

INFOWATCH

# Using Device Monitor Management Console

© AO “InfoWatch”

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

http://www.infowatch.com

24.03.2017

TABLE OF CONTENTS


1 Management Console (DM) Overview 5

1.1 Authorization and Connecting to InfoWatch Device Monitor Server 5

1.2 Management Console (DM) Main Screen 7
1.2.1 Configuring Management Console (DM) Main Screen Elements 8

1.3 Management Console (DM) Sections 9

2 Managing Console (DM) Accounts 9

2.1 Viewing Management Console (DM) account details 11
2.1.1 Adding New Management Console (DM) Account 12
2.1.2 Editing Management Console (DM) Account 16
2.1.3 Locking or Unlocking Management Console (DM) Account 17
2.1.4 Deleting Management Console (DM) Account 17

2.2 Roles of DM Console users 17
2.2.1 Adding role of the Management Console (DM) user 18
2.2.2 Editing role of DM Console user 22
2.2.3 Deleting role of DM Console user 22

2.3 Management Console (DM) Security Schema Operation Activity Log 23
2.3.1 Viewing Audit Log 23
2.3.2 Log Records Filtering 25
2.3.3 Deleting Records from Log 30
2.3.4 Exporting Log Records 30
2.3.5 Analyzing Log Records in Microsoft Excel 31

3 General System Settings 31

3.1 Common Settings for Agents 32

3.2 Settings of Corporate Network 34

3.3 Network Traffic Control 37
3.3.1 Processing Addresses Added to Exclusions 39

3.4 Device Monitor Server Settings. Connecting to Traffic Monitor Server 41

3.5 Connecting to LDAP Server and synchronization with Active Directory and Astra Linux Directory 43

3.6 Employee Notifications about Policy (DM) Violations 47

3.7 Exclusion of Application from Interception 50
3.8 Application Control 52
3.9 Event Storage 54
3.10 Synchronization of Traffic Monitor Policies 55
3.11 InfoWatch Device Monitor Server Manager 55
3.12 Stopping and Starting Device Monitor Agent 57
3.12.1 Stopping agent remotely/starting agent 57
3.12.2 Stopping/starting agent locally 59

4 Managing Security Schema 59

4.1 Security Schema Organization 60
4.1.1 Security Policies (DM) and Rules (DM) 60
4.1.2 Employees and Employee Groups 62
4.1.3 Computers and computer groups 63
4.1.4 Uploading security scheme to managed computers 63
4.2 Security Scheme Overview 64
4.2.1 Viewing Active Security Scheme 64
4.2.2 Viewing Old Security Scheme 65
4.2.3 Security Scheme Comments 67
4.2.4 Editing Security Scheme 68
4.2.5 Updating Security Scheme 69
4.2.6 Exporting/Importing Security Scheme 70
4.3 Security Schema Setup 71
4.3.1 Security Policies (DM) 72
4.3.2 Rules (DM) 77
4.3.3 Employees 114
4.3.4 Computers 123
4.3.5 Mobile Devices 135
4.3.6 White Lists 144
4.3.7 Signatures 152
4.3.8 Application Protocol 155
4.4 Temporary employee access to network 160
4.5 Temporary Employee Access to Devices 162

5 Viewing DM Events 164

5.1 Event Filters 172

5.2 Deleting Events 174

6 Agent Remote Installation, Updating and Uninstallation 175

6.1 Viewing Tasks 176

6.2 Preparing Primary Agent Installation. Distribution Agent 179
6.2.1 Enabling Shared Administrative Resources 180
6.2.2 Firewall Settings 180

6.3 Creating Primary Distribution Task 181

6.4 Creating Update Task 185

6.5 Creating Uninstallation Password Reset Task 187

6.6 Creating Uninstallation Task 188

6.7 Launching, Pausing, Editing, and Deleting Tasks 189

6.8 Agent Installation Errors 190

6.9 Creating Installation Package 191

7 Additional Features 194

7.1 Filter Table Contents 194
7.1.1 Filtering by Date 194
7.1.2 Applying Standard Filters 195
7.1.3 Custom Filter 196
7.1.4 Editing Filters 197
7.1.5 Removing a Filter 198

7.2 Grouping or Sorting Entries 198

7.3 Hotkeys 199

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

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

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

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

# 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").

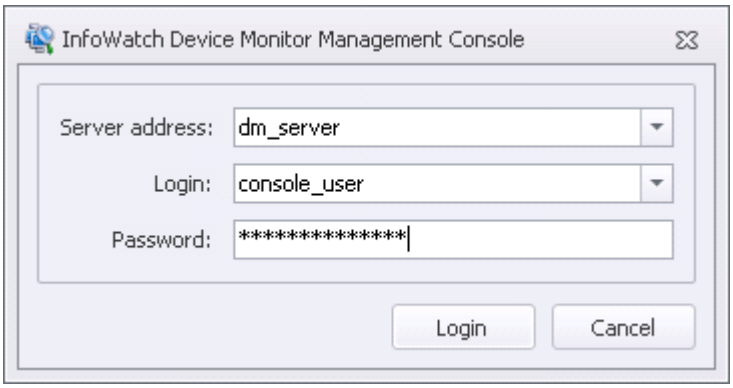
To start working with DM Management Console:

1. Start the Management Console (DM). For this, in the **Start** menu, choose **Programs** > **InfoWatch** > **Device Monitor** > **Management Console** or use the desktop shortcut (created by default during installation)..
2. Perform the authorization procedure as described below.

For successful authorization, the following conditions should be met:

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

Enter the data for authorization in the connection dialog box.



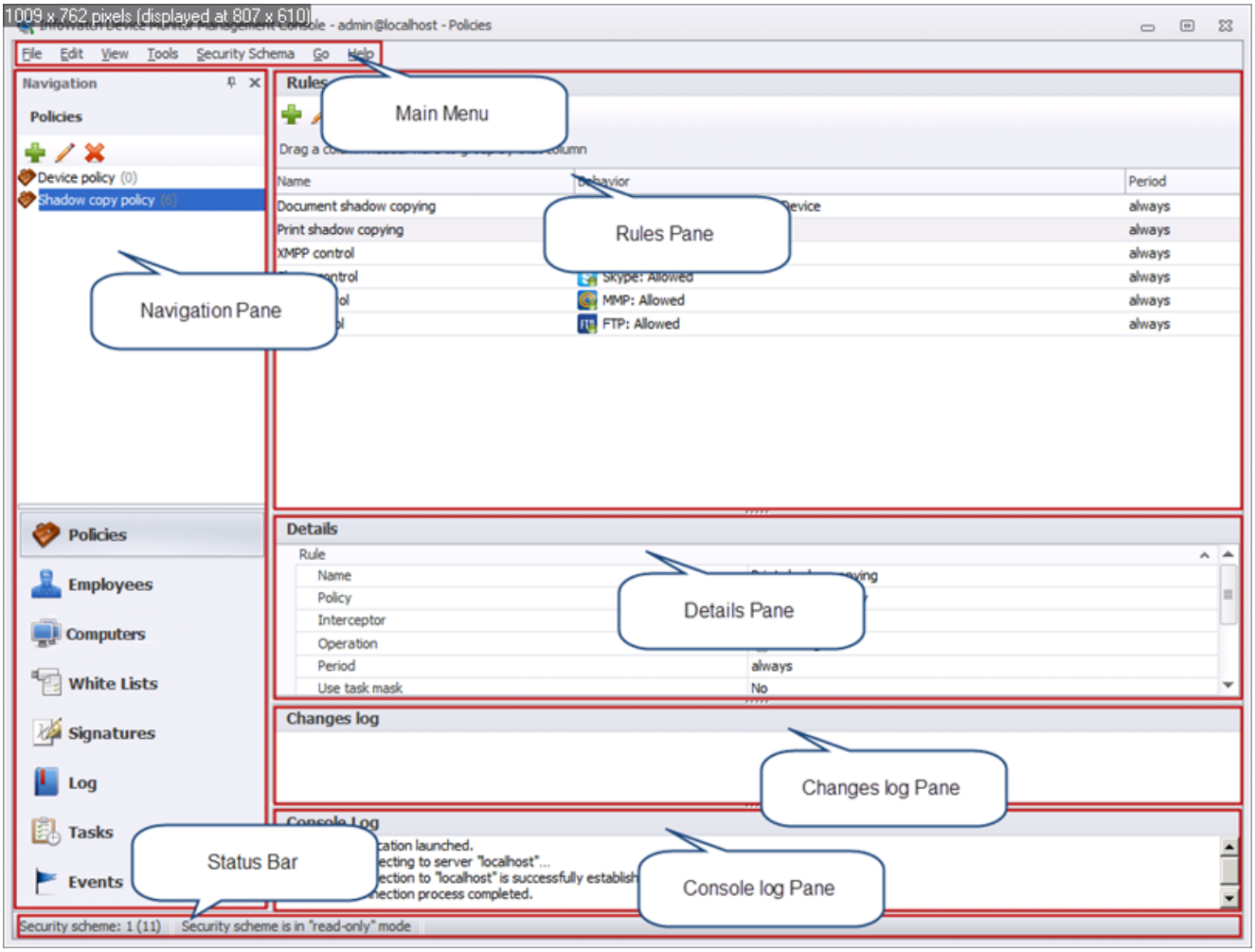

| Parameter | Description |
|---|---|
| Server address | FQDN of the server, the Management Console is connecting to.<br>Th default port for communication between the server and Management Console is 15003. If this port has been changed, enter the server address as follows: `dm_server:port` |
| Login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

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

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

# 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.<br>**Note:** To delete the Navigation pane, you can also use button in the upper right corner of the pane. |
| Enable/disable pane automatic collapse | Click in the upper right corner of the pane. |
| Change pane location | Click on the pane name and drag the pane to a new location. Release the button to place the pane. |
| Return the pane to its original position | Double-click the title bar |
| Change panel size | Move the pointer to the edge of the panel. When the pointer turns into a double arrow, click and hold to drag the margin into the right direction. Release the button when the size is right. |

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 the double-arrow button in the right part of the properties table header.

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

## 1.3 Management Console (DM) Sections

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

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

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

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

# Managing Console (DM) Accounts

For each user who manages the security scheme, an account is created in the Management Console (DM). The account details are used for the authorization in the System and define permission for particular actions.

The Management Console (DM) contains a pre-installed user - **Superuser**, who has permissions for all operations in the Console. This user is intended not for everyday operations, but for initial configuration of the Management Console (DM), creating the Administrator account and then only in case of emergency.

To define privileges of users working in the Management Console (DM), roles are used. One user can have several roles for different groups. For each role, a set of privileges is defined.

The Management Console (DM) has the following preset roles:

- **Administrator** - a role for Console (DM) administrator who manages other Console accounts.
- **Security officer** - a role of Console (DM) end user who manages the security scheme and server settings.
- **Security officer of the group** - a role of Console (DM) end user who manages groups of employees and computers. сотрудников или компьютеров.

You can add custom roles based on preset ones and specify required settings for them (see "Adding role of the Management Console (DM) user").

The list of available actions for preset roles:

| Action | Administrator | Security officer | Security officer of the group |
|---|---|---|---|
| Viewing audit log | | + | |
| Export audit log records | | + | |
| Deleting audit log entries | | | |
| View Management Console accounts information | + | + | |
| Add, edit, delete Management Console (DM) accounts | + | | |
| Assign/delete Management Console account roles | + | | |
| Block/unblock Management Console accounts | + | | |
| Viewing Device Monitor Server settings. Configuring connection to Traffic Monitor server | | + | |
| View security schema versions | | + | |
| Edit security schema | | + | |
| Import/export security policies and rules | | + | |

| Action | Administrator | Security officer | Security officer of the group |
|---|---|---|---|
| Viewing events | | + | |
| Agents Remote Installation, Updating and Uninstallation | | + | |
| Temporary Employee Access to Network | | + | |
| Temporary Employee Access to Devices | | + | |
| Creating group | | | + |
| Viewing and managing employee groups, Viewing and managing computer groups, Viewing events for a group | | | + |
| Viewing and managing whitelists | | | + |
| Managing agents | | + | + |

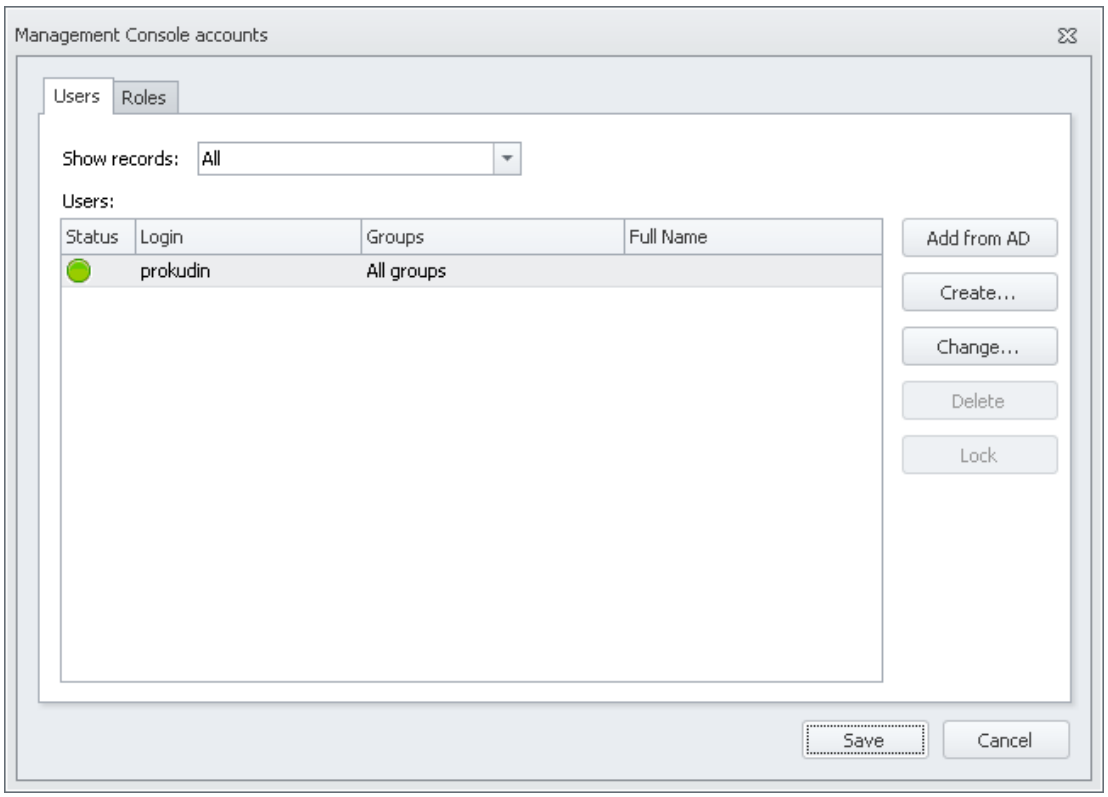
For more information on Management Console (DM) accounts management, see:

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

# 2.1 Viewing Management Console (DM) account details

To view information on the Management Console accounts:

1. In the Main Menu, click **Tools > Console users and roles**. This opens **Management Console accounts** dialog box, **Users** tab.




2. There is **Show records** field at the top of the dialog box. Select displayed accounts type in from the drop-down list:
    - **All**. All accounts regardless of their status.
    - **Active**. List of all active accounts.
    - **Blocked**. List of blocked accounts which can be unblocked (see "Locking or Unlocking Management Console (DM) Account").
    - **Deleted**. List of deleted accounts which cannot be restored. However, the System saves information about actions those users performed.

> **Note:**
>
> Management Console (DM) can be only operated by accounts from the **Active** list. Deleted accounts can only be viewed.

For each entry, the following attributes are displayed:

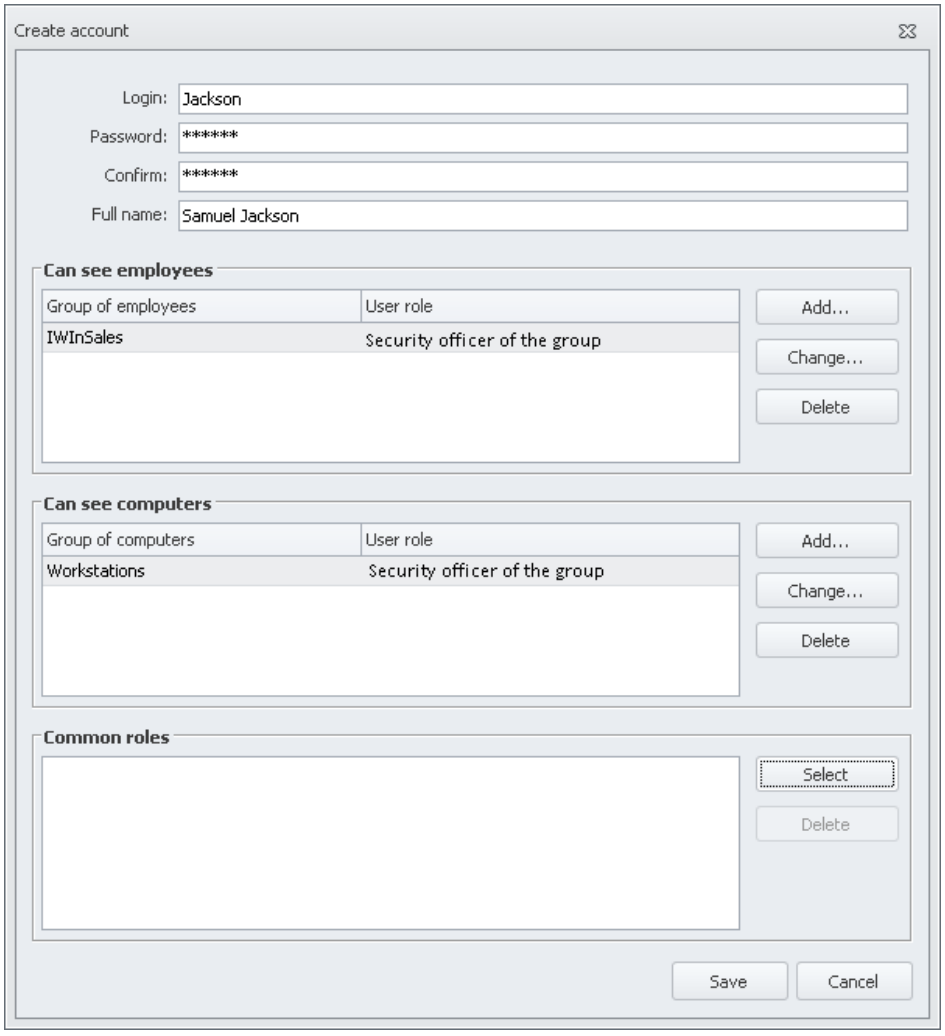
- **Status**. Indicates if the account is active ( ), blocked ( ) or deleted ( ).
- **Login**. Name of the user account.
- **Groups**. Groups available to the user.
- **Full Name**. User's personal data.

Login, password, role, and status are mandatory attributes. For a detailed description of roles, see "Roles of DM Console users".

## 2.1.1 Adding New Management Console (DM) Account

**To add a new Management Console account:**

1. In the Main Menu, click **Tools > Console Accounts and Roles**.
2. Click **Create** at the right of **Management Console Accounts** dialog box.
3. Specify account settings in the **Create account** dialog box:
   - **Login**. Name of the user account.
   - **Password**, **Confirm**. Account password.
   - **Full name**. User's first and last name.




4. Specify visibility of employees and computers for the user (see "Assigning roles to user").
   - **Can see employees**. The list of employee groups available to the user and their roles;
   - **Can see computers**. The list of computer groups available to the user and their roles .
   - **Common roles**. The list of additional user roles.

> **Important!**

At least one role of any type and a role for each available group must be assigned to the user.

5. Click **Save**.
   The **Create account** dialog box will close. Details of the new account will be displayed in the **Management Console Accounts** dialog box.

> **Note:**
>
> The new account status is active. You can lock the account, if necessary (see "Locking or Unlocking Management Console (DM) Accountt").

