a Classification (populating it with categories and terms). Exporting/ importing the Classification database
Text Objects		Creates lists of text objects and their values. Selects text objects to be detected
Sample Documents		Creation of the sample documents database for digital fingerprints analysis
Scripts		Creation of scripts for object analysis, running scripts, exporting/importing scripts
Lists		Creation of lists (to be used when the object analysis scripts are created)
Persons and Workstations		
Persons		Management of person accounts imported from Active Directory. Creation of person accounts using InfoWatch Traffic Monitor
Groups		Management of person groups and workstation groups imported from Active Directory. Creation of person groups and workstation groups using InfoWatch Traffic Monitor
Workstations		Management of workstations accounts imported from Active Directory
Dictionary		
Tags		Tag groups management (creating groups, adding tags)
Colors		Creation of the list of colors (the colors are used for highlighting the objects)
Administration		
Crawler		Настройка параметров работы сканера файлов Crawler, создание и выполнение задач сканирования сетевых ресурсов
Users		User Account Management. Distribution of roles. Selecting recipients for sending reports

Section Name	Section Icon	Section Description
Roles		Management of user roles. Distribution of roles
Responsibility Zones		Management of responsibility zones (creation of responsibility zones, assigning users the responsibility zones)
Hosts		Viewing the list of Traffic Monitor servers. Viewing the configuration uploading status.
Database Usage		Displaying information on the database usage

3.2.3 Management Console Hotkeys

The following table lists the hotkeys - shortcut keys and key combinations used for quick access to different functions of InfoWatch Traffic Monitor Management Console.

Function name	Hotkeys
General functions	
Connect/reconnect the database server	Ctrl+Shift+C
See the Help	F1
Exit the Console	Alt+F4
Refresh data (query result, report result, configuration version, categories, scripts, lists, sample documents, persons, workstations, tags, colors, hosts, database usage statistics)	F5
Conditions in requests and reports	
Create condition	Ctrl+N
Create condition block	Ctrl+B
Edit condition	Ctrl+E
Delete condition	Ctrl+Del
Viewing objects: enclosures	
Select all enclosures	Ctrl+A
Select several enclosures	Ctrl + left mouse button
Select range	Shift + left mouse button

You can call the Main Menu functions with shortcut keys. If needed, select the required element (object, query, entry…) then press key sequences while holding the **Alt** key.

Function name	Hotkeys
Connect/reconnect the database server	Alt+(F->C)
Exit Console	Alt+(F->X)
View information on the Console version	Alt+(H->A)
Refresh data	Alt+(V->R)
Display/hide Navigation pane	Alt+(V->N)
Display/hide Queries pane	Alt+(V->Q)
Display/hide Object Info pane	Alt+(V->O)
Change password	Alt+(T->C)
User settings	Alt+(T->U)
Global settings	Alt+(T->G)
Create new entry	Alt+(E->N)
Edit entry	Alt+(E->E)
Delete entry	Alt+(E->D)
Managing queries	
Create query	Alt+(E->N)
Create folder	Alt+(E->F)
Copy query	Alt+(E->C)
Edit query	Alt+(E->E)
Delete query	Alt+(E->D)
Run query	Alt+(E->R)
Refresh query list	Alt+(E->R)
Managing reports	
Create report	Alt+(E->R)
Create folder	Alt+(E->F)
Edit report	Alt+(E->E)
Delete report	Alt+(E->D)
Build report	Alt+(E->U)
Rebuild report	Alt+(E->B)

Managing objects	
Assign *No Violation* decision	Alt+(E->O->N)
Assign *Violation* decision	Alt+(E->O->V)
Change responsibility zone	Alt+(E->O->H)
Add description	Alt+(E->O->A)
Send e-mail report	Alt+(E->O->O)
Download XML context	Alt+(E->O->S)
View content	Alt+(E->O->W)
Managing configuration versions	
Delete version	Alt+(E->D)
Rollback to selected version	Alt+(E->R)
Open configuration	Alt+(E->C)
Compare two versions	Alt+(E->P)
Upload editable configuration to database: make it active	Alt+(E->A)
Managing categories and terms	
Import from file	Alt+(E->I)
Edit categories and terms	Alt+(E->E)
Delete categories and terms	Alt+(E->D)
Managing scripts	
Activate	Alt+(E->A)
Upload from file	Alt+(E->L)

3.3 Refreshing Data in Management Console

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

The data related to a specific Management Console section is **refreshed automatically** when you go to this section. You can set up automatic refresh of intercepted objects data.

You can also update data **manually** in each section of the Management Console. When handling queries, you can update both data and lists of queries.

To manually refresh the data:

Necessary action	Performance orde
To refresh the data in the section	Do the following: • in the main menu, **select View > Refresh**; • click **Refresh** on the **Objects** pane.
To refresh query list on the **Queries** pane	click **Refresh** on the **Queries** pane

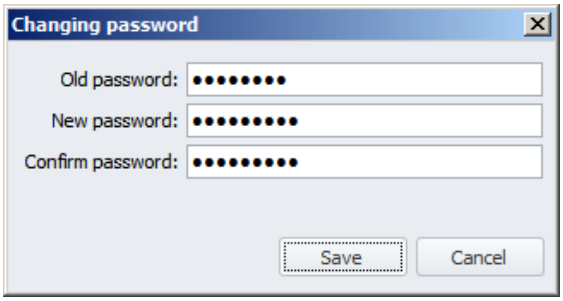
3.4 Changing the User's Password

You can change the password of your Management Console account using this feature.

To change your password:

1. In the main menu, select **Tools > Change Password**.

   The **Change Password** dialog box will appear on the screen.



Changing the user's password

2. In the dialog box that appears please specify the following settings:

Setting	Description
Old password	Current password
New Password **Confirm password**	The password that will be assigned to your account

Note

For detailed password recommendations see "User name and password recommendations".

3. Click **Save**.

4 Management Console Administration

The following administrative tasks are provided for the Management Console users:

- Management Console Access Control
- Configuring Sending/Receiving Reports on Objects
- Configuring the Violation Notifications
- Configuring a Query on Exit from the Management Console
- Working with Hosts
- Viewing the Database Usage Statistics

See also "Responsibility Zones"

4.1 Management Console Access Control

The set of privileges that is assigned to a user defines his ability to carry out different actions in Management Console. Users receive the privileges as a part of roles. Each user (except for the user administrator) can be assigned one or several roles. The user with no assigned role or privileges, can only change his/her password.

To give the user an opportunity to work with Management Console, it's necessary to create an account for this user and assign a role with the necessary privileges.

Important!

In Management Console it's possible to restrict access to the personal information stored in the intercepted objects (data on recipients, message texts, attachments etc.). Fore more details see "Controlling the Access to the Objects Content".

You can view the roles and user accounts in the **Roles** and **Users** sections (the **Administration** area on the **Navigation** pane).

The Management Console is initially configured using the account of the user administrator. The user administrator account is associated with the predefined role of *Administrator*. This role supports just a limited scope of tasks, specifically:

- role management (viewing, creating, editing and deleting);
- user account management (viewing, creating, editing, locking/unlocking and deleting);
- responsibility zone management (viewing, creating, editing, deleting).

There is also a predefined *Officer* account associated with the predefined *Officer* role having all the privileges except administrative ones (see "Privilege List").

For more information about Management Console access control see following sections:

- Management Console User Roles
- Controlling the Access to the Objects Content
- Management Console Accounts

4.1.1 Management Console User Roles

User role is a complex of privileges defining a set of actions user can perform during System usage.

There are two preset user roles:

- **Administrator** has privileges for initial configuring Management Console accounts.
- **Security officer** has all privileges except managing users and roles.

You can view and modify user roles in the **Roles** section (the **Administration** area on the **Navigation** pane).

Detailed information on user roles management:

- Privilege List
- Creating and Editing a Role
- Deleting a Role

4.1.1.1 Privilege List

The following table contains the list of privileges that can be assigned to a role. Some privileges can be available only if any other privileges have already been assigned (specified in the *Necessary additional privileges* column). The features that may be available only if a corresponding privilege has been assigned, are specified in the *Dependent features* column.

Privilege	Dependent features
Global Settings: editing warnings concerning the viewing modes	Changing the warning message to be displayed when viewing object content Changing the warning message displayed in the "Show object content" mode
Global Settings: configuring the Active Directory connection settings	Configuring the Active Directory connection settings and synchronization schedule
Global Settings: configuring the Crawler server connection settings	Connection of Management Console with Crawler Sever
User Settings: edit	Setting the size limits for downloaded SMTP messages Enabling the "Show object content" mode
Users: view	Viewing the user accounts list
Users: edit	Adding / editing user account Locking/unlocking user accounts
Users: delete	Deleting a user account
Roles: view	Viewing the roles list
Roles: edit	Adding / editing roles

Privilege	Dependent features
Roles: delete	Deleting a role
Configuration: view	Viewing the configuration information Comparing configuration versions
Configuration: delete	Deleting a configuration version
Configuration: rollback	Rolling back to a previous configuration version
Configuration: give note	Adding / editing comments
Configuration: transmit	Loading a configuration to a host
Lists: view	Viewing the lists Viewing list items
Lists: edit	Adding list groups Adding a list Editing the list / list group / list item settings Adding a list item
Lists: delete	Deleting a list Deleting a list item
Content base: view	Classification view Viewing the terms list Searching for a term
Content base: edit	Adding a category Editing categories Changing category level Adding a term Import terms from a file Editing terms Moving a term between categories Exporting / importing a Classification
Content base: delete	Deleting a category Deleting a term
Script: view	Viewing the scripts list
Script: edit	Adding a script Export / Importing a script Editing a script Activating a Script

Privilege	Dependent features
Script: delete	Deleting a script
Color: view	Viewing colors
Color: edit	Adding / editing colors
Color: delete	Deleting a color
Tags: view	Viewing tags / tag groups
Tags: edit	Adding tag groups Editing the tag group settings Adding a tag Editing a tag
Tags: delete	Deleting a tag / tag group
Database Usage: view	Viewing the database usage statistics
Responsibility Zones: view	Viewing responsibility zones
Responsibility Zones: edit	Adding / editing responsibility zones
Responsibility Zones: delete	Deleting a responsibility zone
Hosts: view	Viewing the host details Viewing the host profile
Hosts: edit	Adding comments to the host
Hosts: delete	Deleting a host
Objects: run Queries	Viewing the query results in the objects list Using queries Configuring the Object Info pane
Objects: edit Queries	Adding the queries folder Editing the query folder ("Creating and editing a folder" and "Moving queries and reports between folders") Copying a query folder Adding / editing queries Copying queries
Objects: delete Queries	Deleting a query folder Deleting a query
Objects: tag operations	Assigning tags to an object

Privilege	Dependent features
Objects: verdict operations	Making the decision about an object
Objects: commen	Adding a comment to an object
Objects: responsibility zone operations	Moving object to another responsibility zone
Objects: report	Generating and sending reports
Objects: color	Highlighting objects with color
Objects: view content	Enabling the "Show object content" mode Viewing the object content in the Object Info pane (if the the "*Show object content*" mode is disabled) Viewing object attributes in the detailed view Viewing the object log Downloading attachments Saving SMTP message Downloading context
Reports: run	Running reports Rebuilding the report
Reports: edit	Adding the reports folder Editing the report folder ("Creating and editing a folder" and "Moving queries and reports between folders") Copying a report folder Adding / editing reports Copying a report
Reports: delete	Deleting a report folder Deleting a report
Text objects: view	Viewing text objects
Text objects: edit	Editing the text objects settings
Sample documents: view	Viewing the sample documents list
Sample documents: edit	Adding sample documents and creating digital fingerprints Editing sample document information
Sample documents: delete	Deleting a sample document
Active Directory integration: view	Viewing and Filtering Persons Entrys Viewing and Filtering Workstations Entries

Privilege	Dependent features
Active Directory integration: edit	Configuring connection and synchronization with Active Directory Editing descriptions of persons, workstations and groups imported from Active Directory ("Creating and editing a person record", "Editing a workstation entry", " Creating, viewing, and editing a group") Creating / editing / deleting / restoring person records and Traffic Monitor group records ("Persons Directory", "Groups directory") Creating / changing the contact information Loading the Active Directory directories to the server
Crawler: edit	Parameters of Crawler Scanner Creation and Editing the Task for Scanning Deleting the Task for Scanning Execution and Stopping of the Task Hash Base Cleaning

4.1.1.2 Creating and Editing a Role

Important!

The change of user privileges or roles shall apply only at the time of the next authorization of the user in the system.

Note

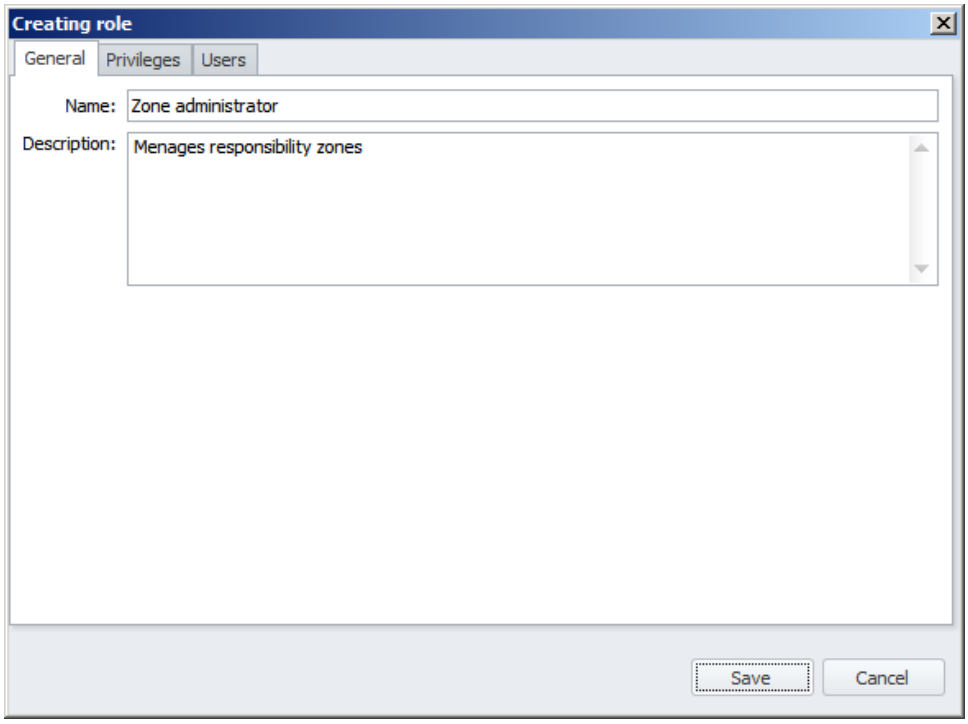
The predefined *Administrator* role cannot be edited.

To create or edit a role:

1. Go to the **Roles** section.
2. Do the following:

Action	Procedure
Create a role	Do one of the following: • in the main menu, select **Edit > New role** • click **New Role** on the toolbar
Edit the role	1. In the roles list select the row with the required role. 2. Do one of the following: • in the main menu, select **Edit > Edit**; • click **Edit** on the toolbar; • double-click the selected row.

The dialog box with the role settings will appear.



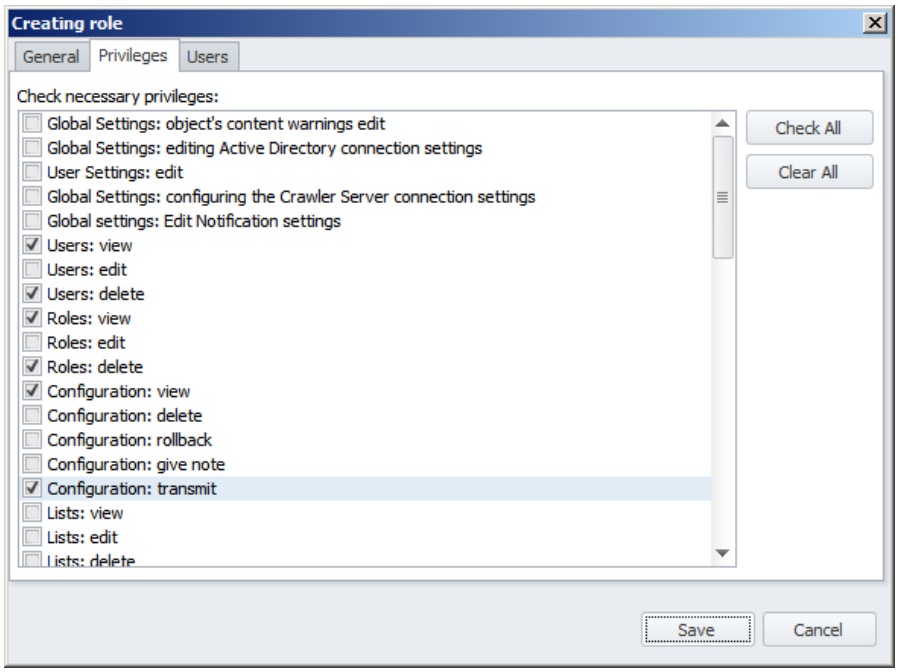
Configuring general settings for a role

3. Configure the general role settings on the **General** tab:

   - **Name**. Role name (mandatory). The name should be unique.
   - **Description**. Additional information.

4. Check all the privileges to be assigned to the role on the **Privileges** tab. To select or clear all the check boxes, use the **Check All** and **Clear All** buttons.

> **Important!**
>
> Some privileges may only be available in combination with other privileges. Assignment of such dependent privileges will automatically set the privileges on which they depend: for example, when choosing the "*Tags: edit"* privilege, the role is also assigned with *"Tags: view*" privilege.
>
> For the complete list of privileges see the section "Privilege list".

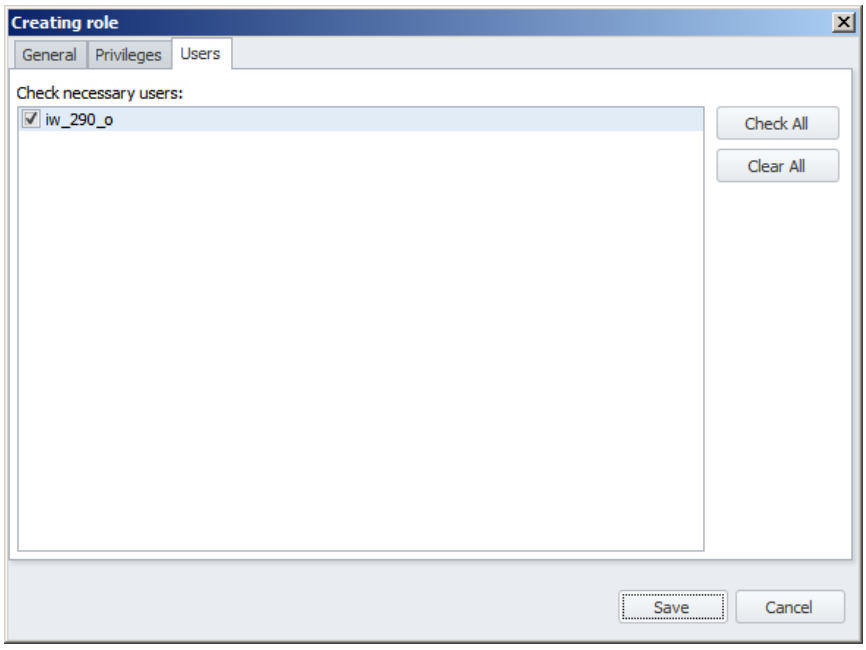


Assigning privileges to a role

5. Check all the accounts to which the role will be assigned on the **Users** tab. To select or clear all the check boxes, use the **Check All** and **Clear All** buttons.

Important!

You can also assign roles when creating and editing user accounts (see "Creating and editing a user account").



Assigning roles to users

6. Click **Save**.

4.1.1.3 Deleting a Role

Important!

The predefined *Administrator* role cannot be deleted.

A role assigned to at least one user cannot be deleted.

To delete a role:

1. Go to the **Roles** section.
2. In the roles list select the row with the required role.
3. Do one of the following:
   - in the main menu, select **Edit > Delete**;
   - click **Delete** on the toolbar.
4. In the confirmation box, click **Yes** to confirm.

4.1.2 Controlling the Access to the Objects Content

Every object intercepted by the System contains the content and the service data. The service data is defined as non-personal. The content of the object (text, attachments and some properties such as list of recipients, subject etc.) can include personal data. "General Object Attributes" and "Envelope Headers and Object Headers" sections contain the lists of service attributes and content attributes.

The information about objects, including the contents of an object, is displayed in queries and reports. The access to the object content is granted only to the users of the role with the *Objects: view content*privilege. For the rest of the users the object content is not displayed in queries and reports.

To grant the user the right to view the content:

1. In the **Roles** section, select the user role.
2. Do one of the following:
   - in the main menu, select **Edit > Edit**;
   - click **Edit** on the toolbar
   - double-click the selected row.
3. In the **Editing Role** dialog box, go to the **Privileges** tab and select the *Objects: view content* checkbox.
4. Click **Save**.

Important!

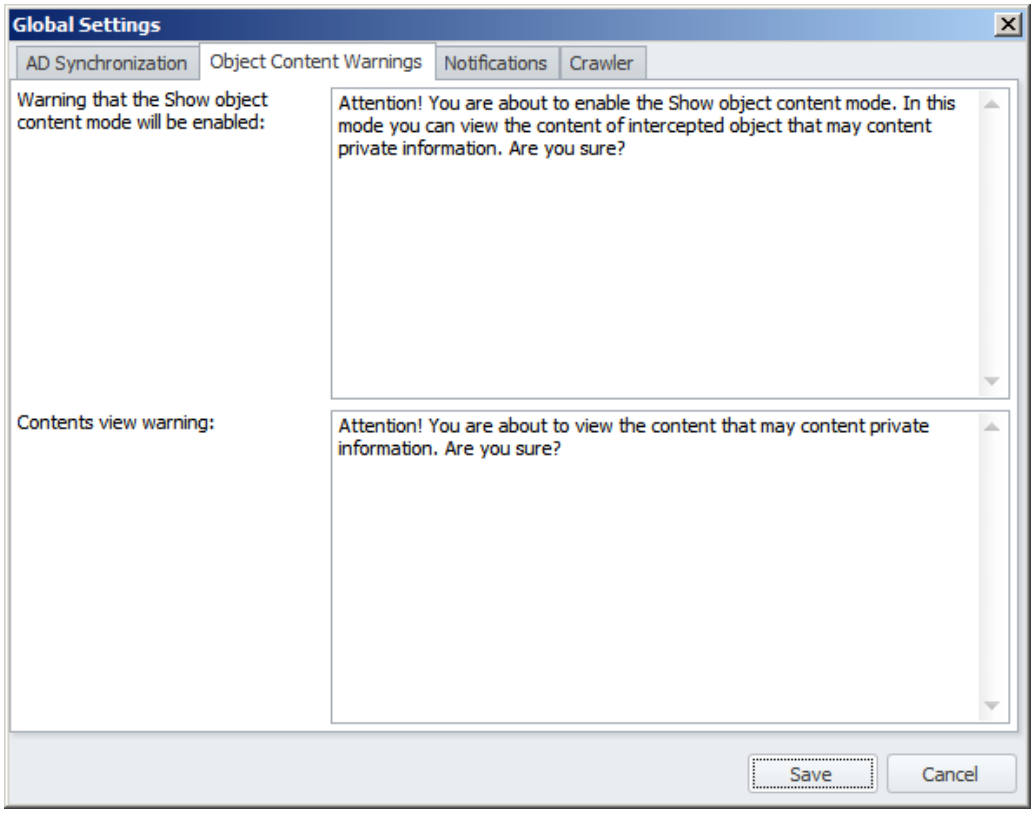
The changes will take effect only after the next authorization of the user in the system.
When changing the role privileges please make sure that this role is assigned to only those users who have the right to view personal data.

By default, the content of an object cannot be viewed even by the users who have access to this content. It's required to run the *Show content* command or to enable the content display mode (see "Configuring the Object Content Preview Mode"). A warning is displayed after running the *Show content* command and enabling the content

display mode. The texts of the warning messages can be edited.

To change the warning text:

1. In the main menu, select **Tools > Global Settings**.
2. In the **Global settings** dialog box go to the **Object Content Warnings** tab and edit the texts of the messages:
   - **Warning that the Show Object Content mode will be enabled**. This notification is displayed when the user changes the view mode.
   - **Contents view warning**. This warning is displayed when the user who works with an object runs the **Show Content** command.



Configuring the object content viewing warnings

3. Click **Save**.

4.1.3 Management Console Accounts

The Management Console user accounts are managed using the following administration tasks:

- Creating and Editing a User Account
- Locking/Unlocking a User Account
- Deleting a User Account

This section also contains user name and password recommendations

4.1.3.1 User Name and Password Recommendations

General recommendations

The user name should be 1-10 characters long. The user name may include English letters, digits and underscore "_". It should start with a letter.

Rules for passwords:

- The user password may include English letters, digits, and also the following characters:
  ! ? # $ % ^ * ( ) _ + - < > , . | \ ; : ~ ` ' [ ] { }
- The password may start with a letter, a digit or character. maximum length is 30 characters long
- Do not start user names or passwords with these combinations: SYS_ and ORA_.

Do not use Oracle reserved words in usernames or passwords:

ACCESS	EXCLUSIVE	MODE	SELECT
ADD	EXISTS	MODIFY	SESSION
ALL	FILE	NOAUDIT	SET
ALTER	FLOAT	NOCOMPRESS	SHARE
AND	FOR	NOT	SIZE
ANY	FROM	NOWAIT	SMALLINT
AS	GRANT	NULL	START
ASC	GROUP	NUMBER	SUCCESSFUL
AUDITBETWEEN	HAVING	OF	SYNONYM
BY	IDENTIFIED	OFFLINE	SYSDATE
CHAR	IMMEDIATE	ON	TABLE
CHECK	IN	ONLINE	THEN
CLUSTER	INCREMENT	OPTION	TO
COLUMN	INDEX	OR	TRIGGER
COMMENT	INITIAL	ORDER	UID
COMPRESS	INSERT	PCTFREE	UNION
CONNECT	INTEGER	PRIOR	UNIQUE
CREATE	INTERSECT	PRIVILEGES	UPDATE
CURRENT	INTO	PUBLIC	USER
DATE	IS	RAW	VALIDATE
DECIMAL	LEVEL	RENAME	VALUES
DEFAULT	LIKE	RESOURCE	VARCHAR
DELETE	LOCK	REVOKE	VARCHAR2
DESC	LONG	ROW	VIEW
DISTINCT	MAXEXTENTS	ROWID	WHENEVER
DROP	MINUS	ROWNUM	WHERE
ELSE	MLSLABEL	ROWS	WITH

Strong password recommendations

Recommended password length: from 10 to 30 characters.

The password must contain both letters, digits and characters.

It is not advised to:

- Include whole words or phrases into a password.
- Use a username in a password (even written backward)
- Use a series of the same character.
- Start and end the password with the same character.
- Create a new password by adding characters to your current password.

4.1.3.2 Creating and Editing a User Account

Important!

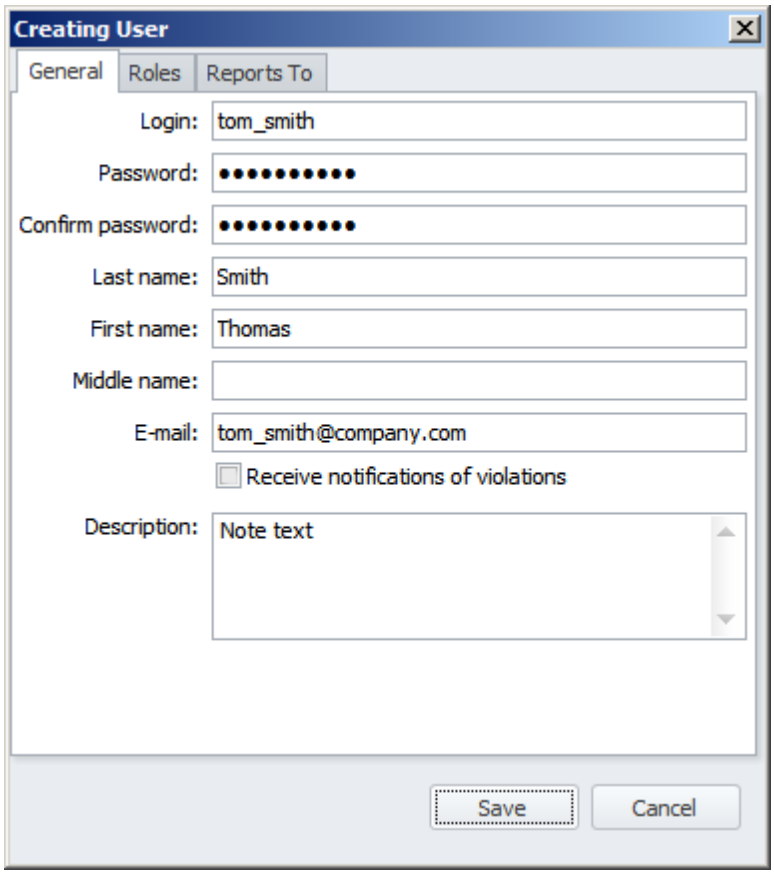
The changes associated with the change of the privileges or roles assigned to the user authorized in the system, shall apply only during the next authorization of the user in the system.

To create or edit a user account:

1. Go to the **Users** section.
2. Do the following:

Action	Procedure
Create a user account	Do one of the following: • In the main menu, select **Edit > New User** • click **New User** on the toolbar
Edit the user account	1. In the user accounts list, select the row with the account you want to edit. 2. Do one of the following: • in the main menu, select **Edit > Edit**; • click **Edit** on the toolbar; • double-click the selected row.

The dialog box with the user account options will appear.



User account (general settings).

3. Configure the general account settings on the **General** tab:

   - **Login**. User account name (mandatory). The name may include English letters, digits, and underscores; it must start from a letter. The name should be unique.
   - **Password**, **Confirm password**. User's password (mandatory).

     Note

     For the detailed user name and password recommendations see "User name and password recommendations".

   - **Last Name**, **First Name**, **Middle name**. User's personal data.
   - **E-mail**. This field is filled only for those users whose tasks include sending/receiving reports (for more details on configuring the report delivery system see "Configuring sending/receiving reports on objects").
   - **Receive notifications of violations** . If security officer must receive an e-mail notifications, that System detected a violation.
   - **Description**. Additional information concerning the user account.

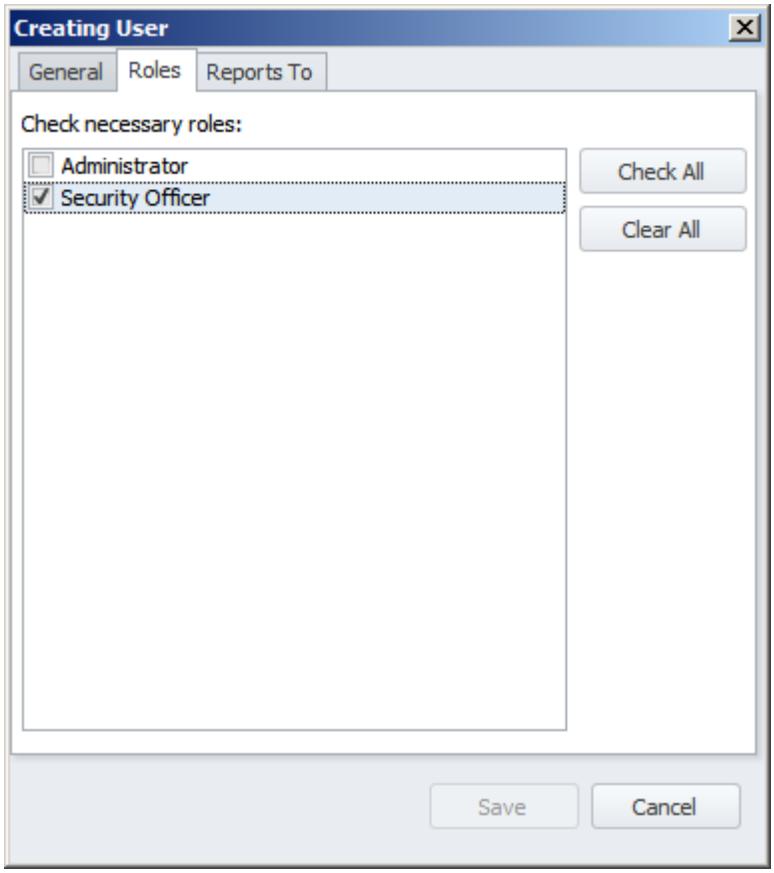
4. Check the roles to be assigned to the user account on **Roles** tab. To select or to clear all the check boxes, use the **Check All** and **Clear All** buttons.

Note

You can also assign the user a certain role when creating/editing roles (see "Creating and editing a role ").

Important!

The user with no assigned role or privileges, can only change his/her password.
When several roles are assigned, their privileges are combined. Consequently, the user will enjoy all privileges of these roles.

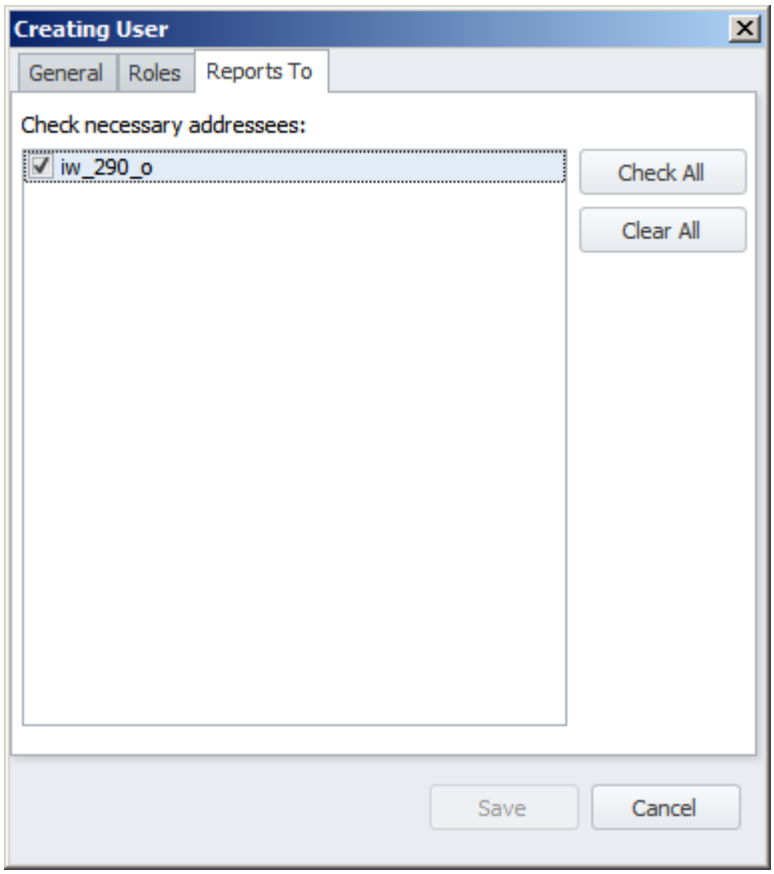


Assigning roles to a user account

5. If the user should send reports on objects (see "Sending a report on an object"), select the recipients of the user's reports. To select or clear all the check boxes, use the **Check All** and **Clear All** buttons.

Important!

The reports will be delivered using the mail server specified in the **User settings** window (see " Configuring the mail server for sending reports").



Selecting report recipients

6. Click **Save**.

4.1.3.3 Locking/Unlocking a User Account

An account can be *Active* or *Locked*. This account status defines whether the user can use the system. The user with a locked account cannot log into the system even if he has the necessary rights.

Important!

If the account status (active/locked) is changed, the new status will apply only at the next logon of the user.

To change the status of a user account:

1. Go to the **Users** section.
2. In the user accounts list select the row with the account you want to edit.
3. Do one of the following:
   - To lock the account, in the main menu, select **Edit > Lock**. Or click **Lock** on the toolbar.

     After that, the user account will become *Locked*.
   - To unlock the account, in the main menu, select **Edit > Unlock**. Or click **Unlock** on the toolbar.

     After that, the user account will become *Active*.

4.1.3.4 Deleting a User Account

You can delete any account with the exception of the user administrator's account and the account you are currently using to log in.

Important!

If the System contains queries or reports that are assigned to the user that is being deleted, then deleting such user account will result in deleting those queries and reports. Before deleting such a user account the System will give an appropriate warning.

It is advised, therefore, to log in to the System using the user account you want to delete (see "Running the Management Console and Connecting to the Database Server"), then change the access rights for the reports (see "Creating and Editing a Report") or queries (see "Setting Permissions for Handling a Query") accessible only by this user.

Before deleting a user account, you should close all active connections to the database (including the ones opened not using Management Console).

To delete a user account:

1. Go to the **Users** section.
2. In the user accounts list select the row with the required account.
3. Do one of the following:
   - in the main menu, select **Edit > Delete**;
   - click **Delete** on the toolbar.
4. In the confirmation box, click **Yes** to confirm.

4.2 Configuring Sending/Receiving Reports on Objects

If you want the users to be able to send and receive reports on objects (for more details see "Sending an Object Report"), configure the following:

1. Specify the mail server for sending reports ("Configuring the Mail Server for Sending Reports").
2. Configure the accounts of the users who can receive reports. In the user account settings, specify an e-mail address to which the report will be delivered
3. Configure the user accounts that will send the reports as follows:
   - Specify an e-mail address that will be used for sending the report.
   - Assign the user a role with the following required privileges: *Objects: starting queries (*and/or *Objects: Run Queries), Objects: report*.
   - Select recipients of the report.

For more information about creating and editing accounts see "Creating and Editing a User Account".

For more information about creating and editing roles see "Creating and Editing a Role"

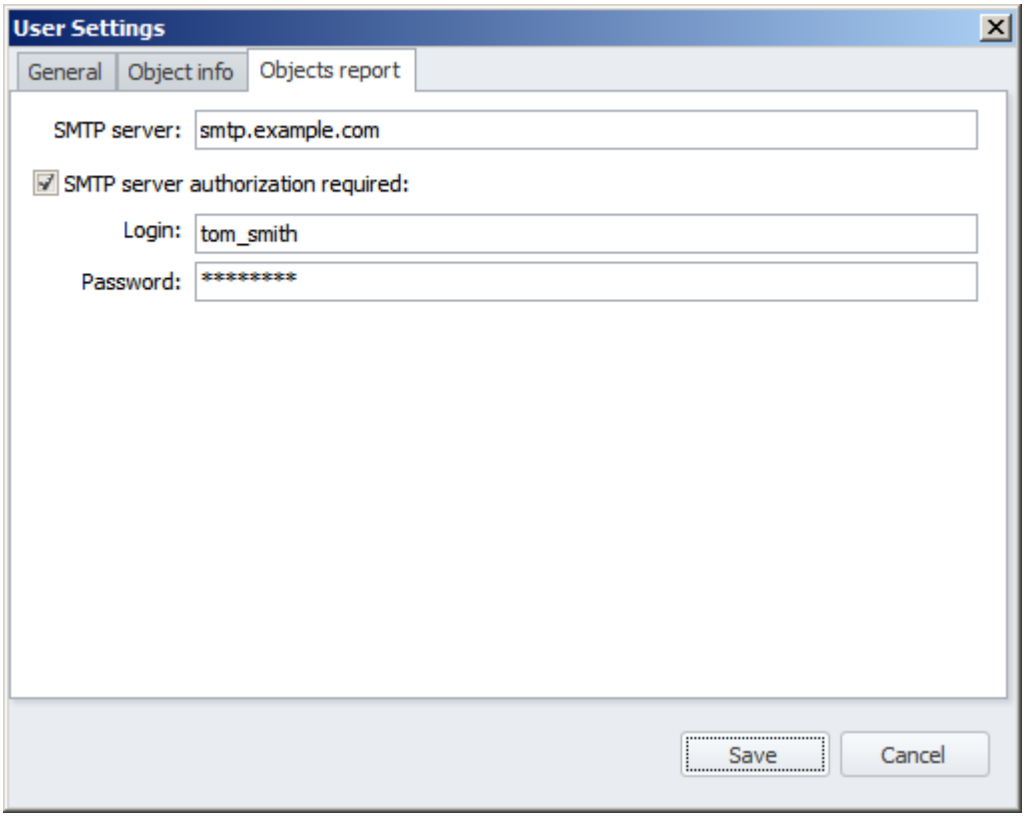
Note

You must change the settings of the operating system on the computer that will be used for sending reports. To do that, open the **Control Panel** (**Start** > **Settings** > **Control Panel**). Select **Regional and Language Options**. In the dialog box that appears, go to the **Advanced** tab and select the language of reports for non-Unicode software.

4.2.1 Configuring the Mail Server for Sending Reports

To specify a mail server for delivering reports to recipients:

1. In the main menu, select **Tools > User Settings**.
2. In the **User Settings** dialog box, on the **Objects report** tab configure the server settings:



Configuring the mail server for sending reports

- in the **SMTP Server** field please specify the domain name or the IP address of the mail server for sending the reports;

  Important!

  If the setting is not specified, then the reports won't be delivered.

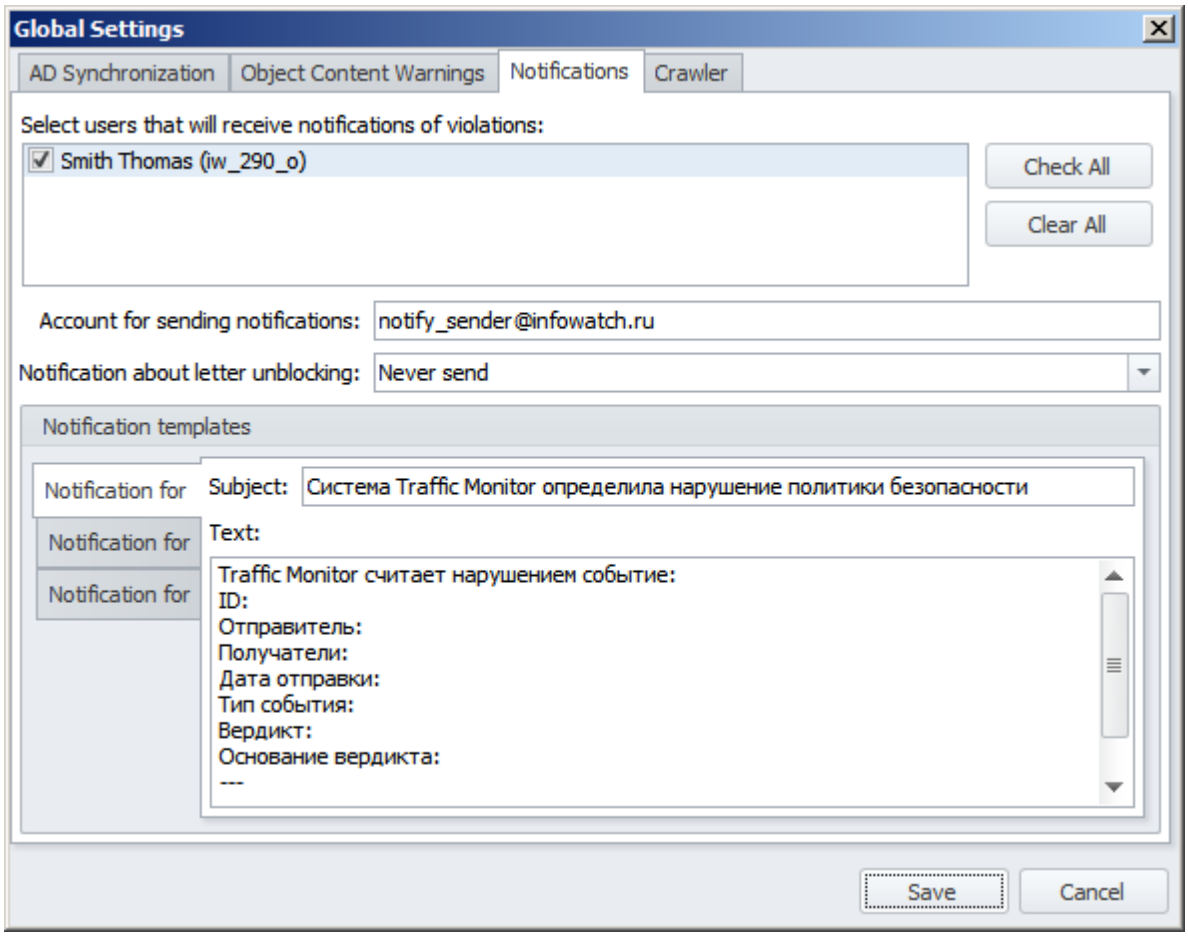
- If your mail server requires password authentication, then select the **SMTP server authorization required** checkbox and specify the credentials in the **Login** and **Password** fields.

3. Click **Save**.

4.3 Configuring the Violation Notifications

The System can automatically send e-mail notifications that the object recognized as potential violation of a security policy is intercepted. Also the System can automatically send e-mail notifications that the object (SMTP letter) which was recognized as potential violation and blocked previously, is allowed for sending (*No violations* decision) .

You can configure these settings using command **Tools > Global settings**, on the **Notifications** tab.



Configuring the violation notifications

You can define the following notifications using this dialog box:

- **Notification for the security officer** – e-mail with data on the intercepted object which has violated a security policy. Define the list of security officers (users of the Traffic Monitor Management Console), who will receive these notices. The **Receive notifications of violations** control has to be checked in parameters of officer's account (see "Creating and Editing a User Account") .
  You can define if a object should initialize the notification, using the `SendNotificationUser` function (see "Sending Notice to Security Officer").
- **Notification for the violator** – e-mail to the user (employee) who has sent object who was recognized as a potential violation of security policy. You can define if a object should initialize the notification, using the `SendNotificationEmployee` function (see "Sending Notice to Violator").
- **Notification for the employee** – if the user (employee) sent the SMTP object which was recognized as potential violation of a security policy and was blocked by system (*Normal* transport mode), the security officer can allow it to sending (see "Making the Decision about an Object", with the decision *No violations*

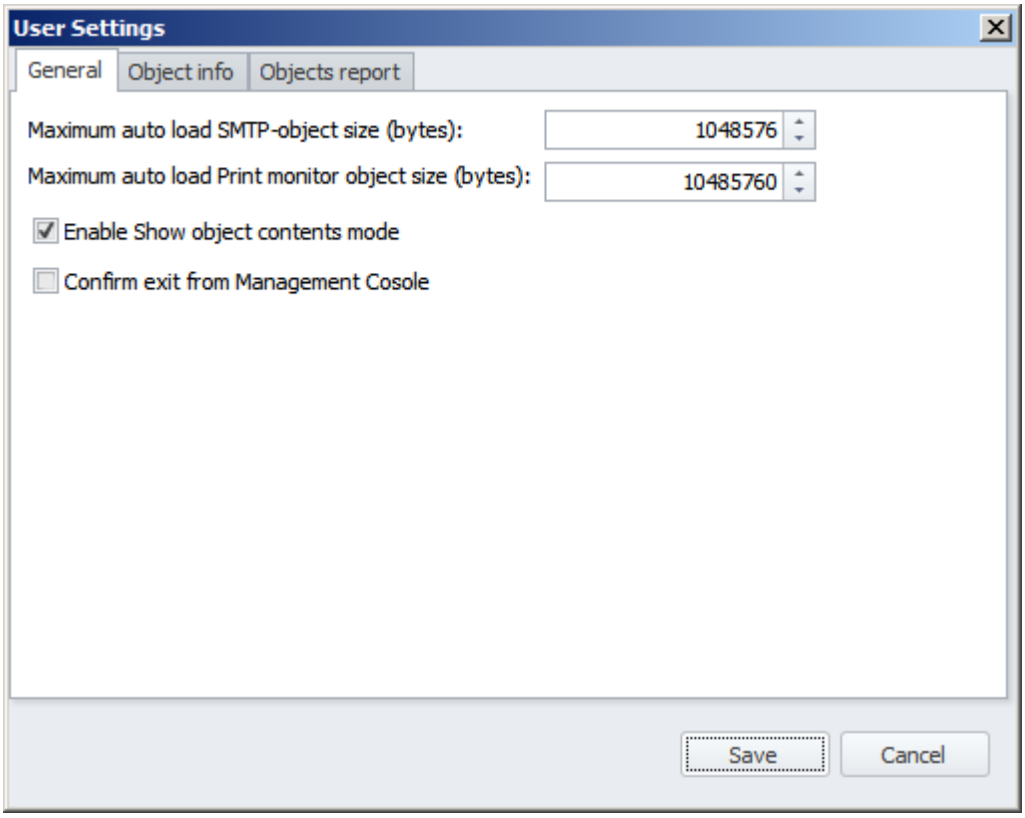
). In this case the blocked object will be complimentarily sent and employee receives a notification containing specified text.

4.4 Configuring a Query on Exit from the Management Console

To avoid closing the Management Console by accident, you can set up a confirmation.

To configure the confirmation:

1. In the main menu, select **Tools > User Settings**.
2. In the **User Settings** dialog box on the **General** tab, select **Confirm exit from Management Console**.



Configuring a Query on exit from the Management Console

3. Click **Save**.

4.5 Working with Hosts

A host is a Traffic Monitor Server computer.

Each host has a profile based upon the settings corresponding to the performed tasks. The following host settings are supported:

Hosts setting	Host tasks
Categories and terms	Search for Classification terms (words and phrases) in the object text (see "Classification"): • retrieving the current Classification from the database when the configuration is uploaded to the host (see "Uploading Configuration to the Hosts"); • receiving the information about the objects from hosts with the **Scripts** setting; • searching for terms in the object text; • transferring information about the found terms and categories to the host with the **Scripts** setting.
Text objects	Searching for structured data according to the specified patterns (passport numbers, credit card numbers, phone numbers etc.) in the object text (see "Text Objects"): • retrieving the current patterns of the text objects from the database when the configuration is uploaded to the host (see "Uploading Configuration to the Hosts"); • receiving the information about the objects from hosts with the **Scripts** setting; • searching for text objects based on patterns; • transferring information about the found matches to the host with the **Scripts** setting.
Lists	Searching for list items in the object text (see "Lists"): • retrieving the current lists from the database when the configuration is uploaded to the host (see "Uploading Configuration to the Hosts"); • receiving the information about the objects from hosts with the **Scripts** setting; • searching for list items in the object text; • transferring information about the found lists to the host with the **Scripts** setting.
Scripts	Processing of the intercepted objects according to the active script of objects processing: • retrieving the current user script from the database when the configuration is uploaded to the host (see "Uploading Configuration to the Hosts"); • processing intercepted objects according to the rules specified in the active script; • transferring information about object senders and recipients to the host with the **Active Directory** setting; • if content analysis is required, forwarding to the content analysis hosts (**Categories and Terms**, **Text Objects**, and **Sample Documents**) the information about the objects and the items to be found; • obtaining results of content analysis, sender and recipient data analysis; • assignment attributes to objects (verdict, verdict reason, colors, etc.) according to the conditions of the active script; • transferring the analysis results to the database. **Note:** Blocking or delivering objects according to the verdicts doesn't depend on the host profile and is defined by the Traffic Monitor Server administrator according to "*InfoWatch Traffic Monitor. Administration Guide*".
Directory Status	Searching for person and workstations data in the object attributes ("Persons and Workstations Directory"):

Hosts setting	Host tasks
	• retrieving the current information about persons and workstations directories from the database when the directories ("Uploading Directories to the Host") or the whole configuration is uploaded (see "Uploading Configuration to the Hosts"); • receiving the information about the objects from hosts with the **Scripts** setting; • processing data to find matches with the records in person and workstations directories; • transferring information about the found matches to the host with the **Scripts** setting. **Note:** Traffic Monitor Server is synchronized with Microsoft Active Directory regardless of the host profile. For more information see "Configuring Connection and Synchronization with Active Directory".
Sample documents	Searching for sample document quotes in the object text (see "Sample Document Database "): • retrieving the current lists from the database when the configuration is uploaded to the host (see "Uploading Configuration to the Hosts"); • receiving the information about the objects from hosts with the **Scripts** setting; • searching for quotes in the object text; • transferring information about the found quotes to the host with the **Scripts** setting.

The **Categories and Terms**, **Text objects** and **Sample Documents** settings may be assigned to a server only together. They provide the content analysis of the text that has been extracted from the intercepted objects.

The **Lists** and **Scripts** settings can be assigned to a server only together. These settings provide the object analysis and the ability to modify its attributes, and they provide a decision concerning the possible violation of the corporate security policy.

Traffic Monitor administrator defines list of hosts and its parameters as it is written in the document «*InfoWatch Traffic Monitor. Administration Guide*».

To work with hosts in Management Console, use the **Hosts** section (the **Administration** area in the **Navigation** pane). The user can only perform the following actions with hosts:

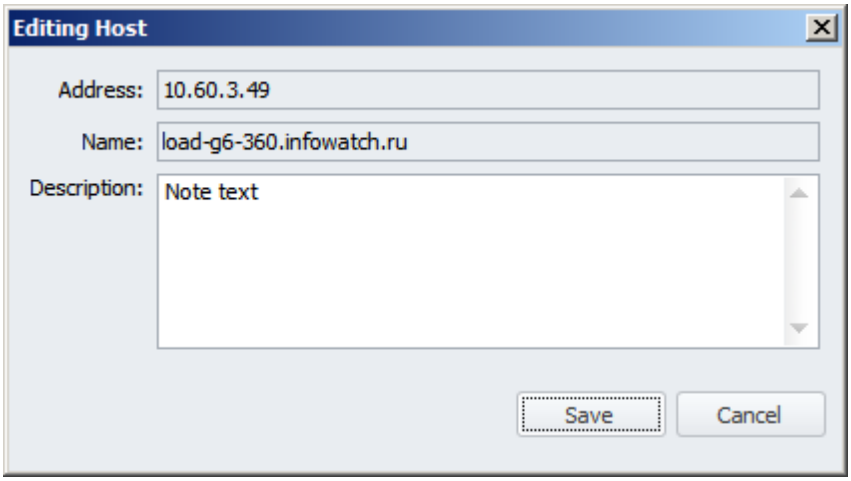
- Add a note to a host entry ("Adding comments to the host").
- Delete an inactive host entry from the list ("Deleting a host").

4.5.1 Adding Comments to the Host

To add or change the host comment:

1. Go to the **Hosts** section.
2. On the host pane, select the required host.
3. Do one of the following:
   - in the main menu, select **Edit > Edit Host**;
   - click  **Edit Host** on the toolbar.

The **Editing Host** dialog box will appear on the screen.



Adding comments to the host

4. Add the necessary information about the host in the **Description** field.
5. Click **Save**.

4.5.2 Deleting a Host

Online hosts have an **Active** status and are marked with ; if a host becomes offline, its status changes to **Inactive** and it is marked with . If the host is inactive you can delete the record on it from the list of hosts.

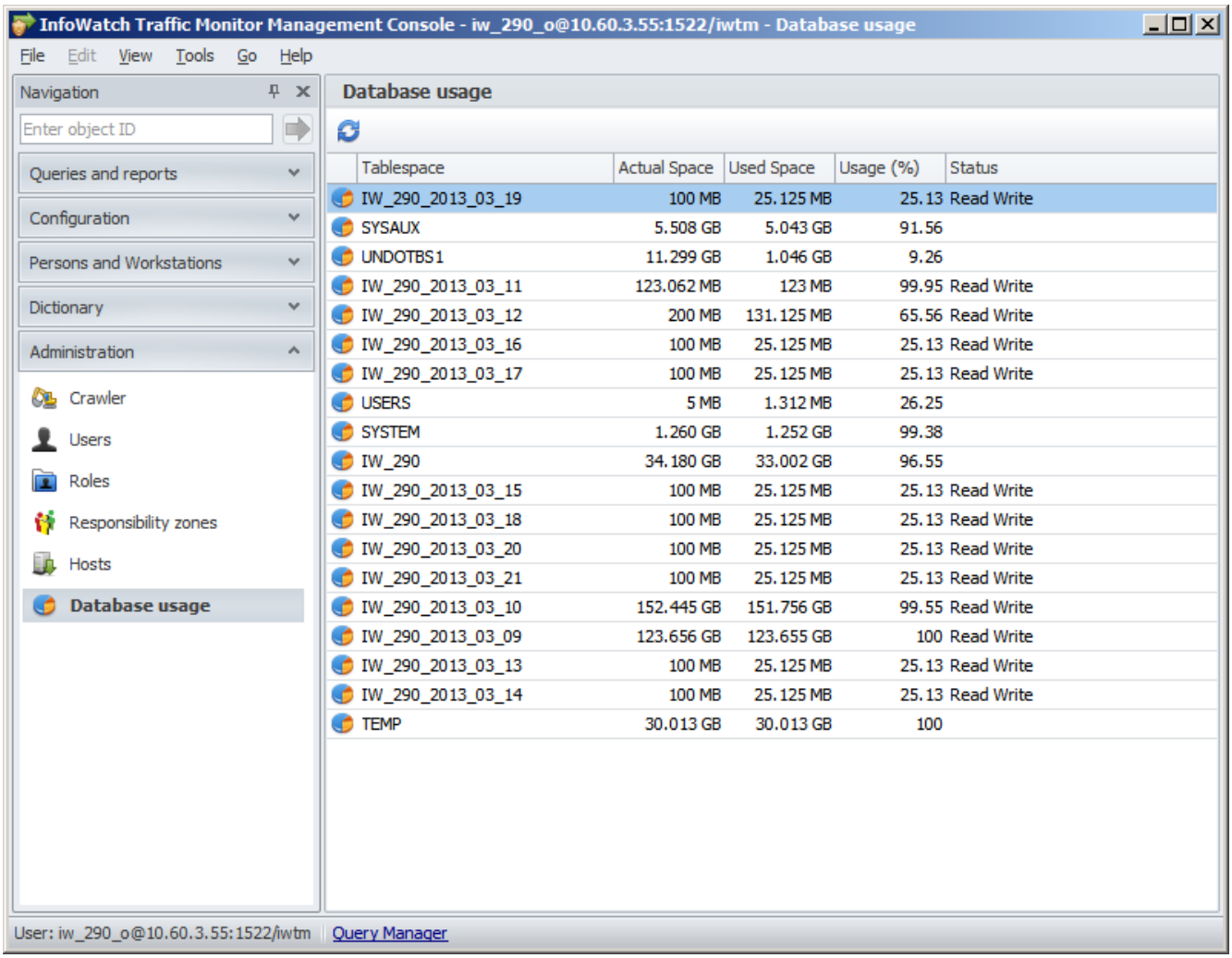
To delete a host:

1. Go to the **Hosts** section.
2. On the host pane, select the required host.
3. Do one of the following:
   - in the main menu, select **Edit > Delete Host**;
   - click  **Delete Host** on the toolbar.
4. In the confirmation box, click **Yes** to confirm.

When the connection to the host will be restored, it will automatically reappear in the list of hosts.

4.6 Viewing the Database Usage Statistics

You can view the information about using tablespaces in the **Database Usage** section (the **Queries & Reports** area on the **Navigation** pane).



