

INFOWATCH

Using Device Monitor Management Console

Using Device Monitor Management Console

© InfoWatch
Tel./Fax +7 (495) 229-00-22
http://www.infowatch.com
Revision date: 2016-08-31

TABLE OF CONTENTS

1 MANAGEMENT CONSOLE (DM) OVERVIEW 7

1.1 AUTHORIZATION AND CONNECTING TO INFOWATCH DEVICE MONITOR SERVER 7
1.2 MANAGEMENT CONSOLE (DM) MAIN SCREEN 8
1.2.1 Configuring Management Console (DM) Main Screen Elements 10
1.3 MANAGEMENT CONSOLE (DM) SECTIONS 10

2 MANAGING CONSOLE (DM) ACCOUNTS 12

2.1 VIEWING MANAGEMENT CONSOLE (DM) ACCOUNTS DETAILS 13
2.2 ADDING NEW MANAGEMENT CONSOLE (DM) ACCOUNT 15
2.3 LOCKING OR UNLOCKING MANAGEMENT CONSOLE (DM) ACCOUNT 16
2.4 EDITING MANAGEMENT CONSOLE (DM) ACCOUNT 16
2.5 DELETING MANAGEMENT CONSOLE (DM) ACCOUNT 17
2.6 MANAGEMENT CONSOLE (DM) SECURITY SCHEMA OPERATION ACTIVITY LOG 17
2.6.1 Viewing Audit Log 18
2.6.1.1 Selector Values 19
2.6.2 Log Records Filtering 20
2.6.2.1 Date/Sequence Number Tab 22
2.6.2.2 Object/Action Tab 23
2.6.2.3 Additional Tab 23
2.6.3 Deleting Records from Log 24
2.6.4 Exporting Log Records 24
2.6.5 Analyzing Log Records in Microsoft Excel 25

3 GENERAL SYSTEM SETTINGS 26

3.1 COMMON SETTINGS FOR CLIENTS 26
3.2 SETTINGS OF CORPORATE NETWORK 29
3.3 NETWORK TRAFFIC CONTROL 32
3.4 DEVICE MONITOR SERVER SETTINGS. CONNECTING TO TRAFFIC MONITOR SERVER 34
3.5 CONNECTING TO LDAP SERVER 36
3.6 EMPLOYEE NOTIFICATIONS ABOUT POLICY (DM) VIOLATIONS 38
3.7 EXCLUSION OF APPLICATION FROM INTERCEPTION 41
3.8 APPLICATION CONTROL 43
3.9 EVENT STORAGE 45
3.10 SYNCHRONIZATION OF TRAFFIC MONITOR POLICIES 46
3.11 IMPORT/EXPORT CONFIGURATION 47
3.12 INFOWATCH DEVICE MONITOR SERVER MANAGER 48
3.13 STOPPING AND STARTING DEVICE MONITOR AGENT 50
3.13.1 Stopping agent remotely/starting agent 50
3.13.2 Stopping/starting agent locally 51

4 MANAGING SECURITY SCHEMA 53

4.1 SECURITY SCHEMA ORGANIZATION 53
4.1.1 Security Policies (DM) and Rules (DM) 54
4.1.2 Employees and Employee Groups 55
4.1.3 Workstations and Workstation Groups 56
4.1.4 Uploading Security Schema to Managed Workstations 56
4.2 SECURITY SCHEMAS OVERVIEW 56
4.2.1 Viewing Active Security Schema 57
4.2.2 Viewing Old Security Schema 58
4.2.3 Security Schema Comments 59
4.2.4 Editing Security Scheme 60

4.2.4.1 Awaiting Editing Ends. Unlocking Security Schema 61
4.2.5 Updating Security Schema 62
4.2.6 Exporting/Importing Security Schema 62
4.3 SECURITY SCHEMA SETUP 63
4.3.1 Security Policies (DM) 64
4.3.1.1 Viewing Security Policies (DM) 64
4.3.1.2 Adding and Configuring New Security Policy (DM) 67
4.3.1.3 Edit Security Policy (DM) 68
4.3.1.4 Deleting Security Policy (DM) 69
4.3.2 Rules (DM) 69
4.3.2.1 Rules Application (DM) 70
4.3.2.1.1 Device Monitor Rules (DM) Application 70
4.3.2.1.2 Creating Shadow Copies and Blocking Operations Due to Free Space Shortage 72
4.3.2.2 Adding a Rule (DM) 73
4.3.2.2.1 Configuring Application Monitor Rule (DM) 74
4.3.2.2.2 Configuring Clipboard Monitor Rule (DM) 77
4.3.2.2.3 Configuring Cloud Storage Monitor Rule (DM) 78
4.3.2.2.4 Configuring Device Monitor Rule (DM) 80
4.3.2.2.5 Configuring File Monitor Rule (DM) 83
4.3.2.2.6 Configuring FTP Monitor Rule (DM) 85
4.3.2.2.7 Configuring HTTPS Monitor Rule (DM) 87
4.3.2.2.8 Configuring IM Client Monitor Rule (DM) 89
4.3.2.2.9 Configuring Mail Monitor Rule (DM) 92
4.3.2.2.10 Configuring Network Monitor Rule (DM) 95
4.3.2.2.11 Configuring Photo Monitor Rule (DM) 97
4.3.2.2.12 Configuring Print Monitor Rule (DM) 98
4.3.2.2.13 Configuring ScreenShot Control Monitor Rule (DM) 99
4.3.2.2.14 Configuring ScreenShot Monitor Rule (DM) 101
4.3.2.3 Editing a Rule (DM) 103
4.3.2.4 Deleting a Rule (DM) 104
4.3.2.5 Copying a Rule (DM) 105
4.3.3 Employees 105
4.3.3.1 Viewing Employee and Employee Groups Details 106
4.3.3.2 Viewing Resultant Policy (DM) and Resultant White List for an employee 107
4.3.3.3 Adding and Editing an Employee Group 108
4.3.3.4 Deleting Employee Group 110
4.3.3.5 Adding Employee Account to a Group 111
4.3.3.6 Editing Employee Account 112
4.3.3.7 Removing Employee Account from Employee Group 113
4.3.3.8 Deleting Employee Account from Security Schema 114
4.3.4 Computers 115
4.3.4.1 Viewing Computer Details 115
4.3.4.2 Viewing Resultant Policy (DM) and Resultant White List for Computer 117
4.3.4.3 Adding and Editing a Computer Group 119
4.3.4.4 Deleting Computer Group 122
4.3.4.5 Adding Computer to a Group 122
4.3.4.6 Removing Computer from a Group 124
4.3.4.7 Deleting Computer from Security Schema 124
4.3.4.8 Updating Clients at Managed Computers 125
4.3.4.9 Diagnostics of the Workstation 126
4.3.5 Mobile Devices 126
4.3.5.1 Preparing a Mobile Device on Android Platform 128
4.3.5.1.1 Step 1. Enabling "USB debugging" mode 128
4.3.5.1.2 Step 2. Connecting to the computer 129
4.3.5.1.3 Step 3. Drivers installation 130
4.3.5.2 Preparing a Mobile Device on iOS Platform 130
4.3.5.2.1 Step 1. Jailbreaking the mobile device 130
4.3.5.2.2 Step 2. Installing iTunes 131
4.3.5.2.3 Step 3. Connecting to the computer 131
4.3.5.2.4 Step 4. Authorizing the device on the computer 131
4.3.5.3 Adding a Mobile Device to Computer Group 132

4.3.5.4 Adding a Mobile Device through Appointment to Employee 134
4.3.5.5 Deleting the Mobile Device 136
4.3.6 White Lists 136
4.3.6.1 Viewing White List Details 137
4.3.6.2 Adding White List 138
4.3.6.2.1 Adding Device Entry 139
4.3.6.2.2 Deleting Device Entry 141
4.3.6.3 Defining Entry Validity Period 142
4.3.6.4 Editing White List 143
4.3.6.5 Deleting White List 143
4.3.7 Signatures 144
4.3.7.1 Adding Signature Category 144
4.3.7.2 Editing Signature Category 146
4.3.7.3 Deleting Signature Category 146
4.3.8 Application Protocol 147
4.3.8.1 Creating an Application List and Adding Applications 148
4.3.8.2 Creating and Editing the Application Protocol Filter 149
4.3.8.3 Adding Application to List Automatically 150
4.3.8.4 Adding Application to List Manually 151
4.3.8.5 Exporting Application Protocol 152
4.4 Temporary Employee Access to Network 152
4.5 Temporary Employee Access to Devices 154

5 VIEWING EVENTS 157

5.1 Event Filters 164
5.2 Deleting Events 166

6 CLIENTS REMOTE INSTALLATION, UPDATING AND UNINSTALLATION 168

6.1 Viewing Tasks 169
6.2 Preparing Primary Client Installation. Distribution Agent 171
6.2.1 Enabling Shared Administrative Resources 172
6.2.2 Firewall Settings 172
6.3 Creating Primary Distribution Task 173
6.4 Creating Update Task 177
6.5 Creating Uninstallation Password Reset Task 179
6.6 Creating Uninstallation Task 180
6.7 Launching, Pausing, Editing, and Deleting Tasks 181
6.8 Client Installation Errors 182
6.9 Creating Installation Package 184

7 ADDITIONAL FEATURES 187

7.1 Filter Table Contents 187
7.1.1 Filtering by Date 187
7.1.2 Applying Standard Filters 188
7.1.3 Custom Filter 189
7.1.4 Editing Filters 190
7.1.5 Removing a Filter 191
7.2 Grouping or Sorting Entries 191
7.3 Hotkeys 192

The Management Console (DM) is designed to address the following tasks:

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

To use Management Console (DM) you have to be familiar with Microsoft Windows OS basics.
For more information on Management Console (DM) workflow, see:

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

1 MANAGEMENT CONSOLE (DM) OVERVIEW

Management Console (DM) basics are available in the following subsections:

- Authorization and Connecting to InfoWatch Device Monitor Server;
- Management Console (DM) Main Screen;
- Management Console (DM) Sections.

1.1 Authorization and Connecting to InfoWatch Device Monitor Server

When working with DM Management Console, you need a permanent connection with Device Monitor Server. For this, you need to go through **authorization**, during which user permissions to start the Management Console are defined.

When you first start DM Management Console, the System uses the data (username and password) of the account with the **Superuser** role (the Superuser role is created during installation of the server, for details, see "*Traffic Monitor. Installation Guide*", "Server End Installation Procedure" article").

To start working with DM Management Console:

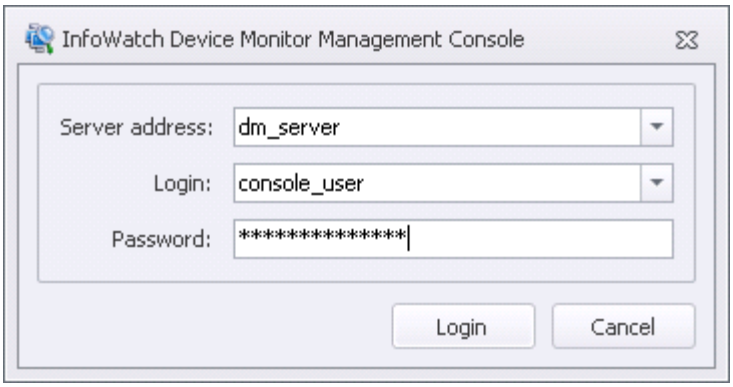
1. Start the Management Console (DM). For this, in the **Start** menu, choose **Programs** > **InfoWatch** > **Device Monitor** > **Management Console**.
2. Perform the authorization procedure as described below.

For successful authorization, the following conditions should be met:

- the database contains a user account with specified parameters;
- a role is assigned to the user account;
- the user account is active (not active);
- the user account is not blocked.

Enter the data for authorization in the connection dialog box.

8



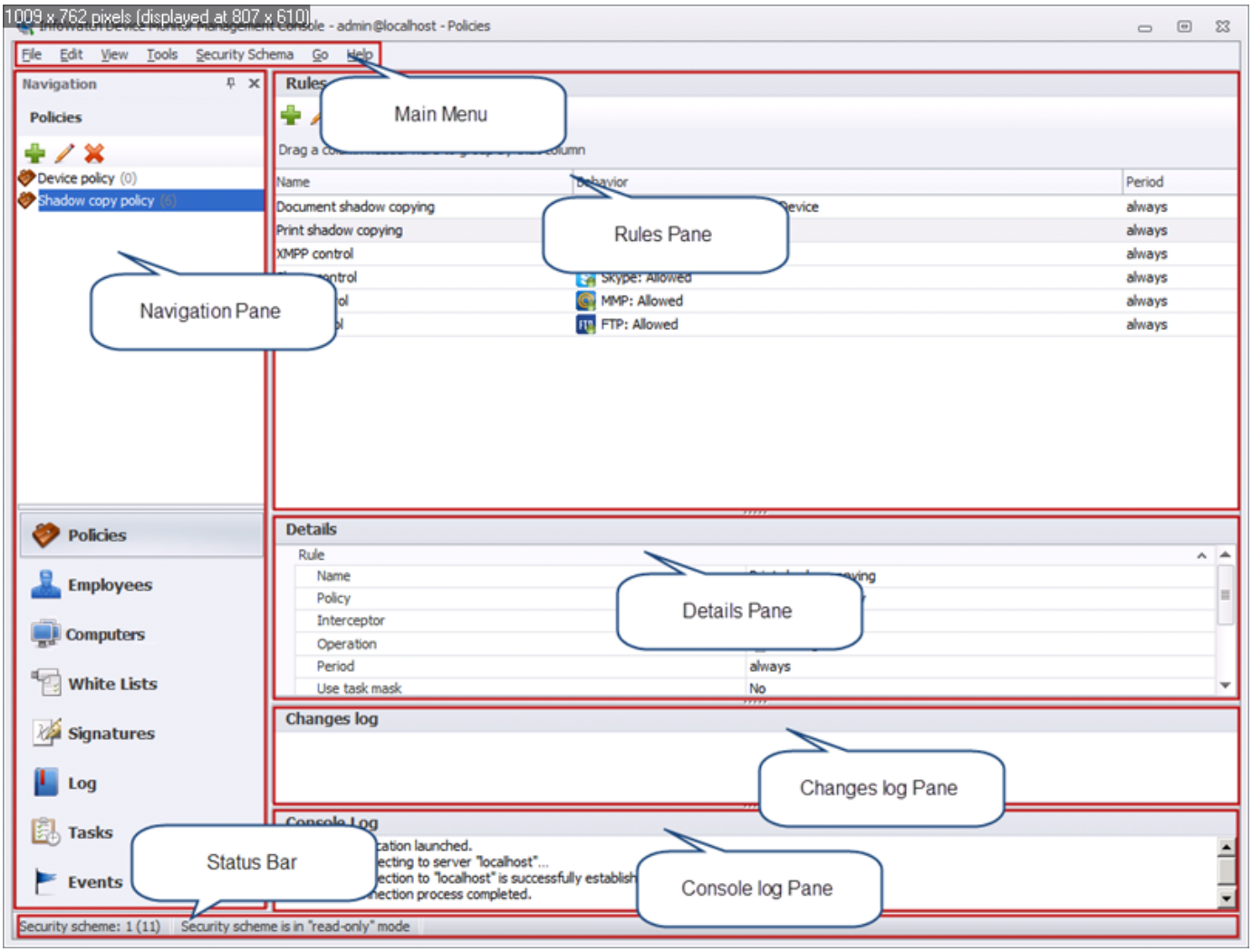
Parameter	Description
Server address	FQDN of the server, the Management Console is connecting to. Th default port for communication between the server and Management Console is 15003. If this port has been changed, enter the server address as follows: `dm_server:port`
Login	Name of the user account
Password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

At the first launch of DM Management Console, logon dialog fields are empty. Later, **Server address** and **Login** fields will contain the credentials entered during the previous authorization attempt. You must fill the **Password** field each time you are trying to log in.
You can track the status of connection with the server via system messages on the **Console log** panel (see "DM Management Console Main Screen").

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

1.2 Management Console (DM) Main Screen

After successful authorization in Management Console (DM), the main window is displayed on the screen:



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

The main screen contains elements required for working with the Management Console (DM):

- The **main menu** contains commands that give you access to all Management Console (DM) essential features.
- The **navigation** pane allows you to switch between different section of the Management Console (DM) and manage elements of the selected section.
- The **main screen workspace** allows you to view elements of the selected group and perform operations with these elements.
- The **toolbars** contain buttons for quick access to some functions of the Console (DM). The toolbars are located on the Navigation page (for elements of the selected section) and in the workspace (for the selected element).
- The **Details** pane displayed extended information about properties of the selected element.
- The **Changes log** pane displays all changes made by the current user and not saved in the security scheme.
- The **Console log** pane displays system messages.

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

General information on the current status is displayed on the status bar at the bottom of the main screen. In particular, the following information is displayed:

- number of the security scheme current version;
- mode of the security scheme;
- versions of control elements - in the **Computer groups** section.

1.2.1 Configuring Management Console (DM) Main Screen Elements

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

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

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

To customize Details panel,
double-click properties table title bar or use 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).

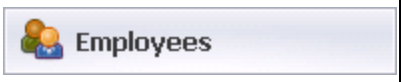
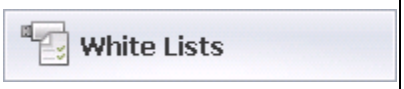
1.3 Management Console (DM) Sections

Management Console (DM) includes the following sections: **Policies, Employees, Computers, White Lists, Signatures, Log, Tasks** and **Events**. Each section corresponds to similar Navigation panel area. To go to the section, do any of the following:

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

- use Navigation panel buttons.

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

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

2 MANAGING CONSOLE (DM) ACCOUNTS

The system registers a Management Console (DM) account for each security schema operator. Account credentials are used for user authorization and access to certain operations.
Management Console (DM) 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 (DM) uses the following roles to manage user privileges:

- **Security officer** - Console (DM) end-user managing security schema and Server settings.
- **Local administrator** - Console (DM) administrator managing other accounts.
- **Super user** - built-in role which have all Console (DM) privileges. Superuser role is not designed for routine System operations: it is recommended to use it only for primary Console (DM) 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 (DM) 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 (DM) accounts	+	+	
Assign/delete Management Console account roles	+	+	
Block/unblock Management Console accounts	+	+	
Viewing Device Monitor Server settings. Configuring connection to Traffic Monitor server	+		+
View security schema versions	+		+
Edit security schema	+		+
Import/export security policies and rules	+		+
Viewing events	+		+

Clients Remote Installation, Updating and Uninstallation	+		+
Temporary Employee Access to Network	+		+
Temporary Employee Access to Devices	+		+

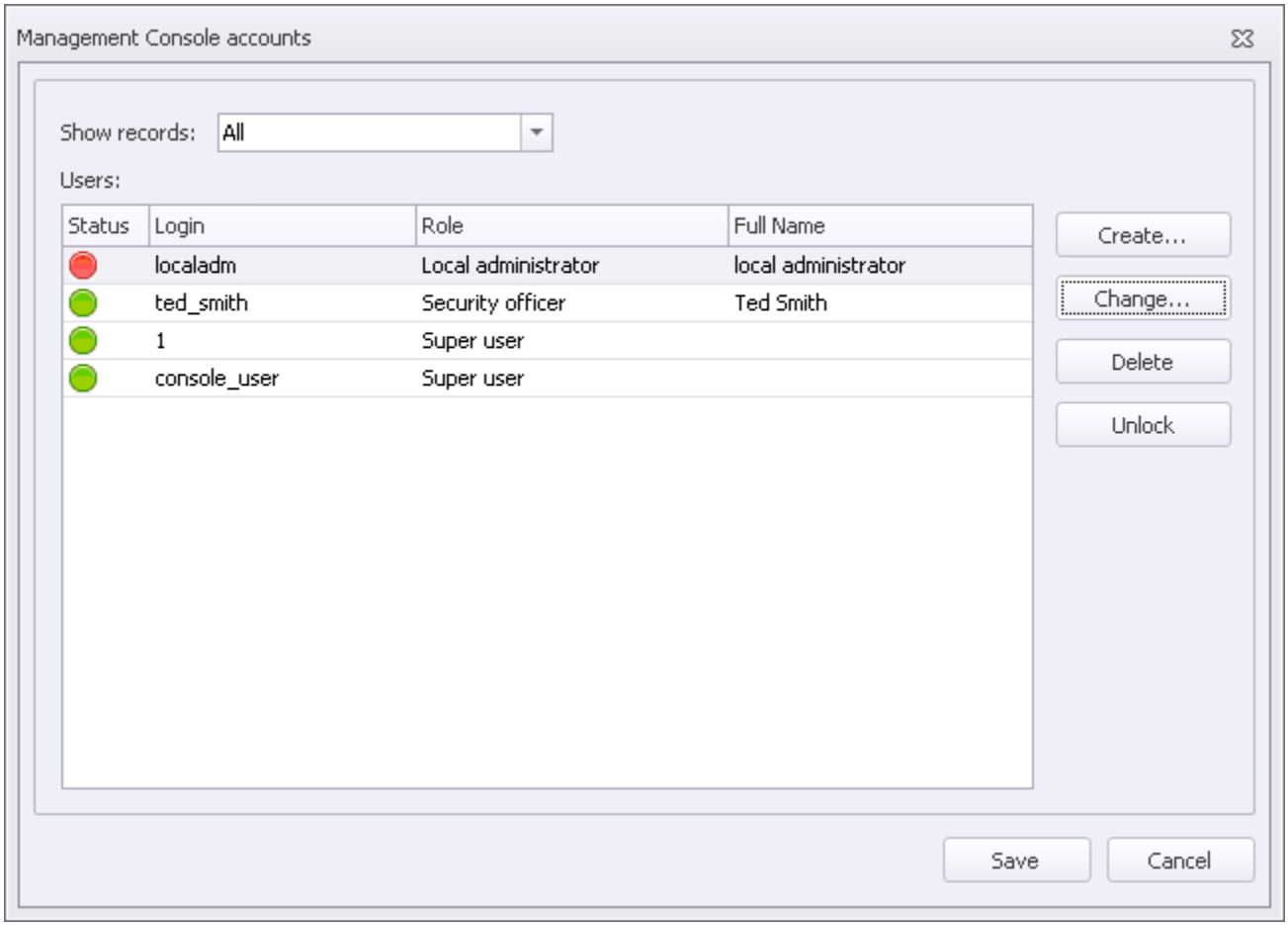
For more information on Management Console (DM) accounts management, see:

- Viewing Management Console (DM) Accounts Details;
- Adding New Management Console (DM) Account;
- Locking or Unlocking Management Console (DM) Account;
- Editing Management Console (DM) Account;
- Deleting Management Console (DM) Account;
- Management Console (DM) Security Schema Operation Activity Log.

2.1 Viewing Management Console (DM) 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 (DM) 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 (DM) can be only operated by the accounts in **Active** list. Deleted accounts can only be viewed.

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

- **Status**. Indicates is an account is active (), blocked () or deleted ().
- **Login**. Name of the user account.
- **Role**. Account role.

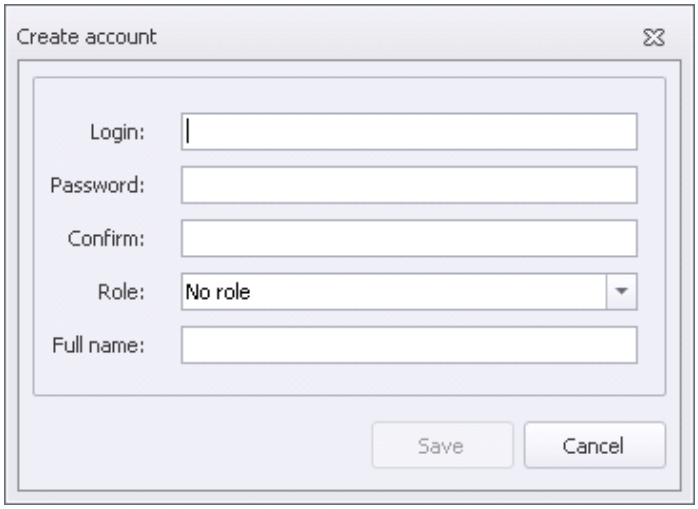
- **Full Name**. User's personal data.

Login and password, as well as account role and status are mandatory attributes. Detailed roles' description is available in "Managing Console (DM) Accounts".

2.2 Adding New Management Console (DM) Account

To add Management Console account:

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



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

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

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

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

Note:

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

2.3 Locking or Unlocking Management Console (DM) 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 (.png] state), click **Lock**.
4. Click **Save** to apply changes.

2.4 Editing Management Console (DM) Account

Warning!

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

To edit Management Console account:

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

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

2.5 Deleting Management Console (DM) 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.

2.6 Management Console (DM) Security Schema Operation Activity Log

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

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

2.6.1 Viewing Audit Log

You can manage audit log of Management Console (DM) users activities in Log section. To go to this section, click Log button on Navigation pane.
Security schema management activities are performed as transactions. Transactions appear as a set of records in the audit log. Each record contains information on one basic action (transaction step). Transaction may only contain one step and will be represented by a single record in audit log.
Configure filters to select records that meet certain criteria (for information on filters see "Log Records Filtering"). Filter list is displayed in Log area of Navigation pane. Records for selected filter are displayed in the main screen workspace.

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

To view full list of audit log records,
click **Show All Records** at the top of Navigation Pane.
To view filtered records,
click the filter name in the filter list.
Log information is displayed in a tabular list where each row contains a single record. Columns contain basic properties of log entries. Extended information on each record is available in **Details** panel.
To view advanced information for particular record,
select the row that contains the record name in the main screen workspace.
Details panel displays properties table containing the following information for selected entry:

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

Some information from the **Details** panel is duplicated in the main screen workspace.
Number of transaction steps (and, therefore, number of log records) varies depending on the object and actions performed.

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

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

Transaction number 3 is associated with adding a comment to security schema.
Transaction number 4 corresponds to one change applied to a security schema. This was done in 9 steps. Steps 1-3 changed rule (DM) named "New IM client rule" in "Test Policy" security policy (DM). Each step configures a single rule (DM) parameter: for example, in step 1 an operation was defined, in step 2-3 an action period was set. Steps 4-7 added a new rule (DM), step 8 deleted another one. In step 9 a comment was added to saving security schema version.
Transaction number 5 is associated with Audit Log records export. This transaction includes one step.

2.6.1.1 Selector Values

Selector parameter contains instructions for target object search. **Selector** parameter value depends on particular object and performed actions. Each object has a different set of **Selector** values.
Edited security schema version is displayed for modified security schema settings followed by "/" and name of modified parameter.
When editing an object (action **Modify**) **Selector** value contains object name before modification.
The following are sample interpretations of *Selector* values.

Example 1
Audit Log includes the following record:

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

This record indicates that a rule was changed in your security schema.
Selector value interpretation
Transaction took place while version 10 of security schema was active. A rule named "New IM client rule" was changed in policy named "test(new)": Skype access was denied.

Example 2
Audit Log includes the following record:

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

This record is a step of transaction which adds a computer group to the security schema.
Selector value interpretation
Transaction took place while version 3 of security schema was active. The "*Device*" policy was assigned to new computer group.

Example 3

Audit Log includes the following record:

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

This record indicates that audit log records were exported.

Selector value interpretation

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

2.6.2 Log Records Filtering

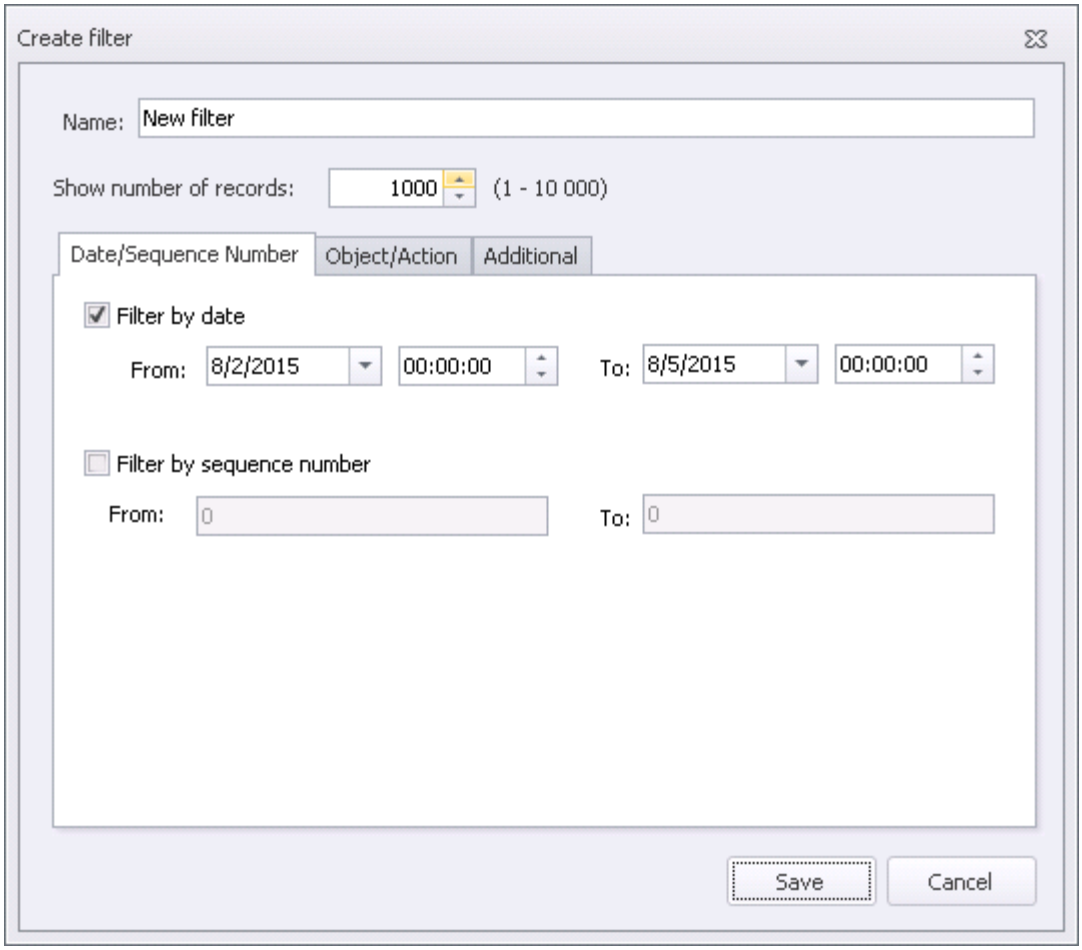
To access Audit Log records that meet certain criteria you can use filters.

To create a new filter or modify an existing one:

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

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

These actions open dialog with filter parameters configuration.



3. Specify general filter options in filter parameters configuration dialog::
    - **Name**.
    - **Show number of records**. Limit on the number of entries displayed in Management Console (DM) workspace (1000 records by default).
4. Specofy filtration criteria. Filtration configuration is performed on several tabs and is described in the following articles:
    - Date/Sequence Number Tab;
    - Object/Action Tab;
    - Additional Tab.

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

5. Click **Save**.

To remove filter:

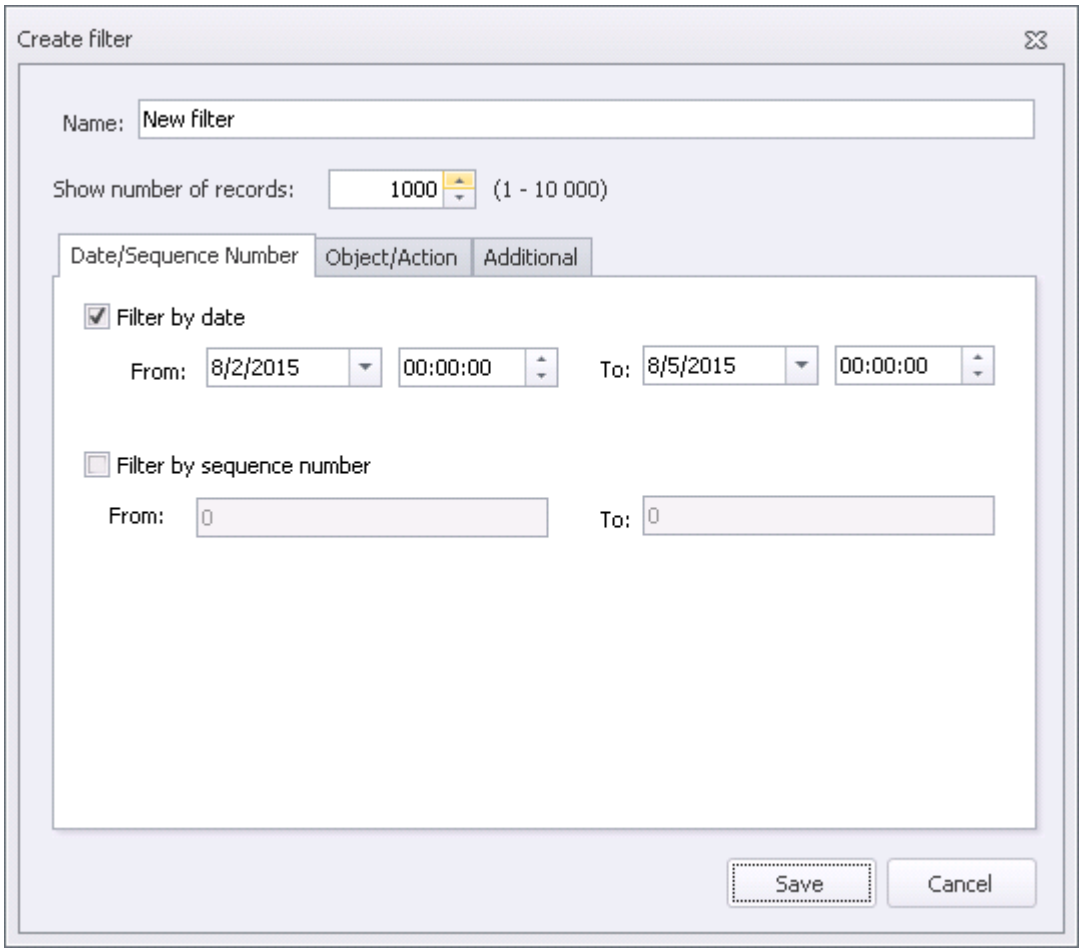
1. Go to **Log**.

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.

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:

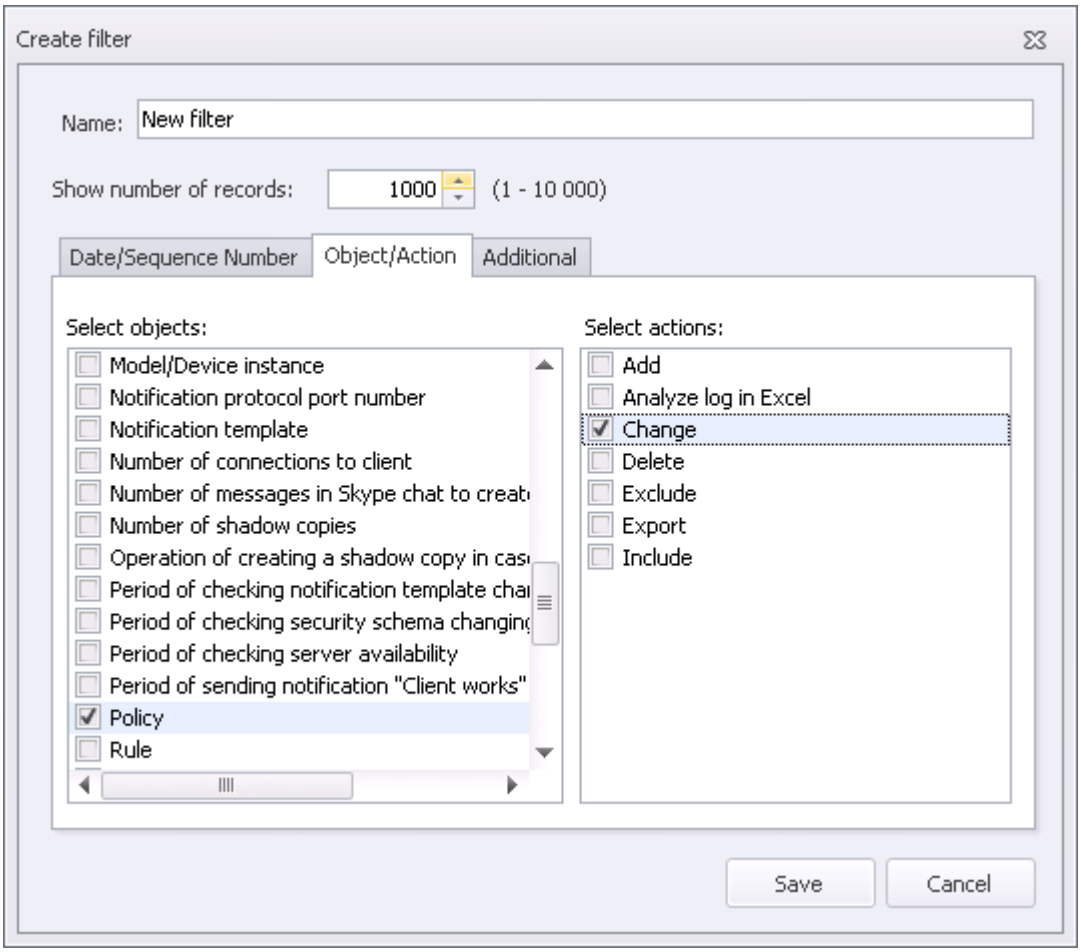
1. Flag **Filter by sequence number** check box.

2. Specify range of numbers in **From** and To fields respectively.
   Database record numbers start from 1.

2.6.2.2 Object/Action Tab

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

- target object;
- action performed.



To specify filtering criteria:

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

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 (DM) attributes (for example, Operation, Action , etc.)
- **Old Value**. Filter records using the rule's (DM) previous attribute value.

- **New Value**. Filter records using the rule's (DM) modified attribute value.
- **User**. Display user's actions list.
- **Windows Account**. Display list of actions performed on behalf of selected Windows account.
- **Computer**. Display selected computer activity records.

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

> **Note:**
> Additional filtering values are not case-insensitive.

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**.

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.

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:
   a.
   - 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 GENERAL SYSTEM SETTINGS

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

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

Warning!

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

3.1 Common Settings for Clients

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

To configure common settings for Device Monitor clients operation:

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

Parameter	Description
Connection	
Period of sending notification "Client works" to the server	Interval (sec) with which the Client sends data to Server

Period of checking server availability	Interval (sec) with which the Client checks Server availability.
Period of checking security schema changing for active client only	If a Client is in active mode (i.e. computer could not open UDP-port for receiving Server notifications) then the Client surveys Server itself to receive data on changing security schema. This parameter sets a survey period (sec).
Period of checking notification template changing for active client only	If a Client is in active mode (i.e. computer could not open UDP-port for receiving Server notifications) then the Client surveys Server itself to receive data on changing notification templates (see "Employee Notifications about Policy (DM) Violations"). This parameter sets a survey period (sec).
Client's disk space control	
Free clients' disk space	Minimal size of free disk space (%) of managed computer: when it is reached, shadow copies would not be created. I.e. if when shadow copy is created, free disk space at a client computer is less then parameter value, then neither shadow copy nor its part won't be created. See details in "Creating Shadow Copies and Blocking Operations Due to Free Space Shortage"
If there is not enough space for events	The managed computer dedicates space for storing 30000 events 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 (DM) defined for employee/computer, then any actions controlled by security schema could be denied. **To deny**, select Operation will be blocked. To allow all actions performed without a control, select **Operation will be permitted**.
Speed of sending data from client	
Limit the speed of sending data	If the channel is narrow you can prevent its excessively uploading by adjusting the speed of shadow copies sending to the Server. To do this check the setting and specify the upper speed limit (Kbps) in **Maximum speed of sending** data field.
Events	

Log events of device and cloud storage interceptors	Level of detailing when saving information about working with external devices received by Device Monitor and Cloud Storage Monitor interceptors: see details in "Configuring Device Monitor Rule (DM)", "Configuring Cloud Storage Monitor Rule (DM)", "Viewing Events". The following options are available: • **None** - do not save events • **In case access denied** - events are created only if security policy (DM) violation is attempted - i.e. when device usage was denied, including blocking attempts of access level exceeding. The using of external devices which are not forbidden by policies, is not logged • **All** - all actions are logged (connection/usage of any devices, even from white lists)
Log connections outside of corporate network	Level of detailing when saving information about data transfer by network connections received by Network Monitor interceptor: see details in "Configuring Network Monitor Rule (DM)". The following options are available: • **None** - do not save events • **In case access denied** - events are created only if security policy (DM) violation is attempted - i.e. when connection attempt was denied.
Agent activity on computer	
Show employee notifications	Indicates if employee attempting to perform action forbidden by security policy (DM), would receive warning message. See details in "Employee Notifications about Policy (DM) Violations"
Hide Agent presence	Indicates if Windows system tray of managed computer hides Client presence on the computer. If this option is not selected, the Windows system tray of the computer where the Client is installed will display  icon. By clicking at this icon, an information on DM Client operation and list of currently controlled devices is displayed. Warning! If there is an antivirus protection enabled on the managed computer then the antivirus program can reveal the operation of Device Monitor: for example, in the list of processes running on the managed computer or in the list of programs that initiate a control.
Code generating key	

Update	Click Update to make the System generate a new key used to make codes of removing network connections or devices access prohibition. See details on codes in "Temporary Employee Access to Network" and "Temporary Employee Access to Devices", Request code and Confirmation code settings. The frequent key refreshment is not recommended.