**To add a user from Active Directory or ALD:**

1. In the main menu, select **Tools > Console Accounts and Roles**.
2. Click **Add from AD** button.
3. In the **Adding user from AD** dialog box, select a user from a group (or use the search field).
4. Assign roles to the added user (for details, see "Assigning roles to user").
5. Click **Save**.

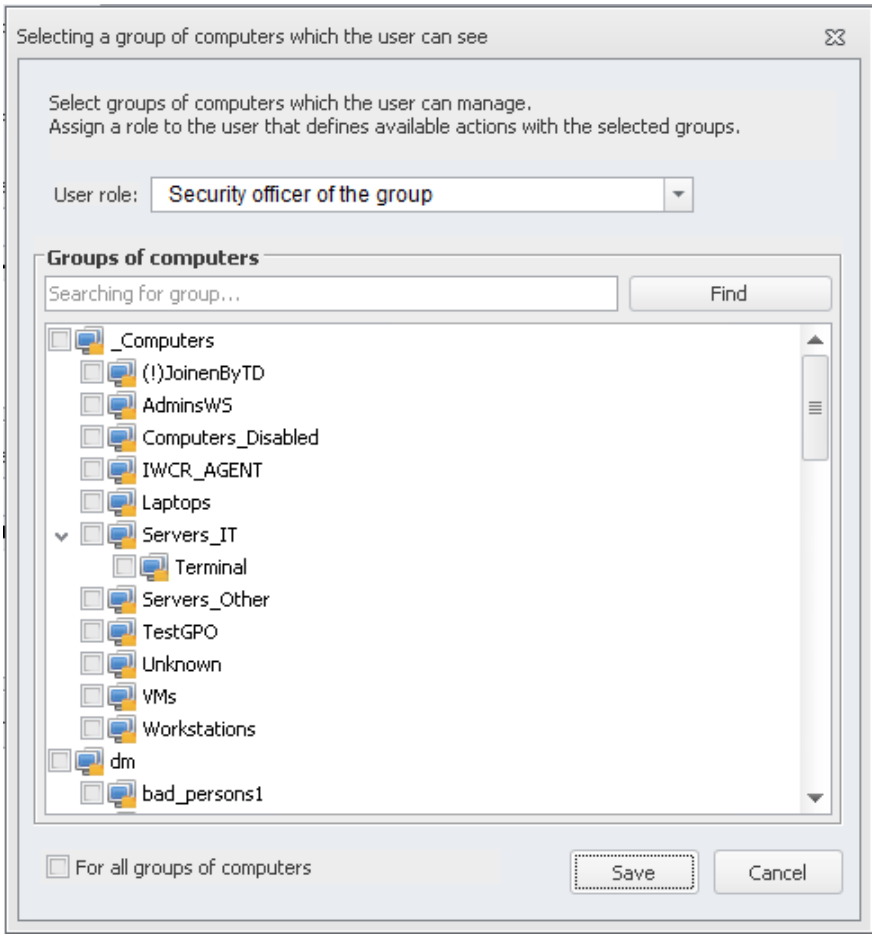
> **Note:**
>
> The login and full name that are displayed in the **Management Console Accounts** dialog box for the imported user will be filled automatically. The password matches the user password in AD.

## Assigning roles to user

**Adding a user role for groups of employees (computers)**

To add a group of employees to the user's visibility scope:

1. Open the **Creating user** (or **Editing user**) dialog box.
2. In the **Can see employees** (**Can see computers**) block, click **Add**.




3. In the window that opens:
    - Specify **User role**;
    - Select one or more groups of employees (or computers) from the tree structure or use the search field. Select **For all user groups** (**For all computer groups**) if you need to add all groups.
    - Click **Save**.
4. In the **Editing user** window, click **Save**.

### Editing a user role for groups of employees (computers)

To change access permissions to the user's visibility scope:

1. Open the **Editing user** dialog box.
2. In the **Can see employees** (**Can see computers**) block, select the required group.
3. Click **Edit**.
4. In the window that opens, assign a role that defines user actions with the group. Further actions with employees (computers) will be performed according to the role privileges.
5. Click **Save**.

To remove a user role:

1. Open the **Editing user** dialog box.
2. In the **Can see employees** (**Can see computers**) block, select the required group.
3. Click **Delete.**
4. Click **Yes** for confirmation. The selected role will be removed from the user.

**Configuring user common roles**

To assign common roles to the user:

1. Open the **Creating user** (or **Editing user**) dialog box.
2. In the **Common roles** block, click **Select**.
3. In the window that opens, select roles that determine actions available to the user.
4. Click **Save**.

To remove common user roles:

1. Open the **Editing user** dialog box.
2. In the **Common roles** block, select the role you want to remove.
3. In the window that opens, click **Delete**. The common role will be removed from the user.

## 2.1.2 Editing Management Console (DM) Account

> **Warning!**
>
> If you edit a role that is currently authorized in the Management Console (DM), then after saving changes, connection with the server is automatically terminated. Then the user has to be authorized with new parameters. All unsaved changes will be lost.

**To edit parameters of the Management Console account:**

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

> **Important!**

For pre-installed users, you can only change a password.

### 2.1.3 Locking or Unlocking Management Console (DM) Account

Information about locked accounts is displayed in the **Management Console Accounts** dialog box.

> **Warning!**
>
> You can lock any account except Superuser and the account you are logged in with.
>
> You cannot log in with a locked account.

**To lock/unlock Management Console account:**

1. In the Main Menu, click **Tools > Management Console Accounts and Roles**. The **Management Console Accounts** dialog box will open.
2. Select a row that contains the account name.
3. Change the locking status:
   - if the account is locked (  state), click **Unlock**.
   - if the account is unlocked (  state), click **Lock**.
4. Click **Save** to apply changes.

### 2.1.4 Deleting Management Console (DM) Account

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

> **Warning!**
>
> Accounts for Superuser and preset users cannot be deleted.
> Deleted accounts cannot be restored.

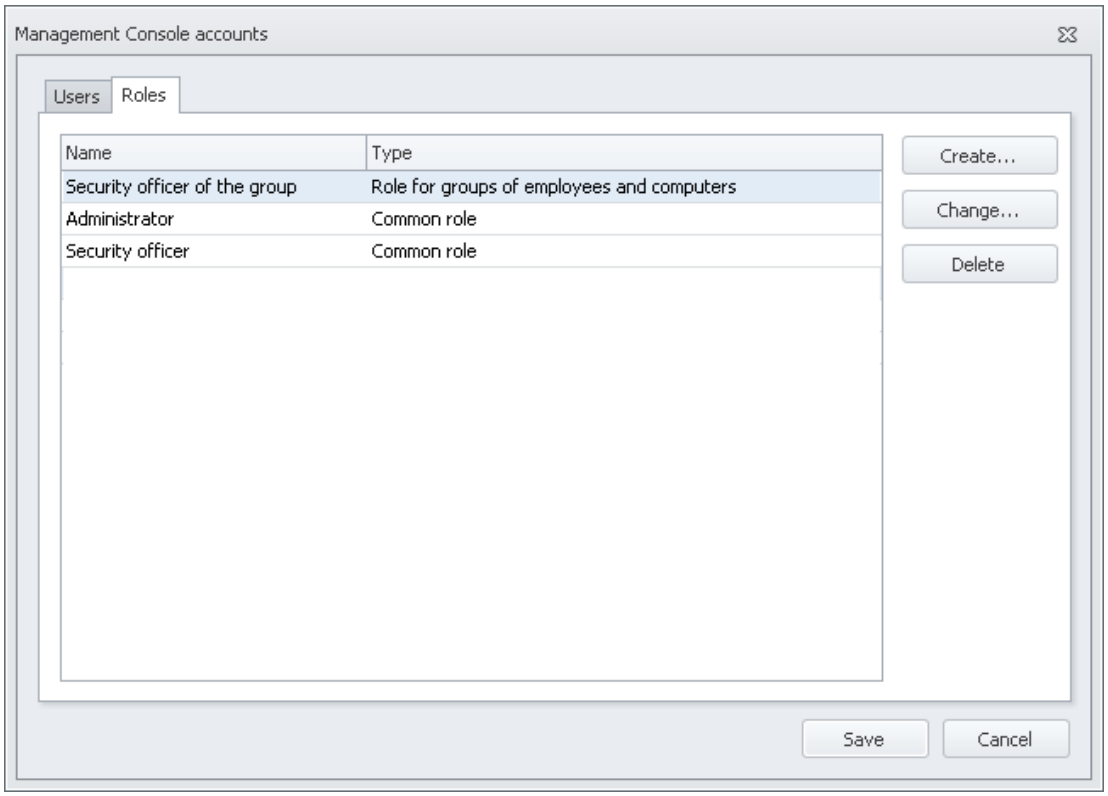
**To delete Management Console account:**

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

# 2.2 Roles of DM Console users

**To view information about role of Console users:**

1. In the main menu, select **Tools** > **Console users and roles**. The **Management Console accounts** dialog box will open.
2. Open the **Roles** tab.




3. The tab contains a table with information on roles with the following attributes:
   - **Name**.
   - **Type**. Possible values:
     - **Role for groups of empoyees and computers** - includes permissions (privileges) for actions with groups of employees or computers.
     - **Common role** - includes permissions (privileges) for common actions in the Console.

For a detailed description of privileges, see "Adding role of the Management Console (DM) user".

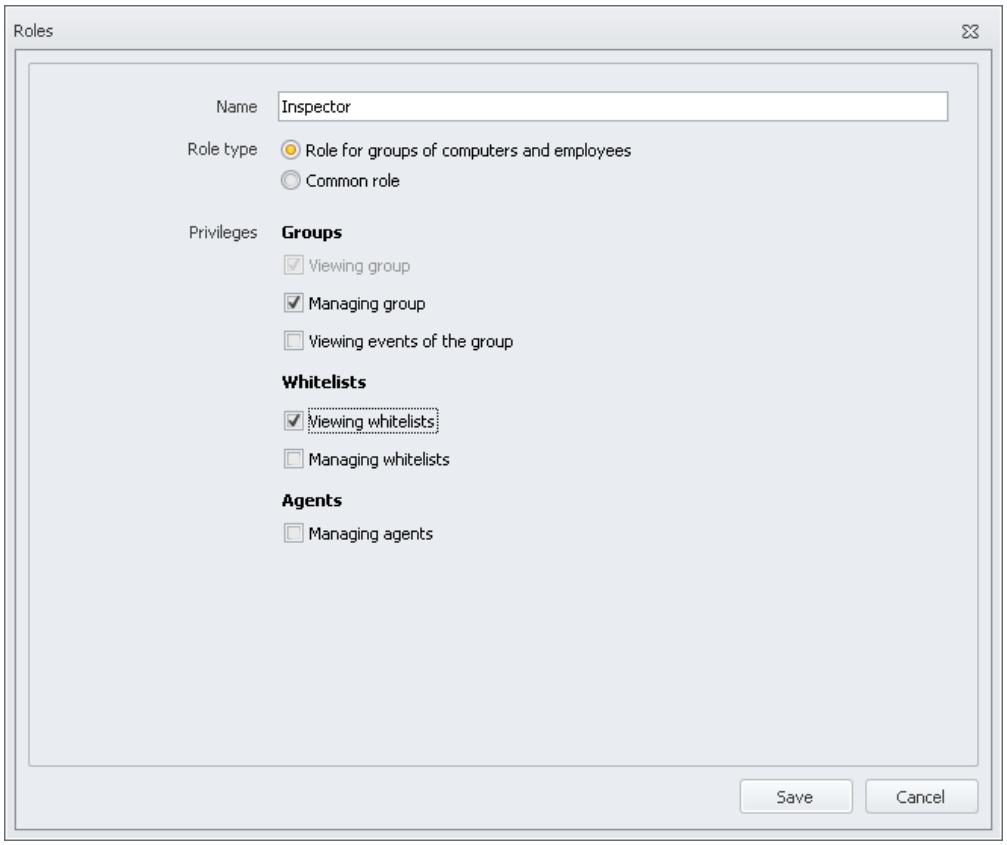
## 2.2.1 Adding role of the Management Console (DM) user

**To add a role for the Management Console user:**

1. In the main menu, choose **Tools** > **Console Users and roles**.
2. Open the **Roles** tab.
3. Click **Create**.

4. In the window that opens, specify parameters of the role:
    - **Name**
    - **Role type**
    - **Privileges**

> **Note:**
>
> A set of available privileges depends on the role type.




5. Click **Save**.
6. The **Creating role** dialog box will close. Information on the new role will appear on the **Roles** tab of the **Management Console Accounts** dialog box.

### User privileges

In Device Monitor Management Console, privileges are actions that the user can perform with:

- a group of employees or computers;
- the whole System (common privileges).

### Privileges for groups of employees/computers

| Privilege | Available actions |
|---|---|
| *Groups* | |

| Privilege | Available actions |
|---|---|
| View group | • View the group in the list of groups<br>• View the group parameters<br>• View the list of computers/employees included in the group<br>• View the effective policy for the computer/employee<br>• View all subgroups of the group |
| Manage group | • Edit group parameters (including the policy assigned to the group; the policy should be available to the user with at least read-only permissions)<br>• Add/delete computers/employees of the group<br>• Copy computers, employees or subgroups of the group<br>• Manage all subgroups of the group<br>• Delete groups |
| View group events | View events received from workstations/employees of the group and its subgroups |
| *Whitelists* | |
| View whitelists | View whitelists related to the group and its subgroups |
| Manage whitelists | Create/edit/delete whitelists for the group and for computers/employees included in the group |
| *Agents* | |
| Manage agents | Add workstations from the group and its subgroups to the tasks to updating/deleting agents or changing the uninstallation password.<br>**Important!** This privilege is not sufficient to create a distribution task for installing DM agent on workstations. To install DM agent on workstations included in the group, the user should also have the **Manage agents on separate computers** privilege |

## Common privileges

| Privilege | Available actions |
|---|---|
| *Policies* | |
| View all policies | View all System policies available for reading and editing and their rules |

| Privilege | Available actions |
|---|---|
| Manage all policies | • Edit all System policies (irrespective of the policy owner and access level) and their rules<br>• Create new policy<br>• Delete policy (available only to the owner) |
| Manage available policies | • Edit policies that are available to the user (policies owned by the user and policies that are available for editing to all users)<br>• Create new policy<br>• Delete policy (available only to the owner) |
| *Other privileges* | |
| Create groups | Create new groups of computers or employees |
| View audit log | Access to the "Log" section |
| Delete log entries | Delete entries from the audit log, clear the audit log |
| Manage users | View/create/edit/delete Console users and roles |
| Manage agents on separate computers | • Add computers from the network environment and through connection to AD or ALD in the agent distribution task<br>• Add computers through the file import or by name/IP<br>• Create installation package<br>• Delete agent from a mobile device |
| Manage settings | Manage global DM settings (excluding "Integration with AD" section) |
| Sync with AD | Configure synchronization of workstations and employees with AD or ALD |
| Import/export of configuration | Import and export the security scheme and settings<br>**Important!** This privilege allows the Console user to import and export the configuration regardless of the user permissions for imported/exported objects |
| Provide temporary access | Provide temporary access to the network or devices on the employee request |

## 2.2.2 Editing role of DM Console user

> **Important!**
>
> If you edit a role that is currently authorized in the Management Console (DM), then after saving changes, connection with the server is automatically terminated. Then the user has to be authorized with new parameters. All unsaved changes will be lost.

To edit parameters of the Console user role:

1. In the main menu, choose **Tools** > **Console users and role**. The **Management Console Accounts** dialog box will open.
2. On the **Roles** tab, select a row with the role you want to edit.
3. Click **Edit** or double-click the selected row.
4. In the **Roles** window that opens, edit the role parameters (the parameters are described in "Adding role of the Management Console (DM) user"). The role type cannot be changed.
5. Click **Save**.
6. To apply changes, click **Save** in the **Management Console Accounts** dialog box.

> **Important!**
>
> Pre-installed roles (Administrator, Security officer, and Security Officer of the group) cannot be edited.

## 2.2.3 Deleting role of DM Console user

**To delete a role of the Console user**:

1. In the main menu, choose **Tools** > **Console users and role**. The **Management Console Accounts** dialog box will open.
2. On the **Roles** tab, select a row with the role you want to delete.
3. Click **Delete** in the right part of the window.
4. In the confirmation window, click **OK**.

   > **Important!**
   >
   > A role assigned to a user cannot be deleted. To delete the role, you should remove it from all users.

5. To apply changes, click **Save** in the **Management Console Accounts** dialog box.

# 2.3 Management Console (DM) Security Schema Operation Activity Log

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

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

## 2.3.1 Viewing Audit Log

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

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

**To view a full list of audit log records,** click **Show All Records** at the top of Navigation Pane.

**To view filtered records,** click the filter name in the filter list.

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

**To view advanced information for a particular record,** select the row that contains the record name in the main screen workspace.

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

| Property | Description |
|---|---|
| Transaction number (#) | Transaction number |

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

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

**For example:**

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

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

Transaction number 3 is associated with adding a comment to security schema.
Transaction number 4 corresponds to one change applied to a security schema. This was done in 9 steps. Steps 1-3 changed rule (DM) named "New IM client rule" in "Test Policy" security policy (DM). Each step configures a single rule (DM) parameter: for example, in step 1 an operation was defined,

in step 2-3 an action period was set. Steps 4-7 added a new rule (DM), step 8 deleted another one. In step 9 a comment was added to saving security schema version.
Transaction number 5 is associated with Audit Log records export. This transaction includes one step.

## Selector Values

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

**Example 1**
Audit Log includes the following record:

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

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

**Example 2**
Audit Log includes the following record:

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

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

**Example 3**
Audit Log includes the following record:

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

This record indicates that audit log records were exported.
*Selector value interpretation*
All records for operation on policy and rules were exported during this transaction.

## 2.3.2 Log Records Filtering

To access audit log records that meet certain criteria, you can use filters.

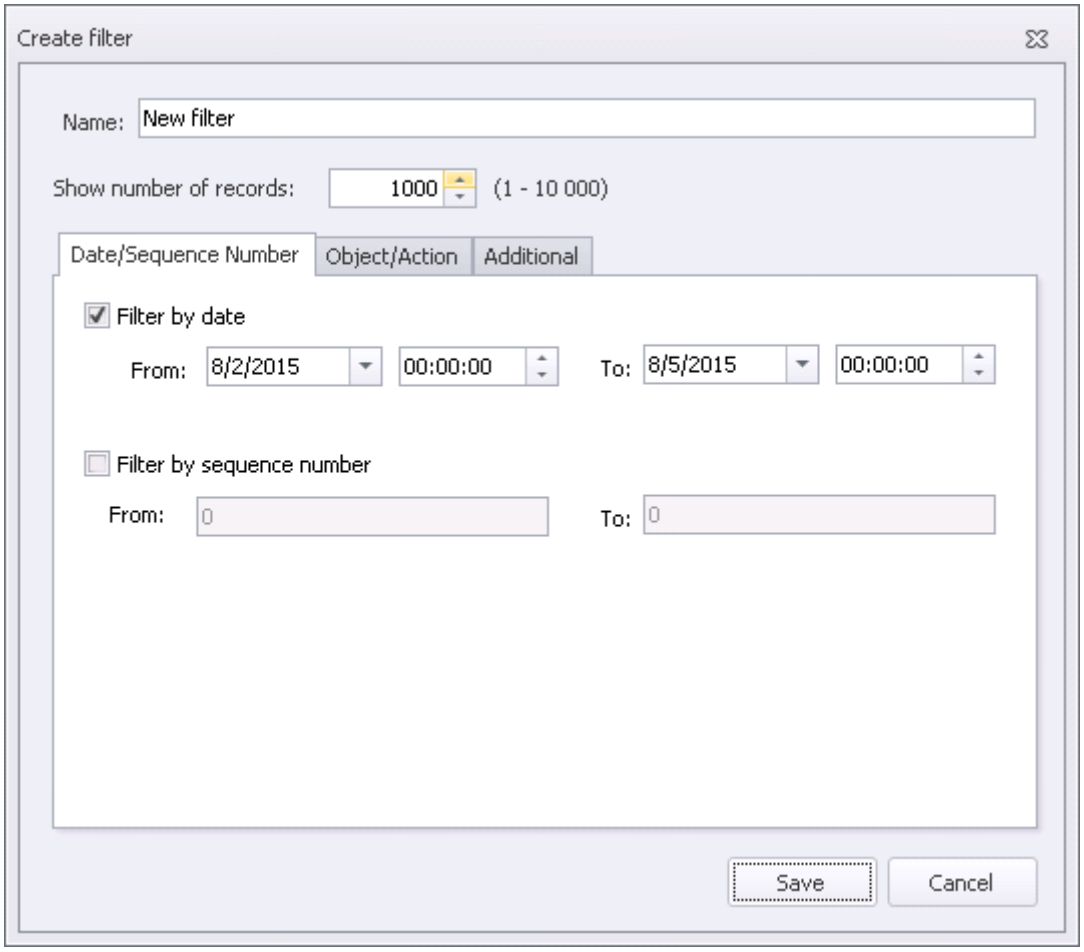
**To create a new filter or modify an existing one:**

1. Go to **Log** section.

2. Perform the following steps:

| Action | Steps |
|---|---|
| Creating filter | • in Main Menu, select **Edit > Create Filter**;<br>• click **Create filter** at the top of Navigation pane;<br>• right-click in the **Log** area and choose **Create Filter** from the context menu;<br>• press Ctrl+N. |
| Editing filter | a. In **Log** area of Navigation pane, select the name of the filter you want to edit.<br>b. Take one of the following steps:<br>• In Main Menu, click **Edit > Edit filter**;<br>• click **Edit Filter** at the top of Navigation pane.<br>• double-click with the left mouse button on the name of the chosen filter;<br>• right-click the selected filter and choose **Edit** from the context menu;<br>• press Ctrl+E. |

These actions open dialog with filter parameters configuration.