Database Statistics

This section displays the information about the data in the Oracle tablespaces:

Attribute	Value
Tablespace	Tablespace name
Actual Space Limit	Current size of the the tablespace on the hard drive
Used Space	Current size of the the tablespace occupied by the data (in bytes). **Note:** The tablespace measurement units are defined by the settings and the version of Oracle DBMS. For more information see the Oracle DBMS documentation.

Attribute	Value
Usage (%)	Current portion of the the tablespace occupied by the data Percentage the actual space limit.
Status	Straus of the daily tablespace. Displayed only for daily tablespaces of the database schema being used.

5 Persons and Workstations Directory

Integration of the system with Active Directory makes easier for the user to work with the intercepted objects. This feature is based upon the information about senders and recipients as well as workstations using specialized directories. The system provides the following features:

- synchronization of the information in directories with the updated information imported from Active Directory;
- possibility to specify the additional person properties: contacts and description;
- ability to create groups of persons and workstations, as well as person records using Traffic Monitor;
- displaying the information about the sender, workstation, and recipient of the intercepted objects using the data from the directories;
- ability to work with the sender, workstation, and recipient data directly from the Object Info pane (for more details see "Processing the Sender, Recipient, and Workstation Data").

For more information about working with directories see the following sections:

- Configuring Connection and Synchronization with Active Directory
- Persons Directory
- Workstations Directory
- Groups Directory
- Uploading Directories to the Host

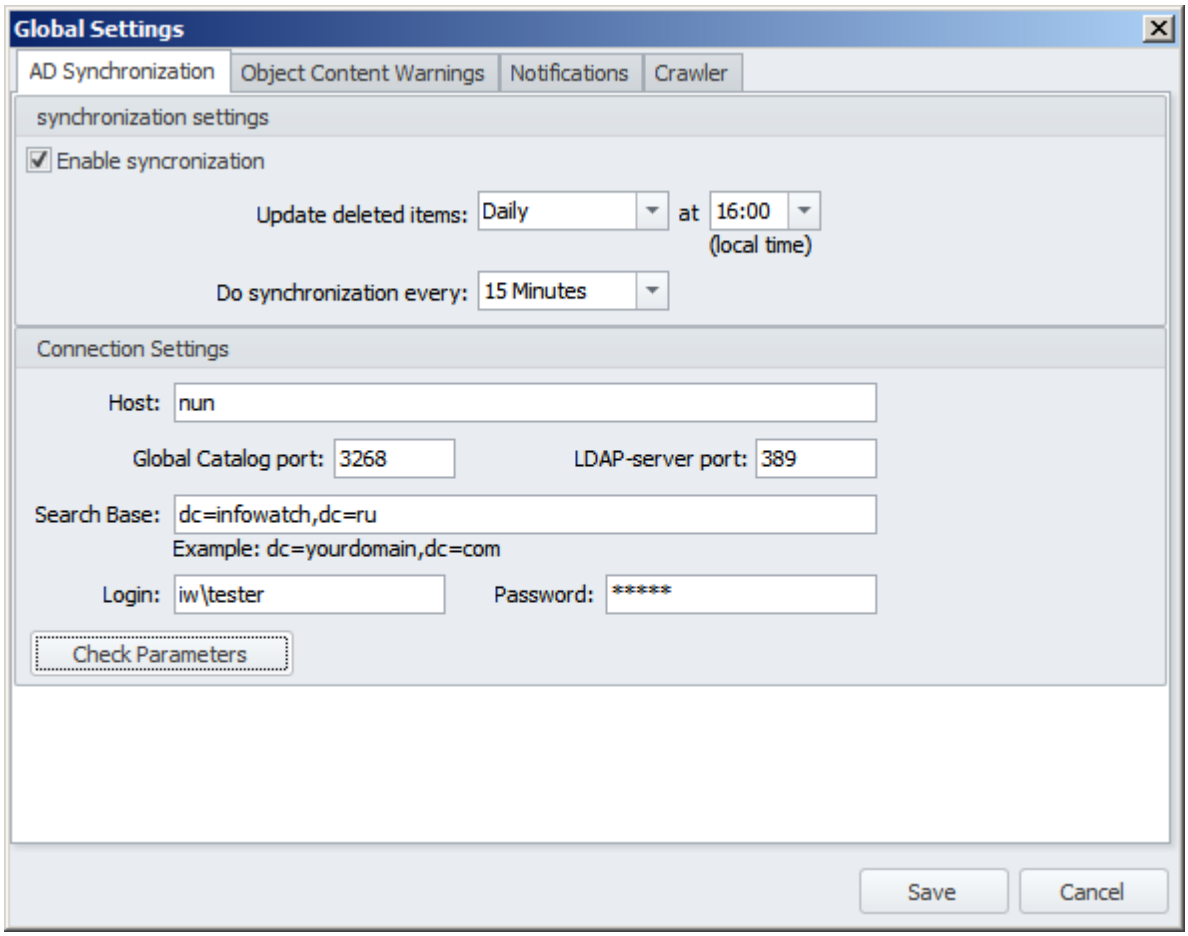
5.1 Configuring Connection and Synchronization with Active Directory

To retrieve data from Microsoft Active Directory, you have to specify the settings to connect to an AD server.

To set up the connection to Active Directory:

1. In the main menu, select **Tools > Global Settings**.

   The **Global Settings** dialog box will appear on the screen.



Configuring connection and synchronization with Active Directory

2. Specify the connection and synchronization settings on the **AD Synchronization** tab:

Setting	**Description**
Synchronization Settings	
Enable synchronization	Select this checkbox to automatically synchronize the directory records with Active Directory according to the schedule.
Update Remote Items	Please select how often do you want to get the updates about the deleted Active Directory items.
Do synchronization every	Select how often should the information about the added and changed Active Directory items should be updated.
Connection Settings	
Host	Name or IP-address of the Microsoft Active Directory server **Note**: To use the AD server name you must specify the DNS address of the Active Directory server in the connection settings. For more information about setting up see "InfoWatch Traffic Monitor. Administration Guide"

Setting	Description
Global Catalog port	The port for the search queries to Active Directory (default is `3268`).
LDAP-server port	The port for the LDAP search queries within the directory partition of one domain (default is `389`).
Search Base	The root domain (LDAP base) where the AD data search begins.
Login	User account used to connect to Microsoft Active Directory. It is specified in the `Domain\Login` format.
Password	The password of the user who connects to Microsoft Active Directory.

To check the connection settings, click **Check Settings**. If the Active Directory server is accessible, a confirmation message will appear. Otherwise, an error message will be displayed.

3. Click **Save**.

After the connection and synchronization settings are modified, the synchronization starts automatically. The synchronization gets the information about the added, modified, and deleted items, and updates the information about the deleted items.

The status of synchronization with AD and the uploading status are displayed in the status bar in the **Persons**, **Workstations**, and **Groups** sections. Below is a list of the possible synchronization and directory upload statuses.

Icon	Description of the synchronization status	Description of the directory upload status
	The last synchronization and deleted elements update has been completed successfully. Hover the mouse pointer to the icon to see the date and time of the following events: • Synchronization has completed successfully • Synchronization in progress • Deleted elements update has completed successfully • Deleted elements update in progress	The last directories upload has completed successfully. Hover the mouse pointer to the icon to display the date and time of the successful upload.
	Synchronization is disabled Updating deleted elements is disabled	Error while uploading directories to at least one host. Hover the mouse pointer to the icon to display the addresses of hosts with errors and the time of errors.
	Synchronization (updating deleted elements) failed Hover the mouse pointer to the icon to display the error message received from LDAP.	All hosts are offline (with the *Inactive* status). Fore more details see "Deleting a Host".
	Synchronization in progress (updating deleted	Uploading directories to the host in

Icon	Description of the synchronization status	Description of the directory upload status
	elements)	progress

Important!

If the time zone has been changed on the Management Console computer, then you have to restart Management Console in order to display the correct synchronization and actualization time, as well as before changing the schedule of synchronization and updating.

5.2 Persons Directory

To work with persons directory, use the **Persons** section (the **Persons and Workstations** area on the **Navigation** pane). The working area of the main window in this section is divided into two parts. The left part contains a list of persons, the right part is the display area to view the settings of the selected person.

The information about persons is imported automatically during synchronization with Active Directory (see " Configuring Connection and Synchronization with Active Directory").

If you have to use the information about a person that is not present in Active Directory, you may create a record using Traffic Monitor.

The records created using Traffic Monitor have less properties than the records imported from Active Directory: **Domain**, **Login**, **E-mail** and **AD Groups**. Mentioned parameters are imported from AD and cannot be edited using Traffic Monitor tools.

In the records imported from Active Directory, the **Status** property corresponds to the person's status in AD and may have the following values: *Active, Locked, Deleted*. In the records created using Traffic Monitor, the **Status** property can only have two values, *Active* or *Deleted*, and it can be changed by the user (see "Deleting and Restoring a Person Record").

Important!

When processing the intercepted objects, only the information about the users with the *Active* and *Locked* status is taken into account.

In all other respects the entries created using Traffic Monitor are similar to the entries imported from Active Directory.

For more details about working with the persons directory see the following sections:

- Creating and Editing a Person Record
- Deleting and Restoring a Person Record
- Viewing and Filtering Persons Entrys

5.2.1 Creating and Editing a Person Record

Note

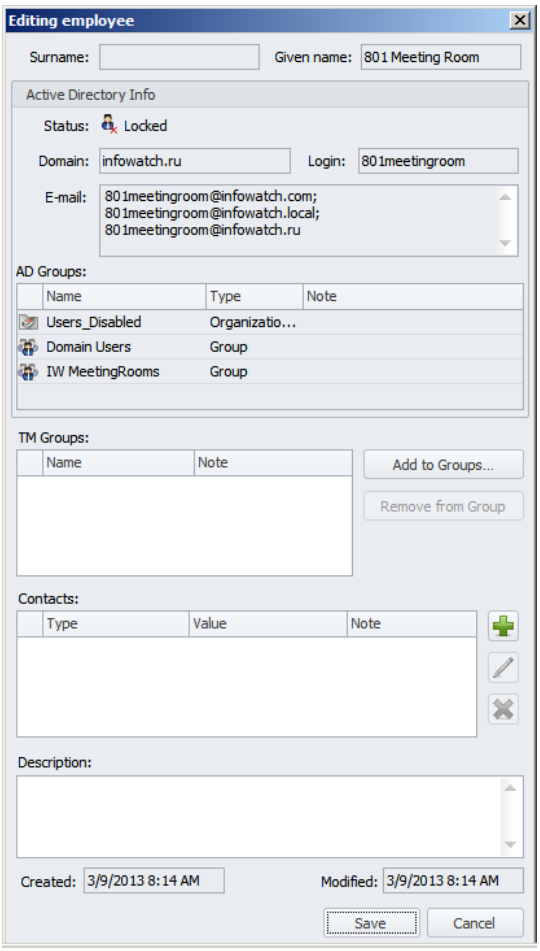
The persons directory cannot contain more than 4,194,304 entries.

To create or edit a person record:

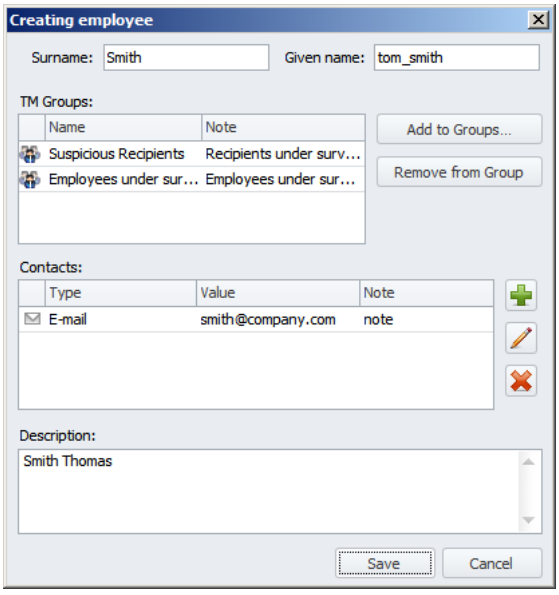
1. Go to the **Persons** section.
2. Do the following:

Action	Procedure
Create a person record	Do one of the following: • in the main menu, select **Edit > New** • click **New** on the toolbar
Edit a person record	1. On the **Persons** pane select the required person record. 2. Do one of the following: • in the main menu, select **Edit > Edit**; • click **Edit** on the toolbar; • click **Edit** in the settings pane of the selected person; • double-click the selected row.

The dialog box with the person settings will appear.



Editing a person record imported from Active Directory



Creating and editing a person record created using Traffic Monitor

3. Please specify the person record settings:

Setting	Description
Surname, **Given Name**	Last name and first name of the person. Can be changed only in records created using Traffic Monitor.
TM Groups	Traffic Monitor groups where the person is the member. • To add the person to a group, click **Add to Groups**. In the **Groups Selection** dialog box, select the required groups. To select or clear all the check boxes, use the **Check All** and **Clear All** buttons. Select the necessary groups and click **Save**. • To delete the person from the group select the necessary group and click **Delete from the group**. **Note:** For more information about creating TM groups see "Creating, Viewing, and Editing a Group".
Contacts	Contact details (e-mail address or ICQ number) of the person. • To add a contact, click **New**. In the dialog box that appears, specify the contact settings: – **Contact Type**. Select the contact type from the dropdown list: *E-mail*, *ICQ*, *Skype* or *Phone*. – **Value**. E-mail address, ICQ number, Skype or phone number according to the setting specified before. – **Description**. Additional information about the contact. Click **OK** after having specified the required settings. • To change a contact, select it in the list and click **Edit**. Configure the settings as described above and then click OK**.** • To delete a contact, select it in the list and click **Delete**.
Description	Additional information about the person

4. Click **Save** once the person settings are configured.

Important!

The new or updated information about a person is used by the system only after the directories are uploaded to the hosts (see"Uploading Directories to the Host").

Note

You can modify the person record while working with a group to which this person belongs. To do this select the required group name in the **Groups** and then on the group pane select the required row. Then take one of the following steps:

- in the main menu, select **Edit > TM Group Members > Edit**;

- click **Edit** on the group members pane
- double-click the selected person record.

The window and the procedure for editing a person record settings are alike those described above.

5.2.2 Deleting and Restoring a Person Record

You can delete a person record created using Traffic Monitor.

To delete the person entry:

1. Go to the **Persons** section.
2. Select the necessary record in the persons list.
3. Do one of the following:
   - right-click the record and choose **Delete**;
   - in the main menu, select **Edit > Delete**;
   - click **Delete** on the toolbar;
   - click **Delete** in the properties area of the selected person.

As a result, the person becomes *Deleted*. After the directory is uploaded to the hosts (see "Uploading Directories to the Host"), the information about this person won't be used by the system any longer.

If you need to reuse a deleted person record, you can restore it.

To restore a person record:

1. Go to the **Persons** section.

   Note

   To view the deleted records, on the **Person** pane select the **All** or **Deleted** filter.

2. Select the necessary record in the persons list.
3. Do one of the following:
   - right-click the record and choose **Restore**;
   - in the main menu, select **Edit > Restore**;
   - click **Restore** on the toolbar;
   - click **Restore** in the properties area of the selected person.

As a result, the person becomes *Active*. After the directory is uploaded to the hosts (see "Uploading Directories to the Host"), the information about this person will be used by the system again.

5.2.3 Viewing and Filtering Persons Entries

Filtration helps to eliminate elements viewing witch is no need. The filtration type "All" is chosen by default, and the System displays all objects. You can also apply other types of a filtration:

- Employees - entries received from Active Directory. It includes the following items:

  a) Active (pictogram ) - entries of stuff;

  b) Dismissed (pictogram ) - entries of ex-employees;

  c) Changed Today (pictogram ) - persond entries which were existed or edited but weren't send to hosts. For more information see "Uploading Directories to the Host".

- External contacts - entries made with Traffic Monitor Management Console. It includes the following items:

  a) Active (pictogram ) - entries of stuff;

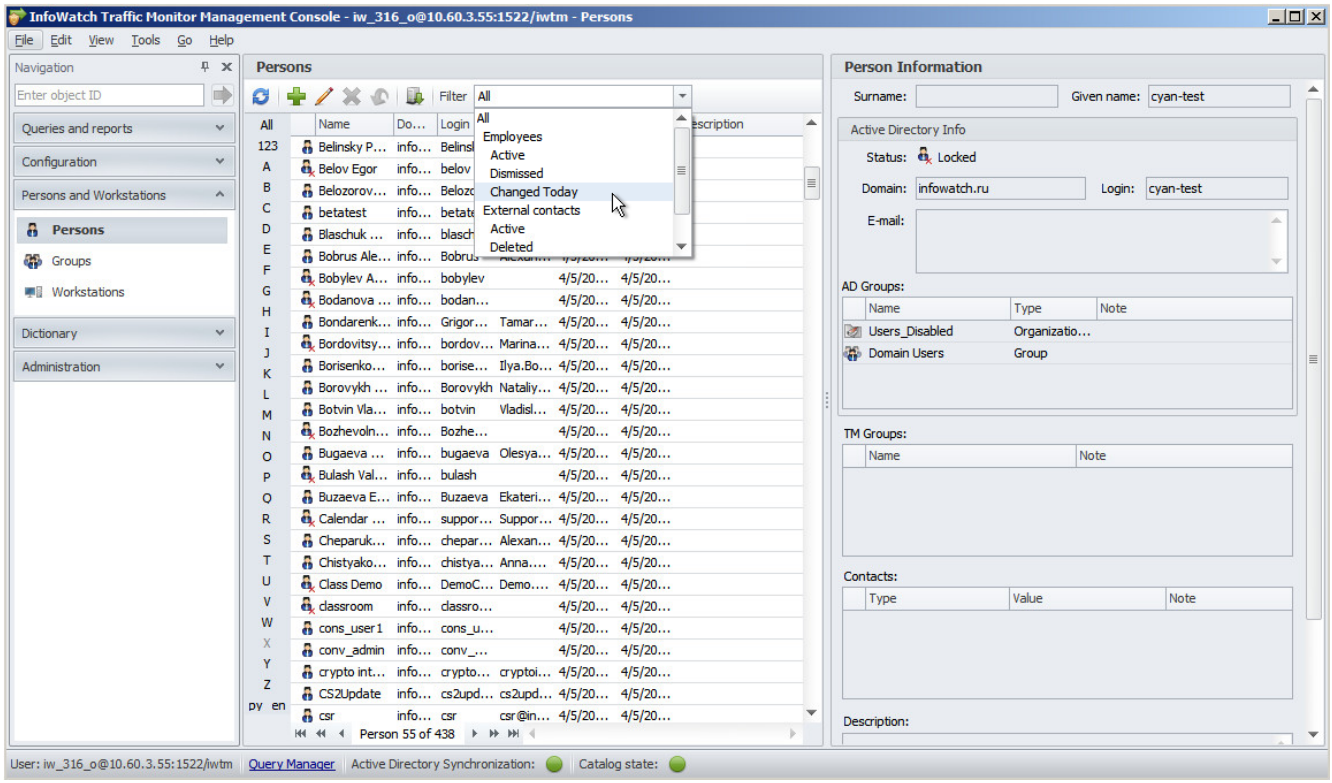
  b) Deleted (pictogram ) - entries of ex-employees;

  c) Changed Today (pictogram ) - persond entries which were existed or edited but weren't send to hosts. For more information see "Uploading Directories to the Host".

- Yet not distributed to hosts - entries which were existed or edited but weren't send to hosts. For more information see "Uploading Directories to the Host".

To filter entries,

go to **Persons** pane and select necessary type of filtration in the dropping list located on the toolbar.



Filtering persons entries

5.3 Workstations Directory

To work with the list of workstations, use the **Workstations** section (the **Persons and workstations** area on the **Navigation** pane). When navigating to this section, the working area of the main window becomes divided into two parts. The left part contains a list of workstations, and the right part contains the display area to view the properties of the selected workstations.

The information about the workstations is imported automatically during synchronization with Active Directory (see "Configuring Connection and Synchronization with Active Directory").

Important!

When processing the intercepted objects, only the information for *Active* and *Locked* workstations is processed.

For more details about working with the workstations directory see the following sections:

- Editing a Workstation Record
- Viewing and Filtering Workstations Entries

5.3.1 Editing a Workstation Record

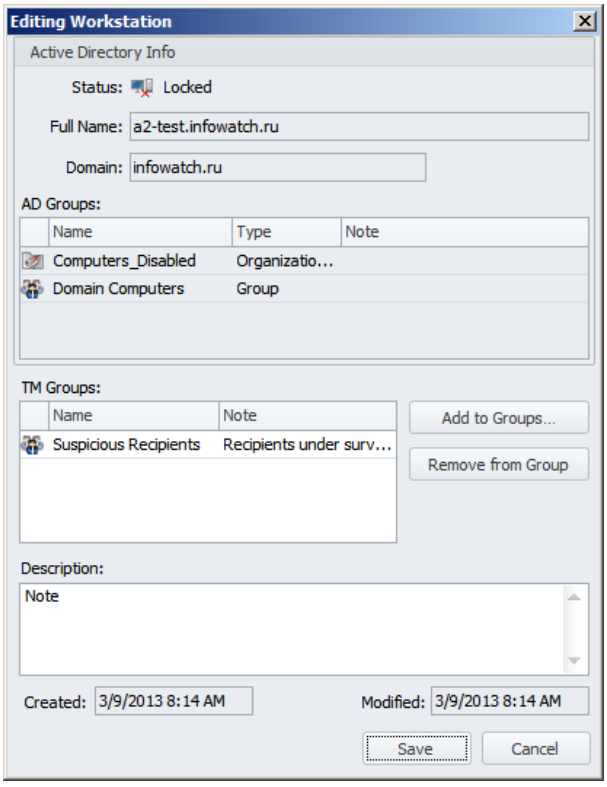
Note

The workstations directory cannot contain more than 4,194,304 records.

To change the workstation record:

1. Go to the **Workstations** section.
2. Select the required workstation record from the list.
3. Do one of the following:
   - double-click the selected workstation;
   - right-click the record and choose **Edit**;
   - in the main menu, select **Edit > Edit**;
   - click **Edit** on the category pane;
   - click **Edit** in the settings pane of the selected workstation.

   The dialog box with the settings of the workstation will appear.



Workstation Settings

4. Edit the necessary workstation settings:

Setting	Description
TM Groups	The Traffic Monitor groups that contain this workstation. • To add the workstation to the group, click **Add to Groups**. In the **Group Selection** dialog box, select the groups to add the workstation. To select or clear all the check boxes, use the **Check All** and **Clear All** buttons. Select the required groups and click **Save**. • To delete the workstation from the group, select the required group and click **Remove from Group**

Setting	Description
	Note: For more information about creating TM groups see "Creating, Viewing, and Editing a Group"
Description	Addition information about the workstation **Warning!** If the workstation description was changed in the Active Directory catalog, then after the next synchronization (see "Configuring Connection and Synchronization with Active Directory") the value of **Description** field will be changed to the renewed one

5. Click **Save** once the workstation settings are successfully defined.

Important!

The updated workstation settings will be used by the system only after the directories are uploaded to the hosts (see "Uploading Directories to the Host").

Note

You can also modify a workstation record when you work with the group that contains this workstation. To do this, select the required group name in the **Groups** section, and then select the required row. Then take one of the following steps:

- in the main menu, select **Edit > TM Group Members > Edit**;
- click **Edit** on the group members pane
- double-click the selected person record.

The workstation record editing window and the settings editing process are similar to those described above.

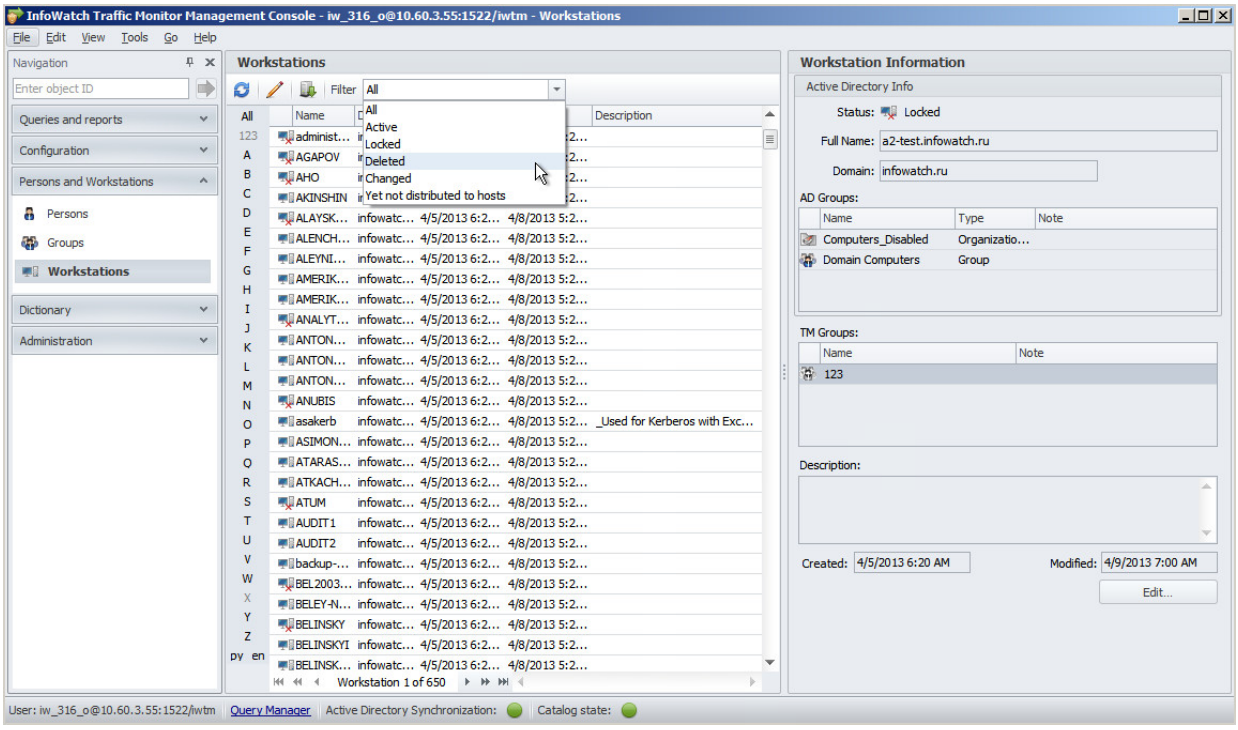
5.3.2 Viewing and Filtering Workstations Entries

Filtration helps to eliminate elements viewing witch is no need. The filtration type "All" is chosen by default, and the System displays all objects. You can also apply other types of a filtration:

- Active (pictogram) - list of workstations available for users;
- Locked (pictogram) - list of workstations which are temporary not available for users;
- Deleted (pictogram) - list of workstations which are forbidden for users;
- Changed (pictogram) - entries which were edited but weren't send to hosts. For more information see " Uploading Directories to the Host".
- Yet not distributed to hosts (pictogram or) - entries which were existed or edited but weren't send to hosts. For more information see "Uploading Directories to the Host".

To filter entries,

go to **Workstations** pane and select necessary type of filtration in the dropping list located on the toolbar.



Filtering workstations entries

5.4 Groups Directory

The Active Directory groups contain the persons and workstations records.

The system supports two types of groups:

- **AD Groups** are the groups, containers or organizational units that have been automatically imported during synchronization with Active Directory (see "Configuring Connection and Synchronization with Active Directory"). For these groups, the user can only change the code and the description.
- **TM Groups** are the groups created using the Traffic Monitor tools. Users can create and edit the settings as well as modify the membership in these groups.

To work with the workstations groups and and person groups, use the **Groups** section (the **Persons and Workstations** area on the **Navigation** pane). When you navigate to this section, the working area of the main window will be divided into two parts: **AD Groups and TM Groups**. Each of these parts, in its turn, is also divided into two areas: lo the left is the group list, and to the right is the list of members of the selected group.

Note

Viewing and filtering of groups are the same as viewing and filtering persons and workstations entries (см. " Viewing and Filtering Persons Entries" и "Viewing and Filtering Workstations Entries").

For more details about working with the groups directory see:

- Creating, Viewing, and Editing a Group
- Adding Members to a TM Group
- Deleting Members from a TM Group
- Deleting and Restoring a TM Group

5.4.1 Creating, Viewing, and Editing a Group

Note

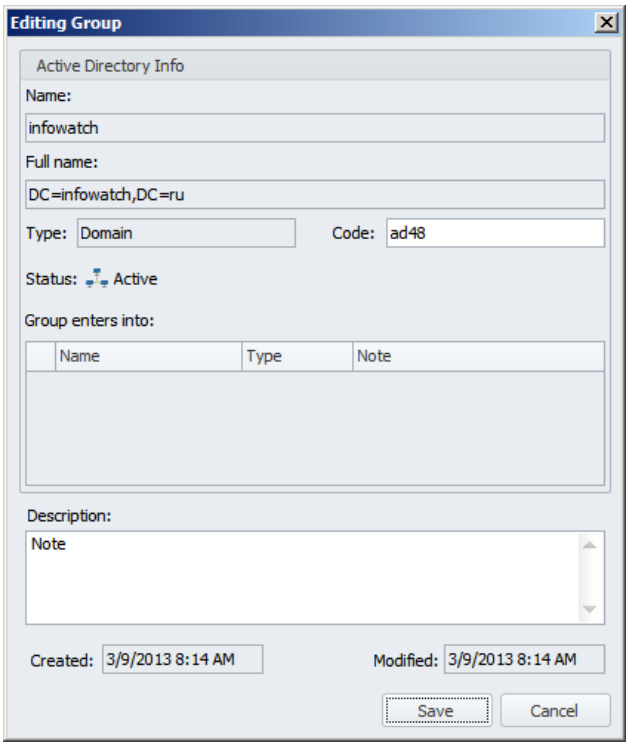
The groups directory cannot contain more than 4,194,304 entries.

To create or change a group:

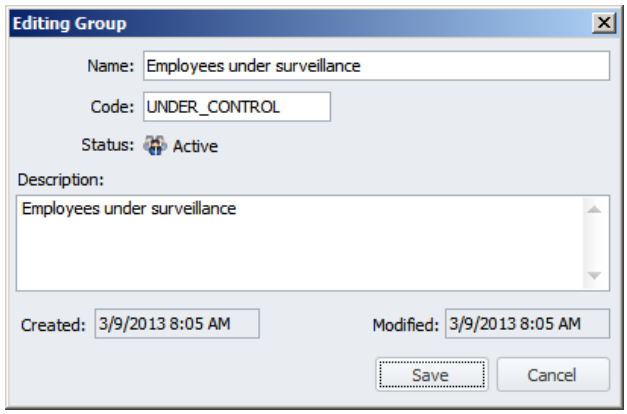
1. Go to the **Groups** section.
2. Do the following:

Action	Procedure
Create a TM group	Do one of the following: • in the main menu, select **Edit > TM Groups > New** • click **New** on the **TM Groups** pane
Edit the group	1. On the **AD Groups** or **TM Groups** pane select the name of the required group from the list. 2. Do one of the following: • in the main menu, select **Edit > TM Groups / AD Groups > Edit**; • click **Edit** on the **AD Groups** or **TM Groups** pane; • right-click the selected row and choose **Edit**; • double-click the selected row.

The dialog box with the group settings will appear.



Viewing and editing an AD group



Configuring TM group settings

3. Specify the group settings:

Setting	Description
Name	Group name. The name should be unique. It can be modified only for TM groups
Code	The code name of the group that will be used when building a script. The name may include English letters, digits, and underscores; it must start with a letter. The code should be unique
Description	Additional information about the group

4. Click **Save** once the parameters of the group are successfully configured.

New TM groups should be populated with the required persons and workstations: see: "Adding Members to a TM

Group".

Important!

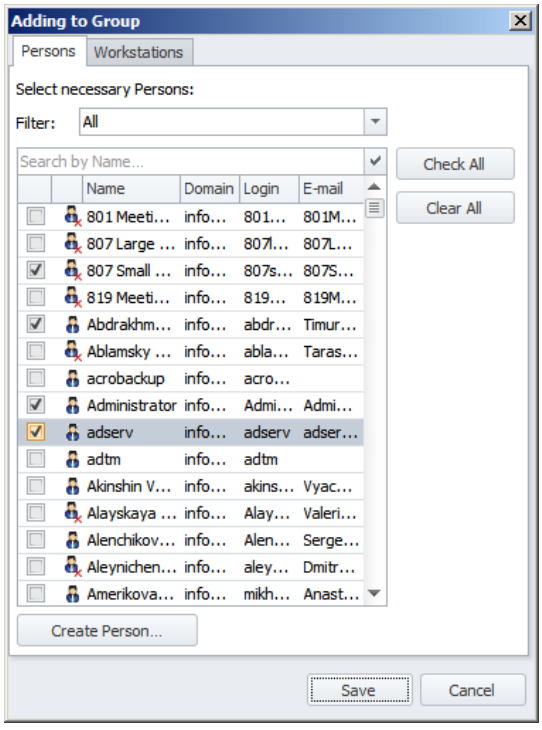
The new or updated information about a group is used by the system only after the directories are uploaded to the hosts (see"Uploading Directories to the Host").

5.4.2 Adding Members to a TM Group

To add a person or a workstation to the TM group:

1. Go to the **Groups** section.
2. On the **TM Groups** pane select the name of the required group from the list.
3. Do one of the following:
   - in the main menu, select **Edit > TM Group Members> Add**;
   - click **New** on the selected group pane.

   The **Adding to Group** dialog box will appear on the screen.



Adding a member to a TM

This window consists of two tabs:

- **Persons** – the list of persons you can add to the group;
- **Workstations** – the list of workstations that you can add to the group.

You can filter out the displayed list of persons/workstations by selecting the desired type from the dropdown list in the **Filter** field.

You can also search for the person name or the workstation name. To search, enter the name or a part of

the name in the appropriate field and click .

On the **Persons** tab you can click **New Person** to add a person record. For more information on creating person records see "Creating and editing a person record".

4. In the workstations/persons list select the elements you want to add to the group.

   To select or clear all the check boxes, use the **Check All** and **Clear All** buttons.

5. Click **Save**.

5.4.3 Deleting Members from a TM Group

To delete a person or a workstation from the TM Group:

1. Go to the **Groups** section.
2. On the **TM Groups** pane select the name of the required group from the list
3. On the pane of the selected group select the row with the required entry.
4. Do one of the following:
   - in the main menu, select **Edit > TM Group Members > Delete from TM Group**;
   - click **Delete from TM Group** on the group members pane.

5.4.4 Deleting and Restoring a TM Group

To delete a TM Group:

1. Go to the **Groups** section.
2. On the **TM Groups** pane select the name of the required group from the list.
3. Do one of the following:
   - in the main menu, select **Edit > TM Group > Delete**;
   - click **Delete** on the **TM Groups** pane.

As a result, the TM group receives *Deleted* status. After the directory is uploaded to the hosts (see "Uploading directories to the host"), the information about this group won't be used by the system any longer.

If you need to reuse a deleted TM group, you can restore it.

To restore the record of a TM group:

1. Go to the **Groups** section.

   Note

   To view the deleted groups, on the **TM Groups** pane select the **All** or **Deleted** filter.

2. Select the required group from the list in the **TM Groups** pane.

3. Do one of the following:
   - right-click the record and choose **Restore**;
   - in the main menu, select **Edit > TM Groups > Restore**;
   - click **Restore** on the **TM Groups** pane.

As a result, the TM group becomes *Active*. After the directory is uploaded to the hosts (see"Uploading directories to the host"), the information about this group will be used by the system again.

5.5 Uploading Directories to the Host

The information that is imported from the Active Directory and entered by the Management Console users is stored in a database. In order for this information to be used in the analysis of objects or to display information about the sender and recipient it is necessary to load the Active Directory directories on the host.

The directories are uploaded during the automatic synchronization with AD (see "Configuring Connection and Synchronization with Active Directory"), and when the configuration is uploaded to a host (see "Uploading Configuration to the Hosts"). However, you can update the information faster by uploading the directories to the host separately.

You can start uploading to the host from any section **Persons and workstations** (**Persons**, **Workstations** or **Groups**). As a result, the Traffic Monitor server will contain the updated Active Directory data.

To upload the directories to the host,

click **Send Directory To Hosts** on the toolbar.

The status of uploading the directories to the host and (in case of a success) the time of the last upload are displayed in the status bar for every section of **Persons and Workstations** (**Persons**, **Workstations** or **Groups**).

6 Crawler

Crawler subsystem of the InfoWatch Traffic Monitor system enables the reviewing of files located in the corporate network, to check if they violate corporative security policies. InfoWatch Crawler allows to supervise file resources of the company for identification and prevention the cases of unauthorized using the confidential data.

InfoWatch Crawler provides executing of the following functions:

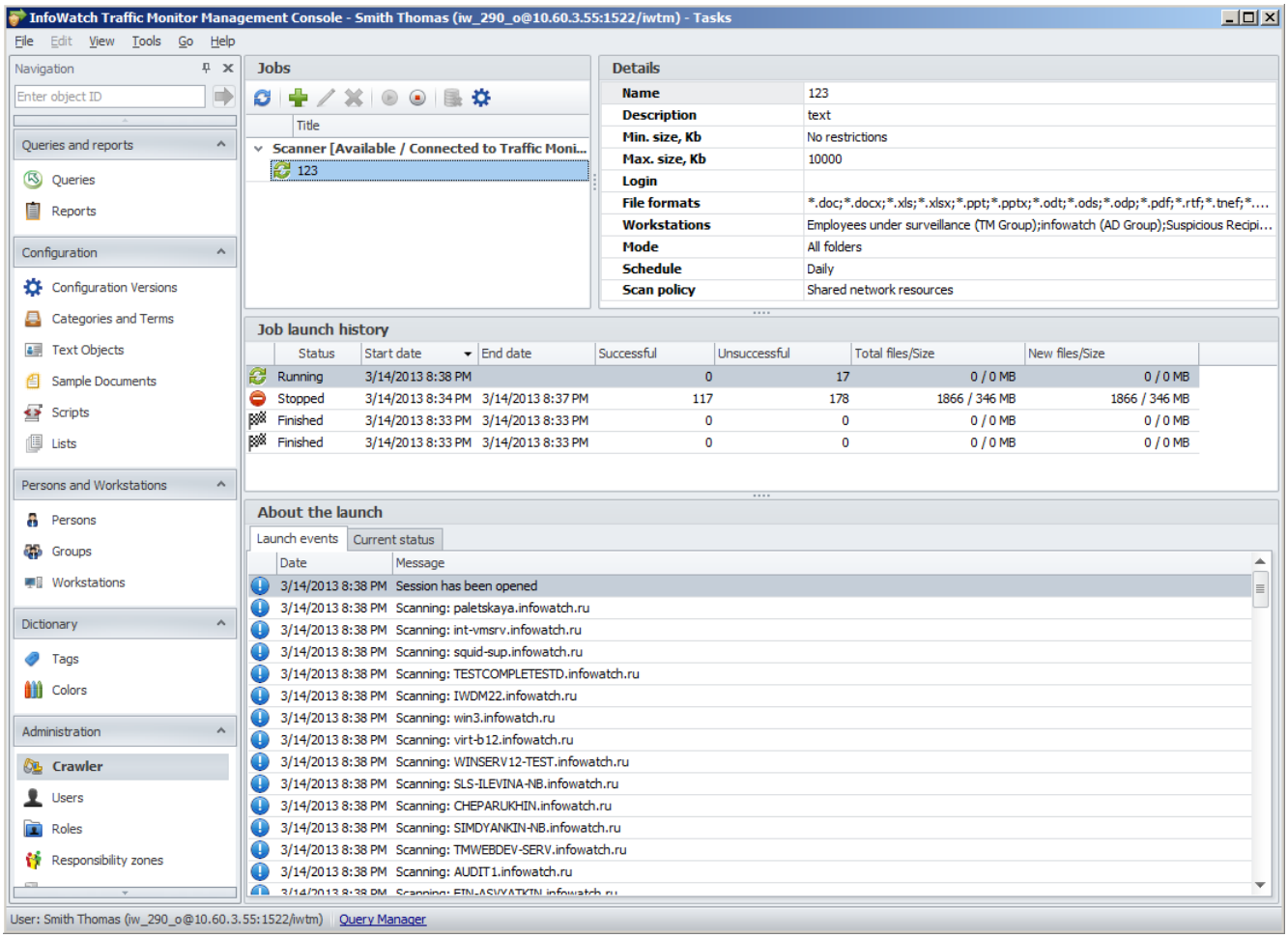
- Scanning of the network folders opened for remote access using SMB protocol.
- Scanning of local disks of the workstations under Windows OS.
- Scanning of file SharePoint file storage and verification of the documents which are storing in a Microsoft SharePoint 2007 Database. Only the current versions of files are tested: the history of changes isn't checked.
- User settings: speed of the file downloading from scanned resources; parameters of file queue for objects uploading to the Traffic Monitor server.
- Creation a scanning jobs with following options:
  - list of folders and network sited on which scanning will be executed;

  - masks of processing files;
  - restrictions by the size of processing files;
  - schedule of a job execution (manual start is also available).
- Selection of only new and changed files: earlier processed files wouldn't be sent to the InfoWatch Traffic Monitor server.
- Transferring files to the InfoWatch Traffic Monitor server for the analysis, with regard to user-defined transfer parameters.
- Saving of files according to policy settings (by default, the incidents would be saved: the files recognized as potential violation of the operating security policy).
- Presenting the scan results in the Management Console: using queries and reports.

InfoWatch Crawler doesn't perform removing, moving, renaming, scrambling or any other actions with files, even if files are recognized as potential violation. System informs the security officer about the incident: the Management Console shows the files recognized as potential violation, with the indication of detailed information on their arrangement and the users having the access to this files.

To use Crawler go to the **Crawler** section of the Management Console (the **Administration** group on the **Navigation** pane). In this section the working area is divided into the following parts:

- **Jobs** – the list of the scanning jobs registered in system. The status of the scanner is specified in its name. For example, status [**Available/Connected to Traffic Monitor**] means that the scanner is fully operable. If the status is:
  - **Offline** – the `Crawler.Scanner` service isn't started. Please check the functioning of a computer where it is installed.
  - **Disconnected with TM** – the `iw_expressd` process isn't found.
- **Details** – detailed information on a job chosen in the jobs list.
- **Job launch history** – the list of sessions of the selected job. There are displayed: job status; date and time of the beginning and the end of session; the general statistics (number of the executed workstations and files).
- **About the launch** – the journal of the session chosen in the launch history. Information on the scanning events is displayed on the **Launch Events** tab. The resources, folders and files scanned at the current moment in the currently running job (session with the **Works** status) are displayed on the **Current status** tab .



For more information about working with Crawler see the following topics:

- Crawler's Work Scheme
- Connecting the Management Console to the Crawler Sever
- Configuring the Crawler Scanner General Settings
- Creating and Editing the Scanning Job
- Deleting the Scanning Job
- Running and Stopping the Job
- Cleaning the Hash Base

6.1 Crawler's Work Scheme

InfoWatch Crawler works as one of the Traffic Monitor interceptors.

The following components of InfoWatch Traffic Monitor system are used in the Crawler subsystem:

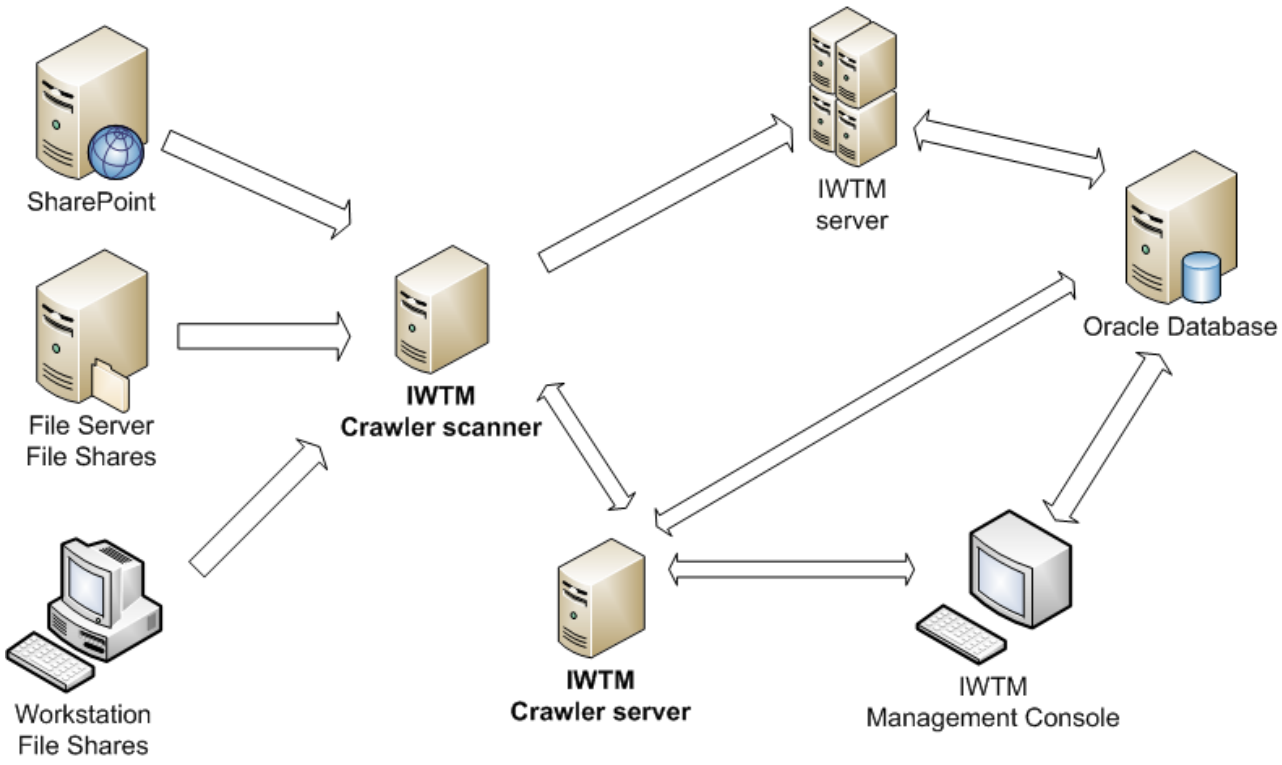
- **Crawler** – the software package providing usage of the main functions. It is designed as two Windows services:
  - `InfoWatch.Crawler.Scanner` – scans the network folders and file storages according to user-defined parameters;
  - `InfoWatch.Crawler.Server` – manages the scanning service and provides communication with the

Traffic Monitor Management Console.

- **Database** – Crawler uses InfoWatch Traffic Monitor database scheme for storing both objects recognized as potential violation and information on scanning job.

InfoWatch Traffic Monitor Management Console – Crawler management elements are presented in the **Crawler** section.

Files obtained as a result of Crawler operation (including the information on their location, on users having access to them and other data) are considered as objects from the Crawler Monitor interceptor.



InfoWatch Crawler Work Scheme

InfoWatch Crawler executes scanning in the following order:

1. Workstations, groups of workstations, file servers or the file storages listed in a scanning job (see. "Creating and Editing the Scanning Job"), are checked for data accessible to the account, which run this scanning job .
2. For each found file:
   - the checking if the file matches search conditions (file mask, sizes) is executed
   - the file is temporarily copied in a working directory of the scanner
   - the checking if the file was earlier processed is executed: if the file was already transferred to the system and has not any changes since, then its temporary copy is removed.
3. If the file matches search conditions and wasn't processed earlier, the following additional attributes are assigned to it:
   - owner of the file
   - list of accounts having access for reading this file.
4. The file goes for the analysis to the InfoWatch Traffic Monitor Server where it would be processed according to the current objects processing script (see. "Configuring Object Analysis Scripts (LUA)").

If default settings are applied on the Traffic Monitor Server:

- the System saves a copy of Crawler object which is recognized as potential violation (*Forbidden* verdict) to the database. At that this copy is an attachment to the intercepted object (for more information see. " Viewing the General Object Information")
- the Crawler object which isn't potential violation (*Allowed* verdict is given) is removed.

6.2 Connecting the Management Console to the Crawler Sever

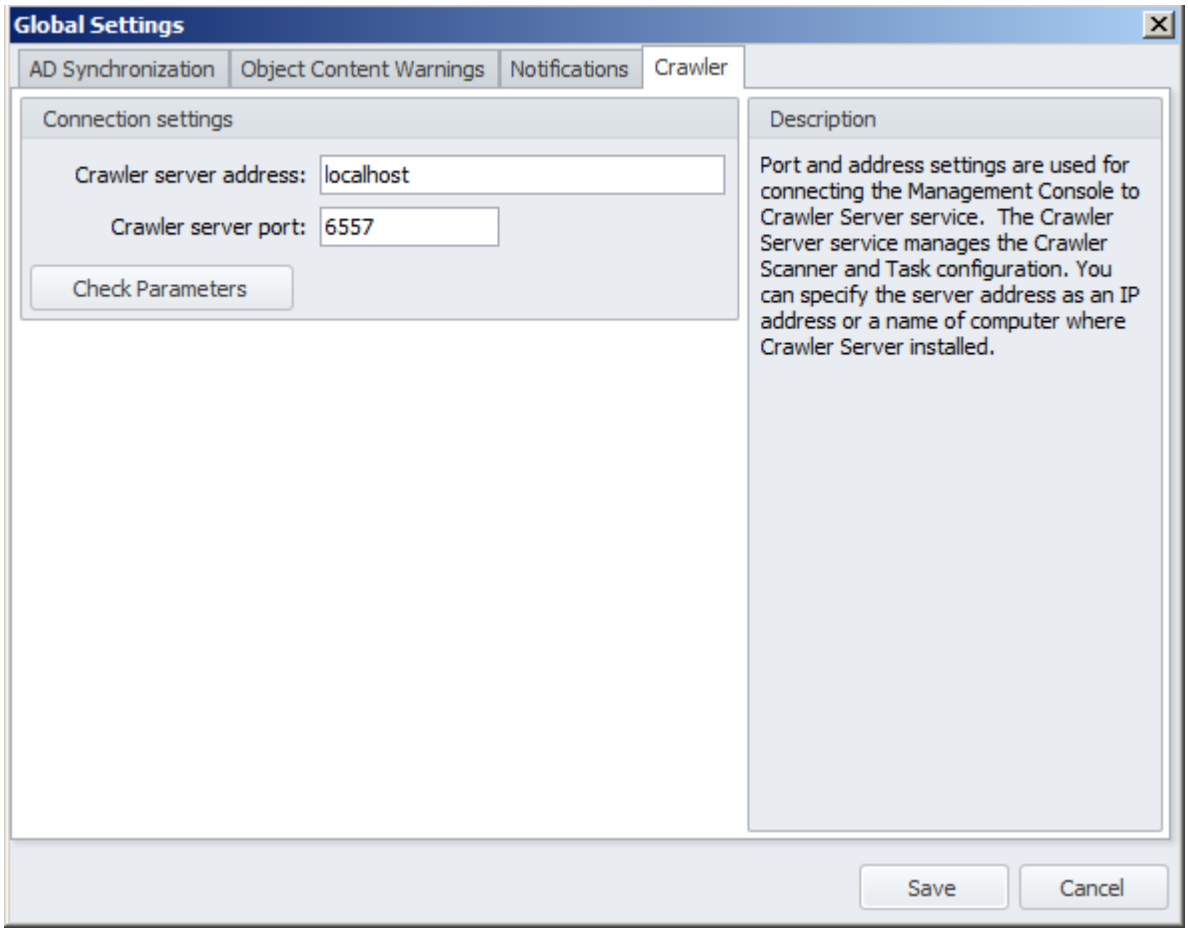
To set connection between Crawler Server and Management Console:

1. In the main menu, select **Tools > Global settings**.
2. Specify connection parameters on the **Crawler** tab in the **Global settings** dialog box:
   - **Crawler server address**. You can define IP address or name of the computer where Crawler server is installed.

     Warning!

     Connection settings extend on all instances of the Management Console operating in System. So if it is supposed that several Management Console will work with Crawler subsystem, then this control has to contain the actual address of the server where Crawler Server is installed (instead of localhost 127.0.0.1).
   - **Crawler server port**
3. Check the settings by clicking **Check Parameters** button.



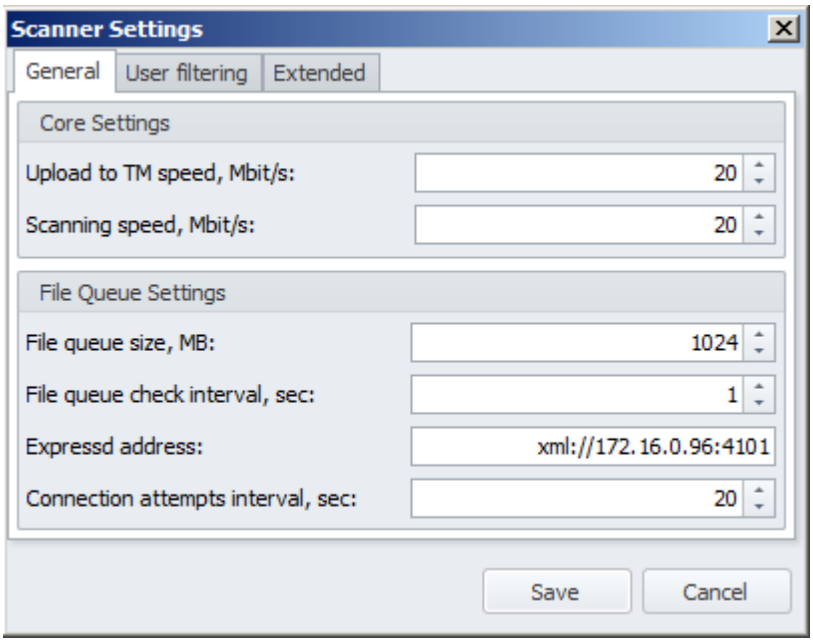
4. Click **Save**.

6.3 Configuring the Crawler Scanner General Settings

To define the general parameters of the Crawler Scanner operation:

1. Go to **Crawler** section in the Management Console.
2. Click **Scanner settings** button located on the toolbar.

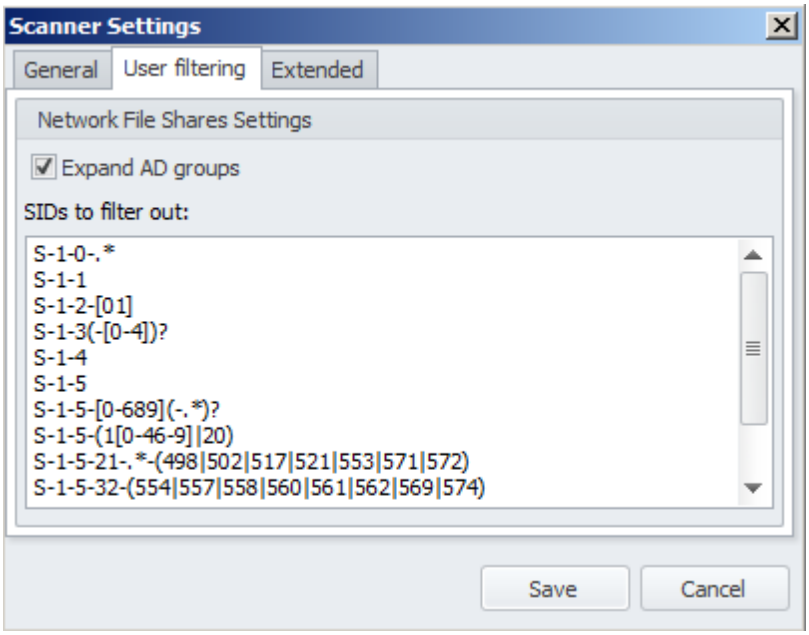
   The **Scanner Settings** dialog box will appeared on the screen.



3. Specify the general settings:

- **Upload to TM speed** – the maximum speed of files uploading to the Traffic Monitor Server, Mbit / sec
- **Scanning speed** – the maximum speed of files downloading from examined resources to temporary storage, Mbit / sec
- **File queue size** – the maximum size of queue where the found files put before sending to the Traffic Monitor Server, Mb
- **The queue check interval** – the interval (in seconds) to check if there any objects in loading queue to the Traffic Monitor Server. If there is at least one object in the queue, the transfer of this object on the Traffic Monitor server will be executed.
- **Expressd address** – connection string with InfoWatch Traffic Monitor server where `iw_expressd` process runs. The format is: `xml://IP_address:port`.
- **Connection attempt interval, sec** – the interval (in seconds) to try to restore connection to the Traffic Monitor server in case of loss of this connection.

4. If necessary, on the **User filtering** tab set the general rules of filtering users accounts to display the Crawler objects information in the Management Console:



- **Expand AD groups**. If the tag is set then when information on the object intercepted by Crawler is displayed (see "Viewing Objects Information") groups of AD users having access rights for the file (**Recipients** parameter) will be shown expanded, in the form of links to cards of employees.

  If the tag isn't set, AD groups will be displayed as records like `group_name@domain`. If the group is local then a name of workstation from which the object was achieved is displayed instead of the domain.

- **SIDs to filter out**. The standard service SIDs are listed in this field. If necessary, you can add your own SID and set masks using regular expressions.

  Record example:

  `S-1-5-21-.*-(498|502|517|527)`

  This record means that in the Management Console it won't be displayed that intercepted file is accessible to accounts with any SIDs beginning with the line "S-1-5-21-", having "0" in the middle or more any letters, figures, etc. symbols, and terminating on "-498" or "-502" or "-517" or "-527".

  Proper SIDs:

  `S-1-5-21-12345-ABCDEF-498`

  `S-1-5-21--527`

  Improper SIDs:

  `1S-1-5-21-12345-ABCDEF-498` - begins not with "S-1-5-21-"

  `S-1-5-21-527` - begins with "S-1-5-21-", but comes to an end with "527", instead of with "-527"

  `S-1-5-21-ABCDEF-100` - doesn't come to an end with "-498", or "-502", or "-517", or "-527".

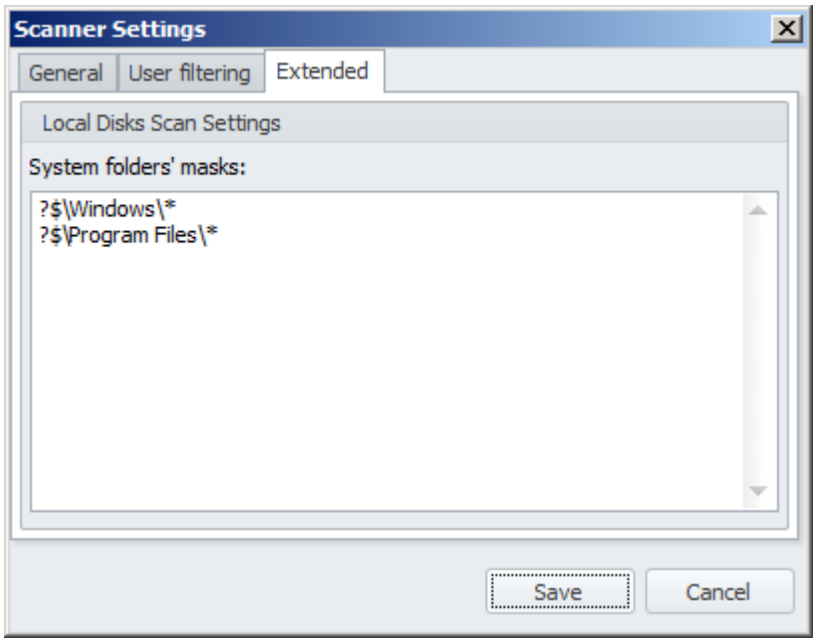
  `S-1-5-21-ABCDEF-502-` - doesn't come to an end with "-498", or "-502", or "-517", or "-527".

