

INFOWATCH

# InfoWatch Device Monitor 4.2

User Guide

INFOWATCH DEVICE MONITOR 4.2

# User Guide

© ZAO “InfoWatch”
tel +7 (495) 229-00-22 • fax +7 (495) 229-00-22
http://www.infowatch.com
Revision date: Октябрь 2014

# Table of contents

Part I InfoWatch Device Monitor Overview 8

1.1 InfoWatch Device Monitor Functions ....8

1.1.1 Operation in Safe Mode ....10

1.2 InfoWatch Device Monitor Workflow ....10

1.3 Security Schema Organization ....12

1.3.1 Security Rules and Policies ....13

1.3.2 Employees and Employee Groups ....14

1.3.3 Workstations and Workstation Groups ....14

1.3.4 Uploading Security Schema to Managed Workstations ....14

1.4 Glossary ....15

Part II Installing and Configuring InfoWatch Device Monitor 17

2.1 Hardware and Software Requirements ....19

2.1.1 Database ....19

2.1.2 InfoWatch Device Monitor Server ....19

2.1.3 InfoWatch Device Monitor Client ....19

2.1.4 Management Console ....20

2.2 InfoWatch Device Monitor Server End Setup ....20

2.2.1 Database deployment under Microsoft SQL Server DBMS ....21

2.2.2 Database Deployment Under Oracle DBMS ....21

2.2.2.1 Configuring InfoWatch Device Monitor Connection to Oracle DBMS Server ....22

2.2.3 Server Setup Recommendations ....22

2.2.4 Server End Installation Procedure ....23

2.3 InfoWatch Device Monitor Client Setup ....28

2.3.1 Standard Client Setup ....28

2.3.2 Client Setup via Software Distribution Tools ....29

2.4 Configuring InfoWatch Device Monitor Server ....31

2.4.1 <applicationSettings> section ....32

2.4.2 <system.diagnostics> section ....34

2.5 Updating InfoWatch Device Monitor ....36

2.5.1 Updating InfoWatch Device Monitor Server End ....36
2.5.2 Updating InfoWatch Device Monitor Client ....37
2.6 Uninstalling InfoWatch Device Monitor ....38
2.6.1 Removing Client Installed via Software Distribution Tools ....39
Part III Using Management Console 39
3.1 Management Console Overview ....39
3.1.1 Authorization and Connecting to InfoWatch Device Monitor Server ....40
3.1.2 Management Console Main Screen ....41
3.1.2.1 Configuring Management Console Main Screen Elements ....42
3.1.3 Management Console Sections ....42
3.2 Management Console Accounts Administration ....43
3.2.1 Viewing Management Console Accounts Details ....45
3.2.2 Adding New Management Console Account ....46
3.2.3 Locking or Unlocking Management Console Account ....46
3.2.4 Editing Management Console Account ....47
3.2.5 Deleting Management Console Account ....47
3.2.6 Management Console Security Schema Operation Activity Log ....47
3.2.6.1 Viewing Audit Log ....48
3.2.6.1.1Selector Values ....49
3.2.6.2 Log Records Filtering ....50
3.2.6.2.1Date/Sequence Number Tab ....52
3.2.6.2.2Object/Action Tab ....52
3.2.6.2.3Additional Tab ....53
3.2.6.3 Deleting Records from Log ....54
3.2.6.4 Exporting Log Records ....54
3.2.6.5 Analyzing Log Records in Microsoft Excel ....54
3.3 General System Settings ....54
3.3.1 Common Settings for Clients ....55
3.3.2 Settings of Corporate Network ....56
3.3.3 Network Traffic Control ....58
3.3.4 Device Monitor Server Settings. Connecting to Traffic Monitor Server ....60
3.3.5 Connecting to LDAP Server ....61

3.3.6 Employee Notifications about Policy Violations ....62
3.4 Managing Security Schema ....63
3.4.1 Security Schemas Overview ....63
3.4.1.1 Viewing Active Security Schema ....64
3.4.1.2 Viewing Old Security Schema ....64
3.4.1.3 Security Schema Comments ....65
3.4.1.4 Editing Security Schema ....66
3.4.1.4.1Awaiting Editing Ends. Unlocking Security Schema ....67
3.4.1.5 Updating Security Schema ....68
3.4.1.6 Exporting/Importing Security Schema ....68
3.4.2 Security Schema Setup ....68
3.4.2.1 Security Policies ....69
3.4.2.1.1Viewing Security Policies ....69
3.4.2.1.2Adding and Configuring New Security Policy ....71
3.4.2.1.3Editing Security Policy ....72
3.4.2.1.4Deleting Security Policy ....73
3.4.2.2 Rules ....73
3.4.2.2.1Rules Application ....73
3.4.2.2.1.1 Device Monitor Rules Application ....74
3.4.2.2.1.2 Creating Shadow Copies and Blocking Operations Due to Free Space Shortage ....76
3.4.2.2.2Adding a Rule ....76
3.4.2.2.2.1 Configuring File Monitor Rule ....77
3.4.2.2.2.2 Configuring Print Monitor Rule ....79
3.4.2.2.2.3 Configuring Device Monitor Rule ....80
3.4.2.2.2.4 Configuring IM Client Monitor Rule ....82
3.4.2.2.2.5 Configuring FTP Monitor Rule ....83
3.4.2.2.2.6 Configuring HTTPS Monitor Rule ....85
3.4.2.2.2.7 Configuring Network Monitor Rule ....86
3.4.2.2.3Editing a Rule ....87
3.4.2.2.4Deleting a Rule ....87
3.4.2.2.5Copying a Rule ....88
3.4.2.3 Employees ....88

3.4.2.3.1Viewing Employee Details 89
3.4.2.3.2Adding and Editing an Employee Group 89
3.4.2.3.3Deleting Employee Group 91
3.4.2.3.4Adding Employee Account to a Group 91
3.4.2.3.5Editing Employee Account 92
3.4.2.3.6Removing Employee Account from Employee Group 93
3.4.2.3.7Deleting Employee Account from Security Schema 94
3.4.2.4 Workstations 94
3.4.2.4.1Viewing Workstation Details 94
3.4.2.4.2Viewing Workstation Effective Policy 96
3.4.2.4.3Adding and Editing a Workstation Group 97
3.4.2.4.4Deleting Workstation Group 98
3.4.2.4.5Adding Workstation to a Group 98
3.4.2.4.6Removing Workstation from a Group 99
3.4.2.4.7Deleting Workstation from Security Schema 100
3.4.2.4.8Updating Clients at Managed Workstations 101
3.4.2.5 White Lists 101
3.4.2.5.1Viewing White List Details 101
3.4.2.5.2Adding White List 102
3.4.2.5.2.1 Adding Device to Database 103
3.4.2.5.2.2 Removing Device from Database 104
3.4.2.5.3Defining Entry Validity Period 105
3.4.2.5.4Editing White List 105
3.4.2.5.5Deleting White List 106
3.4.2.6 Signatures 106
3.4.2.6.1Adding Signature Category 106
3.4.2.6.2Editing Signature Category 107
3.4.2.6.3Deleting Signature Category 108
3.4.3 Temporary Employee Access 108
3.5 Viewing Events 109
3.5.1 Event Filters 113
3.5.2 Deleting Events 114

3.6 Clients Remote Installation, Updating and Uninstallation ....114
3.6.1 View Tasks ....115
3.6.2 Preparing Primary Client Installation. Distribution Agent ....116
3.6.2.1 Enabling Shared Administrative Resources ....117
3.6.2.2 Firewall Settings ....117
3.6.3 Creating Primary Distribution Task ....118
3.6.4 Creating Update Task ....120
3.6.5 Creating Uninstallation Password Reset Task ....120
3.6.6 Creating Uninstallation Task ....121
3.6.7 Launching, Pausing, Editing, and Deleting Tasks ....122
3.6.8 Client Installation Errors ....122
3.6.9 Creating Installation Package ....123
3.7 Additional Features ....124
3.7.1 Filter Table Contents ....124
3.7.1.1 Filtering by Date ....124
3.7.1.2 Applying Standard Filters ....125
3.7.1.3 Custom Filter ....126
3.7.1.4 Editing Filters ....127
3.7.1.5 Removing a Filter ....127
3.7.2 Grouping or Sorting Entries ....128
3.7.3 Hotkeys ....128
Part IV Troubleshooting 131
4.1 Viewing Server Messages ....132
Part V Licensing Information 135
5.1 WiX Common Public License ....135
5.2 InfoWatch Device Monitor End-User License Agreement ....138

# 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 to removable devices from workstations and 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 of InfoWatch Device Monitor system and its components.
- Security Schema Organization. Implementation of InfoWatch Device Monitor security schema and basic concepts of System operation.
- 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.
- Technical Support Service is available to assist you Mon-Fri, 7 AM – 9 PM (Moscow time, GMT+4), except weekends and RF public holidays.

Before contacting support please refer to our *Knowledge Base* at: http://cp.infowatch.com/en/kb. 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 workstations monitoring;
- managing employee access to system peripherals;
- monitoring workstation print operations;
- supervising Instant Messengers: Skype, Jabber (XMPP protocol) and Mail.Ru Agent (MMP protocol);
- supervising traffic transferred by FTP;
- supervising traffic transferred by HTTPS;
- supervising data transferred by network connections beyond corporate network;
- retrieving data from managed workstations;

- transferring retrieved data for InfoWatch Traffic Monitor analysis.

> **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 workstations. ***Managed workstation*** is a workspace 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 workstations you need a Client module. Client module includes the following interceptors: **File Monitor**, **Print Monitor, Device Monitor**, **IM Client Monitor, Ftp Monitor**, **HTTPS Monitor, Network 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 workstations, 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, 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 protocol. You can restrict or completely deny the usage of FTP protocol and create shadow copies of transferred files. See more details in "Configuring FTP Monitor Rule" section.

**HTTPS Monitor** controls data exchange through HTTPS protocol. System able to create shadow copies of transferred files. See more details in "Configuring HTTPS 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.

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.

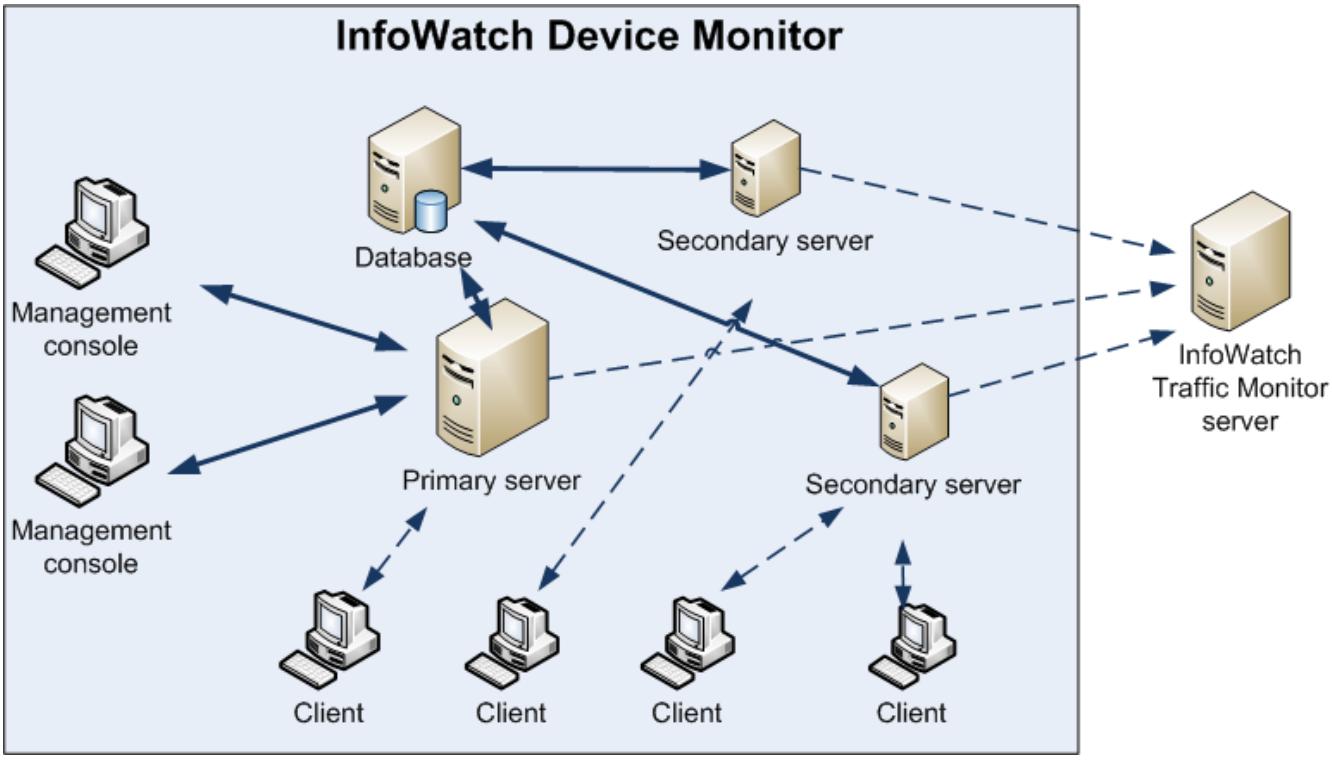
| InfoWatch Device Monitor Feature | Operating system mode |
|---|---|
| Managing access to peripherals (except devices that are unavailable in safe mode) | Safe Mode<br>Safe Mode with Networking |
| Write control on removable devices | Safe Mode<br>Safe Mode with Networking |
| Monitoring managed workstations | 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 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 | Assign |
|---|---|
| InfoWatch Device Monitor Client<br>(InfoWatch device monitor client application, Client) | Intercepting employee actions on managed workstations |
| InfoWatch Device Monitor Server<br>(InfoWatch device monitor server, Server) | Configuring client applications, retrieving data from client applications and sending it to InfoWatch Traffic Monitor |
| InfoWatch Device Monitor Database<br>(database) | Storing critical System data |
| InfoWatch Device Monitor Management Console<br>(Management Console) | System Management |

The following image illustrates System workflow.




The System is deployed and works as follows:

1. **Primary server** is installed first.
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. Use Management Console to configure security schema according to your corporate security policy.
6. Install **Device Monitor Clients** on **workstations**. They connect to any available Device Monitor server, implement and upgrade security schemas, retrieve shadow copies and send them to Device Monitor server.
7. Device Monitor server retrieves updated database versions from security schemas and distribute them over managed workstations. Managed workstations inform server about security schema events and send shadow copies. Events are submitted to the database. Shadow copies are sent to InfoWatch Traffic Monitor.

**Example 1**

1. At the managed workstation 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 workstation 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 workstation. 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 workstation 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 workstation. 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 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 policy** with a set of rules specified for each security policy.
- **Employee groups** registered in Device Monitor. Each employee group must have a security policy.
- **Workstation groups**. Each workstation 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 workstations and accounts are covered by security policy, the System features: default employee group and workstation group.

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
- Workstations and Workstation Groups
- Loading Security Schema to Managed Workstations

# 1.3.1 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 workstation group according to the following principles:

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

  You can't add a new employee group or workstation group without assigning a security policy. The security policy for employee group or workstation 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 workstation group.
- One security policy can be assigned to several employee groups or workstation 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 workstation group.

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

- employee group which the employee belongs to;
- workstation group which include the workstation 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 workstation 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:

- **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.
- **Device Monitor Rule**. Lets you control employee access to selected type of peripherals.
- **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.
- **IM Client Monitor Rule**. Lets you control employee access to instant messengers: Skype, Jabber (XMPP protocol) and Mail.Ru Agent (MMP protocol). 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.
- **Ftp Monitor Rule.** Lets you control data exchange through FTP protocol. You can restrict or completely deny the usage of FTP protocol and create shadow copies of transferred files.

- **HTTPS Monitor** controls data exchange through HTTPS protocol. System able to create shadow copies of transferred files.
  - **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.

## 1.3.2 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* 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**, **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 protocol and set creating shadow copies of all files sent by FTP.

## 1.3.3 Workstations and Workstation Groups

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

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

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

## 1.3.4 Uploading Security Schema to Managed Workstations

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

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

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

If the managed workstation 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 workstation has connected to InfoWatch Device Monitor server, it automatically updates policies and sends shadow copies to server.

# 1.4 Glossary

| Term | Definition |
|---|---|
| **Device Monitor** | InfoWatch Device Monitor client module interceptor. It is designed to control employee access to system peripherals. See: *Interceptor* |
| **File Monitor** | InfoWatch Device Monitor client module interceptor. It is designed to monitor employee activity that involves creating files on removable devices. See: *Interceptor* |
| **FTP Monitor** | InfoWatch Device Monitor client module interceptor. It is designed to control data exchange through FTP 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: Skype, Jabber (XMPP protocol) and Mail.Ru Agent (MMP protocol). 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 Traffic Monitor** | Traffic control system (SMTP, HTTP, ICQ and Lotus Notes). InfoWatch Traffic Monitor analyzes the shadow copies it receives from InfoWatch Device Monitor |
| **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 |
| **Print Monitor** | InfoWatch Device Monitor client module interceptor. It is designed to monitor the activity associated with sending documents to print. See: *Interceptor* |
| **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* |
| **White List** | List of fully accessible devices. See: *Security Polic*y |
| **Database** | See: *InfoWatch Device Monitor database* |
| **InfoWatch Device Monitor database** | Database that contains all InfoWatch Device Monitor information |
| **Employee Group** | Security schema parameter. The group includes employees covered by the same security policy according to the corporate security policy.<br>See: *Default employee group*, *Security policy*, *Employee access level* |
| **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 a employee from all other groups).<br>See: *Employee group*, *Security policy* |
| **Workstation group** | Security schema parameter. Workstation group includes workstations with the same security policy. Workstation groups are formed according to corporate security policy.<br>See:*Default employee group*, *Security policy*, *Employee access level* |

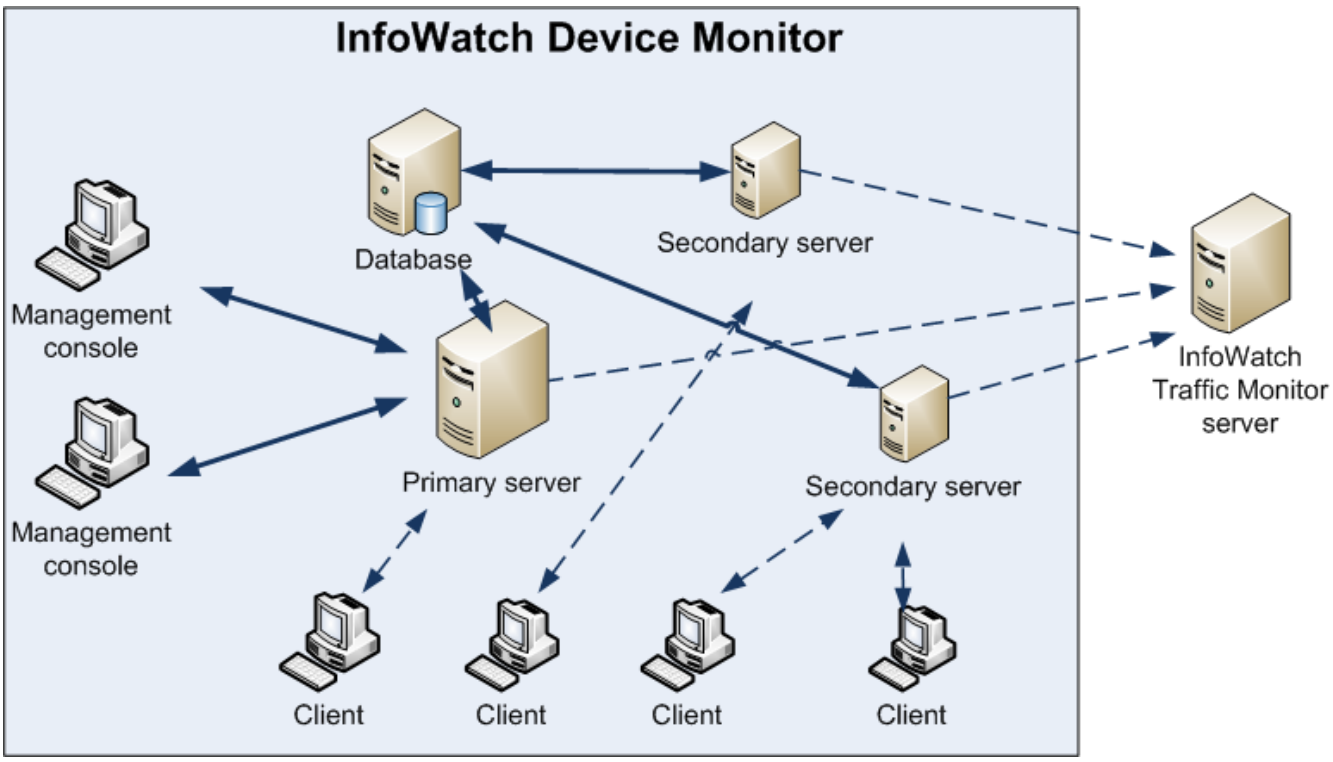
| | |
|---|---|
| **Default workstation group** | Workstation group that is added automatically when you create a new security schema. This group includes workstations that don't belong to any other workstation group (when a new workstation is registered or if you remove a workstation from all other groups).<br>See: *Employee group*, *Security policy* |
| **Log** | System management log of Management Console user.<br>See: *User Activity Log*, *Management Console user* |
| **Client** | See: *InfoWatch Device Monitor Client* |
| **InfoWatch Device Monitor Client** | InfoWatch Device Monitor client module. It is designed to control employee activity |
| **Management Console** | See: *InfoWatch Device Monitor Management Console* |
| **InfoWatch Device Monitor Management Console** | GUI element. It is designed to control InfoWatch Device Monitor (system administration, security schema configuration, etc.) |
| **Managed workstation** | Workplaces that have access to controlled files and peripherals. The InfoWatch Device Monitor Client is installed to managed workstation. |
| **Managed peripheral** | Peripherals (printers, scanners, disk drives, etc.) controlled by InfoWatch Device Monitor. Access to peripherals is based on corporate security policy |
| **Controlled file** | File that is controlled by InfoWatch Device Monitor. Controlled files list is based on corporate security policy |
| **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 workstation groups |
| **Local administrator** | Management Console role which manages accounts |
| **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 |
| **Security officer** | Management Console role which manages security policy and configures InfoWatch Traffic Monitor server connection |
| **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.<br>See: *File Monitor*, *Device Monitor*, *Print Monitor*, *IM Client Monitor, FTP Monitor, HTTPS Monitor, Network Monitor*. |
| **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* |
| **Employee** | Any user registered in InfoWatch Device Monitor as an employee. Employee actions are monitored by client modules installed at workstations. |
| **Management Console user** | User who manages InfoWatch Device Monitor. Each user has a role assigned basing on corporate security policy. |
| **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* |
| **Workstation** | In terms of InfoWatch Device Monitor system, a workstation is a managed workstation. See: *Managed Workstation* |
| **Rendering print jobs** | Rendering process that converts a print job into printing data. |
| **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* |
| **InfoWatch Device Monitor Server** | InfoWatch Device Monitor Server module. It is designed to monitor managed workstations and interact with InfoWatch Traffic Monitor. |
| **DBMS** | Database management system. |
| **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.<br>See: *Employee group*, *Workstation group*, *Security policy* |
| **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. |
| **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. |
| **Employee access level** | Employee security policy set. In other words, security policies assigned to:<br>• employee's groups;<br>• workstation groups that include the workstation. |
| **Windows account** | Employee's Microsoft Windows account. Account credentials are used for InfoWatch Device Monitor registration. |
| **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). |

# 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. You can manage all servers in cluster from Management Console.

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 workstation 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

## 2.1.1 Database

InfoWatch Device Monitor supports the following DBMS:

- Oracle Database 11;

> **Warning!**
> If you install System to the server OS with 64-bit processor, you should use 64-bit Oracle Client application.

- Microsoft SQL Server 2005, 2008, 2012 (Express, Developer, Workgroup, Standard, Enterprise).

## 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 SP 2 (x86, x64);
  - Microsoft Windows Server 2008 (x86, x64);
  - Microsoft Windows 2008 R2 (for x64 systems only);
  - Microsoft Windows Server 2012.
- DBMS client:
  - Oracle 11g R2.
- Microsoft .NET Framework 2.0 Service Pack 1.

> **Warning!**
> Before getting to work, add Server to Active Directory domain.

