

INFOWATCH

InfoWatch Device Monitor 6.1

User Guide

INFOWATCH DEVICE MONITOR 6.1

User Guide

© InfoWatch
tel +7 (495) 229-00-22 • fax +7 (495) 229-00-22
http://www.infowatch.com
Revision date: 29.03.2016

Table of contents

Part I InfoWatch Device Monitor Overview 9

1.1 InfoWatch Device Monitor Functions 9

1.1.1 Operation in Safe Mode 11

1.2 InfoWatch Device Monitor Workflow 11

1.3 Glossary 13

Part II Installing and Configuring InfoWatch Device Monitor 17

2.1 Hardware and Software Requirements 18

2.1.1 Database 18

2.1.2 InfoWatch Device Monitor Server 18

2.1.3 InfoWatch Device Monitor Client 19

2.1.4 Management Console 20

2.1.5 Integration with Traffic Monitor Versions 20

2.2 InfoWatch Device Monitor Server End Setup 21

2.2.1 Database deployment under Microsoft SQL Server DBMS 22

2.2.2 Database Deployment Under Oracle DBMS 22

2.2.2.1 Configuring InfoWatch Device Monitor Connection to Oracle DBMS Server 23

2.2.3 Server Setup Recommendations 23

2.2.4 Server End Installation Procedure 24

2.3 InfoWatch Device Monitor Client Installation 30

2.3.1 Standard Client Installation 30

2.3.2 Client Installation via Software Distribution Tools 31

2.4 Configuring InfoWatch Device Monitor Server 33

2.4.1 <applicationSettings> Section 34

2.4.2 <system.diagnostics> Section 37

2.4.3 Deleting Temporary Files 39

2.5 Updating InfoWatch Device Monitor 39

2.5.1 Updating InfoWatch Device Monitor Server End 40

2.5.2 Updating InfoWatch Device Monitor Client 41

2.6 Uninstalling InfoWatch Device Monitor 41

2.6.1 Removing Client Installed via Software Distribution Tools 42

Part III Using Management Console 43

3.1 Management Console Overview 43

3.1.1 Authorization and Connecting to InfoWatch Device Monitor Server 43

3.1.2 Management Console Main Screen 45

3.1.2.1 Configuring Management Console Main Screen Elements 46

3.1.3 Management Console Sections 46

3.2 Managing Console Accounts 47

3.2.1 Viewing Management Console Accounts Details 48

3.2.2 Adding New Management Console Account 49

3.2.3 Locking or Unlocking Management Console Account 50

3.2.4 Editing Management Console Account 50

3.2.5 Deleting Management Console Account 50

3.2.6 Management Console Security Schema Operation Activity Log 51

3.2.6.1 Viewing Audit Log 51

3.2.6.1.1Selector Values 53

3.2.6.2 Log Records Filtering 53

3.2.6.2.1Date/Sequence Number Tab 55

3.2.6.2.2Object/Action Tab 56

3.2.6.2.3Additional Tab 56

3.2.6.3 Deleting Records from Log 57

3.2.6.4 Exporting Log Records 57

3.2.6.5 Analyzing Log Records in Microsoft Excel 57

3.3 General System Settings 57

3.3.1 Common Settings for Clients 58

3.3.2 Settings of Corporate Network 60

3.3.3 Network Traffic Control 62

3.3.4 Device Monitor Server Settings. Connecting to Traffic Monitor Server 63

3.3.5 Connecting to LDAP Server 65

3.3.6 Employee Notifications about Policy Violations 66

3.3.7 Exclusion of Application from Interception 67

3.3.8 Application Control 69

3.3.9 Event Storage 70
3.3.10 Import/Export Configuration 71
3.3.11 InfoWatch Device Monitor Server Manager 72
3.4 Managing Security Schema 73
3.4.1 Security Schema Organization 73
3.4.1.1 Security Rules and Policies 74
3.4.1.2 Employees and Employee Groups 75
3.4.1.3 Computers and Computer Groups 76
3.4.1.4 Uploading Security Schema to Managed Workstations 76
3.4.2 Common Actions in Managing Security Schema 76
3.4.2.1 Viewing Active Security Schema 76
3.4.2.2 Viewing Old Security Schema 77
3.4.2.3 Security Schema Comments 78
3.4.2.4 Editing Security Schema 79
3.4.2.4.1Awaiting Editing Ends. Unlocking Security Schema 80
3.4.2.5 Updating Security Schema 81
3.4.2.6 Exporting/Importing Security Configuration 81
3.4.3 Security Schema Setup 82
3.4.3.1 Security Policies 82
3.4.3.1.1Viewing Security Policies 83
3.4.3.1.2Adding and Configuring New Security Policy 85
3.4.3.1.3Editing Security Policy 87
3.4.3.1.4Deleting Security Policy 87
3.4.3.2 Rules 87
3.4.3.2.1Rules Application 88
3.4.3.2.1.1 Device Monitor Rules Application 88
3.4.3.2.1.2 Creating Shadow Copies and Blocking Operations Due to Free Space Shortage 90
3.4.3.2.2Adding a Rule 90
3.4.3.2.2.1 Configuring Application Monitor Rule 91
3.4.3.2.2.2 Configuring Cloud Storage Monitor Rule 93
3.4.3.2.2.3 Configuring Device Monitor Rule 95
3.4.3.2.2.4 Configuring File Monitor Rule 97

3.4.3.2.2.5 Configuring FTP Monitor Rule 98
3.4.3.2.2.6 Configuring HTTP(S) Monitor Rule 100
3.4.3.2.2.7 Configuring IM Client Monitor Rule 101
3.4.3.2.2.8 Configuring Mail Monitor Rule 104
3.4.3.2.2.9 Configuring Network Monitor Rule 105
3.4.3.2.2.10 Configuring Photo Monitor Rule 107
3.4.3.2.2.11 Configuring Print Monitor Rule 108
3.4.3.2.2.12 Configuring ScreenShot Control Monitor Rule 110
3.4.3.2.3Editing a Rule 111
3.4.3.2.4Deleting a Rule 111
3.4.3.2.5Copying a Rule 112
3.4.3.3 Employees 112
3.4.3.3.1Viewing Employee Details 113
3.4.3.3.2Viewing Resultant Policy and White List for an Employee 113
3.4.3.3.3Adding and Editing an Employee Group 115
3.4.3.3.4Deleting Employee Group 116
3.4.3.3.5Adding Employee Account to a Group 116
3.4.3.3.6Editing Employee Account 118
3.4.3.3.7Removing Employee Account from Employee Group 118
3.4.3.3.8Deleting Employee Account from Security Schema 119
3.4.3.4 Computers 119
3.4.3.4.1Viewing Computer Details 120
3.4.3.4.2Viewing Resultant Settings, Policy and White List for a Computer 121
3.4.3.4.3Adding and Editing a Computer Group 123
3.4.3.4.4Deleting Computer Group 125
3.4.3.4.5Adding Computer to a Group 125
3.4.3.4.6Removing Computer from a Group 126
3.4.3.4.7Deleting Computer from Security Schema 127
3.4.3.4.8Updating Clients at Managed Computers 128
3.4.3.4.9Diagnostics of the Workstation 128
3.4.3.5 Mobile Devices 129
3.4.3.5.1Preparing a Mobile Device on Android Platform 130

3.4.3.5.2Preparing a Mobile Device on iOS Platform 131
3.4.3.5.3Adding a Mobile Device to Computer Group 132
3.4.3.5.4Adding a Mobile Device through Appointment to Employee 134
3.4.3.5.5Deleting the Mobile Device 135
3.4.3.6 White Lists 136
3.4.3.6.1Viewing White List Details 136
3.4.3.6.2Adding White List 137
3.4.3.6.2.1 Adding Device Entry 138
3.4.3.6.2.2 Deleting Device Entry 140
3.4.3.6.3Defining Entry Validity Period 140
3.4.3.6.4Editing White List 140
3.4.3.6.5Deleting White List 141
3.4.3.7 Signatures 141
3.4.3.7.1Adding Signature Category 142
3.4.3.7.2Editing Signature Category 142
3.4.3.7.3Deleting Signature Category 143
3.4.3.8 Application Protocol 143
3.4.3.8.1Creating an Application List and Adding Applications 144
3.4.3.8.2Creating and Editing the Application Protocol Filter 145
3.4.3.8.3Adding Application to List Automatically 146
3.4.3.8.4Adding Application to List Manually 146
3.4.3.8.5Exporting Application Protocol 147
3.4.4 Temporary Employee Access to Network 148
3.4.5 Temporary Employee Access to Devices 149
3.5 Viewing Events 150
3.5.1 Event Filters 156
3.5.2 Deleting Events 157
3.6 Clients Remote Installation, Updating and Uninstallation 158
3.6.1 View Tasks 159
3.6.2 Preparing Primary Client Installation. Distribution Agent 160
3.6.2.1 Enabling Shared Administrative Resources 161
3.6.2.2 Firewall Settings 161

3.6.3 Creating Primary Distribution Task 162
3.6.4 Creating Update Task 164
3.6.5 Creating Uninstallation Password Reset Task 165
3.6.6 Creating Uninstallation Task 166
3.6.7 Launching, Pausing, Editing, and Deleting Tasks 167
3.6.8 Client Installation Errors 167
3.6.9 Creating Installation Package 168
3.7 Additional Features 170
3.7.1 Filter Table Contents 170
3.7.1.1 Filtering by Date 170
3.7.1.2 Applying Standard Filters 171
3.7.1.3 Custom Filter 172
3.7.1.4 Editing Filters 173
3.7.1.5 Removing a Filter 173
3.7.2 Grouping or Sorting Entries 174
3.7.3 Hotkeys 174
Part IV Troubleshooting 177
4.1 Viewing Server Messages 178
Part V Licensing Information 182
5.1 WiX Common Public License 182
5.2 InfoWatch Device Monitor End-User License Agreement 185

1 InfoWatch Device Monitor Overview

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

This guide contains the following sections:

- Installing and configuring InfoWatch Device Monitor. Installing, configuring, updating or uninstalling InfoWatch Device Monitor.
- Using Management Console. Using the System: managing employees' accounts registered with InfoWatch Device Monitor, security schema management, client remote installation.
- Troubleshooting. Potential issues with InfoWatch Device Monitor and troubleshooting.
- End-User License Agreement. System and Components User License.

For general System information see the following introductory sections:

- InfoWatch Device Monitor Functions. InfoWatch Device Monitor features overview.
- InfoWatch Device Monitor Workflow. Workflow description for InfoWatch Device Monitor system and its components.
- Glossary. List of terms used in software documentation and GUI.

If you have any issues regarding the product operation, please contact support:

- If you have purchased the product from InfoWatch partner, please contact partner support.
- If you purchased the product directly from InfoWatch, you can contact our support at support@infowatch.com or through web-site http://cp.infowatch.com/en/.
- Technical Support Service is available to assist you Mon-Fri, 7 AM – 9 PM (Moscow time, GMT+4), except weekends and Russian Federation public holidays.

Before contacting support please refer to our *Knowledge Base* at https://kb.infowatch.com/. Knowledge Base may already have the answer to your question or description of the problem you are experiencing

1.1 InfoWatch Device Monitor Functions

InfoWatch Traffic Monitor Main Functions:

- realtime monitoring of managed computers (workstations and mobile devices);
- managing employee access to system peripherals;
- monitoring computer print operations;
- supervising Instant Messengers: Skype, WhatsApp, Yahoo (YMSG protocol), Jabber (XMPP protocol) and Mail.Ru Agent (MMP protocol);
- supervising SMS of mobile communication;
- supervising traffic transferred by FTP and FTPS;
- supervising traffic transferred by HTTP and HTTPS;
- supervising data transferred by network connections beyond corporate network;
- supervising emails transferred by protocols (SMTP, POP3, IMAP, MAPI);
- supervising photographs made by cameras of mobile devices;
- retrieving data from managed computers (workstations and mobile devices);
- transferring retrieved data for InfoWatch Traffic Monitor analysis.

- Microsoft RDP and Citrix ICA client control (see "Configuring Device Monitor Rule")
- cloud storage control (see "Configuring Cloud Storage Monitor Rule")
- screenshot control (see "Configuring ScreenShot Control Monitor Rule")
- application control (see "Configuring Application Monitor Rule")
- event storage management (see "Events")

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

User (employee) actions are observed and controlled on managed computers.

Managed computer is a workspace (workstation or mobile device) that gives you access to controlled files and peripherals.

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

Monitored peripherals are system devices controlled by InfoWatch Device Monitor.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1.1.1 Operation in Safe Mode

Some of InfoWatch features are still available in safe mode (with network features or without them).

The following table lists the features available in safe mode.

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

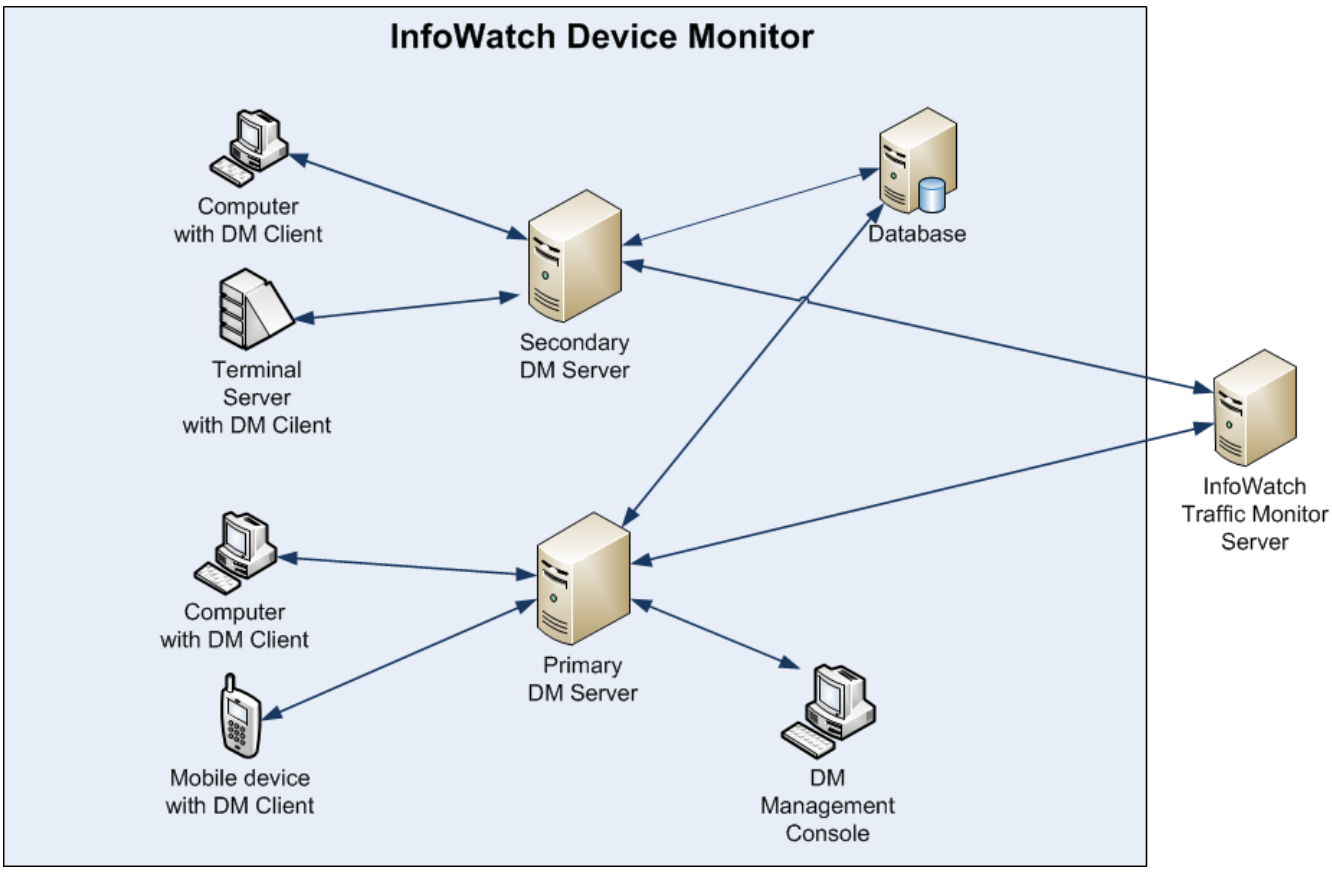
1.2 InfoWatch Device Monitor Workflow

InfoWatch Device Monitor components are listed in the following table.

Component	Purpose
InfoWatch Device Monitor Client (InfoWatch device monitor client application, Client)	Intercepting employee actions on managed computers

Component	Purpose
InfoWatch Device Monitor Server (InfoWatch device monitor server, Server)	Configuring client applications, retrieving data from client applications and sending it to InfoWatch Traffic Monitor
InfoWatch Device Monitor Database (database)	Storing critical System data
InfoWatch Device Monitor Management Console (Management Console)	System Management
Servers Manager	Configuring roles and other attributes of System Servers

The following image illustrates System workflow.



The System is deployed and works as follows:

1. **Primary server** is installed first (changing of server roles is described in "InfoWatch Device Monitor Server Manager").
2. When you install the primary server you must specify the server that will be used by the **database**: DBMS can be stored separately or together with the primary server.
3. Primary server installation generates **database schema** where your **security schema** and other system parameters are stored.
4. You can install **secondary servers**, if needed, to balance the System workload.
5. **Management Console** can be installed on any computer and connect to the primary server. Used to configure security schema according to the corporate security policy.
6. **Device Monitor Clients** are installed on **computers**. Clients connect to any available Device Monitor Server via encrypted channel with binding to the Server by the traffic-encrypting key. Clients implement and upgrade security schemas, retrieve shadow copies and send them to Device Monitor Server.

7. Device Monitor Server retrieves updated security schemas versions from database and distribute them over managed computers. Managed computers inform Server about events responding to security schema rules and send shadow copies. Events information are transferred to the database. Shadow copies are sent to InfoWatch Traffic Monitor.

Example 1

1. At the managed computer the employee accesses managed peripheral (for example, attempts to print a document on USB printer).
2. Client checks if the employee has a right to access the peripheral. If he doesn't, access is denied (in this case, the document won't be printed).

Printing operations on local and network printers are tracked by Print Monitor interceptor. Document copy is sent for InfoWatch Monitor Traffic analysis. Employee can send a document to print, if he/she have access to printer (this is checked by Device Monitor interceptor).

Example 2

Writing to PDF files on removable devices is monitored by System rule. According to the rule, this operation must create a shadow copy of the document.

1. At the managed computer the employee writes to files on a removable device (for example, copying a file to USB flash drive).
2. If writing to removable device is successful, InfoWatch Device Monitor Client generates an event and creates file shadow copy.
3. If you cannot create a shadow copy (for example, if there's no free space on the hard drive), writing operation will be canceled. (In the previous example, the employee wouldn't be able to copy files.)
4. Client transmits data (event and file shadow copy) to InfoWatch Device Monitor Server. If Server connection is unavailable, data is stored on managed computer. Once connection has been recovered, the information will be handed over to Server.
5. Server sends data for InfoWatch Traffic Monitor analysis. If no connection to InfoWatch Traffic Monitor server is available, data is stored in the database. Once connection has been recovered, the information is handed over to InfoWatch Traffic Monitor.

Any attempts to write to files on removable devices are tracked by File Monitor interceptor. Obtained information is analyzed by InfoWatch Traffic Monitor. At the same time, access to removable device is controlled by Device Monitor interceptor. Therefore, you can write to files only if you can access the device.

Example 3

DOC files printing is tracked by System rule. According to the rule, this operation must create a shadow copy of the document.

1. At the managed computer the employee sends a document to print.
2. If print job is created successfully, InfoWatch Device Monitor Client generates an event and creates a shadow copy of printed document.
3. If you cannot create a shadow copy of the document (for example, if there is no free space on hard drive), print operation will be canceled. (In the previous example, employee won't be able to print a file.)
4. Client transmits data (event and file shadow copy) to InfoWatch Device Monitor Server. If Server connection is unavailable, data is stored on managed computer. Once connection has been recovered, the information is handed over to Server.
5. Server sends data for InfoWatch Traffic Monitor analysis. If no connection to InfoWatch Traffic Monitor server is available, data is stored in the database. Once connection has been recovered, the information will be handed over to InfoWatch Traffic Monitor.

1.3 Glossary

Term	Definition
Black list of applications	When the System is in active black lists operation mode then all application listed in the Application Monitor rule will be allowed to run for all employees for which this rule is active. Other applications will be allowed to run. See: *Application Monitor*

Client	See: *InfoWatch Device Monitor Client*
Computer	In terms of InfoWatch Device Monitor system, a computer is a managed computer: desktop, mobile device or other workstation. See: *Managed computer, Mobile device*
Computer group	Security schema parameter. Computer group includes computers with the same security policy. Computer groups are formed according to corporate security policy. See: *Default employee group*, *Security policy*, *Employee access level, Managed computer*
Controlled file	File that is controlled by InfoWatch Device Monitor. Controlled files list is based on corporate security policy
Database	See: *InfoWatch Device Monitor database*
DBMS	Database management system.
Default computer group	Computer group that is added automatically when you create a new security schema. This group includes workstations that don't belong to any other computer group (when a new computer is registered or if you remove a computer from all other groups). See: *Computer*, *Employee group*, *Security policy*
Default employee group	Employee group that is added automatically when you create a new security schema. This group includes all accounts that don't belong to any other employee group (when a new employee is added or if you remove employee from all other groups). See: *Employee group*, *Security policy*
Device Monitor	InfoWatch Device Monitor client module interceptor. It is designed to control employee access to system peripherals. See: *Interceptor*
Document shadow copy	A copy of printed document, received from the print job initiated on the managed computer.
Employee	Any user registered in InfoWatch Device Monitor as an employee. Employee actions are monitored by client modules installed at workstations.
Employee access level	Employee security policy set. In other words, security policies assigned to: • employee's groups to which this employee belongs; • computer groups to which the computer used for managed actions belongs.
Employee group	Security schema parameter. The group includes employees covered by the same security policy according to the corporate security policy. See: *Default employee group*, *Security policy*, *Employee access level*
File mask	Matching file search pattern. You can apply a file mask in InfoWatch Device Monitor to create a rule for File Monitor and Print Monitor
File Monitor	InfoWatch Device Monitor client module interceptor. It is designed to monitor employee activity that involves creating files on removable devices. See: *Interceptor*
File shadow copy	A copy of file, recorded to removable device. It is created only after the file has been successfully saved to removable device. File shadow copies are analyzed by InfoWatch Traffic Monitor.
FTP Monitor	InfoWatch Device Monitor client module interceptor. It is designed to control data exchange through FTP/FTPS protocol. See: *Interceptor*

HTTPS Monitor	InfoWatch Device Monitor client module interceptor. It is designed to control data exchange through HTTPS protocol. See: *Interceptor*
IM Client Monitor	InfoWatch Device Monitor client module interceptor. It is designed to control employee access to instant messengers. See: *Interceptor*
InfoWatch Device Monitor	The System is designed to control employee access to peripherals, monitor file operations on removable devices, network activity, and sending documents to print.
InfoWatch Device Monitor Client	InfoWatch Device Monitor client module. It is designed to control employee activity
InfoWatch Device Monitor database	Database that contains all InfoWatch Device Monitor information
InfoWatch Device Monitor Management Console	GUI element. It is designed to control InfoWatch Device Monitor (system administration, security schema configuration, etc.)
InfoWatch Device Monitor Server	InfoWatch Device Monitor Server module. It is designed to monitor managed workstations and interact with InfoWatch Traffic Monitor.
InfoWatch Traffic Monitor	Traffic control system (SMTP, HTTP, ICQ and Lotus Notes). InfoWatch Traffic Monitor analyzes the shadow copies it receives from InfoWatch Device Monitor
Interceptor	Client module element. Provides control over employee activity basing on security schema. Client module includes the following interceptors: File Monitor, Print Monitor, Device Monitor, IM Client Monitor, FTP Monitor, HTTPS Monitor, Network Monitor. See: *File Monitor*, *Device Monitor*, *Print Monitor*, *IM Client Monitor, FTP Monitor, HTTPS Monitor, Network Monitor*.
Local administrator	Management Console role which manages accounts
Log	System management log of Management Console user. See: *User Activity Log*, *Management Console user*
Mail Monitor	InfoWatch Device Monitor client module interceptor. It is designed to control mail messages transfer via SMTP, POP3, MAPI protocols. See: *Interceptor*
Management Console	See: *InfoWatch Device Monitor Management Console*
Management Console user	User who manages InfoWatch Device Monitor. Each user has a role assigned basing on corporate security policy.
Management Console User Activity Log	Management Console activity control. You can use log system to monitor your security schema building and management (i.e. all actions that change your security schema) and System administration. See: *Log*, *Management Console accounts*
Managed computer	Workplaces that have access to controlled files and peripherals. The InfoWatch Device Monitor Client is installed to managed computer.
Managed peripheral	Peripherals (printers, scanners, disk drives, etc.) controlled by InfoWatch Device Monitor. Access to peripherals is based on corporate security policy
Mobile device	Smartphone or tablet PC
Network Monitor	InfoWatch Device Monitor client module interceptor. It is designed to restrict data transferring by any network connections except corporate ones or connections with specified allowed servers. See: *Interceptor*

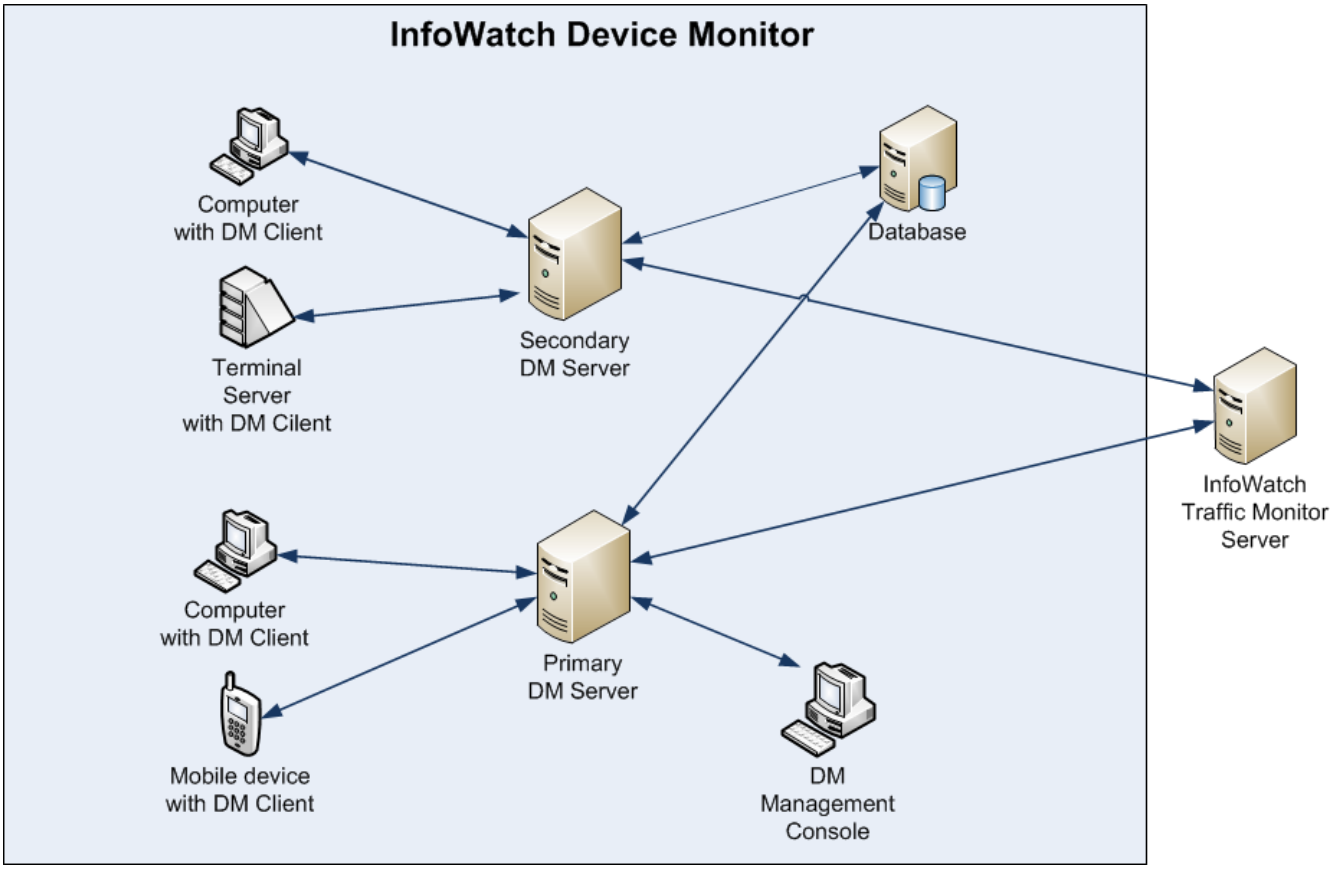
Peripherals access control	Peripherals access differentiation. Peripherals access differentiation is based on corporate security policy. You can configure different access levels to certain peripherals for different employee or computer groups
Print Monitor	InfoWatch Device Monitor client module interceptor. It is designed to monitor the activity associated with sending documents to print. See: *Interceptor*
Rendering print jobs	Rendering process that converts a print job into printing data.
Rule	Set of restrictions and conditions that monitor file operations on removable devices, network activity, printing, and configure access to managed peripherals. Each interceptor features a separate rule type. A rule can be only applied within its security policy. See: *Security Policy*
Security officer	Management Console role which manages security policy and configures InfoWatch Traffic Monitor server connection.
Security policy	Security schema parameter. A set of file monitoring rules for removable devices, network activity, printing and configuring peripherals access level. You can only assign security policy to a group (of employee or workstations.) Employee monitoring is based on access level. See: *Security schema*, *Access level*
Selector	Constant log record attribute. Describes affected object search. Selector parameter value depends on particular object and actions. See: *Log*
Server	See: *InfoWatch Device Monitor Server*
Servers Manager	Software module of InfoWatch Device Monitor intended for appointment the primary and secondary servers
Super user	Management console role with full InfoWatch Device Monitor management privileges. The purpose of this role is to configure Management Console after its installation; operation in emergency situations; deleting log records.
Security Schema	A set of configuration settings for monitoring employee actions controlled by InfoWatch Device Monitor. See: *Employee group*, *Workstation group*, *Security policy*
Terminal device	Devices, which are being connected to a terminal client
Thick terminal client	Workstation with a hard drive and installed software, which is connected to terminal server
Thin terminal client	Workstation without hard drive, which is connected to terminal server. Useful for information input and software GUI display.
Transaction	Mandatory log record attribute. Consists of one elementary action (step) or more. Transaction is completed only after all steps have been performed. Otherwise, transaction remains incomplete, and the System reverts to the state it had been in prior to transaction.
Transaction step	Elementary action within a transaction (for example, a transaction that adds a employee to employee group consists of a single step - adding employee to a group).
White list of applications	When the System is in active white lists operation mode then all application listed in the Application Monitor rule will be allowed to run for all employees for which this rule is active. Other applications will be forbidden to run. See: *Application Monitor*
White list of devices	List of fully accessible devices. See: *Device Monitor*

Windows account	Employee's Microsoft Windows account. Account credentials are used for InfoWatch Device Monitor registration.
YMSG	Network protocol used by the Yahoo! Messenger instant messaging client

2 Installing and Configuring InfoWatch Device Monitor

This section contains information on installing and configuring InfoWatch Device Monitor for those, who are familiar with the basics of Microsoft Windows administration and the database in use.

The following figure shows an example of system deployment.



InfoWatch Device Monitor deployment example

You can use clustering to enhance system performance. The same database schema will be used by multiple servers to store and distribute shared security schema.

Server and database can be hosted by a single computer. To increase system performance, it is recommended that you host the database and server on separate computers.

Management Console can only connect to the main server. From the Management Console you can manage all servers in the cluster.

Installation procedure:

1. InfoWatch Device Monitor Server End Setup.
   Server end consists of the following elements:
   - Database

- Device Monitor Server
- Device Monitor Management Console.

2. Installing InfoWatch Device Monitor Client End.
   Client is installed on each computer that should be controlled by InfoWatch Device Monitor.

System requirements are listed in the "Hardware and Software Requirements" section.

For information on System elements configuration, updating, or deleting, see:

- Configuring InfoWatch Device Monitor Server. Preparing to work with InfoWatch Device Monitor.
- Updating InfoWatch Device Monitor. InfoWatch Device Monitor components updating procedure.
- Uninstalling InfoWatch Device Monitor. Recommendations on uninstalling InfoWatch Device Monitor.

2.1 Hardware and Software Requirements

This section lists hardware and software requirements for each system component:

- Database
- InfoWatch Device Monitor Server
- InfoWatch Device Monitor Client
- Management Console
- Integration with Traffic Monitor Versions

2.1.1 Database

InfoWatch Device Monitor supports the following DBMS:

- Oracle Database 11

  Warning!
  It is necessary to use Oracle Client application with x64 digit capacity if the System is being installed on 64-bit server operating.

- Microsoft SQL Server 2005, 2008, 2012, 2014 (Express, Developer, Workgroup, Standard, Enterprise)
- PostgreSQL 8 or 9.

2.1.2 InfoWatch Device Monitor Server

InfoWatch Device Monitor Server software requirements:

- operating system (supports both x86, x64 and platforms):
  - Microsoft Windows Server 2003;
  - Microsoft Windows Server 2008;
  - Microsoft Windows Server 2008 R2;
  - Microsoft Windows Server 2012;
  - Microsoft Windows Server 2012 R2.
- DBMS client (only if Oracle usage is planned):
  - Oracle 10g R2 or higher.
  - Instant Client with ODBC drivers, ODP.NET (Oracle Data Provider for .NET 2.0). Both components should have the same version.

> **Note:**
> When installing 12g version, `tnsnames.ora` file parameters are being created during installation process. With version 10g R2 and 11g it is necessary to configure parameters of Device Monitor Server in `tnsnames.ora` file: see "Configuring ORACLE DBMS connection"

- additional programs:
  - Microsoft .NET Framework 4.0 or higher.

InfoWatch Device Monitor Server hardware requirements meet minimum OS requirements. Moreover there are following hard disk free space requirements:

- free space - at least 200 MB
- enough hard disk free space to keep intercepted copies if you don't use integration with InfoWatch Traffic Monitor system. You can change the directory for intercepted copies using XML-file (for more information see "<applicationSettings> section", parameter `ShadowCopyTempDir`)

2.1.3 InfoWatch Device Monitor Client

InfoWatch Device Monitor Client can operate in the following operating systems (supports both x86 and x64 platforms):

- Microsoft Windows XP Professional Service Pack 3 with all updates;
- Microsoft Windows Vista Service Pack 2;
- Microsoft Windows 7 Service Pack 1;
- Microsoft Windows 8 and 8.1;
- Microsoft Windows Server 2003;
- Microsoft Windows Server 2008;
- Microsoft Windows Server 2008 R2;
- Microsoft Windows Server 2012;
- Microsoft Windows Server 2012 R2.

> **Warning!**
> Client can be only installed in the above listed environments. We do not guarantee Client's correct interaction with other operating systems.
>
> Client installation in other environments may result in application or operating system malfunctions.

InfoWatch Device Monitor Client hardware requirements meet minimum OS requirements. Additionally:

- Minimum free hard disk space is 320 MB.

> **Note:**
> When installed applications load CPU and RAM, the following configuration is recommended for flawless system performance:
>
> - CPU Intel Core i3 or equivalent;
> - RAM 4 Gb;
> - HDD 50 Gb.

The InfoWatch Device Monitor Client supports installation onto the following models of mobile devices, Android OS versions and build numbers:

Device model	Android version	Build number
ASUS Nexus 7 2013 LTE (K009)	4.3.0	JLS36C
	4.4.2	KOT49H

	4.4.3	KTU84L
	4.4.4	KTU84P
Samsung Galaxy S3 (I9300)	4.3.0	JSS15J.I9300XXUGNK1
		JSS15J.I9300XXUGND2
Samsung Galaxy S4 (I9500)	4.3.0	JSS15J.I9500XXUEMK8
Samsung Galaxy S4 (I9505)	4.3.0	JSS15J.I9505XXUEMK9
		JSS15J.I9505XXUEML4
	4.4.2	KOT49H.I9505XXUGNG8
		KOT49H.I9505XXUFNC9
Samsung Galaxy S5 (SM-G900F)	4.4.2	KOT49H.G900FXXU1ANE2
		KOT49H.G900FXXU1ANK7

InfoWatch Device Monitor Client also supports devices on iOS platform: you can install InfoWatch Device Monitor Client on iPhone or iPad versions 8.0 - 9.0.2.

Warning!
Installing InfoWatch Device Monitor on iPhone or iPad is possible only if the device is jailbroken.

2.1.4 Management Console

InfoWatch Device Monitor Management Console can operate in the following operating systems (supports both x86 and x64 platforms):

- Microsoft Windows Server 2003;
- Microsoft Windows Server 2008;
- Microsoft Windows Server 2008 R2;
- Microsoft Windows Server 2012;
- Microsoft Windows Server 2012 R2;
- Microsoft Windows XP Professional Service Pack 3;
- Microsoft Windows Vista Service Pack 2;
- Microsoft Windows 7 Service Pack 1
- Microsoft Windows 8 and 8.1.

InfoWatch Device Monitor Management Console hardware requirements meet minimum OS requirements. Minimum free hard disk space is 35 MB.

2.1.5 Integration with Traffic Monitor Versions

InfoWatch Device Monitor has a set of features in integration with InfoWatch Traffic Monitor of different versions.

So with following versions integrating the listed interceptor's events will be transferred only:

To TM 4.1:

- IM Client Monitor: Skype, XMPP, MMP
- FTP Monitor
- File Monitor
- Print Monitor
- HTTP, HTTPS Monitor (proceeded and displayed as HTTP events)

To TM 5.1:

- IM Client Monitor: Skype, XMPP, MMP
- FTP Monitor
- File Monitor
- Print Monitor
- HTTPS Monitor (HTTP events are not accepted and not proceeded)
- Mail Monitor: MAPI, POP3, SMTP

To TM 5.4 and 5.5:

- IM Client Monitor: Skype, XMPP, MMP, YMSG
- FTP Monitor
- File Monitor
- Print Monitor
- HTTP, HTTPS Monitor
- Mail Monitor (MAPI, POP3, SMTP)

To TM 6.0:

- IM Client Monitor: Skype (excluding events of forbiddance or lack of acceptance of Skype plug-in usage), WhatsApp, YMSG, XMPP, MMP, SMS
- FTP Monitor
- File Monitor
- Print Monitor
- HTTP, HTTPS Monitor
- Mail Monitor: MAPI, POP3, IMAP, SMTP
- Application Monitor
- Cloud Storage Monitor
- Device Monitor (excluding events of access to "read-only" device, events of device inaccessibility, events of device connection)
- Network Monitor (excluding events of unauthorized server access attempts, events of temporary network connections enabling, events of entering the wrong validation code)
- Photo Monitor
- Print Monitor
- ScreenShot Control Monitor

So for InfoWatch Device Monitor 6.0 integrated with InfoWatch Traffic Monitor 6.0 the API connection with authorization token is provided.

Note:
The events of a free space shortage for the shadow copies are not transferred to the Traffic Monitor system.

The detailed description of each interceptor operation in Device Monitor see in "Adding a Rule" subsections.

2.2 InfoWatch Device Monitor Server End Setup

InfoWatch Device Monitor server end is installed with universal Setup Wizard.

Universal Setup Wizard disk is available on your System installation CD (`Setup.Unified` directory). This program lets you install all System components except the Client: database, Device Monitor Server, and Management Console.

The InfoWatch Device Monitor system can use Microsoft SQL Server or Oracle DBMS or PostgreSQL for managing

the database.

Management Console connects to the primary server.

For more information on installation, see:

- Database deployment under Microsoft SQL Server DBMS
- Database deployment under Oracle DBMS
- InfoWatch Device Monitor Server Setup
- InfoWatch Device Monitor Server End Installation Procedure

2.2.1 Database deployment under Microsoft SQL Server DBMS

You must install Microsoft .NET Framework 2.0 Service Pack 1 and Microsoft .NET Framework 4.0 or higher before launching database scheme generation on your computer.

Database generation account must be configured in advance. Account type depends on database server authentication. Microsoft SQL Server DBMS supports two types of authentication:

- **Windows authentication**. Authentication uses accounts within Windows domain. Authentication data is processed by Microsoft Windows security.
- **SQL Server built-in authentication**. Uses Microsoft SQL Server accounts. Authentication is carried out via DBMS.

Warning!
To ensure satisfactory safety level, we strongly recommend that you use **Windows authentication** method.

If you are going to use Windows authentication method:

1. Make sure Windows domain contains only one account that you will use for database generation. This account must have local administrator privileges on the computer used for database generation. If necessary, create a new account.
2. Add the account to Microsoft SQL Server DBMS and select **Windows authentication**.
3. Assign **dbcreator** role to the account.

If you plan to use SQL Server built-in authentication method:

1. Create a new Microsoft SQL Server account. When configuring an account: select **SQL Server built-in**, enter user name and password.
2. Assign **dbcreator** role to the account.

Note:
Integrated account name and password are specified when configuring the database (see "InfoWatch Device Monitor Server End Installation Procedure", step 6).

2.2.2 Database Deployment Under Oracle DBMS

You must install Oracle DBMS client and Microsoft.NET Framework 2.0 Service Pack 1 before launching database scheme generation on your computer.

Warning!
Due to OLE DB provider operational features, you must install only one client on source computer (i.e. it must have only one Oracle home work directory). This condition is obligatory for proper database installation.

Before you start creating a database scheme, make sure that **tnsnames.ora** file contains database server connection parameters (see "Configuring ORACLE DBMS connection").

2.2.2.1 Configuring InfoWatch Device Monitor Connection to Oracle DBMS Server

To ensure proper connection to Oracle DBMS server for each computer with Oracle DBMS client, you must configure `tnsnames.ora` file located in `[ORACLE_HOME]\network\admin` directory.

tnsnames.ora configuration

Specify Oracle DBMS server connection settings. To do this, add the following entry to `tnsnames.ora` file:

```
tns_name =
 (DESCRIPTION =
  (ADDRESS = (PROTOCOL = TCP)(HOST = host_name)(PORT = port_number))
  (CONNECT_DATA =
   (SERVER = DEDICATED)
   (SERVICE_NAME = service_name)
  )
 )
```

Specify true values for the following parameters:

- `tns_name` - Oracle DBMS server alias;
- `host_name` - Oracle DBMS domain name or IP address;
- `port_number` - server port for listening to client connections;
- `service_name` - database service name.

Example of `tnsnames.ora` file:

```
IWDM =
   (DESCRIPTION =
      (ADDRESS = (PROTOCOL = TCP)(HOST = iwdm.example.com)(PORT = 1521))
      (CONNECT_DATA =
          (SERVER = DEDICATED)
          (SERVICE_NAME = orcl)
      )
   )
```

Warning!
File `tnsnames.ora` is format sensitive. If you are copying the example to edit a file, make sure that copied selection do not contain any blank strings.

2.2.3 Server Setup Recommendations

To enhance system performance, we recommend that you deploy the server and database on separate computers.

Warning!
When deploying a multiple-server pool, each server must have the same InfoWatch Device Monitor server application version installed that is compatible with the appropriate up-to-date database.

To make the InfoWatch Device Monitor Server able to install the Clients onto mobile devices, the server should have a long name. If the used server is not in the Windows domain then you need to configure FQDN. To do this:

1. In the **System Properties**, on the **Computer Name** tab click **Change**.
2. In the **Computer Name/Domain Changes** dialog window click **More**.
3. In the **Change primary DNS suffix when domain membership changes** field enter the domain name.
4. Click **OK**.

5. Make sure that the **Full computer name** field displays the long name.

While configuring the Server (see "InfoWatch Device Monitor Server End Installation Procedure"), you must specify the account that will be launching InfoWatch Device Monitor Server. Available options:

- **Local System**. Launch service from system account.
- **User**. Launch service from Windows domain account.

For Microsoft SQL Server DBMS database. If you select **Windows authentification** for database owner (see "Database deployment under Microsoft SQL Server DBMS"), while database and Server are on separate computers, select **User** variant.

Warning!
It is not recommended to select **Local System** option. In this case, user can obtain unlimited rights, which contradicts the security policy.

Windows domain account (**User**) must be configured in advance. To do this:

1. Allow the account to run process as a service:
   a. In **Control Panel** open **Administration > Local security policy** .
   b. In the following dialog select **Local policies > Assign User Rights**.
   c. Double-click **Log on as service** in right **Details** pane.
   d. On **Local security parameter** tab add the account.
2. Add new account to Microsoft SQL Server DBMS account list.

When setup finishes, allow the account to create new databases. When specifying database access permission, select **db_owner** role.

2.2.4 Server End Installation Procedure

Warning!
Before starting installation, see "Server Setup Recommendations".

Warning!
When deploying a multiple-server pool, each of them must have the same InfoWatch Device Monitor server application version installed compliant with the appropriate up-to-date database.

Step 1. Running the Installation Wizard

Insert the installation CD into your CD-ROM drive. Then open `Server` directory. Run platform-specific setup file from this directory.

You will be redirected to InfoWatch Device Monitor Setup Wizard welcome screen. Click **Next**.

Step 2. Accepting the License Agreement

Read the End User License Agreement. If you accept the licensing terms, select **I accept the terms in the License Agreement** and click **Next**.

Step 3. Selecting components to install

Custom Setup page has all components selected by default:

- Server
- Management Console
- MSM module (Taiga) - component enabling Device Monitor Client installation to mobile devices (see details in "Mobile Devices"). Can be installed and used only together with the Management Console.

You can change the list of components you want to install. For example, if you want to use an existing Management Console with a new Server, you do not need to install this feature: click **Management Console** and select ✕ **Entire feature will be unavailable**.

You can also change the folder to install the component: select this component in the list, click **Browse** and specify the needed location.

Click **Next**.

Step 4. Configuring server settings

On **Type of installed server** page select:

- **Primary Server** - should be installed first. Clients and Management Console will connect to it.
- **Secondary Server** - additional server that balances Clients workload.

To ensure rapid server status updates it is recommended that you select **Publish Server in Active Directory** option.

> **Warning!**
> Workstations occasionally interact with Device Monitor server to update security policies. To let the newly added server handle workstations and notify the Clients about any possible server port changes it is recommended that you publish its details in domain during the installation.
>
> To publish Device Monitor data in domain, the account that installs the server needs privileges to create and delete connection points.

If you have the Device Monitor database of the appropriate version, deselect **Install new Database** option.

Click **Next**.

Step 5. Choosing configuration file

If the installation of the new database is not performed, this step is skipped.

To use the server configuration file exported before (see "Import/Export Configuration"), click **Open** and specify configuration file location.

> **Warning!**
> The configuration file should be placed on the local hard or external device. The Setup Wizard does not support network locations.

Click **Next.**

Step 6. Selecting database server

Specify DBMS that will control Device Monitor database by choosing one of the following options:

- Microsoft SQL Server
- Oracle
- PostgreSQL

If you don't want to install a new database (**Install new Database** option has not been selected in Step 4), you need to specify connectivity settings for existing Device Monitor database.

Click **Next**.

Step 7. Database configuration

You skip this step, if you chose to use an existing database in Step 4.

Database configuration depends on DBMS type.

If you are using Microsoft SQL Server DBMS, specify the following parameters:

- **Database server**. NetBIOS Microsoft SQL Server name where the database will be created.
  Do not enter IP address in **DB server** box, since this will prevent you from connecting to the database

server.

If there are any named instances on the database server, specify server name as follows: `<server_name>\<instance_name>`.

- **Database name**. New database name.

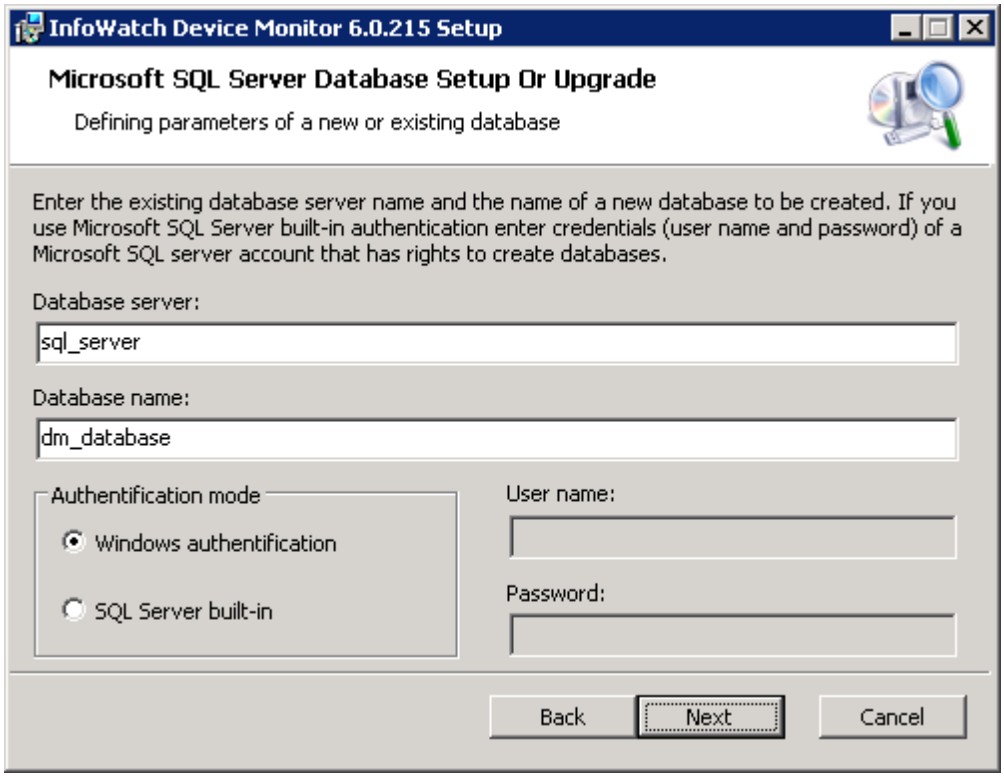
  It may contain Latin letters, numbers, and other characters except spaces and special characters: «*», «?», «/», «\», «|», «^», «:», «"". Name must start with a Latin letter.

  Name may be 1 to 123 characters long.

- **Authentication mode**. Database owner authentication method. For this option, specify the authentication method selected during account preparation (see "Database deployment under Microsoft SQL Server DBMS ").

  If the account uses Windows authentication, select **Windows authentification**. In this case, database will be created by the domain user, who runs the installation.

  If the account uses SQL Server authentication, select **SQL Server built-in**. Then enter user name and password into **User name** and **Password** fields respectively.



Configuring Microsoft SQL Server database

When using Oracle DBMS configure the following settings:

1. Set database server connection options:
   - **Database server**. Database server name. Use server alias from `tnsnames.ora` file for this parameter.
   - **The password of 'SYSTEM' login**. SYSTEM account password.
2. Specify the parameters of database scheme owner account:

   Warning!
   It is not recommended to use existing database scheme settings.

   - **Scheme owner**. Database scheme owner account name.
   - **Password**, **Confirm password**. Database scheme owner account password.

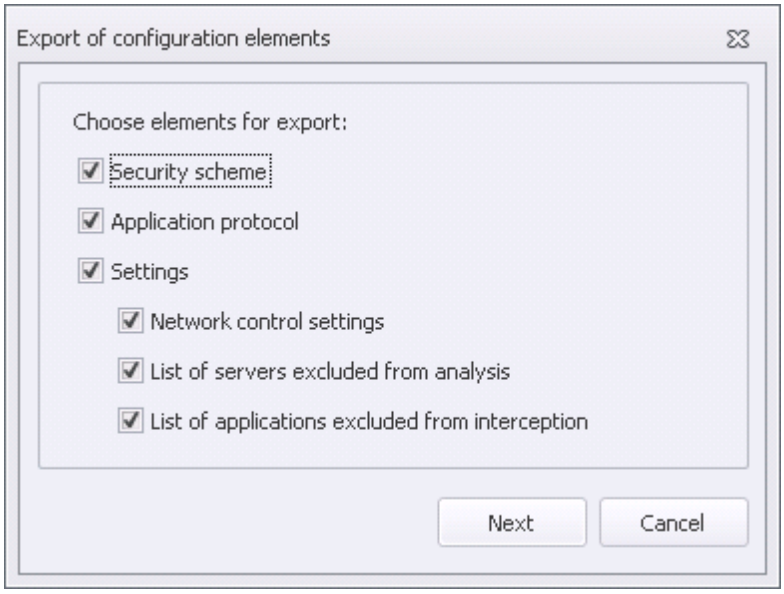
     Password is assigned basing on requirements specified in Oracle DBMS documentation.
3. Configure tablespace settings in **Tablespace** box.

   You can use existing tablespace or create a new one. If you are using existing tablespace, enter the tablespace name in **Name** field.

   To create a new tablespace, check the **Create new** box. Then specify tablespace options:

   - **Name**. Tablespace name.

- **File name**. Name of the file where the new tablespace will be stored.
- **Size**. Maximum size (in MB) of the data file (default size is 3000 MB).
- **Extent size**. Maximum size (in MB) of continuous segment in data file (the default size is 1 MB).
- **Autoextension**. Automatic file extension via Oracle DBMS. If **Autoextension** box is selected, automatic extension is enabled (this feature is disabled by default).



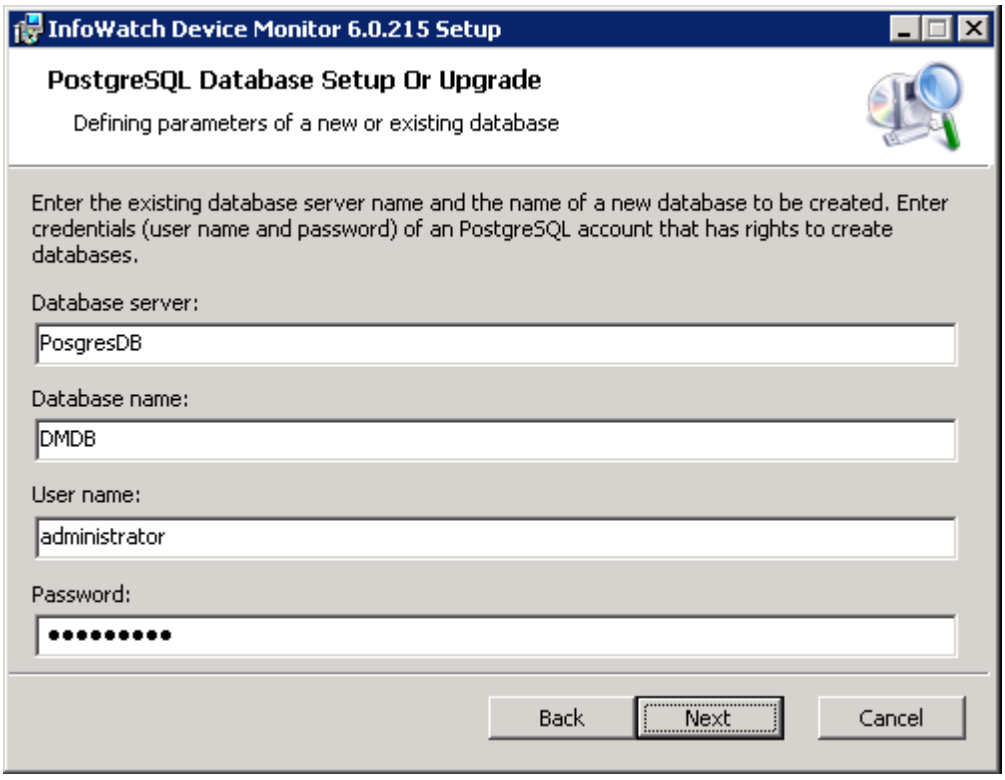
Configuring Oracle DBMS

When using PostgreSQL configure the following settings:

- **Database server**. The name of the PostgreSQL DBMS where the database will be created.
- **Database name**. The name of the newly creating database.

  It may contain Latin letters, numbers and other symbols excluding spaces and special symbols: «*», «?», «/», «\», «|», «^», «:», «"». Name must start with a Latin letter.

  Name may be 1 to 123 characters long.
- **User name** - the name of the account having rights for creating the DB on the PostgreSQL server.
- **Password** - the password of the account having rights for creating the DB on the PostgreSQL server.



Configuring PostgreSQL DB

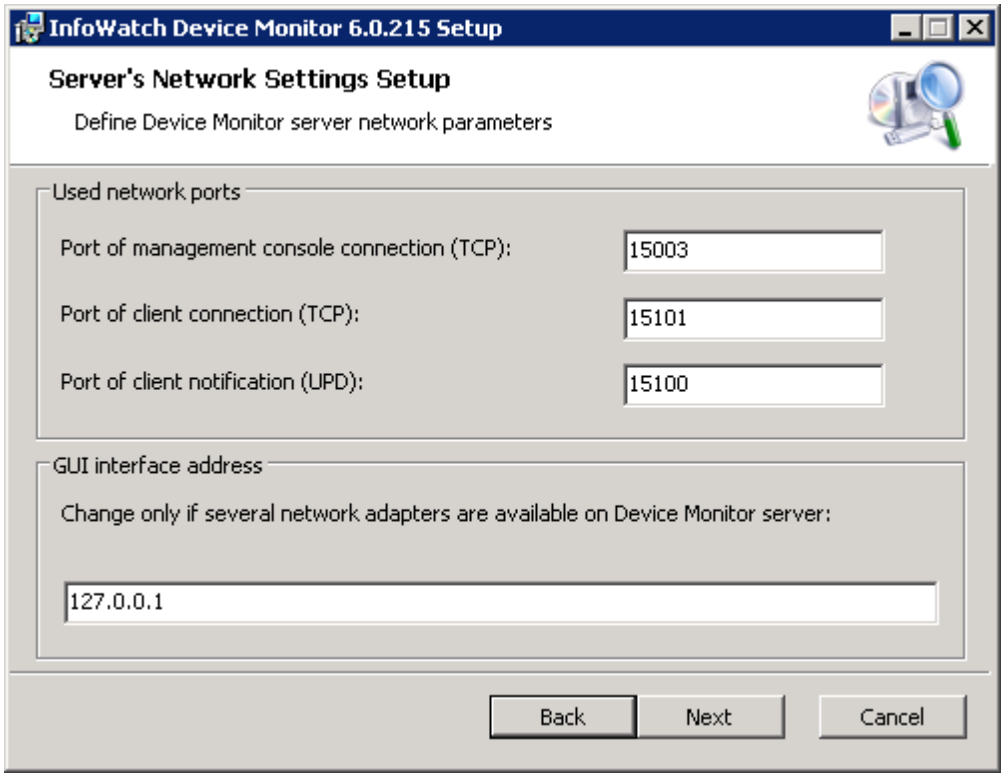
After all necessary parameters have been configured, click **Next**.

Step 8. Configuring the server

Configure Server parameters:

1. In **Used network ports** box set TCP and UDP ports used for:
   - **Management Console connection**;
   - **Clients connection** to transfer security schemas to managed workstations, send information about events and shadow copies to server;
   - **Clients notification** about security schema changes.
2. In **GUI interface address** enter the IP address that will be used for interaction between Server and Management Console.

> **Warning!**
> This value should only be changed if the Server is installed on a computer with multiple network adapters connected to different networks. If there is one network adapter, this value must remain unchanged, otherwise Management Console won't be able to connect to Server.
>
> If you add more network adapters while working with Server, you can change this setting in Server configuration file.



Configuring InfoWatch Device Monitor server parameters

After all necessary parameters have been configured, click **Next**.

Step 9. Configuring secure channel

Specify the port used for traffic transfer between the InfoWatch Device Monitor Client and Server.

If you install a new database (**Install new Database** option was selected in Step 4), then in **Secure channel key** area select:

- if you perform the first installation then leave the **Create new key** setting;
- if you used the server of version 6.0 or higher and deleted it and then you install it again, then to make Device Monitor Clients could connect and bind to the new server, you should specify the encryption key used on the

old server. The recommendations on saving the encryption key are listed in "Uninstalling InfoWatch Device Monitor". Select **Use existing key** and specify path to the file of the encryption key.

Click **Next**.

If you selected **Create new key** setting, specify the path where to the System will save file with key generated.

Step 10. Configuring server account

Select an account that will launch InfoWatch Device Monitor according to "InfoWatch Device Monitor Server Setup Recommendations". If you select **User**, specify Windows domain account name and password. Name is entered in `DOMAIN\USERNAME` format.

Click **Next**.

Step 11. Configuring server administrator account

Provide credentials (user name and password) for server administrator account. This will be a **Super user** account (for further details, see "Administration"): it is used when you first connect to the server from Management Console.