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

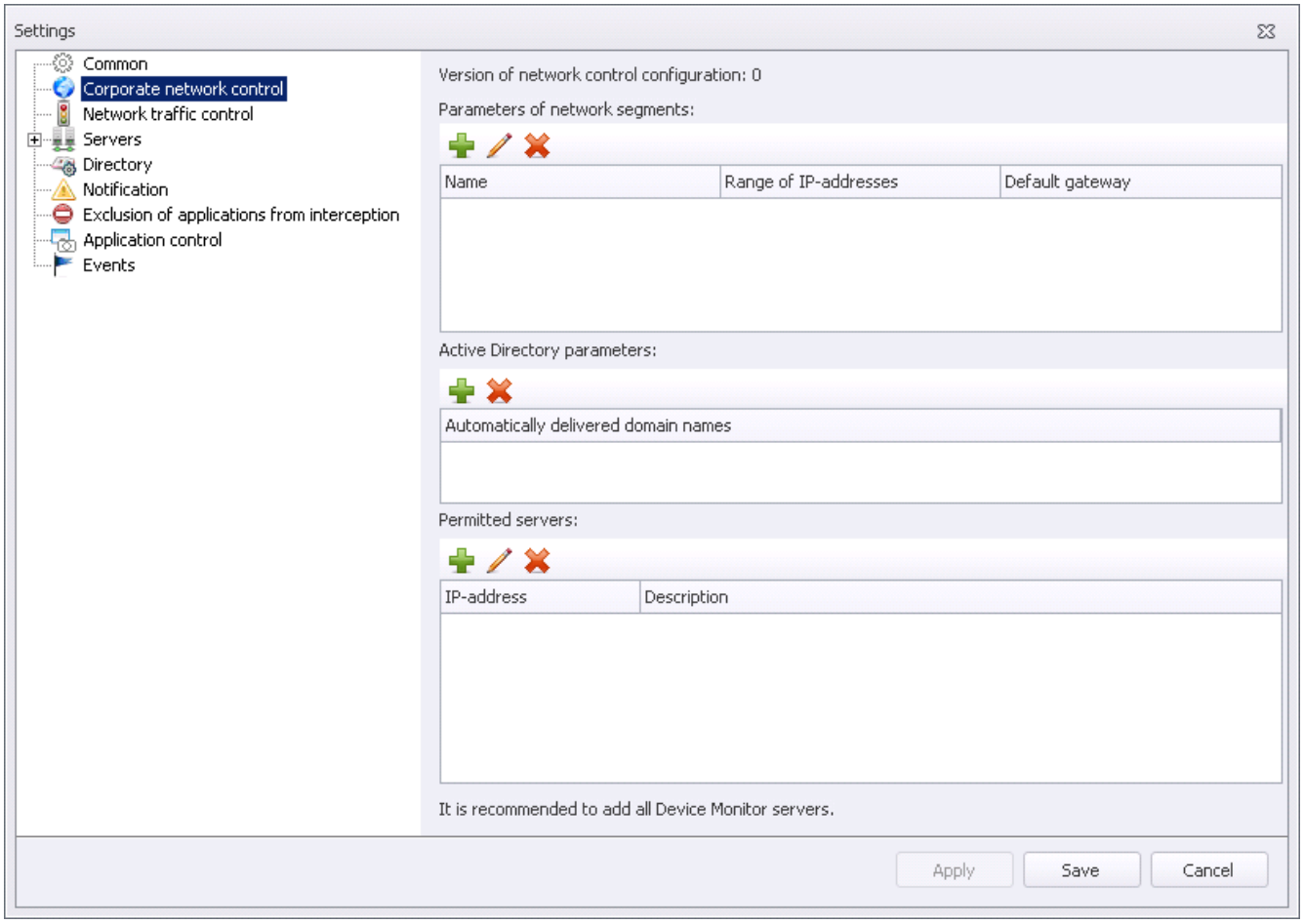
3.2 Settings of Corporate Network

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

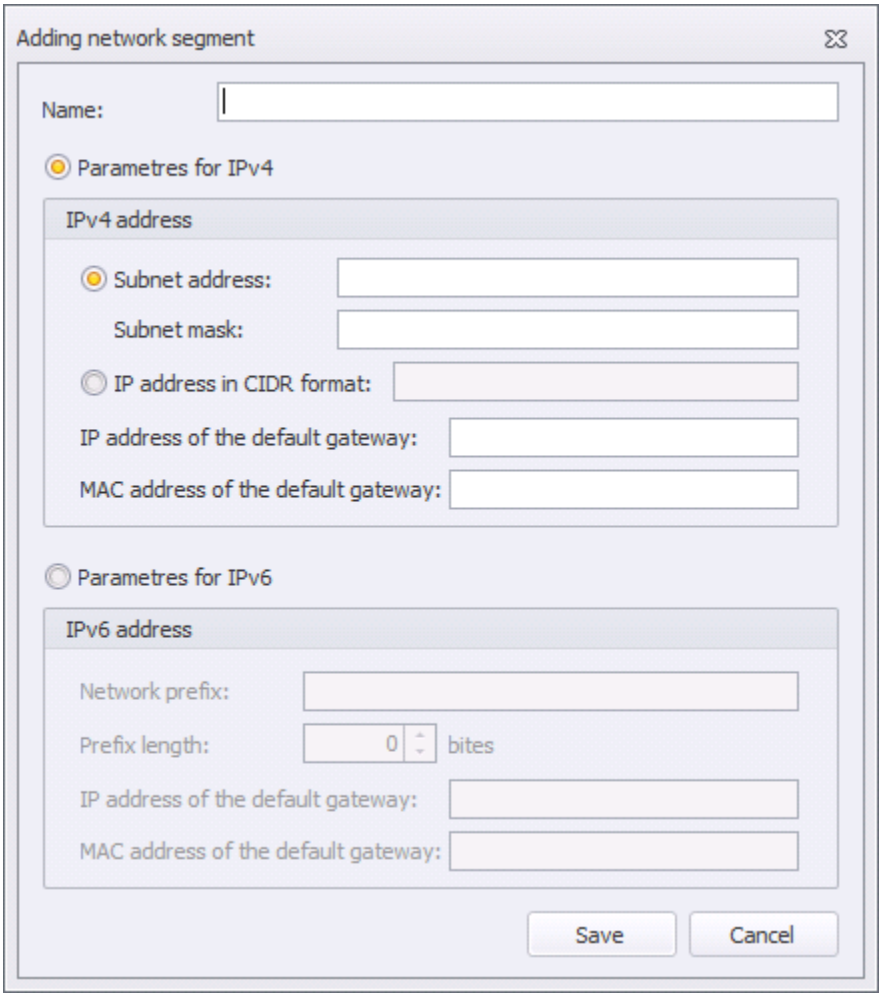
> **Note:**
>
> Permitting the external addresses may be necessary to provide work with external resources when the Client is outside corporate network: for example with VPN server or corporate network.

To configure corporate network settings:

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



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



b. Specify segment's name (description).

c. Select protocol in use: **IPv4** or **IPv6**.
If you selected Parameters for **IPv4**, then select address format (CIDR or address and mask) and specify required parameters. Also specify IP address and MAC address of the default gateway.
If you selected Parameters for **IPv6**, then select network prefix and its length. Also specify IP address and MAC address of the default gateway.

d. Click **Save**.

e. Repeat to add another segments.
To change segment parameters, select it from the list in Parameters of network segments area and click .
To delete a segment from the list, select it, click , then click Yes in confirmation dialog.

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

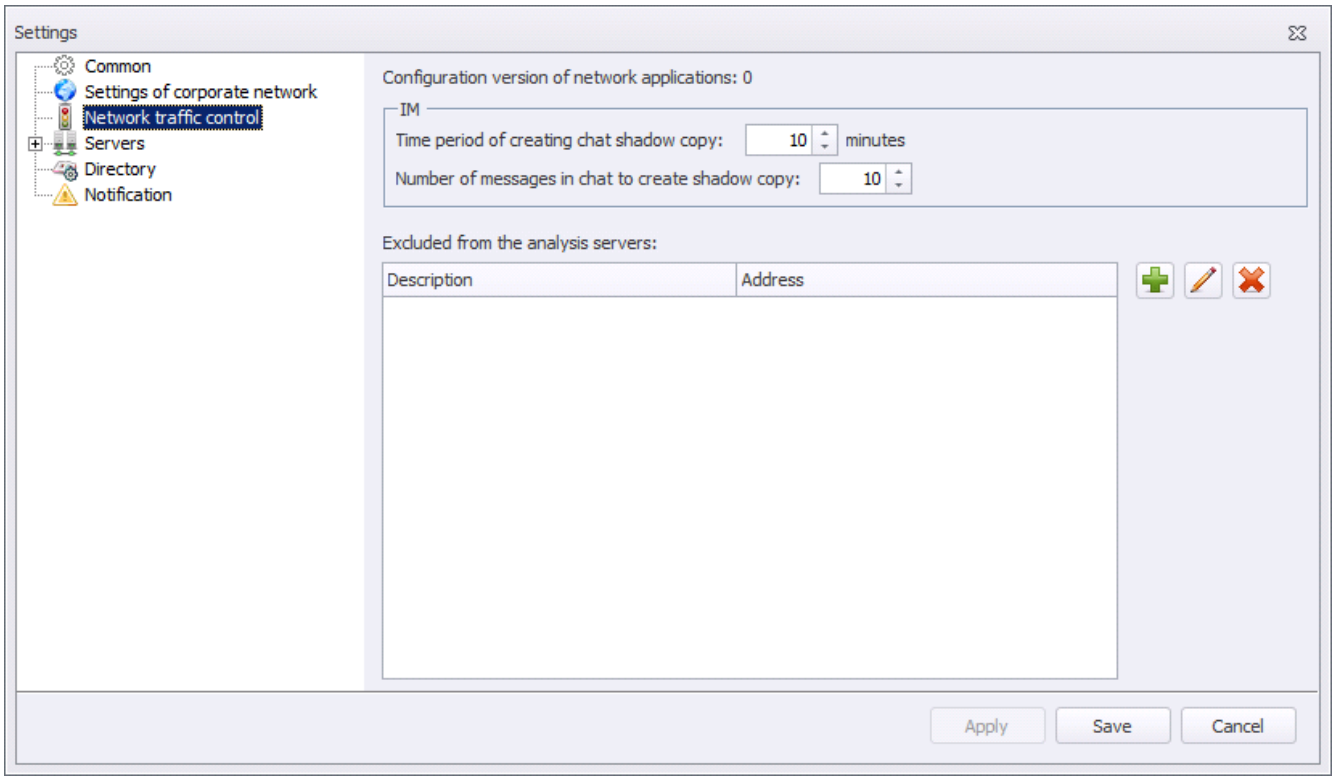
4. To define Active Directory parameters, click . Then the System automatically defines a name and GUID of a domain where Device Monitor server is deployed.
5. To set a list of servers to permit connection with:
    a. In **Permitted servers** area click .
    b. In **Add permitted server** dialog specify DNS name or IP address of a server and server description.
    c. Click **Save**.
    d. Repeat for other permitted addresses.
    To change server parameters, select it from the list and click .
    To delete a server from the list of permitted ones, select it, click , then click Yes in confirmation dialog.
6. You can also refresh a key of temporary access code forming (see "Temporary Employee Access"). Click **Update**.
7. To apply changes click **Apply**.

3.3 Network Traffic Control

In order to provide control of network traffic, Device Monitor Client acts as a transparent proxy server, to which all the connections are redirected (no matter if they are controlled protocols or not). Then Device Monitor Client parses a protocol and defines if this protocol is a subject of interception. Controlled protocols are: FTP, FTPS, POP3, SMTP, IMAP, HTTP, HTTPS, XMPP, and MMP. If data stream is protected with TLS\SSL protocol then proxy server opens traffic and defines if this stream should be controlled.
In network traffic control you can set some additional settings for instant messengers (setting rules (DM) for this interceptor see in "Configuring IM Client Monitor Rule (DM)"), mailing systems (see "Configuring Mail Monitor Rule (DM)") and FTP/FTPS traffic (see "Configuring FTP Monitor Rule (DM)"), 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 Skype control parameters: set a period of creating a chat shadow copy to send to Traffic Monitor. You can set a time period in minutes (**Time period of creating chat shadow copy** option) or a number of messages (**Number of messages in chat to create shadow copy** option) as criteria: the first actuated condition will be applied.
   If a file is be sent in a chat, the shadow copy is formed instantly, without accessing specified criteria.
   For details, see "Configuring IM Client Monitor Rule (DM)".

- You can specify a list of server IP addresses which protocols won't be controlled - i.e. those servers' traffic won't be transferred to the internal proxy server.

Note:

Permitting external addresses can be needed for providing work with external resources and updating installed programs, for example:
Firefox automatic update needs `*.mozilla.com` and `*.mozilla.net` in the list of permitted servers
Filezilla requires `update.filezilla-project.org`
Dropbox needs `*.dropbox.com`
Yandex Disk requires:

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

etc.

To set a list of servers excluded from analysis:

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

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

Note:

DNS name or IP-address allows to exclude or enable interception of address or port:
To exclude by address and port, specify address and port in the following format: `address:port.`
To enable interception, specify address and port in the following format `~!address:port.`
For example, to exclude all traffic to 10.128.0.2, except to traffic to 8080, it is necessary to add exclusions in the following format: `10.128.0.2` and `~!10.128.0.2:8080`. To exclude only traffic to port 80: `10.128.0.2:80`
Excluding range of addresses, # sign is being used. Example: `#192.168.0.1-192.168.0.255!192.168.0.5`

c. Click **Save**.

d. Repeat for other permitted addresses.
To change server parameters, select it from the list and click .
To delete a server from the list of excluded ones, select it, click , then click **Yes** in the confirmation dialog.

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

3.4 Device Monitor Server Settings. Connecting to Traffic Monitor Server

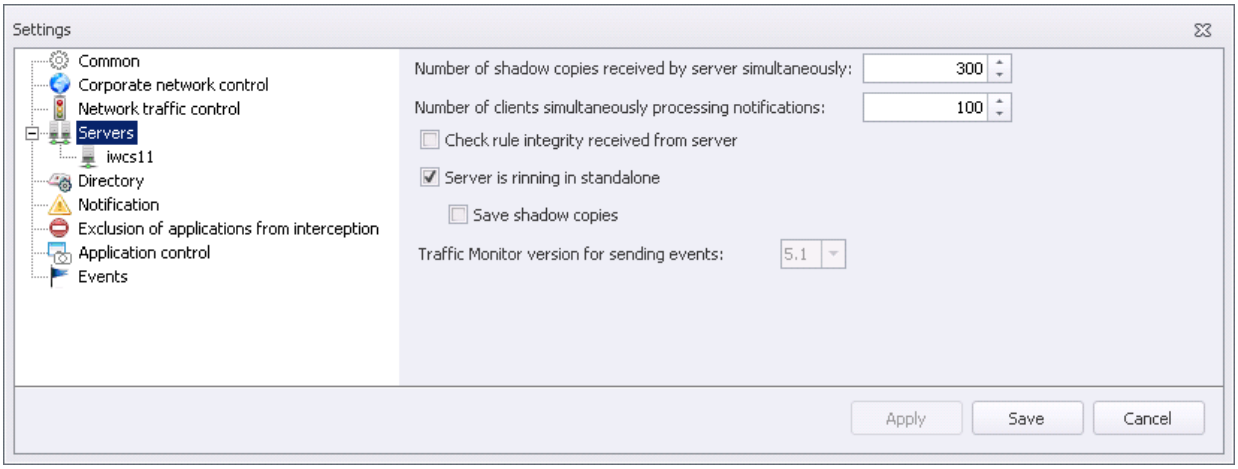
You need to set up connection parameters to be able to send events to Traffic Monitor.

Note:

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

To view and set up Traffic Monitor connection parameters:

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

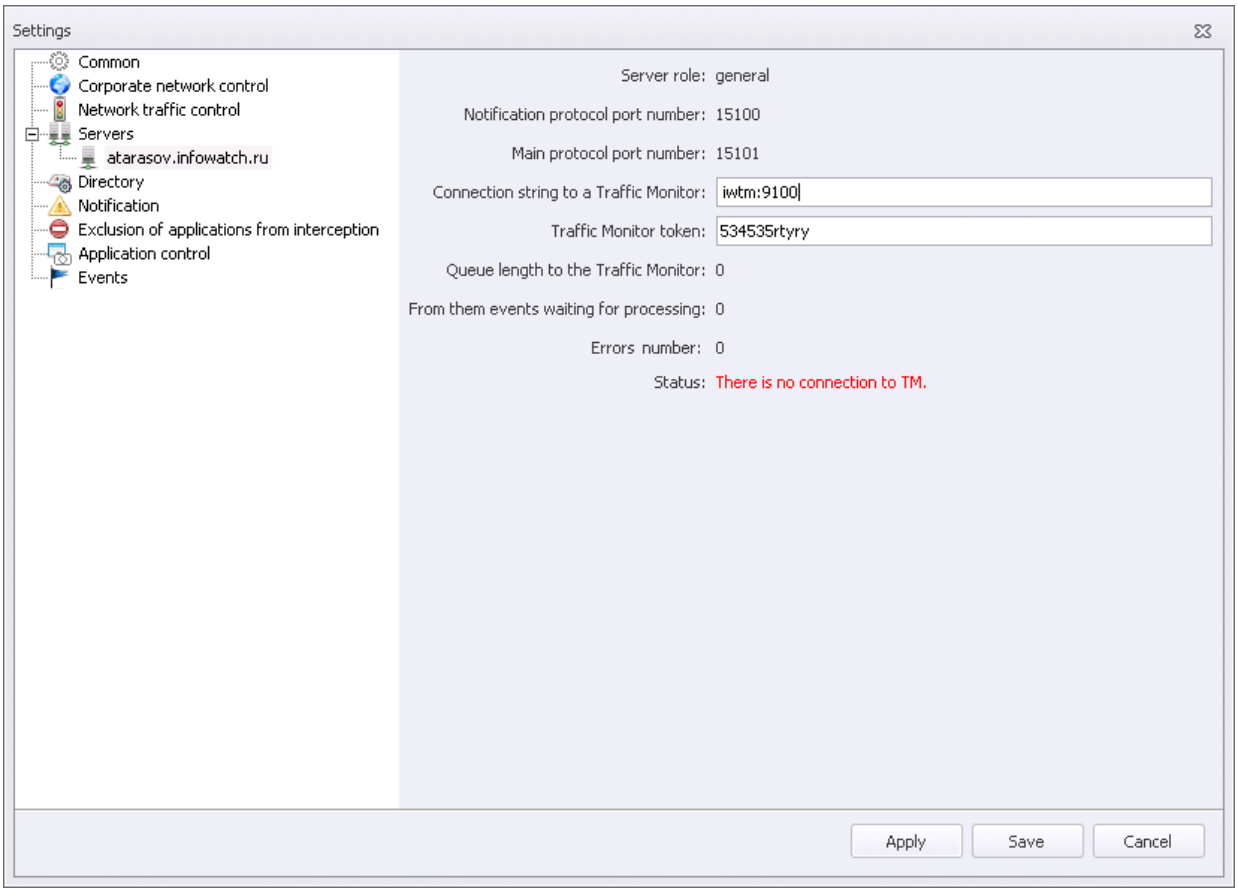


3. When selecting the server name, you will receive information on the following connection parameters:
    - **Server role** – server role (primary or secondary), assigned to this server during installation: see "InfoWatch Traffic Monitor. Installation guide", article "InfoWatch Device Monitor Server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

      `host:4101` - for Traffic Monitor of versions under 6.0;
      `host:9100` - for Traffic Monitor v. 6.0 or higher.

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

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



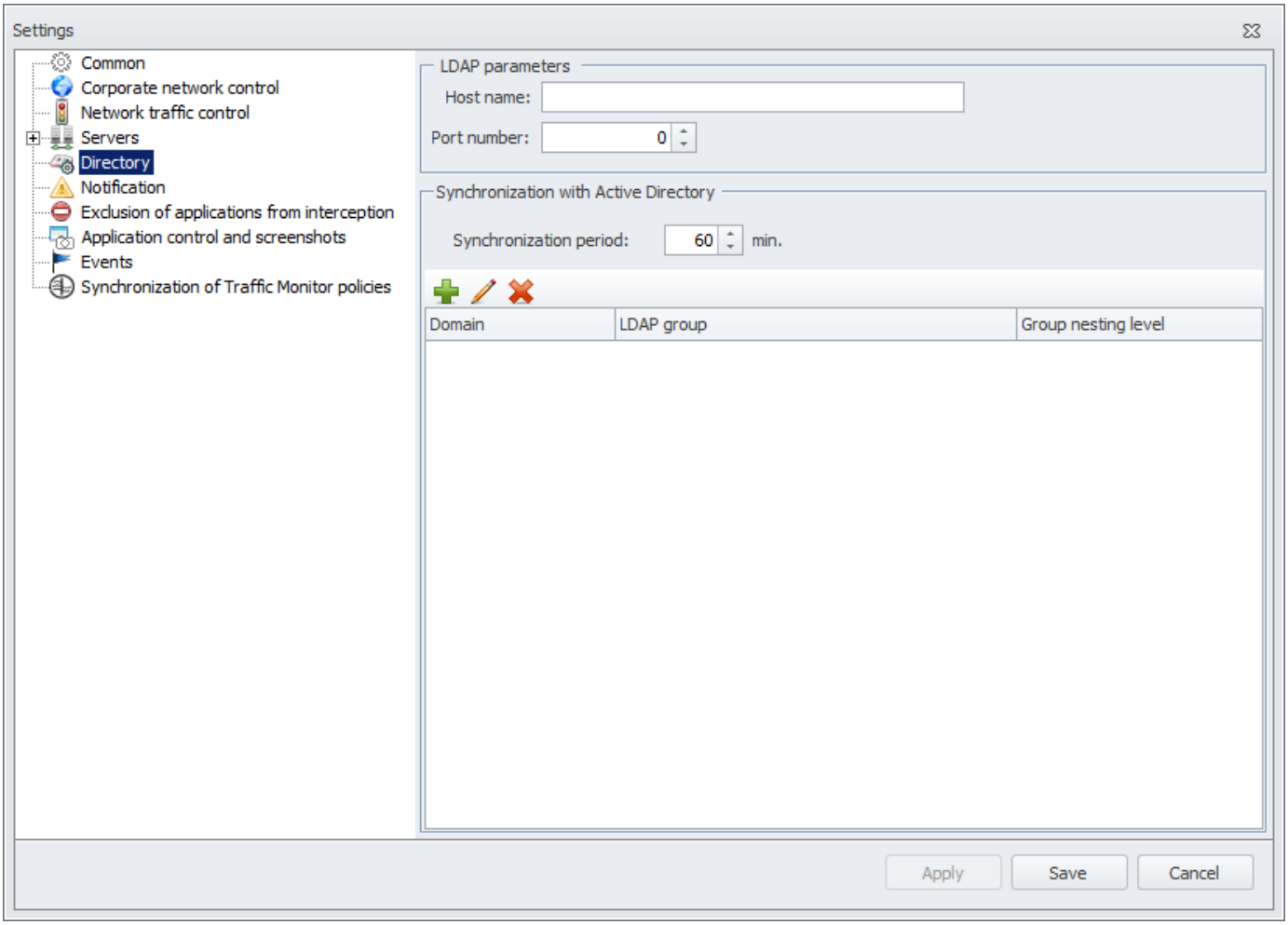
4. When all changes are made, click **Apply**.
5. Click **Save**.

3.5 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 (DM) connection to LDAP server.

To display and configure LDAP connection settings:

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



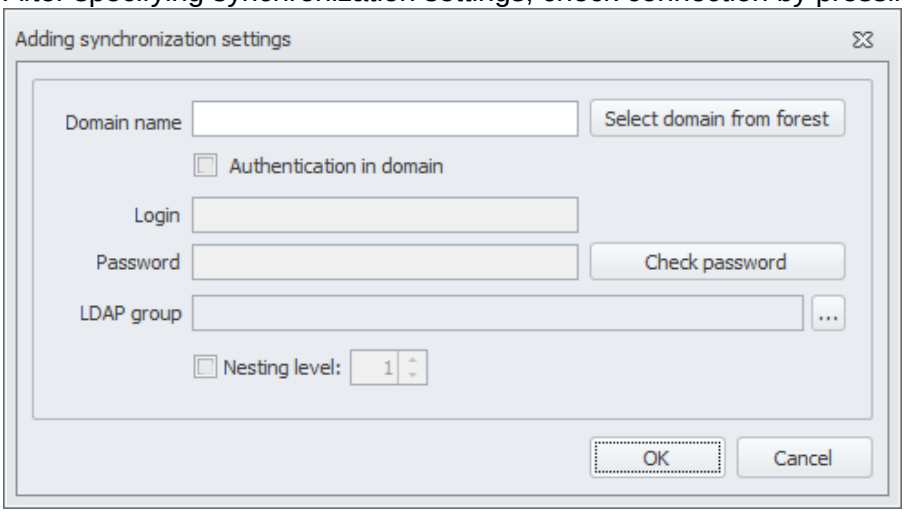
To perform syncronization with Active Directory:

1. In **Syncronization with Active Directory** area click .
2. In dialog window specify synchronization settings:
    - **Domain name.** Domain name to synchronize with.

> **Note:**
> IP-address or DNS-name. DNS-name must be registered in the network.

    - **Login.** To authenticate to the domain (if necessary).
    - **Password.** To authenticate to the domain (if necessary).

- **LDAP group.** AD Groups that need to be synchronized
- **Nesting level.** Required level of synchronized groups nesting.
  After specifying synchronization settings, check connection by pressing **Check password.**



3. Click **OK**.

To edit synchronization settings:

1. In **Syncronization with Active Directory** area click .
2. Edit synchronization settings.
3. Click **OK**.

To disable synchronization with Active Directory,

in **Syncronization with Active Directory** area click .

3.6 Employee Notifications about Policy (DM) Violations

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

- **Access to device denied** – Device Monitor rule which denies reading and writing to the device (see "Configuring Device Monitor Rule (DM)") was actuated.
- **Writing to device denied** – Device Monitor rule which denies writing to the device (see "Configuring Device Monitor Rule (DM)") was actuated.
- **Writing to open area denied** – Device Monitor rule which denies writing to unencrypted floppy drives and detachable devices (see "Configuring Device Monitor Rule (DM)") was actuated.
- **Copying/printing file denied if there is not enough space for incidents** – if Device Monitor 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 (DM) (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 (DM) are forbidden.

- **Data transfer via network protocols denied** – Ftp Monitor or IM Client Monitor rule (DM) which denies data transfer through FTP/FTPS/SMTP/POP3/MAPI/XMPP/MMP/YMSG/Skype (see "Configuring FTP Monitor Rule (DM)" and "Configuring IM Client Monitor Rule (DM)") was actuated.
- **Data transfer via network protocols denied if there is not enough space for incidents** – if Device Monitor 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 (DM) (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 (DM) are forbidden.
- **Network connection forbidden. Reduced** – Network Monitor rule (DM) which denies data transfer through any network connections except corporate network and specified permitted servers (see "Configuring Network Monitor Rule (DM)" and "Settings of Corporate Network") was actuated.
- **Network connection forbidden and request of temporary network access** – Network Monitor which denies denies data transfer through any network connections except corporate network and specified permitted servers was actuated. In this notification employee can request for temporary access to external connections (see "Configuring Network Monitor Rule (DM)", "Settings of Corporate Network" and "Temporary Employee Access").
- **Request of temporary access to the device by phone** – text displayed when user selected Request access command in InfoWatch Device Monitor Client interface, Device list tab (see "Temporary Employee Access to Devices").
- **Request of temporary access to the device by mail** – text displayed when user selected Request access command in InfoWatch Device Monitor Client interface, Device list tab (see "Temporary Employee Access to Devices").
- **Prohibition of access to cloud storage** – Cloud Storage Monitor rule (DM) which controls cloud storages client usage (see "Configuring Cloud Storage Monitor Rule (DM)", Access Denied option) was actuated.
- **Prohibition of writing to cloud storage** – Cloud Storage Monitor rule (DM) which controls cloud storages client usage (see "Configuring Cloud Storage Monitor Rule (DM)", Only download option) was actuated.
- **Prohibition of running application** – Application Monitor rule (DM) which controls user access to applications by means of white lists and black lists (see "Configuring Application Monitor Rule (DM)") was actuated.
- **Prohibition of making screenshot** – ScreenShot Control Monitor rule (DM) which controls making screenshots (see "Configuring ScreenShot Control Monitor Rule (DM)") was actuated.
- **Prohibition of pasting data** - Clipboard Monitor rule (DM) which controls data paste from clipboard (see "Configuring Clipboard Monitor Rule") was actuated.

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

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

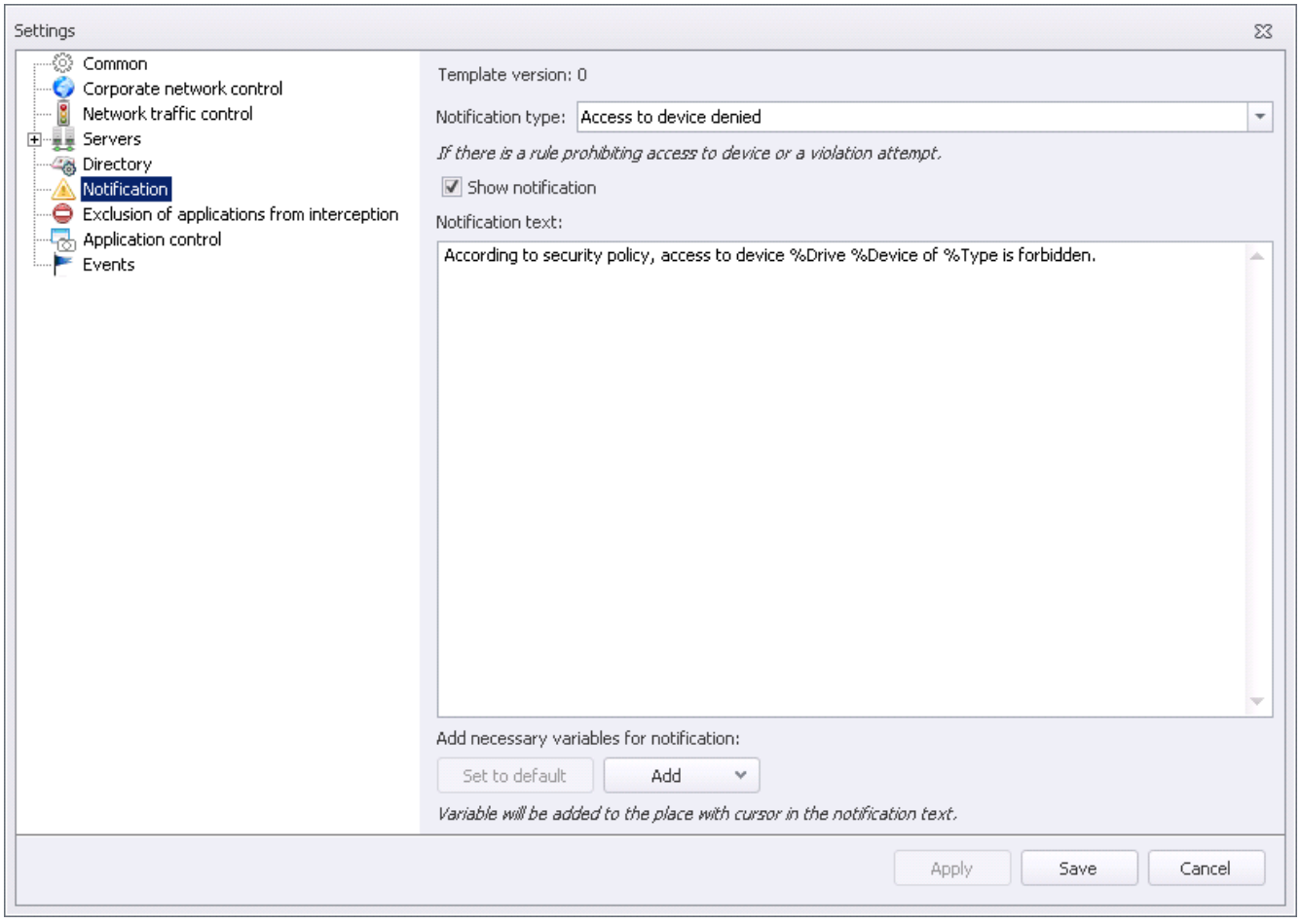
If needed, you can change notification text or disable showing of any certain notification type or enable it back.

Warning!

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

To change notification text or enable\disable certain notifications:

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



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

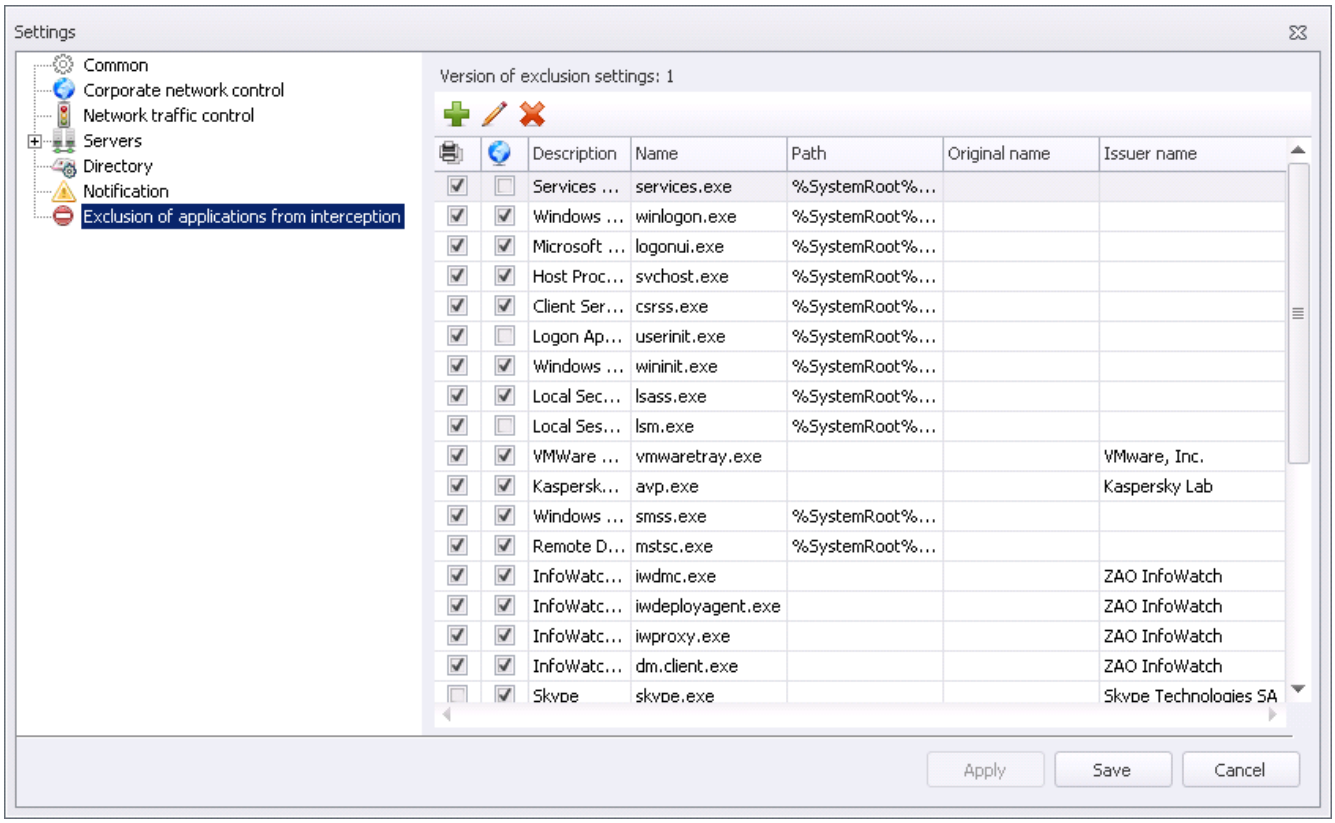
   You can use variables which would be transformed to actual data when displayed to employee: for example, type of blocked device or IP address of permitted host. To do this, set the cursor at required place of text, then click **Add** below textbox and select required variable from the list.
   To cancel changes and set default settings back, click **Set to default**.
6. Click **Apply**. If needed, change settings for other notifications by repeating steps 2-5.
7. When all changes are made, click **Save**.

3.7 Exclusion of Application from Interception

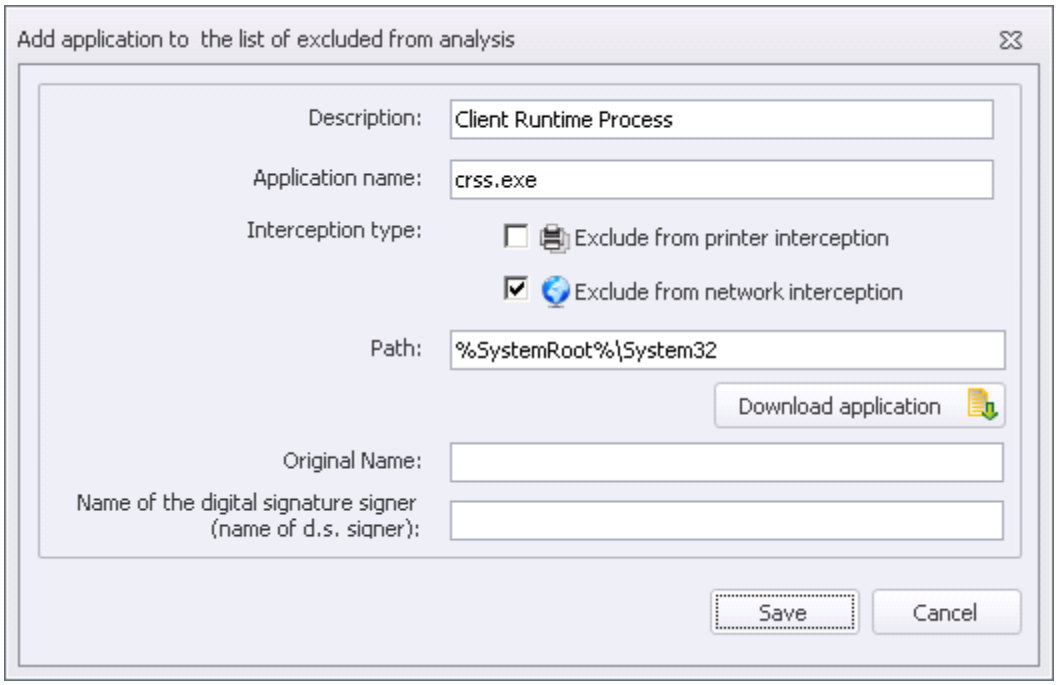
You can configure parameters of applications that will be excluded from interception. These parameters will apply at the next deployment of DM Client on computers.

To view and configure parameters of application exclusion:

1. In the Main Menu, select **Tools > Settings**.
2. Open **Exclusion of Application from Interception** node.



3. On the toolbar, click **Add**.



4. In the **Description** field, add a description of the application . This is a required field.
5. In the **Application name** field, enter the name of the application executable file. The exclusion is performed by the file name. This is a required field.
6. Mark the checkboxes in the **Interception type** field:
   - **Exclude from printer interception** - if you don't want to create events and shadow copies of print jobs initialized from this application;
   - **Exclude from network interception** - if you need to exclude this application activities from network interception (see "Network Traffic Control").

> **Note:**
>
> At least, one interception type must be selected.

7. You can specify application file parameters manually or automatically:
   - To specify file parameters manually:
     i. In the **Path** field, specify the directory on the Client that contains an executable file of the application (you can use system variables). If you use this parameter, then only the application located in the specified directory is excluded.
     ii. In the **Original Name** field, define the name of the application (in the shortcut menu of the executable file, choose **Properties**, **Details** tab, **Original filename** attribute).
     iii. In the **Name of the digital signature signer (name of d.s. singer)** field, define the property of the application (in the context menu of executable file choose **Properties**, **Details** tab, **Digital signature** attribute).

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

- To specify file parameters automatically, click **Download application** button and select the needed file. Fields **Path**, **Original Name**, **Name of the digital signature signer** will be filled automatically.

8. Click **Save**.

3.8 Application Control

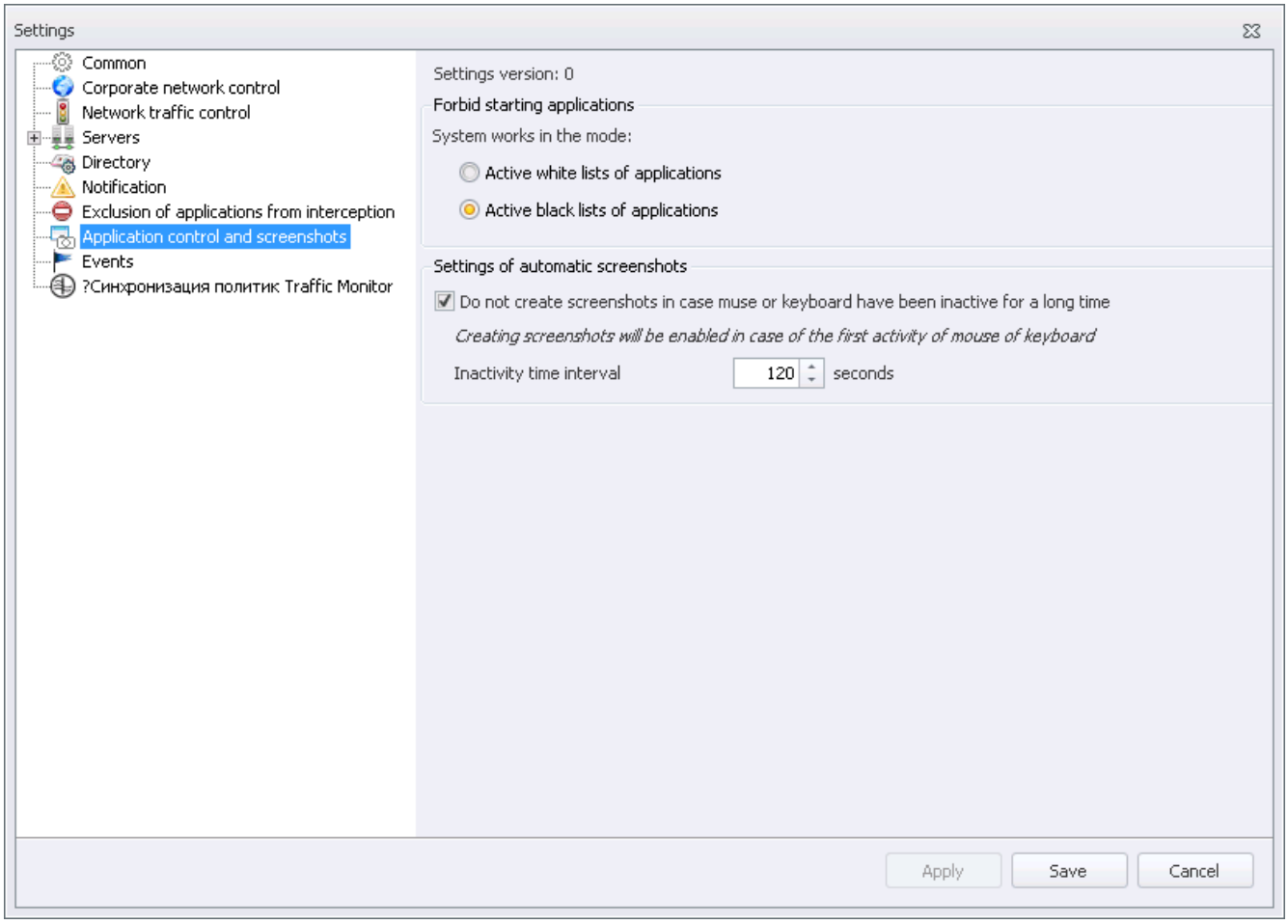
The System allows to control applications running of managed computers by allowing or forbidding some applications. For this purpose there are two operation modes provided:

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

See details on forming application lists in "Application Protocol".
See details on applying lists in rules (DM) regulating application access in "Configuring Application Monitor Rule".
See details on resulting policy (DM) viewing in "Viewing Resultant Policy (DM) and Resultant White List for an employee" and "Viewing Resultant Policy (DM) and Resultant White List for Computer".

To set System mode for application control:

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



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

In **Application control and screenshots** section you can specify, whether it is necessary to create screenshots if there is no activity on the controlled computer.

In case **Do not create screenshots in case mouse or keyboard have been inactive for a long time** option is enabled, screenshot creation will be stopped until value in **Inactivity time interval** field is reached and renewed at first keyboard or mouse activity.

More information on how to configure automatic screenshots creation, see "Configuring ScreenShot Monitor Rule (DM)".

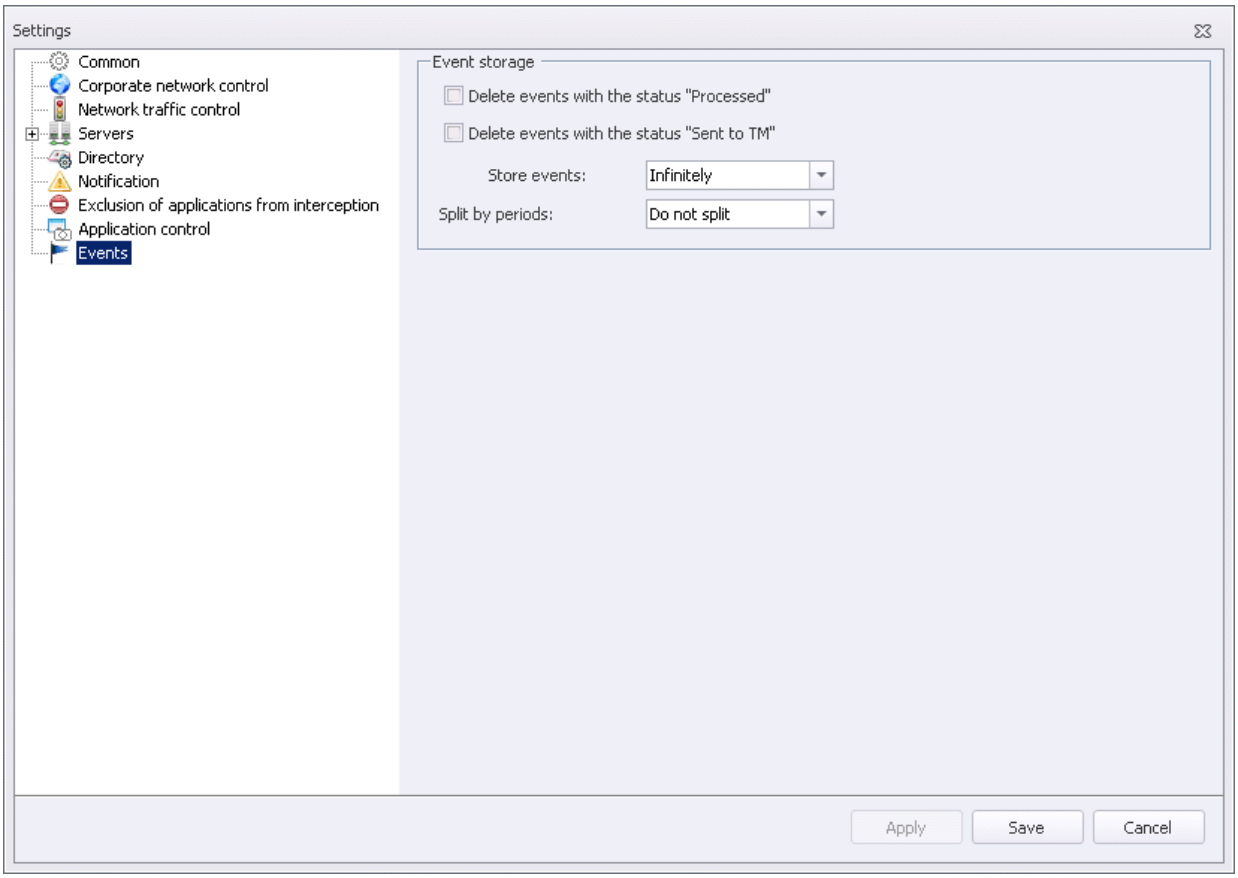
New version of applications and screenshots settings will ne applied to controlled computers after the next restart.