InfoWatch Device Monitor Server hardware requirements meet minimum OS requirements. Moreover:

- Hard disk free space shouldn't be less than 120 MB.
- You should have 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")\

## 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 7 SP1 (x86, x64);

- Microsoft Windows Vista SP2 (x86, x64) with all updates;
- Microsoft Windows XP SP3 (x86, x64) with all updates;
- Microsoft Windows 8 (x86, x64);
- Microsoft Windows 8.1 (x86, x64).

**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 malfunction, operating system and/or data damage (up to complete data destruction)..

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

- Motherboard must provide USB hardware support;
- Minimum free hard disk space is 300 MB.

**Note:**
When installed applications load CPU and RAM, the following configuration is recommended for flawless system performance:

- CPU Intel Core i3 или аналогичный;
- RAM 4 Gb;
- HDD 50 Gb.

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

InfoWatch Device Monitor Management Console hardware requirements meet minimum OS requirements. Minimum free hard disk space is 30 MB.

## 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.

Database is managed through InfoWatch Device Monitor Microsoft SQL Server, Oracle, PostgreSQL DBMS or integrated database.

Management Console connects to the main 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 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` files, 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.

File record example `tnsnames.ora`:

```
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 must 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.

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 authentication** for database owner (see "Database deployment under Microsoft SQL Server DBMS"), while database and Server are on separate computers,

select **User** variant. This rule applies even when you don't need remote Client installation.

**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 "InfoWatch Device Monitor 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 Installation 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.

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**.

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 appropriate version of Device Monitor database, deselect **Install new database** option.

Click **Next**.

### Step 5. Selecting database server

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

- Microsoft SQL Server
- Oracle

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

Click **Next**.

### Step 6. 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.

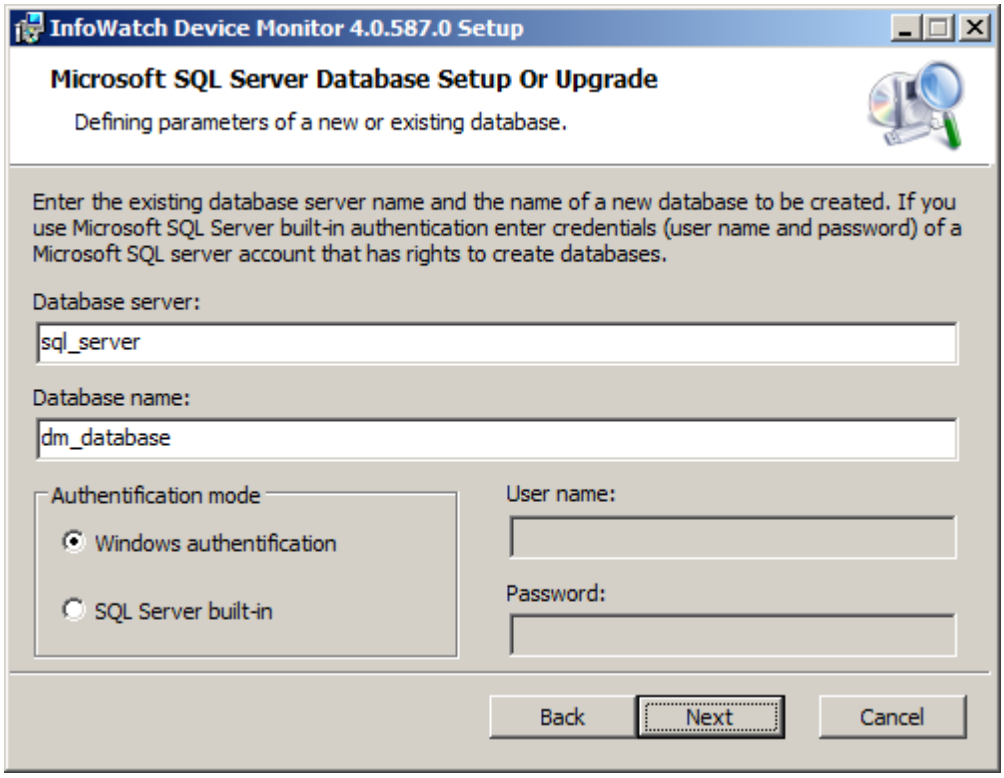
  If there are any named instances on the database server, specify server name as follows: `<server_name>\<instance_name>`.
- **Database name**. New database name.

  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:

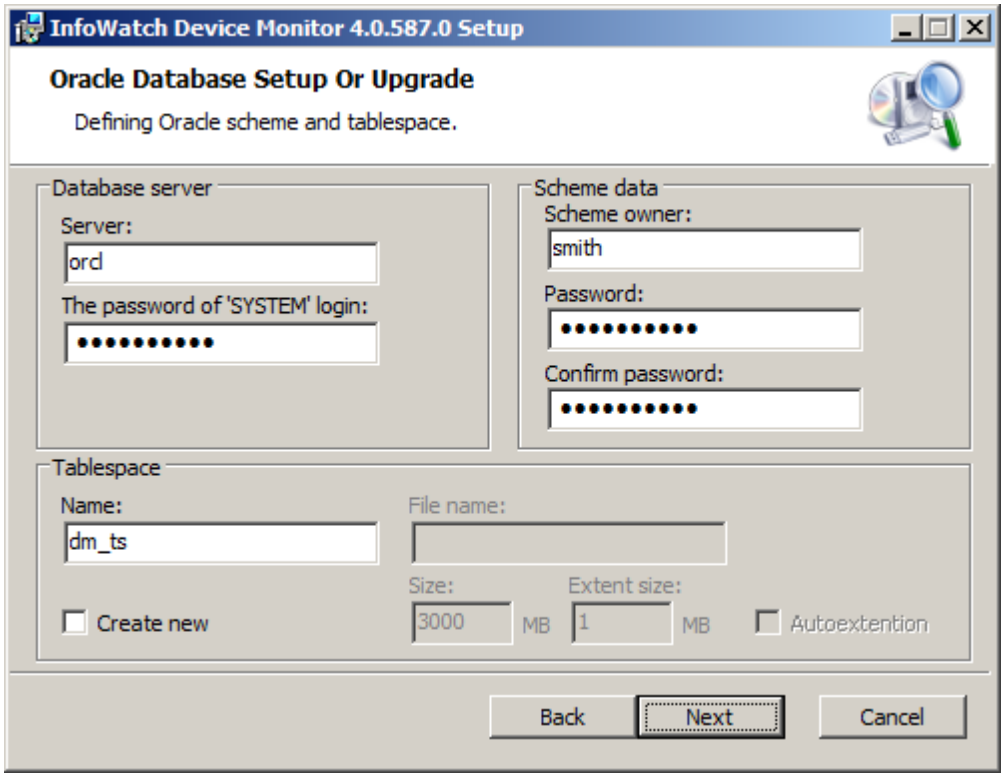
   **Warning!**
   It is not recommended to use existing database scheme settings.

   - **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

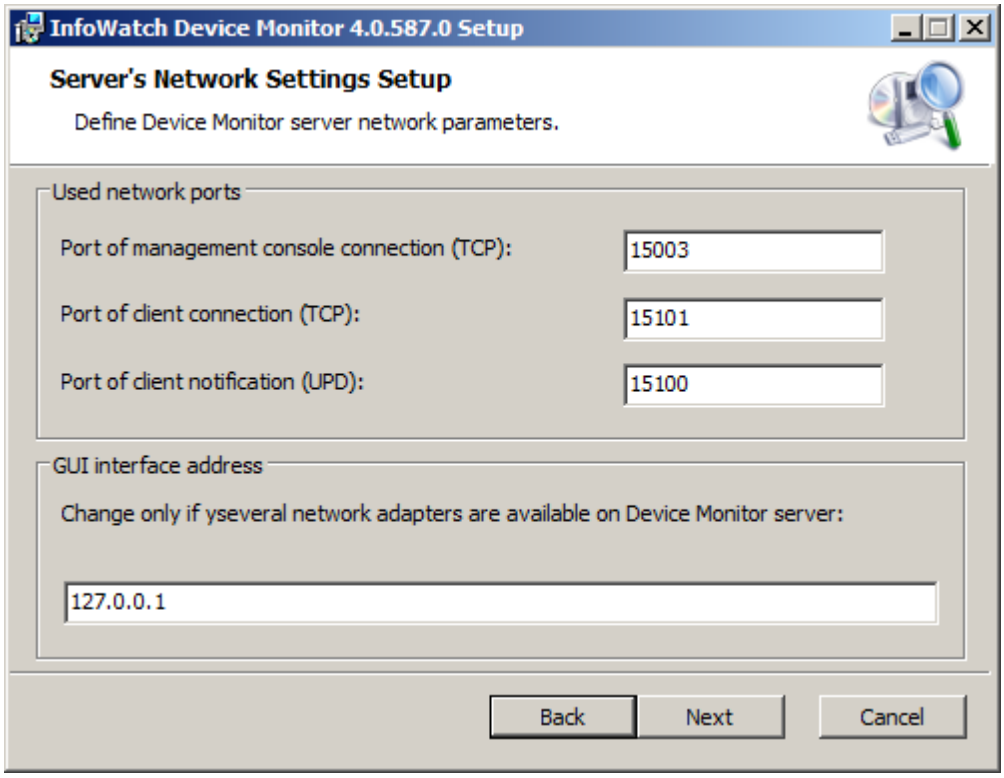
After all necessary parameters have been configured, click **Next**.

## Step 7. 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 8. 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 9. 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 "Management Console Accounts Administration"): it is used when you first connect to the server from Management Console.

Click **Next**.

### Step 10. Configuring InfoWatch Traffic Monitor connection parameters

Specify InfoWatch Traffic Monitor interaction options:

- **TM server address**. InfoWatch Traffic Monitor server address. Interaction with Traffic Monitor Server is carried out according to *xml* scheme. Address must be entered in the following format:

  ```
  xml://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.
- **Number of connections**. Number of InfoWatch Traffic Monitor server connections. You can specify from 1 to 32 connections.

- 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 11. Completing the installation

Click **Install** to start Server installation. Follow the instructions to complete installation.

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

# 2.3 InfoWatch Device Monitor Client Setup

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

- Local setup. It uses the Setup Wizard on each workstation.
- 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.

**Warning!**
For InfoWatch Device Monitor Client proper operation you must ban simultaneous workstation use. To fulfill this requirement, Client allows only one user session; other sessions are blocked until the active session has been completed. This may block quick user switch function (Fast User Switching) and terminal access to managed workstation.

## 2.3.1 Standard Client Setup

**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 workstation, 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 Setup 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 setup 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

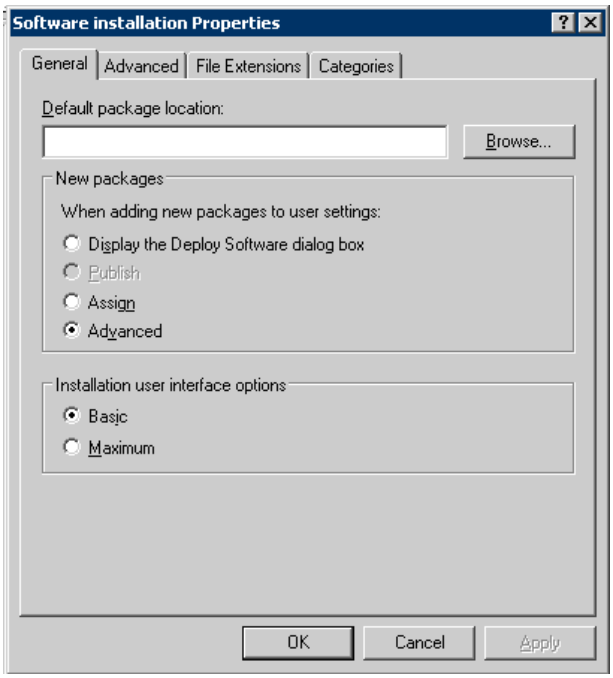
Edit group policy before installing Client from Active Directory.

**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**.

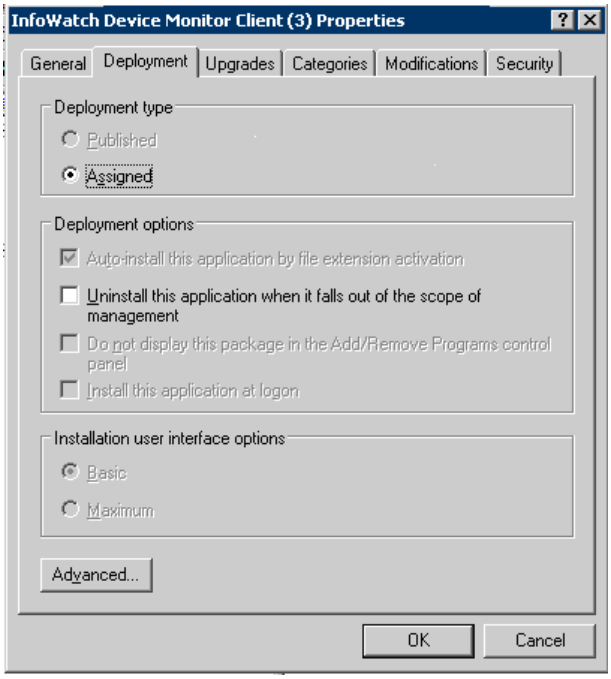



6. When the configuration is complete, click **OK**.

## 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 workstation 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: http://support.microsoft.com/kb/840669/ru.

# 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.

| Configuration section | Description |
|---|---|
| <configSections> | Service section. Describes all remaining sections.<br>You should not edit this section. |
| <runtime> | Contains Microsoft .NET framework environment settings. These settings are required for correct Server operation.<br>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).<br>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. |

## 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.><br>Server kernel configuration | |
| RemotingPort | TCP port processing Management Console service connections.<br>Default value 15003 (it is not recommended to change this value) |
| CultureName | Language of module diagnostic and other messages.<br>Possible values:<br>• ru-RU<br>• en-US |
| MachineName | IP address of network interface used by the Server to accept Management Console connections.<br>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 address used by the Server to accept incoming connections from different instances of Management Console |
| CheckServerSettingsInterva | 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.<br>Default value 10 |
| <InfoWatch.DeviceMonitor.Server.Database.Properties.Settings><br>Settings of the module interacting with the database | |

| Parameter | Description |
|---|---|
| DatabaseType | Database types.<br>Possible values:<br>• Oracle<br>• Microsoft |
| ConnectionString | Database connection string. It must comply with ADO.NET connection string rules.<br>For example:<br>Data Source=isis\s2005;Initial Catalog=g1228_9;Integrated Security= |
| CultureName | Language of module diagnostic messages and other messages.<br>Possible values:<br>• ru-RU<br>• en-US |
| ConnectionPoolSize | Number of DB connections to open and use by server.<br>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.<br>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.<br>Default value 60 |
| <InfoWatch DeviceMonitor.Server.Gui.Properties.Settings.><br>Management Console interface module configuration | |
| CultureName | Language of module diagnostic messages and other messages.<br>Possible values:<br>• ru-RU<br>• 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><br>Client connections module configuration (managed workstations) | |
| Backlog | Pending client connections queue. Default value 128 |
| CultureName | Language of module diagnostic messages and other messages.<br>Possible values:<br>• ru-RU<br>• en-US |
| ShadowCopyTempDir | Full path to temporary shadow copies pending submission to InfoWatch Traffic Monitor.<br>Default value:<br>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:<br>• AllAny - all ports of IP addresses available for the computer (default value);<br>• AllIp4 - ports of all version 4 IP addresses;<br>• AllIp4 - ports of all version 6 IP addresses. |
| Dmpv1TraceLevel | Client-Server protocol trace level.<br>Possible values: |

| Parameter | Description |
|---|---|
| | • 1 - turn tracing off (default value);<br>• 2 - only trace packet information;<br>• 3 - complete tracing. |
| 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.<br>Default value 200. |
| Dmpv1ConnectionsQueueLimit | Max number of connections awaiting for processing. If the number excesses, connections are reduced to Dmpv1ConnectionsQueueLengthAfterCut parameter value.<br>Default value 500. |
| Dmpv1ConnectionsQueueLengt | Number of connections after queue reduced because of max size excesses.<br>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.<br>Default value 120. |
| <InfoWatch.DeviceMonitor.TrafficMonitor.Connector.Properties.Settings><br>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.<br>Possible values:<br>• ru-RU<br>• en-US |
| NumberOfConnections | Number of InfoWatch Traffic Monitor connections.<br>Normal value 4. Maximum value 32 |
| QueueSendLimit | Maximum number of events transferred from database to InfoWatch Traffic Monitor in a single transaction.<br>Default value200 |
| <InfoWatch DeviceMonitor Database.Core.Properties.Settings><br>Low-level database driver configuration | |
| CultureName | Language of module diagnostic messages and other messages.<br>Possible values:<br>• ru-RU<br>• en-US |
| MaxConnectionWaitingTime | Standby time for free connection from pull in seconds. Default value is 150 |
| CommandTimeoutSeconds | Time of the operation or the request in seconds. Default value is 30<br>**Note:** described parameter couldn't be used for work with Oracle DBMS. |
| LongCommandTimeoutSeconds | Time of long-drawn-out operation or the request in seconds. Can be useful when the runtime is a long period. Default value is 0 (infinite).<br>**Note:** described parameter couldn't be used for work with 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").

`<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.

# 2.5 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.

## 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 version 4.0, updates use standard procedure.

### 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. 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.

**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 3. 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.

> **Note:**
> **Management Console** component can be installed and updated apart from the **Server** component. Installation package overwrites installed version with the new one without any additional action on user side.

# 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.

# 2.6 Uninstalling InfoWatch Device Monitor

**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 **Add or remove programs** from Windows Control Panel, select **InfoWatch Device Monitor Server** 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").
4. After specifying the parameters 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".

### 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

Management Console is designed to address the following tasks:

- access to InfoWatch Device Monitor;
- configuring workstations monitoring system;
- workstations 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).
- Management Console User Administration . 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. Working with external devices and data transmitting channels at managed workstations.
- 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).

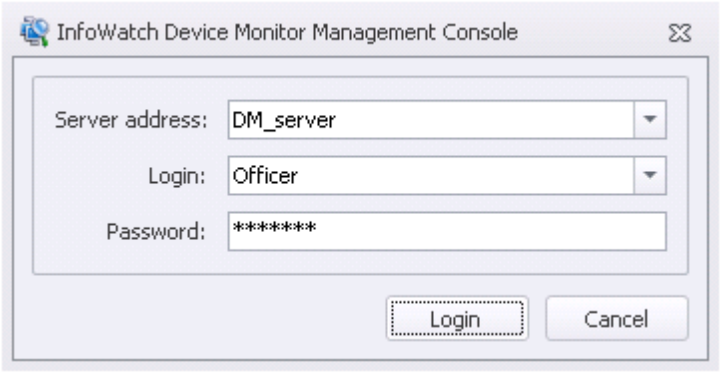
**To get started with Management Console:**

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.<br>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 | Username |
| Password | User password.<br>Check the keyboard layout before entering your credentials. |

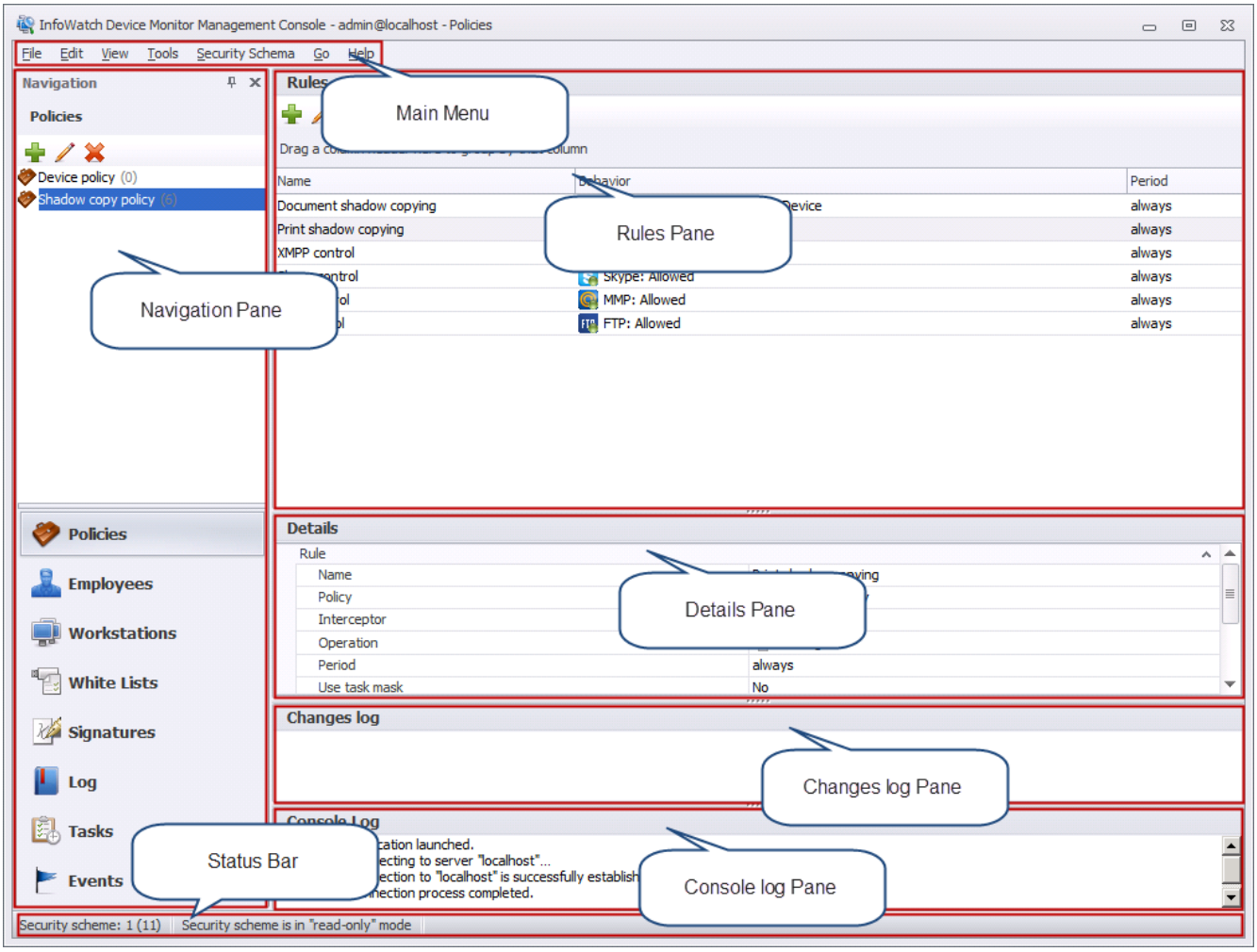
First launch of Management Console **Logon** dialog fields are empty. Later, **Server address** and **Login** fields will contain the credentials entered during the previous authorization attempt. You must fill the **Password** field each time you are trying to log in.

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 >** **Disconnect**, 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.
- **Toolbar** contains shortcuts to some of the Management Console 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.
- **Details** pane displays element's properties.
- **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 **Workstations** 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.<br>or<br>• 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

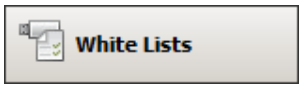
Management Console includes the following sections: **Policies**, **Employees**, **Workstations**, **White Lists**, **Signatures**, **Log**, **Tasks** and **Events**. Each section corresponds to similar Navigation panel area.