Click **Next**.

Step 12. Configuring InfoWatch Traffic Monitor connection parameters

Specify InfoWatch Traffic Monitor interaction options:

- **TM server address**. InfoWatch Traffic Monitor server address. Address must be entered in the following format:

  ```
  rpc://host:port
  ```

  Host parameter should contain domain name or IP address of InfoWatch Traffic Monitor server. The server address is the standard URI address (Uniform Resource Identifier) with its formal syntax described in RFC 3986 http://tools.ietf.org/html/rfc3986.

  Port parameter contains InfoWatch Traffic Monitor server port that delivers events. InfoWatch Traffic Monitor default server port is 4101.

  > **Warning!**
  > If you are going to integrate Device Monitor with Traffic Monitor 5.5 or earlier (those versions need `xml` format only) then you still need to specify `rpc`.
  >
  > Later during system configuration please change the **Connection string to a Traffic Monitor** field value using `xml://host:port` format – see details in "Device Monitor Server Settings. Connecting to Traffic Monitor Server".

- **Number of connections**. Number of InfoWatch Traffic Monitor server connections. You can specify from 1 to 32 connections.
- **Authorization token**. The token used for API connection. Required for Traffic Monitor v. 6.0 or higher. Please get this token from Traffic Monitor administrator.
- if System deployment scheme is not integrated with InfoWatch Traffic Monitor, select **Work in standalone mode** box. In this case, you can save captured shadow copies in server installation directory by selecting **Save shadow copies** box.

Click **Next**.

Step 13. Completing the installation

Click **Install** to start Server installation.

During installation the allowance to install Taiga System software will be requested. The allowance is needed to install drivers providing the support of mobile devices control. Click **Install**: otherwise the Wizard will finish its work prematurely and rollback the System installation.

Note:
This message will appear if at Step 3 "Selecting Components to Install" you have selected the **MSM module (Taiga)** component.

Follow the instructions to complete installation.

Warning!
Installing server end on Microsoft Windows Server 2012 or Microsoft Windows Server 2012 R2, you will see **Windows Security** dialog window, which installs InfoWatch virtual printer, required for processing printer jobs from metro-applications. To install virtual printer press **Install**.

Note:
Signature installation may take a while (up to 30 minutes).

2.3 InfoWatch Device Monitor Client Installation

InfoWatch Device Monitor Client can be installed to workstations in the following ways:

- Local Installation. It uses the Setup Wizard on each computer.
- Remote installation with third-party software. It uses software distribution tools: for example, Microsoft Active Directory group policy.
- Remote installation through InfoWatch Device Monitor Management Console expansion tasks.

InfoWatch Device Monitor Client is installed onto mobile devices when adding this device to the security schema:

- Adding a Mobile Device through Appointment to Employee
- Adding a Mobile Device to Computer Group.

Warning!
Turning off the computer during the installation/uninstallation process may lead to unstable operation of OS.

Warning!
For InfoWatch Device Monitor Client proper operation on computers with antivirus software installed, please disable antivirus self-protect function.

2.3.1 Standard Client Installation

Warning!
It is not recommend to install InfoWatch Device Monitor Clients on computers that have the same name. These computers will be registered as a single computer, affected by the same policies, and register the same events, etc.

Client can be installed by computer's local administrator.

Step 1. Running the Installation Wizard

Insert the installation CD into your CD-ROM drive. Then open `Client` directory. Run platform-specific setup file from this directory.

You will be redirected to InfoWatch Device Monitor Client Installation Wizard welcome screen. Click **Next** to go to

the next installation screen.

Step 2. Choose installation directory

Specify the path to Client installation directory.

Click **Next**.

Step 3. Configuring settings

Specify InfoWatch Device Monitor server connection settings:

- **Server**. InfoWatch Device Monitor server name.
- **Port**. Port number used for communication between InfoWatch Device Monitor Client and Server (port 15101 by default).

Click **Next**.

Step 4. Completing the installation

Proceed to **Confirm installation** screen and click **Next** to start Client installation. Follow the instructions to complete installation. Restart your computer to finish installation.

2.3.2 Client Installation via Software Distribution Tools

Corporate network administrator can perform Client centralized setup via software distribution tools. This section describes installation from Microsoft Active Directory.

Client installation from Microsoft Active Directory is carried out via group policy. To do so, you have to select a group policy that covers all target workstations. This policy may be assigned to:

- Active Directory container that holds all target workstations
- the whole Active Directory domain, but not default domain policy. This policy should only cover the group that includes all controlled workstations.

Step 1. Creating Installation Package

Create `Client.en.msi` installation package as described in "Creating Installation Package". Put the installation package to the network directory that can be ready by all target computers within the domain.

Step 2. Disable Microsoft Windows XP Professional fast logon option

Before you start client setup via group policies, disable fast logon optimization for computers with Microsoft Windows XP Professional OS (so-called asynchronous logon mode). For more details on this functionality see Microsoft Knowledge Base (see KB305293).

To disable the fast logon optimization feature:

1. Open the group policy editor.
2. In console tree, select **Computer Configuration > Administrative templates > System > Logon**. In details section, select **Always wait for the network at computer startup and logon**. Then set the value of this parameter to **Enabled** in properties screen.

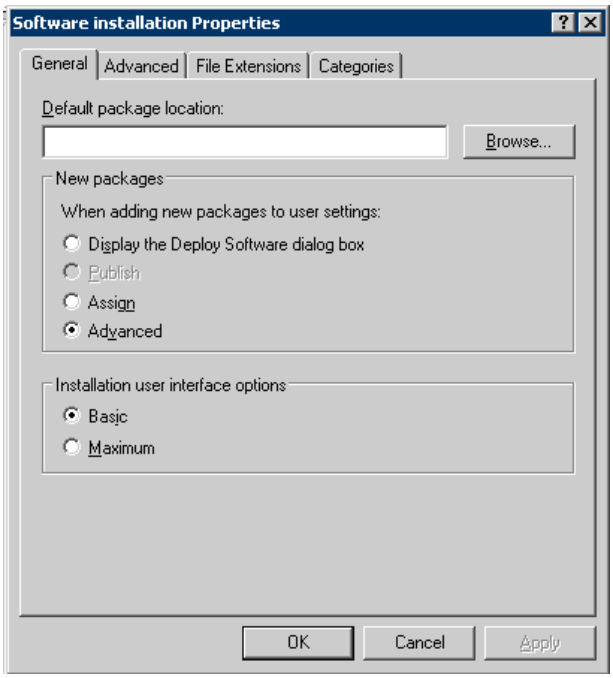
> **Note:**
> If this option has been turned off, you will need to reboot your computer again to let Windows group policy distribution mechanism finishes the installation.

Step 3. Editing Group Policy

Edit group policy before installing Client from Active Directory.

To edit group policy:

1. Open **Active directory users and computers** (**Start > Settings > Control Panel > Administrative tools > Active directory users and computers**).
2. In console tree, select Active Directory container with all target workstations.
3. Open **Group Policy**. To do this, click **Properties** in Active Directory container context menu. In the following dialog box, navigate to **Group policy** tab. On this tab, select group policy and click **Edit**.
4. In console tree, select **Software Installation** (**Computer Configuration > Software Settings**).
5. In **Software Installation** context menu select **Properties**. On **General** tab configure the following settings (see the following figure):
   - set **New packages** value to **Advanced**;
   - set **Installation user interface options** value to **Basic**.

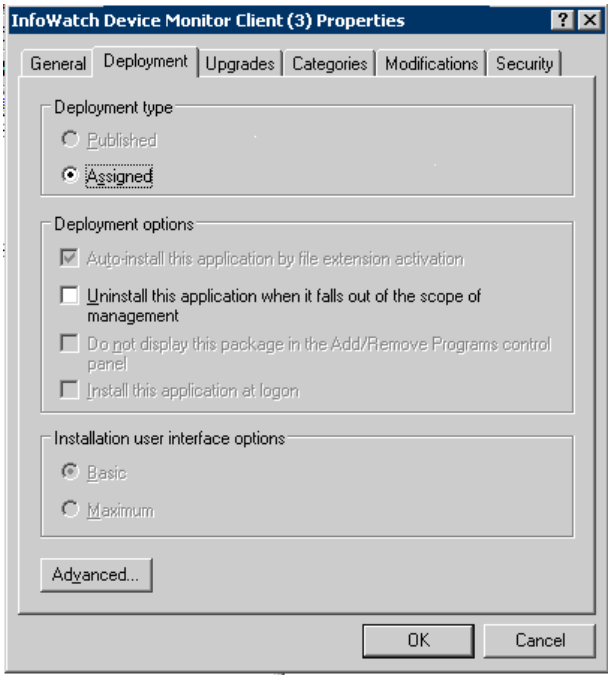


6. When the configuration is complete, click **OK**.

Step 4. Preparing Client installation task

Client installation task is created and configured on **Group Policy Object Editor** screen:

1. After opening **Group Policy Object Editor** box select **Software Settings** (**Computer Configuration > Software Settings**) in console tree. Right-click the selected item and then select **New > Package**.
2. In the following **Open** dialog specify client module installation package `Setup.Client.msi` (first move the installation package to a network directory that is readable for all installation-target computers within the domain).
3. Configure new package properties:
   - Make sure all settings in **Deployment** tab comply with the following figure.



- After all necessary settings have been configured, click **OK**.

4. In the console tree, select **Computer Configuration > Administrative templates > System > Scripts**. In details section, select **Run logon scripts synchronously**. Then set the value to **Enabled** in properties screen.

Step 5. Setup

New task appears in **Software Installation** task list. The task is carried out as soon as the target computer is restarted. InfoWatch Device Monitor Client starts automatically after its installation.

Installation method is displayed in **Deployment state** column. **Assigned** status means that installation is forced, i. e. doesn't need approval of target computer user. **Published** state means installation upon user's approval.

Warning!
You can check if the Client has been installed successfully in InfoWatch Device Monitor Management Console. All workstations the Client has been successfully installed to must appear in the list in **Workstations** area. To view all managed workstations, click **Show all workstations** at the top of Navigation Pane. To obtain up-to-date Client information, click **Update** in Toolbar.
If computer is not in the list, check for "*Group policy application failure on Windows XP with Service Pack 2 (SP2) computer*" error. For error description and troubleshooting go to Microsoft website: https://support.microsoft.com/en-us/kb/840669.

2.4 Configuring InfoWatch Device Monitor Server

Server is configured with `InfoWatch.DeviceMonitor.Server.exe.config` XML configuration file. Configuration file is stored in the same directory as Server executable file `InfoWatch.DeviceMonitor.Server.exe`.

By default, after its installation the Server is located in

```
C:\Program Files\InfoWatch\Device Monitor\Server.
```

You can view and edit configuration file with any text or XML Editor. UTF-8 File Encoding.

`<configuration>` is the root element of configuration file. Root element includes child elements (configuration sections). The following table contains configuration file structure and its partitions description. Section links provide detailed information on their configuration.

Warning!
It is extremely not recommended to edit the configuration file without InfoWatch engineer assistance.
When editing of file is finished, please restart Device Monitor Server.

Configuration section	Description
<configSections>	Service section. Describes all remaining sections. You should not edit this section.
<runtime>	Contains Microsoft .NET framework environment settings. These settings are required for correct Server operation. In `<runtime >` section the `gcServer` element is specified for garbage collector configuration. Element features `enabled` attribute with `true` (parallel garbage collection is enabled) or `false` value (parallel garbage collection is disabled). It is not recommended to edit this section.
<applicationSettings>	Contains individual Server modules settings, such as ports, buffer size, time-out, etc.
<system diagnostics>	Contains logging settings. Logging can be useful for Server components diagnostics.

If you need to delete temporary files generated by the System, you can do it by the special utility: see details in "Deleting Temporary Files".

2.4.1 <applicationSettings> Section

You can use `<applicationSettings>` section to configure individual Server modules. There are six modules. All sections have the same structure: Each section includes a set of elements for module configuration. Each `<setting>` element has the following attributes:

- `name` - setting name.
- `serializeAs`- data serialization method. Data is always serialized as a string (string data type).

Module parameters are defined by `<value>` child element. For example:

```
<setting name="RemotingPort" serializeAs="String">
   <value>15003</value>
</setting>
```

Each module parameters are described in the following table.

Parameter	Description
`<InfoWatch DeviceMonitor.Server.Core.Properties.Settings.>` Server kernel configuration	
`RemotingPort`	TCP port processing Management Console service connections. Default value `15003` (it is not recommended to change this value)
`CultureName`	Language of module diagnostic and other messages. Possible values: • `ru-RU` • `en-US`
`MachineName`	IP address of network interface used by the Server to accept Management Console connections. Default value `127.0.0.1`. You can only change this value, if the Server has 2 or more network interfaces. In this case, you must explicitly specify interface

Parameter	Description
	address used by the Server to accept incoming connections from different instances of Management Console
CheckServerSettingsInterval	With clustering enabled - database synchronization period (in seconds). After this, the Server sends a request to security schema in order to retrieve changes implemented by the main Server that uses the same database. Default value 10
<InfoWatch.DeviceMonitor.Server.Database.Properties.Settings> Settings of the module interacting with the database	
DatabaseType	Database types. Possible values: • Oracle • Microsoft • PostgreSql
ConnectionString	Database connection string. It must comply with ADO.NET connection string rules. For example: Data Source=isis\s2005;Initial Catalog=g1228_9;Integrated Security=
CultureName	Language of module diagnostic messages and other messages. Possible values: • ru-RU • en-US
ConnectionPoolSize	Number of DB connections to open and use by server. Default value 20
CommunicationPort	Port number used for server connection with Deploy agent when installing a Client through task engine. It is not recommended to change this value when operating. Default value 15505
UpdateStatusTimeOut	Time interval of updating the job execution state at remote computer. With this interval server survey remote computers where the Client is deployed about installation state to display on the Management Console. Default value 60
<InfoWatch DeviceMonitor.Server.Gui.Properties.Settings.> Management Console interface module configuration	
CultureName	Language of module diagnostic messages and other messages. Possible values: • ru-RU • en-US
InitialLeaseTime	Management Console valid connection time (in minutes)
RenewOnCallTime	Time (in minutes) to prolongate Console-Server connection lifetime.
<InfoWatch.DeviceMonitor.Server.Client.Properties.Settings> Client connections module configuration (managed workstations)	
Backlog	Pending client connections queue. Default value 128
CultureName	Language of module diagnostic messages and other messages. Possible values: • ru-RU • en-US
ShadowCopyTempDir	Full path to temporary shadow copies pending submission to InfoWatch Traffic Monitor.

Parameter	Description
	Default value: C:\Program Files\InfoWatch\DeviceMonitor\Server\ShadowCopyTempDir
DmpV1Adress	List of IP addresses (with enumeration separator "; ") used by server for listening to ports. The following values are possible: • AllAny - all ports of IP addresses available for the computer (default value); • AllIp4 - ports of all version 4 IP addresses; • AllIp4 - ports of all version 6 IP addresses.
Dmpv1TraceLevel	Client-Server protocol trace level. Possible values: • 1 - turn tracing off (default value); • 2 - only trace packet information; • 3 - complete tracing. **Note:** The tracing will be output to the listener of diagnostic messages (the Windows Log file by default) only of the setting value is 3 and log level fir the module filter is Verbose (see "<system.diagnostics> Section").
Dmpv1TraceClients	List of Client IP addresses (with enumeration separator "; ") that require tracing. All means that tracing is carried out for all Clients.
Dmpv1ConnectionsLimit	Number of simultaneously processed TCP/IP connections with Clients. Default value 200.
Dmpv1ConnectionsQueueLimit	Max number of connections awaiting for processing. If the number excesses, connections are reduced to Dmpv1ConnectionsQueueLengthAfterCut parameter value. Default value 500.
Dmpv1ConnectionsQueueLengt	Number of connections after queue reduced because of max size excesses. Default value 250.
TimeoutPeriodSeconds	Timeout to close hanged Client-Server connection: partially created shadow copies will be deleted, sending of shadow copies will be repeated in next established connection. Default value 120.
SSLPort	Port number for encrypted connections. Default value 15004.
<InfoWatch.DeviceMonitor.TrafficMonitor.Connector.Properties.Settings> Traffic Monitor Server connector basic configuration	
DBPollTime	Database query period (in milliseconds) checking for database events
CultureName	Language of module diagnostic messages and other messages. Possible values: • ru-RU • en-US
NumberOfConnections	Number of InfoWatch Traffic Monitor connections. Normal value 4. Maximum value 32
QueueSendLimit	Maximum number of events transferred from database to InfoWatch Traffic Monitor in a single transaction. Default value 200
ShadowCopyTrasferBlockSize	Size of shadowcopy data block sent to Traffic Monitor server, in MB. Default value 16.
<InfoWatch DeviceMonitor Database.Core.Properties.Settings> Low-level database driver configuration	

Parameter	Description
`CultureName`	Language of module diagnostic messages and other messages. Possible values: • `ru-RU` • `en-US`
`MaxConnectionWaitingTime`	Timeout for free connection from the pull, seconds. Default value `300`
`CommandTimeoutSeconds`	Runtime of the operation or queue, sec. Default value `30` **Note:** this setting is not applied for Oracle DBMS.
`LongCommandTimeoutSeconds`	Runtime of the long operation or queue, seconds. Applied when runtime is a vast interval. Default value `0` (endless). **Note:** this setting is not applied for Oracle DBMS.

2.4.2 <system.diagnostics> Section

Server diagnostics section. It includes the following elements:

- `<trace>`. Diagnostics module general settings.
- `<sources>`. Individual Server components diagnostics settings.
- `<switches>`. Managing diagnostic system's overall level of detail. Includes detalizer definitions. Typically, there is a single detilizer. If different modules require different detalisation settings, you should use a filter. General detalizer's value must contain maximum detail.

<*trace*> element

Used to describe global module diagnostics settings. In this element you can specify message margins and diagnostics data saving parameters.

<*sources*> element

Used to configure individual application modules. Includes `<source>` child elements - one for each application module (see Server module list in "<applicationSettings> section").

The list of modules also includes secondary ones which are needed for debugging output for main components:

- `InfoWatch.DeviceMonitor.Server.FileIdentification.Core` - module describing the signatures object model;
- `InfoWatch.DeploymentSubSystem` - module of the subsystem responsible for deployment on computers;
- `InfoWatch.DeviceMonitor.EventPostProcessorManager` - module for post-processing of print events;
- `InfoWatch.DeviceMonitor.ScreenShotStorage` - module for saving screenshots on the file system;
- `InfoWatch.DeviceMonitor.Server.Remote.Install` - module for launching the remote installation\update\uninstallation of the Agent on the computer.

`<source>` element has the following attributes:

- `name`. Server module name.
- `switchName`. Name of the module that defines diagnostics (detalizer's) level of detail.
- `switchType`. Type of the module that defines diagnosis level of detail. Is always set to `System.Diagnostics.SourceSwitch`.

Each <source> element also contains a definition for diagnostic messages receiver (`<listeners>`). Diagnostic messages can be received by:

- Windows application log (Application log);
- system debug output (can be viewed with special tools like DebugView);
- text file.

`<source>` element has child element `<listeners>`. This element contains parameters of diagnostic messages receiver. `<listeners>` element may contain the following child elements:

- `<add>`. Add a new diagnostic messages receiver

- `<remove>`. Deleting diagnostic messages receiver. You can only apply it to remove default message receiver (Windows application log). To this end, set element name to `Default`:

```
<remove name="Default" />
```

<*add*> element

This item adds diagnostic messages receiver to Server module. Element contains the following attributes:

- `name`. Diagnostic messages receiver name.
- `type`. Diagnostic messages receiver type.
- `initializeData`. Server module ID. Typically, this value is the same as Server module name. If Windows application log is the receiver, this information appears in the `source` column.

Receiver type is fully qualified receiver name from .NET framework library or proprietary type that implements the required diagnostic messages receiver interface.

.NET framework library contains the following diagnostic messages receiver types:

- `System.Diagnostics.EventLogTraceListener`. Windows application log
- `System.Diagnostics.ConsoleTraceListener`. Console application message output
- `System.Diagnostics.TextWriterTraceListener`. Text file output
- `System.Diagnostics.DefaultTraceListener`. Debug Windows output (enabled by default).

`<add>` element also contains diagnostic messages filter. This filter only displays the messages with level of detail exceeding the filter parameters. It features the following levels of detail (listed in descending priority order):

- `Verbose`. Debug level. All events are logged. This level can only be used for System debugging. This level does not allowed for a system running in normal mode, since it cuts the performance significantly.
- `Information`. Information level. Registers the events that are not related to errors, for example, information on server changes.
- `Warning`. Warning level. Registers non-critical System errors, such as an unexpected disconnection from the Server, connection timeout, etc.
- `Error`. Error level. Records errors that cause System malfunction (i.e., errors that require troubleshooting).
- `Critical`. Critical level. Registers serious malfunctions that can lead to System shutdown.

Example 1

Detalizer features *Verbose* logging level, while module filters feature *Warning* level. Then detalizer ignores *Warning* , *Error* and *Critical* events, but filters out *Information* and *Verbose* events.

Example 2

Detalizer features *Error* logging level, while module filters feature *Warning* level. In this case, detalizer ignores *Error* and *Critical* events, but filters out *Warning*, *Information* and *Verbose* events. This happens because overall System level of detail is *Error*, i.e. only *Error* events and higher are registered regardless the filter settings.

<*remove*> element

Deleting message receiver. It is usually used to remove default receiver that displays diagnostic messages in Windows debug output:

```
<remove name="Default" />
```

<*switches*> element

Defines Server detalizers. Typically, there is only one detalizer, which sets the global (for entire Server) level of detail the diagnostic system. If individual Server modules require lower level of detail, you can use filters.

`<switches>` element contains only one child element by default:

```
<add name="eventLog" value="Warning"/>
```

Level of detail is specified as `value` attribute.

2.4.3 Deleting Temporary Files

InfoWatch Device Monitor provides a means for deleting the files generated by the System, namely:

- all files from the temporary files directory of the operating system (%Temp%);
- data from file queue of Device Monitor events processing (`C:\Program Files\InfoWatch\DeviceMonitor\Server\ShadowCopyTempDir` by default; see information on the path configuring in "Configuring InfoWatch Device Monitor Server").

The deleting is performed by `RemShadowCopyFiles` utility located in the Server installation folder (`C:\Program Files\InfoWatch\DeviceMonitor\Server` by default).

The launching of the utility should be performed by administrator account having rights for reading and writing in directories containing deleting files.

Warning!

The System will stop the proceeding of incoming events for a time when deleting procedure runs.

The procedure will delete all the data on events which were not proceeded by the moment of deleting start.

To delete temporary files:

1. Log on at the InfoWatch Device Monitor Server where you need to delete temporary files.
2. Run `RemShadowCopyFiles` utility.
3. Confirm deletion by pressing **Y**.

The utility will stop all Device Monitor services, delete temporary files and start Device Monitor services again.

Warning!

When deleting temporary files from %Temp% system folder the access denial can arise: there can be some files created and used by another processes irrelevant to the System.

2.5 Updating InfoWatch Device Monitor

If you have InfoWatch Device Monitor installed, you can upgrade it to a later version.

System update is similar to its installation:

1. Updating InfoWatch Device Monitor Server End (database, server, and Management Console).

   Warning!

   If you want to upgrade System version 3.4 - 4.0, delete the old server version (don't remove the database) and re-install the server, configuring the connection to existing database. Starting version 4.0, updates use standard procedure.

2. Updating InfoWatch Device Monitor Client.

   System supports earlier Client versions starting build 3.4.875. Therefore Client is upgraded when needed.

Warning!

When upgrading the System version 6.0 by deleting and then installing the Server, you must perform the following actions to let Device Monitor Clients to connect to the new Server:

1. When deleting - save encryption key stored in DM Server installation folder, `SSLServerKey.pfx` file.
2. When installing - specify path to the saved encryption key used on the old Server.

2.5.1 Updating InfoWatch Device Monitor Server End

Warning!
If you want to upgrade System version 3.4 - 4.0, delete the old server version (don't remove the database) and re-install the server, configuring the connection to existing database.

Starting from version 4.0, the upgrading is fulfilled in the standard way.

Step 1. Start update

Insert the installation CD into your CD-ROM drive. Then open `Server` directory. Run platform-specific setup file from this directory.

You will be redirected to InfoWatch Device Monitor Installation Wizard welcome screen. Click **Next** to go to the next installation screen.

Step 2. Accepting the License Agreement

Read the End User License Agreement. If you accept the licensing terms, select **I accept the terms in the License Agreement** and click **Next**.

Step 3. Database configuration

Database is preserved during update, and **Configure Database Connection** box automatically displays old database parameters. However, depending on DBMS, you need to specify particular settings.

Built-in Database Update

Skip this step if you are using built-in DB.

Update Database Under Microsoft SQL Server DBMS

On **Authentication Method** panel, select authentication method for the user, who updates the database. For this option, specify the authentication method selected during account preparation (see."Database deployment under Microsoft SQL Server DBMS").

If the account uses Windows authentication, select **Windows authentication**.

If the account uses built-in SQL Server authentication, select **SQL Server built-in**. Then enter login and password into **User name** and **Password** fields respectively.

Note:
You can specify old or new authentication parameters as the upgrade proceeds. For guidelines on authentication methods and account preparation see section "Database deployment under Microsoft SQL Server DBMS".

Update Database Under Oracle DBMS

On **DB Server** panel specify **Password for 'SYSTEM'** - password for SYSTEM account that manages the database, which is being updated.

On **Scheme Information** panel, fill in **Password**, **Confirm password** fields - password for database scheme owner's account used for database update.

Update PostgreSQL Database

Enter the password of the account that manages the updated database into **Password** field.

After you have configured all parameters, click **Next**.

Step 4. Upgrade Completion

Go to the next screen and click **Install** to run System server upgrade.

Follow Setup Wizard's instructions to complete System server update.

2.5.2 Updating InfoWatch Device Monitor Client

The system supports Client versions starting from build 3.4.875. Therefore, updated system components can work with older Client versions. However, you can update to a later version.

Client update is similar to its installation:

- local update using Setup Wizard;
- remote update using software distribution tools;
- centralized update via Management Console.

In case you need to update Device Monitor Client on a large number of Workstations, you need to take the following steps:

1. Update client on a group of 10 Workstations. Make sure that there are no performance errors for 2-3 days.
2. Update client on a group of 50 Workstations. Make sure that there are no performance errors for 2-3 days.
3. Update client on a group of 500 Workstations. Make sure that there are no performance errors for 2-3 days.
4. Update client on a group of 1000 Workstations. Make sure that there are no performance errors for 2-3 days.
5. Complete the update procedure with the rest of the Workstations.

2.6 Uninstalling InfoWatch Device Monitor

Warning!

If you are planning to install the Device Monitor Server again, then to make Device Monitor Clients could connect and bind to the new server, then starting from version 6.0 you must save the encryption key of the old server.

The encryption key is stored in the installation folder of the InfoWatch Device Monitor Server, `SSLServerKey.pfx` file.

To remove InfoWatch Device Monitor server end with Management Console:

1. Take one of the following steps:
   - Open `Setup\Unified` catalogue on the Installation CD. Run platform-specific setup file from this directory.
   - Run **Uninstall or remove a programs** from Windows Control Panel, select **InfoWatch Device Monitor** and click **Change**.

   You will be redirected to Installation Wizard welcome screen. Click **Next** to move to the next screen.
2. On **Change, repair or remove…** screen select **Remove**.
3. To remove the system and its database, flag **Remove database** on **Remove database…** screen. Then specify parameters for uninstalling: parameters depend on your DBMS:
   - **Integrated DB (CompactSQL)** – doesn't require additional parameters: **Database** string contains the removed DB file.
   - **Microsoft SQL Server** – specify your authentication method by selecting it in **Authentication Method** pane (see "Database deployment under Microsoft SQL Server DBMS").

     In case of SQL-server based authentication (**Integrated into SQL Server**) enter the credentials you used to connect to the database in **Login** and **Password** boxes of **Database Administrator** pane.
   - **Oracle** – enter the password into **The password of 'SYSTEM' login** box. This will remove database scheme owner account and all its objects except the tablespace.
   - **PostgreSQL** – enter the credentials used to create the DB during server setup into **User name** and **Password** boxes (see "InfoWatch Device Monitor Server End Installation Procedure").

Note:
If the database is not working or working partially, then to delete the InfoWatch Device Monitor you should uncheck the **Remove database** field, otherwise the deletion can be performed incompletely.

4. After specifying the parameters click **Next** and then click **Remove** to start uninstallation.

To remove only InfoWatch Device Monitor server end or Management Console:

1. Run **Add or remove programs** and click **Change**.
2. In **Custom Setup** click  to the left of the elements you want to remove and select **Disable this element**. Click **Next**.
3. If you selected server uninstallation at the previous step, specify whether you want to remove the database and enter the authorized account parameters, if necessary, on **Remove database…** screen (see details above).
4. Click **Change** to start uninstallation.

To remove InfoWatch Device Monitor Client:

run **Add or remove programs**, select **InfoWatch Device Monitor Client** and click **Remove**.

You can also use centralized uninstallation to remove Clients:

- with Active Directory tools (if Clients were installed via software distribution tools) as described in "Remove Client Installed via Software Distribution Tools".
- with Management Console distribution tasks, as described in "Clients Remote Setup, Updating and Uninstallation".

Warning!
Turning off the computer during the installation/uninstallation process may lead to unstable operation of OS.

The order of deleting the Clients from mobile devices is described in "Deleting the Mobile Device".

2.6.1 Removing Client Installed via Software Distribution Tools

If client was installed via software distribution tools, you can use them to remove it.

For example, if Clients were installed via Microsoft Active Directory, corporate network administrator can use group policy to remove the installation task. Group policy editing procedure is described in "Client setup via software distribution tools", step 3.

To remove Client from all managed workstations:

1. Select the installation task you want to remove. Then right-click the selected row and select **All tasks > Remove**.
2. Select **Remove software** in **Immediately uninstall software from users and computers** dialog.

   Note:
   Other options remove installation task without uninstalling all existing Clients. After that you won't be able to remove these Clients with Microsoft Active Directory tools.
3. Click **OK**.

Client will be removed from all computers under selected group policy.

3 Using Management Console

The Management Console is designed to address the following tasks:

- access to InfoWatch Device Monitor;
- configuring computers monitoring system;
- computers access control.

To use Management Console you have to be familiar with Microsoft Windows OS basics.

For more information on Management Console workflow see:

- Management Console Overview. InfoWatch Device Monitor general actions (startup, interface configuration).
- Managing Console Accounts. How to perform InfoWatch Device Monitor administration tasks: managing InfoWatch Device Monitor Management Console accounts, working with log, etc.
- General System Settings. Defining global settings which are common for all rules and policies.
- Managing Security Schema. How to use security schema and configure security settings.
- Viewing Events. Viewing information on managed devices and channels of data transfer on the managed computers.
- Clients Remote Installation, Updating and Uninstallation. InfoWatch Device Monitor Client installation and configuring via Management console.
- Additional Features. Secondary functions enhancing InfoWatch Device Monitor Management Console user experience: records filtering, grouping and sorting, Management Console shortcuts.

3.1 Management Console Overview

Management Console basics are available in the following subsections:

- Authorization and Connecting to InfoWatch Device Monitor Server
- Management Console Main Screen
- Management Console Sections

3.1.1 Authorization and Connecting to InfoWatch Device Monitor Server

Management Console requires constant connection to InfoWatch Device Monitor Server. This can be accomplished through **authorization** that defines, if user has access to Management Console.

First launch of Management Console uses account credentials (user name and password) of **Super user** account (super user account is created during Server installation; for more details see "InfoWatch Device Monitor Server End Installation Procedure").

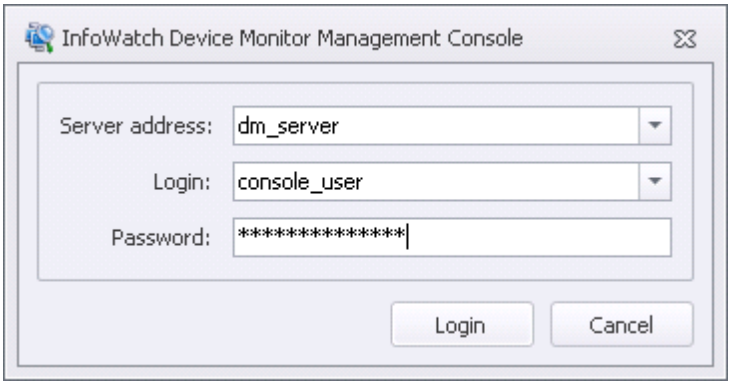
To get started with Management Console:

1. Launch Management Console. To do this, select **Start Programs > InfoWatch > Device Monitor > Management Console**.
2. Perform authorization as described below.

Successful authorization is only possible upon meeting all of the following conditions:

- database contains an account with specified parameters;
- account has a role;
- account is active (not deleted);
- account is not blocked.

Credentials are entered in logon dialog.



Parameter	Description
Server address	FQDN of the server Management Console is connecting to. Default communication port for server and Management Console is `15003`. If this port has been changed, enter server address as follows: `dm_server:port`.
Login	Name of the user account
Password	User password. Check the keyboard layout before entering your credentials.

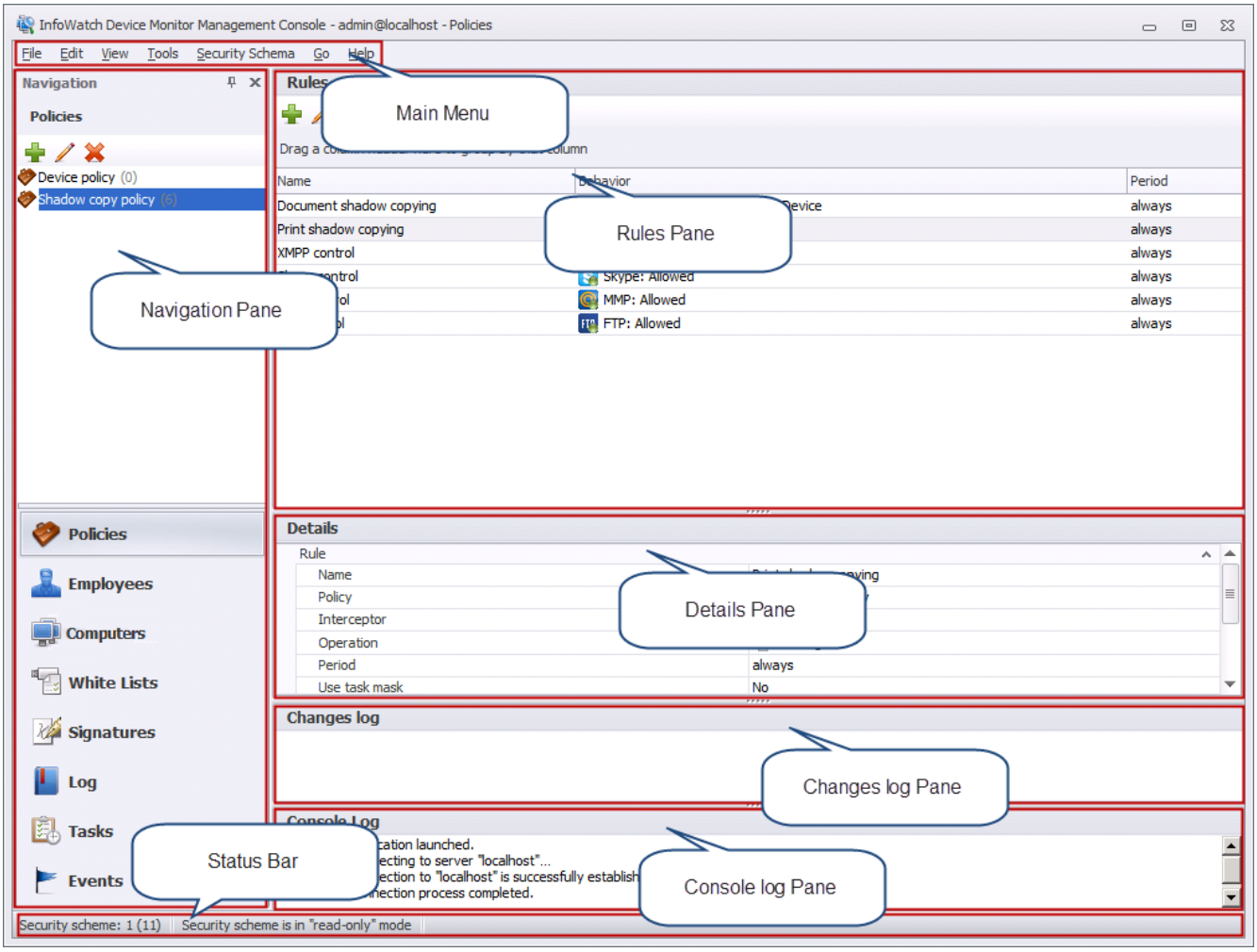
At the first launch of Management Console logon dialog fields are empty. Later, **Server address** and **Login** fields will contain the credentials entered during the previous authorization attempt. You must fill the **Password** field each time you are trying to log in.

You can track server connection status via system messages on **Console log** panel (see "Management Console Main Screen").

If you need, you can open authorization box and change your parameters: this connects you to the same or another server using any account. To do this, in the Main Menu select **File >** **Connect**, then connect to the Server as described above.

3.1.2 Management Console Main Screen

Successful Management Console authorization redirects you to the main screen:



For information on main screen customization see "Configuring Management Console Main Screen Elements".

Main screen contains the elements required for Management Console operation:

- **Main Menu** contains the commands that give you access to all Management Console essential features.
- **Navigation pane** lets you move between Management Console sections and manipulate elements groups within a section.
- **Main screen workspace** is intended for reviewing and managing group elements.
- **Toolbars** contain shortcuts to some of the Management Console features. There is a toolbar on the Navigation pane (for elements of a selected section) and one in the Main screen workspace (for selected element of the section).
- **Details** pane displays selected element's properties.
- **Changes log** pane displays all unsaved changes made by current user.
- **Console log** pane displays system messages.

If you are working with a single object, most commands are available in context menu. To open the context menu, right-click the object.

General status information is displayed on **status bar** at the bottom of the main screen. For example, the following information is displayed:

- current security schema version number;
- security schema mode;
- in **Computers** section - control elements versions.

3.1.2.1 Configuring Management Console Main Screen Elements

You can customize the appearance and location of **Navigation**, **Details**, **Console log** panes.

Action	Steps
Hide pane	• Click **View** in the Main Menu and click on the bar title you want to hide. To open the pane again, repeat this step. or • Click ⊠ in the upper right corner of the pane.
Enable/disable pane automatic collapse	Click 📌 in the upper right corner of the pane.
Change pane location	Click on the pane name and drag the pane to a new location. Release the button to place the pane.
Return the pane to its original position	Double-click the title bar
Change panel size	Move the pointer to the edge of the panel. When the pointer turns into a double arrow, click and hold to drag the margin into the right direction. Release the button when the size is right.

Details panel displays individual element properties. You can collapse or expand property table for any item.

To customize Details panel,
double-click properties table title bar or use double-arrow button in the right part of the properties table header.

To hide/display toolbar or Status panel,
right-click on toolbar or status panel. In context menu, flag the elements that will be displayed (all the elements are flagged by default).

3.1.3 Management Console Sections

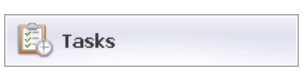
Management Console includes the following sections: **Policies**, **Employees**, **Computers**, **White Lists**, **Signatures**, **Log**, **Tasks** and **Events**. Each section corresponds to similar Navigation panel area.

To go to the section, do any of the following:

- in the Main Menu select **Go**. In drop-down menu, click on the section title;
- use Navigation panel buttons.

Sections **Policies**, **Employees**, **Computers**, **White Lists** and **Signatures** designed for managing the security schema, **Log** section for monitoring security schema management, **Tasks** - for managing Client installation and uninstallation tasks, **Events** - for viewing the events on managed computers. Detailed description of section functions is available in the following table:

Section icon and name	Section assignment
	Security policy management: creating security policies, setting policy rules
	Employee management: creating employee groups, adding employees to groups
	Computers management: creating computer groups, adding managed computers to groups

Section icon and name	Section assignment
	Managing white lists of fully accessed devices.
	View and manage signature categories that assign File Monitor rules to certain file formats.
	Application protocol and creating application lists to permit or forbid applications start.
	Security schema management activity log (logging administrating responsibility zones and configuring security schema)
	InfoWatch Device Monitor Clients centralized installation, updating, and uninstallation on computers
	Viewing information on employee activities at managed computers using controlled means

3.2 Managing Console Accounts

The system registers a Management Console account for each security schema operator. Account credentials are used for user authorization and access to certain operations.

Management Console authorized users' rights are defined by their **roles**. Each role features a set of responsibility zone privileges. User cannot perform actions outside the assigned role.

Management Console uses the following roles to manage user privileges:

- **Security officer** - Console end-user managing security schema and Server settings.
- **Local administrator** - Console administrator managing other accounts.
- **Super user** - built-in role which have all Console privileges. Superuser role is not designed for routine System operations: it is recommended to use it only for primary Console configuring, Local administrator account creating and then - just in emergency cases.

The following table lists roles privileges.

Action	Super user	Local administrator	Security officer
Management Console first launch and configuration	+		
Work in emergency situations	+		
Unlocking security schema	+		
Viewing audit log	+		+
Export audit log records	+		+
Deleting audit log entries	+		
View Management Console accounts information	+	+	+
Add, edit, delete Management Console accounts	+	+	
Assign/delete Management Console account roles	+	+	
Block/unblock Management Console accounts	+	+	
Viewing Device Monitor Server settings. Configuring connection to Traffic Monitor server	+		+
View security schema versions	+		+

Edit security schema	+		+
Import/export security policies and rules	+		+
Viewing events	+		+
Clients Remote Installation, Updating and Uninstallation	+		+
Temporary Employee Access to Network	+		+
Temporary Employee Access to Devices	+		+

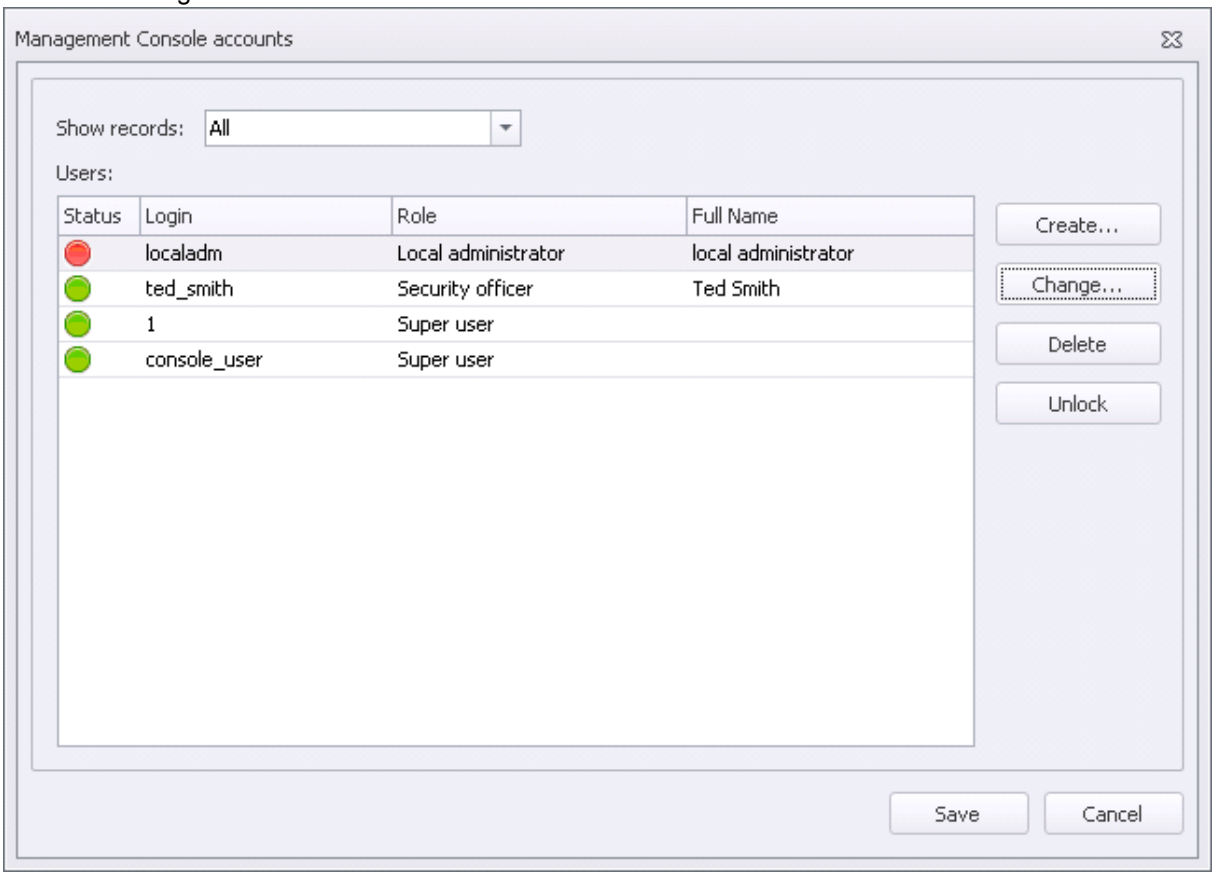
For more information on Management Console accounts management, see:

- Viewing Management Console Account Details
- Add Management Console account
- Locking or Unlocking Management Console Account
- Editing Management Console Account
- Deleting Management Console Account
- Management Console Security Schema Operation Activity Log

3.2.1 Viewing Management Console Accounts Details

To view Management Console accounts information:

1. In the Main Menu click **Tools > Management Console accounts**. This opens **Management Console Accounts** dialog box.



2. There is Show records field at the top of the dialog box. Select displayed accounts type in from the drop-down list:

- **All**. All accounts regardless of their status.
- **Active**. List of all active accounts.
- **Blocked**. List of accounts, which were blocked but can be unblocked (see "Locking or Unlocking Management Console Account").
- **Deleted**. List of accounts which were deleted and cannot be restored. However the System saves an information about actions those users performed.

> **Note:**
> Management Console can be only operated by the accounts in **Active** list. Deleted accounts can only be viewed.

Management Console account information is displayed as tabular list. Each row contains a single account. Columns contain the following account attributes values:

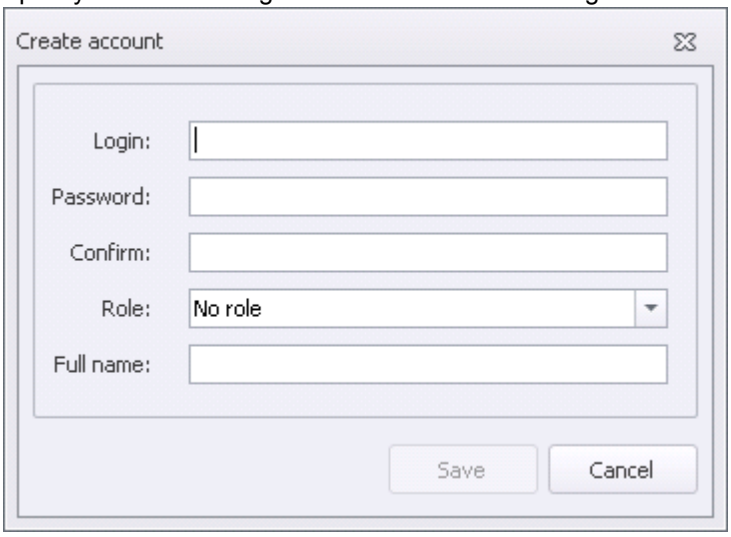
- **Status**. Indicates is an account is active ( ), blocked ( ) or deleted ( ).
- **Login**. Name of the user account.
- **Role**. Account role.
- **Full Name**. User's personal data.

Login and password, as well as account role and status are mandatory attributes. Detailed roles' description is available in "Management Console Accounts Administration".

3.2.2 Adding New Management Console Account

To add Management Console account:

1. In the Main Menu click **Tools > Management Console Accounts**.
2. Click **Create** at the right of **Management Console Accounts** dialog box.
3. Specify account settings in **Create account** dialog box:



- **Login**. Name of the user account.
- **Password**, **Confirm**. Account password.
- **Role**. Role assigned to the account. For more information on roles see "Management Console Accounts Administration".

> **Warning!**
> Role **parameter** is set to **No role** by default. You won't be able to authorize in Management Console with this account.
> Each account can have only one role.

- **Full name**. Personal information about account owner.

4. Click **Save**.

This close **Create account** dialog box. A new account details will be displayed in **Management Console Accounts** dialog box.

Note:
New account is not locked. You can lock the account, if necessary (see "Locking or Unlocking Management Console Account").

3.2.3 Locking or Unlocking Management Console Account

Account lockout is displayed in **Management Console Accounts** dialog box.

Warning!
You can lock any account except Superuser or the account you are logged in with.
You cannot log in with locked account.

To lock/unlock Management Console account:

1. In the Main Menu click **Tools > Management Console Accounts**. This opens **Management Console Accounts** dialog box.
2. Select the row that contains the account name.
3. Change account's lock status:
   - if the account has been locked (state), click **Unlock**.
   - if the account is unlocked (state), click **Lock**.
4. Click **Save** to apply changes.

3.2.4 Editing Management Console Account

Warning!
Editing a role of Management Console authorized account leads to the following: After you save the changes, connection to server is automatically terminated. Then you are prompted to authorize with your new settings. However, all your unsaved data will be lost.

To edit Management Console account:

1. In the Main Menu click **Tools > Management Console accounts**. This opens **Management Console Accounts** dialog box.
2. Select the row that contains the name of the account you want to edit.
3. Click **Change** at the right of the dialog box or double-click the highlighted row.
4. In **Change account** dialog box edit account settings, as described in "Adding New Management Console Account").
5. After all necessary settings have been configured, click **Save**.
6. To apply changes, click **Save** in the **Management Console Accounts** dialog box.

3.2.5 Deleting Management Console Account

Deleted account is moved to deleted accounts list. Account information remains in the database. You can view deleted accounts in **Management Console Accounts** dialog box. To do this, select **Obsolete** in **Accounts** drop-down list.

Warning!
Superuser account could not be deleted.
Deleted accounts cannot be recovered.

To delete Management Console account:

1. In the Main Menu click **Tools > Management Console Accounts**. This opens **Management Console Accounts** dialog box.
2. Select the row that contains the account you want to remove.
3. Click **Delete** at right of the dialog box.
4. In the confirmation dialog select **Yes**.
5. To apply changes, click **Save** in the **Management Console Accounts** dialog box.

3.2.6 Management Console Security Schema Operation Activity Log

Management Console operation involves various security schema managing activities. Records related to activities that change database information (security schema customization, System administration) are stored in the Audit Log.

For information on Audit Log see:

- Viewing Log
- Log Records Filtering
- Deleting Records from Log
- Exporting Log Records
- Analyzing Log Records in Microsoft Excel

3.2.6.1 Viewing Audit Log

You can manage audit log of Management Console users activities in **Log** section. To go to this section, click **Log** button on **Navigation** pane.

Security schema management activities are performed as transactions. Transactions appear as a set of records in the audit log. Each record contains information on one basic action (transaction step). Transaction may only contain one step and will be represented by a single record in audit log.

Configure filters to select records that meet certain criteria (for information on filters see "Log Records Filtering"). Filter list is displayed in **Log** area of Navigation pane. Records for selected filter are displayed in the main screen workspace.

Note:
Use additional options to adjust audit log records display (see "Additional Features").

To view full list of audit log records,

click **Show All Records** at the top of Navigation Pane.

To view filtered records,

click the filter name in the filter list.

Log information is displayed in a tabular list where each row contains a single record. Columns contain basic properties of log entries. Extended information on each record is available in **Details** panel.

To view advanced information for particular record,

select the row that contains the record name in the main screen workspace.

Details panel displays properties table containing the following information for selected entry:

Property	Description
Transaction number (#)	Transaction number
Step	Basic action number within selected transaction
Date and time occurred	Action date and time
Object	Target object name
Action	Activity type
Object selector	Contains information that helps identify the target object. **Selector** values interpretation see in "Selector Values".
Field name	Object attribute changed by the action
Old value	Previous value of the attribute
New value	New value of the attribute
User	Name of Management Console account that initiated the transaction
Windows account	Account with credentials for Windows authorization
Computer	Name of the computer that initiated the action
Sequence number	Record number in the database

Some information from the **Details** panel is duplicated in the main screen workspace.

Number of transaction steps (and, therefore, number of log records) varies depending on the object and actions performed.

For example:

The image contains a few log records referring to different transactions.

#	Step	Date and Time ...	Object	Action	Object Selector	Field Name	Old Value	New Value	User	Seq...
10	1	5/29/2012 10:17...	Rule	Add	4/Device policy/Floppy control	Active since		1/1/1753 12:00:00 AM	1	38
10	2	5/29/2012 10:17...	Rule	Add	4/Device policy/Floppy control	Active until		12/31/9999 11:59:59 PM	1	39
10	3	5/29/2012 10:17...	Rule	Add	4/Device policy/Floppy control	Operation		Floppy: Full Access	1	40
10	4	5/29/2012 10:17...	Rule	Add	4/Device policy/Floppy control	Allow only to en...		No	1	41
10	5	5/29/2012 10:17...	Securit...	Add	4/Floppy read-only for Device Policy	Comment		Floppy read-only for Device P...	1	42
9	1	5/29/2012 9:54:...	Log	Export	Object in (Rule, Policy)				1	37
8	1	5/29/2012 9:49:...	Rule	Change	3/Device policy/CD/DVD Access	Operation	CD/DVD: Full Ac...	CD/DVD: Read Only	1	35
8	2	5/29/2012 9:49:...	Securit...	Add	3/CD/DVD read-only for Device Policy	Comment		CD/DVD read-only for Device ...	1	36

Transaction number 3 is associated with adding a comment to security schema.

Transaction number 4 corresponds to one change applied to a security schema. This was done in 9 steps. Steps 1-3 changed rule named "*New IM client rule*" in "*Test Policy*" security policy. Each step configures a single rule parameter: for example, in step 1 an operation was defined, in step 2-3 an action period was set. Steps 4-7 added a new rule, step 8 deleted another one. In step 9 a comment was added to saving security schema version.

Transaction number 5 is associated with Audit Log records export. This transaction includes one step.

3.2.6.1.1 Selector Values

Selector parameter contains instructions for target object search. **Selector** parameter value depends on particular object and performed actions. Each object has a different set of **Selector** values.

Edited security schema version is displayed for modified security schema settings followed by "/" and name of modified parameter.

When editing an object (action **Modify**) **Selector** value contains object name before modification.

The following are sample interpretations of *Selector* values.

Example 1

Audit Log includes the following record:

#	Step	Date and Time Occurred	Object	Action	Object Selector	Field Name	Old Value	New Value	User	Sequence ...
7	1	5/28/2012 3:42:42 PM	Policy	Add	2/New Policy	Policy		New Policy	1	17

This record indicates that a rule was changed in your security schema.

Selector value interpretation

Transaction took place while version 10 of security schema was active. A rule named *"New IM client rule"* was changed in policy named "*test(new)":* Skype access was denied.

Example 2

Audit Log includes the following record:

#	Step	Date and Time Occurred	Object	Action	Object Selector	Field Name	Old Value	New Value	U...	Sequence...
8	1	5/29/2012 9:49:22 AM	Rule	Change	3/Device policy/CD/DVD Access	Operation	CD/DVD: Full Access	CD/DVD: Read Only	1	35

This record is a step of transaction which adds a computer group to the security schema.

Selector value interpretation

Transaction took place while version 3 of security schema was active. The *"Device"* policy was assigned to new computer group.

Example 3

Audit Log includes the following record:

#	Step	Date and Time Occurred	Object	Action	Object Selector	Field Name	Old Value	New Value	User	Sequence Number
9	1	5/29/2012 9:54:04 AM	Log	Export	Object in (Rule, Policy)				1	37

This record indicates that audit log records were exported.

Selector value interpretation

All records for operation on policy and rules were exported during this transaction.

3.2.6.2 Log Records Filtering

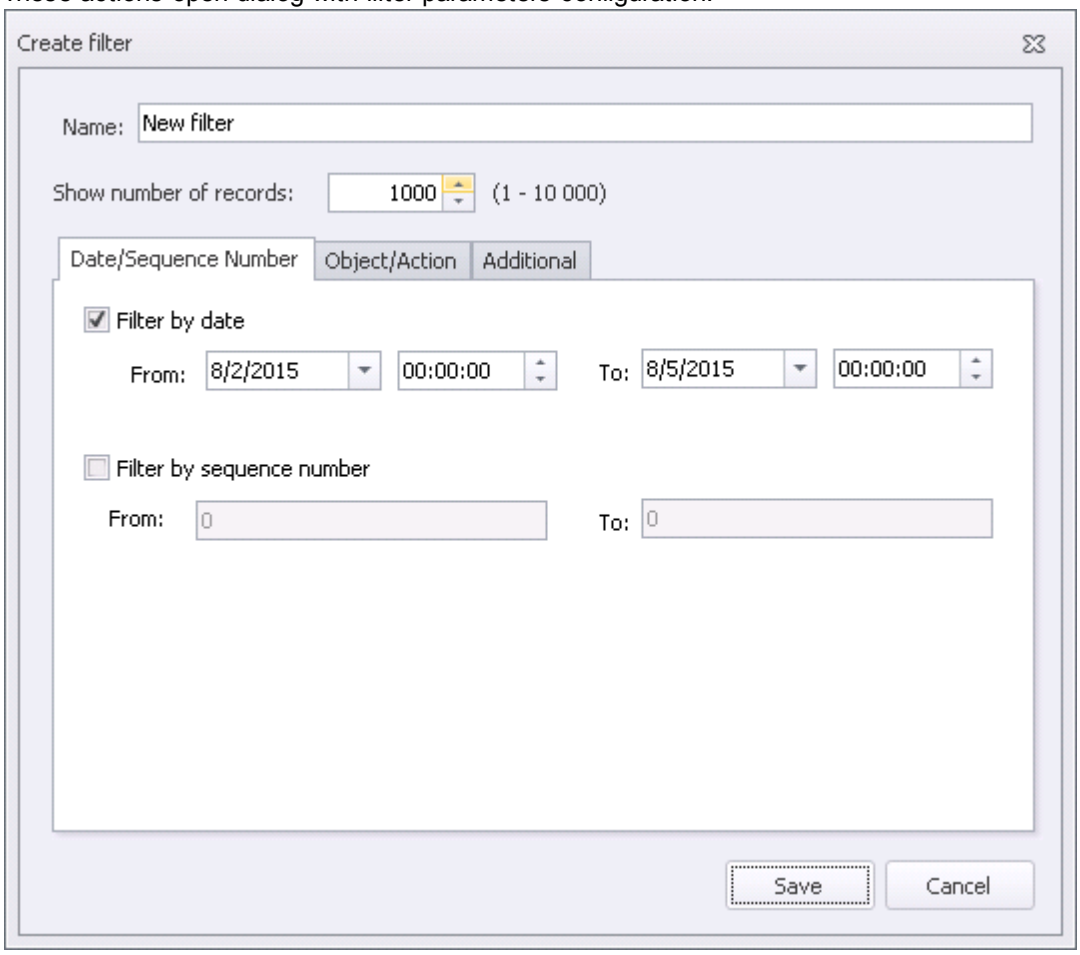
To access Audit Log records that meet certain criteria you can use filters.

To create a new filter or modify an existing one:

1. Go to **Log**.
2. Follow the necessary steps:

Action	Steps
Creating filter	• in Main Menu select **Edit > Create Filter**; • click **Create filter** at the top of Navigation pane.
Editing filter	1. In **Log** area of Navigation pane, select the name of the filter you want to edit. 2. Take one of the following steps: • In Main Menu click **Edit > Edit filter**; • click **Edit Filter** at the top of Navigation pane. • double-click selected filter name.

These actions open dialog with filter parameters configuration.



3. Specify general filter options in filter parameters configuration dialog:
   - **Name**.
   - **Show number of records**. Limit on the number of entries displayed in Management Console workspace (1000 records by default).
4. Set filter criteria. You can configure filters at following tabs:
   - Date/Sequence Number Tab
   - Object/Action Tab
   - Additional Tab

Warning!
If no condition is specified in filter parameters configuration dialog, filtering parameters are disabled. When this filter is applied, all records from the Audit Log will be displayed.