3.9 Event Storage

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

To set up event storage:

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



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

Note:

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

3.10 Synchronization of Traffic Monitor Policies

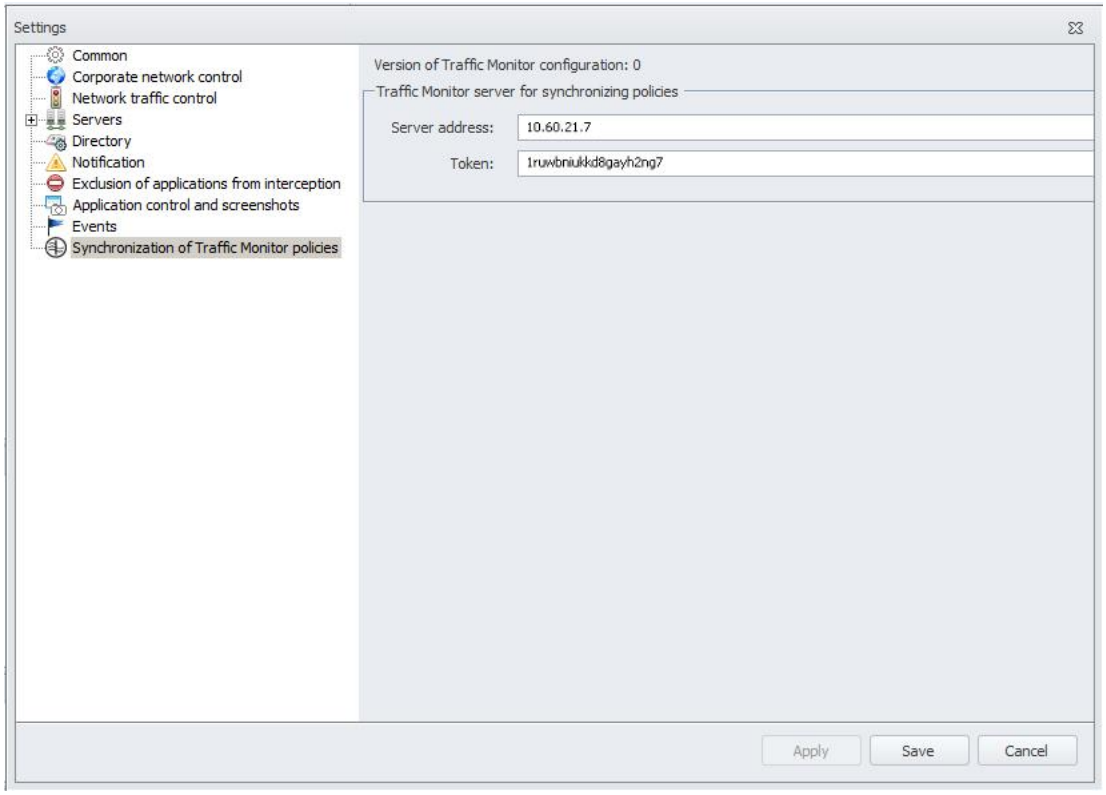
In the **Synchronization of Traffic Monitor policies** node, specify Traffic Monitor server from which Device Monitor will receive a configuration version. This configuration version is then deployed to Device Monitor agents.

Note:

The configuration version that is used in Traffic Monitor is displayed in TM console (see "Configuring the System"). If necessary, you can compare version numbers in Traffic Monitor and Device Monitor to make sure that Device Monitor uses an actual version.

To synchronize policies in TM:

1. From Console (DM) main menu, choose **Tools** > **Settings**.
2. Open **Synchronization of Traffic Monitor Policies** node.
3. Make sure that the server address (host) matches earlier specified settings (see "Device Monitor Server Settings. Connecting to Traffic Monitor Server").



4. Click **Apply**.
5. Click **Save**.

3.11 Import/Export Configuration

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

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

Warning!

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

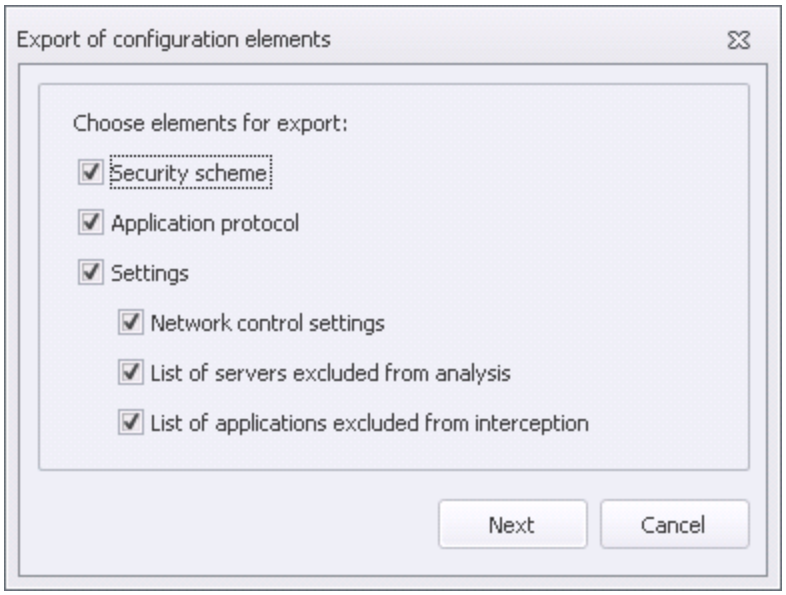
To import configuration settings:

1. In main menu choose **Tools -> Import Configuration**.

2. Find a .dmc file and click **Open**.

To export configuration settings:

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



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

3.12 InfoWatch Device Monitor Server Manager

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

Warning!

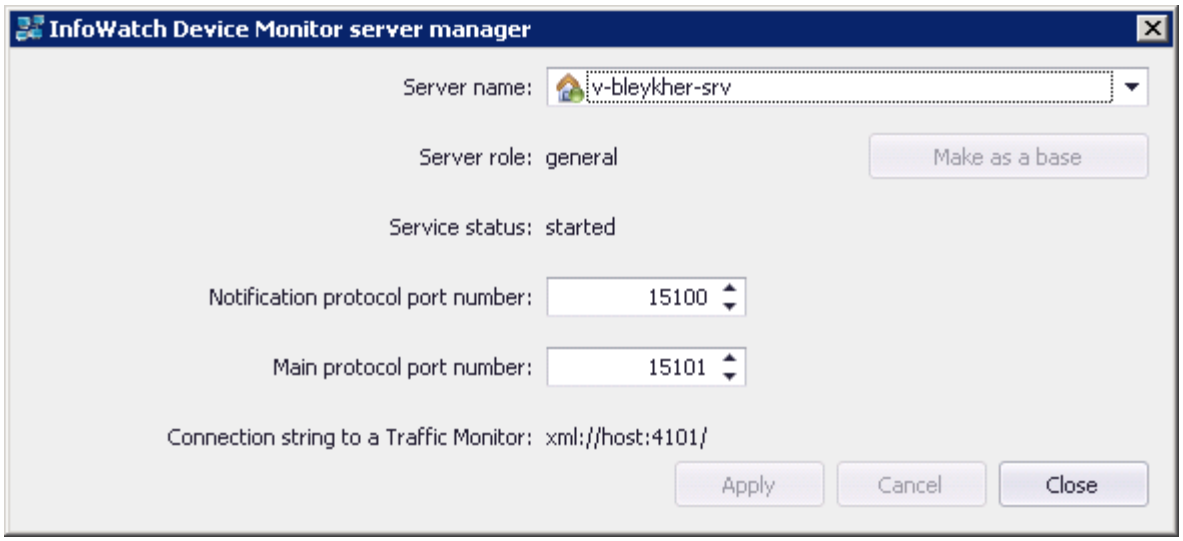
There are following requirements to run the InfoWatch Device Monitor Server Manager utility:

- the computer where utility will run, must be included to the domain
- the user on behalf of which the utility will run, must have Administrator role at each of the servers to be changed
- there must be FQDN access granted to the servers (to check use ping `<server_name>.<domain_name>`)

- the utility must be run on behalf of the Administrator (use the option in the drop-down menu opened by clicking the right mouse button on the utility icon); or User Access Control must be disabled the computer.

To set up server ports, proceed with following steps:

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



   Info Watch Device Monitor server manager window will be opened.
2. From **Server name** drop-down menu pick the necessary server.
3. Edit fields **Notification protocol port number** and **Main protocol port number**.
4. Click **Apply**.
5. Click **Close**.

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

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

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

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

3.13 Stopping and Starting Device Monitor Agent

When there are conflicts with third-party programs as well as in critical situations, user can stop Device Monitor agent running on a workstation. One can do it locally or remotely

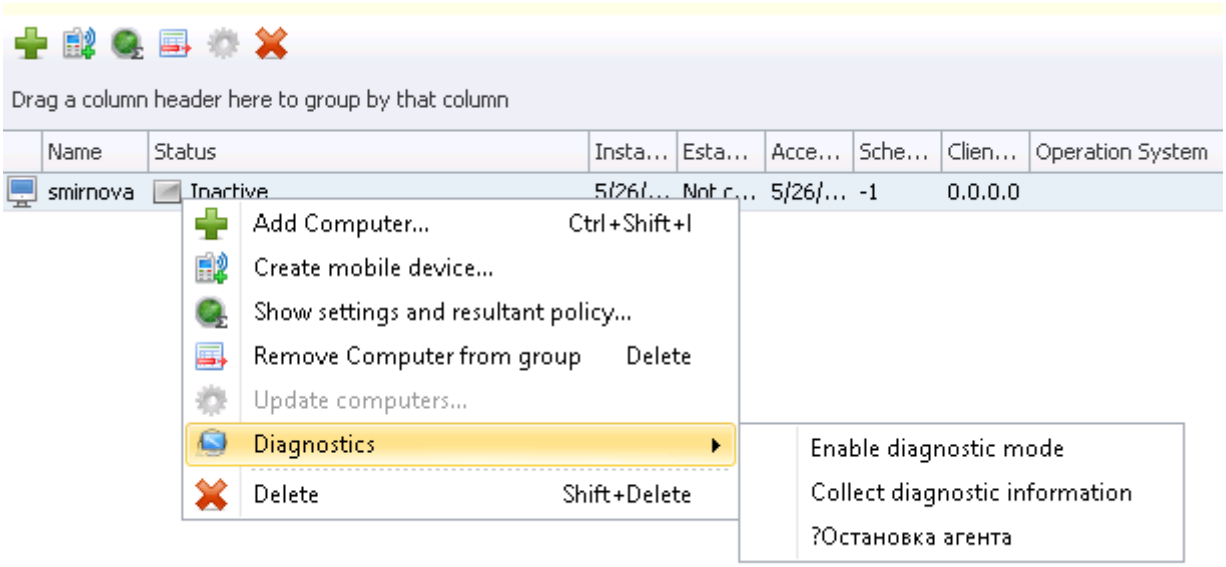
Note:

Some restrictions:

- When you stop the DM agent, Self Protection module is not disabled.
- The Diagnostics menu is unavalable during collecting logging results) .
- In case stopped agent has been updated, it will be started after update.
- In case agent is hidden, it cannot be stopped locally.

3.13.1 Stopping agent remotely/starting agent

Remote DM agent s being performed from DM Management Console. To stop agent, right-click on a Workstation and choose **Diagnostics -> Stop agent** (in case agent is already started on a Workstation).



When choosing **Stop Agent**, agent's work will be suspended and status of Workdtation will be changed to "Inactive".

Note:

Stopped agent is available for update or deletion, but stopping is unavailable during

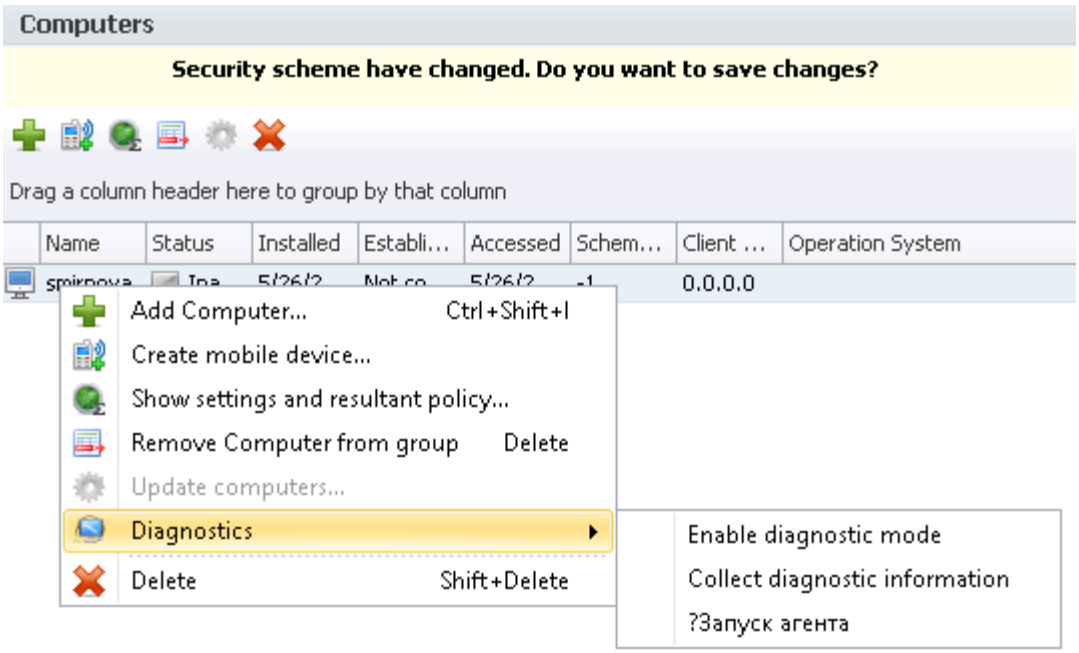
update/deletion.In case there is no connection with the agent, stop/start are unavailable.

After the Agent has been stopped:

- events are not intercepted;
- actions are forbidden;
- notifications and DM icon on the toolbar are not dosplayed.

To start DM agent remotely, right-click on a Workstation and choose **Diagnostics -> Start agent** (in case agent is stopped).

Afte choosing agent Start option, its work will be resumed and Workstation status will go back to " Working normally".



3.13.2 Stopping/starting agent locally

Agent can be stopped/started using Windows command prompt. Run **rmtdiag.exe**, specifying the full path to it on Workstation, with the required parameters. For example:

- **rmtdiag.exe /cle** - to start agent;
- **rmtdiag.exe /cld** - to stop agent.

Warning!

To stop the agent it is reqired to type in DM agent uninstall password. The password is not required to start the agent.

For more information on uninstall password see "Creating Uninstallation Password Reset Task".

4 MANAGING SECURITY SCHEMA

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

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

4.1 Security Schema Organization

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

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

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

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

This topic also contains:

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

4.1.1 Security Policies (DM) and Rules (DM)

Security policy (DM) is a set of rules (DM) used for monitoring operations of data transfer to removable devices, sending documents to print and network activity; it also defines access level to managed peripherals.
The security policy (DM) is assigned to employee group or computer group according to the following principles:

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

Note:

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

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

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

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

Warning!

In case of a multiuser access to workstation and when it is not possible to identify the initiator of the process (event), it is important to configure interception rights not only for employees, but for the computer as well.

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

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

Rule (DM) types include:

- **Application Monitor Rule** provides application access control via black and white lists.
- **Cloud Storage Monitor Rule** provides web-client control.
- **Clipboard Monitor Rule** provides control of data paste from clipboard. You can prohibit data paste to specified applications or to all appliations of a terminal session.
- **Device Monitor Rule**. Lets you control employee access to selected type of peripherals.

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

4.1.2 Employees and Employee Groups

Registration of controlled users (employees) is done according to the following rules:

1. Each employee belongs to at least one employee group (default group). The reason for this requirement is that security policy (DM) can only be assigned to employee groups.
   Default group includes all accounts that have not been added to other groups (employees newly registered in Device Monitor or employees excluded from all other groups).
   You can exclude an employee from "*Default*" group, if the account is added to at least one employee group besides the Default group.
2. After System installed, the "*Shadow copy policy*" is assigned to "*Default*" employee group. The "*Shadow copy policy*" contains following rules:

- **Document shadow copying**. File Monitor rule which sets creating shadow copies of all files written to removable devices.
- **Print shadow copying**. Print Monitor rule which sets creating shadow copies of all print jobs.
- **Skype control**, **XMPP control**, **MMP control**. IM Client Monitor rules which allow instant messengers and set creating shadow copies of all messages, chats and outgoing files.

- **FTP control**. FTP Monitor rule which allows FTP/FTPS protocol and set creating shadow copies of all files sent by FTP/FTPS.
- **HTTPS control**. HTTPS Monitor rule, which creates a post-event, without any dependence on its size, in case transfer is being performed via encrypted channel. Shadow copy is being created, in case request size, transferred via encrypted channel is not smaller than 40 B and not bigger than 40 MB.
- **Mailing subsystem control**. Mail Monitor, which allows incoming and outgoing mail and creates shadow copies for email, sent via encrypted channel, when its size is not bigger than 40 MB.

4.1.3 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 (DM) 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 (DM) is empty: it does not contain any rule (DM).
You can remove a workstation from default group only if it is added to at least one workstation group besides default group.

4.1.4 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 (DM) 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 (DM) and sends shadow copies to server.

4.2 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".

4.2.1 Viewing Active Security Schema

Active security schema is displayed on Management Console (DM) by default.
Security schema configuration information is displayed in **Policies**, **Employees**, **Workstations**, **White Lists** and **Signatures** sections (see "Management Console (DM) 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 (DM) 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").

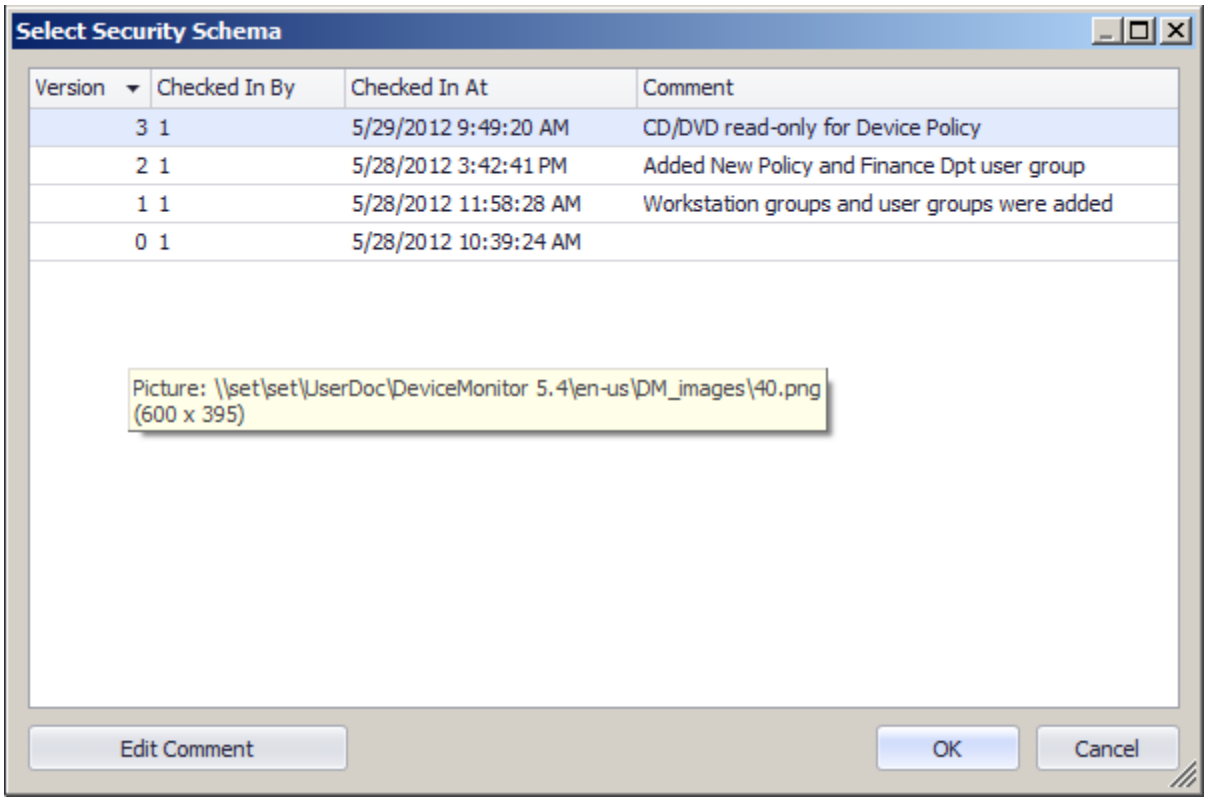
4.2.2 Viewing Old Security Schema

Note:

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

To view older security schema:

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



   Each security schema features the following information:

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

> **Note:**
>
> You can edit comments to any version in this screen (see "Security Schema Comments").
> Information on current Management Console (DM) 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 (DM). 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

4.2.3 Security Schema Comments

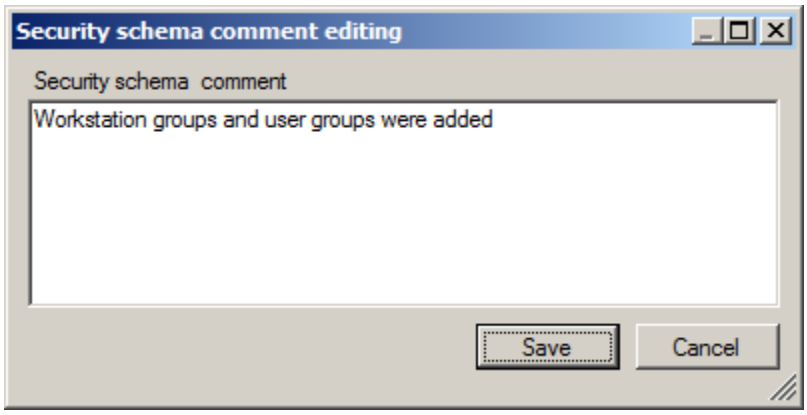
In comments you can specify additional information on your security schema. You can add comments to each version of security schema.
Comments to current security schema are displayed in brackets to the right from schema version number on the status panel.
You can view comments to all security schema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

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

To add/edit security schema comment:

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

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



2. Enter your comment in the dialog box. Maximum comment length - 512 characters.

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

3. Click **Save**.

4.2.4 Editing Security Scheme

> **Warning!**
>
> Security scheme can be edited only by one user at a time. If security scheme 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 Scheme".

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

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

To edit security scheme:

1. Take one of the following steps:
   - in the Main Menu select **Security Scheme > Edit**
   - click **Edit** on Toolbar

- make any change of security scheme parameters (security policies (DM), workstations, employee accounts, device white lists, signature categories).
  These actions open security scheme editing mode.

> **Note:**
>
> You can edit only the latest version of the security scheme. Thus, Save command is not available when viewing previous versions. To open current security scheme version, open **Security scheme** > **View Latest Security Scheme** from the main menu. Information on security scheme currently used by Management Console (DM) is displayed on the status bar.

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

> **Note:**
>
> To discard changes, select **Security Scheme** > **Undo editing** or click **Undo editing** button on the toolbar. This closes scheme editing mode discarding all changes.

4.2.4.1 Awaiting Editing Ends. Unlocking Security Schema

Security schema can be edited only by one user at a time. Changes are applied only after you have saved your security schema.
If security schema is edited, an information about user who edits and 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 (DM), workstations, employee accounts, device white lists, signature categories) while security schema is editing by another user:

1. Management Console (DM) 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.

4.2.5 Updating Security Schema

The system can be simultaneously operated by multiple users. To keep security schema details in Management Console (DM) 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.

4.2.6 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 (DM) with sets of rules (DM);
- 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 (DM) and sets of rules (DM) 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.

4.3 Security Schema Setup

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

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

Security schema configuration principles:

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

Adding workstations to security schema
There are two ways to add a managed workstation:

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

In case of automatic registration a workstation is added to "*Default*" group. Later you can move it to other groups.
If you add it manually, you can select the group immediately.

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

Adding white lists to security schema
Before you create a white list, add device models and instances to the database. Then 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 (DM). When a white list record expires, access rights are distributed according to the policies (DM).
Security schema configuration details are available in the following subsections:

- Security Policies (DM);
- Rules (DM);
- Workstations;

- Employees;
- White Lists;
- Signatures;
- Temporary Employee Access to Network;
- Temporary Employee Access to Devices;
- Awaiting Editing Ends. Unlocking Security Schema.

4.3.1 Security Policies (DM)

> **Note:**
>
> For security policy (DM) configuration guidelines see "Security Policies (DM) and Rules (DM)".

Each security policy (DM) is a set of rules (DM) that define employees' level of access to controlled files and devices.
Security policies (DM) are assigned to **employee groups** and **workstation groups**. Security policy (DM) of employee group affects all the employees included to this group. Security policy (DM) of workstation group affects all the employees which work at managed workstations included to this workstation group.
Security policies (DM) 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 (DM) managing guidelines see:

- Viewing Security Policies (DM);
- Adding and Configuring New Security Policy (DM);
- Edit Security Policy (DM);
- Deleting Security Policy (DM).

4.3.1.1 Viewing Security Policies (DM)

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

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

To view security policy rules,
select security policy (DM) name in **Policies** area of Navigation pane.
Rules are displayed in a form of a table where each row contains a rule. Columns contain general rule properties. Each rule (DM) has an icon depicting the rule's (DM) coverage and a color mark depicting if a rule (DM) is an allowing one (green), forbidding (red) or partially restricting (yellow).
Extended information on each rule (DM) is displayed on **Details** panel.

To view all rule properties,
select the row that contains the rule (DM) name in the main screen workspace.
This opens a table containing rule (DM) information on **Details** panel.

General information:

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

Application Monitor rules feature additional details:

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

Clipboard Monitor rules feature additional details:

- **Within the same application**. Indicates that data paste within the same application triggers the rule.
- **To applications of termanal session**. Indicates that data paste to applications of terminal session triggers the rule.

Cloud Storage Monitor rules feature additional details:

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

File Monitor rules feature additional details:

- **Exclude from interception**. Indicates if files corresponding to mask or category won't be proceeded.
- **Use file mask**. File mask attribute.
- **File mask**. Mask that selects the files covered by the rule (DM).
- **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 (DM).
- **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/FTPS-sent file should be created.
- **Minimum file size**. Lower limit of file size.
- **Maximum file size**. Upper limit of file size.

HTTPS Monitor rules feature additional details:

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

Network Monitor rules feature additional details:

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

Mail Monitor rules feature additional details:

- **Transferred via**. Indicates whether encrypted or any other traffic is being intercepted.
- **Maximum mail size, Mbytes**. Maximum mail size.

ScreenShot Control Monitor rules feature additional details:

- **Forbid an employee to make screensho**ts. Any screenshots or when particular application run only.

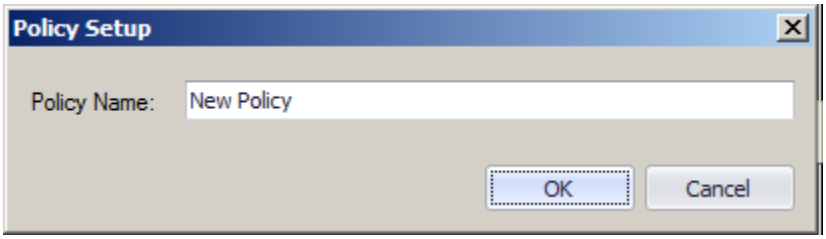
Note:

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

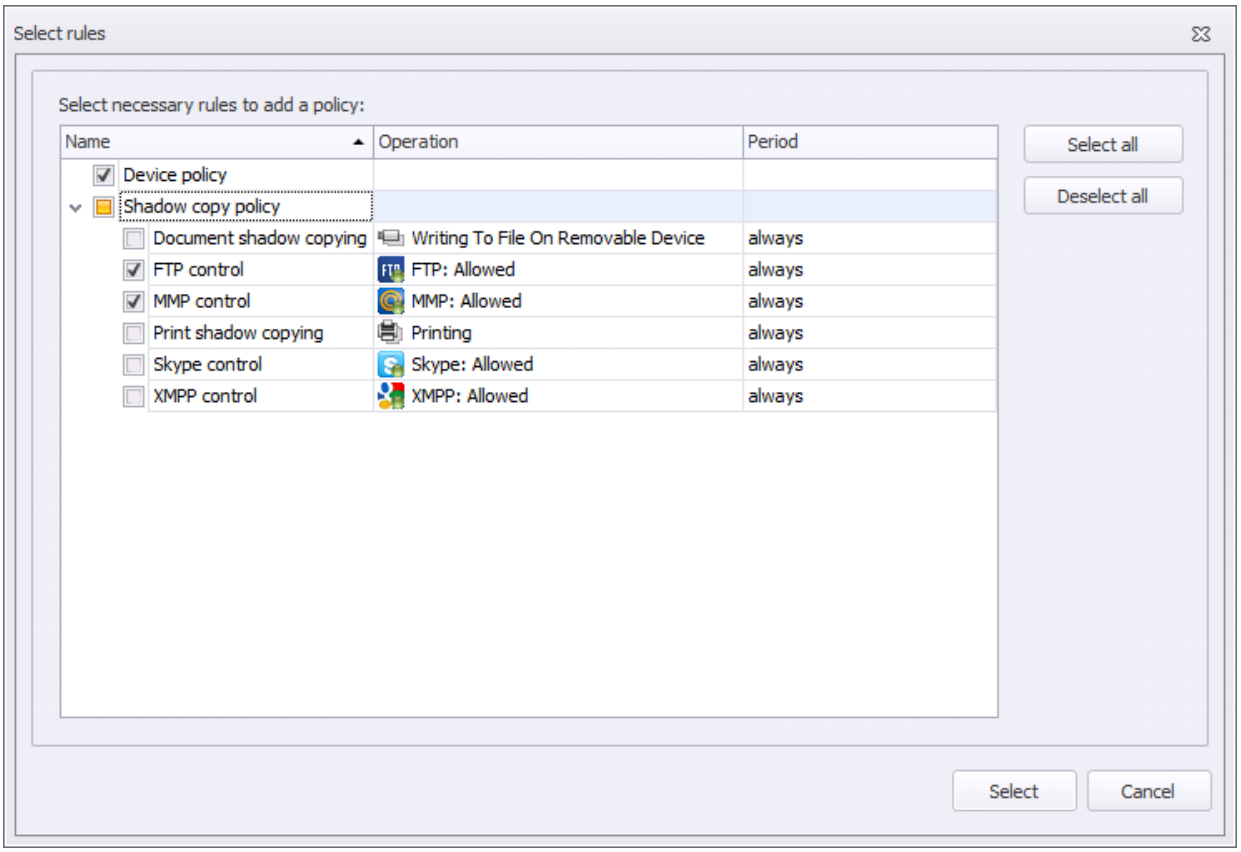
4.3.1.2 Adding and Configuring New Security Policy (DM)

To create and configure security policy:

1. Go to **Policies**.
2. Take one of the following steps:
   - click **Create Policy** at the top of Navigation panel;
   - in Main Menu select **Edit > Create Policy**.
   - Use **Ctrl+N** shortcut on a keyboard.
     This opens **Create policy** dialog.



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



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

- To create a new rule (DM) click **Create** and specify rule (DM) parameters as described:
  - Configuring Application Monitor Rule (DM);
  - Configuring Clipboard Monitor Rule;
  - Configuring Cloud Storage Monitor Rule (DM);
  - Configuring Device Monitor Rule (DM);
  - Configuring File Monitor Rule (DM);
  - Configuring FTP Monitor Rule (DM);
  - Configuring HTTPS Monitor Rule (DM);
  - Configuring IM Client Monitor Rule (DM);
  - Configuring Mail Monitor Rule (DM);
  - Configuring Network Monitor Rule (DM);
  - Configuring Photo Monitor Rule (DM);
  - Configuring Print Monitor Rule (DM);
  - Configuring ScreenShot Control Monitor Rule (DM);
  - Configuring ScreenShot Monitor Rule (DM).

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

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

Warning!

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

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

4.3.1.3 Edit Security Policy (DM)

To edit security policy (DM):

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

- use **Ctrl+E** shortcut;
- double-click selected security policy (DM) name.

These actions open **Edit Policy** dialog.

4. In this dialog, edit security policy (DM) name by entering a new one in **Name** field.
5. Click **OK**.

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

4.3.1.4 Deleting Security Policy (DM)

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

To delete security policy:

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

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

4.3.2 Rules (DM)

Rules (DM) are used basing on the security policy (DM) they are assigned to. Each security policy (DM) has individual set of rules (DM). Information on rules (DM) is available in the following subsections:

- Rules Application (DM);
- Adding a Rule (DM);
- Editing a Rule (DM);
- Deleting a Rule (DM);
- Copying a Rule (DM).

4.3.2.1 Rules Application (DM)

To make a set of rules (DM) effective, keep in mind all possible instances of their application.
The event is considered as satisfying the rule (DM) if it meets all rule (DM) parameters (for example both event time is within rule (DM) time period and a size of outgoing document is not less than minimal file size and so on).
If the event meets several rules (DM) at the same time, then in general more limiting rule overrides the permissive one. In details:

1. The excluding rule (DM) (Exclude from interception option is selected: see "Configuring File Monitor Rule (DM)") has a highest priority.
2. The forbidding rule (DM) overrides the permitting one. For example, Device Monitor rule (DM) (see "Configuring Device Monitor Rule (DM)") with No access limitation overrides rule which permits Read only, and the last one overrides a rule (DM) with Full access to encrypting devices. Also FTP Monitor rule (DM) (see "Configuring FTP Monitor Rule (DM)") with Forbid using FTP-protocol is applied instead of rule (DM) 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 (DM) which make a copy of voice traffic (Create voice copy option is selected: see "Configuring IM Client Monitor Rule (DM)"), the rule (DM) which has a constraint of lesser recording duration overrides a rule (DM) with longer recording duration.

Other important information on rules (DM) application:

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

4.3.2.1.1 Device Monitor Rules (DM) Application

Access to all Device Monitor interceptor controlled peripherals is a collection of rules (DM) assigned to each device.
Employee access rights are defined basing on:

- rules (DM) applied to employee groups which an employee is included in;
- rules (DM) applied to workstation groups of the workstation using for device access;
- white lists.

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

For example:
There is a rule (DM) that lets workstation group A write to CD/DVD drive. Workstation WS belongs only to workstation group A. Employee Smith belongs only to employee group B with no device rules (DM). Employee Smith tries to view a CD on workstation WS. In this case, employee won't be able to view CD contents of a disk and write new data.
You can assign multiple rules (DM), in several policies (DM) either, with various access levels to the same device. This causes rule (DM) conflict. General conflict resolution principle: higher limit means higher priority (see the table for further details).

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

Examples:

Example 1. There is a rule (DM) for workstation group C that forbids an access to removable storage device. There is a rule (DM) in employee group D policy (DM) that allows access to removable storage devices in read only mode. Employee Smith belongs to employee group D and tries to access removable storage device from workstation that belongs to workstation group C. Conflict is resolved in favor of more restrictive rule (DM), i.e. employee Smith cannot read from removable storage device.
Example 2. There is a rule (DM) in employee group E policy (DM) that allows read-only access to removable storage device. There is a rule (DM) in employee group F that grants a full access only to encrypted removable storage devices. Employee Smith belongs to both groups. Conflict is resolved in favor of the more restrictive rule (DM): i.e. employee Smith can get a read-only access: both encrypted and not encrypted (less priority rule (DM) is not applied at all).

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

Note:

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

Rule (DM)	Overlapping rules	Notes
Floppy	No	
CD/DVD	No	
Parallel port (LPT)	Local printer (LPT) Imaging devices (LPT)	If there is no access to LPT port, the device connected to this port will be unavailable
Serial port (COM)	Modem Local printer (COM) Imaging devices (COM)	A modem connected to COM port is only accessed basing on COM port rule If there is no access to COM port, the device connected to this port will be unavailable

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

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

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

1. Applied rule rule (DM) creates shadow copies and file size meets the requirements.

2. Free space at managed workstation is more then minimum size required by the policy (DM) (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 (DM) 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 (DM) (see "Viewing Events") with "*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 (DM) 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**.

4.3.2.2 Adding a Rule (DM)

To add a rule to security policy:

1. Go to **Policies**.
2. In **Policy** area of Navigation pane select the name of the security policy (DM) you want to add the rule (DM) to.
3. Take one of the following steps
   - in Main Menu click **Edit > Create Rule**;
   - click **Create Rule** in the top of **Policies area**;
   - right-click in **Policies** area and select **Create Rule** from the drop-down list;
   - use **Ctrl+Shift+N** shortcut.
4. Specify the interceptor rule (DM):
   - Configuring Application Monitor Rule (DM)
   - Configuring Clipboard Monitor Rule (DM)
   - Configuring Cloud Storage Monitor Rule (DM)
   - Configuring Device Monitor Rule (DM)
   - Configuring File Monitor Rule (DM)
   - Configuring FTP Monitor Rule (DM)
   - Configuring HTTPS Monitor Rule (DM)
   - Configuring IM Client Monitor Rule (DM)

- Configuring Mail Monitor Rule (DM)
- Configuring Network Monitor Rule (DM)
- Configuring Photo Monitor Rule (DM)
- Configuring Print Monitor Rule (DM)
- Configuring ScreenShot Control Monitor Rule (DM)
- Configuring ScreenShot Monitor Rule (DM)

5. After you have set all necessary parameters, click **OK** in rule (DM) settings.

Warning!

To apply changes you have to save current security scheme (see "Editing Security Scheme"). If you don't save the security scheme, all changes will be discarded.

4.3.2.2.1 Configuring Application Monitor Rule (DM)

An employee can perform actions which can lead to the leakage of confidential information throught third-party applications installed on a Workstation and not controlled by InfoWatch Device Monitor.

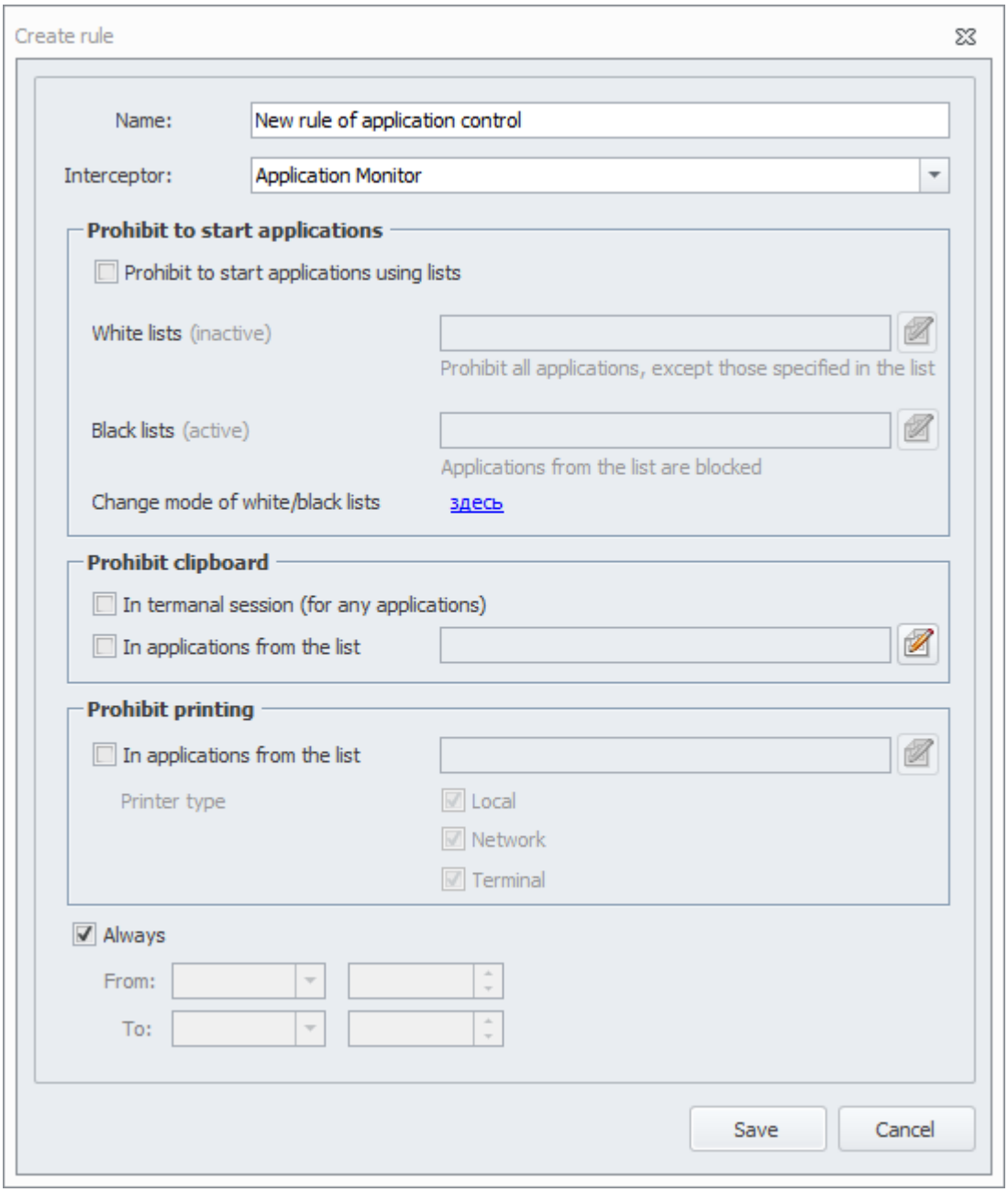
Application Monitor interceptor allows to controll employees' access to applications through ban of:

- appliaction start;
- clipboard;
- print.

The above bans can be activated both separately and together.

Note:

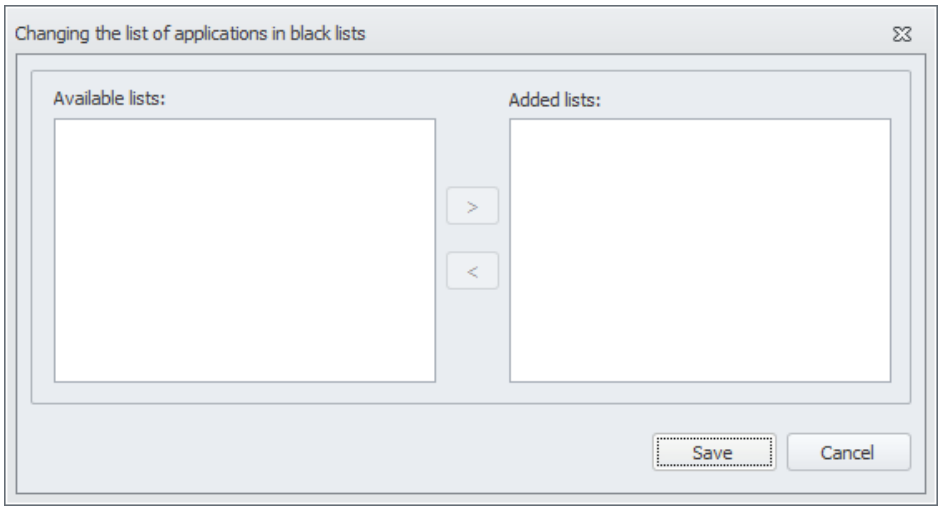
To switch between active black and white application lists, press link here.



To configure the rule, perform the following steps:

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

6. In **Prohibit to start applications** block add white and black applications lists by clicking .



> **Note:**
>
> On application list formation see "Application protocol".

7. In the opened window choose necessecary types of availables lists and move them to Added lists area by pressing >.
8. Click **Save**.
9. In **Prohibit to start applications** block check the boxes in front of groups of applications that should not be allowed to copy the data:
   - In terminal session (for any applications);
   - In applications from list (add lists by clicking).

   Upon

> **Warning!**
>
> Upon ban clipboard is blocked completely for all data types without separation of copy/paste, regardless of the black/white list mode.