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**, **Workstations**, **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 managed workstations events. 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 |

| Section icon and name | Section assignment |
|---|---|
|  | Workstations management: creating workstation groups, adding managed workstations to groups |
|  | Managing white lists of fully accessed devices. |
|  | View and manage signature categories that assign File Monitor rules to certain file formats. |
|  | Security schema management activity log (logging administrating responsibility zones and configuring security schema) |
|  | InfoWatch Device Monitor Clients centralized installation, updating, and uninstallation on workstations |
|  | Viewing information on employee activities at managed workstations using controlled means |

# 3.2 Management Console Accounts Administration

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 | + | | + |

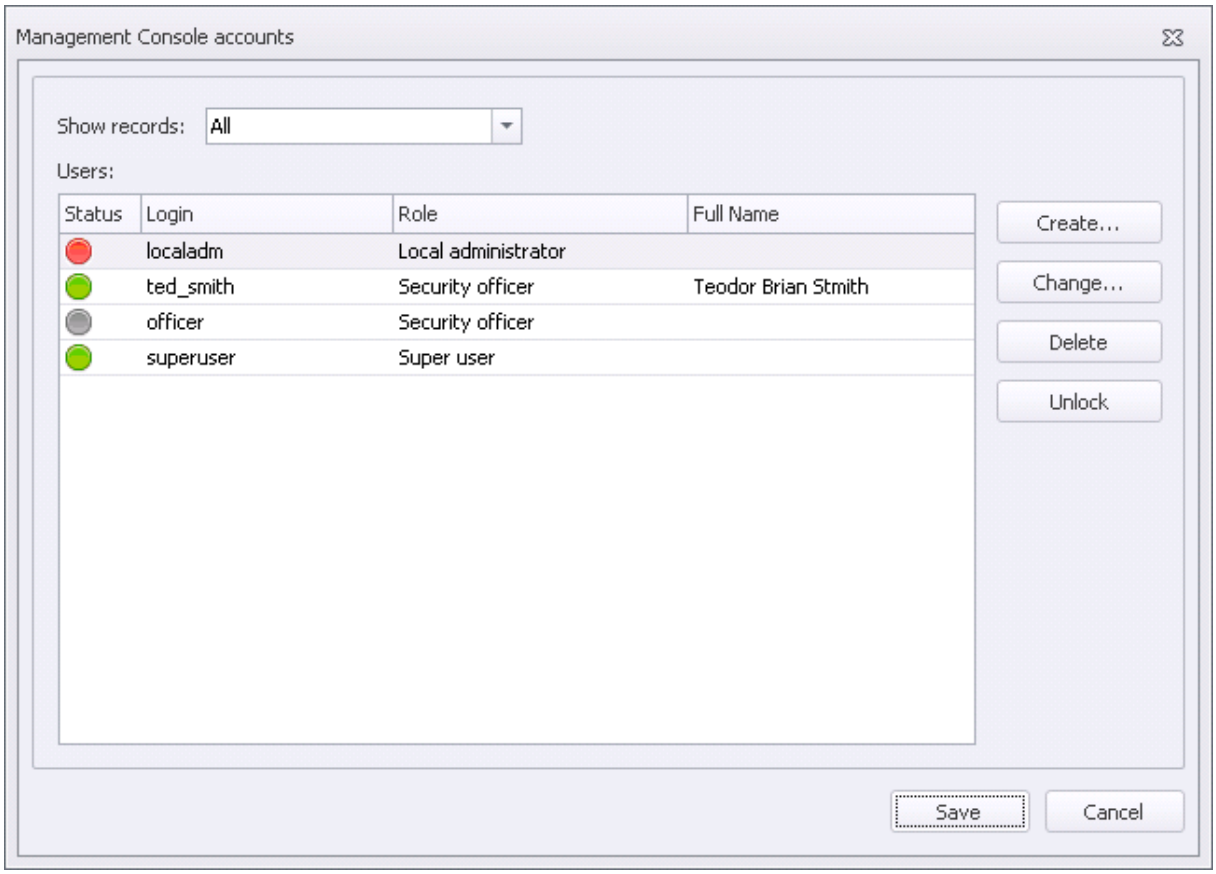
For more information on Management Console accounts management, see:

- 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:

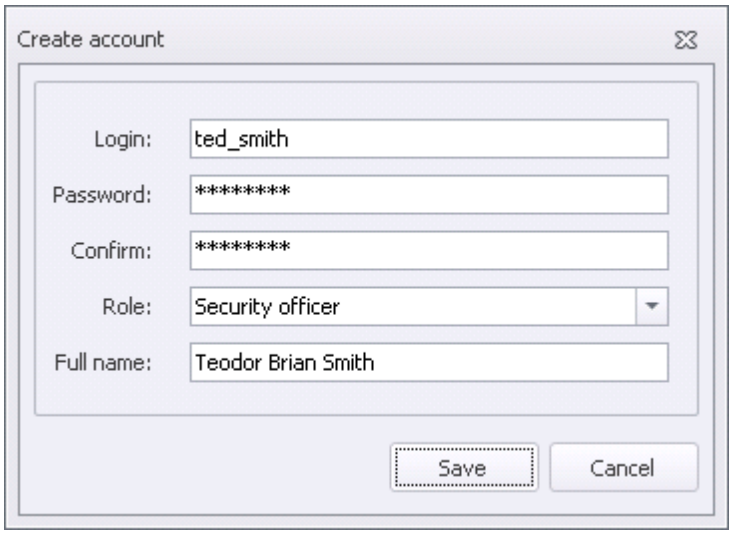
- **Status**. Indicates is an account is active ( ), blocked ( ) or deleted ( ).
- **Login**. Login.
- **Role**. Account role.
- **Full Name**. User's personal data.

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**
- **Password**, **Confirm Password**
- **Role**. Role assigned to your 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**.
   After this **Create account** dialog box will be closed. 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 t**o 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 section "Adding New Management Console Account").
5. After all necessary settings have been configured, click **Save**.
6. To apply changes, click **OK** 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.<br>**Selector** values interpretation is available 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 |

| Property | Description |
|---|---|
| User | Name of Management Console account that initiated the transaction |
| Windows account | Account with credentials for Windows authorization |
| Workstation | Name of the workstation that initiated the action |
| Sequence number | Record number in the database |

Piece of information, on **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 workstation 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 workstation 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

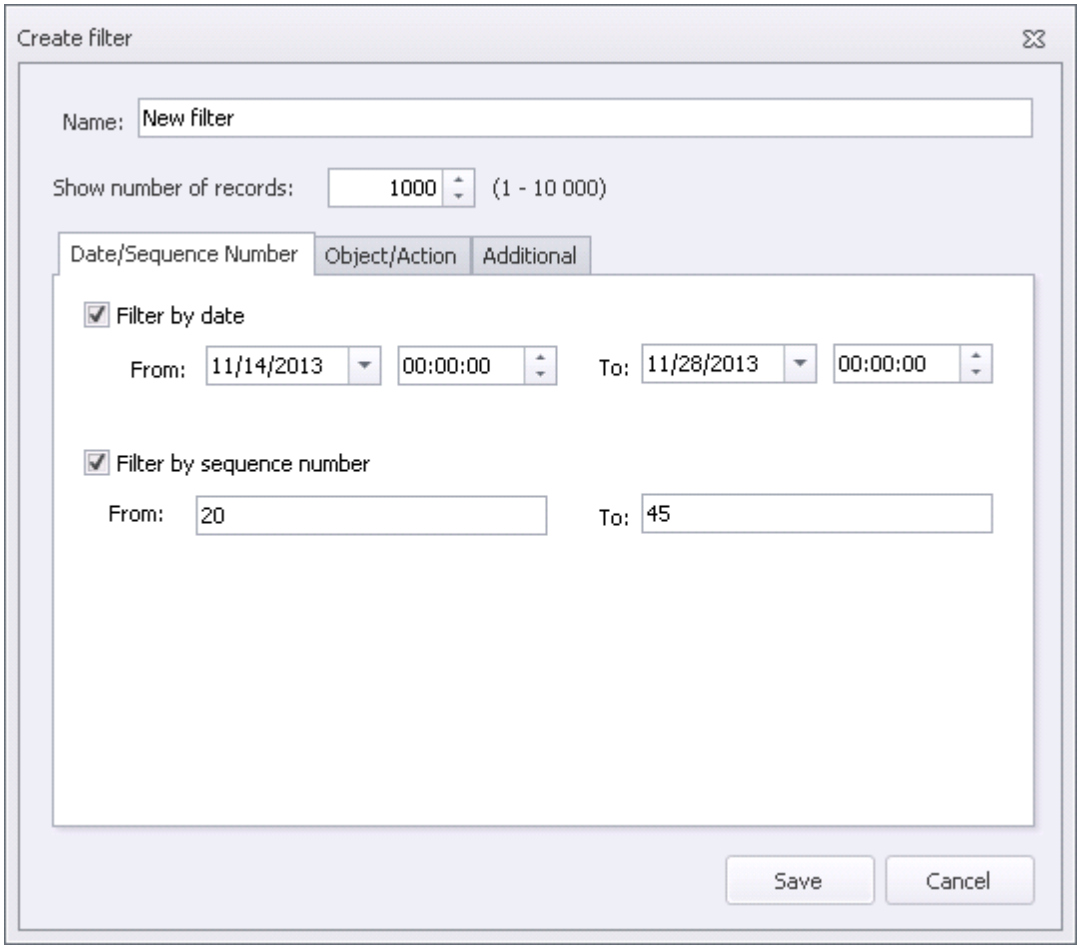
Records related to Management Console users activities that change database information (security schema customization, System administration) are stored in the Audit Log. To access Audit Log records that meet certain criteria you can use filters.

**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**;<br>• 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.<br>2. Take one of the following steps:<br>• In Main Menu click **Edit > Edit filter**;<br>• click **Edit Filter** at the top of Navigation pane.<br>• double-click selected filter name. |

These actions open 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:**

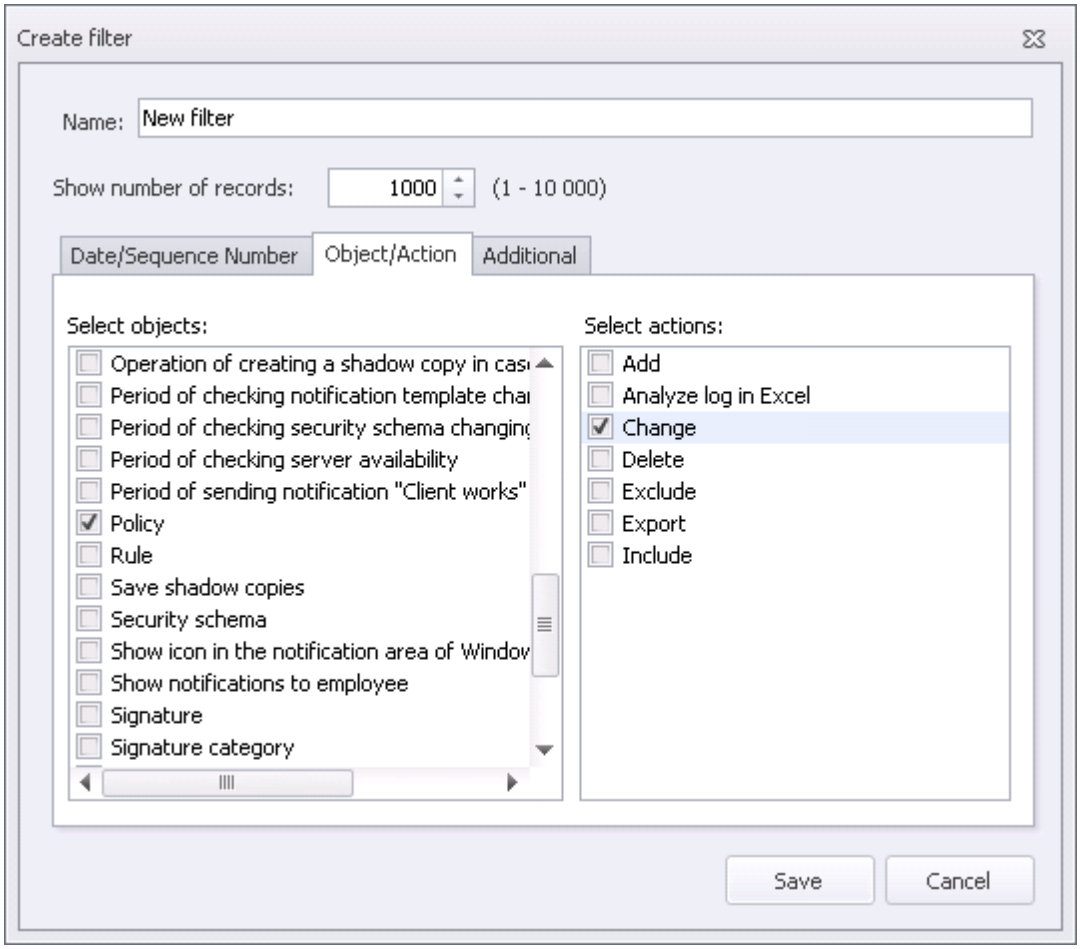
1. Flag **Filter by sequence number** check box.
2. Specify range of numbers in **From** and **To** fields respectively.
   Database record numbers start from 1.

# 3.2.6.2.2 Object/Action Tab

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

- target object;
- action performed.

**Warning!**
When combining object and action filtering criteria, only specify the actions that affect the object. For example, you can Add, Change or Delete an Account, or Include, Exclude, or Delete a Workstation. List of objects and actions is available in "Selector Values".




**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.
- **Workstation**. Display selected workstation 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

**Warning!**
Modified settings will apply at managed workstations after Clients at every workstation 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. workstation 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. workstation 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 workstation: when it is reached, shadow copies would not be created. I.e. if when shadow copy is created, free disk space at a client workstation 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 disk space the operation will | The managed workstation dedicates space for storing 30000 events 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/workstation, then any actions controlled by security schema could be denied. To deny, select **Operation is blocked**. To allow all actions performed without a |

| Parameter | Description |
|---|---|
| | control, select **Operation is allowed**. |
| **Events** | |
| Event's detailisation level of Device Monitor | Level of detailing when saving information about working with external devices received by Device Monitor interceptor: see details in "Configuring Device Monitor Rule" and "Viewing Events". The following options are available:<br>• **None** - do not save events<br>• **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<br>• **All** - all actions are logged (connection/usage of any devices, even from white lists) |
| Event's detailisation level of Network Monitor | 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:<br>• **None** - do not save events<br>• **Access denied** - events are created only if security policy violation is attempted - i.e. when connection attempt was denied. |
| **Employee notification** | |
| 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" |
| Show tray icon interface | Indicates if Windows system tray of managed workstation displays  icon. By clicking at this icon, an information on DM Client operation and list of currently controlled devices is displayed. |

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

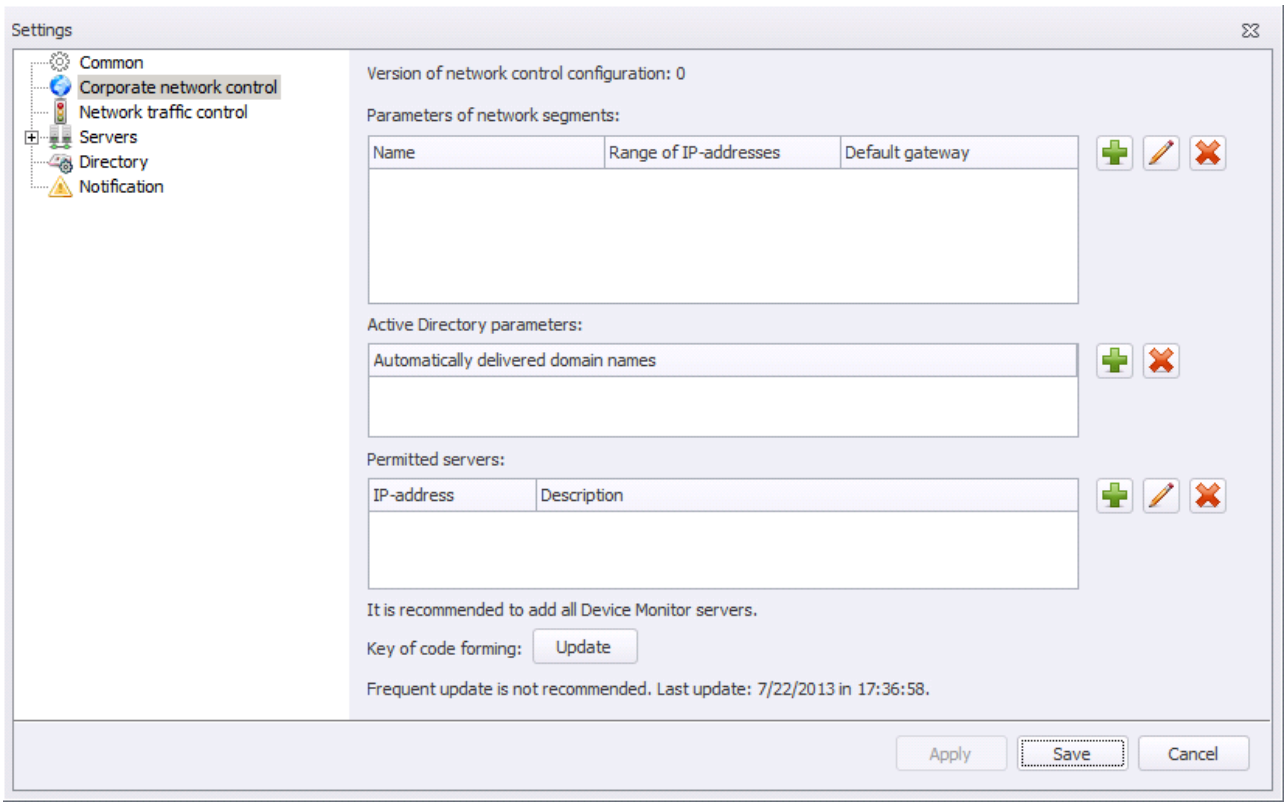
# 3.3.2 Settings of Corporate Network

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.

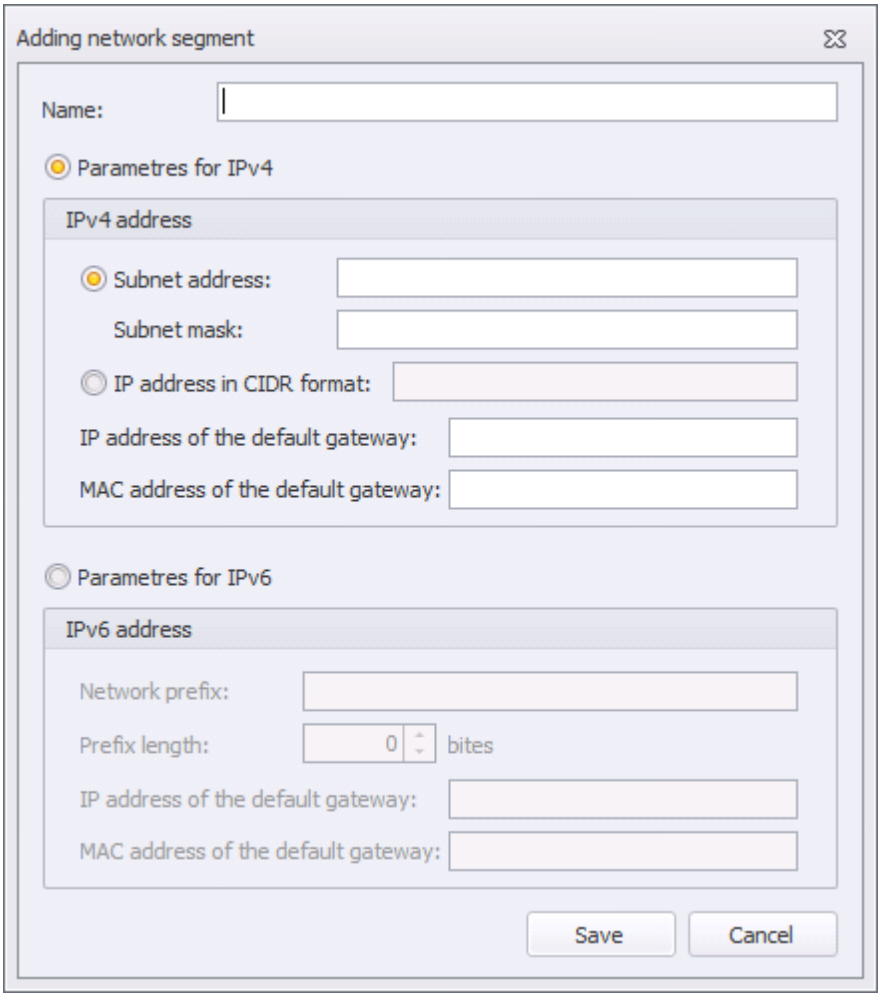
**To configure corporate network settings:**

1. In the Main Menu select **Tools > Settings**.
2. At the left panel select **Settings of corporate network** 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.

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**.

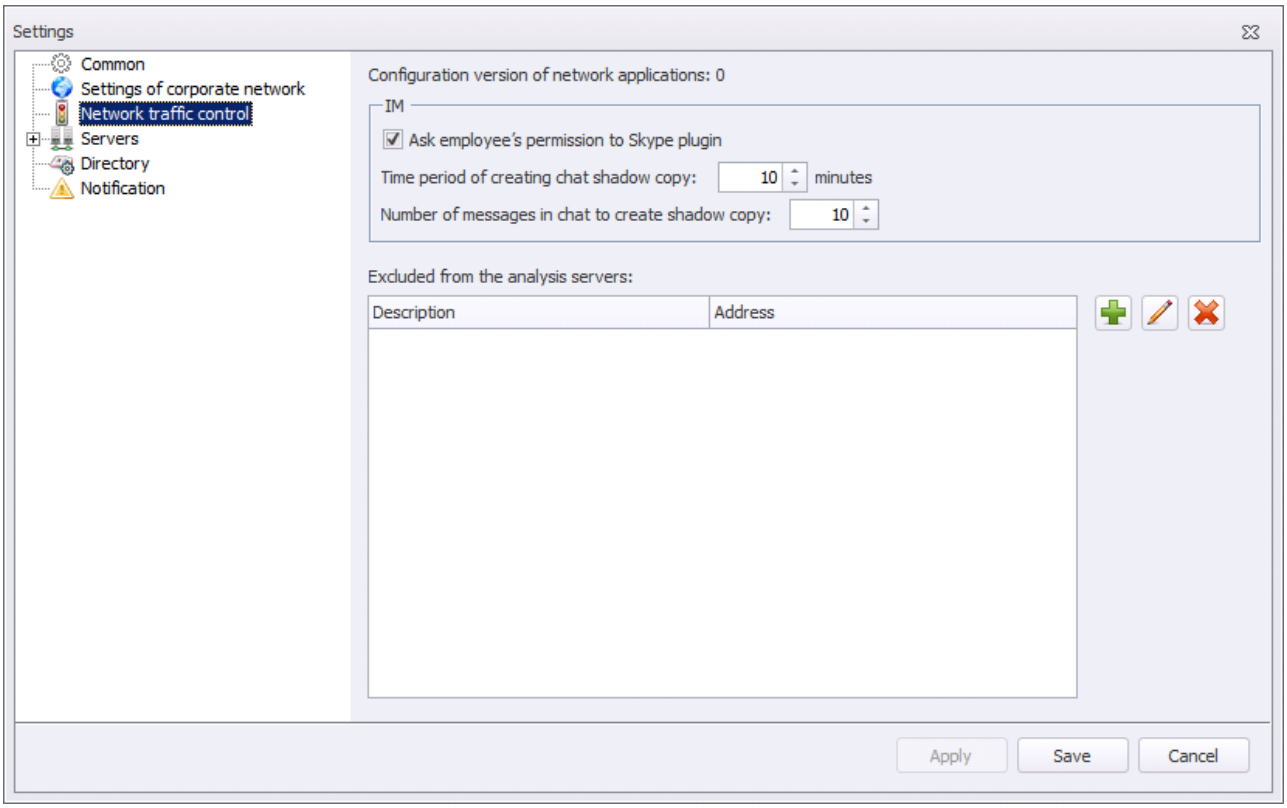
# 3.3.3 Network Traffic Control

In order to provide a control of network traffic transferred through XMPP, MMP and FTP protocols, 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. If data stream is protected with TLS\SSL protocol then proxy server performs "Man in the middle" attack to open 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") and FTP 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:
   - If you want that after Client installed, the employee would be requested a permission for interceptor work , then flag **Ask employee's permission to Skype plugin**. If this field is not flagged, then employee's confirmation to launch interceptor is not required.

     **Warning!**

     To allow Skype control, employee should enter Skype menu: **Tools -> Options -> Advanced -> Manage other programs' access to Skype**, select **DM.Client.exe** application, click **Change**, select **Allow this program to use Skype** option and click **OK**.
     - If the employee agrees to launch interceptor, it will work until employee won't disable it in Skype menu. In the latter case, Skype will be forced to stop.
     - If the employee blocks the interceptor, Skype will be stopped. If the the tries to start Skype later, he will be prompted to give another permission to use interceptor.
   - 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, and 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.
   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**.