5. Click **Save**.

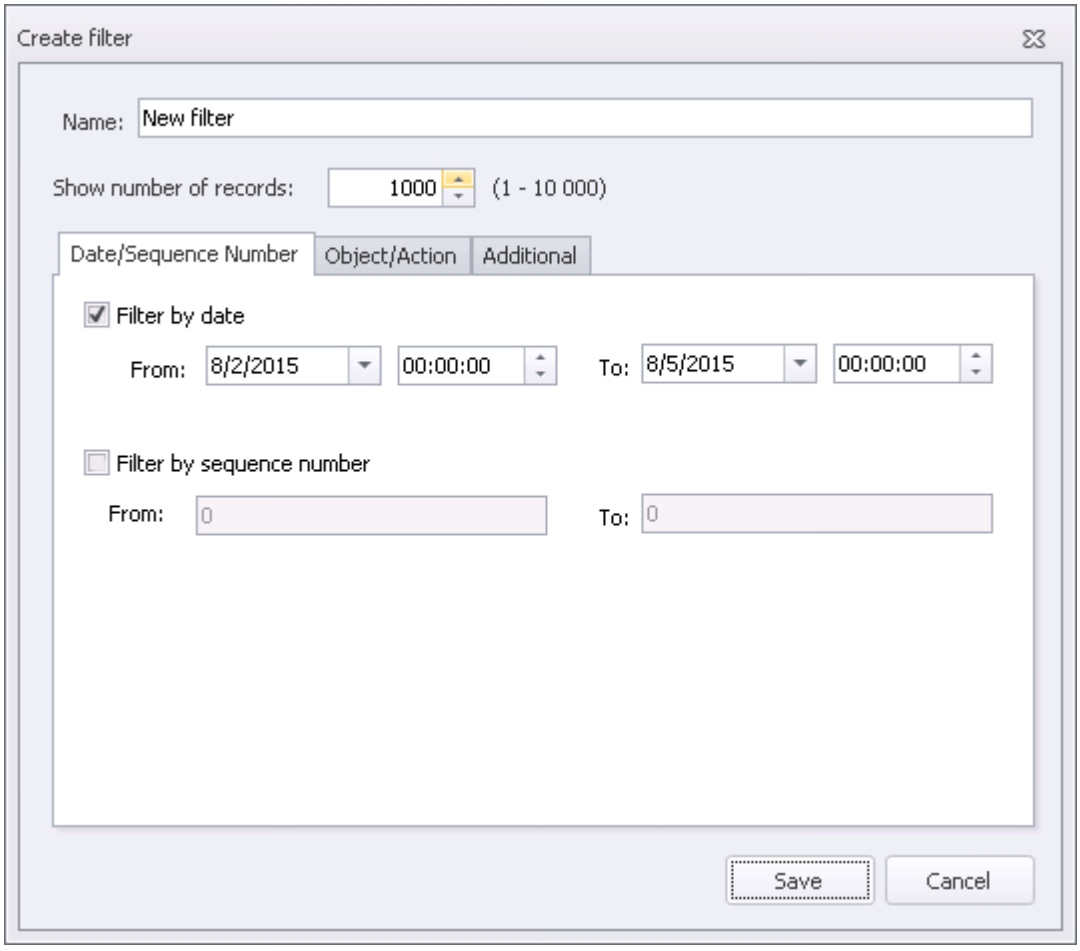
To remove filter:

1. Go to **Log**.
2. In **Log** area of Navigation pane, select the name of the filter you want to remove.
3. Take one of the following steps:
   - in the Main Menu select **Edit > Delete Filter**;
   - click **Delete Filter** at the top of Navigation pane.
4. In the following confirmation dialog select **Yes** to confirm that you want to remove the filter.

3.2.6.2.1 Date/Sequence Number Tab

Configure the following criteria on **Date/Sequence Number** tab:

- date and time the action took place;
- record number in the database.



To specify date and time criteria:

1. Flag **Filter by date** check box.
2. Specify the desired period.

   Starting and ending time is specified in **From** and **To** fields respectively. Set the date and time in right and left field respectively.

To filter by number:

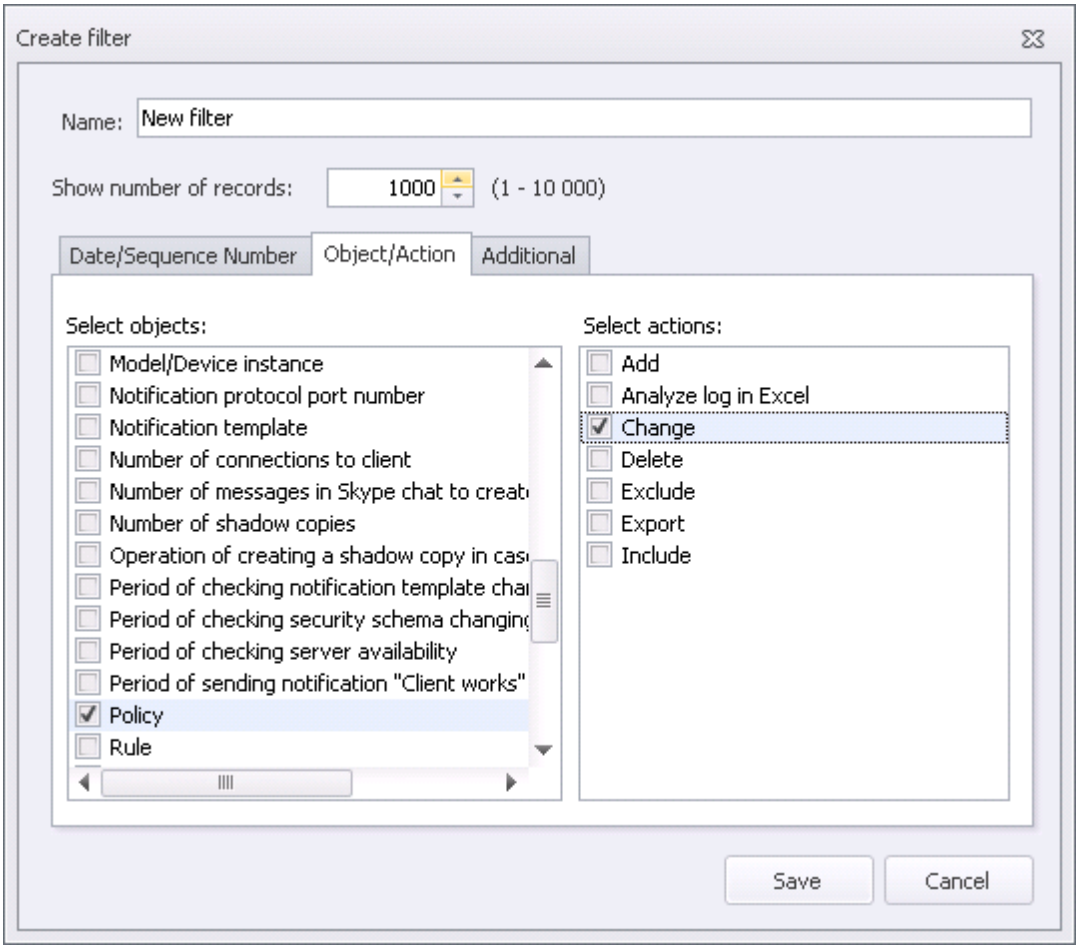
1. Flag **Filter by sequence number** check box.
2. Specify range of numbers in **From** and **To** fields respectively.

   Database record numbers start from 1.

3.2.6.2.2 Object/Action Tab

Use **Object/Action** tab to specify the following filtering criteria:

- target object;
- action performed.



To specify filtering criteria:

1. Set object filtering criteria: in the left list flag the objects you want to filter out.
2. Set action filtering criteria: in the right list flag the actions you want to filter out.

3.2.6.2.3 Additional Tab

You can use **Additional** tab to configure additional filter settings. These settings include:

- **Object Selector**. Filter records using Selector values.
- **Field Name**. Filter records using one of the rule's attributes (for example, *Operation*, *Action* , etc.)
- **Old Value**. Filter records using the rule's previous attribute value.
- **New Value**. Filter records using the rule's modified attribute value.
- **User**. Display user's actions list.
- **Windows Account**. Display list of actions performed on behalf of selected Windows account.
- **Computer**. Display selected computer activity records.

To configure additional filtering parameters, enter their values in the appropriate filed.

Note:
Additional filtering values are not case-insensitive.

3.2.6.3 Deleting Records from Log

Warning!
Log records can be deleted only by Superuser.

To delete log records:

1. In Main Menu click **Edit > Delete log entries**.
2. Enter transaction number in **Delete** dialog.

   Warning!
   Note that audit log records relating to selected transaction or previous transactions will be deleted.
3. Click **OK**.

3.2.6.4 Exporting Log Records

You can export log records to XLS, HTM or TXT files. Later you will be able to view exported records with applications associated with appropriate file formats.

To export audit log records:

1. Go to **Log**.
2. Take one of the following steps:
   - To export records selected by the filter, click the filter on Navigation pane.
   - To export the whole log, click **Show All Records** at the top of Navigation pane.
3. Take one of the following steps:
   - click **Export Log** button in the top of **Records** area
   - in Main Menu click **Edit > Export Log**
4. In the next dialog, specify target file name, type and directory.
5. Click **Save**.

This exports audit log records to selected file.

3.2.6.5 Analyzing Log Records in Microsoft Excel

To enable audit log analysis in Microsoft Excel, you must install the application on the computer that will be used to run the operation.

To view Audit Log records in Excel:

1. Go to **Log**.
2. Take one of the following steps:
   - To view records selected by the filter, click the filter on Navigation pane.
   - To view the whole log, click **Show All Records** at the top of Navigation pane.
3. In the Main Menu click **Edit > Analyze Log in Excel**.

This opens selected log in Microsoft Excel.

3.3 General System Settings

The System has a set of global settings that should be general for all active polities and rules in Device Monitor system. You can configure this settings from menu: **Tools > Settings**. See more information:

- Common Settings for Clients

- Settings of Corporate Network
- Network Traffic Control
- Device Monitor Server Settings. Connecting to Traffic Monitor Server
- Connecting to LDAP Server
- Employee Notifications about Policy Violations
- Exclusion of Application from Interception
- Application control
- Event Storage
- Import/Export Configuration
- InfoWatch Device Monitor Server Manager

Warning!
Modified settings will apply at managed computers after Clients at every computer would receive notification from Server (when checking server availability or when checking security schema changing or when checking notification templates changing) and then Clients would perform update.

3.3.1 Common Settings for Clients

In order to provide efficient operation of Device Monitor Client applications you need to specify a set of common settings.

To configure common settings for Device Monitor clients operation:

1. In the Main Menu select **Tools > Settings**.
2. At the left panel select **Common** node.
3. Change needed settings:

Parameter	Description
Connection	
Period of sending notification "Client works" to the server	Interval (sec) with which the Client sends data to Server
Period of checking server availability	Interval (sec) with which the Client checks Server availability.
Period of checking security schema changing for active client only	If a Client is in active mode (i.e. computer could not open UDP-port for receiving Server notifications) then the Client surveys Server itself to receive data on changing security schema. This parameter sets a survey period (sec).
Period of checking notification template changing for active client only	If a Client is in active mode (i.e. computer could not open UDP-port for receiving Server notifications) then the Client surveys Server itself to receive data on changing notification templates (see "Employee Notifications about Policy Violations"). This parameter sets a survey period (sec).
Client's disk space control	
Free clients' disk space	Minimal size of free disk space (%) of managed computer: when it is reached, shadow copies would not be created. I.e. if when shadow copy is created, free disk space at a client computer is less then parameter value, then neither shadow copy nor its part won't be created. See details in "Creating Shadow Copies and Blocking Operations Due to Free Space Shortage"
If there is not enough space for events	The managed computer dedicates space for storing 30000 events

Parameter	Description
	at the hard drive where Device Monitor Client is installed. If Device Monitor Client did not have connections with Device Monitor Server so that there is stored more than 30000 events controlled by rules defined for employee/computer, then any actions controlled by security schema could be denied. To deny, select **Operation will be blocked**. To allow all actions performed without a control, select **Operation will be permitted**.
Speed of sending data from client	
Limit the speed of sending data	If the channel is narrow you can prevent its excessively uploading by adjusting the speed of shadow copies sending to the Server. To do this check the setting and specify the upper speed limit (Kbps) in **Maximum speed of sending data** field.
Events	
Log events of device and cloud storage interceptors	Level of detailing when saving information about working with external devices received by Device Monitor and Cloud Storage Monitor interceptors: see details in "Configuring Device Monitor Rule", "Configuring Cloud Storage Monitor Rule", "Viewing Events ". The following options are available: • **None** - do not save events • **In case access denied** - events are created only if security policy violation is attempted - i.e. when device usage was denied, including blocking attempts of access level exceeding. The using of external devices which are not forbidden by policies, is not logged • **All** - all actions are logged (connection/usage of any devices, even from white lists)
Log connections outside of corporate network	Level of detailing when saving information about data transfer by network connections received by Network Monitor interceptor: see details in "Configuring Network Monitor Rule". The following options are available: • **None** - do not save events • **In case access denied** - events are created only if security policy violation is attempted - i.e. when connection attempt was denied.
Agent activity on computer	
Show employee notifications	Indicates if employee attempting to perform action forbidden by security policy, would receive warning message. See details in " Employee Notifications about Policy Violations"
Hide Agent presence	Indicates if Windows system tray of managed computer hides Client presence on the computer. If this option is not selected, the Windows system tray of the computer where the Client is installed will display  icon. By clicking at this icon, an information on DM Client operation and list of currently controlled devices is displayed. **Warning!** If there is an antivirus protection enabled on the managed computer then the antivirus program can reveal the operation of Device Monitor: for example, in the list of processes running on the managed computer or in the list of programs that initiate a control.
Code generating key	
Update	Click **Update** to make the System generate a new key used to

Parameter	Description
	make codes of removing network connections or devices access prohibition. See details on codes in "Temporary Employee Access to Network" and "Temporary Employee Access to Devices", **Request code** and **Confirmation code** settings. The frequent key refreshment is not recommended.

4. To apply changes click **Apply**.

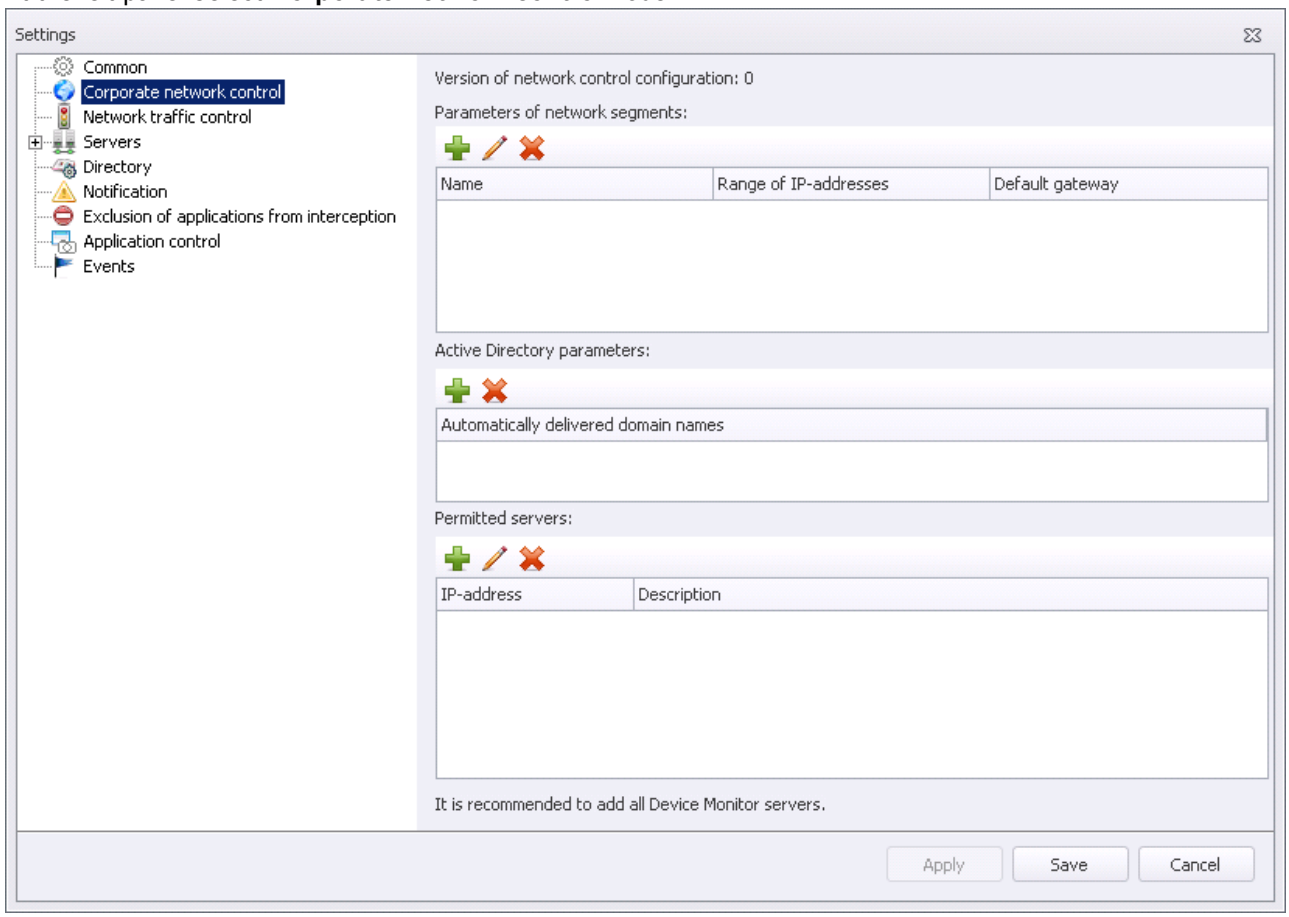
3.3.2 Settings of Corporate Network

In order to provide control of data transfer by network connections with **Network Monitor** (information on rule configuring see in "Configuring Network Monitor Rule") you should specify, which network segments are considered as a corporate network and which external addresses are permitted.

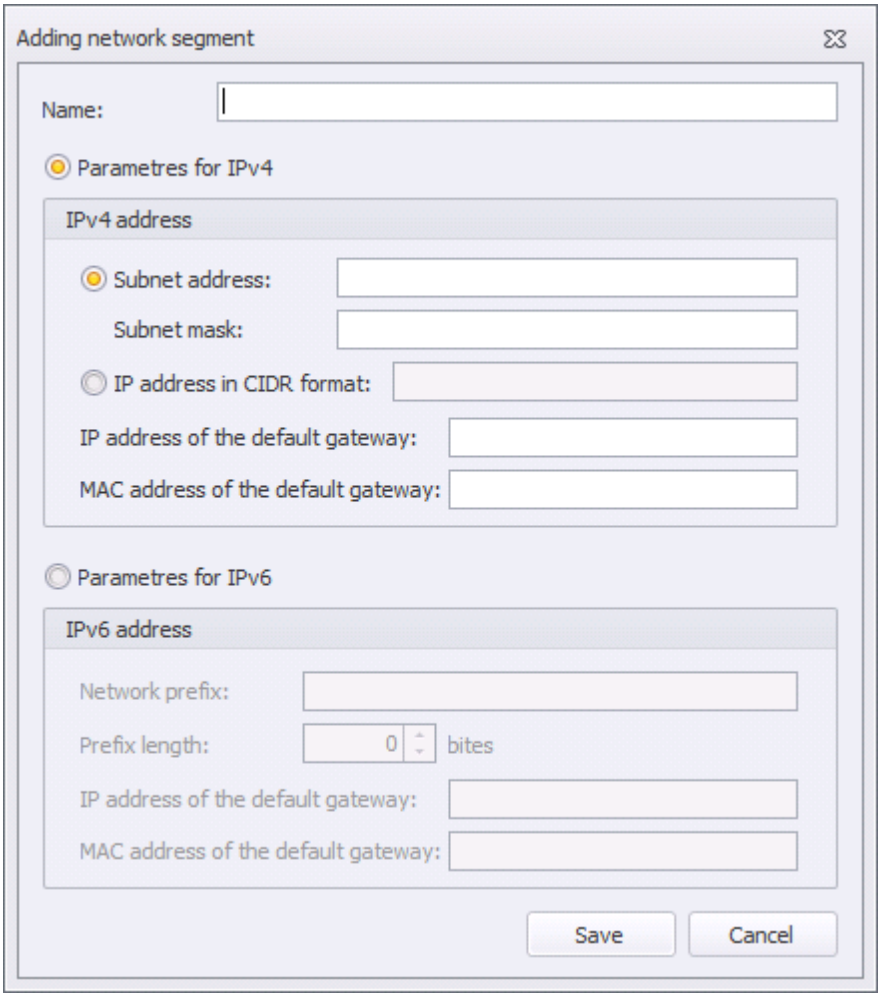
Note:
Permitting the external addresses may be necessary to provide work with external resources when the Client is outside corporate network: for example with VPN server or corporate network.

To configure corporate network settings:

1. In the Main Menu select **Tools > Settings**.
2. At the left panel select **Corporate network control** node.



3. To configure network segments:
   a. In **Parameters of network segments** area click . This opens **Adding network segments** dialog.



b. Specify segment's name (description).

c. Select protocol in use: **IPv4** or **IPv6**.

If you selected **Parameters for IPv4**, then select address format (CIDR or address and mask) and specify required parameters. Also specify IP address and MAC address of the default gateway.

If you selected **Parameters for IPv6**, then select network prefix and its length. Also specify IP address and MAC address of the default gateway.

d. Click **Save**.

e. Repeat to add another segments.

To change segment parameters, select it from the list in **Parameters of network segments** area and click .

To delete a segment from the list, select it, click , then click **Yes** in confirmation dialog.

Warning!

When configuring the corporate network connections you should keep in mind that domain setting takes precedence over the network segments settings.

4. To define Active Directory parameters, click . Then the System automatically defines a name and GUID of a domain where Device Monitor server is deployed.
5. To set a list of servers to permit connection with:
   a. In **Permitted servers** area click .
   b. In **Add permitted server** dialog specify DNS name or IP address of a server and server description.
   c. Click **Save**.
   d. Repeat for other permitted addresses.

To change server parameters, select it from the list and click .

To delete a server from the list of permitted ones, select it, click , then click **Yes** in confirmation dialog.

6. You can also refresh a key of temporary access code forming (see "Temporary Employee Access"). Click **Update**.
7. To apply changes click **Apply**.

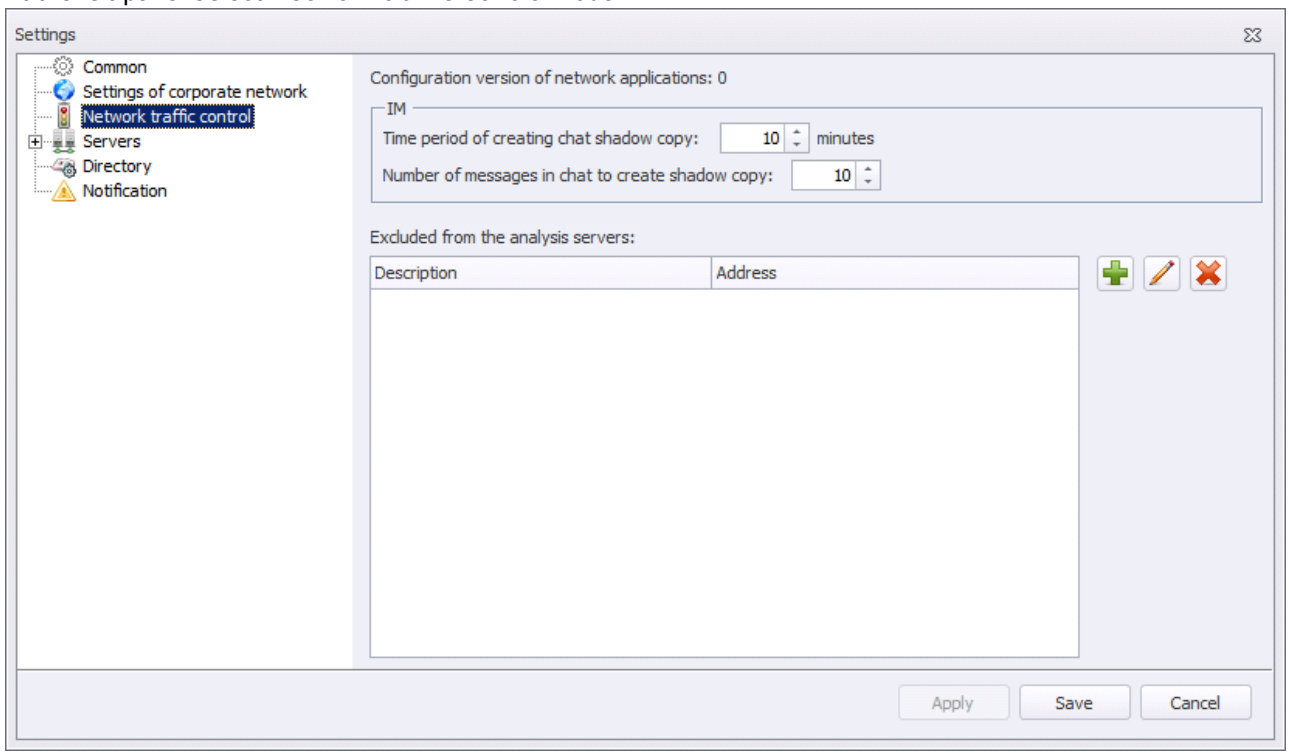
3.3.3 Network Traffic Control

In order to provide control of network traffic, Device Monitor Client acts as a transparent proxy server, to which all the connections are redirected (no matter if they are controlled protocols or not). Then Device Monitor Client parses a protocol and defines if this protocol is a subject of interception. Controlled protocols are: FTP, FTPS, POP3, SMTP, IMAP, HTTP, HTTPS, XMPP, MMP and YMSG (the last is used in Yahoo! Messenger). If data stream is protected with TLS\SSL protocol then proxy server opens traffic and defines if this stream should be controlled.

In network traffic control you can set some additional settings for instant messengers (setting rules for this interceptor see in "Configuring IM Client Monitor Rule"), mailing systems (see "Configuring Mail Monitor Rule") and FTP/FTPS traffic (see "Configuring FTP Monitor Rule"), and define excluded servers which traffic should not be controlled.

To configure network traffic control settings:

1. In the Main Menu select **Tools > Settings**.
2. At the left panel select **Network traffic control** node.



3. Specify instant messengers control parameters:
   - Set a period of creating a chat shadow copy to send to Traffic Monitor. You can set a time period (in minutes) and number of messages as a criteria: the first actuated condition will be applied.
     If a file will be sent in a chat, the shadow copy is formed instantly, without accessing specified criteria.
     Details see in "Configuring IM Client Monitor Rule".
4. You can specify a list of server IP addresses which protocols won't be controlled - i.e. those servers' traffic won't be transferred to the internal proxy server.

Note:

Permitting external addresses can be needed for providing work with external resources and updating installed programs, for example:

- Firefox automatic update needs **.mozilla.com* and **.mozilla.net* in the list of permitted servers
- Filezilla needs *update.filezilla-project.org*
- Dropbox needs **.dropbox.com*

To set a list of servers excluded from analysis:

a. In **Excluded from the analysis servers** area click .

b. In **Add server** dialog specify DNS name or IP address of a server and server description.

Note:

DNS name or IP-address allows to exclude or enable interception of address or port:

To exclude by address and port, specify address and port in the following format: `address:port`.

To enable interception, specify address and port in the following format `~!address:port`.

For example, to exclude all traffic to 10.128.0.2, except to traffic to 8080, it is necessary to add exclusions in the following format: `10.128.0.2` and `~!10.128.0.2:8080`. To exclude only traffic to port 80: `10.128.0.2:80`

Excluding range of addresses, # sign is being used. Example: `#192.168.0.1-192.168.0.255! 192.168.0.5`

c. Click **Save**.

d. Repeat for other permitted addresses.

To change server parameters, select it from the list and click .

To delete a server from the list of excluded ones, select it, click , then click **Yes** in confirmation dialog.

5. When all changes are made, click **Apply**.

3.3.4 Device Monitor Server Settings. Connecting to Traffic Monitor Server

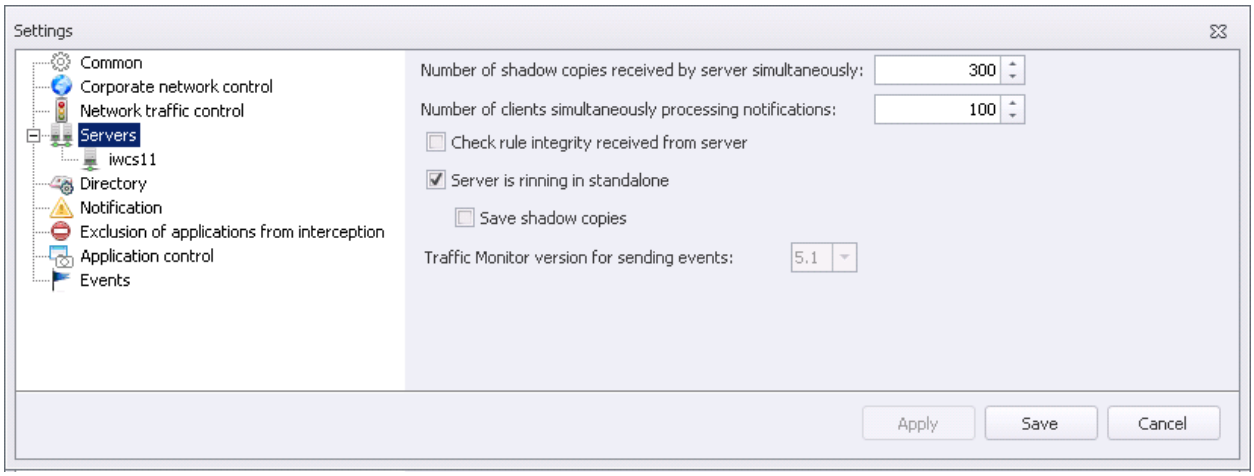
You need to set up connection parameters to be able to send events to Traffic Monitor.

Note:

Changing server role (*General* or *Secondary*) and attribute **Notification protocol port number** and **Main protocol port number** is being executed with **InfoWatch Device Monitor Server Manager** (see "InfoWatch Device Monitor Server Manager").

To view and set up Traffic Monitor connection parameters:

1. In main menu choose **Tools -> Settings**.
2. In **Servers** node set up the following parameters:
   - **Number of shadow copies received by server simultaneously**: - determine the number of copies which can be send to Traffic Monitor Server simultaneously.
   - **Number of clients simultaneously processing notifications**: determines number of clients, which can receive notifications (security schema) from server at a time.
   - **Check rule integrity received from server** - compares rules on server and client to avoid management on client's side.
   - **Server is running in standalone -** server is running without integration with Traffic Monitor.
     - **Save shadow copies -** shadow copies are being saved locally in `ShadowCopyTempDir`.
   - **Traffic Monitor version for sending events** - current version of used Traffic Monitor. Format of events, sent to Traffic Monitor may differ depending on a version.



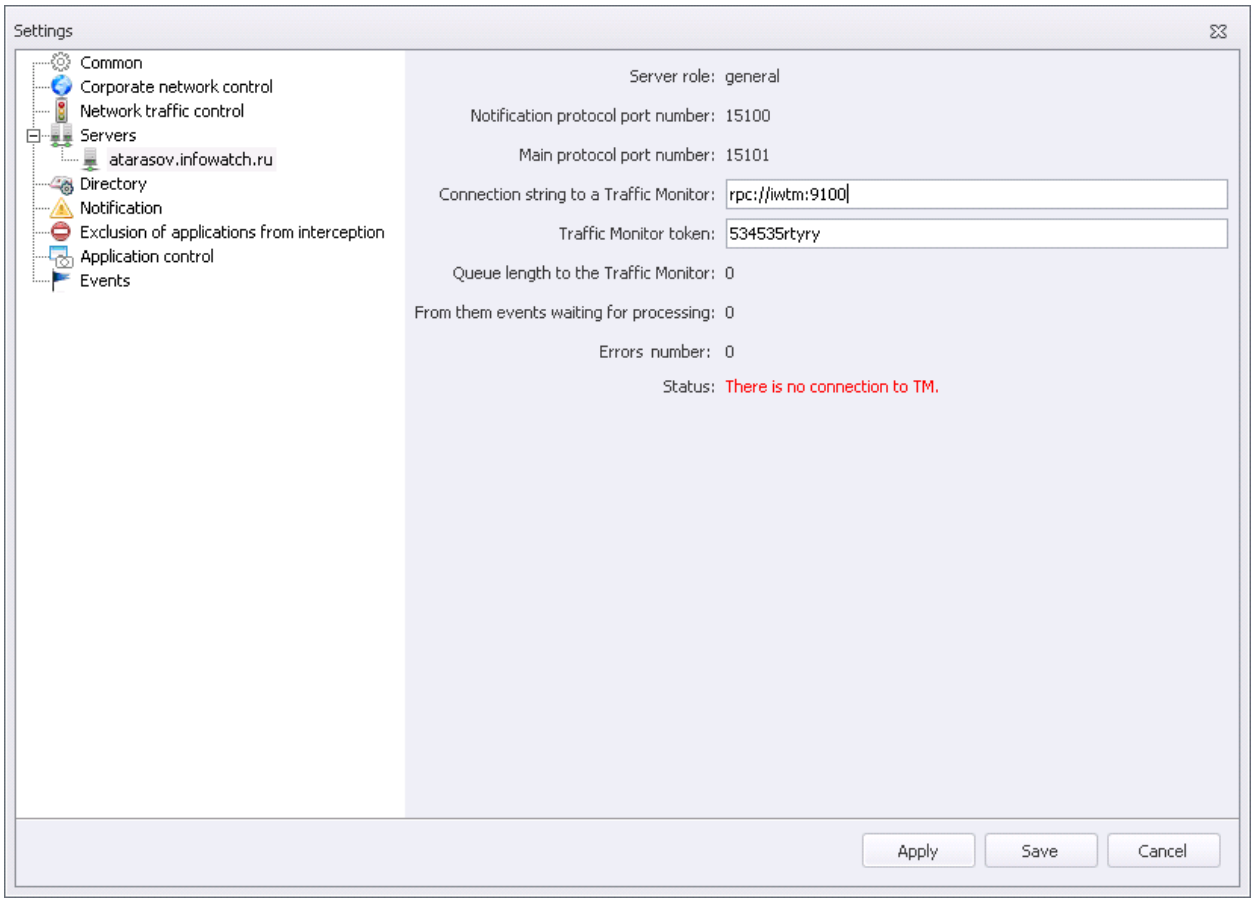
3. When selecting the server name, you will receive information on the following connection parameters:
   - **Server role** – server role (*primary* or *secondary*), assigned to this server during installation: see " InfoWatch Device Monitor Server End Installation Procedure".
   - **Notification protocol port number**.
   - **Main protocol port number**.
   - **Connection string to a Traffic Monitor** - InfoWatch Traffic Monitor server address that will receive events. Address must be entered in the following format:

     `xml://host:port` - for Traffic Monitor of versions under 6.0;

     `rpc://host:port` - for Traffic Monitor v. 6.0 or higher.

     host parameter should contain domain name or IP address of InfoWatch Traffic Monitor server. The server address is the standard URL address (Uniform Resource Identifier) with its formal syntax described in RFC 3986 http://tools.ietf.org/html/rfc3986.

     port parameter contains InfoWatch Traffic Monitor server port that delivers events. InfoWatch Traffic Monitor default server port is 4101.
   - **Traffic Monitor token** – the token to connect to API. Required for Traffic Monitor v. 6.0 or higher. You can get the actual token from your Traffic Monitor administrator.
   - **Queue length to the Traffic Monitor** - number of events pending submission to InfoWatch Traffic Monitor.
   - **Among them events awaiting for processing** – number of events pending processing before sending to InfoWatch Traffic Monitor.
   - **Errors number** – number of events in the errors queue.
   - **Status** – information on Traffic Monitor connection state.



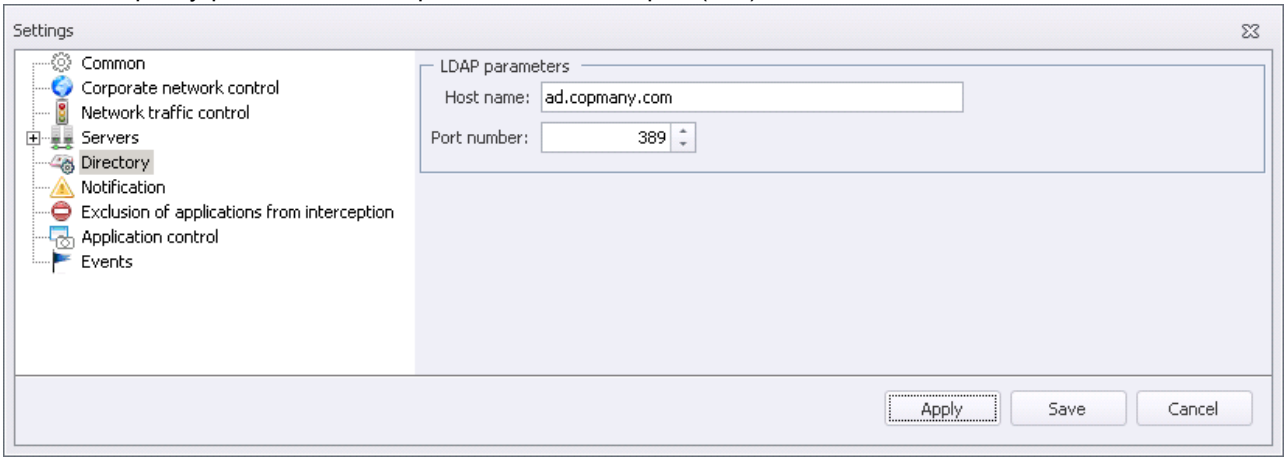
4. When all changes are made, click **Apply**.
5. Click **Save**.

3.3.5 Connecting to LDAP Server

In order to receive the information on workstations and employees from directory services (Active Directory or Novell eDirectory), configure Management Console connection to LDAP server.

To display and configure LDAP connection settings:

1. In the Main Menu select **Tools > Settings**.
2. At the left panel select **Directory** node.
3. In **Host name** field specify domain name or IP-address of LDAP server.
4. If needed, specify port to redirect requests when default port (**389**) is unavailable.



5. Click **Apply**.

3.3.6 Employee Notifications about Policy Violations

When an employee working at managed computer tries to perform an action forbidden by security policy, the notification is displayed. Notifications are displayed in following cases:

- **Access to device denied** – Device Monitor rule which denies reading and writing to the device (see "Configuring Device Monitor Rule") was actuated.
- **Writing to device denied** – Device Monitor rule which denies writing to the device (see "Configuring Device Monitor Rule") was actuated.
- **Writing to open area denied** – Device Monitor rule which denies writing to unencrypted floppy drives and detachable devices (see "Configuring Device Monitor Rule") was actuated.
- **Copying/printing file denied if there is not enough space for incidents** – if Device Monitor Client did not have connections with Device Monitor Server so that there is out of dedicated space for storing information on events controlled by rules (30000 events) and common settings have **Operation is blocked** option selected (see in "Common Settings for Clients") then any operations controlled by current security policy are forbidden.
- **Data transfer via network protocols denied** – Ftp Monitor or IM Client Monitor rule which denies data transfer through FTP/FTPS/SMTP/POP3/MAPI/XMPP/MMP/YMSG/Skype (see "Configuring FTP Monitor Rule" and "Configuring IM Client Monitor Rule") was actuated.
- **Data transfer via network protocols denied if there is not enough space for incidents** – if Device Monitor Client did not have connections with Device Monitor Server so that there is out of dedicated space for storing information on events controlled by rules (30000 events) and common settings have **Operation is blocked** option selected (see in "Common Settings for Clients") then any operations controlled by current security policy are forbidden.
- **Network connection forbidden. Reduced** – Network Monitor rule which denies data transfer through any network connections except corporate network and specified permitted servers (see "Configuring Network Monitor Rule" and "Settings of Corporate Network") was actuated.
- **Network connection forbidden and request of temporary network access** – Network Monitor which denies denies data transfer through any network connections except corporate network and specified permitted servers was actuated. In this notification employee can request for temporary access to external connections (see "Configuring Network Monitor Rule", "Settings of Corporate Network" and "Temporary Employee Access").
- **Request of temporary access to the device by phone** – text displayed when user selected **Request access** command in InfoWatch Device Monitor Client interface, **Device list** tab (see "Temporary Employee Access to Devices").
- **Request of temporary access to the device by mail** – text displayed when user selected **Request access** command in InfoWatch Device Monitor Client interface, **Device list** tab (see "Temporary Employee Access to Devices").
- **Prohibition of access to cloud storage** – Cloud Storage Monitor rule which controls cloud storages client usage (see "Configuring Cloud Storage Monitor Rule", **Access Denied** option) was actuated.
- **Prohibition of writing to cloud storage** – Cloud Storage Monitor rule which controls cloud storages client usage (see "Configuring Cloud Storage Monitor Rule", **Only download** option) was actuated.
- **Prohibition of running application** – Application Monitor rule which controls user access to applications by means of white lists and black lists (see "Configuring Application Monitor Rule") was actuated.
- **Prohibition of making screenshot** – ScreenShot Control Monitor rule which controls making screenshots (see "Configuring ScreenShot Control Monitor Rule") was actuated.

To disable showing notifications for employees entirely or to enable it back:

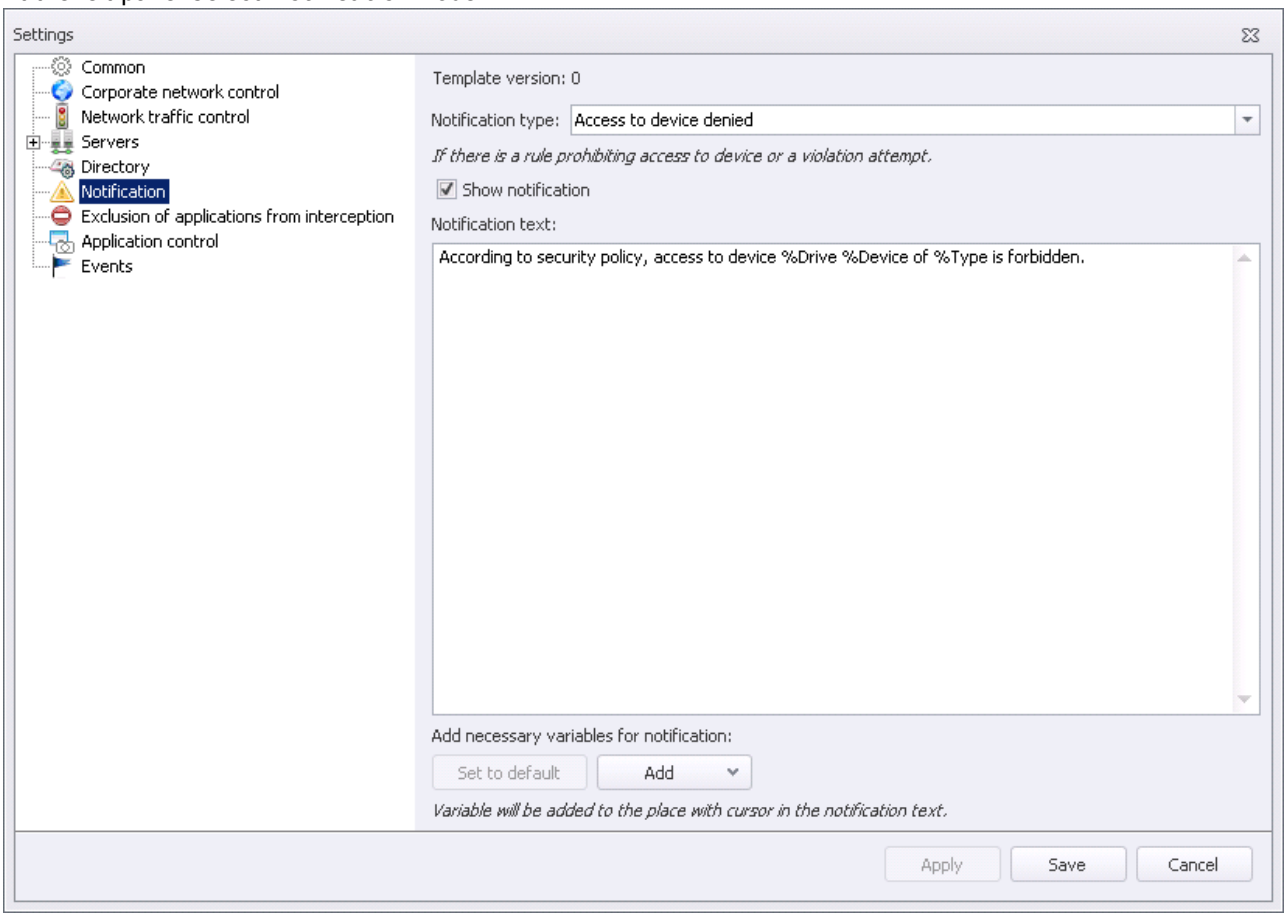
1. In the Main Menu select **Tools > Settings**.
2. At the left panel select **Common** node.
3. Deselect **Show notification** to disable showing notifications for employees, or flag it to enable notifications.
4. Click **Apply**.

If needed, you can change notification text or disable showing of any certain notification type or enable it back.

Warning!
If you disabled notifications using method described above, then notifications enabled using method described below won't displayed yet.

To change notification text or enable\disable certain notifications:

1. In the Main Menu select **Tools > Settings**.
2. At the left panel select **Notification** node.



3. From **Notification type** list select a notification type.
4. To enable (disable) displaying notification of chosen type, select (deselect) **Show notification**.
5. Enter notification text.

   You can use variables which would be transformed to actual data when displayed to employee: for example, type of blocked device or IP address of permitted host. To do this, set the cursor at required place of text, then click **Add** below textbox and select required variable from the list.

   To cancel changes and set default settings back, click **Set to default.**
6. Click **Apply**. If needed, change settings for other notifications by repeating steps 2-5.
7. When all changes are made, click **Save**.

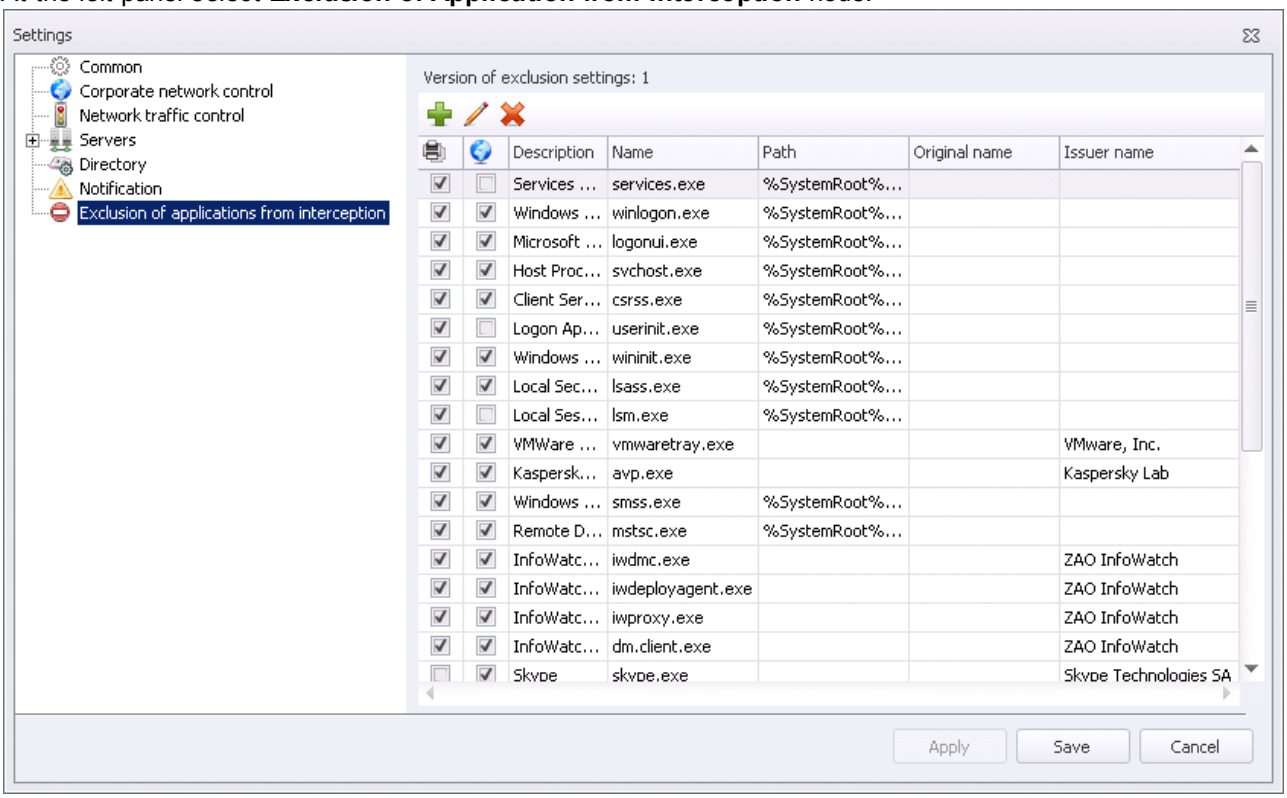
3.3.7 Exclusion of Application from Interception

Specify the parameters described below to exclude the application from the interception. After exclusion parameters have been set up, they will be automatically applied to the computer before reboot during installation process.

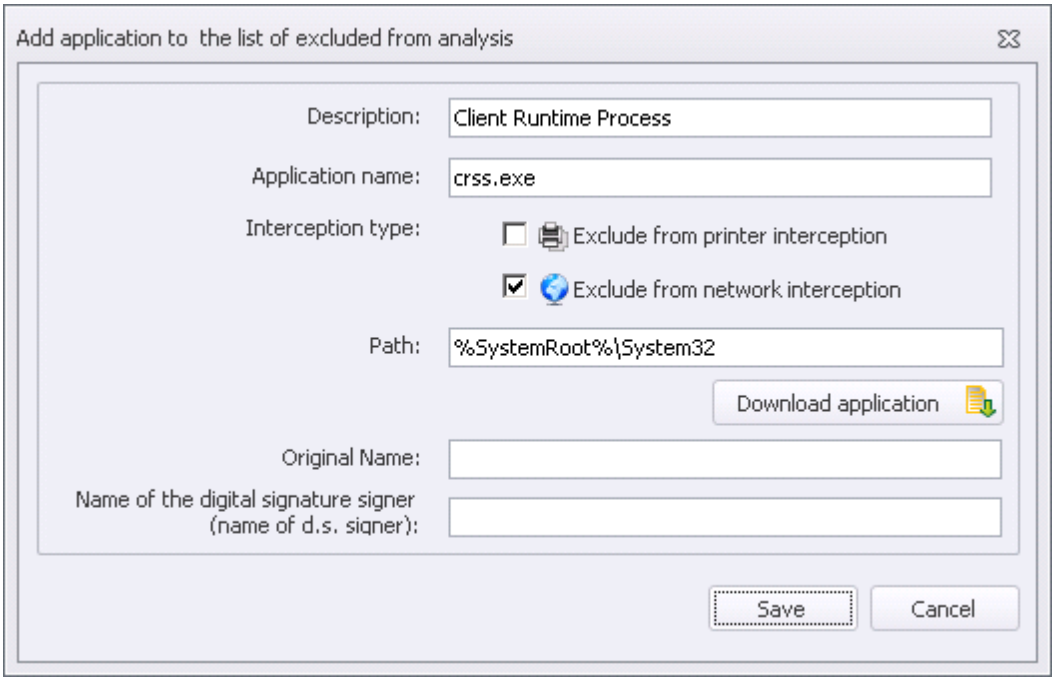
To view and configure parameters of application exclusion:

1. In the Main Menu select **Tools > Settings**.

2. At the left panel select **Exclusion of Application from Interception** node.



3. At the toolbar click **Add**.



4. In the **Description** field type the arbitrary text. This field must be filled.
5. In the **Application name** field type the name of executed file. Excluding will be processed for the name set on this step. This field must be filled.
6. Mark the checkboxes in the **Interception type** field:
   - **Exclude from printer interception** - if you don't want to create events and shadow copies of print jobs initialized from this application;
   - **Exclude from network interception** - if you need to exclude this application's activities from the network interception (see "Network Traffic Control").

Note:
One type must be checked at least.

7. You can specify application file parameters manually or automatically:
   - To specify file parameters manually:
     a. In the **Path** field specify the directory containing executable file of application (you can use the system variables). If you use this parameter only the application located in defined directory is excluded.
     b. In the **Original Name** field define the name of application (in the context menu of executable file choose **Properties**, **Details** tab, **Original filename** attribute).
     c. In the **Name of the digital signature signer (name of d.s. singer)** field define the property of application (in the context menu of executable file choose **Properties**, **Details** tab, **Digital signature** attribute).

Warning!
While filling the **Original Name** and **Name of the digital signature signer (name of d.s. singer)** fields you can prevent for example the user's unapproved attempt to rename the application to make its name look like the name of application excluded from interception.

   - To specify file parameters automatically, click 

Download application button and select the needed file. Fields **Path**, **Original Name**, **Name of the digital signature signer** will be filled automatically.
8. Click **Save**.

3.3.8 Application Control

The System allows to control applications running of managed computers by allowing or forbidding some applications. For this purpose there are two operation modes provided:

- **Active white lists of applications** - all applications from the lists selected in the Application Monitor rule from the resulting policy are allowed. Other applications are forbidden.
- **Active black lists of applications** - all applications from the lists selected in the Application Monitor rule from the resulting policy are forbidden. Other applications are allowed.

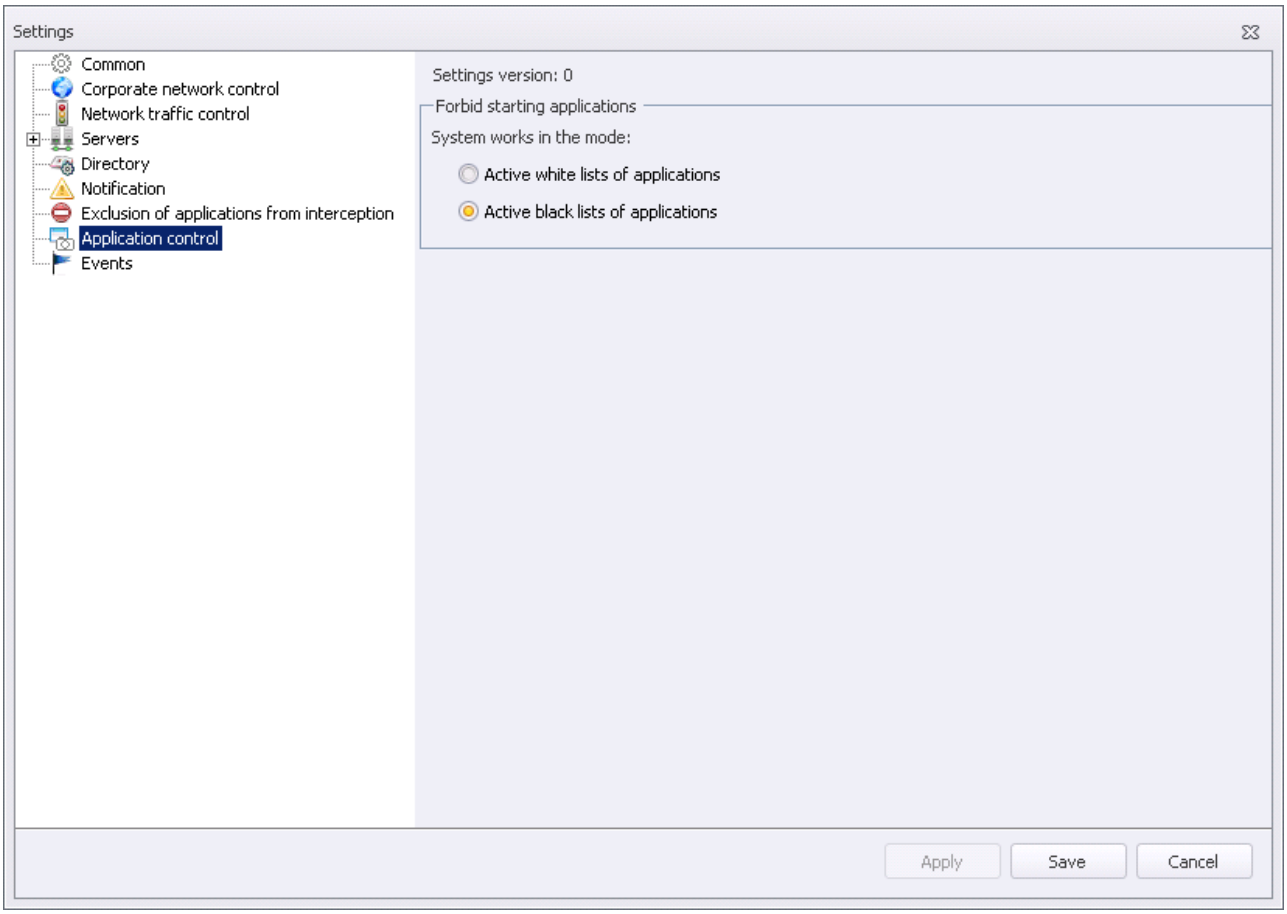
See details on forming application lists in "Application Protocol".

See details on applying lists in rules regulating application access in "Configuring Application Monitor Rule".

See details on resulting policy viewing in "Viewing Resultant Policy and White List for an Employee" and "Viewing Resultant Settings, Policy and White List for a Computer".

To set System mode for application control:

1. In the Main Menu select **Tools > Settings**.
2. At the left panel select **Application control**.



3. Change mode if needed.
4. Click **Save**.

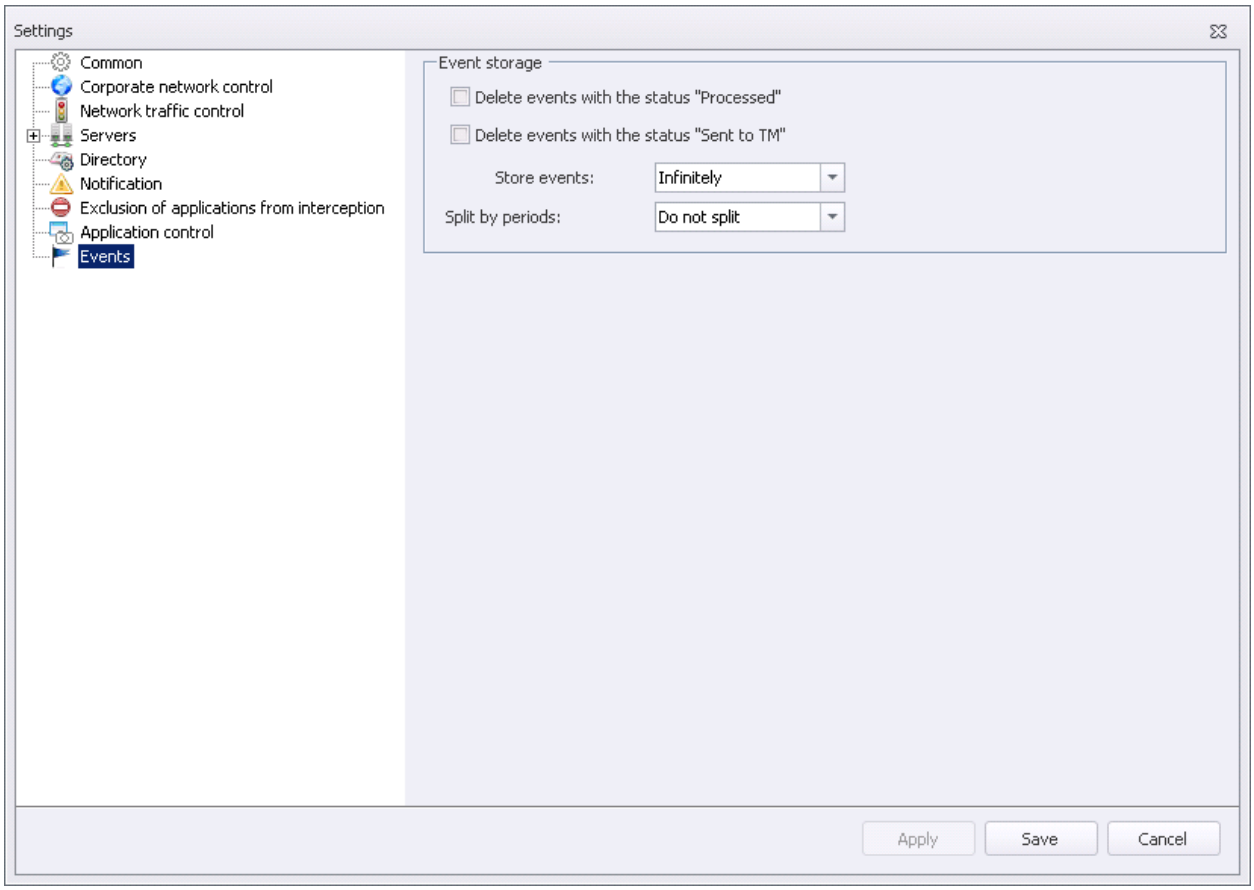
The new settings version will be applied on controlled computers after next reboot of those computers.