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

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

5. Click **Save**.

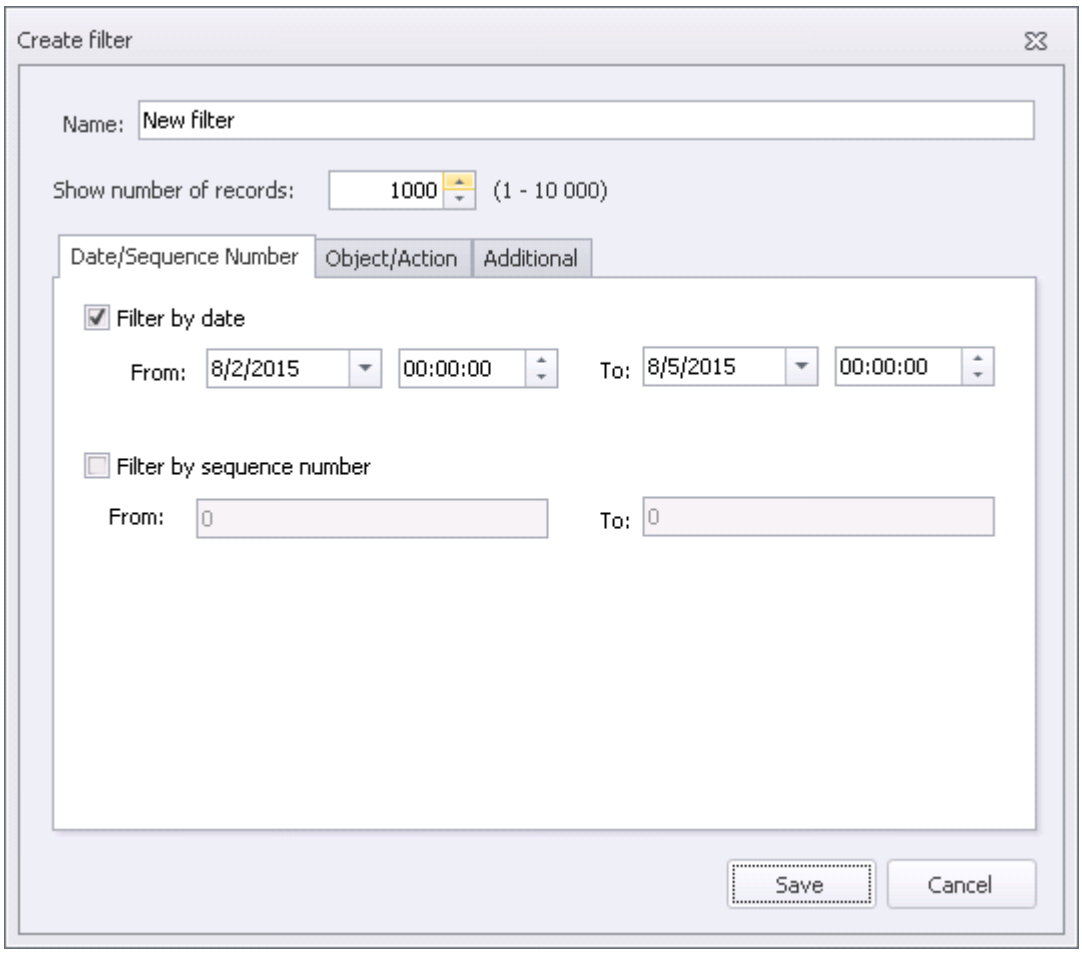
**To remove filter:**

1. Go to **Log** section.
2. In the **Log** area of Navigation pane, select the name of the filter you want to remove.
3. Take one of the following steps:
    - in the Main Menu, select **Edit > Delete Filter**;
    - click  **Delete Filter** at the top of Navigation pane;
    - right-click the selected filter and choose **Delete** from the context menu;
    - press Ctrl+D.
4. In the confirmation dialog, select **Yes** to confirm the deletion.

## Date/Sequence Number Tab

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

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




**To specify date and time criteria:**

1. Flag **Filter by date** check box.
2. Specify the desired period.
   Starting and ending time is specified in **From** and **To** fields respectively. Set the date and time in right and left field respectively.

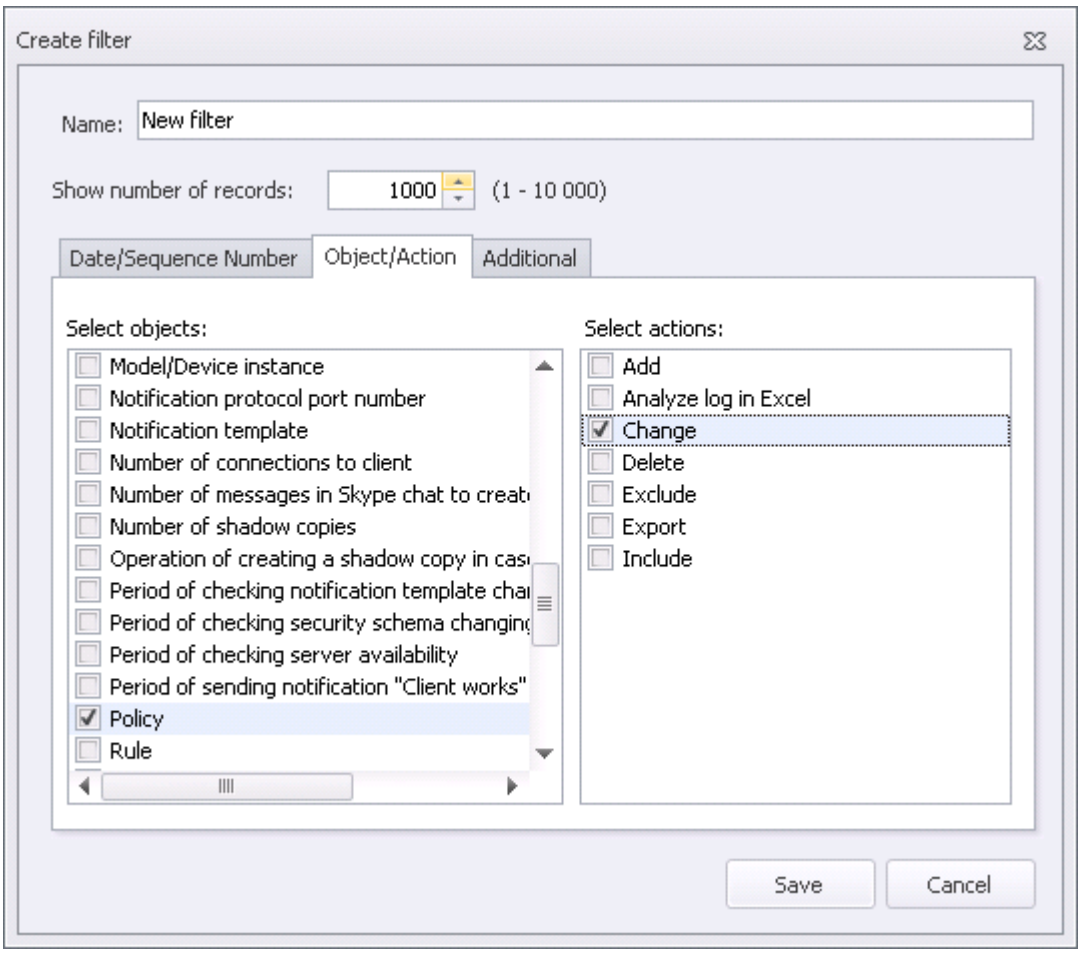
**To filter by number:**

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

## Object/Action Tab

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

- target object;
- action performed with an object.




**To specify filtering criteria:**

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

## Additional Tab

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

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

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

> **Note:**

Additional filtering values are not case-insensitive.

### 2.3.3 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**.

### 2.3.4 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**;
   - right-click in the **Records** area and choose **Export Log** from the context menu.
4. In the next dialog, specify the target file name, type, and directory.
5. Click **Save**.

Now, the audit log records are exported to the selected file.

### 2.3.5 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.

# General System Settings

The System has a set of global settings that should be general for all active policies and rules in Device Monitor system. You can configure these settings from **Tools > Settings** menu. For more information, see the following articles:

- Common Settings for Agents
- 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
- InfoWatch Device Monitor Server Manager

**Warning!**

Modified settings will apply on controlled computers after Agents at every computer receive notification from the Server (when checking server availability or when checking security scheme changing or when checking notification templates changing) and then Agents will be updated.

# 3.1 Common Settings for Agents

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

**To configure common settings for Device Monitor agents operation:**

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

| Parameter | Description |
|---|---|
| **Connection** | |
| Period of sending notification "Agent works" to the server | Interval (sec) with which the Agent sends data to Server |
| Period of checking server availability | Interval (sec) with which the Agent checks Server availability. |
| Period of checking security schema changing for active agent only | If a Agent is in active mode (i.e. computer could not open UDP-port for receiving Server notifications) then the Agent 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 agent only | If a Agent is in active mode (i.e. computer could not open UDP-port for receiving Server notifications) then the Agent surveys Server itself to receive data on changing notification templates (see "Employee Notifications about Policy (DM) Violations"). This parameter sets a survey period (sec). |
| **Agent's disk space control** | |

| Parameter | Description |
|---|---|
| Free agents' 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 a shadow copy is created, free disk space at the agent computer is less then parameter value, then neither shadow copy nor its part won't be created. See details in "Creating Shadow Copies and Blocking Operations Due to Free Space Shortage" |
| If there is not enough space for events | The managed computer dedicates space for storing 30000 events at the hard drive where Device Monitor Agent is installed. If Device Monitor Agent did not have connections with Device Monitor Server so that there is stored more than 30000 events controlled by rules (DM) defined for employee/computer, then any actions controlled by security schema could be denied. **To deny**, select Operation will be blocked. To allow all actions performed without a control, select **Operation will be permitted**. |
| **Speed of sending data from agent** | |
| Limit the speed of sending data | If the channel is narrow you can prevent its excessively uploading by adjusting the speed of shadow copies sending to the Server. To do this check the setting and specify the upper-speed limit (Kbps) in **Maximum speed of sending** data field. |
| **Events** | |
| Log events of device and cloud storage interceptors | Level of detailing when saving information about working with external devices received by Device Monitor and Cloud Storage Monitor interceptors: see details in "Configuring Device Monitor Rule (DM)", "Configuring Cloud Storage Monitor Rule (DM)", "Viewing Events". The following options are available:<br>• **None** - do not save events<br>• **In case access denied** - events are created only if security policy (DM) violation is attempted - i.e. when device usage was denied, including blocking attempts of access level exceeding. The using of external devices which are not forbidden by policies, is not logged<br>• **All** - all actions are logged (connection/usage of any devices, even from white lists) |
| Log connections outside of corporate network | Level of detailing when saving information about data transfer by network connections received by Network Monitor interceptor: see details in "Configuring Network Monitor Rule (DM)". The following options are available:<br>• **None** - do not save events<br>• **In case access denied** - events are created only if security policy (DM) violation is attempted - i.e. when connection attempt was denied. |
| **Agent activity on computer** | |
| Show employee notifications | Indicates if employee attempting to perform action forbidden by security policy (DM), would receive a warning message. See details in "Employee Notifications about Policy (DM) Violations" |
| Hide Agent presence | |

| Parameter | Description |
| --- | --- |
| | Indicates if Windows system tray of managed computer hides Agent presence on the computer.<br>If this option is not selected, the Windows system tray of the computer where the Agent is installed will display  icon. Clicking this icon displays information on DM Agent operation and the list of currently controlled devices.<br>**Warning**! If there is an antivirus protection enabled on the managed computer then the antivirus program can reveal the operation of Device Monitor: for example, in the list of processes running on the managed computer or in the list of programs that initiate a control. |
| **Code generating key** | |
| **Update** | Click Update to make the System generate a new key used to make codes of removing network connections or devices access prohibition. See details on codes in "Temporary Employee Access to Network" and "Temporary Employee Access to Devices", Request code and Confirmation code settings. The frequent key refreshment is not recommended. |

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

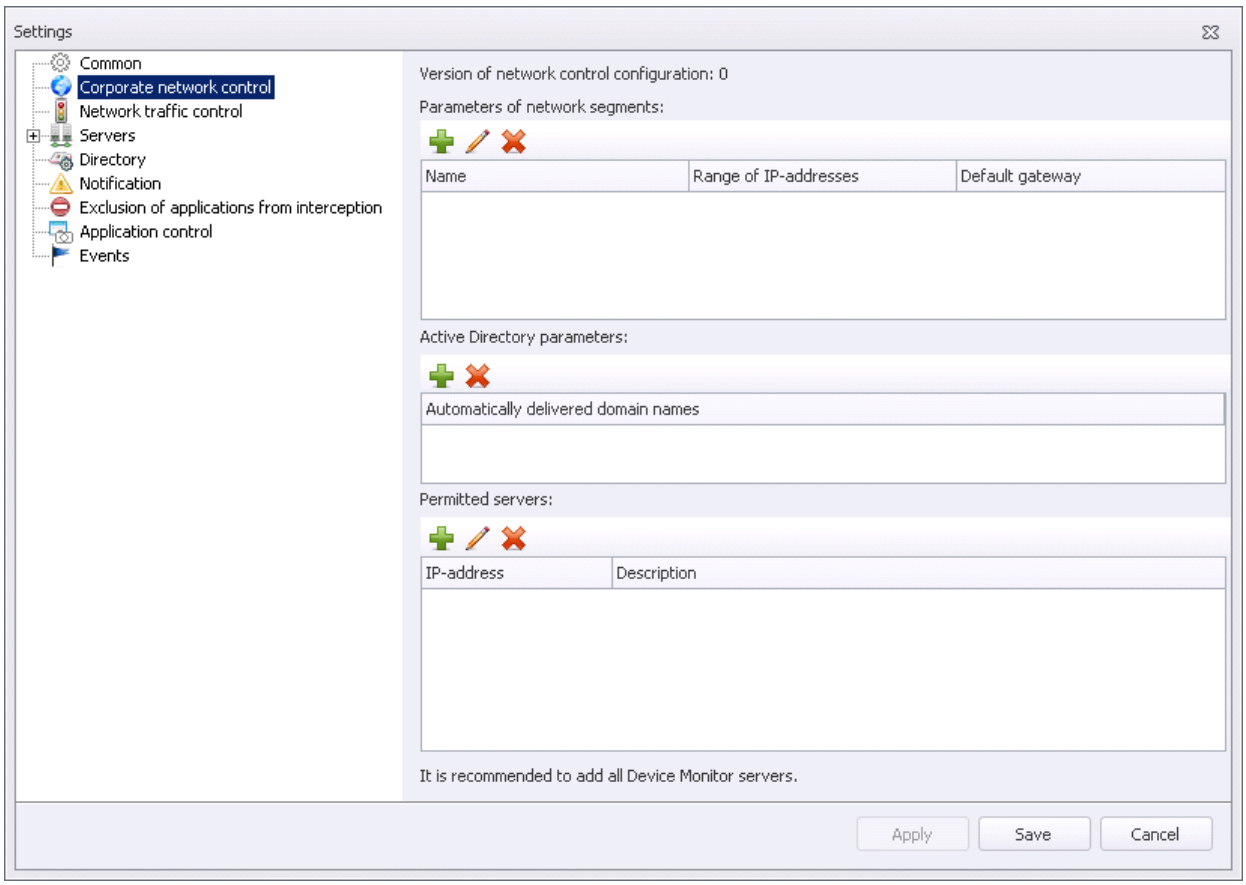
# 3.2 Settings of Corporate Network

In order to provide control of data transfer by network connections with **Network Monitor** (information on configuring the rule (DM) 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 Agent is outside corporate network: for example with VPN server or corporate network.

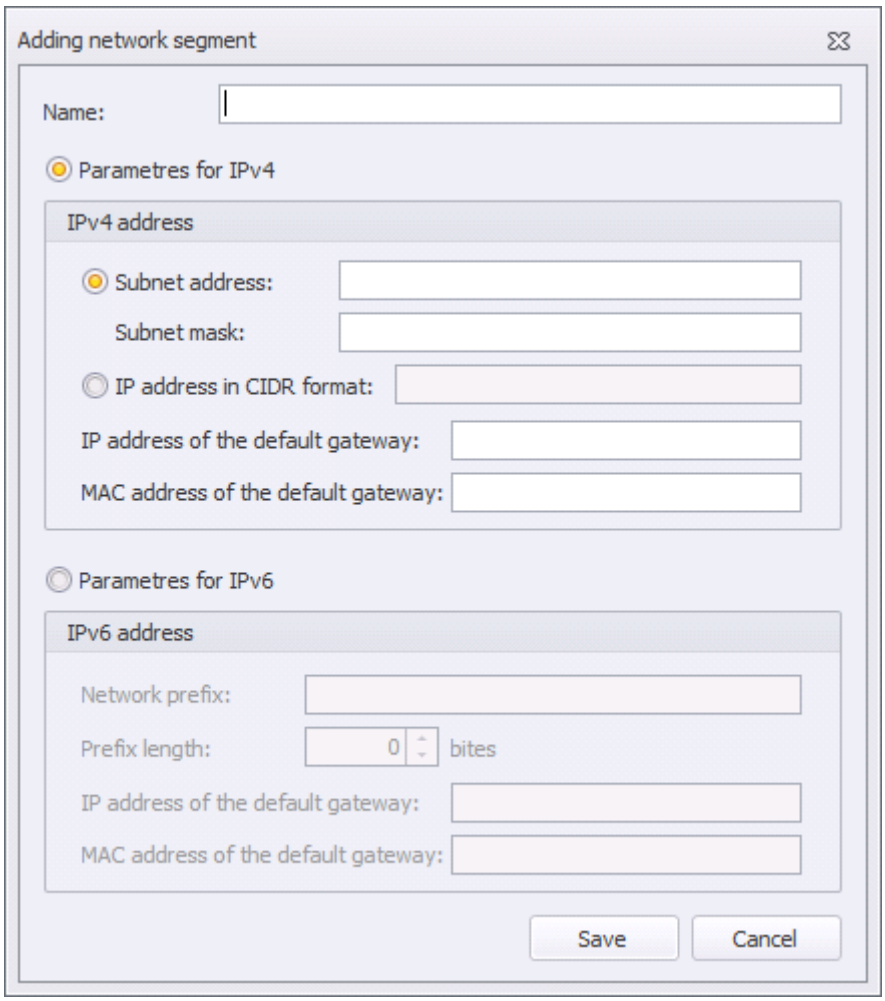
**To configure corporate network settings**:

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 (or press Ctrl+Shift+S). This opens **Adding network segments** dialog.




b. Specify segment's name (description).

c. Select protocol in use: **IPv4** or **IPv6**.
If you 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 other segments.
To change segment parameters, select it from the list in **Parameters of network segments** area and click (or press Ctrl+E).
To delete a segment from the list, select it, click (or press **Delete**), then click **Yes** in the confirmation dialog.