  `S-1-6-21-ABCDEF-502` - begins not with "S-1-5-21-".

Note

The language format of regular expressions can be studied here:
http://msdn.microsoft.com/ru-ru/library/az24scfc(v=vs.100).aspx

5. On a **Extendend** tab there are masks of folders ignored in workstation's local disks scanning are listed. This list is used only if at job creation the **Exclude system folders** function was checked:



If necessary, remove or add folders.

Note

Each folder set on a separate line.

To replace one or several symbols use "?" or "*" correspondingly.

If the folder name does not have «*» at the end of a name, then symbol «*» is added automatically to the end of a string when settings saved.

6. Click **Save**.
The system will display the message about the successful updating of scanner configuration.

6.4 Creating and Editing the Scanning Job

InfoWatch Crawler performs the following types of scanning:

- **Scanning of the network file shares**: the policy of scanning "**Network file shares**". Performs scanning of the folders opened for remote access using the SMB protocol. The account with the right of reading network folders at target workstations is necessary to execute the job.
  For more details about creation and editing this job see "Scanning the Network File Shares".
- **Scanning of the workstation's local disks**: the policy of scanning "**Workstation's local disks**". Performs scanning of local disks of the workstations working under Windows OS. The account with the administrative rights for the target workstations is necessary to execute the job.

For more details about creation and editing this job see "Scanning the Workstation's Local Discs".

- **Scanning of the SharePoint file storage**: the policy of scanning "**SharePoint file storage**". Performs the verification of documents stored in the Microsoft SharePoint 2007 database. Only the current versions of files are considered: the history of changes isn't investigated. The account with the right to read data located in the checking storage is necessary to execute the job.

  For more details about creation and editing this job see "Scanning the SharePoint File Storage".

You cannot change or remove started job (**Running** status) or being edited in other Management Console instance.

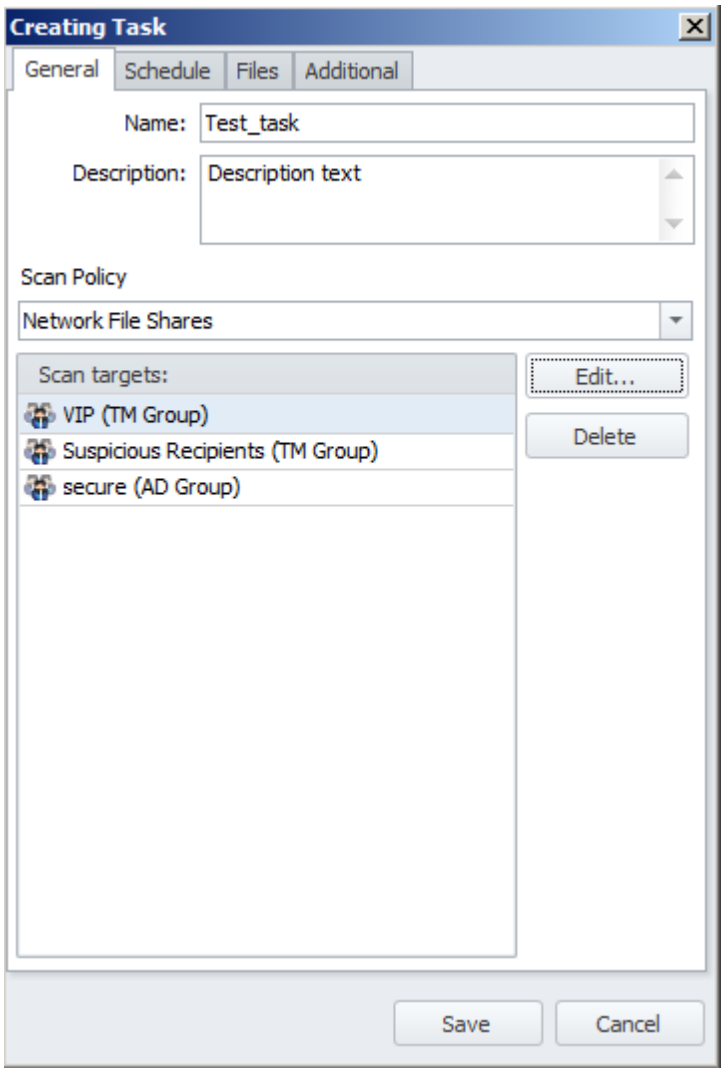
6.4.1 Scanning the Network File Shares

The job of scanning shared network resources provides verification of open network folders. To execute this job you need an account with the right of reading network folders at target workstations (parameters of the account are set at the **Additional** tab).

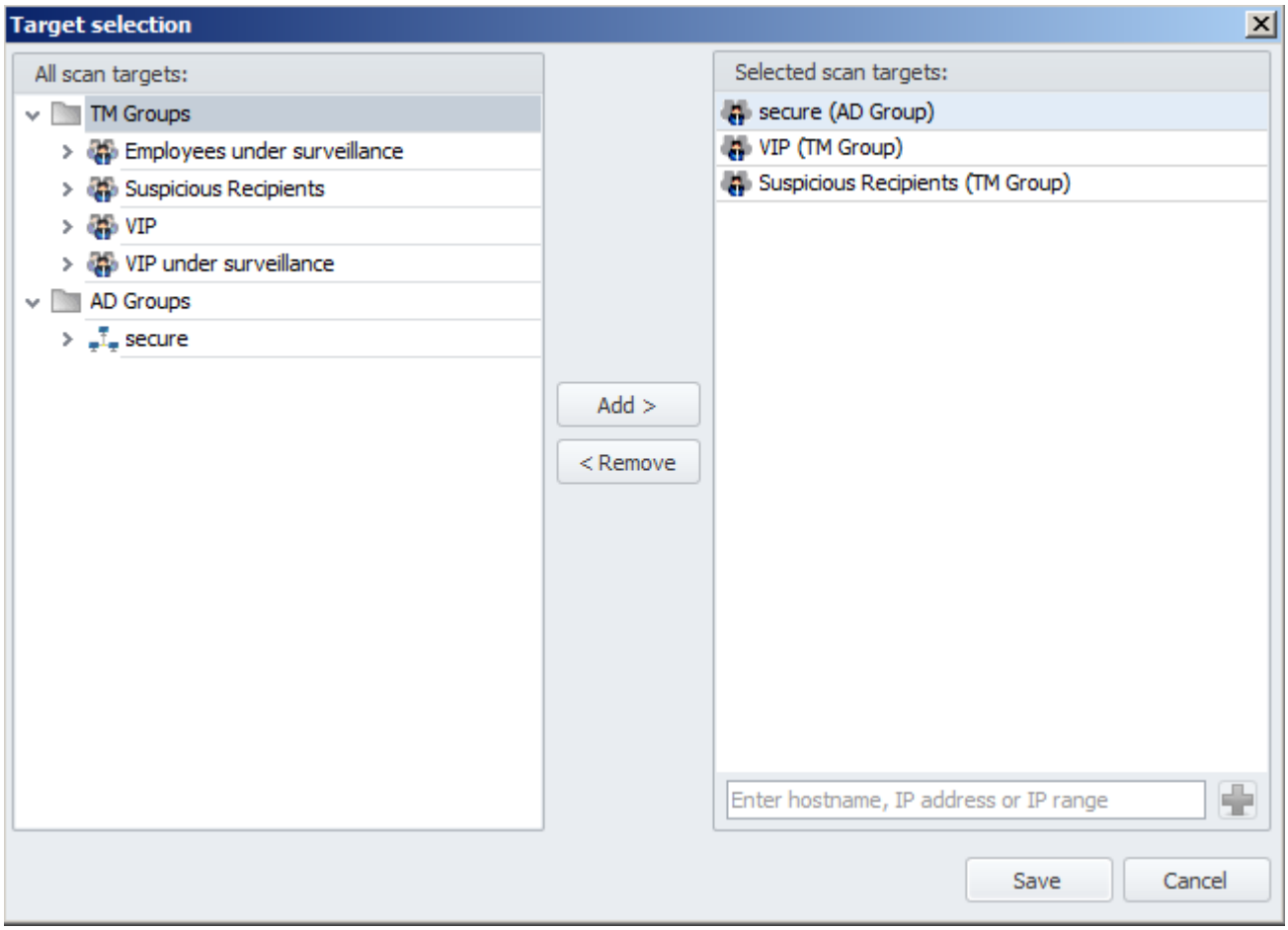
To create or change a job of scanning shared network resources:

1. Go to the **Crawler** section in the Management Console.
2. Do one of the following:
   - to create the new job, click **Add** button located on the toolbar
   - to edit the existed job, click **Edit** button located on the toolbar

   The job settings dialog box will appeared on the screen.
3. Define the general parameters of a job at the **General** tab:
   - **Name** – a job name.
   - **Description** – an optional field with any text
   - **Scan policy** – choose the **Network File Shares** from the drop-down list.



4. At the **Scan targets** area define the list of workstations and groups you want to be scanned. To add workstations or groups to the list, click **Edit**, then in the appeared dialog box choose groups and workstations and transfer them to the list, using the **Add** button.



Warning!

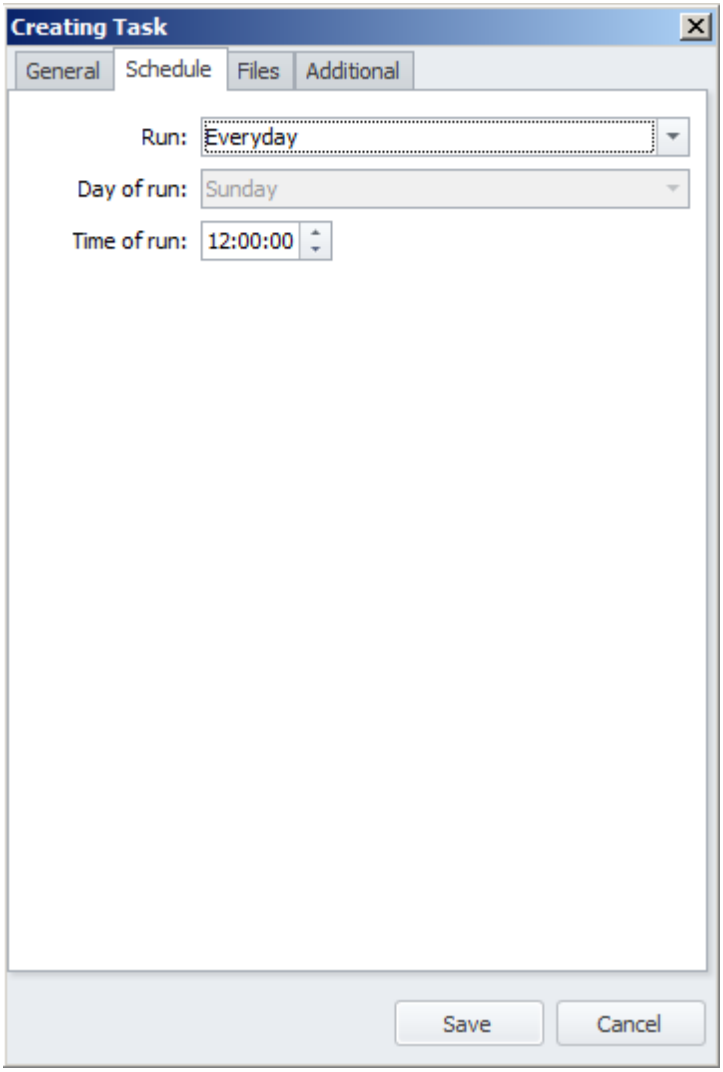
If you have large AD catalogs, the first opening of a workstations selecting window can take some time (several minutes).

You can also specify workstation's FQDN name or IP address in the entry field under the list and then click . To set the range of IP addresses, specify it with a hyphen (-) or a virgule (/) .

After the list of workstations is defined, click **Save**.

To remove workstations or groups from the list, click them in a job settings dialog box and click **Remove**.

5. At the **Schedule** tab set the schedule of job automatic starting.



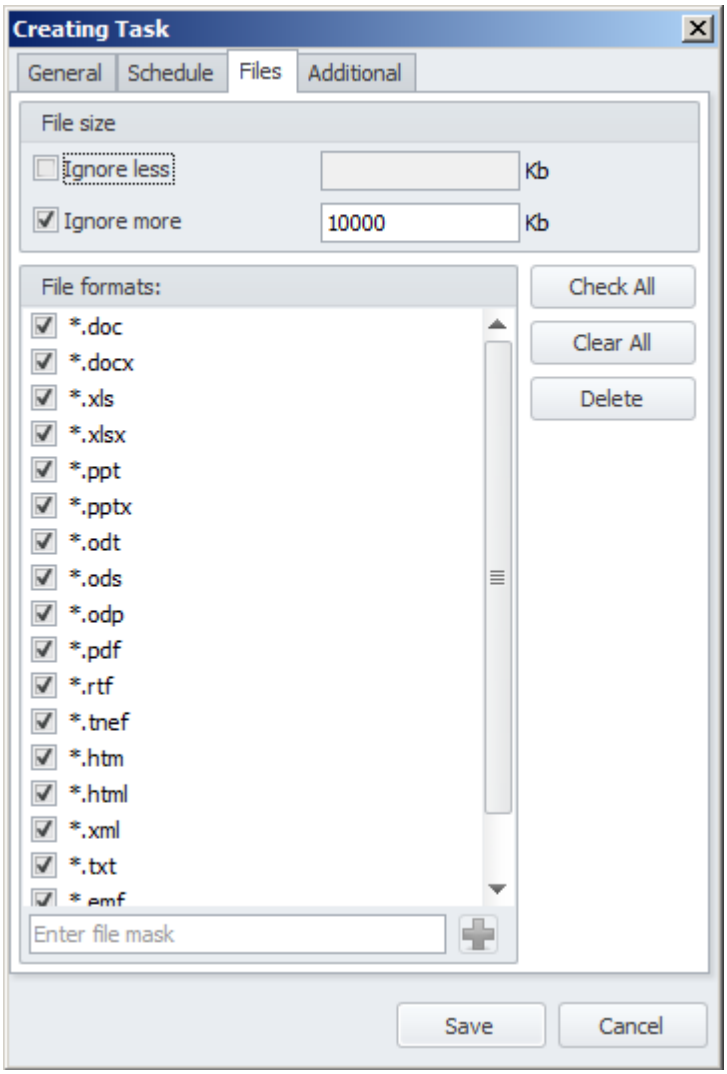
Choose one of the job start options:

- **Weekly** – specify a day of the week and time for automatic start
- **Daily** – specify a day of the week and time for automatic start
- **Manually** – in this case the start of a job can be executed only as described in the "Running and Stopping of the Job" section.

Important!
The job won't be restarted at defined time if the previous session of this job didn't finished yet.

By default, the job is started only manually, at the command of the user.

6. At the **Files** tab set the sizes and formats of files which need to be sent to the analysis.



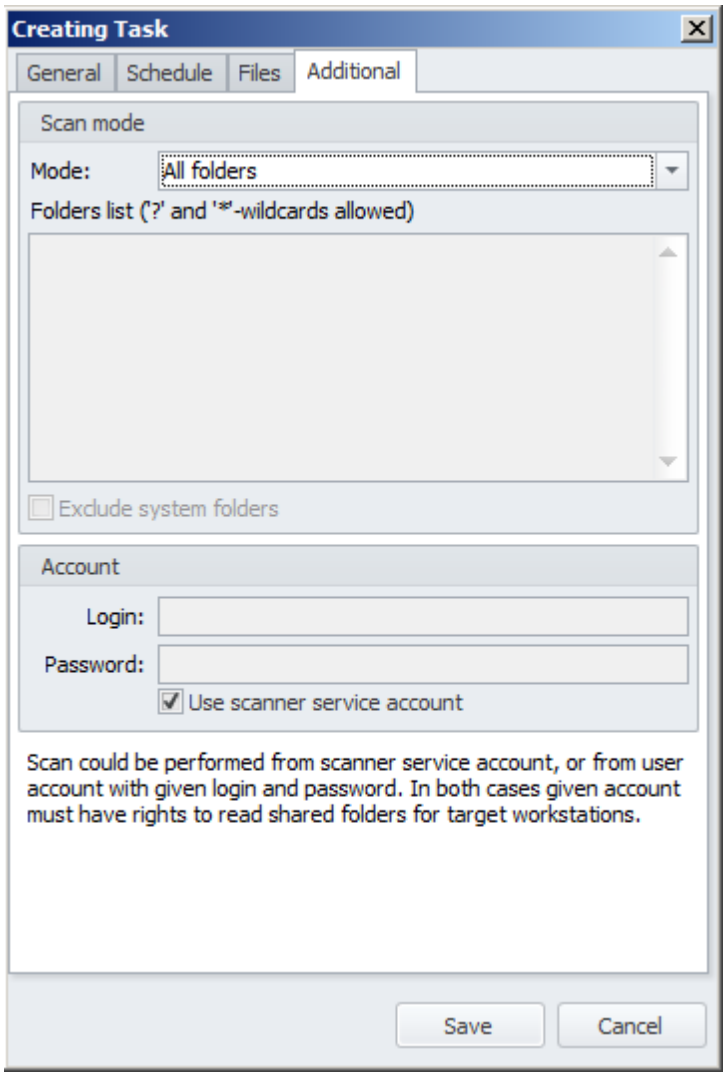
Specify:

- **File size** – maximum and minimum sizes of files which need to be sent to the analysis
- **File formats** – choose the file masks in the list of preset masks or add your own masks, entering them into the field in the bottom of the list and clicking .

Important!

If you use *.* mask, it can significantly reduce the speed of scanning and increase loading of the Traffic Monitor Server.

7. At the **Additional** tab you can narrow down the scanned targets by setting the list of scanned folders. Also you can specify parameters of the account on behalf of which the job will be started. Scanning of shared network resources has to be executed on behalf of the account with the rights of reading network folders of target workstations.



Specify a necessary mode of folders scanning:

- All folders
- All folders except specified
- Only the listed folders.

By defining the folder list:

- Each folder has to be set on a separate line
- To replace of one or several symbols use symbols "?" or "*" correspondingly
- If the folder name does not have «*» at the end of a name, then symbol «*» is added automatically to the end of a string when settings saved.
- The «:» symbol is forbidden. Use masks like «Windows*» to define the path to the directory.

8. Click **Save**.

The saved job can be executed automatically according to the set schedule (if it was defined), or manually (as described in "Running and Stopping the Job" section).

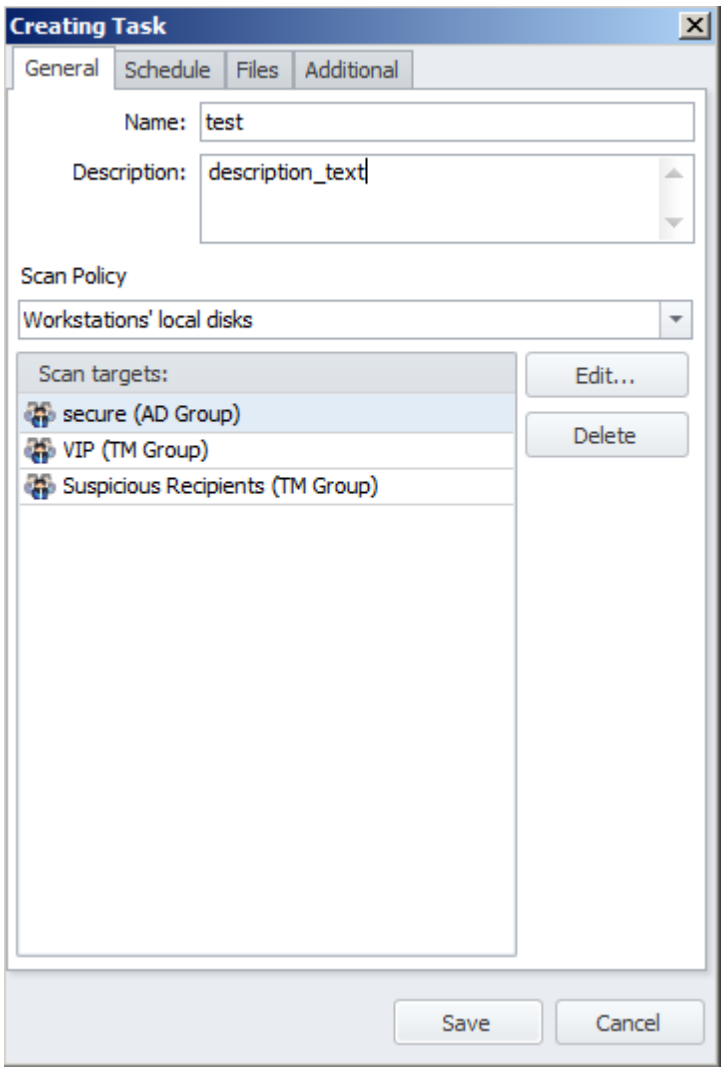
6.4.2 Scanning the Workstation's Local Disks

The job of scanning the workstation's local disks provides verification of files located on local disks of computers operating under Windows OS. To execute this job you need an account with the administrative rights for the target workstations (parameters of the account are set at the **Additional** tab).

To create or change a job of scanning workstation's local disks:

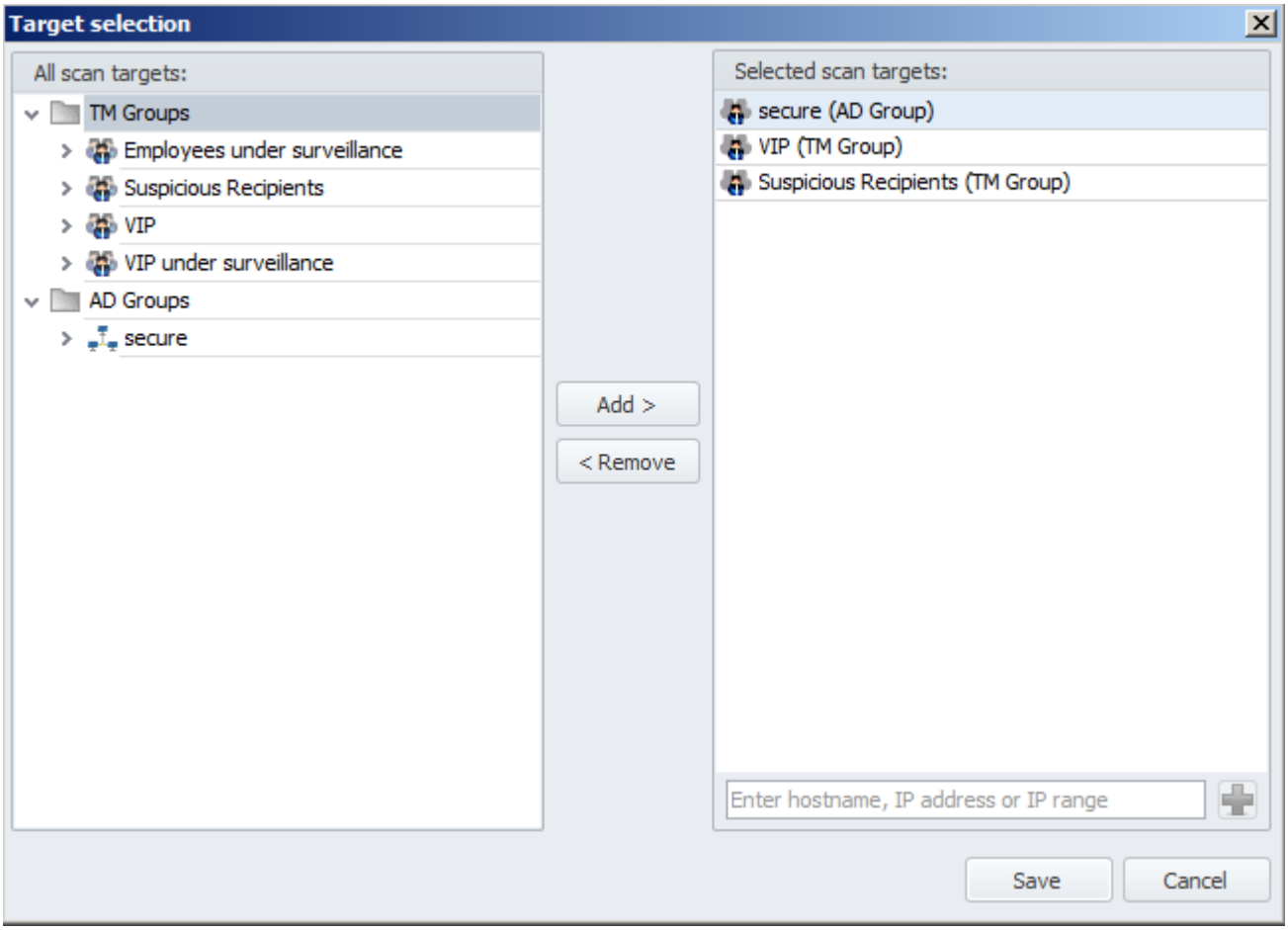
1. Go to the **Crawler** section in the Management Console.
2. Do one of the following:
   - to create the new job, click **Add** button located on the toolbar
   - to edit the existed job, click **Edit** button located on the toolbar

   The job settings dialog box will appeared on the screen.
3. Define the general parameters of a job at the **General** tab:
   - **Name** – a job name.
   - **Description** – an optional field with any text
   - **Scan Policy** – choose the **Workstation's local disks** from the drop-down list.



4. At the **Scan targets** area specify the list of workstations and the groups you want to be scanned. To add

workstations or groups to the list, click **Edit**, choose groups and workstations in the appeared dialog box and transfer them to the list using the **Add** button.



Warning!

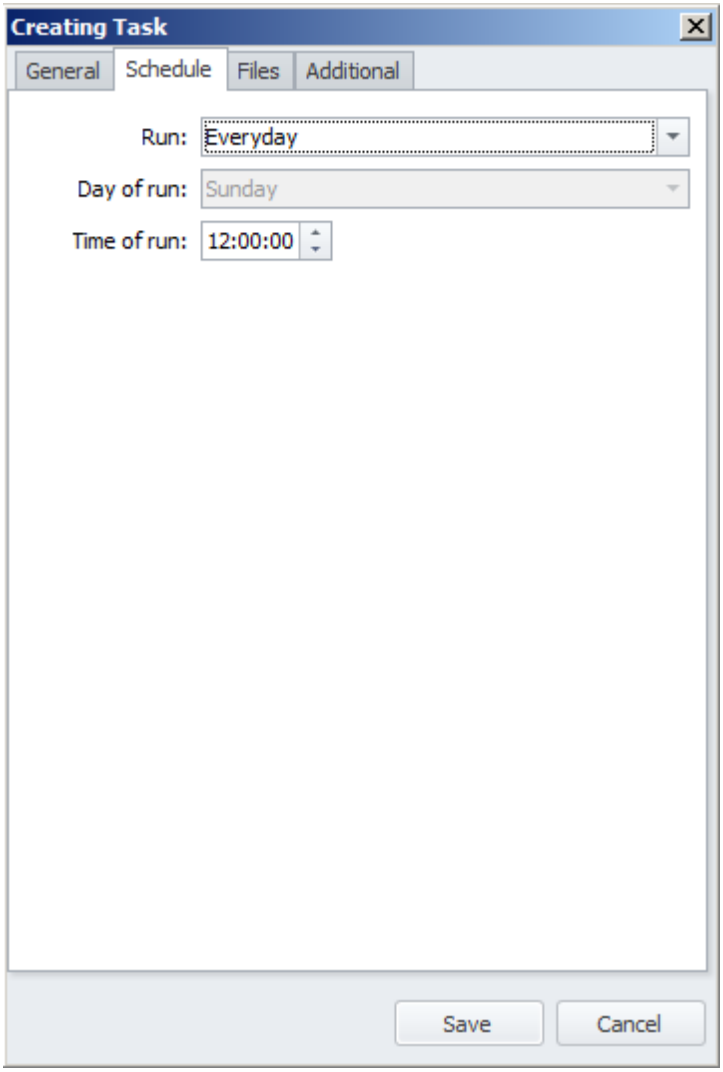
If you have large AD catalogs, the first opening of a workstations selecting window can take some time (several minutes).

You can also specify workstation's FQDN name or IP address in the entry field under the list and then click . To set the range of IP addresses, specify it with a hyphen (-) or a virgule (/) .

After the list of workstations is defined, click **Save**.

To remove workstations or groups from the list, click them in a job settings dialog box and click **Remove**.

5. At the **Schedule** tab set the schedule of job automatic starting.



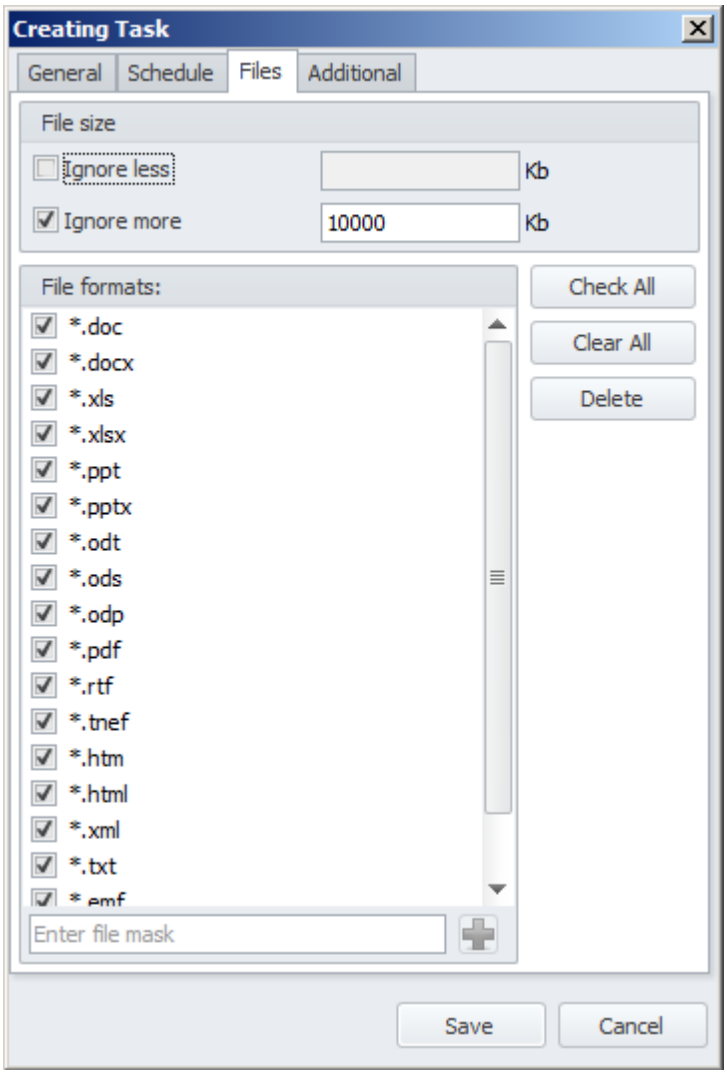
Choose one of the job start options:

- **Weekly** – specify a day of the week and time to automatic start
- **Daily** – specify a day of the week and time to automatic start
- **Manually** – in this case the start of a job can be executed only by the way described in the section " Running and Stopping of the Job".

Important!
The job won't be restarted at defined time if the previous session of this job didn't finished yet.

By default the job is started only manually, at the user command.

6. At the **Files** tab set the sizes and formats of files which need to be sent to the analysis.



Define:

- **File size** – maximum and minimum sizes of files which need to be sent to the analysis
- **File formats** – choose the file masks in the list of preset masks or add your own masks, entering them into the field in the bottom of the list and clicking .

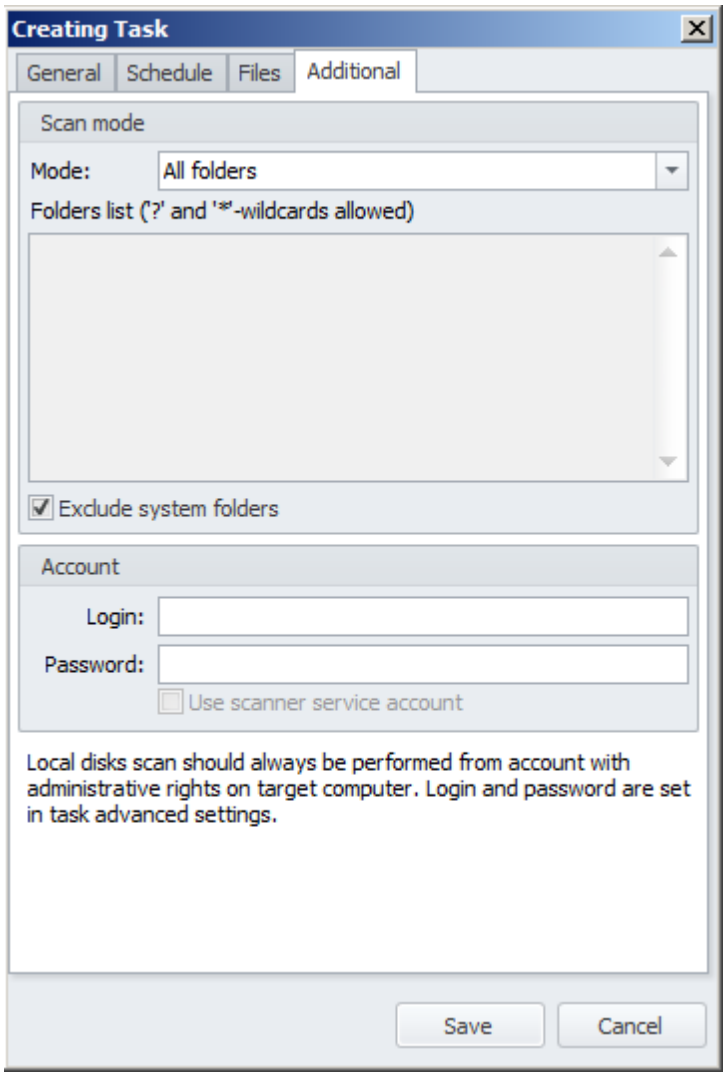
Important!

If you use *.* mask, it can significantly reduce the speed of scanning and increase loading of the Traffic Monitor Server.

7. At the **Additional** tab you can narrow down the scanned targets by setting the list of scanned folders. Also you can specify parameters of the account on behalf of which the job will be started. Scanning of local disks has to be executed on behalf of the account with the administrator rights at target workstations.

Note

To scan workstations under MS Windows Vista, MS Windows 7 or MS Windows 8 it is strongly recommended to use the domain administrator account.



Specify a necessary mode of folders scanning:

- All folders
- All folders except specified
- Only the listed folders.

By defining the folder list:

- Each folder has to be set on a separate line
- To replace of one or several symbols use symbols "?" or "*" correspondingly
- If the folder name does not have «*» at the end of a name, then symbol «*» is added automatically to the end of a string when settings saved.
- The «:» symbol is forbidden. Use masks like «C$\Windows*» или «?$\Windows*» to define the path to the directory.

This type of job has default setting **Exclude system folders**. You can view and edit the list of excluded system folders in the dialog window of setting Scanner parameters (see details in "Configuring the Crawler Scanner General Settings").

8. Click **Save**.

The saved job can be executed automatically according to the set schedule (if it was defined), or manually (as it is described in the section "Running and Stopping of the Job").

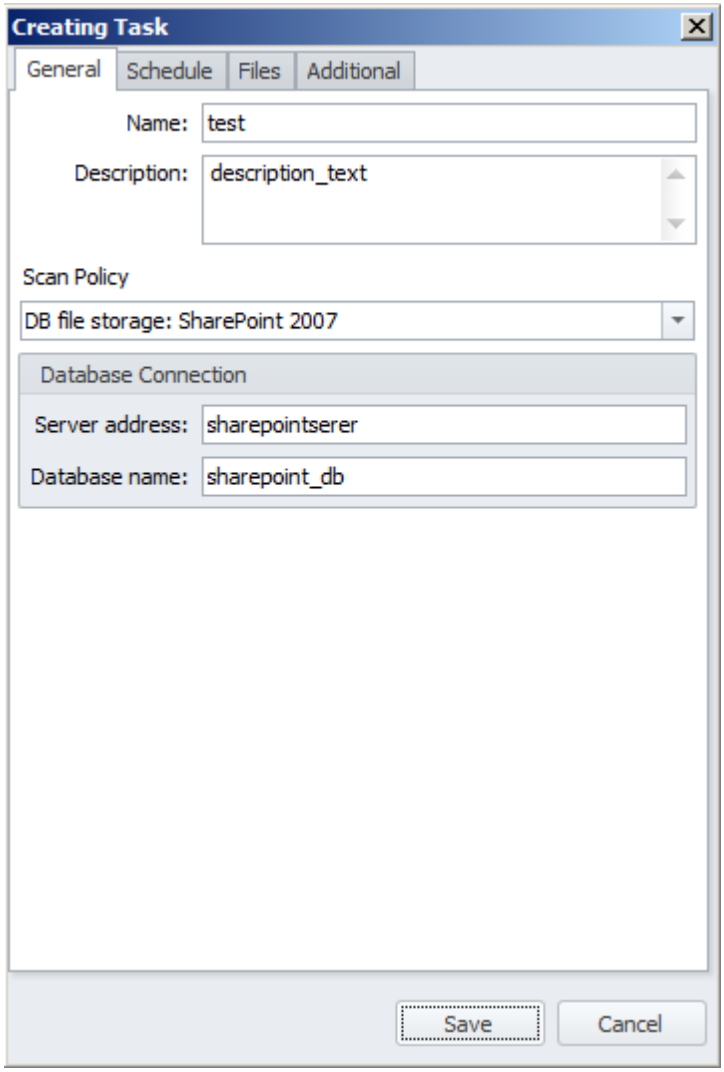
6.4.3 Scanning the SharePoint File Storage

The job of scanning the SharePoint file storage provides verification of documents which are stored in the Microsoft SharePoint 2007 database. To execute this job you need an account with the right to read data located in the checking storage (parameters of the account are set at the **Additional** tab).

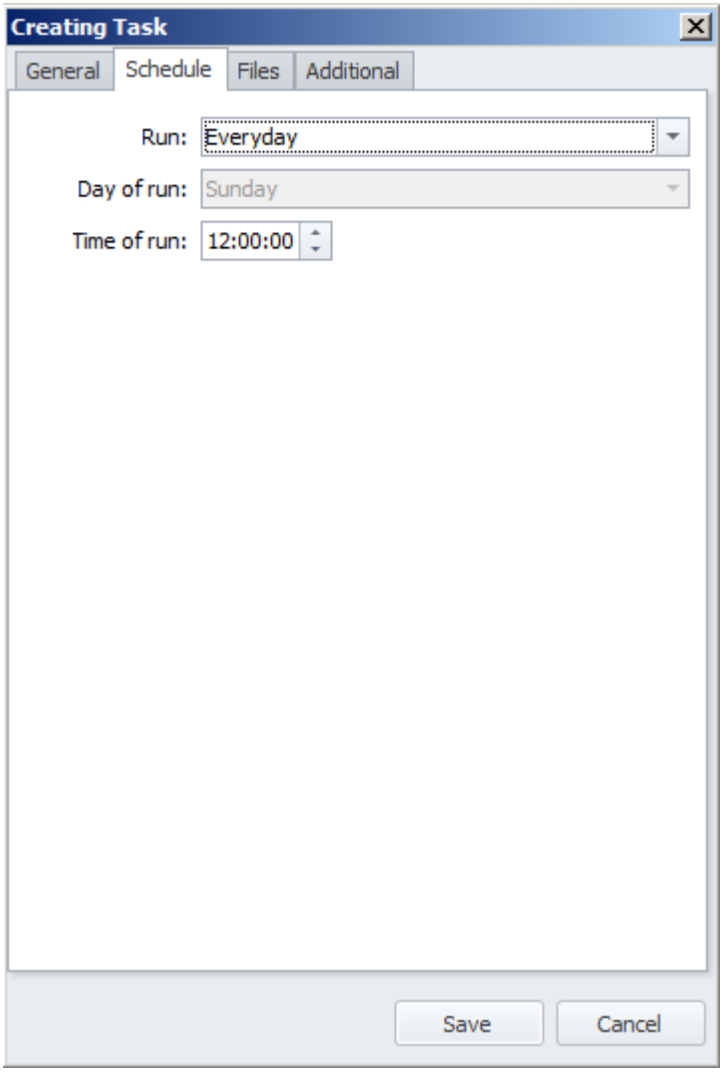
To create or change a job of scanning the SharePoint file storage:

1. Go to the **Crawler** section in the Management Console.
2. Do one of the following:
   - to create the new job, click  **Add** button located on the toolbar
   - to edit the existed job, click  **Edit** button located on the toolbar

   The job settings dialog box will appeared on the screen.
3. Define the general parameters of a job at the **General** tab:
   - **Name** – a job name.
   - **Description** – an optional field with any text.
   - **Scan Policy** – choose the **DB file storage: SharePoint 2007** from the drop-down list.



4. At **Database Connection** area set parameters of target SharePoint database :
   - **Server address** – name of SharePoint database.
   - **Database name** – name of SharePoint database instance.
5. At the **Schedule** tab set the schedule of job automatic starting.



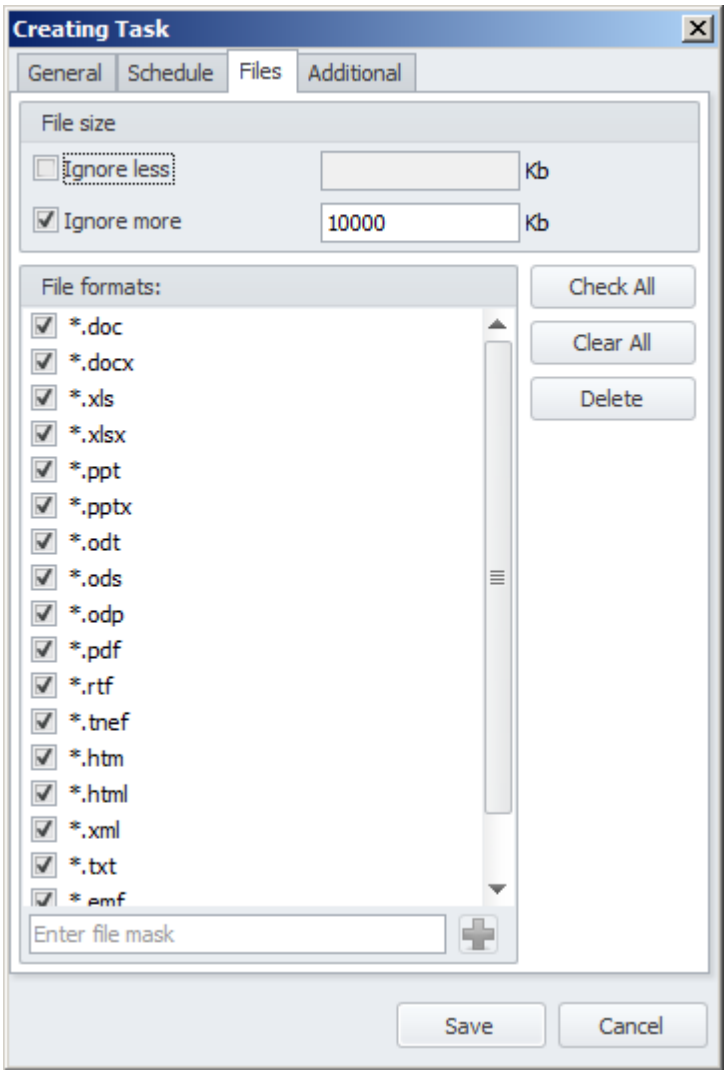
Choose one of the job start options:

- **Weekly** – specify a day of the week and time to automatic start
- **Daily** – specify a day of the week and time to automatic start
- **Manually** – in this case the job start can be executed only as described in "Running and Stopping the Job" section.

Warning!
The job won't be restarted at defined time if the previous session of this job didn't finished yet.

By default, the job is started only manually, at the user command.

6. At the **Files** tab set the sizes and formats of files which need to be sent to the analysis.



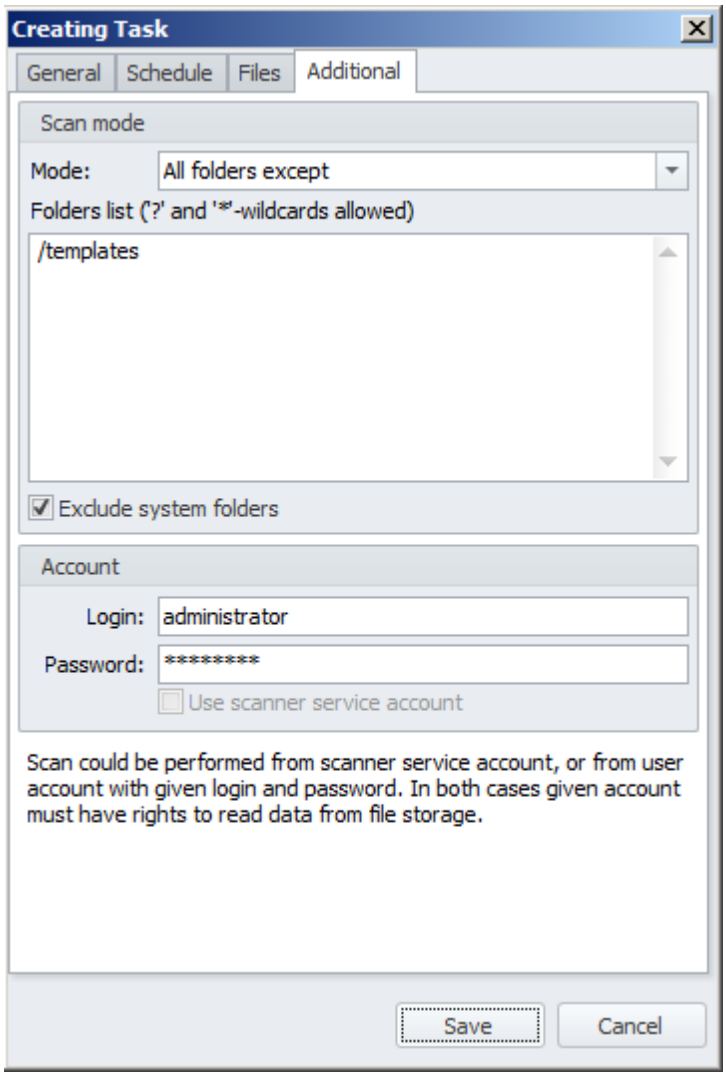
Define:

- **File size** – maximum and minimum sizes of files which need to be sent to the analysis
- **File formats** – choose the file masks in the list of preset masks or add your own masks, entering them into the field in the bottom of the list and clicking .

Warning!

If you use *.* mask, it can significantly reduce the speed of scanning and increase loading of the Traffic Monitor Server.

7. At the **Additional** tab you can narrow down the scanned targets by setting the list of scanned folders. Also you can specify parameters of the account on behalf of which the job will be started. Scanning of SharePoint database has to be executed on behalf of the account with the rights of reading data from the scanned file storage.



Specify a necessary mode of folders scanning:

- All folders
- All folders except specified
- Only the listed folders.

At the moment of defining the folder list:

- Each folder has to be set on a separate line.
- For replacement of one or several symbols you can use symbols "?" or "*" accordingly.
- At the moment of settings saving symbol «*» is automatically added in the end of string if at the indication of a folder name wasn't specified «*» at the end of a name.
- Use masks like «Windows*» to define the path, because using the «:» symbol is forbidden.

8. Click **Save**.

The saved job can be executed automatically according to the set schedule (if it was defined), or manually (as it is described in the section "Running and Stopping the Job").

6.5 Deleting the Scan Job

To delete a scan job:

1. Go to the **Crawler** section in the Management Console.
2. Choose the job in the list.
3. Do one of the following:
   - click  **Delete** button located on the toolbar.
   - right-click the job and choose  **Delete** button from the context menu.

6.6 Running and Stopping the Job

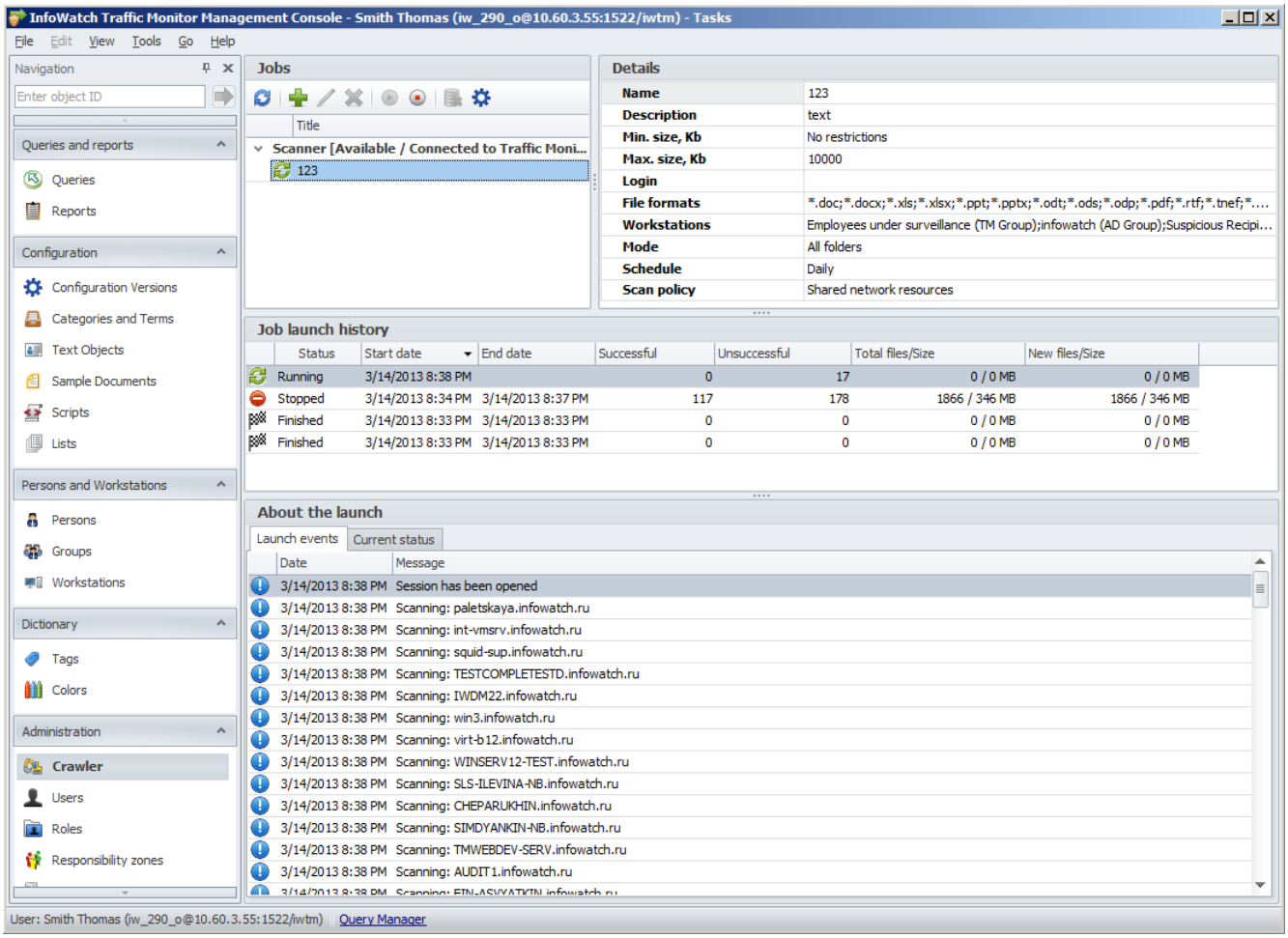
The job will be automatically executed without interference of the security officer if at job creation (see. "Creating and Editing the Scanning Job") you chose weekly or daily start on the **Schedule** tab. If you chose a **Manually** way of start, the start of a job can be executed only as described below.

The manual start of a job is also helpful if you stopped a job and then you need to restart it.

To run the scanning job:

1. Go to the **Crawler** section in the Management Console.
2. Choose the necessary job in the list.
3. Do one of the following:
   - click  **Launch** button located on the toolbar.
   - right- click the job and choose  **Launch** button in the appeared context menu.

An entry of new session with a  **Running** status will appeared in the **Job launch history** area.



Events arising during the scanning are presented on the **Launch events** tab, **About the launch** pane.

The resources, folders and files are scanned at the moment are presented on the **Current status** tab. Also the total amount of the data processed for the current session is displayed.

After session ending, the job receives the **Finished** status.

To stop a scanning job which runs:

1. Choose the running job from the list.
2. Do one of the following:
   - click **Stop** button located on the toolbar.
   - right- click the job and choose **Run** button in the appeared context menu.

The job receives **Stopped** status.

Note:

If there are many workstations scanned in the job, the stopping can take a while. Stop, Run and Edit functions for the stopping job are blocked for this period.

6.7 Cleaning the Hash Base

To provide Crawler work optimization, the storage of hashes (checksums of files) is designed. If during previous scan job session the hash of some file was saved, and in latest session of the same job the hash of this file wasn't changed, this means that the file wasn't exposed to changes and it shouldn't be sent it to executing with the Traffic Monitor server. This reduces a load of a channel between Crawler and Traffic Monitor Server, and also a load of the Traffic Monitor Server itself, and also excludes duplication of identical events for each start of a scanning job.

Features of hash base storage:

- Hash base is saved separately for each scanning job. Therefore if some file was already processed by one job, then at creation and start of another job it won't be considered.
- Hash sums are stored for files considering workstations at which these files were found. Therefore if the same file is located are at several workstations, it will be processed individually for each workstation.

It is recommended to do a periodical cleaning of hash base. For example, it is needed when the Traffic Monitor configuration was edited – in other words according new script or term list or etc, the decision if the intercepted object is a potential violation, will be accepted by system using another algorithm. As a result of cleaning the hash base, the job will "forget" that it ever processed any files, and will send all files corresponding to conditions of this job for the analysis to the Traffic Monitor Server.

To clear the hash base:

1. Go to the **Crawler** section in the Management Console.
2. Choose the necessary job in the list.
3. Do one of the following:
   - click **Purge hashes** button located on the toolbar.
   - right- click the job and choose **Purge hashes** button in the appeared context menu.

7 Configuring Objects Analysis

You can configure the way the objects are analyzed by the system using the following sections:

- Configuration Management
- Directories
- Configuring object analysis scripts

7.1 Configuration Management

A configuration is a set of different settings that are required for checking the objects by the Traffic Monitor Server, and also for monitoring and analyzing data. The Management Console (the **Configuration** section) displays the information about all versions of configuration (see "Configuration versions").

Every object transferred to the Traffic Monitor is processed according configuration version which is actual at the moment of receiving. Then the object together with applied attributes is saved to the database.

Warning!

The system does not perform the object's reprocessing according newly changed configuration.

In order to configure the settings you need to do the following:

- *Only when using the Linguistic Analysis*. Create a Classification (see "Classification").
- *Only when using the Detecting Text Objects.* Select the text object type to be detected (see "Text Objects").
- Create the lists to use for object analysis (see "Lists").
- Create a custom script to check the objects in Traffic Monitor Server (see "Object Analysis Script").

In addition, in order for the script to work properly you need to configure additional settings:

- *Only when using the Digital Fingerprints Detecting.* Create a sample document database (see "Sample Document Database").
- Create the responsibility zones for the objects to be checked by the system (see "Responsibility Zones").
- Create tags to assign to the objects (see "Tags").
- Create a set of colors to highlight the objects (see "Colors").

When the configuration is ready, you should upload it to the hosts (see "Uploading Configuration to the Hosts").

7.1.1 Configuration versions

Version of the configuration used to monitor changes in the object analysis settings. Version change management is only supported for the configuration elements. These elements are:

- Classification;
- object analysis scripts;
- lists;
- text objects.

The state of each version is defined by its status:

Configuration version status	Status description
Editable	The version is being edited. Once all the necessary settings are configured, you can upload an editable version to the host.
Active	The configuration is uploaded to Traffic Monitor Server (for the list of servers, see the **Hosts** section). Traffic Monitor Server performs the analysis of objects in accordance with the settings of this version. Active version cannot be edited
Archive	The version is stored in the database but it cannot be edited or uploaded to Traffic Monitor server

If needed, you can roll back to an earlier version of the configuration (see "Rolling Back to a Previous Configuration Version").

Note

You can return previous version only for the configuration which is saved in the database. The configuration version is changed on the host only after the configuration is re-uploaded to that host.

For more details about working with configuration versions see the following sections:

- Viewing the Configuration Information
- Adding Comments to the Configuration Version
- Comparing Two Configuration Versions
- Uploading Configuration to the Hosts
- Rolling Back to a Previous Configuration Version
- Deleting a Configuration Version

7.1.1.1 Viewing the Configuration Information

You can view the general configuration settings in the **Configuration Versions** section (the **Configuration** area in the **Navigation** pane). The configuration tree is displayed in the working area of the main window.

The working area of the main window displays the general information for each configuration version:

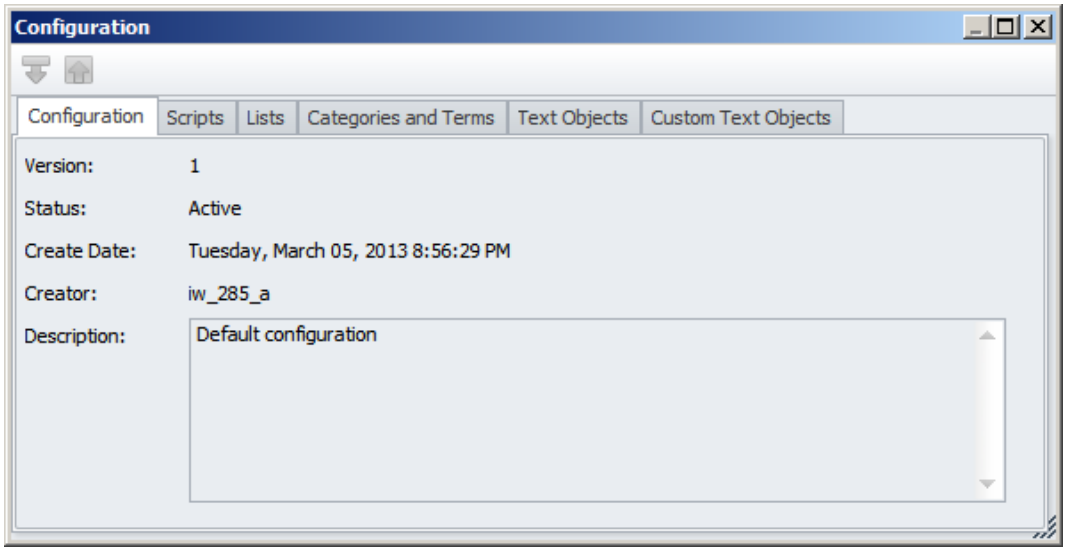
Configuration attribute	Description
Version	The number of the configuration version
Status	The current status of the version. Every configuration version can have one of the following statuses: • **Editable** (marked in green). The configuration version that is being edited. Click **Go To Editable** button located on toolbar to find this version in a list of configuration versions. • **Active** (marked in yellow). The configuration version that has been uploaded to Traffic Monitor Server. Click **Go To Active** button located on toolbar to find this version in a list of configuration versions. • **Archive**. The configuration version that has been saved.
Creation date	The date and time when the version was created
Creator	The account of the user who has saved the version
Description	Additional information about the version

To view the detailed information for a specified configuration version:

1. In the configuration tree, select a row with the required configuration version.

2. Do one of the following:
   - in the main menu, select **Edit > Details**;
   - click **Details** on the toolbar;
   - right-click the selected row and choose **Details**;
   - double-click the selected row.