3.3.9 Event Storage

In the **Events** tab you can set the parameters of automatic event storage and deletion.

To set up event storage:

1. In the Main Menu select **Tools > Settings**.
1. At the left panel select **Events** node.
2. Mark the following boxes:
   - **Delete events with "Processed" status** - to delete processed Device Monitor events or events of a standalone server;
   - **Delete events with "Sent to TM" status** - to delete events already sent to TM.



2. From drop-down lists select:
   - **Store events** - to set up the time for event to be stored in DB and be displayed in the console;
   - **Split by periods** - splitting traffic into blocks depending on the time it has been created to speed up connection process.

Note:
When **Delete events with the status "Processed"** and **Delete events with the status "Sent to TM"** options are chosen simultaneously, **Store events** becomes automatically disabled.

3.3.1 Import/Export Configuration

You can save the current configuration settings as a file. The saved file can be used for Device Monitor Server fast configuring after its reinstalling.

The exported server configuration includes the following elements:

- **Security scheme** (see "Managing security schema")
- **Application protocol** (see "Application protocol")
- **Network control settings** (see "Settings of corporate network")
- **List if servers excluded from analysis** (see "Network traffic control")
- **List of applications excluded from interception** (see "Exclusion of application from interception")

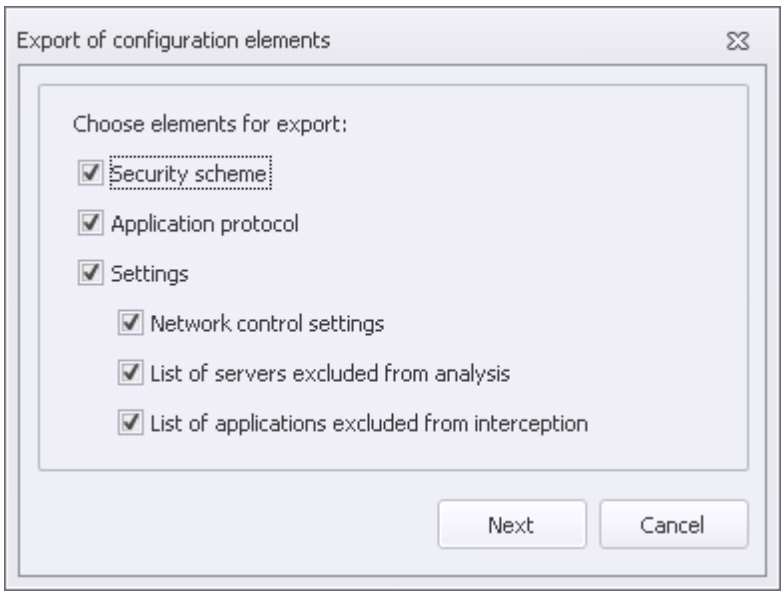
Warning!
You cannot import to the System v. 6.0 the configuration file exported from the earlier version.

To import configuration settings:

1. In main menu choose **Tools -> Import Configuration**.
2. Find a `.dmc` file and click **Open**.

To export configuration settings:

1. In main menu choose **Tools -> Export Configuration**.
2. In dialog window choose object to export.
3. Click **Next**.



4. In the opened dialog window specify the name and the location of the export configuration file in `.dmc` format and click **Save**.

3.3.1 InfoWatch Device Monitor Server Manager

InfoWatch Device Monitor Server Manager is being used to define roles and change server settings.

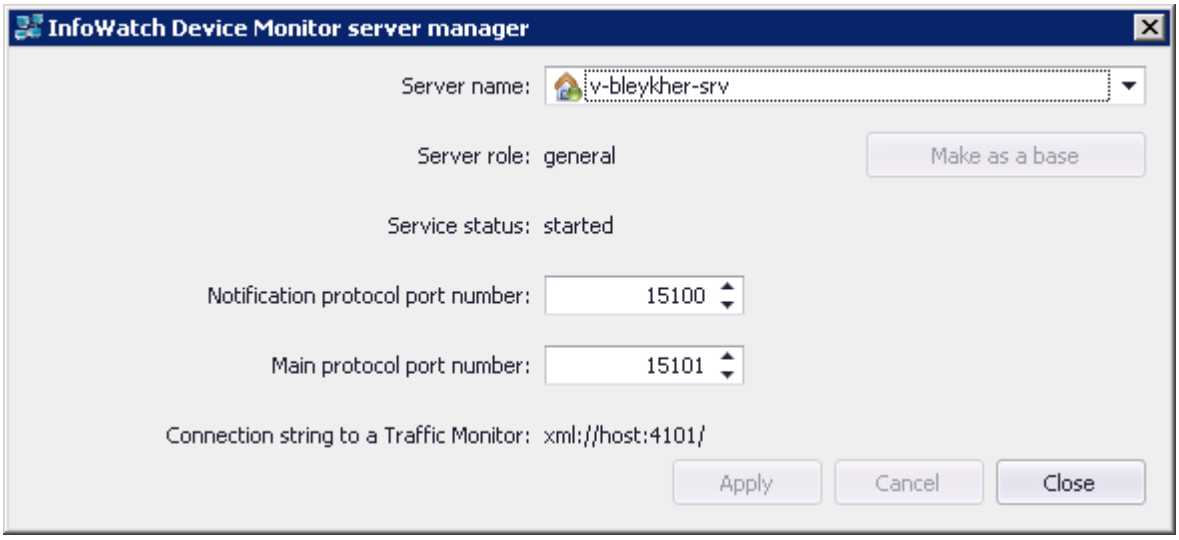
Warning!

There are following requirements to run the InfoWatch Device Monitor Server Manager utility:

- the computer where utility will run, must be included to the domain
- the user on behalf of which the utility will run, must have *Administrator* role at each of the servers to be changed
- there must be FQDN access granted to the servers (to check use *ping* <*server_name*>.<*domain_name*>)
- the utility must be run on behalf of the Administrator (use the option in the drop-down menu opened by clicking the right mouse button on the utility icon); or User Access Control must be disabled the computer.

To set up server ports, proceed with following steps:

1. Go to **Start -> All programs -> InfoWatch -> Device Monitor -> InfoWatch Device Monitor Server Manager**.



Info Watch Device Monitor server manager window will be opened.

2. From **Server name** drop-down menu pick the necessary server.
3. Edit fields **Notification protocol port number** and **Main protocol port number**.
4. Click **Apply**.
5. Click **Close**.

To assign *general* role to the server, proceed with the following steps:

1. Go to **Start -> All programs -> InfoWatch -> Device Monitor -> InfoWatch Device Monitor Server Manager**.
   Info Watch Device Monitor server manager window will be opened.
2. From **Server name** drop-down menu pick the necessary server.
3. Click **Make as a base**.

> **Note:**
> Making one of the servers general makes other servers secondary automatically.

4. Click **Apply**.
5. Click **Close**.

3.4 Managing Security Schema

Security schema description and operation procedures for its managing are provided in the following sections:

- Security Schema Organization
- Common Actions in Managing Security Schema
- Security Schema Setup
- Temporary Employee Access to Network
- Temporary Employee Access to Devices

3.4.1 Security Schema Organization

Security schema of InfoWatch Device Monitor is a set of configuration parameters for managing employee controlled by InfoWatch Device Monitor. Security schema is created during server installation and is stored in the database.

Security schema includes the following parameters:

- **Security polices** with a set of rules specified for each security policy.
- **Employee groups** registered in Device Monitor. Each employee group must have a security policy.
- **Computer groups**. Each computer group must have a security policy.
- **White lists** of fully accessed devices.
- **Signature categories** that apply File Monitor rules to certain file formats.

Note:
To make sure all computers and accounts are covered by security policy, the default employee group and default computer group are provided in the System.

Security schema can be edited multiple times. Updated security schema will be saved as a new version of the existing one. Old security schemas are stored in the database. Use Management Console to preview security schema versions.

This topic also contains:

- Security Policies and Rules
- Employees and Employee Groups
- Computers and Computer Groups
- Loading Security Schema to Managed Computers

3.4.1.1 Security Rules and Policies

Security policy is a set of rules used for monitoring operations of data transfer to removable devices, sending documents to print and network activity; it also defines access level to managed peripherals.

The security policy is assigned to employee group or computer group according to the following principles:

- Each employee group and each computer group must have a security policy.

  You can't add a new employee group or computer group without assigning a security policy. The security policy for employee group or computer group is selected from available policies. Therefore, security policy must be created before you add a group.
- You can't assign more than one security policy to employee group or computer group.
- One security policy can be assigned to several employee groups or computer groups. However, it is recommended that you assign an individual security policy to each group.

  Note:

  You can't remove a security policy from security schema, if it is assigned to at least one employee group or computer group.

Controlled files and devices access level is defined by security policies assigned to:

- employee group which the employee belongs to;
- computer group which include the computer used by the employee.

If employee was registered with Device Monitor for the first time, his account is automatically added to *Default* employee group. Therefore, each new employee's access level is initially defined by default employee group security policy and employee's computer group security policies. You can change access level later by adding employee to various employee groups.

Rules are restrictions and conditions that monitor data transfer to removable devices, network activity, sending documents to print, and control access to managed peripherals. A new set of rules is created for each security policy.

Each rule has a validity period and is disabled after its expiry.

Rule types include:

- **Application Monitor Rule** provides application access control via black and white lists.
- **Cloud Storage Monitor Rule** provides web-client control.

- **Device Monitor Rule**. Lets you control employee access to selected type of peripherals.
- **File Monitor Rule**. Monitors data transfer and editing on removable devices. Rule can be configured to create file shadow copy and send it to InfoWatch Traffic Monitor when attempting to save a file to removable device.
- **FTP Monitor Rule**. Both complete deny and partially restrict are available for FTP/FTPS protocol usage: for example, you can allow downloading only. Also you can set creating shadow copies of transferred files to send them to the InfoWatch Traffic Monitor for further analysis.
- **HTTP(S) Monitor Rule** controls data exchange through HTTP and HTTPS protocol. System allows to create shadow copies of transferred files.
- **IM Client Monitor Rule**. Allows to control employee access to instant messengers: Skype, WhatsApp, XMPP, MMP (used in Mail.Ru Agent messenger), YMSG (used in Yahoo! Messenger) and mobile SMS). Rule can block access to application or just make copies of transferred files, messages and chats. InfoWatch Device Monitor sends shadow copies of files and chat sessions to InfoWatch Traffic Monitor without saving them.
- **Mail Monitor Rule**. Provides full control of incoming and outgoing e-mail. Lets you to deny of sending and receiving e-mail completely or to allow receiving only or to allow both sending and receiving e-mail completely. The creating of shadow copies transferred to InfoWatch Traffic Monitor for analysis is available too.
- **Network Monitor Rule**. Lets you deny data transferring by any network connections except corporate ones or connections with specified allowed servers. The System has a global setting of which network segments are corporate network and which external addresses are allowed.
- **Photo Monitor Rule.** Lets you to set creating of shadow copies of photos made by cameras of controlled mobile devices.
- **Print Monitor Rule**. Lets you to monitor printing activity. Rule can be configured to create shadow copies of print jobs, which will be sent for InfoWatch Traffic Monitor analysis.
- **ScreenShot Control Monitor Rule** allows to control screen shots on a client side.

3.4.1.2 Employees and Employee Groups

Employee registration rules:

- Each employee belongs to at least one employee group (default group). The reason for this requirement is that security policy can only be assigned to employee groups.

  Default employee group includes all accounts that have not been added to other groups (employees newly registered in Device Monitor or employees excluded from all other groups).

  You can delete an employee from "*Default*" group, if the account will be added to at least one employee group besides the *Default* group.
- After System installed, the *"Shadow copy policy"* is assigned to "*Default employee group*". The *"Shadow copy policy"* contains following rules:
  - **Document shadow copying**. File Monitor rule which sets creating shadow copies of all files written to removable devices.
  - **Print shadow copying**. Print Monitor rule which sets creating shadow copies of all print jobs.
  - **Skype control**, **Yahoo! control, XMPP control**, **MMP control**. IM Client Monitor rules which allow instant messengers and set creating shadow copies of all messages, chats and outgoing files.
  - **FTP control**. FTP Monitor rule which allows FTP/FTPS protocol and set creating shadow copies of all files sent by FTP/FTPS.
  - **HTTPS control**. HTTP(S) Monitor rule, which creates a post-event, without any dependence on its size, in case transfer is being performed via encrypted channel. Shadow copy is created, if the size of a request transferred via encrypted channel is in range from 40 B to 40 MB.
  - **Mail control**. Mail Monitor rule which allows incoming and outgoing mail sending and creates shadow copies of e-mails sent via encrypted channel and having size in range from 40 B to 40 MB.

3.4.1.3 Computers and Computer Groups

The computer registered in the Device Monitor belongs to at least one computer group (default group). The reason for this requirement is that security policy can only be assigned to computer groups.

The *Default computer group* includes all computers that don't belong to other computer groups (Device Monitor workstations newly registered in the System or workstations excluded from all other groups). "*Device policy*" is assigned to default computer group after the System installation. This policy is empty: it does not contain any rule.

You can remove a computer from default group only if it is added to at least one computer group besides default group.

Mobile devices can be added to the security schema with binding to the employee and installation the Device Monitor Client onto mobile device. This can be performed through the computer group (specifying the employee previously created in the System or added from LDAP) or from employee group (specifying the computer group to which the mobile device should be added).

3.4.1.4 Uploading Security Schema to Managed Workstations

The security schema of managed computers must be up to date. This is ensured by Client-Server interaction on managed computers.

Server transmits security schema to managed computers automatically in the following cases:

- when you save your new or edited security schema
- if the employee with unidentified access level is registered. Such employee is automatically added to default employee group, and security schema is updated.

If the managed computer is disconnected from the network where InfoWatch Device Monitor is deployed, the polices will still be active, but they won't be updated and shadow copies will be stored on the hard drive. After the managed computer has connected to InfoWatch Device Monitor server, it automatically updates policies and sends shadow copies to server.

3.4.2 Common Actions in Managing Security Schema

Security schema guidelines are available in the following sections:

- Viewing Active Security Schema
- Viewing Old Security Schema
- Security Schema Comments
- Editing Security Schema
- Updating Security Schema
- Exporting/Importing Security Configuration

For general information on security schemas see "Security Schema Organization".

For security schema configuration guidelines see "Security Schema Setup".

3.4.2.1 Viewing Active Security Schema

Active security schema is displayed on Management Console by default.

Security schema configuration information is displayed in **Policies**, **Employees**, **Computers**, **White Lists** and **Signatures** sections (see "Management Console Sections").

Security schema configuration is displayed as groups of elements. Section groups list are displayed in Navigation pane preview. Each group of elements has an icon (see the table).

Icon	Elements group
	Default computer group
	Computer group
	Default employee group
	Employee group
	Default signature category
	Signature category
	Devices white list for employee
	Devices white list for employee group
	Devices white list for computer
	Devices white list for a group of computers
	Audit log filter
	Security policy

To view an information about security schema section:

1. Open the section (see "Management Console Sections"). The list of element groups will be displayed on Navigation pane.
2. On Navigation pane select the element group you want to view. This will display all elements of the group in the main screen workspace.
3. To view detailed information on individual elements, click the row containing element name. This opens the element's properties table on **Details** panel.

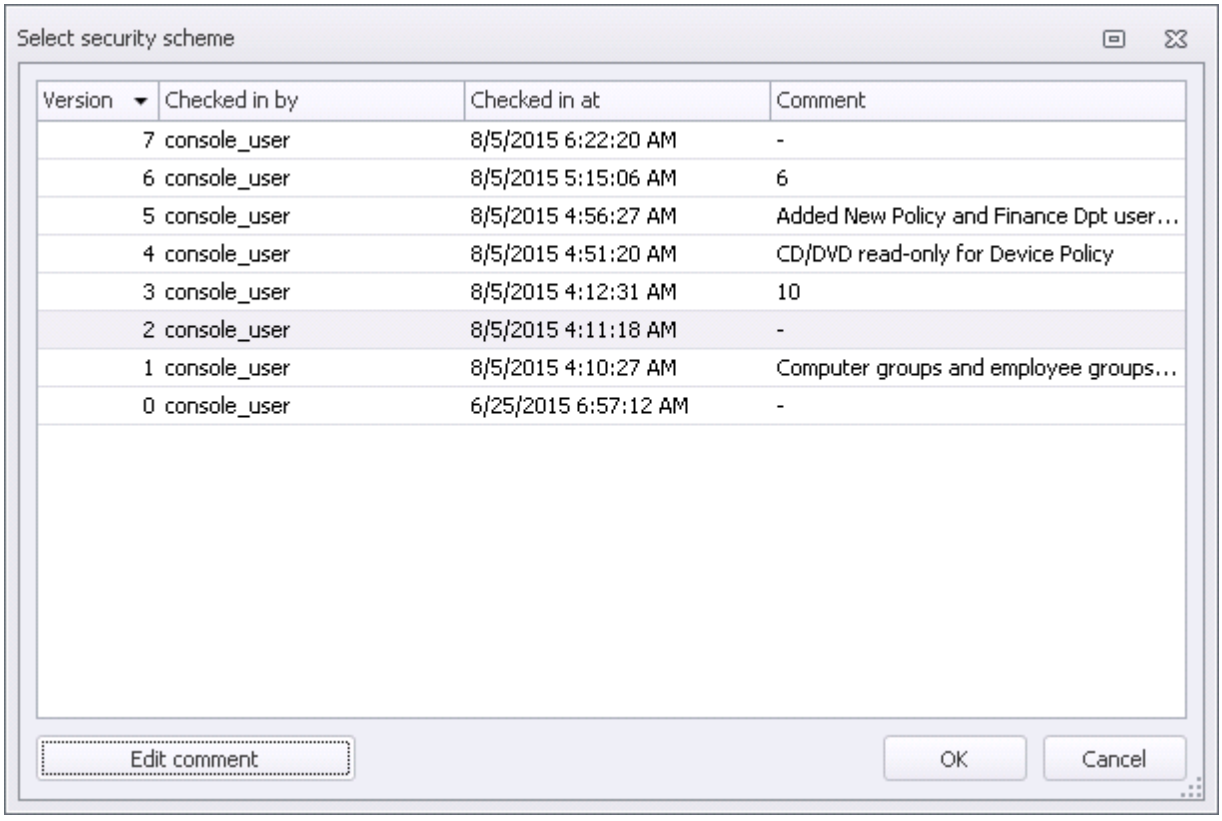
Note:
You can customize the main screen appearance (see "Main screen customization").

3.4.2.2 Viewing Old Security Schema

Note:
If you view previous security schemas in editing mode, your recent changes will be discarded.

To view older security schema:

1. In Main Menu select **Security Schema > View Old Security Schema**.
   This opens **Select security scheme** dialog.



Each security schema features the following information:

- **Version**. Security schema version number.
- **Checked in by**. Name of the version owner.
- **Checked in at**. Last saved version date and time.
- **Comment**. Additional information.

> **Note:**
> You can edit comments to any version in this screen (see "Security Schema Comments"). Information on current Management Console security schema (version number and comment) is displayed on the status bar.

2. In **Select security scheme** dialog select the row that contains the version number of security schema you want to viewed.
3. Click **OK**.

After you click **OK** the selected security schema version will be loaded into Management Console. When working with old version, the state bar displays: "*Old security schema*".

To return to preview and active security schema,

open **Security Schema > View the Latest Security schema** in the Main Menu.

3.4.2.3 Security Schema Comments

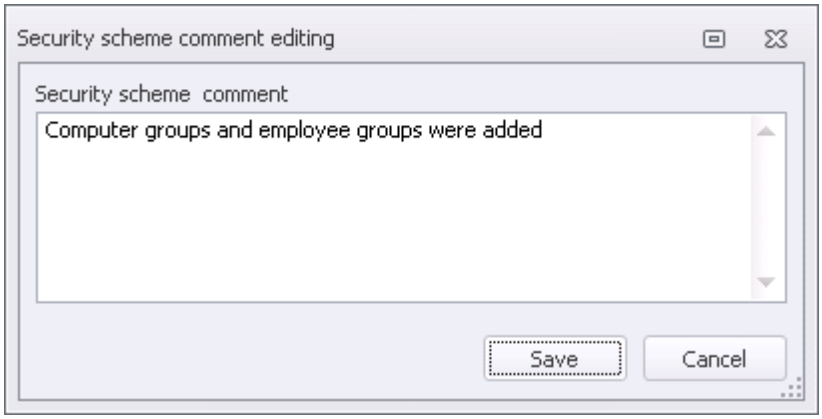
In comments you can specify additional information on your security schema. You can add comments to each version of security schema.
Comments to current security schema are displayed in brackets to the right from schema version number on the status panel.
You can view comments to all security schema versions in the **Select Security Schema** dialog (see "Viewing Old Security Schemas").

Note:
You can add comments to security schema regardless of its state (whether it is in editing mode or not).

To add/edit security schema comment:

1. Take one of the following steps:
   - *(For the current security schema only).* In Main Menu select **Security Schema > Edit Current Security Schema Comment**.
   - *(For any security schema version except the current one).* In the Main Menu select **Security schema > View Old Security Schema**. This opens **Select Security Schema** dialog. In this dialog, select the row containing the right security schema version. Then click **Edit Comment**.

   These actions open **Security schema comment editing** dialog.



2. Enter your comment in the dialog box. Maximum comment length - 512 characters.
3. Click **Save**.

3.4.2.4 Editing Security Schema

Warning!
Security schema can be edited only by one user at a time. If security schema is edited, an information about user who edits and computer where editing is performed, is displayed at red-highlighted string at the top of main screen. See details in "Awaiting Editing Ends. Unlocking Security Schema".

All changes are implemented in security schema editing mode. This mode protects existing security schema from potential editing errors. The System automatically switches to editing mode just after any Console user makes any change of security schema parameters. Changes are saved only by **Save** command.

Warning!
If server connection terminates during security schema editing process, all unsaved changes will be lost.

To edit security schema:

1. Take one of the following steps:
   - in the Main Menu select **Security Schema > Edit**
   - click **Edit** on Toolbar
   - make any change of security schema parameters (security policies, computers, employee accounts, device white lists, signature categories).

   These actions open security schema editing mode.

Note:
You can edit only the latest version of security schema. Thus schema editing is not available when viewing previous versions. To open current security schema version, select **Security schema > View Latest Security Schema** from the main menu.
Information on security schema currently used by Management Console is displayed on the status bar.

2. Edit security schema parameters:
   - security policies (see "Security Policies")
   - computer groups (see "Computers")
   - employee accounts lists (see "Employees")
   - device white lists (see "White Lists")
   - file signature categories (see "Signatures").
3. When all changes are made, save your security schema. To do this, follow these steps:
   - click **Save** at the top string of main screen workspace where "*Security Schema have changed. Save changes?*" message is displayed
   - in the Main Menu select **Security schema > Save**
   - click **Save** on Toolbar.

These actions save the changes and close security schema editing mode.

Note:
To discard changes:
- at the top string of main screen workspace where "*Security Schema have changed. Save changes?*" message is displayed click **Cancel**
- select **Security Schema > Undo editing**
- click **Undo editing** button on the toolbar.

This closes schema editing mode discarding all changes.

3.4.2.4.1 Awaiting Editing Ends. Unlocking Security Schema

Security schema can be edited only by one user at a time. Changes are applied only after you have saved your security schema.

If security schema is edited, an information about user who edits and computer where editing is performed, is displayed at red-highlighted string at the top of main screen.

If you try to edit any parameters of security schema (security policies, computers, employee accounts, device white lists, signature categories) while security schema is editing by another user:

1. Management Console displays warning message.
2. When another user saves his changes (or cancel them) Windows system tray would display notification: "***Security schema is available for editing***".

Information about user who edits the schema currently, is displayed at the string at the top of main screen and in status bar.

Security schema might be blocked even if it is not being edited. This may occur if the last editing operation wasn't properly completed (i.e. due to disconnection from the server).

When user who blocked a schema will connect the server again, the security schema automatically unlocks and all unsaved changes made by this user are lost.

There is also a special function that targets the blocking issue - security schema unblock.

Warning!
Security schema can be unblocked only by Superuser.

To unblock security schema,

in the Main Menu click **Security Schema > Unlock Security Schema**.

All unsaved changes will be lost.

3.4.2.5 Updating Security Schema

The system can be simultaneously operated by multiple users. To keep security schema details in Management Console up-to-date, run updates regularly. The schema update security is automatically (in the process of connecting to the server) or manually (when working with the Microsoft Management Console).

You might need to upgrade your security schema in the following cases:

- registering a new computer;
- registering an unknown employee;
- modifying your security schema.

To update security schema manually, do one of the following:

- select **View > Refresh** in the Main Menu;
- click **Update** in Toolbar.

3.4.2.6 Exporting/Importing Security Configuration

You might need to save existing settings of the System. You might want to do this, if you reinstall your operating system or InfoWatch Device Monitor.

Configuration exporting saves to `*.dmc` file the current version of a security schema including:

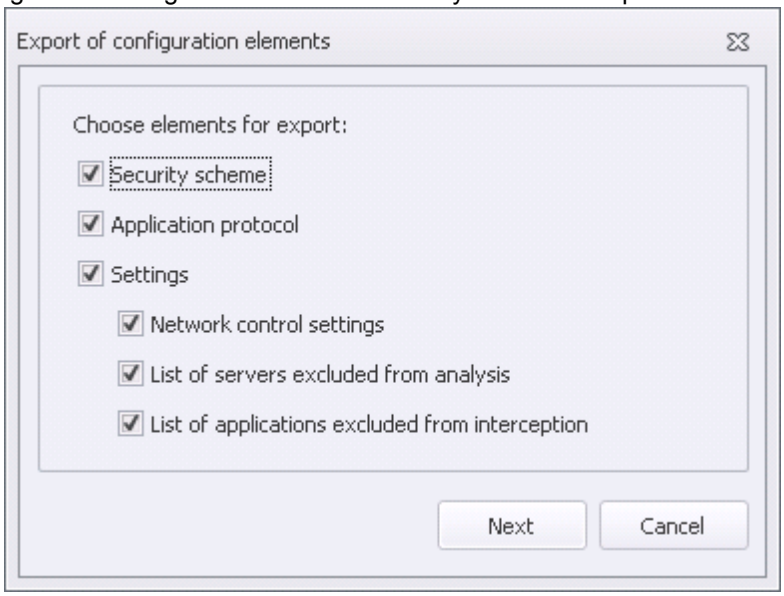
- security policies with sets of rules;
- employee groups
- computer groups
- device white lists
- signature categories.

The application protocol and general System settings are also subject to save.

You can import your saved settings into new security schema later.

To export System configuration:

1. In the Main Menu select **Tools > Export Configuration**.
2. In the opened dialog select configuration elements which you want to export.



3. Click **Next**.
4. In the saving dialog enter a name of the file where your data will be exported and specify a directory for the file. Click **Save**.

To import security schema:

1. In the Main Menu select **Tools > Import Configuration**.

2. In the next dialog choose the file that contains previously saved configuration and click **Open**.

This imports saved security schema settings into the active security schema. If your current security schema contains items with similar names, the System will add **1** to each imported name.

3.4.3 Security Schema Setup

After system installation, you must configure your security schema. Security schema is configured as follows:

1. Configure "*Default*" employee group and "*Default*" computer group.
2. Configuring the rest of security settings.

Security schema configuration principles:

- security policy must be created before you create an employee group or computer group the policy will be assigned to
- it is recommended that you assign an individual security policy for each employee group and computer group
- each security policy assigned to a group must have a specific set of rules.

Adding computers to security schema

There are two ways to add a managed computer:

- add a new computer automatically during registration
- add computer manually via Management Console.

In case of automatic registration a computer is added to "*Default*" group. Later you can move it to other groups.

If you add it manually, you can select the group immediately.

Adding employee accounts to security schema

You can add new account information manually or automatically. You can register a new employee while editing your security schema. However, if an unknown employee is registered on a computer, the account will automatically be added to security schema ("*Default*" employee group).

Adding white lists to security schema

Before you create a white list, add device models and instances to the database. Then devices white list is created for a specific employee/employee group/computer/computer group. These employees/computers have access to whitelisted device models and instances regardless the policy. When a white list record expires, access rights are distributed according to the policies.

Security schema configuration details are available in the following subsections:

- Security Policies
- Rules
- Employees
- Computers
- Mobile Devices
- White Lists
- Signatures
- Application Protocol
- Temporary Employee Access to Network
- Temporary Employee Access to Devices

3.4.3.1 Security Policies

Note:
For security policy configuration guidelines see "Security Policies and Rules".

Each security policy is a set of rules that define employees' level of access to controlled files and devices.

Security policies are assigned to **employee groups** and **computer groups**. Security policy of employee group affects all the employees included to this group. Security policy of computer group affects all the employees which work at managed computers included to this computer group.

Security policies are managed in **Policies** section. To go to this section, click **Policies** button in Navigation pane or select in Main Menu **Go > Policies**.

For security policy managing guidelines see:

- Viewing Security Policies
- Adding and Configuring New Security Policy
- Editing Security Policy
- Deleting Security Policy

3.4.3.1.1 Viewing Security Policies

Policies area of Navigation pane displays a list of security schema policies. Main screen workspace displays a list of security policy rules.

> **Note:**
> Use additional options to adjust list display (see "Additional Features").

To view security policy rules,

select security policy name in **Policies** area of Navigation pane.

Rules are displayed in a form of a table where each row contains a rule. Columns contain general rule properties. Each rule has an icon depicting the rule's coverage and a color mark depicting if a rule is an allowing one (green), forbidding (red) or partially restricting (yellow).

Extended information on each rule is displayed on **Details** panel.

To view all rule properties,

select the row that contains the rule name in the main screen workspace.

This opens a table containing rule information on **Details** panel.

General information:

- **Name**. Rule name.
- **Policy**. Name of security policy that contains the rule.
- **Interceptor**. Interceptor type assigned to the rule.
- **Operation**. Operation, controlled by the rule.
- **Period**. Rule starting and expiry time.

Application Monitor rules feature additional details:

- **White Lists**. White list of applications mentioned in the rule.
- **Black Lists**. Black list of applications mentioned in the rule.

Cloud Storage Monitor rules feature additional details:

- **Google drive**.Shows current access type.
- **DropBox**. Shows current access type.
- **YandexDisk**. Shows current access type.
- **OneDrive**. Shows current access type.
- **EverNote**. Shows current access type.
- **SugarSync**. Shows current access type.

File Monitor rules feature additional details:

- **Exclude from interception**. Indicates if files corresponding to mask or category won't be proceeded.
- **Use file mask**. File mask attribute.
- **File mask**. Mask that selects the files covered by the rule.
- **Use category**. Attribute of file filtering against signature categories (see "Signatures").
- **Category**. Signature category for file formats selection.
- **Create shadow copy**. Stored files shadow copying attribute.
- **Limit by minimum file size**. Attribute of minimum size restriction for shadow copied file.
- **Minimum file size**. Lower limit of file size.
- **Limit maximum file size**. Attribute of maximum size restriction for shadow copied file.
- **Maximum file size**. Upper limit of file size.

Print Monitor rules feature additional details:

- **Use task mask**. Task mask attribute.
- **Task mask**. Mask for selecting print jobs covered by the rule.
- **Use process mask**. Process mask attribute.
- **Process mask**. Mask of the process that initiated a print job.
- **Create shadow copy**. Printed document shadow copy attribute.

Device Monitor rules feature additional details:

- **Allow only for encrypted devices**. Action will be allowed, if the media is protected by supported encryption software.

IM Client Monitor rules feature additional details:

- **Create file shadow copy**. Indicates if a shadow copy of sending files should be created.
- **Minimum file size**. Lower limit of file size.
- **Maximum file size**. Upper limit of file size.
- **Maximum call size**. Length of call (in minutes) which should be saved in one shadow copy file.

Ftp Monitor rules feature additional details:

- **Create shadow copy**. Indicates if a shadow copy of FTP/FTPS-sent file should be created.
- **Minimum file size**. Lower limit of file size.
- **Maximum file size**. Upper limit of file size.

HTTP(S) Monitor rules feature additional details:

- **Do not create a shadow copy of traffic of internal resources.** Does not intercept objects sent within internal resources.
- **Create shadow request copy**. Value of document shadow copy sent by HTTP and HTTPS.
- **Minimum request size, Bytes**. Lower limit of file size.
- **Maximum request size, Mbytes**. Upper limit of file size.
- **Transferred via**. Indicates whether encrypted or any other traffic is being intercepted.

Network Monitor rules feature additional details:

- **Access**. Always has value "*Forbidden connections out of corporate network*".

Mail Monitor rules feature additional details:

- **Transferred via**. Indicates whether encrypted or any other traffic is being intercepted.

- **Maximum mail size, Mbytes**. Maximum mail size.

ScreenShot Control Monitor rules feature additional details:

- **Forbid employee to make a screenshot**. Any screenshots or when particular application run only.

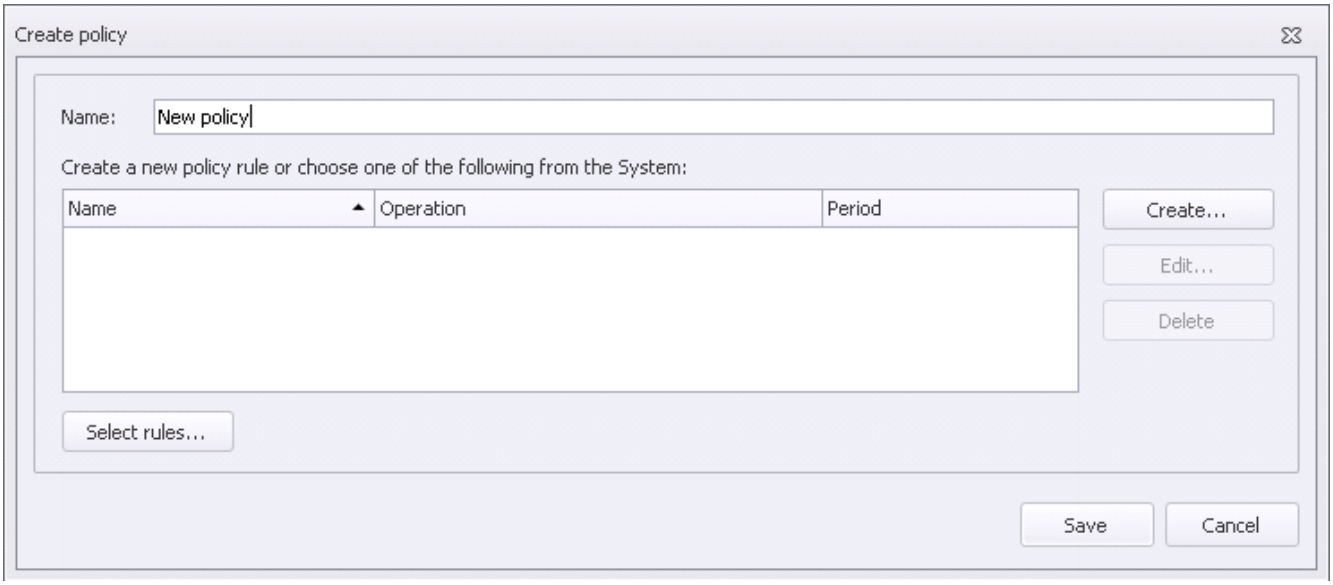
Note:
Information retrieved from some attributes is duplicated in the main screen workspace.

3.4.3.1.2 Adding and Configuring New Security Policy

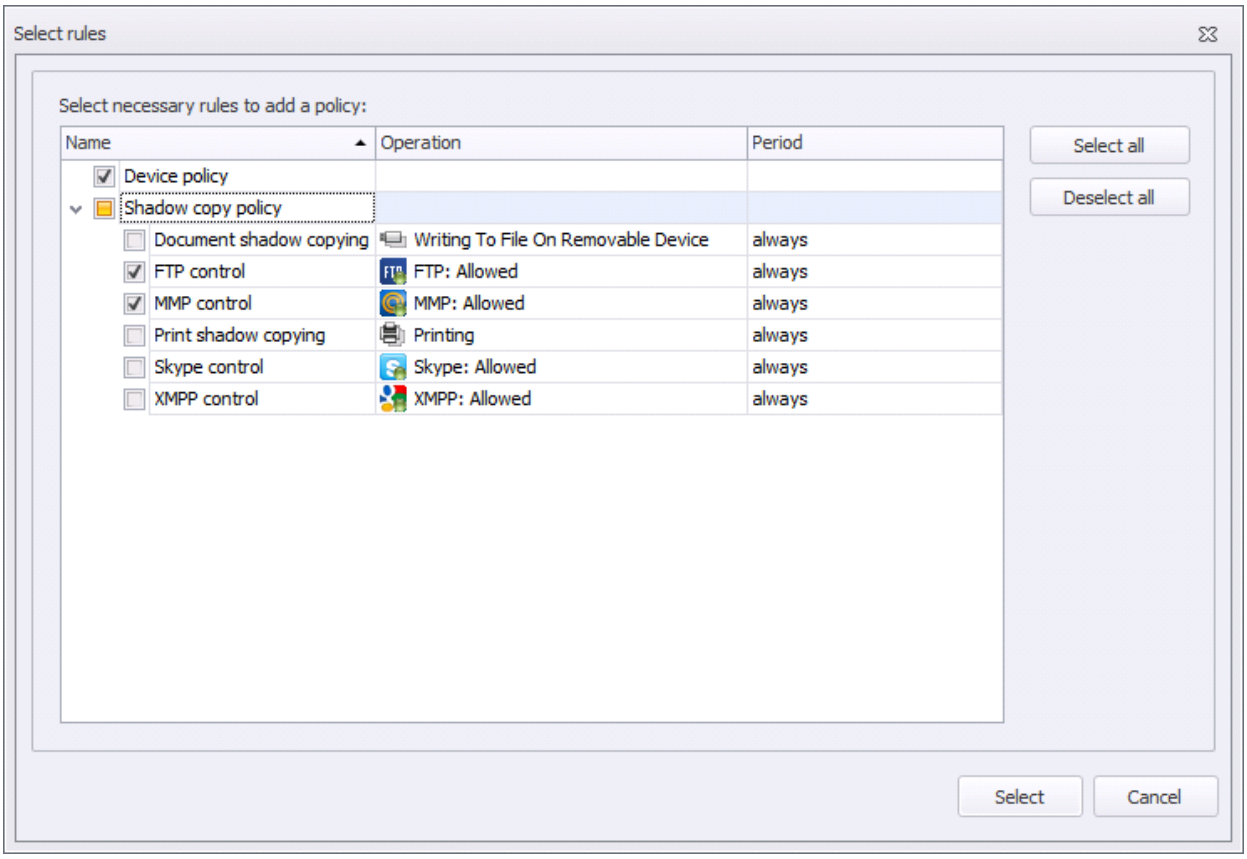
To add and configure security policy:

1. Go to **Policies**.
2. Take one of the following steps:
   - click **Create Policy** at the top of Navigation panel;
   - in Main Menu select **Edit > Create Policy**.

   This opens **Create policy** dialog.



3. In **Name** field, enter new security policy name. Maximum length is 64 characters.
4. Make a list of rules for new security policy:
   - To copy rule from another policy click **Select rules**. In new dialog flag the rules you want to copy to a new security policy.



You can also select the whole policy - then all rules it contains will be added to a new security policy. After you mark all rules click **Select**.

- To create a new rule click **Create** and specify rule parameters as described:
  - Configuring Application Monitor Rule
  - Configuring Cloud Storage Monitor Rule
  - Configuring Device Monitor Rule
  - Configuring File Monitor Rule
  - Configuring FTP Monitor Rule
  - Configuring HTTP(S) Monitor Rule
  - Configuring IM Client Monitor Rule
  - Configuring Mail Monitor Rule
  - Configuring Network Monitor Rule
  - Configuring Print Monitor Rule
  - Configuring Screenshot Control Monitor Rule

You can also edit or delete policy rule by selecting it and clicking **Edit** or **Delete** appropriately.

5. When all rules to be included to policy are defined, click **Save**.

Warning!
To apply changes you have to save current security schema (see "Editing Security Schema"). If you don't save your security schema, all changes will be discarded.

Later you will be able to edit or remove security policies: (see "Editing Security Policy", "Removing Security Policy "), as well as their rules (see "Adding a Rule", "Editing a Rule", "Deleting a Rule", "Copying a Rule").

3.4.3.1.3 Editing Security Policy

To edit security policy:

1. Go to **Policies**.
2. In **Policies** area of Navigation pane select security policy name.
3. Take one of the following steps:
   - in the Main Menu select **Edit > Edit Policy**
   - click **Edit Policy** at the top of Navigation pane
   - double-click selected security policy name.

   These actions open **Edit Policy** dialog.
4. In this dialog, edit security policy name by entering a new one in **Name** field.
5. Click **Save**.

Warning!
To apply changes you have to save current security schema (see "Editing Security Schema"). If you don't save your security schema, all changes will be discarded.

3.4.3.1.4 Deleting Security Policy

Warning!
The policy appointed at least one employee group or computer groups, cannot be deleted. Before security policy deleting make sure that this policy is not appointed to any employee group (see "Viewing Employee Details") or computer group (see "Viewing Computer Details").

To delete security policy:

1. Go to **Policies**.
2. In **Policies** area of Navigation pane select security policy name.
3. Take one of the following steps:
   - in the Main Menu select **Edit > Delete Policy**
   - click **Delete Policy** at the top of Navigation pane.
4. In the following confirmation dialog select **Yes** to confirm that you want to remove security policy.

Warning!
To apply changes you have to save current security schema (see "Editing Security Schema"). If you don't save your security schema, all changes will be discarded.

3.4.3.2 Rules

Rules are used basing on the security policy they are assigned to. Each security policy has individual set of rules.

Information on rules is available in the following subsections:

- Rules Application
- Adding a Rule
- Editing a Rule
- Deleting a Rule
- Copying a Rule

3.4.3.2.1 Rules Application

To make a set of rules effective, keep in mind all possible instances of their application.

The event is considered as satisfying the rule if it meets all rule parameters (for example both event time is within rule time period and a size of outgoing document is not less than minimal file size and so on).

If the event meets several rules at the same time, then in general more limiting rule overrides the permissive one. In details:

1. The excluding rule (*Exclude from interception* option is enabled: see "Configuring File Monitor Rule") has a highest priority.
2. The forbidding rule overrides the permitting one.

   Example 1. The **Device Monitor** rule (see "Configuring Device Monitor Rule") with *No access* limitation overrides rule which permits *Read only*, and the last one overrides a rule with *Full access to encrypting devices*.

   Example 2.The For **FTP Monitor** rule (see "Configuring FTP Monitor Rule") with *Forbid using FTP-protocol* is applied instead of rule with *Full access to encrypting devices*, and the last one - instead of rule with *Permit using FTP-protocol*.

   Example 3. The **HTTP(S) Monitor** rule (see "Configuring HTTP(S) Monitor Rule") with *Not intercept internal requests* option overrides a rule with this option disabled.
3. The rule creating shadow copies (*Create a shadow copy* option is enabled) overrides a rule without shadow copying.

Other important information on rules application:

- Device Monitor Rules Application
- Creating Shadow Copies and Blocking Operations Due to Free Space Shortage

3.4.3.2.1.1 Device Monitor Rules Application

Access to all Device Monitor interceptor controlled peripherals is a collection of rules assigned to each device.

Employee access rights are defined basing on:

- rules applied to employee groups which an employee is included in
- rules applied to computer groups of the computer using for device access
- white lists.

During Client installation controlled are fully accessible by default. Therefore, all forbidden operations with the device must be set explicitly (i.e., in form of a rule).

Initially, each new registered computer is added to the *Default* group. This group has a *"Shadow copy policy"* which contains no rules. Device rules are nor applied to default employees. Thus, the System always allows access to all managed computers after installation.

For example:

There is a rule that lets computer group A write to CD/DVD drive. Workstation WS belongs only to computer group A. Employee Smith belongs only to employee group B with no device rules. Employee Smith tries to view a CD on computer WS. In this case, employee won't be able to view CD contents of a disk and write new data.

You can assign multiple rules, in several policies either, with various access levels to the same device. This causes rule conflict. General conflict resolution principle: higher limit means higher priority (see the table for further details).

Device type	All devices, except CD/DVD, Floppy drives and removable storage devices	CD/DVD	Floppy drives and removable storage devices
Access in descending order of priority	1. Forbidden	1. No access 2. Read-only	1. No access 2. Read-only 3. Full access to the encrypted

Device type	All devices, except CD/DVD, Floppy drives and removable storage devices	CD/DVD	Floppy drives and removable storage devices
			devices only

Examples:

Example 1. There is a rule for computer group C that forbids an access to removable storage device. There is a rule in employee group D policy that allows access to removable storage devices in read only mode. Employee Smith belongs to employee group D and tries to access removable storage device from computer that belongs to computer group C. Conflict is resolved in favor of more restrictive rule, i.e. employee Smith cannot read from removable storage device.

Example 2. There is a rule in employee group E policy that allows read-only access to removable storage device. There is a rule in employee group F that grants a full access only to encrypted removable storage devices. Employee Smith belongs to both groups. Conflict is resolved in favor of the more restrictive rule: i.e. employee Smith can get a read-only access: both encrypted and not encrypted (less priority rule is not applied at all).

Rules for certain controlled device types may overlap (see the table). These rules should also be considered when banning access to controlled devices.

Note:
A list of controlled devices types and a set of matching operations is provided in "Configuring Device Monitor Rule".

Rule	Overlapping rules	Notes
Floppy	No	
CD/DVD	No	
Parallel port (LPT)	Local printer (LPT) Imaging devices (LPT)	If there is no access to LPT port, the device connected to this port will be unavailable
Serial port (COM)	Modem Local printer (COM) Imaging devices (COM)	A modem connected to COM port is only accessed basing on COM port rule If there is no access to COM port, the device connected to this port will be unavailable
Removable Storage (USB and IEEE 1394 devices)	FireWire (IEEE 1394)	If there is no access to FireWire (IEEE 1394) port, the device connected to this port will be unavailable
Local Printer (with USB, IEEE 1394, SCSI connection, etc.)	FireWire (IEEE 1394) Serial port (COM) Parallel port (LPT)	If there is no access to FireWire (IEEE 1394), COM, LPT port, the device connected to this port will be unavailable
Image-processing Devices (cameras, scanners)	FireWire (IEEE 1394) Serial port (COM) Parallel port (LPT)	If there is no access to FireWire (IEEE 1394), COM, LPT port, the device connected to this port will be unavailable
Bluetooth Device	No	
IrDA Device	No	
Other USB Devices	No	
FireWire	Removable storage device (IEEE 1394)	If there is no access to FireWire (IEEE 1394) port, the device connected to this

Rule	Overlapping rules	Notes
	Local printer (IEEE 1394) Imaging devices (IEEE 1394)	port will be unavailable
Modem	Serial port (COM)	Modem access rules do not affect modems connected to COM port. A modem connected to COM port is only accessed basing on COM port rule
Smart Card Reader	No	
Tape Device	No	
Multifunctional Device	No	
PCMCI device	No	
USB Network Adapter	No	
Network printer	No	
Pocket Computer (Windows Mobile and Palm OS pocket computers)	No	

3.4.3.2.1.2 Creating Shadow Copies and Blocking Operations Due to Free Space Shortage

Shadow copy of a file, document, message or chat is created when all conditions are met:

1. Applied rule creates shadow copies and file size meets the requirements.
2. Free space at managed computer is more than minimum size required by the policy (see "Common Settings for Clients", **Free clients' disk space** setting, default value is 10%).
3. Managed computer has more free space then shadow copy creation requires.

Warning!
If there is at least one valid rule that enables shadow copying, and there is less free space available on the computer than required for file saving, then the controlled operation will be performed without shadow copy creation. Such an event will be displayed in a Management Console (see "Viewing Events") wit "*Error of copy creating*" state.

Besides shadow copies, managed computer temporary (until the connection with Device Monitor Server is established) stores information about events. For this purpose the drive where Device Monitor Client is installed has dedicated space for storing up to 30000 events (about 300 MB). If:

- Device Monitor Client did not have connections with Device Monitor Server so that there is stored more than 30000 events controlled by rules defined for employee/computer

and

- in common settings for Clients the **If there is not enough disk space to save shadow copy, the operation will** setting has **Operation is blocked** value,

then **any employee's actions controlled by security schema will be blocked**.

3.4.3.2.2 Adding a Rule

To add a rule to security policy:

1. Go to **Policies**.
2. In **Policy** area of Navigation pane select the name of the security policy you want to add the rule to.

3. Take one of the following steps:
   - in Main Menu click **Edit > Create Rule**
   - click **Create Rule** in the top of **Policies** area
   - right-click in **Policies** area and select **Create Rule** from the drop-down list
   - press **Ctrl+Shift+N**.

   These actions open rule edit dialog.
4. Specify the interceptor rule:
   - Configuring Application Monitor Rule
   - Configuring Cloud Storage Monitor Rule
   - Configuring Device Monitor Rule
   - Configuring File Monitor Rule
   - Configuring FTP Monitor Rule
   - Configuring HTTP(S) Monitor Rule
   - Configuring IM Client Monitor Rule
   - Configuring Mail Monitor Rule
   - Configuring Network Monitor Rule
   - Configuring Photo Monitor Rule
   - Configuring Print Monitor Rule
   - Configuring Screenshot Control Monitor Rule
5. After you have set all necessary parameters, click **OK** in rule settings.

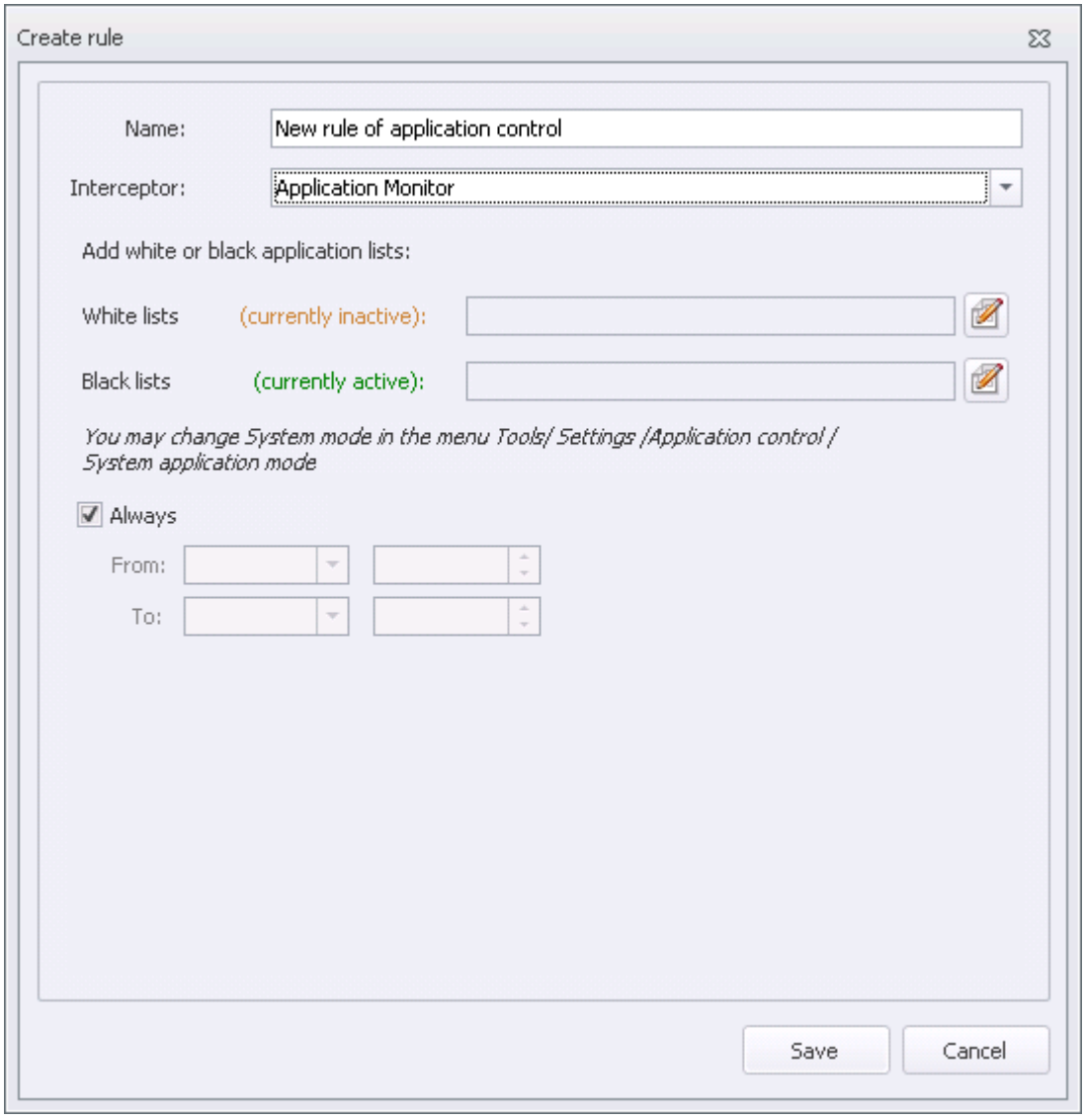
Warning!
To apply changes you have to save current security schema (see "Editing Security Schema"). If you don't save your security schema, all changes will be discarded.

3.4.3.2.2.1 Configuring Application Monitor Rule

Application Monitor interceptor provides application access control via black and white lists.

See details on configuring System operation mode (active white lists or active black lists) in "Application control".

See details on application lists formation in "Application Protocol".



To configure the rule, perform the following steps:

1. Go to **Policies** section.
2. In **Policies** area at Navigation pane select a security policy which you want to add a rule to.
3. Take one of the following steps:
   - in the Main Menu select **Edit > Create rule**
   - click **Create rule** at the top of **Policies** area
   - right-click at the empty space in **Policies** area and select **Create rule** from the drop-down list.
4. In **Create rule** dialog in **Interceptor** field select **Application Monitor**.
5. Enter rule name to **Name** field.
6. Add white or black lists by pressing button.
7. Define a period of rule action. By default, the rule is always in effect (**Always** option is checked). To specify rule duration, clear **Always** check box and specify dates and time in **From** and **To** fields.
8. When all parameters are configured, click **Save**.

To set up the System for applications operating mode:

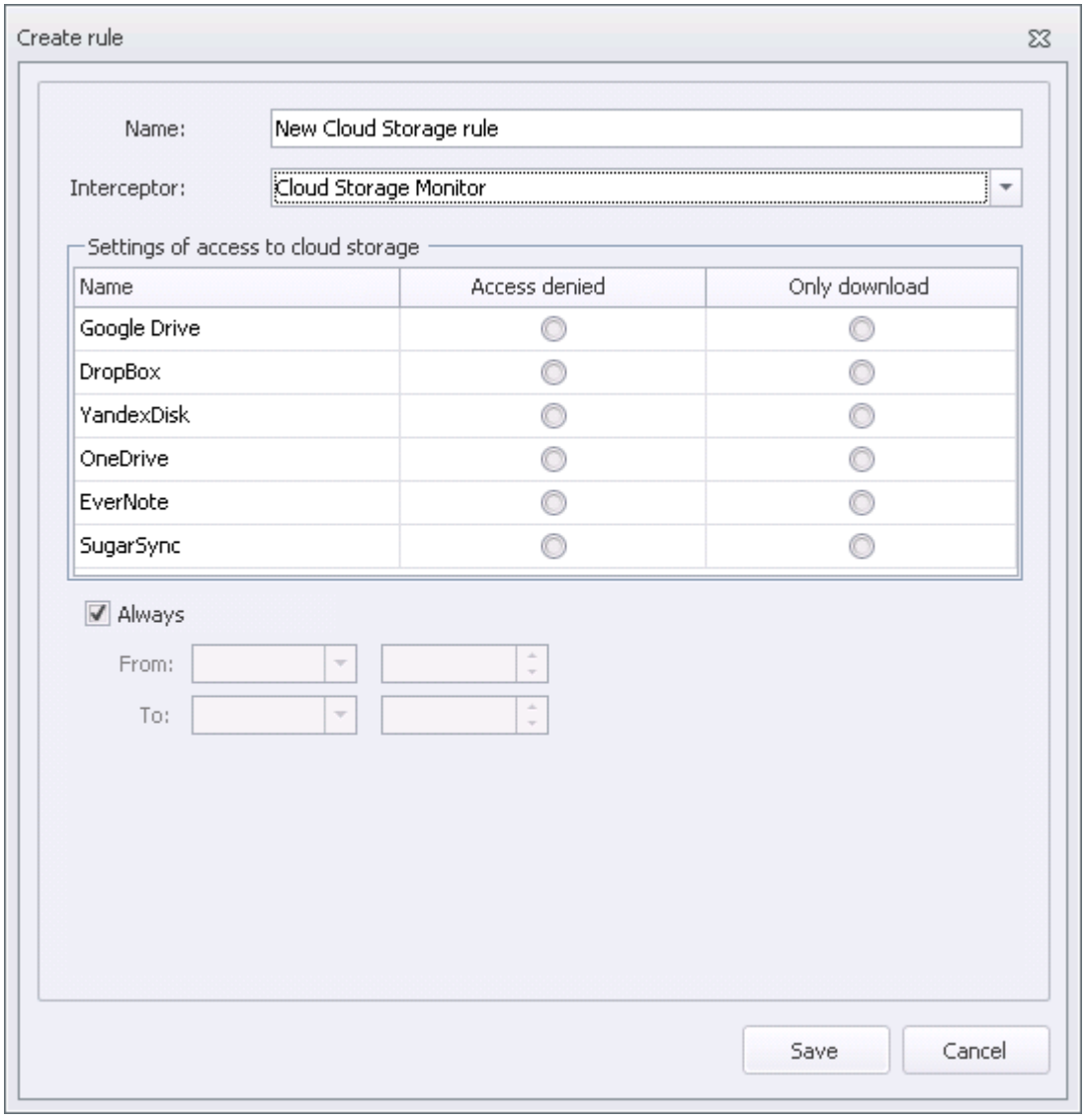
1. Go to **Tools > Settings**.
2. At the left panel select **Application control** node.

3. Pick one of two processing modes:
   - **White lists** - all applications from the lists selected in the Application Monitor rule from the resulting policy are allowed. Other applications are forbidden.
   - **Black lists** - all applications from the lists selected in the Application Monitor rule from the resulting policy are forbidden. Other applications are allowed.
4. Click **Save**.

3.4.3.2.2.2 Configuring Cloud Storage Monitor Rule

Cloud Storage Monitor interceptor provides web-client control. One can manage the following cloud storages:

Storage name	Variants of devise usage access restrictions
Google Drive	Access Denied / Only download
DropBox	Access Denied / Only download
YandexDisk	Access Denied / Only download
OneDrive	Access Denied / Only download
EverNote	Access Denied / Only download
SugarSync	Access Denied / Only download



To configure the rule, perform the following steps:

1. Go to **Policies** section.
2. In **Policies** area at Navigation pane select a security policy which you want to add a rule to.
3. Take one of the following steps:
   - in the Main Menu select **Edit > Create rule**
   - click **Create rule** at the top of **Policies** area
   - right-click at the empty space in **Policies** area and select **Create rule** from the drop-down list.
4. In **Create rule** dialog in **Interceptor** field select **Cloud Storage Monitor**.
5. Enter rule name to **Name** field.
6. In **Setting of access to cloud storage** mark the option for access limitation (see table above).
7. Define a period of rule action. By default, the rule is always in effect (**Always** option is checked). To specify rule duration, clear **Always** check box and specify dates and time in **From** and **To** fields.
8. When all parameters are configured, click **Save**.

3.4.3.2.2.3 Configuring Device Monitor Rule

Device Monitor interceptor allows you to control employee access to peripheral devices and the devices connected to the thin and thick terminal clients.