> **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  (or press Ctrl+E).
    To delete a server from the list of permitted ones, select it, click  (or press **Delete**), then click **Yes** in the confirmation dialog.
6. To apply changes, click **Apply**.

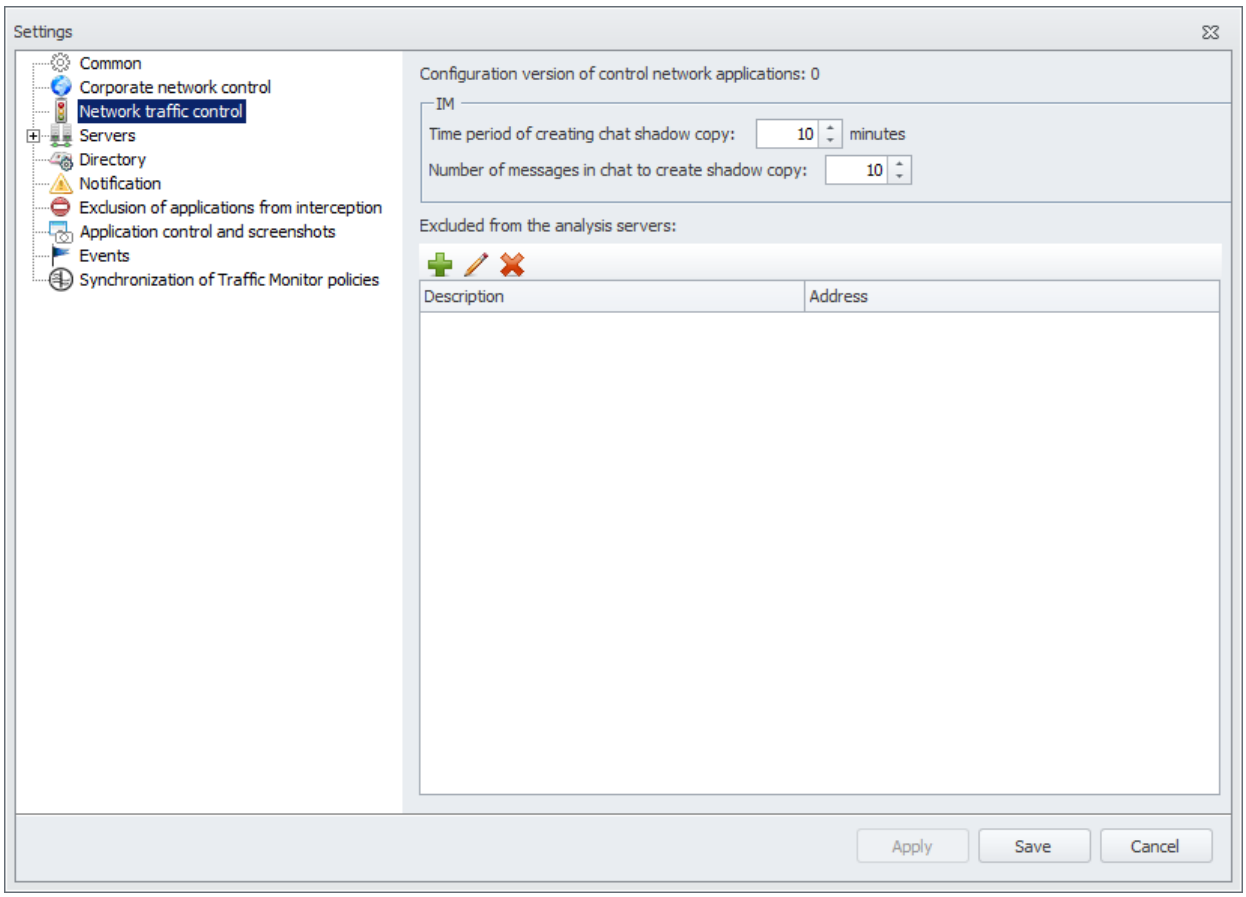
# 3.3 Network Traffic Control

In order to provide control of network traffic, Device Monitor Agent acts as a transparent proxy server, to which all the connections are redirected irrespective of the protocol. Then Device Monitor Agent parses the protocol and defines if this protocol is a subject of interception. Controlled protocols are FTP, FTPS, POP3, SMTP, IMAP, HTTP, HTTPS, XMPP, and MMP. If a data stream is protected with TLS\SSL protocol, then the proxy server decrypts the traffic and defines if this stream should be controlled.

When configuring the traffic control, you can specify additional parameters for instant messanger (for more information about configuring rules (DM) for this control type, see "Configuring IM Client Monitor Rule (DM)") , mail systems (see "Configuring Mail Monitor Rule (DM)"), and FTP/FTPS taffic (see " Configuring FTP Monitor Rule (DM)"). Besides, you can define servers excluded from interception: traffic sent to these servers should not be controlled.

To configure network traffic control settings:

1. In the main menu, select **Tools > Settings**.
2. At the left panel, select **Network traffic control** node.




3. Specify control parameters for messengers: 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)".
4. You can specify a list of server IP addresses which protocols won't be controlled - i.e. traffic sent to those servers won't be redirected 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.

> **Note:**
>
> For agents installed on Astra Linux, only traffic sent to the server through SSL protocol is excluded from analysis.

5. To set a list of servers excluded from analysis:
   a. In **Excluded from the analysis servers** area, click .
   b. In **Add server to the list of excluded from the analysis** dialog, specify DNS name or IP address of a server and server description. For more information on addresses that can be added, see "Processing Addresses Added to Exclusions".
   c. Click **Save**.
   d. Repeat for other permitted addresses.
   e. To change the server parameters, select it in the list and click .
   f. To delete a server from the list of excluded ones, select it, click , then click **Yes** in the confirmation dialog.
6. When all changes are made, click **Apply**.

### 3.3.1 Processing Addresses Added to Exclusions

When you exclude a server from analysis (see "Network Traffic Control"), you need to specify the server IP address or DNS name. To exclude from analysis a specific port or address range or, conversely, explicitly enable interception for a specific port, specify the value in the following format:

- to exclude a specific port from interception, use the following format: `address:port` (e.g., `10.128.0.2:80`)
- to exclude from interception all traffic sent to the address `10.128.0.2` except for the traffic sent on port `8080`, add two exceptions: `10.128.0.2` and `!~10.128.0.2:8080`
- to exclude from interception a range of addresses, use # character: `#192.168.0.1-192.168.0.255!192.168.0.5`
- to explicitly enable interception for a specific port, use the following format: `!~address:port`

Each line is processed according to the following algorithm:

**Step 1**. The System looks for a position of '#' character. If '#' character is found, then the following actions are performed (otherwise, go to step 2):

1. The System looks for a position of '!' character, and then checks the relative position of '#' and '!' characters.

2. In the place where '!' character is located, the string is divided into two parts. The part to the left of '!' contains addresses to be excluded from interception, the part to the right of '!' contains addresses for which interception should be explicitly enabled (explicitly enabled interception has a higher priority than any added exclusions).
3. In each part of the string, the System looks for ',' character. This character delimiters separate addresses or address ranges (substrings).
4. In each address or address range (substring) defined at step 3, the System looks for '-' character.
5. If '-' character is not found, then the substring is considered a separate IP address (not FQDN).
6. If '-' character is found, then the substring is considered a range of addresses IP1-IP2.
7. When all substrings are processed, obtained addresses or address ranges are added either as addresses to be excluded from interception or as addresses for which interception should be explicitly enabled.

*Example*: `#192.168.1.1-192.168.255.255,10.10.0.0-10.10.255.255!192.168.1.5-192.168.1.0,10.10.10.10`. This string contains two address ranges to be excluded from interception, and a range of addresses with an address for which interception should be enabled.

> **Note:**
>
> The System does not check if specified address regions intersect or if addresses for which interception is explicitly enabled are in the list of addresses excluded from interception.

**Step 2**. The System looks for a position of '~' character. If '~' character is found, then the following actions are performed (otherwise, go to step 3):

1. The System looks for positions of '~', '!', ':' characters and checks the relative position of these characters. If their relative position is incorrect, the further check is not performed.
2. If '!' character is not found, then the string in `address:port` format will be excluded from interception (e.g., `~192.168.1.1:5122`). Requests sent to this address and port will not be redirected to the proxy server.
3. If '!' character is found, then for the string in `address:port` format, interception will be explicitly enabled (e.g., `!~192.168.1.1:5122`). Requests sent to this address and port will be redirected to the proxy server even if this server and port have been excluded from interception.

**Step 3**. The System looks for a position '*' character. If '*' character is found, the address is considered a template one and is excluded from SSL interception. Requests sent to this address will not be redirected to the proxy server. If '*' character is not found, go to step 4.

**Step 4**. If neither of the '#', '~', '*' characters is found, then the address excluded from interception is considered a common address or FQDN. By means of OS functions, such an address is converted to IP address and added to the list of addresses excluded from interception (e.g., `192.168.1.1`, `example.infowatch.ru`). Requests sent to this address will not be redirected to the proxy server.

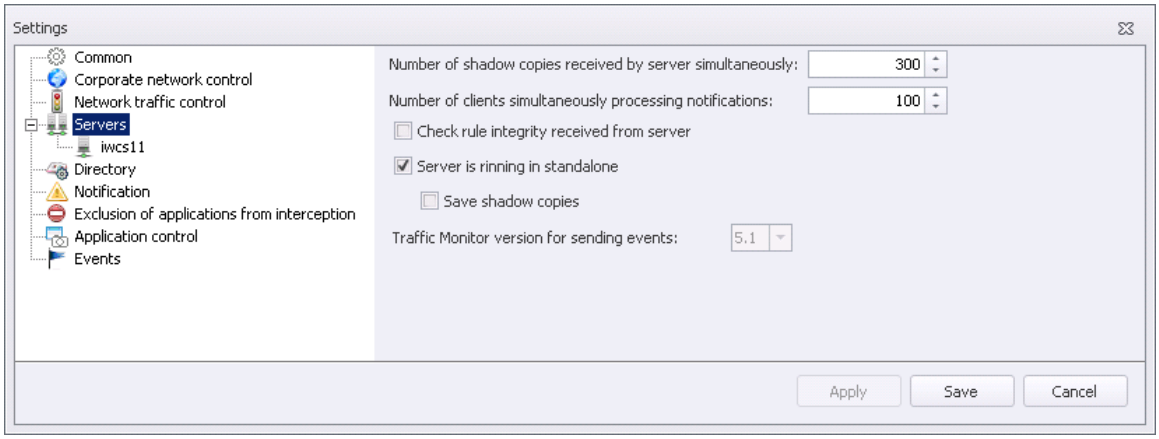
# 3.4 Device Monitor Server Settings. Connecting to Traffic Monitor Server

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 sent to Traffic Monitor Server simultaneously.
   - **Number of clients simultaneously processing notifications**: determines the number of agents, which can receive notifications (security schema) from server at a time
   - **Check rule integrity received from server** - compares rules (DM) on server and agent to avoid management on agent 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.

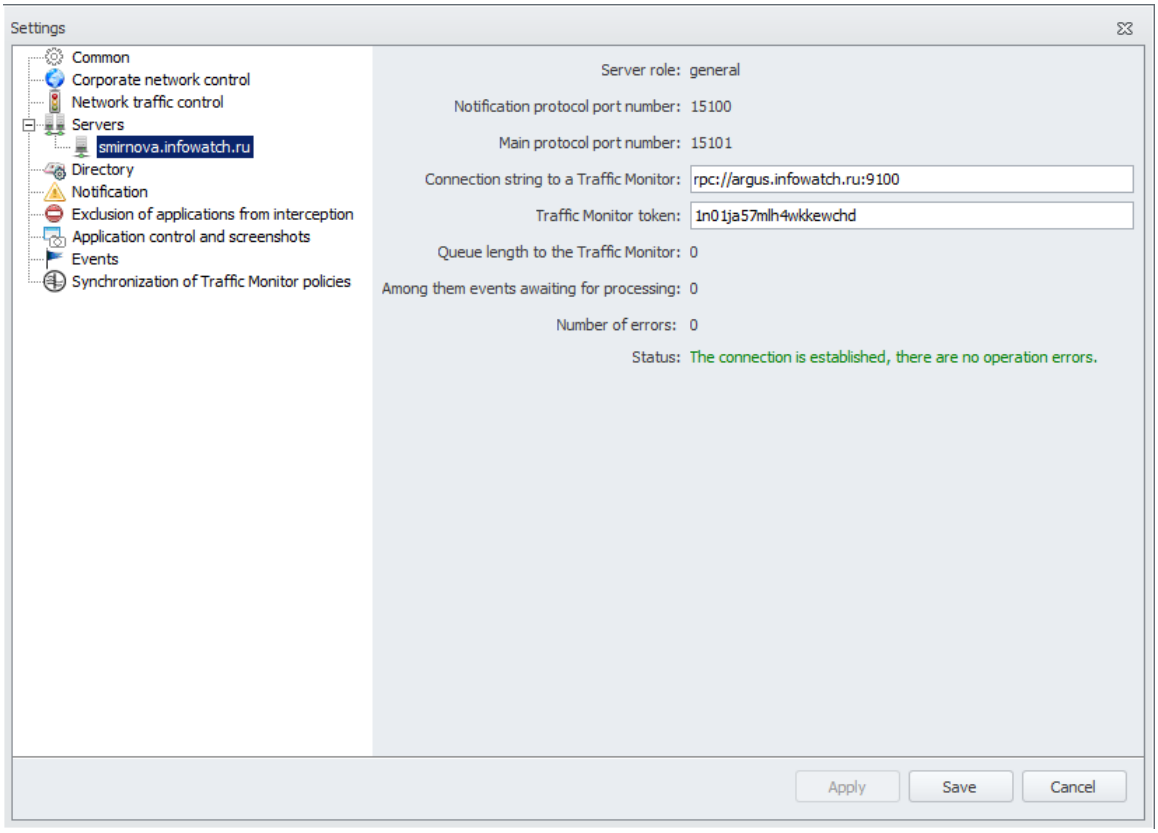



3. When selecting the server name, you will receive information on the following connection parameters:

- **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:

  `xml://host:port` - for Traffic Monitor v. 6.0 or higher.
  `rcp://host:port` - for Traffic Monitor versions under 6.0.

  ***host*** parameter should contain domain name or IP address of InfoWatch Traffic Monitor server. The server address is the standard URL address (Uniform Resource Identifier) with its formal syntax described in RFC 3986 http://tools.ietf.org/html/rfc3986.
  ***port*** parameter contains InfoWatch Traffic Monitor server port that delivers events. InfoWatch Traffic Monitor default server port is 9100.
- **Traffic Monitor token** – the token to connect to API. Required for Traffic Monitor v. 6.0 or higher. You can get the actual token from your Traffic Monitor administrator.
- **Queue length to the Traffic Monitor** - number of events pending submission to InfoWatch Traffic Monitor.
- **Among them events awaiting for processing** – number of events pending processing before sending to InfoWatch Traffic Monitor.
- **Errors number** – 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**.

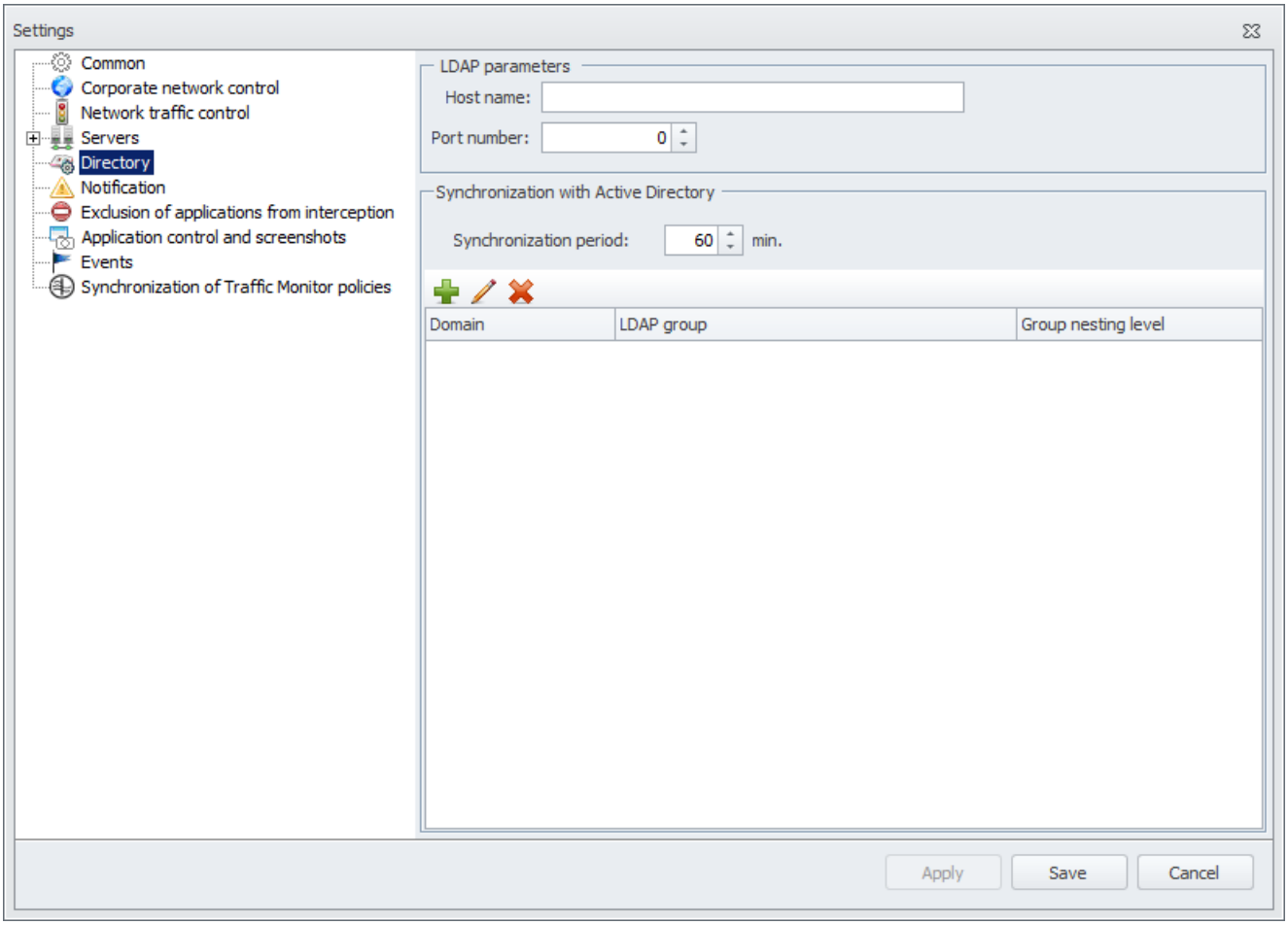
# 3.5 Connecting to LDAP Server and synchronization with Active Directory and Astra Linux Directory

### Configuring parameters of connection with LDAP server

In order to receive information on computers and employees from directory services, configure parameters of connection with LDAP server.

To view and configure LDAP connection settings:

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




> **Note:**
>
> Connection to LDAP server is performed in an anonymous mode.