**Warning!**

If you use Yandex Disk software and Device Monitor on one computer, you should add the following servers to the excluded from the analysis servers list:

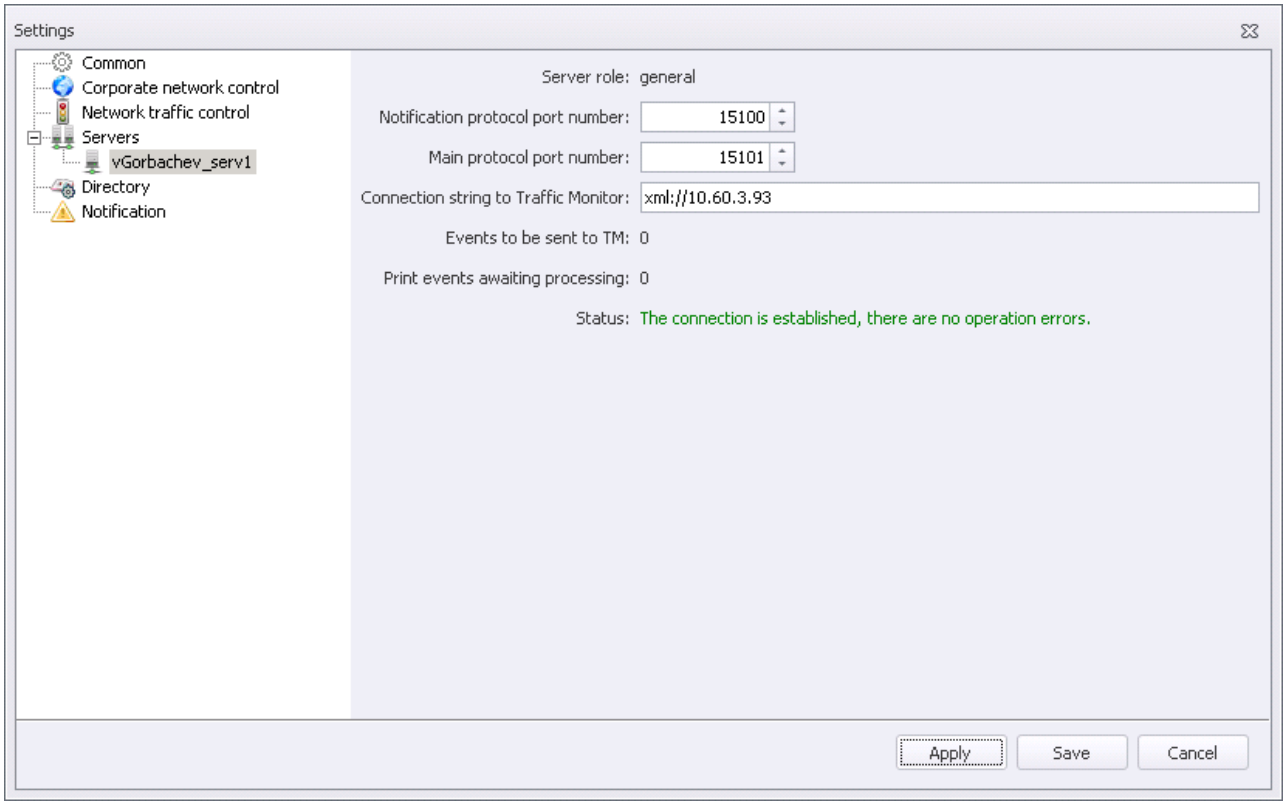
- oauth.yandex.ru;
- webdav.yandex.ru;
- clck.yandex.ru;
- push.xmpp.yandex.ru.

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

In order InfoWatch Device Monitor to be able to send events to InfoWatch Traffic Monitor, configure its server connection.

**To display and configure InfoWatch Traffic Monitor connection settings:**

1. In the Main Menu select **Tools > Settings**.
2. At the left panel select **Servers** node, then select server's 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, Step 4.
- **Events to be sent to TM** - statistics of events pending submission to InfoWatch Traffic Monitor.
- **Print events awaiting processing** - statistics of print events pending submission to be processed.
- **Status -** Traffic Monitor connection state.

3. You can change the following settings:

- **Notification protocol port number**
- **Main protocol port number**

> **Warning!**
> Protocol port changes will apply only after service restarted.