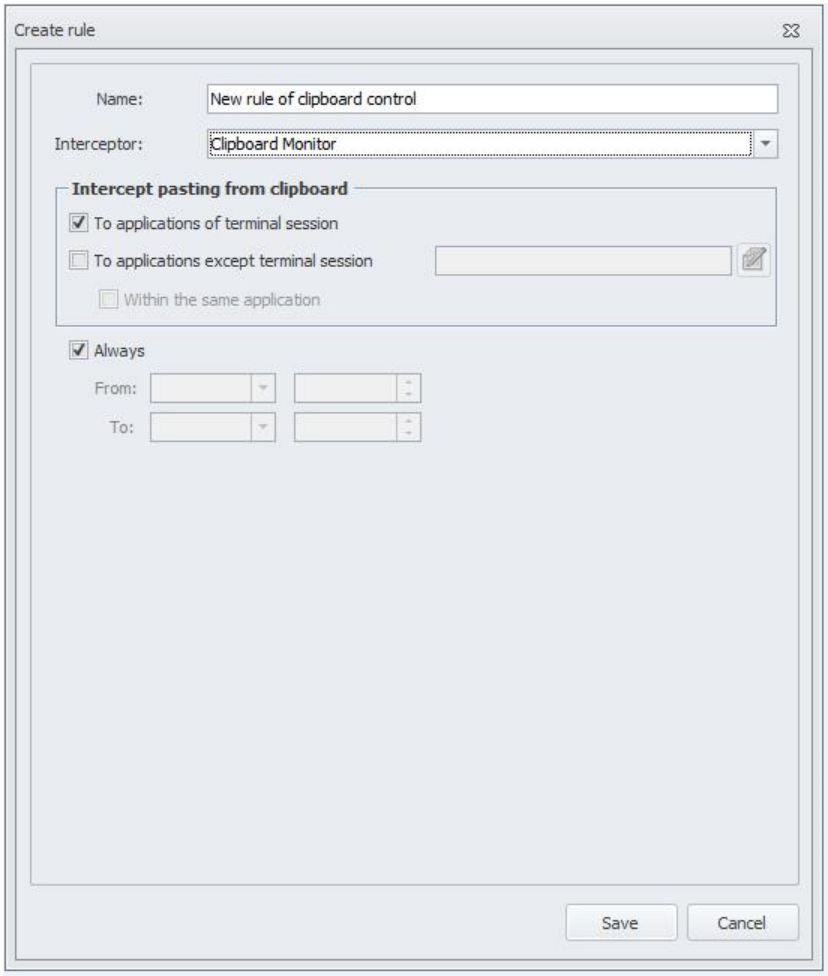
10. In **Prohibit printing** block specify applications, which are banned from printing as well as printer type:
    - Local;
    - Network;
    - Terminal.

User cannot send to print data in specified applications. He will also have no access to chosen printers.

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

4.3.2.2.2 Configuring Clipboard Monitor Rule (DM)

The Clipboard Monitor interceptor allows you to control access of employees to the clipboard.



To configure the rule, perform the following steps:

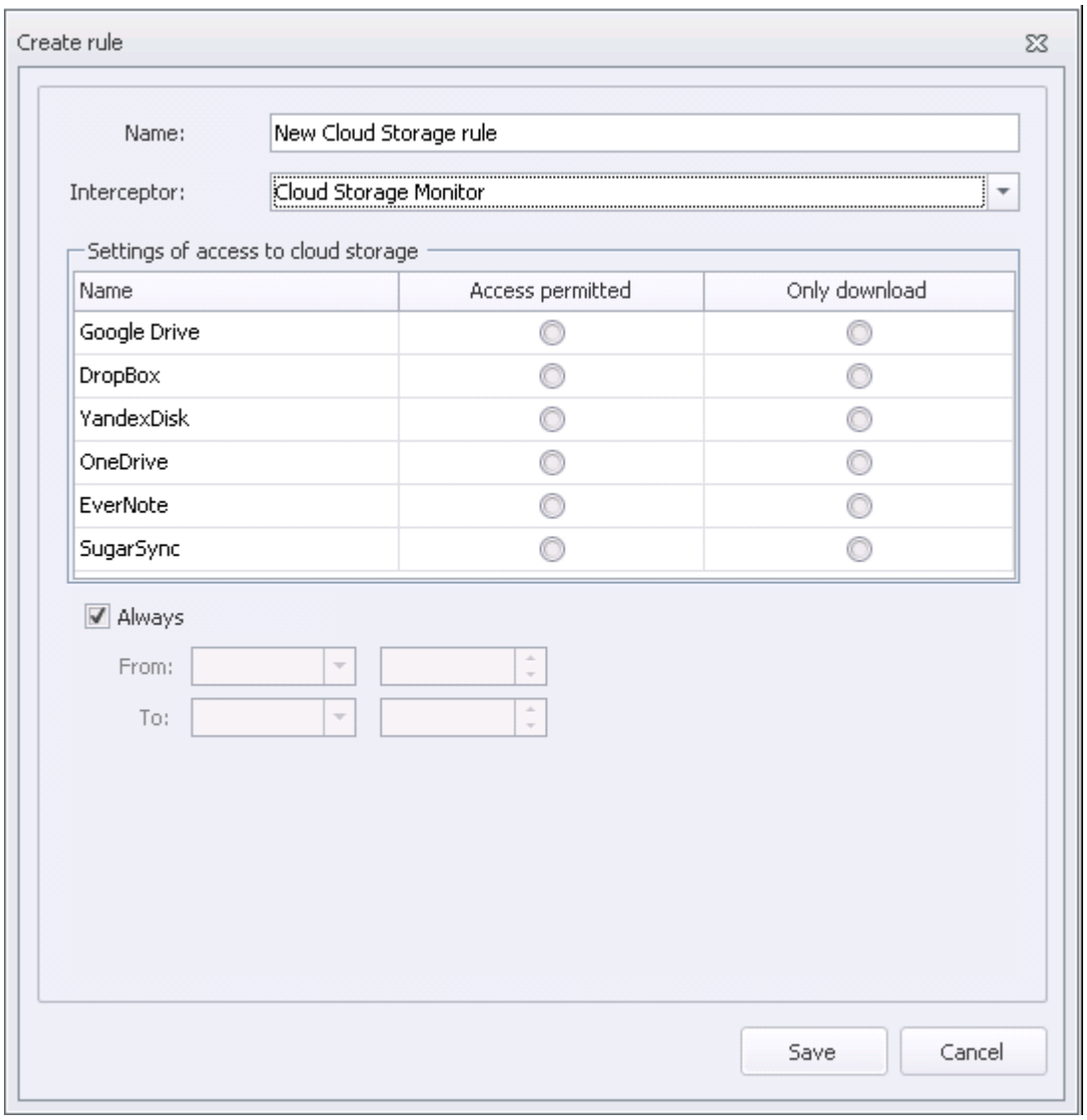
1. Go to **Policies** section.
2. In **Policies** area at Navigation pane, select a security policy (DM) to which you want to add a rule (DM).
3. Do either of the following:
   - in the main menu, select **Edit > Create rule**;
   - click **Create rule** at the top of **Policies** area;
   - right-click at the empty space in **Policies** area and select **Create rule** from the drop-down list.
4. In **Create rule** dialog in the **Interceptor** field, select **Clipboard Monitor**.
5. Enter rule (DM) name to **Name** field.

6. In **Intercept pasting from clipboard** area, define in which case the rule (DM) will trigger:
    - **To applications of terminal session**. If the option is selected, then the rule (DM) will trigger when data is pasted to applications of a terminal session. Pasting data within a terminal session does not trigger the rule.
    - **To applications except terminal session**. If the option is selected, then the rule (DM) will trigger only when data is pasted to specified applications. To choose applications, click  button (see "Application protocol"). The rule also applies to data copied from a terminal session
      If you need the rule to be trigger when data is pasted to the application from which it has been copied, select the **Within the same application** option.
7. Define a period of rule (DM) action. By default, the rule (DM) is always in effect (**Always** option is checked). To specify the rule (DM) duration, clear **Always** check box and specify dates and time in **From** and **To** fields.
8. When all parameters are configured, click **Save**.

4.3.2.2.3 Configuring Cloud Storage Monitor Rule (DM)

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

Storage name	Restriction options
Google Drive	Access Denied/Only download
DropBox	Access Denied/Only download
YandexDisk	Access Denied/Only download
OneDrive	Access Denied/Only download
EverNote	Access Denied/Only download
SugarSync	Access Denied/Only download



To configure the rule, perform the following steps:

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

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

4.3.2.2.4 Configuring Device Monitor Rule (DM)

Device Monitor interceptor allows you to control employee access to peripheral devices and the devices connected to the thin and thick terminal clients.
(see "Glossary").
Control of terminal clients, which are connected to Device Monitor Client Workstation via Microsoft RDP or Citrix ICA can be useful in the following situation:

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

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

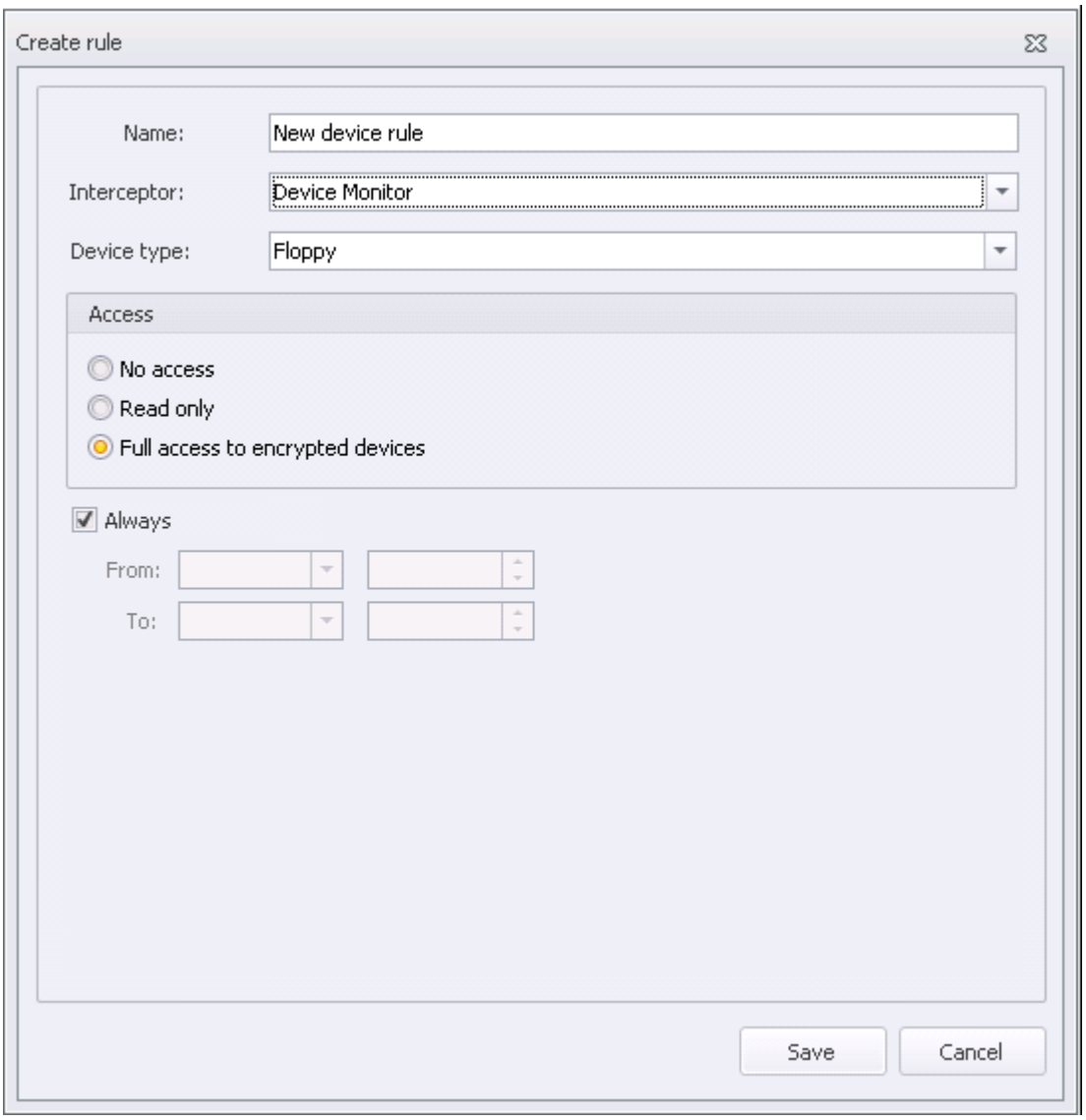
Pocket Computer (Windows Mobile and Palm OS pocket computers)	Denied
Network printer	Denied
Microsoft RDP or Citrix ICA connection control	
Terminal printer	Denied
Terminal storage	Read only/Access denied
Terminal port (thin client port)	Denied
Terminal Plug and Play devices	Denied

Note:

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

Warning!

If event matches multiple rules (DM), see "Rules Application (DM)" and "Device Monitor Rules (DM) Application".



To configure the rule, perform the following steps:

1. Go to **Policies** section.
2. In **Policies** area at Navigation pane select a security policy (DM) which you want to add a rule to.
3. Take one of the following steps:
   - in the Main Menu select **Edit > Create rule**;
   - click **Create rule** at the top of **Policies** area;
   - right-click at the empty space in **Policies** area and select **Create rule** from the drop-down list.
4. In **Create rule** dialog in **Interceptor** field select **Device Monitor**.
5. Enter rule (DM) name to **Name** field.
6. Select a peripheral type controlled by this rul (DM)e from **Device type** drop-down list.
7. In **Access** area select needed access level (see table above).

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

4.3.2.2.5 Configuring File Monitor Rule (DM)

File Monitor interceptor allows you to monitor the following operations: copying files to network resources and writing to the file on a removable device. The System registers only successful operations. With this rule, you can monitor the following actions of employees:

- Copying a file to network resources using UNC (for example, *Server**SharedFolder**Folder**File*)
- Copying or moving files to a removable device. The System monitor operation of copying/moving from a controlled computer, another removable device or a network resource

> **Note:**
>
> The following removable devices are supported:
>
> - devices connected via USB and IEEE 1394 ports (FireWire, i-Link)
> - floppy disk storage systems (floppy disk drive, ZIP drive)
> - optical disks (CD, DVD, BD) in Live File System mode
> - network volumes

- Creating a file directly on a removable device
- Editing a file directly on a removable device, including file renaming
- Copying a file to media devices connected via MTP

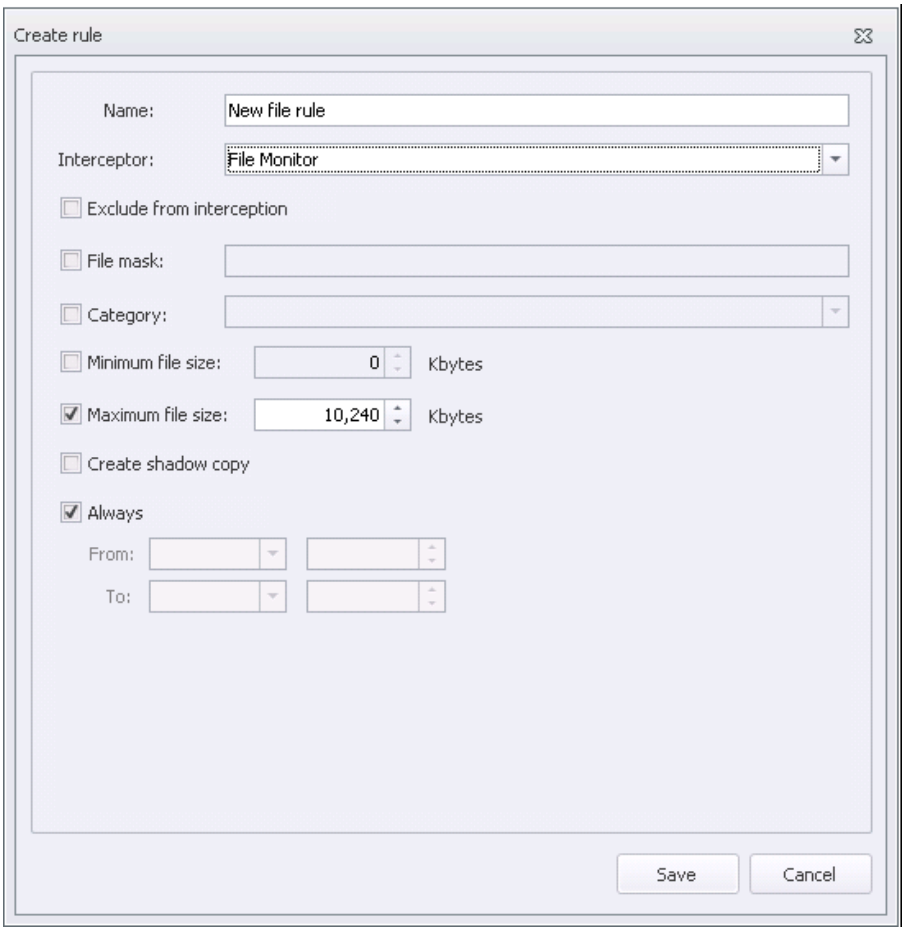
> **Note:**
>
> File renaming on media devices is not supported.

- Copying a file to a terminal session application
- Copying a file to resource connected via a terminal session (redirection for network folders and virtual devices is supported)

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

Warning!

Information about rule (DM) conflict resolving see in "Rules Application (DM)".



To configure the rule, perform the following steps:

1. Go to **Policies** section.
2. In **Policies** area at Navigation pane, select a security policy (DM) to which you want to add a rule.
3. Do either of the following:
   - in the Main Menu select **Edit > Create rule**;
   - click **Create rule** at the top of **Policies** area;
   - right-click at the empty space in **Policies** area and select **Create rule** from the drop-down list.
4. In **Create rule** dialog in **Interceptor** field, select **File Monitor**.
5. Enter rule (DM) name to the **Name** field.
6. If you want to exclude specific files from interception, flag **Exclude from interception**. For operation satisfying this rule, no events or shadow copies will be created.

Warning!

If file record event is a subject of several rules (DM), the excluding rule (DM) has the highest priority.

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

Warning!

There should be only one mask for one rule (DM). In case it is required to type in several masks, one should create a rule (DM) corresponding to mask.

8. You can constrain controlled files by signature category (see "Signatures"). Flag Category checkbox and select a category from a drop-down list: the rule (DM) will be applied to files with chosen signature type.
9. To control files by size, specify:
    - **Minimum File Size**. When checked, rule (DM) will be applied only to files larger or of the specified size.
    - **Maximum File Size**. When checked, rule (DM) will be applied only to files smaller or of the specified size.
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 (DM) for File Monitor that enables shadow copying, and there is less free space at the hard drive than required by the policy (DM) (see "Creating Shadow Copies and Blocking Operations Due to Free Space Shortage"), then file saving will be performed without shadow copy creating.

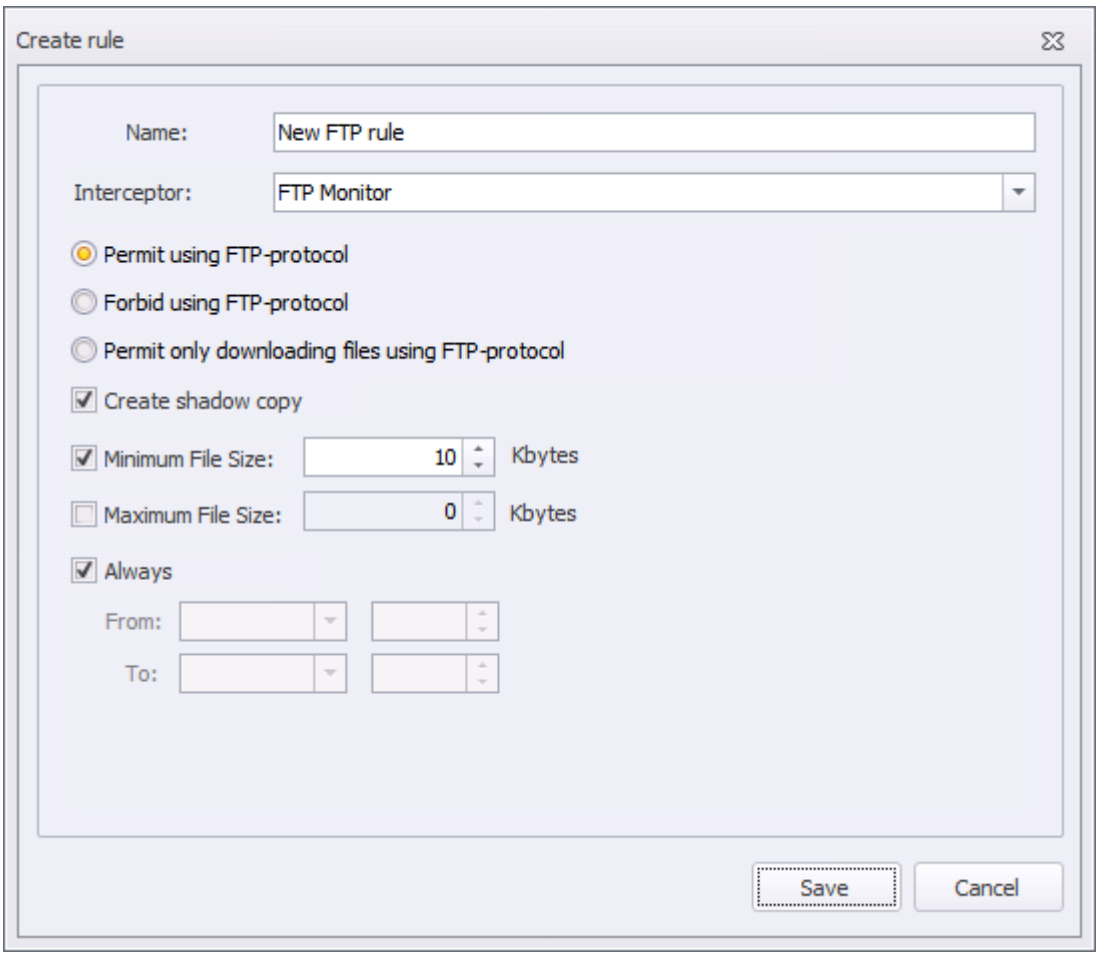
11. Define a period of rule (DM) action. By default, the rule (DM) is always in effect (**Always** option is checked). To specify rule (DM) duration, clear **Always** check box and specify dates and time in From and To fields.
12. When all parameters are configured, click **Save**.

4.3.2.2.6 Configuring FTP Monitor Rule (DM)

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

Warning!

The file is subject to **FTP Monitor** rule (DM) if **ALL** file parameters meet rule (DM) conditions **EXCEPT** maximum and minimum file size. **Maximum file size** and **Minimum file size** are taken into consideration only for shadow copying. So if 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 (DM) which you want to add a rule (DM) to.
3. Take one of the following steps:
   - in the Main Menu select **Edit > Create rule**;
   - click **Create rule** at the top of **Policies** area;
   - right-click at the empty space in **Policies** area and select **Create rule** from the drop-down list.
4. In **Create rule** dialog in Interceptor field select **Ftp Monitor**.
5. Enter rule (DM) name to **Name** field.
6. Select inspection level for data transfer through FTP/FTPS protocol:
   - **Permit using FTP-protocol**

- **Forbid using FTP-protocol**
- **Permit only downloading files using FTP-protocol**

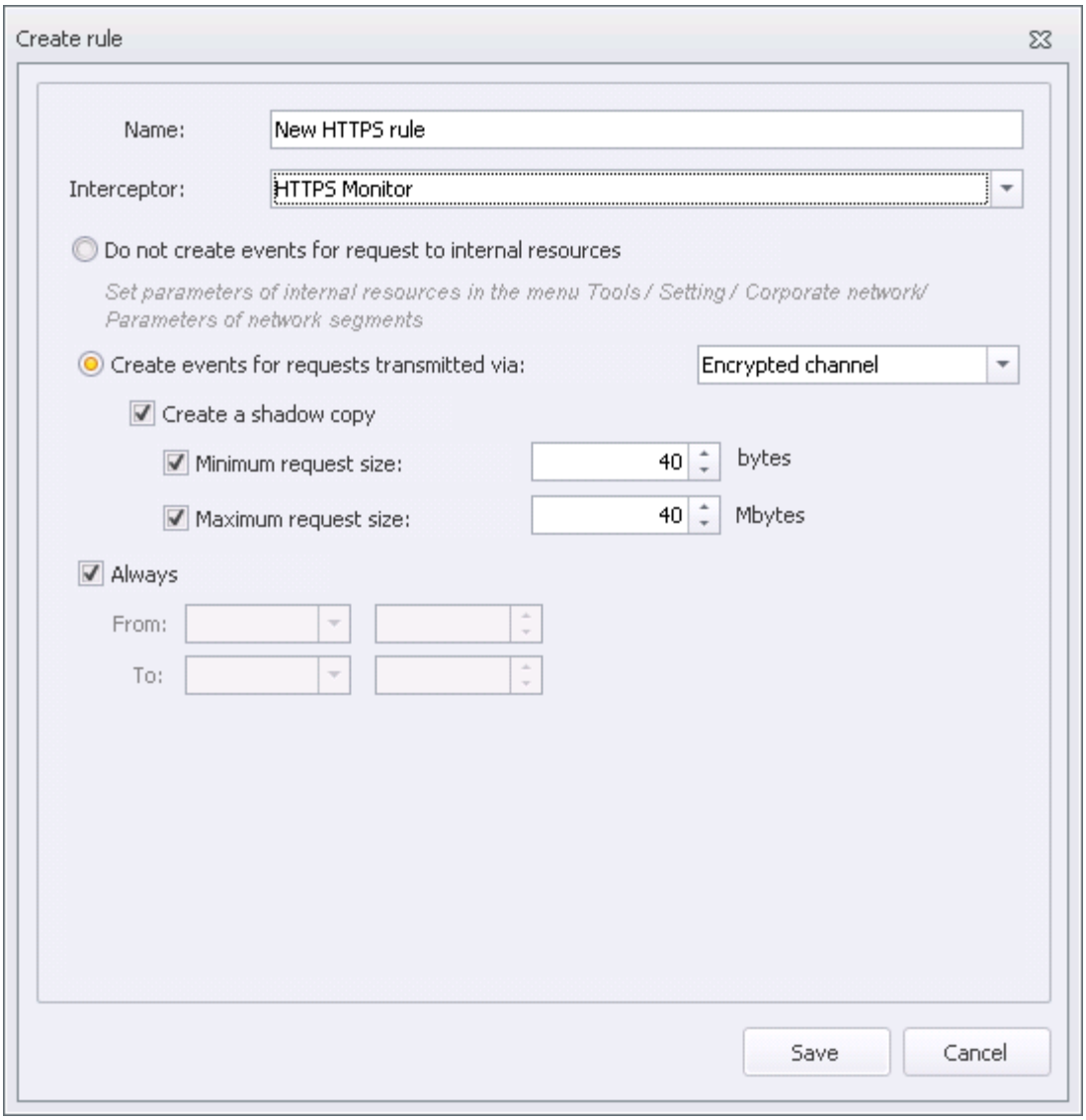
7. If you allowed using FTP/FTPS protocol then you can also configure creating of shadow copies of outgoing files. You can select **Create a shadow copy** check box and specify additional settings:
   - **Minimum File Size**. If the check box is selected, shadow copies will be enabled only for files of specified size or larger.
   - **Maximum File Size**. If the check box is selected, shadow copies will be enabled only for files of specified size or smaller.

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

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

4.3.2.2.7 Configuring HTTPS Monitor Rule (DM)

HTTPS Monitor interceptor lets to control data transfer through HTTP and 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 (DM) which you want to add a rule (DM) to.
3. Take one of the following steps:
   - in the Main Menu select **Edit > Create rule**;
   - click **Create rule** at the top of **Policies** area;
   - right-click at the empty space in **Policies** area and select **Create rule** from the drop-down list.
4. In **Create rule** dialog in Interceptor field select **HTTPS Monitor**.
5. Enter rule (DM) name to **Name** field.
6. Specify the interception of internal resources queries. To do this in the **Do not create events for request to 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. To setup interception of HTTP, mark the checkbox **Create requests for events transmitted via**: pick **All Channels**. To setup interception of HTTPS, pick **Encrypted channel**.
8. 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!**
>
> In case there is not enough space available on a Workstation (see. "Creating Shadow Copies and Blocking Operations Due to Free Space Shortage"), shadow copy will not be created.

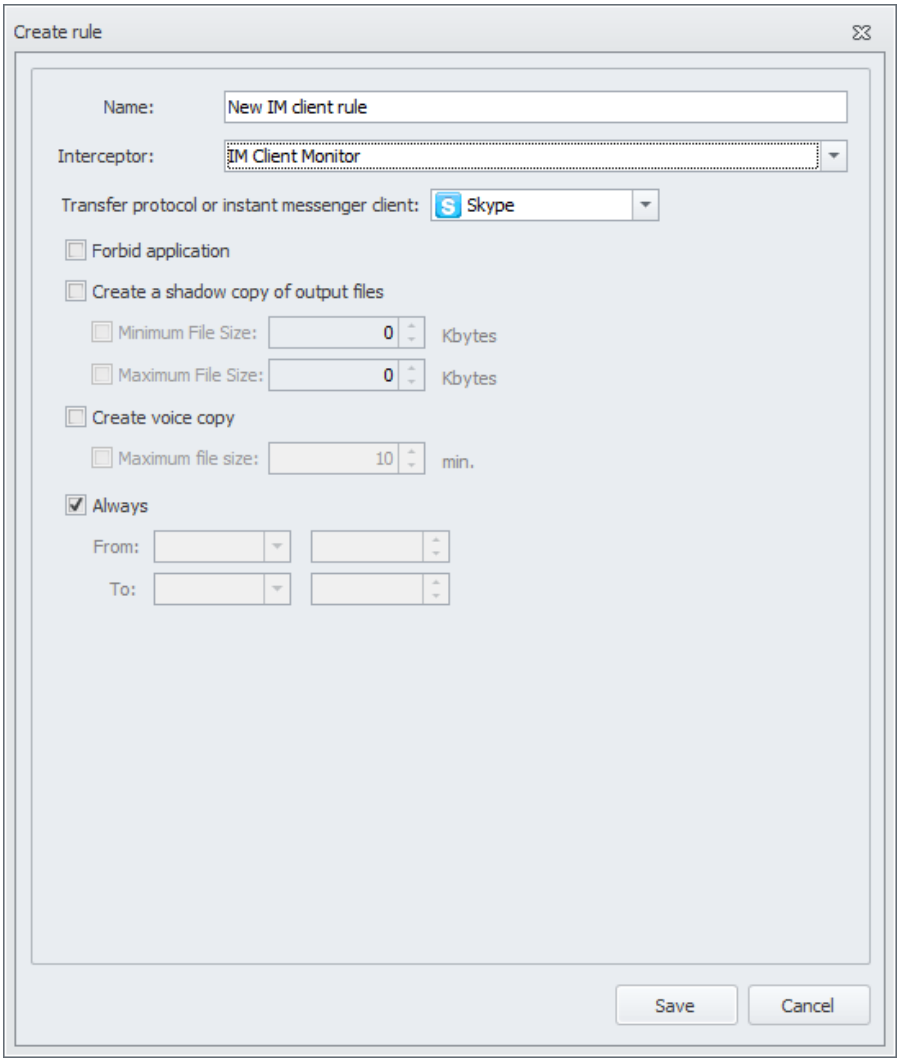
9. Define a period of rule (DM) action. By default, the rule (DM) is always in effect (**Always** option is checked). To specify rule (DM) duration, clear **Always** check box and specify dates and time in **From** and **To** fields.
10. When all parameters are configured, click **Save**.

4.3.2.2.8 Configuring IM Client Monitor Rule (DM)

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 (DM): see "Network Traffic Control".

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



To configure the rule, perform the following steps:

1. Go to **Policies** section.
2. In **Policies** area at Navigation pane select a security policy (DM) which you want to add a rule (DM) to.
3. Take one of the following steps:
   - in the Main Menu select **Edit > Create rule**;
   - click **Create rule (DM)** at the top of **Policies** area;
   - right-click at the empty space in **Policies** area and select **Create rule** from the drop-down list.
4. In **Create rule** dialog in Interceptor field select **IM Client Monitor**.
5. Enter rule (DM) name in the **Name** field.
6. In **Transfer protocol or instant messenger client** field, select messenger type which is controlled by this rule (DM):
   - Skype - to control Skype usage;
   - XMPP - to control Jabber usage;

- MMP - to control Mail.Ru Agent usage;
- SMS - to control mobile devices usage;
- WhatsApp - to control WhatsApp usage on mobile devices.

7. In case it is required to intercept Skype voice messages, mark the **Create shadow copy of output files** checkbox and, if necessary, specify file size (sound file will be saved in *.ogg format)
   - If **Maximum File Size** box is checked, then several events with shadow copies will be created for talks, whose length exceeds the specified value.

> **Note:**
>
> Voice traffic is not supported for a mobile version.

8. In case you want to entirely ban using Client of this type, mark the **Forbid application** checkbox (not available for **SMS of mobile connection** and **WhatsApp**).

> **Note:**
>
> To Skype, the setting applies as follows: the interceptor checks if the application is started and, if yes, forcibly closes it. The check is performed every minute.

> **Warning!**
>
> To forbid using WhatsApp and Skype mobile version, use Application Monitor Rule (DM) (see "Configuring Application Monitor Rule (DM)")

9. If you want to create and transfer shadow copies of transferred files to Traffic Monitor, mark the **Create shadow copy of output file** checkbox. In this case, you will be able to define additional parameters for these copies:
   - **Minimum File Size**. When checked, shadow copying will only be performed for files larger or equal in size.
   - **Maximum File Size**. When checked, shadow copying will only be performed for files smaller or equal in size.

Warning!

Shadow copy of chats and messages are always created (regardless of **Create shadow copy** setting), in case there is at least one **IM Client Monitor** active rule (DM) on the computer.

The frequency of creating shadow copies from chats and messages (time period and the number of messages, which form a shadow copy) is described in the article "Network Traffic Control".

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

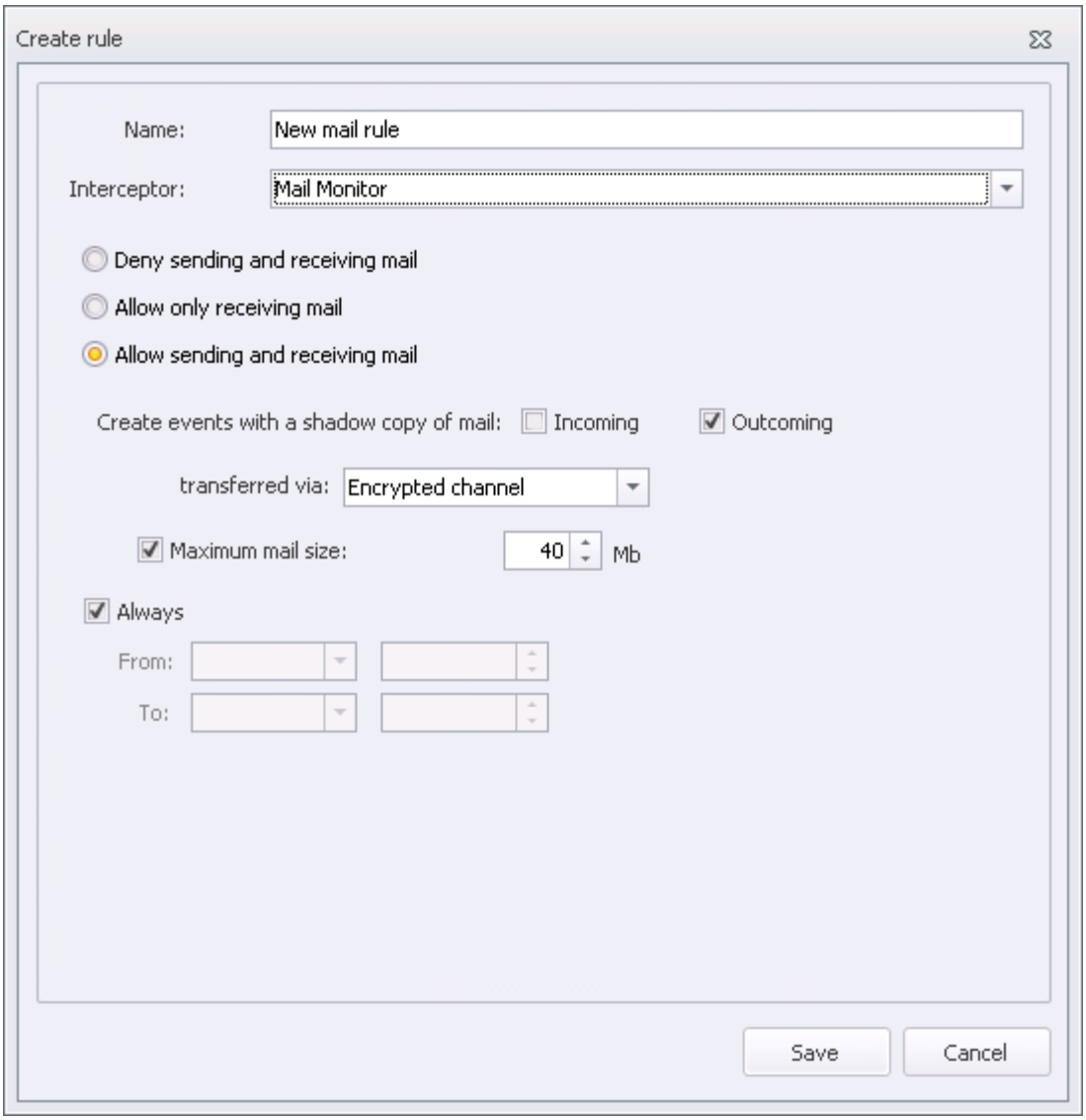
Warning!

In case shadow copy of message or chat must be created in accordance with an active IM Client Monitor rule (DM), but there is less free space on a computer, than it was defined by a policy (DM) (see "Creating Shadow Copies and Blocking Operations Due to Free Space Shortage"), then shadow copies of the messages will be saved, but files will be transferred without shadow copy creation.

4.3.2.2.9 Configuring Mail Monitor Rule (DM)

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

Mail Monitor allows control of SMTP, IMAP, POP3, MAPI mail protocols.



To configure the rule, perform the following steps:

1. Go to **Policies** section.
2. In **Policies** area at Navigation pane select a security policy (DM) which you want to add a rule (DM) to.
3. Take one of the following steps:
   - in the Main Menu select **Edit > Create rule**;
   - click **Create rule** at the top of **Policies** area;
   - right-click at the empty space in **Policies** area and select **Create rule** from the drop-down list.
4. In **Create rule** dialog in Interceptor field select **Mail Monitor**.
5. Enter rule (DM) name to **Name** field.
6. Choose control level fpor sent and recieved mail:
   - **Deny sending and recieving mail**;

- **Allow only recieving mail**;
- **Allow sending and receiving mail**.

> **Warning!**
>
> Depending on the outgoing and incoming mail control method, the following variants of shadow copy creation are possible:
>
> - **Deny sending and receiving mail** -shadow copies are not being created;
> - **Allow only receiving mail** - for incoming mail (for shadow copy creation, tick the **Incoming** box);
> - **Allow sending and receiving mail** - for incoming and outgoing mail (for shadow copy creation, tick the **Incoming** and **Outcoming**).

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

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

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

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

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

Warning!

In case existing rule (DM) has attributes:

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

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

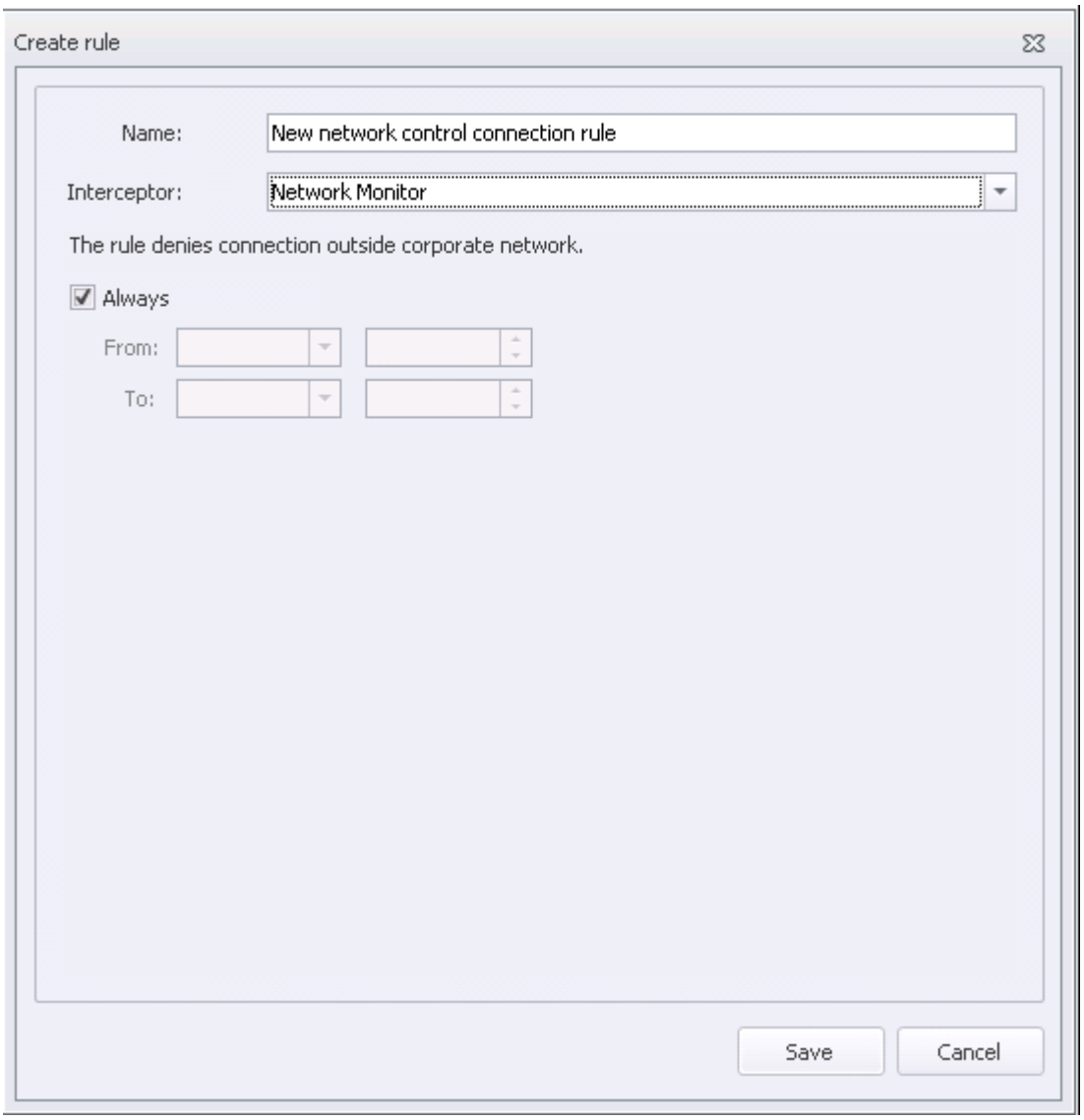
Manage shadow copy creation. Tick the Incoming or Outcoming box in a Create events with a shadow copy of mail line.

4.3.2.2.10 Configuring Network Monitor Rule (DM)

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

Warning!

As at least one Network Monitor takes effect, Device Monitor Agent installed on the computer will try to approve DNS-names of opened internet pages. To prevent problems with external connections, it is required to configure forwarders usage on a corporate DNS-server (see internet article "Configure a DNS Server to Use Forwarders").