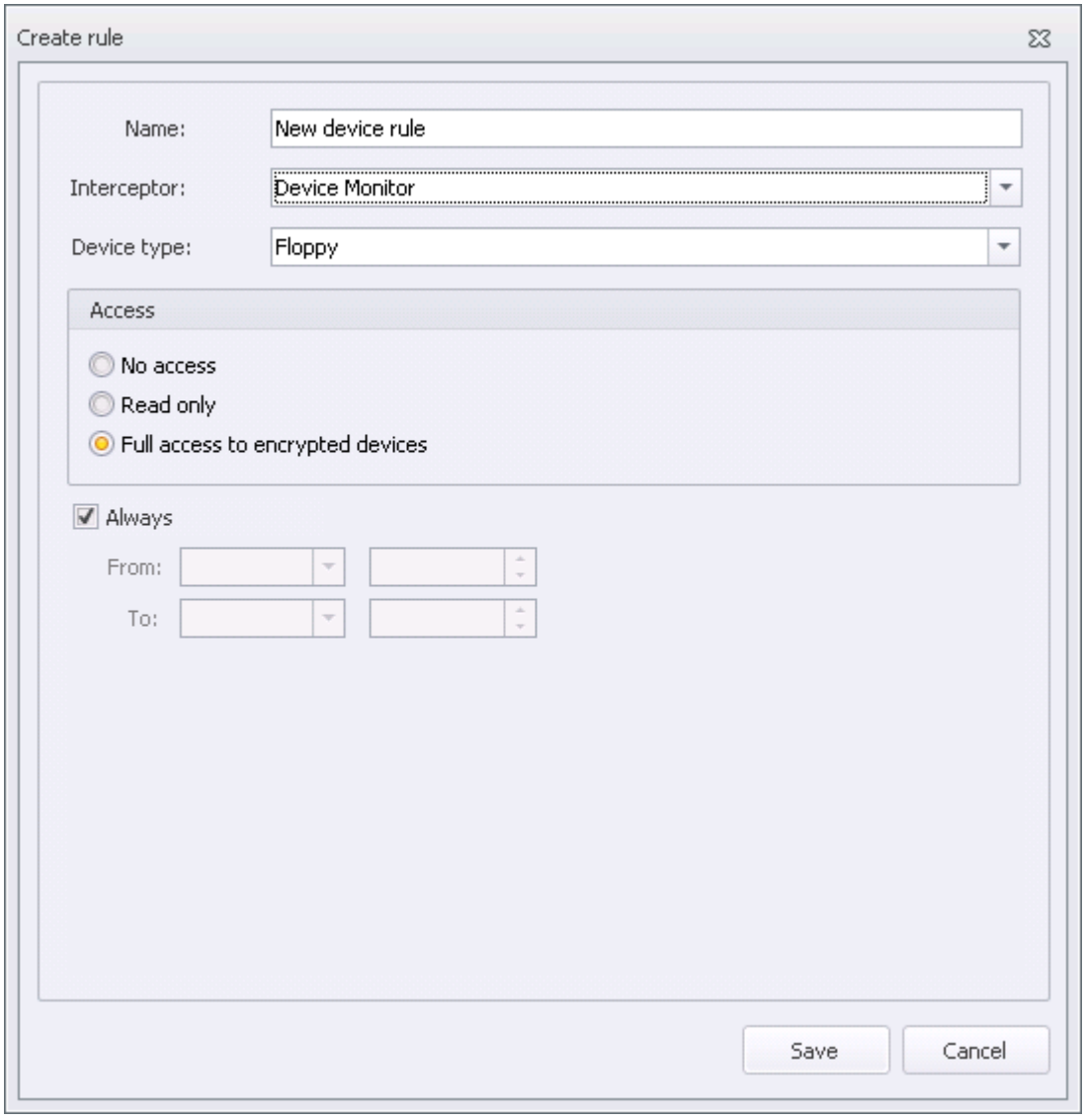
Control of terminal clients, which are connected via Microsoft RDP or Citrix ICA can be useful in the following situation:

1. Remote user connects to Device Monitor computer from terminal client.
2. There is a storage or a printer connected to terminal client.
3. Remote terminal client attempts to print out/copy data from Device Monitor Workstation (Terminal storage/ printer should be connected to Device Monitor Workstation via Microsoft RDP or Citrix ICA in this case).

Device type	Available access restrictions
Floppy	Full access to encrypted devices only / Read only / Access denied
CD/DVD	Read only / Access denied
LPT port	Denied
COM port	Denied
Portable disk drives (USB and IEEE 1394 devices)	Full access to encrypted devices only / Read only / Access denied
Local Printer (with USB, IEEE 1394, SCSI connection, etc.)	Denied
Image Editing Devices (cameras and scanners)	Denied
Bluetooth Device	Denied
IrDA Device	Denied
Other USB Devices	Denied
FireWire	Denied
Modem	Denied
Smart Card Reader	Denied
Tape Drive	Denied
Multifunctional Device	Denied
PCMCI device	Denied
USB Adapter	Denied
Pocket Computer (Windows Mobile and Palm OS pocket computers)	Denied
Network printer	Denied
Microsoft RDP or Citrix ICA connection control	
Terminal printer	Denied
Terminal storage	Read only / Access denied
Terminal port (thin client port)	Denied
Terminal Plug and Play devices	Denied

Note:
InfoWatch Device Monitor supports devices encrypted by InfoWatch CryptoStorage SOHO 2.1, InfoWatch CryptoStorage Enterprise 1.0, Kaspersky KryptoStorage 1.0 and TrueCrypt 7.1.

Warning!
If event matches multiple rules, see "Rules Application" and "Device Monitor Rules Application".



To configure the rule, perform the following steps:

1. Go to **Policies** section.
2. In **Policies** area at Navigation pane select a security policy which you want to add a rule to.
3. Take one of the following steps:
   - in the Main Menu select **Edit > Create rule**
   - click **Create rule** at the top of **Policies** area
   - right-click at the empty space in **Policies** area and select **Create rule** from the drop-down list.
4. In **Create rule** dialog in **Interceptor** field select **Device Monitor**.
5. Enter rule name to **Name** field.
6. Select a peripheral type controlled by this rule from **Device type** drop-down list.
7. In **Access** area select needed access level (see table above).
8. Define a period of rule action. By default, the rule is always in effect (**Always** option is checked). To specify rule duration, clear **Always** check box and specify dates and time in **From** and **To** fields.
9. When all parameters are configured, click **Save**.

3.4.3.2.2.4 Configuring File Monitor Rule

File Monitor interceptor lets to monitor operations of writing to the file at removable device, at that only successful operation accomplishment is registered. This enables monitoring following employees' actions:

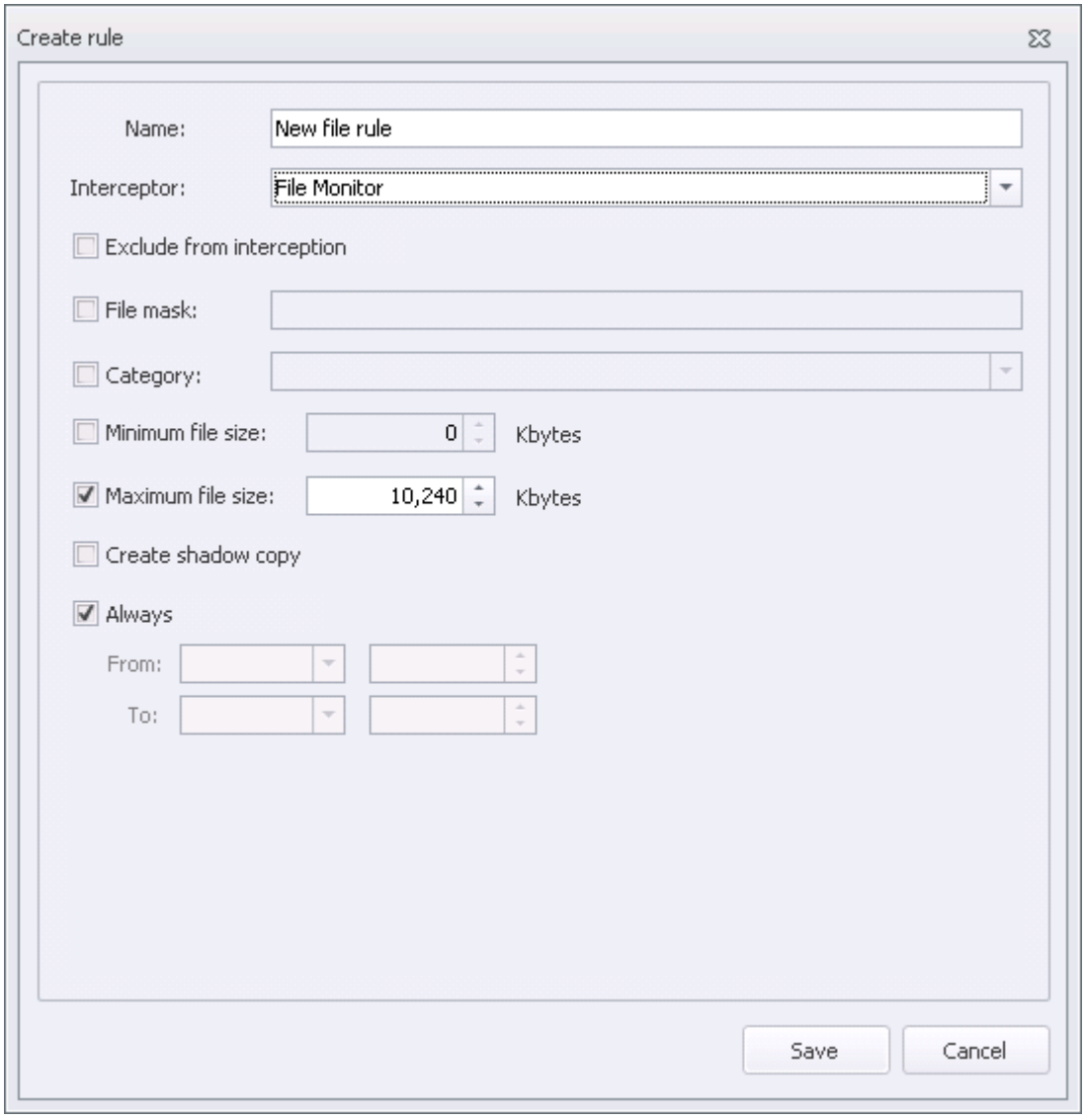
- file creating/editing at removable device
- file copying/moving to removable device. In this case operations of file copying/moving from managed computer, another removable device or network resources are monitored.

Warning!

The file is subject to **File Monitor** rule if **ALL** file parameters meet rule conditions. For example, if the rule sets shadow copying and **maximum and minimum file size** are specified, then processed file should have a size within specified range.

Warning!

Information about rule conflict resolving see in "Rules Application".



To configure the rule, perform the following steps:

1. Go to **Policies** section.
2. In **Policies** area at Navigation pane select a security policy which you want to add a rule to.
3. Take one of the following steps:

- in the Main Menu select **Edit > Create rule**
- click **Create rule** at the top of **Policies** area
- right-click at the empty space in **Policies** area and select **Create rule** from the drop-down list.

4. In **Create rule** dialog in **Interceptor** field select **File Monitor**.
5. Enter rule name to **Name** field.
6. To make a rule defining interception exclusion, flag **Exclude from interception**. There will be no events neither shadow copies created for file record operations which are subject of this rule.

> **Warning!**
> If file record event is a subject of several rules, the excluding rule has a highest priority.

7. You can constrain controlled files by mask. Flag **File mask** checkbox and specify mask. You can use wildcard characters when specifying a file mask: «?» to replace a character or «*» to replace a character set. For example, `*.doc`. The space character is interpreted as a part of file name.
8. You can constrain controlled files by signature category (see "Signatures"). Flag **Category** checkbox and select a category from drop-down list: the rule will be applied to files with chosen signature type.
9. You can constrain controlled files by size. Specify file size limits in **Minimum File Size** and **Maximum File Size** fields.
10. If you want to create shadow copies of outgoing files and then analyze them in Traffic Monitor, flag **Create a shadow copy**.

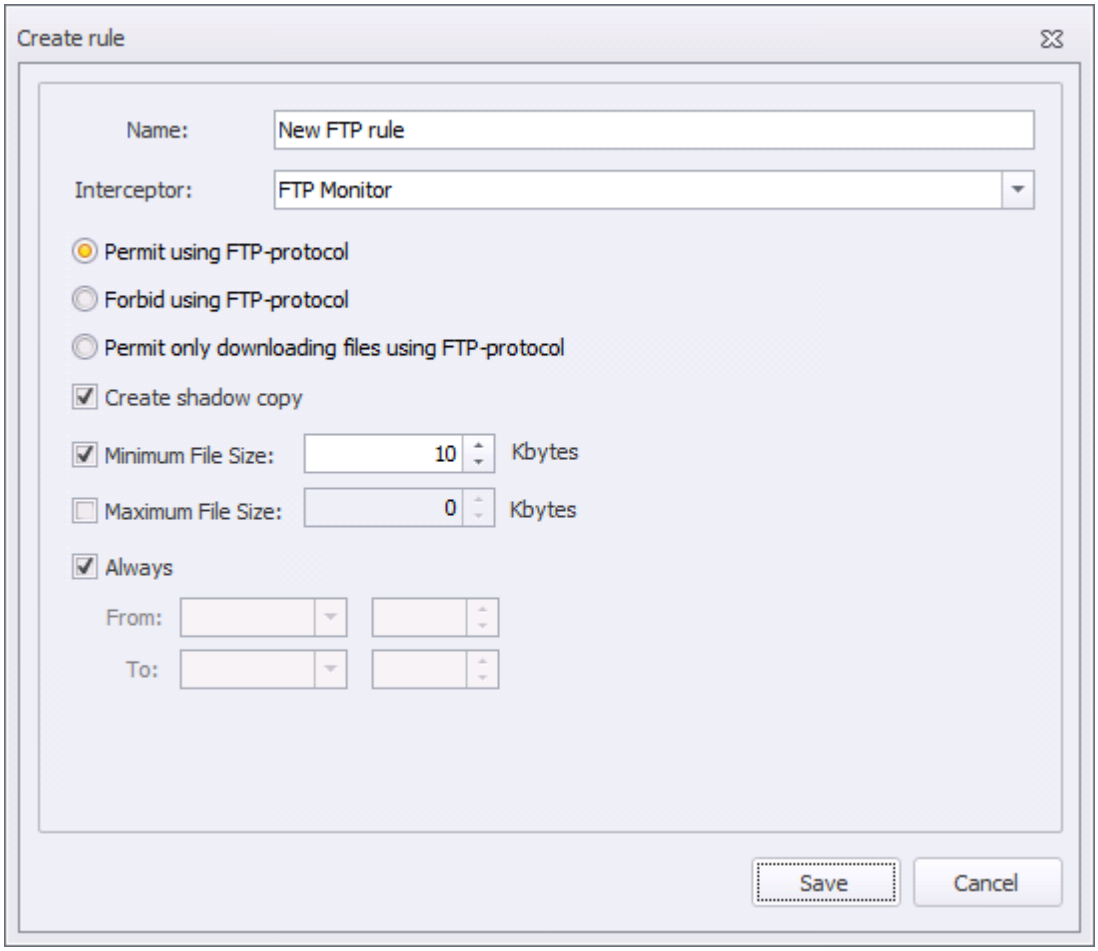
> **Warning!**
> If there is at least one valid rule for File Monitor that enables shadow copying, and there is less free space at the hard drive than required by the policy (see "Creating Shadow Copies and Blocking Operations Due to Free Space Shortage"), then file saving will be performed without shadow copy creating.

11. Define a period of rule action. By default, the rule is always in effect (**Always** option is checked). To specify rule duration, clear **Always** check box and specify dates and time in **From** and **To** fields.
12. When all parameters are configured, click **Save**.

3.4.3.2.2.5 Configuring FTP Monitor Rule

FTP Monitor interceptor lets to control data transfer through FTP/FTPS protocol.

> **Warning!**
>
> The file is subject to **FTP Monitor** rule if **ALL** file parameters meet rule conditions **EXCEPT** maximum and minimum file size. **Maximum file size** and **Minimum file size** are taken into consideration only for shadow copying. So if file size is within specified range, then file transfer event will contain a shadow copy; otherwise event will be created without shadow copy.



To configure the rule, perform the following steps:

1. Go to **Policies** section.
2. In **Policies** area at Navigation pane select a security policy which you want to add a rule to.
3. Take one of the following steps:
   - in the Main Menu select **Edit > Create rule**
   - click **Create rule** at the top of **Policies** area
   - right-click at the empty space in **Policies** area and select **Create rule** from the drop-down list.
4. In **Create rule** dialog in **Interceptor** field select **Ftp Monitor**.
5. Enter rule name to **Name** field.
6. Select inspection level for data transfer through FTP/FTPS protocol:
   - **Permit using FTP-protocol**
   - **Forbid using FTP-protocol**
   - **Permit only downloading files using FTP-protocol**
7. If you allowed using FTP/FTPS protocol then you can also configure creating of shadow copies of outgoing files. You can select **Create a shadow copy** check box and specify additional settings:
   - **Minimum File Size**. If the check box is selected, shadow copies will be enabled only for files of specified size or larger.
   - **Maximum File Size**. If the check box is selected, shadow copies will be enabled only for files of specified size or smaller.

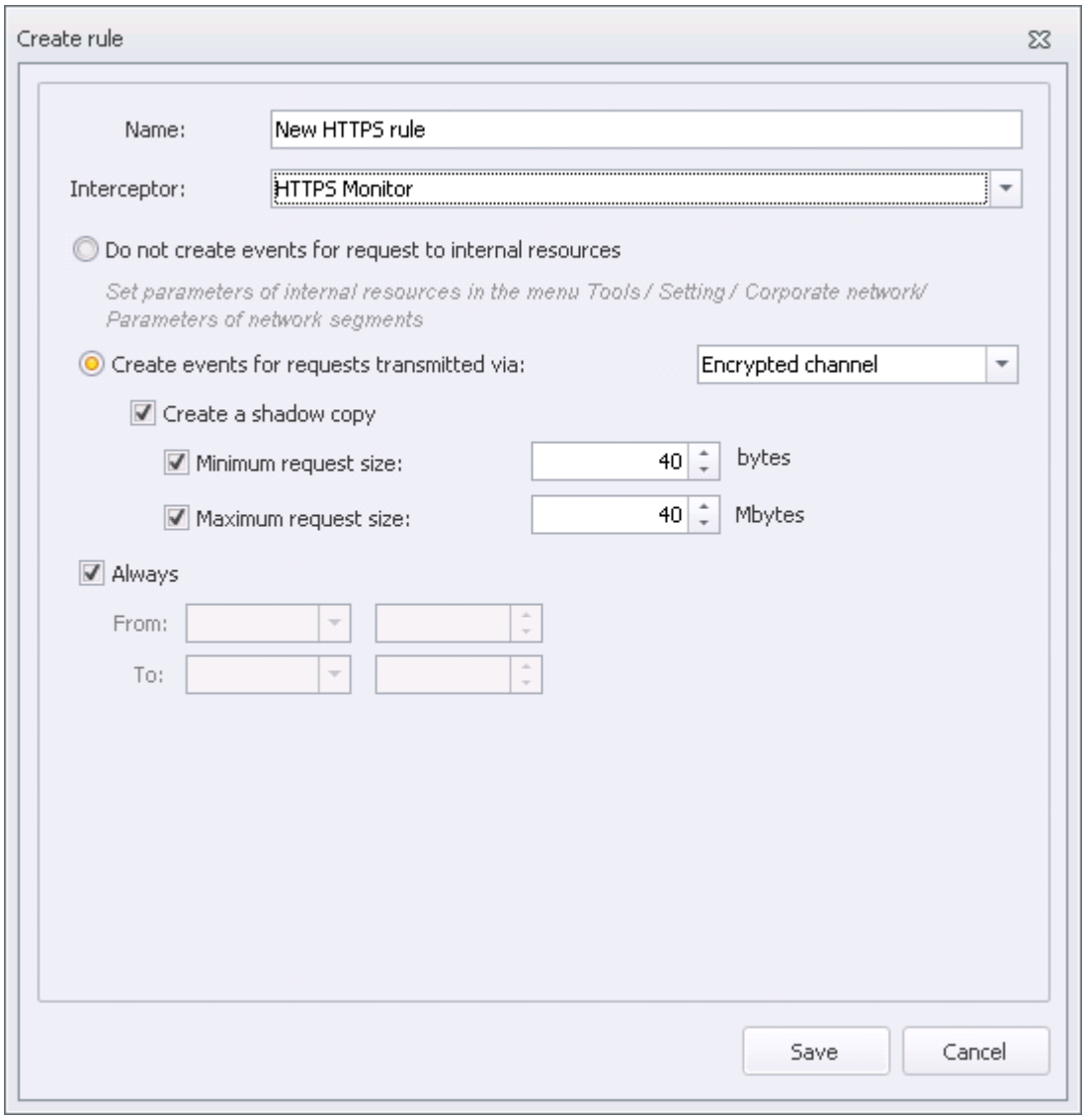
> **Warning!**
> If FTP Monitor rule should create a shadow copy of file but there is less free system drive space left than required by the policy (see "Creating Shadow Copies and Blocking Operations Due to Free Space

Shortage") then shadow copies of messages still will be created but files will be sent without shadow copying.

8. Define a period of rule action. By default, the rule is always in effect (**Always** option is checked). To specify rule duration, clear **Always** check box and specify dates and time in **From** and **To** fields.
9. When all parameters are configured, click **Save**.

3.4.3.2.2.6 Configuring HTTP(S) Monitor Rule

HTTPS Monitor interceptor allows you to control transferring data via HTTP and HTTPS protocol.



To configure the rule, perform the following steps:

1. Go to **Policies** section.
2. In the **Policies** area of the Navigation pane, select a security policy to which a rule will be added.
3. Do either of the following:
   - in the main menu, select **Edit > Create rule**, or
   - click **Create rule** button at the top of **Policies** area, or
   - right-click at the empty space in **Policies** area and select **Create rule** from the drop-down list.

4. In the **Create rule** dialog box that opens, select **HTTPS Monitor** from the **Interceptor** drop-down list.
5. Enter a name of the rule in the **Name** field.
6. Configure parameters of events created on traffic interception. You can:
   - exclude interception of requests for internal resources. Select **Do not create events for request to internal resources** if you do not need to intercept all requests inside the corporate network (see details on segments configuring in "Settings of Corporate Network" section, **Parameters of network segments** configuration group).

     Warning!

     If the checkbox is selected, creating a shadow copy in this rule will become unavailable. If you need that:
     - events for requests for internal resources are not created

     and
     - shadow copies are created,

     then you create a separate rule for each case.

     Warning!
     The excluding of traffic sent on internal resources is not available for mobile devices.
   - configure traffic interception only on encrypted channels or every channel. To do this mark **Create requests for events transmitted via** checkbox and from the drop-down list, select:
     - **Encrypted channel**
     - **All channels**.

   If you want to save shadow copies of the transferred files mark **Create shadow copy** checkbox. You can also specify additional parameters for shadow copies:
     - **Minimum request size** - if the check box is selected, shadow copies will be sent only for requests of specified size or larger.
     - **Maximum request size** - if the check box is selected, shadow copies will be sent only for request of specified size or smaller.

   Warning!
   In case there is not enough space available on a the computer (see "Creating Shadow Copies and Blocking Operations Due to Free Space Shortage"), shadow copy will not be created.
7. Define a period of rule action. By default, the rule is always in effect (**Always** option is checked). To specify rule duration, clear **Always** check box and specify date and time in the **From** and **To** fields.
8. When all parameters are configured, click **Save**.

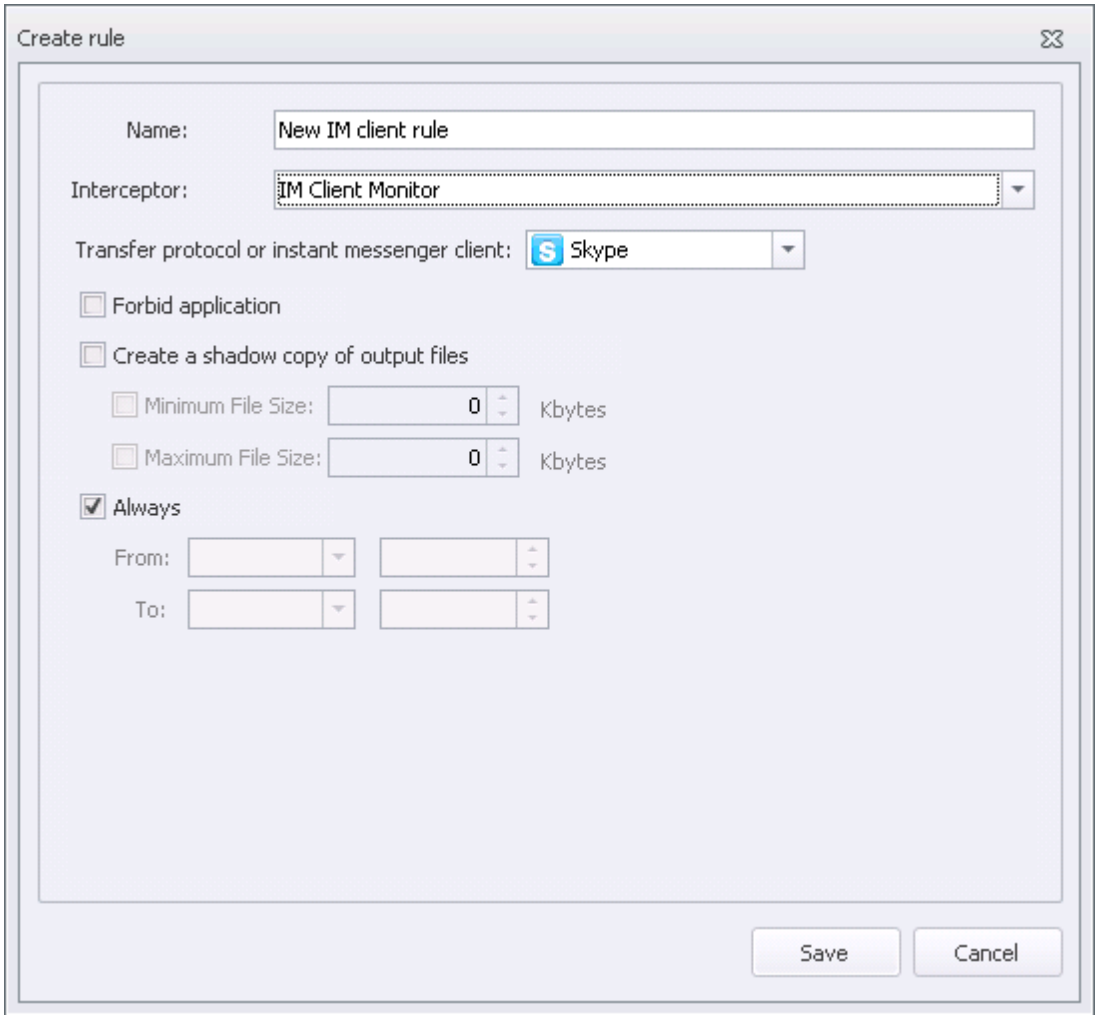
3.4.3.2.2.7 Configuring IM Client Monitor Rule

IM Client Monitor interceptor lets to control employee access to instant messengers: Skype, WhatsApp, Yahoo! Messenger (YMSG protocol), Jabber (XMPP protocol), Mail.Ru Agent (MMP protocol) and mobile phone SMS.

Warning!
IM Client Monitor interceptor global settings (employee request to launch the interceptor, configuring chat shadow copying period) are configured along with general security policies: see "Network Traffic Control".

Warning!

The file is subject to **IM Client Monitor** rule if **ALL** file parameters meet rule conditions **EXCEPT** maximum and minimum file size. **Maximum file size** and **Minimum file size** are taken into consideration only for shadow copying. So if file size is within specified range, then file transfer event will contain a shadow copy; otherwise event will be created without shadow copy.



To configure the rule, perform the following steps:

1. Go to **Policies** section.
2. In **Policies** area at Navigation pane select a security policy which you want to add a rule to.
3. Take one of the following steps:
   - in the Main Menu select **Edit > Create rule**
   - click **Create rule** at the top of **Policies** area;
   - right-click at the empty space in **Policies** area and select **Create rule** from the drop-down list.
4. In **Create rule** dialog in **Interceptor** field select **IM Client Monitor**.
5. Enter rule name to **Name** field.
6. In **IM Client** field select type of messenger controlled by this rule:
   - **Skype** - to control Skype usage
   - **XMPP** - to control Jabber usage
   - **MMP** - to control Mail.Ru Agent usage
   - **Yahoo!** - to control Yahoo! Messenger usage
   - **SMS** - to control messages on mobile devices
   - **WhatsApp** - to control WhatsApp usage on mobile devices
7. If you want to completely forbid using a client of this type of messenger, flag **Forbid application** (unavailable for SMS and WhatsApp).

Warning!
To efficiently forbid Skype and WhatsApp usage we highly recommend you to apply Application Monitor rules: see. "Configuring Application Monitor Rule".

8. If you want to create shadow copies of outgoing files and then analyze them in Traffic Monitor, flag **Create a shadow copy of output files**. Then you can specify additional parameters of shadow copies:
   - **Minimum File Size**. If the check box is selected, shadow copies will be enabled only for files of specified size or larger.
   - **Maximum File Size**. If the check box is selected, shadow copies will be enabled only for files of specified size or smaller.

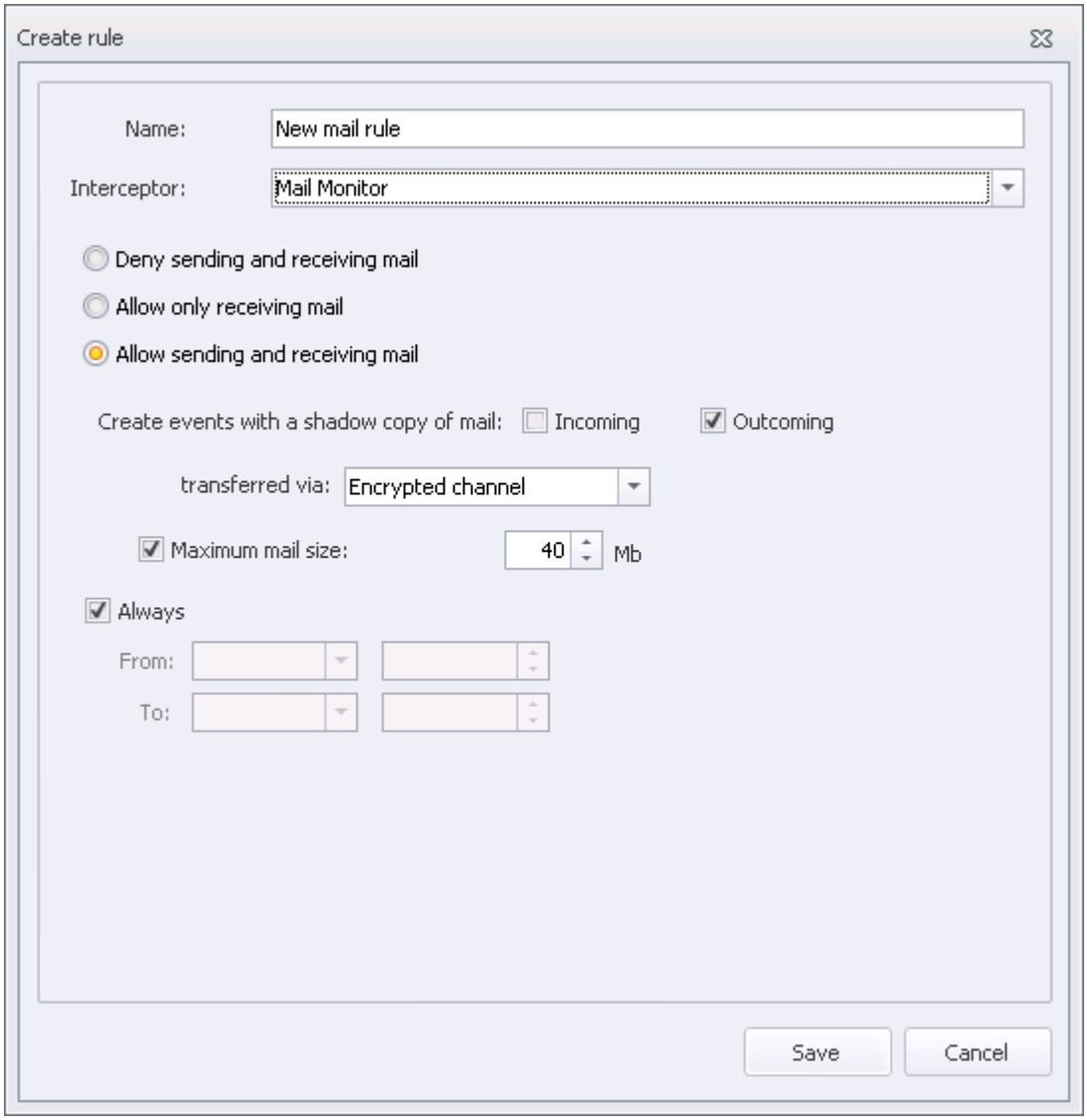
   Warning!
   Shadow copies of chats and messages are always created (regardless of **Create a shadow copy** setting value), if there is at least one **IM Client Monitor** rule in action at the computer.
   To configure chat and messages shadow copying intervals (interval and number of messages required for a shadow copy) is described in "Network Traffic Control".
9. Define a period of rule action. By default, the rule is always in effect (**Always** option is checked). To specify rule duration, clear **Always** check box and specify dates and time in **From** and **To** fields.
10. When all parameters are configured, click **Save**.

Warning!
If IM Client Monitor rule should create a shadow copy of file, message or chat but there is less free system drive space left than required by the policy (see "Creating Shadow Copies and Blocking Operations Due to Free Space Shortage") then shadow copies of messages still will be created but files will be sent without shadow copying.

3.4.3.2.2.8 Configuring Mail Monitor Rule

Mail Monitor interceptor provides full control of incoming and outgoing e-mail.

Mail Monitor controls the following mail protocols: SMTP, IMAP, POP3, MAPI.



To configure the rule, perform the following steps:

1. Go to **Policies** section.
2. In **Policies** area at Navigation pane select a security policy which you want to add a rule to.
3. Take one of the following steps:
   - in the Main Menu select **Edit > Create rule**
   - click **Create rule** at the top of **Policies** area
   - right-click at the empty space in **Policies** area and select **Create rule** from the drop-down list.
4. In **Create rule** dialog in **Interceptor** field select **Mail Monitor**.
5. Enter rule name to **Name** field.
6. Select outgoing and incoming mail control method:
   - **Deny sending and receiving mail**
   - **Allow only receiving mail**
   - **Allow sending and receiving mail**

Warning!
Depending on the outgoing and incoming mail control method, the following variants of shadow copy creation are possible:

- **Deny sending and receiving mail** -shadow copies are not being created;
- **Allow only receiving mail** - for incoming mail (for shadow copy creation, tick the **Incoming** box);
- **Allow sending and receiving mail -** for incoming and outgoing mail (for shadow copy creation, tick the **Incoming** and **Outgoing**).

7. Manage shadow copy creation. Tick the **Incoming** or **Outgoing** box in a **Create events with a shadow copy of mail** line.

Warning!
Allow sending and receiving mail option requires ticking either **Incoming** or **Outgoing** box, or else a rule won't be saved.

You can, as well, manage additional parameters of shadow copies:

- **Transferred via**. Variants possible:
  - **All channels** - to create a shadow copy of mail, transferred per any channel, but encrypted;
  - **Encrypted channel** - to create a shadow copy of mail, transferred per encrypted channels.
- **Maximum mail size**. When ticked, all created shadow copies will be for mail smaller or equal to the number mentioned.

Warning!
In case there is not enough space available on the computer (see "Creating Shadow Copies and Blocking Operations Due to Free Space Shortage"), shadow copy will not be created.

8. Define a period of rule action. By default, the rule is always in effect (**Always** option is checked). To specify rule duration, clear **Always** check box and specify dates and time in **From** and **To** fields.
9. When all parameters are configured, click **Save**.

Warning!
In case existing rule has attributes:

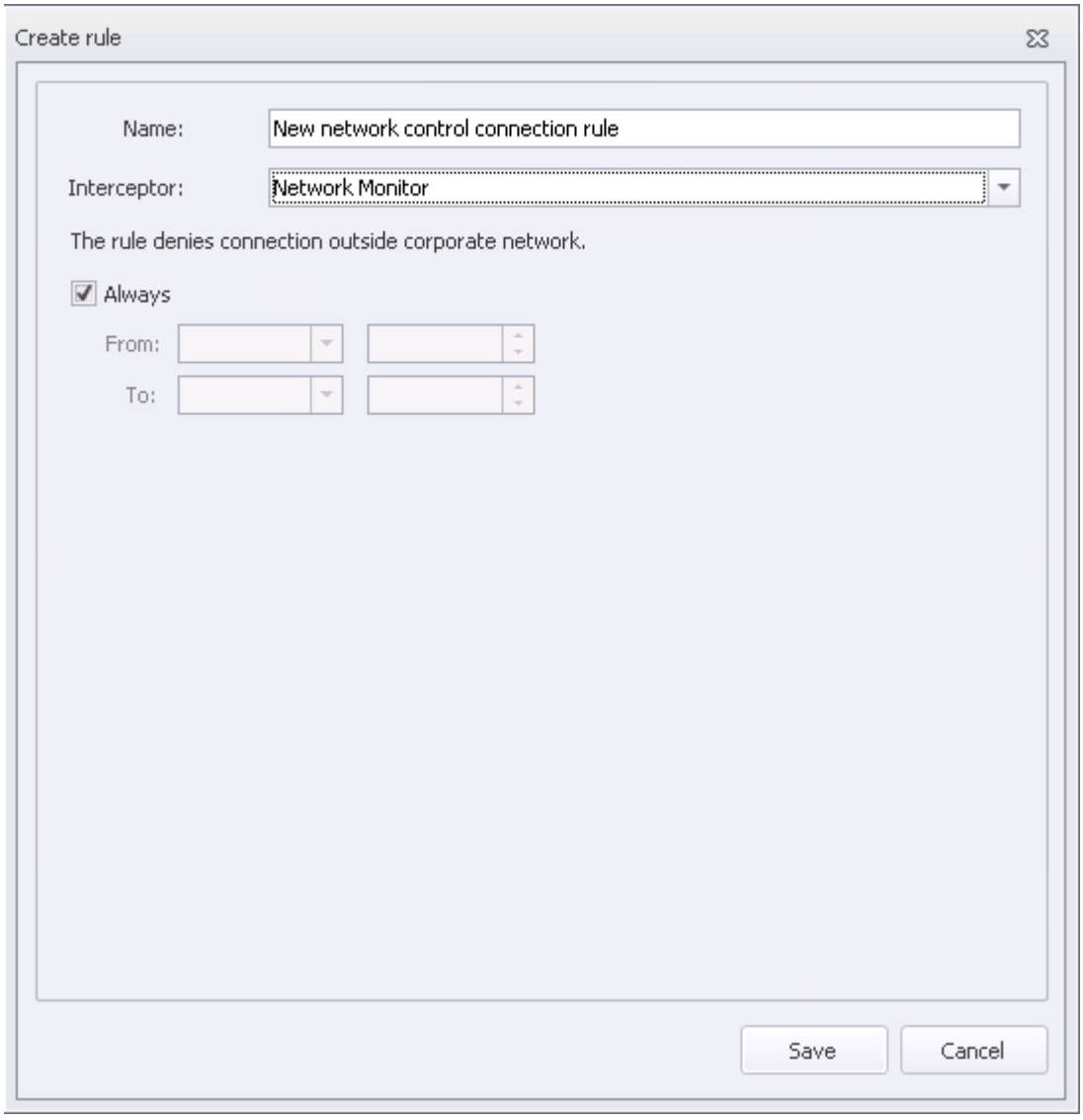
- **Allow sending and receiving mail**;
- **Create events with a shadow copy of mail**: **Incoming** and **Outgoing**, **transferred via: All channels**

and there is a saving mail on the mail server setting configured in the mailer, then each mail sending event will generate two interception objects: one of **Outgoing** type and other of **Incoming** type. The name of the mailer option might change depending on the program in use.

3.4.3.2.2.9 Configuring Network Monitor Rule

Network Monitor interceptor lets to deny transferring data by any network connections except connections with corporate network or specified permitted servers. Configuring segments of corporate network and permitted external addresses is performed as described in "Settings of Corporate Network".

Warning!
When any Network Monitor rule will take effect, the Device Monitor Agent installed onto computer, will try to resolve DNS names of opening webpages. So to prevent troubles with external connections you should configure corporate DNS server to use forward servers: see details in "Configure a DNS Server to Use Forwarders" internet article.

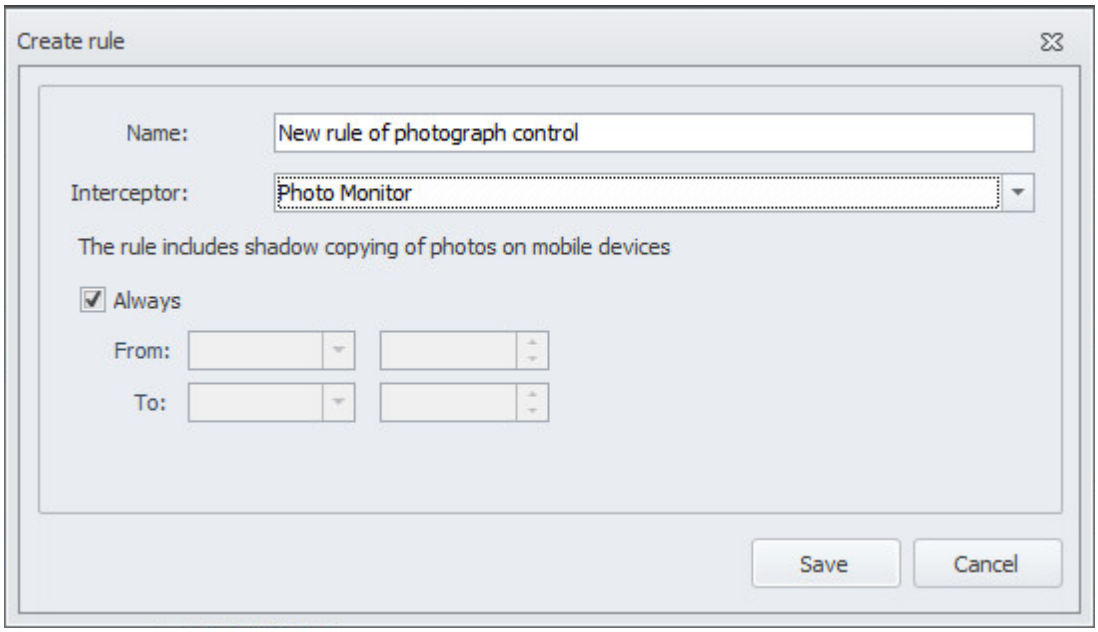


To configure the rule, perform the following steps:

1. Go to **Policies** section.
2. In **Policies** area at Navigation pane select a security policy which you want to add a rule to.
3. Take one of the following steps:
   - in the Main Menu select **Edit > Create rule**
   - click **Create rule** at the top of **Policies** area
   - right-click at the empty space in **Policies** area and select **Create rule** from the drop-down list.
4. In **Create rule** dialog in **Interceptor** field select **Network Monitor**.
5. Enter rule name to **Name** field.
6. Define a period of rule action. By default, the rule is always in effect (**Always** option is checked). To specify rule duration, clear **Always** check box and specify dates and time in **From** and **To** fields.
7. When all parameters are configured, click **Save**.

3.4.3.2.2.10 Configuring Photo Monitor Rule

Photo Monitor interceptor lets to make shadow copies of photographs made by cameras of controlled mobile devices.



To configure the rule, perform the following steps:

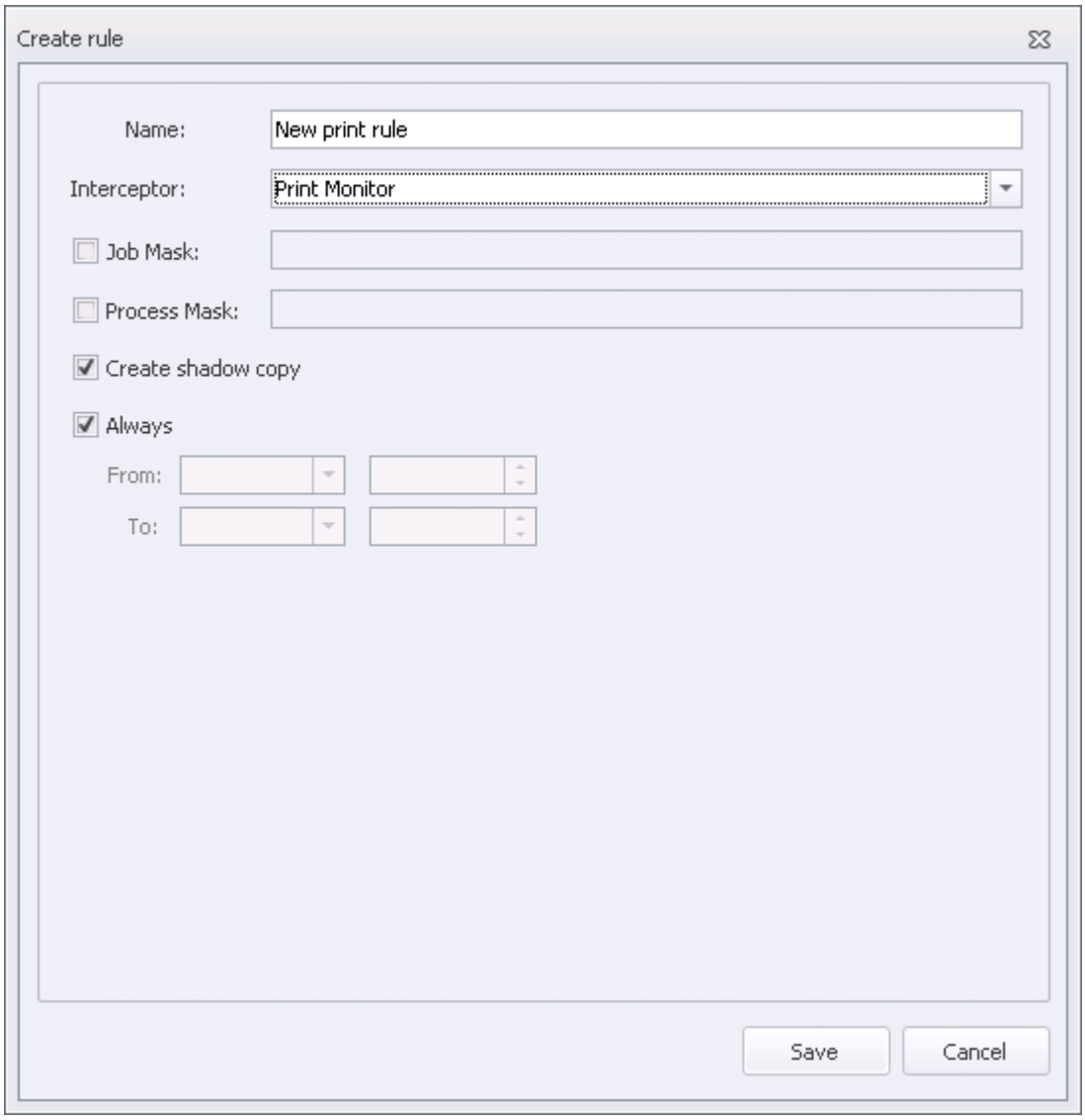
1. Go to **Policies** section.
2. In **Policies** area at Navigation pane select a security policy which you want to add a rule to.
3. Take one of the following steps:
   - in the Main Menu select **Edit > Create rule**
   - click **Create rule** at the top of **Policies** area
   - right-click at the empty space in **Policies** area and select **Create rule** from the drop-down list.
4. In **Create rule** dialog in **Interceptor** field select **Photo Monitor**.
5. Enter rule name to **Name** field.

   Warning!
   If Photo Monitor rule should create print job shadow copy but there is less free space at the hard drive than required by the policy (see "Creating Shadow Copies and Blocking Operations Due to Free Space Shortage"), then the printing will be performed without shadow copy creating.

6. Define a period of rule action. By default, the rule is always in effect (**Always** option is checked). To specify rule duration, clear **Always** check box and specify dates and time in **From** and **To** fields.
7. When all parameters are configured, click **Save**.

3.4.3.2.2.11 Configuring Print Monitor Rule

Print Monitor interceptor lets to monitor operations of document printing on local and network printers.



To configure the rule, perform the following steps:

1. Go to **Policies** section.
2. In **Policies** area at Navigation pane select a security policy which you want to add a rule to.
3. Take one of the following steps:
   - in the Main Menu select **Edit > Create rule**
   - click **Create rule** at the top of **Policies** area
   - right-click at the empty space in **Policies** area and select **Create rule** from the drop-down list.
4. In **Create rule** dialog in **Interceptor** field select **Print Monitor**.
5. Enter rule name to **Name** field.
6. You can constrain controlled print jobs by masks:
   - **Job mask**. Using print job (document) mask. If you want to use job mask, select this check box and specify a job mask.

     The name of print job is provided by the application that sends documents to print. Therefore, a name can be represented by any text string and doesn't have to indicate document type.

     You can use wildcard characters when specifying a job mask: «?» to replace a character or «*» to

replace a character set. The space character is interpreted as a part of job name.

- **Process mask**. Using masks for print job process. If you want to use process mask, select this check box and specify a process mask.

  Process name (full path) will be received for print job rendering process. In some cases (local LPT and COM printers) a printing subsystem can perform a rendering in a context of **Print Spooler** service. Link to service's executable file: `%SystemRoot%\system32\spoolsv.exe`.

  Select **Send directly to printer** parameter (**Printer properties> Advanced**) to make sure the process name is correctly identified. Print job will be processed by the application that sends documents to print. In this case, synchronous printing will be used, i.e. you will be unable to use the application until printing has been finished.

  Available replace symbols: «?» to replace one symbol or «*» to replace several symbols. Space character is interpreted as a part of file name.

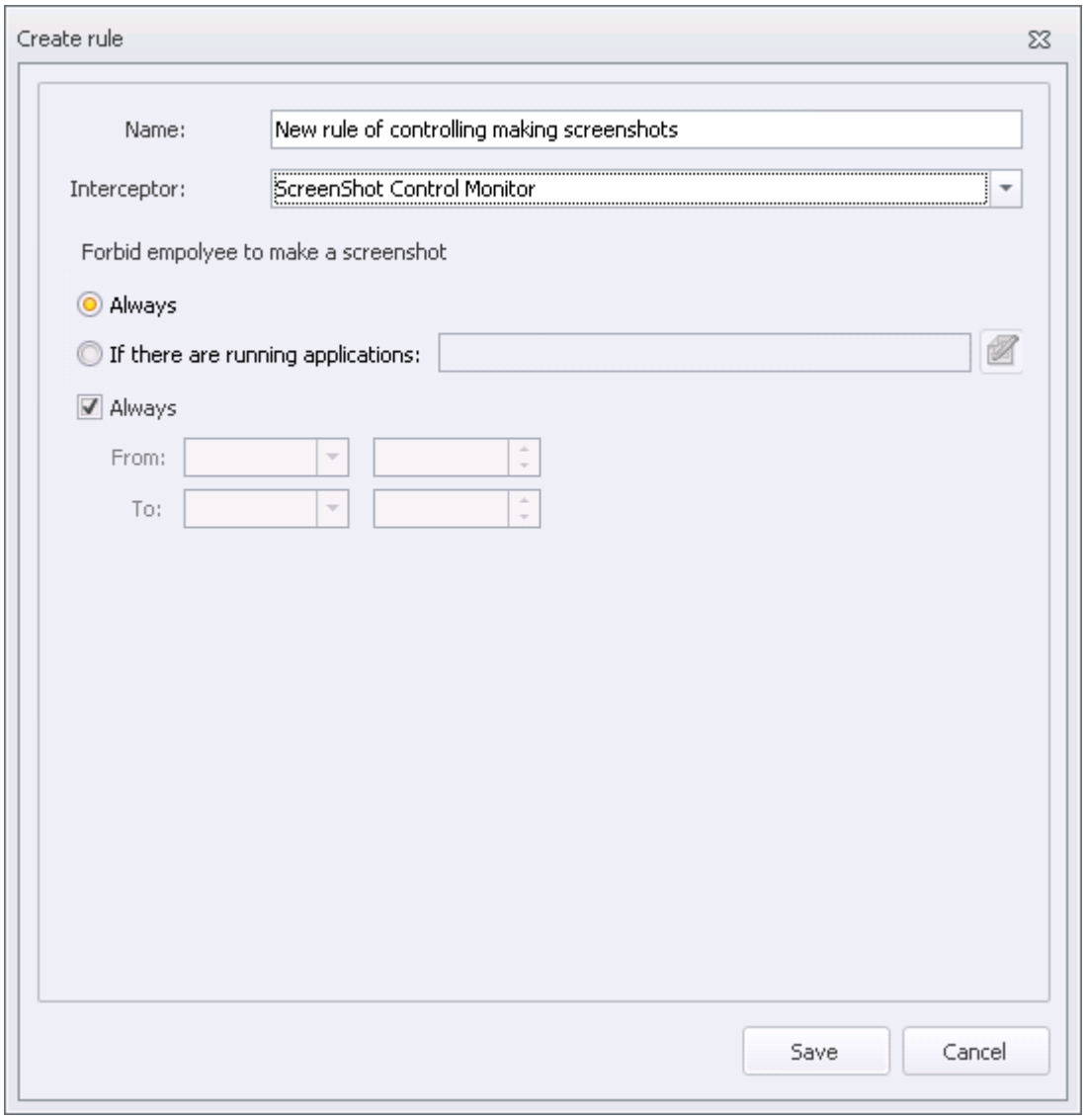
7. If you want to create shadow copies of outgoing files and then analyze them in Traffic Monitor, flag **Create a shadow copy**.

   Warning!
   If Print Monitor rule should create print job shadow copy but there is less free space at the hard drive than required by the policy (see "Creating Shadow Copies and Blocking Operations Due to Free Space Shortage"), then the printing will be performed without shadow copy creating.

8. Define a period of rule action. By default, the rule is always in effect (**Always** option is checked). To specify rule duration, clear **Always** check box and specify dates and time in **From** and **To** fields.
9. When all parameters are configured, click **Save**.

3.4.3.2.2.12 Configuring ScreenShot Control Monitor Rule

ScreenShot Control Monitor interceptor allows to control screen shots on a client side.



To configure the rule, perform the following steps:

1. Go to **Policies** section.
2. In **Policies** area at Navigation pane select a security policy which you want to add a rule to.
3. Take one of the following steps:
   - in the Main Menu select **Edit > Create rule**
   - click **Create rule** at the top of **Policies** area
   - right-click at the empty space in **Policies** area and select **Create rule** from the drop-down list.
4. In **Create rule** dialog in **Interceptor** field select **ScreenShot Control Monitor**.
5. Enter rule name to **Name** field.
6. In area **Forbid employee to make a screenshot** define a rule period:
   - **Always.** Has no time limit by default.
   - **If there are running applications.** Pick a list of applications using button (see "Applications protocol").
   - Define a period of rule action. By default, the rule is always in effect (**Always** option is checked). To

specify rule duration, clear **Always** check box and specify dates and time in **From** and **To** fields

7. When all parameters are configured, click **Save**.

3.4.3.2.3 Editing a Rule

To edit a rule:

1. Go to **Policies**.
2. In **Policy** area of Navigation pane select the title of security policy that contains the rule. The main window will display the full list of the policy rules.
3. Select the row with the name of the rule you want to edit.
4. Take one of the following steps:
   - in Main Menu click **Edit > Edit Rule**
   - double-click the selected row
   - click **Edit Rule** at the top of **Policy** area.

   These actions open rule configuration dialog.
5. Edit rule parameters:
   - Configuring Application Monitor Rule
   - Configuring Cloud Storage Monitor Rule
   - Configuring Device Monitor Rule
   - Configuring File Monitor Rule
   - Configuring FTP Monitor Rule
   - Configuring HTTP(S) Monitor Rule
   - Configuring IM Client Monitor Rule
   - Configuring Mail Monitor Rule
   - Configuring Network Monitor Rule
   - Configuring Photo Monitor Rule
   - Configuring Print Monitor Rule
   - Configuring Screenshot Control Monitor Rule
6. When all changes are made click **OK** in rule configuration dialog.

Warning!
To apply changes you have to save current security schema (see "Editing Security Schema"). If you don't save your security schema, all changes will be discarded.

3.4.3.2.4 Deleting a Rule

To delete a rule:

1. Go to **Policies**.
2. In **Policy** area of Navigation panel select the name of security policy that contains the rule. The main window will display the full list of the policy rules.
3. Select the row that contains the rule you want to remove.

   Note:
   To delete multiple rules from a single security policy, select the rows with the names of all rules you want to remove.
4. Take one of the following steps:
   - in Main Menu click **Edit > Delete Rule**

- press **Delete** keyboard button
- click **Delete Rule** at the top of **Policy** area.

5. In request box select **Yes** to confirm that you want to remove the rule.

Warning!
To apply changes you have to save current security schema (see "Editing Security Schema"). If you don't save your security schema, all changes will be discarded.

3.4.3.2.5 Copying a Rule

Rules can be copied from one security policy to another.

To copy a rule:

1. Go to **Policies**.
2. In **Policy** area of Navigation pane, select the name of the security policy that contains the rule you want to copy.
3. In main screen workspace select the row that contains the name of the rule you want to copy. You can select multiple rows to copy group rules into a single security policy.
4. Click and hold the selected row and drag the rule into **Policies** area of Navigation pane. Move the pointer over the title of security policy you are adding the rule to. Release the button when a yellow arrow appears next to the selected policy.

This copies the rule to selected security policy.

You can also copy rules from the dialog of editing the policy to which you want to add rules from other policies.

To copy a rule while editing a policy:

1. Go to **Policies**.
2. In **Policy** area of Navigation pane, select the name of the security policy that you want to add a rule to.
3. Take one of the following steps:
   - in the Main Menu select **Edit > Edit Policy**
   - click **Edit Policy** at the top of Navigation pane
   - double-click selected security policy name.
4. click **Select rules**. In new dialog flag the rules you want to copy to a new security policy. You can select the whole policy - then all rules it contains will be added to editing security policy.
5. After you mark all rules click **Select**.
6. Click **Save** to save policy.

Warning!
To apply changes you have to save current security schema (see "Editing Security Schema"). If you don't save your security schema, all changes will be discarded.

3.4.3.3 Employees

Employee and employee group management basics are available in "Employees and Employee Groups".

Existing security policies can be assigned only to employee groups. Security policy for an employee is defined by including his/her account to the employee group.

Warning!
In addition to employee group security policy, each employee is covered by computer security policy. Information about rule conflict resolving see in "Rules Application".

To go to Console section designed for accounts management, click **Employees** button on Navigation pane.

Guidelines on account management are available in:

- Viewing Employee Details
- Viewing Resultant Policy and White List for an Employee
- Adding and Editing an Employee Group
- Deleting Employee Group
- Adding Employee Account to a Group
- Editing Employee Account
- Removing Employee Account from Employee Group
- Deleting Employee Account from Security Schema

3.4.3.3.1 Viewing Employee Details

Employees area of Navigation pane displays employee group list. Selected employee group employees are listed in the main window work pane.

Note:
Use additional features to adjust employee list view (see "Additional Features").

To view information for specific employee group,

select group name in employee group list.

To view all registered employees information,

click **Show All Employees** at the top of Navigation pane.

Employee account information is represented as tabular list. Each row in the list contains a single account. Columns contain accounts' general properties. Extended information on each account is available in **Details** panel.

To view account's detailed properties,

select the row that contains the account name.
Details panel displays table properties including the following information:

- **Account**. Account name.
- **Last Name**, **First Name**, **Middle Name**. Account owner's last, first and middle name.
- **SID**. Operating System internal ID.

Note:
Some information from **Details** panel is duplicated in the main screen workspace.