- **Connection string to Traffic Monitor** - InfoWatch Traffic Monitor server address that will receive events. Interaction with Traffic Monitor server is based on *xml scheme*. Address must be entered in the following format:

  ```
  xml://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.

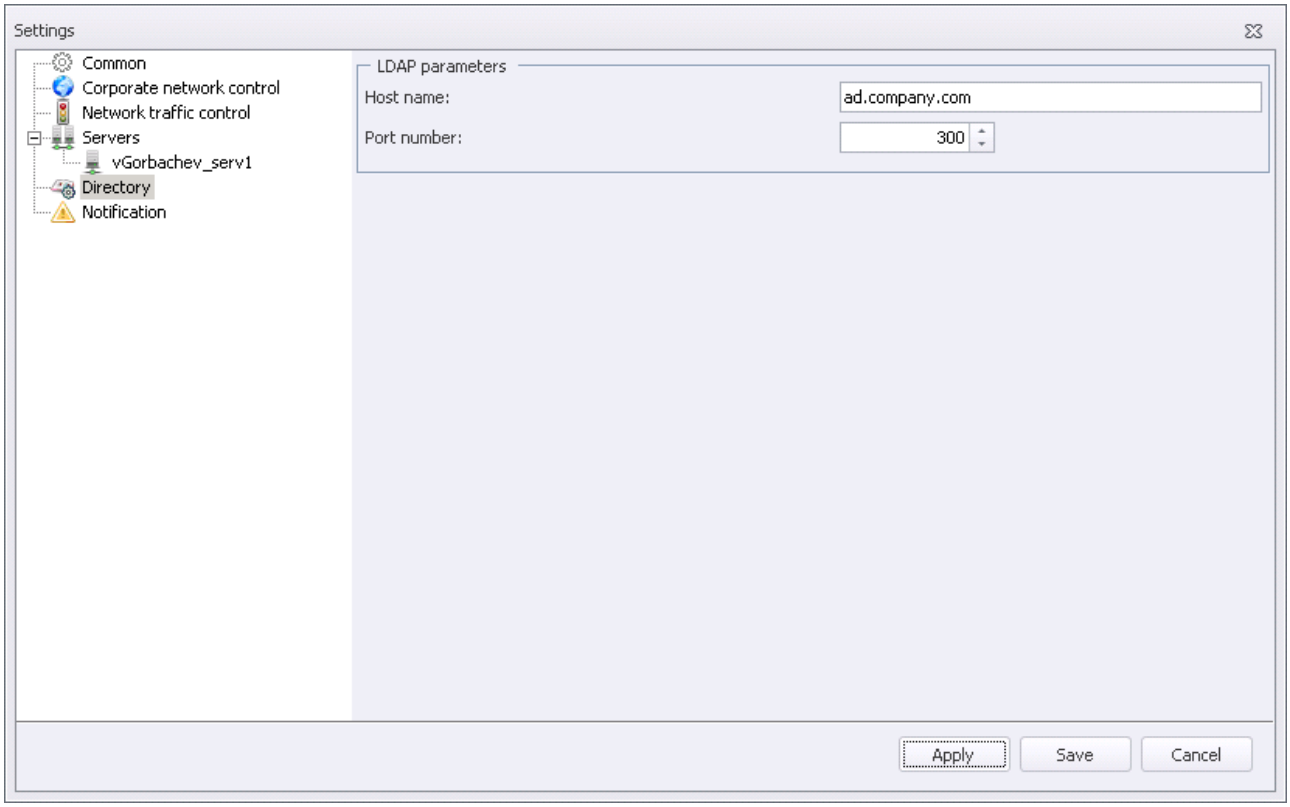
4. When all changes are made, click **Apply**.

## 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 300(**389**) is unavailable.




5. Click **Apply**.

# 3.3.6 Employee Notifications about Policy Violations

When an employee working at managed workstation 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/XMPP/MPP/Skype protocol (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.
- **Skype forbidden, because the employee prohibited Skype plugin** – IM Client Monitor rule which controls Skype usage (see "Configuring IM Client Monitor Rule" and "Network Traffic Control", **Ask employee's permission to Skype plugin** option) was actuated.
- **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. Detailed** – 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").

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

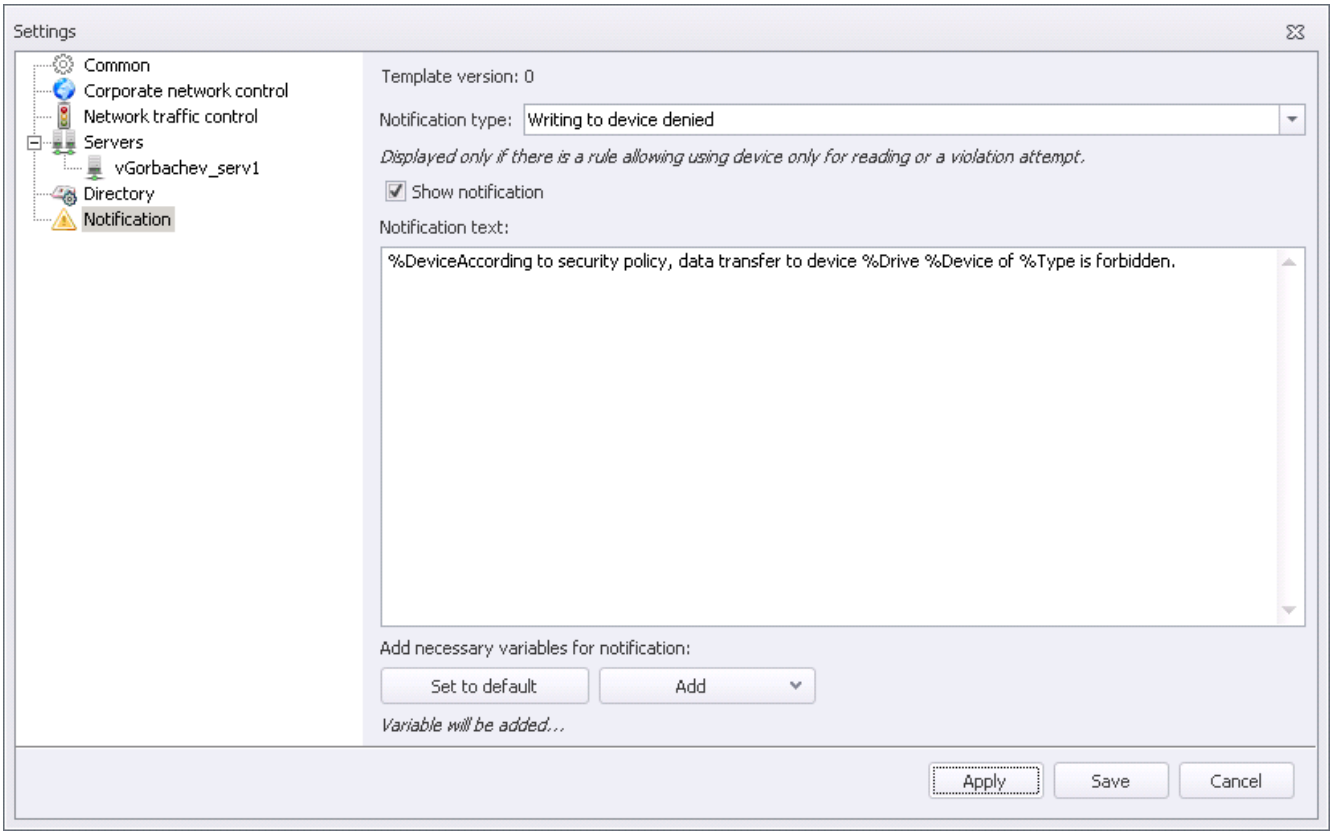
1. In the Main Menu select **Tools > Settings**.
2. At the left panel select **Common** node.
3. Deselect **Show notification** to disable showing notifications for employees, or flag it to enable notifications.
4. Click **Apply**.

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:**

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 clock **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 **Apply**.

# 3.4 Managing Security Schema

General information on the InfoWatch Device Monitor security schema is provided in "Security Schema Organization" section.

Operation procedures for security schema managing is provided in the following sections:

- Security Schemas Overview
- Security Schema Setup
- Temporary Employee Access

## 3.4.1 Security Schemas Overview

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 Schema

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

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

## 3.4.1.1 Viewing Active Security Schema

Active security schema is displayed on Management Console by default.

Security schema configuration information is displayed in **Policies**, **Employees**, **Workstations**, **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 workstation group |
|  | Workstation group |
|  | Default employee group |
|  | Employee group |
|  | Default signature category |
|  | Signature category |
|  | Devices white list for employee |
|  | Devices white list for employee group |
|  | Devices white list for workstation |
|  | Devices white list for a group of workstations |
|  | Audit log filter |
|  | Security policy |

**To view 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").

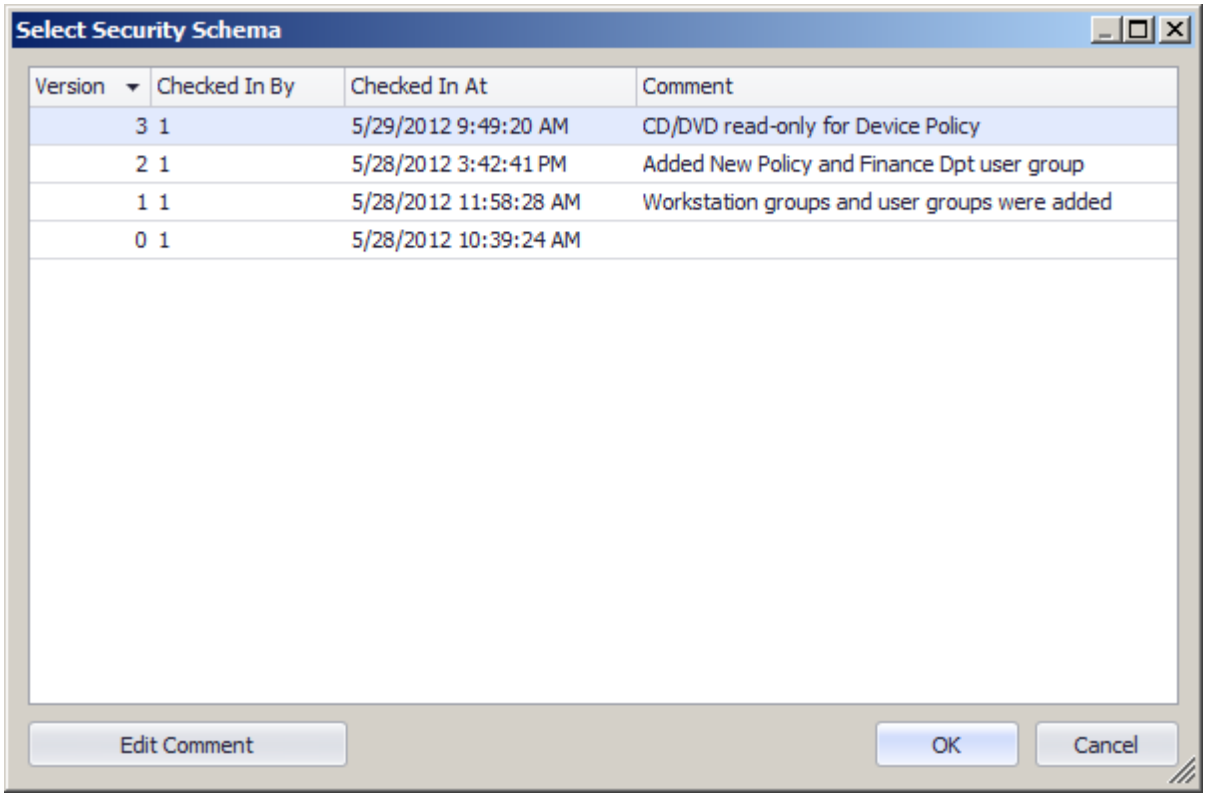
## 3.4.1.2 Viewing Old Security Schema

**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 Latest Security schema** in the Main Menu.

## 3.4.1.3 Security Schema Comments

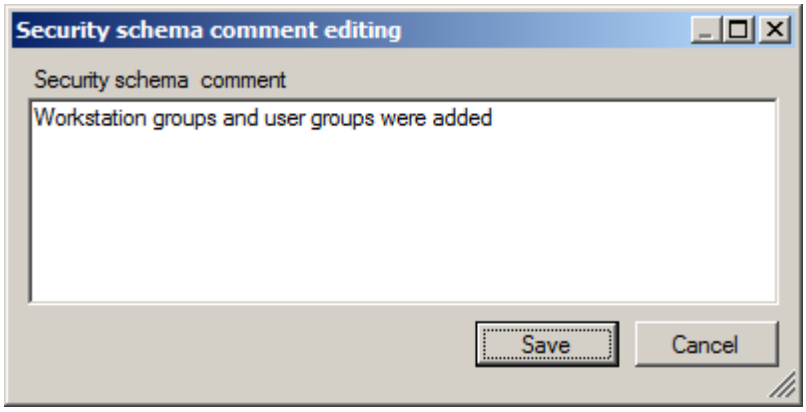
In comments you can specify additional information on your security schema. You can add comments to each version of security schema.
Comments to current security schema are displayed in brackets to the right from schema version number on the status panel.
You can view comments to all security schema 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.

   **Note:**
   For line break, press **<ENTER>** or **<CTRL>+<ENTER>**.

3. Click **Save**.

## 3.4.1.4 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 workstation 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, workstations, 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, **Save** command is not available when viewing previous versions. To open current security schema version, open **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")
   - workstation groups (see "Workstations")
   - employee accounts lists (see "Employees")
   - device white lists (see "White Lists")
   - file signature categories (see "Signatures").
3. When all changes are made, save your security 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, select **Security Schema > Undo editing** or click **Undo editing** button on the toolbar. This closes schema editing mode discarding all changes.

## 3.4.1.4.1 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 workstation 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, workstations, 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 in "read-only" mode***".

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**.

All unsaved changes will be lost.

### 3.4.1.5 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 workstation;
- 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.

### 3.4.1.6 Exporting/Importing Security Schema

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

Exporting security schema saves to XML file the current version of a security schema including:

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

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

**To export security schema:**

1. In the Main Menu select **Security Schema > Export**.
2. In the next dialog, enter a name of the XML file where your data will be exported and specify a directory for the file. After choosing the file name and directory click **Save** .

**To import security schema:**

1. In the Main Menu select **Security Schema > Import**.
2. In the next dialog choose the XML file that contains security policies and sets of rules 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.

## 3.4.2 Security Schema Setup

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

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

Security schema configuration principles:

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

**Adding workstations to security schema**

There are two ways to add a managed workstation:

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

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

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

**Adding employee accounts to security schema**

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

**Adding white lists to security schema**

Before you create a white list, add device models and instances to the database. Then devices white list is created for a specific employee/employee group/workstation/workstation group. These employees/workstations have access to whitelisted device models and instances regardless the policy. 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
- Workstations
- Employees
- White Lists
- Signatures

## 3.4.2.1 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 **workstation groups**. Security policy of employee group affects all the employees included to this group. Security policy of workstation group affects all the employees which work at managed workstations included to this workstation 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

### 3.4.2.1.1 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.

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 call shadow copy**. Indicates if a shadow copy of voice Skype traffic should be created.
- **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-sent file should be created.
- **Minimum file size**. Lower limit of file size.
- **Maximum file size**. Upper limit of file size.

Network Monitor rules feature additional details:

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

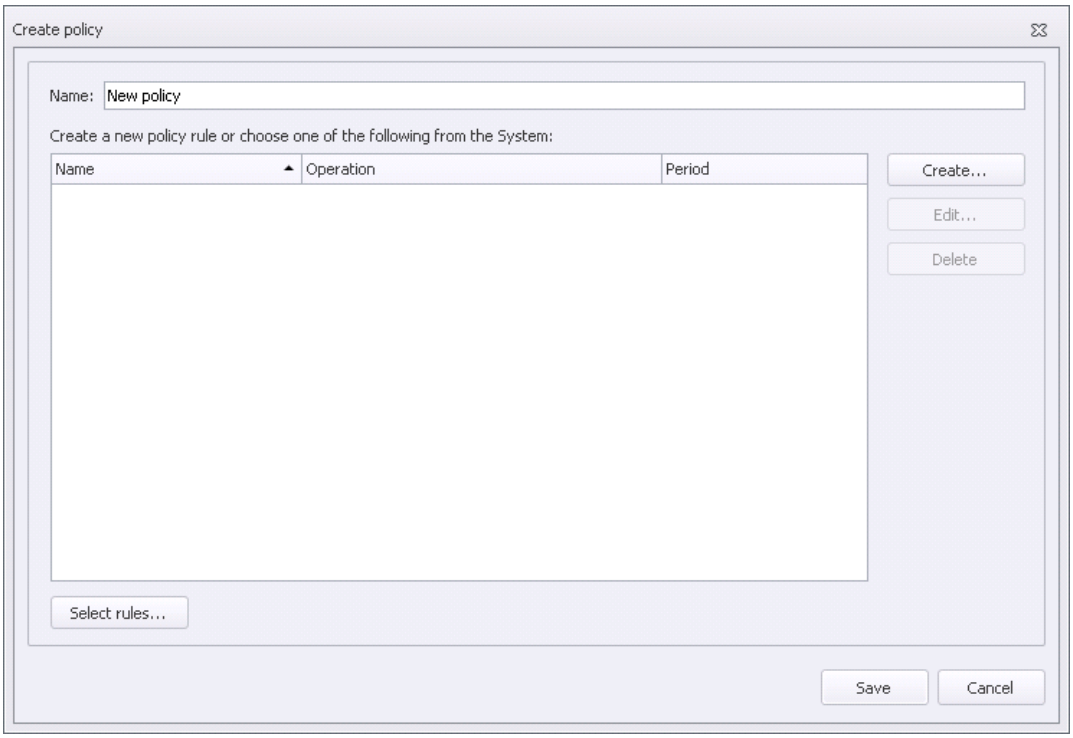
**Note:**
Information retrieved from some attributes is duplicated in the main screen workspace.

## 3.4.2.1.2 Adding and Configuring New Security Policy

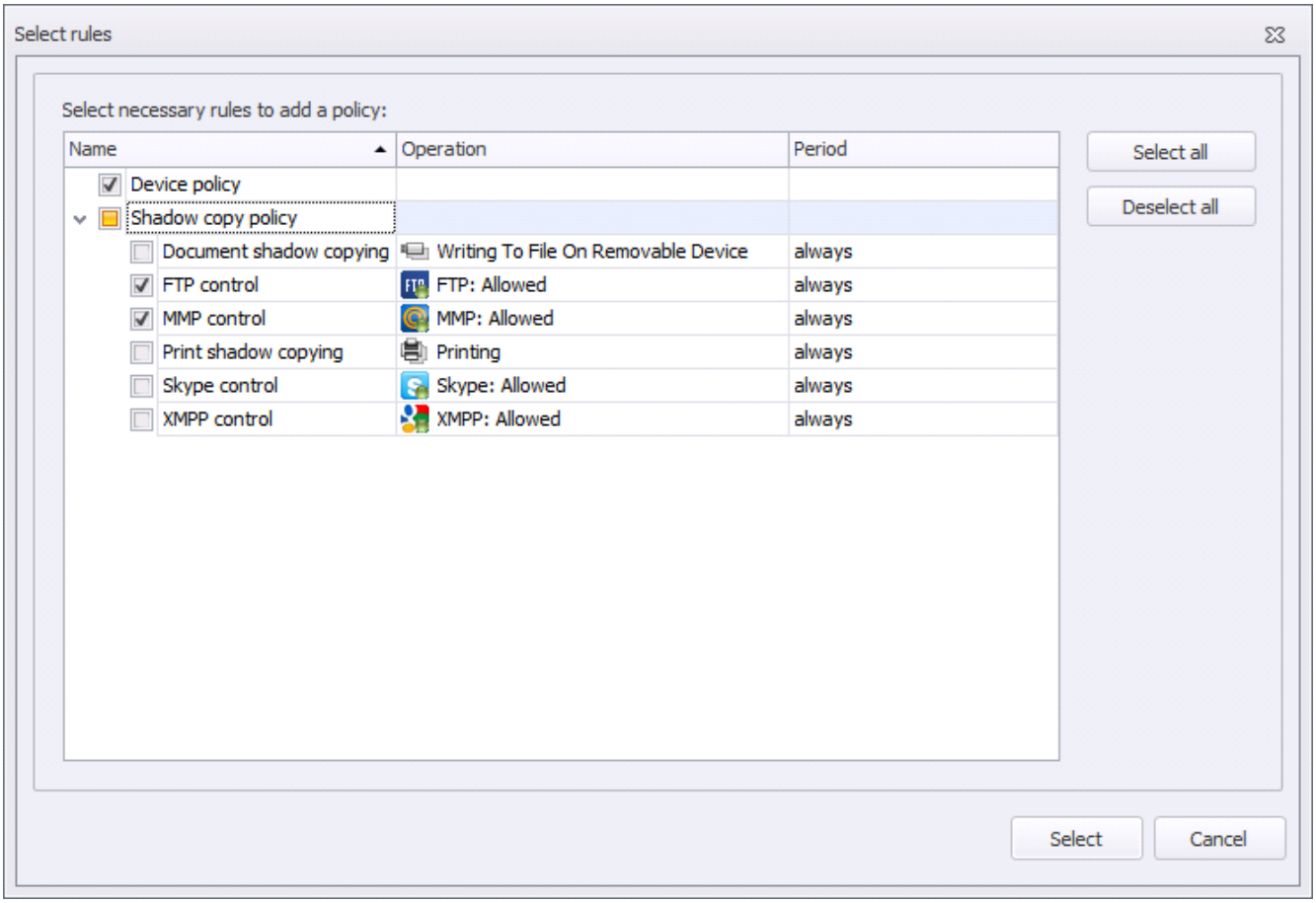
**To add and configure security policy:**

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 File Monitor Rule
  - Configuring Print Monitor Rule
  - Configuring Device Monitor Rule
  - Configuring IM Client Monitor Rule
  - Configuring FTP Monitor Rule
  - Configuring Network 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).

## 3.4.2.1.3 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 **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.

## 3.4.2.1.4 Deleting Security Policy

**Warning!**
The policy appointed at least one employee group or workstation groups, cannot be deleted. To delete security policy make sure that this policy is not apointed to any employee group (see "Viewing Employee Details") or workstation group (see "Viewing Workstation Details").

**To delete security policy:**

1. Go to **Policies**.
2. In **Policies** area of Navigation pane select security policy 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.

## 3.4.2.2 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

## 3.4.2.2.1 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 selected: see "Configuring File Monitor Rule") has a highest priority.
2. The forbidding rule overrides the permitting one. For example, **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***. Also **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***. And so on.

3. The rule creating shadow copies (**Create a shadow copy** option is selected) overrides a rule without shadow copying.
4. For **IM Client Monitor** rules which make a copy of voice traffic (**Create voice copy** option is selected: see "Configuring IM Client Monitor Rule"), the rule which has a constraint of lesser recording duration overrides a rule with longer recording duration.

Other important information on rules application:

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

# 3.4.2.2.1.1 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 workstation groups of the workstation 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 workstation 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 workstations after installation.

**For example:**

There is a rule that lets workstation group A write to CD/DVD drive. Workstation WS belongs only to workstation group A. Employee Smith belongs only to employee group B with no device rules. Employee Smith tries to view a CD on workstation 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. Banned from use | 1. No access<br>2. Read-only | 1. No access<br>2. Read-only<br>3. Full access to the encrypted devices only |

**Examples:**

**Example 1.** There is a rule for workstation 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 workstation that belongs to workstation 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)<br>Imaging devices (LPT) | If there is no access to LPT port, the device connected to this port will be unavailable |
| Serial port (COM) | Modem<br>Local printer (COM)<br>Imaging devices (COM) | A modem connected to COM port is only accessed basing on COM port rule<br>If there is no access to COM port, the device connected to this port will be unavailable |
| Removable Storage (USB and IEEE 1394 devices) | FireWire (IEEE 1394) | If there is no access to FireWire (IEEE 1394) port, the device connected to this port will be unavailable |
| Local Printer (with USB, IEEE 1394, SCSI connection, etc.) | FireWire (IEEE 1394)<br>Serial port (COM)<br>Parallel port (LPT) | If there is no access to FireWire (IEEE 1394), COM, LPT port, the device connected to this port will be unavailable |
| Image-processing Devices (cameras, scanners) | FireWire (IEEE 1394)<br>Serial port (COM)<br>Parallel port (LPT) | If there is no access to FireWire (IEEE 1394), COM, LPT port, the device connected to this port will be unavailable |
| Bluetooth Device | No | |
| IrDA Device | No | |
| Other USB Devices | No | |
| FireWire | Removable storage device (IEEE 1394)<br>Local printer (IEEE 1394)<br>Imaging devices (IEEE 1394) | If there is no access to FireWire (IEEE 1394) port, the device connected to this port will be unavailable |
| Modem | Serial port (COM) | Modem access rules do not affect modems connected to COM port.<br>A modem connected to COM port is only accessed basing on COM port rule |
| Smart Card Reader | No | |
| Tape Device | No | |
| Multifunctional Device | No | |
| PCMCI device | No | |
| USB Network Adapter | No | |
| Pocket Computer (Windows | No | |

| Rule | Overlapping rules | Notes |
|---|---|---|
| Mobile and Palm OS pocket computers) | | |

## 3.4.2.2.1.2 Creating Shadow Copies and Blocking Operations Due to F

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

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

and

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

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

## 3.4.2.2.2 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 File Monitor Rule
   - Configuring Print Monitor Rule
   - Configuring Device Monitor Rule
   - Configuring IM Client Monitor Rule
   - Configuring FTP Monitor Rule
   - Configuring HTTPS Monitor Rule
   - Configuring Network 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.

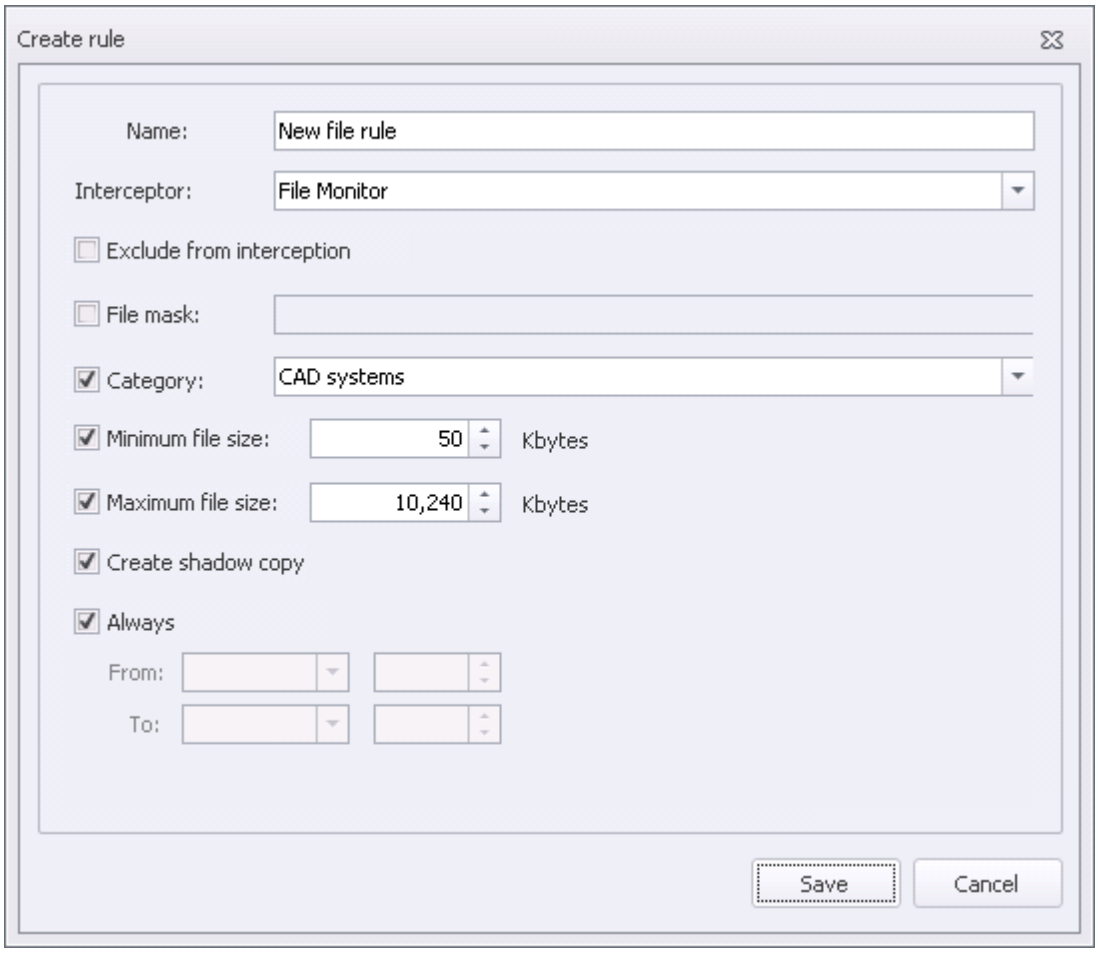
## 3.4.2.2.2.1 Configuring File Monitor Rule

**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 workstation, 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 **Rules** 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.

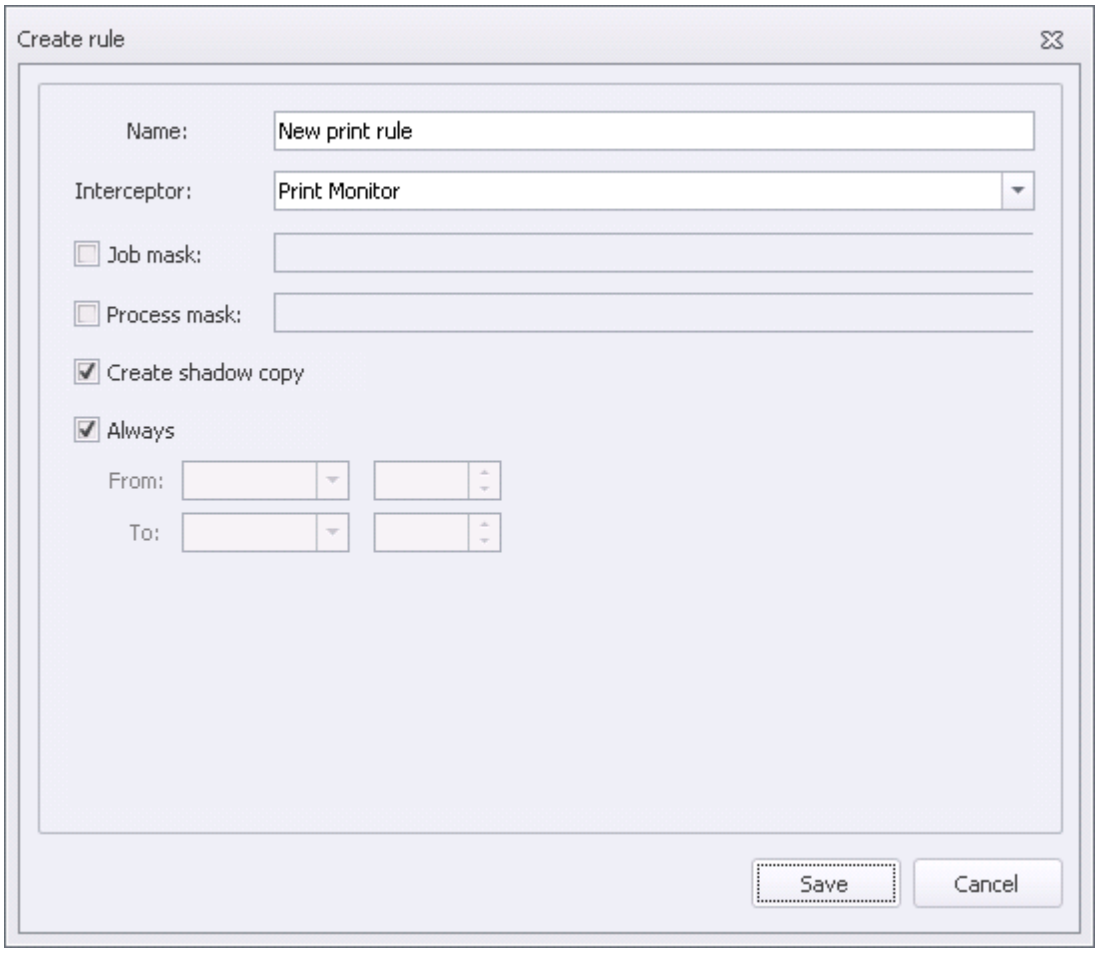
7. You can constrain controlled files by mask. Flag **File mask** checkbox and specify mask. You can use wildcard characters when specifying a file mask: «?» to replace a character or «*» to replace a character set. For example, `*.doc`. The space character is interpreted as a part of file name.
8. You 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**.

# 3.4.2.2.2.2 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 **Rules** 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**.

## 3.4.2.2.2.3 Configuring Device Monitor Rule

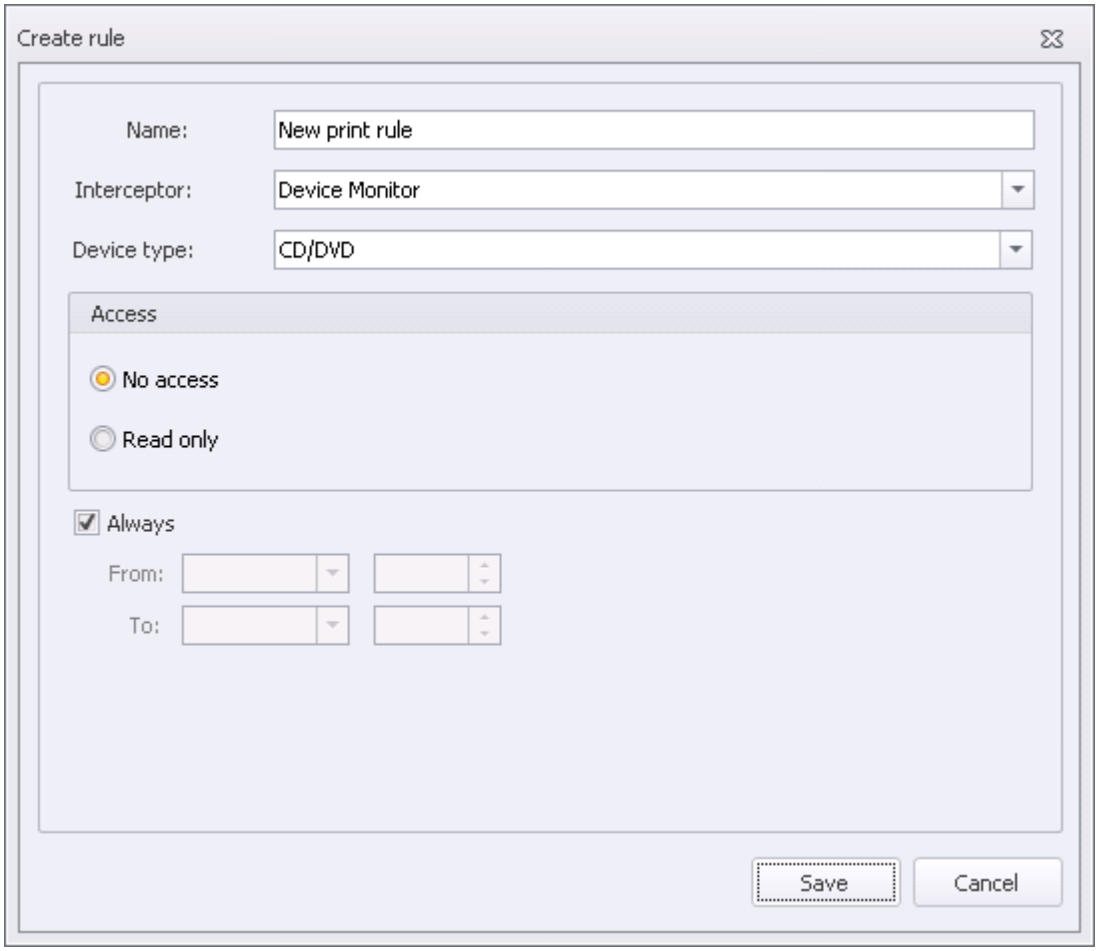
**Device Monitor** interceptor lets to control employee access to peripheral devices. Possible access limitation levels are dependent on device type.

Access levels for different device types

| Name | Behavior |
|---|---|
| Floppy | Full access to encrypted devices only / Read only / Access denied |
| CD/DVD | Read only / Access denied |
| LPT port | Denied |
| COM port | Denied |
| Portable disk drives (USB and IEEE 1394 devices) | Full access to encrypted devices only / Read only / Access denied |
| Local Printer (with USB, IEEE 1394, SCSI connection, etc.) | Denied |
| Image Editing Devices (cameras and scanners) | Denied |
| Bluetooth Device | Denied |
| IrDA Device | Denied |
| Other USB Devices | Denied |
| FireWire | Denied |
| Modem | Denied |
| Smart Card Reader | Denied |
| Tape Drive | Denied |
| Multifunctional Device | Denied |
| PCMCI device | Denied |
| USB Adapter | Denied |
| Pocket Computer (Windows Mobile and Palm OS pocket computers) | Denied |

**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 "Device Monitor Rules Application".




**To configure the rule, perform the following steps:**

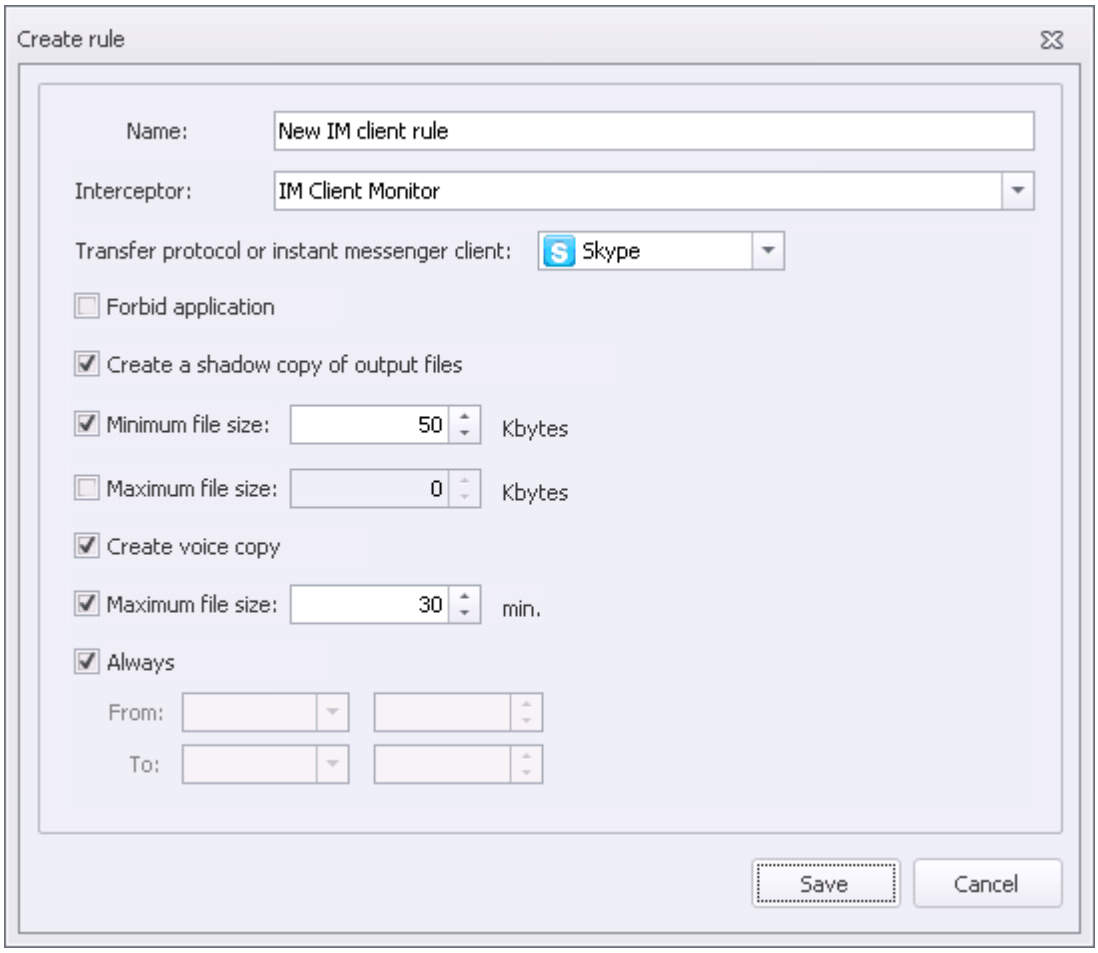
1. Go to **Policies** section.
2. In **Policies** area at Navigation pane select a security policy which you want to add a rule to.
3. Take one of the following steps:
   - in the Main Menu select **Edit > Create rule**
   - click **Create rule** at the top of **Policies** area
   - right-click at the empty space in **Rules** 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**.

# 3.4.2.2.2.4 Configuring IM Client Monitor Rule

**IM Client Monitor** interceptor lets to control employee access to instant messengers: Skype, Jabber (XMPP protocol) and Mail.Ru Agent (MMP protocol).

**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 **Rules** 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 **Transfer protocol or instant messenger 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
7. If you want to completely forbid using a client of this type of messenger, flag **Forbid application**.
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 workstation.
   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. For **Skype** client you can also save files with voice chat records. Flag **Create voice copy** field. In **Maximum File Size** field specify how the chat will be split: if the length of one conversation is longer then specified recording duration (in minutes) then there will be several shadow copies (and several events) created for one chat.