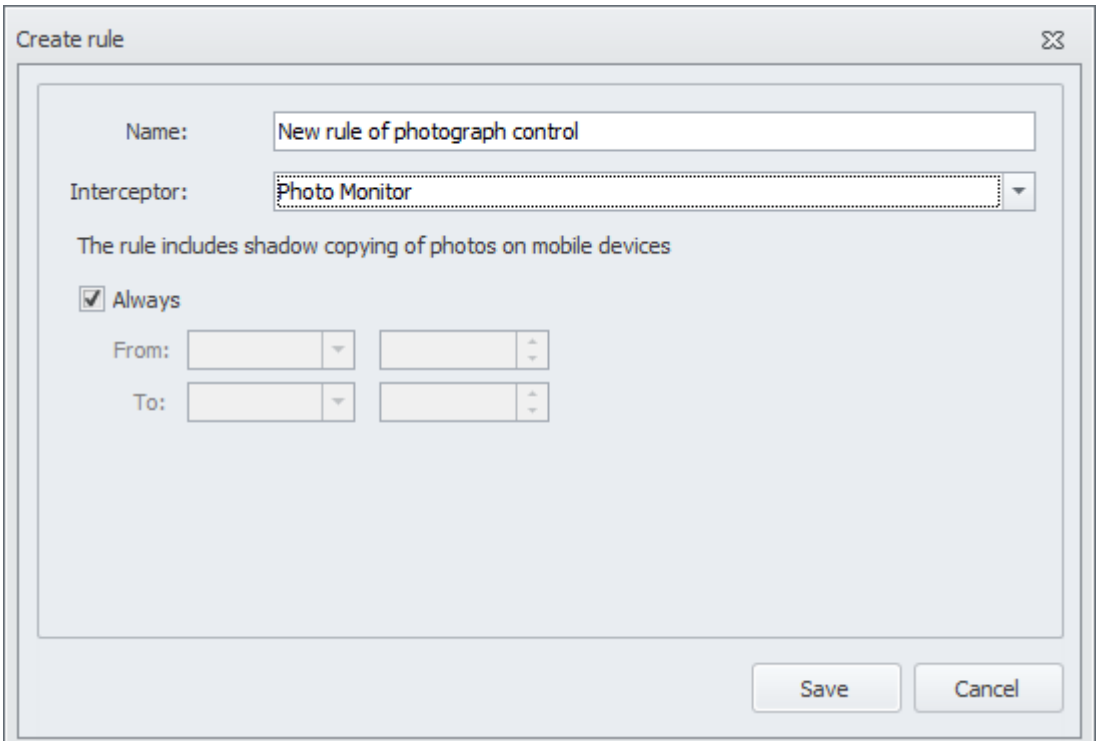


To configure the rule, perform the following steps:

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

4.3.2.2.11 Configuring Photo Monitor Rule (DM)

Photo Monitor interceptor allows to perform shadow copying of photos, created with the cameras on controlled mobile devices.



To configure the rule, perform the following steps:

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

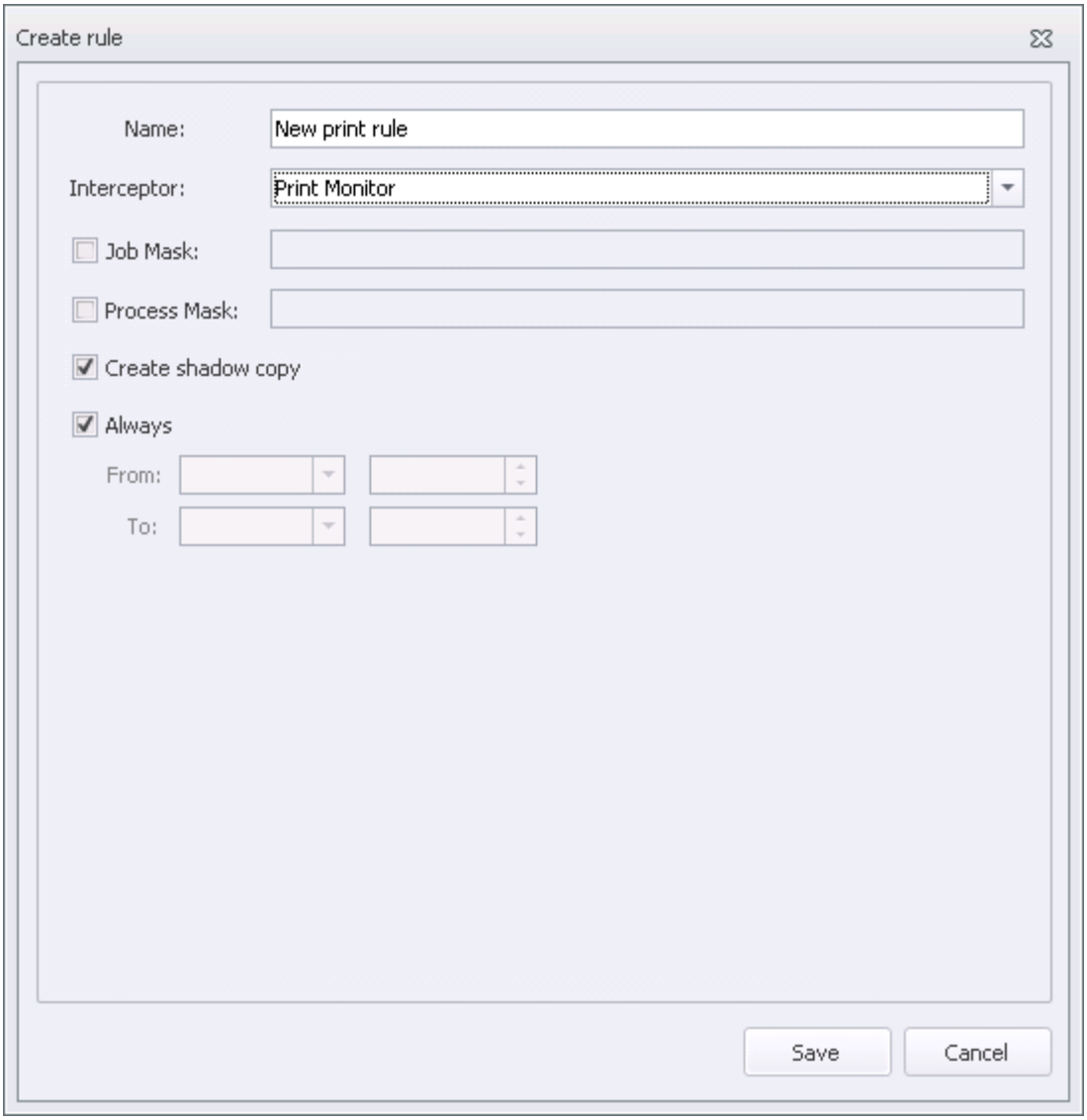
> **Warning!**
>
> In case there is not enough space available on a Workstation (see. "Creating Shadow Copies and Blocking Operations Due to Free Space Shortage"), shadow copy will not be created.

6. Define a period of rule (DM) action. By default, the rule (DM) is always in effect (**Always** option is checked). To specify rule (DM) duration, clear **Always** check box and specify dates and time in **From** and **To** fields.

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

4.3.2.2.12 Configuring Print Monitor Rule (DM)

Print Monitor interceptor allows you to perform monitoring of operations, which are connected with printing documents on local and network printers.



To configure the rule, perform the following steps:

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

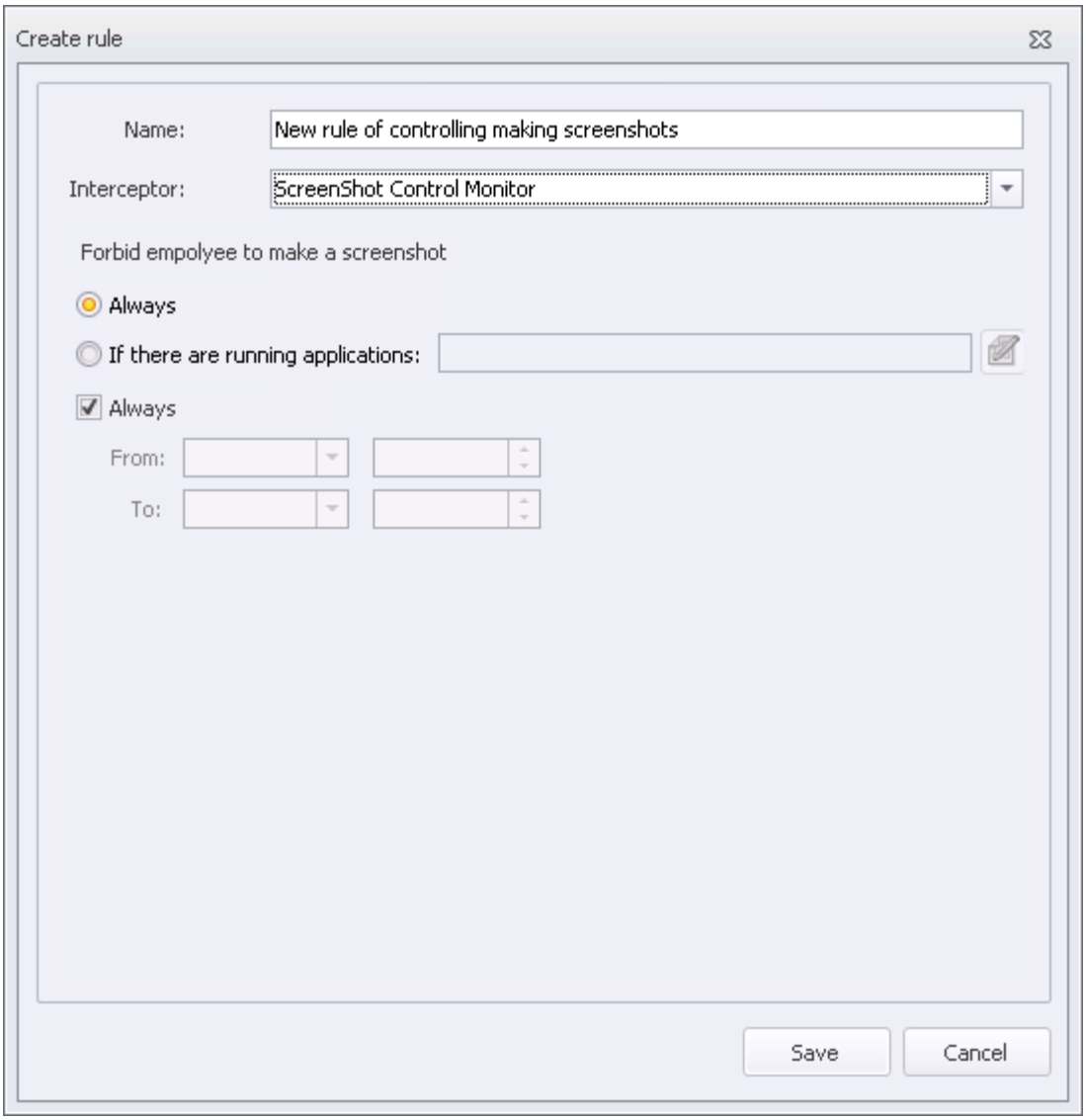
4. In **Create rule** dialog in Interceptor field select **Print Monitor**.
5. Enter rule (DM) name to **Name** field.
6. If necessary, you can limit controlled print tasks with the help of masks:
    - **Job Mask**. Using mask for task (document) which is sent for print. If required to specify job task, check the box and specify the task.
      Name of the printing task is formed by application, from which document is sent for print. Therefore, name can look like any text line, including not connected to the printed document type.
      In task mask one can use substitution symbols: «?» to replace one character or «*» to replace character set. "Space" is interpreted as part of the task name.
    - **Process Mask**. Using mask for process, which takes the print job. If required to create process mask, check the box and specify process mask.
      Name (full path) of the process will be aquired for the process, in which context rendering of a print job is performed. In some cases (local LPT- and COM-printers) printing subsystem can perform rendering in the context of the Print Spooler service. Path to the executable file of the service: `%SystemRoot%\system32\spoolsv.exe`.
      For the process name to be identified correctly, it is necessary to set **Print directly to the printer** (**Printer properties** > **Additionally**) parameter in printer properties. In this case, task processsing will take place in context of the appliaction, from which the document was sent to print.
      However, in this case, the print will occur synchronously, i.e interaction with applications will be impossible until the printing is over.
      In task mask one can use substitution symbols: «?» to replace one character or «*» to replace character set. "Space" is interpreted as part of the task name.
7. If you want to create and transfer shadow copies of printing documents to Traffic Monitor, mark **Create shadow copy** checkbox.

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

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

4.3.2.2.13 Configuring ScreenShot Control Monitor Rule (DM)

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



To configure the rule, perform the following steps:

1. Go to **Policies** section.
2. In **Policies** area at Navigation pane select a security policy (DM) which you want to add a rule (DM) to.
3. Take one of the following steps:
   - in the Main Menu select **Edit > Create rule**;
   - click **Create rule** at the top of **Policies** area;
   - right-click at the empty space in **Policies** area and select **Create rule** from the drop-down list.
4. In **Create rule** dialog in Interceptor field select **ScreenShot Control Monitor**.
5. Enter rule (DM) name to **Name** field.
6. In area Forbid employee to make a screenshot define a rule (DM) period::
   - **Always**. Has no time limit by default.

- **If there are running applications**. Pick a list of applications using  button (see "Applications protocol").

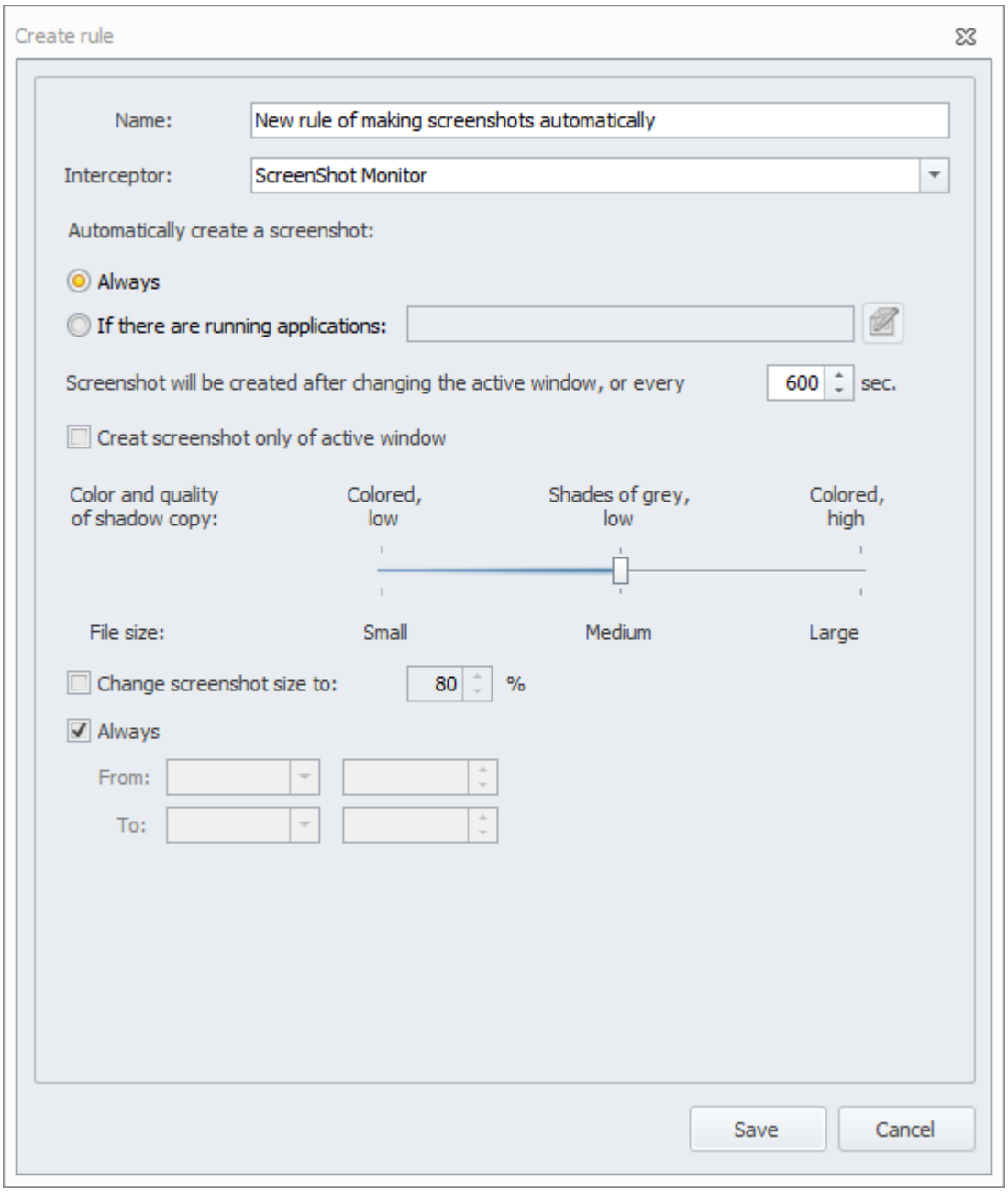
7. Define a period of rule (DM) action. By default, the rule (DM) is always in effect (**Always** option is checked). To specify rule (DM) duration, clear **Always** check box and specify dates and time in **From** and **To** fields.
8. When all parameters are configured, click **Save**.

4.3.2.2.14 Configuring ScreenShot Monitor Rule (DM)

The **ScreenShot Monitor** interceptor allows you to automatically create screenshots on controlled computers.

Warning!

The **Do not create screenshots in case mouse or keyboard have been inactive for a long time** parameter, which defines how the rule works depending on the activity on controlled computers, is configured along with general security settings (see "Control of Applications and Screenshots").



To configure the rule, perform the following steps:

1. Go to **Policies** section.
2. In **Policies** area at Navigation pane, select a security policy (DM) to which you want to add a rule (DM).
3. Do either of the following:
   - in the main menu, select **Edit > Create rule**;
   - click **Create rule** at the top of **Policies** area;
   - right-click at the empty space in **Policies** area and select **Create rule** from the drop-down list.
4. In **Create rule** dialog in the **Interceptor** field, select **ScreenShot Monitor**.
5. Enter rule (DM) name to **Name** field.

6. In the **Automatically create a screenshot** area, define in which case the rule (DM) will be valid:
    - **Always**. Has no time limit by default.
    - **If there are running applications**. Pick a list of applications using  button (see "Application protocol").
7. Specify periodicity of screenshots creation (in seconds). The default value is 600. A screenshot is also created when the active window changes.
8. If necessary, mark the **Create screenshot only of active window** checkbox. By default, a picture of the whole screen is taken.
9. Choose the color mode and the quality of created copies. Available color modes:
    - **Colored, low**. A colored file in a low resolution. Use this mode, in case you need files of small size.
    - **Shades of gray, low**. A file in greyscale mode in a low resolution.
    - **Colored, high**. A colored file in a high resolution. Use this mode, when you need high-quality images regardless of their size .
10. If you need to decrease the file size while saving, mark the **Change screenshot size to** checkbox and specify the value in percent (the percentage is calculated from the original file size).
11. Define a period of rule (DM) action. By default, the rule (DM) is always in effect (**Always** option is checked). To specify the rule (DM) duration, clear **Always** check box and specify dates and time in **From** and **To** fields.
12. When all parameters are configured, click **Save**.

4.3.2.3 Editing a Rule (DM)

To edit a rule:

1. Go to **Policies**.
2. In **Policy** area of Navigation pane select the title of security policy (DM) that contains the rule (DM). The main window will display the full list of the policy (DM) rules (DM).
3. Select the row with the name of the rule (DM) you want to edit.
4. Take one of the following steps:
    - in Main Menu click **Edit > Edit Rule**;
    - double-click the selected row;
    - click  **Edit Rule** at the top of **Policy** area;
    - use **Ctrl+Shift+E** shortcut.
5. Edit rule (DM) parameters:
    - Configuring Application Monitor Rule (DM);
    - Configuring Clipboard Monitor Rule (DM);
    - Configuring Cloud Storage Monitor Rule (DM);
    - Configuring Device Monitor Rule (DM);
    - Configuring File Monitor Rule (DM);

- Configuring FTP Monitor Rule (DM);
- Configuring HTTPS Monitor Rule (DM);
- Configuring IM Client Monitor Rule (DM);
- Configuring Mail Monitor Rule (DM);
- Configuring Network Monitor Rule (DM);
- Configuring Photo Monitor Rule (DM);
- Configuring Print Monitor Rule (DM);
- Configuring ScreenShot Control Monitor Rule (DM);
- Configuring ScreenShot Monitor Rule (DM).

6. When all changes are made click **Save** in rule (DM) configuration dialog.

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

4.3.2.4 Deleting a Rule (DM)

To delete a rule:

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

> **Note:**
>
> To delete multiple rules (DM) from a single security policy (DM), select the rows with the names of all rules (DM) you want to remove.

4. Take one of the following steps:
   - in Main Menu click **Edit > Delete Rule**;
   - use  **Delete rule**, which is located in the upper part of **Policies** area;
   - click **Delete** button on a keyboard.
5. In request box select **Yes** to confirm that you want to remove the rule (DM).

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

4.3.2.5 Copying a Rule (DM)

Rules (DM) can be copied from one security policy to another.
To copy a rule:

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

This copies the rule (DM) to selected security policy (DM).

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

To copy a rule while editing a policy:

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

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

4.3.3 Employees

Employee and employee group management basics are available in "Employees and Employee Groups". Existing security policies (DM) can be assigned only to employee groups. Security policy (DM) for an employee is defined by including his/her account to the employee group.

Warning!

In addition to employee group security policy (DM), each employee is covered by workstation security policy (DM). Information about rule (DM) conflict resolving see in "Rules Application (DM)".

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

Guidelines on account management is available in:

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

4.3.3.1 Viewing Employee and Employee Groups Details

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

Note:

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

To view information for specific employee group,
select group name in employee group list.
To view all registered employees information,
click  **Show All Employees** at the top of Navigation pane.
Employee account information is represented as tabular list. Each row in the list contains a single account. Columns contain accounts' general properties. Extended information on each account is available in **Details** panel.

To view account's detailed properties,
select the row that contains the account name.
Details panel displays table properties including the following information:

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

Note:

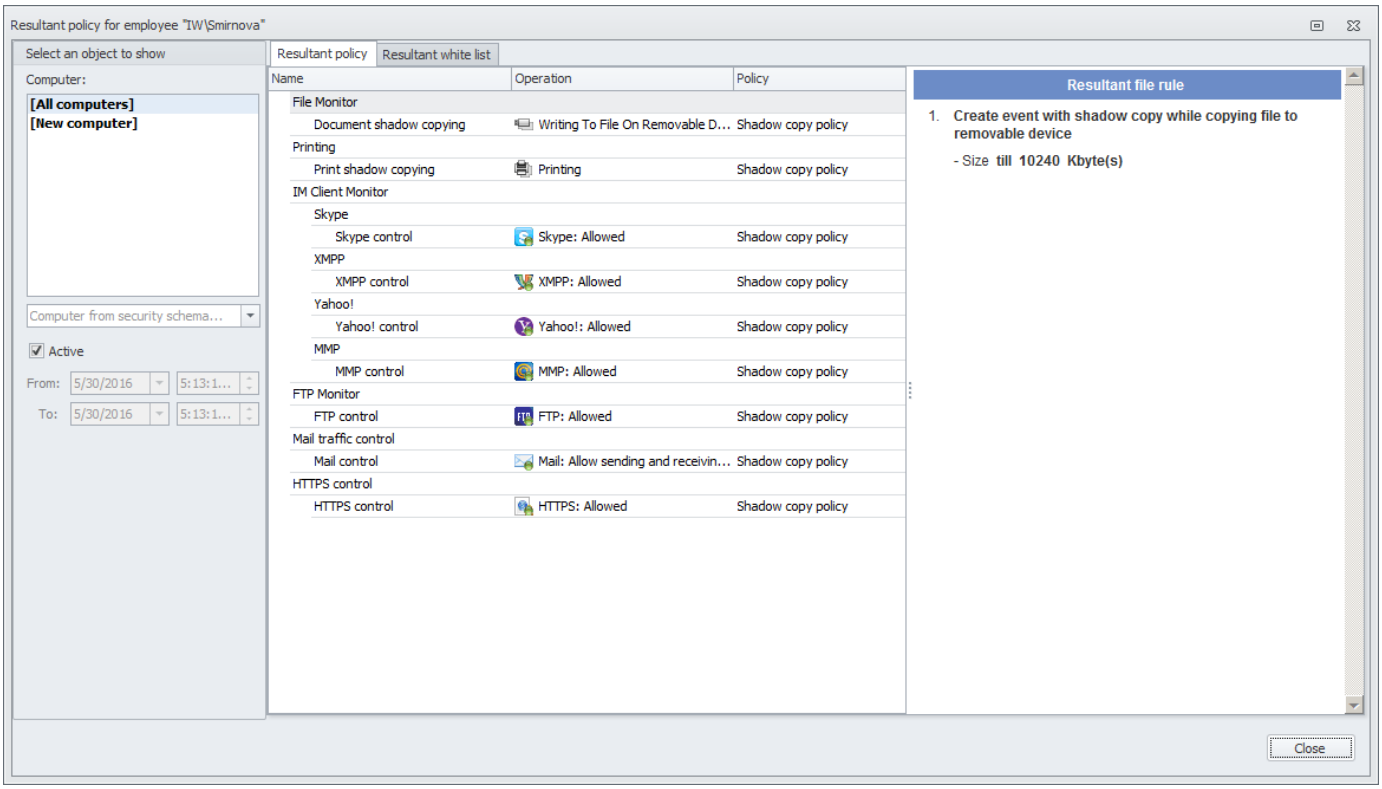
Some information on **Details** panel is duplicated in the main screen workspace.

4.3.3.2 Viewing Resultant Policy (DM) and Resultant White List for an employee

To view information about policy for an employee:

1. In the **Employee** list, pick an employee you want to view policy (DM) and white list for.
2. Proceed with one of the following actions:
   - in the Main Menu choose **Edit -> Show effective policy**.
   - on **Employees pane** click **Show effective policy**.

As a result, a window **Resulting policy for employee<employee name>** will be displayed**:** where by default all resulting policies (DM) for all employees on the chosen computer are displayed.



The main window **Resulting policy for employee<computer name>** area contains three tabs:

- **Resultant policy** - rules (DM) are displayed, that are resulting on a computer. Resulting policy (DM) folds from rules (DM), configured by default, rules (DM), applied for this computer and rules (DM) for computer's users (see "Device Monitor Rules (DM) Application"). To see detailed information about a rule (DM), select it from the list: detailed information will be displayed on the panel on the right.
- **Resultant white list** - displays devices, which are allowed for computer (see "White lists"). To see detailed information about device, select it from the list: detailed information will be displayed on the panel on the right.

On a Workstation pane:

- **All Workstations** - resulting policy (DM) for an employee account without attachment to a workstation.
  Note: to view resulting policy (DM) of an employee for a definite workstation, pick a workstation from Workstation pane or drop-down list Workstations from security schema.

- **New workstation** - resulting policy (DM) for an employee on a new workstation (it is not yet present in the security schema).
- To see resulting policy (DM) for chosen user on a definite computer:
  - from the **Computer** list, choose the name of the computer, on which chosen account is registered

or

- from the **Computer from seciruty schema** drop-down list choose any account on computer, which is registered in the System (see "Computers").

You can choose time period for resulting policy/white list:

- Default setting is **Active** and current resulting policies (DM) and white list is displayed;
- To see resulting policy/white lists for chosen emloyee for defined period, untick the **Active** checkbox and specify time period.

4.3.3.3 Adding and Editing an Employee Group

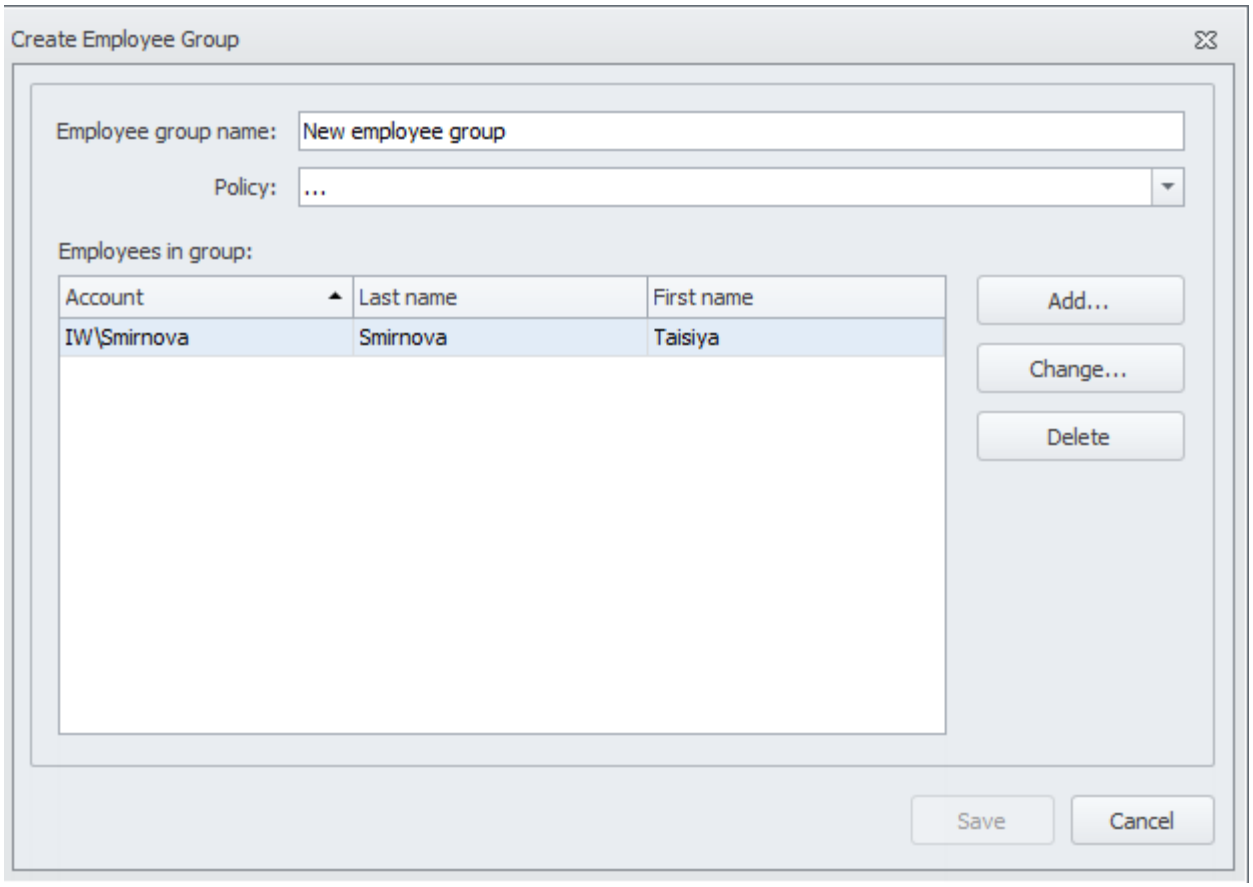
To add or edit an employee group:

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

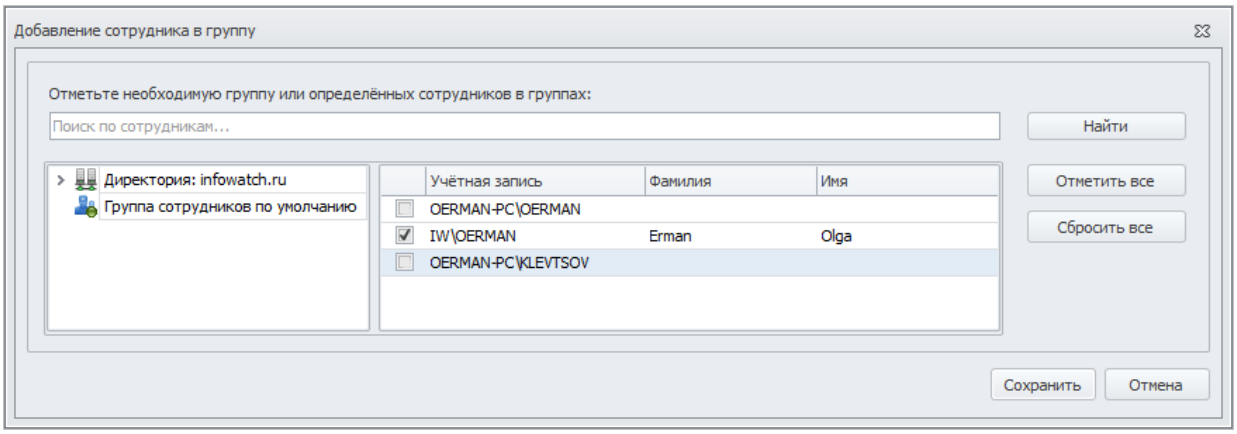
Action	Steps
Add employee group	• select **Edit > Create Employee Group** in the Main Menu; • click **Create Employee Group** at the top of the Navigation Pane.

Edit employee group	1. I**n Employees** area of Navigation Pane select the employee group name. 2. Take one of the following steps: ○ in the Main Menu, click **Edit > Edit Employee Group**; ○ click **Edit Employee Group** at the top of Navigation pane; ○ double-click selected employee group name.

As a result of any of these actions, dialog window will appear to define parameters of employees group.



3. Specify the following parameters:
   - **Employee group name**. Name of employees group.
   - **Policy**. Choose security policy (DM) from the drop-down list, which will be applied to this employess group.
4. Determine the list of employees in the group:
   - To add one or several entries, click **Add**.



The Add employee to the group dialog displays a list of accounts imported from the directory service (see "Connecting to LDAP Server") and 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 (see "Editing Employee Account").

- To edit account parameters, select it from the list of employees belonging to the group and click **Change** (see "Editing Employee Account").
- To delete an entry from the group, select it and click **Delete**.

5. Click **Save**.

Warning!

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

4.3.3.4 Deleting Employee Group

To delete employee group:

1. Go to **Employees** section.
2. Click the employee group you want to delete.
3. Take one of the following steps:
   - select **Edit > Delete Employee Group** in the Main Menu;
   - click **Delete Employee Group** at the top of **Navigation Pane**.
4. Click **Yes** in confirmation box to confirm that you want to remove employee group.

Warning!

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

4.3.3.5 Adding Employee Account to a Group

After InfoWatch Device Monitor Client is installed to the workstation (see document "InfoWatch Traffic Monitor. Inastallation guide" article "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 (DM) assigned to "Default" employee group will be applied to all newly registered employees. In prospect security policy (DM) for an employee is defined by including its account to different employee groups.

To move an employee account from one group to another:

1. Go to **Employees** section.
2. In **Employees area** of Navigation pane select a group containing employee's entry.
3. In **Employees** area of 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.

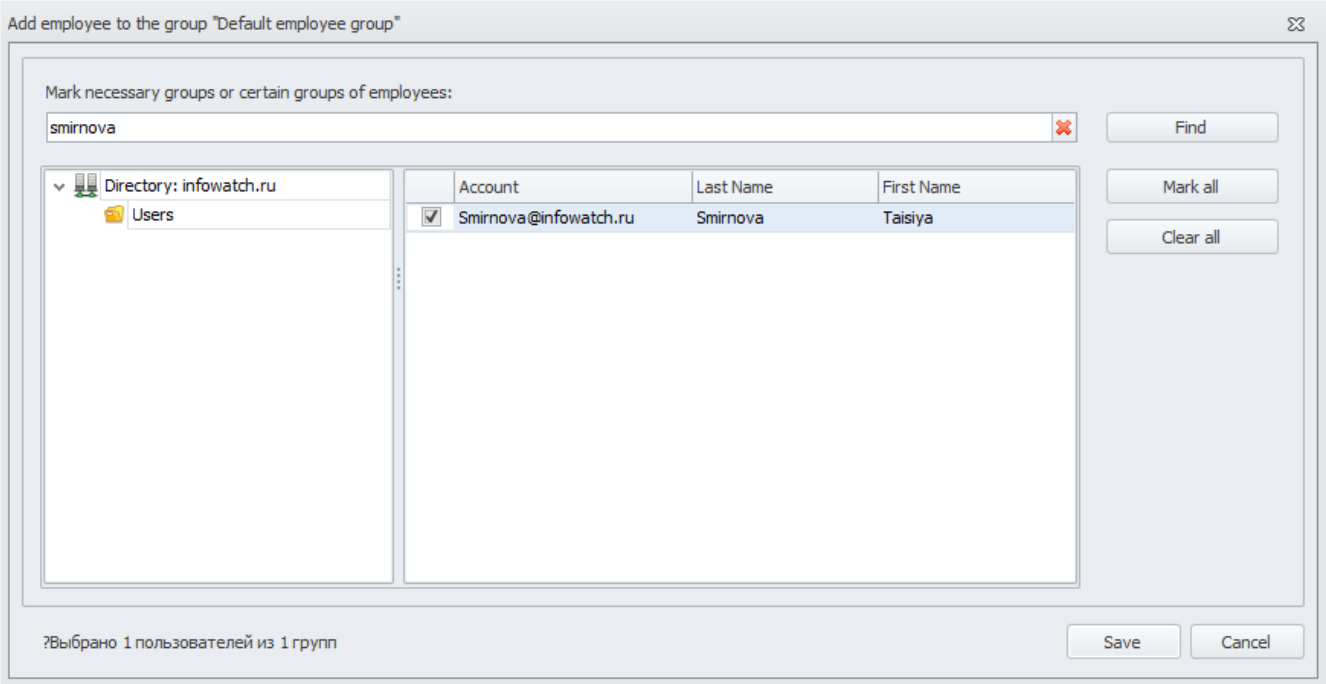
This adds an account to the selected group.

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 (DM) of a group where the employee is added to.

To add one or several accounts to employee group:

1. Go to **Employees** section.
2. In **Employees** area of Navigation pane select a group which you want to add employee's account to.
3. Take one of the following steps:
   - in the Main Menu, click **Edit > Add Employee**;
   - click **Add Employee** at the top of **Employees** area;
   - right-click in Employees area and select **Add Employee** from the drop-down list;

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



4. To add an employee, in left pane select a node in groups tree, then flag accounts you want to add to edited group.
   To flag all accounts of selected node, click **Mark all**. To clear selection, click **Clear all**.
   You can also make a search of account by all available elements: enter a part of account name to the field at the top and click **Find**.
5. After you selected all needed accounts, click **Save** to close **Add employee to the group** dialog and return to a dialog box with group parameters.
6. Click **Save**.

Warning!

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

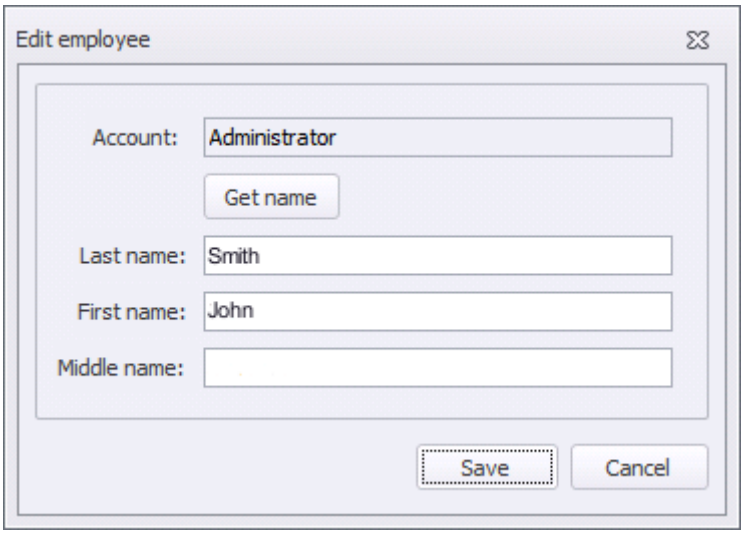
4.3.3.6 Editing Employee Account

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

To edit an employee account:

1. Go to **Employees** section.
2. In **Employees** area of Navigation pane select the group the account belongs to.
3. Select the row that contains the name of the account you want to edit.
4. Take one of the following steps:
   - in the Main Menu, click **Edit > Edit Employee**;

- click **Edit Employee** at the top of **Employees** area;
- double-click the selected row.



5. In the **Edit employee** dialog window you can modify the following optional parameters: **Last Name**, **First Name** and **Middle Name**. You can either enter new values into appropriate fields manually or import them from directory service with **Get name** button.
6. Click **Save**.

Warning!

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

4.3.3.7 Removing Employee Account from Employee Group

To remove an account from employee group:

1. Go to **Employees** section.
2. In **Employees** area of Navigation pane select employee group the account belongs to.
3. Select the row that contains the name of the account you want to remove from this group.

Note:

To remove multiple accounts from a group, select the rows with employee's accounts you want to exclude from this group.

4. Take one of the following steps:
   - In the Main Menu, click **Edit > Remove** employee from group;
   - click **Remove employee** from group at the top of **Employees** area;

- press **Delete** keyboard button.

This removes employee account from selected employee group.

> **Note:**
>
> If employee account belongs to a single employee group, then after excluding it will be automatically added to default employee group.

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

4.3.3.8 Deleting Employee Account from Security Schema

To remove employee account from security schema:

1. Go to **Employees** section.
2. In **Employees** area of Navigation pane select employee group the account belongs to.
3. Select the row that contains the account you want to remove.

> **Note:**
>
> To remove multiple accounts from security schema, select all the rows that contain the accounts you want to remove.

4. Take one of the following steps:
   - In the Main Menu, click **Edit > Delete employee from security schema**;
   - click  **Delete employee from security schema** at the top of **Employees** area;
   - press **Shift+Delete** at the keyboard.
5. In the confirmation box click **Yes** to confirm that you want to remove the account.

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

4.3.4 Computers

InfoWatch Device Monitor workstation is a managed workstation - computer where InfoWatch Device Monitor. Client is installed.
General principles of managing workstations are described in "Computers and Computer Groups" section. Actual security policies (DM) can be applied only to a workstation group. You can define a security policy (DM) for a certain workstation by including it to various workstation groups.

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

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

For more information on managed workstations see:

- Viewing Computer Details;
- Viewing Computer Effective Policy;
- Adding and Editing a Computer Group;
- Deleting Computer Group;
- Adding Computer to a Group;
- Removing Computer from a Group;
- Deleting Computer from Security Schema;
- Updating Clients at Managed Computers;
- Diagnostics.

On the procedure of Clients for mobile devices installation and installation, see "Mobile devices".

4.3.4.1 Viewing Computer Details

In **Computers** area of Navigation pane displays a list of computer groups. Main screen workspace displays the list of computers in selected computers group.

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

To view the list of computers that belong to a separate group, on the panel **Computers** choose the name of the required group:

list of computers, included in group, will be displayed in the working area.

To view a full list of registered workstations, click  **Show All Computers** at the top of Navigation pane.

Computer information is displayed in tabular list. Each row in the list contains a computer (row starts with) or a mobile device (row starts with) . Columns contain basic computer properties.

Tabular list contains the following basic information:

- **Name.** Domain name of computer.
- **Status**. Managed computer and Client status. This parameter may have the following values:
  - **Works properly**. Managed computer is enabled, Client is running.
  - **Inactive**. Managed computer is disabled or unavailable for a long time. The same status is displayed, if the Client is uninstalled from the managed computer.
- **Installed**. Date and time of computer Client's first access to the server.
- **Established**. Date and time of Client launch on computer.
- **Accessed**. Date and time of computer Client's last access to the Server.
- **Schema version**. Client's current security schema version number.
- **Client version**. Client version number.
- **Operation system**. Operation system version.
- **Comment.** Field to type in comment.
- **IP address**. IP address of computer.
- **User.** Last user account logged-in computer.

Extended information on each workstation is available in **Details** panel.

To view properties of a separate computer, choose row with the description of the required computer in working srea of the main window..

Details panel will display table of properties with the following workstation data:

- **Type.** Type of computer - displayed only for stationary or mobile computers.
- **Model name**. Model of mobile device - disaplayed for mobilr devices only.
- **Settings**. Common security policy (DM) settings version number (see "General System Settings").
- **Version of network control settings**. Data transmission through network connections with the help of Network Monitor control version (see "Settings of Corporate Network").
- **Configuration version of network applications control**. Version of network traffic control configuration, using protocols YMSG,XMPP, MMP, FTP, FTPS, SMTP/MAPI/POP3, HTTPS (see "Settings of Corporate Network").
- **Configuration version of excluded applications control**. Version number of application exclusion settings (see "Exclusion of Application from Interception"). In brackets the last application version number is specified.
- **Free disk space on computers**. Free space size on disks, where shadow copies are saved (i.e in percentages) and the minimum allowable size of this space.

Warning!

If there is at least one valid rule (DM) that allows shadow copying, and there is less free space on the host drive than specified by the policy (DM) (see "Creating Shadow Copies and Blocking Operations Due to Free Space Shortage"), no data will be printed or written to removable media:

even if these steps aren't covered by any rule (DM).

Note:

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

Each registered workstation is automatically added to "default" workstation group. At the same time, "default" workstation group security policy (DM) is assigned to the new workstation.
You can do the following as you work:

- manage computer groups:
  - add computer groups;
  - edit computer group parameters;
  - delete workstation groups.
- manage computers:
  - add computers' information to computer groups and thus define computer security policy;
  - remove computers from workstation group;
  - delete computer from security schema;
  - update Clients at managed computers.