### Adding synchronization settings

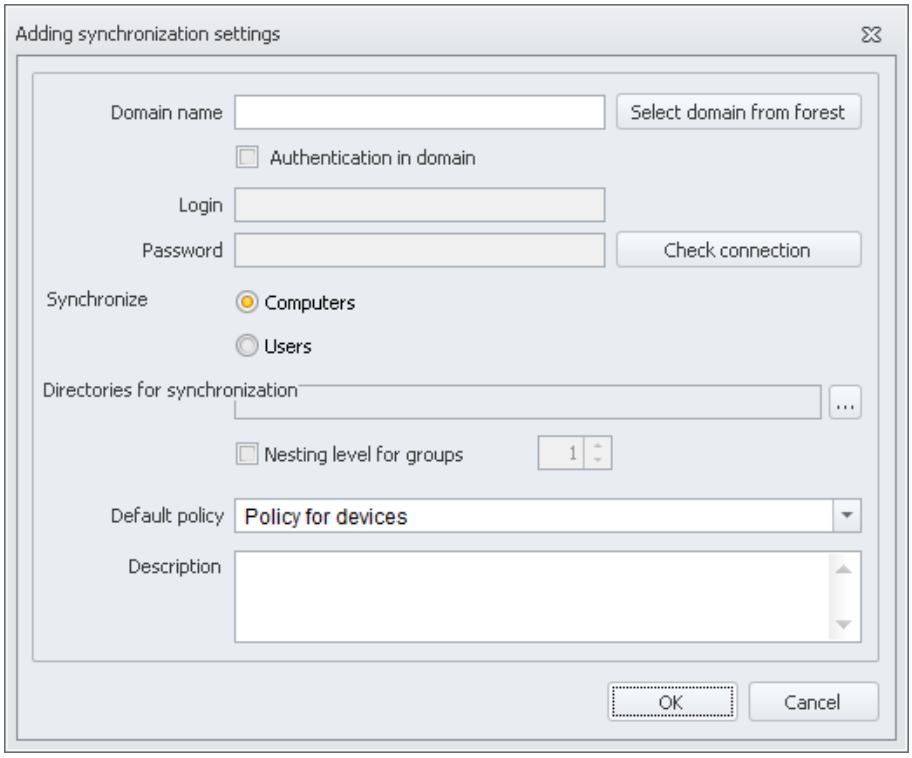
To add a synchronization setting with Active Directory or Astra Linux Directory:

1. In **Synchronization with Active Directory** area, click .
2. In a dialog window, specify synchronization settings:
   - **Domain name.** Name of the domain with which you want to synchronize (you can type the name manually or choose it from the domain forest).

     > **Note:**
     >
     > The domain name is an IP address or a DNS name. A DNS name must be registered in the network.

   - **Login.** To authenticate to the domain (if **Authentication in domain** option is selected).
   - **Password.** To authenticate to the domain (if **Authentication in domain** option is selected).
   - **Synchronize**. Synchronization objects - **Computers** or **Users**.

- **Directories for synchronization**. Directories in Active Directory that must be synchronized. For synchronization:
    a. Click
    
    .
    b. In the tree, specify directories for synchronization.
    c. Click **Select**.
- **Nesting level for groups** (if necessary). The maximum nesting level is 100.
- **Default policy**. A policy that will apply to synchronized groups after the first synchronization.
- **Description**. A comment (if necessary).




3. If the **Authentication in domain** option is selected, click **Check connection** to check connection with the domain.
4. If the connection is successful, click **OK**.
5. To apply changes, click **Apply** in the **Settings** window.

> **Note:**
>
> **Domain name** and **Directories for synchronization** fields are required.

The table in the **Settings** window contains data on the synchronization settings and results:

| Parameter | Description |
|---|---|
| Domain | IP address of DNS name of the server |
| Synchronize | Object of synchronization: computers or users |
| Directories | Folders and groups for synchronization |
| Synchronization status | Possible values:<br>• **Is running** (the synchronization process is in progress)<br>• **Successfully** (the synchronization process is complete),<br>• **Failed** (the synchronization process has failed). |
| Synchronization time | Date and time of the last synchronization |

> **Note:**
>
> For users and computers, the synchronization is configured separately. You can add several synchronization settings for the same domain.

### Launching/editing/disabling synchronization

To launch synchronization with Active Directory or Astra Linux Directory:

1. In the **Synchronization with Active Directory** area, select the required row in the table.
2. Click
   
   (to launch synchronization manually).
3. To update the synchronization status, select **View** > **Refresh** or press **F5**.

> **Note:**
>
> You can launch the synchronization automatically in specified periods. For this, specify the synchronization period and click **Apply**.

To edit synchronization settings:

1. In the **Synchronization with Active Directory** area, choose the desired row.
2. Click  .
3. Edit synchronization settings.

4. Click **OK**.

To disable synchronization with Active Directory or Astra Linux Directory:

1. In the **Synchronization with Active Directory** area, choose the desired row.
2. Click  .
3. In the confirmation window, click **Yes**.

> **Important!**
>
> When deleting a synchronization setting, all groups of computers or employees associated with this setting will also be deleted.

# 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 Agent did not have connections with Device Monitor Server so that there is out of dedicated space for storing information on events controlled by rules (DM) (30000 events) and common settings have Operation is blocked option selected (see in "Common Settings for Agents") then any operations controlled by current security policy (DM) are forbidden.
- **Data transfer via network protocols denied** – Ftp Monitor or IM Agent 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 Agent did not have connections with Device Monitor Server so that there is out of dedicated space for storing information on events controlled by rules (DM) (30000 events) and common settings have Operation is blocked option selected (see in "Common Settings for Agents") then any operations controlled by current security policy (DM) are forbidden.
- **Pasting from clipboard is denied if there is not enough space for incidents** – the «Forbid operation if there is no free space for incidents» option was triggered, there is no space for incidents and the operation of pasting data from clipboard to an application is performed.

- **Access to clipboard in applications is forbidden** – the rule (DM) which prohibits applications to access the clipboard at the attempt to paste/copy data in the application was triggered.
- **Printing in applications is forbidden** – the rule (DM) which prohibits printing for applications at the attempt to print from the application was triggered.
- **Copying file is forbidden when a data protection policy is triggered** – is displayed if the file copying is blocked because of applying a data protection policy (DM).
- **Passing data via network protocols is forbidden when a data protection policy is triggered** – is displayed when sending data via mail protocols, FTP or HTTP(S) is forbidden because of applying a data protection policy (DM).
- **Passing data via network protocols is forbidden if there is not enough space for events** – if Device Monitor Agent has not connected with the server for a long time and has run out of space for storing information on events (30000 events), and **Forbid operaton** option is selected in general settings (for details, see. "Common Settings for Agents"), then all operations controlled by the current security policy (DM) are forbidden.
- **Network connection forbidden** – Network Monitor rule (DM) which denies data transfer through any network connections except corporate network and specified permitted servers (see " 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 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 Agent 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 Agent interface, Device list tab (see " Temporary Employee Access to Devices").
- **Prohibition of access to cloud storage** – Cloud Storage Monitor rule (DM) which controls cloud storages agent usage (see "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 agent 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**:

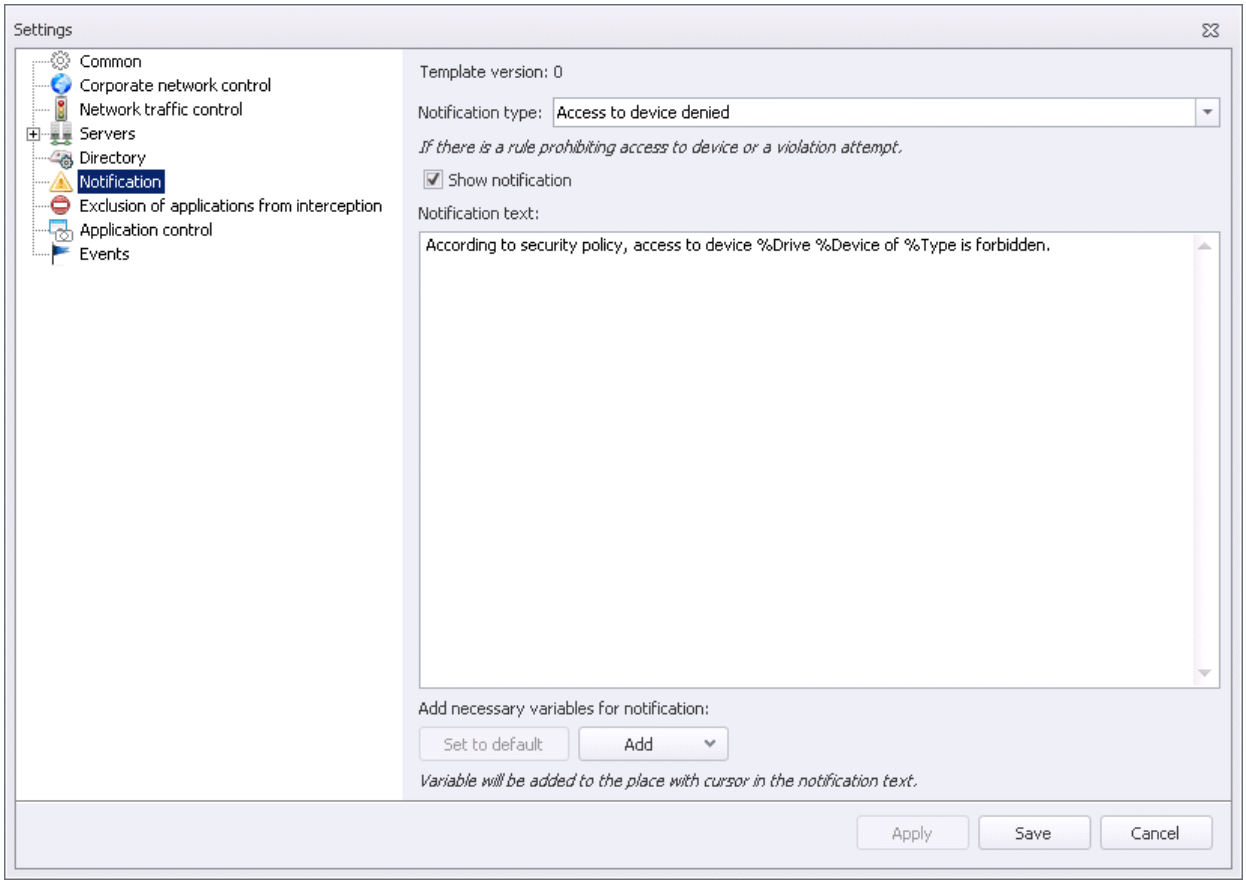
1. In the Main Menu select **Tools > Settings**.
2. At the left panel select **Common** node.
3. Deselect **Show notification** to disable showing notifications for employees, or flag it to enable notifications.
4. Click **Apply**.

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.



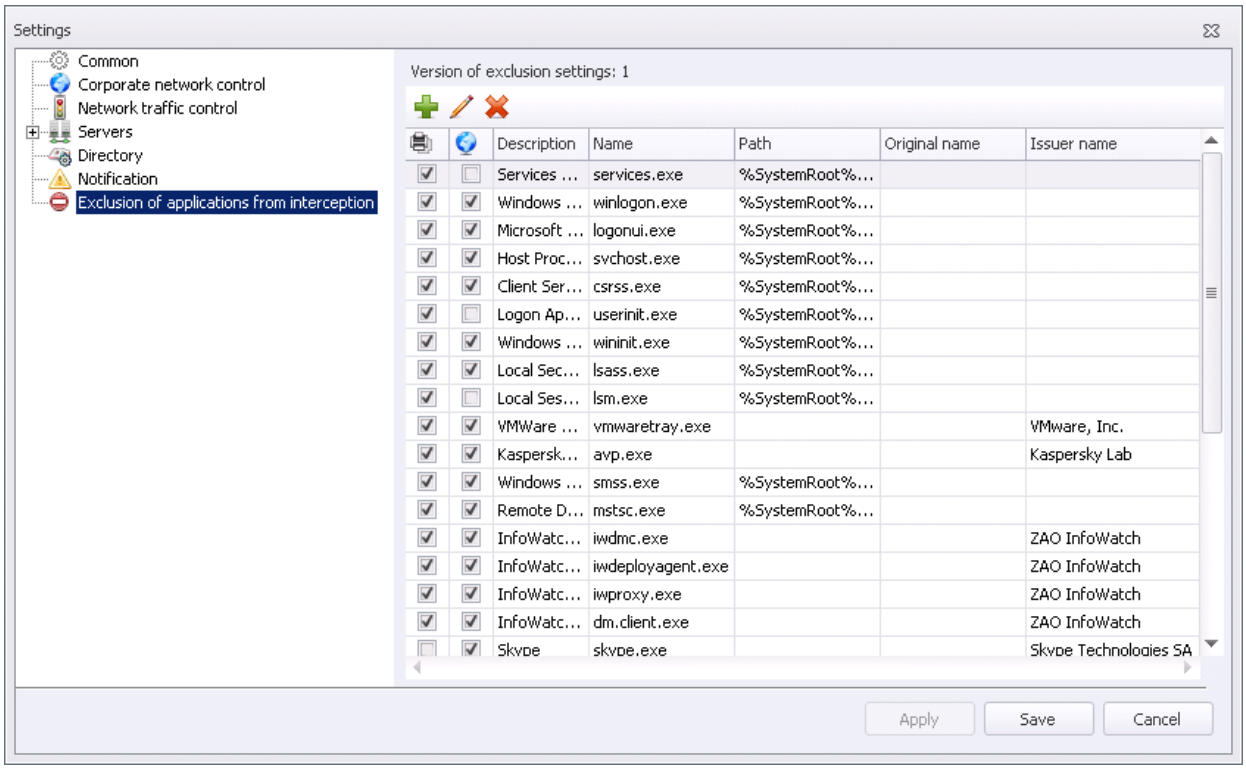
3. From **Notification type** list, select a notification type.
4. To enable (disable) displaying notification of chosen type, select (deselect) **Show notification**.
5. Enter notification text.
   You can use variables which would be transformed to actual data when displayed to employee: for example,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

# 3.7 Exclusion of Application from Interception

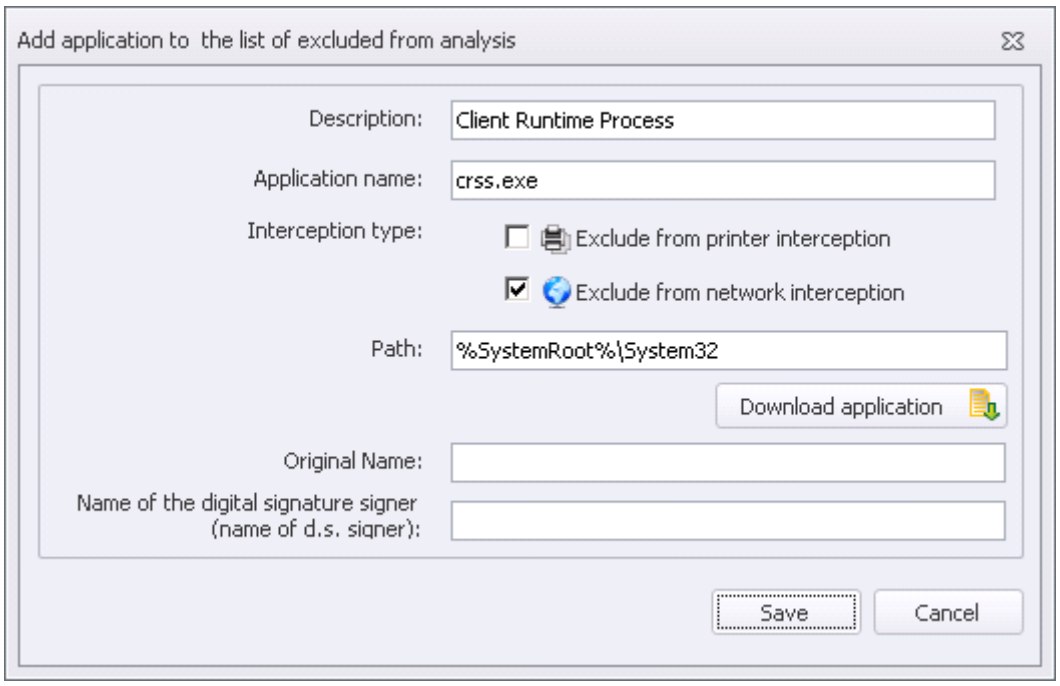
You can configure parameters of applications that will be excluded from interception. These parameters will apply the next time you deploy DM Agent on computers.

**To view and configure parameters of excluding applications**:

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




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




4. In the **Description** field, add a description of the application. This is a required field.
5. In the **Application name** field, enter the name of the application executable file. The exclusion is performed by the file name. A field is required and not case sensitive.

> **Note:**
>
> Instead of the application name, you can enter *. In this case, all applications with the specified path or specified digital signature (see i. 7) will be excluded from interception.

6. In the **Interception type** field, select:
   - **Exclude from printer interception** - neither events nor shadow copies will be created when you print data from the application;
   - **Exclude from network interception** - network activity of the application will be excluded from interception (see "Network Traffic Control").

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

7. You can specify the application file parameters manually or automatically:
   - To specify the file parameters manually:

a. In the **Path** field, specify a folder on the Agent that contains the application executable file or an upper-level folder (you can use system variables). The path to the file must begin with the specified string. For example, if you set an exclusion as: «*» + %Programm Files%\Citrix, then all applications in *.exe format located in the Citrix folder or any its subfolder will be excluded from interception.

b. In the **Original Name** field, specify the application name (in the file shortcut menu, choose **Properties**, **Details** tab, **Original filename** attribute).

c. In the **Name of the digital signature signer (name of d.s. singer)** field, enter the value specified in the application properties (in the file shortcut menu, choose **Properties**, **Digital signatures** tab, **Name of signer** attribute). You can specify the whole name or its part. For example, if you set an exclusion as: «*» + Kaspersky, then all applications whose digital signature contains "Kaspersky" substring will be excluded from interception.

> **Note:**
>
> The **Path** and **Original Name** fields are not case sensitive. The **Name of the digital signature signer (name of d.s. singer)** field is case sensitive.