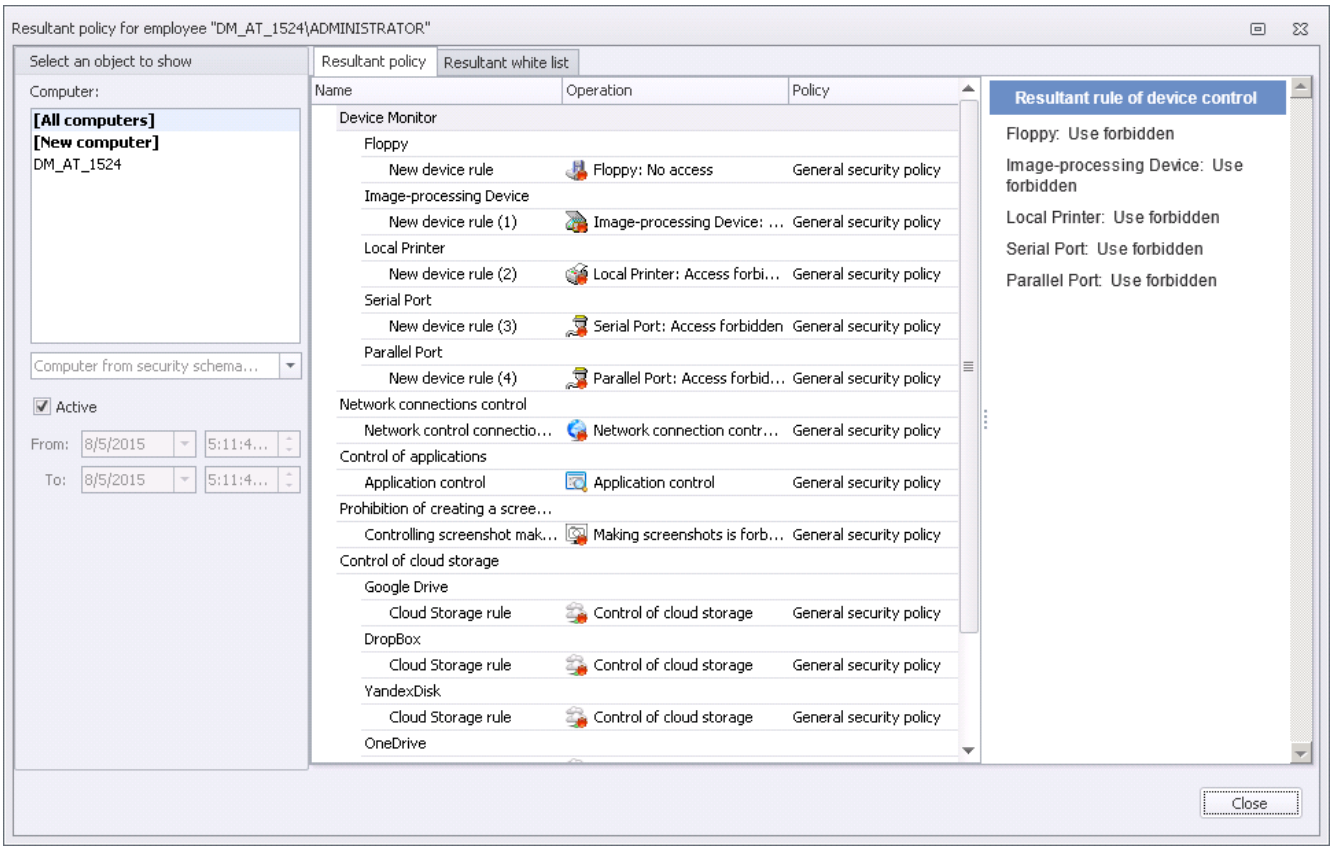
3.4.3.3.2 Viewing Resultant Policy and White List for an Employee

To view information about policy and white list for an employee:

1. In the **Employee** list select an employee you want to view policy and white list for.
2. Proceed with one of the following actions:
   - in the main menu choose **Edit -> Show effective policy**.
   - on **Employees** pane click **Show effective policy**.

   As a result, a window **"Resulting policy for employee"** will be displayed with the resultant policy for

selected employee.



The main area of the **Resultant policy and settings for employee** window contains two tabs:

- **Resultant settings** displays acting rules for the employee. The resultant policy consists of rules configured by default and rules configured for selected computer and rules for selected employee (see "Device Monitor Rules Application"). Select the rule from the list: the panel on the right will display the detailed information on the selected rule.
- **Resultant white list** displays the list of devices allowed for the employee (see "White Lists"). Select device from the list: the panel on the right will display the detailed information on the selected device.

On the **Computer** pane you can select the object to view:

- **All computers** - displays resultant policy\white list\settings for all computers regardless of which one the selected employee is logged on.
- **New computer** - displays resultant policy\white list\settings for the selected employee and a new computer (which is absent in the security schema for now).
- to view the resultant policy\white list\settings for a certain computer:
  - from the **Computer** list select account registered for the selected employee

  or
  - from the **Computer from security schema** drop-down list select any account registered in the System (see "Computers").

You can select time to display policy\white list\settings acting in:

- the setting **Active** displays current resultant policy\white list\settings, this is a default setting;
- to view resultant policy\white list\settings for a certain time period, deselect **Active** field and specify needed time interval.

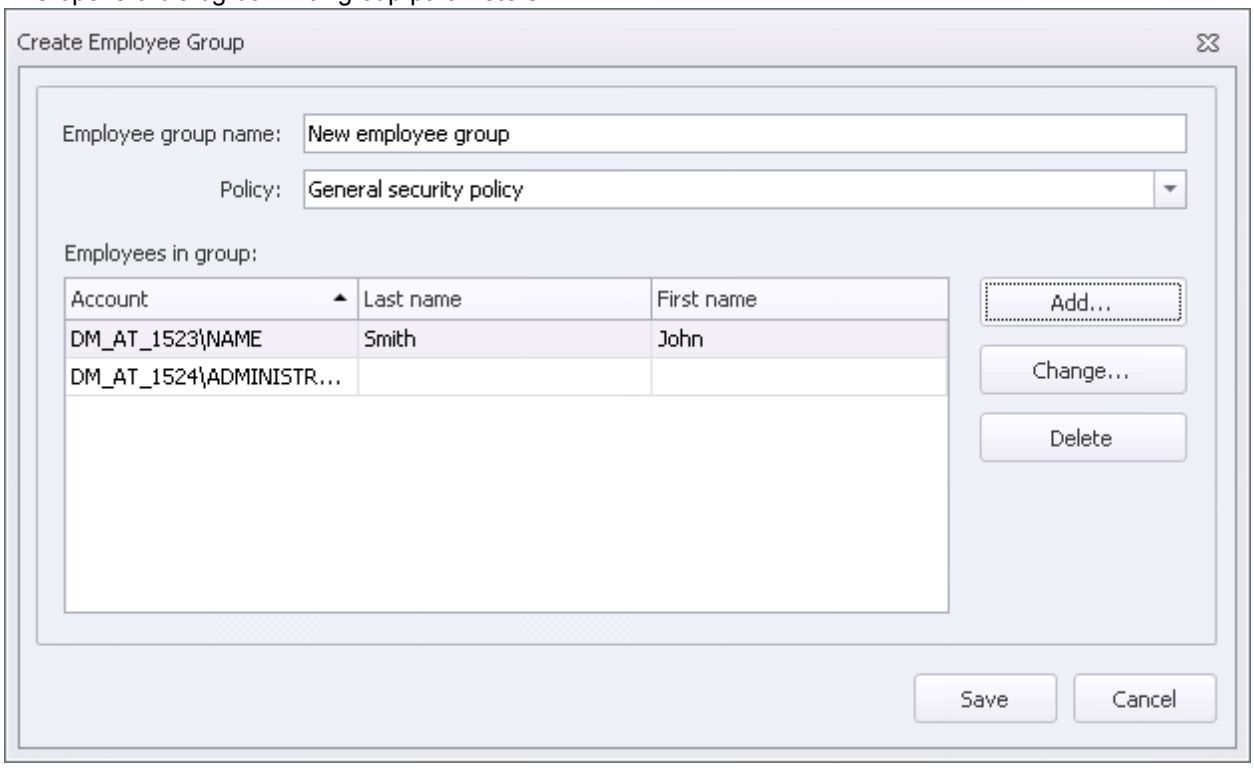
3.4.3.3.3 Adding and Editing an Employee Group

To add or edit an employee group:

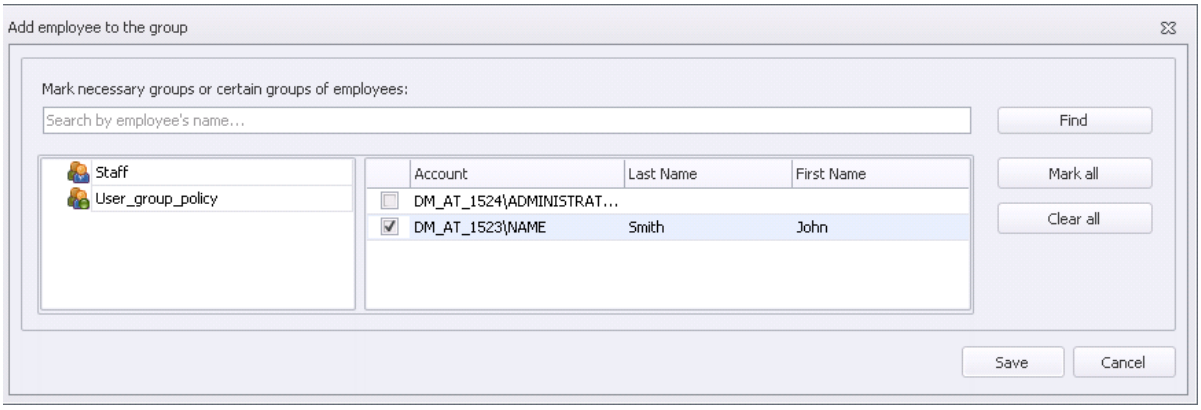
1. Go to **Employees** section.
2. Take one of the following steps:

Action	Steps
Add employee group	• select **Edit > Create Employee Group** in the Main Menu; • click **Create Employee Group** at the top of the Navigation Pane.
Edit employee group	1. In **Employees** area of Navigation Pane select the employee group name. 2. Take one of the following steps: • in the Main Menu, click **Edit > Edit Employee Group**; • click **Edit Employee Group** at the top of Navigation pane; • double-click selected employee group name.

This opens a dialog box with group parameters.



3. Specify the following parameters:
   - **Employee group name**.
   - **Policy**. From drop-down list select a security policy for employee group.
4. Set a list of employees in the group:
   - To add one or several accounts, click **Add**.



The **Add employee to the group** dialog displays a list of accounts imported from the directory service (see "Connecting to LDAP Server") and already registered in the System (for example, when Device Monitor Client was installed to the computer) and belonging to existing Device Monitor employee groups.

To add an employee, in left pane select a node in groups tree, then flag accounts you want to add to edited group.

To flag all accounts of selected node, click **Mark all**. To clear selection, click **Clear all**.

You can also make a search of account by all available elements: enter a part of account name to the field at the top and click **Find**.

After you selected all needed accounts, click **Save** to close **Add employee to the group** dialog and return to a dialog box with group parameters.

- To edit account parameters, select it from the list of employees belonging to the group and click **Change**. The description of entry editing see in "Editing Employee Account".
- To delete an entry from the group, select it and click **Delete**.

5. Click **Save**.

Warning!
To apply changes you have to save current security schema (see "Editing Security Schema"). If you don't save your security schema, all changes will be discarded.

3.4.3.3.4 Deleting Employee Group

To delete employee group:

1. Go to **Employees** section.
2. Click the employee group you want to delete.
3. Take one of the following steps:
   - select **Edit > Delete Employee Group** in the Main Menu;
   - click **Delete Employee Group** at the top of **Navigation Pane**.
4. Click **Yes** in confirmation box to confirm that you want to remove employee group.

Warning!
To apply changes you have to save current security schema (see "Editing Security Schema"). If you don't save your security schema, all changes will be discarded.

3.4.3.3.5 Adding Employee Account to a Group

After InfoWatch Device Monitor Client is installed to the computer (see "InfoWatch Device Monitor Client Setup"), data on all employees registered at it is automatically added to the Device Monitor security schema, "*Default*" employee group. Therefore the policy assigned to "*Default*" employee group will be applied to all newly registered employees. In prospect security policy for an employee is defined by including its account to different employee groups.

To move an employee account from one group to another:

1. Go to **Employees** section.
2. In **Employees** area of Navigation pane select a group containing employee's entry.
3. In **Employees** area of main screen workspace select an account which you want to add to another group. Left-click and hold the selected row and drag it to **Employees** area of Navigation pane. Move the cursor over the name of the group you want to add an account to. When a yellow arrow appears at the left of selected group, release left mouse button.

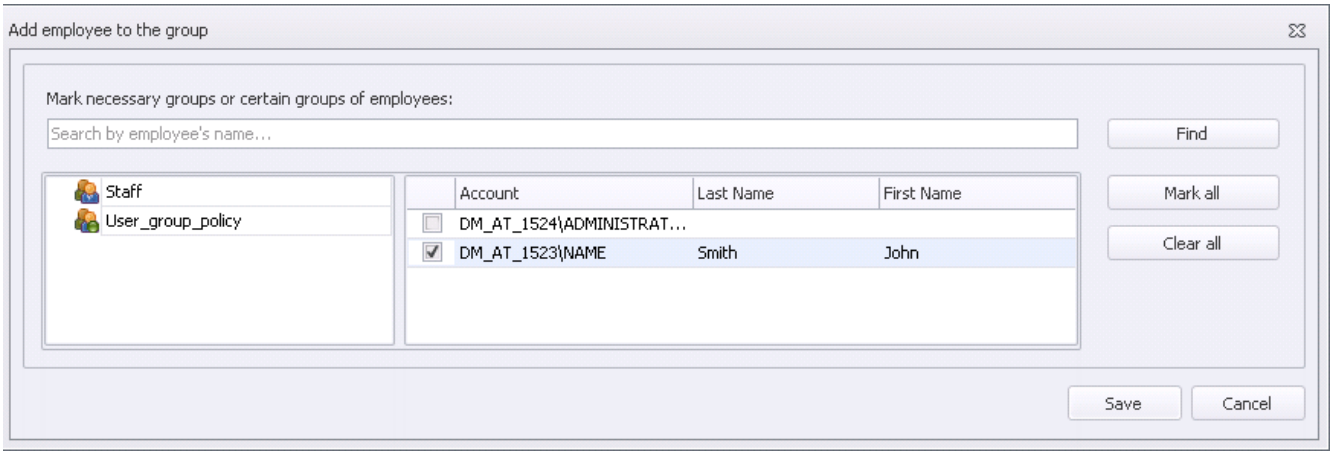
This adds an account to the selected group.

You can also manually import an information on the employee from directory service (see connection configuring description in "Connecting to LDAP Server"). Then after this employee is registered at the computer where InfoWatch Device Monitor Client installed, this employee will be subject of policy of a group where the employee is added to.

To add one or several accounts imported from the directory service or already registered in the System to employee group:

1. Go to **Employees** section.
2. In **Employees** area of Navigation pane select a group which you want to add employee's account to.
3. Take one of the following steps:
   - in the Main Menu, click **Edit > Create Employee**
   - click **Create Employee** at the top of **Employees** area
   - right-click in **Employees** area and select **Create Employee** from the drop-down list
   - double-click selected employee group name.

   These actions open employees adding dialog displaying a list of accounts imported from the directory service (see "Connecting to LDAP Server") and already registered in the System (for example, when Device Monitor Client was installed to the computer) and belonging to existing Device Monitor employee groups.



4. To add an employee, in left pane select a node in groups tree, then flag accounts you want to add to edited group.
   To flag all accounts of selected node, click **Mark all**. To clear selection, click **Clear all**.
   You can also make a search of account by all available elements: enter a part of account name to the field at the top and click **Find**.
   After you selected all needed accounts, click **Save** to close **Add employee to the group** dialog and return to a dialog box with group parameters.
5. Click **Save**.

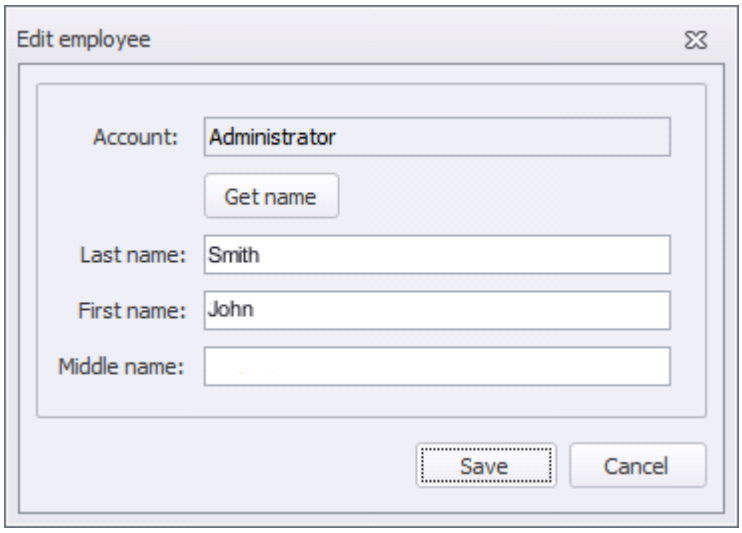
Warning!
To apply changes you have to save current security schema (see "Editing Security Schema"). If you don't save your security schema, all changes will be discarded.

3.4.3.3.6 Editing Employee Account

Parameters of employee account are imported from directory service or while installing a InfoWatch Device Monitor Client to the computer where this employee is registered. If you want to add some information, you can enter employee's personal data as described below.

To edit an employee account:

1. Go to **Employees** section.
2. In **Employees** area of Navigation pane select the group the account belongs to.
3. Select the row that contains the name of the account you want to edit.
4. Take one of the following steps:
   - in the Main Menu, click **Edit > Edit Employee**
   - click **Edit Employee** at the top of **Employees** area
   - double-click the selected row.



5. In **Edit employee** dialog you can modify the following optional parameters: **Last Name**, **First Name** and **Middle Name**. You can either enter new values into appropriate fields manually or import them from directory service with **Get name** button.
6. Click **Save**.

Warning!
To apply changes you have to save current security schema (see "Editing Security Schema"). If you don't save your security schema, all changes will be discarded.

3.4.3.3.7 Removing Employee Account from Employee Group

To remove an account from employee group:

1. Go to **Employees** section.
2. In **Employees** area of Navigation pane select employee group the account belongs to.
3. Select the row that contains the name of the account you want to remove from this group.

   Note:
   To remove multiple accounts from a group, select the rows with employee's accounts you want to exclude from this group.
4. Take one of the following steps:
   - In the Main Menu, click **Edit > Remove employee from group**
   - click **Remove employee from group** at the top of **Employees** area
   - press **Delete** keyboard button.

This removes employee account from selected employee group.

Note:
If employee account belongs to a single employee group, then after excluding it will be automatically added to default employee group.

Warning!
To apply changes you have to save current security schema (see "Editing Security Schema"). If you don't save your security schema, all changes will be discarded.

3.4.3.3.8 Deleting Employee Account from Security Schema

To remove employee account from security schema:

1. Go to **Employees** section.
2. In **Employees** area of Navigation pane select employee group the account belongs to.
3. Select the row that contains the account you want to remove.

   Note:
   To remove multiple accounts from security schema, select all the rows that contain the accounts you want to remove.
4. Take one of the following steps:
   - In the Main Menu, click **Edit > Delete employee from security schema**
   - click **Delete employee from security schema** at the top of **Employees** area
   - press **Shift+Delete** at the keyboard.
5. In the confirmation box click **Yes** to confirm that you want to remove the account.

Warning!
To apply changes you have to save current security schema (see "Editing Security Schema"). If you don't save your security schema, all changes will be discarded.

3.4.3.4 Computers

InfoWatch Device Monitor computer is a managed computer - computer where InfoWatch Device Monitor. Client is installed.

General principles of managing the computers are described in "Computers and Computer Groups" section.

Actual security policies can be applied only to a computer group. You can define a security policy for a certain computer by including it to various computer groups.

Warning!
Each computer is a subject both of security policy of a computer group and security policy of an employee which is currently authorized at that computer. Information about rule conflict resolving see in "Rules Application".

To go to Management Console computer section, click **Computers** button on Navigation pane.

For more information on managed computers see:

- Viewing Computer Details
- Viewing Resultant Settings, Policy and White List for a Computer
- Adding and Editing a Computer Group
- Deleting Computer Group
- Adding Computer to a Group
- Removing Computer from a Group
- Deleting Computer from Security Schema
- Updating Clients at Managed Computers

- Diagnostics of the Workstation

See details on installing and deleting the Client for mobile devices in "Mobile Devices" section.

3.4.3.4.1 Viewing Computer Details

Computers area of Navigation pane displays a list of computer groups. Main screen workspace displays the list of computers in selected computer group.

> **Note:**
> Use additional options to adjust computers list display (for details see "Additional Features").

To view the list of computers that belong to a separate group,

select the group name from computer groups list.

To view a full list of registered computers,

click **Show All Computers** at the top of Navigation pane.

Computer information is displayed in tabular list. Each row in the list contains a computer. Columns contain basic computer properties. Extended information on each computer is available in **Details** panel.

To view specific computer's properties,

in the main screen workspace, select the row with computer description.

After this, **Details** panel will display table of properties with the following computer data:

- **Status**. Managed computer and Client status. This parameter may have the following values:
  - **Works properly**. Managed computer is enabled, Client is running.
  - **Inactive**. Managed computer is disabled or unavailable for a long time. The same status is displayed, if the Client is uninstalled from the managed computer.
- **Address**. Computer address. Domain name or IP address for workstations or a name of mobile device.
- **Installed**. Date and time of computer Client's first access to the server.
- **Established**. Date and time of Client launch on computer.
- **Last check-in**. Date and time of computer Client's last access to the Server.
- **Schema version**. Client's current security schema version number.
- **Client version**. Client version number.
- **Operating system**. Version of OS installed on the computer.
- **Model**. Mobile device model - displayed for mobile devices only.
- **Settings version**. General settings security policy version number (see "General System Settings").
- **Template version**. Employee notification templates version number (see "Employee Notifications about Policy Violations").
- **Network settings version**. Version number of settings of data transferring through network connections with Network Monitor (see "Settings of Corporate Network").
- **Network traffic control version**. Version number of settings of network traffic transferred through XMPP, MMP, FTP, FTPS, SMTP/IMAP/POP3,HTTP and HTTPS protocols (see "Network Traffic Control").
- **Exclusion of applications version**. Exclusion of applications from interception version number (see "Exclusion of application from interception"). In brackets you will see the number of the latest version.
- **Free disk space on shadow copy drive**. Free space on hard drive where shadow copies are stored (incl. percent) and minimum free space.

  > **Warning!**
  > If there is at least one valid rule that allows shadow copying, and there is less free space on the host drive than specified by the policy (see "Creating Shadow Copies and Blocking Operations Due to Free Space Shortage"), no data will be printed or written to removable media: even if these steps aren't covered by any rule.

Note:
Information retrieved from some attributes is duplicated in the main screen workspace.

Each registered computer is automatically added to "default" computer group. At the same time, "default" computer group security policy is assigned to the new computer.

You can do the following as you work:

- manage computer groups:
  - add computer groups
  - edit computer group parameters
  - delete computer groups.
- manage computers:
  - add computers' information to computer groups and thus define computer security policy
  - remove computers from computer group
  - delete computer from security schema
  - update Clients at managed computers.

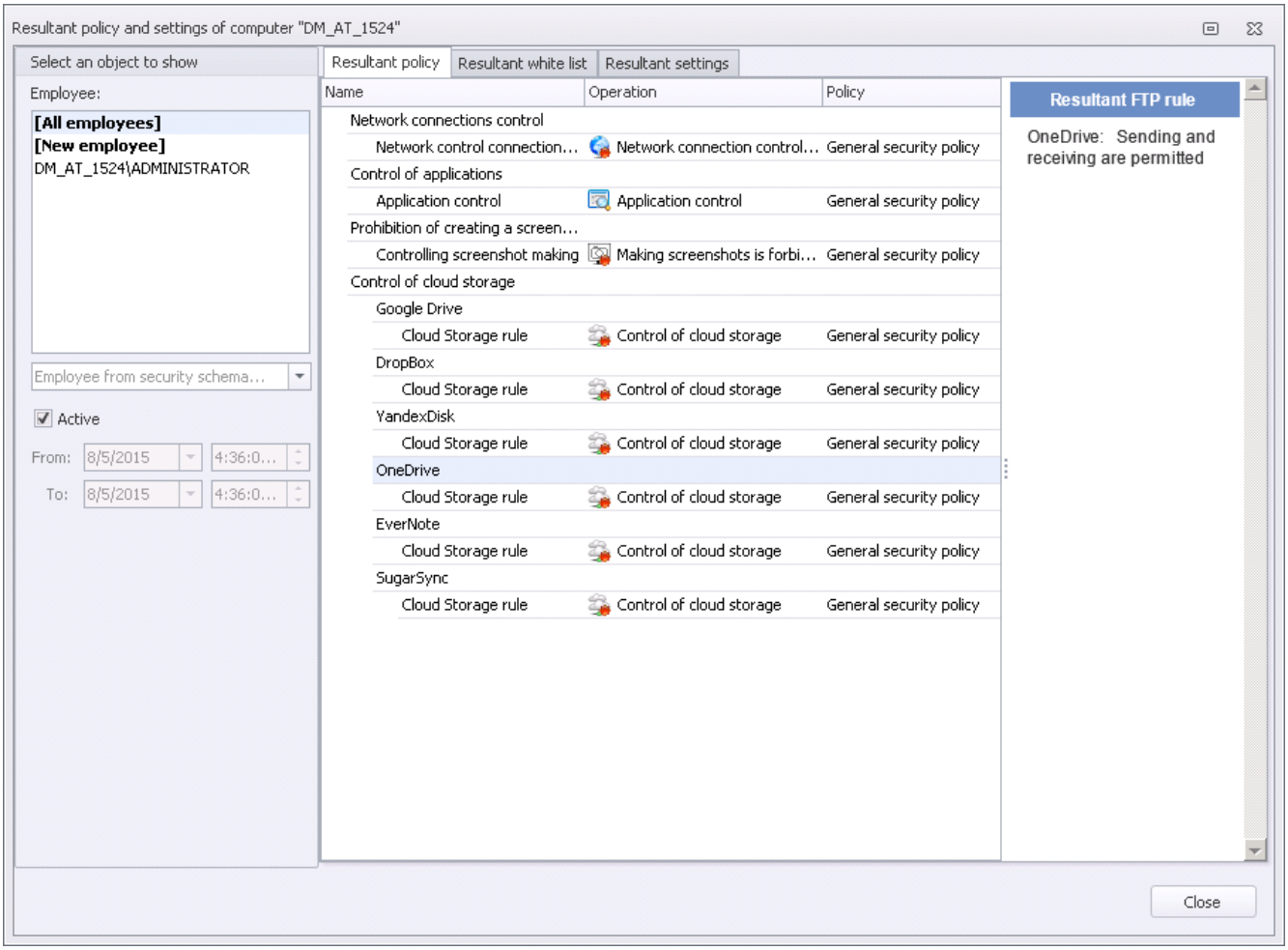
See details on installing and deleting the Client for mobile devices in "Mobile Devices" section.

3.4.3.4.2 Viewing Resultant Settings, Policy and White List for a Computer

To view information about resultant settings, policy and white list for a computer:

1. In the **Computers** list select the employee you want to view policy and white list for.
2. Proceed with one of the following actions:
   - in the Main Menu select **Edit -> Show settings and resultant policy**.
   - on **Computers** pane click **Show settings and resultant policy**.

As a result, a window **Resultant policy and settings of computer** will be displayed with the resultant policy for selected computer.



The main area of the **Resultant policy and settings of computer** window contains three tabs:

- **Resultant settings** displays acting rules on the computer. The resultant policy consists of rules configured by default and rules configured for selected computer and rules for employees - users of this computer (see "Device Monitor Rules Application"). Select the rule from the list: the panel on the right will display the detailed information on the selected rule.
- **Resultant white list** displays the list of devices allowed for the computer (see "White Lists"). Select device from the list: the panel on the right will display the detailed information on the selected device.
- **Resultant settings** displays **Limit the speed of sending data** and **Client's disk space control** settings which are resultant for the computer. The resultant settings are composed of default settings and settings for computers group to which the selected computer belongs (see "Common Settings for Clients" and "Adding and Editing a Computer Group").

On the **Employee** pane you can select the object to view:

- **All employees** - displays resultant policy\white list\settings for all employees regardless of who is logged on the selected computer.
- **New employee** - displays resultant policy\white list\settings on the selected computer for a new employee (which is absent in the security schema for now).
- to view the resultant policy\white list\settings for a certain employee:
  - from the **Employee** list select account registered on the selected computer

  or
  - from the **Employee from security schema** drop-down list select any account registered in the System (see "Employees").

You can select time to display policy\white list\settings acting in:

- the setting **Active** displays current resultant policy\white list\settings, this is a default setting;
- to view resultant policy\white list\settings for a certain time period, deselect **Active** field and specify needed time interval.

3.4.3.4.3 Adding and Editing a Computer Group

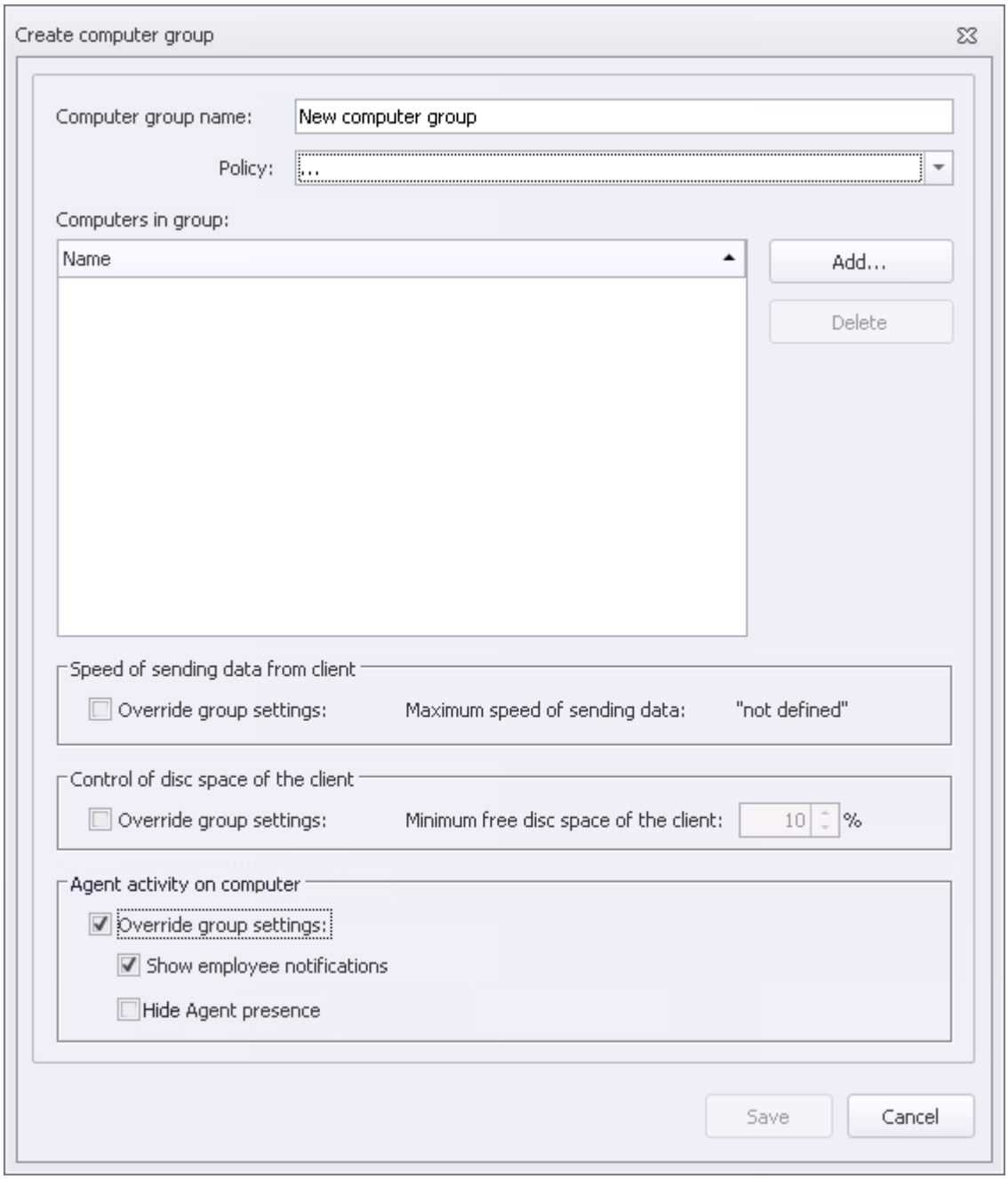
Warning!
When a new computer is registered its information is automatically added to security schema (to "*Default*" group).

To add or edit a computer group:

1. Go to **Computers**.
2. Take one of the following steps:

Action	Steps
Add computer group	• in the Main Menu, click **Edit > Create computer group**; • click **Create Computer Group** at the top of Navigation pane.
Edit computer group	1. In **Computers** area of Navigation pane select computer group name. 2. Take one of the following steps: • in the Main Menu select **Edit > Edit** • click **Edit** at the top of Navigation pane; • double-click selected computer group name.

This opens a dialog box with group parameters.



3. In this dialog, specify the following parameters:
   - **Computer group name**.
   - **Policy**. From the drop-down list select security policy that will be assigned to this computer group .
4. Define a list of computers in a group:
   - To add one or several computers click **Add**. In the opened **Add computer to the group** dialog you can select computers from:
     - directory service (for example, Active Directory)
     - Microsoft Windows Network
     - ones registered in System previously (for example, after manual Device Monitor Client installation) and already belonging to other Device Monitor groups.

     Select a node from a tree in left panel then flag computers which you want to add to the group.
     You can also make a search of a computer in the directory. For this end enter a part or a computer name to the upper field and click **Find**.
     When all needed computers are selected click **Save**: this closes addition window and returns you to configuring group settings.
   - To delete computer from the list select it and click **Delete**.
5. You can set particular speed of sending data from the Clients for computers belonging to the group (the

configuring of a common value is described in "Common Settings for Clients", **Limit the speed of sending data** setting). To do this:

a. in the **Speed of sending data from client** area select **Override group settings**;

b. in the **Maximum speed of sending data** field specify the needed value, Kbps.

The setting is not selected by default.

6. You can set particular volume of a minimum free disk space (when it is reached on the managed computer, shadow copies would not be created) for computers belonging to the group (the configuring of a common value is described in "Common Settings for Clients", **Minimum free disc space of the client** setting). To do this:

a. in the **Control of disk space of the client** area select **Override group settings**;

b. in the **Minimum free disc space of the client** field specify the needed value, percent.

The setting is not selected by default.

7. You can set particular mode of Client hiding for computers belonging to the group (the configuring of a common value is described in "Common Settings for Clients", **Agent activity on computer** setting group). To do this:

a. in the **Agent activity on computer** area select **Override group settings**;

b. select or deselect **Show employee notifications** and **Hide Agent presence** settings.

The setting is not selected by default.

8. Click **Save**.

Warning!
To apply changes you have to save current security schema (see "Editing Security Schema"). If you don't save your security schema, all changes will be discarded.

3.4.3.4.4 Deleting Computer Group

To edit or delete computer group:

1. Go to **Computers**.
2. In **Computers** area of Navigation pane select computer group name.
3. Take one of the following steps:
   - in the Main Menu select **Edit > Delete**;
   - click **Delete** at the top of Navigation pane.
4. In the following confirmation dialog select **Yes** to confirm that you want to delete computer group.

   Warning!
   The group you are deleting may contain computers that don't belong to any other group. If you delete the only group these computers belong to, they will be automatically added to "default" group.

5. Click **OK**.

Warning!
To apply changes you have to save current security schema (see "Editing Security Schema"). If you don't save your security schema, all changes will be discarded.

3.4.3.4.5 Adding Computer to a Group

When installing InfoWatch Device Monitor Client (see "InfoWatch Device Monitor Client Setup"), computer is added to "default" computer group. All computers inside "default" group will be affected by security policy assigned to this group. Further on, you can assign security policies by assign a computer to various computer groups.

To move a computer from one computer group to another:

1. Go to **Computers**.
2. In **Computers** area of Navigation pane, select computer group that contains the computer.

3. Select a row that contains the computer you want to add to another group. Click and hold the selected row and drag the computer to **Computers** area of Navigation pane. Move the pointer over the name of computer group you want to add the computer to. When a yellow arrow appears to the left of the selected group name, release the mouse button.

This adds computer to selected computer group.

You can also add information about computers without InfoWatch Device Monitor Client manually. Computer information is imported from directory service (connection configuring settings see in "Connecting to LDAP Server") or your network environment. Then after InfoWatch Device Monitor installation this computer (see "Creating Primary Distribution Task") will be affected by the policy of the group it was added to.

The mobile devices do not allow this option.

Warning!
It is not recommended to add computers with similar names. These computers will be registered in InfoWatch Device Monitor system as a single computer, affected by the same policies, and register the same events, etc.

To add computer to a group:

1. Go to **Computers**.
2. In **Computers** area of Navigation pane select computer group name. Main screen will display a list of all computers inside the group.
3. Take one of the following steps:
   - in the main menu select **Edit > Add computer**
   - click **Add computer** located at the top of **Computers** area
   - right-click in the workspace and select **Add computer** from the drop-down menu.

   In the opened dialog you can select computers:
   - imported from directory service (for example Active Directory)
   - received from Microsoft Windows Network;
   - among previously registered in the System.
4. Flag computers or computer groups. Minimized groups are marked with an icon; expanded - . Double-click a group, to expand or collapse it.

   Warning!
   By marking a group you select the computers that are included in that particular group. Subgroups and subgroup computers of selected group are not selected: you have to select them separately.

   You can also specify computer name in the line at the bottom of dialog box. When listing names, separate them with semicolons.
5. Click **OK**.

This closes **Select computer** dialog and adds the information on selected computers to computer group.

Warning!
To apply changes you have to save current security schema (see "Editing Security Schema"). If you don't save your security schema, all changes will be discarded.

3.4.3.4.6 Removing Computer from a Group

Computer is added to a group basing on needed security policies. You might need to disable policy's action to the computer. To perform this procedure, you must remove computer from computer group with this policy.

Note:
If you remove a computer from a single group it belongs to, it will be automatically added to "default" group.

To exclude computer from computer group:

1. Go to **Computers**.
2. In **Computers** area of Navigation pane, select computer group that contains the computer. This displays a full list of computers that belong to selected group.
3. Select a row that contains the computer you want to remove from computer group.
4. Take one of the following steps:
   - in the main menu select **Edit > Remove Computer From Group**
   - click **Remove Computer From Group** located at the top of **Computers** area
   - press **Delete** keyboard button

This removes computer from the group.

Warning!
To apply changes you have to save current security schema (see "Editing Security Schema"). If you don't save your security schema, all changes will be discarded.

3.4.3.4.7 Deleting Computer from Security Schema

You can remove a computer from the list of registered computers (for example, computer discontinued operation). Computer information will not be deleted, but it will be marked as **Inactive** due to Client deactivation.
If you don't want to save inactive computer information, you can delete its record.

To remove computer from security schema:

1. Go to **Computers**.
2. In **Computers** area of Navigation pane, select computer group that contains the computer.
3. In the Main screen workspace, select the row that contains the inactive computer you want to remove.
4. Take one of the following steps:
   - in the Main Menu, click **Edit > Delete Computer From Security Schema**;
   - click **Delete Computer From Security Schema** located at the top of **Computers** area
   - right-click computer row and select **Delete Computer From Security Schema**
   - press **Shift+Delete** at the keyboard.
5. In the following confirmation dialog select **Yes** to confirm that you want to remove the computer.

This removes computer information from all groups the computer was assigned to.

Warning!
To apply changes you have to save current security schema (see "Editing Security Schema"). If you don't save your security schema, all changes will be discarded.

3.4.3.4.8 Updating Clients at Managed Computers

Device Monitor Clients at managed computers can be simply updated by the task (see task details in "Clients Remote Installation, Updating and Uninstallation" and "Creating Updating Task").

To update Device Monitor Clients at all managed computers of the group:

1. Go to **Computers**.
2. In **Computers** area of Navigation pane, select computer group.
3. Click **Update All Computers** located at the top of Navigation pane.

To update Device Monitor Clients at selected managed computers:

1. Go to **Computers**.
2. In **Computers** area of Navigation pane, select computer group.
3. In the Main screen workspace, select the row(s) containing managed computer(s). To select several computers click at them while pressing **Shift** or **Ctrl** button.
4. Click **Update Computers** located at the top of **Computers** area.

This creates and runs the update task for selected computers.

3.4.3.4.9 Diagnostics of the Workstation

The System provides the feature of remote collection of diagnostic data from the workstations.

Warning!
The collection of diagnostic data is available for workstations only: the mobile devices do not have this opportunity.

To start diagnostic data collection on the computer:

1. Go to **Computers** section.
2. In **Computers** area of Navigation pane select computer group name.
3. In the computer list right-click the computer row and select **Diagnostics > Enabling diagnostic mode**.

To stop diagnostic data collection on the computer:

1. Go to **Computers** section.
2. In **Computers** area of Navigation pane select computer group name.
3. In the computer list right-click the computer row and select **Diagnostics > Disabling diagnostic mode** .

To get the archive containing all provided diagnostic data:

1. Go to **Computers** section.
2. In **Computers** area of Navigation pane select computer group name.
3. In the computer list right-click the computer row and select **Diagnostics > Gathering diagnostic data**.
4. In the **Select path to save archive with diagnostic data** dialog specify folder and file name.
5. Click **OK**.

3.4.3.5 Mobile Devices

Besides workstations, InfoWatch Device Monitor allows you to control employees' mobile devices (smartphones and tablet PCs).

InfoWatch Device Monitor Client can work with the following models of mobile devices, Android OS versions and build numbers:

Device model	Android version	Build number
ASUS Nexus 7 2013 LTE (K009)	4.3.0	JLS36C
	4.4.2	KOT49H
	4.4.3	KTU84L
	4.4.4	KTU84P
Samsung Galaxy S3 (I9300)	4.3.0	JSS15J.I9300XXUGNK1
		JSS15J.I9300XXUGND2
Samsung Galaxy S4 (I9500)	4.3.0	JSS15J.I9500XXUEMK8
Samsung Galaxy S4 (I9505)	4.3.0	JSS15J.I9505XXUEMK9
		JSS15J.I9505XXUEML4
	4.4.2	KOT49H.I9505XXUGNG8
		KOT49H.I9505XXUFNC9
Samsung Galaxy S5 (SM-G900F)	4.4.2	KOT49H.G900FXXU1ANE2
		KOT49H.G900FXXU1ANK7

InfoWatch Device Monitor Client also supports devices on iOS platform: you can install InfoWatch Device Monitor Client on iPhone or iPad versions 8.0 - 9.0.2.

Warning!

Installing InfoWatch Device Monitor on iPhone or iPad is possible only if the device is jailbroken.

The System can associate several mobile devices with one employee, but a single mobile device can be associated with one employee only.

Warning!

To manage a mobile device entry and to install or uninstall InfoWatch Device Monitor Client, the following requirements should be met:

- USB Debugging mode must enabled on the mobile device and all required drivers should be installed (for devices on Android platform only);
- the Management Console should run on a physical workstation (using virtual machines or remote desktop connections is not recommended; Microsoft Windows XP is not supported);
- the mobile device directly must be connected via USBe to the computer where the Management Console is running.

See details in "Preparing a Mobile Device on Android Platform" and "Preparing a Mobile Device on iOS Platform".

Guidelines on Clients installation and uninstallation for mobile devices are available in:

- Preparing a Mobile Device on Android Platform
- Preparing a Mobile Device on iOS Platform
- Adding a Mobile Device to Computer Group

- Adding a Mobile Device through Appointment to Employee
- Deleting the Mobile Device

3.4.3.5.1 Preparing a Mobile Device on Android Platform

If you are using a mobile device on Android platform, then to install, update or delete InfoWatch Device Monitor Client, you should:

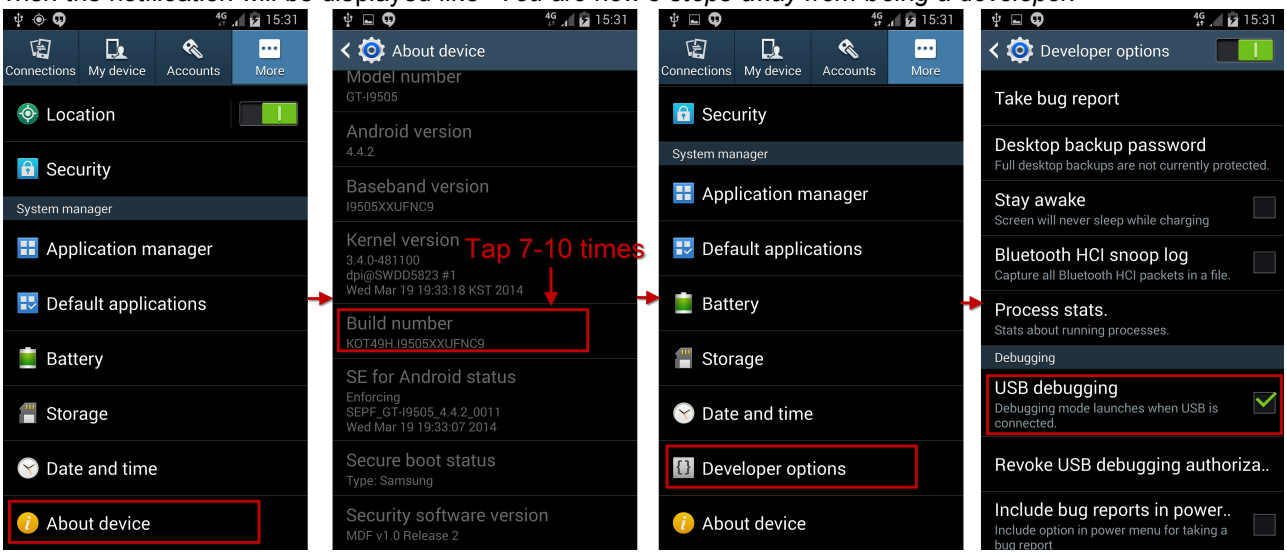
1. Enable "**USB debugging**" mode on the device: see example below.
2. Via a USB-wire connect this device to the computer where Device Monitor Management Console is running.
3. If necessary (for example, for some builds of Samsung), install additional drivers.

Step 1. Enabling "USB debugging" mode

The process of enabling the "USB debugging" mode can slightly vary for different models of mobile devices, different versions of OS and firmware.

Enabling the debugging mode for Samsung Galaxy S4 with Android 4.4.2:

1. Enable developer mode: **Settings -> About device -> Build number**; tap the build number several times (7 - 10).
   Then the notification will be displayed like "*You are now 3 steps away from being a developer.*"



2. Continue tapping till successful mode enabling.
3. Return to **Settings** menu. Select **Developer options** appeared near **About device**.
4. Select **USB debugging**.

You can disable the debugging mode when the installation, updating or deleting the InfoWatch Device Monitor Client is successfully completed.

Huawei feature:

The Huawei models can automatically disable USB debugging mode if the connection with the computer is lost. Therefore the debugging mode should be enabled every time after connecting to the the computer.

Step 2. Connecting to the computer

To install or update the InfoWatch Device Monitor Client, you should connect the mobile device to the physical workstation where Device Monitor Management Console is running, via the USB-wire.

Warning!

If you are using a virtual machine or connection to a remote desktop, then the installation can fail due to increasing of the System response time. Therefore, we recommend that you should not use virtual machines or remote desktops.

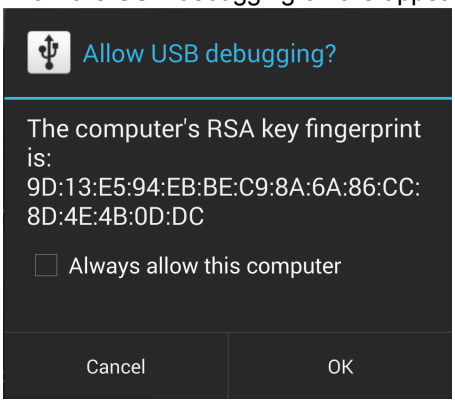
The System does not support installation of Device Monitor Client to mobile devices if the Management Console is running on a computer with Microsoft Windows XP. Therefore, we do not recommend using Microsoft Windows XP either.

You can see if the connection was successful and control the further installation of drivers in **Device Manager** (**Control Panel -> Hardware and Sound -> Device Manager**).

Samsung feature:

If the phone is "clear" - for example the build is just updated, - then you can need to perform additional actions:

1. On the phone slide down the notification panel.
2. Switch the device from the "**Multimedia**" connection mode to the "**Camera**" mode.
3. Allow the USB debugging on the appeared query.



Step 3. Drivers installation

In a first connecting of the mobile device to the computer where the Device Monitor server is working the automatic installation of the following drivers is performed:

- a driver for operation in a normal mode
- the **libusb** driver for operation in the downloaded mode

During installation of the drivers, the icon on the Device Monitor server's computer taskbar displays the process of drivers searching and installation.

Warning!

Do not disconnect the mobile device during drivers installation! Wait for installation completion.

When installation of a driver is completed successfully, the computer will display a notification that this driver is ready to use.

In case of some errors in drivers installation, you can find solutions in InfoWatch Knowledge base: "Mobile Device Driver Cannot Run Automatic Installation" or "Installing the Driver for Downloaded Mode" (libusb0)" for example.

3.4.3.5.2 Preparing a Mobile Device on iOS Platform

If you are using a mobile device on iOS platform, then to install, update or delete InfoWatch Device Monitor Client, you should:

1. Jailbreak your mobile device (iPhone or iPad).

2. On the computer where Device Monitor Management Console is installed, install iTunes.
3. Connect the mobile device to the computer, where Device Monitor Management Console is installed, via a USB-wire.
4. Authorize the mobile device on the computer.

Step 1. Jailbreaking the mobile device

Installing InfoWatch Device Monitor Client on iPhone or iPad is possible only if the device is jailbroken.

Note:
The supported versions of iPhone and iPad are 8.0 - 9.0.2.

Step 2. Installing iTunes

To install InfoWatch Device Monitor Client on a mobile device, it is necessary that Apple Mobile Device Support application should be installed on the computer (it is installed together with iTunes).

Step 3. Connecting to the computer

To install or update InfoWatch Device Monitor Client, you should connect the mobile device to the physical workstation where Device Monitor Management Console is running, via the USB-wire.

Warning!
If you are using a virtual machine or connection to a remote desktop, then the installation can fail due to increasing of the System response time. Therefore, we recommend that you should not use virtual machines or remote desktops.

The System does not support installation of Device Monitor Client to mobile devices if the Management Console is running on a computer with Microsoft Windows XP. Therefore, we do not recommend using Microsoft Windows XP either.

You can see, if the connection was successful, and control the further installation of drivers in **Device Manager** (**Control Panel -> Hardware and Sound -> Device Manager**).

Step 4. Authorizing the device on the computer

Once you have connected the device to your computer, you should authorize the device on this computer. For this:

1. Run iTunes on the computer.
2. In the message that appears on the device, confirm that this computer can be trusted.
3. On the computer, in the iTunes menu bar, select **Store** -> **Authorize this computer**.

3.4.3.5.3 Adding a Mobile Device to Computer Group

Mobile devices can be added to the security schema from the computer group with specifying the employee created in the System before or added from LDAP.

Warning!
To install InfoWatch Device Monitor Client, there should be:

- USB Debugging mode enabled on the mobile device and all required drivers installed (for devices on Android platform only);

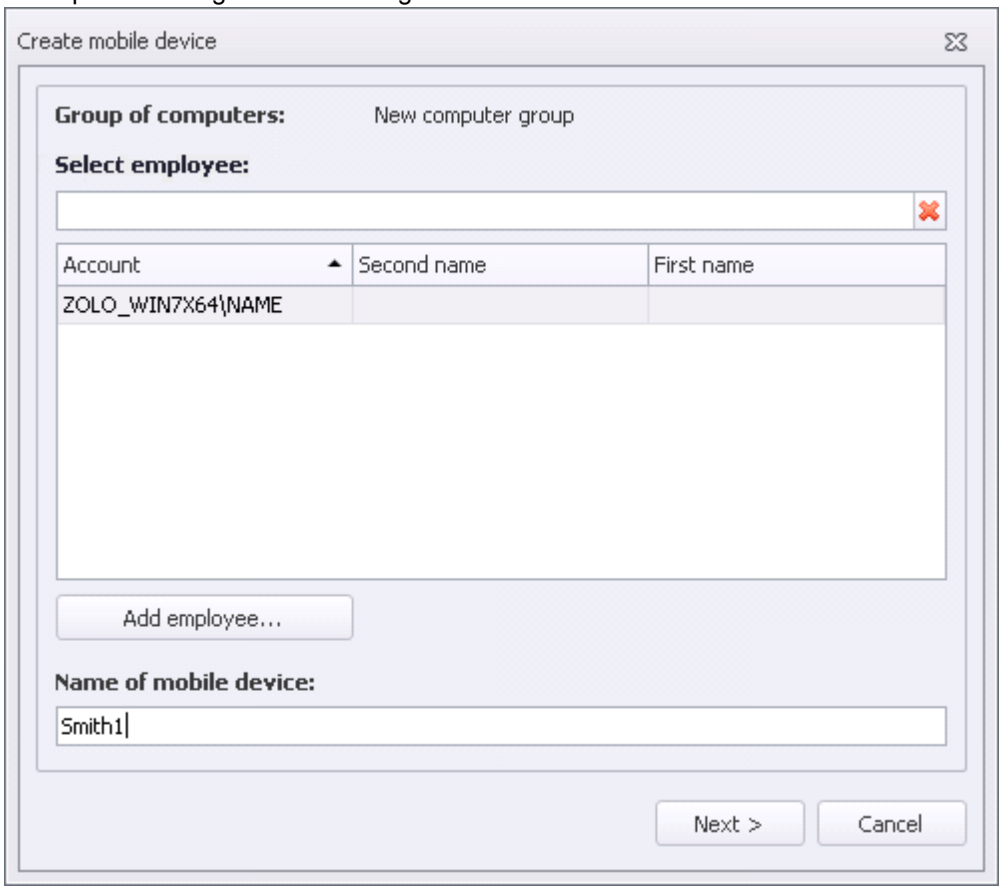
- the Management Console running on the physical workstation (using virtual machines or remote desktop connections is not recommended; using of the Microsoft Windows XP is not supported);
- mobile device directly connected via USB wire to the computer where the Management Console is running.

Details see in "Preparing a Mobile Device" and "Preparing a Mobile Device on iOS Platform".

To add a mobile device to the computers group and install the InfoWatch Device Monitor Client to it:

1. Go to the **Computers** section.
2. In **Computers** area of Navigation pane select computer group name where you want to add a mobile device to.
3. Take one of the following steps:
   - in the main menu select **Edit > Create mobile device**;
   - click **Create mobile device** button located in the upper part of the **Computers** area;
   - right-click on the workspace and select **Create mobile device** from the context menu.

   This opens a dialog box for creating the mobile device.



4. In the employees list select the needed account.
   You can also start typing the account name to the entry field: the list will be filtered.
   If there is no needed account in the list, you can add it: click **Add employee**. The adding procedure see in "Adding Employee Account to a Group".
5. If needed, change the name of the mobile device entry.
6. Click **Next**.
7. In the opened installation dialog window select the connected mobile device.
8. Click **Install**.
9. When the installation is completed, click **Finish**.

This will install the InfoWatch Device Monitor Client to the mobile device and add the entry of the new mobile device to the selected computer group of the security schema. The new mobile device will be associated with the selected

employee.

Warning!

Just after the Client installed to the mobile device, this device will have a policy appointed to the default computer group, and only when the security schema will be saved, the device will have a policy appointed to the computer group specified on mobile device adding.

Information on saving the security schema see in "Editing Security Schema".

3.4.3.5.4 Adding a Mobile Device through Appointment to Employee

Mobile devices can be added to the security schema from the entry of the employee which you want to assign this mobile device.

Warning!

To install InfoWatch Device Monitor Client, there should be:

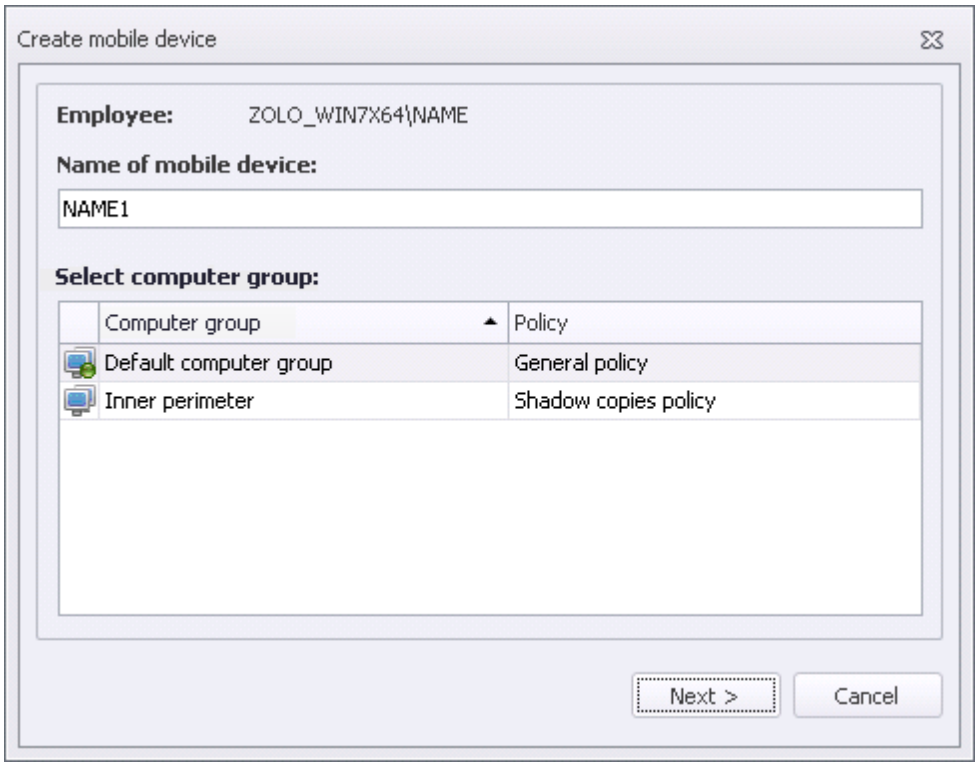
- USB Debugging mode enabled on the mobile device and all required drivers installed (for devices on Android platform only);
- the Management Console running on the physical workstation (using virtual machines or remote desktop connections is not recommended; using of the Microsoft Windows XP is not supported);
- mobile device directly connected via USB wire to the computer where the Management Console is running.

Details see in "Preparing a Mobile Device" and "Preparing a Mobile Device on iOS Platform".

To add a mobile device to the security schema through the employees group and install the InfoWatch Device Monitor Client to this device:

1. Go to the **Employees** section.
2. In the **Employees groups** area on the Navigation pane select the group which contains the needed employee.
3. Select the employee list which you want to assign a mobile device to.
4. Take one of the following steps:
   - in the main menu select **Edit > Create mobile device**;
   - click **Create mobile device** button located in the upper part of the **Employees** area;
   - right-click on the workspace and select **Create mobile device** from the context menu.

   This will display the dialog of creating the mobile device.



5. If needed, change the name of the mobile device entry.
6. Select the needed computer group from the list.
7. Click **Next**.
8. In the opened installation dialog window select the connected mobile device.
9. Click **Install**.
10. When the installation is completed, click **Finish**.

This will install the InfoWatch Device Monitor Client to the mobile device and add the entry of the new mobile device to the selected computer group of the security schema. The new mobile device will by associated with the selected employee.

Warning!

Just after the Client installed to the mobile device, this device will have a policy appointed to the default computer group, and only when the security schema will be saved, the device will have a policy appointed to the computer group specified on mobile device adding.

Information on saving the security schema see in "Editing Security Schema".

3.4.3.5.5 Deleting the Mobile Device

The removing the mobile device from the security schema without uninstalling the InfoWatch Device Monitor Client is performed in the way common for all the computers: see "Deleting Computer from Security Schema". For this action no device connection is needed.

Warning!

To uninstall InfoWatch Device Monitor Client, there should be:

- USB Debugging mode enabled on the mobile device and all required drivers installed (for devices on Android platform only);
- the Management Console running on the physical workstation (using virtual machines or remote desktop connections is not recommended; using of the Microsoft Windows XP is not supported);

- mobile device directly connected via USB wire to the computer where the Management Console is running.

Details see in "Preparing a Mobile Device" and "Preparing a Mobile Device on iOS Platform".

To delete the mobile device from the security schema and uninstall the InfoWatch Device Monitor Client from this mobile device:

1. In the main menu select **Tools > Delete mobile device**.
2. In the opened installation dialog window select the connected mobile device.
3. Click **Uninstall**.
4. When the uninstallation is completed, click **Finish**.

This will uninstall the InfoWatch Device Monitor Client from the mobile device and delete the entry of the new mobile device from the computer group and security schema.