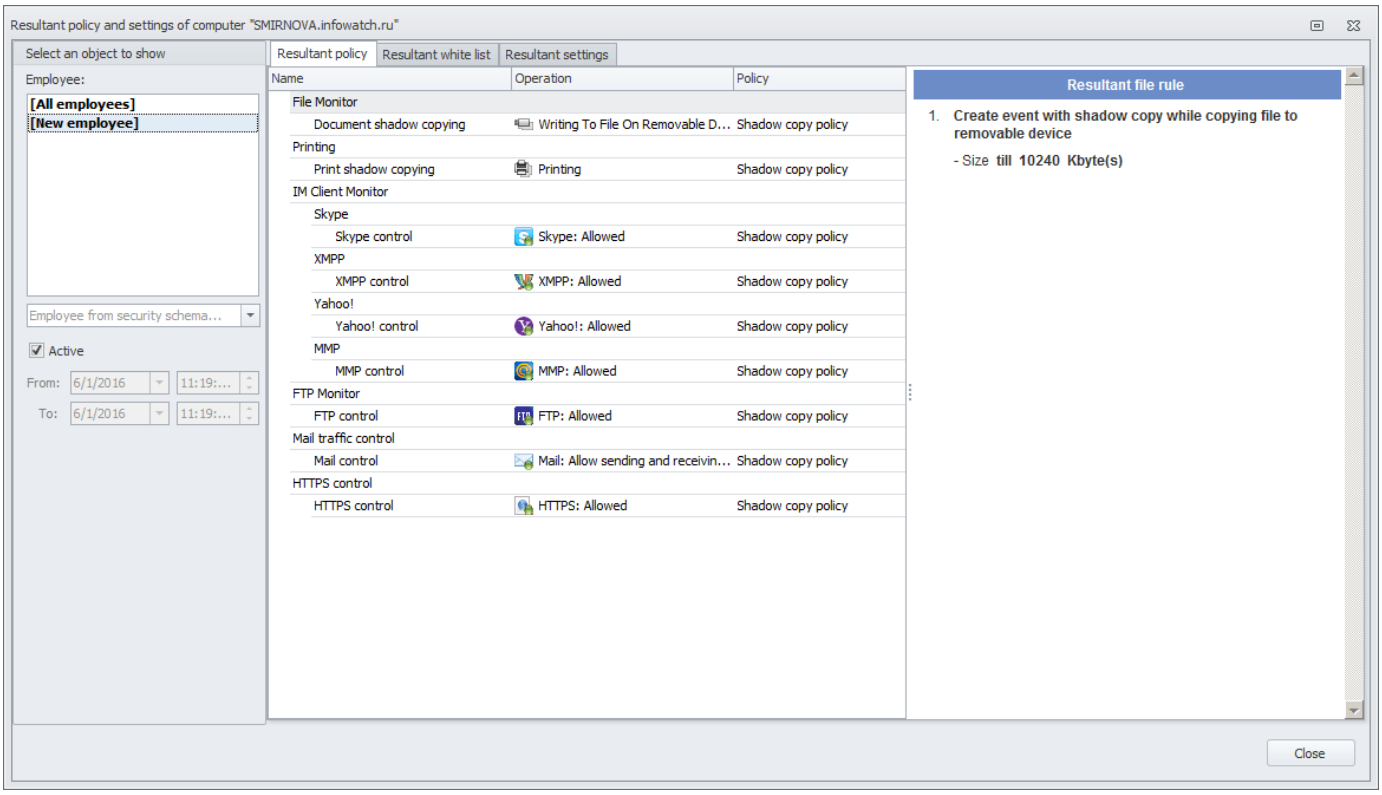
For more information on installing and deliting Clients for mobile devices see "Mobile devices".

4.3.4.2 Viewing Resultant Policy (DM) and Resultant White List for Computer

To view information about policy for computer:

1. In the **Computers** list, choose the required one:
2. Proceed with one of the following actions:
   - in the Main Menu choose **Edit -> Show settings and resultunt policy**.
   - on **Computers** pane click **Show settings and resultunt policy**.

As a result, a window **Show settings and resultunt policy <computer name>** will be displayed**:** where by default all resulting policies (DM) for all employees on the chosen computer are displayed.



The main window **Resulting policy for employee<computer name>** area contains three tabs:

- **Resultant policy** - rules (DM) are displayed, that are resulting on a computer. Resulting policy (DM) folds from rules (DM), configured by default, rules (DM), applied for this computer and rules (DM) for computer's users (see "Device Monitor Rules (DM) Application"). To see detailed information about a rule (DM), select it from the list: detailed information will be displayed on the panel on the right.
- **Resultant white list** - displays devices, which are allowed for computer (see "White lists"). To see detailed information about device, select it from the list: detailed information will be displayed on the panel on the right.
- **Resultunt settings** - settings of Sending data to the client speed and Control disk space on client, which are resultant on computer, are displayed. Resultant settings consist of default settings and settings for computer group, which includes the selected computer. (see "Common Settings for Clients" and "Adding and Editing an Employee Group").

On a **Employee** pane you can choose object for review:

- **All Employees** - when chosen, resulting policy\white list\settings for all employees are displayed, regardless of who is logged on the selected computer.
- **New Employee** - when chosen, resulting policy\white list\settings for all employees are displayed for new employee (which is not yet registered in security scheme).
- To view resulting policy\white list\settings for a definite user:
    - Choose account name, registered on chosen computer from **Employee** list

  or

- From **Employee** drop-down list in security schema choose any account, which is registered in the System (see "Employees").

You can, as well, choose period for resultant policy/white list/settings to be displayed:

- tick **Active** box, to view current resultant policy/white list/settings for an employee;
- untick **Active** box, to view resultant policy/white list/settings for a definite period.

4.3.4.3 Adding and Editing a Computer Group

Important!

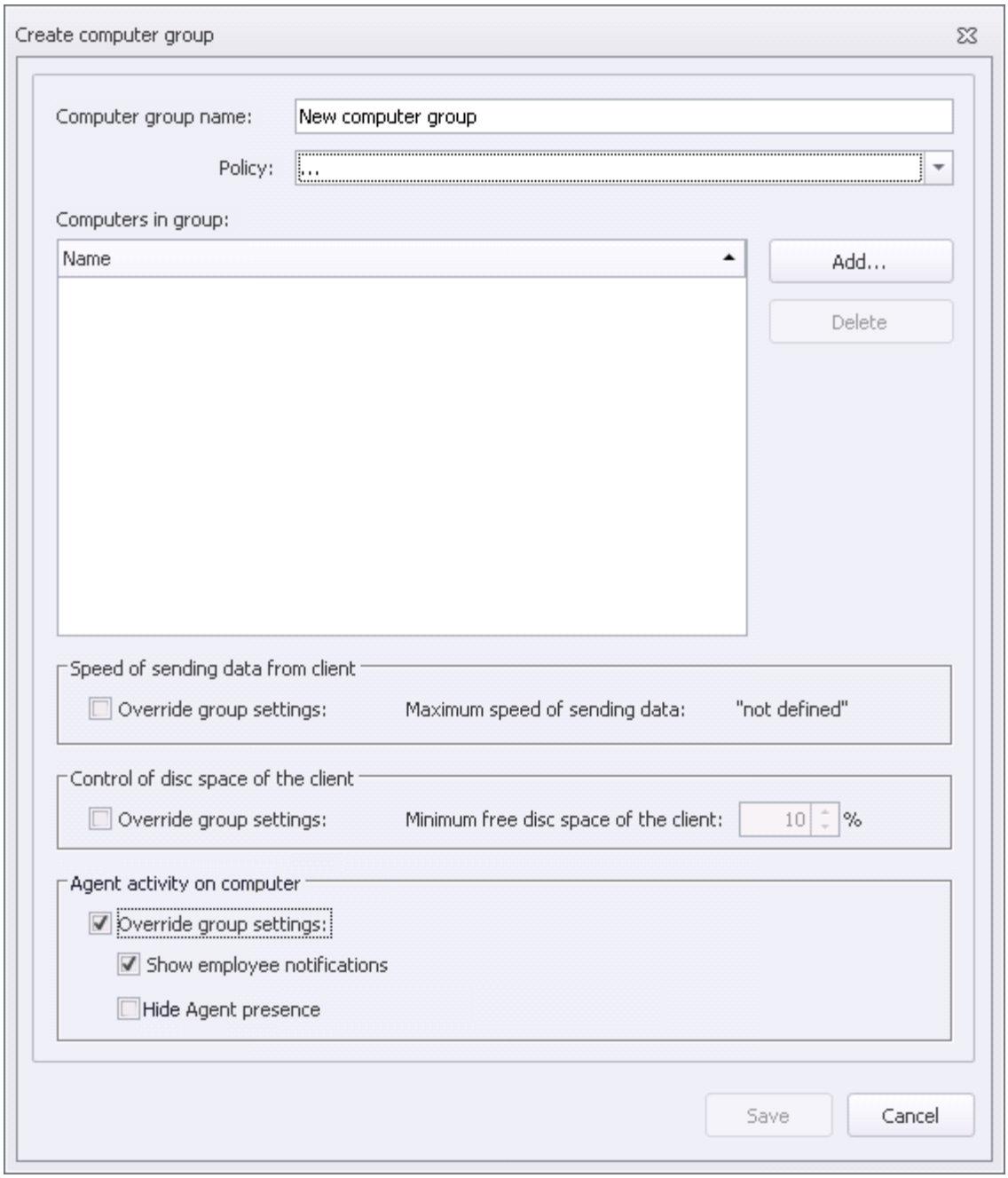
When you register a new computer, information on this computer is automatically added to the security scheme (to the "default" computer group).

To create computer group:

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

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

This opens a dialog box with group parameters.



3. In this dialog, specify the following parameters:
   - **Workstation group name**.
   - **Policy (DM)**. From the drop-down list select security policy (DM) that will be assigned to this computer group.
4. Define a list of computers in a group:
   - To add one or several computers click **Add**. In the opened **Add computer to the group** dialog you can
     select computers from:
     - directory service (for example, Active Directory);
     - Microsoft Windows Network;

- ones registered in System previously (for example, after manual Device Monitor Client installation) and already belonging to other Device Monitor groups.

Select a node from a tree in left panel then flag computers which you want to add to the group. You can also make a search of a computer in the directory. For this end enter a part or a computer name to the upper field and click **Find**.
When all needed computers are selected click **Save**: this closes the add window and returns you to configuring group settings.

- To delete a computer from the list select it and click **Delete**.

5. You can set particular speed of sending data from the Clients for computers belonging to the group (configuring of a common value is described in "Common Settings for Clients", **Limit the speed of sending data** setting). To do this:
   a. in the **Speed of sending data from client** area select **Override group settings**;
   b. in the **Maximum speed of sending data** field, specify the needed value, Kbps.

   The setting is not selected by default.
6. You can set particular volume of a minimum free disk space (when it is reached on the managed computer, shadow copies would not be created) for computers belonging to the group (the configuring of a common value is described in "Common Settings for Clients", **Minimum free disc space of the client** setting). To do this:
   a. in the **Control of disk space of the client** area select **Override group settings**;
   b. in the **Minimum free disc space** of the client field, specify the needed value, percent.

   The setting is not selected by default.
7. You can set a particular mode of Client hiding for computers belonging to the group (the configuring of a common value is described in "Common Settings for Clients", **Agent activity on computer** setting group).
   To do this:
   a. in the **Agent activity on computer** area select **Override group settings**;
   b. select or deselect **Show employee notifications** and **Hide Agent presence** settings.

   The setting is not selected by default.
8. Click **Save**.

Warning!

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

4.3.4.4 Deleting Computer Group

To edit or delete computer group:

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

> **Warning!**
>
> The group you are deleting may contain computers that don't belong to any other group. If you delete
> the only group these computers belong to, they will be automatically added to "default" group

5. Click **OK**.

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

4.3.4.5 Adding Computer to a Group

When installing InfoWatch Device Monitor Client (see document "Traffic Monitor. Installation guide" article InfoWatch Device Monitor Client Setup"), computer is added to "default" computer group. All computers inside "default" group will be affected by security policy (DM) assigned to this group. Further on, you can assign security policies (DM) by assign a computer to various computer groups.

To move a computer from one computer group to another:

1. Go to **Computers**.
2. In **Computers** area of Navigation pane, select computer group that contains the computer.
3. Select a row that contains the computer you want to add to another group. Click and hold the selected row
   and drag the computer to **Computers** area of Navigation pane. Move the pointer over the name of computer group you want to add the computer to. When a yellow arrow appears to the left of the selected group name, release the mouse button.
   This adds computer to selected computer group.

You can also add information about computers without InfoWatch Device Monitor Client manually. Computer
information is imported from directory service (connection configuring settings see in "Connecting to LDAP Server")
or your network environment. Then after InfoWatch Device Monitor installation this computer (see "Creating Primary
Distribution Task") will be affected by the policy (DM) of the group it was added to.
The mobile devices do not allow this option.

Warning!

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

To add computer to a group:

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

   In the opened dialog you can select computers:
   - imported from directory service (for example Active Directory);
   - received from Microsoft Windows Network;
   - among previously registered in the System.
4. Flag computers or computer groups. Minimized groups are marked with an icon ; expanded - . Doubleclick
   a group, to expand or collapse it.

   Warning!

   By marking a group you select the computers that are included in that particular group. Subgroups and
   subgroup computers of selected group are not selected: you have to select them separately.

   You can also specify computer name in the line at the bottom of dialog box. When listing names, separate
   them with semicolons.
5. Click **OK**.

This closes **Select computer** dialog and adds the information on selected computers to computer group.

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

4.3.4.6 Removing Computer from a Group

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

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

To exclude computer from computer group:

1. Go to **Computers**.
2. In **Computers** area of Navigation pane, select computer group that contains the computer. This displays a
   full list of computers that belong to selected group.
3. Select a row that contains the computer you want to remove from computer group.
4. Take one of the following steps:
   - in the main menu select **Edit > Remove Computer From Group**;
   - click  **Remove Computer From Group** located at the top of Computers area;
   - press **Delete** keyboard button.

This removes computer from the group.

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

4.3.4.7 Deleting Computer from Security Schema

You can remove a computer from the list of registered computers (for example, computer discontinued operation).

Computer information will not be deleted, but it will be marked as **Inactive** due to Client deactivation. If you don't want to save inactive computer information, you can delete its record.

To remove computer from security schema:

1. Go to **Computers**.
2. In **Computers** area of Navigation pane, select computer group that contains the computer.
3. In the Main screen workspace, select the row that contains the inactive computer you want to remove.
4. Take one of the following steps:
   - in the Main Menu, click **Edit** > **Delete Computer From Security Schema**;
   - click **Delete Computer From Security Schema** located at the top of **Computers** area;
   - right-click computer row and select **Delete Computer From Security Schema**;
   - press **Shift+Delete** at the keyboard.
5. In the following confirmation dialog select **Yes** to confirm that you want to remove the computer.

This removes computer information from all groups the computer was assigned to.

Warning!

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

4.3.4.8 Updating Clients at Managed Computers

Device Monitor Clients at managed computers can be simply updated by the task (see task details in "Clients
Remote Installation, Updating and Uninstallation" and "Creating Updating Task").

To update Device Monitor Clients at all managed computers of the group:

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

To update Device Monitor Clients at selected managed computers:

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

This creates and runs the update task for selected computers.

4.3.4.9 Diagnostics of the Workstation

The System allows you to remotely collect diagnostic data from workstations.

> **Warning!**
>
> It is only possible to collect diagnostic data for workstations: for mobile devices, this feature is unavailable.

To start collecting diagnostic data on the computer:

1. Go to **Computers** section.
2. In **Computers** area of the Navigation pane, select the group which includes the required workstation.
3. In the computer list, right-click the desired workstation and select **Diagnostics > Enabling diagnostic mode**.

To stop diagnostic data collection on the computer:

1. Go to **Computers** section.
2. In **Computers** area of Navigation pane, select the group which includes the required workstation.
3. In the computer list, right-click the desired workstation and select **Diagnostics > Disabling diagnostic mode**.

To get the archive that contains all provided diagnostic data:

1. Go to **Computers** section.
2. In **Computers** area of Navigation pane, select the group which includes the required workstation.
3. In the computer list, right-click the desired workstation row and select **Diagnostics > Gathering diagnostic data**.
4. In the **Select path to save archive with diagnostic data** dialog, specify the folder and the archive name.
5. In the notification window that opens, click **OK**.

4.3.5 Mobile Devices

Besides workstations, InfoWatch Device Monitor allows you to control employees' mobile devices (smartphones
and tablet PCs).
InfoWatch Device Monitor Client can work with the following models of mobile devices, Android OS versions and
build numbers:

Device model	Android version	Build number
ASUS Nexus 7 2013 LTE (K009)	4.3.0	JLS36C
	4.4.2	KOT49H
	4.4.3	KTU84L

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

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

Warning!

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

The System can associate several mobile devices with one employee, but a single mobile device can be associated with one employee only.

Warning!

To manage a mobile device entry and to install or uninstall InfoWatch Device Monitor Client, the following
requirements should be met:

- USB Debugging mode must enabled on the mobile device and all required drivers should be installed (for devices on Android platform only);
- the Management Console (DM) should run on a physical workstation (using virtual machines or remote desktop connections is not recommended; Microsoft Windows XP is not supported);
- the mobile device directly must be connected via USBe to the computer where the Management Console (DM) is running.

See details in "Preparing a Mobile Device on Android Platform" and "Preparing a Mobile Device on iOS
Platform".

Guidelines on Clients installation and uninstallation for mobile devices are available in:

- Preparing a Mobile Device on Android Platform;
- Preparing a Mobile Device on iOS Platform;
- Adding a Mobile Device to Computer Group;
- Adding a Mobile Device through Appointment to Employee;
- Deleting the Mobile Device.

4.3.5.1 Preparing a Mobile Device on Android Platform

If you are using a mobile device on Android platform, then to install, update or delete InfoWatch Device Monitor
Client, you should:

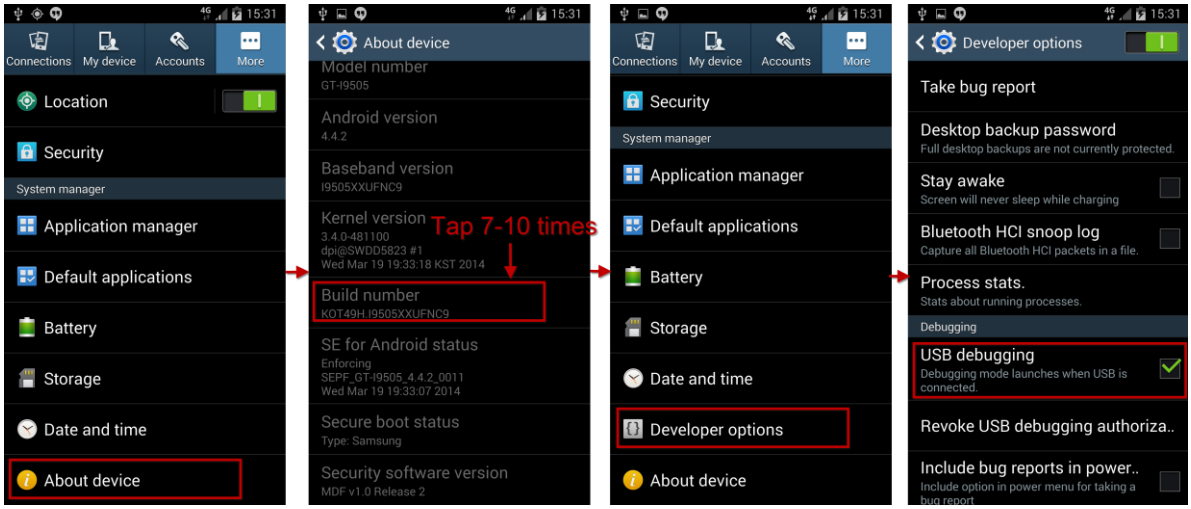
1. Enable "**USB debugging**" mode on the device: see example below.
2. Via a USB-wire connect this device to the computer where Device Monitor Management Console is running.
3. If necessary (for example, for some builds of Samsung), install additional drivers.

4.3.5.1.1 Step 1. Enabling "USB debugging" mode

The process of enabling the "USB debugging" mode can slightly vary for different models of mobile devices, different versions of OS and firmware.

Enabling the debugging mode for Samsung Galaxy S4 with Android 4.4.2:

1. Enable developer mode: **Settings -> About device -> Build number**; tap the build number several times (7
   - 10).
2. Then the notification will be displayed like "*You are now 3 steps away from being a developer*."



3. Continue tapping till successful mode enabling.
4. Return to **Settings** menu. Select **Developer options** appeared near About device.
5. Select **USB debugging**.

You can disable the debugging mode when the installation, updating or deleting the InfoWatch Device Monitor
Client is successfully completed.

Huawei feature:
The Huawei models can automatically disable USB debugging mode if the connection with the computer is lost.
Therefore the debugging mode should be enabled every time after connecting to the the computer.

4.3.5.1.2 Step 2. Connecting to the computer

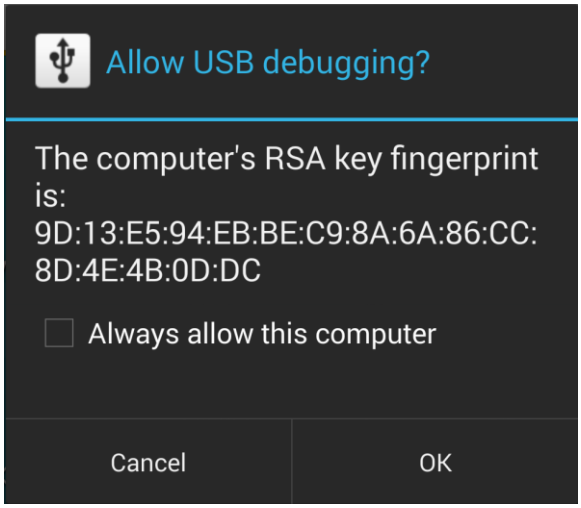
To install or update the InfoWatch Device Monitor Client, you should connect the mobile device to the physical
workstation where Device Monitor Management Console is running, via the USB-wire.

> **Warning!**
>
> If you are using a virtual machine or connection to a remote desktop, then the installation can fail due to
> increasing of the System response time. Therefore, we recommend that you should not use virtual machines or remote desktops.
> The System does not support installation of Device Monitor Client to mobile devices if the Management
> Console (DM) is running on a computer with Microsoft Windows XP. Therefore, we do not recommend using
> Microsoft Windows XP either.

You can see if the connection was successful and control the further installation of drivers in Device Manager (**Control Panel -> Hardware and Sound -> Device Manager**).

Samsung feature:
If the phone is "clear" - for example the build is just updated, - then you can need to perform additional actions:

1. On the phone slide down the notification panel.
2. Switch the device from the "**Multimedia**" connection mode to the "**Camera**" mode.
3. Allow the USB debugging on the appeared query.



4.3.5.1.3 Step 3. Drivers installation

In a first connecting of the mobile device to the computer where the Device Monitor server is working the automatic
installation of the following drivers is performed:

- a driver for operation in a normal mode
- the **libusb** driver for operation in the downloaded mode

During installation of the drivers, the icon on the Device Monitor server's computer taskbar displays the process of
drivers searching and installation.

> **Warning!**
>
> Do not disconnect the mobile device during drivers installation! Wait for installation completion.

When installation of a driver is completed successfully, the computer will display a notification that this driver is
ready to use. In case of some errors in drivers installation, you can find solutions in InfoWatch Knowledge base: "Mobile Device
Driver Cannot Run Automatic Installation" or "Installing the Driver for Downloaded Mode" (libusb0)" for example.

4.3.5.2 Preparing a Mobile Device on iOS Platform

If you are using a mobile device on iOS platform, then to install, update or delete InfoWatch Device Monitor Client,
you should:

1. Jailbreak your mobile device (iPhone or iPad).
2. On the computer where Device Monitor Management Console is installed, install iTunes.
3. Connect the mobile device to the computer, where Device Monitor Management Console is installed, via a
   USB-wire.
4. Authorize the mobile device on the computer.

4.3.5.2.1 Step 1. Jailbreaking the mobile device

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

Note:

The supported versions of iPhone and iPad are 8.0 - 9.0.2.

4.3.5.2.2 Step 2. Installing iTunes

To install InfoWatch Device Monitor Client on a mobile device, it is necessary that Apple Mobile Device Support
application should be installed on the computer (it is installed together with iTunes).

4.3.5.2.3 Step 3. Connecting to the computer

To install or update InfoWatch Device Monitor Client, you should connect the mobile device to the physical
workstation where Device Monitor Management Console is running, via the USB-wire.

Warning!

If you are using a virtual machine or connection to a remote desktop, then the installation can fail due to
increasing of the System response time. Therefore, we recommend that you should not use virtual machines or remote desktops.
The System does not support installation of Device Monitor Client to mobile devices if the Management
Console (DM) is running on a computer with Microsoft Windows XP. Therefore, we do not recommend using
Microsoft Windows XP either.

You can see, if the connection was successful, and control the further installation of drivers in Device Manager (**Control Panel -> Hardware and Sound -> Device Manager**).

4.3.5.2.4 Step 4. Authorizing the device on the computer

Once you have connected the device to your computer, you should authorize the device on this computer. For this:

1. Run iTunes on the computer.
2. In the message that appears on the device, confirm that this computer can be trusted.
3. On the computer, in the iTunes menu bar, select **Store -> Authorize this computer**.

4.3.5.3 Adding a Mobile Device to Computer Group

Mobile devices can be added to the security schema from the computer group with specifying the employee earlier created in the System or added from LDAP.

Warning!

To manage the mobile device account and to install or delete InfoWatch Device Monitor Client, the following settings are required:

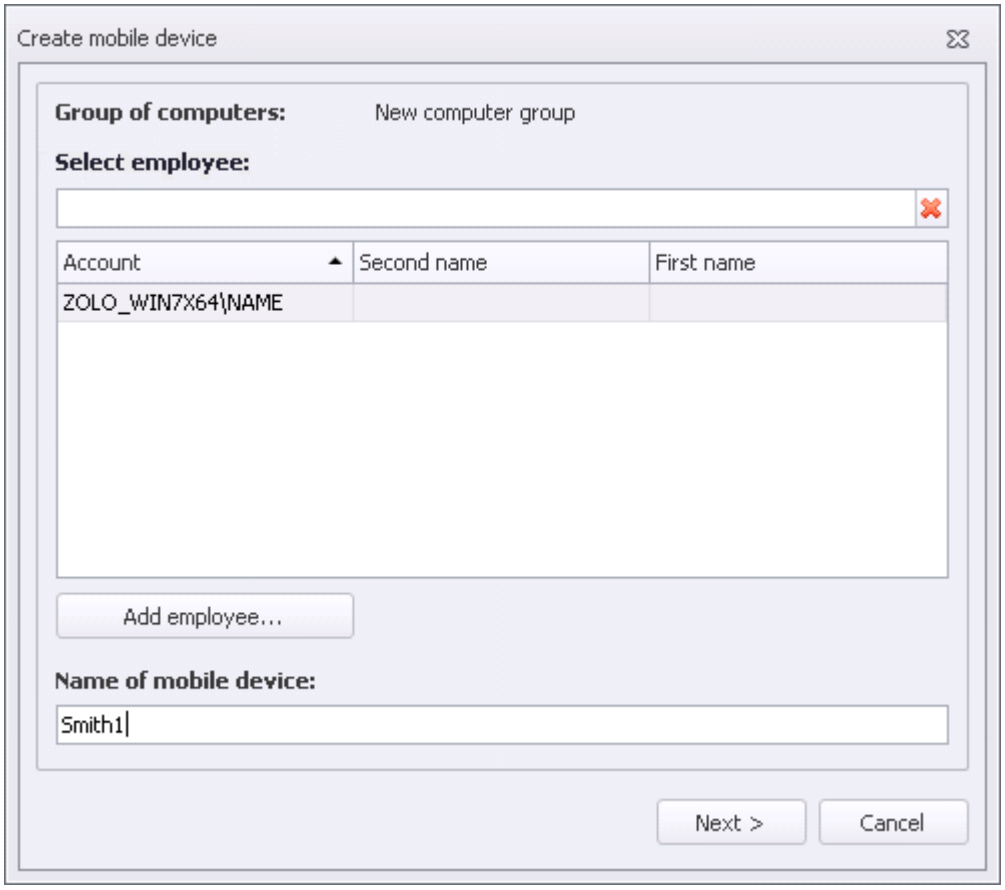
- USB Debugging or similar mode should be enabled on the mobile device and all required drivers should be installed (for devices on Android platform only);
- the Management Console (DM) should be running on a physical workstation (using virtual machines or remote desktop connections is not recommended; using Microsoft Windows XP is not supported);
- the mobile device should be directly connected via USB wire to the computer where the Management Console (DM) is running.

Details see in "Preparing a Mobile Device" and "Preparing a Mobile Device on iOS Platform".

To add a mobile device to the computers group and install the InfoWatch Device Monitor Client to it:

1. Go to the **Computers** section.
2. In the **Computers** area of Navigation pane, select the name of the group to which you want to add a mobile device.
3. Do either of the following:
   - in the main menu, select **Edit > Create mobile device**;
   - click  **Create mobile device** button located in the upper part of the **Computers** area;
   - right-click the workspace and select  **Create mobile device** from the shortcut menu.

This opens a dialog box for creating a mobile device.



4. In the list of employees, select the required account.
   You can also start typing the account name in the entry field: the list will be filtered.
   If there is no needed account in the list, you can add it: click **Add employee**. On adding accounts, see "Adding Employee Account to a Group".
5. If necessary, change the entry name for the mobile device that was automatically created by the System.
6. Click **Next**.
7. In the installation wizard dialog box that opens, select the connected mobile device.
8. Click **Install**.
9. When the installation is complete, click **Finish**.

This will install InfoWatch Device Monitor Client to the mobile device and add the entry of the new mobile device to the selected computer group of the security scheme. The new mobile device will be associated with the selected employee.

Warning!

Once the Client is installed on the mobile device, a policy (DM) that is assigned to a default computer group will be deployed to this device. The policy (DM) assigned to the specified policy will be deployed on the mobile device after you save the security scheme.
On how to save the security scheme, see "Editing Security Scheme".

4.3.5.4 Adding a Mobile Device through Appointment to Employee

Mobile devices can be added to the security schema from the entry of the employee which you want to assign this
mobile device.

Warning!

To install InfoWatch Device Monitor Client, there should be:

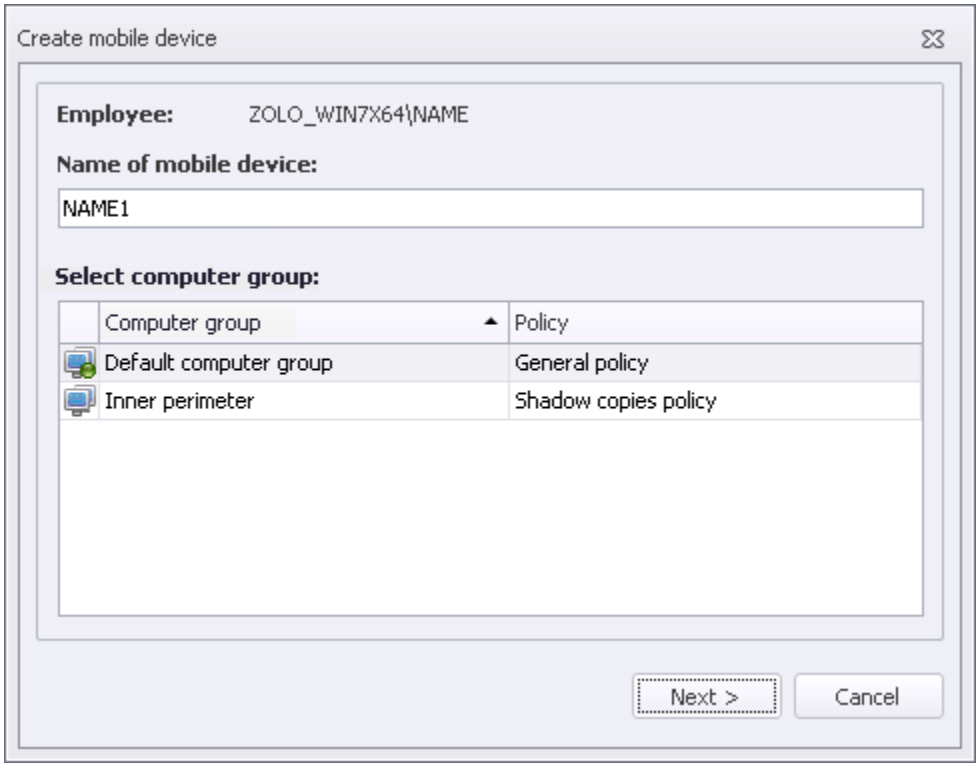
- USB Debugging mode enabled on the mobile device and all required drivers installed (for devices on Android platform only);
- the Management Console (DM) running on the physical workstation (using virtual machines or remote desktop connections is not recommended; using of the Microsoft Windows XP is not supported);
- mobile device directly connected via USB wire to the computer where the Management Console (DM) is running.

Details see in "Preparing a Mobile Device" and "Preparing a Mobile Device on iOS Platform".

**To add a mobile device to the security schema through the employees group and install the InfoWatch
Device Monitor Client to this device**:

1. Go to the **Employees** section.
2. In the **Employees groups** area on the Navigation pane select the group which contains the needed employee.
3. Select the employee list which you want to assign a mobile device to.
4. Take one of the following steps:
   - in the main menu select **Edit > Create mobile device**;
   - click **Create mobile device** button located in the upper part of the **Employees** area;
   - right-click on the workspace and select **Create mobile device** from the context menu.

This will display the dialog of creating the mobile device.



5. If needed, change the name of the mobile device entry.
6. Select the needed computer group from the list.
7. Click **Next**.
8. In the opened installation dialog window select the connected mobile device.
9. Click **Install**.
10. When the installation is completed, click **Finish**.

This will install the InfoWatch Device Monitor Client to the mobile device and add the entry of the new mobile device
to the selected computer group of the security schema. The new mobile device will bó associated with the selected
employee.

Warning!

Just after the Client installed to the mobile device, this device will have a policy (DM) appointed to the default
computer group, and only when the security schema will be saved, the device will have a policy (DM) appointed to
the computer group specified on mobile device adding.
Information on saving the security schema see in "Editing Security Scheme".

4.3.5.5 Deleting the Mobile Device

The removing the mobile device from the security schema without uninstalling the InfoWatch Device Monitor Client
is performed in the way common for all the computers: see "Deleting Computer from Security Schema". For this
action no device connection is needed.

Warning!

To uninstall InfoWatch Device Monitor Client, there should be:

- USB Debugging mode enabled on the mobile device and all required drivers installed (for devices on Android platform only);
- the Management Console (DM) running on the physical workstation (using virtual machines or remote desktop connections is not recommended; using of the Microsoft Windows XP is not supported);
- mobile device directly connected via USB wire to the computer where the Management Console (DM) is running.

Details see in "Preparing a Mobile Device" and "Preparing a Mobile Device on iOS Platform".

**To delete the mobile device from the security schema and uninstall the InfoWatch Device Monitor Client
from this mobile device**:

1. In the main menu select **Tools > Delete mobile device**.
2. In the opened installation dialog window select the connected mobile device.
3. Click **Uninstall**.
4. When the uninstallation is completed, click **Finish**.

This will uninstall the InfoWatch Device Monitor Client from the mobile device and delete the entry of the new
mobile device from the computer group and security schema.

4.3.6 White Lists

You can manage lists of devices with full access from **White Lists** section. To go to this section, click **White Lists** button at Navigation pane.
For more information on white lists see:

- Viewing White List Details;
- Adding White List;
- Defining Entry Validity Period;
- Editing White List;

- Deleting White List.

You can view an information on acting white lists as described in "Viewing Resultant Policy (DM) and Resultant White List for an employee" and "Viewing Resultant Policy (DM) and Resultant White List for Computer".

4.3.6.1 Viewing White List Details

White Lists area of Navigation pane displays all white lists. Main screen work pane displays devices (models and
instances) in selected white list.

> **Note:**
>
> You can make search in white list index: type the name of the list in the search box below the index on
> Navigation pane.
> You can adjust the displaying of selected white list using additional features (see "Additional Features").

To view information for separate white list,
select white list title in the group.
White lists information is available as a list of devices grouped by their type. Each row in the list contains device
model or instance. Columns contain devices' general properties. Extended information on device properties is
displayed in **Details** panel.

To view detailed information on device properties,
select the row that contains device model or instance name.

Details panel displays properties table including the following information:

- **Device instance or model identifier**. Model code (VID - Vendor ID) or device instance serial number (PID-Product ID).
- **Device description**.
- **Device type**.
- **Category**. Model or instance.
- **Period**. Full access period starting and expiry date and time.
- **Detected on computer**. Name of computer where the device was detected.
- **Added to database at**. Date of device information submission to database (see "Adding Device to Database").

> **Note:**
>
> Some of the properties on **Details** panel are duplicated in the main screen workspace.

4.3.6.2 Adding White List

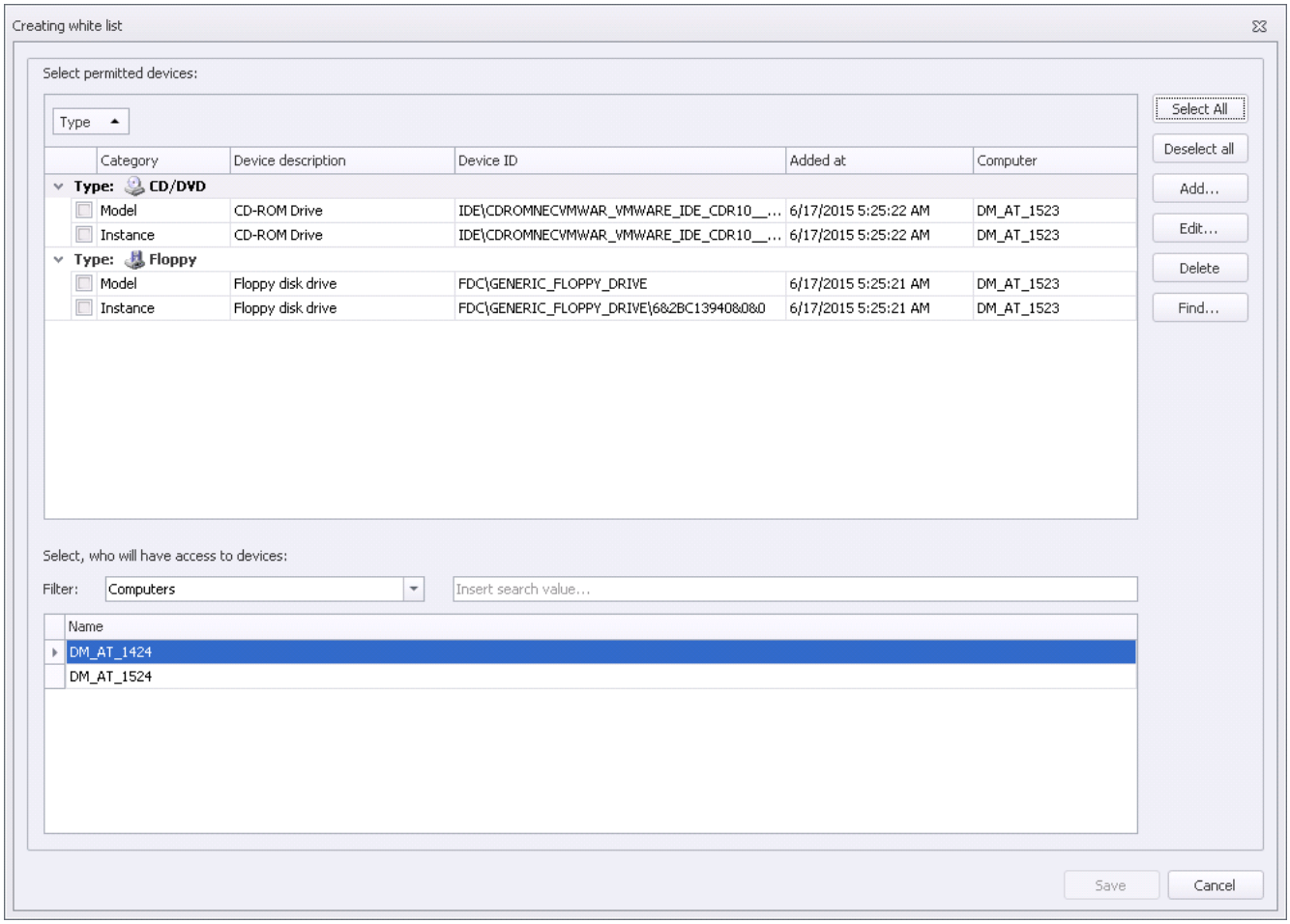
White list affects selected objects: employees, employee groups, computers or computer groups.

> **Warning!**
>
> A single object (employee, employee group, computer or computer group) can have only one white list
> assigned to.

To add white list:

1. Go to **White Lists** section.
2. Take one of the following steps:
   - select **Edit > Create White List** in the Main Menu;
   - click **Create White List** at the top of Navigation pane..

This opens **Creating White List** dialog displaying table containing all devices registered in the System.



3. In the table of devices select models and instances which should have full access to.

> **Warning!**
>
> Information on creating a list of registered device models and instances see in:
> Adding Device Entry;
> Deleting Device Entry.

4. In **Select, who will have access to devices** area select a filter: who will be affected to white list action:
    - employees
    - employee groups
    - computers
    - computer groups

   The list of entries will appear below.
   You can also use a search string by entering a name or its part.
5. Select employee / employee group / computer / computer group that will have full access to selected devices.
6. Click **Save**.

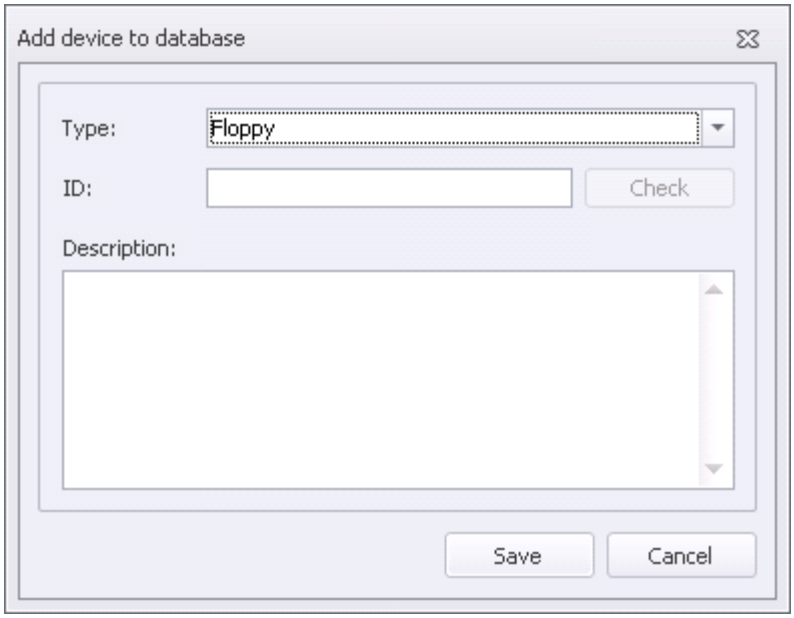
4.3.6.2.1 Adding Device Entry

You can add to white lists only device models and instances which were previously registered in the System.
Device information is added in two ways:

- manually (if device ID is provided)
- via search engine (if device is connected to managed computer).

To add device information manually:

1. Open **Creating White List** dialog box (see "Adding White List").
2. Click **Add** button at the right of the window.
   This opens **Add device into database** dialog box.



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

> **Note:**
>
> To retrieve device instance string, connect the device and use standard Windows tools (for example,
> **Device Manager**) to view its properties. Device instance string is displayed on Information tab.
> Device instance string is displayed as XXX\YYY\ZZZ where XXX is device type (usually, connection
> type, such as USB, IDE or ACPI), YYY is device model string (Vendor ID), and ZZZ is device
> instance string (Product ID).
> Model ID is displayed as XXX\YYY where XXX is device type and YYY is model ID string (VID).