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

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

8. Click **Save**.

# 3.8 Application Control

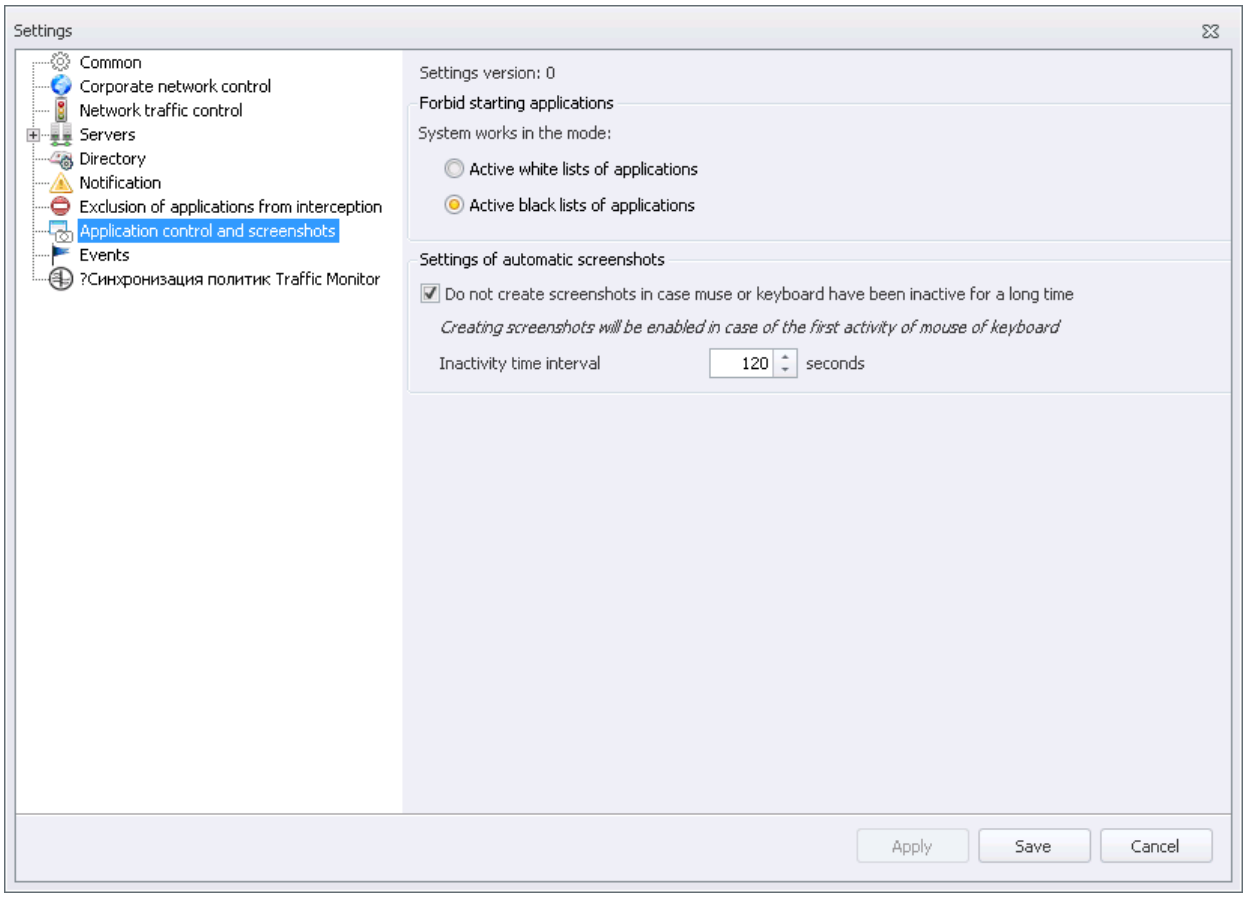
The System allows to control applications running of managed computers by allowing or forbidding some applications. For this purpose there are two operation modes provided:

- **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)".

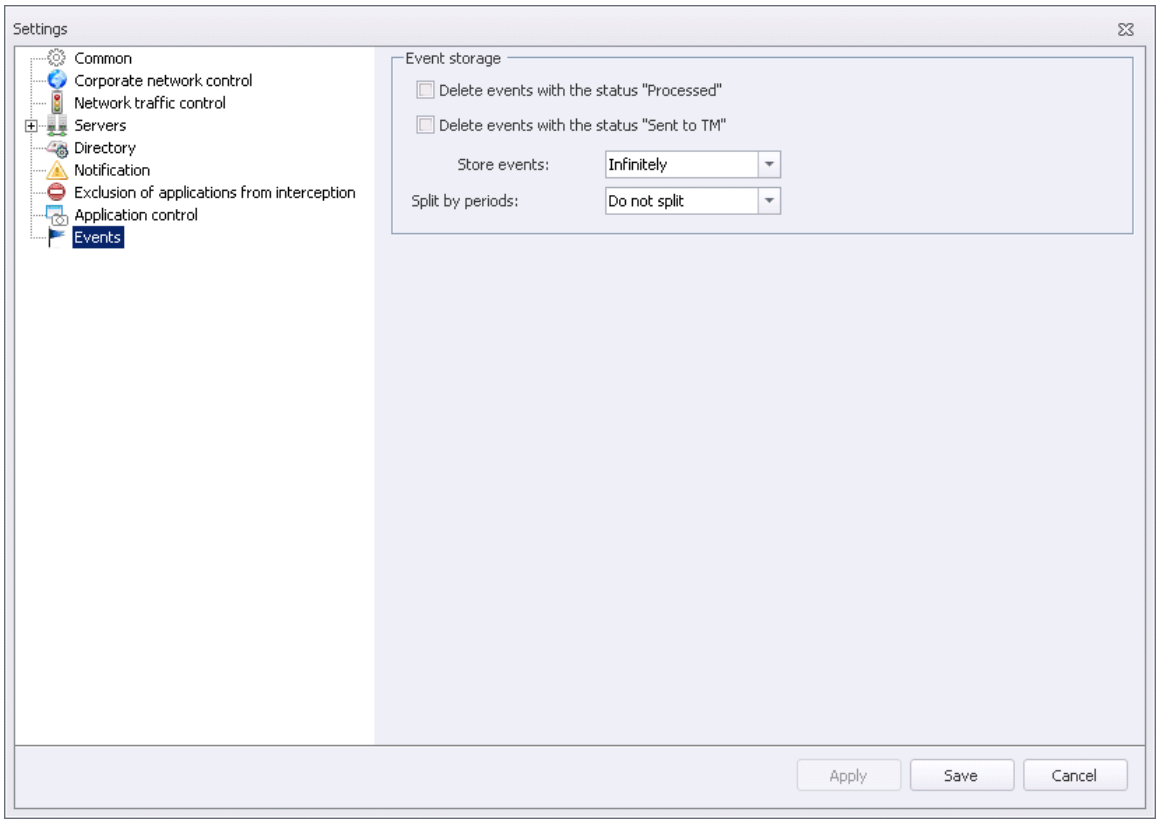
New version of applications and screenshots settings will ne applied to controlled computers after the next restart.

# 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 events 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.

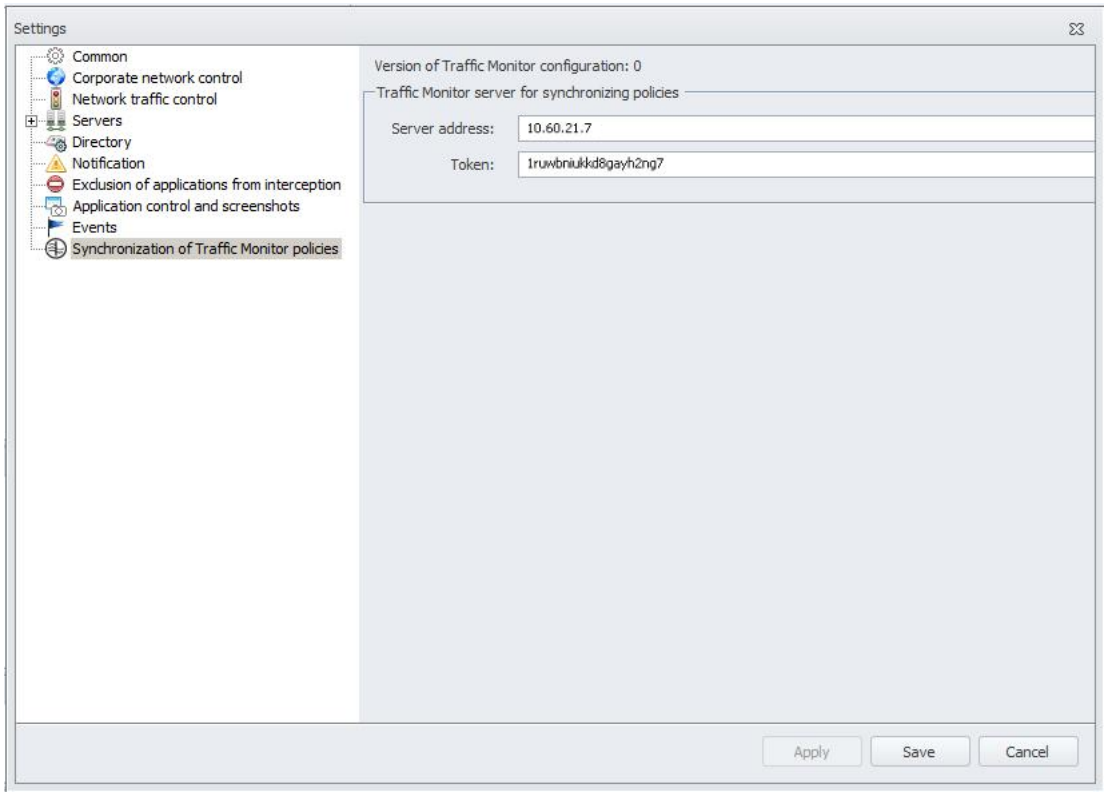
# 3.10 Synchronization of Traffic Monitor Policies

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**.

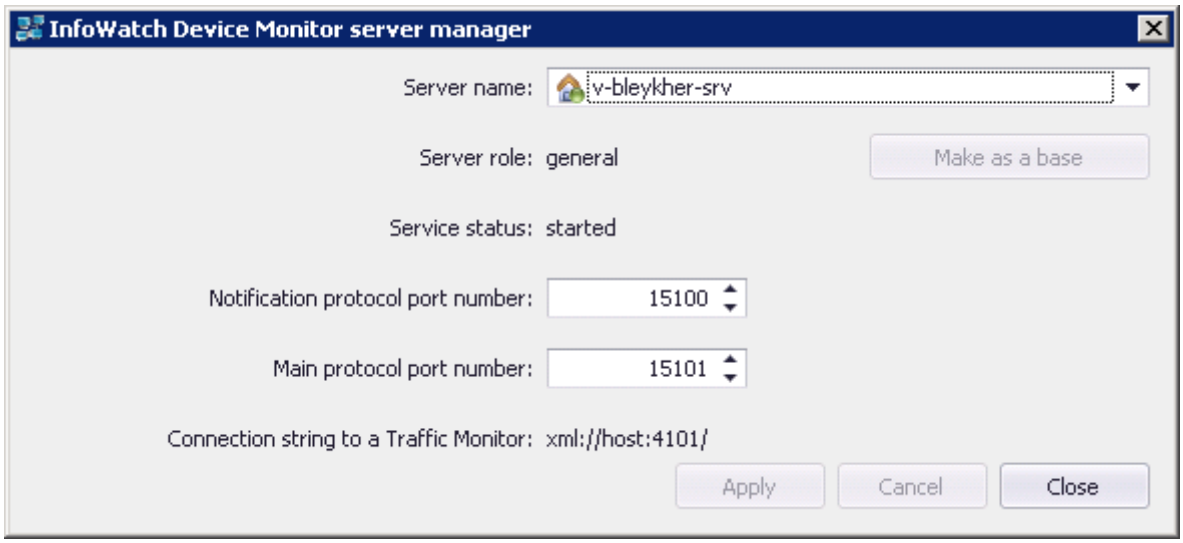
# 3.11 InfoWatch Device Monitor Server Manager

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

1. Go to **Start -> All programs -> InfoWatch -> Device Monitor -> InfoWatch Device Monitor Server Manager**.
   **Info Watch Device Monitor server manager** window will be opened.




2. From **Server name** drop-down menu, pick the necessary server.
3. Click **Make as a base**.

> **Note:**
>
> Specifying one of the servers as the main one automatically makes other servers secondary.

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

**To set up server ports, proceed with following steps:**

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

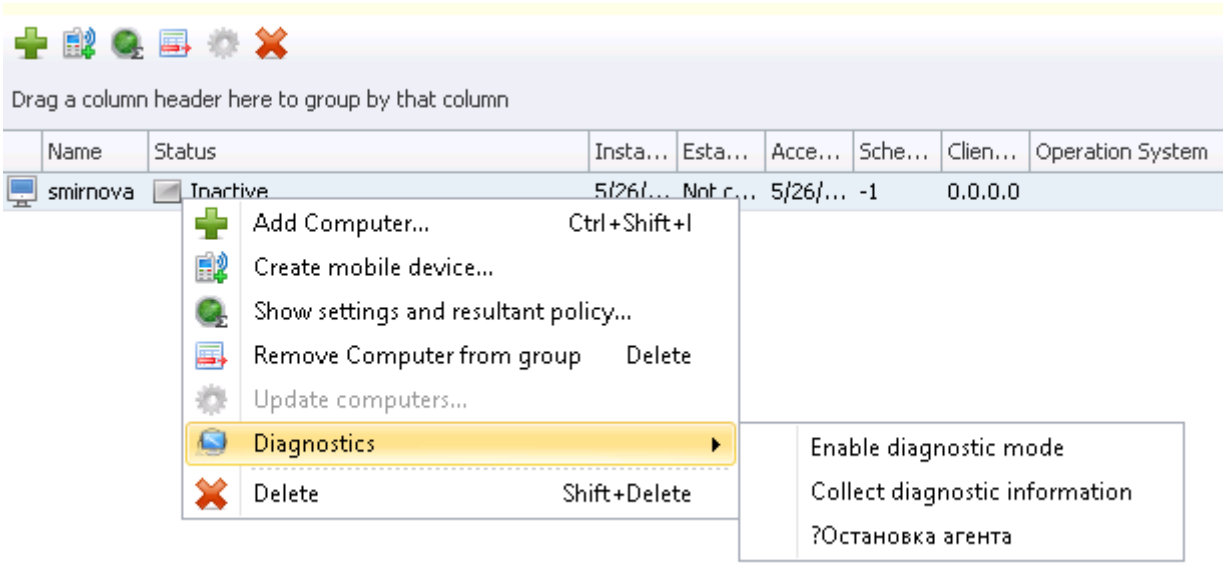
# 3.12 Stopping and Starting Device Monitor Agent

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

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

## 3.12.1 Stopping agent remotely/starting agent

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



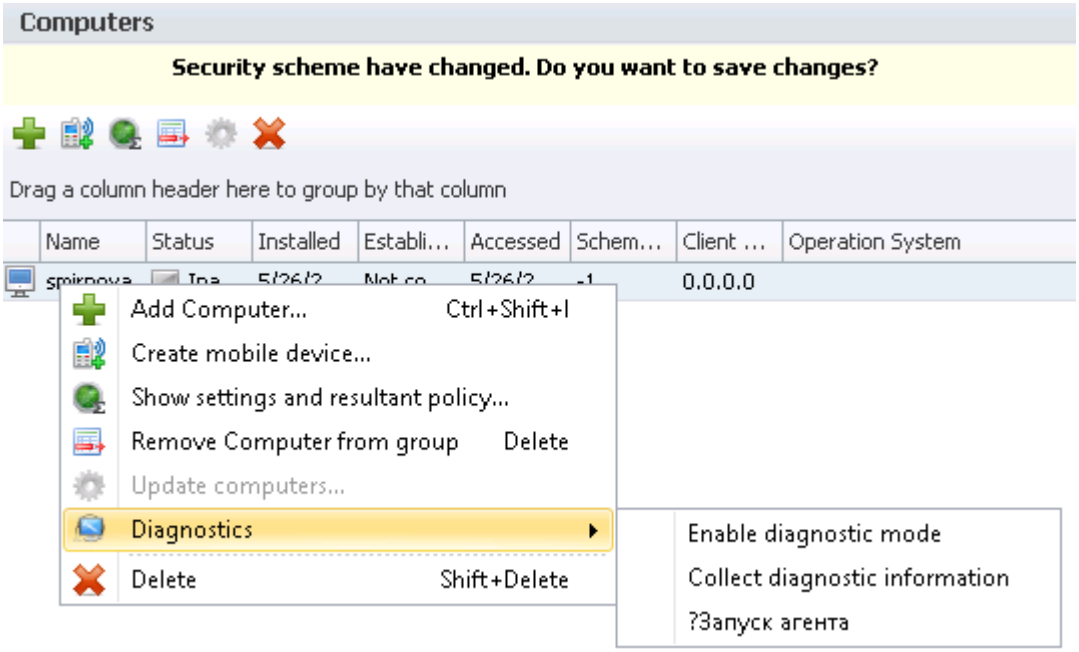

When choosing **Stop Agent**, its operation will be suspended and status of the workstation will change to " Inactive".

> **Note:**
>
> Stopped agent is available for update or deletion, but stopping is unavailable during update /deletion.In case there is no connection with the agent, stop/start are unavailable.

After the Agent has been stopped:

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

To start DM agent remotely, right-click on a Workstation and choose **Diagnostics -> 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".

### 3.12.2 Stopping/starting agent locally

Agent can be stopped/started using Windows command prompt. Run **rmtdiag.exe**, specifying the full path to it on the workstation (by default, C:\Program Files\InfoWatch\DeviceMonitor\Client) with the required parameter. For example:

- **C:\Program Files\InfoWatch\DeviceMonitor\Client\rmtdiag.exe /cle** - to start agent;
- **C:\Program Files\InfoWatch\DeviceMonitor\Client\rmtdiag.exe /cld** - to stop agent.

> **Warning!**
>
> To stop the agent, you need to enter DM agent uninstallation password. The password should be entered after **/cld** key and a space. To start the agent, the password is not required.
>
> For more information on uninstallation password, see "Creating Uninstallation Password Reset Task".

# 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 scheme 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 includes the computer used by the employee.

If an 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 the employee to various employee groups.

> **Warning!**
>
> In case of a multiuser access to the 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 applications 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. The rule can block access to the 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 the agent side.

For each rule, there is a list of operating systems where the rule can apply. The way how the rule applies also depends on the OS. For more information on applying rules, see the "Rules (DM)" subsection.

### 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 Computers and computer groups

A computer registered in Device Monitor should be included in at least one computer group (the "default" group). The reason for this requirement is that the security policy (DM) can only be assigned to a computer group.

The default group includes all computers that do not belong to other computer groups (computers that are newly registered in Device Monitor or computers excluded from all other groups). The "*Device policy*" is assigned to the default computer group after the System installation. This policy (DM) does not contain any rule.

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

You can also add mobile devices to the security scheme, connect them to an employee and install Device Monitor Agent on the mobile device. You can add the mobile device in two ways:

- from a computer group: in this case, you should specify the employee who has been earlier created in the System or added from LDAP;
- from a group of employees: in this case, you should specify the computer group to which you want to add the mobile device.

### 4.1.4 Uploading security scheme to managed computers

The security scheme of managed computers must be up to date. This is ensured by Agent-Server interaction on managed computers.
Server transmits security scheme to managed computers automatically in the following cases:

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

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

# 4.2 Security Scheme Overview

For information on operation of the security scheme, see the sections:

- Viewing Active Security Scheme
- Viewing Old Security Scheme
- Security Scheme Comments
- Editing Security Scheme
- Updating Security Scheme
- Exporting/Importing Security Scheme

For general information on the security scheme, see "Security Schema Organization".
For information on the security scheme configuration, see "Security Schema Setup".

## 4.2.1 Viewing Active Security Scheme

By default, the Management Console (DM) displays a security scheme which is currently active.

Information on the security scheme configuration is displayed in **Policies**, **Employees**, **Workstations**, **White Lists**, and **Signatures** sections (see "Management Console (DM) Sections").