10. 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.
11. When all parameters are configured, click **Save**.

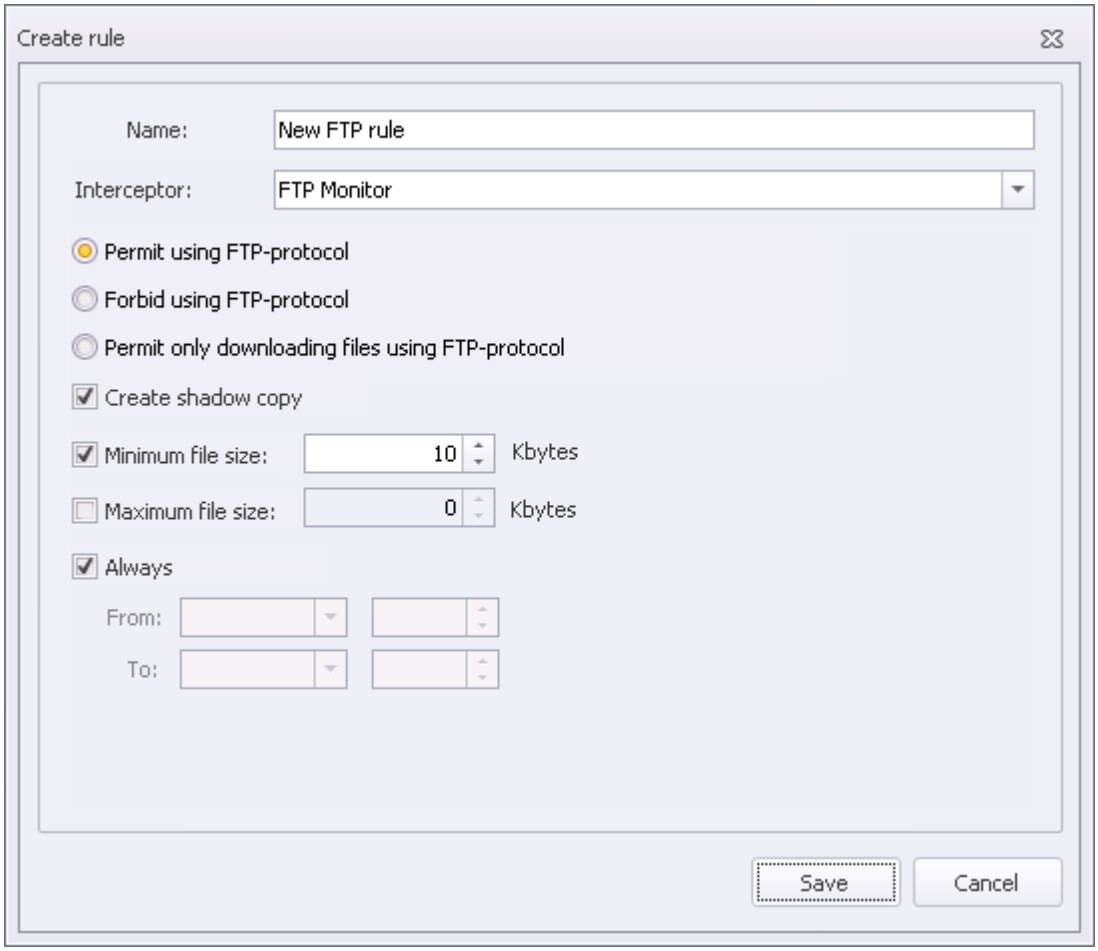
**Warning!**
If IM Client Monitor rule should create a shadow copy of file, message or chat but there is less free system drive space left than required by the policy (see "Creating Shadow Copies and Blocking Operations Due to Free Space Shortage") then shadow copies of messages still will be created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

## 3.4.2.2.2.5 Configuring FTP Monitor Rule

**FTP Monitor** interceptor lets to control data transfer through FTP 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 **Rules** 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 protocol:
   - **Permit using FTP-protocol**
   - **Forbid using FTP-protocol**
   - **Permit only downloading files using FTP-protocol**
7. if you allowed using FTP 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!**

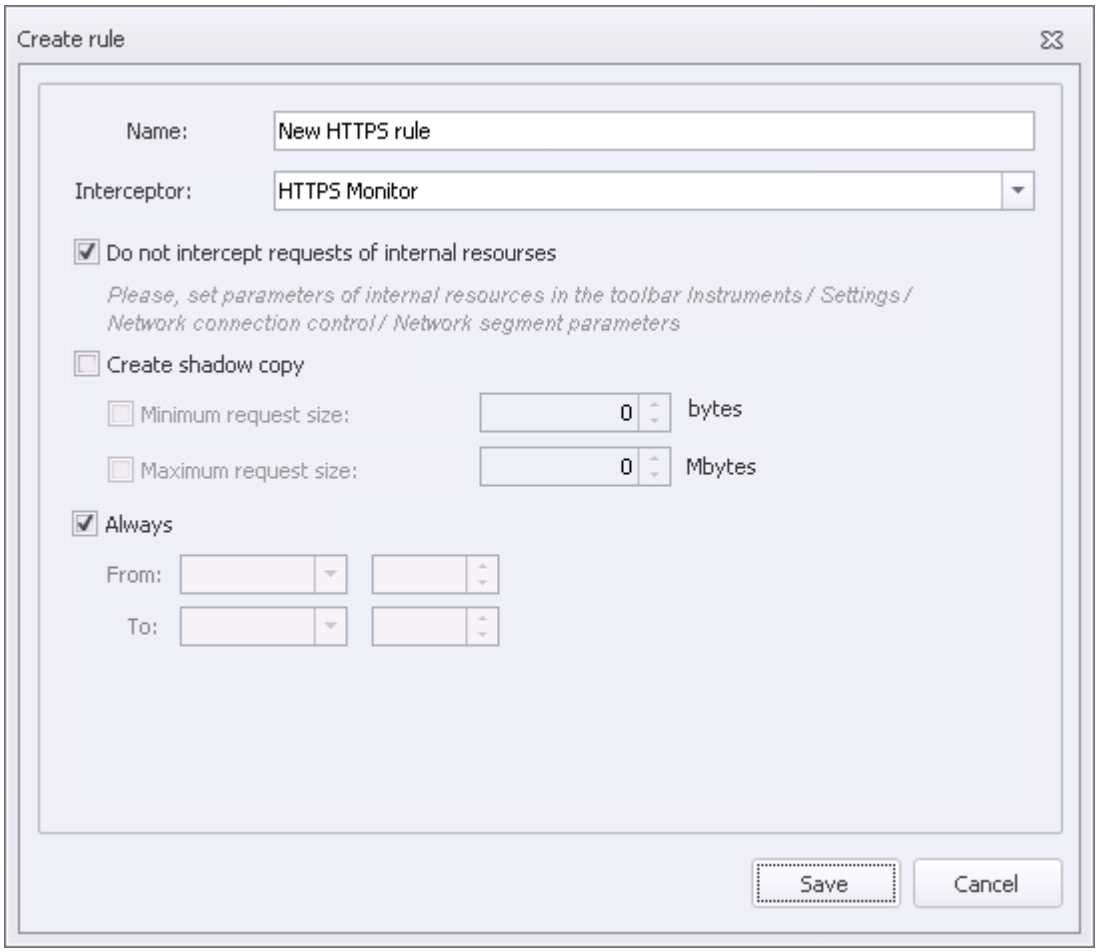
If FTP Monitor rule should create a shadow copy of file but there is less free system drive space left than required by the policy (see "Creating Shadow Copies and Blocking Operations Due to Free Space

Shortage") then 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**.

## 3.4.2.2.2.6 Configuring HTTPS Monitor Rule

**HTTPS Monitor** interceptor lets to control data transfer through HTTPS 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 **Rules** area and select **Create rule** from the drop-down list.
4. In **Create rule** dialog in **Interceptor** field select **HTTPS Monitor**.
5. Enter rule name to **Name** field.
6. Specify the interception of internal resources queries. To do this in the **Do not intercept requests of internal resources**:
   - mark the checkbox - if you don't need to intercept the query;

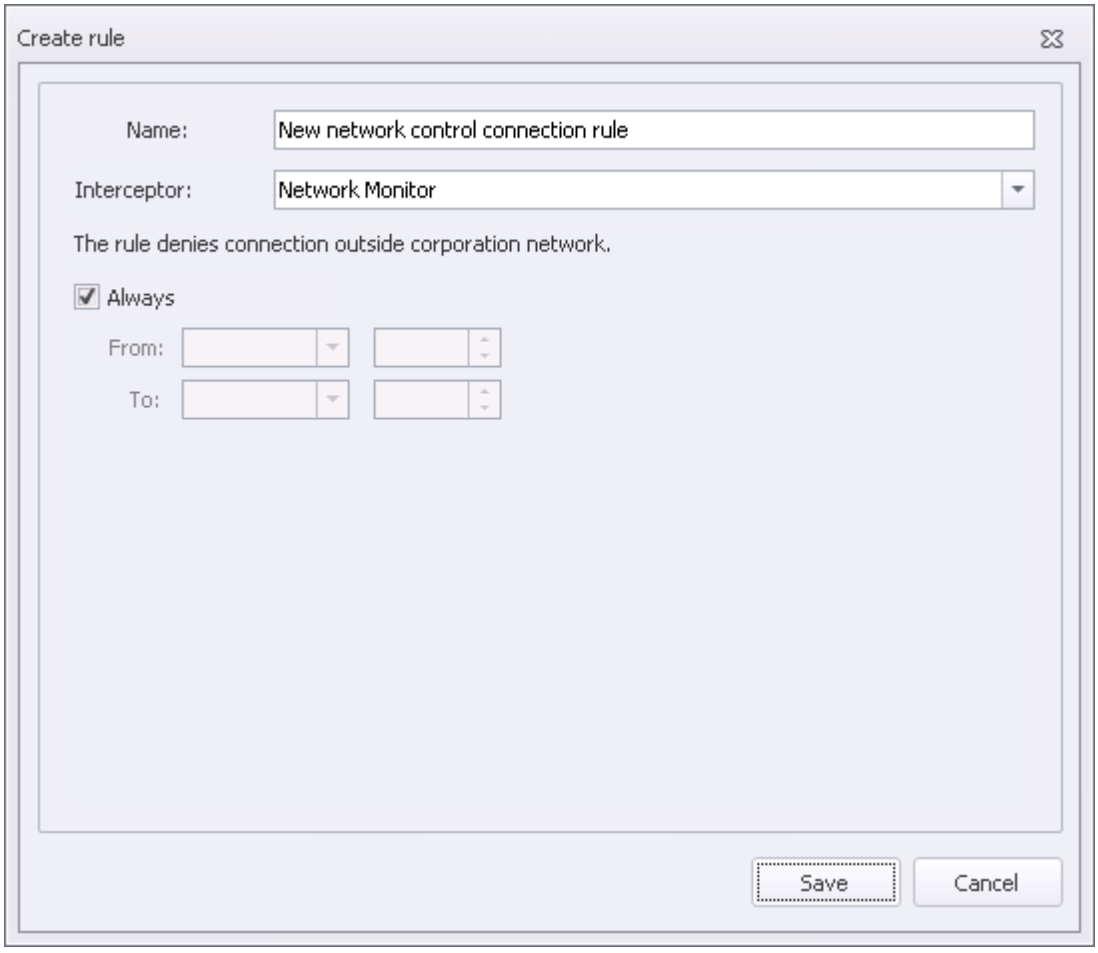
- unmark the checkbox - if you need to intercept the query.

7. Specify creating of the transferred files shadow copies. To do this mark the **Create shadow copy** checkbox. You can also define additional parameters for shadow copies:
   - **Minimum request size**. If the check box is selected, shadow copies will be enabled only for files of specified size or larger.
   - **Maximum request size**. If the check box is selected, shadow copies will be enabled only for files of specified size or smaller.

   **Warning!**
   If HTTPS 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 the file 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**.

## 3.4.2.2.2.7 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".




**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 **Rules** 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**.

## 3.4.2.2.3 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 File Monitor Rule
   - Configuring Print Monitor Rule
   - Configuring Device Monitor Rule
   - Configuring IM Client Monitor Rule
   - Configuring FTP Monitor Rule
   - Configuring Network 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.

## 3.4.2.2.4 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.

## 3.4.2.2.5 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.

## 3.4.2.3 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 workstation 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 is available in:

- Viewing Employee Details
- 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

## 3.4.2.3.1 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 on **Details** panel is duplicated in the main screen workspace.

## 3.4.2.3.2 Adding and Editing an Employee Group

**To add or edit an employee group:**

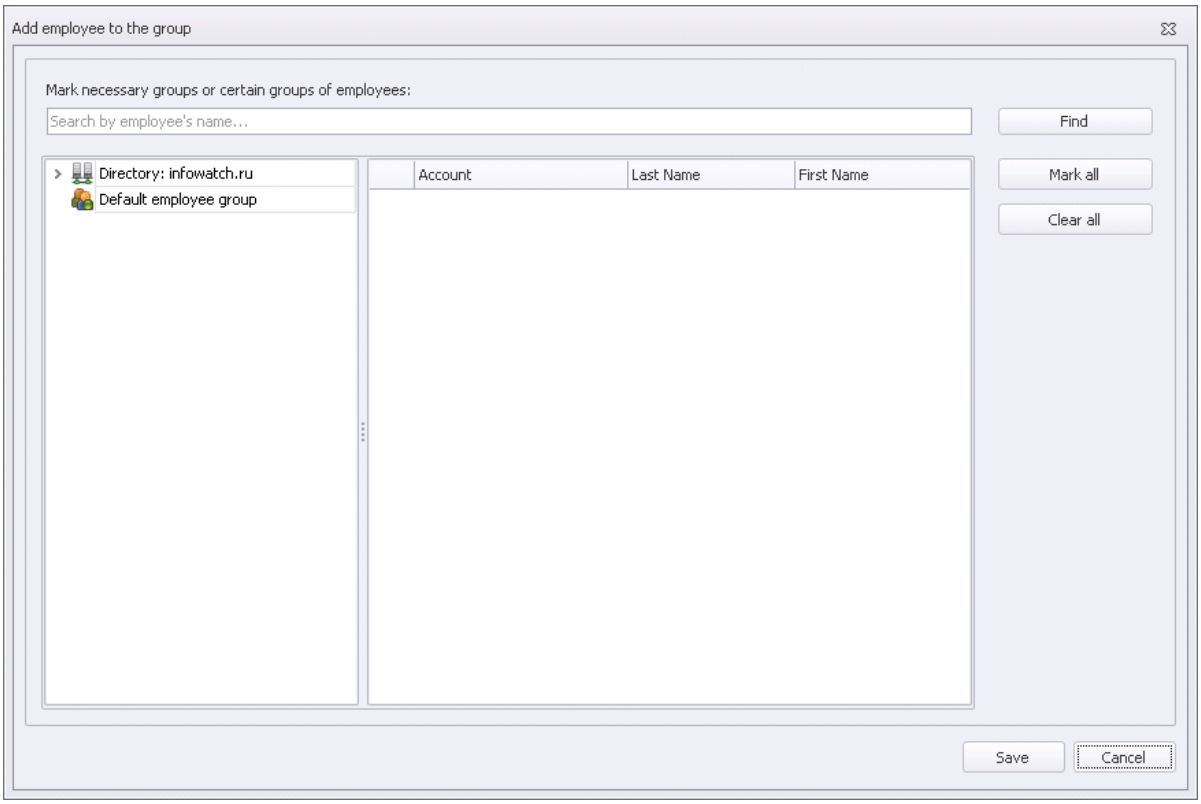
1. Go to **Employees** section.
2. Take one of the following steps:

| Action | Steps |
|---|---|
| Add employee group | • select **Edit > Create Employee Group** in the Main Menu;<br>• click **Create Employee Group** at the top of the Navigation Pane. |
| Edit employee | 1. In **Employees** area of Navigation Pane select the employee group name. |

| | |
|---|---|
| group | 2. Take one of the following steps:<br>• in the Main Menu, click **Edit > Edit Employee Group**;<br>• click **Edit Employee Group** at the top of Navigation pane;<br>• double-click selected employee group name. |

**Create employee group** window will appeared.

3. In this window 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 workstation) and belonging to existing Device Monitor employee groups.

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

## 3.4.2.3.3 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.

## 3.4.2.3.4 Adding Employee Account to a Group

After InfoWatch Device Monitor Client is installed to the workstation (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.

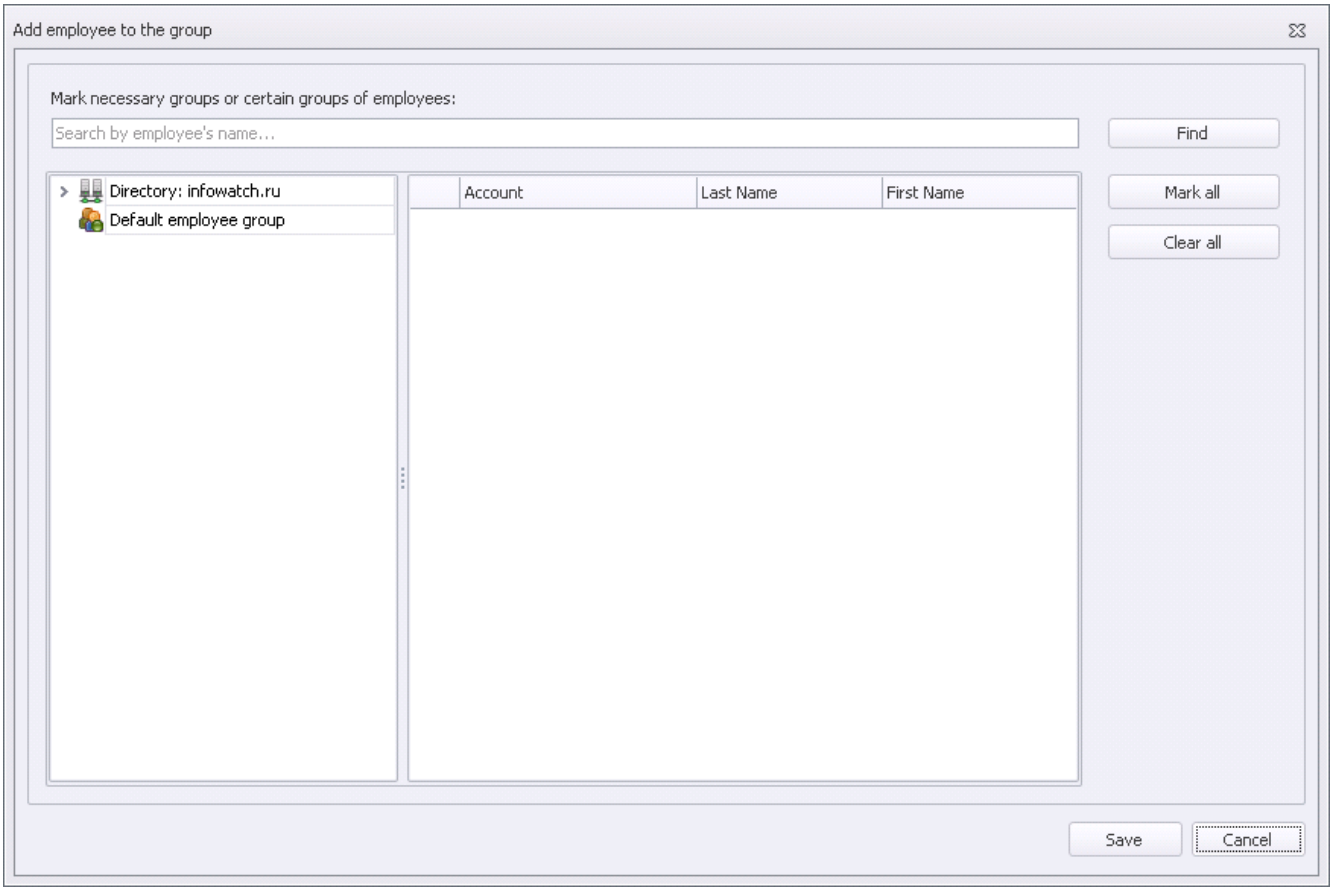
This adds an account to the selected group.

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 workstation 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 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.




4. 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 workstation) and belonging to existing Device Monitor employee groups.
   - To add an employee, in left pane select a node in groups tree, then flag accounts you want to add to 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**.
   - 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.

## 3.4.2.3.5 Editing Employee Account

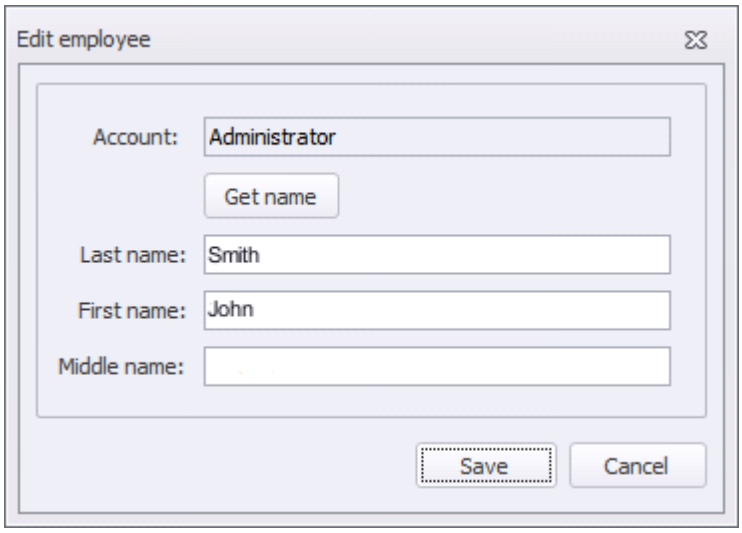
Parameters of employee account are imported from directory service or while installing a InfoWatch Device Monitor Client to the computer where this employee is registered. If you want to add some information, you can enter employee's personal data as described below.

**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.

   These actions open **Edit employee** dialog.




5. Edit the options in this dialog. While editing, 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.

## 3.4.2.3.6 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.

### 3.4.2.3.7 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.

## 3.4.2.4 Workstations

InfoWatch Device Monitor workstation is a managed workstation - computer where InfoWatch Device Monitor. Client is installed.

General principles of managing workstations are described in "Workstations and Workstation Groups" section.

Actual security policies can be applied only to a workstation group. You can define a security policy for a certain workstation by including it to various workstation groups.

**Warning!**
Each workstation is a subject both of security policy of a workstation group and security policy of an employee which is currently authorized at that workstation. Information about rule conflict resolving see in "Rules Application".

To go to Management Console workstation section, click **Workstations** button on Navigation pane.

For more information on managed workstations see:

- Viewing Workstation Details
- Viewing Workstation Effective Policy
- Adding and Editing a Workstation Group
- Deleting Workstation Group
- Adding Workstation to a Group
- Removing Workstation from a Group
- Deleting Workstation from Security Schema
- Updating Clients at Managed Workstations

### 3.4.2.4.1 Viewing Workstation Details

**Workstations** area of Navigation pane displays a list of workstation groups. Main screen workspace displays the list of workstations in selected workstation group.

**Note:**
Use additional options to adjust workstations list display (for details, see "Additional Features").

**To view the list of workstations that belong to a separate group,**

select the group name from workstation groups list.

**To view a full list of registered workstations,**

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

Workstation information is displayed in tabular list. Each row in the list contains a workstation. Columns contain basic workstation properties. Extended information on each workstation is available in **Details** panel.

**To view specific workstation's properties,**

in the main screen workspace, select the row with workstation description.

After this, **Details** panel will display table of properties with the following workstation data:

- **Status**. Managed workstation and Client status. This parameter may have the following values:
  - **Works properly**. Managed workstation is enabled, Client is running.
  - **Inactive**. Managed workstation is disabled or unavailable for a long time. The same status is displayed, if the Client is uninstalled from the managed workstation.
- **Address**. Workstation address. When specifying the address you may use domain name or IP address.
- **Installed**. Date and time of workstation Client's first access to the server.
- **Established**. Date and time of Client launch on workstation.
- **Last check-in**. Date and time of workstation Client's last access to the Server.
- **Schema version**. Client's current security schema version number.
- **Client version**. Client version number.
- **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 and FTP protocols (see "Network Traffic Control").
- **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 workstation is automatically added to "default" workstation group. At the same time, "default" workstation group security policy is assigned to the new workstation.

You can do the following as you work:

- manage workstation groups:
  - add workstation groups
  - edit workstation group parameters
  - delete workstation groups.
- manage workstations:
  - add computers' information to workstation groups and thus define workstation security policy
  - remove workstations from workstation group

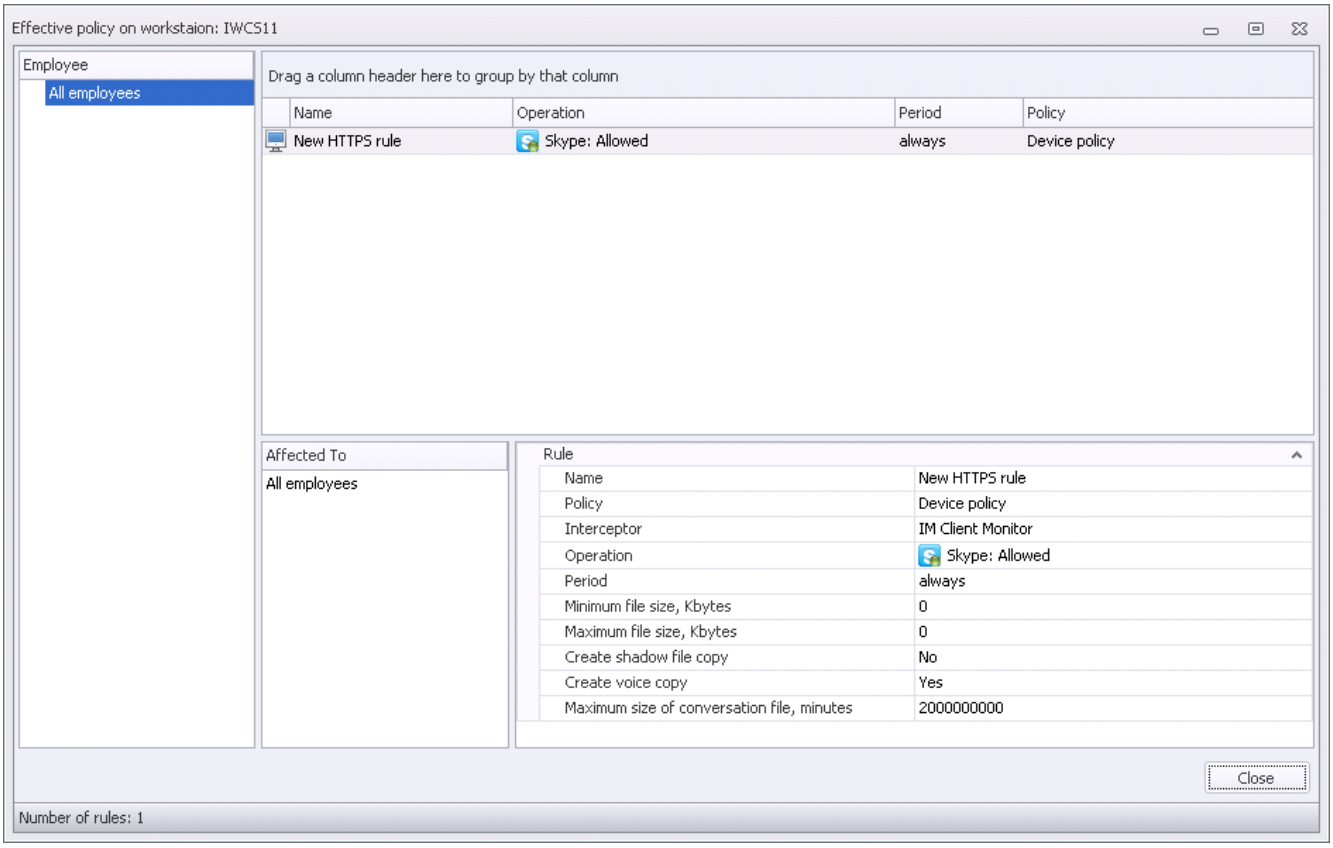
- delete workstation from security schema
- update Clients at managed workstations.

## 3.4.2.4.2 Viewing Workstation Effective Policy

**To view information about a policy which is currently active at the workstation:**

1. Select workstation from the list.
2. Take one of the following steps:
   - in the Main Menu select **Edit > Show effective policy**.
   - double-click workstation name.

This opens the screen **Effective policy on workstation: <Workstation name>**.




Left pane of this screen contains a list of accounts that have access to this workstation, and the right pane contains a set of workstation's applicable rules. The list may contain default rules, workstation's rules, and workstation employees' rules.

**To view a set of rules for a specific employee,**

in **Employee** pane select the appropriate account.

**To view rule's detailed information,**

select it from the list of rules.

**Affected To** panel displays a list of employees who are subject to this rule, and **Rule** panel contains detailed information on selected rule.

# 3.4.2.4.3 Adding and Editing a Workstation Group

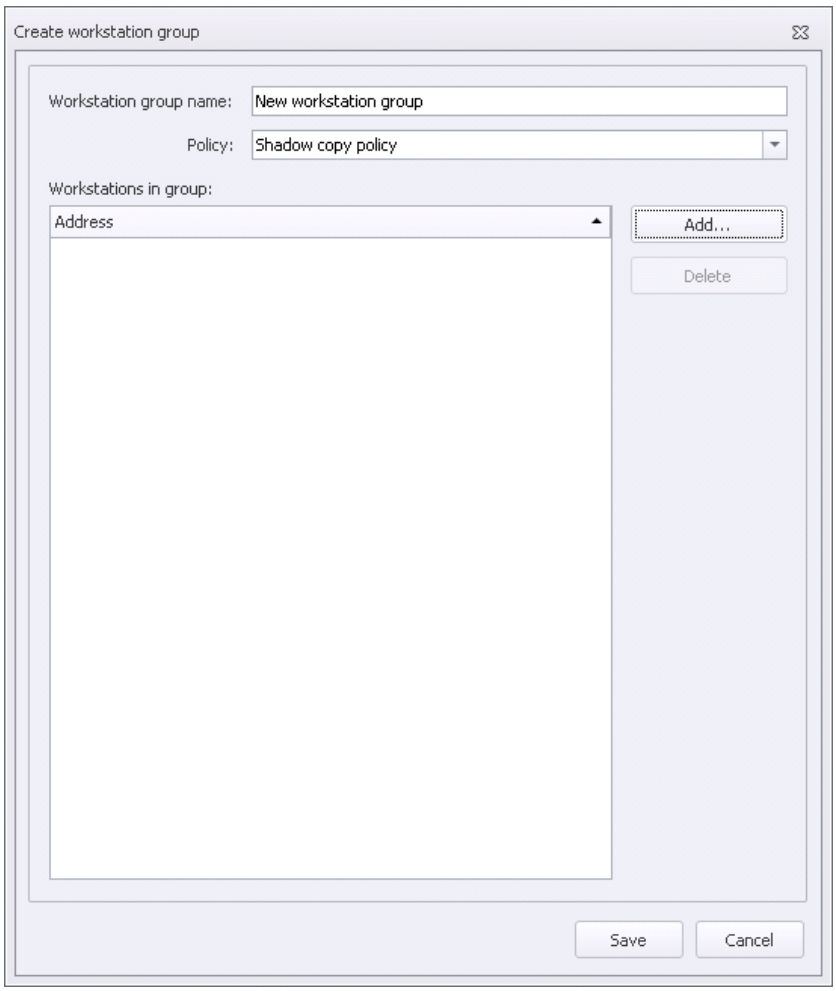
**Warning!**
When a new workstation is registered its information is automatically added to security schema (to "*Default*" group).

**To add or edit a workstation group:**

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

| Action | Steps |
|---|---|
| Add workstation group | • in the Main Menu, click **Edit > Create workstation group**;<br>• click **Create Workstation Group** at the top of Navigation pane. |
| Edit workstation group | 1. In **Workstations** area of Navigation pane select workstation group name.<br>2. Take one of the following steps:<br>• in the Main Menu select **Edit > Edit**<br>• click **Edit** at the top of Navigation pane;<br>• double-click selected workstation group name. |

This opens the **Create workstation group** window.




3. In this window specify the following parameters:
   - **Workstation group name**.
   - **Policy**. From the drop-down list select security policy that will be assigned to this workstation group .
4. Define a list of workstations in a group:
   - To add one or several workstations click **Add**. In the opened **Add workstation to the group** dialog you

can select workstations 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 workstations which you want to add to the editing group .

You can also search a workstation: enter a part of workstation name to the upper string and click **Find**.

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

- To edit workstation parameters, select it from the list of ones belonging to the group and click **Change** .
- 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.

## 3.4.2.4.4 Deleting Workstation Group

**To edit or delete workstation group:**

1. Go to **Workstations**.
2. In **Workstations** area of Navigation pane select workstation group name.
3. Take one of the following stepssteps:
   - 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 workstation group.

   **Warning!**
   The group you are deleting may contain workstations that don't belong to any other group. If you delete the only group these workstations 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.

## 3.4.2.4.5 Adding Workstation to a Group

When installing InfoWatch Device Monitor Client (see "InfoWatch Device Monitor Client Setup"), workstation is added to "default" workstation group. All workstations inside "default" group will be affected by security policy assigned to this group. Further on, you can assign security policies by assign a workstation to various workstation groups.

**To move a workstation from one workstation group to another:**

1. Go to **Workstations**.
2. In **Workstations** area of Navigation pane, select workstation group that contains the workstation. Main screen will display a list of all workstations inside the group.
3. Select a row that contains the workstation you want to add to another group. Click and hold the selected row and drag the workstation to **Workstations** area of Navigation pane. Move the pointer over the name of workstation group you want to add the workstation to. When a yellow arrow appears to the left of the

selected group name, release the mouse button.

This adds workstation to selected workstation 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 workstation (see "Creating Primary Distribution Task") will be affected by the policy of the group it was added to.

**Warning!**
It is not recommended to add computers with similar names. These computers will be registered in InfoWatch Device Monitor system as a single workstation, affected by the same policies, and register the same events, etc.

**To add workstation to a group:**

1. Go to **Workstations**.
2. In **Workstations** area of Navigation pane select workstation group name. Main screen will display a list of all workstations inside the group.
3. Take one of the following steps:
   - in the main menu select **Edit > Add Workstation**
   - click **Add Workstation** located at the top of **Workstations** area
   - right-click in the workspace and select **Add Workstation** from the drop-down menu.

   In the opened dialog you can select workstations:
   - imported from directory service (for example Active Directory)
   - received from Microsoft Windows Network.
4. Flag workstations or workstation 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 workstation 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 workstation 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.

## 3.4.2.4.6 Removing Workstation from a Group

Workstation is added to a group basing on needed security policies. You might need to disable policy's action to the workstation. To perform this procedure, you must remove workstation from workstation group with this policy.

**Note:**
If you remove a workstation from a single group it belongs to, it will be automatically added to "default" group.

**To exclude workstation from workstation group:**

1. Go to **Workstations**.
2. In **Workstations** area of Navigation pane, select workstation group that contains the workstation. This displays a full list of workstations that belong to selected group.

3. Select a row that contains the workstation you want to remove from workstation group.
4. Take one of the following steps:
   - in the main menu select **Edit > Remove Workstation From Group**
   - click **Remove Workstation From Group** located at the top of **Workstations** area
   - press **Delete** keyboard button