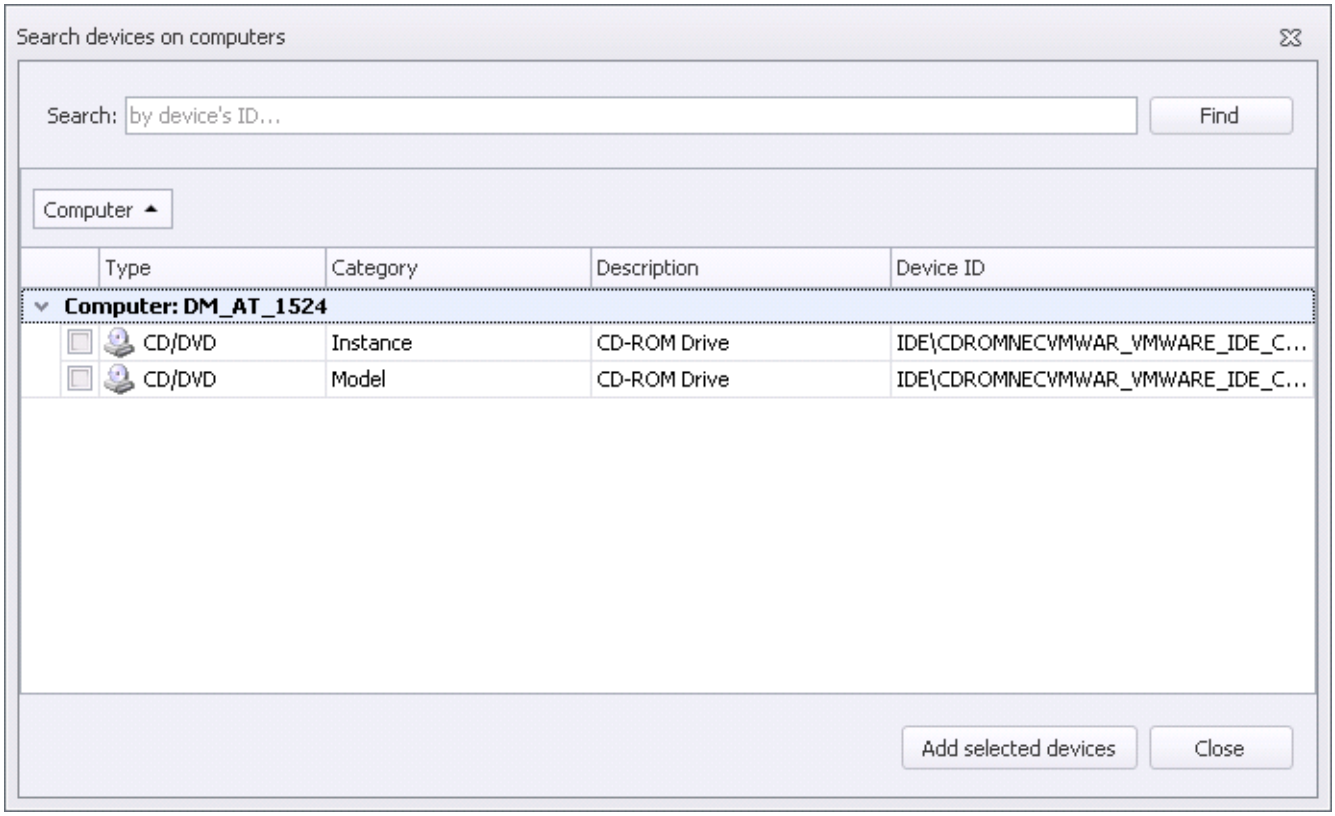
To make sure the ID is valid, click **Check**.

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

   - enter description into **Description** box.
4. Click **Add**.

To add device information via searching devices connected to managed computers:

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



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

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

4.3.6.2.2 Deleting Device Entry

To remove device entry from database:

1. Open **Creating White List** dialog (see "Adding white list").
2. Select and right-click device instance or model in device database table. In the drop-down menu, select **Delete device**.
3. In confirmation dialog click **OK**.

4.3.6.3 Defining Entry Validity Period

Each device instance or model from the white list has an access permission displayed separately. This item's
(permission's) default validity period is practically infinite (from 01.01.1753 to 31.12.9999). You can limit full access
period for this device. This device will be subject to general rules (DM) that apply to this device type before and after the
specified period.

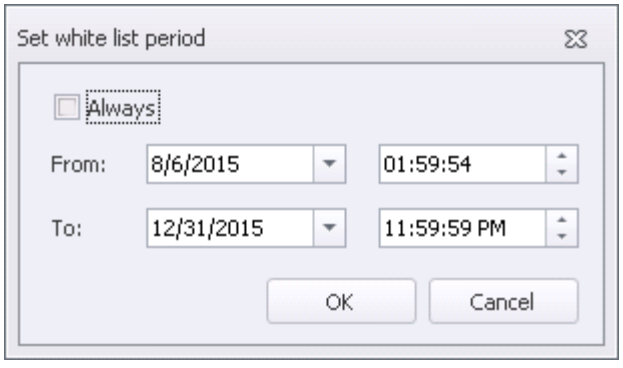
To set white list entry period:

1. Go to **White Lists**.
2. In **White Lists** area of Navigation pane select white list that contains the item.
3. If white list items are grouped in (for example, by the type of devices), expand them (see "Grouping Entries
   ").

> **Note:**
>
> If you set validity period for the entire group, the change will only take effect for the first item of the
> group.

4. Select the row that contains device instance or model you want to assign validity period to and take one of
   the following steps:
   - select **Edit > Edit Item** in the Main Menu;
   - click **Edit Item** at the top of **Permitted devices** area;
   - double-click selected entry name;
   - right-click entry row and select **Edit Item** from drop-down menu.

   This opens **Set white list item period** dialog.



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

4.3.6.4 Editing White List

To edit white list parameters:

1. Go to **White Lists**.
2. In **White Lists** area of Navigation pane select the name of white list.
3. Take one of the following steps:
   - in the Main Menu, click **Edit > Edit**;
   - click **Edit** at the top of Navigation pane;
   - double-click selected white list name.

   These actions open **Edit white list** dialog box. This dialog is similar to **Creating white list** dialog with the exception of **Select, who will have access to devices** area, which is unavailable.
4. You can add or remove devices from database, if needed (see "Adding Device to Database" and "Removing Device from Database"). You can also change the description of previously registered device: to do this select the device in the index and click **Edit** button at the right of the window. In the opened window change the description text and click **Save**.
5. Add or remove flags in device database table to change the catalog of models and instances in the white list.
6. Click **Save**.

Warning!

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

4.3.6.5 Deleting White List

To delete white list:

1. Go to **White Lists** section.
2. Click the white list you want to delete.
3. Take one of the following steps:
   - select **Edit > Delete** in the Main Menu;
   - click **Delete** at the top of Navigation pane..

4. In confirmation box click **Yes** to confirm that you want to remove the white list.

Warning!

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

4.3.7 Signatures

File Monitor rules (DM) can be configured to affect only files of specific structure distinguishing defined file format. To do
this, InfoWatch Device Monitor defines file format basing on its signature.
Signatures section contains a list of signatures which the System can recognize. Signatures are conveniently
grouped into **categories**.

To view available signatures:

1. Go to **Signatures** by clicking the Signatures button in Navigation pane or selecting in Main Menu Go > **Signatures**.
   Signatures area of Navigation pane displays a list of signature categories.
2. Select a signature category from the list.
   Main screen workspace will display a list of all signatures in the selected category.

Warning!

Predefined signature categories cannot be edited or deleted. You can't create new signatures.

You can do the following:

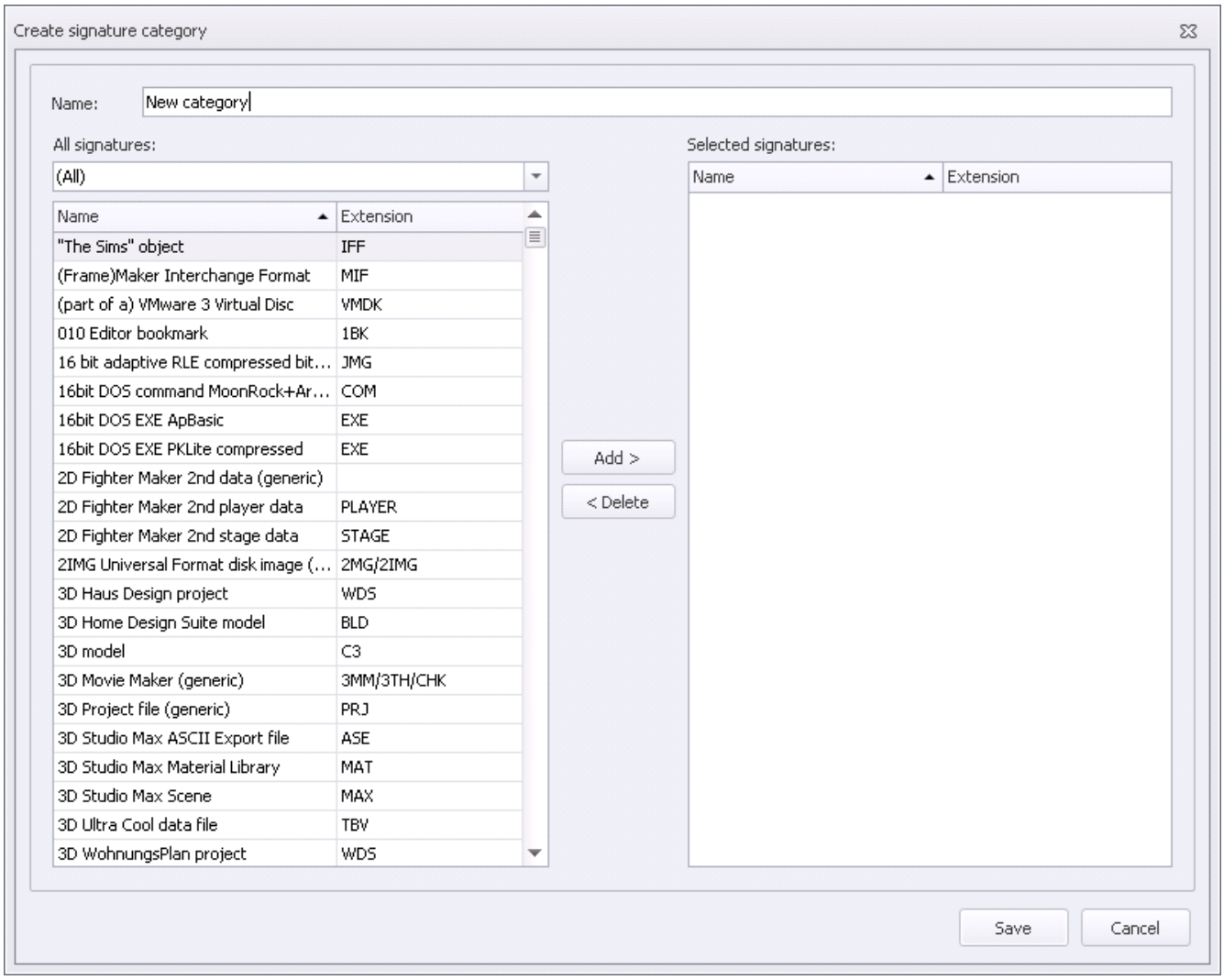
- create signature categories;
- fill created categories by copying predefined signatures;
- delete your signature categories, if they are not used by any rule.

4.3.7.1 Adding Signature Category

To add signature category:

1. Go to **Signatures**.
2. Take one of the following steps:
   - in the main menu select **Edit > Create signature category**;
   - click **Create signature category** at the top of Navigation pane..

Create signature category dialog appears.



3. Enter new category's name..
4. In **All signatures** area you can select one of preset categories from the list. All preset signatures are displayed by default.
5. In the left panel select signatures you want to add to a new category.

   To delete signatures from the list of included to a new category selected them at the right panel **Selected signatures** and click **Delete**.

   To select several signatures hold **Ctrl** or **Shift** button.

   To move selected signatures to a new category click **Add**.

   To delete signatures from the list of included to a new category selected them at the right panel **Selected signature**s and click **Delete**.
6. Click **Save**.

4.3.7.2 Editing Signature Category

After you have created a signature category (see "Adding Signature Category"), you can fill it. For this, do either of the following:

- in the signature category editing dialog (select a category and click **Edit > Edit** in the Main Menu or click **Edit** at the top of Navigation pane, or double-click the selected category name), define the list of signatures as described in "Adding Signature Category".

or

- copy signatures from other categories directly in the Console workspace.

To copy a signature from one category to another:

1. Go to **Signatures** section.
2. In **Signatures** area of the Navigation pane, select the name of a predefined category that contains the signature you want to copy.
3. In the main window workspace, select a row that contains the name of the signature you want to copy. You can select multiple signatures with **Ctrl** or **Shift**.
4. Click and hold the selected row, then drag the pointer to **Signatures** area of Navigation pane. Move the pointer over the category you created earlier where signatures will be added. Release the button when a yellow arrow appears next to the selected category.

As a result, the signature will be copied to the selected category.

To remove a signature from the category, select the signature and do either of the following:

- click **Remove signature from category** at the top of **Signatures** area;
- right-click and select **Remove signature from category** in the drop-down menu;
- press **Delete** key.

4.3.7.3 Deleting Signature Category

Warning!

The following categories cannot be deleted:

- signature categories used by any File Monitor rule (DM)
- predefined signature categories.

To delete a signature category:

1. Go to **Signatures**.
2. Click the signature category name.
3. Take one of the following steps:
    - in the main menu select **Edit > Delete**;
    - click **Delete** at the top of Navigation pane.
4. In the next confirmation dialog select Yes to confirm that you want to remove signature category.

Warning!

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

4.3.8 Application Protocol

After the InfoWatch Device Monitor Client is installed onto the computer (computer or mobile device) and the
computer is rebooted, the System automatically starts to receive data on applications launched on managed
workstations and installed on managed mobile devices.
Data on all launches and installations produces an *application protocol*.

Warning!

Application protocol excludes system vital applications. One can not forbid application which absence is
obstructive for computer properly operation.

Managing the application protocol is performed in the **Applications** section. To go to this section click Applications button located on the Navigation pane or select **Go > Applications** command in the main menu.

The Navigation pane is divided onto two groups in this section: **List of applications** and **Applications Protocol**:

- The **List of applications** group contains lists used to control employee's access to applications:
    - forbid launching applications in one of two modes: white lists and black lists. See details in "Configuring Application Monitor Rule (DM)".
    - forbid screenshots creating. See details in "Configuring ScreenShot Control Monitor Rule (DM)";
    - automatic creating the screenshots by the System (see "Configuring ScreenShot Monitor Rule (DM)".
- The **Applications Protocol** group is intended for creating filters showing data on all applications launched on
managed workstations and installed on managed mobile devices. In this group you can add applications to
lists.

One can find information about working with protocols and application lists in the following articles:

- Creating an application list and adding applications;
- Creating and editing the application protocol filter;
- Adding Application to List Automatically;

- Adding Application to List Manually;
- Exporting Application Protocol.

4.3.8.1 Creating an Application List and Adding Applications

To manage white and black application list, the System offers application lists creation from the **Application protocol** (see "Application protocol").
Lists are used to permit or forbid application usage on computers.

To create an empty application list:

1. Go to **Applications** section..
2. On the Navigation pane set the cursor on the **List of applications** group and take one of the following steps:
   - in **List of applications** group menu click **Create list of applications**;
   - select **Edit > Create list of applications** command in the main menu;
   - right-click in the **List of applications** group and select **Create list of applications** from the dropdown list.
3. In the **List Name** field enter a name for a list you create.
4. Click **Save**.

Details on filling lists and creating lists from application protocols see "Adding Application to List Automatically"

and "Adding Application to List Manually".

To select an application from the list:

1. Go to **Applications** section.
2. Set the cursor on the **List of applications** group.
3. Click in **List of applications** group menu.
4. Select application(s) from list(s) and click **Add applications to the list**.
5. From the drop-down list select **Add applications automatically** or **Add applications manually**.

To edit application in the list:

1. Click button on the **List of applications** group.
2. You can edit details which will be used to filter the application (see "Adding Application to List Manually").

To delete application from the list:

1. Click button on the **List of applications** group.
2. Click **Yes** to delete application from the security scheme.

in List of applications group menu click Create list of applications

4.3.8.2 Creating and Editing the Application Protocol Filter

Filters allow to configure an application protocol (see "Application protocol") to display an information on applications corresponding to your conditions only.

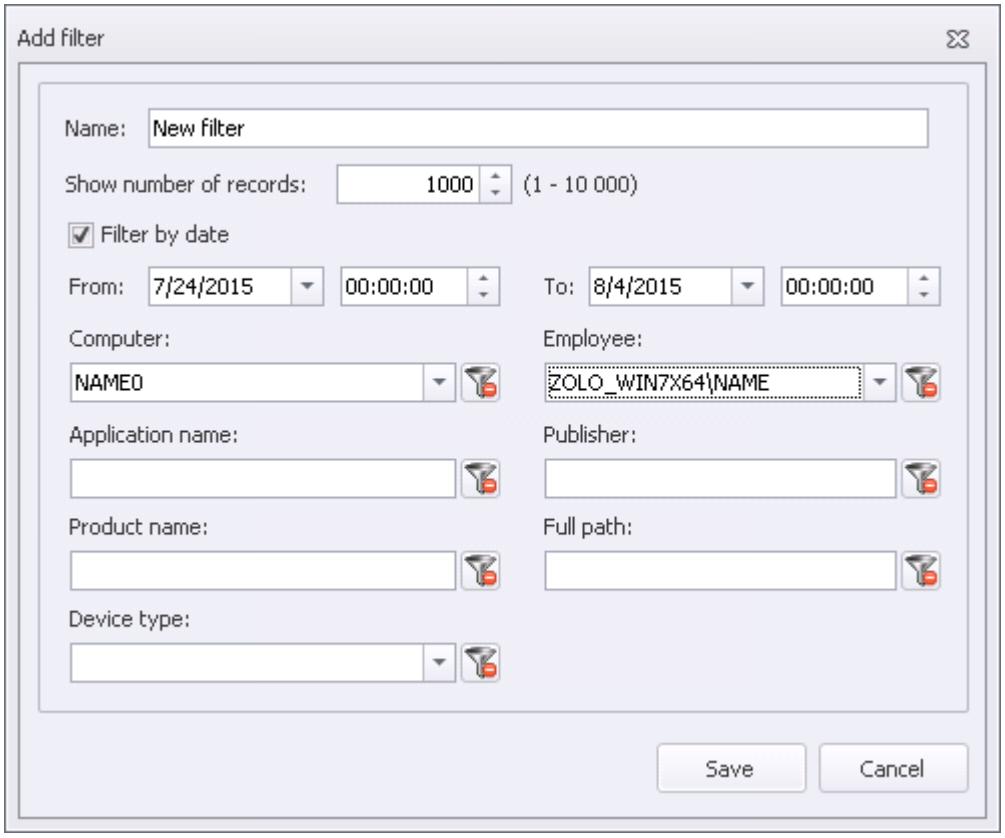
Warning!

Preset **Today** filter shows applications which have been started on particular day since initial installation of the
Client.
All filter shows applications which have been started right upon Client installation.

To create a new filter:

1. Go to **Applications** section.
2. On the Navigation pane set the cursor on the **Application Protocol** group and take one of the following
steps:
   - in the click button in **Application Protocol** group on Navigation pane;
   - select **Edit > Create filter** command in the main menu;
   - right-click in the Application Protocol group and select **Create filter** from the drop-down list.

This opens a dialog box with filter parameters.



3. Enter the name of the filter in **Name** field.
4. In the **Show number of records** field enter the number of records you want to see in the protocol.
5. To set up period for the records to be displayed flag the **Filter by date** option and specify parameters **From** and **To**.
6. If needed, specify additional filter conditions:
    - in **Computer** field select employee's computer which protocol you need to view;
    - in **Employee** field select account of employee which launches applications;
    - in **Application name** field type in the name of the application you want to see information about;
    - in **Publisher** field type in the program publisher;
    - in **Product** name field pick the name of the product;
    - in **Full path** specify the path to the application location;
    - from **Device type** drop-down list select whether the filter should display information on applications
      launched on computers or installed on mobile devices.

    Click  button to delete filter.
7. Click **Save**.

To edit filter:
Click  button in **Application protocol** on Navigation pane or press **Ctrl+E**.

To delete filter:
1. Click  button in **Application protocol** on Navigation pane or press **Ctrl+D**.
2. Click **OK** to confirm deletion.

4.3.8.3 Adding Application to List Automatically

The System allows to fill application lists automatically using data received from the application protocol.

To add application to the list automatically:

1. Go to **Applications** section.
2. On the Navigation pane select the needed filter in the **Application protocol** group.
3. On the **Application protocol** pane select one or several entries. To select several entries click at them
   while pressing **Shift** or **Ctrl** button.
4. Take one of the following steps:
    - on the **Application protocol** pane click  A**dd application to list automatically**;
    - select **Edit > Add application to list automatically** command in the main menu;
    - right-click in the **Application Protocol** pane and select  **Add application to list automatically**
      manually from the drop-down list.
5. In the appeared window:

- select existing list

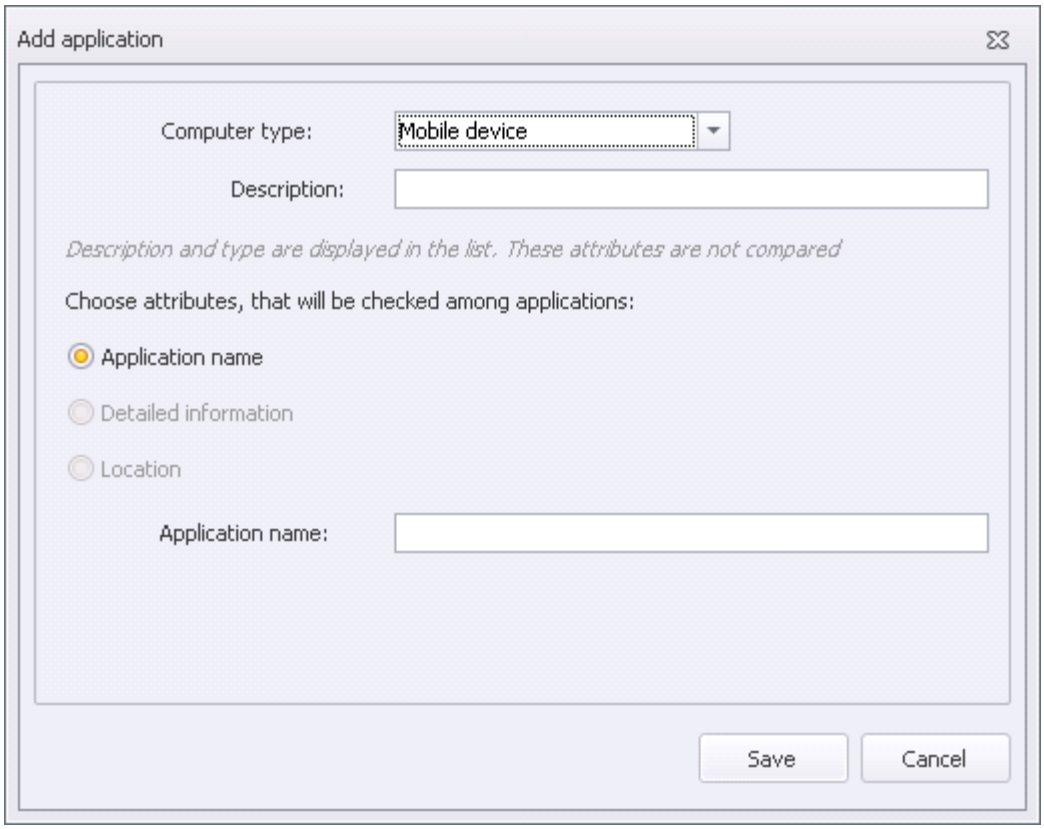
or

6. click **Create new** then enter a list name to the **List name** field and click **Save**.
7. Click **Select**.
8. Click **OK**.

4.3.8.4 Adding Application to List Manually

To add application to the list manually:

1. Go to **Applications** section.
2. On the Navigation pane select the needed filter in the **Application protocol** group.
3. On the **Application protocol** pane select one or several entries. To select several entries click at them
   while pressing **Shift** or **Ctrl** button.
4. Take one of the following steps:
   - on the **Application protocol** pane click  A**dd application to list manually**;
   - select **Edit > Add application to list manually** command in the main menu;
   - right-click in the **Application Protocol** pane and select **Add application to list manually** manually from the drop-down list.
5. In the **Add application** window you can set parameters of checking application correspondence:
   - **Application name**
     Enter the full name of the application file
   - **Detailed information**
     Filtering application by detailed information of Publisher, Product Name, Application Name.
   - **Location**
   - Filtering application by detailed information of **Location** (type in path to the file up to the folder), **Application name** (type in the file name).



6. Click **Select**.
7. If you have selected several entries, repeat steps 5 and 6 for other entries.
8. Click **OK**.

Filtering application by detailed information of Publisher, Product Name, Application Name.

4.3.8.5 Exporting Application Protocol

To export the application protocol:

1. Go to **Applications** section.
2. On the Navigation pane, in the **List of applications** group, select the needed protocol.
3. In the **List of applications** group menu click **Export application protocol**.
4. Specify export location and click **Save**.

The protocol will be exported in .**xls** format.

4.4 Temporary Employee Access to Network

An employee for which a rule (DM) denying connections outside corporate network is active (see "Settings of Corporate Network" and "Configuring Network Monitor Rule (DM)"), can request temporary access to external connections from InfoWatch Device Monitor Client menu, **Network control** command.

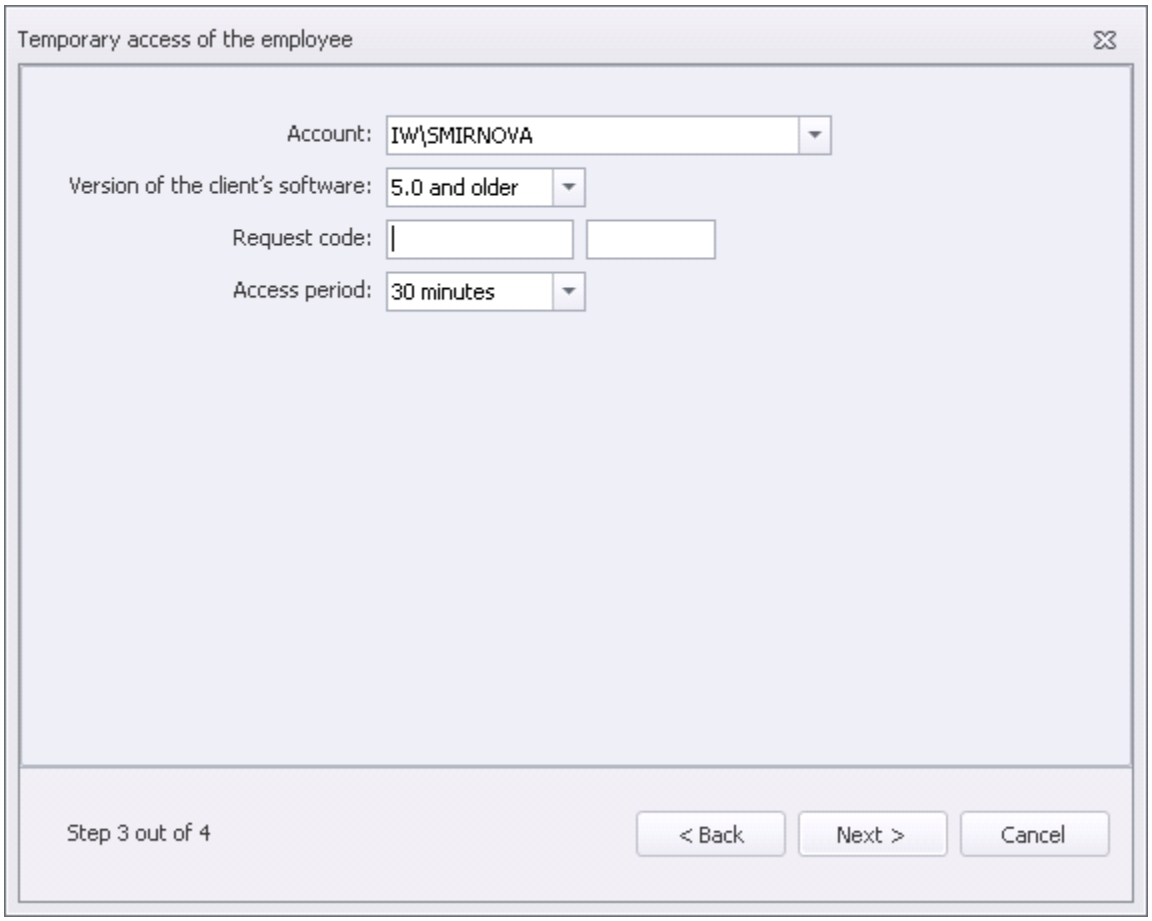
Warning!

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 (DM) Violations", **"Network connection forbidden. Detailed**" notification type.

An employee should send received request code to security officer.

To grant an access to external connections for employee:

1. In Main Menu select **Tools > Temporary employee access**.
2. In the dialog window choose **Dictated by phone**, click **Next**:
3. Choose option **To the network**, click **Next**.



4. From **Account** drop-down list select an account of employee to which a temporary access should be granted.
5. In **Version of client's software** choose version of Device Monitor Client installed on employee's computer.

> **Note:**
>
> When not sure about client's version, choose **4.1** or **4.2**.

6. To **Request code** field enter a code sent by employee.
7. From **Access period** drop-down list select time period for which a temporary access should be granted.
8. Click **Next**.
   The code which should be sent to employee is displayed in **Response code** field.
9. Click **Close**.

4.5 Temporary Employee Access to Devices

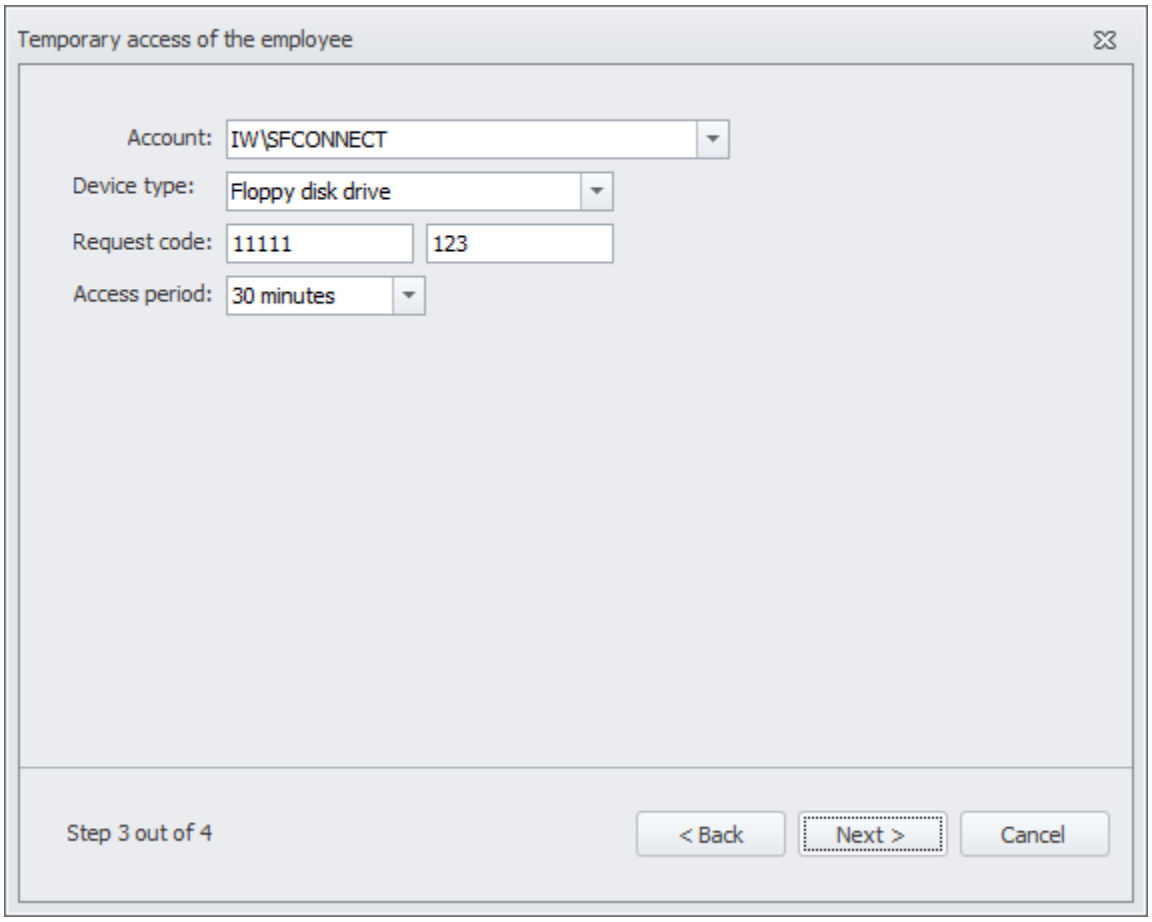
An employee for which a rule (DM) denying using devices is active (see "Configuring Device Monitor Rule"), can request temporary access to a device from InfoWatch Device Monitor Client menu, **Device list** tab.

> **Warning!**
>
> An employee can request access only if the **Show tray icon** option is selected (see "Common Settings for Clients"). On to configure the text displayed to the employee, see "Employee Notifications about DM Policy Violations", "**Access to device denied**" notification type.

The employee should send a received request code to the security officer.
You can communicate with the employee using phone or e-mail.

To grant temporary access to devices for an employee who called by phone:

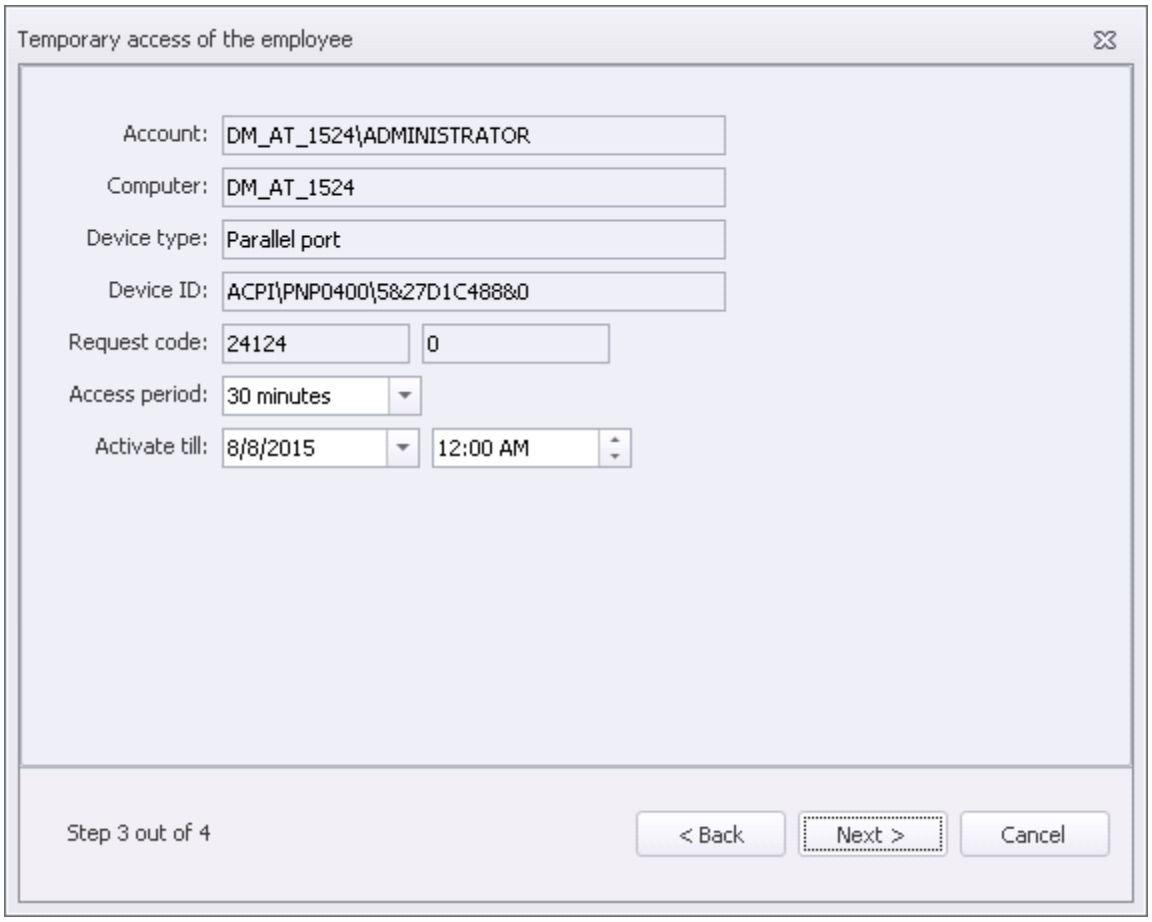
1. In Main Menu select **Tools > Temporary employee access**.
2. Select **Dictated by phone (digital text code)**, click **Next**.
3. Select **To the device**, click **Next**.



4. From the **Account** drop-down list, select an account of the employee to which temporary access should be granted.
5. From the **Device type** drop-down list, select the necessary device type.
6. In the **Request code** field, enter the code dictated by the employee.
7. From the **Access period** drop-down list, select the time period for which temporary access should be granted.
8. Click **Next**.
   The code you should provide to the employee is displayed in **Confirmation code** field.
9. Click **Finish**.

To grant access to devices for employee who sent an e-mail:

1. In Main Menu select **Tools > Temporary employee access**.
2. Select **Obtained via e-mail or other means of communication (query text code)**, click **Next**.
3. In the **Enter request text** field, enter the code sent by the employee, and click **Next**.



4. From the **Access period** drop-down list, select the time period for which temporary access should be granted.
5. From **Activate till** drop-down lists, define the time period, when the employee can activate access to the device (after the activation, access will be provided for the time selected from **Access period** drop-down list).
6. Click **Next**.
   The code which should be sent to the employee is displayed in **Copy answer text to clipboard** field.
7. Click **Finish**.

5 VIEWING EVENTS

InfoWatch Device Monitor Clients installed at managed computers provide keeping data on using external devices, transferring data via network connections and using instant messengers for data transfer. This information is stores as **events** and transferred to InfoWatch Device Monitor servers along with data of shadow copies. Events (unlike shadow copies) are registered in InfoWatch Device Monitor database and are available from Management Console (DM).
You can define the information logging level (keep all information on access attempts, policy (DM) violations only or save nothing) in general settings of your security schema: for further details see "Common Settings for Clients".

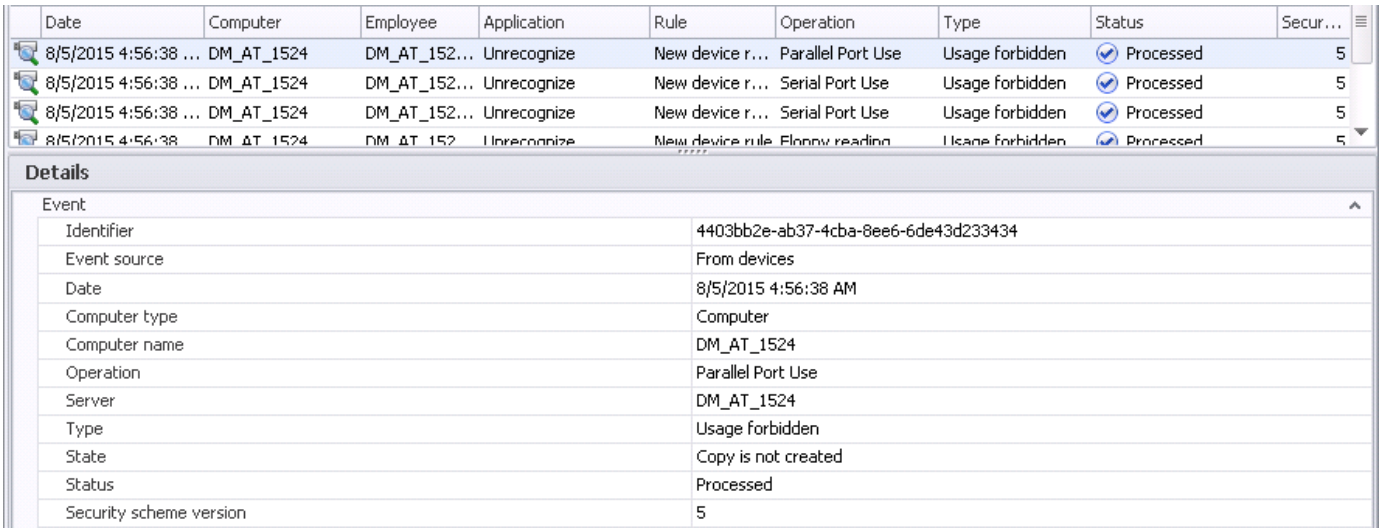
You can view events in **Events** section. To go to this section, click **Events** button on Navigation pane.

To view events,
click the filter name in the filter list.
There are two predefined filters:

- **Last: 4 hours**
- **Today**

You can create custom filters to view events, as described in "Event Filters".