The security scheme configuration is displayed as groups of elements. Element groups of the selected section are displayed in Navigation pane. Each group of elements has its icon (see the table below).

| Icon | Elements group |
|---|---|
|  | Default workstation group |
|  | Workstation group |
|  | Default employee group |
|  | Employee group |
|  | Default signature category |
|  | Signature category |

| Icon | Elements group |
|---|---|
|  | Devices white list for employee |
|  | Devices white list for employee group |
|  | Devices white list for workstation |
|  | Devices white list for a group of workstations |
|  | Audit log filter |
|  | Security policy |

**To view information about a security scheme section**:

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

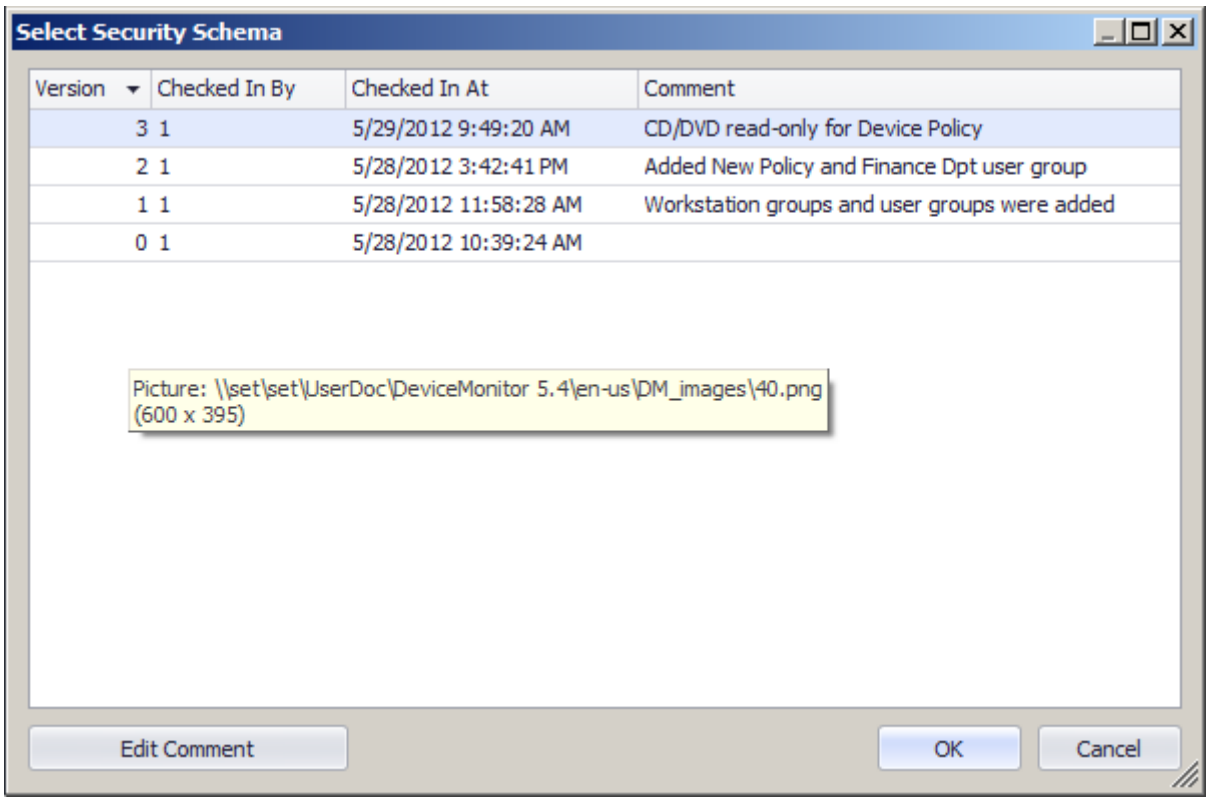
> **Note:**
>
> You can customize the main screen appearance (see "Main screen customization").

## 4.2.2 Viewing Old Security Scheme

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

**To view older security schema**:

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




Each security scheme features the following information:

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

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

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

After you click **OK** the selected security schema version will be loaded into Management Console (DM). When working with an 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 Scheme Comments

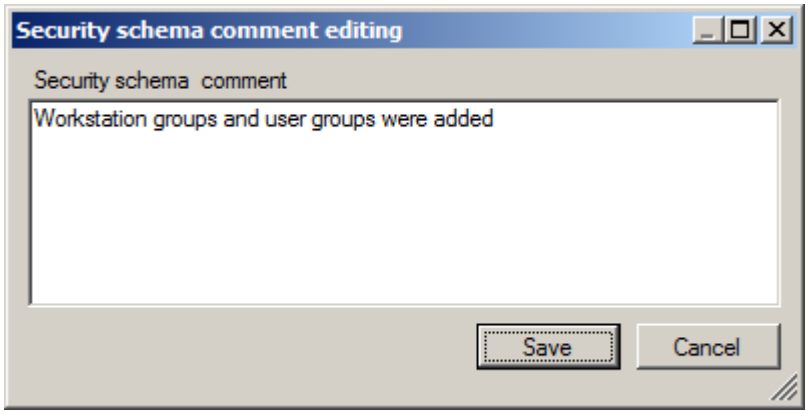
You can specify additional information on your security scheme as a comment. You can add comments to each version of the security scheme.
Comments on current security scheme are displayed in brackets to the right of the scheme version number on the status panel.
You can view comments for all security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

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

**To add/edit security scheme comment**:

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

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




2. Enter your comment in the dialog box. The maximum comment length is 512 characters.

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

3. Click **Save**.

### 4.2.4 Editing Security Scheme

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

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

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

**To edit security scheme**:

1. Take one of the following steps:
   - in the Main Menu select **Security Scheme > Edit**
   - click **Edit** on Toolbar
   - make any change of security scheme parameters (security policies (DM), computers, employee accounts, device white lists, signature categories).
     These actions open security scheme editing mode.

     > **Note:**
     >
     > You can edit only the latest version of the security scheme. Thus, Save command is not available when viewing previous versions. To open current security scheme version, open **Security scheme** > **View Latest Security Scheme** from the main menu.
     > Information on security scheme currently used by Management Console (DM) is displayed on the status bar.
2. Edit security scheme parameters:
   - security policies (see "Security Policies");
   - workstation groups (see "Workstations");
   - employee accounts lists (see "Employees");

- device white lists (see "White Lists");
- file signature categories (see "Signatures").

3. When all changes are made, save your security scheme. To do this, follow these steps:
   - click **Save** at the top string of main screen workspace where "*Security Scheme have changed. Save changes?*" message is displayed
   - in the Main Menu, select **Security scheme > Save**
   - click **Save** on Toolbar.
     These actions save the changes and close security scheme editing mode.

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

## Awaiting Editing Ends. Unlocking Security Scheme

The security scheme can be edited only by one user at a time. Changes are applied only after you have saved your security scheme.
If security scheme is being edited, information about the user who is editing it and the computer where editing is performed is displayed at red-highlighted string at the top of the main screen.
If you try to edit any parameters of security scheme (security policies (DM), workstations, employee accounts, device white lists, signature categories) while security scheme is being edited by another user:

1. Management Console (DM) displays warning message.
2. When another user saves changes (or cancel them) Windows system tray displays a notification: "***Security schema is in "read-only" mode***".

Information about the user who is currently editing the scheme is displayed at the string at the top of the main screen and in the status bar.

Security schema might be blocked even if it is not being edited. This may occur if the last editing operation wasn't properly completed (i.e. due to disconnection from the server).
When a user who blocked a scheme connects the server again, the security scheme is automatically unlocked and all unsaved changes made by this user are lost.
There is also a special function that targets the blocking issue - security scheme unblock.

> **Warning!**
>
> Security scheme can be unblocked only by Superuser.

**To unblock security schema**, in the Main Menu click **Security Schema > Unlock**. All unsaved changes will be lost.

### 4.2.5 Updating Security Scheme

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

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

- registering a new workstation;
- registering an unknown employee;
- modifying your security scheme.

**To update security scheme manually, do one of the following**:

- select **View > Refresh** in the Main Menu;
- click **Update** on the toolbar;
- press F5.

### 4.2.6 Exporting/Importing Security Scheme

You might need to save existing settings of a security scheme. You might want to do this if you need to configure Device Monitor server after reinstalling it or when deploying new Device Monitor servers.

When exporting the configuration, a file in .dmc format is saved to your computer. The file contains the current version of the security scheme including:

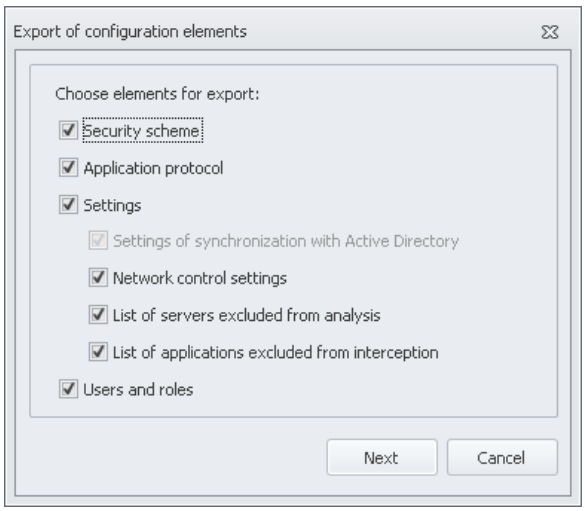
- **Security scheme** (including security policies with rules, groups of employees and computers, categories of signatures) (see "Managing Security Schema")
- **Applicaiton protocol** (see "Application Protocol")
- **Network control settings** (see "Settings of Corporate Network")
- **Servers included from analysis** (see "Network Traffic Control")
- **Applications excluded from interception** (see "Exclusion of Application from Interception")
- **User and roles** (see "Managing Console (DM) Accounts")

> **Important!**
>
> Device Monitor version 6.0 or later does not support importing a configuration file that was exported from earlier versions.

Saved settings can be then imported to a new security scheme.

**To export the System configuration:**

1. In the main menu, select **Tools** > **Export configuration**.
2. In the dialog box that opens, select configuration elements you want to export.




3. Click **Next**.
4. Specify the export file name and select a folder where the file will be saved. Click **Save**.

**To import the System configuration:**

1. In the main menu, select **Tools** > **Import configuration**.
2. In the dialog box that opens, choose a file in *.dmc format which stores the saved configuration.
3. Click **Open**.
4. In the **Import of configuration elements** dialog box, select elements you want to import.
5. Click **Next**.
6. In the confirmation window, click **OK**.
7. In the informational message, click **Save**.




The saved settings of the security scheme will be imported to the active scheme. If the active scheme contains items with similar names, then **1** will be added to the names of imported items.

# 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:

- A security policy (DM) must be created before you create an employee group or workstation group the policy (DM) will be assigned to.

- It is recommended that you assign an individual security policy (DM) for each employee group and workstation group.
- Each security policy (DM) assigned to a group must have a specific set of rules (DM).

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

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

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

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

## 4.3.1 Security Policies (DM)

On Device Monitor agents, policies apply in the following order:

1. Prohibiting policies (DM).
2. Data protection policies on agents created in TM.
3. Policy of shadow copying (DM).

> **Note:**

For recomendations on configuring the security policy (DM), see "Security Policies (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 **computer groups**. The security policy (DM) assigned to the employee group applies to all employees included in this group. The security policy (DM) assigned to a group of computers applies to all employees who work at managed computers included in this group.

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

For information on working with security policies (DM), see:

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

## Viewing Security Policies (DM)

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

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

**To view security policy rules**, select security policy (DM) name in **Policies** area of Navigation pane.

Rules are displayed in a form of a table where each row contains a rule. Columns contain general rule properties. Each rule (DM) has an icon depicting the rule's (DM) coverage and a 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.

For you each rule, you can view general information and additional and additional attributes which depend on the rule type.

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

General information:

- **Name**. Rule (DM) name.
- **Policy**. Name of the security policy (DM) that includes the rule (DM).
- **Interceptor**. Interceptor type assigned to the rule (DM).
- **Operation**. The operation controlled by the rule (DM).

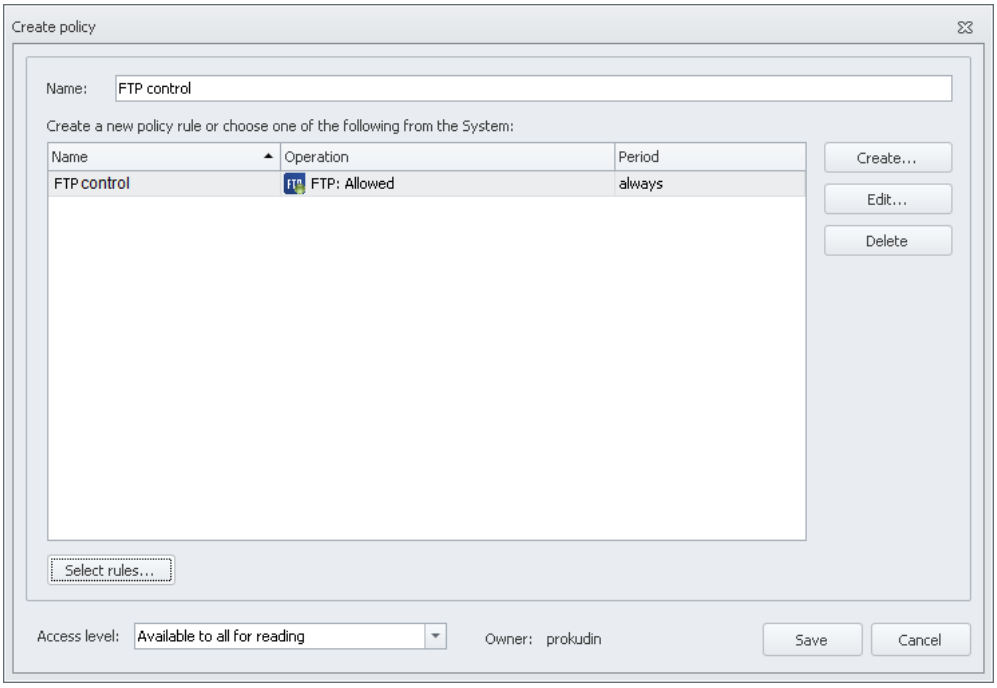
- **Period**. Rule starting and expiry time.

> **Note:**
>
> Information for some attributes is duplicated on the main screen.

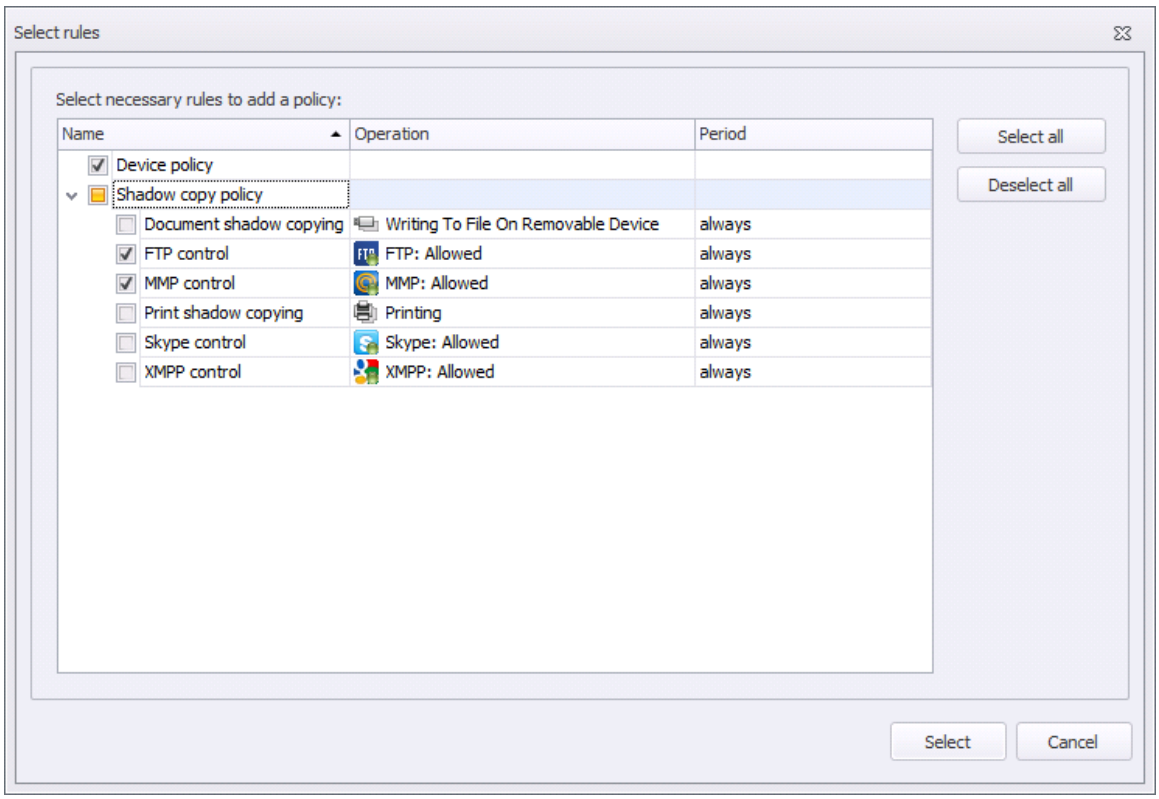
## Adding and Configuring New Security Policy (DM)

**To create and configure security policy:**

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




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




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

- To create a new rule (DM) click **Create** and specify rule (DM) parameters as described:
  - 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. In the **Access level** drop-down list, specify permissions for reading and editing the policy.
6. When all rules (DM) to be included in the policy (DM) are defined, click **Save**.

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

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

## Edit Security Policy (DM)

**To edit security policy (DM):**

1. Go to **Policies**.
2. In **Policies** area of Navigation pane, select security policy (DM) name.
3. Take one of the following steps:
   - in the Main Menu, select **Edit > Edit Policy**;
   - click **Edit Policy** at the top of Navigation pane;
   - use **Ctrl+E** shortcut;
   - double-click selected security policy (DM) name;
   - right-click the policy name and choose **Edit** from the context menu.

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

> **Warning!**
>
> To apply changes, save current security scheme (see "Editing Security Scheme"). Otherwise, all changes will be discarded.

## Deleting Security Policy (DM)

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

**To delete security policy**:

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

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

### 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:

- Applying Rules (DM)
- Adding a Rule (DM)
- Editing a Rule (DM)
- Deleting a Rule (DM)
- Copying a Rule (DM)

### Applying Rules (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 the 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 encrypted devices* . Also, FTP Monitor rule (DM) (see "Configuring FTP Monitor Rule (DM)") with *Forbid using FTP-protocol* applies instead of the rule (DM) with *Full access to encrypted devices*, and the last one - instead of the 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 applying rules (DM):

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

## Device Monitor Rules (DM) Application

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

Employee access rights are defined 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 Agent 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 newly 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, the 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<br>2. Read-only | 1. No access<br>2. Read-only<br>3. Full access to the encrypted devices only |

**Examples**:

**Example 1**. There is a rule (DM) for workstation group C that forbids an access to a 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 the workstation that belongs to workstation group C. Conflict is resolved in favor of more restrictive rule (DM), i.e. employee Smith cannot read from a removable storage device.
**Example 2**. There is a rule (DM) in employee group E policy (DM) that allows read-only access to a 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 are provided in "Configuring Device Monitor Rule (DM)".

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

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

## 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 (DM) creates shadow copies and file size meets the requirements.
2. Free space at managed workstation is more than the minimum size required by the policy (DM) (see "Common Settings for Agents", **Free clients' disk space** setting, the 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 Agent is installed has dedicated space for storing up to 30000 events (about 300 MB). If:

- Device Monitor Agent did not have connections with Device Monitor Server so that there is stored more than 30000 events controlled by rules (DM) defined for employee/workstation and
- in common settings for agents 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 scheme will be blocked**.

## 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 **Save** 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.

## Configuring Application Monitor Rule (DM)

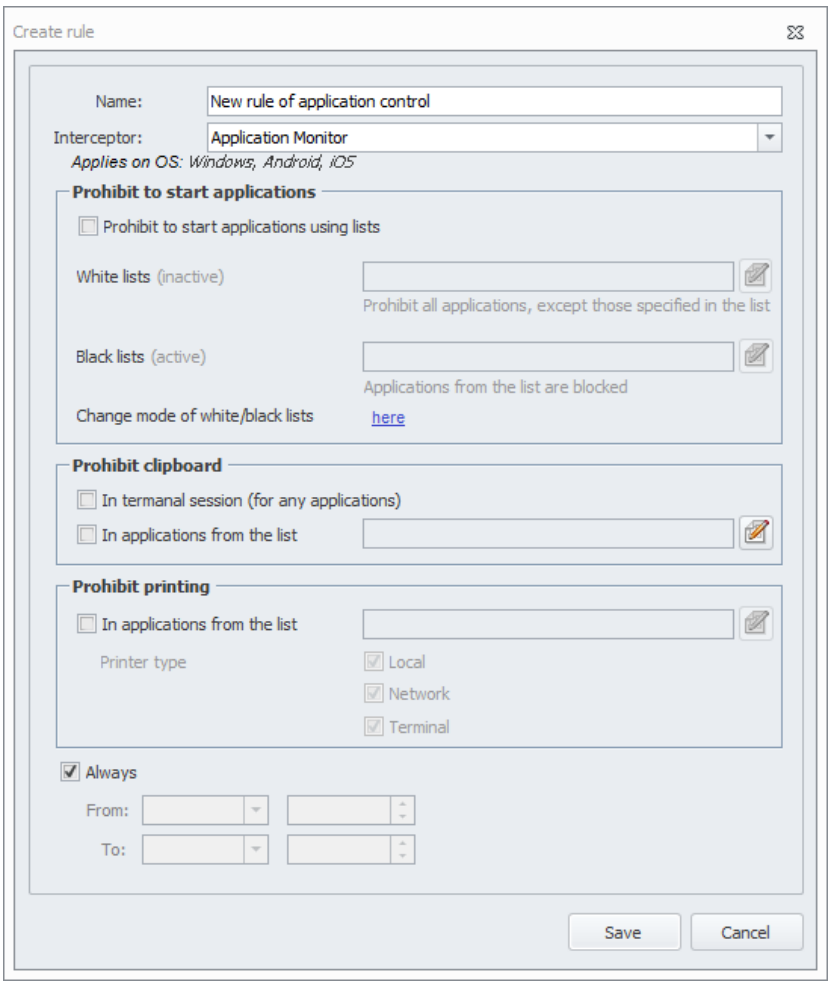
An employee can perform actions which can lead to the leakage of confidential information through third-party applications installed on a workstation and not controlled by InfoWatch Device Monitor.