   The dialog box for viewing the version settings will appear.



Viewing information for the selected configuration version

The **Configuration** tab contains the general configuration settings such as the version number, status, creation date etc. Other tabs contain detailed information about the configuration.

7.1.1.2 Adding Comments to the Configuration Version

To add a comment for a configuration version:

1. In the configuration tree, select a row with the the required version.
2. Do one of the following:
   - in the main menu, select **Edit > Change Description**;
   - click **Change Description** on the toolbar;
   - right-click the selected row and choose **Change Description**.

   In the **Editing Note** dialog box add a comment to the version and click **Save**.

7.1.1.3 Comparing Two Configuration Versions

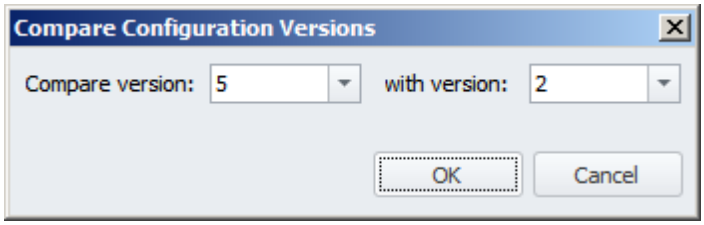
You can track the configuration changes by comparing two configuration versions.

To compare the two versions of a configuration:

1. Go to the **Configuration versions** section.

2. Do one of the following:
   - in the main menu, select **Edit > Compare**.
   - click **Compare** on the toolbar.

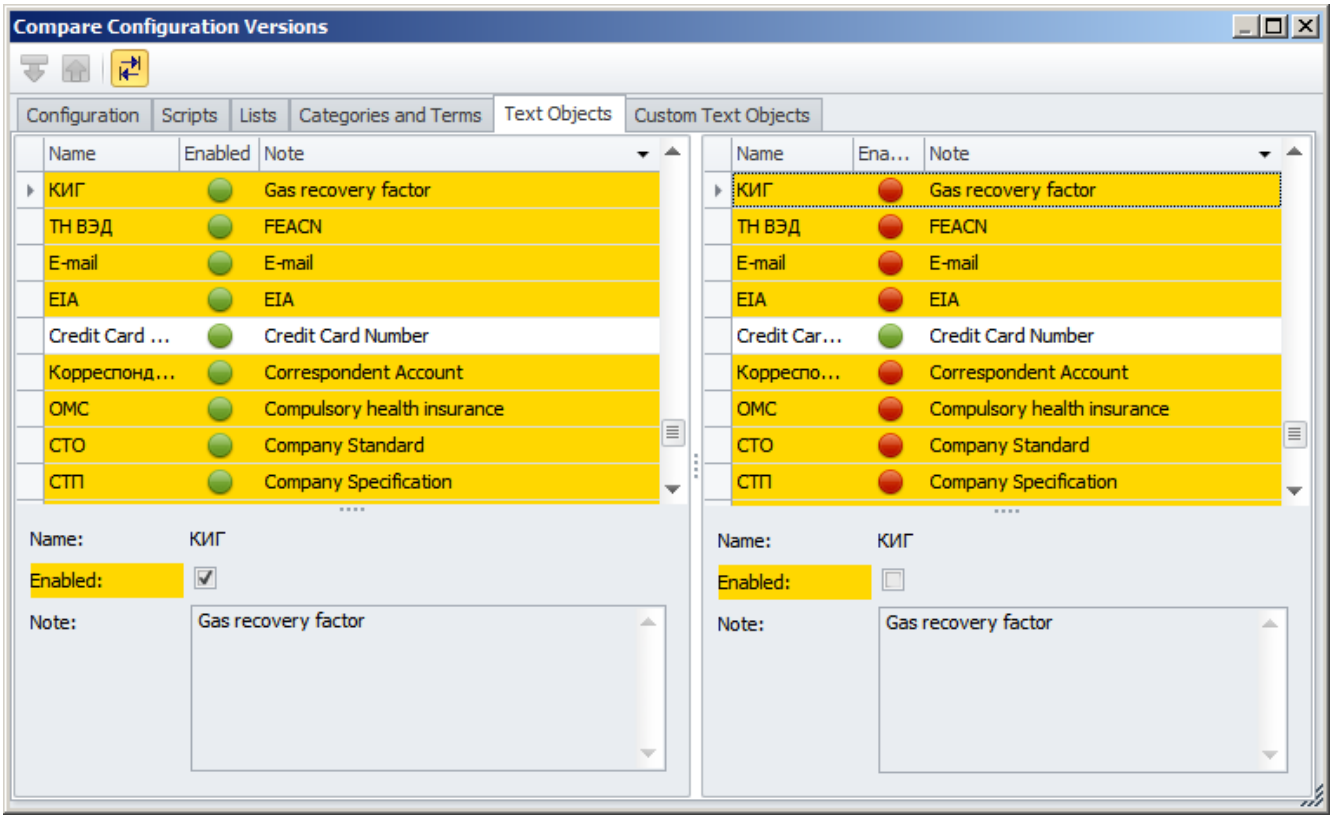
   The **Compare Configuration Versions** dialog box will appear on the screen.



Selecting the versions to compare

3. Select the necessary configuration versions and then click **OK**.

   Then the window for comparing the versions will appear.



Viewing differences between the two versions

This window is similar to the one used to display the information for one version (see "Viewing the Configuration Information"). But when the two versions are compared, the window is divided into two parts: the left part contains information about the source version, and the right part displays the information about the version being compared.

While working with the lists or tree structures, you can use the synchronized view. If the function is enabled, then you can synchronously view the matching values for both versions. To activate the synchronized view, click **Synchronize Focus**. Then the button will look like (synchronous view mode).

If the configuration is changed, the changes are highlighted with the following colors:

- **Green**. A new value is added.
- **Yellow**. The value of the existing parameter has been changed.
- **Red**. The value has been deleted.

7.1.1.4 Uploading Configuration to the Hosts

The configuration is stored in the database. The user may upload the configuration with the **Editable** status (including the Active Directory directories) to the hosts. During the update process, the host contains both the new and the old versions of the configuration. Both versions are **Active**. If an administrator navigates to the **Configuration Versions** section or updates the section data at that time, a warning is displayed saying that there are two configurations with the **Active** status.

After the update process is complete, only the newly uploaded configuration will keep the **Active** status. Updating a configuration usually takes about 10 minutes. If after 15 minutes after the update the **Configuration Versions** section still contains two **Active** versions, it indicates an error. This situation requires immediate response. It is not advised to use Management Console until the failure is resolved. Therefore, go to the **Hosts** section and check which hosts have not had their configuration updated (if a host is assigned several settings, then all the settings them should be checked). Then you should check the status of the process responsible for uploading the configuration to Traffic Monitor (to be checked by the administrator of the Traffic Monitor Server: see "*InfoWatch Traffic Monitor. Administration Guide*"). Start or restart this process. Try uploading the configuration to the hosts again.

To upload a configuration to the database:

1. Go to the **Configuration Versions** section.
2. Do one of the following:
   - in the main menu, select **Edit > Activate Editable Configuration**;
   - click  **Activate Editable Configuration** on the toolbar.

   After that, the configuration (as well as the persons and workstations directories) will be uploaded to the database. The configuration will be uploaded to the host when the host queries the database.

 **Note**

The configuration uploading may take several minutes. At the end of this process, the statuses of uploading configuration to the hosts and the active configuration version in the **Configuration Version** section will be updated.

The status of loading configuration to the host, as well as the date and time of the last update are displayed on the host profile pane (see "Working with Hosts").

7.1.1.5 Rolling Back to a Previous Configuration Version

You may want to return to a previous configuration version. You can roll back to a backup version or to the version uploaded to the host.

The rollback process is the following. The version with the **Editable** status is saved to the database and its status changes to **Archive**. The version to which the configuration is rolled back is saved in the database as the new version with the **Editable** status. A separate branch of versions is created for this configuration. You can edit the editable version again and upload it to the host.

Important!

You can revert to a previous version only if the configuration is saved in the database. The configuration version is changed on the host only after the editable configuration is uploaded to the host (see "Uploading Configuration to the Hosts").

To roll back to an older configuration version:

1. Go to the **Configuration versions** section.
2. In the configuration tree, select a row with the version to roll back to.
3. Do one of the following:
   - in the main menu, select **Edit > Rollback**;
   - click **Rollback** on the toolbar;
   - right-click the selected row and choose **Rollback**.
4. In the confirmation window, click **Yes** to confirm that you want to roll back to the selected version.

7.1.1.6 Deleting a Configuration Version

If you do not need a configuration version any more, it can be deleted from the system. You can delete any versions with the exception of:

- Version with the **Editable** status;
- Version with the **Active** status;
- Version with **Archive** status if it has been previously downloaded to the server and the database contains the objects that are connected with this version;
- The initial version (Version 0).

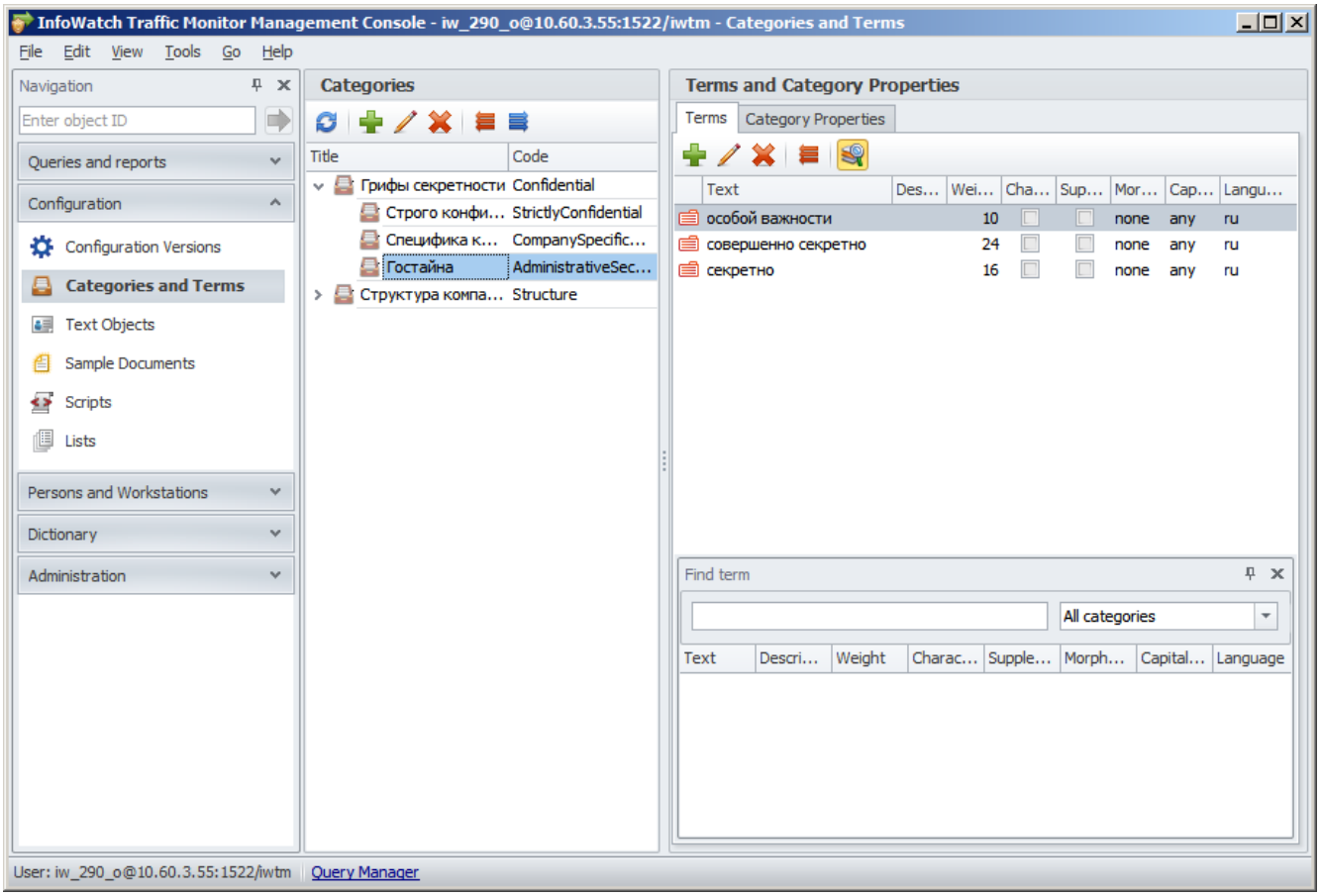
To delete a configuration version:

1. Go to the **Configuration versions** section.
2. In the configuration tree, select a row with the required version.
3. Do one of the following:
   - in the main menu, select **Edit > Delete**;
   - click **Delete** on the toolbar;
   - right-click the selected row and choose **Delete**.
4. In the dialog box that appears click **Yes**.

7.1.2 Classification

Classification is a database of a hierarchically listed (tree-organized) **categories** created by probabilistic and mathematical methods. Each category reflects characteristic aspects of some subject. Categories contain **terms** - words and phrases indicating the subject and sensitivity of a document which they belong to. For example, the *Finances* category will include financial terminology (payment, investors, prices, etc.). This way, a text that contains a term from, a certain category is matched with this category.

To work with the Classification, use the **Categories and Terms** section (the **Configuration** area on the **Navigation** pane). The working area of the main window in this section is divided into two parts. The left part contains the pane of categories; the right part contains the display area for viewing category parameters.



The Categories and Terms section

The **Categories** pane displays the **category tree** – the hierarchical list of categories. The *Category* item is represented by the icon .

To view the detailed information for a category,

in the category tree, select the row with the required category.

The settings for the selected category will be displayed in the area to the right. The **Category Properties** tab displays the general properties of the category. The information about terms is displayed on the **Terms** tab.

For more details about working with the Classification see the following sections:

- Main Principles for Creating a Classification
- Creating a Category
- Adding a Term to the Category
- Editing Categories
- Changing Categories Level
- Configuring Term Settings
- Searching for a Term
- Deleting a Category

- Exporting/Importing the Classification

7.1.2.1 Main Principles for Creating a Classification

Using the deliverable Classifications

After installing the System using the deliverable distribution kit, the typical Classification is available: English or Russian, depending on installation options. The typical configuration contains terms met in almost any field and ensures the detecting of data with subjects as *«Logistics»*, *«Law»*, *«Finances»*, *«Accounting»*, «HR» and so on.

Additionally the industrial classificatots (financial, medical, building and some other subjects) and Classification, which allows to find terms related to the violation of russian laws, can be provided. Also there are Classifications ensuring the detecting of terms in Spanish, Uzbek, Kazakh, Arabian and some other languages.

InfoWatch also provides a service of Classification customization: it can be upgraded in respect of your company specifics. Updating the industrial Classification by categories reflecting your company specifics effects in better categorization and more precise detecting of confidential information in the company data traffic. Classification customization can be performed manually by linguist experts or using the special software – InfoWatch Aulolinguist. This software allows you to automatically create a set of terms and categories based on a text collection, and allows you to evaluate the quality of the resulting set.

Installation of additional Classifications is performed by importing the provided XML file: see "Exporting/Importing the Classification".

Creating the Classification manually

To create the Classification you should create a category list and populate each category with terms. The same term could be present in several categories. For example, the *Salary* term could be included in *Internal payments* and *Working conditions* categories.

When making a Classification of the checked objects into categories it is important to keep in mind how many terms were found in the analyzed text, how often each of these terms appear in the document, and to what type this term belongs. The term types are:

- **Characteristic**. If a text contains a characteristic term that referrers to a certain category, the text is classified as referring to this category. The weight of terms is calculated for these terms for the purpose of obtaining additional statistic information.
  Example: The *Finances* category has the characteristic term *Financial report*. If the phrase "financial report" is found at least once in the text of an intercepted object, then the text will be considered relevant to the Finances category.
- **Standard**. The standard terms (as opposed to the characteristic ones) cannot absolutely indicate whether the text belongs to a certain category. The decision as to whether the text corresponds to the category or not is made according to the total weight of all terms of this category were found in the text. When calculating the overall weight sum of terms, both the standard and the supplementary terms belonging to the same category are taken into account.
- **Supplementary**. The supplementary terms are used as additional terms: their weight will be considered when calculating the total weight of standard terms.

Linguistic analysis of an object can take into account the inflection (morphology). The morphology settings are configured when configuring the term settings (see "Configuring Term Settings"). The Classification supports morphology for the following languages:

- Russian (ru)
- English (en)
- French (fr)
- German (de)

- Spanish (es)
- Italian (it)
- Arabic (ara)
- Ukrainian (ukr)

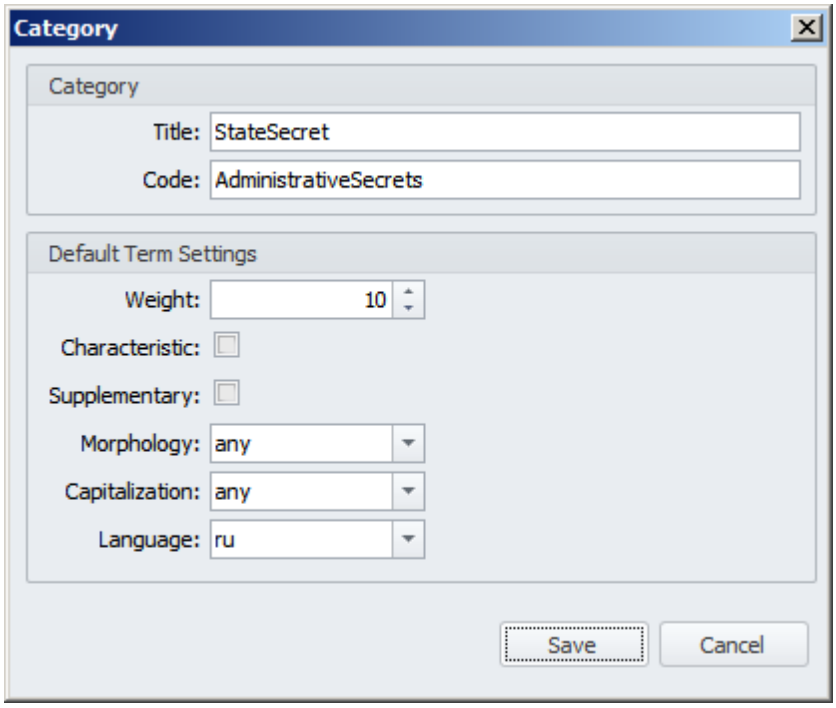
Also the System checks a longer list of supported languages for full-matching of defined terms in the analyzed text.

7.1.2.2 Creating a Category

To create a category:

1. Go to the **Categories and Terms** section.
2. To create a subcategory, in the category tree, select the name of the parent category.
3. Do one of the following:
   - in the main menu, select **Edit > New Category**;
   - click **New Category** on the Categories pane.

   The **Category** dialog box will appear on the screen.



Configuring settings for a category

4. Configure the category settings.

   On the **Category** pane, configure the general settings:

   - **Name**. Category name (mandatory). The names are not required to be unique. However, it is not advised to use the same name for categories.
   - **Code**. The code name of the category that will be used when creating a script (mandatory). This name may include English letters, digits, and underscores; and must not start from the letter. The code should be unique.

On the **Default Term Settings** pane, configure the settings for the terms in this category (see " Configuring Term Settings"). The specified values will be used as the default values for all terms of this category.

5. Click **Save**.

Once the new category will be added to the Classification, you'll need to compile a list of terms for this category. You can add a term to the category in several ways:

- Create a Term
- Import Terms from a File
- Move a Term from Another Category

7.1.2.3 Adding a Term to the Category

You can add terms to a category in one of the following ways:

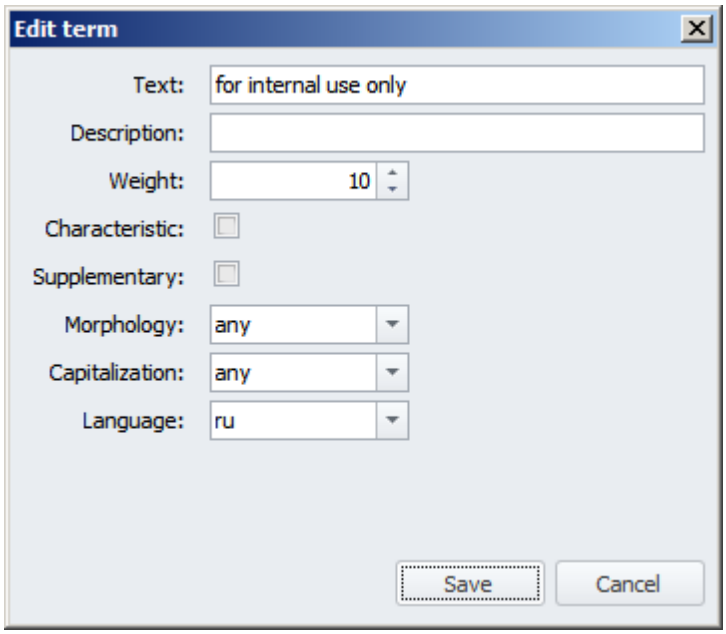
- Create a Term
- Import Terms from a File
- Move a Term from Another Category

7.1.2.3.1 Creating a Term

To create a term:

1. Go to the **Categories and Terms** section.
2. In the category tree, select the category you need.
3. In category settings area, go to the **Terms** tab.
4. Do one of the following:
   - in the main menu, select **Edit >Term > New**;
   - click  **New Term** on the toolbar of the **Terms** tab.

   The **Term** dialog box will appear on the screen.



Configuring term settings

5. Set up the term settings (see "Configuring Term Settings").
6. Click **Save**.

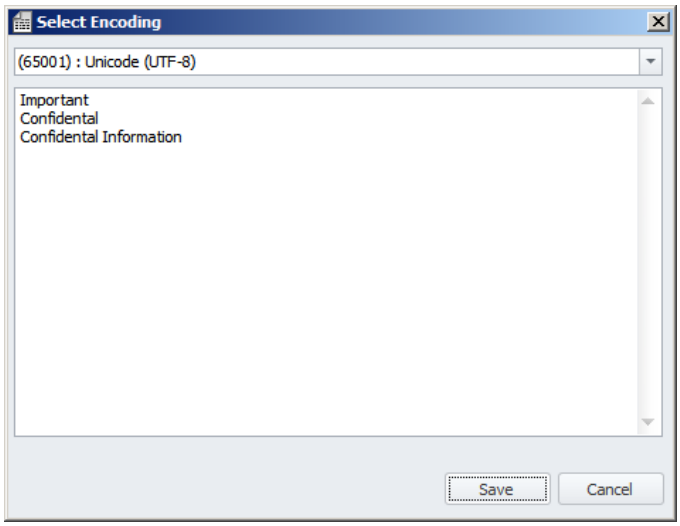
7.1.2.3.2 Importing Terms from a File

You can import terms into the Classification from the `TXT` files.

To import a term:

1. Go to the **Categories and Terms** section.
2. In the category tree, select the category you need.
3. In category settings area, go to the **Terms** tab.
4. Click **Import** in the top part of the **Terms** tab.
5. In the dialog box that appears, select the required text file and click **Open**.

   A dialog box with the content of the selected file will appear on the screen.



Configuring settings for imported terms

6. In the top part of the window, select a character set from the drop down list.

7. Edit the text so that each line contains one term. Delete the terms you do not want to import. If necessary, add more terms.

   Important!

   The changes you make in this dialog box impact only the import of terms and do not impact the original text file.

8. Click **Save** to start importing.

As the result, the terms are imported to the selected category. Terms are being imported with the default settings. After the import is complete, you can modify the term settings (see "Configuring Term Settings").

7.1.2.3.3 Moving a Term from Another Category

To move a term to another category:

1. Go to the **Categories and Terms** section.

2. In the category tree, select the category containing the term you need.

3. In the category settings area, go to the **Terms** tab.

4. Click the term you want to move. Keep the mouse button pressed and point the name of the target category to move the term to. Once the yellow arrow appears to the left of the name of the selected category, release the mouse button.

7.1.2.4 Editing Categories

The following operations are available when editing a category:

- modifying the category settings;
- adding a new term to a category;
- editing a term in the category;

- deleting a term from the category.

To modify the settings of a category:

1. Go to the **Categories and Terms** section.
2. In the category tree, select the category you need.
3. Do the following:

Necessary step	Procedure
Change the category settings	1. Do one of the following: • in the main menu, select **Edit > Edit**; • click  **Edit** on the category pane. • double-click the selected category. 2. In the **Category** dialog box, configure the required settings (see "Configuring Term Settings"). 3. Click **Save**.
Add new term to the category	The procedure is described on the following sections: • Creating a Term • Importing Terms from a File • Moving a Term from Another Category
Edit the term properties	1. In category settings area, go to the **Terms** tab. 2. On the terms pane, select the required term. 3. Do one of the following: • in the main menu, select **Edit > Term > Edit**; • click  **Edit** on the **Terms** pane; • double-click the selected term. In the **Term** dialog box, configure the required settings (see "Configuring Term Settings"). 4. Click **Save**.
Delete the term from the category	1. In category settings area, go to the **Terms** tab. 2. On the terms pane, select the required term. 3. Do one of the following: • in the main menu, select **Edit > Term > Delete**; • click  **Delete** on the **Terms** pane; • right-click the selected row and choose  **Delete**.

Necessary step	Procedure
	4. In the confirmation box, click **Yes** to confirm.

7.1.2.5 Changing the Level of a Category

To change the level of a category:

1. Go to the **Categories and Terms** section.
2. Select the title of the specified category.
3. Do one of the following:
   - Click the title of the category you want to move down. Then keep the mouse button pressed and point the name of the parent category for the category being moved. Once the yellow arrow appears to the left of the name of the selected category, release the mouse button.
   - To move the category up, press and hold the <**SHIFT**> key. Click the title of the category you want to move. Then keep the mouse button pressed and point the name of any category at the target level. Once the blue arrow appears to the left of the selected content category, release the mouse button.

   As a result of one of those two actions, the content category will be moved to the selected level.

7.1.2.6 Configuring Term Settings

Term settings are configured in the **Term Settings** dialog box.

All settings except **Text** and **Description** have default values. The default values are used when configuring settings for a category and are applied to all the terms of this category.

General Term Settings:

- **Text**. The text of the term (mandatory). It must be unique within the category.

  Note

  The content analysis processes only the letters of the supported languages.

- **Description**. Additional information (optional).

The following settings impact the decision of matching the text with the term category:

- **Weight**. How characteristic is the term for the given category. Value in an integer between 0 and 25. By default the value of the term weight is set when the category settings are configured (see "Creating a Category").
- Term type. Each term can be of only one type. To select the term type, select the **Characteristic** or **Supplementary** checkbox. If these checkboxes are cleared, the term is considered *Standard* (default value).

Note

For the description of the term types see "Main Principles for Creating a Classification"

Text search rules:

- **Morphology**. This setting specifies the morphology usage mode for searching terms in a text. This setting can have the following values:
  - **any**: morphology is used. All word forms are considered valid results.
  - **none**: morphology is not used. Only exact matches are considered valid results.

  The default value is **any**.

- **Capitalization**. This setting specifies the case sensitivity for searching terms in text. This setting can have the following values:
  - **any**: the search is case-insensitive;
  - **native**: the search is case-sensitive.

Important!

Selecting **native** will disable the morphology.

The following reference types are available:

Reference type	Reference description	Example
lowercase	Every reference word contains lowercase letters	trading agreement
titlecase	Every reference word starts with an uppercase letter	John Smith
uppercase	Every reference word contains uppercase letters	ACCEPTATION REPORT
nocase	Reference contains characters, case insensitive (digits, punctuation marks, etc.)	256

If **native** option is selected, the results will be as follows ("+" means that this term will be found):

Word in text	Reference			
	lowercase	titlecase	uppercase	nocase
lowercase	+	–	–	–
titlecase	–	+	–	–

Word in text	Reference			
	lowercase	titlecase	uppercase	nocase
uppercase	–	–	+	–
nocase	–	–	–	+

- **no** – all the letters of the term found in the text should be lowercase;
- **all** – all the letters of the term found in the text must be uppercase;
- **first** – the first letter of the found term should be capitalized;
- **word** – first letters of all words of the found term must be capitalized.

The default value is **any**.

- **Language**. Term language.

7.1.2.7 Searching for a Term

To find a term:

1. Go to the **Categories and Terms** section.
2. In the category tree, select the category for searching for a term. If you do not know what category may contain the term, select any category.
3. In category settings area, go to the **Terms** tab. The bottom part of the tab contains the **Find term** pane.

   Note

   To hide or to show the **Term Search** pane, click **Find** in the top part of the **Terms** tab.

4. On the **Find term** pane, enter the required term into the field on the left.

   Note

   The term search is case-insensitive.

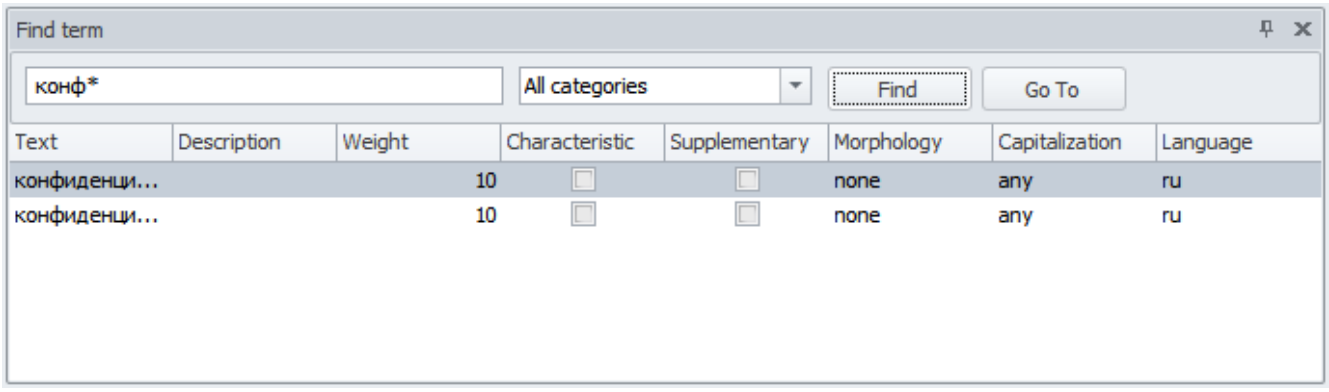
   When searching for a term, you can use wildcards: "*****" for a group of characters and "**?**" for a single character.

   To search for phrases, enter the entire phrase or use wildcards.

5. From the drop down list located more to the left of the **Find** button, select the search method:
   - **All categories**. The term is searched in all categories.
   - **Current category**. The term is searched only in the selected category. If you select this method of search, then you must select the required category in the category tree.
6. Select the category and click **Find**.

The search results are displayed in the viewing area on the **Term Search** pane.

To navigate to the category of the found term, select a row with this term and click **Go To**.



The term search results

7.1.2.8 Deleting a Category

To delete a category:

1. Go to the **Categories and Terms** section.
2. In the category tree, select the category you need.
3. Do one of the following:
   - in the main menu, select **Edit > Delete**;
   - click **Delete** on the toolbar;
   - right-click the selected category and choose **Delete**.
4. In the confirmation box, click **Yes** to confirm.

7.1.2.9 Exporting/Importing the Classification

You can export the Classification to a hard disk, to a network folder, or to a removable media. The Classification is exported as an XML file and can be reloaded to the system later on.

Note

You can export the Classification that is included in a configuration with the **Editable** status.

Categories and terms are exported with all their settings except for the term notes.

To export or import a Classification, use the **Categories and Terms** section (the **Configuration** area on the **Navigation** pane).

Important!

If you already have a Classification, importing will result in adding the new Classification to the existing one. If the category names in the current Classification are the same as the category names in the imported Classification, then these categories will be replaced by the imported ones.

To export a Classification:

1. Go to the **Categories and Terms** section.
2. Do one of the following:
   - in the main menu, select **Edit > Export**;
   - click **Export** on the categories pane.
3. In the **Save as** dialog box, select a folder to save the Classification and the name of the XML file.
4. Click **Save** to export the Classification to an XML file.

To import a Classification:

1. Go to the **Categories and Terms** section.
2. Do one of the following:
   - in the main menu, select **Edit > Import**;
   - click **Import** on the toolbar.
3. In the **Open** dialog box, select an XML file to import the Classification from.
4. Click **Open** to start importing the Classification from the XML file.

Once the Classification is imported, the Classification information will appear in the **Categories and Terms** section.

7.1.3 Lists

A list is a set of elements of the same type that is used in a script to generate the object analysis rules (see " Configuring Object Analysis Scripts (LUA)").

For example, if you know static IP addresses of the servers that cannot transmit sensitive information (i.e. they only update software), these addresses can be consolidated in a separate list. Then you can put a condition in the script that checks if the sender's IP address is in the list (see example in the section "Search for a String in a List).

Note

It's strictly recommended to consider sets of sender, recipient, and workstation data (e.g. names, e-mails, domains etc.) using the person directory (see "Persons Directory") and use them in the scripts using the methods described in "Search for a Sender in a Group", "Search for a recipient in a group", "Search for a Workstation in a Group".

The lists are consolidated into list groups. The list groups can also be used to define the object analysis rules in the scripts.

The following list groups are pre-defined: *File Types* and *Web Resources*. They are used only to assign tags to the objects from the corresponding preset tag groups, *File types* and *Web resources*. Preset lists cannot be modified.

Note

The pictograms of unchangeable lists, elements of lists and groups of lists include a sign of system files - a gear wheel (cogwheel). Changeable lists, elements of lists and groups of lists haven't such sign.

Example:

- *Unchangeable* lists, elements of lists and groups of lists.
- *Changeable* lists, elements of lists and groups of lists.

To work with lists, use the **Lists** section (the **Configuration** area on the **Navigation** pane).

Guidelines of working with lists

1. The lists in a script should be set in the Management Console.
2. A list can contain set of values for any property that can be assigned to an object in the process of analysis and processing. These properties are described in the InfoWatch Traffic Monitor data model (see "InfoWatch Traffic Monitor Data Model").
3. All values in the list should be of the same type. For example, you can't put both IP addresses and host domain names in the same list.

For more details about working with lists see the following sections:

- Creating a List Group
- Creating a List
- Creating a List Item
- Editing a List or a List Group
- Viewing and Filtering List Items
- Deleting a List or a List Group

7.1.3.1 Creating a List Group

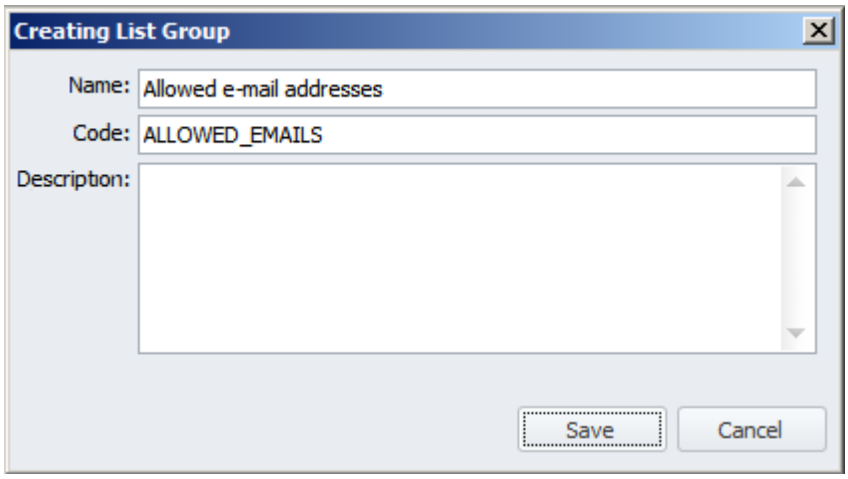
Note

The system can contain a maximum of 4,194,304 list groups.

To create a list group:

1. Go to the **Lists** section.
2. Do one of the following:
   - in the main menu, select **Edit > New List Group**.
   - click **Creating List Group** on the tag groups pane.

   The **New List Group** dialog box will appear on the screen.



Creating a list group

3. Specify the list group settings:
   - **Name**. List group name (mandatory).
     The name should be unique.
   - **Code**. The list group name to will be used when creating a script (mandatory).
     The list group code name may include English letters, digits, and underscores. It should start with a letter.
     The list group code should be unique.
   - **Description**. Additional information about the list group.
4. Click **Save**.

After the list group is created, you should populate it with lists (see "Creating a List").

Note

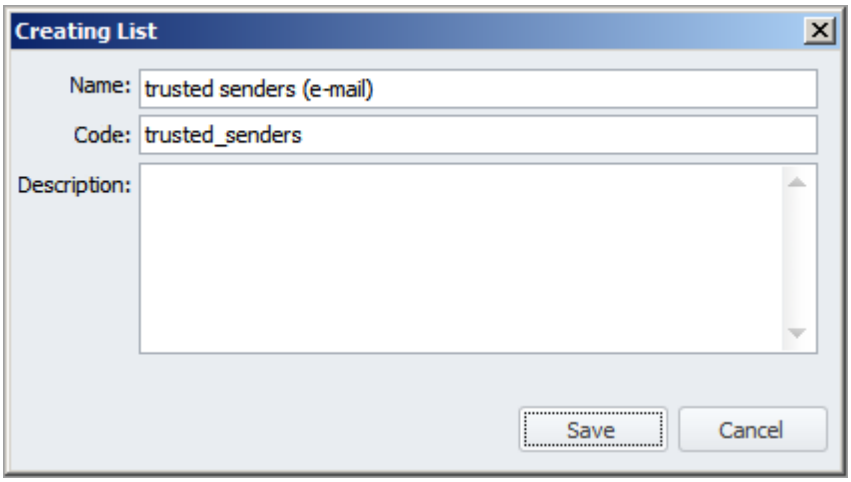
You can populate the group with list by creating new lists (see "Creating a List"), and by moving lists between groups. To move the list from one group to another, click the name of the list you need to move. Then keep the mouse button pressed and point the name of the group to add the list to. Once a yellow arrow appears to the left of the name of the selected group, release the mouse button.

7.1.3.2 Creating a List

To create a list:

1. Go to the **Lists** section.
2. If a list should be included in a list group, select the group in the list of lists.
3. Do one of the following:
   - in the main menu, select **Edit > New List**;
   - click **New List** on the toolbar.

   The **New List** dialog box will appear.



Configuring list settings

4. Specify the list settings:
   - **Name**. List name (mandatory). The name should be unique.
   - **Code**. The list name to be used when creating a script (mandatory).
     List code name may include English letters, digits, and underscores. It should start with a letter. The code should be unique.
   - **Description**. Additional information about the list.
5. Click **Save**.

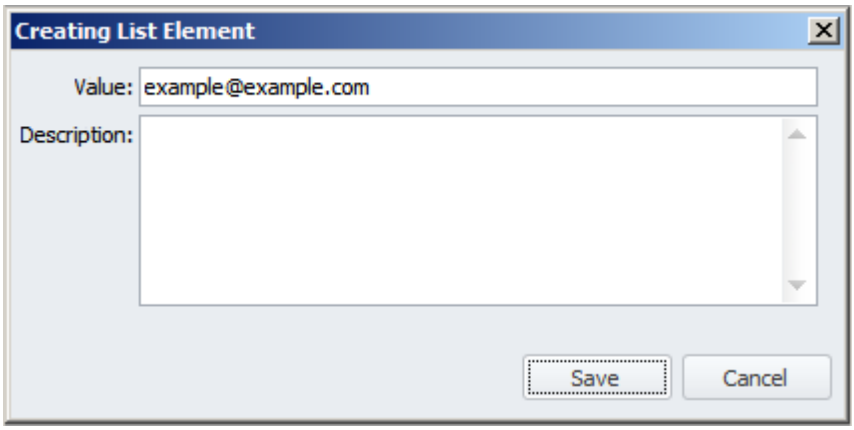
After creating a new list you should populate it with data (see "Creating a List Item").

7.1.3.3 Creating a List Item

To create a list item:

1. Go to the **Lists** section.
2. On the list pane, select the required list.
3. Do one of the following:
   - in the main menu, select **Edit > List Element > New**;
   - on the List Item pane, click **New list item**.

   The **Creating List Element** dialog box will appear on the screen.



Configuring settings for a list item

4. Specify the item settings:
   - **Value**. A list item value defined in the format specified for this list type (mandatory).
   - **Description**. Additional information about the item.
5. Click **Save**.

Repeat the steps 3-4 to add other items to the list.

7.1.3.4 Editing a List or a List Group

The following operations are available when editing lists:

- editing list group properties
- editing list properties
- adding a new item to a list
- editing an item in a list
- deleting an item from a list.

To edit a list:

1. Go to the **Lists** section.
2. On the list pane, select the name of the required list (list group).
3. Do the following:

Necessary step	Procedure
Edit the list (list group) settings: list name, code, description.	1. Do one of the following: • in the main menu, select **Edit > Edit**; • click **Edit** on the **Lists** pane. • double-click the selected list (list group). 2. In the **List** or **List Group** dialog box, configure the required settings (see "Creating a List Group"; "Creating a List").

Necessary step	Procedure
	3. Click **OK**.
Add a new item to a list	See: "Creating a List Item"
Edit list item options (value, code, description)	1. On the list pane, select the required list item. 2. Do one of the following: • in the main menu, select **Edit > List Item > Edit**; • click **Edit** on the **List Elements** pane. • double-click the selected list item. In the **List Item** dialog box, configure the required settings (see " Creating a List Item"). 3. Click **OK**.
Delete the item from the list	1. On the list pane, select the required list item. 2. Do one of the following: • in the main menu, select **Edit > List Item > Delete**; • click **Delete** on the **List Elements** pane; • right-click the selected row and choose **Delete**. 3. In the confirmation box, click **Yes** to confirm. **Note:** Exclude the deleted item from text of every script where it was used.

7.1.3.5 Viewing and Filtering List Items

Only the first 1000 items are shown when viewing lists on the items pane. You can narrow down the set of displayed items by filtering the displayed list items..

To filter a list:

1. Go to the **Lists** section.
2. In the list tree, select the name of the list to filter.
3. Please enter the filtering template in the list items pane in the **Filter** field.

   Note

   List item filtering is case-insensitive.

   You can use wildcards in filtering patterns: "*****" for a group of characters and "**?**" for a single character.

4. Enter the filtering pattern and click **Apply**.

The results are displayed in the viewing area on the List Items pane.

The details on the item numbers are displayed in the bottom part of the items pane:

- **Shown** – number of shown list items;
- **Filtered** – number of entries matching the set filtering template;
- **Total** is the a total number of items in the selected list.

You can save the filtering settings when moving between lists. Clear the field **Filter** and click  to cancel the filtration.

7.1.3.6 Deleting a List or a List Group

To delete a list (list group):

1. Go to the **Lists** section.
2. On the list pane, select the name of the required list (list group).
3. Do one of the following:
   - in the main menu, select **Edit > Delete**;
   - click  **Delete** on the Lists pane;
   - right-click the selected row and choose  **Delete**.
4. In the confirmation box, click **Yes** to confirm.

 **Note**

Exclude the deleted list (list group) from text of each script where it was used.

7.1.4 Object Analysis Script

A **script** is a set of rules used to analyze and process all the intercepted objects. To work with analysis scripts, use the **Scripts** section (the **Configuration** area on the **Navigation** pane).

After the installation, the Management Console contains a default script that is active. Active script (marked with ) is used to analyze the objects in Traffic Monitor Server. The other scripts are disabled (marked with ). To change the object verification rules in Traffic Monitor Server you need to configure and activate your own script.

 **Important!**

The script is written in the LUA programming language. For more information about writing scripts see "Configuring Object Analysis Scripts (LUA)".

For more details about working with scripts see the following sections:

- Creating a Script
- Loading a Script from a File
- Editing a Script

- Activating a Script
- Saving a Script to a File
- Deleting a Script

7.1.4.1 Creating a Script

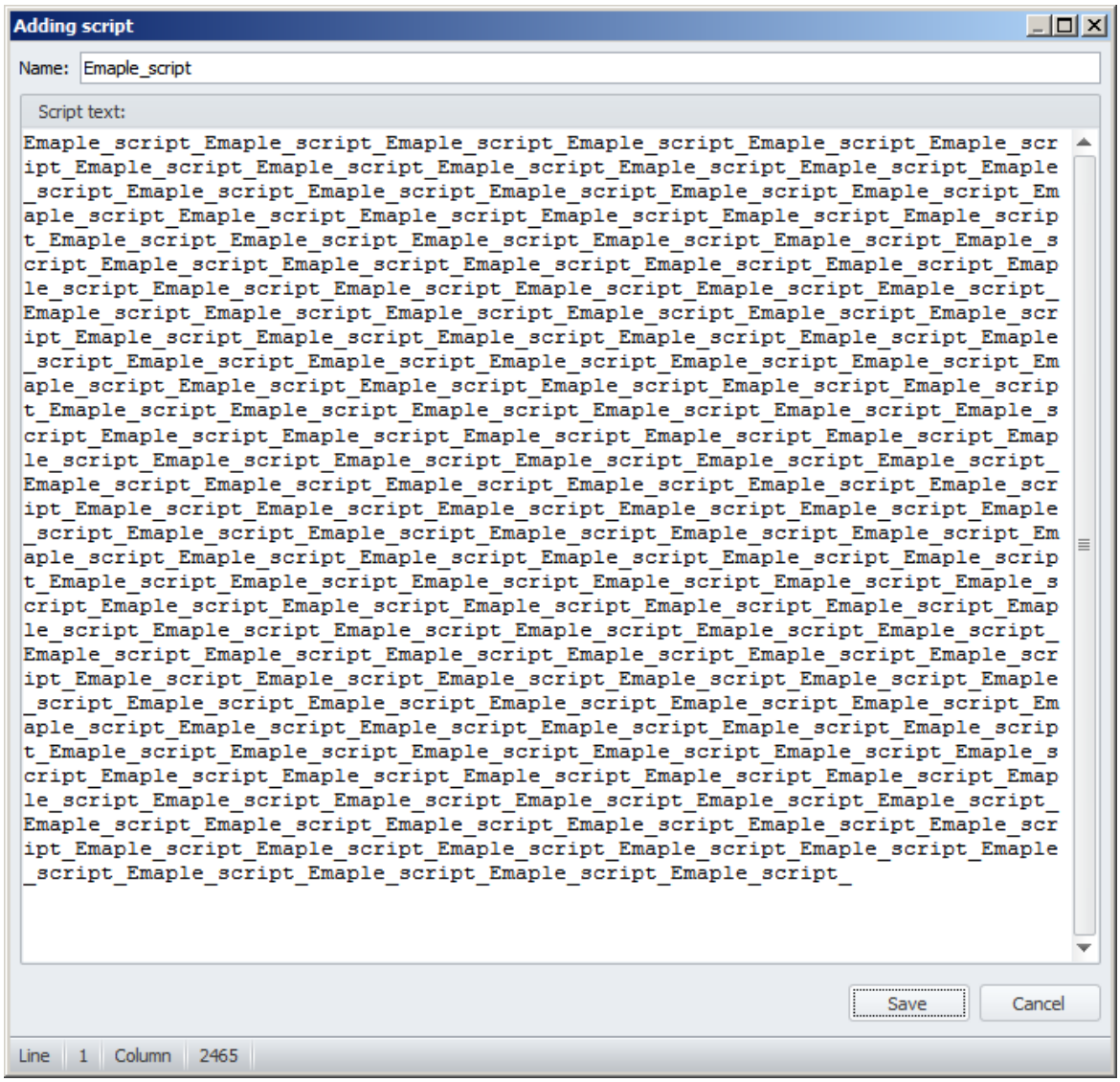
Important!

A configuration may contain several scripts. However, only one script can be active at any given moment.

To create a script:

1. Go to the **Scripts** section.
2. Do one of the following:
   - in the main menu, select **Edit > New Script**;
   - click **New** on the toolbar.

   The **New Script** dialog box will appear.



Configuring a script

3. Configure the general settings of the script:
   - **Name**. Script name (mandatory). The name should be unique.
   - **Script text**. In the text field, type the script text.

   Important!

   The script is written in the LUA programming language. For more information about writing scripts see "Configuring Object Analysis Scripts (LUA)".

   Script text can be large enough, so it is convenient to use text search and replaces. Press **Ctrl + F**: the standard Windows text searching dialog will be displayed.

4. Click **Save**.

7.1.4.2 Loading a Script from a File

The object analysis scripts in the files (see "Saving a Script to a File") can be loaded into Management Console.

To load a script from a file:

1. Go to the **Scripts** section.
2. Do one of the following:
   - in the main menu, select **Edit > Load from File**;
   - click **Load from File** on the toolbar.
3. In the **Open** dialog box, select a LUA file to load the script from.
4. Click **Open** to start importing the script from the LUA file.

7.1.4.3 Editing a Script

To edit a script:

1. Go to the **Scripts** section.
2. In the script list select the row with the required script.
3. Do one of the following:
   - in the main menu, select **Edit > Edit**;
   - click **Edit** on the toolbar;
   - double-click the selected script.
4. In the **Edit Script** dialog box, edit the script settings. You can change the script name or its text.

   Important!

   The script is written in the LUA programming language. For more information about writing scripts see "Configuring Object Analysis Scripts (LUA)".

   Script text can be large enough, so it is convenient to use text search and replaces. Press **Ctrl + F**: the standard Windows text searching dialog will be displayed.
5. When all necessary script settings are changed, click **Save**.

7.1.4.4 Activating a Script

A configuration may contain several scripts. However, only one script will be loaded within the Traffic Monitor Server configuration — the one that is currently active.

To activate a script:

1. Go to the **Scripts** section.

2. In the script list select a row with the script you need to activate.
3. Do one of the following:
   - in the main menu, select **Edit > Activate**;
   - click **Activate** on the toolbar.

The selected script becomes active and the other scripts are going to be inactive.

7.1.4.5 Saving a Script to a File

You can save scripts to a hard disk, to a network folder, or to a removable media. The script is saved in the LUA file format and can be loaded back into the system (see "Loading a Script from a File").

To save the script to a file:

1. Go to the **Scripts** section.
2. Do one of the following:
   - in the main menu, select **Edit > Save to File**;
   - click **Save to File** on the toolbar.
3. In the **Save as** dialog box, select a folder to save the script to and the name of the LUA file.
4. Click **Save** to export the script to the LUA file.

7.1.4.6 Deleting a Script

To delete a script:

1. Go to the **Scripts** section.
2. In the script list select the row with the required script.
3. Do one of the following:
   - in the main menu, select **Edit > Delete**;
   - click **Delete** on the toolbar.
4. In the confirmation box, click **Yes** to confirm.

7.1.5 Text Objects

Text objects are data with the fixed structure. These objects are passport numbers, credit card numbers, phone numbers, e-mail addresses, social security numbers, bank account requisites, Classification codes, registration numbers etc.

In the content text analysis, the system can detect text objects using preset templates. The system has a number of preset templates for the most common text object types. To search text objects using these templates you need to include them in configuration that is uploaded to the host. For more information about including and

excluding text objects from the configurations see "Enabling and Disabling a Text Object and its Values"; for more information about uploading configurations to hosts see "Uploading Configuration to the Hosts".

Example:

Only the *E-mail address* text object type is enabled in the configuration loaded to the host.

The following letter text is being checked:

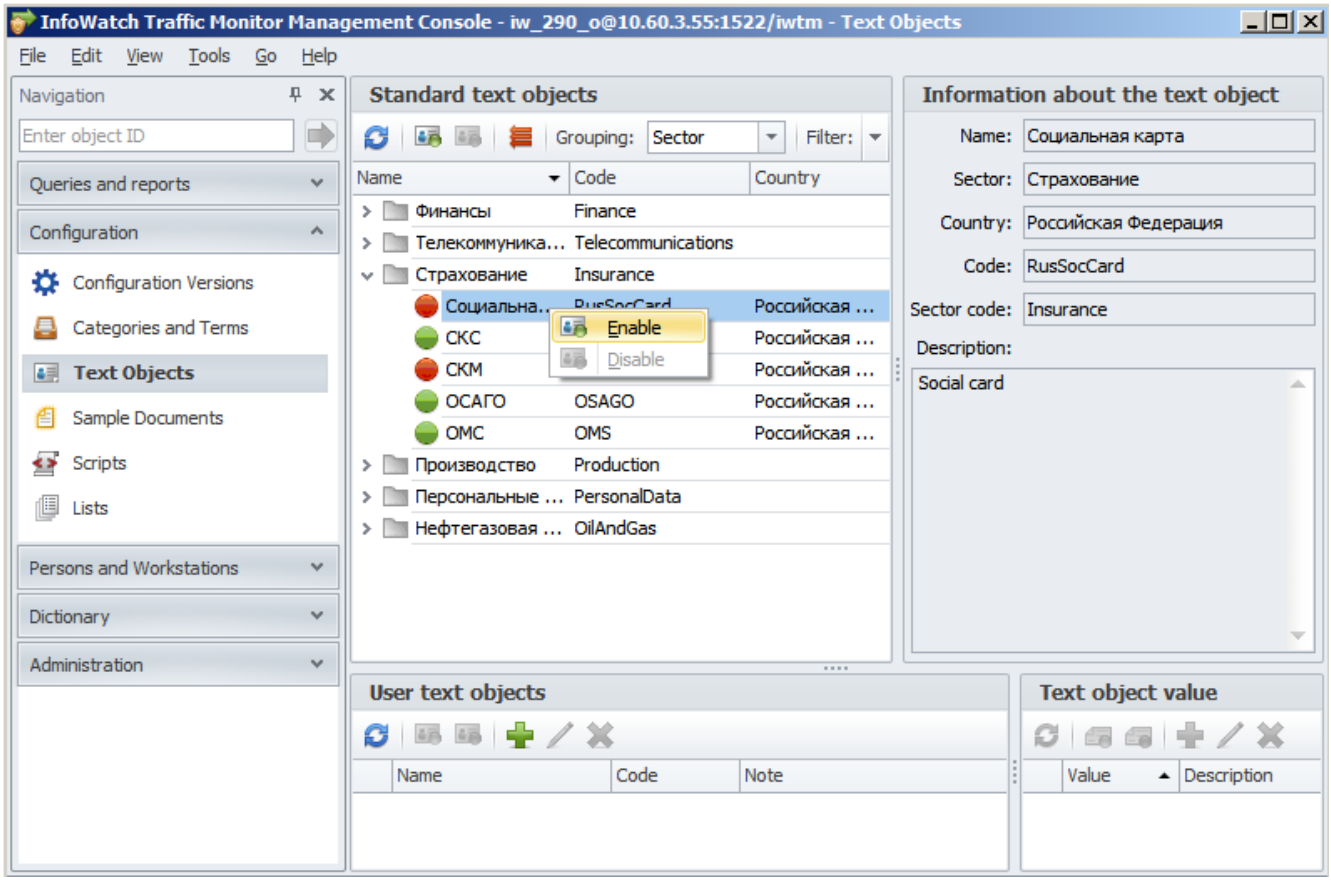
Sending you the data that might be of interest: belov@company.com, phone: 357-4555, sedov@company.ru, phone: 357-3586.

The analysis detects two text objects of the *E-mail address* type:

belov@company.com

sedov@company.ru

The phone numbers *357-4555* and *357-3586* won't be detected because the *Phone number* text object type is not enabled in the server configuration.



Text objects section

To work with text objects, use the **Text Objects** section (the **Configuration** area on the **Navigation** pane).

The system supports two types of text objects:

- **Standard text objects**: they are preset, cannot be modified or deleted. You can only include them into a configuration or exclude them from it.
- **User text objects**: created by the users, can be modified or deleted.

Information about chosen standard text object is displayed on Information pane. Data is presented on sections:

- **Name** - the object name in System;
- **Sector** - belonging of object to financial, production or other branch;
- **Country** - the state to which the object belongs;
- **Code** - the unique identifier of object;
- **Sector code** - the unique identifier of branch of object;
- **Description** - explaining information on object.