This removes workstation 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.

## 3.4.2.4.7 Deleting Workstation from Security Schema

You can remove a workstation from the list of registered workstations (for example, workstation discontinued operation). Workstation information will not be deleted, but it will be marked as **Inactive** due to Client deactivation. If you don't want to save inactive workstation information, you can delete its record.

**To remove workstation from security schema:**

1. Go to **Workstations**.
2. In **Workstations** area of Navigation pane, select workstation group that contains the workstation.
3. In the Main screen workspace, select the row that contains the inactive workstation you want to remove.
4. Take one of the following steps:
   - in the Main Menu, click **Edit > Delete Workstation From Security Schema**;
   - click **Delete Workstation From Security Schema** located at the top of **Workstations** area
   - right-click workstation row and select **Delete Workstation 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 workstation.

This removes workstation information from all groups the workstation 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.

# 3.4.2.4.8 Updating Clients at Managed Workstations

Device Monitor  Clients at managed workstations 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 workstations of the group:**

1. Go to **Workstations**.
2. In **Workstations** area of Navigation pane, select workstation group.
3. Click  **Update** All **Workstations** located at the top of Navigation pane.

**To update Device Monitor Clients at selected managed workstations:**

1. Go to **Workstations**.
2. In **Workstations** area of Navigation pane, select workstation group.
3. In the Main screen workspace, select the row(s) containing managed workstation(s). To select several workstations click at them while pressing **Shift** or **Ctrl** button.
4. Click  **Update Workstations** located at the top of **Workstations** area.

This creates and runs the update task for selected workstations.

# 3.4.2.5 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

# 3.4.2.5.1 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:**
Use additional features to adjust white list display (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 workstation**. Name of workstation 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 is duplicated in the main screen workspace.

## 3.4.2.5.2 Adding White List

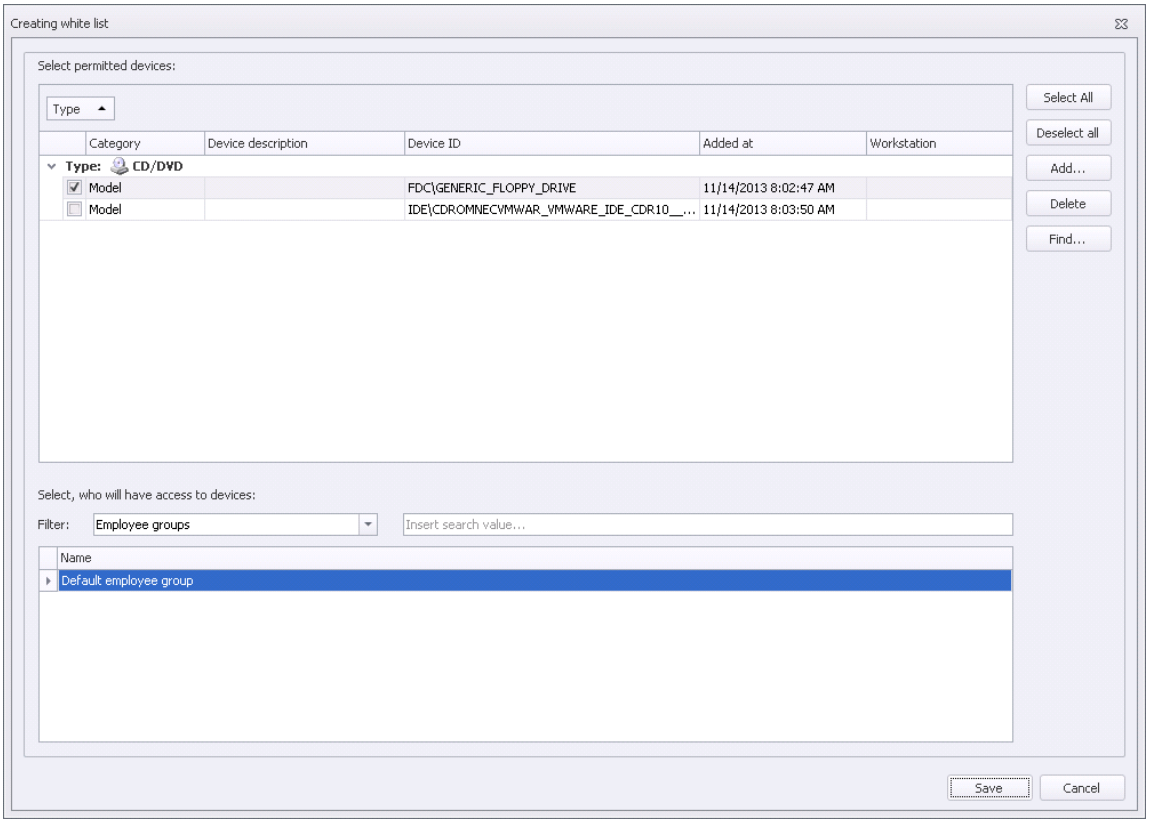
White list affects selected objects: employees, employee groups, workstations or workstation groups.

**Warning!**
A single object (employee, employee group, workstation or workstation 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 box.




3. In the table of devices registered in the System 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 to Database;
- Removing Device from Database.

4. In **Select, who will have access to devices** area select a filter: who will be affected to white list action:
   - employees
   - employee groups
   - workstations
   - workstation 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 / workstation / workstation group that will have full access to selected devices.
6. Click **Save**.

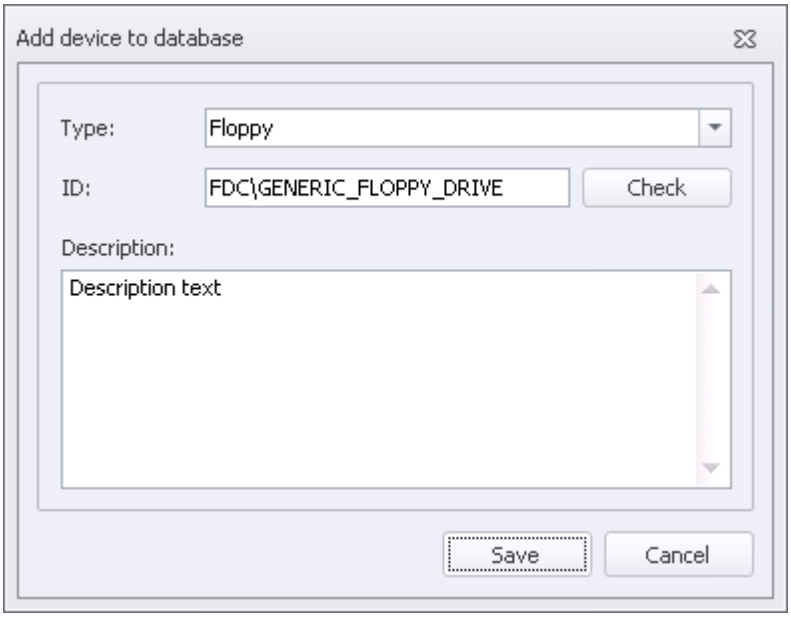
## 3.4.2.5.2.1 Adding Device to Database

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 workstation).

**To add device information manually:**

1. Open **Creating White List** dialog box (see "Adding white list").
2. Click **Add** at the right.
   This opens **Add device to database** dialog box.




3. Specify device parameters:
   - select device type from **Type** drop-down list
   - enter the device instance or model ID 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**.

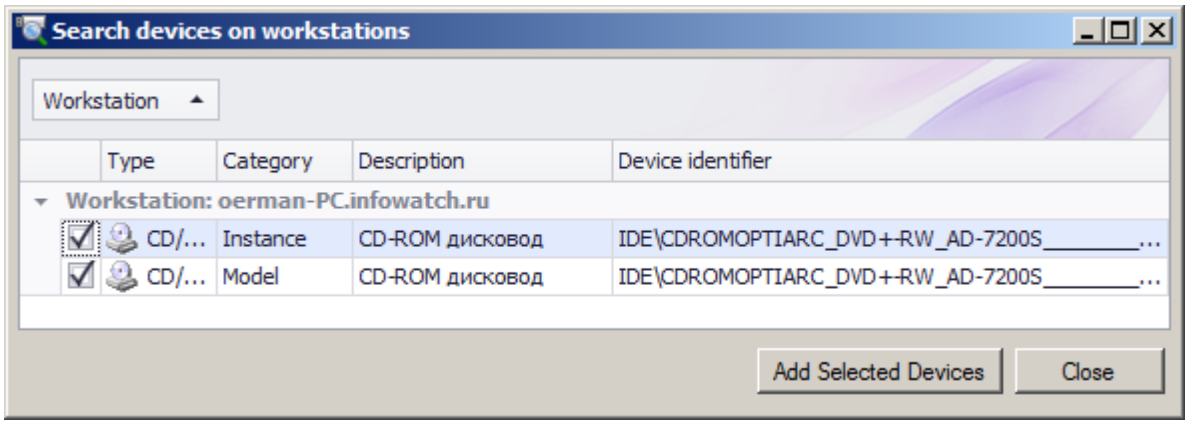
**Warning!**
When using instance code, take into account that some devices do not have unique ID: ID can be changed dynamically and differed evet when connecting to different ports of the same workstation. In such case using device model code is recommended.

- enter description into **Description** box.

4. Click **Add**.

**To add device information via searching devices connected to managed workstations:**

1. Open **Creating White List** dialog (see "Adding white list").
2. Click **Find** at the right.
   This opens **Search devices on workstations** dialog box.




3. Use one of the following ways to select a managed workstation from the list:
   - click next to workstation;
   - double-click workstation name.

   You will see a list of devices which were connected to selected workstation during all the time Device Monitor Client was installed at the workstation.
4. Flag the devices you want to add.
5. Click **Add selected devices**.

## 3.4.2.5.2.2 Removing Device from Database

**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 screen click **OK**.

## 3.4.2.5.3 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.

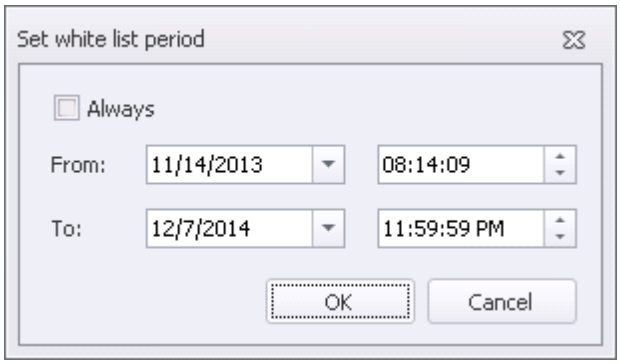
**To set white list entry period:**

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 period** dialog.




5. Set item validity period and click **OK**.

## 3.4.2.5.4 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").
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.

## 3.4.2.5.5 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.

## 3.4.2.6 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 existing signatures:**

1. Go to **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:

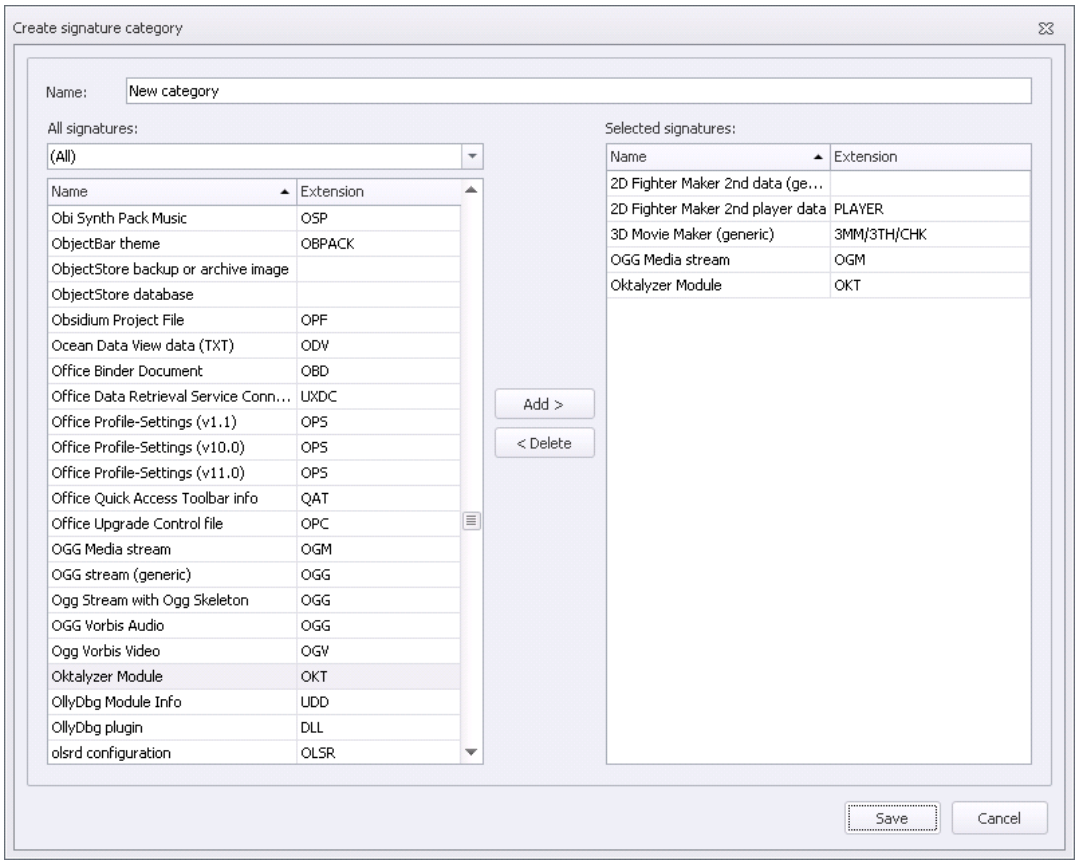
- create signature categories
- fill created categories by copying predefined signatures
- delete your signature categories, if they are not used by any rule.

## 3.4.2.6.1 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 drop-down 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**.

## 3.4.2.6.2 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.

## 3.4.2.6.3 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 Temporary Employee Access

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!**

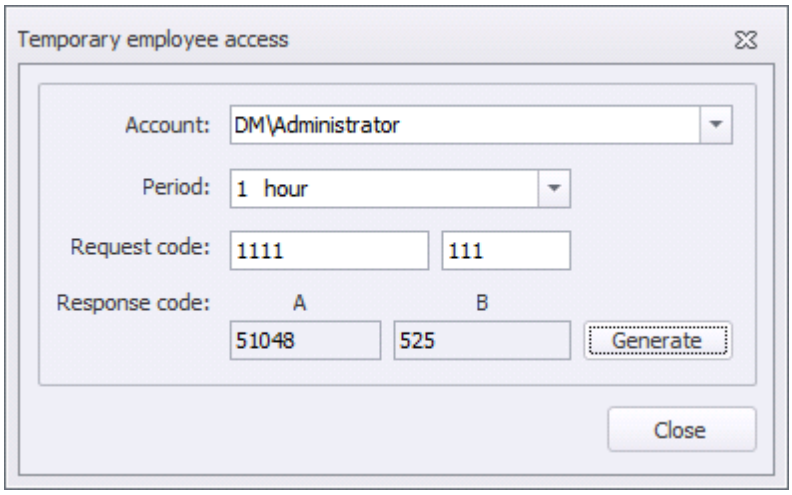
An employee can request an access only if the **Show tray icon interface** option is selected (see "Common Settings for Clients").

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. From **Account** drop-down list select an account of employee to which a temporary access should be granted.
3. From **Period** drop-down list select time period for which a temporary access should be granted.
4. To **Request code** field enter a code sent by employee.
5. Click **Generate**.

   The code which should be sent to employee is displayed in **Response code** field.
6. Click **Close**.

# 3.5 Viewing Events

InfoWatch Device Monitor Clients installed at managed workstations 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,**

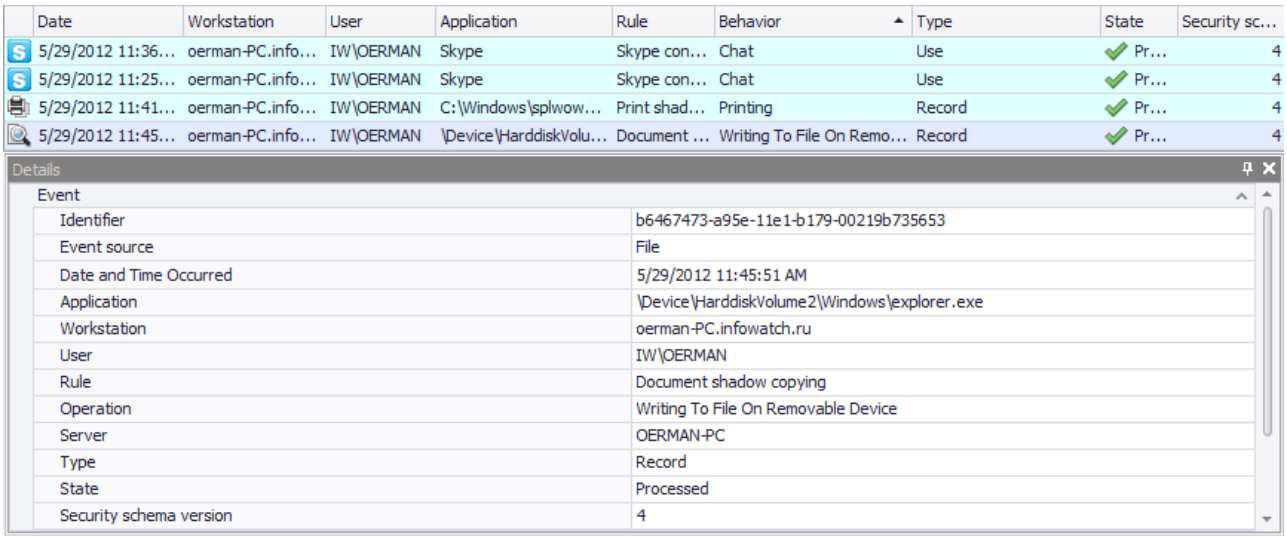
click the filter name in the filter list.

There are two predefined filters:

- **All events**
- **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;<br>- **Devices** – Device Monitor;<br>- **Printer** – Print Monitor;<br>- **Skype, XMPP, MMP** – IM Client Monitor;<br>- **FTP** – FTP Monitor;<br>- **HTTPS** – HTTPS Monitor;<br>- **Network** – Network Monitor. |
| Date | Event date and time (in hours and minutes) registered on workstation. Device Monitor server keeps an event in UTC, and Management Console displays it according to the local time of a computer where Console installed | |
| Application | Executable file name and/or name of the process responsible for the action, if detected | |
| Workstation | Name of the workstation that registered the event | |
| Employee | Name of the domain (workstation 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 | |
| Operation | Employee initiated action or attempt | |
| Server | Name of InfoWatch Device Monitor server the Client transmits event information to | |
| Type | Action-based event type | - **Record** - adding or changing data (including renaming) on external device; sending files via messenger; sending print jobs to printer; voice chat; sending data via FTP<br>- **Use** - connecting an external device |

| | | |
|---|---|---|
| | | that allows unmonitored read/write operations or sending messages<br>- **Violation** - IM Client interceptor user-initiated violation<br>- **Warning** - user-initiated a ban or didn't give consent to use IM Client plug-in, while monitoring is required by security policy<br>- **Usage forbidden** – attempt of sending data via forbidden channel |
| State | Status of event processing on the server | - **New**<br>- **Processed**<br>- **Sent to Traffic Monitor** |
| Security schema version | Number of security schema version that was active on the workstation when the event was registered | |
| Operation verdict | Attribute of allowed action. For *Devices* events ( **Device Monitor** rule) the blocking is also available. | - **Allowed**<br>- **Forbidden** – only for *Devices* events<br>- **Unprotected data copying is disabled** – only for *Devices* events<br>- **Allowed (in white list)** - for whitelisted device events |
| **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<br>- **copy created** - shadow copy created successfully<br>- **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 workstation where the Client is installed | |
| **For events with *Skype, XMPP, MMP source*** | | |
| IM user ID | UIN of the user authorized in the messenger at workstation | |
| Object status | Shadow copy of transferred data | - **no copies created** - rule does not require shadow copying<br>- **copy created** - shadow copy created successfully<br>- **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 or voice record file size | |
| Shadow copy | File, message or chat shadow copy | - **No** - no shadow copy was created<br>- **Yes** - shadow copy created successfully |
| **For events with *Printer source*** | | |
| Document | Full name of the file sent to print | |
| Printer | Name of target network printer | |
| Object status | Result of creating shadow copy of the print job | - **no copies created** - rule does not require shadow copying<br>- **copy created** - shadow copy created successfully<br>- **copying error** - for example, if there is no free space on the client |
| **For events with *Ftp source*** | | |
| Object status | Result of creating shadow copy of transferred data | - **no copies created** - rule does not require shadow copying<br>- **copy created** - shadow copy created successfully<br>- **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 | |
| 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<br>- **Yes** – shadow copy created successfully |
| **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. | |

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

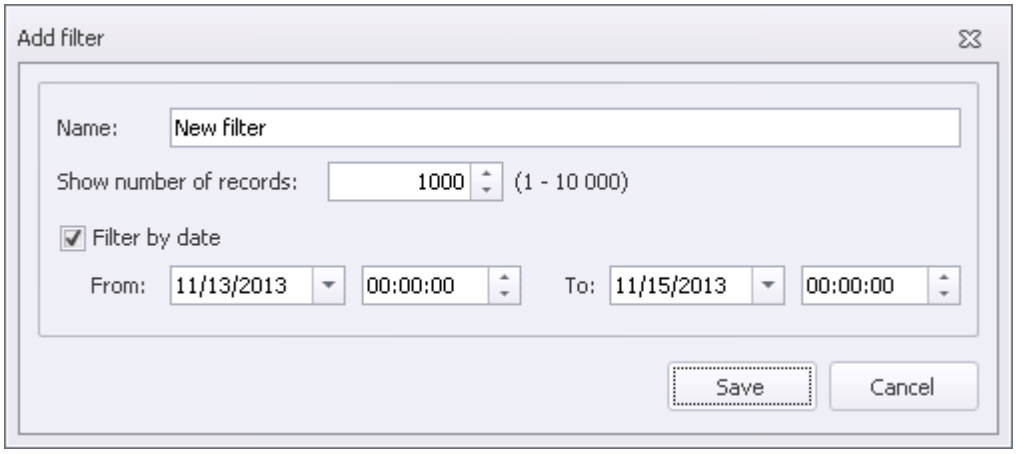
In addition to predefined filters you can create custom filters to view event information.

**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**;<br>• click **Add Filter** at the top of Navigation pane. |
| Editing filter | 1. In **Events** area of Navigation pane, select the name of the filter you want to edit.<br>2. Take one of the following steps:<br>• In Main Menu click **Edit > Edit Filter**;<br>• click **Edit Filter** at the top of Navigation pane.<br>• double-click selected filter name |

These actions open **Add filter** dialog.




3. Specify filter options in **Edit Filter** dialog:
   - **Name**.
   - **Show number of records**. Limit on the number of entries displayed in Management Console workspace (1000 records by default).

     **Note:**
     If there is more events matching filter conditions than **Show number of records** value, then the most matching to the primary filter value will be displayed.

   - 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.
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 needer 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 workstation 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** which requires the following:

- Target workstations must meet hardware and software requirements: see "InfoWatch Device Monitor Client Hardware and Software Requirements".
- Proactive virus protection for workstations must be turned off.
- 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).

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 workstations for the selected task.

**Details** panel displays the following parameters for selected task:

| Parameter | Description |
|---|---|
| Name | Original name of the task |
| Description | Original description of the task |
| Type | One of the following task types:<br>• primary distribution<br>• change password<br>• update<br>• uninstall |
| Status | Current task status. Possible values:<br>• running<br>• stopped<br>• completed |
| Restart period, min | Intervals between task launches on workstation, if the previous attempt failed, in minutes.<br>If the task fails, it won't be launched again. |
| Number of restart trials | Maximum number of retries to restart distribution task on workstation . 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** | |
| Ask for employee permission for loading Skype plugin | Indicates that Skype will display a request to start InfoWatch Device Monitor interceptor after Client installation. For further details, see "General System Settings" and "Creating Installation Package". |
| 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" |
| Show Windows interface tray icon | Indicates that an icon will be displayed in Windows taskbar notification area on Client computer. Client information and list of controlled devices is available upon a click on this icon. |
| Uninstallation product password | Shows if the password requested from employee that attempts to remove Device Monitor Client. |
| **For primary distribution and update tasks** | |
| Installation directory | Installation directory for Device Monitor Client at target workstations. |
| Installation login | Name of the Console user that launches the task on workstations. |
| Waiting fir restart duration, hours | Workstation reboot waiting period (in hours); if the workstation 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 force reboot | Indication whether the warning is shown before forced reboot (the employee has 5 minutes to complete all operations) or reboot will be made mandatory. |
| **For change password tasks** | |
| Uninstallation product password | Shows if the password requested from user that attempts to remove Device Monitor Client. |

Each target workstation's main screen workspace displays the following parameters:

| Parameter | Description |
|---|---|
| Address | Workstation IP address or domain name |
| Status | Current status of task for the relevant workstation. Possible values:<br>• **Not running**<br>• **Preparing**<br>• **In progress**<br>• **Waiting for reboot** (only for installation and upgrade tasks)<br>• **Error** (for further details, see "Client Installation Errors")<br>• **No access**<br>• **Completed** |
| Client version | Client version currently installed on workstation |
| Operation system | Workstation operating system. |
| System type | Type of operating system on the workstation: x64 or x32. |
| Connections count | Number of connection attempts to unavailable workstation. |
| Time | Date and time of the last connection to workstation. |

## 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 workstations must meet hardware and software requirements: see "InfoWatch Device Monitor Client Hardware and Software Requirements".
- Proactive virus protection for workstations must be turned off.
- Workstations 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).

- The root centers of certification must be up-to-date at the workstations.

Additional requirements vary depending on distribution method:

**Method 1:**

Distribute `Setup.DeployAgent.msi` installation package (provided along with installation software) to target workstations.

**Method 2:**

Transmit Distribution agent through shared administrative resources:

- Workstation 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 workstations through shared administrative resources, the following requirements must be met:

- If workstation with Windows XP is outside a domain, in security policy settings of this workstation set **Network access configuration parameter: Sharing and security model for local accounts** value to `Classic`.