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



Attribute name	Description	Available values
Common attributes		
Identifier	Unique event number	

Event source	Interceptor-based event type	• **File** – File Monitor; • **Devices** – Device Monitor; • **Printer** – Print Monitor; • **Skype, XMPP, MMP, WhatsApp, SMS** – IM Client Monitor; • **FTP/FTPS** – FTP Monitor; • **HTTP/HTTPS** – HTTP(S) Monitor; • **Mail** - Mail Monitor; • **Network** – Network Monitor; • **Mobile device camera** - Photo Monitor; • **System** - event on ending disc space for shadow copy saving. *Such event is not transferred to Traffic Monitor.*
Date	Event date and time (in hours and minutes) registered on computer. Device Monitor server keeps an event in UTC, and Management Console (DM) displays it according to the local time of a computer where Console (DM) installed	
Computer type	Indicates if the computer where the event arisen is the workstation or mobile device	• Workstation • Mobile device
Computer name	Name of the computer that registered the event	
Operation	Employee initiated action or attempt	
Server	Name of InfoWatch Device Monitor server the Client transmits event information to	
Application	Executable file name and/or name of the process responsible for the action, if detected	

Type	Action-based event type	• **Record** – adding or changing data (including renaming) on external device; sending files via messenger; sending print jobs to printer; sending data via FTP/FTPS. • **Use** – connecting an external device that allows unmonitored read/write operations or sending messages; • **Violation** – IM Client interceptor user-initiated violation; • **Warning** – user-initiated a ban or didn't give consent to use IM Client plug-in, while monitoring is required by security policy (DM). • **Usage forbidden** – attempt of sending data via forbidden channel.
Status	Status of event processing on the server and sending to Traffic Monitor server	• **New** • **Awaiting for proceeding** • **Awaiting for sending to TM** • **Sent to TM** **Note**: If the Server is in standalone mode then the event has the **Processed** status only
Security schema version	Number of security schema version that was active on the computer when the event was registered	
Operation verdict	Attribute of allowed action. For Devices events (**Device Monitor** rule) the blocking is also available.	• **Allowed** • **Forbidden** – only for Devices events • **Unprotected data copying is disabled** – only for Devices events • **Allowed (in white list)** - for whitelisted device events
Employee	Name of the domain (computer name outside the domain) and user login used for event registration or operating system reference for events outside user sessions	
Rule (DM)	Name of policy (DM) rule (DM) managing the event	
Terminal client	Terminal client name, if detected	
Network address of a terminal client	Terminal client IP, if detected	

For events with *File* source		
Assign	Full target file name	
File size	Target file size	
Object status	Shadow copy of transferred data	• **no copies created** - rule (DM) does not require shadow copying • **copy created** - shadow copy created successfully • **copying error** - for example, if there is no free space on the client
Device description	Target device instance or model ID	
For events with *Devices* source		
Device type	For supported device types list see "InfoWatch Device Monitor Functions"	
Device instance or model identifier	Model identifier (VID) and serial number (PID) of external device or printer used for the operation	
Device description	Device description received from OS of the computer where the Client is installed	
For events with *Skype, XMPP, MMP, WhatsApp, SMS source*		
IM user ID	UIN of the user authorized in the messenger at computer	
Object status	Shadow copy of transferred data	• **no copies created** - rule (DM) does not require shadow copying • **copy created** - shadow copy created successfully • **copying error** - for example, if there is no free space on the client
List of senders	UIN of IM users, who sent the message/file via messenger	
List of recipients	UIN of IM users, who received the message/file via messenger	
File name	Full name of transferred file	
File size	Transferred file size	

Shadow copy	File, message or chat shadow copy	• **No** - no shadow copy was created • **Yes** - shadow copy created successfully
For events with *Printer* source		
Document	Full name of the file sent to print	
Printer	Name of target network printer	
Object status	Result of creating shadow copy of the print job	1. Shadow copy of print job was successfully created. The job contained graphic and text data. 2. Shadow copy of print job was not created. The job contained no graphic or text data. 3. An error occurred while creating a shadow copy of print job. 4. Shadow copy of print job was successfully created. The job contained only graphic data. 5. The shadow copy should not have been created. 6. Shadow copy of print job was partially created. Graphic data were fully processed. Text data were partially processed. 7. Shadow copy of print job was partially created. Graphic data were partially processed. Text data were fully processed. 8. Shadow copy of print job was successfully created. The job contained only text data. 9. Shadow copy of print job was partially created. Graphic data were partially processed. The job contained no text data. 10. Shadow copy of print job was partially created. The job contained no graphic data. Text data were partially processed.
Object status	Result of creating shadow copy of transferred data	• ○ **no copies created** - rule (DM) does not require shadow copying ○ **copy created** - shadow copy created successfully ○ **copying error** - for example, if there is no free space on the client
For events with *FTP/FTPS* source		

Object status	Result of creating shadow copy of transferred data	• ○ **no copies created** - rule (DM) does not require shadow copying ○ **copy created** - shadow copy created successfully ○ **copying error** - for example, if there is no free space on the client
Sender	Name used for employee authorization at FTP server	
FTP server	Name or IP address of FTP server	**Note**: When using the FTP via proxy server this field can contain proxy address instead of FTP.
Relative path	Directory at FTP server where to the file is transferred	
File name	Full name of transferred file	
Real file size	File size calculated after transfer	
Declared file size	File size according to data of application which performs a transfer to FTP server (browser for example)	
Starting point	When file is transferred by piecemeals, position which starts the of the current part transfer.	
Shadow copy	Result of creating file shadow copy	• **No** – shadow copy was not created • **Yes** – shadow copy created successfully
For events with *HTTP or HTTPS* source		
State	Result of creating shadow copy	• ○ **no copies created** - rule (DM) does not require shadow copying ○ **copy created** - shadow copy created successfully ○ **no free space on disk** - client does not have enough free space ○ **copying error** - for example, if there is no free space on the client
Reciever DNS	DNS name of a computer	
Reciever IP	IP-address of a computer	

Request size	Size of a request in Kbps	
Rule (DM)	Name of policy (DM) rule (DM) managing the event	
For events with *Mail* source		
State	Result of creating shadow copy	• ○ **no copies created** - rule (DM) does not require shadow copying ○ **copy created** - shadow copy created successfully ○ **no free space on disk** - client does not have enough free space ○ **copying error** - for example, if there is no free space on the client
Sender	DNS name of a sender computer	
List of recipients	Receiver addresses	**Note**: For events with a large number of senders you should remember that when Device Monitor Management Console can't display more than 1024 symbols in this field. However, if the shadow copy is set for this event then Traffic Monitor will receive and display the full list of recipients (under 4000 Bytes).
Subject	Mail Subject	
Transmission type	Used protocol	
Message type	Mail direction	• **Incoming** • **Outgoing**
Size, bite	Size in bites	
Channel type	Encrypted or not encrypted	• **All channels** • **Encrypted channel**
Rule (DM)	Name of policy (DM) rule (DM) managing the event	
For events with *Network* source		

Time of ban removal starts	For *Network* operations temporary ban removal operation - start of temporary access period. See details in "Temporary Employee Access".	
Time of ban removal ends	For *Network* operations temporary ban removal operation - end of temporary access period. See details in "Temporary Employee Access".	
Connection server	For *Connection forbidden* operation - address or name of forbidden server which was attempted to gain access to	
Port	For *Connection forbidden* operation - port number used for connection attempt.	
For events with *Mobile* device camera source		
Photo size	Size of photo shadow copy, in bytes	

If needed, you can free some space in the database by deleting all the information about already processed events
(Processed or Sent to Traffic Monitor state). See details in "Deleting Events".

5.1 Event Filters

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

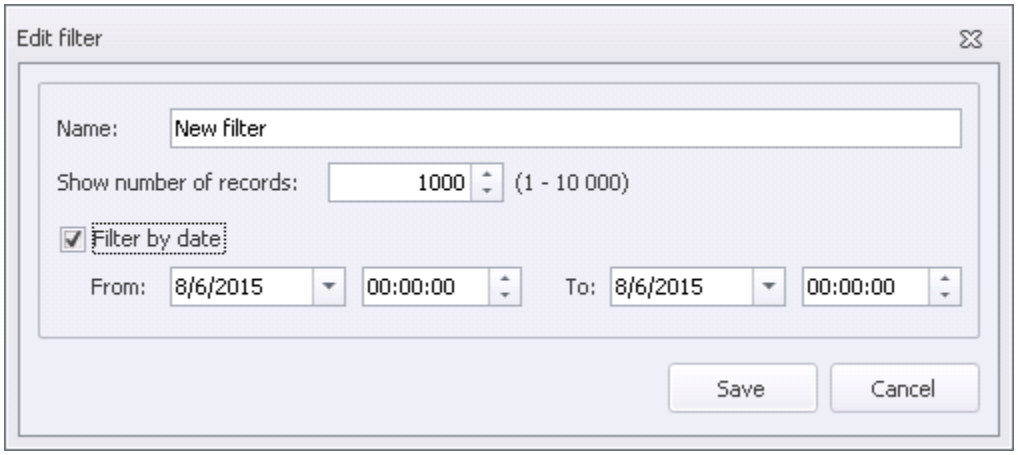
To add or edit a filter:

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

Action	Steps
Creating filter	• in Main Menu select **Edit > Add Filter**; • click **Add Filter** at the top of Navigation pane.

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

These actions open Edit filter dialog.



3. Specify filter options in **Edit Filter** dialog:
   - **Filter Name**.
   - **Show number of records**. Limit on the number of entries displayed in Management Console (DM) workspace (1000 records by default).
   - To filter by a date, flag **Filter by date** box and specify the desired period in From and To fields. Set the date and time in right and left field respectively.

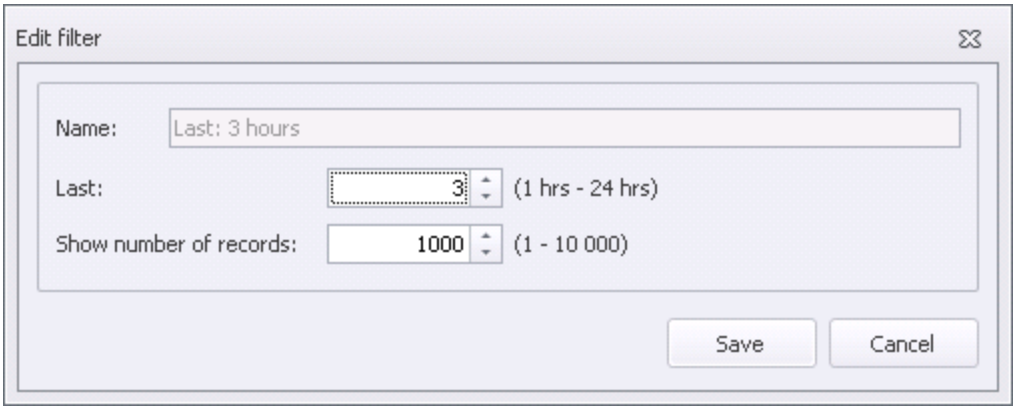
> **Note:**
>
> For the predefined filters **Filter Name** and **Filter by date** parameters cannot be edited.

4. Click **Save**.

The predefined filter **Last: 4 hours** has another editing interface and lets to make filters displaying events for last
several hours.

To edit predefined filter to view events for the selected number of hours:

1. In **Events** area of Navigation pane, select the **Last: 4 hours** filter.
2. Take one of the following steps:
   - in Main Menu click **Edit > Edit Filter**;
   - click **Edit Filter** at the top of Navigation pane.
   - double-click the filter name.



3. Specify filter options in **Edit Filter** dialog:
    - **Last**. Specify the number of hours, entries for which should be displayed in the Management Console (DM) workspace.
    - **Show number of records**. Limit on the number of entries displayed (1000 records by default).
4. Click **Save**.

5.2 Deleting Events

The information about already processed events (**Processed** or **Sent to Traffic Monitor** state) can be deleted.

You can delete events:

- for certain time period;
- all matching certain filter.

To delete from the database an information about events for a period:

1. Go to **Events**.
2. Take one of the following steps:
    - click **Delete events** at the top of Navigation pane.
    - in Main Menu click **Edit > Delete events**.
3. In the opened dialog window **Deleting from database**, specify needed time period for which you want to delete events.
4. Click **Delete**.

Then a number of deleted events will be displayed.

To delete from the database an information about events matching certain filter:

1. Go to **Events**.
2. In the filter list select needed filter name.
3. Take one of the following steps:
    - click **Delete filter events**at the top of **Events** area.

- in Main Menu click **Edit > Delete filter events**.

4. In request box select **Yes** to confirm.

Then a number of deleted events will be displayed.

6 CLIENTS REMOTE INSTALLATION, UPDATING AND UNINSTALLATION

You can install, update, or delete InfoWatch Device Monitor Clients from a computer via InfoWatch Device Monitor
Management Console (DM). These operations are performed through **tasks**. You can run tasks to install, update or
remove client software, change uninstallation password, or monitor these processes.

Remote client management is carried out by special **Distribution Agent** transmitted onto client workstations. The
Agent requires the following:

- Target computers must meet hardware and software requirements: see document "Traffic Monitor. Installation guide", article "InfoWatch Device Monitor Client Hardware and Software Requirements".
- Proactive virus protection for computers must be turned off at the time of installation.
- Device Monitor server and target computers should resolve each other by domain names.
- On computers, where firewall, different from windows standard one, is installed, it should be disabled. Except
  for disabling, you can also allow any network connections for the following Device Monitor components:
  `IWDeployAgent.exe, iwdmc.exe, DM.Client.exe, IWProxy.exe, rmtlogctr.exe.`

Note:

To install Client on Windows 7 computer, go to **Control Panel -> Network and sharing center -> Change advanced sharing settings**. Enable file and printer sharing. Upon completion, **Distribution**
Agent can be copied to computer. Firewall will be automatically configured.

To go to Management Console (DM) 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 (DM)). For more information see document "Traffic Monitor. Installation guide", article "Client Installation via Software Distribution Tools". To run these operations, use installation package that was created as described in "Creating Installation Package".

6.1 Viewing Tasks

Tasks area of Navigation pane displays a list of all created, executed and outstanding tasks. Main screen work pane displays a list of target computers for the selected task.

Details panel displays the following parameters for selected task:

Parameter	Description
Name	Original name of the task
Description	Original description of the task
Type	One of the following task types: • Primary distribution • Change password • Update • Uninstall
Status	Current task status. Possible values: • Executing • Stopped • Completed
Restart period, min	Intervals between task launches on computer, if the previous attempt failed, in minutes. Counted from ending the last workstation proceeding in previous task launch. If the task fails, it won't be launched again.
Number of restart trials	Maximum number of retries to restart distribution task on computer. After all attempts have been used, **Task status** parameter value will be set to **Error** (for further details, see "Client Installation Errors").
For primary distribution tasks	
Show employee notifications	Indicates that employee's attempt to perform a banned action will trigger a warning. For further details, see "General System Settings", "Creating Installation Package" and "Employee Notifications about Policy (DM) Violations"

Hide presence of agent on workstation	Indicates if Windows system tray of managed computer hides Client presence on the computer. Otherwise, Windows system tray of the computer where Client installed will display  icon. By clicking this icon, an information on DM Client operation and list of currently controlled devices is displayed. **Warning!** If there is an antivirus protection enabled on the managed computer then the antivirus program can reveal the operation of Device Monitor: for example, in the list of processes running on the managed computer or in the list of programs that initiate a control.
Install the component of network connections control	Indicates if iw_proxy component is installed.
Install the component of network connections control	Indicates if Network Monitor interceptor is installed.
Uninstallation product password	Shows if the password requested from employee that attempts to remove Device Monitor Client.
Proxy Root Issuer DN	The unique name of Device Monitor proxy server certificate, issuer distinguished name.
For primary distribution and update tasks	
Installation directory	Installation directory for Device Monitor Client at target computers.
Installation login	Name of the Console (DM) user that launches the task on computers.
Waiting fir restart duration, hours	Computer reboot waiting period (in hours); if the computer is not restarted manually during this period, the System will notify the employee (if notifications are enabled), and force operating system restart.
Duration of restart notifications, hours	Period of displaying requests for rebooting computer, in hours.
Restart notifications rate, min	Time intervals between repeated reboot requests, in minutes.
Reboot messages	Text displayed to the employee in reboot request.
Show a warning before forced reboot	Indicates if a notification about forced reboot will be displayed when reboot wait durations are expired but employee did not reboot the computer.
For change password tasks	
Uninstallation product password	Shows if the password requested from user that attempts to remove Device Monitor Client.

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

Parameter	Description

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

6.2 Preparing Primary Client Installation. Distribution Agent

Remote client installation is carried out by InfoWatch Device Monitor special **Distribution Agent**.
Correct remote client installation via InfoWatch Device Monitor requires the following:

- Target computers must meet hardware and software requirements: see document "Traffic Monitor. Installation guide", article "InfoWatch Device Monitor Client Hardware and Software Requirements".
- Proactive virus protection for computers must be turned off.
- Computers with the firewall that differ from Windows firewall, that firewall:
    - should be disabled
      or
    - should have a permission for InfoWatch Device Monitor Distribution Agent
      or
    - should have **15505** port (default port by which the Distribution Agent awaits for a connection) opened for
      incoming connections, if it was not changed in connection settings (see document "Traffic Monitor. Installation guide", article "<applicationSettings> section", **CommunicationPort** parameter).

Additional requirements vary depending on distribution method:

Method 1:
Distribute `Setup.DeployAgent.msi` installation package (provided along with installation software) to target computers.

Method 2:
Transmit Distribution agent through shared administrative resources:

- Computer firewalls must be either turned off, or set required exceptions: see "Firewall Settings".
- Specify settings for network access to shared resources: see "Enabling Shared Administrative Resources".

If all requirements are met, you can start creating and then start primary distribution tasks.

6.2.1 Enabling Shared Administrative Resources

To transfer InfoWatch Device Monitor distribution agent to target computers through shared administrative resources, the following requirements must be met:

- If computer with Windows XP is outside a domain, in security policy (DM) settings of this computer set **Network access configuration parameter: Sharing and security model for local accounts** value to `Classic`.
- Computers must have their shared administrative resources (like `\\computername\admin$`) enabled (in
  Windows Vista and Windows 7 they are disabled by default). To enable them:
  a. 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.
  b. 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**.

6.2.2 Firewall Settings

Firewall settings requirements:

Application protocol	Transport protocol	Port
RPC	TCP	135
RPC over HTTPS	TCP	593
NetBIOS Datagram Service	UDP	138
NetBIOS Name Resolution	UDP	137
NetBIOS Session Service	TCP	139
SMB	TCP	445

For computer availability defining quickness the ICMP protocol should be permitted.
For Windows firewall the "**File printing and sharing**" preset rule should be permitted.

6.3 Creating Primary Distribution Task

Primary distribution (installation from Management Console (DM)) of InfoWatch Device Monitor Client using installation **agents**. Installation agent is an executable file. It is passed on to computers and starts automatically during task execution, receiving Client updates from server.

Warning!

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

- all target computers
- computer where Management Console (DM) 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 (see "*Traffic Monitor. Installation guide*", arcticle "Creating Installation Package") and install it by other means (see "*Traffic Monitor. Installation guide*", arcticle "Standard InfoWatch Device Monitor Client Setup" and "Client Setup via Software Distribution Tools").

Warning!

If the workstation has Kaspersky Internet Security installed then you need to disable its self-protection to install the InfoWatch Device Monitor Client. See internet article "How to enable/disable self-defense in Kaspersky Internet Security" internet article.

To create a primary InfoWatch Device Monitor client application distribution task:

1. Go to **Tasks**.
2. Take one of the following steps:
   - in the Main Menu select **Edit > Add Task**;
   - click **Add Task** at the top of Navigation pane.

   These actions open **Deployment task wizard** dialog.
3. Enter task name, select **Initial deployment task** and type task description, then click **Next**.

4. Create a list of computers which you need to install Device Monitor Client to. To add computer (or several computers):
    a. Click **Add Select computer** dialog will display a list of computers from:
        - from directory;
        - Microsoft Windows Network;
        - ones registered before (for example, after manual Client installation) and belonging to computer groups (**DM server computers** node).
    b. Flag computers or computer groups. Minimized groups are marked with an icon ; expanded - . Doubleclick a group, to expand or collapse it.

> **Warning!**
>
> By marking a group you select the computers that are included in that particular group. Subgroups and subgroup computers of selected group are not selected: you have to select them separately.

    You can also specify computer name or IP addresses:
        - in the line at the bottom of dialog box. When listing addresses, separate them with semicolons;
        - click **Import** and download text file where one entry should be placed in the each line; text should
          contain no blank lines.
    c. After you specify the computers you want to add, click Select. The dialog will be closed and selected computers list will be displayed in **Task target computers list** area. To remove a computer from the list, select it and click **Remove**. When you make a full list of computers click **Next**.
5. Then InfoWatch Device Monitor servers currently registered in the System are displayed. You can change Client installation directory (%Program Files%\Infowatch\DeviceMonitor\Client is used by default).

> **Important!**
>
> Path to the catalogue may contain the following characters: 0-9, a-z, A-Z, ":", ".", "_", "-", "\", " ". If the path includes other characters, the client installtion will be incorrect.

    Click **Next**.
6. The unique name of Device Monitor proxy server certificate (Issuer Distinguished name, Proxy Root Issuer DN) will be displayed. You can change it with accordance to X.509 standard, CN (Common Name) field is mandatory, all fields comma-separated. Click **Next**.
7. Specify options of computer reboot:
    - **Wait for reboot without notifying the employee**. The Agent can:
        - start notifications immediately (*Do not wait* option),

- start notifications in specified time (*Wait for option* - please specify time period to start notifications),
- or do not notify at all (*Wait infinitely* option).

- **Notify the employee about reboot necessity and wait for reboot**. Upon completing reboot waiting in "silent" mode (see **Wait for reboot without notifying the employee** setting) or immediately after installation ends, Device Monitor Client starts to notify employee on reboot necessity:
  - during specified time period (*Notify within option*);
  - permanently (*Notify infinitely* option);
  - do not notify at all (*Do not notify* option).

  If needed, change continuance and frequency of notifications appearance and enter text of the message displaying in reboot notification.
- **Show a warning before forced reboot**. If this check box is flagged, then the Client displays a notification about forced reboot and allows 5 minutes to end operations. Then the computer will be forced to reboot. If the option is not checked then the forced reboot (if it should be made according your settings) will be performed unexpectedly for the employee.

> **Warning!**
>
> Forced reboot is performed in case when neither **Wait while employee reboots computer** setting no S**how a warning before force reboot** setting do not flagged, or their wait durations are expired but employee did not reboot the computer.

Click **Next**.

8. Configure Client settings:
   - To protect Client application from deleting by employee, enter the password that will be requested when trying to uninstall the Client and confirm it.
   - **Show employee notifications** - if employee attempts to perform an action restricted by security policy (DM), a warning will be displayed. For further details, see "Employee Notifications about Policy (DM) Violations".
   - **Hide Agent presence** - indicates if Windows system tray of managed computer hides Client presence on the computer.

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

> **Important!**
>
> Hiding/notifying settings apply on the Client up to the first call to the server. On calling to the server, the Client will start using settings of the group the workstation belongs to.

> **Warning!**
>
> If there is an antivirus protection enabled on the managed computer then the antivirus program can reveal the operation of Device Monitor: for example, in the list of processes running on the managed computer or in the list of programs that initiate a control.

If this option is not selected, the Windows system tray of the computer where the Client is installed will display  icon. By clicking this icon, information on DM Client operation and list of currently controlled devices is displayed.

- **Install the component of network traffic interception** - installs **iw_proxy** component on a computer.
  Component will not be installed if you leave the checkbox empty.
- **Install the component of network connections control** - installs **Network Monitor** interceptor on a computer. Component will not be installed if you leave the checkbox empty.

> **Warning!**
>
> You should not install the component of network control to the server with Citrix Provisioning Services: this can lead to the serious problems concerning server operation.

- Task run parameters: they will be used in case the task wasn't launched at the first attempt. Specify the number of attempts and their intervals, in minutes.
- To launch a task immediately after saving, flag **Run task immediately** check box.
- Enter the credentials for the account that launches the task.This account must have administrator rights on all target computers.

> **Warning!**
>
> The System does not save passwords for accounts used to launch tasks. If the new task is not launched immediately, you will have to use password next time to launch it from Management Console (DM).
> If a password of used account is expiring (Windows warns that the password expires in 3 days and need to be changed) then primary distribution task cannot run on behalf of this user.

Click **Next**.

9. Look through the task summary. If you need to change any settings click **Back** to return. If all settings are correct, click **Finish**.

6.4 Creating Update Task

InfoWatch Device Monitor client applications update is required after InfoWatch Device Monitor server upgrade: for
further details, see document "Traffic Monitor. Installation guide", article "Updating InfoWatch Device Monitor Server End".

> **Note:**
>
> Beside the following method, you can create update task with a simplified function as described in document "Traffic Monitor. Installation guide", article "Updating Clients at Managed Computers".

To create and schedule InfoWatch Device Monitor client applications update task:

1. Go to **Tasks**.
2. Take one of the following steps:
   - in the Main Menu select **Edit > Add Task**;
   - click **Add Task** at the top of Navigation pane.

   These actions open **Deployment task wizard** dialog.
3. Select **Update task**, enter task name and description and click **Next**.
4. Create a list of computers that require Device Monitor Client update. To add computer (or several computers):
   a. Click **Add**. The **Select computers** dialog, **DM server computers** node, contains the list of computers where Device Monitor Client version does not match Device Monitor Server version but can be automatically updated (client software version should be 4.0.651 and higher).
   b. Flag computers or computer groups. Minimized groups are marked with an icon ; expanded - . Double-click a group, to expand or collapse it.

> **Warning!**
>
> By marking a group you select the computers that are included in that particular group. Subgroups and subgroup computers of selected group are not selected: you have to select them separately.

c. Use **Filter by computer name** field to specify computer. Click **Find**.

d. After you specify the computers you want to add, click **OK**. **Select computers** dialog will be closed. Selected computers list will be displayed in **Task target computers list** area.
To remove a computer from the list, select it and click **Remove**.

When you make a full list of computer click **Next**.

5. Please specify reboot settings:
   - **Wait for reboot without notifying.** The Agent can**:**
     - Start to notify immediately (*Do not wait* parameter),
     - Start to notify after mentioned time period (Wait for hour(s) parameter - you need to specify time
     - before notification),
     - Do not notify before forced reboot (*Wait infinitely* parameter)..
   - **Notify the employee about reboot necessity and wait for reboot.** After "silent mode" wait to notify
     (see Wait for reboot without notifying setting), or right after update process completion, Device Monitor client will start to notify the employee about reboot necessity during specified time period (*Notify*
     within hour(s) within: minutes parameter) or infinitely (*Notify infinitely every x minutes*), or do not notify (
     Do not notify). When necessary, change length and frequency and specify text of the message, which
     will be displayed along with notification.
   - **Show a warning before reboot** - is a parameter to specify whether forced reboot notification will be
   - displayed (an employee can complete current tasks within 5 minutes before forced reboot) or forced
   - reboot will be performed without any additional text.
6. Specify:
   - Task retry parameters: they will be used in case the task wasn't launched at first attempt; if launching failed, the task won't be launched again. Specify the number of attempts and their intervals, in minutes.
   - To launch a task immediately after saving, flag **Run task immediately** check box.

Click **Next**.

7. Look through the task summary. If you need to change any settings click **Back** to return. If all settings are
correct, click **Finish**.

> **Warning!**
>
> If the workstation has the Kaspersky Internet Security installed then you need to disable its selfprotecting
> function for successful InfoWatch Device Monitor Client update.
> See details in internet article "How to enable/disable self-defense in Kaspersky Internet Security".

6.5 Creating Uninstallation Password Reset Task

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 **Change uninstall password task**, enter task name and description and click **Next**.
4. Create a list of computers that need their uninstallation passwords to be changed on **Deployment target
computers** screen. To add computer (or several computers):
   a. Click **Add**. The **Select computers** dialog, **DM server computers** node, contains the list of computers where Device Monitor Client is installed.
   b. Flag computers or computer groups. Minimized groups are marked with an icon ; expanded -. Double-click a group, to expand or collapse it. Use **Filter by computer name** field to specify the computer.

      Click **Find**.

      > **Warning!**
      >
      > By marking a group you select the computers that are included in that particular group. Subgroups and subgroup computers of selected group are not selected: you have to select them separately.

   c. After you specify the computers you want to add, click **OK**. **Select computers** dialog will be closed.

Selected computers list will be displayed in **Task target computers list** area.
To remove a computer from the list, select it and click **Remove**.

When you make a full list of computer click **Next**.

5. 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**.

> **Warning!**
>
> If the workstation has the Kaspersky Internet Security installed then you need to disable its selfprotecting
> function for successful InfoWatch Device Monitor Client update.
> See details in internet article "How to enable/disable self-defense in Kaspersky Internet Security".

6.6 Creating Uninstallation Task

To create a centralized task that removes InfoWatch Device Monitor client applications:

1. Go to **Tasks**.
2. Do either of the following:
   - from the main menu, choose **Edit** > **Add task**;
   - use **Add task** button which is located at the top of the **Tasks** section.

   The **Deployment task** wizard dialog box will appear.
3. At step 1, select **Uninstall task**, enter the task name and description, then click **Next**.
4. At step 2, create a list of workstations, from which you want to uninstall Device Monitor Client. To add workstations:
   a. Click **Add**. The **Select computers** dialog box will open. The **DM server computers** node contains the list of workstations, where Device Monitor Client is installed. You can also use the search field **Filter by computer name**. Enter the computer name and click **Find**.
   b. Flag required workstations or computer groups. Minimized groups are marked with



; expanded ones are marked with



. To expand or collapse a group, double-click its name.

> **Important!**
>
> When you select a group, only computers included in this group are selected. Subgroups of the selected group and computers included in the subgroup are not selected: you should select them separately.

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

To remove a workstation from the list, select its name and click **Remove**.
If all required workstation are present in the list, click **Next**.

5. At step 3, specify restart options for the task: they will be used if, for some reasons, the task was not started at the first attempt; if the task start failed with an error, the task will not be started again. Specify the number of attempts and the interval between attempts in minutes.
To launch the task immediately after saving, select **Run task immediately** check box.
Click **Next**.
6. View the task summary. If you need to change some settings, click **Back**. If all settings are specified correctly, click **Finish**.

> **Important!**
>
> If Kaspersky Internet Security is installed on a workstation, then, before uninstalling InfoWatch Device Monitor Client applications, you should disable self-defense in Kaspersky Internet Security.
>
> For more details, see "How to enable/disable self-defense in Kaspersky Internet Security".

6.7 Launching, Pausing, Editing, and Deleting Tasks

If you flagged L**aunch task immediately** when creating a task, it will start immediately. Otherwise, you will need
to manually launch the task. You might need this option, if for some reason you had to stop the task and want to
start it again.

For instructions see the following table.

To perform any of these procedures, you must first select a task from the list on **Tasks** panel.

Action	Steps
Start task	• in the Main Menu select **Edit > Perform** task; • click **Perform task** located at the top of Navigation pane.
Stop task	• in the Main Menu select **Edit >Stop task**; • click **Stop task** at the top of Navigation pane.
Edit list of computers in task	• at the top of **Task execution result** panel click **Add computer** or **Exclude computer from task** • right-click computer row and select **Add computer** or **Exclude computer from task**. **Warning!** You can't remove a computer if the task is running and not completed.
Edit task	• in the Main Menu select **Edit > Edit**; • click **Edit** at the top of Navigation pane. • right-click on task name and select **Edit**. Specify new settings for the task like it is done for a new task (see "Creating Primary Distribution Task", "Creating Updating Task", "Creating Uninstallation Password Reset Task", "Creating Uninstallation Task")
Delete task	• in the Main Menu select **Edit > Delete**; • click **Delete** at the top of Navigation Pane. • right-click on task name and select **Delete**. **Warning!** You can't remove a task with computer that has a running task.
View computer error log	• at the top of **Task execution result** panel click **Computer log** • right click computer row and select **Computer log**

6.8 Client Installation Errors

You may encounter installation problems during remote InfoWatch Device Monitor client applications installation
tasks to computers. This will be indicated by Task status value in the list of tasks: see "Viewing Tasks".

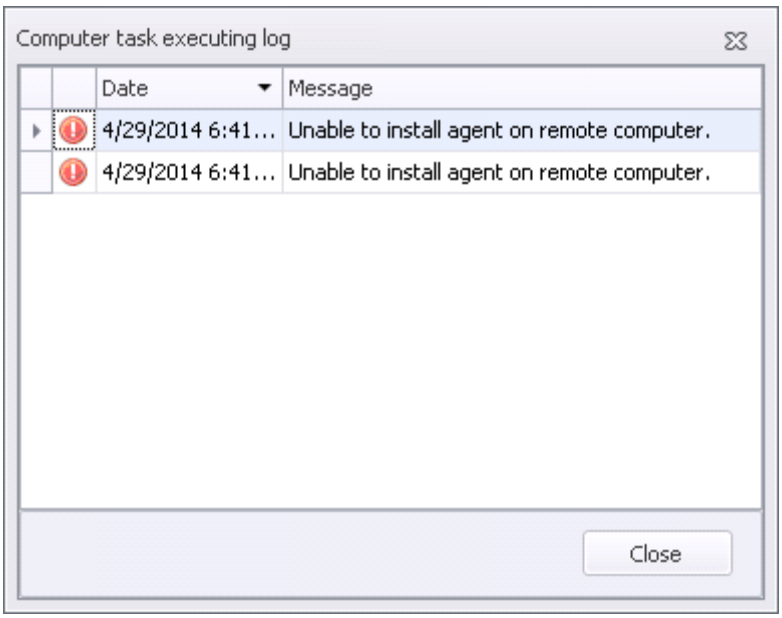
To view task errors:

1. Go to **Tasks**.
2. On **Tasks** panel select the task you want to review.

3. In **Status** column select filter value **Error** (for more information on filters see "Applying Standard Filters").

> **Note:**
>
> Status **No access** indicates that computer is not available (switched off or disconnected from network)

4. In the row of the target computer do one of the following:
   - right-click the row and select **Computer Log;**
   - double-click the target computer row;
   - at the top of **Task execution result** panel click **Computer log**.



5. To view detailed error information, click the row. This opens a screen with Windows error description.

For detailed information on the error see its description, error code, or log in error's description. In particular, the errors may be caused by the following things:

- computer is not available (switched off or disconnected from network);
- the installation process or reboot is blocked by another task or user (common description could be "*Other task is running*");
- target computer does not allow administrative resources;
- account in use doesn't have enough rights on target computer.

If all remote Client installation conditions in "Preparing Primary Client Installation. Distribution Agent" are met and the task is not blocked by the user, but the error persists, please contact InfoWatch technical support at support@infowatch.com and attach error description and log.

6.9 Creating Installation Package

Supplied InfoWatch Device Monitor Client installation package contains the following default settings:

- Client installation directory on computer system drive - `%Program Files%\Infowatch\DeviceMonitor\Client.`
- There is no uninstallation password.
- After installation Device Monitor Client starts to remind an employee that a reboot is required. Message text -
  "*Please reboot your computer as soon as possible*". Reminders are displayed infinitely, with 10 min intervals.

To change these settings create your own installation package. When you run it, it will use the settings specified
when installation package created: no other parameters are needed to specify.

To create InfoWatch Device Monitor Client installation package:

1. In the Main Menu select **Tools > Create install package**.
   This opens distribution task manager dialog box.
2. The InfoWatch Device Monitor servers currently registered in the System are displayed. Client will use them
   for primary installation.

   If necessary, change Client installation directory at computers.
   Specify local or network directory where to the installation packages will be saved.
   Click **Next**.
3. The unique name of Device Monitor proxy server certificate (Issuer Distinguished name, Proxy Root Issuer
   DN) will be displayed. You can change it with accordance to X.509 standard, CN (Common Name) field is
   mandatory, all fields comma-separated. Click **Next**.
4. Specify options of computer reboot:
   - **Wait for reboot without notifying the employee**. The Agent can:
     - start notifications immediately (*Do not wait option*),
     - start notifications in specified time (*Wait for option* - please specify time period to start notifications),
     - do not notify at all (*Wait infinitely option*).
   - **Notify the employee about reboot necessity and wait for reboot**. Upon completing reboot waiting in
     "silent" mode (see **Wait for reboot without notifying the employee** setting) or immediately after
     installation ends, Device Monitor Client starts to notify employee on reboot necessity:
     o during specified time period (*Notify within* option)
     o permanently (*Notify infinitely* option)
     o do not notify at all (*Do not notify* option).
     If needed, change continuance and frequency of notifications appearance and enter text of the message
     displaying in reboot notification.

- **Show a warning before forced reboot**. If this check box is flagged, then the Client displays a notification about forced reboot and allows 5 minutes to end operations. If the option is not checked then
the forced reboot (if it should be made according your settings) will be performed unexpectedly for the
employee.

> **Warning!**
>
> Forced reboot is performed in case when neither **Wait while employee reboots computer** setting
> no **Show a warning before force reboot** setting do not flagged, or their wait durations are expired
> but employee did not reboot the computer.

Click **Next**.

5. Define Client settings before it connects to the server for the first time:
   - To protect Client application from deleting by employee, enter the password that will be requested when
   trying to uninstall the Client and confirm it.
   - **Show employee notifications** - if employee attempts to perform an action restricted by security policy (DM),
   a warning will be displayed. For further details, see "Employee Notifications about Policy (DM) Violations"
   - **Hide Agent presence** - indicates if Windows system tray of managed computer hides Client presence
   presence on the computer.

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

> **Warning!**
>
> If there is an antivirus protection enabled on the managed computer then the antivirus program can
> reveal the operation of Device Monitor: for example, in the list of processes running on the managed
> computer or in the list of programs that initiate a control.

If this option is not selected, the Windows system tray of the computer where the Client is installed will
display icon. By clicking at this  icon, an information on DM Client operation and list of

currently
controlled devices is displayed.

- **Install the component of network interception** - installs **iw_proxy** component on a computer.
  Component will not be installed if you leave the checkbox empty.
- **Install the component of network control** - installs **Network Monitor** interceptor on a computer.
  Component will not be installed if you leave the checkbox empty.

> **Warning!**
>
> You should not install the component of network control to the server with Citrix Provisioning
> Services: this can lead to the serious problems concerning server operation.

Click **Next**.

6. Look through the task summary. If you need to change any settings click **Back** to return. If all settings are
   correct, click **Finish**.

Client installation package will be saved in the folder you specified at the first step.

7 ADDITIONAL FEATURES

You can use the following functions to enhance your Management Console (DM) experience: filtering, grouping and
sorting table entries.
Certain functions can be also accessed with hotkeys.

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:

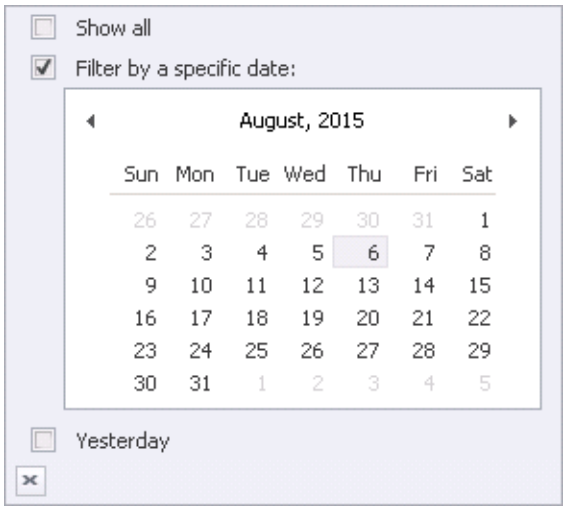
- Filter by Date;
- Applying Standard Filters;
- Custom Filter;
- Editing Filters;
- Removing a Filter.

7.1.1 Filtering by Date

If the table shows temporary parameter characteristics (for example, Client installation date and time, Console (DM) log
time, last computer access, registered event date, etc.), you can filter the column against the desired date or
period.

To view the records for specific date or period:

1. Move the pointer over the time/date attribute in the column header.
2. Click the button ▾ to the right of the column header.



3. Select one of the following filters:
   - **Show all** - select this check box to view all records regardless the date.
   - **Filter by a specific date** - select the date in the calendar.
     To select a period, select it holding the mouse button.
     To go from date to month or year display, click the month/year.
     Use arrows to go forward or backward.
   - **Today; Yesterday; Last week; Earlier this week; Earlier this year** fields depend on column values: for
     example, if there are no records for the date, **Today** field won't be displayed. Check this box to display
     only the records inside specific date range.
4. Click ✖ to apply the filter and close the form.

7.1.2 Applying Standard Filters

To filter table entries against a single attribute:

1. Move the pointer over the time/date attribute in the column header.
2. To view filter list, click ▽ to the right of the column.
3. Select one of the following filters from the list:
   - **Blanks**. Display records with `<Is Null>` value (the field is empty).
   - **Non blanks**. Display records with `<Is Not Null>` value (i.e., the field contains attribute value).
   - `<attribute value>`. Display records that contain selected attribute.

> **Note:**
>
> **Custom** option lets you configure your filtering criteria (for more info see "Custom Filter").

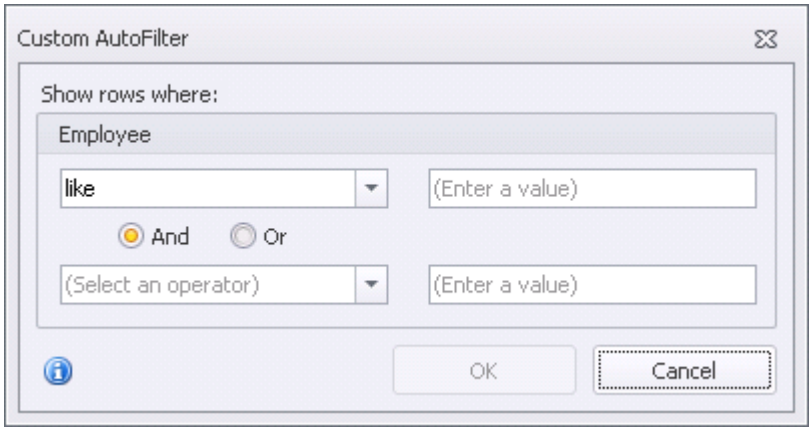
The table will only display filtered values.

To filter values against several attributes,
repeat simple filtering procedure against all filter attributes you want to apply.
Complex filter reduces the table contents to records filtered against several attributes.

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.

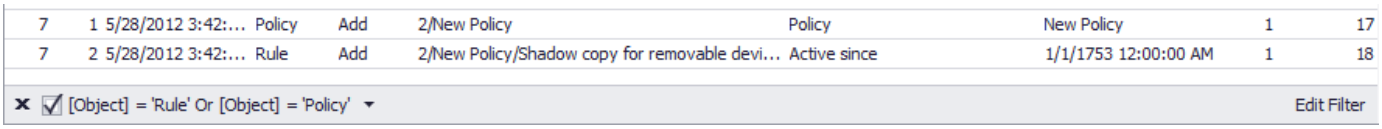
> **Note:**
>
> You can use comparison operators to limit filtering criteria: *equal, not equal, greater than, greater than or equal to, less than, less than or equal to; values empty (blank) and nonempty (non-blank field)*; or
> text filter with a mask. To get a text filter syntax tip, click .

   - 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.

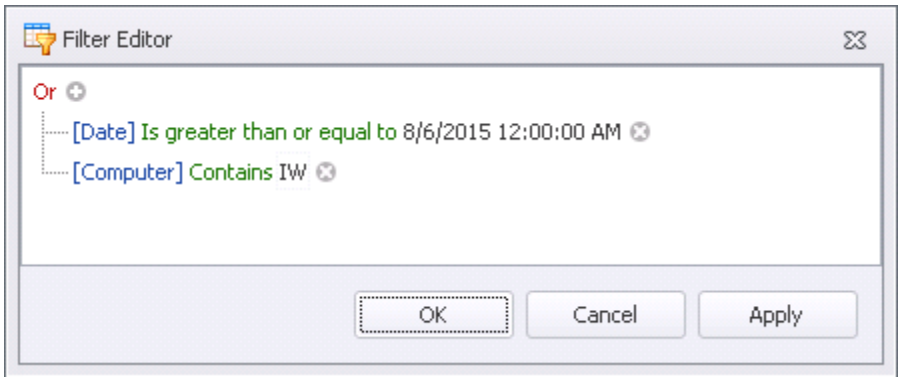


To remove filter and view all items, clear the check box in filter string. To apply the filter again, select the check box.
To re-use a filter, click the filter string and select filter from drop-down filter history list. Custom filters are stored until you close the window with filtered content.

7.1.4 Editing Filters

To edit active filter:

1. Click **Edit Filter** at the end of the filtering conditions string. The following dialog box displays **Filter Editor**.



2. Edit filtering criteria. Available actions:

Action	Steps
Edit an attribute, attribute value or operator	1. Click attribute/value name of attribute/operator 2. Select the value from the drop-down list or enter the value to the field
Add a simple condition	Click the button ⊕ to the right of the logical operator or Click **Add Condition** in logical operator menu
Delete condition	Click the button ⊕ at the end of condition string

Add criteria group	1. Click the logical operator name 2. Select **Add Group** in the menu
Delete criteria group	1. Click the name of operator criteria group 2. Select **Delete Group** in the menu
Delete all criteria	Click **Clear All** in logical operator menu

3. Click **Apply** and view the filtered results without closing **Filter Editor** screen.
4. Click **OK**.

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.

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.

7.3 Hotkeys

The following table lists the keys and key combinations, used for quick access to various system functions.

Feature name	Hotkeys
Server connection	
Connect to server	F4
Exit Console	Alt+F4
Main screen customization	
Hide/show Navigation bar	Ctrl+Shift+1
Hide/show Details	Ctrl+Shift+2
Hide/show Console log	Ctrl+Shift+3
Management Console sections	
Go to Policies	Ctrl+2
Go to Employees	Ctrl+3
Go to Computers	Ctrl+4
Go to White Lists	Ctrl+5
Go to Signatures	Ctrl+6
Go to Log	Ctrl+7
Go to Tasks	Ctrl+8

Go to Events	Ctrl+9
Manage security schema (overview)	
Go to security schema editing mode	F11
Save security schema	F12
Cancel saving security schema	Shift+F11
Unblock security schema (Superuser only)	Ctrl+Shift+U
Update security schema	F5
Go to the latest security schema version (when viewing an earlier version)	F9
Manage security policies	
Add security policy	Ctrl+N
Edit security policy	Ctrl+E
Delete security policy	Ctrl+D
Manage rules	
Add rule	Ctrl+Shift+N
Edit rule	Ctrl+Shift+E
Delete rule	Delete
Manage employee groups	
Add new employee group	Ctrl+N
Edit employee group	Ctrl+E
Delete employee group	Ctrl+D
Manage employee accounts	
Add employee account to a group	Ctrl+Shift+N
Edit employee account	Ctrl+Shift+E
Remove employee account from a group	Delete
Delete employee account from security schema	Shift+Delete
Manage computer groups	
Add new computer group	Ctrl+N
Edit computer group	Ctrl+E

Delete computer group	Ctrl+D
Manage computers	
Add computer	Ctrl+Shift+I
Remove computer from a group	Delete
Delete computer from security schema	Shift+Delete
Manage white lists	
Add white list	Ctrl+N
Edit white list	Ctrl+E
Delete white list	Ctrl+D
Edit white list entries	Ctrl+Shift+E
Manage signatures	
Add signature category	Ctrl+N
Edit signature category	Ctrl+E
Delete signature category	Ctrl+D
Remove signature from category	Delete
Configure filters for Audit Log and Event Viewer	
Add filter	Ctrl+N
Edit filter	Ctrl+E
Delete filter	Ctrl+D
Manage Client remote installation and upgrade tasks	
Add task	Ctrl+N
Edit task	Ctrl+E
Delete task	Ctrl+D
Add computer to selected task	Ctrl+Shift+N
Remove computer from selected task	Delete
Display target computer error log	Ctrl+L