For more details about working with text objects see the following sections:

- Creating and Editing a User Text Object
- Adding Values to a User Object
- Enabling and Disabling a Text Object and its Values
- Deleting a User Text Object and its Value

7.1.5.1 Uploading Standard Text Objects from XML-files

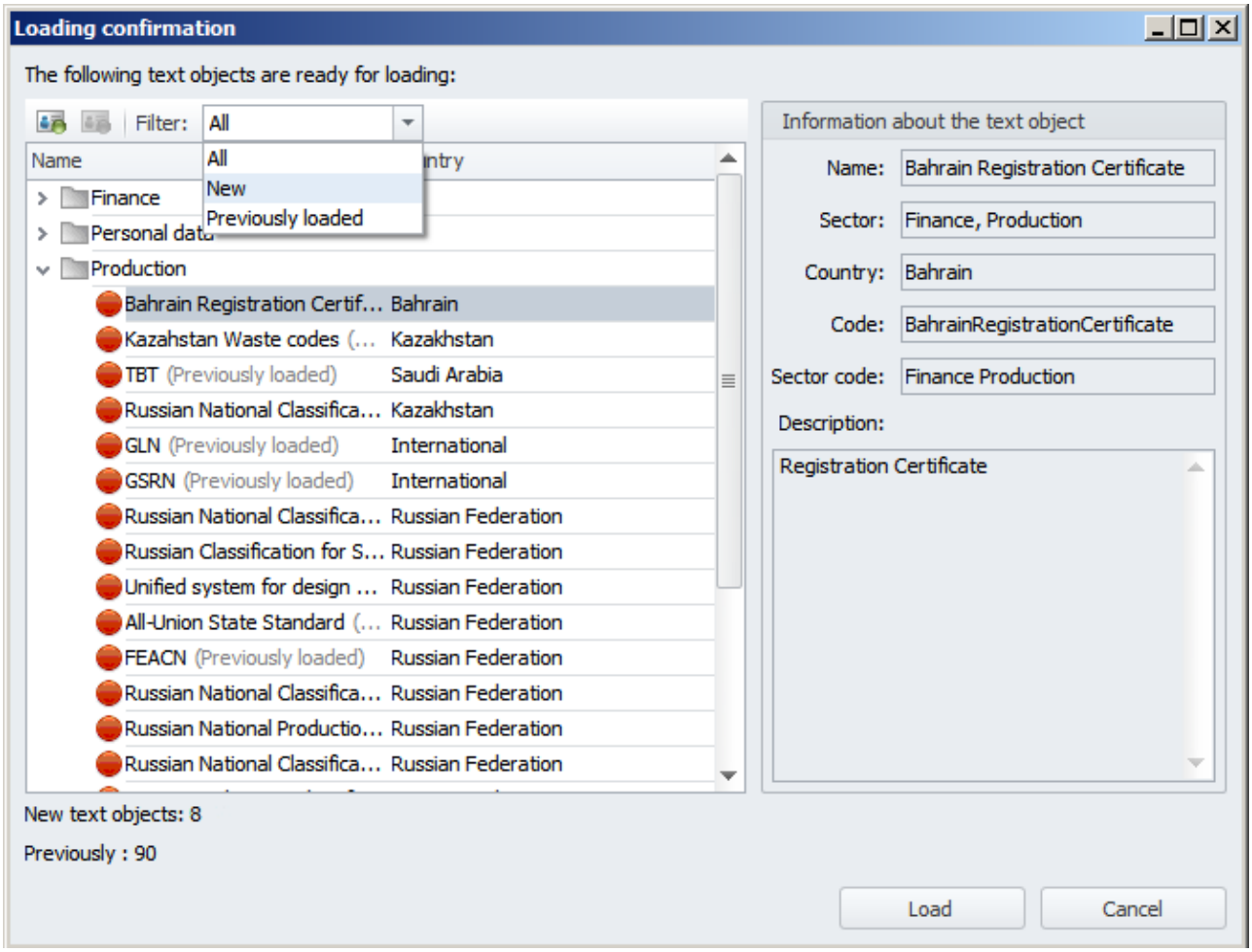
The standard text objects storing in XML files, can be loaded into the Management Console. XML files can be delivered within updatings or by request.

To load standard text objects from the XML file:

1. Go to the **Text objects** section.
2. Click  **Load from file** button located on toolbar.
3. In **Open** dialog box choose the XML file contains the object.
4. Click **Open** to start object's importing from the XML file.
5. Choose the object or objects in the appeared list of objects.
6. Click Download to add chosen files to Management Console.

If you execute the filtration in **Downloading confirmation** dialog box, the objects categories will appeared:

- all objects;
- the new;
- the earlier downloaded.



Choosing the filtration type

You can also turn on or off any new object by clicking **Enable** or **Disable** buttons located on toolbar (see " Enabling and Disabling a Text Object and its Values"). By default, all objects are switched off.

Note

If the standard text documents was downloaded earlier, you can't enable or disable it in **Downloading confirmation** dialog box.

7.1.5.2 Creating and Editing a User Text Object

Note

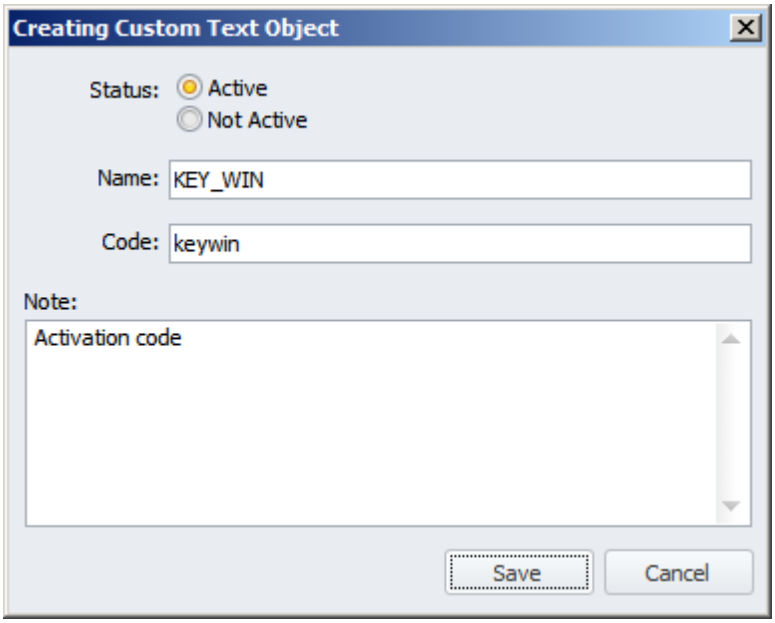
standard text objects are not editable.

To create or edit a text object:

1. Go to the **Text Objects** section.
2. Do the following:

Action	Procedure
New text object	Do one of the following: • in the main menu, select **Edit > User Text Objects > Add** • in the **User text objects** area click **Add** on the toolbar
Edit text object	1. In the user text objects list, select the row with the required record. 2. Do one of the following: • in the main menu, select **Edit > User Text Objects > Edit**; • in the **User text objects** area click **Edit** on the toolbar; • double-click the selected row.

A dialog box with the text object settings will appear on the screen.



User text object

3. Specify the text object settings.
   - **Status**. If you want to be able to use the text object in text search scripts after uploading the configuration to the content analysis server, please select the **Active** check box.
   - **Name**. Text object name.
   - **Code**. The text object designation name to will be used when creating a script (mandatory).
     The code name may include English characters, digits and underscore. It should start with a letter. The code should be unique.
   - **Note**. Additional information about the text object.
4. Click **Save**.

To create a user text object you should also specify its values according to the section "Adding Values to a User Object".

In order to be able to search for active text objects, you should upload the updated configuration to the host. For

more information see "Uploading Configuration to the Hosts".

7.1.5.3 Adding a Values of User Text Object

Important!

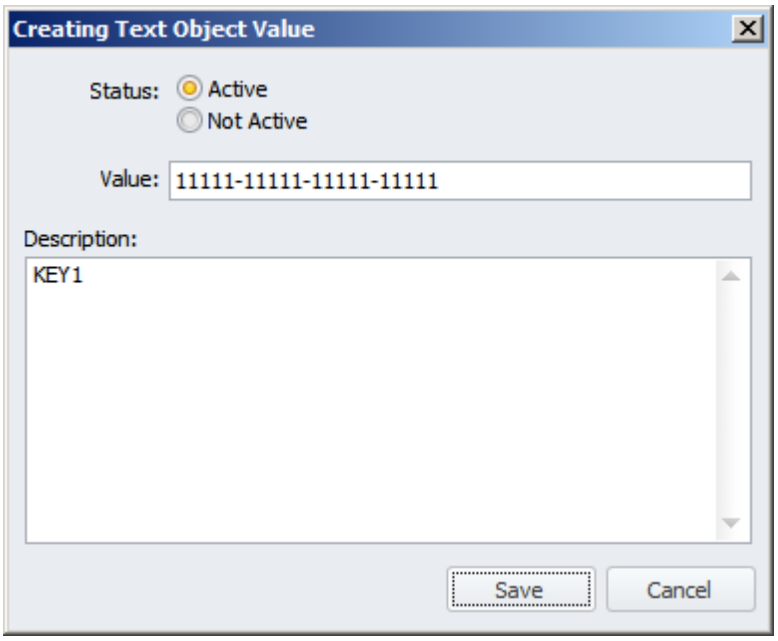
Every user object can have a maximum of 256 active values.

To create or edit an item in the user object values list:

1. Go to the **Text Objects** section.
2. In the **User text objects** area select the required text object.
3. Do the following:

Action	Procedure
Create the text object value	Do one of the following: • in the main menu, select **Edit > Text Object Values > Add** • on the **Text Object Values** area toolbar, click **Add**
Edit the text object value	1. In the **Text Object Values** area select the required row. 2. Do one of the following: • in the main menu, select **Edit > Text Object Values > Edit**; • on the **Text Object Values** area toolbar, click **Edit**; • double-click the selected row.

The dialog box with the text object settings will appear on the screen.



Text object value

4. Specify the item settings:
   - **Status**. If you want to be able to use the text object value in text search scripts after uploading the configuration to the content analysis server, please select the **Active** check box.
   - **Value**. Text object values.
   - **Description**. Additional information about the value.
5. Click **Save**.

Repeat the steps 3-5 to add other values.

In order to be able to search for active text object values, you should upload the updated configuration to the host. For more information see "Uploading Configuration to the Hosts".

7.1.5.4 Enabling and Disabling a Text Object and its Values

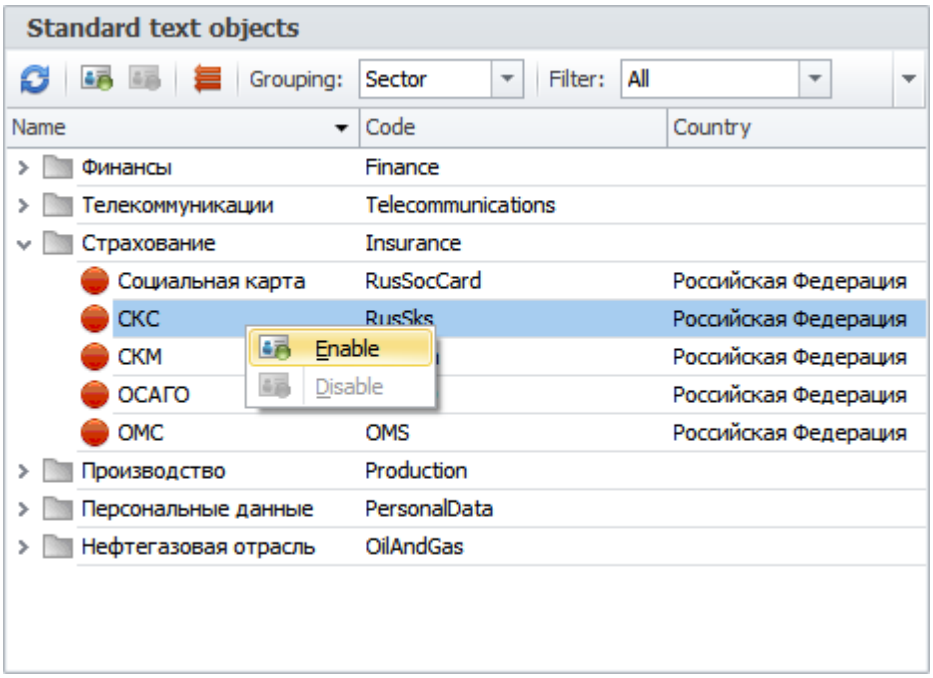
Important!

Each text object list (typical objects or user objects) can contain up to 256 active objects.

To include a text object in the configuration:

1. Select one or more text objects in the **Text Objects** pane.
2. Do one of the following:
   - right-click the selected object and choose **Enable** ;
   - click in the top part of the text objects pane
   - in the main menu, select **Edit > Standard Text Objects > Enable** (for standard text objects) or **Edit > User Text Objects > Enable** (for user text objects).

The text object will become *Active*.



Enabling the text object

To exclude a text object from the configuration:

1. Select one or more text objects in the **Text Objects** pane.
2. Do one of the following:
   - click in the top part of the text objects pane.
   - right-click the selected object and choose **Disable**;
   - in the main menu, select **Edit > Standard Text Objects > Disable** (for standard text objects) or **Edit > User Text Objects > Disable** (for user text objects).

The text object will become *Inactive*.

Important!

Every user object can have a maximum of 256 active values.

To include a text object value into a configuration:

1. In the **User Text Objects** area, select the text object with the value you want to include.
2. On the **Text Object Values** pane, select the required value.
3. Do one of the following:
   - on the **Text Object Values** pane, click .
   - right-click the selected value and choose **Enable** ;
   - in the main menu, select **Edit > Text Object Values > Enable**.

   If the text object is inactive, then the search won't process the value. In this situation a message will appear with the prompt to activate the text object itself. To activate a text object, click **Yes**.

The text object value will become *Active*.

7.1.5.5 Deleting a User Text Object and its Values

> **Note**
>
> Standard text objects cannot be deleted.

To delete a text object value:

1. Go to the **Text Objects** section.
2. In the **User Text Objects** pane, select the required row.
3. In the **Text Object Values** pane, select the required value.
4. Do one of the following:
   - in the main menu, select **Edit > Text Object Values > Delete**;
   - on the **Text Object Values** pane, click **Delete**;
   - right-click the selected value and choose **Delete**.
5. In the confirmation box, click **Yes** to confirm.

To delete a text object:

1. Go to the **Text Objects** section.
2. In the **User Text Objects** pane, select the required row.
3. Do one of the following:
   - in the main menu, select **Edit > User Text Objects > Delete**;
   - in the **User Text Objects** pane, click **Delete**.
4. In the confirmation box, click **Yes** to confirm.

7.1.5.6 Groupping and Filtration of Records

Grouping and filtration functions were realized for convenience of viewing of standard text objects.

There are two types of group of objects: territorial (Country) and thematic (Branch). By default, objects are grouped with the Segment parameter

To group records,

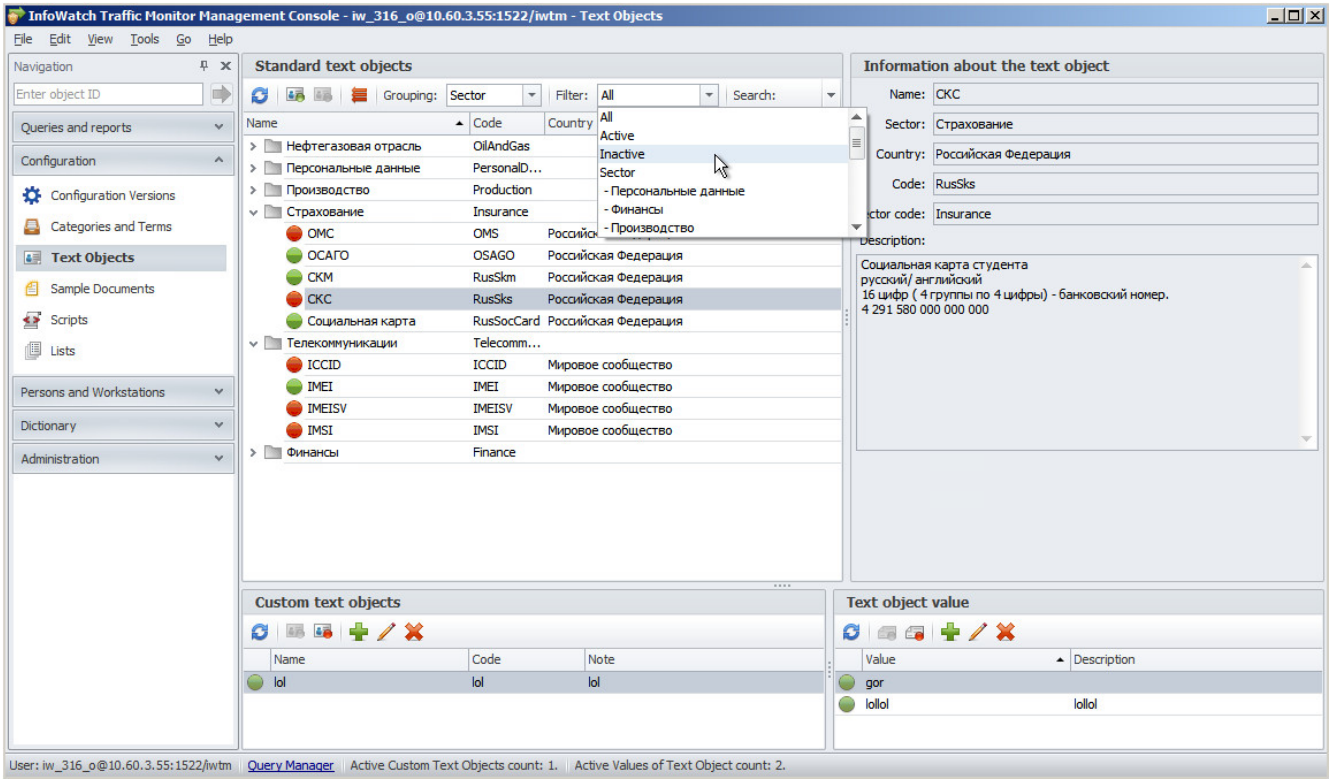
choose the necessary parameter in the dropping list at control pane.

Filtration helps to eliminate elements viewing witch is no need. The filtration type "All" is chosen by default, and the System displays all objects. You can also apply other types of a filtration:

- only the active;
- only the inactive;
- corresponding to one of branches;
- corresponding to one of the countries.

To filter records,

choose the necessary parameter of a filtration in dropping list at control pane of **Standard text objects** pane.



Group and filtration of standard text objects

Records on the panel are displayed in the curtailed mode. To unroll the group, press the button located to the left of value of parameter of group. To curtail group, press the button.

7.1.6 Sample Document Database

Sample document database is a set of typical documents that are used in the *Digital Fingerprints technology*. This technology allows to search for the quotes from the sample document database in the text of the intercepted objects (letters, files, print jobs etc.). The sample documents can consist of the texts related to the confidential documentation (e.g. orders, financial statements, agreements, etc.). After the digital fingerprints are created, the sample documents are unavailable to view for users and administrators.

Important!

If several hosts are present (see "Working with Hosts"), the Digital Fingerprint Analysis using the sample documents can only run on one host.

For more details about working with the sample documents database see the following sections:

- Creation of the Sample Documents Database
- Editing Sample Document Information
- Deleting a Sample Document
- Grouping of Records

7.1.6.1 Creation the Sample Documents Database

Creation of sample document database includes the following processes:

1. Adding sample documents.
2. Capturing digital fingerprints of the sample documents.

Important!

Please note that capturing digital fingerprints does not involve storing the document in the database. The database contains just individual quotes from the document. These quotes are encrypted, and there is no possibility to restore the original document based on these quotes. This way all the sensitive information that may exist in the sample documents remains undisclosed.

To work with the sample document database, use the **Sample Documents** section (the **Configuration** area on the **Navigation** pane).

To add one or more sample documents to the database:

1. Do one of the following:
   - in the main menu, select **Edit > Add Sample Document**;
   - click **Add Sample Document** in the top part of the sample document pane.
2. In the dialog box that appears, select one or more documents to be loaded to the sample documents database You can select several documents at once by holding keys Shift or Ctrl.

   Note

   By default, the added file can't exceed 128 Mb. At the moment of adding the document exceeding the admissible size, the corresponding warning will be displayed. Administrator of System configures the value of the maximum available size: see the document "InfoWatch Traffic Monitor. Administration Guide".
3. Click **Open**.

As a result, the document is going to be added into the database with the *New* status. The sample document is automatically assigned the following properties: **ID**, **Path**, **Filename**, **Status**, **Size**, **Type**, **Create date** (date and time), **Insert date** (data and time of adding to the database).

The **Title**, **Author**, and **Note** fields are blank by default. You can add the necessary information in these fields, if needed (see "Editing Sample Document Information").

Note

For some document types (such as Word documents) the information about the title and the author is extracted from the document properties when the digital fingerprint is captured.

In order to use a sample document for the text analysis, you need to capture a digital fingerprint of the the document.

To generate digital fingerprints for all sample **documents with the *New* status,**

do one of the following:

- in the main menu, select **Edit > Create sample documents**;
- click **Create sample documents** in the top of the sample documents pane.

When complete, each sample document receives the *Digital fingerprint is generated* status.

Important!

You can left-click on the document status if it is accompanied by the pictogram or to see notification with the description of problems in creation of a digital print.

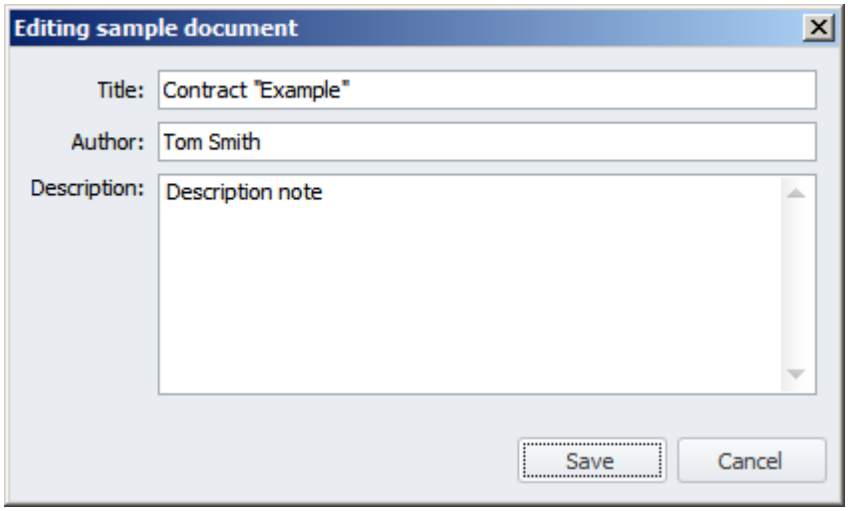
7.1.6.2 Editing Sample Document Information

You can edit information on documents with any status.

To edit sample document information:

1. Go to the **Sample Documents** section.
2. On the sample document pane, select the required sample document.
3. Do one of the following:
   - in the main menu, select **Edit > Edit**;
   - click **Edit** in the top part of the sample document pane;
   - double-click the selected sample document.

   The **Sample document** dialog box will appear on the screen.



Adding a sample document to the database

4. Please specify sample document properties:
   - **Title**. Name in the sample document database.
   - **Author**. The user who has uploaded this sample document to the database.
   - **Comment**. Additional information.
5. Click **Save**.

7.1.6.3 Deleting a Sample Document

You can remove the sample document in two cases:

If the digital print for this document wasn't created yet and, therefore couldn't be used earlier in the analysis. It belongs to documents with the status *New* and the *Error of processing*. In that case you can completely remove the document and record about it.

Documents with any other statuses (*Expects processing*, *Is being processed*, *The Digital print is ready*, *Error of removing*) can be removed, but record about it remains. Such reference documents receive the status *Is removed* and won't be used any more in the text analysis

Important!

One a document has been deleted, it cannot be restored. If you need to use the deleted sample document again, you should upload it to the database again and capture its digital fingerprint (see "Creation of the Sample Documents Database").

To delete a sample document:

1. Go to the **Sample Documents** section.
2. On the sample document pane, select the required sample document.
3. Do one of the following:
   - in the main menu, select **Edit > Delete**;
   - click **Delete** in the top of the sample document pane.
4. In the confirmation box, click **Yes** to confirm.

Then, the document will have the *Deleted* status and it won't be used for text analysis any longer.

7.1.6.4 Grouping of Records

You can use grouping for convenience of viewing the entries in the big table. You can group records using one or more headings (columns) of the table. This possibility is available only in the section **Sample documents**.

To group records:

1. Click on the necessary parameter in the line with headings of the table.
2. Holding the button, drag column heading on the group pane. The name of parameter used to grouping of records will be displayed on the group pane.

To group the records using several headings, repeat steps 1 – 2 for all headings assigned to participate in grouping.

Note:

You can change the order of grouping, interchanging the position of headings. The column which heading is located at the top on the left side participates in grouping earlier than others.

Records on the panel are displayed in the curtailed mode. To unroll the group, press the button located to the left of value of parameter of group. To curtail group, press the button.

You can cancel grouping on one or several parameters, deleting headings from the group scheme.

To cancel grouping of records on any parameter:

1. Click on heading which you want to remove from the scheme on the pane of group, and, holding the button, drag it in a line of headers of the table. Location of a column will be specified by two arrows.
2. To choose the necessary situation, move the column header along a line of headers and then release the left button of a mouse. As a result the column will be moved on the chosen place.

7.1.7 Responsibility Zones: objects access differentiation

Responsibility zones are used to restrict user access to the intercepted objects. The objects belonging to a certain responsibility zone are visible to the users who belong to the same responsibility zone (provided that the user has privileges to view or/and work with the objects).

To configure and manage the responsibility zones, use the **Responsibility Zones** section (the **Configuration** area on the **Navigation** pane).

Each object can belong to one responsibility zone at the same time. Presence of the object in one or another responsibility zone is determined based on responsibility zone placement conditions (detection of category, AD or TM groups, tags, text objects or sample document attributes) (see "Creating and Editing a Responsibility Zone") and their priorities (see "Changing Responsibility Zone Priorities"). The processed objects can be moved from one responsibility zone to another (see "Moving Object to Another Responsibility Zone") according to the list of available transitions defined for the current zone (see "Creating and Editing a Responsibility Zone").

For more details about working with responsibility zones see the following sections:

- Creating and Editing a Responsibility Zone
- Changing Responsibility Zone Priorities
- Deleting a Responsibility Zone

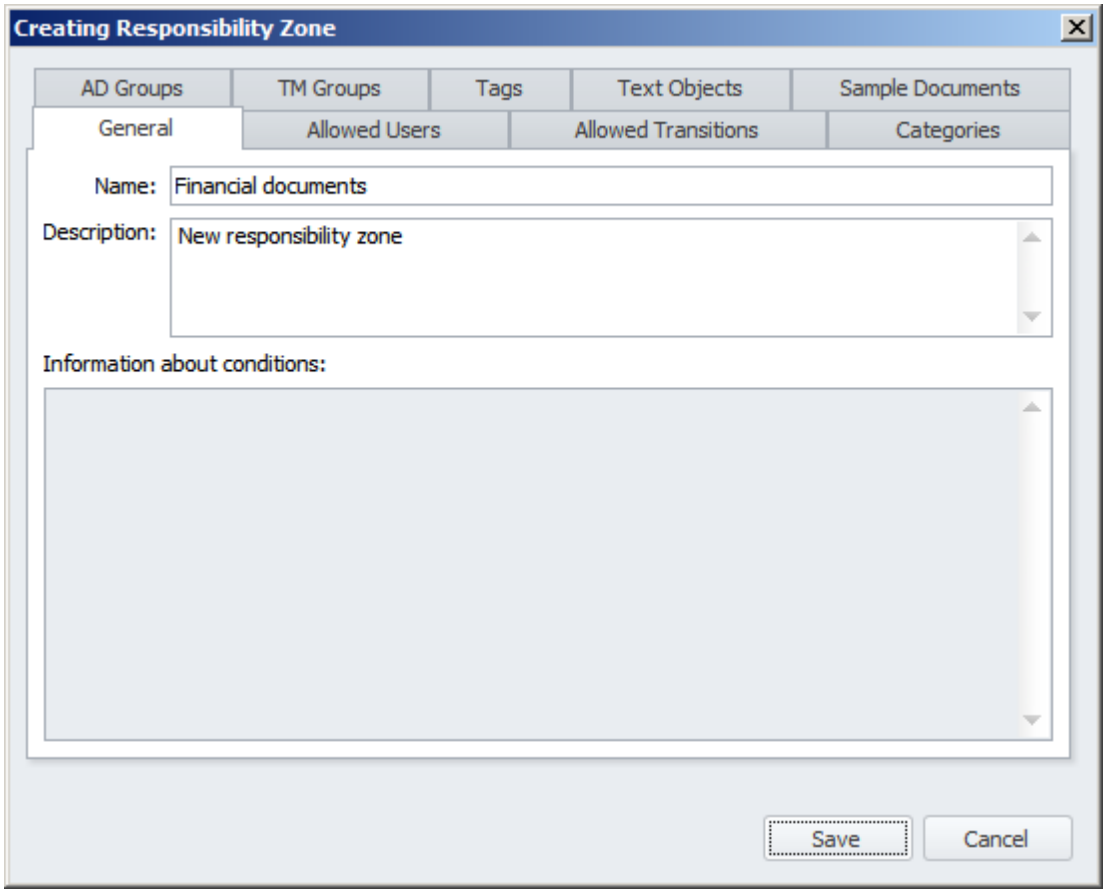
7.1.7.1 Creating and Editing a Responsibility Zone

To create or edit a responsibility zone:

1. Go to the **Responsibility Zones** section.
2. Do the following:

Action	Procedure
Create a responsibility zone	Do one of the following: • in the main menu, select **Edit > New Responsibility Zone** • click **New Responsibility Zone** on the toolbar
Edit a responsibility zone	In the responsibility zones list, select a row with the zone you need and perform one of the necessary actions: • in the main menu, select **Edit > Edit**; • click **Edit** on the toolbar; • double-click the selected row.

The responsibility zone settings dialog box will be opened.



Configuring general responsibility zone settings

3. On the **General** tab, please specify the following settings:

   - **Name**. Name of the responsibility zone (mandatory).

     The name should be unique.

     Note

     For the *Default* responsibility zone you can't change the **Name** setting.

   - **Note**. Additional information about the responsibility zone.

4. Please define conditions to add an object to the responsibility zone using the following tabs. The object will be added to the responsibility zone if any of checked attributes is present in it.

Tab	Condition to include the object into the responsibility zone
Categories	A category is assigned to the object (regardless of the configuration version)
AD Groups	AD group is defined for the object sender
TM Groups	TM group is defined for the object sender

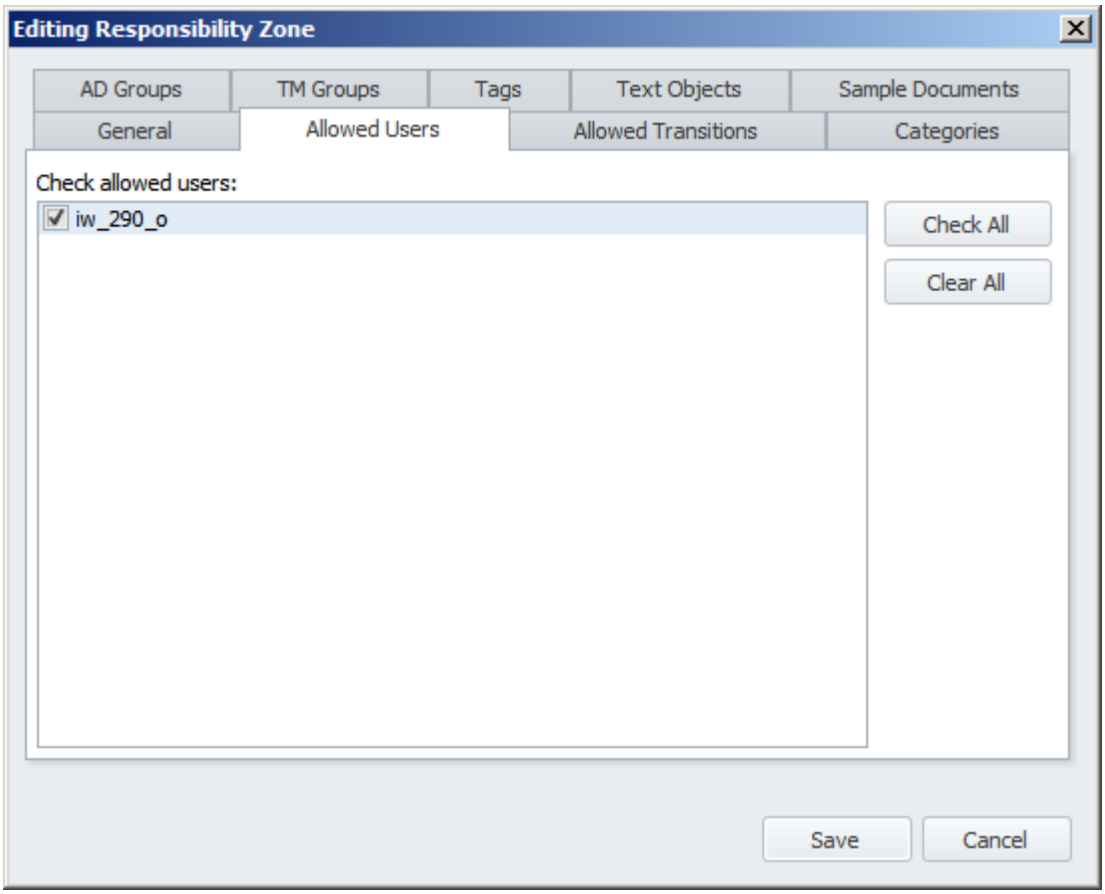
Tab	Condition to include the object into the responsibility zone
Tags	A group of tags or a tag is assigned to the object
Text objects	The text object type is found
Sample documents	A part of a sample document is found in the object

To select or clear all the check boxes, use the **Check All** and **Clear All** buttons.

Important!

You can't change the conditions to add an object to the responsibility zone for *Default* responsibility zone. An object is added to the *Default* responsibility zone if no condition for other responsibility zones is met.

5. On the **Allowed Users** tab, please select the users to allow the access to the objects in this responsibility zone.



Adding users to a responsibility zone

Important!

Highly confidential messages and queries could be included into the *Default* responsibility zone. Therefore, it's strictly recommended to include only users with the highest privileges to *Default* responsibility zone.

To select or clear all the check boxes, use the **Check All** and **Clear All** buttons.

Important!

The change of a responsibility zone for a user authorized in the system will take effect only when the user is authorized again in the Management Console.

6. On the **Allowed Transitions** tab, check all the responsibility zones to which you want to be able to move an object from the current responsibility zone. To select or clear all the check boxes, use the **Check All** and **Clear All** buttons.

7. Click **Save**.

7.1.7.2 Changing Responsibility Zone Priorities

When a responsibility zone is defined, the object is consequently matched with all responsibility zones and is put into the first responsibility zone with matching conditions. The responsibility zone verification order is defined by zone priority: the zone with the highest priority is verified first, while the preset *Default* responsibility zone has the lowest priority (1).

Note

The *Default* responsibility zone priority (1) cannot be modified.

To change the responsibility zone priority:

1. Go to the **Responsibility Zones** section.
2. In the responsibility zones list, select the zone you need.
3. Do one of the following:
   - to promote the responsibility zone, click **Increase Priority** on the toolbar or select **Edit > Increase Priority** in the main menu;
   - to demote the responsibility zone, click **Decrease Priority** on the toolbar or select **Edit > Decrease Priority** in the main menu.

As the result, the responsibility zone will moved one row up or down; the **Priority** value will be increased or decreased respectively.

7.1.7.3 Deleting a Responsibility Zone

Important!

The *Default* responsibility zone cannot be deleted.

You also cannot delete the responsibility zone that is assigned to a user; you cannot delete the responsibility zone containing at least one object.

To delete a responsibility zone:

1. Go to the **Responsibility Zones** section.
2. In the responsibility zones list, select the zone you need.
3. Do one of the following:
   - in the main menu, select **Edit > Delete**;

- click  **Delete** on the toolbar.

4. In the confirmation box, click **Yes** to confirm.

7.2 Directories

For an object analysis script to work correctly and for the further data analysis in Management Console, besides defining configuration settings and creating sample documents, you need to define the tags and create colors. This operation is performed using the corresponding directories:

- Tags
- Colors

7.2.1 Tags

The tags are text markers with a brief description of an object. Tags can be assigned to an object using Traffic Monitor Server and the Management Console (see "Assigning Tags to an Object").

Preset tags

There are three preset tag groups: *File Types, Web Resources* and *Resources*.

- The File Types tags describe the content of the attachments (music, video, images etc.).
- The *Web Resources* tags describe the target sites of the HTTP requests (blogs, file sharing portals, job search sites etc.)
- The *Resources* tags describe the local and remote resources delivering traffic, which is defined not to be processed and saved to system database.

These tags are mapped with the corresponding preset list groups: every list is mapped with a tag with the same code. For example, the *Blogs* tag (code: `_BLOGS_`) from the *Web Resources* tag group (code: `_WEBRESOURCES_`) is mapped with the *Blogs* list (code: `_BLOGS_`) from the *Web Resources* list group (code: `_WEBRESOURCES_`).

If an object matches any list (i.e. the request URL contains an address that matches one of the *Blogs* list items), then this object is assigned the corresponding tag (the *Blogs* tag in this example).

In Traffic Monitor Standard there is *Prevent Deletion* preset tag (code:`_DELETE_PROTECT_TAG_`). This tag can be assigned only by user (see "Assigning Tags to an Object") not the script. IW TMS performs a periodic checking: if the remaining free space is less then required for the new objects, then the old objects are deleted. However objects with `_DELETE_PROTECT_TAG_` are not deleted.

Preset tags cannot be modified.

Using tags in scripts

You can create your own tags and tag groups to describe the objects the way you need. Then, you can create a rule in the script that will assign a tag to all the files of certain type.



Important!

Before working with an object analysis script you have to create tags and tag groups that will be used in this

script.

To work with tags, use the **Tags** section (the **Configuration** area on the **Navigation** pane).

For more details about working with tags see the following sections:

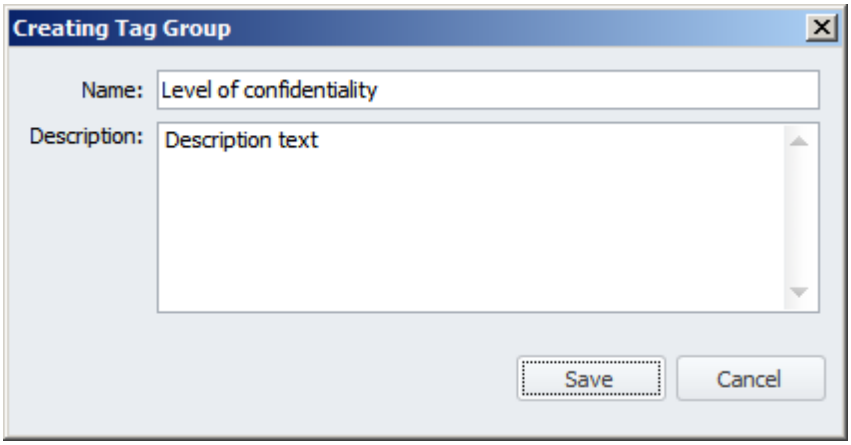
- Creating a Tag Group
- Creating a Tag
- Editing Tags and Tag Groups
- Deleting a Tag Group

7.2.1.1 Creating a Tag Group

To create a tag group:

1. Go to the **Tags** section.
2. Do one of the following:
   - in the main menu, select **Edit > New Tag Group**.
   - click **New Tag Group** on the tag groups pane.

   The **Creating Tag Group** dialog box will appear on the screen.



Creating a tag group

3. Please specify the tag group settings:
   - **Name**. Tag group name (mandatory). The name should be unique.
   - **Description**. Additional information about the tag group.
4. Click **Save**.

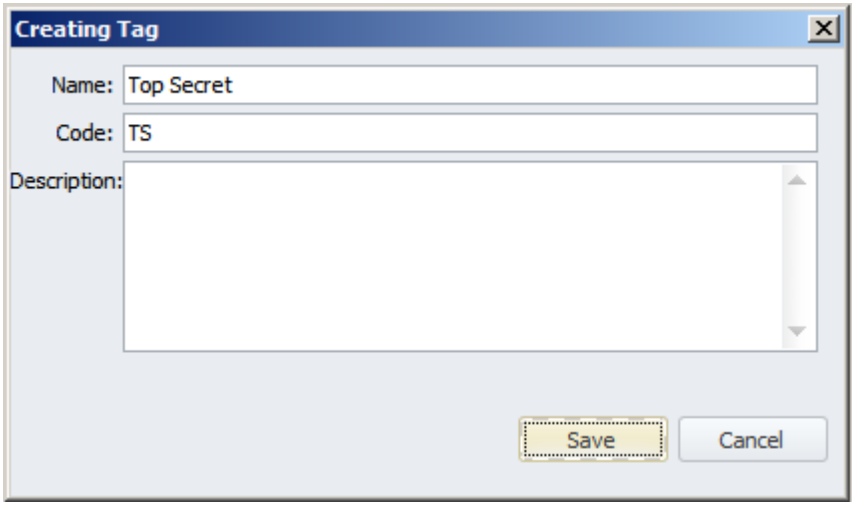
After the tag group is created, you should populate it with tags (see "Creating a Tag").

7.2.1.2 Creating a Tag

To create a tag:

1. Go to the **Tags** section.
2. On the tag group pane, select the name of the group to add the tag.
3. Do one of the following:
   - in the main menu, select **Edit > Tag > New**.
   - On the tag pane, click **New Tag**.

   The **Creating Tag** dialog box will appear.



Configuring tag settings

4. Configure the tag settings:
   - **Name**. Tag name (mandatory). The name should be unique.
   - **Code**. The name of the tag that which will be used when creating a script (mandatory).
     The code name may include English characters, digits and underscore. The name must not start with a digit. The code should be unique.
   - **Description**. Additional information about the tag.
5. Click **Save**.

Repeat steps 3 to 4 to add other tags to the group.

7.2.1.3 Editing Tags and Tag Groups

You can change the tags and tag groups using the following operations:

- editing tag group parameters
- adding a new tag to a group
- editing a tag in a group

- deleting a tag from a group.

To edit a tag group:

1. Go to the **Tags** section.
2. On the **Tag Groups** pane, select the name of the group you need.
3. Do the following:

Action	Procedure
Edit the tag group options (group name, description)	1. Do one of the following: • in the main menu, select **Edit > Edit**; • click  **Edit** on the **Tag Groups** pane. • double-click the selected tag group. 2. In the **Editing Tag Groups** dialog box, configure the required settings (see " Creating a Tag Group"). 3. Click **Save**.
Add a new tag to a group	See: "Creating a Tag"
Edit the tag options (group name, description)	1. On the tag pane, select the required tag. 2. Do one of the following: • in the main menu, select **Edit > Tag > Edit**; • click  **Edit** on the **Tags** pane. • double-click the selected tag. 3. In the **Editing Tag** dialog box, configure the required settings (see. "Creating a Tag"). 4. Click **Save**.
Delete the tag from the group	1. On the tag pane, select the required tag. 2. Do one of the following: • in the main menu, select **Edit > Tag > Delete**; • click  **Delete** on the tag pane. 3. In the confirmation box, click **Yes** to confirm. **Note:** Remove the deleted tag from all the scripts where it has been used.

7.2.1.4 Deleting a Tag Group

To delete a tag group:

1. Go to the **Tags** section.
2. On the tag group pane, select the name of the group you need.
3. Do one of the following:
   - in the main menu, select **Edit > Delete**;
   - click **Delete** on the toolbar.
4. In the confirmation box, click **Yes** to confirm.

Note

Exclude the deleted tag group from text of every script where it was used.

7.2.2 Colors

To make it more convenient, you can paint objects with colors when performing analyzing the objects in Management Console.

Setting up objects colors:

1. Set up the required color theme (see "Creating and Editing a Color", "Deleting a Color")
2. Set the rules to automatically paint the intercepted objects (see "Editing a Script" and the `Root.Processing.color` property overview in "Configuring Object Analysis Scripts (LUA)")
3. When analyzing objects, you can set and and change the color of objects (see "Highlighting Objects with Color").

7.2.2.1 Creating and Editing a Color

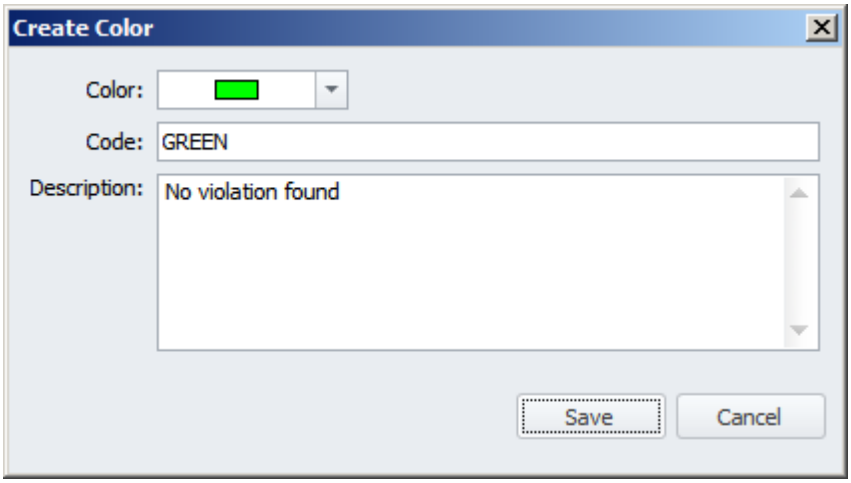
To add a color:

1. Go to the **Colors** section.
2. Do the following:

Action	Procedure
Create a color	Do one of the following: • In the main menu, select **Edit > New color** • click **New color** on the toolbar
Edit a color	1. In the color list select a row with the color you need.

Action	Procedure
	2. Do one of the following: • in the main menu, select **Edit > Edit**; • click **Edit** on the toolbar; • double-click the selected row.

The dialog box with the color settings will appear.



Configuring color settings

3. Specify the color settings:
   - **Color**. Color to mark an object with (mandatory). The color should be unique.
   - **Code**. The color name that will be used when creating a script (mandatory).

     This code may include English letters, digits and underscore, and it can't start with a digit. The code should be unique.
   - **Description**. Additional information about the color.
4. Click **Save**.

7.2.2.2 Deleting a Color

To delete a color:

1. Go to the **Colors** section.
2. In the color list, select a row with the color you need.
3. Do one of the following:
   - in the main menu, select **Edit > Delete**;
   - click **Delete** on the toolbar.
4. In the confirmation box, click **Yes** to confirm.

Note

Exclude the deleted color from every script where it has been used.

7.3 Configuring Object Analysis Scripts (LUA)

The object analysis script is written in the LUA programming language (version 5.1). You can find the Reference manual for LUA 5.1 at http://www.lua.org/manual/5.1/).

The script text is a set of rules according to which the objects will be analyzed and processed by Traffic Monitor Server. A rule consists of a set of conditions for analyzing objects and actions to be performed when the specified conditions are met/not met.

When creating a script, you must also define a set of mandatory actions to be executed for each object. These actions are:

- Selecting a transport mode.
- Assigning a verdict to an object.

If the script does not contain any of the actions listed above or an invalid value is specified for the defined attribute, then the values of the default script are used. Also see "Using the System without an Objects Analysis Script".

The conditions for checking and handling objects are specified according to the data definition in the InfoWatch Traffic Monitor type model. When creating a rule, you can specify the conditions for any data type. However, the actions can only be specified for the *Processing* and *ObjectProcessing* types.

Important!

Before you can create a script, you must specify the elements to be included in the script using Management Console. These elements are: lists, groups, categories, tags, and colors.

For more details about script configuration see the following sections:

- Specifics of Creating LUA Scripts
- InfoWatch Traffic Monitor Data Model
- Data Types
- Operators
- Methods
- Script Example

7.3.1 Specifics of Creating LUA Scripts

LUA is a case sensitive language. The system uses the following conventions:

- properties and methods are lowercase;
- data types and enumeration values are capitalized.

Example:

```
root.processing.transport_mode = TransportMode.Normal
```

Where:

- `root.processing` – path to *`Processing`* data type;
- `transport_mode` is a property of the *`Processing`* data type;
- `TransportMode` – data type;
- `Normal` is one of the *`TransportMode`* data type values.

All object analysis script rules should have the following format:

```
function Process(root)
   ---rule 1 -----
   ---rule 2 -----
   ---    …     -----
   ---rule N -----
end;
```

Before the beginning of the rule block `function Process(root)` you must do the following:

- Connect the `usertoolkit` preset helper function library using the following string:
  `require('usertoolkit');`
- Define the helper functions and variables if they will be used in a script.

When you create a condition, you must specify a value to be matched with the data. The actions are used to specify the value to be assigned to a certain data type. To specify a value, you must specify the data path and the value itself.

The path always starts with the root element followed by the data properties. (A period is used as the delimiter.)

Example

Let us assume that we should specify an action resulting in assigning a certain verdict to an object. A *Verdict* is one of properties of the *Processing* data type. At the same time, the data of this type is a property (*processing*) of the *root* element. Consequently, the path to the data of the *Verdict* type will look like as in the example below:

```
root.processing.verdict
```

You may want to create an alias if you need to access certain data many times. For example, to create an alias for the `root.processing` data, type the following:

```
processing = root.processing;
```

Then, accessing the `verdict` property will look as follows:

```
processing.verdict
```

The data values of the *string* type are defined in quotes (double quotes or single quotes). Example:

```
root.processing.color = "GREEN";
```

The enumeration type data is defined in the following way:

```
DataType.Value
```



Note

Unlike properties, a data type must not contain an underscore.

Example:

```
root.processing.verdict = Verdict.Forbidden;
```

7.3.2 InfoWatch Traffic Monitor Data Model

The InfoWatch Traffic Monitor model includes the data types.

Data type displays information on any entity (an object, a user). InfoWatch Traffic Monitor data model uses the following data types:

Data type	Description
string (simple type)	The basic type for displaying the string values
integer (simple type)	The basic type for displaying the number values
boolean (simple type)	The basic type for displaying the logical data which can take one of the two values: *true* or *false*
composite type	User-defined type. Can contain objects and methods applied to these objects. Examples of composite types: *Processing* (result of object processing), *ObjectProcessing* (result of text content analysis), *Envelope* (information extracted from the object envelope)
collection	User-defined type for displaying objects of the same type. Examples of collections: *Objects* (list of attachments), *SemanticMirror* (set of categories), *Tags* (list of tags)
enumeration	User-defined type. Contains a set of values; only one of them can be assigned to the object. Examples of enumerations: *Monitor* (residents), *TransportMode* (transport modes)

Each data type has its own set of properties.

Property is an identifying feature of the data of the specified type. For example, the data of the *Envelope* type have such properties as: *id* (unique object number), *capture_date* (date and time when the object was intercepted), *monitor* (monitor type), etc.

Method is an that which can be applied to the data of the specified type. Specifically, the *addTag* method (assigning a tag to an object) is applied to the data of the *Processing* type.

7.3.3 Data Types

In the InfoWatch Traffic Monitor model, the data types are joined in a tree where the top element is *the root element* .

The following data types can be used in scripts:

- **Object analysis Envelope**
  - Envelope (envelope of an object)

- **Object analysis**
  - Object (object content and content analysis results)
  - ObjectHeaders (headers extracted from the object)
  - ObjectHeader (names of object headers)
  - ObjectProcessing (content analysis results)
  - Objects (list of attachments)
- **Processing Objects**
  - Processing (object processing results)

7.3.3.1 The root element

The *root* element is the top level of the tree; the data types are the child nodes of this tree. The root element is of the *RootObject* data type.

Path to the data:

```
root.property_name
```

The following table contains the list of properties:

Property name	Data type	Description
envelope	Envelope composite type	The general information (configuration version, monitor type, date of interception), addresses of the sender and recipient(s), contents of the envelope headers
object	The Object composite type	The information on the contents of the intercepted object and its content analysis results
processing	The Processing composite type	The results of processing the intercepted object

Methods applied to the *root* element*: xFind*.

Methods applied to the *processing* property of the *Processing* type*: addTag*.

7.3.3.2 Object envelope (Envelope)

The *Envelope* composite data type displays the content extracted from the envelope of the intercepted object.

Data path:

```
root.envelope.property_name
```

The following table contains the list of properties.

Property name	Data type	Description
monitor	*Monitor* enumeration	The monitor used to intercept the object (e-mail, request, message). Possible values: • `Smtp`: SMTP traffic interception • `Icq`: ICQ traffic interception • `Http`: HTTP traffic interception • `Print`: shadow copies of the text from the print jobs intercepted by InfoWatch Device Monitor • `Skype`: shadow copies of the text and files that has been sent using Skype and intercepted by InfoWatch Device Monitor • `Device`: shadow copies of the files that has been sent to the portable devices intercepted by InfoWatch Device Monitor • `Dla`: shadow copies of the files that has been sent to the portable devices (DeviceLock Adapter)
id	string	Unique object identifier
capture_date	string	Date and time when the object was intercepted by the System
headers	*Headers* enumeration	Information extracted from the envelope headers. The possible enumeration values are listed in the table below
config_version	integer	Configuration version that has been current at the time the object was analyzed
identity	*Identity* enumeration	Information about the object sender and recipient
summary	string	Full object details

The following table contains the possible values of the *Headers* enumeration for different objects.

Note

When you work with the HTTP Monitor objects, it's assumed that URL has the following structure:

`<scheme>://<username>:<password>@<host>:<port>/<path>?<options>.`

Object type	Value	Description
All types	source_ip	The originating IP address of the sent object
	destination_ip	The IP address of the destination server
	destination_port	Destination server port
	creator_application	Agent (from User-Agent header value)
	capture_server	Traffic Monitor server that has intercepted the object
SMTP Monitor	mail_from	Sender e-mail address from the SMTP envelope
	rcpt_to	Recipient e-mail addresses from the SMTP envelope

Object type	Value	Description
SMTP Monitor	source_port	Originating port of the query
	url_schema	Value of the <scheme> parameter from URL
	url_username	Value of the <username> parameter from URL
	url_password	Value of the <password> parameter from URL
	url_host	Value of the <Host> parameter from URL
	url_host_fqdn	Domain name of the requester host
	url_host_ip	Domain IP address of the requested host
	url_port	The value of the <port> parameter from URL
	url_path	Value of the <path> parameter from URL
	url_options	Value of the <parameters> parameter from URL
ICQ Monitor	initiator_uin	UIN of ICQ-session initiator
Device Lock Adapter, Device Monitor, Skype Monitor	device_name	Device name
	device_type	Device Type
	destination_path	Object destination path for copying
	policy_name	Name of the policy used to intercept of the object
	rule_name	Name of the rule used to intercept of the object
	action	Operation property: allowed or forbidden
	operation	Operation type
	domain	Name of the Microsoft Windows domain in which the workstation currently resides
	workstation	Name of the workstation
	login	User account in Microsoft Windows
	userlastname	Last name of the user
	userfirstname	First name of the user
	job	Job name

7.3.3.3 Object content and content analysis results (Object)

The *Object* composite data type is used to display the information about the intercepted object and the results of the content analysis.

Path to the data:

```
root.object.property_name
```

The following table contains the list of properties:

Property	Data type	Description
type	string	Object type
objects	The Object collection	List of attachments of the object
processing	ObjectProcessing composite type	Results of the text content analysis. Messages generated while analyzing and processing the intercepted object
headers	The ObjectHeaders collection	List of headers extracted from the object
smark	The SmarkType enumeration	Object attribute, can have one of the following values: `from`; `to`; `cc`; `bcc`; `subject`; `body`; `file`
object_id	integer	Object identifier

Methods applied to the *`processing`* property of the *`ObjectProcessing`* composite type:

- addMessage.

7.3.3.4 Object headers (ObjectHeaders)

The *ObjectHeaders* collection type is used to display information about the headers extracted from an object.

Path to the data:

```
root.object.headers.property_name
```

The following table contains the list of properties:

Property name	Data type	Description
header	ObjectHeader composite type	The header extracted from the object

7.3.3.5 Object headers names (ObjectHeader)

The *ObjectHeader* data type is used to display the list of headers extracted from an intercepted object.

Path to the data:

```
root.object.headers.header.property_name
```

The following table contains the list of properties.

Property name	Data type	Description
name	string	Name of the header extracted from the object

Property name	Data type	Description
smark	*Smark Type* enumeration	The object attribute, can have one of the following values: `from`; `to`; `cc`; `bcc`; `subject`; `body`; `file`

7.3.3.6 Content analysis results (ObjectProcessing)

The *ObjectProcessing* data type is used to display the results of the text content analysis. This data type is also used for displaying the messages that were generated while analyzing and processing an intercepted object.

Path to the data:

```
root.object.processing.property_name
```

The following table contains the list of properties.

Property name	Data type	Description
messages	*Messages* collection	Messages generated while analyzing and processing the object
semantic_mirror	*SemanticMirror* collection	List of categories found when analyzing the text content
text_obj_detector	*TextObjectDetector* collection	List of categories and terms assigned to the detected text objects
copyright_analysis	*CopyrightAnalysis* collection	List of messages generated while analyzing and processing an object

7.3.3.7 List of attachments (Objects)

The *Objects* data type is used to display the list of attachments of the intercepted object.

Path to the data:

```
root.object.objects.property_name
```

The following table contains the list of properties.

Property name	Data type	Description
object	Object composite type	Information on one attachment of the intercepted object

Note

Since the *objects* data type, being a property of the *object* data type, also has the *object* data type, the access path for the intercepted objects with attachments of a certain depth can have the following format:

```
root.object.objects[.object.objects[...object.objects]...].property_name
```

where the attachment depth is equal or more than 1.

7.3.3.8 Object processing results (Processing)

The *Processing* composite data type contains information on the results of processing the intercepted object.

Path to the data:

```
root.processing.property_name
```

The following table contains the list of properties.

Object property	Data type	Description
verdict	*Verdict* enumeration	The verdict assigned to the object. By default, the verdict is *Forbidden*. Possible values: • `Allowed` • `Forbidden`
transport_mode	*TransportMode* enumeration	The transport mode of the object. Possible values: • `Normal` • `Transparent` • `Copy` For information on how to set up the transport mode in a script, see the table below
delivery_state	*DeliveryState* enumeration	Object delivery status. Possible values: • `Pending` • `Blocked` • `Delivered` • `DeliveryFailed` • `DeliveryAttemptFailed`
delete_content	Boolean	The property defines if the object should be deleted without saving to the database. Possible values: • `true` – delete the object without saving it to the database • `false` – save the object to the database
verdict_reazon	string	Description of the reason: why the specified verdict was assigned to the object
tags	*Tags* collection	The list of tags assigned to the object during processing

Object property	Data type	Description
color	string	The code of a color to highlight the object when displaying it in the Management Console (the name is specified in the **Code** field when creating a color)

The following table explains how to set up the transport mode in a script.

Object interception method	Value of the transport_mode property in a script
SMTP	
The system intercepts and delivers the SMTP traffic using Postfix. Set the normal transport mode if you need to filter traffic – the delivery can be allowed or blocked	Normal / Transparent
The system receives a copy of the SMTP traffic from the enterprise mail system or from Sniffer	Copy
HTTP	
The system intercepts and delivers the HTTP traffic using the ICAP protocol. Set the normal transport mode if you need to filter traffic – the delivery can be allowed or blocked	Normal / Transparent
The system receives a copy of the HTTP traffic from Sniffer.	Copy
Other object types	
The system receives a copy of the ICQ traffic and print jobs from Sniffer	Copy
The system receives a copy of the Skype traffic, the shadow copies of the files and the print jobs from InfoWatch Device Monitor	Copy
The system receives shadow copies of files from DeviceLock	Copy

7.3.4 Operators

You can use the following operators in the scripts:

- The Assignment operator
- The Comparison operator
- The Condition operator
- The Cycle operator

7.3.4.1 Assignment operator

The assignment operator is used to assign values to data.

Syntax:

```
path_to_the_data = Data_type.Value
```

here:

- `path_to_the_data`. The path to the data to be changed. It is set based upon the root element (period is used as a separator), the name of each element is specified according to InfoWatch Traffic Monitor type model.
- `DataType.Value`. The data type and the assigned value.

Example:

```
root.processing.verdict = Verdict.Forbidden
```

7.3.4.2 Comparison operator

The comparison operator compares the current value with the value in the operator.