- Workstations 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 workstation 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 workstations and starts automatically during task execution, receiving Client updates from server.

**Warning!**
If server account doesn't have administrator rights on all target workstations, primary Device Monitor Client distribution will require credentials of an account having administrator rights at:

- all target workstations
- 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").

**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. Select **Initial deployment task**, enter task name and description and click **Next**.
4. Create a list of workstations which you need to install Device Monitor Client to. To add workstation (or several workstations):

a. Click **Add**. **Select computer** dialog will display a list of workstations from:
   - directory service (Active Directory for example)
   - Microsoft Windows Network
   - ones registered before (for example, after manual Client installation) and belonging to workstation groups (**DM server computers** node).

b. Flag workstations or workstation 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 workstation name or IP address in the line at the bottom of dialog box. When listing addresses, separate them with semicolons.

c. After you specify the workstations you want to add, click **OK**. **Select computers** dialog will be closed. Selected workstations list will be displayed in **Task target computers list** area.

   To remove a workstation from the list, select it and click **Remove**.

   When you make a full list of workstations 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. Configure task running settings:

- 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.
- **Wait for reboot without notifying the employee**. If this check box is flagged, the Client will await for workstation reboot for specified time (in hours) without any employee notifications.
- **Notify the employee about reboot necessity and wait for reboot**. If this check box is flagged, then after "silent" reboot awaiting ends (see **Wait for reboot without notifying the employee** setting), or just after installation, Device Monitor Client starts to notify employee that the reboot is required. If needed, change notifications duration and intervals and edit the message text.
- **Show a warning before force reboot** - if checked, the message about force reboot will appeared and employee will have 5 minutes to finish all operations at computer. If is not checked, the reboot will start forcibly.

  **Warning!**
  The message about force reboot will appeared If neither **Wait for reboot without notifying the employee** setting, no **Notify the employee about reboot necessity and wait for reboot** setting do not flagged or their durations are expired but employee did not reboot the workstation.

Click **Next**.

7. 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.
   - **Ask employee permission to work Skype plug-in** - after installation of the Client, Skype will display a requesting to launch Skype interceptor:
     - If employee agrees to launch interceptor, it will work until it is disabled in Skype menu (**Tools -> Options -> Advanced settings -> Manage other programs' access to Skype**). In the latter case, Skype will be forced to stop.
     - If the employee blocks the interceptor, Skype will be stopped. If you try start Skype later, you will be prompted to give another permission to use interceptor.
     - If this box is not flagged, interceptor doesn't require employee's permission.

     **Warning!**
     Not notifying the user about interceptor operation may contradict the applicable laws of your country.
   - **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"
   - **Show Windows tray icon interface** - an icon will be displayed in Windows taskbar notification area at managed workstation. Upon a click on this icon the Client information and list of controlled devices is available.
   - 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 workstations.

     **Warning!**
     The **Warning** 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**.
8. 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 Workstations".

**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 workstations that require Device Monitor Client update. To add workstation (or several workstations):
   a. Click **Add**. The **Select computers** dialog, **DM server computers** node, contains the list of workstations 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 workstations or workstation 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 workstations you want to add, click **OK**. **Select computers** dialog will be closed. Selected workstations list will be displayed in **Task target computers list** area.

   To remove a workstation from the list, select it and click **Remove**.

   When you make a full list of workstations click **Next**.
5. 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**.
6. Look through the task summary. If you need to change any settings click **Back** to return. If all settings are correct, click **Finish**.

# 3.6.5 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 workstations that need their uninstallation passwords to be changed on **Deployment target computers** screen. To add workstation (or several workstations):
   a. Click **Add**. The **Select computers** dialog, **DM server computers** node, contains the list of workstations

where Device Monitor Client is installed.

b. Flag workstations or workstation 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 workstations you want to add to task, click **OK**. **Select computers** dialog will be closed. Selected workstations list will be displayed in **Task target computers list** area.

To remove a workstation from the list, select it and click **Remove**.

When you make a full list of workstations 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 click **Next**.
4. Create a list of workstations you are removing Device Monitor Client from in **Deployment target computers** screen. To add workstation (or several workstations):

   a. Click **Add**. The **Select computers** dialog, **DM server computers** node, contains the list of workstations where Device Monitor Client is installed.

   b. Flag workstations or workstation 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 workstations you want to add, click **OK**. **Select computers** dialog will be closed. Selected workstations list will be displayed in **Task target computers list** area.

   To remove a workstation from the list, select it and click **Remove**.

   When you make a full list of workstations click **Next**.
5. 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**.
6. Look through the task summary. If you need to change any settings click **Back** to return. If all settings are correct, click **Finish**.

## 3.6.7 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 thetask. 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 > Run**;<br>• click **Run** located at the top of Navigation pane. |
| Stop task | • in the Main Menu select **Edit >Stop**;<br>• click **Stop** at the top of Navigation pane. |
| Edit list of workstations in task | Right-click workstation row and select **Add workstation to task** or **Delete workstation from task**.<br>**Warning!** You can't remove a workstation if the task is running and not completed. |
| Edit task | • in the Main Menu select **Edit > Edit task**;<br>• click **Edit task** at the top of Navigation pane.<br>• right-click on task name and select **Edit task**.<br>Specify new settings for the task like it is done for a new task (see "Creating Primary Distribution Task", "Creating Updating Task", "Creating Uninstallation Password Reset Task", "Creating Uninstallation Task") |
| Delete task | • in the Main Menu select **Edit > Delete task**;<br>• click **Delete task** at the top of Navigation Pane.<br>• right-click on task name and select **Delete task**.<br>**Warning!** You can't remove a task with workstation that has a running task. |
| View workstation error log | • right click workstation row and select **Workstation Log**;<br>• double-click target workstation row. |

## 3.6.8 Client Installation Errors

You may encounter installation problems during remote InfoWatch Device Monitor client applications installation tasks to workstations. 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 workstation is not available (switched off or disconnected from network).
4. In target workstation row, do one of the following:
   - right-click and select **Workstation Log**;
   - double-click target workstation row.

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:

- workstation 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 workstation does not allow administrative resources;
- account in use doesn't have enough rights on target workstation.

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, 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 workstation 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.

**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. At **InfoWatch Device Monitor servers pool** 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 workstations.
   Specify local or network directory where to the installation packages will be saved.
   Click **Next**.
3. Specify options of workstation reboot:
   - **Wait while employee reboots computer**. If this check box is flagged, the Client will await for workstation reboot for specified time (in hours) without any employee notifications.
   - **Remind employee about reboot**. If this check box is flagged, then after "silent" reboot awaiting ends (see **Wait while employee reboots computer** setting), or just after installation, Device Monitor Client starts to notify employee that the reboot is required. If needed, change notifications duration and intervals and edit the message text.

     **Warning!**
     If neither **Wait while employee reboots computer** setting, no **Remind employee about reboot** setting do not flagged or their durations are expired but employee did not reboot theworkstation, then the Client displays a notification about forced reboot and allows 5 minutes to end operations. Then the computer will be forced to reboot.

   Click **Next**.
4. Define Client settings before it connects to the server for the first time:
   - **Ask employee permission to work Skype plug-in** - when Client installation is finished, Skype will display a request to launch Skype interceptor:
     - If employee agrees to launch interceptor, it will work until it is disabled in Skype menu (**Tools -> Options -> Advanced settings -> Manage other programs' access to Skype**). In the latter case,

Skype will be forced to stop.
- If the employee blocks the interceptor, Skype will be stopped. If you try start Skype later, you will be prompted to give another permission to use interceptor.
- If this box is not flagged, interceptor doesn't require employee's permission.

> **Warning!**
> Not notifying the user about interceptor operation may contradict the applicable laws of your country.

- **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"
- **Show Windows tray icon interface** - an icon will be displayed in Windows taskbar notification area at managed workstation. Upon a click on this icon the Client information and list of controlled devices is available.

Click **Next**.

5. 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:

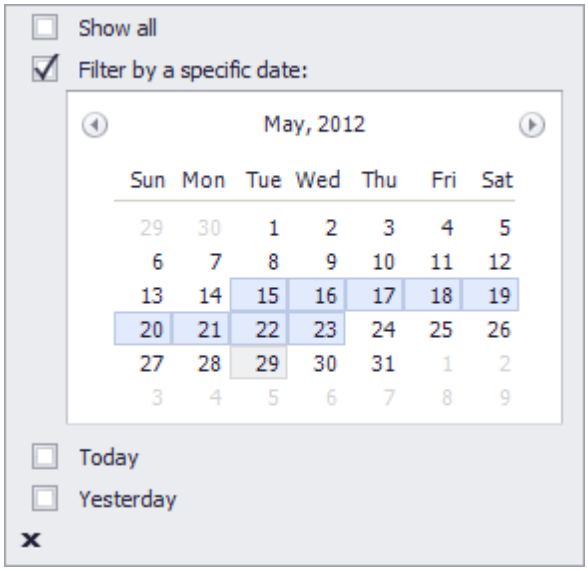
- Filter by Date
- Applying Standard Filters
- Custom Filter
- Editing Filters
- Removing a Filter

### 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 workstation 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,**

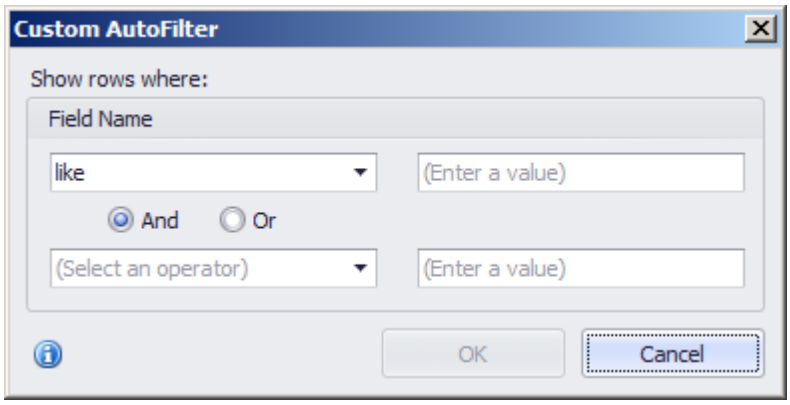
repeat simple filtering procedure against all filter attributes you want to apply.

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.

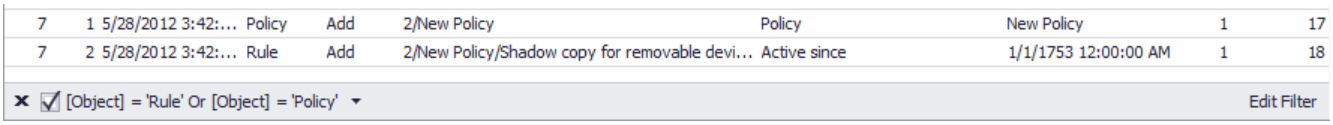
> **Note:**
> You can use comparison operators to limit filtering criteria: *equal*, *not equal*, *greater than*, *greater than or equal to*, *less than*, *less than or equal to*; values *empty* (blank) and *nonempty* (non-blank field); or text filter with a mask. To get a text filter syntax tip, click .

   - 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.



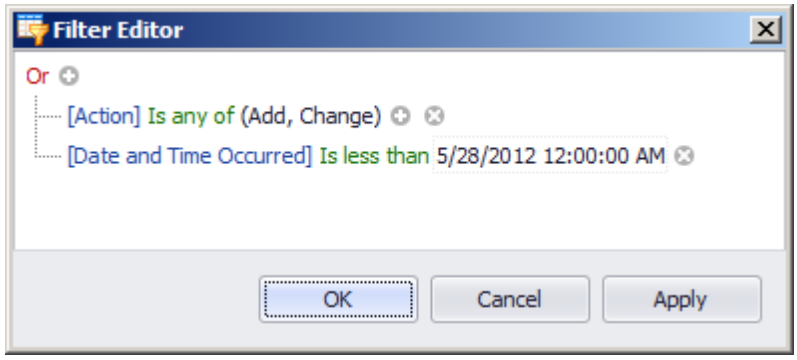

To remove filter and view all items, clear the check box in filter string. To apply the filter again, select the check box.

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<br>2. Select the value from the menu |
| Add a simple condition | Click the button ⊕ to the right of the logical operator<br>or<br>Click **Add Condition** in logical operator menu |
| Delete condition | Click the button ⊗ at the end of condition string |
| Add criteria group | 1. Click the logical operator name<br>2. Select **Add Group** in the menu |
| Delete criteria group | 1. Click the name of operator criteria group<br>2. Select **Delete Group** in the menu |
| Delete all criteria | Click **Clear All** in logical operator menu |

3. Click **Apply**, to filter 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 Workstations | 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 workstation groups | |
| Add new workstation group | Ctrl+N |
| Edit workstation group | Ctrl+E |
| Delete workstation group | Ctrl+D |
| Manage workstations | |
| Add workstation | Ctrl+Shift+I |
| Remove workstation from a group | Delete |
| Delete workstation 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 workstation to selected task | Ctrl+Shift+N |
| Remove workstation from selected task | Delete |
| Display target workstation error log | Ctrl+L |

# 4 Troubleshooting

If a server error occurs, you can view all server module error and informational messages in Windows Application Log. For server error code descriptions, see Windows Application Log section "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 workstation was removed from security schema, but its information is displayed in **Workstations** section

**Description:** Removed workstation record remains in security schema with **Agent Disabled** status.

**Solution:** You can delete managed workstations records manually, if necessary. You can find more

information on how to remove a workstation from security schema in "Removing Workstation from Security Schema".

# 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 facade for clients)<br>Event source in Windows Log: `InfoWatch.DeviceMonitor.Server.Client`<br>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 workstation 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 workstation 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 workstations 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 workstations. 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 |

| Error code | Severity | Description |
|---|---|---|
| | | workstation from security schema (see "Removing Workstation 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 |
| 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)<br>Event source in Windows Log: `InfoWatch.DeviceMonitor.TrafficMonitor.Connector`<br>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. |

| Error code | Severity | Description |
|---|---|---|
| 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 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)<br>Event source in Windows Log: `InfoWatch.DeviceMonitor.Server.Core`<br>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. |

| Error code | Severity | Description |
|---|---|---|
| 3003 | Error | Error deleting GUI facade channel registration. Contact InfoWatch support. |
| `InfoWatch.DeviceMonitor.Server.Database` Module (DB interaction Module)<br>Event source in Windows Log: `InfoWatch.DeviceMonitor.Server.Database`<br>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 |
| 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 workstation 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 (ZAO)

Phone/fax: +7(495)229-00-22

Sales department: sales@infowatch.com

Technical support service: support@infowatch.com

Web site: www.infowatch.com

**InfoWatch©**