3.4.3.6 White Lists

You can manage lists of devices with full access from **White Lists** section. To go to this section, click **White Lists** button at Navigation pane.

For more information on white lists see:

- Viewing White List Details
- Adding White List
- Defining Entry Validity Period
- Editing White List
- Deleting White List

You can view an information on acting white lists as described in "Viewing Resultant Policy and White List for Employee" and "Viewing Resultant Settings, Policy and White List for a Computer".

3.4.3.6.1 Viewing White List Details

White Lists area of Navigation pane displays all white lists. Main screen work pane displays devices (models and instances) in selected white list.

Note:
You can make search in white list index: type the name of the list in the search box below the index on Navigation pane.
You can adjust the displaying of selected white list using additional features (see "Additional Features").

To view information for separate white list,

select white list title in the group.

White lists information is available as a list of devices grouped by their type. Each row in the list contains device model or instance. Columns contain devices' general properties. Extended information on device properties is displayed in **Details** panel.

To view detailed information on device properties,

select the row that contains device model or instance name.

Details panel displays properties table including the following information:

- **Device instance or model identifier**. Model code (VID - Vendor ID) or device instance serial number (PID-Product ID).
- **Device description**.
- **Device type**.
- **Category**. Model or instance.

- **Period**. Full access period starting and expiry date and time.
- **Detected on computer**. Name of computer where the device was detected.
- **Added to database at**. Date of device information submission to database (see "Adding Device to Database ").

Note:
Some of the properties on **Details** panel are duplicated in the main screen workspace.

3.4.3.6.2 Adding White List

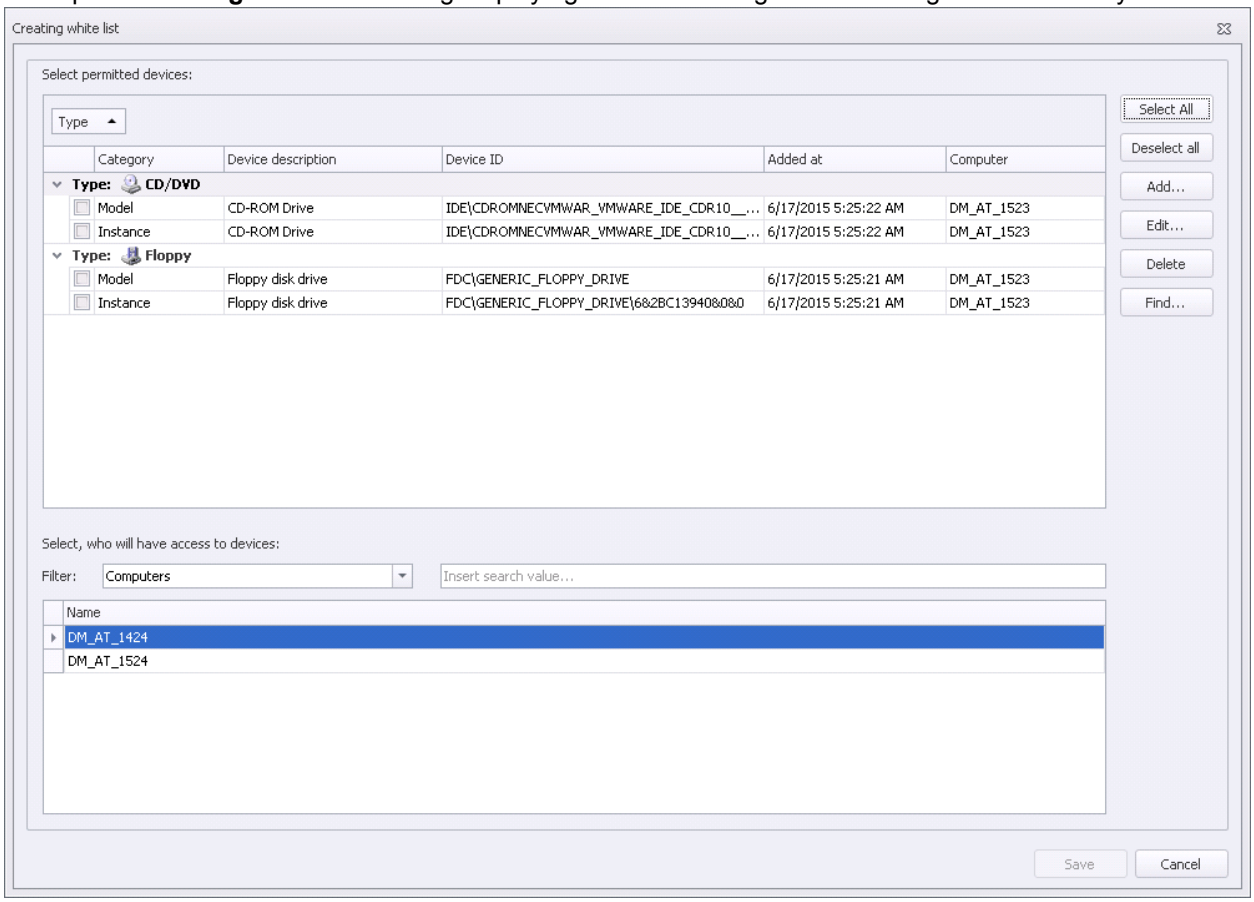
White list affects selected objects: employees, employee groups, computers or computer groups.

Warning!
A single object (employee, employee group, computer or computer group) can have only one white list assigned to.

To add white list:

1. Go to **White Lists** section.
2. Take one of the following steps:
   - select **Edit > Create White List** in the Main Menu;
   - click **Create White List** at the top of Navigation pane.

   This opens **Creating White List** dialog displaying table containing all devices registered in the System.



3. In the table of devices select models and instances which should have full access to.

> **Warning!**
>
> Information on creating a list of registered device models and instances see in:
>
> - Adding Device Entry;
> - Deleting Device Entry.

4. In **Select, who will have access to devices** area select a filter: who will be affected to white list action:
   - employees
   - employee groups
   - computers
   - computer groups

   The list of entries will appear below.

   You can also use a search string by entering a name or its part.
5. Select employee / employee group / computer / computer group that will have full access to selected devices.
6. Click **Save**.

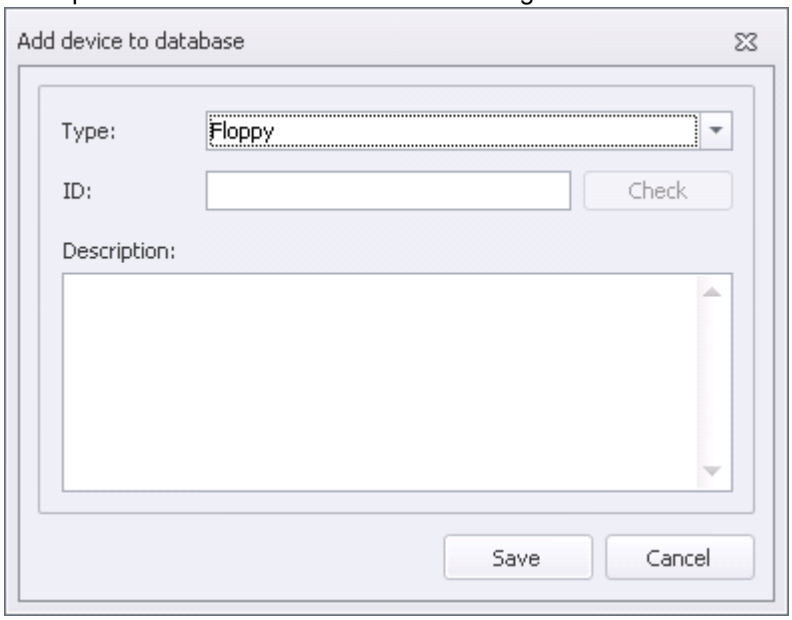
3.4.3.6.2.1 Adding Device Entry

You can add to white lists only device models and instances which were previously registered in the System. Device information is added in two ways:

- manually (if device ID is provided)
- via search engine (if device is connected to managed computer).

To add device information manually:

1. Open **Creating White List** dialog box (see "Adding White List").
2. Click **Add** button at the right of the window.
   This opens **Add device into database** dialog box.



3. Specify device parameters:
   - select device type from **Type** drop-down list
   - enter the device instance or model identifier into **ID** box

Note:
To retrieve device instance string, connect the device and use standard Windows tools (for example, **Device Manager**) to view its properties. Device instance string is displayed on **Information** tab.
Device instance string is displayed as XXX\YYY\ZZZ where XXX is device type (usually, connection type, such as USB, IDE or ACPI), YYY is device model string (Vendor ID), and ZZZ is device instance string (Product ID).
Model ID is displayed as XXX\YYY where XXX is device type and YYY is model ID string (VID).

To make sure the ID is valid, click **Check**.

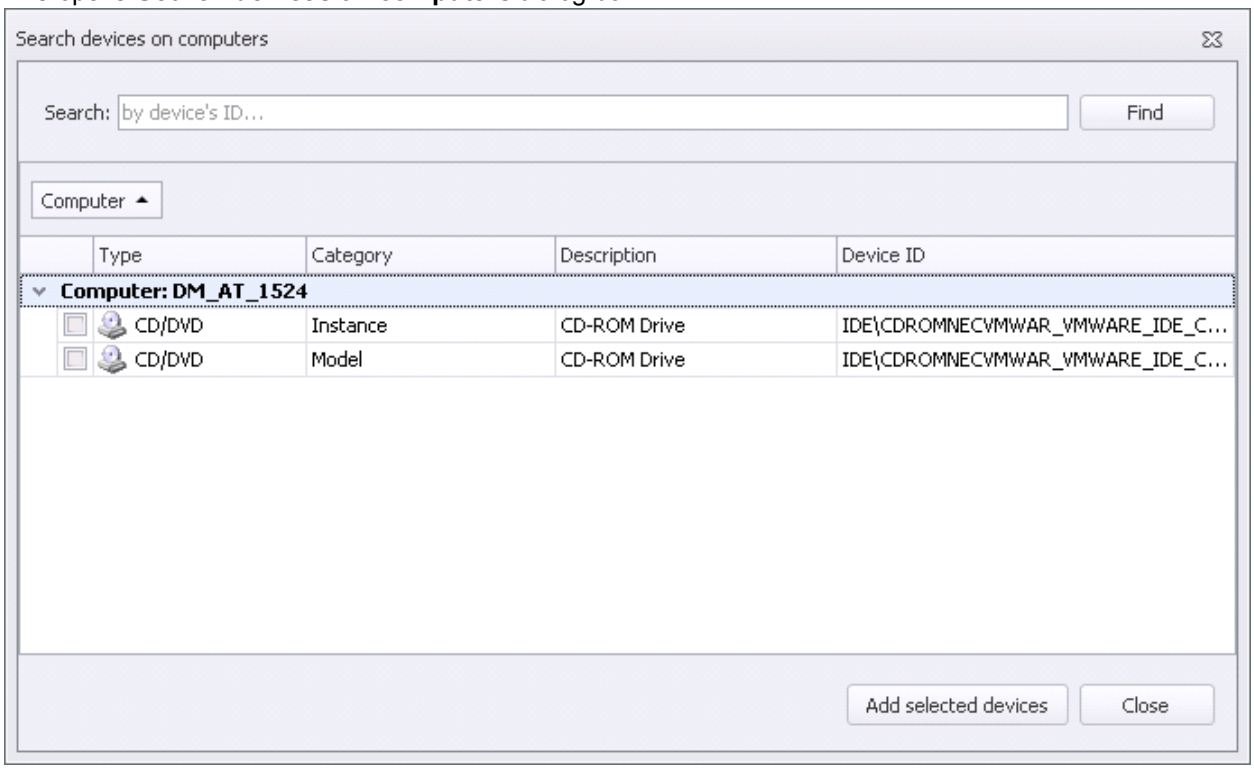
Warning!
When using instance code, take into account that some devices do not have unique ID: ID can be changed dynamically and differed even when connecting to different ports of the same computer. In such case using device model code is recommended.

- enter description into **Description** box.

4. Click **Add**.

To add device information via searching devices connected to managed computers:

1. Open **Creating White List** dialog (see "Adding White List").
2. Click **Find** at the right.
   This opens **Search devices on computers** dialog box.



3. Use one of the following ways to select a managed computer from the list:
   - click next to computer;
   - double-click computer name.

   You will see a list of devices which were connected to selected computer during all the time Device Monitor Client was installed at the computer.
4. Flag the devices you want to add.
5. Click **Add selected devices**.

3.4.3.6.2.2 Deleting Device Entry

To remove device entry from database:

1. Open **Creating White List** dialog (see "Adding white list").
2. Select and right-click device instance or model in device database table. In the drop-down menu, select **Delete device**.
3. In confirmation dialog click **OK**.

3.4.3.6.3 Defining Entry Validity Period

Each device instance or model from the white list has an access permission displayed separately. This item's (permission's) default validity period is practically infinite (from 01.01.1753 to 31.12.9999). You can limit full access period for this device. This device will be subject to general rules that apply to this device type before and after the specified period.

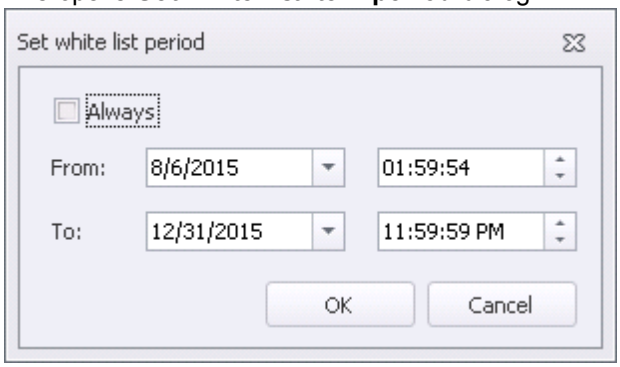
To set white list entry period:

1. Go to **White Lists**.
2. In **White Lists** area of Navigation pane select white list that contains the item.
3. If white list items are grouped in (for example, by the type of devices), expand them (see "Grouping Entries ").

   Note:
   If you set validity period for the entire group, the change will only take effect for the first item of the group.

4. Select the row that contains device instance or model you want to assign validity period to and take one of the following steps:
   - select **Edit > Edit Item** in the Main Menu
   - click **Edit Item** at the top of **Permitted devices** area
   - double-click selected entry name;
   - right-click entry row and select **Edit Item** from drop-down menu.

   This opens **Set white list item period** dialog.



5. Set item validity period and click **OK**.

3.4.3.6.4 Editing White List

To edit white list parameters:

1. Go to **White Lists**.
2. In **White Lists** area of Navigation pane select the name of white list.
3. Take one of the following steps:
   - in the Main Menu, click **Edit > Edit**;
   - click **Edit** at the top of Navigation pane;
   - double-click selected white list name.

These actions open **Edit white list** dialog box. This dialog is similar to **Creating white list** dialog with the exception of **Select, who will have access to devices** area, which is unavailable.

4. You can add or remove devices from database, if needed (see "Adding Device to Database" and "Removing Device from Database").
   You can also change the description of previously registered device: to do this select the device in the index and click **Edit** button at the right of the window. In the opened window change the description text and click **Save**.
5. Add or remove flags in device database table to change the catalog of models and instances in the white list.
6. Click **Save**.

Warning!
To apply changes you have to save current security schema (see "Editing Security Schema"). If you don't save your security schema, all changes will be discarded.

3.4.3.6.5 Deleting White List

To delete white list:

1. Go to **White Lists** section.
2. Click the white list you want to delete.
3. Take one of the following steps:
   - select **Edit > Delete** in the Main Menu;
   - click **Delete** at the top of Navigation pane.
4. In confirmation box click **Yes** to confirm that you want to remove the white list.

Warning!
To apply changes you have to save current security schema (see "Editing Security Schema"). If you don't save your security schema, all changes will be discarded.

3.4.3.7 Signatures

File Monitor rules can be configured to affect only files of specific structure distinguishing defined file format. To do this, InfoWatch Device Monitor defines file format basing on its **signature**.

Signatures section contains a list of signatures which the System can recognize. Signatures are conveniently grouped into **categories**.

To view available signatures:

1. Go to **Signatures** by clicking the **Signatures** button in Navigation pane or selecting in Main Menu **Go > Signatures**.
   Signatures area of Navigation pane displays a list of **signature categories**.
2. Select a signature category from the list.
   Main screen workspace will display a list of all signatures in the selected category.

Warning!
Predefined signature categories cannot be edited or deleted. You can't create new signatures.

You can do the following:

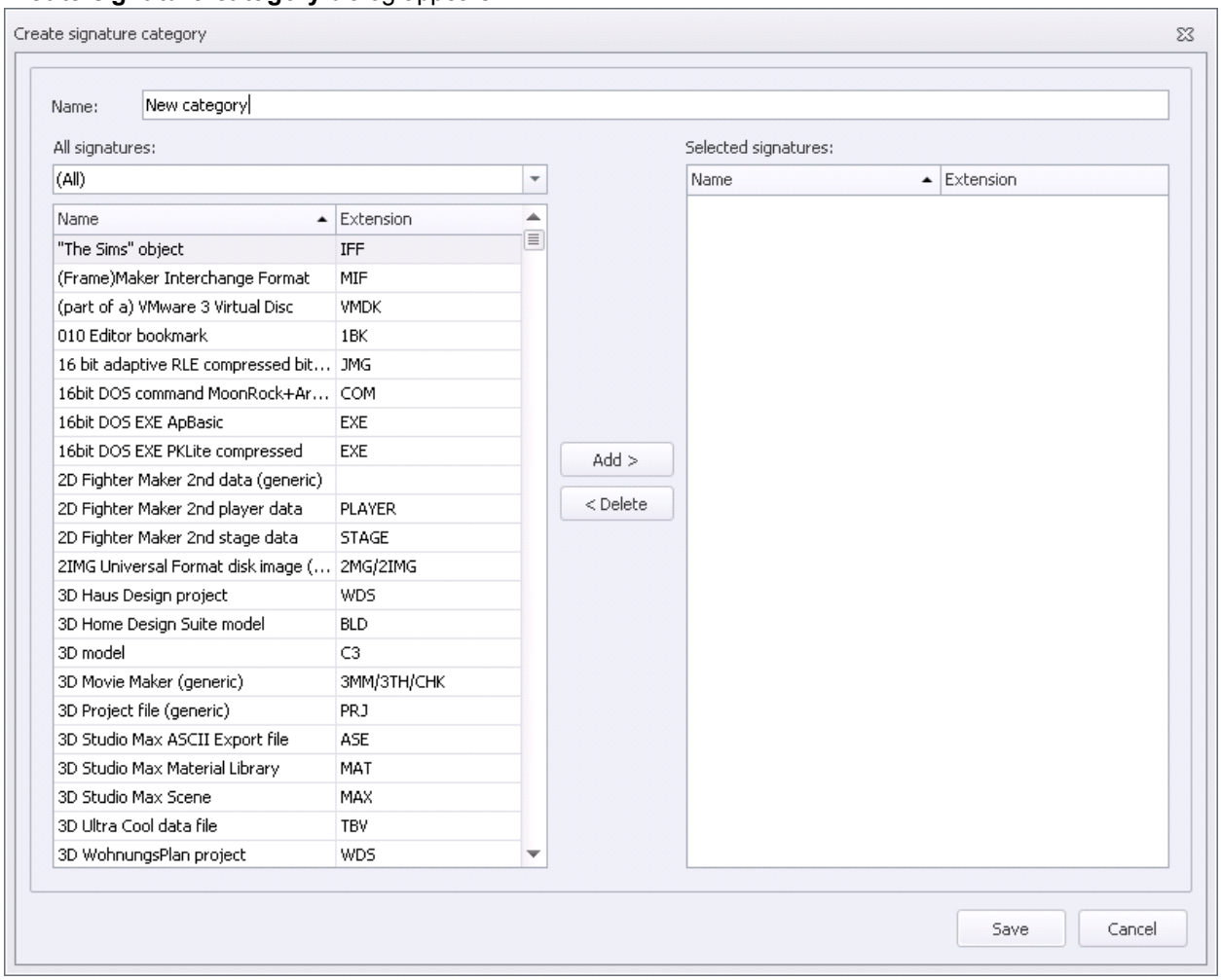
- create signature categories
- fill created categories by copying predefined signatures
- delete your signature categories, if they are not used by any rule.

3.4.3.7.1 Adding Signature Category

To add signature category:

1. Go to **Signatures**.
2. Take one of the following steps:
   - in the main menu select **Edit > Create signature category**;
   - click **Create signature category** at the top of Navigation pane.

   Create signature category dialog appears.



3. Enter new category's name.
4. In **All signatures** area you can select one of preset categories from the list. All preset signatures are displayed by default.
5. In the left panel select signatures you want to add to a new category.
   To select several signatures hold **Ctrl** or **Shift** button.
   To move selected signatures to a new category click **Add**.
   To delete signatures from the list of included to a new category selected them at the right panel **Selected signatures** and click **Delete**.
6. Click **Save**.

3.4.3.7.2 Editing Signature Category

After you have created a signature category (see "Adding Signature Category") you can fill it by:

- in signature category editing dialog (select a category and click **Edit > Edit** in the Main Menu or click **Edit** at the top of Navigation pane or double-click selected category name) define a list of signatures as

described in "Adding Signature Category".

or

- by copying signatures from other categories directly at main screen workspace .

To copy signature from one category to another:

1. Go to **Signatures**.
2. In **Signatures** area of Navigation pane select the name of predefined category that contains the signature you want to copy.
3. In main screen workspace select the row that contains the name of the signature you want to copy. You can select multiple signatures at a time with **Ctrl** or **Shift**.
4. Click and hold the selected row and drag the pointer to **Signatures** area of Navigation pane. Move the pointer over the category you created earlier where signatures will be added. Release the button when a yellow arrow appears next to the selected category.

As a result, the signature will be copied into selected category.

To remove a signature from category,

select signature and do one of the following:

- click **Remove signature from category** at the top of **Signatures** area
- right-click and select **Remove signature from category** in the drop-down menu.
- press **Delete** keyboard button.

3.4.3.7.3 Deleting Signature Category

Warning!
The following categories cannot be deleted:

- signature categories used by any File Monitor rule
- predefined signature categories.

To delete a signature category:

1. Go to **Signatures**.
2. Click the signature category name.
3. Take one of the following steps:
   - in the main menu select **Edit > Delete**
   - click **Delete** at the top of Navigation pane.
4. In the next confirmation dialog select **Yes** to confirm that you want to remove signature category.

Warning!
To apply changes you have to save current security schema (see "Editing Security Schema"). If you don't save your security schema, all changes will be discarded.

3.4.3.8 Application Protocol

After the InfoWatch Device Monitor Client is installed onto the computer (computer or mobile device) and the computer is rebooted, the System automatically starts to receive data on applications launched on managed workstations and installed on managed mobile devices.

Data on all launches and installations produces an *application protocol*.

Warning!
Application protocol excludes system vital applications. One can not forbid application which absence is

obstructive for computer properly operation.

Managing the application protocol is performed in the **Applications** section. To go to this section click **Applications** button located on the Navigation pane or select **Go > Applications** command in the main menu.

The Navigation pane is divided onto two groups in this section: **List of applications** and **Applications Protocol**:

- The **List of applications** group contains lists used to control employee's access to applications:
  - forbid launching applications in one of two modes: white lists and black lists. See details in "Configuring Application Monitor Rule";
  - forbid screenshots creating. See details in "Configuring ScreenShot Control Monitor Rule";
  - automatic creating the screenshots by the System.
- The **Applications Protocol** group is intended for creating filters showing data on all applications launched on managed workstations and installed on managed mobile devices. In this group you can add applications to lists.

Information on protocols and applications managing see in:

- Creating an application list and adding applications
- Creating and editing the application protocol filter
- Adding Application to List Automatically
- Adding Application to List Manually
- Exporting Application Protocol

3.4.3.8.1 Creating an Application List and Adding Applications

To manage white and black application list, the System offers application lists creation from the **Application protocol** (see "Application protocol").

Lists are used to permit or forbid application usage on computers.

To create an empty application list:

1. Go to **Applications** section.
2. On the Navigation pane set the cursor on the **List of applications** group and take one of the following steps:
   - in **List of applications** group menu click **Create list of applications**
   - select **Edit > Create list of applications** command in the main menu
   - right-click in the **List of applications** group and select **Create list of applications** from the drop-down list.
3. In the **List Name** field enter a name for a list you create.
4. Click **Save**.

Details on filling lists and creating lists from application protocols see "Adding Application to List Automatically" and "Adding Application to List Manually".

To select an application from the list:

1. Go to **Applications** section.
2. Set the cursor on the **List of applications** group.
3. Click in **List of applications** group menu.
4. Select application(s) from list(s) and click **Add applications to the list**.
5. From the drop-down list select **Add applications automatically** or **Add applications manually**.

To edit application in the list:

Click button on the **List of applications** group.

You can edit details which will be used to filter the application (see "Adding Application to List Manually")

To delete application from the list:

1. Click button on the **List of applications** group.
2. Click **Yes** to delete application from the security scheme.

3.4.3.8.2 Creating and Editing the Application Protocol Filter

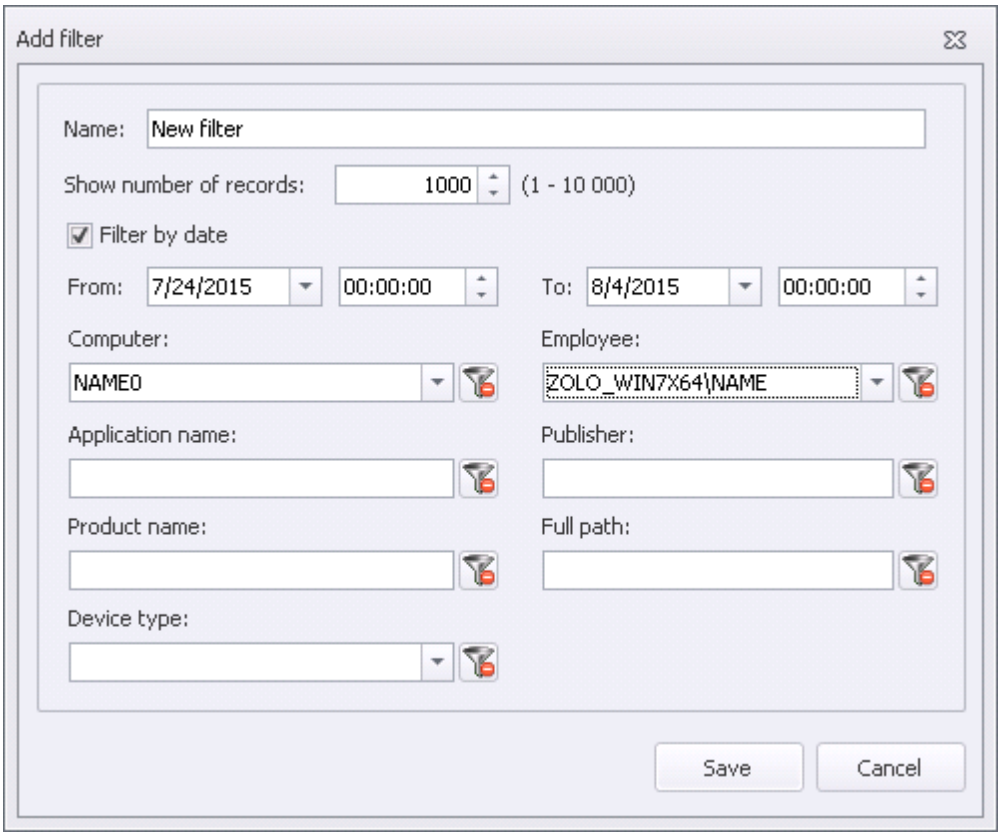
Filters allow to configure an application protocol (see "Application protocol") to display an information on applications corresponding to your conditions only.

Warning!
Preset **Today** filter shows applications which have been started on particular day since initial installation of the Client.
All filter shows applications which have been started right upon Client installation.

To create a new filter:

1. Go to **Applications** section.
2. On the Navigation pane set the cursor on the **Application Protocol** group and take one of the following steps:
   - in the click button in **Application Protocol** group on Navigation pane
   - select **Edit > Create filter** command in the main menu
   - right-click in the **Application Protocol** group and select **Create filter** from the drop-down list.

   This opens a dialog box with filter parameters.



3. Enter the name of the filter in **Name** field.
4. In the **Show number of records** field enter the number of records you want to see in the protocol.
5. To set up period for the records to be displayed flag the **Filter by date** option and specify parameters **From**

and **To**.

6. If needed, specify additional filter conditions:
   - in **Computer** field select employee's computer which protocol you need to view
   - in **Employee** field select account of employee which launches applications
   - in **Application name** field type in the name of the application you want to see information about
   - in **Publisher** field type in the program publisher
   - in **Product name** field pick the name of the product
   - in **Full path** specify the path to the application location
   - from **Device type** drop-down list select whether the filter should display information on applications launched on computers or installed on mobile devices.

   Click button to delete filter.
7. Click **Save**.

To edit filter:

Click button in **Application protocol** on Navigation pane or press **Ctrl+E**.

To delete filter:

1. Click button in **Application protocol** on Navigation pane or press **Ctrl+D**.
2. Click **OK** to confirm deletion.

3.4.3.8.3 Adding Application to List Automatically

The System allows to fill application lists automatically using data received from the application protocol.

To add application to the list automatically:

1. Go to **Applications** section.
2. On the Navigation pane select the needed filter in the **Application protocol** group.
3. On the **Application protocol** pane select one or several entries. To select several entries click at them while pressing **Shift** or **Ctrl** button
4. Take one of the following steps:
   - on the **Application protocol** pane click **Add application to list automatically**
   - select **Edit > Add application to list automatically** command in the main menu
   - right-click in the **Application Protocol** pane and select **Add application to list automatically manually** from the drop-down list.
5. In the appeared window:
   - select existing list

   or
   - click **Create new** then enter a list name to the **List name** field and click **Save**.
6. Click **Select**.
7. Click **OK**.

3.4.3.8.4 Adding Application to List Manually

To add application to the list manually:

1. Go to **Applications** section.
2. On the Navigation pane select the needed filter in the **Application protocol** group.
3. On the **Application protocol** pane select one or several entries. To select several entries click at them while pressing **Shift** or **Ctrl** button

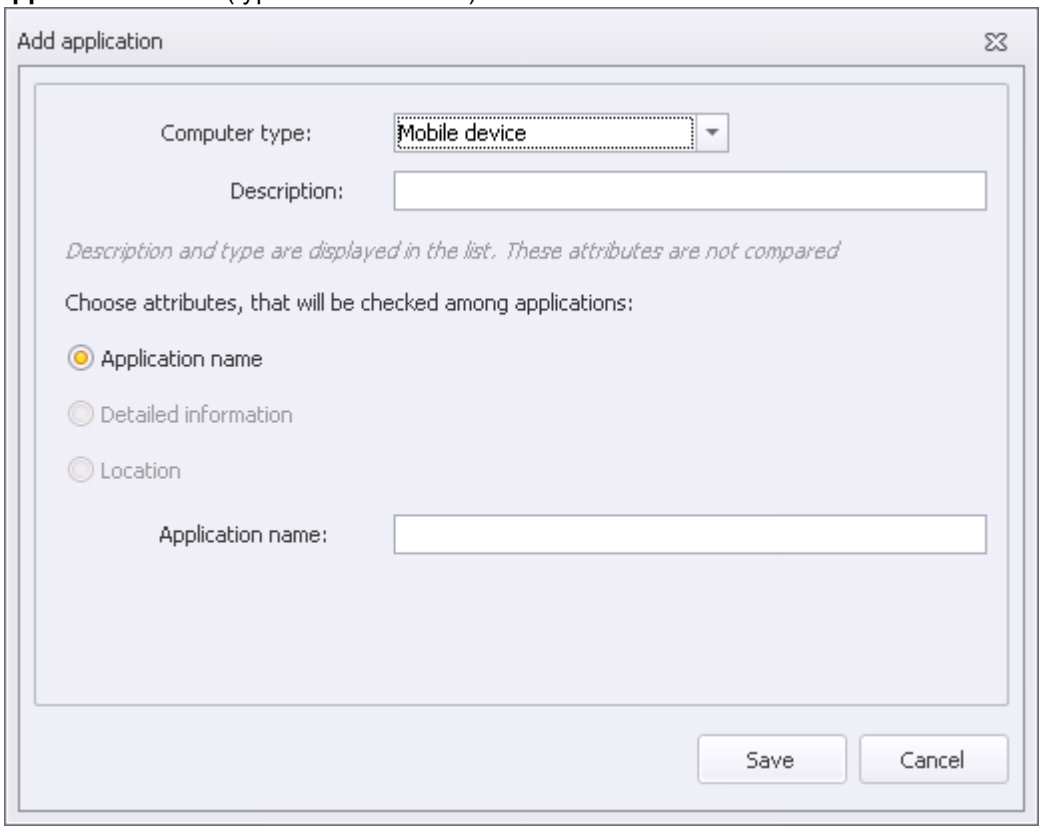
4. Take one of the following steps:
   - on the **Application protocol** pane click **Add application to list manually**
   - select **Edit > Add application to list manually** command in the main menu
   - right-click in the **Application Protocol** pane and select **Add application to list manually** from the drop-down list.

   This opens a dialog box with filter parameters.
5. In the **Add application** window you can set parameters of checking application correspondence:
   - **Application name**

     Enter the full name of the application file.
   - **Detailed information**

     Filtering application by detailed information of **Publisher**, **Product Name**, **Application Name**.
   - **Location**

     Filtering application by detailed information of **Location** (type in path to the file up to the folder), **Application name** (type in the file name).



6. Click **Save**.
7. If you have selected several entries, repeat steps 5 and 6 for other entries.
8. Click **OK**.

3.4.3.8.5 Exporting Application Protocol

To export the application protocol:

1. Go to **Applications** section.
2. On the Navigation pane, in the **List of applications** group, select the needed protocol.
3. In the **List of applications** group menu click **Export application protocol**.
4. Specify export location and click **Save**.

   The protocol will be exported in **.xls** format.

3.4.4 Temporary Employee Access to Network

An employee for which a rule denying connections outside corporate network is active (see "Settings of Corporate Network" and "Configuring Network Monitor Rule"), can request temporary access to external connections from InfoWatch Device Monitor Client menu, **Network control** command.

Warning!

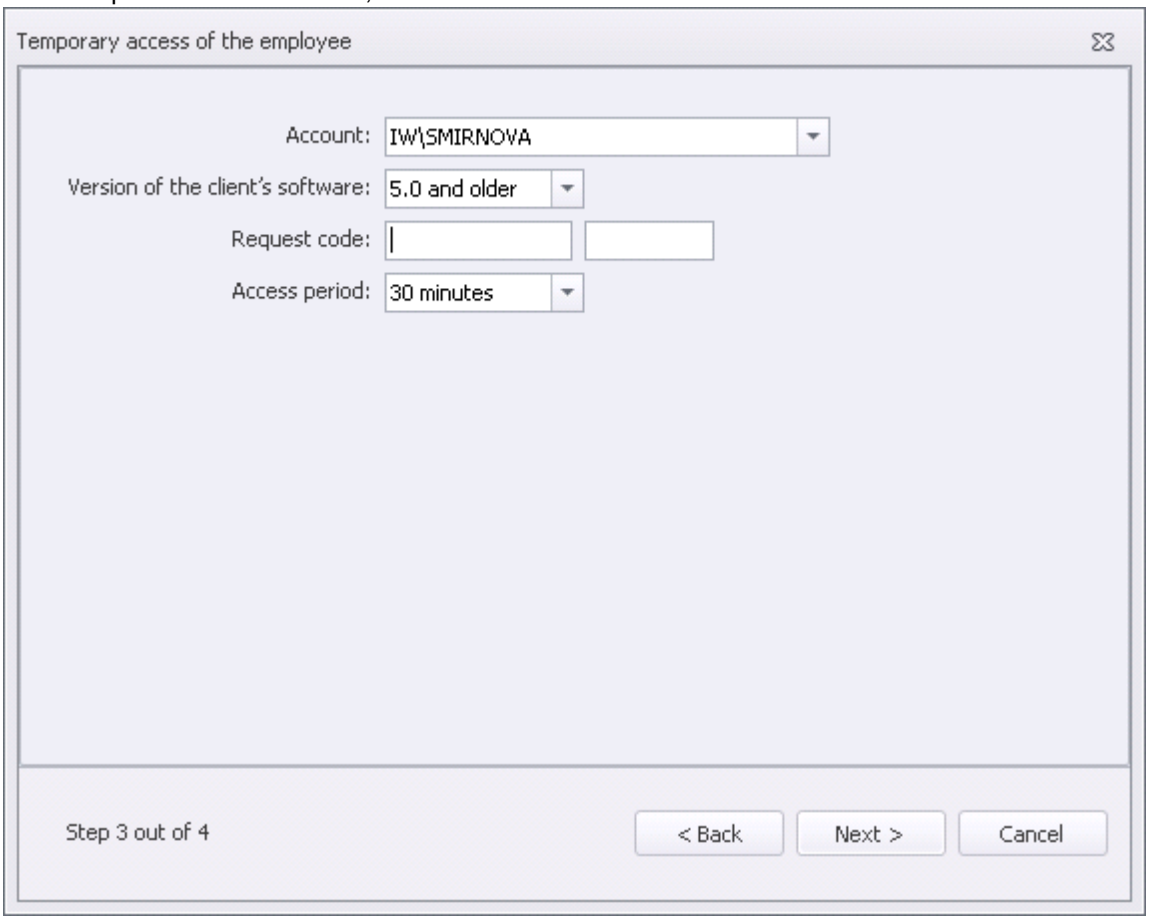
An employee can request an access only if the **Show tray icon interface** option is selected (see "Common Settings for Clients").

The way how to configure text displayed to an employee is described in "Employee Notifications about Policy Violations", "**Network connection forbidden. Detailed**" notification type.

An employee should send received request code to security officer.

To grant an access to external connections for employee:

1. In Main Menu select **Tools > Temporary employee access**.
2. In the dialog window choose **Dictated by phone**, click **Next**:
3. Choose option **To the network**, click **Next**.



4. From **Account** drop-down list select an account of employee to which a temporary access should be granted.
5. In **Version of client's software** choose version of Device Monitor Client installed on employee's computer.

   Note:
   When not sure about client's version, choose **4.1** or **4.2**.

6. To **Request code** field enter a code sent by employee.
7. From **Access period** drop-down list select time period for which a temporary access should be granted.

8. Click **Next**.

   The code which should be sent to employee is displayed in **Response code** field.

9. Click **Close**.

3.4.5 Temporary Employee Access to Devices

An employee for which a rule denying using devices is active (see "Configuring Device Monitor Rule"), can request temporary access to device from InfoWatch Device Monitor Client menu, **Device list** tab.

Warning!

An employee can request an access only if the **Show tray icon interface** option is selected (see "Common Settings for Clients").

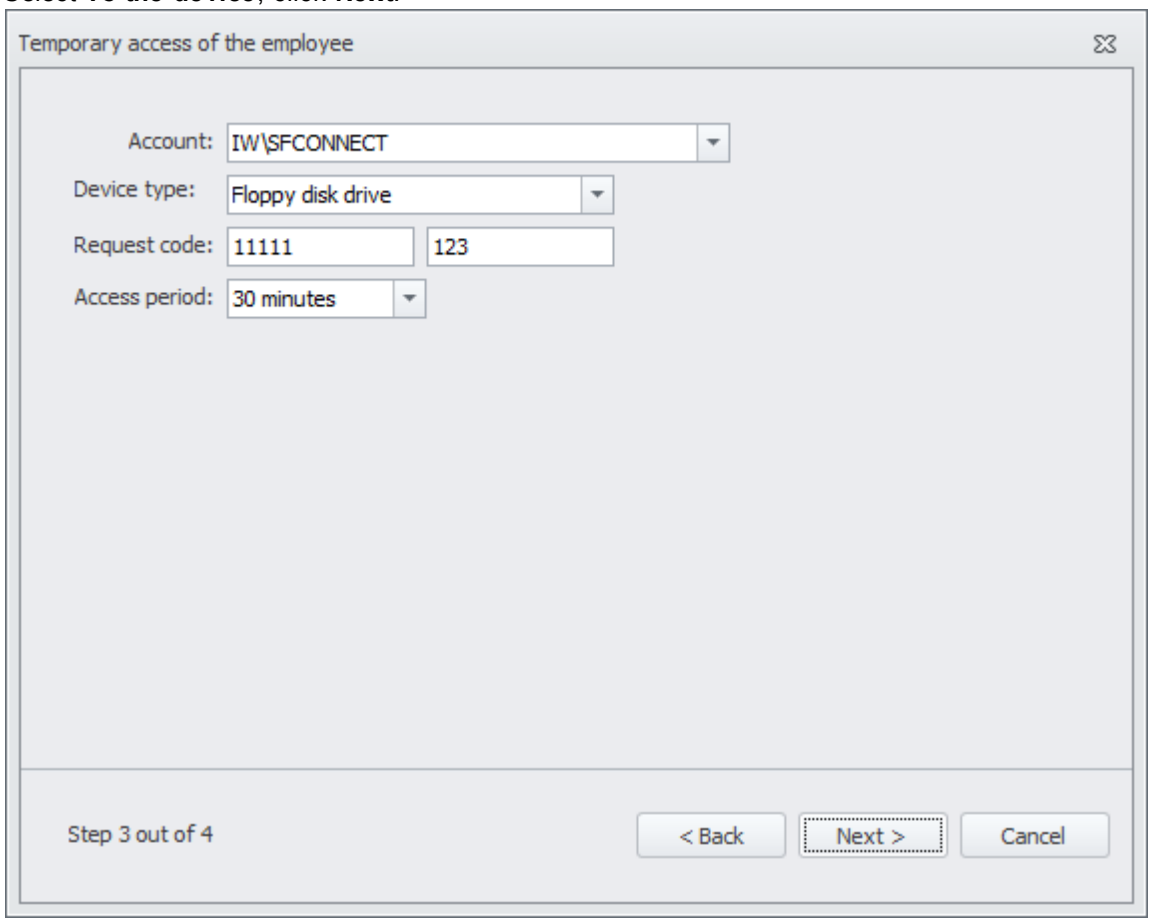
The way how to configure text displayed to an employee is described in "Employee Notifications about Policy Violations", "**Access to device denied**" notification type.

An employee should send received request code to security officer.

You can interact with employee using phone or e-mail.

To grant an access to devices for employee who called by phone:

1. In Main Menu select **Tools > Temporary employee access**.
2. Select **Dictated by phone (digital text code)**, click **Next**.
3. Select **To the device**, click **Next**.



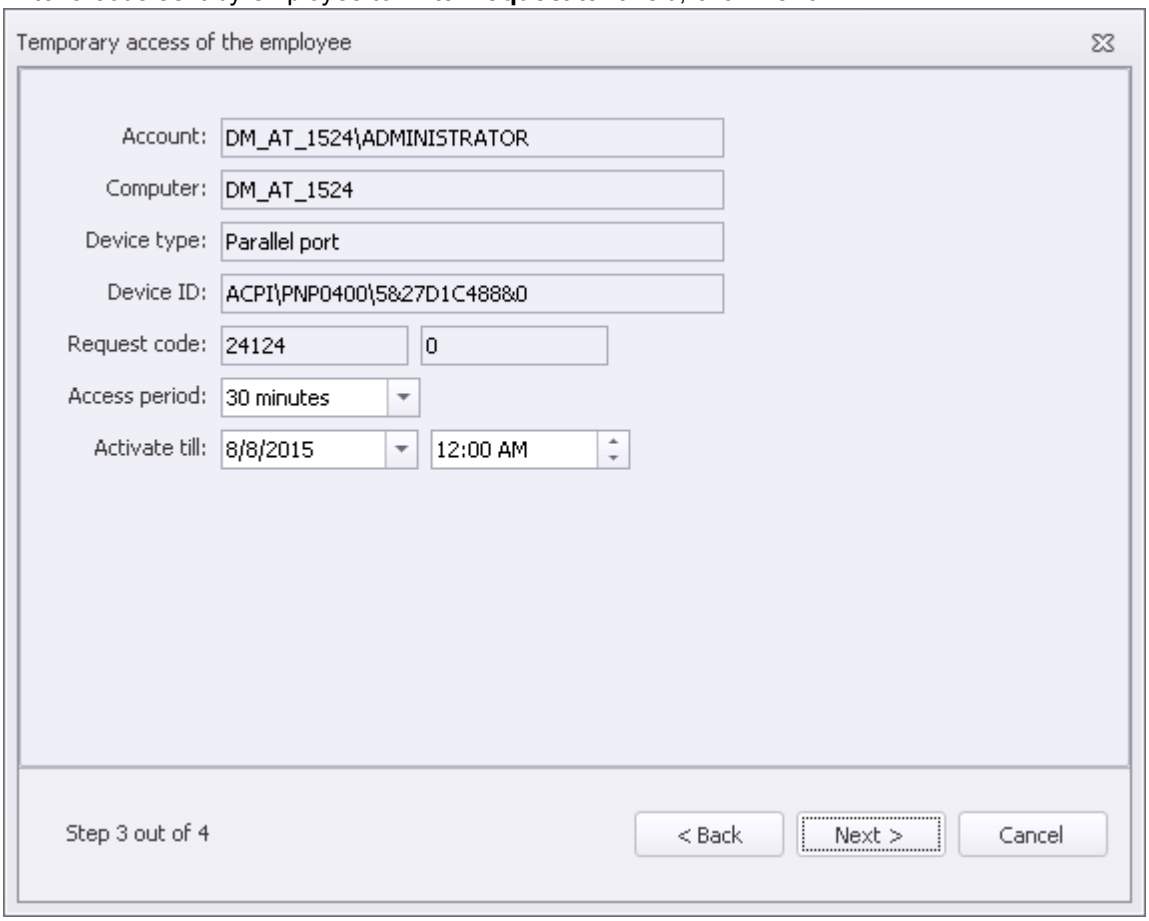
4. From **Account** drop-down list select an account of employee to which a temporary access should be granted.
5. From **Device type** drop-down list select the type of necessary device.

6. To **Request code** field enter a code sent by employee.
7. From **Access period** drop-down list select time period for which a temporary access should be granted.
8. Click **Next**.

   The code which should be sent to employee is displayed in **Confirmation code** field.
9. Click **Finish**.

To grant an access to devices for employee who sent e-mail:

1. In Main Menu select **Tools > Temporary employee access**.
2. Select **Obtained via e-mail or other means of communication (query text code)**, click **Next**.
3. Enter a code sent by employee to **Enter request text** field, click **Next**.



4. From **Access period** drop-down list select time period for which a temporary access should be granted.
5. In **Activate till** drop-down lists define, when employee will be able to activate access to the device (employee will have access to device for the time defined with **Access period** drop-down list).
6. Click **Next**.
   The code which should be sent to employee is displayed in **Copy answer text to clipboard** field.
7. Click **Finish**.

3.5 Viewing Events

InfoWatch Device Monitor Clients installed at managed computers provide keeping data on using external devices, transferring data via network connections and using instant messengers for data transfer. This information is stores as **events** and transferred to InfoWatch Device Monitor servers along with data of shadow copies. Events (unlike shadow copies) are registered in InfoWatch Device Monitor database and are available from Management Console.

You can define the information logging level (keep all information on access attempts, policy violations only or save nothing) in general settings of your security schema: for further details see "Common Settings for Clients".

You can view events in **Events** section. To go to this section, click **Events** button on Navigation pane.

To view events,

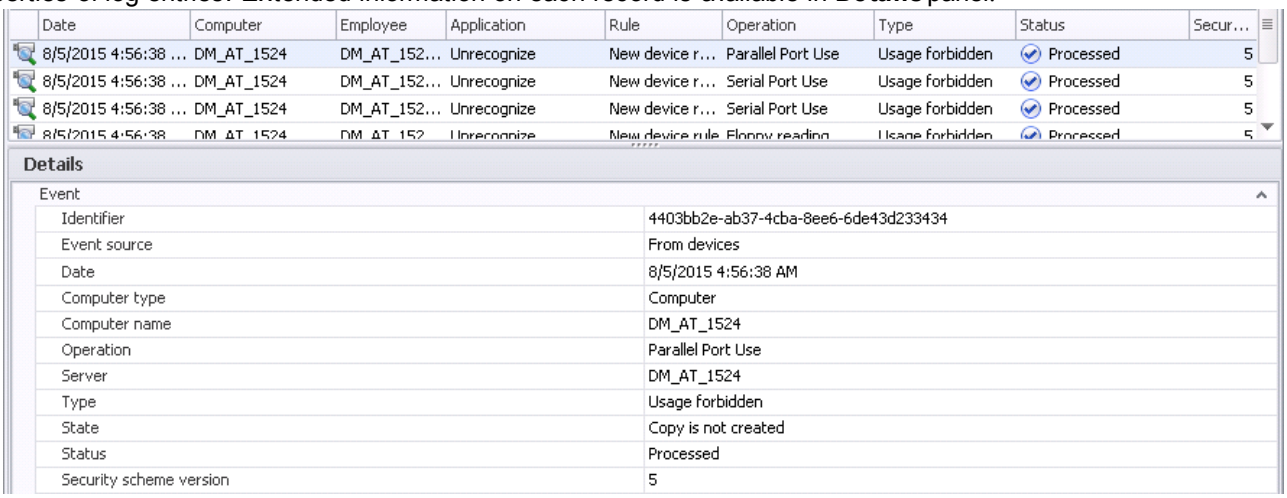
click the filter name in the filter list.

There are two predefined filters:

- **Last: 4 hours**
- **Today**

You can create custom filters to view events, as described in "Event Filters".

Event information is displayed in a tabular list where each row contains a single record. Columns contain basic properties of log entries. Extended information on each record is available in **Details** panel.



Attribute name	Description	Available values
Common attributes		
Identifier	Unique event number	
Event source	Interceptor-based event type	- **File** – File Monitor; - **Devices** – Device Monitor; - **Printer** – Print Monitor; - **Skype, XMPP, MMP, Yahoo, WhatsApp, SMS** – IM Client Monitor; - **FTP/FTPS** – FTP Monitor; - **HTTP/HTTPS** – HTTP(S) Monitor; - **Mail** - Mail Monitor; - **Network** – Network Monitor; - **Mobile device camera** - Photo Monitor; - **System** - event on ending disc space for shadow copy saving. *Such event is not transferred to Traffic Monitor.*
Date	Event date and time (in hours and minutes) registered on computer. Device Monitor server keeps an event in UTC, and Management Console displays it according to the local time of	

	a computer where Console installed	
Computer type	Indicates if the computer where the event arisen is the workstation or mobile device	– Workstation – Mobile device
Computer name	Name of the computer that registered the event	
Operation	Employee initiated action or attempt	
Server	Name of InfoWatch Device Monitor server the Client transmits event information to	
Application	Executable file name and/or name of the process responsible for the action, if detected	
Type	Action-based event type	– **Record** - adding or changing data (including renaming) on external device; sending files via messenger; sending print jobs to printer; sending data via FTP/ FTPS – **Use** - connecting an external device that allows unmonitored read/write operations or sending messages – **Violation** - IM Client interceptor user-initiated violation – **Warning** - user-initiated a ban or didn't give consent to use IM Client plug-in, while monitoring is required by security policy – **Usage forbidden** – attempt of sending data via forbidden channel
Status	Status of event processing on the server and sending to Traffic Monitor server	– **New** – **Awaiting for proceeding** – **Awaiting for sending to TM** – **Sent to TM** **Note:** If the Server is in standalone mode then the event has the **Processed** status only
Security schema version	Number of security schema version that was active on the computer when the event was registered	
Operation verdict	Attribute of allowed action. For *Devices* events (**Device Monitor** rule) the blocking is also available.	– **Allowed** – **Forbidden** – only for *Devices* events – **Unprotected data copying is disabled** – only for *Devices* events – **Allowed (in white list)** - for whitelisted device events
Employee	Name of the domain (computer name outside the domain) and user login used for event registration or operating system reference for events outside user sessions	

Rule	Name of policy rule managing the event	
Terminal client	Terminal client name, if detected	
Network address of a terminal client	Terminal client IP, if detected	
For events with *File* source		
Assign	Full target file name	
File size	Target file size	
Object status	Shadow copy of transferred data	- **no copies created** - rule does not require shadow copying - **copy created** - shadow copy created successfully - **copying error** - for example, if there is no free space on the client
Device description	Target device instance or model ID	
For events with *Devices* source		
Device type	For supported device types list see "InfoWatch Device Monitor Functions"	
Device instance or model identifier	Model identifier (VID) and serial number (PID) of external device or printer used for the operation	
Device description	Device description received from OS of the computer where the Client is installed	
For events with *Skype, XMPP, MMP, Yahoo, WhatsApp, SMS* source		
IM user ID	UIN of the user authorized in the messenger at computer	
Object status	Shadow copy of transferred data	- **no copies created** - rule does not require shadow copying - **copy created** - shadow copy created successfully - **copying error** - for example, if there is no free space on the client
List of senders	UIN of IM users, who sent the message/file via messenger	
List of recipients	UIN of IM users, who received the message/file via messenger	
File name	Full name of transferred file	
File size	Transferred file size	
Shadow copy	File, message or chat shadow copy	- **No** - no shadow copy was created - **Yes** - shadow copy created successfully
For events with *Printer* source		
Document	Full name of the file sent to print	
Printer	Name of target network printer	
Object status	Result of creating shadow copy of the print job	- Shadow copy of print job was successfully created. The job contained graphic and text data. - Shadow copy of print job was not created. The job contained no

		graphic or text data. - An error occurred while creating a shadow copy of print job. - Shadow copy of print job was successfully created. The job contained only graphic data. - The shadow cope should not have been created. - Shadow copy of print job was partially created. Graphic data were fully processed. Text data were partially processed - Shadow copy of print job was partially created. Graphic data were partially processed. Text data were fully processed. - Shadow copy of print job was successfully created. The job contained only text data. - Shadow copy of print job was partially created. Graphic data were partially processed. The job contained no text data. - Shadow copy of print job was partially created. The job contained no graphic data. Text data were partially processed.
For events with *FTP/FTPS* source		
Object status	Result of creating shadow copy of transferred data	- **no copies created** - rule does not require shadow copying - **copy created** - shadow copy created successfully - **copying error** - for example, if there is no free space on the client
Sender	Name used for employee authorization at FTP server	
FTP server	Name or IP address of FTP server	**Note:** When using the FTP via proxy server this field can contain proxy address instead of FTP.
Relative path	Directory at FTP server where to the file is transferred	
File name	Full name of transferred file	
Real file size	File size calculated after transfer	
Declared file size	File size according to data of application which performs a transfer to FTP server (browser for example)	
Starting point	When file is transferred by piecemeals, position which starts the of the current part transfer.	
Shadow copy	Result of creating file shadow copy	- **No** – shadow copy was not created

		- **Yes** – shadow copy created successfully
For events with *HTTP* or *HTTPS* source		
State	Result of creating shadow copy	- **no copies created** - rule does not require shadow copying - **copy created** - shadow copy created successfully - **no free space on disk** – client does not have enough free space - **copying error** - for example, if there is no free space on the client
Reciever DNS	DNS name of a computer	
Reciever IP	IP-address of a computer	
Request size	Size of a request in Kbps	
Rule	Name of policy rule managing the event	
For events with *Mail* source		
State	Result of creating shadow copy	- **no copies created** - rule does not require shadow copying - **copy created** - shadow copy created successfully - **no free space on disk** – client does not have enough free space - **copying error** - for example, if there is no free space on the client
Sender	DNS name of a sender computer	
List of recipients	Receiver addresses	**Note:** For events with large number of senders you should remember that when Device Monitor Management Console can't display more than 1024 symbols in this field. However if the shadow copy is set for this event then Traffic Monitor will receive and display the full list of recipients (under 4000 Bytes).
Subject	Mail Subject	
Transmission type	Used protocol	
Message type	Mail direction	- **Incoming** - **Outgoing**
Size, bite	Size in bites	
Channel type	Encrypted or not encrypted	- **All channels** - **Encrypted channel**
Rule	Name of policy rule managing the event	
For events with *Network* source		
Time of ban removal starts	For *Network operations temporary ban removal* operation - start of temporary access period. See details in "Temporary Employee Access".	
Time of ban removal ends	For *Network operations temporary ban removal* operation - end of temporary access period. See	

	details in "Temporary Employee Access".	
Connection server	For *Connection forbidden* operation - address or name of forbidden server which was attempted to gain access to	
Port	For *Connection forbidden* operation - port number used for connection attempt.	
For events with *Mobile device camera* source		
Photo size	Size of photo shadow copy, in bytes	

If needed, you can free some space in the database by deleting all the information about already processed events (**Processed** or **Sent to Traffic Monitor** state). See details in "Deleting Events".

3.5.1 Event Filters

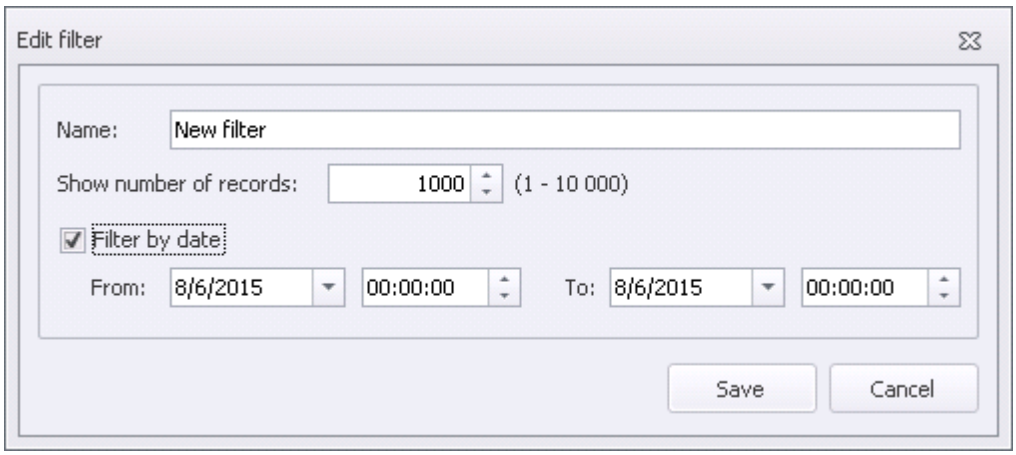
In addition to predefined filters you can create custom filters to view event information.

To add or edit a filter:

1. Go to **Events**.
2. Follow the necessary steps:

Action	Steps
Creating filter	• in Main Menu select **Edit > Add Filter**; • click **Add Filter** at the top of Navigation pane.
Editing filter	1. In **Events** area of Navigation pane, select the name of the filter you want to edit. 2. Take one of the following steps: • in Main Menu click **Edit > Edit Filter**; • click **Edit Filter** at the top of Navigation pane. • double-click selected filter name

These actions open **Edit filter** dialog.



3. Specify filter options in **Edit Filter** dialog:
   - **Filter Name**.
   - **Show number of records**. Limit on the number of entries displayed in Management Console workspace (1000 records by default).
   - To filter by a date, flag **Filter by date** box and specify the desired period in **From** and **To** fields. Set the date and time in right and left field respectively.

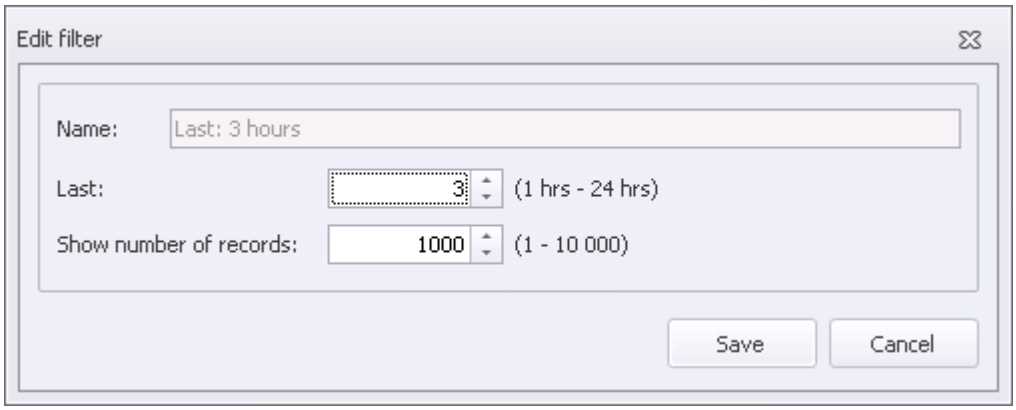
Note:
For the predefined filters **Filter Name** and **Filter by date** parameters cannot be edited.