Syntax:

```
path_to_the_data == DataType.Value
```

here:

- `path_to_the_data`. The path to the data being compared. It is set based upon the root element (period is used as a separator), the name of each element is specified according to InfoWatch Traffic Monitor type model.
- `DataType.Value`. The data type and the value to be compared with the current value.

Example:

```
If root.processing.verdict == Verdict.Forbidden
```

7.3.4.3 Condition operator

The condition operator "**if**" is used to check if an expression matches the specified condition. The operator is used with any expressions that return `Boolean` type.

Syntax:

```
if expression_1 then
   expression_2;
else
   expression_3;
end;
```

If `expression_1` is true, then the `expression_2 is` executed. Otherwise, the `expression_3` is executed, or (if the `else` operator is not used) the next rule in the script .

Example:

```
if root.envelope.monitor == Monitor.ICQ then
   root.processing.verdict = Verdict.Allowed;
   root.processing.transport_mode = TransportMode.Normal;
end;
```

In this example, the rule is specified for processing objects intercepted by the ICQ monitor. At first the condition is checked. If the object is intercepted by the ICQ monitor, then the object is assigned the *Allowed* verdict and the *Normal* transport mode.

7.3.4.4 Cycle operator

The cycle operator "**for**" is used to perform a set of actions with the same type of data. The operator is used for collections.

Syntax:

```
for property in path_to_the_data_collection do
   set_of_operations;
end;
```

Where:

- `property`. The property of the data collection type. For example, "recipient" is the property of the Recipients collection.
- `path_to_the_data`. The path to the data being compared. It is set based on the root element (period is used as a separator). The name of each element should be specified in full conformity with the InfoWatch Traffic Monitor type model.
- `set_of_operations`. One or more operations which to be carried out for each object of the specified collection.

Example:

```
for header in root.envelope.headers do
   if(header.name == 'source_ip') then
      if vademecum:IsStringInList('SERVERS_IP', header.value, SearchMode.Exact) then
      root.processing.delete_content = true;
      end;
   end;
end;
```

In this example, the object sender's IP address is searched for in the `SERVERS_IP` list. This list contains the IP addresses of the servers used for service purposes. The traffic from these servers may not contain sensitive information. If the sender IP address is included in the list, then the intercepted object is deleted without being saved in the database.

7.3.5 Methods

For the list of methods that can be used to create scripts, see the following table:

Important!

Starting with Traffic Monitor version 3.4 and 3.4 MP1 some methods are replaced with updated equivalents. It is not recommended to use obsolete methods. The *equal_wild* and *equal_incase* methods are no longer

supported; you can use the LUA 5.1 functions instead (e.g., *string.find* and *string.upper*). Fore more details see the LUA 5.1 documentation at http://www.lua.org/manual/5.1/.

Method name	Usage	Applies to the data type
addMessage	Adding a message	ObjectProcessing, Processing
addTag	Adding a tag	Processing
IsStringInList (old name – is_in)	Search for a string in a list	-
GetListNames (old name – Lookup)	Search for a string in a list group	-
xFind	Search for XML context elements	RootObject
IsSenderInGroup (old name – IsSenderInGroupCode)	Search for a sender in a group	-
IsRecipientInGroup (old name – IsAnyRecipientInGroupCode)	Search for a recipient in a group	-
IsWorkstationInGroup (old name – IsWorkstationInGroupCode)	Search for a workstation in a group	-
IsListItemInText	Search for list elements in a text	-

7.3.5.1 Adding a message

The method for adding a message to an object is used only with *ObjectProcessing* data type.

Syntax:

```
path_to_the_data:addMessage(Message.Message_type, "Text")
```

For the Message_type you should specify the message type based on its importance:

- Info - information;
- Warning – a warning;
- Error - an error message.

Method usage example:

```
root.object.processing:addMessage(Message.Info, "Script run successfully")
```

7.3.5.2 Adding a tag

The method of adding a tag to an object is used only with the *Processing* data type.

Syntax:

```
path_to_the_data:addTag("Tag_code")
```

Note

You can view the code name of the tag in its properties (the **Code** field).

Method usage example:

```
root.processing:addTag("MUSIC")
```

7.3.5.3 Search for a string in a list

The string occurrence detection checks for the given string in a defined list or group of lists.

Syntax:

```
vademecum:IsStringInList("list_or_list_group_code", "string", SearchMode.search_mode)
```

The SearchMode setting sets matching mode when searching lists and can have the following values:

- `SearchMode.Exact`: search for an exact match with the specified string.
- `SearchMode.DomainExplicit` and `SearchMode.DomainImplicit`: for user-created lists and groups (see "Lists") with possible query addresses. The closest matching address is found according to the domain name structure (according to RFC1034 http://www.ietf.org/rfc/rfc1034).

  For `SearchMode.DomainExplicit` the search is performed from full domain match to a higher level subdomain match. For example, if you are looking for the **info.mail.ru** address, then the search engine will first try to find the **info.mail.ru** item in the list. If there is no such list, the search engine will then try to find the items ***.mail.ru** , ***.ru** and **.ru**.

  In `SearchMode.DomainImplicit` the search goes from full domain match to a higher level subdomain match, then to a higher level domain where a match. Note that the parent domain match implicitly covers its subdomains. For example, if you are looking for the **info.mail.ru** address, then the search engine will first try to find the **info.mail.ru** item in the list. If there is no such item in the list, the search engine will then try to find the items ***.mail.ru** , **mail.ru**, ***.ru**, **.ru** and **ru**.

Therefore, in most cases you should use the `SearchMode.Exact` value. Other values can be used only in the special case when you need to search a list of domains that are not present in the "*Web resources*" system list.

Method usage example:

```
for header in root.envelope.headers do
   if(header.name == 'source_ip') then
      if vademecum:IsStringInList('SERVERS_IP', header.value, SearchMode.Exact) then
      root.processing.delete_content = true;
      end;
   end;
end;
```

In this example, the object sender's IP address is searched for in the `SERVERS_IP` list. This list contains the IP

addresses of the servers used for service purposes. The traffic from these servers may not contain sensitive information. If the sender IP address is in the list, then the intercepted object is deleted without saving in the database.

7.3.5.4 Search for a string in a list group

This search method is searching the lists included in the specified list group where the specified string occurs.

Syntax:

```
vademecum:GetListNames("list_group_code", "string", SearchMode.search_mode)
```

For the description of the `SearchMode` setting see "Search for a string in a list". In search modes with domain hierarchy consideration (`DomainExplicit`, `DomainImplicit`), the results are grouped by the found matches for the top level domains.

This method can be used in the following scenario. For example, a Management Console user has created a `COMPANY_ADDRESSES` list group that contains all the domains of the competitors, contractors etc. The user has also created a tag group that corresponds to these lists. In this case you should add the following rule in the script to assign tags to a HTTP request:

```
for tag in vademecum:GetListNames('COMPANY_ADDRESSES', url_host, SearchMode.DomainImplicit)
do
   --- the tag variable is assigned values that correspond to the codes of lists with
   url_host ---
end;
```

This works in the following way. The `url_host` property (received from the URL query) is matched with the lists in the `COMPANY_ADDRESSES` list group. A tag from the corresponding tag group is mapped to every list in the `COMPANY_ADDRESSES` list group. In the end, the object is assigned tags for matching list.

7.3.5.5 Search by XML context elements

Search for XML context elements of an object (for more details on XML context see "Uploading object into database" and "Viewing the objects information") is used only with the RootObject data.

Syntax:

```
root:xFind("xPath-expression").XPath-method
```

Where:

- xPath-expression. The expression created according to the xPath syntax.
- xPath-method. The method of an XPath object (the XPath object is returned by the xFind method).

  The methods of the XPath object:

  - count. Number of objects that correspond to the specified condition.
  - nodes. The collection of the XMLNode class objects.

Method usage example:

```
if root:xFind('object[type == "video/avi"]').count then
   …
end
```

In this case the attachment are searched for the AVI files.

7.3.5.6 Search for a sender in a group

This search method searches for the object sender data in the the person directories (see "Persons Directory").

Syntax:

```
GCC:IsSenderInGroup(root, 'groupcode')
```

where `groupcode` is the code of the group being searched. You can specify several groups using the following characters as separators: ,", "|", and ";".

Method usage example:

```
if GCC:IsSenderInGroup(root, 'Group1|Group2') then
   root.object.processing:addMessage(Message.Info, 'The sender belongs to "Group1" or
   "Group2"');
end;
```

This example searches for sender data in `Group1` and `Group2` lists. If the sender address is in the specified list, then the *"The sender belongs to "Group1" or "Group2"* message is added to the object.

7.3.5.7 Search for a recipient in a group

This search method looks for the object recipient data in the persons directories (see "Persons Directory").

Syntax:

```
GCC:IsRecipientInGroup(root, 'groupcode')
```

where `groupcode` is the code of the group being searched. You can specify several groups using the following characters as separators: ,", "|", and ";".

Method usage example:

```
if GCC:IsRecipientInGroup(root, 'BLACK_RECIPIENTS_LIST') then
   root.object.processing:addMessage(Message.Info, 'One of the recipients is included in
   the black list');
end;
```

This example searches for recipient data in the BLACK_RECIPIENTS_LIST list. If any recipient detail is included in the specified list the message "One of the recipients is included in the black list" is added to the object.

7.3.5.8 Search for a workstation in a group

This method searches for the workstation object sender data in the the person directories (see "Workstations directory").

Syntax:

```
GCC:IsWorkstationInGroup(root, 'groupcode')
```

where `groupcode` is the code of the group being searched. You can specify several groups using the following characters as separators: ",", "|", and ";".

Method usage example:

```
if GCC:IsWorkstationInGroup(root, 'BLACK_SENDER_LIST') then
   root.object.processing:addMessage(Message.Info, 'One of the workstations is in the black
```

```
    list of senders');
end;
```

This example searches for the workstation data in the TM group with BLACK_SENDER_LIST code. If any sender setting is in the specified group, then the message "One of the workstations is in the black list of senders" is added to the object.

7.3.5.9 Search for list elements in a text

This method searches the specified text for elements from user-defined lists (see "Lists").

Syntax:

```
vademecum:IsListItemInText('text', 'list')
```

where `text` is a text to search in, and `list` is a code of the user list that is searched for. You can specify several lists using the following characters as separators: ',', '|', and ';'.

Note

The *IsListItemInText* method is not used for the lists in the *File Types* and *Web resources* preset list groups.

Method usage example:

```
for header in obj.headers do
    if vademecum:IsListItemInText(header.value, 'GARBAGE_LIST') then
        root.processing.delete_content = true;
    end;
end;
```

This example searches for object header values of any depth in the GARBAGE_LIST list. This list contains the words that characterize unwanted traffic. If the object header contains any element from the list, then the object is not saved in the database.

7.3.6 Helper Function Library

The usertoolkit helper function library allows you to use the common checks easily. The usertoolkit library includes the following helper functions:

Function name	Purpose
CategoryDetected	Detection if any categories were found in the object context
CategoriesFromListDetected	Several tags detection
SampleDocumentDetected	Detection if any quotes from sample documents were found in the object context
TextObjectDetected	Detection if any text objects were found in the object context
root_has_sector_text_object	Text Object Relating to Specified Sector Detection

UnknownFormatDecteted	Detection if any files of unknown format are attached to the object
EncryptedContentDecteted	Detection if any encrypted files are attached to the object
AnyError	Detection if any any object processing errors occurred
ExctactorError	Detection if any object attachment processing errors occurred during object processing
ContentAnalysisError	Detection if any content analysis errors occurred during object processing
IsGarbage	Checking if the object is a "garbage traffic"
first	Searching of the first node from the nodelist
IsIdentityConflict	Identification error detection
SendNotificationUser	Sending notification to security officer
SendNotificationEmployee	Sending notification to violator
TagsFromListDetected	Several Tags Detection



Important!

To use this helper function library you need to add the following string in the beginning of a script:

```
require('etc/scripts/usertoolkit')
```

7.3.6.1 Categories Detection

To check if the object context contains any categories (see "Classification"), use the following function:

```
CategoryDetected(root)
```

Example:

```
if CategoryDetected(root) then
   root.object.processing:addMessage(Message.Info, 'Found categories');
end;
```

7.3.6.2 Categories from List Detection

To check if certain categories (see "Classification") have been assigned to the object use the following function:

```
CategoriesFromListDetected(root, { category })
```

where `category` is a list of required categories. You can enumerate some categories, using symbols «,», «|» и «;» as dividers.

Example:

```
 if CategoriesFromListDetected(root, {'CONFIDENTIAL','STRUCTURE'}) then
   return true,Verdict.Forbidden,'Leak of confidential information','RED';
 end;
```

7.3.6.3 Quotes from Sample Documents Detection

To check if the object context contains any quotes from the sample documents (see "Sample Document Database "), use the following function:

```
SampleDocumentDetected(root)
```

Example:

```
if SampleDocumentDetected(root) then
   root.object.processing:addMessage(Message.Info, 'Found quotes');
end;
```

7.3.6.4 Text Objects Detection

To check if the object context contains any text objects (see "Text Objects"), use the following function:

```
TextObjectDetected(root)
```

Example:

```
if TextObjectDetected(root) then
   root.object.processing:addMessage(Message.Info, 'Found text objects');
end;
```

7.3.6.5 Text Object Relating to Specified Sector Detection

Use the following function to check if any text object (see "Text objects") relating to the specified sector (for example, financial, production, etc.) has been assigned to the object:

```
root_has_sector_text_object(root, 'sector')
```

where `sector` is a sector code.

Example:

```
if root_has_sector_text_object(root, 'CreditCard') then
    return true,Verdict.Forbidden,'Leak of private financial information','RED';
end;
```

7.3.6.6 Attachments of Unknown Format Detection

To check if the object has any attachments of an unknown format, use the following function:

```
UnknownFormatDecteted(root)
```

Example:

```
if UnknownFormatDecteted(root) then
   root.object.processing:addMessage(Message.Info, 'Found attachments of unknown format');
end;
```

7.3.6.7 Encrypted Attachments Detection

To check if the object contains any encrypted attachments, use the following function:

```
EncryptedContentDecteted(root)
```

Example:

```
if EncryptedContentDecteted(root) then
   root.object.processing:addMessage(Message.Info, 'Found encrypted attachments');
end;
```

7.3.6.8 Object Processing Errors Detection

To check if there any errors occurred in object processing, use the following function:

```
AnyError(root)
```

Example:

```
if AnyError(root) then
   root.object.processing:addMessage(Message.Info, 'Object processing errors');
end;
```

7.3.6.9 Attachment Processing Errors Detection

To check if there any errors occurred in attachment processing, use the following function:

```
ExctactorError(root)
```

Example:

```
if ExctactorError(root) then
   root.object.processing:addMessage(Message.Info, 'Attachment processing errors');
end;
```

7.3.6.10 Content Analysis Errors Detection

To check for object text processing errors use the following function:

```
ContentAnalysisError(root)
```

Example:

```
if ContentAnalysisError(root) then
   root.object.processing:addMessage(Message.Info, 'Content analysis errors');
end;
```

7.3.6.11 Checking Garbage Traffic

The script cam make a check if the object is a "garbage traffic". "Garbage traffic" is considered POST-request which don't contain any information useful for analysis (text and body of object cannot be formalized; no text extracted from headers). For example, background status requests in social networks are a garbage traffic.

The list of web-resources which traffic can be analyzed if it is garbage, is specified in "Specific Features of Blocking HTTP-queries and Messages Sent Through Web-services" section.

To check HTTP objects if they are garbage traffic, use the following function:

```
IsGarbage(root,hmask)
```

Example:

```
if IsGarbage(root,hmask) then
return true,Verdict.Allowed,'Бесполезный трафик','GREY';
end;
```

7.3.6.12First Node Searching

To search the first node from the nodelist described in в xPath (see "Search for XML context elements") use the following function:

```
first(root:xFind('/root/envelope/headers/url_host').nodes)
```

For example instead of script with two cycles:

```
local url_node = root:xFind('/root/envelope/headers/url_host').nodes;
local url_path = root:xFind('/root/envelope/headers/url_path').nodes;
    for url_host_nodes in url_node do
        for url_path_nodes in url_path do
            full_url_path = url_host_nodes.text..url_path_nodes.text;
        end;
    end;
```

You can use the following:

```
local url_node = first(root:xFind('/root/envelope/headers/url_host').nodes);
local url_path = first(root:xFind('/root/envelope/headers/url_path').nodes);
full_url_path = url_node.text .. url_path.text;
```

7.3.6.13Identification Errors Detection

Use the following function ti check if several matches with the records of persons and workstations (for more information about the identification errors see "Processing the Sender, Recipient, and Workstation Data") were assigned to the one object attribute:

```
IsIdentityConflict(root)
```

Example:

```
if IsIdentityConflict(root) then
   root.object.processing:addMessage(Message.Info, 'Ошибка идентификации');
end;
```

7.3.6.14 Sending Notice to Security Officer

If you want the security officer to receive e-mail notifications (for more information see "Configuring the Violation Notifications") about the object interception in the case of the security policy breaking, use the following function:

```
SendNotificationUser(root)
```

Example:

```
result,verdict,verdict_reason,color = CheckViolationPolicy(root);
```

```
if result then
  SendNotificationUser(root);
  return;
end;
```

7.3.6.15 Sending Notice to Violator

If you want the violator (employee) officer to receive e-mail notifications (подробнее см. "Configuring the Violation Notifications") about the object interception in the case of the security policy breaking, use the following function:

```
SendNotificationEmployee(root)
```

Example:

```
result,verdict,verdict_reason,color = CheckViolationPolicy(root);
if result then
  SendNotificationEmployee(root);
  return;
end;
```

7.3.6.16Several Tags Detection

To check if any tags have been assigned to the object use the following function:

```
TagsFromListDetected(root, { tag })
```

where `tag` is a list of required tags. You can enumerate some tags, using symbols «,» and «;» as dividers.

Important!

Using the `TagsFromListDetected` function you can find only lowercase tags.

For example, if you use the function

```
if TagsFromListDetected(root,{'_DANGEROUS_','_AGGRESSIVE_','_ADULT_'}[...]
```

you will find `'_dangerous_','_aggressive_'` and `'_adult_'` tags

If you need find uppercase tags, you should search by XML context elements

Example:

```
if TagsFromListDetected(root,{'_DANGEROUS_','_AGGRESSIVE_','_ADULT_'}) then
   return true,Verdict.Forbidden,'Violation of the law of Russian Federation','LIGHT_RED';
end;
```

7.3.7 Script Example

The script example contains several preset policies. A policy is a set of rules that define which of the intercepted objects are considered violations, and how the System should react to all types of intercepted objects. The script operates as follows:

1. Default values are set (defined by the transport mode for every monitor).
2. Intercepted object is checked for the possibility to apply one of the policies.
3. If the object matches the policy requirements, the policy actions are applied to the object.

4. Processing policy is applied for standard objects – objects that were not considered violations when previous policies were verified.

The reference script uses the following policies to process the intercepted objects:

- The policy that allows to transfer any information to a sender from the VIP group.
- The policy that detects the transfer of illegal information.
- The policy that detects the suspicious activity of the employees.
- The policy that detects the improper use of resources.
- The policy that allows to transfer of the permitted information. It is applied last to process the permitted events, that is the events that didn't match the conditions of any of the previous policies.

If these policies are applicable to your company, you should add some employees to the preset TM group called "*VIP* " in Management Console. All undesirable recipients should be added to a preset TM group called "*Suspicious Recipients*". Otherwise the senders and recipients won't be matched with these groups.



Important!

If you want to create your own script based on the script example and you need to change the preset ***Copy*** mode (`TransportMode.Copy`) to the ***Normal*** mode (`TransportMode.Normal`), then keep in mind that the system will block the delivery of all the objects with the "Forbidden" verdict (`verdict.Forbidden`).

It's assumed that the linguistic analysis uses the standard Classification included with the system (you should upload it to the Management Console), and all the sample documents are set. Otherwise, the categories and sample document quotes won't be searched for.

In addition, before the script is run, the "usertoolkit" additional function library should be enabled.

Script

```
-- Activation of the library of additional functions
----------------------------------------

require('etc/scripts/usertoolkit')

-- Defining additional functions ---------------------------------------------------
--
-- Function of transport modes setting (for each monitor)

function SetDefaultTransportMode (root)
  if root.envelope.monitor == Monitor.Smtp then
    -- SMTP
    root.processing.transport_mode = TransportMode.Copy;
    return;
  elseif root.envelope.monitor == Monitor.Device then
    --DEVICE MONITOR
    root.processing.transport_mode = TransportMode.Copy;
    return;
  elseif root.envelope.monitor == Monitor.Dla then
    --DEVICE LOCK ADAPTER [DLA]
    root.processing.transport_mode = TransportMode.Copy;
    return;
  elseif root.envelope.monitor == Monitor.Print then
    --PRINT MONITOR
    root.processing.transport_mode = TransportMode.Copy;
    return;
```

```
  elseif root.envelope.monitor == Monitor.Http then
    -- HTTP
    root.processing.transport_mode = TransportMode.Copy;
    return;
  elseif root.envelope.monitor == Monitor.Icq then
    -- ICQ
    root.processing.transport_mode = TransportMode.Copy;
    return;
  end;
  root.processing.transport_mode = TransportMode.Copy;
end;

-- function of checking the applicability of the permission policy returns an indication -
policy is applicable or not
-- verdict, reason of the verdict and color of the marked object

function CheckPermissionPolicy(root)
  -- checks whether the sender is in the VIP group
  if GCC:IsSenderInGroup(root, 'VIP') then
    -- If the sender is found, there is an indication, that the policy is applicable and the
list of parameters;
    return true, Verdict.Allowed, 'The sender is found in the VIP list','LIGHT_GREEN';
  end;
  -- otherwise, there is an indication that the policy is not applicable
  return false;
end;

-- function of applicability of the violation check policy, returns an indication, whether the
policy is applicable
-- verdict, reason of the verdict and color of the marked object
--
-- All violations are divided into leaks of restricted information and violation of the law of
Russian Federation.
-- Objects considered to be the leak of restricted information are marked with red.
-- Objects considered to be the violation of the law of Russian Federation are marked with
light red.

function CheckViolationPolicy(root)
  -- checks whether the object was assigned with any categories belonging to the parent
categories “Confidential information”,
  -- “Company structure”
  if CategoriesFromListDetected(root, {'CONFIDENTIAL','STRUCTURE'}) then
    -- if such categories are found, there is an indication that the policy is applicable the
list of parameters
    return true,Verdict.Forbidden,'Leak of confidential information','RED';
  end;

  -- checks whether the object contains any extracts from sample documents
  if SampleDocumentDetected(root) then
    -- if extracts are found, there is an indication that the policy is applicable and the
list of parameters
    return true,Verdict.Forbidden,'Leak of confidential information','RED';
  end;

  -- checks whether the object contains any text objects defined as personal data
  if root_has_sector_text_object(root, 'PersonalData') then
      return true,Verdict.Forbidden,'Leak of personal data','RED';
  end;

  -- checks whether the object contains any text objects defined as private financial
information
  if root_has_sector_text_object(root, 'Finance') then
      return true,Verdict.Forbidden,'Leak of finance information','RED';
```

```
  end;

  if root_has_sector_text_object(root, 'Insurance') then
      return true,Verdict.Forbidden,'Leak of insurance information','RED';
  end;

  if root_has_sector_text_object(root, 'OilAndGas') then
      return true,Verdict.Forbidden,'Leak of sensetive data','RED';
  end;

  if root_has_sector_text_object(root, 'Production') then
      return true,Verdict.Forbidden,'Leak of sensetive data','RED';
  end;

  if root_has_sector_text_object(root, 'Telecommunications') then
      return true,Verdict.Forbidden,'Leak of sensetive data','RED';
  end;

  -- checks whether the object is assigned with any categories belonging to the parent
category “Violation of the law of Russian Federation”
  if CategoryFromListDetected(root,'BAZA_PROTIVOD') then
    -- if such category is detected, there is an indication that the policy is applicable and
the list of parameters
    return true,Verdict.Forbidden,'Violation of the law of Russian Federation','LIGHT_RED';
  end;

  -- checks whether the object contains any information indicating using prohibited web-
resources
  if TagsFromListDetected(root,{'_DANGEROUS_','_AGGRESSIVE_','_ADULT_'}) then
    -- if there is such information, there is an indication that the policy is applicable and
the list of parameters
    return true,Verdict.Forbidden,'Violation of the law of Russian Federation','LIGHT_RED';
  end;

  -- otherwise there is an indication that the policy is not applicable
  return false;
end;

-- the function of checking the potential violation policy applicability returns an indication
- whether the policy is applicable,
-- verdict, reason of verdict and the color of the marked object
--
-- The object may be a potential violation in case the System could not carry out the full
analysis of its content
-- or the object contains any suspicious data.
-- Objects, for which the System could not carry out the full analysis of its content, are
marked with light orange.
-- Objects, the recipients of which are found in the group of suspicious recipients are marked
with orange.

function CheckPotentialViolationPolicy (root)
  -- checks, whether any recipients are included in the group of suspicious recipients
  if GCC:IsRecipientInGroup(root, 'SUSPICIOUS_RECIPIENTS') then
    -- if any recipients are found, there is an indication that the policy is applicable and
the list of parameters
    return true,Verdict.Forbidden,'Recipient is found in the group of suspicious
recipients','ORANGE';
  end;

   -- проверяется если конфликт идентификации отправителя, получателя, или рабочей станции
  if IsIdentityConflict(root) then
    -- если конфликт есть, возвращается признак того, что политика применима и перечень
параметров
```

```
    return true,Verdict.Forbidden,'Identity Conflict','ORANGE';
  end;

  -- checks, whether the object contains any attachments with unknown format
  if UnknownFormatDecteted(root) then
    -- if the object contains any of these, there is an indication and the list of parameters
    return true,Verdict.Forbidden,'File with unknown format','LIGHT_ORANGE';
  end;

  -- checks, whether the object contains any encrypted content
  if EncryptedContentDecteted(root) then
    -- if the object contains any of these, there is an indication that the policy is
applicable and the list of parameters
    return true,Verdict.Forbidden,'Encrypted content','LIGHT_ORANGE';
  end;

  -- checks, whether any error occurred during object processing
  if ExtractorError(root) then
    -- if an error occurred, there is an indication that the policy is applicable and the list
of parameters
    return true,Verdict.Forbidden,'Extraction error','LIGHT_ORANGE';
  end;

  -- checks, whether any error occurred during content analysis
  if ContentAnalysisError(root) then
    -- if an error occurred, there is an indication that the policy is applicable and the list
of parameters
    return true,Verdict.Forbidden,'Content analysis error','LIGHT_ORANGE';
  end;

  -- otherwise, there is an indication that the policy is not applicable
  return false;
end;


-- function of applicability of the policy of resources misuse, returns an indication, whether
the policy is applicable,
-- verdict, reason of the verdict and color of the marked object

function CheckNoPurposeResourcesUsagePolicy(root)

  -- checks, whether the object contains attachments with entertaining content: video, music,
images
  if TagsFromListDetected(root,{'_VIDEO_','_MUSIC_','_IMAGE_'}) then
    -- if the object contains such attachments, there is an indication that the policy is
applicable and the list of parameters
    return true,Verdict.Forbidden,'Transmission of entertaining content','LIGHT_YELLOW';
  end;

  --checks, whether the object contains information about using entertaining web-resources
  if TagsFromListDetected(root,{'_BLOGS_','_MEDIA_','_ENTERTAINMENT_','_FILESHARING_'}) then
    -- if the object contains such information, there is an indication that the policy is
applicable and the list of parameters
    return true,Verdict.Forbidden,'Use of entertaining web-resources','LIGHT_YELLOW';
  end;

  --checks, whether the object contains information about the use of job search web-resources
  if Tagged(root,'_JOBSEARCH_') then
    -- if the object contains such information, there is an indication that the policy is
applicable and the list of parameters
    return true,Verdict.Forbidden,'Use of job search web-resources','LIGHT_YELLOW';
  end;
```

```
  -- Otherwise, there is an indication that the policy is not applicable
  return false;
end;

-- the function of using predefined policies contains the list of actions that have to be
carried out in case the policy is applicable

function ApplyPolicy(root, delete_content, verdict, verdict_reason, color)
  -- verdict processing
  root.processing.verdict = verdict;

  -- checks, whether the object has to be saved in the database
  if not delete_content then
    -- verdict reason is indicated
    root.processing.verdict_reason = verdict_reason;
    -- the object is marked with a color
    root.processing.color = color;
  else
    -- otherwise, the object is not stored in the database
    root.processing.delete_content = true;
  end;
end;

function CheckGarbage(root)
    --checks whether the object contains garbage traffic
    local garbage, tag;

    garbage,tag=IsGarbage(root);

    if garbage then
    -- if the object contains garbage traffic
        return true,Verdict.Allowed,'Garbage traffic','GREY';
    end;

    -- otherwise there is an indication that the policy is not applicable
    return false;
end;


function CheckCrawlerPolicy(root)
  -- checks whether the object was assigned with any categories belonging to the parent
categories “Confidential information”,
  -- “Company structure”
  if CategoriesFromListDetected(root, {'CONFIDENTIAL','STRUCTURE'}) then
    -- if such categories are found, there is an indication that the policy is applicable the
list of parameters
    return true,Verdict.Forbidden,'Leak of confidential information','RED';
  end;

  -- checks whether the object contains any extracts from sample documents
  if SampleDocumentDetected(root) then
    -- if extracts are found, there is an indication that the policy is applicable and the
list of parameters
    return true,Verdict.Forbidden,'Leak of confidential information','RED';
  end;

  -- checks whether the object contains any text objects defined as personal data
  if root_has_sector_text_object(root, 'PersonalData') then
      return true,Verdict.Forbidden,'Leak of personal data','RED';
  end;

  -- checks whether the object contains any text objects defined as private financial
information
```

```
  if root_has_sector_text_object(root, 'Finance') then
      return true,Verdict.Forbidden,'Leak of finance information','RED';
  end;

  if root_has_sector_text_object(root, 'Insurance') then
      return true,Verdict.Forbidden,'Leak of insurance information','RED';
  end;

  if root_has_sector_text_object(root, 'OilAndGas') then
      return true,Verdict.Forbidden,'Leak of sensetive data','RED';
  end;

  if root_has_sector_text_object(root, 'Production') then
      return true,Verdict.Forbidden,'Leak of sensetive data','RED';
  end;

  if root_has_sector_text_object(root, 'Telecommunications') then
      return true,Verdict.Forbidden,'Leak of sensetive data','RED';
  end;

  -- checks whether the object is assigned with any categories belonging to the parent
category “Violation of the law of Russian Federation”
  if CategoryFromListDetected(root,'BAZA_PROTIVOD') then
    -- if such category is detected, there is an indication that the policy is applicable and
the list of parameters
    return true,Verdict.Forbidden,'Violation of the law of Russian Federation','LIGHT_RED';
  end;

  -- checks whether the object contains any information indicating using prohibited web-
resources
  if TagsFromListDetected(root,{'_DANGEROUS_','_AGGRESSIVE_','_ADULT_'}) then
    -- if there is such information, there is an indication that the policy is applicable and
the list of parameters
    return true,Verdict.Forbidden,'Violation of the law of Russian Federation','LIGHT_RED';
  end;

  -- checks, whether any recipients are included in the group of suspicious recipients
  if GCC:IsRecipientInGroup(root, 'SUSPICIOUS_RECIPIENTS') then
    -- if any recipients are found, there is an indication that the policy is applicable and
the list of parameters
    return true,Verdict.Forbidden,'Recipient is found in the group of suspicious
recipients','ORANGE';
  end;

   -- проверяется если конфликт идентификации отправителя, получателя, или рабочей станции
  if IsIdentityConflict(root) then
    -- если конфликт есть, возвращается признак того, что политика применима и перечень
параметров
    return true,Verdict.Forbidden,'Identity conflict','ORANGE';
  end;

  -- checks, whether the object contains any attachments with unknown format
  if UnknownFormatDecteted(root) then
    -- if the object contains any of these, there is an indication and the list of parameters
    return true,Verdict.Forbidden,'File with unknown format','LIGHT_ORANGE';
  end;

  -- checks, whether the object contains any encrypted content
  if EncryptedContentDecteted(root) then
    -- if the object contains any of these, there is an indication that the policy is
applicable and the list of parameters
    return true,Verdict.Forbidden,'Encrypted content','LIGHT_ORANGE';
  end;
```

```
  -- otherwise there is an indication that the policy is not applicable
  return false;
end;

-- Script ------------------------------------------------------------------------

function Process(root)
  -- * Transport mode setting (for each monitor)
  SetDefaultTransportMode(root);

  -- setting local variables

  local result,verdict, verdict_reason,color;


  if root.envelope.monitor == Monitor.Crawler then
    result,verdict,verdict_reason,color=CheckCrawlerPolicy(root);

    if result then
      ApplyPolicy(root,false,verdict,verdict_reason,color);
      return;
    end;

    ApplyPolicy(root,true,Verdict.Allowed,'Nothing is detected','');
    return;

  end;

  -- Garbage traffic
  result,verdict,verdict_reason,color = CheckGarbage(root);
  -- if the object falls under the conditions of the policy
  if result then
    -- apply the policy, delete the object
    ApplyPolicy(root,true,verdict,verdict_reason,color);
    -- stop object processing, do not use other policies
    return;
  end;

  -- * Checking an intercepted object for applicability of one of the policies

  -- Checking the applicability of the permission policy
  result,verdict,verdict_reason,color = CheckPermissionPolicy(root);
  -- if the object falls under the conditions of the policy
  if result then
    -- apply the policy
    ApplyPolicy(root,false,verdict,verdict_reason,color);
    -- if it is not necessary to store an object in the database, set the second parameter
(delete_content) true
    -- stop object processing, do not use other policies
    return;
  end;

  -- Checking the applicability of the violation check policy
  result,verdict,verdict_reason,color = CheckViolationPolicy(root);
  -- if the object falls under the conditions of the policy
  if result then
    -- send notification to user
    SendNotificationUser(root);
    -- apply the policy
    ApplyPolicy(root,false,verdict,verdict_reason,color);
    -- stop object processing, do not use other policies
    return;
```

```
  end;

  -- Checking the potential violation policy applicability
  result,verdict,verdict_reason,color = CheckPotentialViolationPolicy(root);
  -- if the object falls under the conditions of the policy
  if result then
    -- apply the policy
    ApplyPolicy(root,false,verdict,verdict_reason,color);
    -- stop object processing, do not use other policies
    return;
  end;

  -- Checking the applicability of the policy of web-resources misuse
  result,verdict,verdict_reason,color = CheckNoPurposeResourcesUsagePolicy(root);
  -- if the object falls under the conditions of the policy
  if result then
    -- apply the policy
    ApplyPolicy(root,false,verdict,verdict_reason,color);
    -- stop object processing, do not use other policies
    return;
  end;

  -- Applying the policy that permits the transmission of regular objects
  ApplyPolicy(root,false,Verdict.Allowed,'Nothing is detected','');

end;
```

8 Analyzing Intercepted Objects

During the analysis of the objects the user can perform the following actions:

- Generation of Queries by Objects
- Working with Objects
- Generating Object Reports
- Managing the Queries and Reports Folders

8.1 Generation of Queries by Objects

Objects verified by the system are stored in the database. If you want to view the information about the objects loaded into the database in the Management Console, you should create and run a query.

To work with queries, use the **Queries** section (the **Monitoring** area on the **Navigation** pane). You can group queries by folders for more convenience (see "Managing the Queries and Reports Folders").

For more details about creating queries reports see the following sections:

- Query Optimization Rules
- Text Search Features
- Creating and Editing a Query
- Copying a Query
- Deleting a Query

8.1.1 Query Optimization Rules

In order to optimize the queries, the object attributes (for the full list, see "General Object Attributes" and "Envelope Headers and Object Headers") are divided into 3 groups:

- **General attributes**. The information associated with the object being processed by InfoWatch Traffic Monitor. Also contains the information about the object sender and receiver.
- **Envelope headers**. An envelope is a data set for transferring an object, for example, *Source IP address*, *Interception Server*, *Destination Port* etc.
- **Object headers**. This group displays the information about the headers of an object. The header set is defined by object type, for example, *From*, *To*, *Cc*, *Subject* etc.

Running queries on the general attributes require the least amount of time. If you add envelope and/or object header to the query condition, the time to execute the query will increase.

To speed up a query, follow the rules below (the rules are arranged in the order of efficiency, that is, the first rule gives the best performance boost):

1. Create a condition to search for objects by the *Object ID attribute*. Searching objects by the identifier is the fastest search method.
2. Create a condition to search for objects by the *Capture Date attribute*. The shorter the time period is specified in this condition, the faster the query will run.
3. Create a condition to search for objects by the following general attributes: *Verdict*, *Configuration Version, Delivery Date, Responsibility Zone*, *Monitor*, *Sender*, *List of recipients*, *Last Name .*
4. Create a condition that searches using either the envelope headers or the object headers or the following general attributes: *Category*, *Tag*, *Object Type*, *Color*.
5. Avoid joining conditions with the *OR* operator whenever possible.

If you want to optimize a query containing only the general attributes that are not mentioned in rules 3 and 4, please contact the customer support service.

8.1.1.1 General Object Attributes

This section lists general object attributes and indicates the availability of these attributes in different forms:

- **Queries/Reports** (see "Creating and editing a query" and "Creating and Editing a Report"):
  - **Query/report conditions** - if the creating of a condition using this attribute value is available (see " Configuring Query Conditions");
  - **Viewable fields** - if this attribute is a viewable field at the object pane (see "Selecting Fields to View");
  - **Sorting** - if the sorting according values is possible for this attribute values (see "Configuring Sorting Conditions");
  - **Grouping** - if the grouping according values is possible for this attribute values (see "Configuring Grouping");
- **Object Info pane** - if the attribute information displays at the object information pane (see "Configuring the Object Info Pane");
- **Visibility** - if the attribute information displays at the object information pane when the "Show object context mode" disabled (see "Configuring the Object Content Preview Mode")

Object attribute	Description	Queries/Reports				Object Infopane	Visibility
		Query/report conditions	Viewable Fields	Sorting	Grouping		
Identity Errors	Signs of errors that occurred when identifying the object: if several matches were found for one value in the Active Directory, when identifying the *Sender*, *Recipients* or *Workstation* attributes (see "Persons and Workstations Directory").	+	-	-	-	-	-
Attachments	Presence of any attachments in the object	+	+	+	+	-	-
Capture Date	The date and time when the object was intercepted by the System	+	+	+	+	+	+
Category	Categories assigned to an object during the analysis	+	-	-	-	+	+
Color	Color assigned to an object	+	+	-	-	+	+
Configuration Version	Version of configuration used to analyze the object	+	+	+	+	+	+
Decision	The user decision made on an object	+	+	+	+	+	+
Delivery Attempts	Count of attempts to deliver the object to the recipient	+	+	+	+	+	+
Delivery Date	Date and time of transmitting the object for further delivery	+	+	+	+	+	+
Delivery State	The status of the object delivery	+	+	+	+	+	+
Insert Date	The date and time of saving the object to the database	+	+	+	+	+	+
Monitor	Type of intercepting monitor	+	+	+	+	+	+
Object Errors	Signs of errors that occurred when processing the object	+	+	+	+	+	+
Object ID	The unique identification number of the object in the database. **Note**. A unique identification code is assigned not only to objects but also to attachments. Therefore, when sorting the entries by this attribute, the ID numbering may appear with inconsistent (1, 3, 5, etc.)	+	+	+	+	+	+
Object Size	Size of the object	+	+	+	+	+	+
Object Text	Text extracted from the intercepted object	+	-	-	-	+	-
Object Type	Type of the object	+	-	-	-	+	+
Recipients	One or several recipients of an object	+	+	+	+	+	-
Responsibility Zone	Responsibility zone assigned to an object during its processing	+	+	+	+	+	+
Sample document	Sample documents with matching quotes detected during the analysis. The code (unique identification code), file name and path are displayed for each document	+	-	-	-	+	+
Sender	Information about the sender of the object	+	+	+	+	+	+

Summary	Object description. Generated by the system according to the template: <Monitor> object from <Sender>	+	+	+	+	+	+
Tag	Tags assigned to an object	+	-	-	-	+	+
Text Object	Types of text objects found in object during the analysis	+	-	-	-	+	+
Transport Mode	Transport mode defined for the object	+	+	+	+	+	+
Verdict	A verdict assigned to the object	+	+	+	+	+	+
Verdict Reason	Description of the reason why a certain verdict was assigned to the object	+	+	+	+	+	+
Workstation	The workstation from where the object was sent **Note**. The value of this attribute can be displayed in one of the following formats: • name of workstation from Active Directory, if defined; • DNS, if the name of the workstation was not found in Active Directory; • IP address, if the name of the workstation not found in Active Directory or DNS.	+	+	+	+	+	+
Workstation description	Additional data on the workstation imported from Active Directory	-	+	+	+	+	+

8.1.1.2 Envelope Headers and Object Headers

This section lists headers of envelopes and objects, corresponding names in context (see "detailed view of an object") and descriptions.

Header name	Context header name	Description
Envelope header		
Domain	auth_domain	Domain or analog of the domain (from authorization data)
Workstation	auth_host	Information about workstation (from authorization data)
Scheme	auth_scheme	Authorization scheme name (basic, digest, ntlm, local, radius)
Authentification	auth_source	Initial line with authorization data after decoding and format prefixes removing
User	auh_user	The identifier of the user (from authorization data)
Domain	domain	Domain
User	login	Login

First name	userfirstname	User's first name
Last name	userlastname	User's last name
ICQ-initiator	initiator_uin	UIN of the employee from which object interception is made
ICQ-initiator	session_initiator_uin	UIN of the session initiator
IM-initiator	im_initiator	Name of the employe's account from which object interception is made
SMTP-sender	mail_from	Sender e-mail (from a SMTP envelope)
SMTP-recipients	rcpt_to	Recipients e-mail (from a SMTP envelope)
Workstation	workstation	The workstation identifier on which object interception is made
Source IP-address	source_ip	The IP address from which a request was sent
Port	source_port	Port from which a request was sent
Path	source_path	Directory containing the query source
Path to file	destination_path	Network way to the file
IP-address destination	destination_ip	The server IP address (corresponds to the IP address for which TCP session is opened)
Destination port	destination_port	The server port (corresponds to port for which TCP session is opened)
Device type	device_type	Peripheral type
Device name	device_name	Peripheral name
URL, full	url_host_fqdn	Full URL of resource on which the file is transferred
URL, IP-address	url_host_ip	URL including the IP address of resource on which the file is transferred

URL resource	url_host	URL of resource on which the file is transferred
URL, parameters	url_parameters	Value of parameter <parameter> contained in URL
URL, password	url_password	Value of parameter <password> contained in URL
URL, path	url_path	Directory at resource on which the file is transferred
URL, port	url_port	Port on which the file is transferred
URL, schema	url_schema	Value of parameter <scheme> contained in URL
URL, user	url_username	Value of parameter <username> contained in URL
Operation type	operation	Operation is being processed
Job	job	Task name
Application	creator_applicaion	The application from which data transmission was made
Interceptor	interceptor	Name of interceptor monitor
Interception result	action	Information on results of the intercepted object processing
Policy	policy_name	Name of scanning policy
Rule	rule_name	Name of scanning rule
Policy rule	policy_rule	Name of the policy rule (used for ensuring compatibility of different versions of System)
Interception server	capture_server	The identifier of the server which intercepted the object
Presence of shadow copy	event_type	Event type. Can accept one of the following values: • [Monitor] EventFull - with the shadow copy, • [Monitor] EventNoShadowCopy - without the shadow copy
VLAN 802.1AD	vlan_802_1ad	Data on used VLAN in a point of object interception
VLAN 802.1Q	vlan_802_1q	

Object header		
Shadow copy	cc	File copy which has been successfully created on the removable device
Cookie	cookie	The office data on using the HTTP protocol by the workstation
Date	date	Date and time of sending message
Sender	from	Information on the object sender. For Skype Monitor - information on the user of Skype from which workstation the object was received
Importance	importance	Level of the object importance, specified for SMTP object by the user
Name	name	Object name
Priority	priority	Condition for definition of object check sequence
Subject	subject	Message subject
Recipient	(to)	Information abut the object recipient
Chain of addresses	x-forvarded-for	The established chain of information transfer - from the Sender to the Recipient

8.1.2 Features of Searching in the Text

Searching for objects and attachments in the text is done using Oracle Text. When building a query, you must consider the specifics of Oracle Text.

For more details about text search specifics see the following sections:

- Indexing
- Syntax in Query Conditions
- Examples

8.1.2.1 Indexing in Oracle Text

Text indexes are used for searching words in a text. Text index is a list of words generated by Oracle Text based on intercepted objects and attachments texts with links to the objects where the specified words are found.

In a text index query the user specifies the text that should be found in the object. When running the query, this text is processed according to the same rules that are used for indexing the original document. That provides for the correct search in the text index.

When a text index is built, separate words or characters are selected from the text. Space or tab are used as separators for Western European languages.

Then the selected words that can be formed from different characters are converted to words containing the alphanumeric characters:

- The "-" and "\" characters are considered hyphenation marks. If this character is placed at the end of a line, then a part of the word before the character and the part of the word after the character are considered a single word.

  Example:

Original word	Processed word
yellow- green	yellowgreen
yellow-green	yellow green

- The ".", "!", and "?" characters are considered punctuation marks. They are deleted in the process of indexing.

Text search is not case sensitive. For example, "MoM" and "mom" are identical for text search.

Indexing preserves the word order, and therefore you can search for phrases.

In addition, when indexing texts, Oracle Text excludes the words that appear in the stop list. These words are usually pronouns, prepositions, particles. For example, the following words are specified for English: *just*, *some*, *Mrs*, etc.

For more information on how to use Oracle Text, see the Oracle DBMS documentation (Oracle Text Reference, version 11g).

8.1.2.2 Syntax in Query Conditions

You can use the following characters and keywords to create query conditions:

Character	Keyword	Operator description
&	AND	Condition includes all the words joined by the operator
=	EQUIV	The words joined by the operator are considered equivalent
~	NOT	A word following the operator is excluded from the condition
|	OR	Condition includes any word joined by the operator
{ }		Escapes the bracketed word. It's used to find a reserved word (see the table below)
\		Escapes the next character. It's used to find a reserved character (see the table below)

Character	Keyword	Operator description
( )		Bracketed expression has a higher priority
[ ]		Bracketed expression has a higher priority
%		Replaces any number of characters in a word
_		Replaces one character in a word

You should shied the following reserved words and characters in the search query conditions:

ABOUT	MINUS	TR	-
ACCUM	NEAR	TRSYN	;
AND	NOT	TT	~
BT	NT	WITHIN	|
BTG	NTG	,	$
BTI	NTI	&	!
BTP	NTP	=	>
EQUIV	OR	?	*
FUZZY	PT	{ }	%
HASPATH	RT	\	_
INPATH	SQE	( )	
MDATA	SYN	[ ]	

8.1.2.3 Examples

InfoWatch Traffic Monitor builds text indexes with default settings. You must consider it when building search queries. The examples of processing search queries are provided below.

Let us assume that there are several text fragments taken from different documents:

D1	A big pond- skater was found in Novospasskaya village in the south of Smolensky region. Its length is 5 cm and its width is 4.32 cm.
D2	Village inhabitants say that it has blue-black color and mov#s very fast.
D3	It was first noticed on 5/14/2008. Before that, a huge pond-skater was discussed by Grigorovo village inhabitants who reported an even bigger size of the insect. They said it was dark-green in color.
D4	The suite includes two walk-in closets and a bath-room with a deep Jacuzzi tub and separate white tile

	shower.

The analysis will select the following words from the document:

D1	**D2**	**D3**	**D4**
4,32	FAST	05	BATH
5	S	14	CLOSETS
A	SAY	2008	DEEP
BIG	VILLAGE	MORE	INCLUDES
WAS	HABITANTS	WAS	JACUZZI
IN	AND	POND-SKATER	ROOM
POND-SKATER	HAS	FIRST	SEPARATE
VILLAGE	BLUE	GRIGOROVO	SHOWER
LENGTH	IT	IT	SUITE
IT	VERY	EVEN	TILE
IN	MOV	INHABITANTS	TUB
THE	COLOR	NOTICED	TWO
NOVOSPASSKAYA	BLACK	REPORTED	WALK
REGION	THAT	GREEN	WHITE
FOUND		THAT	
CM		SAID	
CM		INSECT	
SMOLENSKY		EVEN	
IS		ABOUT	
WIDTH		DISCUSSED	
SOUTH		HUGE	
		IT	
		THEY	
		SIZE	
		BEFORE	
		VILLAGE	
		DARK	
		COLOR	

The *4.32* number is included in the index although the "." character separates the string in two parts. The reason is that the digits are located to the left and to the right of the period, so the whole set is considered a single number.

The date *14.05.2008* is divided into separate numbers.

In the second document (D2), the word *moves* is misspelled: *mov#s*. Therefore, the index includes two words: *MOV* and *ES*.

The word *blue-black* is divided into two words, *BLUE* and *BLACK*.

The following examples demonstrate the principles of creating search queries.

Example 1. Search for single words

Query condition: *pond-skater*

Result: D1 and D3

Comments: In the D1 document the word *pond-skater* is hyphenated. Therefore it was merged into one word and found by the query. In the D3 document text, the word is present in the same form as it is in the query.

Example 2. Search for phrases

Query condition: *blue black*

Result: D2

Comments: The words *blue* and *black* are located in D2 near next to each other. Therefore, the phrase *blue-black* will be found in D2.

This example can be used to find words following each other, i.e. forming a phrase. The example 4 shows the query to search for words separated by the other words.

Example 3. Shielding a reserved character

Query condition: *blue\-black*

Result: D2

Comments: The reserved "-" character is shielded with "\" and is therefore processed as an ordinary character. When the query is lemmatized according to general rules the *blue black* phrase found in D2 will remain.

Example 4. Search for non-adjacent words

If you need to find words that don't make a phrase (i.e. they are separated by the other words in the text) then the phrase search won't give you the results you need. Example:

Query condition: *blue fast*

Result: no results

Comments: The words *blue* and *fast*are present in D2. However, they are separated by another word. So nothing will be found.

To search for non-adjacent words please use the *&* character or the "AND" operator. Example:

Query condition: *pond-skater & length*

or

pond-skater AND length

Result: D1

Comments: In this case the "&" character and the word "AND" are reserved. This expression means that the document contains the words *pond-skater* and *length*. Both words are present only in the D1 document.

Example 5. Using EQUIV

Query condition: *big EQUIV huge pond-skater*

or

big = huge pond-skater

Result: D1 and D3

Comments: The EQUIV operator states that the words around it are equivalent parts of the query. Practically it means that the following queries will be executed: *big pond-skater* and *huge pond-skater .* Therefore, the D1 and D3 documents will be found.

Example 6. Using NOT

Query condition: *pond-skater NOT grigorovo*

Result: D1

Comments: This expression is interpreted as follows: the document should contain only the *pond-skater* word and should not contain the word *grigorovo.* Only the D1 document matches these conditions.

Example 7. Using OR

Query condition: *novospasskaya OR grigorovo*

Result: D1 and D3

Comments: This expression is interpreted as follows: the document should contain the word *novospasskaya* or the word *grigorovo.* The D1 and D3 documents match these requirements.

Example 8. Shielding a reserved word and character

Query condition: *closets {and} a bath\-room*

Result: D4

Comments: The word AND and the "_" character are escaped in this example. Search result – document D4.

Example 9. Using brackets

Query condition 1: *(pond-skater OR very) AND color*

Result 1: D2 and D3

Query condition 2: *pond-skater OR (very AND color)*

Result 2:	D1, D2 and D3
Comments:	Condition 1 means that the document should contain one of the words: *pond-skater* or *very,* and it must also contain the word *color.* D2 includes the words *color* and *very,* D3 includes the words *pond-skater* and *color*. Condition 2 means that the document should include the word *pond-skater* or the words *very* and *color.* D1 and D3 include the word *pond-skater* , and D2 includes both the words *very* and *color*.

Example 10. Using the "%" wildcard

Query condition:	*big%*
Result:	D2 and D3
Comments:	The "%" wildcard replaces any number of characters so the query returns the documents D2 with the word *Big and* D3 with the word *bigger*.

Example 11. Using the "_" wildcard

Query condition:	*villag_*
Result:	D1 and D2
Comments:	The "_" wildcard replaces one character so the query returns the D1 document and D2 document.

Example 12. Using several features

Query condition:	*(Novospasskay% villag_=Grigorov_) OR walk\-in*
Result:	D2, D3 and D4
Comments:	The condition *(Novospasskay% villag_=Grigorov_)* results in the D2 and D3 documents containing *Novospasskaya village* and *Grigorovo* respectively. The *walk\-in* condition returns the D4 document. Since these conditions are joined with the OR operator, all the three documents will be returned as the result.

8.1.3 Creating and Editing a Query

Important!

The section "Query Optimization Rules" gives recommendations on speeding up the queries.

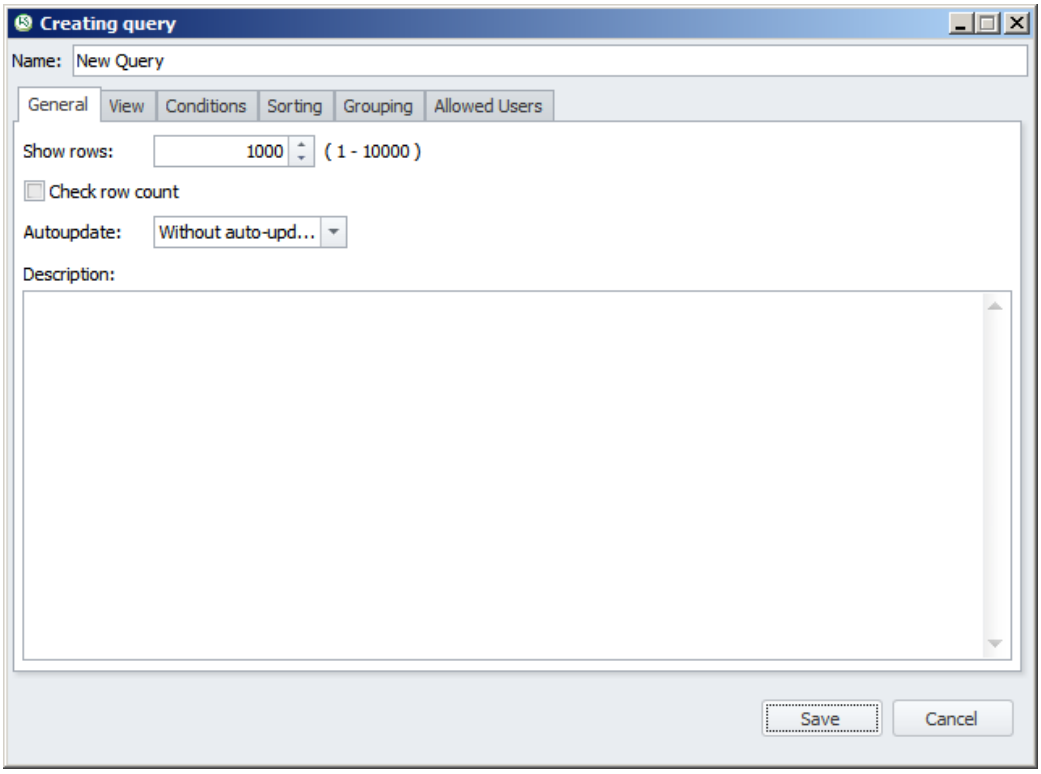
To create a query:

1. Go to the **Queries** section.

2. Do the following:

Action	Procedure
Create a query	Do one of the following: • in the main menu, select **Edit > New Query** • click **New Query** on the toolbar
Edit a query	1. In the list of queries select the row with the required query. 2. Do one of the following: • in the main menu, select **Edit > Edit**; • click **Edit** on the toolbar.

A dialog box to configure the query will appear on the screen.



The query configuration dialog box

3. In the **Name** field, specify the query name.

4. Configure the query settings using the following tabs:

Tab name	Action
General	Configuring general settings
View	Selection of object attributes that will be shown on the objects pane

Tab name	Action
Conditions	Configuring query conditions
Sorting	Setting the objects sorting order
Grouping	Setting the objects grouping order
Allowed Users	Selection of users who can run the query

5. After having configured all the settings click **Save**.

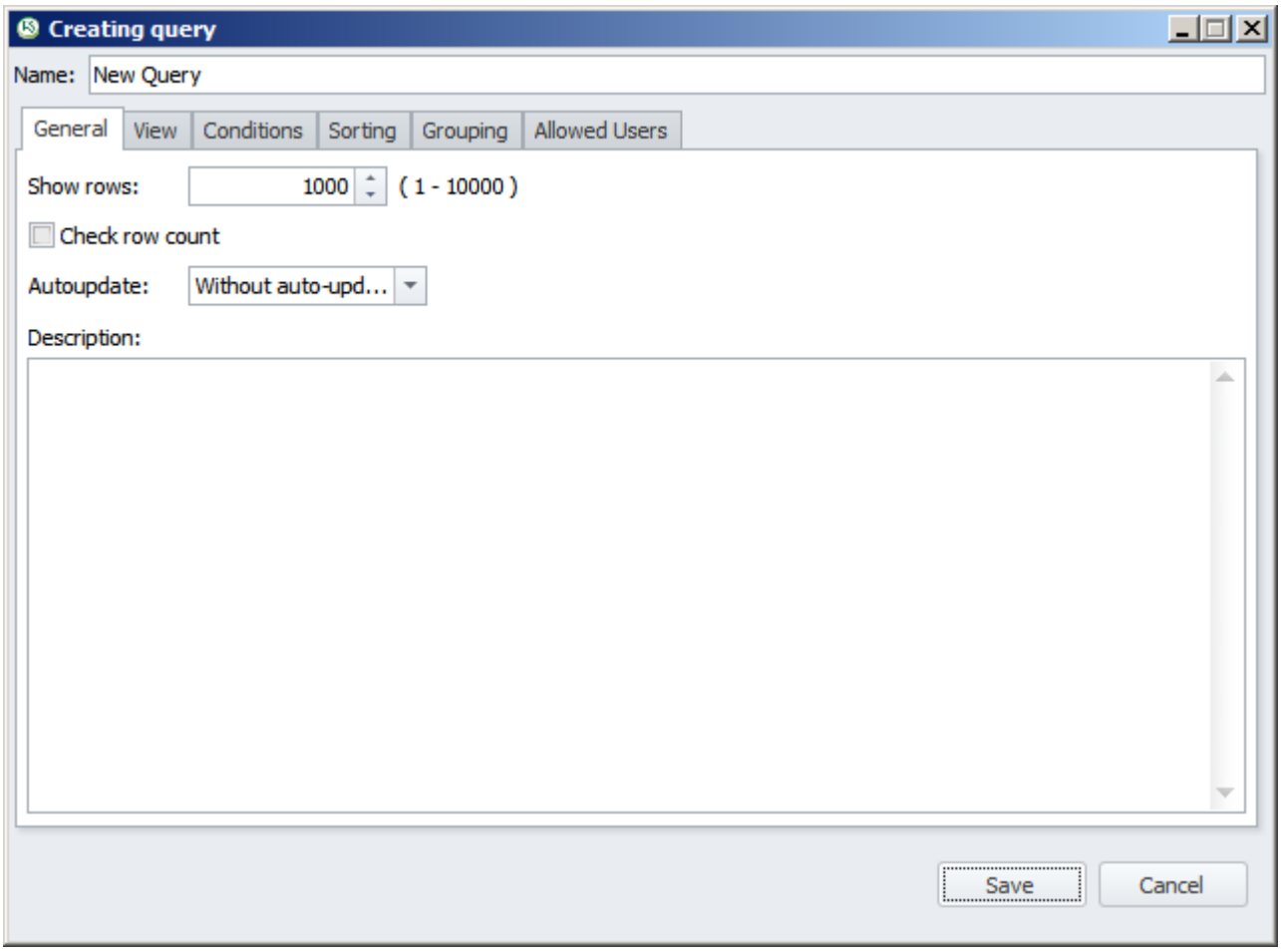
Note

To view the records that match the new query, you must run the query (see "Running Object Queries").

8.1.3.1 General Query Settings (General tab)

The **General** tab is used to configure the general settings of a query:

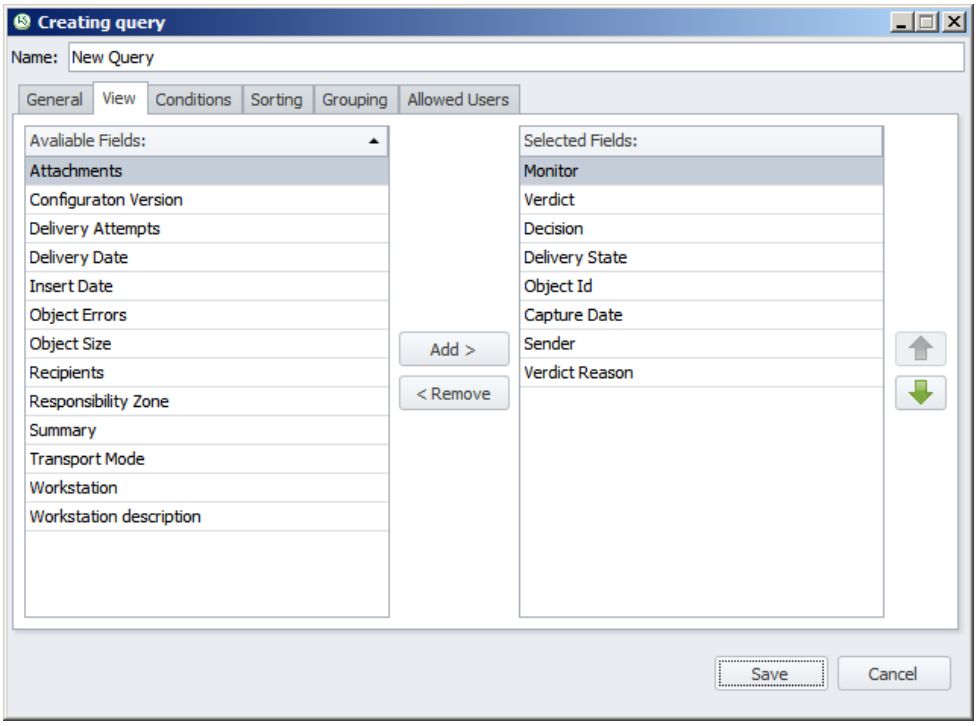
- **Show rows**. The maximum number of records to be displayed in the working area of Management Console (from **1** to **10000** records). Default value: **1000** records.
- **Autoupdate**. To define the automatic update you should choose needed period in the dropping list (for more information about changing the autoupdate period for pre-existed query see "Query Autoupdate").
- **Check row count**. If this checkbox is selected and the number of records is more than the value in the **Row Count** field, then the status bar will show the total number of DB records matching the query. The check box is clear by default.
- **Description**. Query description.



The "General" tab

8.1.3.2 Selecting Fields to View (View tab)

The **View** tab is used to select the record attributes to show the information in the viewing area (by default only some general attributes are shown).



The "View fields" tab

View fields are configured using the following buttons:

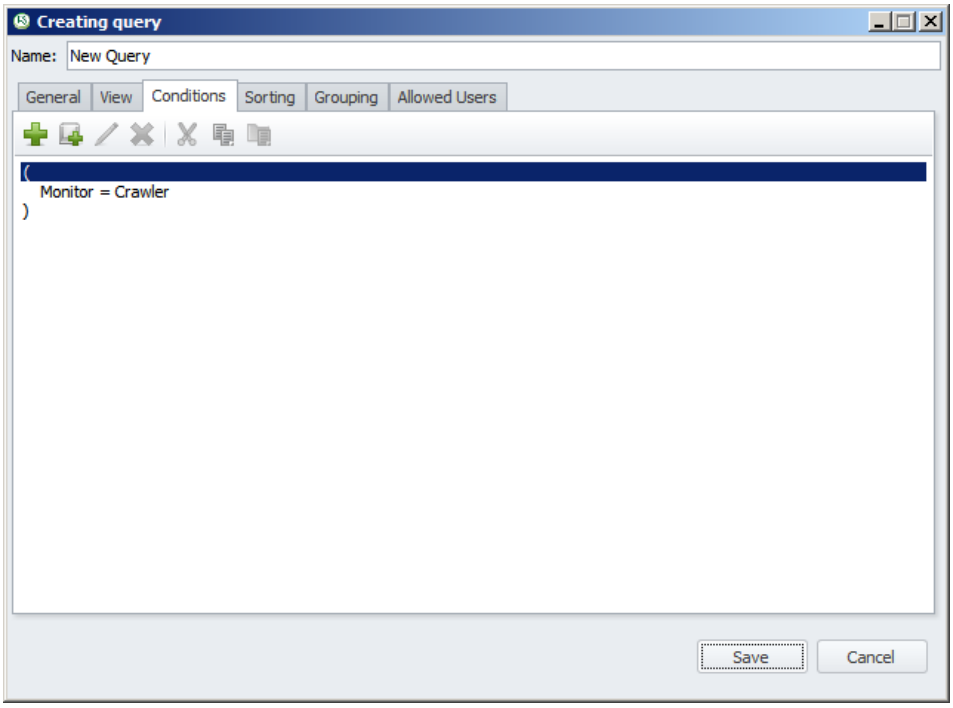
Button	Button name	Button function
Add >	**Add**	Move the field from the Available list to the Selected list.
< Remove	**Remove**	Move the field from the Selected list to the Available list.
	**Up**	Move the selected field one row up (the column with values of this setting will be shown to the left of the view area)
	**Down**	Move the selected field one row down (the column with values of this setting will be shown to the right of the view area)

Important!

If some attributes are removed from the list, their information will not be displayed. All the query settings (query conditions, sorting order, grouping) of these attribute will be lost.

8.1.3.3 Configuring Query Conditions (Conditions tab)

When creating a query, you can configure the search by general attributes and/or the context search by object headers. The **Conditions** tab is used to select the database records.



The "Conditions" tab

Note

In order to perform the context search, the system supports re-indexing with a default interval of 10 minutes. The database administrator can change the interval, if necessary (see "*InfoWatch Traffic Monitor. Administration Guide*").

For mode details about conditions see:

- Creating a Query Condition
- Condition Settings
- Editing Query Conditions

8.1.3.3.1 Creating a Query Condition

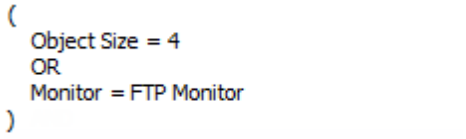
Note

Before creating conditions you should learn how to speed up queries ("Query Optimization Rules").

A condition can be simple (without operators) or compound. A compound condition contains several simple conditions joined by logical operators. To create a compound condition, the **AND** and **OR** logical operators are used.

If you use the **AND** logical operator, the returned records will meet all the specified conditions. If you want to find the records that meet at least one condition, use the **OR** logical operator.

Below is an example of linking two conditions using the **OR** logical operator.



Joining two conditions

You can use condition blocks to create more complex conditions. A **Condition Block** is a group consisting of a simple or compound condition, separated from another condition or group of conditions by a logical operator and brackets.

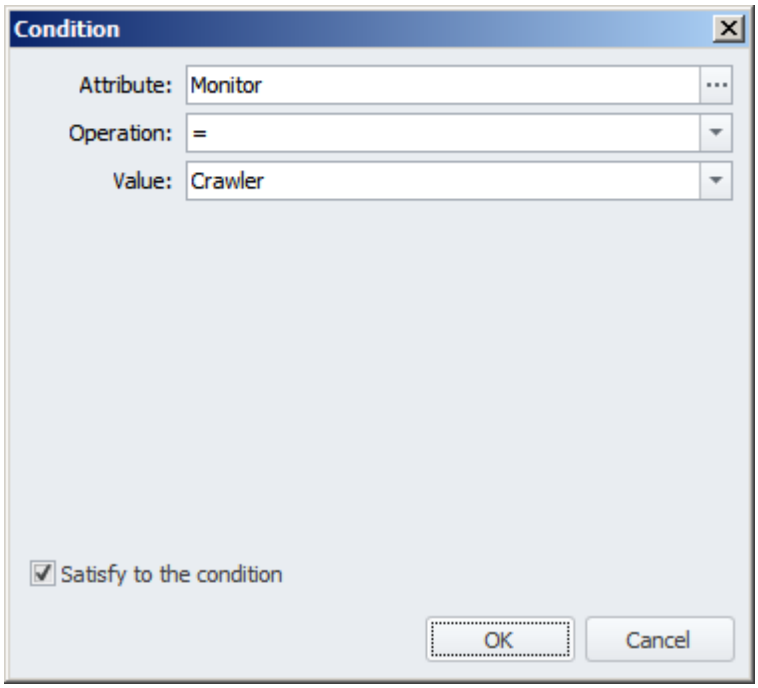
Specifics of using condition blocks:

- All conditions are inserted into the root block, which cannot be deleted.
- You can add other condition blocks into the condition block. Therefore, you can create several condition blocks linked by one logical operator inside the root block.
- The conditions of the same block are separated with brackets from the rest of the conditions.

To add a simple condition:

1. Select the row with an opening or closing parenthesis.
2. Click  **Add condition** in the top part of the tab.

   The **Condition** dialog box will appear on the screen.



Configuring query conditions

3. Set up the condition (see "Condition Settings").
4. Click **OK**.

   Click **OK**. The new condition will be displayed on the **Conditions** tab.

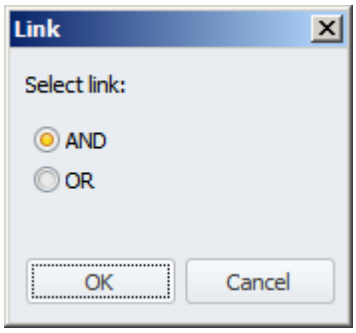
To add a composite condition:

1. Select the row with an opening or closing parenthesis.
2. Click **Add condition** in the top part of the tab. In the **Condition** dialog box, set up the first condition (see "Condition Settings").
3. Select the row to insert the condition after.

   Note

   If you select the closing bracket, the new condition will be inserted before the bracket.

4. Click **Add condition**. Specify the second condition and click **OK**. The **Link** dialog box will appear on the screen.



Select a logical operator

5. Select the required operator and click **OK**.

   After that, the **Conditions** tab will display the two conditions linked with the specified operator.

To add a condition block:

1. Select the row to insert the condition block after.

   Note

   If you select the closing bracket, the new condition block will be inserted before this bracket.

2. Click **Add Block**.

   If the brackets already contain a condition or a condition block, then clicking **Add Block** will result in opening the **Link** dialog box where you should select one of the available logical operators. Select the logical operator you need and click **OK**.

   A new condition block will then be displayed on the **Conditions** tab of the query dialog window.

3. Add a simple or a composite condition to the block.

You can also set more complex conditions. The example of a query combining several conditions is shown on the picture.

```
(
  Object Size = 4
  OR
  Monitor = FTP Monitor
  AND
  (
    Object Type = BMP image
)
```

Example of a complex condition

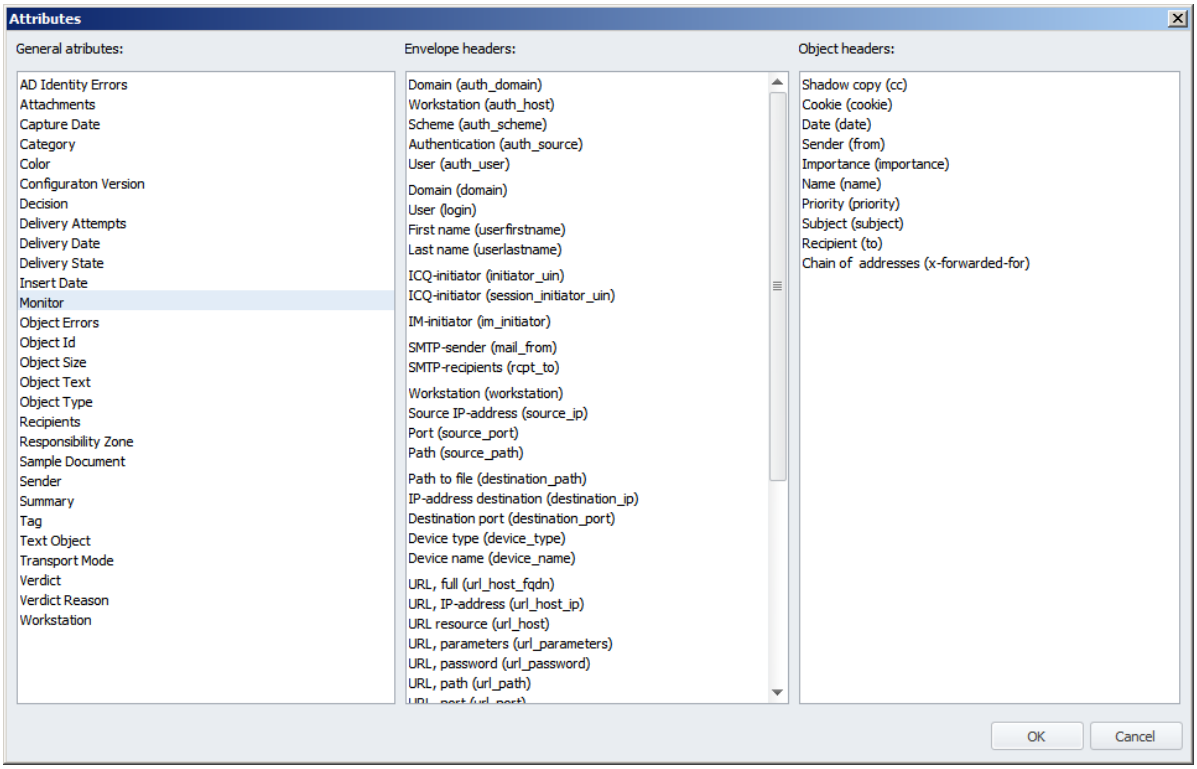
8.1.3.3.2 Condition Settings

Note

Before creating conditions you should learn how to speed up queries (see "Query Optimization Rules").

In the **Condition** dialog box, the settings of conditions are set:

- **Attribute**. Click ... . In the dialog box that appears, select the attribute to create a query condition for. You can set the conditions based on the general object attributes and on the headers. For the description of the attribute types see "Query Optimization Rules"; for the description of general attributes see "General Object Attributes"; for the description of several envelope headers see "Envelope Headers and Object Headers"; for the description of setting up the object headers to include into query conditions see "Configuring Search on Object Headers".



Selecting record attributes

- **Interval**. This setting is used only for searching records by date. Select the required time interval from the dropdown list. The following table contains the list of available intervals.

Interval	Description
Last {0} hour(s)	The last N hours (the beginning is the query start time minus N hours). The required value is set in the counter field (default value is 3 hours)
Current day	From 00 h 00 min 00 sec sec of the current day to the time of the query
Current week	From 00 h 00 min 00 sec of the first day of the current week to the time of the query
Current month	From 00 h 00 min 00 sec of the first day of the current month to the time of the query
Last day	From 00 h 00 min 00 sec sec of the previous day to the time of the query For example, the query is executed on May 16th, at 16.00.00. Then the resulting selection will contain the data from 00.00.00 of May 15th to 16.00.00 of May 16th
Last week	From 00 h 00 min 00 sec of the first day of the last week to the time of the query For example, the query is executed on Friday, May 16th, at 16.00.00. Then the resulting selection will contain the data from 00.00.00 of May 5th to 16.00.00 of May 16th
Last month	From 00 h 00 min 00 sec of the first day of the last month to the time of the query For example, the query is executed on May 16th, at 16.00.00. Then the resulting selection will contain the data from 00.00.00 of April 1st to 16.00.00 of May 16th
Arbitrary period	The period is defined by the user. The interval is set in the **Operation** and **Value** fields.

- **Operation**. In the drop down list, select a comparison operator.

  Each attribute has its own set of comparison operators. For the description of the values of comparison operators, see the following table.

Operator	Value
=	Equal
!=	Not equal
>	Greater than
<	Less than
>=	Greater than or equal to
<=	Less than or equal to
Between	A value range
is null	The object contains an attribute with a null value.
exists	The object contains the selected attribute
is empty	For the **Text object** attribute: no text has been received from the object and its attachments; for all other attributes: the selected header has no value
contains (a context search operator)	Text contains the specified value
All from the list	For ***Tag***, ***Sender***, ***Recipients*** and ***Workstation*** attributes there is a choice of

Operator	Value
assigned / Is in list / Not defined ... etc	reference values available. Available operations depends of selected attribute.

- **Value**. Select or enter the attribute value.

  Note

  To search records by attributes with empty fields, use the **"is null"** operator.

  When entering attribute values, you can use wildcards: "_" and "?" to represent one character; "%" and "*" to represent several characters.

  When you select the **between** operator, you can set the range limits in the **Values** fields: the top field contains the minimum value9964}, and the bottom field contains the maximum value.

  If you select the **contains** operator, the object text is searched using the Oracle Text function. For more information on configuring search settings see "Text Search Features". You can only use wildcards when entering the attribute values for the **contains** operator: "_" to represent one character and "%" to represent several characters. To check entered text of the condition click **Check**.

  Important!

  The "?" and "*" wildcards are not used in the **contains** operator.

- **Configuration**. This setting is only specified when creating conditions by the *Category* and *Tag*attributes, since these attributes support different versions of configuration. You can specify a certain version of configuration in a condition. In this case the query returns data on the objects that have been blocked when the specified configuration version was active on the server.

  To select a version, click ... In the dialog box that appears, select a row with the required version and click **OK**.

  Note

  To search objects regardless of the configuration version, select the **Find selected value in all configurations where it exists** check box.

- **Case insensitive**. Please specify it the search by attributes with text values should be case-sensitive. If the check box is selected, then the search is not case-sensitive. The check box is clear by default: the search is case sensitive.

- **Matches the condition**. Unselect the check box if you want to display the records that do not meet the specified conditions. The check box is checked by default.

8.1.3.3.3 Editing Query Conditions

The following actions are available when you edit query conditions:

- change the search condition;
- cut the search condition;
- copy search condition;
- insert search condition;

- change the logical operator between conditions;
- delete a simple query condition;
- delete a condition block;

The buttons used to edit query conditions are located in the top part of the **Conditions** tab.

To edit the search conditions

Do the following:

Action	Procedure
Change the search condition	1. Select the row with a condition to change. 2. Do one of the following: • click **Edit**; • double-click the selected row. 3. In the **Condition** dialog box, edit the settings of the selected condition (see "Condition Settings"). 4. Click **OK**.
Cut the search condition	1. Select the row with the condition to cut. 2. Click **Cut**.
Copy the search condition to the clipboard	1. Select the row with the condition to copy. 2. Click **Copy**.
Insert search condition	1. Point to the place you want to insert the condition from the clipboard. 2. Click **Paste**. By default, the condition is inserted using the **AND** operator. If necessary, you can change this operator (see below).
Change the logical operator between conditions	1. Select the row with the logical operator to change. 2. Do one of the following: • click **Edit**; • double-click the selected row. 3. In the **Link** dialog box please select another logical operator.
Delete a simple query condition	1. Select the row with the required condition. 2. Click **Delete**. **Note:** To delete a compound condition, you must delete all the simple conditions it contains.

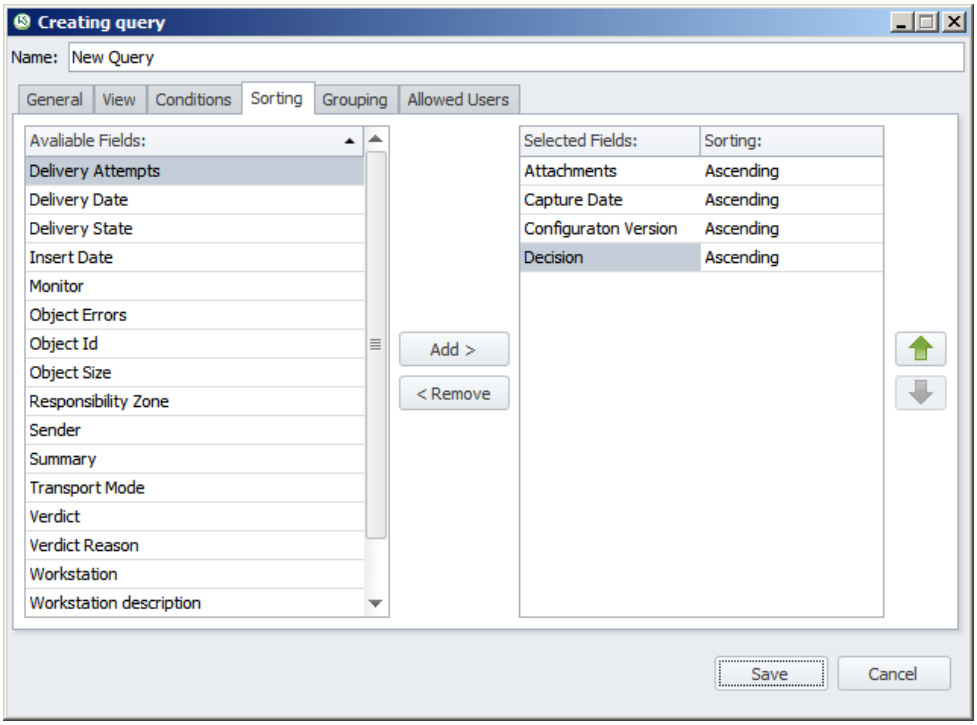
Action	Procedure
Delete a condition block	1. Select an opening or closing bracket of the condition block to be deleted. 2. Click **Delete**.

8.1.3.4 Configuring Sorting Conditions (Sorting tab)

The **Sorting** tab is used to set the record sorting rules. If the sorting is arranged by several attributes, the attribute on top of the list is applied first. Then the second attribute applies, etc.

Note

If sorting options are not set in the query condition, the objects will be sorted by *Object ID* in descending order when the query is run.



The "Sorting" tab

Sorting conditions are set using the buttons in the top part of the tab. Button functions:

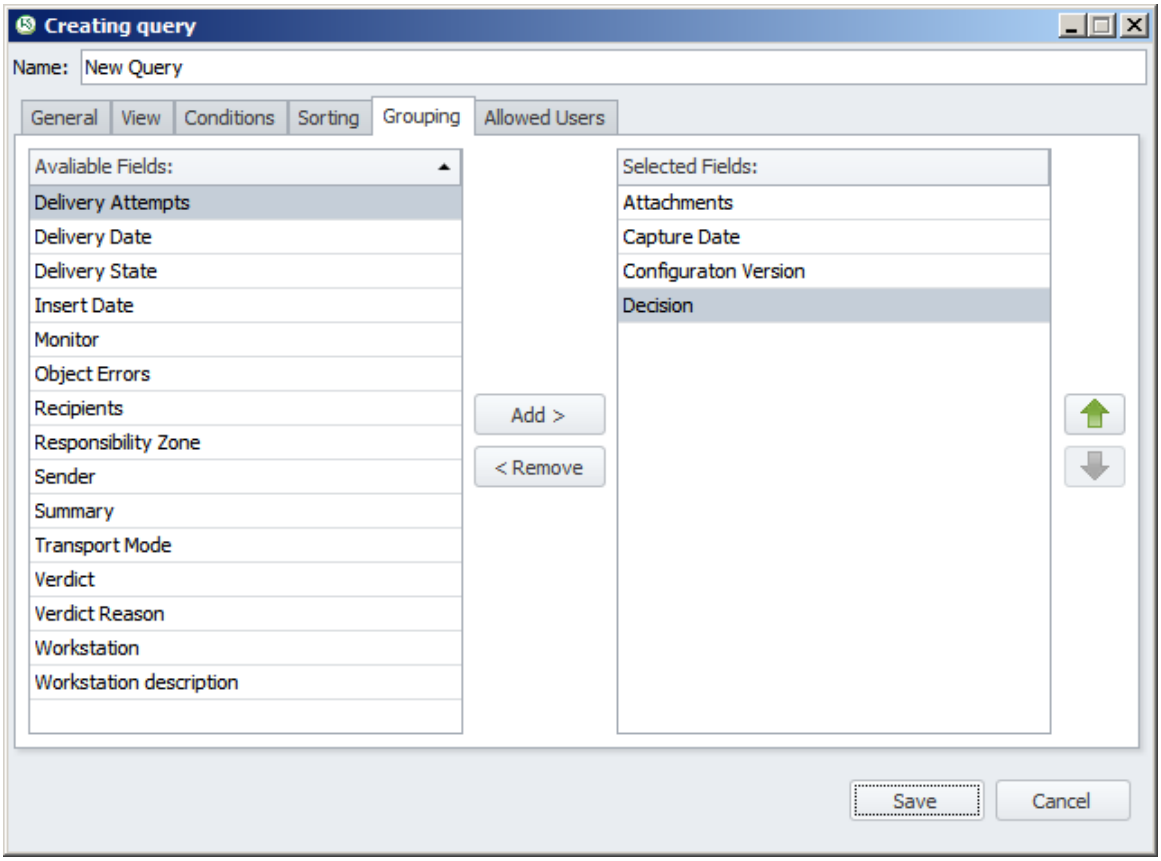
Button	Button name	Button function
Add >	**Add**	Move the field from the Available list to the Selected list.
< Remove	**Remove**	Move the field from the Selected list to the Available list.
	Up	Move the selected field one row up

Button	Button name	Button function
	**Down**	Move the selected field one row down

You can choose the sorting direction for selected fields: **Ascending** or **Descending** by choosing the desired value from the dropdown list in **Sorting** column. By default, ascending sorting is used.

8.1.3.5 Configuring Grouping (Grouping tab)

The **Grouping** tab is used to set up the grouping order. If the grouping is based upon several attributes, then the top attribute in the list is applied first. Then the second attribute applies, etc.



The "Grouping" tab

Grouping conditions are set using the buttons on top of the tab. Button functions:

Button	Button name	Button function
Add >	**Add**	Move the field from the Available list to the Selected list.
< Remove	**Remove**	Move the field from the Selected list to the Available list.
	**Up**	Move the selected grouping field one row up

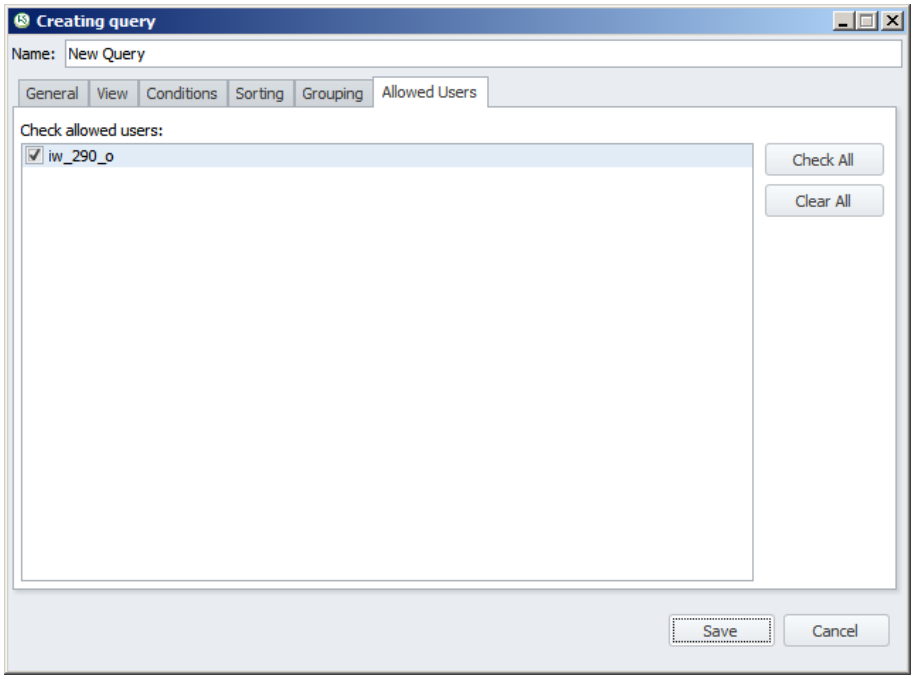
Button	Button name	Button function
	**Down**	Move the selected grouping field one row down

8.1.3.6 Setting Permissions for Handling a Query (Allowed Users tab)

The **Allowed Users** tab is used to set the users who will have the rights to work with the query (changing, deleting, executing, grouping).

Important!

Working with queries is allowed only if the role assigned to a user has the appropriate privileges.



The "Allowed Users" tab

To assign the privileges for working with the query,

select the check box to the left of the user's account.

To assign the right to view the query to all users, click the **Check All** button. If you do not want any of the users to be able to view the specified query, click the **Clear All** button.

8.1.4 Copying a Query

You can create a query by copying existing query

To copy a query:

1. Go to the **Queries** section.
2. On the query list pane, select the required query.
3. Do one of the following:
   - in the main menu, select **Edit > Copy**;
   - click  **Copy** on the toolbar.

The copy of the query will have the same parameters as the original query, but the number will be added to its name. For example, the copy of the "*All events for the period*" query will have the name: "*All events for the period* (1)".

8.1.5 Deleting a Query

To delete a query:

1. Go to the **Queries** section.
2. On the query list pane, select the required query.
3. Click  **Delete** on the query list pane.
4. In the confirmation box, click **Yes** to confirm.

8.2 Working with Objects

The following sections describe the general ways to work with objects:

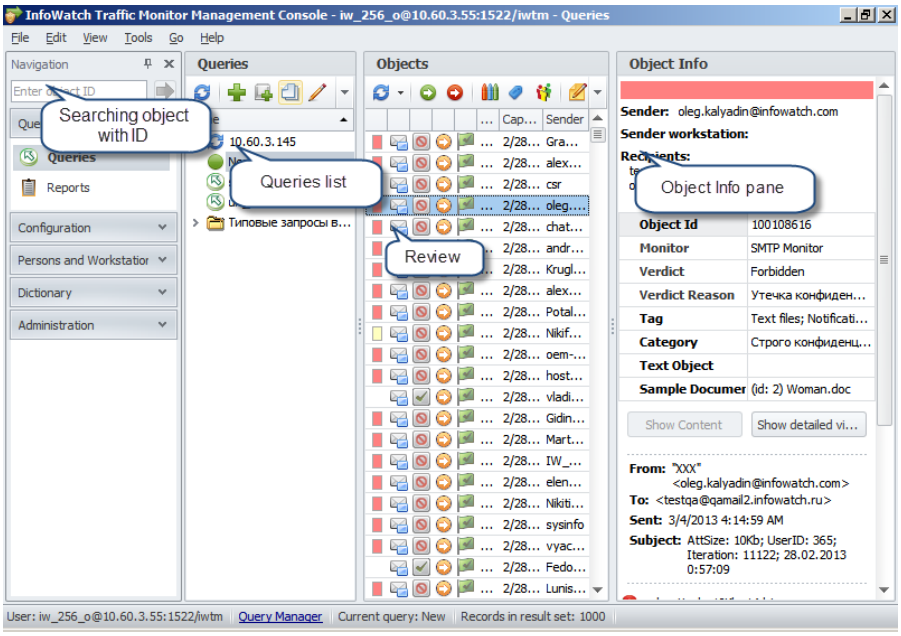
- Object Custom Analysis
- Moving Object to Another Responsibility Zone
- Sending an Object Report
- Assigning Tags to an Object
- Highlighting Objects with Color
- Adding a Comment to an Object
- Downloading Attachments, Messages, and XML Context

8.2.1 Object Custom Analysis

The object information is displayed in the **Queries** section (the **Monitoring** area in the **Navigation** pane). In every section the working area of the main window contains three panes:

Pane name	Pane purpose
Queries	List of available queries **Note:** If the query list pane is not displayed in the main window, select **View > Query List** in the main menu.
Objects	Display general object information **Note:** This pane shows information only for the attributes (view fields) set in query conditions
Object Info	General object information including the list of attachments and the object text. **Note:** If the Object Info pane is not displayed in the main window, select **View > Object Info** in the main menu. **Note:** For more information about setting up the fields on the Object Info pane see " Configuring the Object Info pane".

You can open the detailed view (see "Detailed View of an Object") of object without a query: just enter its ID to the field at the top of Navigation pane and click .



View general object information

For more details about running object analysis see the following sections:

- Configuration of Object Content Preview Mode
- Setting the Size Limits for Downloaded SMTP Messages and Print Jobs
- Configuring the Object Info pane

- Running Object Queries
- Query Autoupdate
- Query Manager
- Viewing Objects Information
- Processing the Sender, Recipient, and Workstation Data
- Making the Decision about an Object
- Putting under Control

8.2.1.1 Configuring the Object Content Preview Mode

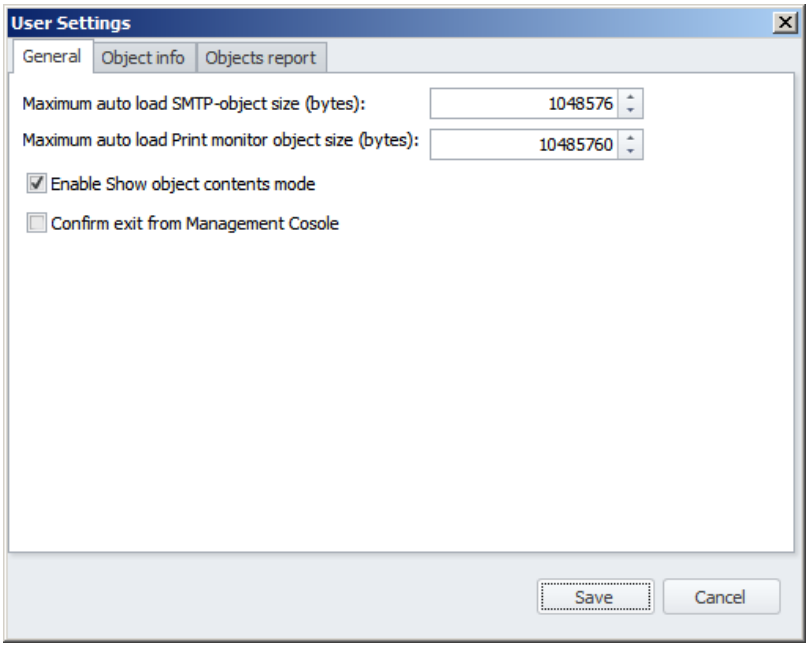
Every object intercepted by the system contains the content and the service data. The service data is defined as non-personal. The content of an object (text, attachments and some properties such as list of recipients, subject etc.) can include personal data. For lists of service attributes and content attributes see "General Object Attributes " and "Envelope Headers and Object Headers".

By default the content is not displayed even for users with permissions to view the content. To view the content you should use the corresponding menu item (**Edit> Object > Show Content**). If you need to view the content of all objects you can enable the content display mode. In this case the content will be shown when the corresponding object is selected.

To set up the content display mode:

1. In the main menu, select **Tools > User Settings**.

   The **User Settings** dialog box will appear on the screen.



Configuring content display mode

2. Take one of the following steps on **General** tab:
   - To disable showing object content by default, clear the **Enable Show object contents mode** checkbox.
   - Select the **Enable Show object contents mode** checkbox to show the object content without prior notification.

3. Click **Save**.

8.2.1.2 Setting the Size Limits for Downloaded SMTP Messages and Print Jobs

The size of the downloaded messages and print jobs is one of critical factors that impacts the query execution time. For this purpose there is an option to limit the size of the autodownloaded files in Management Console. If the size of e-mail or print job exceeds the specified limit, then the Management Console only downloads the results of the object analysis.

Note

SMTP messages and print jobs larger than the autodownload size can be downloaded manually (see "Viewing the General Object Information").

To set a limitation for autodownloading:

1. In the main menu, select **Tools > User Settings**.

   The **User Settings** dialog box will appear on the screen.

2. On the **General tab**:

   - in the **Maximum auto load SMTP-object size** field, specify the size of an e-mail in bytes (the default value is 1048576 bytes)
   - in the **Maximum auto load Print monitor object size** field, specify the size of PDF file from the print job, in bytes (the default value is 10 485 760 bytes)

3. Click **Save**.

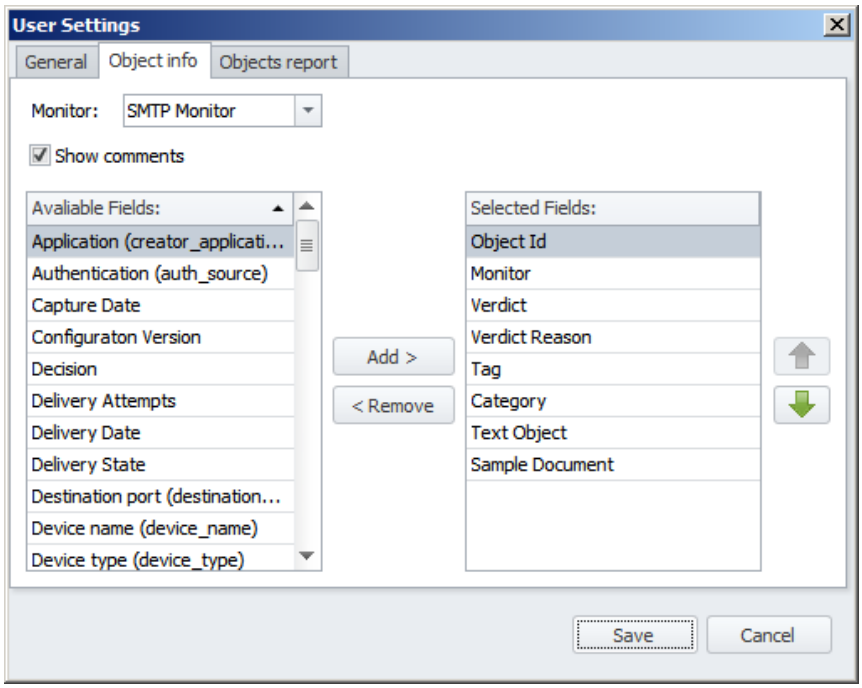
8.2.1.3 Configuring Object Info Pane

You can configure the fields displayed on the object information pane for the objects intercepted by different monitors. The same default fields will be displayed on the **General** tab of detailed object view.

To configure the fields in the Quick View:

1. In the main menu, select **Tools > User Settings**.

2. In the **User Settings** dialog box go to the **Object info** tab.



Configuring content display mode

3. Select the **Show comments** checkbox to display the last added description on the **Object Info** pane.

4. Select the required monitor type and set up a list of fields in the same way as when creating or editing queries on the **Available Fields** tab (see "Creating and Editing a Query").

5. Click **Save**.

8.2.1.4 Running Object Queries

Intercepted objects data is loaded to Management Console as a result of executing the query to the database. When working with queries, keep in mind has the following specifics:

- The duration of the query depends both on the number of objects being downloaded and on their size. By default the size of autoloaded messages in Management Console is limited to 1 Mb. If the size of a message exceeds the specified limit, the reading pane displays a notification. In this case you can download the object by clicking the notification.

  Note

  For more information about setting up the size of the automatically downloaded objects see "Setting the Size Limits for Downloaded SMTP Messages".

- The content of the object is displayed only for the users who have the right to view the content of the object. For the list of service attributes and content attributes see "General Object Attributes" and "Envelope Headers and Object Headers".
- If a query contains a condition to search for a certain file type, then the all objects with files of the specified type in attachments (including the attached archives) will be displayed.
- If the sorting settings are not specified in the query condition, then the objects are sorted by the Object ID (descending).
- Processing an object (for example, moving the object to another responsibility zone, see "Moving Object to Another Responsibility Zone", assigning a tag, see "Assigning Tags to an Object", changing colors, see " Highlighting Objects with Color", etc.), may cause the object not to match the query conditions any longer.

In this case, the object won't be removed from the query result at once; instead, the object will be still present in the query results until the query is run again.

To run a query:

1. Go to the **Queries** section.
2. On the query list pane, select the required query.
3. Do one of the following:
   - in the main menu, select **Edit > Run**;
   - click **Run** on the toolbox of query list pane;
   - double-click the selected query;
   - right click on selected query and choose **Run** in the appeared menu.

To get information about working with executed queries see "Query Manager"

Then the viewing area will display a list of records that meet the query conditions. For more information about viewing object info see "Viewing Object Info".

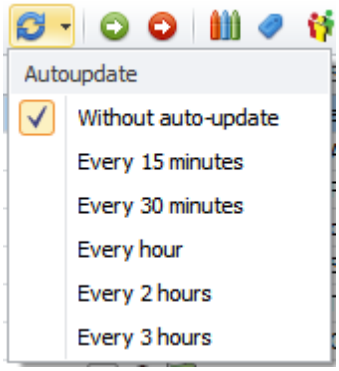
If you want query to run automatically through the specified periods, you can use **Autoupdate** function (see "Query Autoupdate").

8.2.1.5 Query Autoupdate

The autoupdate option makes the query automatically refresh its results through specified periods. If you have access to the query, you can enable the autoupdate for it (for more information about query management see " Creating and Editing a Query"). For more information about enabling the autoupdate during adding or editing the query, see "General Query Settings (General tab)"

To enable/disable the autoupdating or to change its period:

1. Go to the **Queries** section.
2. Click the required query.
3. Click the near the **Refresh** button to open the refresh period list.



4. Select the autoupdate period in the opened list. If you want stop the autoupdate, select **Without auto-update**.

Warning!

If you cancel the query with enabled autoupdate (see "Query Manager" to get information on the queries cancelling), its autoupdate would be stopped. Run the query to restart the autoupdating of this query.

8.2.1.6 Query Manager

Query Manager:

- displays the list of running queries (name, status, date of launch and update)
- allows to cancel or restart running the queries presented in list
- allows to go to queries results (see. "Viewing the Objects Information")

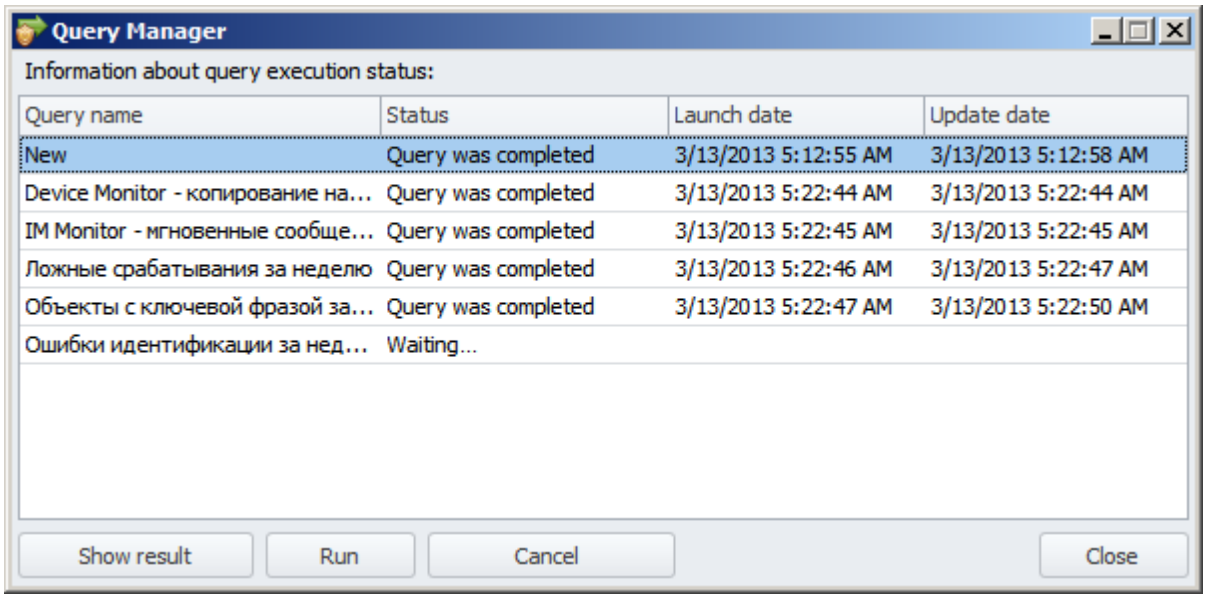
The Query Manager could be called from every section of the Management Console

To launch Query Manager,

do one of the following actions:

- in the main menu click **Tools > Query Manager**
- click the **Query Manager** link located at the status bar (bottom of Management Console window).

Query Manager dialog box will appeared at the screen.



Query Manager dialog box

To go to query result:

1. Select the carried-out query (with "*Query was completed*" status).
2. Click **Show result**.

As a result you will go to **Queries** section and the current query would be selected.

The Query Manager contains the list of all queries which were executed by user during the session of work in the Management Console. But the System can store results for up to five queries. All following queries receive the

status "*Waiting*" and form the waiting queue.

To execute the query with "*Waiting*" status:

1. Choose the executed query (with "*Query was completed*" status), which result you don't intend to look any more.
2. Click **Cancel**.

The executed query would be removed from the list, and the query with the "*Waiting*" status which was sent to performance before the rest, would start being executing.

Warning!

If you cancel the query for which autoupdate was enabled (see "General Query Settings (General tab)"), its automatic refresh would be stopped. Run the query to restart the autoupdate for that query (see "Running Object Queries", "Query Autoupdate").

8.2.1.7 Viewing Objects Information

The executing of a query (see "Running Object Queries") results in displaying a list of entries matching the query conditions. For the information about viewing the object data, see:

- Viewing the General Object Information
- Detailed View of an Object
- Configuring Search on Object Headers
- Viewing the Object Log

8.2.1.7.1 Viewing the General Object Information

When the query is fulfilled (see "Running Object Queries"), the list of objects found by the query is displayed in the viewing area. A set of general object attributes displayed in the viewing area, depends on the settings of the specific query (see "Selecting Fields to View"). Complete list of available attributes is listed in "General Object Attributes" and "Envelope Headers and Object Headers" sections. The details for some attributes are displayed as icons:

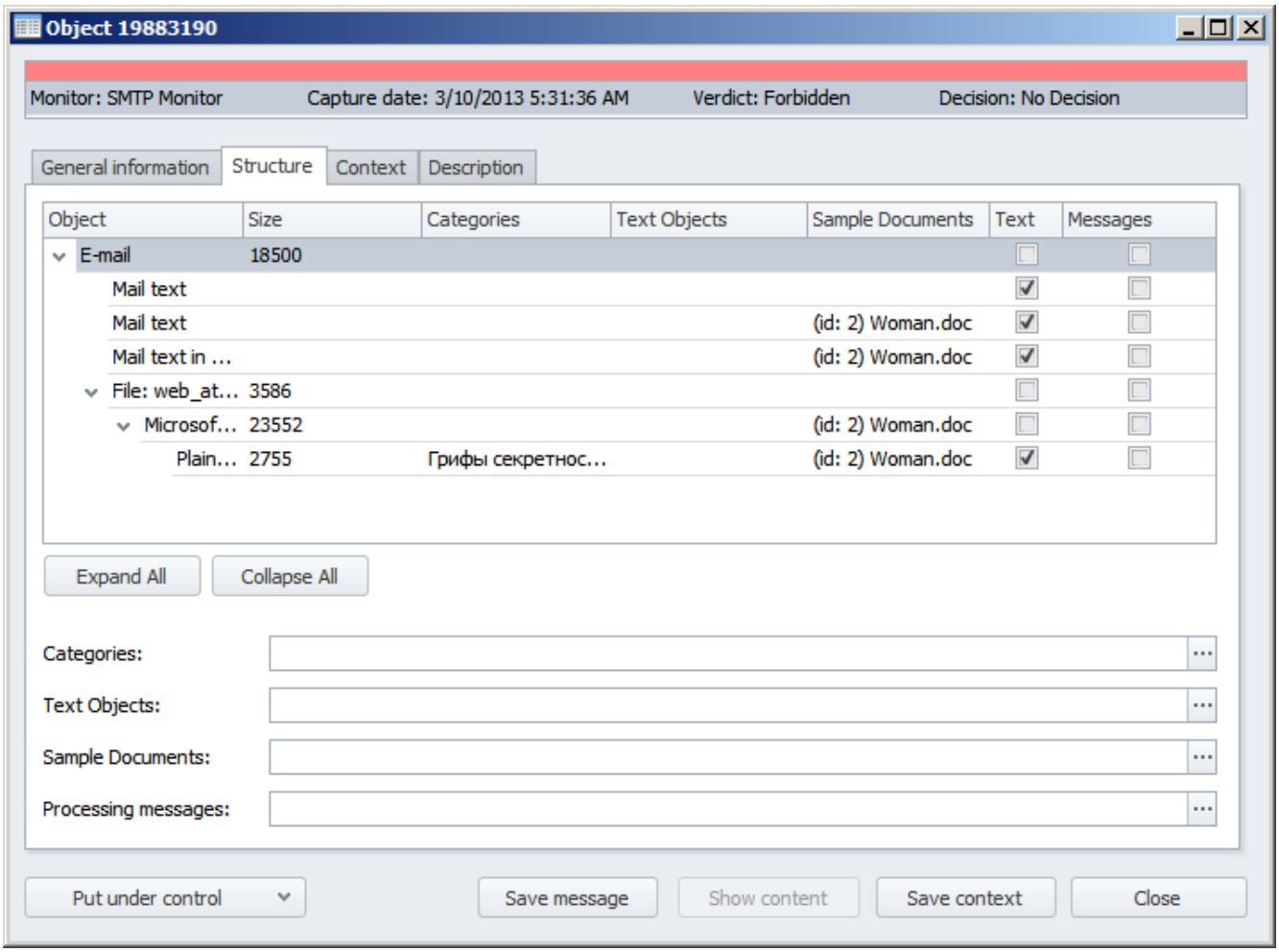
Icon	Attribute value
The *Monitor attribute*	
	SMTP Monitor
	HTTP Monitor
	ICQ Monitor
	Print Monitor
	Device Monitor
	DeviceLock Monitor
	Skype Monitor
	Crawler Monitor
	FTP Monitor

Icon	Attribute value
	Lotus Notes Monitor
	MMP Monitor
	XMPP Monitor
The *Verdict attribute*	
	Allowed
	Forbidden
The *Decision attribute*	
	No Decision
	No Violation
	Violation
The *Delivery State attribute*	
	Pending
	Delivered
	Failed
	Attempt Failed
	Locked
The *Transport Mode attribute*	
	Normal
	Transparent
	Copy
The *Object Errors attribute*	
	Yes
The *Attachments attribute*	
	Yes

Basic information on the specific object (including the text and the list of attachments) can be viewed on the Object Info pane.

To display the object information on the Object Info pane:

In the view pane, select a row of the specified object.



The *Sender*, *Workstation* and *Recipients List* attributes are displayed on the top of the Object Info pane.

Below is the list of the attribute values (ordered as described in "Configuring the Object Info pane".

If the notes are displayed (see "Configuring the Object Info pane"), then the last added note is also displayed.

If the the "Show Object Content" mode is disabled (see "Configuring the Object Content Preview Mode"), and you have the right to view the object content, you can view the content using one of the following ways:

- click **Show Content** on the Object Info pane;
- in the main menu, select **Edit> Object > Show Content**.

When the *Show Object Content* mode is on, the content of the SMTP objects won't be displayed if the size of such objects exceeds the autoloading limit (see "Setting the Size Limits for Downloaded SMTP Messages") or if the size of extracted text more than 32 Mb. If you select this object, a notification will appear. To view the text of an object, click this notification.

The content may be displayed in different ways for different types of objects .

- The attachments as well as following fields (if present) are displayed for the SMTP messages: *From*, *To*, *CC*, *Subject*, and *Sent*.
- For the ICQ messages this dialog box contains the table with the *From*, *To*, *Sent, and Message* columns. The number of messages displayed in the dialog box (the default value is 2) depends on the configuration file settings (see *"InfoWatch Traffic Monitor. Administration Guide*": `tm.conf` file configuration description, `[PROXY_ICQ]` section, `MessageWindow` setting).
- For Skype messages, GTalk messages or Mail.Ru Agent the following properties are displayed: *From*, *Sent* and *Message*. Attachments are displayed for messages with files.

- The shadow copies of files are displayed for the Device Monitor, FTP Monitor and DeviceLock objects.
- For Print Monitor objects pdf files and copies for the print jobs are displayed. Also System displays the text from the print jobs extracted with Device Monitor or OCR-Extractors.
- For POST requests to some websites (see the table below) the system has pre-defined rules of matching between the POST request variables and the general object attributes. For these requests the following information is displayed (if present): attachments and the following fields: *From*, *To*, *CC*, *Subject*, and *Sent*. Only attachments (if any) are displayed for the rest of HTTP requests.

Note

If the structure of the HTTP query involves transmission of any data in the query headers, then this data be may not found using the text search even if displayed on the Object Info pane.

When working with the text of an object you can use the context menu with the standard set of Internet Explorer commands.

Note

If text of the message is displayed in the wrong encoding, then right-click the text of the object. Choose **Encoding** from the popup menu. Then specify the required encoding or select **Auto select**.

To view an attachment of the object:

1. In the view pane, select the row containing the information on the required object.
2. Select the required attachment on the **Object Info** pane
3. Do one of the following:
   - Right-click the selected attachment and choose **Open**;
   - Double-click the selected file.

The attachment will be opened using the application associated with the file type of this attachment.

8.2.1.7.2 Detailed View of an Object

The detailed view displays the detailed information about the service data of the object and the content of the object. The content of the object is a private information (text, attachments, some properties such as the list of recipients, subject, etc.). Therefore, the content viewing mode is turned off by default and only the service information is displayed for the object.

Note

For the list of service attributes and content attributes see "General Object Attributes" and "Envelope Headers and Object Headers".

To display the content for all objects by default, you should enable the content viewing mode (see " Configuration of Object Content Preview Mode").

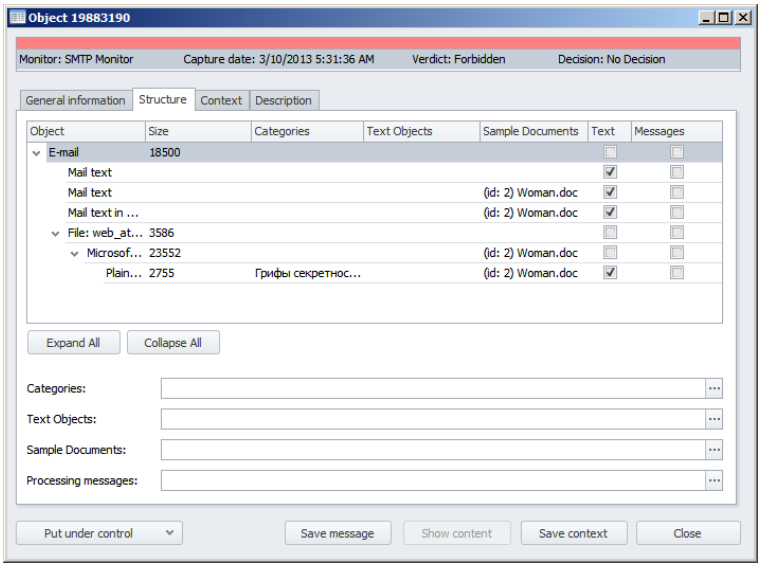
To open the detailed view of an object:

1. In the view pane, select a row with the required object.
2. Do one of the following:
   - double-click the selected row;

- click **Show Detailed View**;
- in the main menu, select **Edit > Object > Show Detailed View**;
- click **Show Detailed View** button on the Object Info pane.

If the object identifier (ID) is known, you can open its detailed view without query. Just enter the identifier to the field at the top of Navigation pane and click . If the object with this ID does not exist or does not belong to your responsibility zone (see. "Resposibility Zones"), the message "*Object not found*" will be displayed.

The **Object <Object ID>** dialog box will appear on the screen.



Viewing object attributes

The top part of the detailed view contains the general information about the object: monitor, date and time of interception, verdict and the decision on the object. There is also a band with a color assigned to the object.

The detailed view has four tabs:

- **General**. Information on general object attributes. The **Sender**, **Sender Workstation** and **Recipients** properties are displayed, as well as the information pane fields (see "Configuring the Object Info pane").
- **Structure**. Information about the object content and the results of the analysis. In the main area the object content is displayed in a tree structure; the nodes of the tree may vary depending on the object type.

  The following properties are displayed for each item of the tree structure:

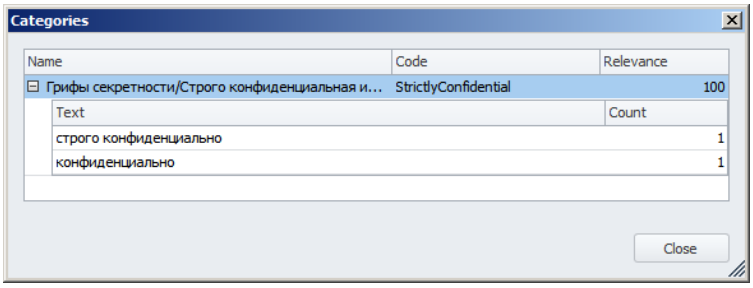
  - **Size** – the size of the item (in bytes). Indicated only for the root nodes and files;
  - **Categories**, **Text Objects**, **Sample Documents** – results of the content analysis;
  - **Text** – this field is checked if text was is extracted from the element;
  - **Messages** – this field is checked if there are messages resulting from processing the element.

  The fields with the information about the results of the context analysis are displayed under the tree structure:

  Note

  If you view an object in the Hide Content mode, then these fields will display the information for the entire object. If you view an object in the Show Content mode, then these fields will display the information only for the selected row in the tree.

- **Categories –** assigned categories, comma-separated. For more information click ⋯. A dialog box will appear that lists the assigned categories with their codes and relevance (degree of conformity of the text of the object to this category).



Viewing the assigned categories

To view the detected terms, click ⊞ to the right of the category name.

Note

You can view the terms only in the content display mode.

- **Text objects** – the found text objects are listed, separated by commas. For more information click ⋯. A dialog box will appear that lists the found text objects with their descriptions and quantity.
- **Sample documents** – the found sample documents are listed, separated by commas. For more information click ⋯. A dialog box will appear that lists the found sample documents with their ID, name, file name and relevance (degree of conformity of the text of the object to this sample document).
- **Processing messages –** the first informational message is displayed for the given object. For more information click ⋯. A dialog box will appear with all the messages that have been generated while processing the object. For every message the following details are provided: level, originating module and text.
- **Extracted text –** the text that was extracted from the object is displayed.