4. Click **Save**.

The predefined filter **Last: 4 hours** has another editing interface and lets to make filters displaying events for last several hours.

To edit predefined filter to view events for the selected number of hours:

1. In **Events** area of Navigation pane, select the **Last: 4 hours** filter.
2. Take one of the following steps:
   - in Main Menu click **Edit > Edit Filter**;
   - click **Edit Filter** at the top of Navigation pane;
   - double-click the filter name.



3. Specify filter options in **Edit Filter** dialog:
   - **Last**. Specify the number of hours, entries for which should be displayed in the Management Console workspace.
   - **Show number of records**. Limit on the number of entries displayed (1000 records by default).
4. Click **Save**.

3.5.2 Deleting Events

The information about already processed events (**Processed** or **Sent to Traffic Monitor** state) can be deleted.

You can delete events:

- for certain time period;
- all matching certain filter.

To delete from the database an information about events for a period:

1. Go to **Events**.
2. Take one of the following steps:
   - click **Delete events** at the top of Navigation pane
   - in Main Menu click **Edit > Delete events**.

   This opens **Deleting from database** dialog
3. Specify needed time period for which you want to delete events.
4. Click **Delete**.

Then a number of deleted events will be displayed.

To delete from the database an information about events matching certain filter:

1. Go to **Events**.
2. In the filter list select needed filter name.
3. Take one of the following steps:
   - click  **Delete filter events** at the top of **Events** area.
   - in Main Menu click **Edit > Delete filter events**.
4. In request box select **Yes** to confirm.

Then a number of deleted events will be displayed.

3.6 Clients Remote Installation, Updating and Uninstallation

You can install, update, or delete InfoWatch Device Monitor Clients from a computer via InfoWatch Device Monitor Management Console. These operations are performed through **tasks**. You can run tasks to install, update or remove client software, change uninstallation password, or monitor these processes.

Remote client management is carried out by special **Distribution Agent** transmitted onto client workstations. The Agent requires the following:

- Target computers must meet hardware and software requirements: see "InfoWatch Device Monitor Client Hardware and Software Requirements".
- Proactive virus protection for computers must be turned off at the time of installation.
- Device Monitor server and target computers should resolve each other by domain names.
- On computers, where firewall, different from windows standard one, is installed, it should be disabled. Except for disabling, you can also allow any network connections for the following Device Monitor components: `IWDeployAgent.exe, iwdmc.exe, DM.Client.exe, IWProxy.exe, rmtlogctr.exe.`

> **Note:**
> To install Client on Windows 7 computer, go to **Control Panel** -> **Network and sharing center** -> **Change advanced sharing** settings. Enable file and printer sharing. Upon completion, **Distribution Agent** can be copied to computer. Firewall will be automatically configured.

To go to Management Console task section, use **Tasks** button on Navigation pane.

Tasks management guidelines are available in:

- View Tasks
- Preparing Primary Client Installation
- Creating Primary Distribution Task
- Creating Update Task
- Creating Uninstallation Password Reset Task
- Creating Uninstallation Task
- Launching, Pausing, Editing, and Deleting Tasks
- Client Installation Errors

You can also install and upgrade your Client with software distribution tools (for example, via Microsoft Active Directory group policies). To run these operations, use installation package that was created as described in "Creating Installation Package".

3.6.1 View Tasks

Tasks area of Navigation pane displays a list of all created, executed and outstanding tasks. Main screen work pane displays a list of target computers for the selected task.

Details panel displays the following parameters for selected task:

Parameter	Description
Name	Original name of the task
Description	Original description of the task
Type	One of the following task types: • Primary distribution • Change password • Update • Uninstall
Status	Current task status. Possible values: • Executing • Stopped • Completed
Restart period, min	Intervals between task launches on computer, if the previous attempt failed, in minutes. Counted from ending the last workstation proceeding in previous task launch. If the task fails, it won't be launched again.
Number of restart trials	Maximum number of retries to restart distribution task on computer . After all attempts have been used, **Task status** parameter value will be set to **Error** (for further details, see "Client Installation Errors").
For primary distribution tasks	
Show employee notifications	Indicates that employee's attempt to perform a banned action will trigger a warning. For further details, see "General System Settings", "Creating Installation Package" and "Employee Notifications about Policy Violations"
Hide Agent presence	Indicates if Windows system tray of managed computer hides Client presence presence on the computer. Otherwise Windows system tray of the computer where Client installed will display  icon. By clicking at this icon, an information on DM Client operation and list of currently controlled devices is displayed. **Warning!** If there is an antivirus protection enabled on the managed computer then the antivirus program can reveal the operation of Device Monitor: for example, in the list of processes running on the managed computer or in the list of programs that initiate a control.
Install the component of network traffic interception	Indicates if iw_proxy component is installed.
Install the component of network connections control	Indicates if Network Monitor interceptor is installed.
Uninstallation product password	Shows if the password requested from employee that attempts to remove Device Monitor Client.
Proxy Root Issuer DN	The unique name of Device Monitor proxy server certificate, issuer distinguished name.
For primary distribution and update tasks	
Installation directory	Installation directory for Device Monitor Client at target computers.

Installation login	Name of the Console user that launches the task on computers.
Waiting fir restart duration, hours	Computer reboot waiting period (in hours); if the computer is not restarted manually during this period, the System will notify the employee (if notifications are enabled), and force operating system restart.
Duration of restart notifications, hours	Period of displaying requests for rebooting computer, in hours.
Restart notifications rate, min	Time intervals between repeated reboot requests, in minutes.
Reboot messages	Text displayed to the employee in reboot request.
Show a warning before forced reboot	Indicates if a notification about forced reboot will be displayed when reboot wait durations are expired but employee did not reboot the computer.
For change password tasks	
Uninstallation product password	Shows if the password requested from user that attempts to remove Device Monitor Client.

Each target computer's main screen workspace displays the following parameters:

Parameter	Description
Address	Computer IP address or domain name
Status	Current status of task for the relevant computer. Possible values: • **Not running** • **Prepare to start** • **In progress** • **Waiting for reboot** (only for installation and upgrade tasks) • **Error** (for further details, see "Client Installation Errors") • **No access** • **Completed**
Client version	Client version currently installed on computer
Operation system	Computer operating system.
System type	Type of operating system on the computer: x64 or x32.
Connections count	Number of connection attempts to unavailable computer.
Time	Date and time of the last connection to computer.

3.6.2 Preparing Primary Client Installation. Distribution Agent

Remote client installation is carried out by InfoWatch Device Monitor special **Distribution Agent**.

Correct remote client installation via InfoWatch Device Monitor requires the following:

- Target computers must meet hardware and software requirements: see "InfoWatch Device Monitor Client Hardware and Software Requirements".
- Proactive virus protection for computers must be turned off.
- Computers with the firewall that differ from Windows firewall, that firewall:
  - should be disabled

    or

- should have a permission for InfoWatch Device Monitor Distribution Agent

  or

- should have **15505** port (default port by which the Distribution Agent awaits for a connection) opened for incoming connections, if it was not changed in connection settings (see "<applicationSettings> section", **CommunicationPort** parameter).

Additional requirements vary depending on distribution method:

Method 1:

Distribute `Setup.DeployAgent.msi` installation package (provided along with installation software) to target computers.

Method 2:

Transmit Distribution agent through shared administrative resources:

- Computer firewalls must be either turned off, or set required exceptions: see "Firewall Settings".
- Specify settings for network access to shared resources: see "Enabling Shared Administrative Resources ".

If all requirements are met, you can start creating and then start primary distribution tasks.

3.6.2.1 Enabling Shared Administrative Resources

To transfer InfoWatch Device Monitor distribution agent to target computers through shared administrative resources, the following requirements must be met:

- If computer with Windows XP is outside a domain, in security policy settings of this computer set **Network access configuration parameter: Sharing and security model for local accounts** value to `Classic`.
- Computers must have their shared administrative resources (like `\\computername\admin$`) enabled (in Windows Vista and Windows 7 they are disabled by default). To enable them:
  1. Make sure that sharing of files and printers is enabled. In Control Panel, open **Network and sharing Center -> Change advanced sharing settings**. In desired profile enable file sharing and printer sharing.
  2. In the registry, in `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System` path, add **DWORD (32-bit)** parameter named **LocalAccountTokenFilterPolicy**. Set its value to **1**.

3.6.2.2 Firewall Settings

Firewall settings requirements:

Application protocol	Transport protocol	Port
RPC	TCP	135
RPC over HTTPS	TCP	593
NetBIOS Datagram Service	UDP	138
NetBIOS Name Resolution	UDP	137
NetBIOS Session Service	TCP	139
SMB	TCP	445

For computer availability defining quickness the ICMP protocol should be permitted.

For Windows firewall the "**File printing and sharing**" preset rule should be permitted.

3.6.3 Creating Primary Distribution Task

Primary distribution (installation from Management Console) of InfoWatch Device Monitor Client using **installation agents**. Installation agent is an executable file. It is passed on to computers and starts automatically during task execution, receiving Client updates from server.

Warning!
If server account doesn't have administrator rights on all target computers, primary Device Monitor Client distribution will require credentials of an account having administrator rights at:

- all target computers
- computer where Management Console is running
- computer where Device Monitor server is running

If a password of used account is expiring (Windows warns that the password expires in 3 days and need to be changed) then primary distribution task cannot run on behalf of this user.

If you are unable to enter administrator name and password, you can create your own InfoWatch Device Monitor Client installation package ("Creating Installation Package") and install it by other means ("Standard InfoWatch Device Monitor Client Setup" and "Client Setup via Software Distribution Tools").

Warning!
If the workstation has Kaspersky Internet Security installed then you need to disable its self-protection to install the InfoWatch Device Monitor Client. See "How to enable/disable self-defense in Kaspersky Internet Security" internet article.

To create a primary InfoWatch Device Monitor client application distribution task:

1. Go to **Tasks**.
2. Take one of the following steps:
   - in the Main Menu select **Edit > Add Task**;
   - click **Add Task** at the top of Navigation pane.

   These actions open **Deployment task wizard** dialog.
3. Enter task name, select **Initial deployment task** and type task description, then click **Next**.
4. Create a list of computers which you need to install Device Monitor Client to. To add computer (or several computers):
   a. Click **Add**. **Select computer** dialog will display a list of computers from:
      - directory service (Active Directory for example)
      - Microsoft Windows Network
      - ones registered before (for example, after manual Client installation) and belonging to computer groups (**DM server computers** node).

   b. Flag computers or computer groups. Minimized groups are marked with an icon ▸; expanded - ▾. Double-click a group, to expand or collapse it.

      Warning!
      By marking a group you select the computers that are included in that particular group. Subgroups and subgroup computers of selected group are not selected: you have to select them separately.

      You can also specify computer name or IP addresses:
      - in the line at the bottom of dialog box. When listing addresses, separate them with semicolons.
      - click **Import** and download text file where one entry should be placed in the each line; text should contain no blank lines.

   c. After you specify the computers you want to add, click **Select**. The dialog will be closed and selected

computers list will be displayed in **Task target computers list** area.

To remove a computer from the list, select it and click **Remove**.

When you make a full list of computers click **Next**.

5. Then InfoWatch Device Monitor servers currently registered in the System are displayed.
   You can change Client installation directory (`%Program Files%\Infowatch\DeviceMonitor\Client` is used by default) .
   Click **Next**.
6. The unique name of Device Monitor proxy server certificate (Issuer Distinguished name, Proxy Root Issuer DN) will be displayed. You can change it with accordance to X.509 standard, CN (Common Name) field is mandatory, all fields comma-separated. Click **Next**.
7. Specify options of computer reboot:
   - **Wait for reboot without notifying the employee**. The Agent can:
     - start notifications immediately (*Do not wait* option),
     - start notifications in specified time (*Wait for* option - please specify time period to start notifications),
     - do not notify at all (*Wait infinitely* option).
   - **Notify the employee about reboot necessity and wait for reboot**. Upon completing reboot waiting in "silent" mode (see **Wait for reboot without notifying the employee** setting) or immediately after installation ends, Device Monitor Client starts to notify employee on reboot necessity:
     - during specified time period (*Notify within* option)
     - permanently (*Notify infinitely* option)
     - do not notify at all (*Do not notify* option).

     If needed, change continuance and frequency of notifications appearance and enter text of the message displaying in reboot notification.
   - **Show a warning before forced reboot**. If this check box is flagged, then the Client displays a notification about forced reboot and allows 5 minutes to end operations. Then the computer will be forced to reboot. If the option is not checked then the forced reboot (if it should be made according your settings) will be performed unexpectedly for the employee.

     Warning!
     Forced reboot is performed in case when neither **Wait while employee reboots computer** setting no **Show a warning before force reboot** setting do not flagged, or their wait durations are expired but employee did not reboot the computer.

   Click **Next**.
8. Configure Client settings:
   - To protect Client application from deleting by employee, enter the password that will be requested when trying to uninstall the Client and confirm it.
   - **Show employee notifications** - if employee attempts to perform an action restricted by security policy, a warning will be displayed. For further details, see "Employee Notifications about Policy Violations".
   - **Hide Agent presence** - indicates if Windows system tray of managed computer hides Client presence presence on the computer.

     Warning!
     Not notifying the user about interceptor operation may contradict the applicable laws of your country.

     Warning!
     If there is an antivirus protection enabled on the managed computer then the antivirus program can reveal the operation of Device Monitor: for example, in the list of processes running on the managed computer or in the list of programs that initiate a control.

     If this option is not selected, the Windows system tray of the computer where the Client is installed will display  icon. By clicking at this icon, an information on DM Client operation and list of currently controlled devices is displayed.

- **Install the component of network traffic interception -** installs **iw_proxy** component on a computer. Component will not be installed if you leave the checkbox empty.
- **Install the component of network connections control -** installs **Network Monitor** interceptor on a computer. Component will not be installed if you leave the checkbox empty.

  Warning!
  You should not install the component of network control to the server with Citrix Provisioning Services: this can lead to the serious problems concerning server operation.

- Task run parameters: they will be used in case the task wasn't launched at first attempt. Specify the number of attempts and their intervals, in minutes.
- To launch a task immediately after saving, flag **Run task immediately** check box.
- Enter the credentials for the account that launches the task.This account must have administrator rights on all target computers.

  Warning!
  The System does not save passwords for accounts used to launch tasks.
  If the new task is not launched immediately, you will have to use password next time to launch it from Management Console.
  If a password of used account is expiring (Windows warns that the password expires in 3 days and need to be changed) then primary distribution task cannot run on behalf of this user.

Click **Next**.

9. Look through the task summary. If you need to change any settings click **Back** to return. If all settings are correct, click **Finish**.

3.6.4 Creating Update Task

InfoWatch Device Monitor client applications update is required after InfoWatch Device Monitor server upgrade: for further details, see "Updating InfoWatch Device Monitor Server End".

Note:
Beside the following method, you can create update task with a simplified function as described in "Updating Clients at Managed Computers".

To create and schedule InfoWatch Device Monitor client applications update task:

1. Go to **Tasks**.
2. Take one of the following steps:
   - in the Main Menu select **Edit > Add Task**;
   - click **Add Task** at the top of Navigation pane.

   These actions open **Deployment task wizard** dialog.
3. Select **Update task**, enter task name and description and click **Next**.
4. Create a list of computers that require Device Monitor Client update. To add computer (or several computers):
   a. Click **Add**. The **Select computers** dialog, **DM server computers** node, contains the list of computers where Device Monitor Client version does not match Device Monitor Server version but can be automatically updated (client software version should be 4.0.651 and higher).
   b. Flag computers or computer groups. Minimized groups are marked with an icon; expanded - . Double-click a group, to expand or collapse it.

      Warning!
      By marking a group you select the computers that are included in that particular group. Subgroups and subgroup computers of selected group are not selected: you have to select them separately.

   c. Use **Filter by computer name** field to specify computer. Click **Find**.
   d. After you specify the computers you want to add, click **OK**. **Select computers** dialog will be closed.

Selected computers list will be displayed in **Task target computers list** area.

To remove a computer from the list, select it and click **Remove**.

When you make a full list of computer click **Next**.

5. Please specify reboot settings:
   - **Wait for reboot without notifying**. The Agent can:
     - Start to notify immediately (*Do not wait* parameter)
     - Start to notify after mentioned time period (Wait for hour(s) parameter - you need to specify time before notification)
     - Do not notify before forced reboot (*Wait infinitely* parameter).
   - **Notify the employee about reboot necessity and wait for reboot**. After "silent mode" wait to notify (see **Wait for reboot without notifying** setting), or right after update process completion, Device Monitor client will start to notify the employee about reboot necessity during specified time period (*Notify within hour(s) within: minutes* parameter) or infinitely (*Notify infinitely every x minutes*), or do not notify (*Do not notify*). When necessary, change length and frequency and specify text of the message, which will be displayed along with notification.
   - **Show a warning before reboot** - is a parameter to specify whether forced reboot notification will be displayed (an employee can complete current tasks within 5 minutes before forced reboot) or forced reboot will be performed without any additional text.
6. Specify:
   - Task retry parameters: they will be used in case the task wasn't launched at first attempt; if launching failed, the task won't be launched again. Specify the number of attempts and their intervals, in minutes.
   - To launch a task immediately after saving, flag **Run task immediately** check box.

   Click **Next**.
7. Look through the task summary. If you need to change any settings click **Back** to return. If all settings are correct, click **Finish**.

> **Warning!**
> If the workstation has the Kaspersky Internet Security installed then you need to disable its self-protecting function for successful InfoWatch Device Monitor Client update.
> See details in "How to enable/disable self-defense in Kaspersky Internet Security".

3.6.5 Creating Uninstallation Password Reset Task

To create uninstallation password change task, InfoWatch Device Monitor client application:

1. Go to **Tasks**.
2. Take one of the following steps:
   - in the Main Menu select **Edit > Add Task**;
   - click **Add Task** at the top of Navigation pane.

   These actions open **Deployment task wizard** dialog.
3. Select **Change uninstall password task**, enter task name and description and click **Next**.
4. Create a list of computers that need their uninstallation passwords to be changed on **Deployment target computers** screen. To add computer (or several computers):
   a. Click **Add**. The **Select computers** dialog, **DM server computers** node, contains the list of computers where Device Monitor Client is installed.
   b. Flag computers or computer groups. Minimized groups are marked with an icon; expanded - . Double-click a group, to expand or collapse it. Use **Filter by computer name** field to specify the computer. Click **Find**.

> **Warning!**
> By marking a group you select the computers that are included in that particular group. Subgroups and subgroup computers of selected group are not selected: you have to select them separately.

c. After you specify the computers you want to add to task, click **OK**. **Select computers** dialog will be closed. Selected computers list will be displayed in **Task target computers list** area.

To remove a computer from the list, select it and click **Remove**.

When you make a full list of computers click **Next**.

5. Specify:
   - The password that will be requested when trying to uninstall the Client. Confirm it.
   - Task retry parameters: they will be used in case the task wasn't launched at first attempt; if launching failed, the task won't be launched again. Specify the number of attempts and their intervals, in minutes.
   - To launch a task immediately after saving, flag **Run task immediately** check box.

   Click **Next**.
6. Look through the task summary. If you need to change any settings click **Back** to return. If all settings are correct, click **Finish**.

3.6.6 Creating Uninstallation Task

To create a centralized task that removes InfoWatch Device Monitor client applications:

1. Go to **Tasks**.
2. Take one of the following steps:
   - in the Main Menu select **Edit > Add Task**;
   - click **Add Task** at the top of Navigation pane.

   These actions open **Deployment task wizard** dialog.
3. Select **Uninstall task**, enter task name and description and click **Next**.
4. Create a list of computers you are removing Device Monitor Client from in **Deployment target computers** screen. To add computer (or several computers):
   a. Click **Add**. The **Select computers** dialog, **DM server computers** node, contains the list of computers where Device Monitor Client is installed. Use **Filter by computer name** field to specify computer. Click **Find**.
   b. Flag computers or computer groups. Minimized groups are marked with an icon; expanded - . Double-click a group, to expand or collapse it.

   > **Warning!**
   > By marking a group you select the computers that are included in that particular group. Subgroups and subgroup computers of selected group are not selected: you have to select them separately.

   c. After you specify the computers you want to add, click **Select**. Selected computers list will be displayed in **Task target computers list** area.

   To remove a computer from the list, select it and click **Remove**.

   When you make a full list of computers click **Next**.
5. Specify:
   - Task retry parameters: they will be used in case the task wasn't launched at first attempt. Specify the number of attempts and their intervals, in minutes.
   - To launch a task immediately after saving, flag **Run task immediately** check box.

   Click **Next**.
6. Look through the task summary. If you need to change any settings click **Back** to return. If all settings are correct, click **Finish**.

   > **Warning!**
   > If the workstation has the Kaspersky Internet Security installed then you need to disable its self-protecting function for successful InfoWatch Device Monitor Client uninstallation.
   > See details in "How to enable/disable self-defense in Kaspersky Internet Security".

3.6.7 Launching, Pausing, Editing, and Deleting Tasks

If you flagged **Launch task immediately** when creating a task, it will start immediately. Otherwise, you will need to manually launch the task. You might need this option, if for some reason you had to stop the task and want to start it again.

For instructions see the following table.

To perform any of these procedures, you must first select a task from the list on **Tasks** panel.

Action	Steps
Start task	• in the Main Menu select **Edit > Perform task**; • click **Perform task** located at the top of Navigation pane.
Stop task	• in the Main Menu select **Edit >Stop task**; • click **Stop task** at the top of Navigation pane.
Edit list of computers in task	• at the top of **Task execution result** panel click **Add computer** or **Exclude computer from task** • right-click computer row and select **Add computer** or **Exclude computer from task**. **Warning!** You can't remove a computer if the task is running and not completed.
Edit task	• in the Main Menu select **Edit > Edit**; • click **Edit** at the top of Navigation pane. • right-click on task name and select **Edit**. Specify new settings for the task like it is done for a new task (see "Creating Primary Distribution Task", "Creating Updating Task", "Creating Uninstallation Password Reset Task", "Creating Uninstallation Task")
Delete task	• in the Main Menu select **Edit > Delete**; • click **Delete** at the top of Navigation Pane. • right-click on task name and select **Delete**. **Warning!** You can't remove a task with computer that has a running task.
View computer error log	• at the top of **Task execution result** panel click **Computer log** • right click computer row and select **Computer log**

3.6.8 Client Installation Errors

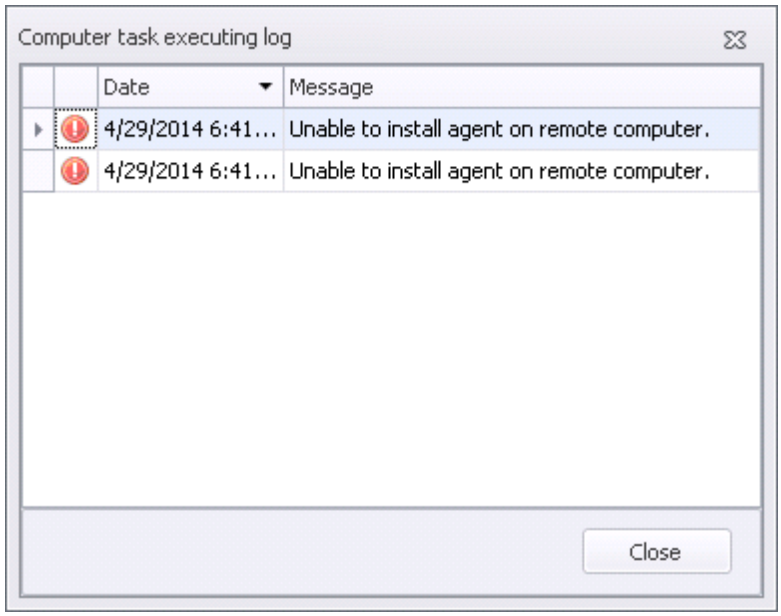
You may encounter installation problems during remote InfoWatch Device Monitor client applications installation tasks to computers. This will be indicated by **Task status** value in the list of tasks: see "View Tasks".

To view task errors:

1. Go to **Tasks**.
2. On **Tasks** panel select the task you want to review.
3. In **Status** column select filter value **Error** (for more information on filters see "Applying Standard Filters").

> **Note:**
> Status **No access** indicates that computer is not available (switched off or disconnected from network).

4. In the row of the target computer do one of the following:
   - right-click the row and select **Computer Log**
   - double-click the target computer row
   - at the top of **Task execution result** panel click **Computer log**.



5. To view detailed error information, click the row. This opens a screen with Windows error description.

For detailed information on the error see its description, error code, or log in error's description. In particular, the errors may be caused by the following things:

- computer is not available (switched off or disconnected from network);
- the installation process or reboot is blocked by another task or user (common description could be "*Other task is running*");
- target computer does not allow administrative resources;
- account in use doesn't have enough rights on target computer.

If all remote Client installation conditions listed in "Preparing Primary Client Installation" are met and the task is not blocked by the user, but the error persists, please contact InfoWatch technical support at support@infowatch.com and attach error description and log.

3.6.9 Creating Installation Package

Supplied InfoWatch Device Monitor Client installation package contains the following default settings:

- Client installation directory on computer system drive - `%Program Files%\Infowatch\DeviceMonitor\Client`.
- There is no uninstallation password.
- After installation Device Monitor Client starts to remind an employee that a reboot is required. Message text - "*Please reboot your computer as soon as possible*". Reminders are displayed infinitely, with 10 min intervals.

To change these settings create your own installation package. When you run it, it will use the settings specified when installation package created: no other parameters are needed to specify.

To create InfoWatch Device Monitor Client installation package:

1. In the Main Menu select **Tools > Create install package**.
   This opens distribution task manager dialog box.
2. The InfoWatch Device Monitor servers currently registered in the System are displayed. Client will use them for primary installation.

If necessary, change Client installation directory at computers.

Specify local or network directory where to the installation packages will be saved.

Click **Next**.

3. The unique name of Device Monitor proxy server certificate (Issuer Distinguished name, Proxy Root Issuer DN) will be displayed. You can change it with accordance to X.509 standard, CN (Common Name) field is mandatory, all fields comma-separated. Click **Next**.
4. Specify options of computer reboot:
   - **Wait for reboot without notifying the employee**. The Agent can:
     - start notifications immediately (*Do not wait* option),
     - start notifications in specified time (*Wait for* option - please specify time period to start notifications),
     - do not notify at all (*Wait infinitely* option).
   - **Notify the employee about reboot necessity and wait for reboot**. Upon completing reboot waiting in "silent" mode (see **Wait for reboot without notifying the employee** setting) or immediately after installation ends, Device Monitor Client starts to notify employee on reboot necessity:
     - during specified time period (*Notify within* option)
     - permanently (*Notify infinitely* option)
     - do not notify at all (*Do not notify* option).

     If needed, change continuance and frequency of notifications appearance and enter text of the message displaying in reboot notification.
   - **Show a warning before forced reboot**. If this check box is flagged, then the Client displays a notification about forced reboot and allows 5 minutes to end operations. If the option is not checked then the forced reboot (if it should be made according your settings) will be performed unexpectedly for the employee.

     Warning!
     Forced reboot is performed in case when neither **Wait while employee reboots computer** setting no **Show a warning before force reboot** setting do not flagged, or their wait durations are expired but employee did not reboot the computer.

   Click **Next**.
5. Define Client settings before it connects to the server for the first time:
   - To protect Client application from deleting by employee, enter the password that will be requested when trying to uninstall the Client and confirm it.
   - **Show employee notifications** - if employee attempts to perform an action restricted by security policy, a warning will be displayed. For further details, see "Employee Notifications about Policy Violations"
   - **Hide Agent presence** - indicates if Windows system tray of managed computer hides Client presence presence on the computer.

     Warning!
     Not notifying the user about interceptor operation may contradict the applicable laws of your country.

     Warning!
     If there is an antivirus protection enabled on the managed computer then the antivirus program can reveal the operation of Device Monitor: for example, in the list of processes running on the managed computer or in the list of programs that initiate a control.

     If this option is not selected, the Windows system tray of the computer where the Client is installed will display  icon. By clicking at this icon, an information on DM Client operation and list of currently controlled devices is displayed.
   - **Install the component of network interception -** installs **iw_proxy** component on a computer. Component will not be installed if you leave the checkbox empty.
   - **Install the component of network control -** installs **Network Monitor** interceptor on a computer. Component will not be installed if you leave the checkbox empty.

> **Warning!**
> You should not install the component of network control to the server with Citrix Provisioning Services: this can lead to the serious problems concerning server operation.

Click **Next**.

6. Look through the task summary. If you need to change any settings click **Back** to return. If all settings are correct, click **Finish**.

Client installation package will be saved in the folder you specified at the first step.

3.7 Additional Features

You can use the following functions to enhance your Management Console experience: filtering, grouping and sorting table entries.

Certain functions can be also accessed with hotkeys.

3.7.1 Filter Table Contents

You can filter table contents against one parameter or more with various filters. A filter makes a table display only the entries that comply with filtering conditions.

More information on filters is available in the following subsections:

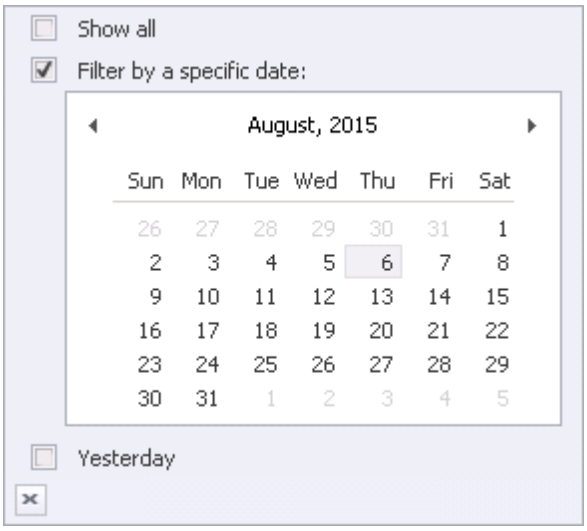
- Filter by Date
- Applying Standard Filters
- Custom Filter
- Editing Filters
- Removing a Filter

3.7.1.1 Filtering by Date

If the table shows temporary parameter characteristics (for example, Client installation date and time, Console log time, last computer access, registered event date, etc.), you can filter the column against the desired date or period.

To view the records for specific date or period:

1. Move the pointer over the time/date attribute in the column header.
2. Click the button to the right of the column header.



3. Select one of the following filters:
   - **Show all** - select this check box to view all records regardless the date.
   - **Filter by a specific date** - select the date in the calendar.

     To select a period, select it holding the mouse button.

     To go from date to month or year display, click the month/year.

     Use arrows to go forward or backward.
   - **Today**; **Yesterday**; **Last week**; **Earlier this week**; **Earlier this year** fields depend on column values: for example, if there are no records for the date, **Today** field won't be displayed. Check this box to display only the records inside specific date range.
4. Click ✖ to apply the filter and close the form.

3.7.1.2 Applying Standard Filters

To filter table entries against a single attribute:

1. Move the pointer over the column header that contains required attribute.
2. To view filter list, click ▽ to the right of the column.
3. Select one of the following filters from the list:
   - **Blanks**. Display records with `<Is Null>` value (the field is empty).
   - **Non blanks**. Display records with `<Is Not Null>` value (i.e., the field contains attribute value).
   - `<attribute value>`. Display records that contain selected attribute.

> **Note:**
> **Custom** option lets you configure your filtering criteria (for more info see "Custom Filter").

The table will only display filtered values.

To filter values against several attributes,

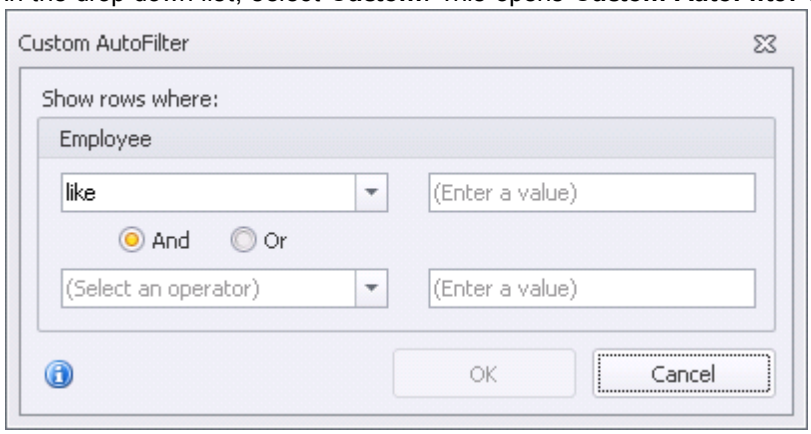
repeat simple filtering procedure against all filter attributes you want to apply.

Complex filter reduces the table contents to records filtered against several attributes.

3.7.1.3 Custom Filter

To specify your own filtering criteria for table entries:

1. Move the pointer over the column header that contains required attribute.
2. Expand filter list by clicking ▽ to the right of the column header.
3. In the drop-down list, select **Custom**. This opens **Custom AutoFilter** dialog.



4. In this box, specify filtering criteria:
   - Select conditions from the drop-down list in the upper-left box.

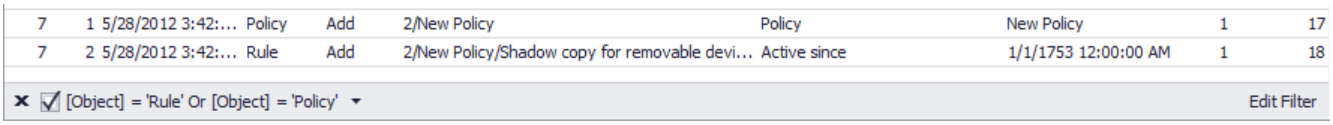
> **Note:**
> You can use comparison operators to limit filtering criteria: *equal*, *not equal*, *greater than*, *greater than or equal to*, *less than*, *less than or equal to*; values *empty* (blank) and *nonempty* (non-blank field); or text filter with a mask. To get a text filter syntax tip, click ⓘ.

   - Enter condition value into the top right box.
   - Specify additional criteria, if needed, by selecting a logical operator for and entering the second condition at the bottom.

> **Note:**
> Choose logical operator **AND**, if you want the items that match both conditions at the same time. Select logical operator **OR** filters the items that match at least one condition.

5. Click **OK** to apply the filter.

Filtered table only displays the items that match filtering criteria. Filtering criteria string is at the bottom of the screen that contains filtered items.



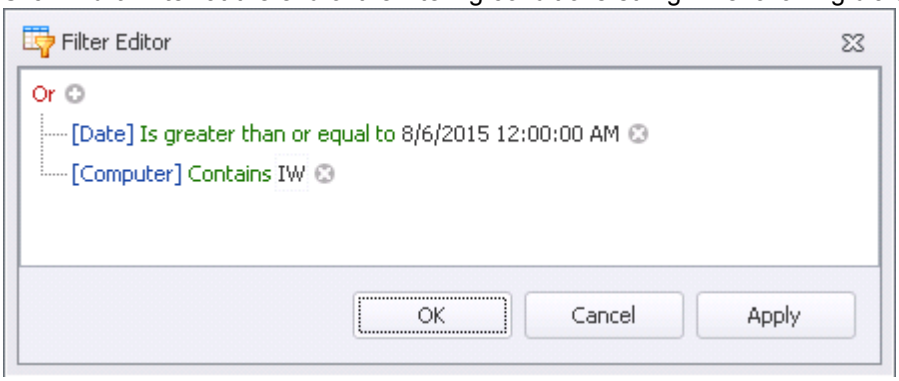
To remove filter and view all items, clear the check box in filter string. To apply the filter again, select the check box.

To re-use a filter, click the filter string and select filter from drop-down filter history list. Custom filters are stored until you close the window with filtered content.

3.7.1.4 Editing Filters

To edit active filter:

1. Click **Edit Filter** at the end of the filtering conditions string. The following dialog box displays **Filter Editor**.



2. Edit filtering criteria. Available actions:

Action	Steps
Edit an attribute, attribute value or operator	1. Click attribute/value name of attribute/operator 2. Select the value from the drop-down list or enter the value to the field
Add a simple condition	Click the button ⊕ to the right of the logical operator or Click **Add Condition** in logical operator menu
Delete condition	Click the button ⊗ at the end of condition string
Add criteria group	1. Click the logical operator name 2. Select **Add Group** in the menu
Delete criteria group	1. Click the name of operator criteria group 2. Select **Delete Group** in the menu
Delete all criteria	Click **Clear All** in logical operator menu

3. Click **Apply** and view the filtered results without closing **Filter Editor** screen.
4. Click **OK**.

3.7.1.5 Removing a Filter

To remove a filter,

take one of the following steps:

- Click filtered column header and select **All** from the drop-down filter list.

  If you are using complex filter, repeat the step for every condition you want to remove.
- Remove the flag in filter conditions string.
- Click ✖ in filter conditions string. This closes filter conditions string.

3.7.2 Grouping or Sorting Entries

Grouping function is intended for managing table entries according to selected schema. Group scheme is displayed on the group panel over the column title row. Contents are grouped basing on a single attribute or more (table columns).

To group the contents basing on an attribute:

1. In table's title row, click the column title that corresponds to the attribute name.
2. Click and hold the title to drag it over the group panel. Name of the grouping attribute appears on the group panel.

To group the contents basing on multiple attributes, repeat steps 1-2 for all attributes participating in the process.

Note:
You can change the grouping procedure by changing the order of column titles in group scheme. The column with the title is at the top right of the group scheme is processed first.

Grouped entries appear collapsed. To view information for a specific entry, click ⊞ on the left of the record you want to expand. To minimize entry, click ⊟ to the entry's left.
You can ungroup entries basing on one or more attributes, removing columns from the group scheme.

To ungroup entries basing on any attribute:

1. In group panel, click and hold the column title you want to remove from the group scheme and drag it into table title row. Column location is indicated with a rectangular frame.
2. Move column title over the title row to the desired position and release the button. This will move the column to specified location.

Use sorting feature to display table contents in ascending or descending order of any attribute.

To change attribute values sorting order of the in a column,
move the pointer over the column title you want to use for sorting. Click the selected title. This will sort all table contents in ascending/descending order of the attribute values.

To go back to the old sorting order,
click the selected header once again.

3.7.3 Hotkeys

The following table lists the keys and key combinations, used for quick access to various system functions.

Feature name	Hotkeys
Server connection	
Connect to server	F4
Exit Console	Alt+F4
Main screen customization	
Hide/show Navigation bar	Ctrl+Shift+1
Hide/show Details	Ctrl+Shift+2
Hide/show Console log	Ctrl+Shift+3

Feature name	Hotkeys
Management Console sections	
Go to Policies	Ctrl+2
Go to Employees	Ctrl+3
Go to Computers	Ctrl+4
Go to White Lists	Ctrl+5
Go to Signatures	Ctrl+6
Go to Log	Ctrl+7
Go to Tasks	Ctrl+8
Go to Events	Ctrl+9
Manage security schema (overview)	
Go to security schema editing mode	F11
Save security schema	F12
Cancel saving security schema	Shift+F11
Unblock security schema (Superuser only)	Ctrl+Shift+U
Update security schema	F5
Go to the latest security schema version (when viewing an earlier version)	F9
Manage security policies	
Add security policy	Ctrl+N
Edit security policy	Ctrl+E
Delete security policy	Ctrl+D
Manage rules	
Add rule	Ctrl+Shift+N
Edit rule	Ctrl+Shift+E
Delete rule	Delete
Manage employee groups	

Feature name	Hotkeys
Add new employee group	Ctrl+N
Edit employee group	Ctrl+E
Delete employee group	Ctrl+D
Manage employee accounts	
Add employee account to a group	Ctrl+Shift+N
Edit employee account	Ctrl+Shift+E
Remove employee account from a group	Delete
Delete employee account from security schema	Shift+Delete
Manage computer groups	
Add new computer group	Ctrl+N
Edit computer group	Ctrl+E
Delete computer group	Ctrl+D
Manage computers	
Add computer	Ctrl+Shift+I
Remove computer from a group	Delete
Delete computer from security schema	Shift+Delete
Manage white lists	
Add white list	Ctrl+N
Edit white list	Ctrl+E
Delete white list	Ctrl+D
Edit white list entries	Ctrl+Shift+E
Manage signatures	
Add signature category	Ctrl+N
Edit signature category	Ctrl+E

Feature name	Hotkeys
Delete signature category	Ctrl+D
Remove signature from category	Delete
Configure filters for Audit Log and Event Viewer	
Add filter	Ctrl+N
Edit filter	Ctrl+E
Delete filter	Ctrl+D
Manage Client remote installation and upgrade tasks	
Add task	Ctrl+N
Edit task	Ctrl+E
Delete task	Ctrl+D
Add computer to selected task	Ctrl+Shift+N
Remove computer from selected task	Delete
Display target computer error log	Ctrl+L

4 Troubleshooting

If you have any issues regarding the product operation, please contact support:

- If you have purchased the product from InfoWatch partner, please contact partner support.
- If you purchased the product directly from InfoWatch, you can contact our support at support@infowatch.com or through web-site http://cp.infowatch.com/en/.
  Technical Support Service is available to assist you Mon-Fri, 7 AM – 9 PM (Moscow time, GMT+4), except weekends and Russian Federation public holidays.

Before contacting support please refer to our *Knowledge Base* at https://kb.infowatch.com/. Knowledge Base may already have the answer to your question or description of the problem you are experiencing.

In the appeal to the support, aside from error description, we recommend you to apply the archive of files with diagnostic data to the letter. The order of receiving the archive of files with diagnostic data see "Diagnostics of the Workstation".

If a server error occurs, you can view all server module error and informational messages in Windows Application Log. For descriptions of server error codes in Windows Application Log see "Viewing Server Messages".

Here are several examples of potential problems, their sources and solutions.

Problem: Security Officer can't edit security schema

Reason: Security schema editing commands aren't active.

Solution: You can edit only the latest version of security schema. Status bar contains information on security schema that is being loaded to Management Console (if the latest security schema is used, the status bar displays security schema version and mode). To exit old security schema mode, click **Edit > View the latest security schema** in the Main Menu or press **F9** .

Problem: Managed computer was removed from security schema, but its information is displayed in **Computers** section

Description: Removed computer record remains in security schema with **Agent Disabled** status.

Solution: You can delete managed computers records manually, if necessary. You can find more information on how to remove a computer from security schema in "Removing Computer from Security Schema".

Problem: When installing the InfoWatch Device Monitor Client to the workstation, the error "no access to Agent" is displayed.

Probable reasons and alternate solutions:

1. Not enough rights for Agents installation.
   On the computer to which the Client is installed, please provide local administrator rights for account on behalf of which the installation is executed.
2. Access to shared administrative folders C$ and admin$ is denied.
   Please provide the access to those folders to the account on behalf of which the installation is executed.
3. Ports in the firewall are closed.
   Open the following ports: TCP-15003,15101,15505,15506,4101,1521,1433; UDP-15100.
4. Antivirus blocks Agents installation.
   Configure the exception in antivirus settings or disable self-protecting module.

Problem: Error in Agent installation.

Probable reasons and alternate solutions:

1. The hard drive is filled up, not enough place on the disk.
   Clear enough space.
2. Installation error. There is an error code 1603 in the log.
   The directory to which the installation is performed, is encrypted or located on the removable device or the system account does not have an access to it. Please change the installation directory (select unencrypted one located on the local media accessed by SYSTEM account) and run distributive installation on behalf of user having full access to the directory.

4.1 Viewing Server Messages

If a server error occurs, you can view all server module error and informational messages in Windows Application Log. The following table describes potential server error codes in Windows Application Log.

Warning!

If the problem persists, please contact InfoWatch support and specify the following information:

- problem description,
- error code,
- error message text,
- what actions have been taken to address the problem.

Error code	Severity	Description
`InfoWatch.DeviceMonitor.Server.Client` Module (server side for clients) Event source in Windows Log: `InfoWatch.DeviceMonitor.Server.Client` Error module base number: 1000		
1000	Critical error	Packaging error prior to sending data to client. Contact InfoWatch support.
1001	Error	Unable to write client disconnection/connection event to database. Typically, the problem is caused by disconnection from the database. Occasionally, it can be caused by server code errors. More in-depth diagnostic information should be maintained basing on the error message text
1002	Error	Unable to register new computer in the database. Typically, the problem is caused by disconnection to the database. Very occasionally, it can be caused by server code errors. More in-depth diagnostic information should be maintained basing on the error message text
1003	Error	Client connection has been lost. Can be caused by anything, starting from network problems to code errors. More in-depth diagnostic information should be maintained basing on the error message text
1004	Warning	Client connection timeout. Generally, this is caused by network problems or client-end errors (unexpected shutdown, etc.)
1005	Warning	Connection to client closed (socket closed). Generally, this is caused by network problems.
1006	Error	Raw server error. Occurs because of client connection errors or raw errors due to server service termination.
1007	Error	Occurs because computer DB update errors. Typically, the problem is caused by disconnection from the database. Occasionally, it can be caused by server code errors. More in-depth diagnostic information should be maintained basing on the error message text
1008	Error	Error occurs because of inactive computers monitoring errors (exceptions). Caused by network problems or server code errors. More in-depth diagnostic information should be maintained basing on the error message text.
1009	Warning	Unable to find specified computer name on the network. Error occurs when monitoring inactive computers. Caused by networking problems or inability to recognize names on the network, or absence of host (if it was removed). We recommend that you remove computer from security schema (see "Deleting Computer from Security Schema").
1010	Error	Unable to connect to the Client. Error caused by network problems or server code errors. More in-depth diagnostic information should be maintained basing on the error message text
1011	Error	Failed to prepare data for sending to client. Almost always caused by errors in Server facade code for clients. Contact InfoWatch support.
1012	Error	Client data parsing error. May be caused by errors in server facade code for clients, damaged network packets, or packaging errors on client-end. More in-depth diagnostic information should be maintained basing on the error message text
1013	Critical error	Invalid package signature. Signature doesn't adhere to the protocol. May be caused by errors in server facade code for clients, damaged network packets, packaging errors on client-end. More in-depth diagnostic information should be maintained basing on the error message text
1014	Error	Packet (excluding users package) exceeds maximum length. Error might be caused by damaged network packets or packaging errors on client-end. More in-depth diagnostic information should be maintained basing on the error message text

Error code	Severity	Description
1015	Error	User packet exceeds maximum length. Error might be caused by damaged network packets or packaging errors on client-end. More in-depth diagnostic information should be maintained basing on the error message text.
1016	Error	Unsupported package type. Error might be caused by damaged network packets or packaging errors on client-end. More in-depth diagnostic information should be maintained basing on the error message text
1017	Error	Event package parsing error. May be caused by errors in server facade code for clients, damaged network packets, packaging errors on client-end. More in-depth diagnostic information should be maintained basing on the error message text.
1018	Warning	Empty event packet received. The packet might also contain "bad events" that caused the parsing error. May be caused by errors in server facade code for clients, damaged network packets, packaging errors on client-end. More in-depth diagnostic information should be maintained basing on the error message text
1019	Error	DB event saving error. May be caused by violation of integrity constraints: for example, event contains an unknown server rule ID. This error may also occur, if you attempt saving a duplicate event.
1020	Information	Server facade for clients is running.
1021	Information	Server facade for clients has been stopped.
1022	Warning	Server received a bad security schema checksum (hash) from the client. Client's security schema may be corrupted or deliberately changed.
1023	Warning	Maximum number of client connections in Demo version has been exceeded.
`InfoWatch.DeviceMonitor.TrafficMonitor.Connector` Module (Traffic Monitor connector) Event source in Windows Log: `InfoWatch.DeviceMonitor.TrafficMonitor.Connector` Error module base number: 2000		
2000	Error	A negative value of TM connections in server's configuration file. Change configuration file (see "<applicationSettings> section", `NumberOfConnections` setting).
2001	Warning	TM connections value (> 32) in server configuration file is too large. Number of connections is set to 32. Change configuration file (see "<applicationSettings> section", `NumberOfConnections` setting).
2002	Error	Failed to connect to DB while sending events to TM. Check DB state and availability.
2003	Error	DB request error while sending events to TM. May be caused by blockage or very occasionally by server code errors. More in-depth diagnostic information should be maintained basing on the error message text.
2004	Error	Unknown error when sending messages to TM. More in-depth diagnostic information should be maintained basing on the error message text.
2005	Error	Error reading queue length from DB. Check DB state and availability.
2006	Information	TM connection change.
2007	Error	Unable to delete shadow copy. Shadow copy file may be opened by another application or missing . Can also be caused by server code error. More in-depth diagnostic information should be maintained basing on the error message text.
2008	Error	TM response reading error. May be caused by invalid message format, network problems, etc. More in-depth diagnostic information should be maintained basing on the error message text.
2009	Error	An error occurred during network communication. Verify that the network is functioning.
2010	Error	TM connection has been lost. May be caused by network problems or TM stop. More

Error code	Severity	Description
		in-depth diagnostic information should be maintained basing on the error message text.
2011	Error	Unknown TM messaging error. More in-depth diagnostic information should be maintained basing on the error message text.
2012	Error	Attempt to add an exhausted connection to a filled pool. Contact InfoWatch support.
2013	Warning	The event must have a shadow copy, but it's not on the DM server. It might not be transmitted by the client or lost during transmission.
2014	Critical error	TM connector is misconfigured. Server configuration file contains errors. Check server configuration file (see section 5.9 on page 93). More in-depth diagnostic information should be maintained basing on the error message text.
2015	Information	Sending the message to TM was cancelled.
2016	Warning	E-mail message that contains the event exceeds maximum size. Applies to TM 2.5
2017	Warning	Invalid login format for transmission to TM 2.5. DOMAIN\LOGIN is expected. The problem may be caused by the client that sent an invalid login. Invalid login could also be added manually from Management Console.
2018	Information	Connected to TM.
2019	Warning	TM sent an empty response. An issue on TM end.
2020	Warning	Unable to read message type attribute from TM 3.x response. The problem is caused by TM response formatting errors.
2021	Warning	Invalid TM 3.x message type. The problem is caused by TM response formatting errors.
`InfoWatch.DeviceMonitor.Server.Core` Module (server startup code) Event source in Windows Log: `InfoWatch.DeviceMonitor.Server.Core` Error module base number: 3000		
3000	Critical error	GUI facade TCP port (15003 by default) is already in use. Check if any running applications use this port, and modify their settings or server configuration by assigning it to a different GUI facade port in server configuration file
3001	Critical error	Unable to connect to database. Server launches and will attempt to establish a connection to DB. Check DB state and availability.
3002	Critical error	Unable to launch TM connector. More in-depth diagnostic information should be maintained basing on the error message text.
3003	Error	Error deleting GUI facade channel registration. Contact InfoWatch support.
`InfoWatch.DeviceMonitor.Server.Database` Module (DB interaction Module) Event source in Windows Log: `InfoWatch.DeviceMonitor.Server.Database` Error module base number: 4000		
4000	Critical error	Unsupported DBMS. Server configuration file error. Check server configuration file
4001	Error	Failed to read server settings from DB. More in-depth diagnostic information should be maintained basing on the error message text
4002	Error	Error copying new server settings to DB. More in-depth diagnostic information should be maintained basing on the error message text
4003	Error	Error updating server settings in DB. More in-depth diagnostic information should be maintained basing on the error message text
4004	Warning	Error reading security schema version from DB. The problem is caused by absence of security schema. Create a new security schema

Error code	Severity	Description
4005	Warning	Reading ban has been converted into No access rule.
4006	Warning	Writing ban has been converted into Read Only rule.
4007	Warning	Writing permission has been converted into Full Access.
4008	Information	Security schema doesn't contain the computer specified in the message.
4009	Information	Failed to read last event number from log.
4010	Critical error	Unsupported database type. Contact InfoWatch support.
4011	Error	Empty user list received from the client. Investigate client end or packet parsing.
4012	Warning	DB has been upgraded from version 3.1 to 3.2
4013	Warning	DB has been upgraded from version 3.2 to 3.3
4014	Warning	To hard drive rule is not supported and has been deleted from security schema.

5 Licensing Information

End-User License Agreement

The system contains third-party software components:

- **WiX toolset** – WiX Common Public License

5.1 WiX Common Public License

WiX Common Public License

Top Previous Next

Common Public License Version 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

"Contribution" means:

a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

b) in the case of each subsequent Contributor:

i) changes to the Program, and

ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents " mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and

distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

5.2 InfoWatch Device Monitor End-User License Agreement

This End-User License Agreement (hereafter referred to as the “Agreement”) is the legal agreement between InfoWatch (hereafter referred to as the “InfoWatch”) and the User, either an individual or a legal entity who legally possess a copy of the software (hereafter referred to as the “System”).

1. Definitions

1.1. “Software” means the System, accompanying documents, System Documentation, additionally ordered updates whether taken together or separately.

1.2. “User” (or “You”) means an individual who installs or uses the software on his or her own behalf or legally owns a copy of this Software. If the Software is purchased or downloaded on behalf of any legal entity, then the “User” (“You”) term further refers to the legal entity for which this Software is downloaded or purchased and which authorized a natural person to accept this Agreement on its behalf.

1.3. “Partners” means third parties authorized to distribute the Software on the basis of an agreement with the InfoWatch.

1.4. “System Documentation” means all accompanying printed or other materials, the User Guide, Administration Guide, reference, help file and similar accompanying documentation, whether in print or electronic form, legally owned by InfoWatch Corporation.

2. Grant of License

2.1 The InfoWatch hereby grants you a non-exclusive license to use the Software for purposes described in the System Documentation, provided that the technical requirements, stated in the System Documentation, and also all restrictions and conditions for the use of the System, prescribed in this Agreement, are met.

2.2 If you have purchased, downloaded and/or installed the Software intended for trial purposes, you may use the Software only for trial purposes and only during one trial period, unless otherwise stated, starting

from the date of first installation of the Software. This Software may not be used for any other purposes or beyond the trial period.

2.3 If you use different versions of the Software or Software versions for other languages, or if you have purchased the Software on multiple media, if you otherwise received multiple copies of the Software or if you received the Software bundled other software, the total number of your computers where all versions of the System are installed and/or used shall correspond with the number of licenses you have obtained from the InfoWatch.

2.4 You may create a copy of the Software provided that the copy is intended solely for back-up purposes or to replace a legally purchased copy of the Software, if such a copy is lost, destroyed or unusable. This copy may not be used for any other purposes and must be deleted if the Software license is ceased.

2.5 The User may transfer the User's rights for this Software provided that the successor User agrees to be bound by the terms and conditions of this Agreement and with prior written consent of the InfoWatch or the InfoWatch's authorized Partner. Therewith, in terms of the use of this Software, the successor User becomes the legal successor of the current User, provided that the current User is fully substituted by the successor User (transferee) in terms of this Agreement.

2.6 You are solely responsible for compliance with applicable export and import laws and regulations, and also applicable trade sanctions and embargo in relation to the transfer of rights and the use of this Software.

3. Restrictions

3.1 You may not decompile, disassemble, modify or create derivative works based on the Software in whole or in part.

3.2. You may not directly or indirectly rent, distribute, transfer, license, sublicense, sell, assign, pledge or furnish to any third party all or any part of, the System or copies of any part thereof. You may not publish the results of the bench testing of the System.

3.3. The System is licensed to you only. Subject to the compliance with the terms herein, You may install and use the System only within premises owned and controlled by you.

3.4 You may not transfer the right to use the Software to any third party except as allowed by Clause 2.5.

3.5 You may not transfer or grant access to the license key to any third party in violation of this Agreement, except as allowed by Clause 2.5. The license key is confidential information. The InfoWatch reserves the right to use authentication methods to verify the authenticity of your license key.

3.6 The InfoWatch may block the license key upon any violation by the User of this Agreement.

3.7 If you use the trial version of the Software, you may not, in any manner, give or sell the Software copy to any third party.

3.8 You may not use the Software for a purpose or in a manner not permitted or restricted by applicable Laws. You are solely responsible for any unlawful use of this Software.

3.9 If you fail to comply with any of terms of this License Agreement, the InfoWatch may at any time, without notice, terminate this License Agreement to use the Software without refunding the purchase price or any part thereof.

4. Limited Warranty and Disclaimer

4.1 The InfoWatch guarantees that the Software will substantially perform according to the specifications and descriptions set forth in the System Documentation provided.

4.2 You acknowledge, accept and agree that no software is error free and You are advised to regularly back-up your files.

4.3 The InfoWatch does not provide any guarantee that the Software will operate correctly if the conditions stated in the System Documentation are violated or if the User violates the terms of this Agreement.

4.4 EXCEPT FOR THE FOREGOING, THE SOFTWARE IS PROVIDED “AS IS”. THE INFOWATCH AND ITS PARTNERS MAKE NO REPRESENTATION AND GIVE NO WARRANTY AS TO ITS USE OR PERFORMANCE. EXCEPT FOR ANY WARRANTY, CONDITION, REPRESENTATION OR TERM THE EXTENT TO WHICH CANNOT BE EXCLUDED OR LIMITED BY APPLICABLE LAW THE INFOWATCH AND ITS PARTNERS MAKE NO WARRANTY, CONDITION, REPRESENTATION, OR TERM (EXPRESS OR IMPLIED, WHETHER BY STATUTE, COMMON LAW, CUSTOM, USAGE OR OTHERWISE) AS TO ANY MATTER INCLUDING, WITHOUT LIMITATION, NONINFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABILITY, SATISFACTORY QUALITY, INTEGRATION, OR APPLICABILITY FOR A PARTICULAR PURPOSE. YOU ASSUME ALL FAULTS, AND THE ENTIRE RISK AS TO PERFORMANCE AND RESPONSIBILITY FOR SELECTING THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS, AND FOR THE INSTALLATION OF, USE OF, AND RESULTS OBTAINED FROM THE SOFTWARE.

5. Exclusion and Limitation of Liability

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE INFOWATCH OR ITS PARTNERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, PUNITIVE, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS OR CONFIDENTIAL OR OTHER INFORMATION, FOR BUSINESS INTERRUPTION, FOR LOSS OF PRIVACY, FOR CORRUPTION, DAMAGE AND LOSS OF DATA OR PROGRAMS, FOR FAILURE TO MEET ANY DUTY INCLUDING ANY STATUTORY DUTY, DUTY OF GOOD FAITH OR DUTY OF REASONABLE CARE, FOR NEGLIGENCE, FOR ECONOMIC LOSS, AND FOR ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SOFTWARE, THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT OR OTHER SERVICES, INFORMATON, SOFTWARE, AND RELATED CONTENT THROUGH THE SOFTWARE OR OTHERWISE ARISING OUT OF THE USE OF THE SOFTWARE, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY PROVISION OF THIS AGREEMENT, OR ARISING OUT OF ANY BREACH OF CONTRACT OR ANY TORT (INCLUDING NEGLIGENCE, MISREPRESENTATION, ANY STRICT LIABILITY OBLIGATION OR DUTY), OR ANY BREACH OF STATUTORY DUTY, OR ANY BREACH OF WARRANTY OF THE INFOWATCH OR ANY OF ITS PARTNERS, EVEN IF THE INFOWATCH OR ANY PARTNER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

6. Third-party Software Products

6.1 Third-party technology that may be appropriate or necessary for use with this Software is specified in the System Documentation. Such third-party technology is licensed to the end-user under the terms of the third-party license agreement specified in the System Documentation. Such third-party Agreement supplements the provisions of this Agreement.

6.2 Software products included in the System are licensed for limited use and may be used only as parts of the System. When the license agreement for the Software expires, the User must stop using the Software

and delete all existing copies.

7. Open (Free) Software

The Software may include some software programs that are licensed (or sublicensed) to the User under the GNU General Public License (GPL) or other similar 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 license requires that for any software, which is distributed to someone in an executable binary format, the source code also be made available to those users, then the source code should be made available by sending the request to the InfoWatch or be provided with the product. If any Open Source Software licenses require that the InfoWatch provide rights to use, copy or modify an Open Source Software program that are broader than the rights granted in this Agreement, then such rights shall take precedence over the rights and restrictions herein.

8. Intellectual Property Ownership

8.1 You agree that the Software, documentation and all other intellectual property and also the systems, ideas, trademarks, methods of operation and other information contained in the Software are proprietary intellectual property of the InfoWatch or its Partners. Except as stated herein, this Agreement does not grant to You any rights to the intellectual property including any of the Trademarks or Service Marks of the InfoWatch and/or its Partners.

8.2 You acknowledge that the source code and license key file for the Software are proprietary to the InfoWatch and/or its Partners.

8.3 You may not remove or alter any copyright notices or other proprietary notices on any copies of the Software.

9. Contact Information of the InfoWatch

InfoWatch

Phone/fax: +7(495)229-00-22

Sales department: sales@infowatch.com

Technical support service: support@infowatch.com

Web site: www.infowatch.com

InfoWatch©