- **Context**. Details about the data received after the object analysis and processing. Represented as a tree of the XML context.

Note

The representation of context is based on the model of InfoWatch Traffic Monitor types (see "Data Types").

When working with the context, you can filtering the elements based on the attributes and the values.

- **Description**. Additional information about the object. Contains the history of all notes added to the object. To add new comment, enter the required text in the **Add Comment** field and click **Add**.

On all the tabs of the detailed view form you can perform a number of common actions:

Action	**Procedure**
Expand/collapse data	Click **Expand All** / **Collapse All**
Download the SMTP message in the EML format	Click **Save Message.**

Action	Procedure
Display the contents of the object (if you have the rights to view it)	Click **Show Content**
Download the XML context of an object to a file	Click **Save Context**

The information on the **General**, **Structure** and **Context** tabs depends on the status of the Show Object Content mode (see table below). For more information about restrictions on showing the content see "Controlling the Access to the Objects Content".

Displaying the object content	The General tab	The Context tab
Displaying of the object content is allowed	All viewable fields are displayed	The context representation fully complies with the InfoWatch Traffic Monitor type model.
Displaying of the content is disabled	Only the fields with service data are displayed	The context tree is displayed with changes: • the *envelope* branch contains only service data; • the *object* branch is not displayed. The service data from this branch are displayed in the *Processing* branch

8.2.1.7.3 Configuring Search for Object Headers

When creating queries ("Configuring Query Conditions") and reports ("Creating and Editing a Report"), the query builder is used. The query builder allows to perform search in the headers of envelopes and objects. The following object headers are used in the query builder by default:

- `From`
- `To`
- `Cc`
- `Date`
- `Subject`
- `Importance`
- `Priority`
- `X-Forwarded-For`

In the detailed view, you can add the headers extracted by the system from the object into the list of available to use in the query builder.

To change the list of object headers for use in the query builder:

1. Open the detailed view of the specified object (see "Detailed View of an Object").
2. On the **Context** tab expand the `root > object > headers node`.

   All headers that are available for use in the query builder, are marked with .

3. Right-click the required header and choose:
   - To make the header available for use in the query builder, select **Enable search on the header with Query Builder**.
   - To remove the header from the query builder, select the **Disable search on the header with Query Builder**.

8.2.1.7.4 Viewing the Object Log

The object log contains the information related to processing of the object by Traffic Monitor Server (specifically, the error reports are displayed).

To open the object log:

1. In the view pane, select a row with the required object.
2. Do one of the following:
   - in the main menu, select **Edit > Object > Object System Log**;
   - click **Object System Log** on the toolbar.

The **Object System Log** dialog box will appear. This window displays the messages generated while processing the object. The following information is displayed for each message:

- **Date and Time**. Date and time of the system message.
- **Severity**. The message severity level. These message types are information (*info*), warning messages (*warning*) and error messages (*error*).
- **Module**. The module that has generated the message.
- **Content**. Message text.

8.2.1.8 Processing the Sender, Recipient, and Workstation Data

During the analysis, the system extracts the information about the sender, the sending workstation and the list of recipients. Then, the system searches for matching between the attribute value (*Sender*, *Recipients* and *Workstation*) and the Active Directory records: persons directory (see "Persons Directory") or workstations directory (see "Workstations Directory").

Matching between attribute values and records from directories may lead to the following situations:

- no matching records found;
- one matching record found;
- several matching records found.

If one attribute value matches several records, this counts as an **identification error** (a conflict). Specifics of identification error event:

- Event is marked with orange color by default.
- By default, the event get "Forbidden" verdict and "Identification error" verdict reason.
- The value of this attribute is highlighted red on the Object Info pane.
- Click the attribute to display the dropdown list of records corresponding to this value appears. Select the

desired record from the list to open a window for editing it.

Important!

It is recommended to process the objects with the identification errors first.

To view the list of the objects with identification errors, you should create a query with a condition of the *Identification error* attribute (for more details see "Configuring Query Conditions ").

Important!

It's possible to always get the identification error for the objects intercepted from the same IP-address. This may be due to the fact that one IP-address corresponds to several computer names in DNS. To avoid such situations, the network administrator should set up the DNS configuration so that every one IP-address would be assigned to one workstation.

If the system has matched compared the information about the recipient/sender/workstation of an object with a directory record, then the name and last name of a person or the name of the workstation will be displayed as the attribute value on the Object Info pane. In this case you can edit and view the correspondent directory record or you can add a person or a workstation to the Traffic Monitor group.

Note

Prior to adding a person or a workstation to a group please make sure that the required TM group has already been created (see "Creating, Viewing, and Editing a Group") and uploaded to the host (see "Uploading Directories to the Host").

To open a directory record,

do one of the following:

- double-click the attribute value;
- right-click the attribute value, and choose **Open**.

Note

For more information about editing person records see "Creating and Editing a Person Record". For more information about editing workstation records see "Creating, Viewing, and Editing a Group".

To add a person or a workstation to the TM group:

1. Right-click the attribute value.
2. Choose **Add to group** in the the context menu.
3. In the **Group selection** dialog box, check the TM Group to add the person or the workstation.
4. Click **Save**.

If no matches were found between the existing records and the information about the sender or the recipient, then the value of the *Sender* or *Recipient* attribute will be displayed on the Object Info pane in the form of the e-mail address, ICQ number, Skype ID or phone number. In this case, you can add this value as a contact to one of the existing persons or create a new person entry with this contact directly from the Object Info pane.

To add the attribute value as contact to one of the existing persons

1. Right-click the attribute value.
2. Select **Add contact to person** from the context menu.
3. In the **Select necessary Persons** dialog box, check the required person record and click **OK**.

The **Editing User** window will appear with the **Creating Contact** dialog box opened.

4. Specify the information about the contact:
   - In the **Contact Type** dropdown list select the required type (**E-mail**, **ICQ**, **Skype**, or **Phone**).
   - Specify any additional information about the added contact in the **Note** field.

   Then click **OK**.

5. If needed, you can modify the person record (For more information about editing person records see " Creating and Editing a Person Record"). Then click **Save**.

To create a new person record with the contact from an object:

1. Right-click the attribute value.
2. Choose **Create person with contact**.

   The **Creating User** window will appear with the **Creating Contact** dialog box opened.
3. Specify the information about the contact:
   - In the **Contact Type** dropdown list select the required type (**E-mail**, **ICQ**, **Skype**, or **Phone**).
   - Specify any additional information about the added contact in the **Note** field.

   Then click **OK**.
4. Provide other information according to the section "Creating and Editing a Person Record". Then click **Save**.

8.2.1.9 Making the Decision about an Object

Each object that was analyzed by the System is assigned specified values for the following attributes: *Transport Mode*, *Verdict* and *Delivery State*. When analyzing an object in the Management Console you can make your own decision (*User Decision*). The user decision does not affect the verdict.

In all transport modes, except for the general mode, the user decision does not affect the object delivery. That is why the *Delivery State* attribute keeps its original value. However if traffic filtering is on (the normal transport mode is set), then in some cases the user decision can change the delivery status of the object.

Example 1

The SMTP e-mail is approved for delivery but it has not yet been sent to the recipient. After being analyzed in Management Console, the e-mail is qualified as violating the corporate security policy. You can block this e-mail. To do that, please change the user decision on this e-mail to *Violation*.

Example 2

The SMTP e-mail is violates the corporate security policy. However, the additional analysis in Management Console has shown that the e-mail does not contain any violation and can be delivered to recipients. In this case you should change the user decision on the e-mail to *No Violation*.

The possible user decisions that also result in changing the delivery status are listed in the following table. In all other cases the user decision does not affect the delivery status.

Initial delivery status	User Decision	New delivery status	Operation is available for objects
Failed	Violation	Locked	SMTP
Pending	Violation	Locked	SMTP, HTTP
Delivery Attempt Failed	Violation	Locked	SMTP
Locked	No Violation	Pending	SMTP

The information on the user decision is displayed when viewing the object (see "Viewing the Objects Information") in the **Decision** field. By default each object is assigned the *No Decision* value. The value is represented by the icon .

To make a user decision on an object:

1. Go to the **Queries** section.
2. On the query list pane, select a query and double-click it.
3. In the view pane, select one or more rows with the required objects.
4. Do the following:

Necessary step	Procedure
Assign the *No Violation* decision to the object	Do one of the following: • in the main menu, select **Edit > Object > No Violation** • click  **No Violation** on the toolbar • right-click the object row and choose  **No Violation**
Assign the *Violation* decision to the object	Do one of the following: • in the main menu, select **Edit > Object > Violation** • click  **Violation** on the toolbar • right-click the object row and choose  **Violation**

8.2.1.10 Putting under Control

You can use the **Putting under control** function at investigation of incidents. The result of applying this function to the necessary object and defining additional attributes, is the auto-created query which helps you to control:

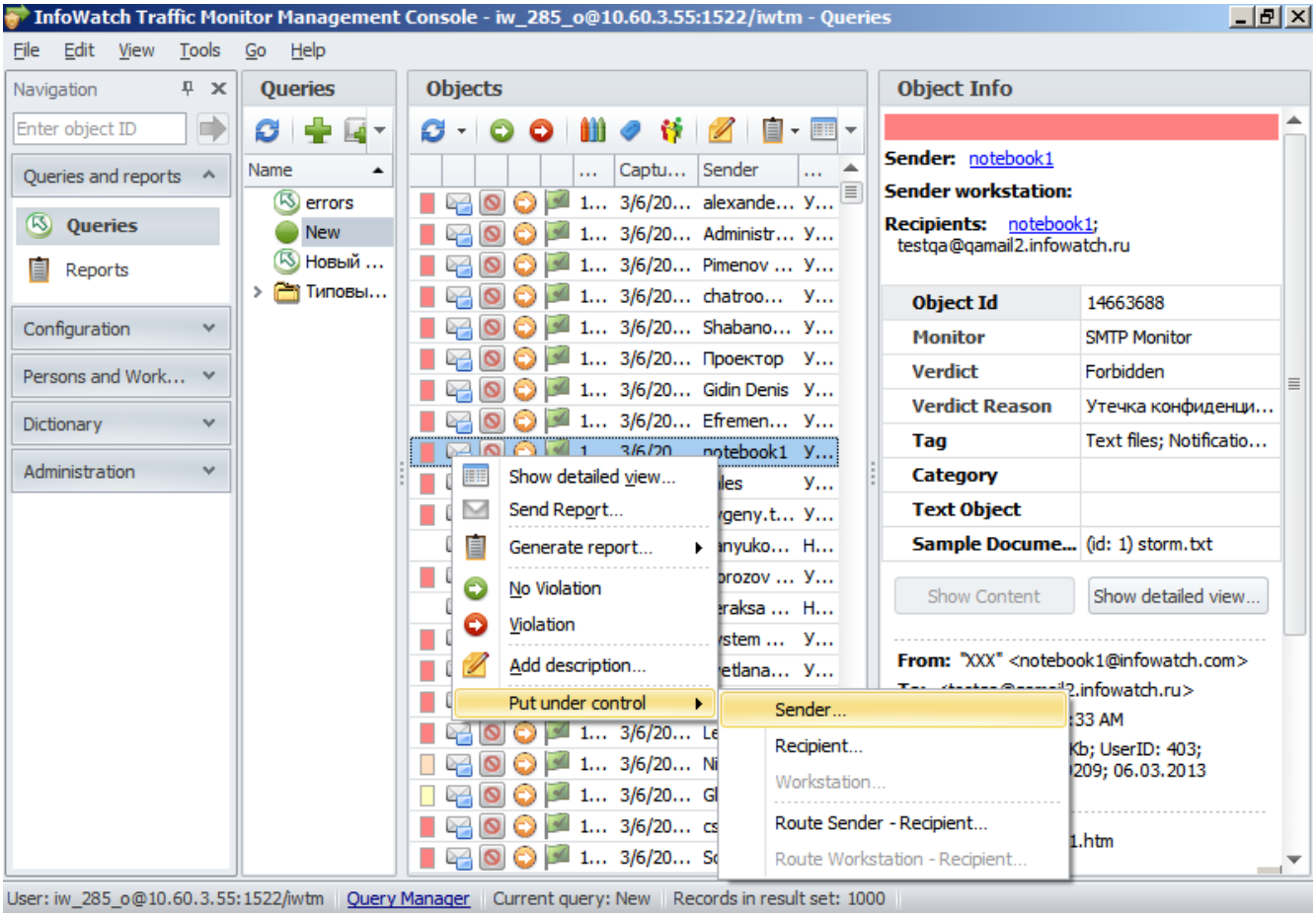
- **Sender** - data on all objects sent by the sender of selected object;
- **Recipient** - data on all objects received by the sender of selected object;
- **Workstation** - data on all objects sent from the same workstation, as the selected object;

- **Route Sender - Recipient** - data on all objects sent by the sender and the recipient of selected object to each other;
- **Route Workstation - Recipient** - data on all objects which were sent between the workstation and recipients of selected object.

So, you can supervise possible channels of leak by analyzing the data presented in a convenient type.

Object controlling includes the following steps:

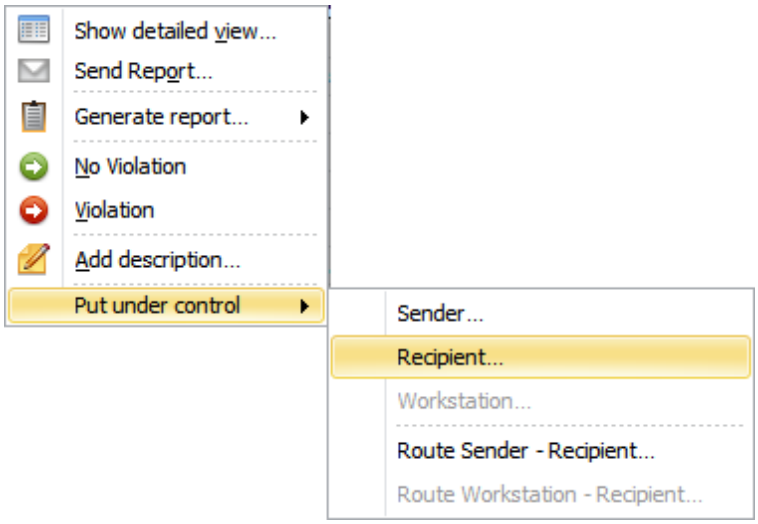
1. Security officer puts object under control.
2. The System creates new query according to the chosen attributes.
3. Security officer works with the created query: executes, changes parameters, updates, etc.



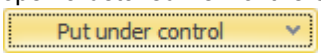
Putting under control

To put the object under control:

1. Go to the **Queries** section and execute the required query (for example, double click on it with the left button of a mouse).
2. Select one or more objects.
3. Do one of the following:
   - in the main menu choose **Edit > Object > Put under control**;
   - click **Put under control** button located at a toolbar;
   - in the view pane, in a context menu for the selected objects, choose **Put under control**;



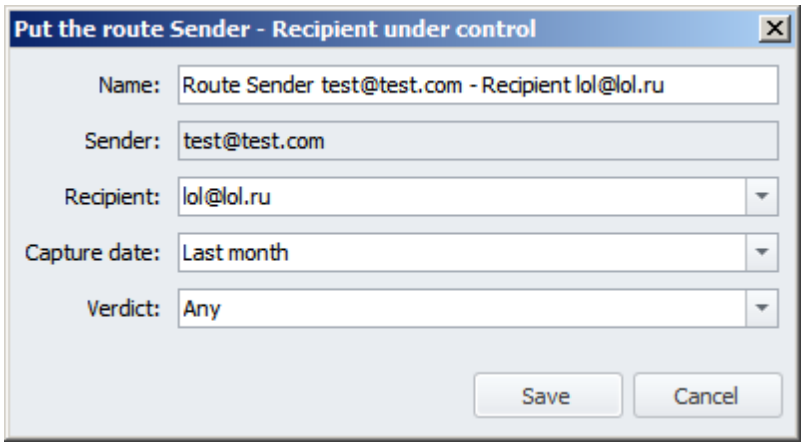
Putting under control using context menu

- open a detailed view of the object (see. "Detailed View of an Object") and click 

Put under control button in the left bottom corner of a window.

4. Select the required attribute in the appeared list.
5. You can set additional query parameters in the opened dialog box. For example, if the object has several recipients, you can choose one of the recipients in the drop-down list. You can also set values of the "*Capture date*" (by default the query displays objects for the last month) and "*Verdict*" parameters.

> **Note**
>
> Value of attribute can be highlighted with red color if there is an identification error (see "Processing the Sender, Recipient, and Workstation Data").



Put the route Sender - Recipient under control

6. Click **Save**.

You will go to the "*Under control*" folder and the query generated by the System would be checked.

The created query would:

- have the query conditions corresponding to chosen attributes;
- be available only to the user who put it under control;
- not be executed;
- automatic updating of query is disabled by default. You execute the query manually (see. "Running Object

Queries") or set its autoupdate (see "Query Autoupdate" and "General Query Settings (General tab)").

8.2.2 Moving Object to Another Responsibility Zone

An object within a specific responsibility zone can be viewed by all users belonging to this responsibility zone. In the meantime, an object may contain information that is not intended to be viewed by the users of this responsibility zone. In this case you can move this object to another responsibility zone.

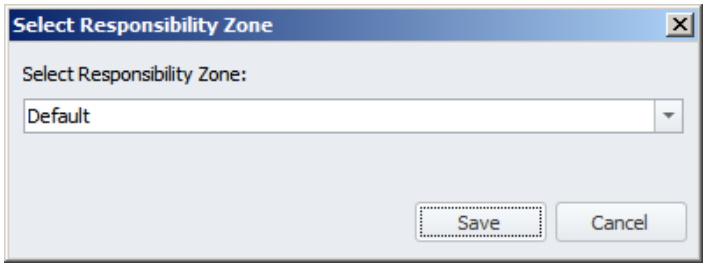
Important!

You can only move an object to the responsibility zones that are specified as possible transitions for the current responsibility zone.

To move an object to another responsibility zone:

1. Go to the **Queries** section.
2. On the query list pane, select a query and double-click it.
3. In the view pane, select one or more rows with the required objects.
4. Do one of the following:
   - in the main menu, select **Edit > Object > Change Responsibility Zone**;
   - click **Change Responsibility Zone** on the toolbar.

   The **Select Responsibility Zone** dialog box will appear on the screen.



Changing responsibility zone for an object

5. Select the required responsibility zone from the drop-down list.
6. Click **Save**.

   Then the selected object will be excluded from the current responsibility zone and will be moved to the selected responsibility zone.

8.2.3 Sending an Object Report

If you need to draw the attention of other system users to any objects, you can send them a report: an e-mail with the numbers of the selected objects and the accompanying message (report text). To allow a user to send the report to another user:

- The e-mail address should be specified in the recipient account;
- The recipient should be selected as the report recipient in the sender's account.

For more information about configuring these user account options see "Creating and Editing a User Account".

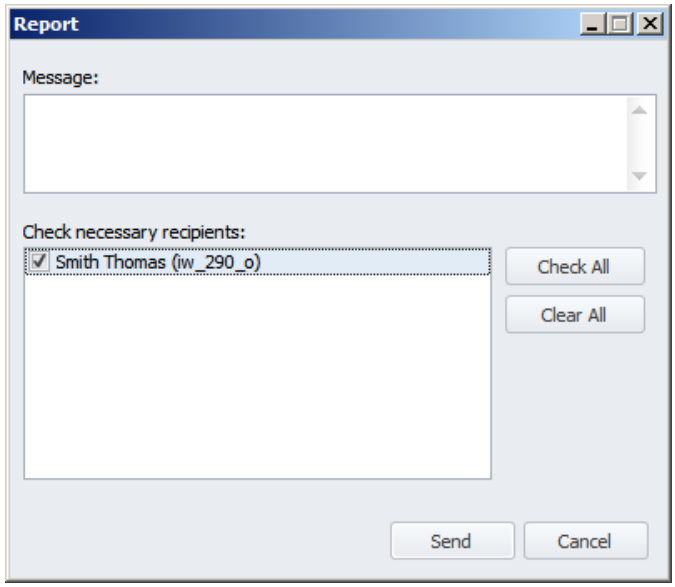
Important!

You must change the settings of the operating system on the computer that will be used for sending reports. To do that, open the **Control Panel** (**Start** > **Settings** > **Control Panel**). Select **Regional and Language Options**. In the dialog box that appears, go to the **Advanced** tab and select the language of reports for non-Unicode software.

To send a report on an object:

1. Go to the **Queries** section.
2. On the query list pane, select a query and double-click it.
3. In the view pane, select one or more rows with the required objects.
4. Do one of the following:
   - in the main menu, select **Edit > Object > Send Report**;
   - click **Send Report** on the toolbar;
   - right-click the object row and choose **Send Report**.

   The **Report** dialog box will appear on the screen.



Sending an object report

5. Type the report text in the **Message** field, .
6. Check all recipients of the report. To select or clear all the check boxes, use the **Check All and** Clear All **buttons**.
7. Click **Send**.

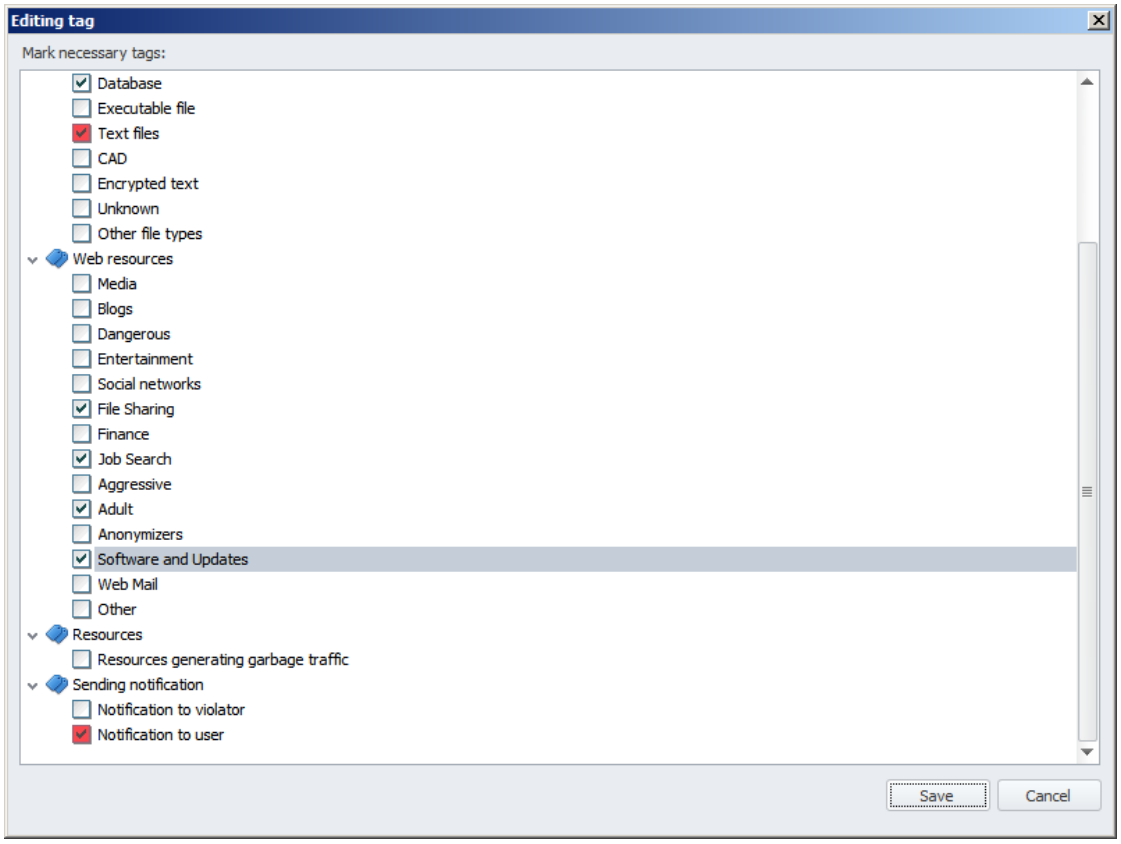
8.2.4 Assigning Tags to an Object

The tags are text markers with a brief description of an object. For example, if a configuration has a MUSIC tag, it is possible to assign the same tag to an audio file with recorded music.

To assign a tag to an object:

1. Go to the **Queries** section.
2. On the query list pane, select a query and double-click it.
3. In the view pane, select one or more rows with the required objects.
4. Do one of the following:
   - in the main menu, select **Edit > Object > Tags**;
   - click **Tags** on the toolbar.

   The **Select Tags** dialog box will appear on the screen.



Configuring tags for an object

5. Check all the tags that should be assigned to an object.

   If you want to remove a tag, clear its checkbox.

> **Note**
>
> All the tags that have been assigned to an object following the content analysis are highlighted in red and cannot be unassigned.

6. Click **Save**.

Important!

The database in InfoWatch Traffic Monitor Standard is periodically cleaned to free up more space: if the remaining free space is less then required for the new objects, then the old objects are deleted.

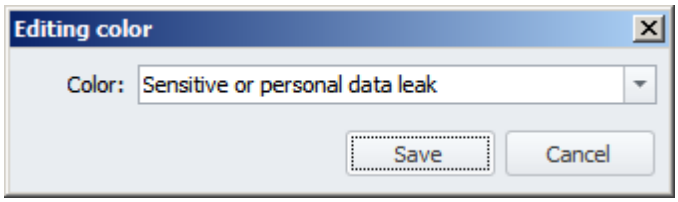
If you want to protect an object from the deletion, use the "*Prevent Deletion*" tag (tag code is `_DELETE_PROTECT_TAG_`)

8.2.5 Highlighting Objects with Color

To highlight an object with color or to cancel the highlighting:

1. Go to the **Queries** section.
2. On the query list pane, select a query and double-click it.
3. In the view pane, select one or more rows with the required objects.
4. Do one of the following:
   - in the main menu, select **Edit > Object > Select Color**;
   - click **Select Color** on the toolbar.

   A dialog box will appear on the screen.



Selecting a color to highlight an object

5. In the drop-down list, select a color to highlight the object.
6. Click **Save**.

The object will be highlighted with the selected color. To cancel the highlighting, repeat the steps from 2 to 5. In a dialog box that appears, click **Clear**, and then click **Save**.

8.2.6 Adding a Comment to an Object

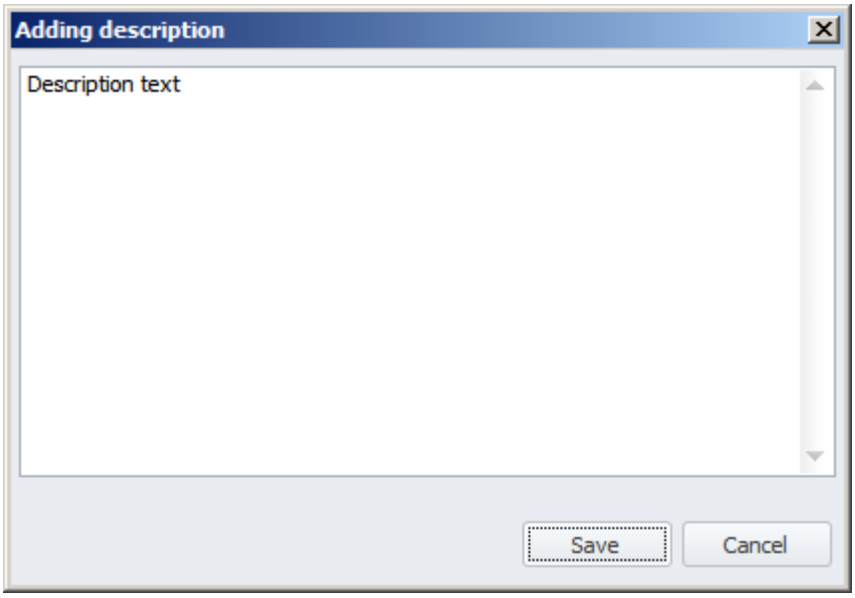
You can add comments when analyzing an object. The notes are displayed in the reading pane when you select an object (in the the *Comment* section).

To add a comment for an object:

1. Go to the **Queries** section.
2. On the **Query List** pane, select a query and double-click it.

3. In the view pane, select one or more rows with the required objects.
4. Do one of the following:
   - in the main menu, select **Edit > Object > Add Description**;
   - click **Add Description** on the toolbar;
   - right-click the object row and choose **Add Description**.

   A dialog box will appear on the screen.



Adding a description to an object

5. Type the dscription.
6. Click **Save**.

8.2.7 Downloading Attachments, Messages, and XML Context

The information from, the intercepted and processed objects can be downloaded from the system and saved using one of the following ways:

- Downloading the Attachments of an Object
- Downloading SMTP Messages
- Downloading Context

8.2.7.1 Downloading the Attachments of an Object

Important!

To view the attachments, you must have the software associated with the attachment formats installed on your

computer.

To download an attachment by copying or saving:

1. Go to the **Queries** section.
2. On the **Query List** pane, select a query and double-click it.
3. In the view pane, select a row containing the information on the specified object.
4. Select the required attachment on the Object Info pane
5. Right-click the selected attachment and choose:
   - To copy the attachment to the Windows clipboard, choose **Copy**. Then paste the attachment to the required folder.
   - To save the attachment, select **Save**. Then in the **Browse Folder** dialog box, select the folder to save the attachment.
6. Click **OK**.

8.2.7.2 Downloading SMTP Messages

If the object content view is on (see "Configuration of Object Content Preview Mode" and "Viewing the Objects Information"), then you can upload the SMTP messages using the EML files.

To download an SMTP message to a file:

1. Go to the **Queries** section.
2. On the **Query List** pane, select a query and double-click it.
3. In the view pane, select a row with the required SMTP message.
4. Do one of the following:
   - in the main menu, select **Edit > Object > Save Message**;
   - click **Save Message** on the toolbar.
5. In the dialog box that appears, enter the name and the location of the file. Then click **Save**.

8.2.7.3 Downloading XML Context

You can save the XML contexts of the processed objects (one or more) to files.

Important!

The content of the uploaded XML context will depend on whether or not the object content is displayed in Management Console at the time of uploading (for more details see "Viewing the Objects Information").

To upload the XML context of the objects:

1. Go to the **Queries** section.
2. On the **Query List** pane, select a query and double-click it.
3. In the view pane, select rows with the required objects.
4. Do one of the following:
   - in the main menu, select **Edit > Object > Save Context**;
   - click  **Save Context** on the toolbar.
5. In the dialog box that appears, select the location to save the downloaded files. Then click **Save**.

You can also upload the XML context of the object from the detailed view. Click **Save Context** in the detailed form.

8.3 Generating Object Reports

Using object reports, you can have a visual representation of the statistics about the intercepted and processed data.

To work with queries, use the **Reports** section (the **Monitoring** area on the **Navigation** pane).

Since the reports are designed to work with large amounts of data, the sampling of data may take a long time. The current status of the report is displayed in the main window in the **Status** column. For the description of the report statuses see the following table.

Report status	Status description
Pending for update	Is assigned to a new report
Is updating	The sampling in the database is made
Ready	The sampling is successfully complete
Error	An error occurred while sampling

The report can be run if it has the *Ready* status.

After running the report, only the data of the current view will be displayed. To display the updated data, you must refresh the view from time to time (see "Rebuilding the Report").

Important!

Only the users who have the right to generate the reports also have the right to rebuild the reports.

You can group reports by folders for more convenience (see "Managing the Queries and Reports Folders").

For more details about generating object reports see the following sections:

- Report Types
- Creating and Editing a Report
- Recreating report
- Viewing report results
- Printing Report
- Exporting a Report
- Copying a Report
- Deleting a Report

8.3.1 Report Types

All the reports are based upon the common report types. When creating a report, you can adjust the dataset for the report by specifying additional conditions: see: "Creating and Editing a Report".

For the description of the report types see the following table.

Report type	Description	Results grouping attribute	Configuring the Settings pane	Diagram type
Categories – most popular	The report shows which categories are most often found in the intercepted traffic. Contains the absolute value and the percentage.	Categories	**Number of displayed records** **Sorting the report results** (number of objects for the given category)	Bar chart
Categories – detection frequency	The report shows how often the objects corresponding to the selected categories are found in the intercepted traffic. Contains the absolute value and the percentage.	Categories	**sorting the report results** (number of objects for the given category) **Select the categories to get more details**	Bar chart
Content routes by monitors	**Content Route** is an established chain of communication, a pair consisting of a Sender and a Recipient. The chain of communication is considered established if for the given pair (a Sender and a Recipient) the system has intercepted more than **L** objects, where **L** is the attribute of an **established chain of communication.** The report shows the amount	Monitor	**Content route parameter** (established chain of communication)	Pie chart

Report type	Description	Results grouping attribute	Configuring the Settings pane	Diagram type
	(numbers and percentage) of the identified content routes for each monitor.			
Content routes – most popular	**Content route** is an established chain of communication, a pair consisting of a Sender and a Recipient. The chain of communication is considered established if for the given pair (a Sender and a Recipient) the system has intercepted more than L objects, where L **is the attribute of an established chain of communication.** The report displays the most common content routes.	the Sender and Recipient pair	**Number of displayed entries** **Content route parameter** (established chain of communication) **sorting the report results** (number of objects sent by the same route)	Bar chart
Senders – web-resources usage	Senders with the maximum number of objects intercepted by HTTP monitor. The number of requests (absolute and percentage) sent to the site of each category. The website category is determined by the presence of the corresponding tags from the preset *Website Categories* tag group. For each category, the addresses of the relevant sites are determined using the preset *Web Resources* list group.	Sender	**Number of displayed entries** **sorting the report results** (number of objects for the given sender)	Bar chart
Senders: types of files being sent	Senders with the maximum number of file sending events. The number each type of objects (absolute and percentage) is displayed for each sender. The type of the object is determined by the presence of the corresponding tag from the preset *Files types tag group*	Sender	**Number of displayed entries** **sorting the report results** (number of objects for the given sender)	Bar chart
Senders: most active	Senders with the maximum number of sent objects intercepted, and the number of intercepted objects (absolute and percentage)	Sender	**Number of displayed entries** **sorting the report results** (number of objects for the given sender)	Bar chart

Report type	Description	Results grouping attribute	Configuring the Settings pane	Diagram type
Recipients – the most popular	E-mail addresses to which the maximum number of intercepted objects was sent. The number of intercepted objects is specified for each recipient (absolute and percentage)	Recipient	**Number of displayed entries** **sorting the report results** (number of objects for the given recipient)	Bar chart
Workstations - the most popular	Workstations to which the maximum number of intercepted objects was sent. The number of intercepted objects is specified for each workstation (absolute and percentage)	Workstations	**Number of displayed entries** **sorting the report results** (number of objects for the given recipient)	Bar chart
Statistics – user activity	Trends in the intercepted objects statistics for the given period, with detailed verdicts: • **Number** – the total number of intercepted objects; • **Forbidden** – the *Forbidden* verdict • **Allowed** – the *Allowed* verdict	Date of the object interception (details of the selected interval: year, month, week…)	**Interval** (year, month, week…) Details: • **View all** • **View Allowed** • **View Forbidden**	Linear chart
Statistics – false detections	Number (absolute and percentage) of objects, grouped by the following types of user decisions: • **Verdict has not been analyzed**: no user decision made; • **Verdict approved by the user**: user has made a decision and it corresponds to the verdict of the system; • **False positive verdict**: Verdict: *Forbidden*, user decision: *No Violation*; • **False negative verdict**: Verdict: *Allowed*, user decision: *Violation*.	User decision	-	Pie chart
Statistics – categories found	Number of objects (absolute and percentage) found in any category.	Categories	**View the percentage value**	Pie chart
Statistics – sample documents found	Number of objects (absolute and percentage) with any text objects were found	Sample documents	**View the percentage value**	Pie chart

Report type	Description	Results grouping attribute	Configuring the Settings pane	Diagram type
Statistics – text objects found	Number of objects (absolute and percentage) with any sample documents were found.	Text object types	**View the percentage value**	Pie chart
Statistics – objects processing	Number (absolute and percentage) of objects, grouped by user decisions: • **Not Processed**: no user decision; • **Processed**: user decision was made.	User decision	-	Pie chart
Statistics – objects by verdicts	Number (absolute and percentage) of objects intercepted by the verdicts.	Verdict	**View the percentage value**	Pie chart
Statistics – objects by monitors	Number (absolute and percentage) of objects intercepted by the monitors.	Monitor	**View the percentage value**	Pie chart
Tags – detection frequency	The report shows the number of the intercepted objects with each tag from the selected tag group. Contains data in absolute value and as a percentage	The tags of the selected tags group	**Sorting the reports results** (number of objects with this tag from the selected group tag) **Select the tag groups for more details**	Bar chart
Text objects – most popular	The types of text objects to which the maximum amount of object in the intercepted traffic were assigned. The amount of the intercepted objects is specified for each type of text objects (number and percentage)	Text object types	**Number of displayed entries** **Sorting the report results** (number of objects for the given text object type)	Bar chart
Text objects – detection frequency	The amount of objects (number and percentage) where the selected text objects were found.	Text object types	**Sorting the report results** (number of objects for the given text object type) **Select the text objects for more details**	Bar chart
Sample documents – most popular	The sample documents with the maximum amount of objects in the intercepted traffic. The number of intercepted objects is specified for each sample	Sample documents	**Number of displayed entries** **Sorting the report results** (number of objects for the	Bar chart

Report type	Description	Results grouping attribute	Configuring the Settings pane	Diagram type
	document (absolute and percentage)		given sample document)	
Sample documents – detection frequency	The number of objects (absolute and percentage) where the selected sample documents were found.	Sample documents	**Sorting the report results** (number of objects for the given sample document) **Select the sample documents for more details**	Bar chart

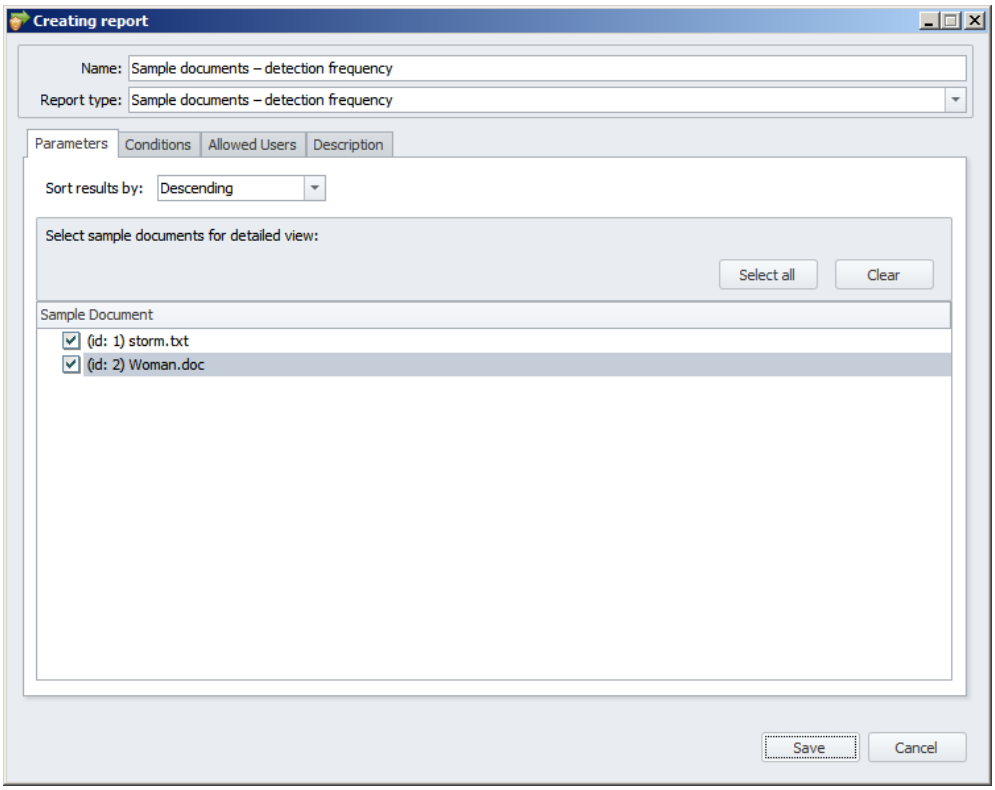
8.3.2 Creating and Editing a Report

To create a query for generating a report:

1. Go to the **Reports** section.
2. Do the following:

Action	Procedure
Generate the report	Do one of the following: • in the main menu, select **Edit > New Report** • click **New Report** on the toolbar.
Edit report	1. In the reports list, select the row with the report you want to edit. 2. Do one of the following: • in the main menu, select **Edit > Edit**; • click **Edit** on the toolbar; • right-click the report name and choose **Edit**.

A dialog box with the report settings will appear on the screen.



Generate the report

3. Specify the report settings in the dialog box that appears:

   - **Name**. Specify the report name.
   - **Report type**. Select the required report type from the drop-down list.
   - On the **Parameters** tab please specify the settings of the generated report. The set of settings depends on the type of report selected in the previous step. For the description of the settings for every type of report see "Report Types".
   - On the **Conditions** tab specify the conditions for generating the reports. The conditions of generating reports are set in the same way as the conditions for generating queries (see "Configuring Query Conditions (Conditions tab)").
   - On the **Allowed users** tab select the check boxes of the users who can view this report. To select or clear all the check boxes, use the **Select All** and **Clear** buttons.
   - On the **Description** tab, type the description of the report.

4. Click **Save**.

After generating the report will have the *Pending for update* status. When the report becomes *Ready* (use the update function: see "Refreshing Data in Management Console"), you can view report results, print the report and export report to file.

8.3.3 Viewing the Report Results

You can view the data of the reports with the *Ready* status. Building the report will result in displaying the information (including graphics) on the number of objects matching certain conditions.

Note

The overall number of objects in a report is counted only for the responsibility zones that are assigned to the user who generates the report.

To generate a report:

1. Go to the **Reports** section.
2. Select the required report in the working area of the main window.
3. Do one of the following:
   - in the main menu, select **Edit > Run**;
   - double-click the selected report;
   - click **Run** on the toolbar.

   Then the **View** dialog box will open on the screen with the report for the selected objects.

Note

You can view the multi-page reports using the standard navigation controls located on the report window toolbar.

Reports can be printed (see "Printing a Report") and exported to files (see "Exporting a Report").

8.3.4 Rebuilding a Report

The data displayed in a report correspond to the view associated with this report. However, the data are being constantly updated during the work process. To receive reports based on the current data it is recommended to run the update process prior to generating the report.

To update the report data:

1. Go to the **Reports** section.
2. Select the required report in the working area of the main window.
3. Click **Rebuild** on the toolbar.
4. In the confirmation window, click **Yes** to start updating the data.

8.3.5 Printing a Report

The report is printed from the **View** window where report results are displayed.

To configure the print options and print a report,

1. Do one of the following:
   - in the main menu, select **File > Print**;
   - click **Print** on the toolbar.
2. In the **Print** dialog box configure the print options.

To print a report without configuring the print options,

do one of the following:

- in the main menu, select **File** > **Print...**
- click **Print** on the toolbar.

8.3.6 Copying a Report

You can create a report by copying an existing report

To copy a report:

1. Go to the **Reports section**.
2. Select the required report in the working area of the main window.
3. Do one of the following:
   - in the main menu, select **Edit > Copy**;
   - click **Copy** on the toolbar.

The copy of the report will have the same parameters as the initial report with the addition of the number of the copy to the name. For example, the copy of "*Total number of incidents detected by the system*" report will have the name: "*Total number of incidents detected by the system (1)*".

8.3.7 Exporting a Report

You can export a report to a file using any of the supported formats: `.pdf`, `.xls`, `.rtf`, `.html`, graphic formats, etc. You can view and process the exported report using the program that supports the file format of the report.

The report is exported from the **View** window.

To export a report to a file:

1. Do one of the following:
   - in the main menu, select **File > Export** and select the required file type in the submenu;
   - click **Export** on the toolbar. Click the arrow to the right of the **Export** button, and then select the necessary file type.

2. In the **Save** dialog box, select a folder to save the exported report and a name of the file.

8.3.8 Deleting a Report

To delete a report:

1. Go to the **Reports** section.
2. Select the required report in the working area of the main window.
3. Do one of the following:
   - in the main menu, select **Edit > Delete**;
   - click **Delete** on the toolbar.
4. In the confirmation box, click **Yes** to confirm.

8.4 Managing the Queries and Reports Folders

You can group the queries and reports into folders for more convenient viewing. For more information about working with folders see:

- Creating and Editing a Folder
- Moving Queries and Reports between Folders
- Copying a Folder
- Deleting a Folder

8.4.1 Creating and Editing a Folder

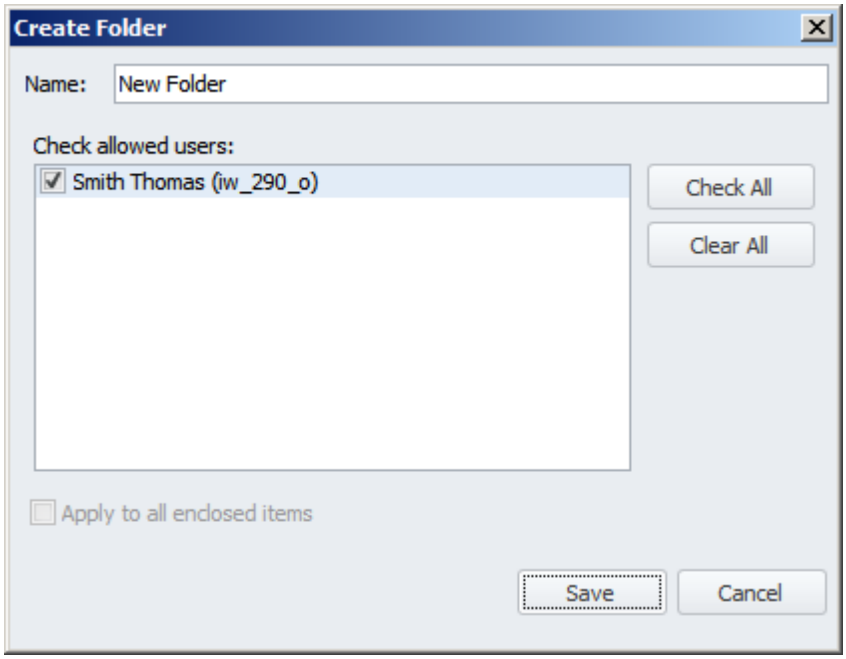
To create or edit a folder:

1. Go to the section you need (**Queries** or **Reports**).
2. Do the following:

Action	Procedure
Creating a folder	Do one of the following: • in the main menu, select **Edit > New Folder**; • click **New Folder** on the toolbar.
Editing a folder	1. Select the required folder.

Action	Procedure
	2. Do one of the following: • in the main menu, select **Edit > Edit**; • click **Edit** on the toolbar; • right-click the folder name and select **Edit**.

A dialog box will appear on the screen.



Configuring folder settings

3. Configure the folder settings:
   - **Name**. Folder name.
   - **Check allowed users**. Mark the user accounts that should have the right to manage this folder. To select or clear all the check boxes, use the **Check All** and **Clear All** buttons.

     Important!

     To create a folder there must be at least one allowed user.

   - **Apply to all enclosed items**. If you are editing a folder and want to allow (or deny) a user the right to manage all queries or reports in a folder, then you should select (or unselect) the check box opposite the name of this user in the list of allowed users and select the **Apply to all enclosed items** check box.

     Note

     If you don't select the **Apply to all enclosed items** check box, then the user will see this folder as empty, and will be able only to add his own queries and reports into it.

     Important!

     Adding a user to the allowed list for all the attached objects will lead to the fact that he/she can change, copy or delete all the allowed folders and queries/reports.

4. Click **Save**.

In the new folder you can create queries (see "Creating and Editing a Query") or reports (see "Creating and Editing a Report"), or move other queries, reports and folders into it (see "Moving Queries and Reports between Folders").

8.4.2 Moving Queries and Reports between Folders

To move a query, a report, or a folder from one folder to another:

1. Go to the section you need (**Queries** or **Reports**).
2. Click the required query/report/folder.
3. Hold the mouse button down and drag the line containing the name of the query/report/folder to the specified folder. When a yellow arrow appears to the left of the selected folder name, release the mouse button.

As the result, the query/report/folder will be added to the selected folder.

To move the query one level up:

1. Click the required query/report/folder while holding the `Shift` key pressed.
2. Hold the mouse button and the `Shift` key, move the line with the name of the query/report/folder to the folder one level below your target. Once the blue arrow appears on the left, please release the mouse button and the `Shift` key.

As the result, the query/report/folder will be moved to the upper level folder.

8.4.3 Copying a Folder

To create a copy of the folder:

1. Go to the section you need (**Queries** or **Reports**).
2. Select the required folder.
3. Do one of the following:
   - in the main menu, select **Edit > Copy**;
   - click  **Copy** on the toolbar.

A folder-copy will be created, which contains copies of all subfolders and reports/queries to be copied from the original folder. A name of the folder-copy will be similar to the original folder with the addition of the copy number to the title. For example, the copy of "*All events for the period*" report will have the name: "*All events for the period* (1)". The names of subfolders and reports/queries that have been copied from the source folder will be similar to the source.

By default only the user who has performed the copying can work the copy of the folder and its content.

If necessary, you can modify the name of the copy and the list of the authorized users as described in "Creating and Editing a Folder".

8.4.4 Deleting a Folder

Note

Any folder may contain hidden queries, reports or subfolders, including the queries (reports, folders) that you are not permitted to view. This folder can be deleted by the user who has the privileges for working with all the queries/reports in this folder.

To delete a folder:

1. Go to the section you need (**Queries** or **Reports**).
2. On the **Queries** pane, select a folder.
3. Click **Delete** on the **Queries** pane.
4. In the confirmation box click **Yes** to delete the folder containing the query group.

9 Licensing information

Summary of the section:

- End-User License Agreement
- Third-Party Licenses

9.1 End-User License Agreement

IMPORTANT! Read this End-User License Agreement (EULA) carefully before using the Software.

Clicking the Accept button in the License Agreement box at installation time or any use of the installed Software will signify your irrevocable acceptance of the terms and conditions of this EULA. If you do not accept the terms and conditions of this EULA, You should terminate the installation process and/or the use of the Software.

Licence Agreement

This End-User Licence Agreement ("Agreement") is a joinder agreement between ZAO InfoWatch ("Rightholder") and you, a person or legal entity ("User"), legally possessing a copy of InfoWatch Traffic Monitor ("System").

The System is designed for monitoring, filtering, and the prevention of leaks of data, transferred beyond the company's frontiers through Right holder, Internet or Internet pagers, as well as for network and local printing. The System also allows you to control access to ports and monitor data, copied to removable storage devices.

1. **Definitions**

   1.1. "Software" means, in whole or in part, the System, the accompanying documentation and optionally ordered updates to the System, copyrighted by ZAO "InfoWatch".

1.2. "Computer" means the hardware that the Software is designed for and where the System will be installed and/or used.

1.3. User (You) means a person or legal entity that installs the Software on its behalf and legally possesses a copy of the Software. If the Software has been downloaded or acquired on behalf of a legal entity, the term "User" (you) means the legal entity for which the Software was downloaded or acquired and that an authorized person accepts the terms and conditions of this Agreement on its behalf.

1.4. "Partners" means the organizations distributing the Software under the agreement with the Rightholder.

1.5. "System Documentation" means the accompanying printed and other materials, User Guide, Administrator Guide, reference book, help file and similar System-related printed and electronic documents, copyrighted by ZAO "InfoWatch".

2. Grant of License

2.1. The Rightholder grants you a non-exclusive license to use the Software within the functionality, as described in the System Documentation, provided that you meet all the technical requirements specified in the System Documentation, as well as all the restrictions and terms of use of the System, specified in this Agreement.

2.2. Unless otherwise specified, if you have received, downloaded, or installed an evaluation version of the Software, you may use the Software only for evaluation purposes within one evaluation period, starting with the software installation date. Any use of the Software for other purposes or after the evaluation period expires is prohibited.

2.3. Unless otherwise specified in the license agreement, if you are using different versions of the Software or versions for different languages, if you have received the Software on several media or otherwise possess several copies of the Software or if you have received the Software as part of some other software, the total number of your computers, where all the versions are installed and/or used, must correspond to the number of licenses, procured from the Rightholder. Each purchased license gives you the right to install and use the System on a certain number of computers or for a certain number of licensed objects, as set forth in Clause 2.2.

2.4. The User has the right to make a single copy of the Software, provided that this copy is only used for archive purposes or for the replacement of a duly purchased Software copy, should the original be lost, destroyed, or become unusable. This copy cannot be used for any other purposes and must be destroyed, if the User's right to use the Software becomes invalid.

2.5. Any legal transfer of rights for the use of the Software is only possible after entering this Agreement and upon prior consent of the Rightholder or its authorized Partner. The successor of the rights for the use of the Software then becomes a legal successor of the User, provided that the User under this Agreement is fully replaced.

2.6. You are fully responsible for compliance with all applicable export and import laws and regulations, as well as trade sanctions and embargos, concerning the transfer of rights for the use of the Software.

3. Restrictions

3.1. You shall not decompile, disassemble, or modify the Software, as well as produce derived works on its basis, in whole or in part, unless it is allowed by law.

3.2. You shall not transfer or assign your rights to use the Software to any third party, except as set forth in Clause 2.6.

3.3. You shall not transfer or provide access to the license key to any third parties, except for as set forth in Clause.2.6 of this Agreement. Any other transfer of rights will be considered a violation of this Agreement. A license key is considered confidential information. The Rightholder reserves the right to

verify the validity of your license key with the available means.

3.4. You shall not rent, lease, or lend the Software to any third parties or disclose the results of the benchmark testing of the System.

3.5. The Rightholder has the right to block the license key, should the User breach any of the terms or conditions of this Agreement.

3.6. If you are using an evaluation version of the Software, you shall not transfer your copy of the Software to any third party.

3.7. Any violation of the intellectual property rights on the Software will result in civil, administrative, or criminal responsibility under the applicable law.

3.8. You shall not use the Software for any purposes or in any ways, restricted or prohibited by the applicable law. You are fully responsible for any unauthorized use of the Software.

3.9. Should you violate any terms or conditions of this Agreement, the Rightholder has the right to terminate this Agreement for the use of the Software at any time without notice or any refund of the cost of the Software, full or partial.

4. Limited Warranty and Disclaimer

4.1. The Rightholder guarantees that the Software will substantially perform according to the description in the System Documentation.

4.2. You agree that no software is free of errors and are recommended to back up your files regularly.

4.3. The Rightholder does not guarantee proper Software operation, if any requirements, described in the System Documentation, or any terms and conditions of this Agreement are violated by the User.

4.4. EXCEPT AS SET FORTH IN THIS LIMITED WARRANTY, THE SOFTWARE IS PROVIDED "AS IS". THE RIGHTHOLDER OR ITS PARTNERS GIVE NO WARRANTY AS TO ITS USE OR PERFORMANCE. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE RIGHTHOLDER AND ITS PARTNERS MAKE NO WARRANTY, CONDITION, OR REPRESENTATION, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, NON-INFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABILITY, SATISFACTORY QUALITY, INTEGRATION, OR FITNESS FOR A PARTICULAR PURPOSE. YOU ASSUME FULL RESPONSIBILITY FOR SELECTING THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS, FOR THE INSTALLATION AND USE OF THE SOFTWARE AND FOR THE RESULTS OBTAINED WITH THE SOFTWARE.

5. Limitation of Liability

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE RIGHTHOLDER AND/OR ITS PARTNERS BE LIABLE FOR ANY DAMAGES (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION, LOSS OF INFORMATION, ETC.) IN CONNECTION WITH THE USE OR INABILITY TO USE THE SOFTWARE, EVEN IF THE RIGHTHOLDER OR ITS PARTNERS WERE ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN ANY CASE, THE LIABILITY OF THE RIGHTHOLDER OR ITS PARTNERS IN CONNECTION WITH ANY PROVISION OF THIS AGREEMENT IS LIMITED BY THE COST OF THE SOFTWARE, ACTUALLY PAID BY YOU. THESE RESTRICTIONS MAY NOT BE EXCLUDED OR LIMITED UNDER APPLICABLE LAW.

6. Software Products

6.1. Any third party technologies, the use of which within the Software is necessary or reasonable, are specified in the System Documentation. Such a technology is licensed to the end user on the terms and conditions of a license agreement with the third party, specified in the System Documentation.

This license agreement with the third party is included in this Agreement by reference.

6.2. The software products, making part of the System, are only licensed for limited use within the System. When the license agreement for the use of the Software expires, the User must destroy all the copies of the Software.

7. Open (Free) Software

This product may contain programs that are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or other similar free software/open source licenses, which, among other rights, permit the user to copy, modify, and redistribute certain programs, or portions thereof, and have access to the source code ("Open Source Software"). If such licenses require that for any software, distributed in an executable binary format, the source code should also be made available to the user, such source code should be obtained by sending a query to the Rightholder or supplied with the product. If any Open Source Software licenses require that the Rightholder provide rights to use, copy or modify an Open Source Software program beyond the rights granted in this Agreement, then such rights take precedence over the rights and restrictions in this Agreement.

8. Intellectual Property Rights

8.1. You agree that the Software, documentation, other copyright matter, any systems, ideas, methods of operation, documentation and other information contained in the Software, as well as the trademarks are the intellectual property of the Rightholder or its Partners. This Agreement does not grant you any rights to the intellectual property, including any trademarks or service marks of the Rightholder or its Partners, except for the rights, provided by this Agreement.

8.2. You agree that the source code and the license key for the Software are the intellectual property of the Rightholder and its Partners.

8.3. You may not delete or modify any copyright or other proprietary notices on any copy of the Software.

9. Rightholder Contact Information

ZAO "InfoWatch"

Phone/fax:+7 (495) 229-00-22

Sales department: sales@infowatch.com

Technical support service: support@infowatch.com

Website: www.infowatch.com

9.2 Third-Party Licenses

The system contains third-party components distributed under the MIT License (http://www.opensource.org/licenses/mit-license.html):

- Lua – http://www.lua.org/license.html
- LuaBind – http://www.rasterbar.com/products/luabind.html
- libxml2 – http://www.xmlsoft.org/

The system also contains software

- distributed under the BSD Licenses (http://www.opensource.org/licenses/bsd-license.php):

- Stringencoders – http://code.google.com/p/stringencoders/

- distributed under the GNU GENERAL PUBLIC LICENSE (http://www.gnu.org/licenses/gpl-2.0.html):
  - Pdftotext – http://www.foolabs.com/xpdf/
  - Tnef – http://sourceforge.net/projects/tnef/
  - Unzip – http://www.info-zip.org/UnZip.html
  - libcole.so – arturo@directmail.org; andy.scriven@research.natpower.co.uk
  - libhtmltree.so – pauljlucas@mac.com