Application Monitor interceptor allows you to control employees' access to applications prohibiting the following actions:

- starting applications;
- using clipboard;
- printing.

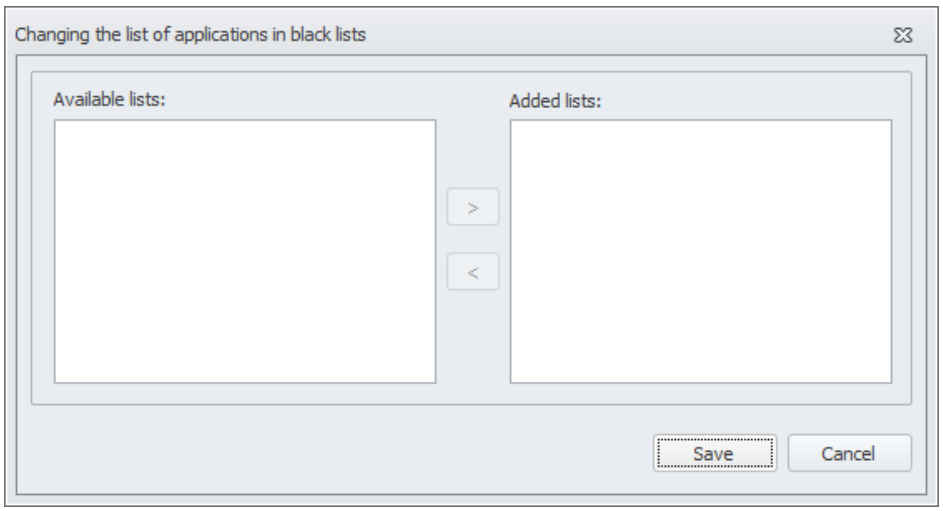
These prohibitions can be activated both separately and together.

> **Note:**
>
> The rule applies on computers with Windows OS and mobile devices on Android and iOS platforms.




**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;
   - click Ctrl+N.
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:**
>
> To switch between active black and white application lists, click the link here .
>
> On creating the application list, see "Application protocol".

7. In the window that opens, choose necessary types of available lists and move them to **Added lists** area by pressing > .
8. Click **Save**.
9. In **Prohibit to start applications** block, select check boxes next to the application groups for which data copying should be prohibited:
   - In terminal session (for any applications);
   - In applications from the list (add lists by clicking ).

   > **Warning!**
   >
   > If using the clipboard is prohibited, the prohibition applies to all data types to both copying and pasting data, regardless of the black/white list mode.
10. In the **Prohibit printing** block, specify applications for which printing should be prohibited and the printer type:
    - local;
    - network;
    - terminal.

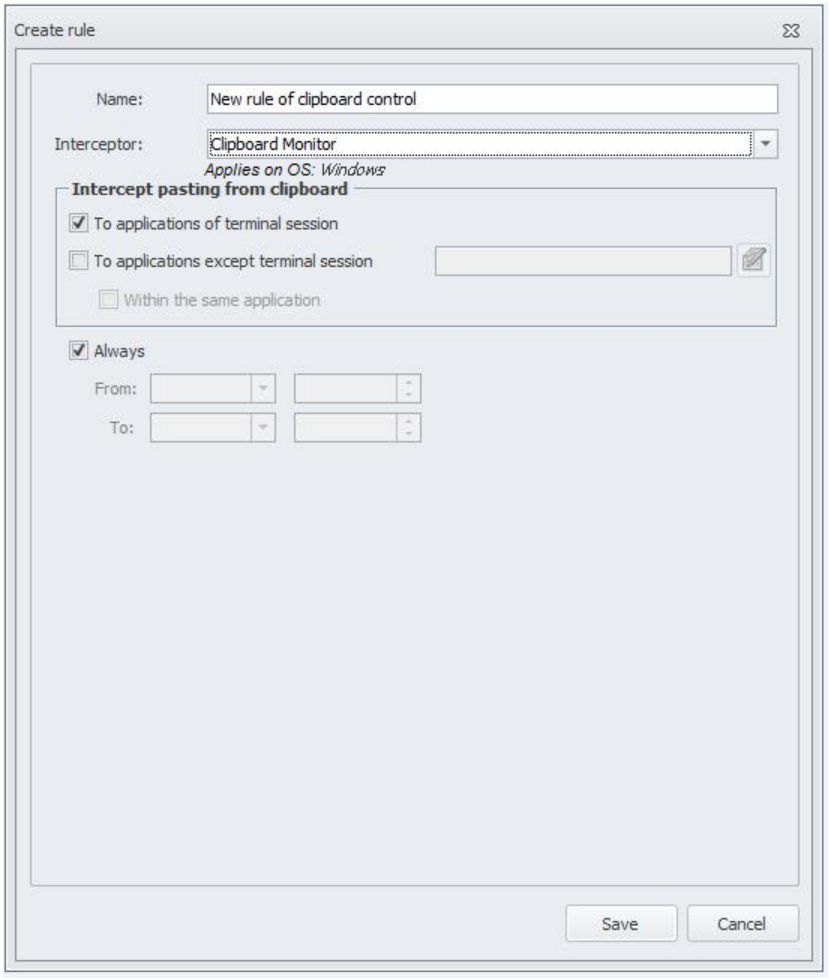
    The user will not be able to print data in specified applications. Choosing specified printer types is not available either.

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

## Configuring Clipboard Monitor Rule (DM)

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

> **Note:**
>
> The rule applies on computers with Windows OS.




**To configure the rule, 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;
- press Ctrl+Shift+N.

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 period, clear the **Always** check box and specify dates and time in **From** and **To** fields.
8. When all parameters are configured, click **Save**.

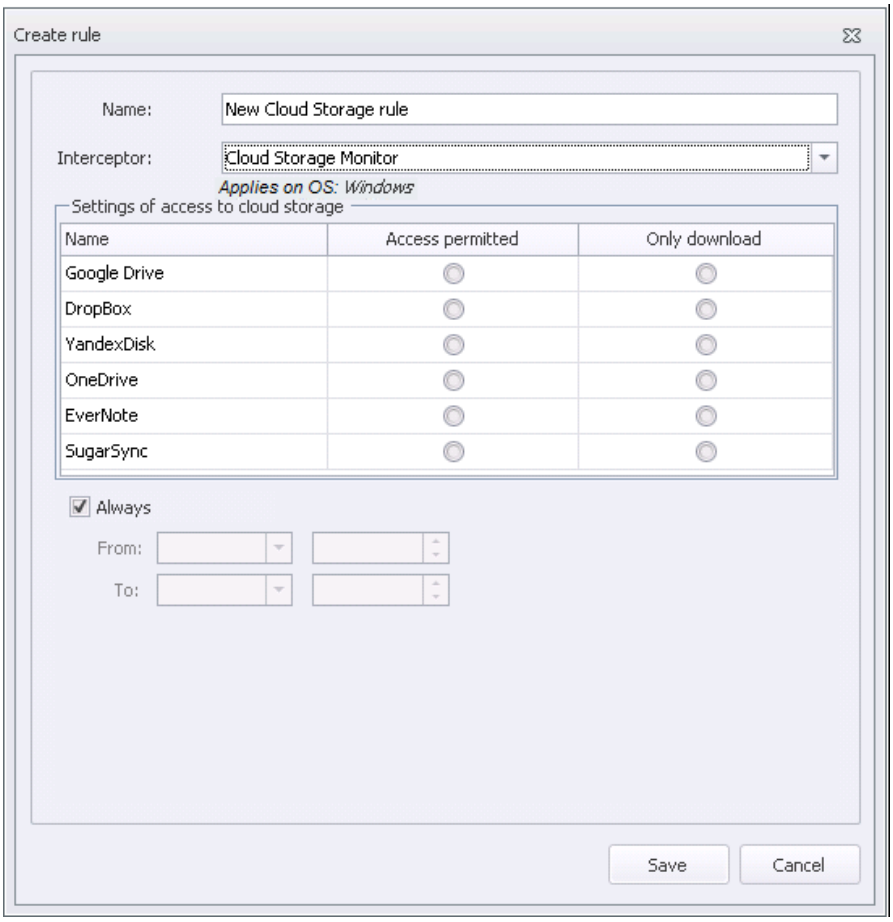
## Configuring Cloud Storage Monitor Rule (DM)

**Cloud Storage Monitor** interceptor allows you to control web clients of 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 |

**Note:**

The rule applies on computers with Windows OS.




**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. 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;
   - press Ctrl+Shift+N.
4. In **Create rule** dialog in **Interceptor** field, select **Cloud Storage Monitor**.
5. Enter rule (DM) name to the **Name** field.
6. In **Setting of access to cloud storage** area, 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 a period, clear **Always** check box and specify dates and time in **From** and **To** fields.
8. When all parameters are configured, click **Save**.

## Configuring Device Monitor Rule (DM)

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

> **Note:**
>
> The rule applies on computers with Windows OS.

**Control of terminal clients connected via Microsoft RDP or Citrix ICA can be useful in the following cases**:

1. A remote user connects to a computer with installed Device Monitor Agent from a terminal client.
2. There is a storage device or a printer connected to a terminal client.
3. A remote user tries to print/copy data from a computer (the terminal storage/printer must be connected to the computer via Microsoft RDP or Citrix ICA).

| 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 |

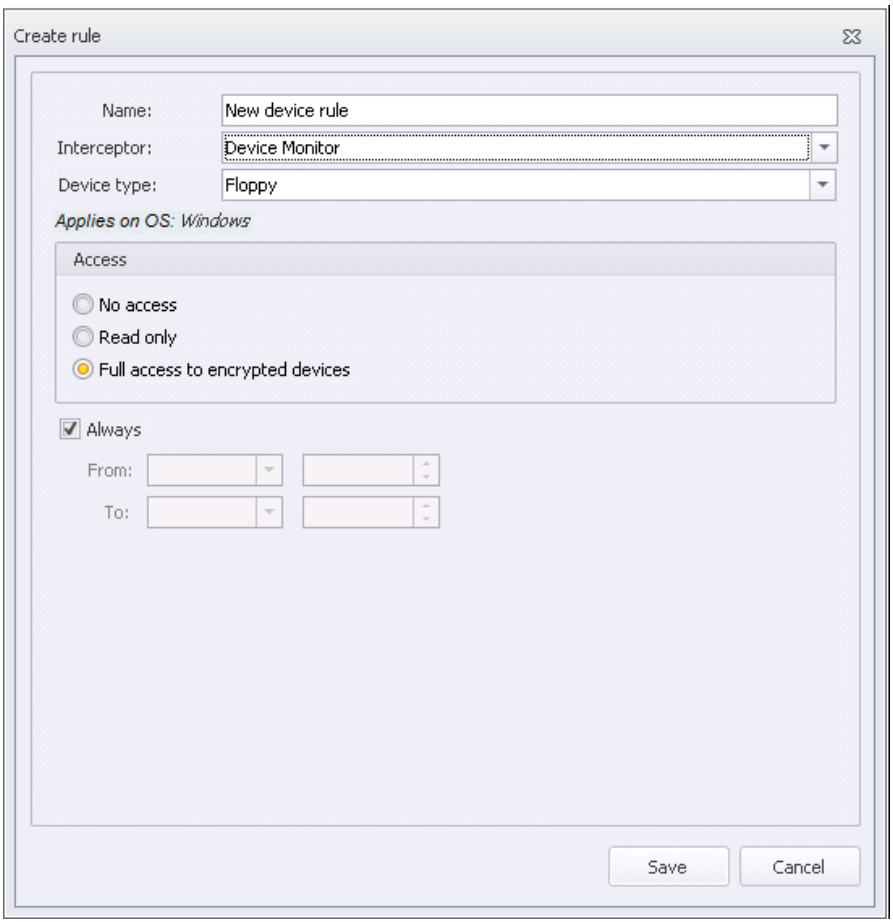
| Name | Behavior |
|---|---|
| Other USB Devices | Denied |
| FireWire | Denied |
| Modem | Denied |
| Smart Card Reader | Denied |
| Tape Drive | Denied |
| Multifunctional Device | Denied |
| PCMCI device | Denied |
| USB Adapter | Denied |
| Pocket Computer (Windows Mobile and Palm OS pocket computers) | Denied |
| Network printer | Denied |
| **Microsoft RDP or Citrix ICA connection control** | |
| Terminal printer | Denied |
| Terminal storage | Read only/Access denied |
| Terminal port (thin client port) | Denied |
| Terminal Plug and Play devices | Denied |

### Note:

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

### Warning!

If event matches multiple rules (DM), see "Applying Rules (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) to which you want to add a rule.
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 the **Name** field.
6. Select the device type controlled by this rule from **Device type** drop-down list.
7. In the **Access** area, select the required access level (see the 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 a period, clear **Always** check box and specify dates and time in **From** and **To** fields.
9. When all parameters are configured, click **Save**.

## 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.

The following removable devices are supported:

- devices connected via USB and IEEE 1394 ports (FireWire, i-Link)
- floppy disk storage systems (floppy disk drive, ZIP drive)
- optical disks (CD, DVD, BD) in Live File System mode
- media devices
- external devices connected through a terminal session

The following network devices are supported:

- network resources
- network volumes

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
- 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

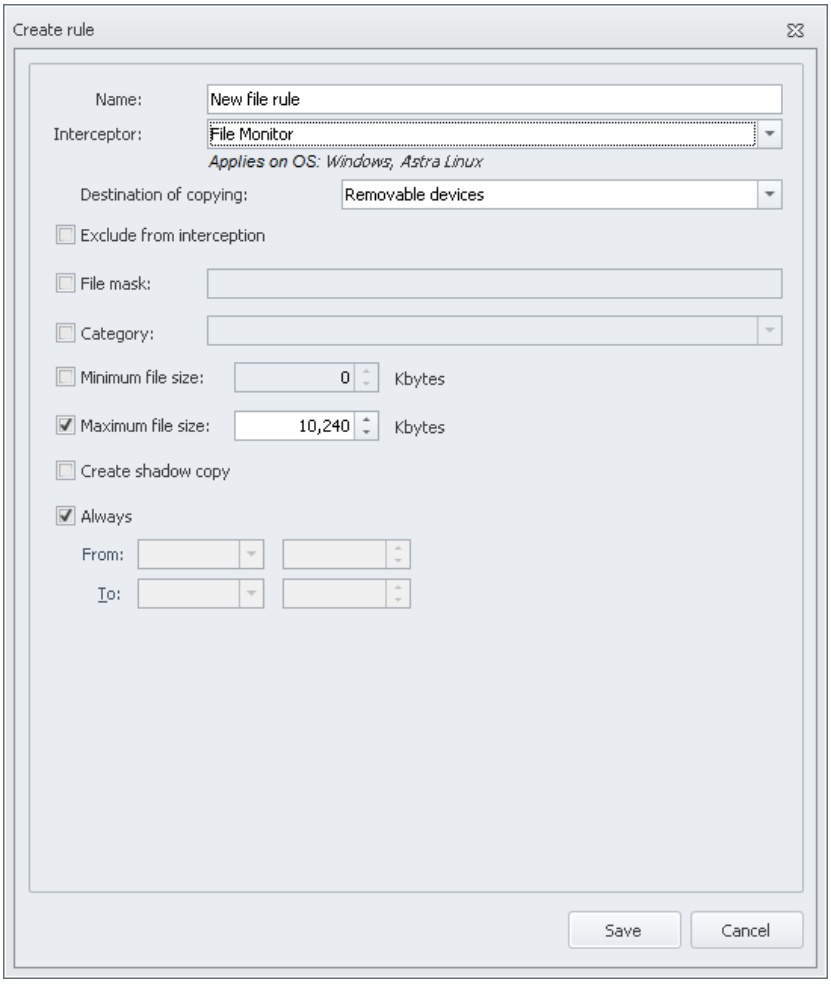
  > **Note:**
  >
  > File renaming on media devices is not supported.

- 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 rule applies on computers with MS Windows and Astra Linux OS.
>
> On computers with Astra Linux, the rule controls only copying/moving files to removable devices connected via USB and FireWire.

> **Warning!**

Information about rule (DM) conflict resolving see in "Applying Rules (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;
   - press Ctrl+Shitf+N.
4. In **Create rule** dialog in **Interceptor** field, select **File Monitor**.
5. Enter rule (DM) name to the **Name** field.
6. In the **Destination of copying** field, specify objects whose copying will be intercepted. The can be removable devices or network volumes.

7. If you want to exclude specific files from interception, flag **Exclude from interception**. For operations 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.

8. 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.

> **Note:**
>
> On computers with Astra Linux, file masks are ignored.

9. 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.

> **Note:**
>
> On computers with Astra Linux, signature categories are ignored.

10. 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.
11. 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.

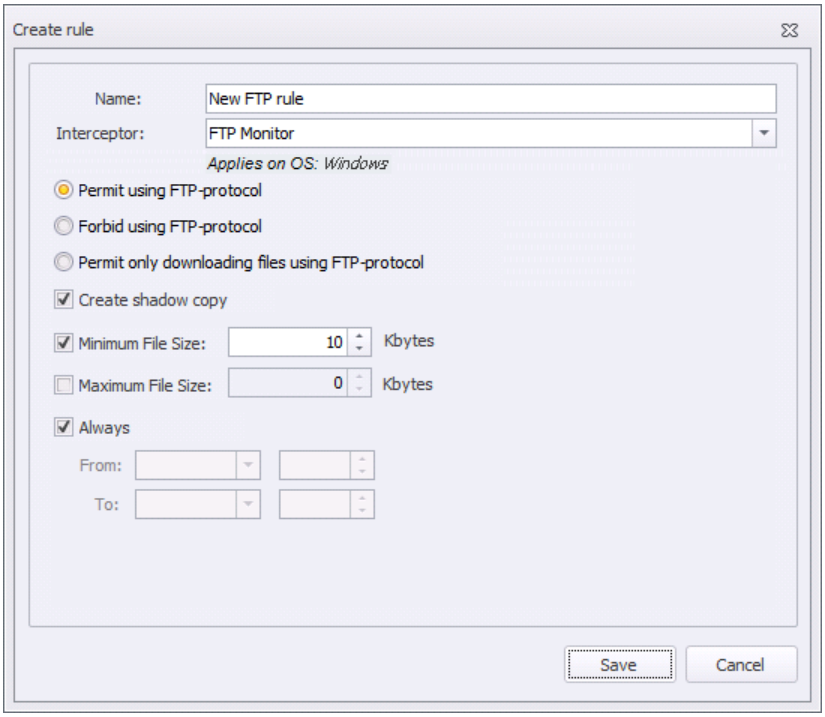
12. Define a period of rule (DM) action. By default, the rule (DM) is always in effect (**Always** option is checked). To specify a period, clear **Always** check box and specify dates and time in **From** and **To** fields.
13. When all parameters are configured, click **Save**.

## Configuring FTP Monitor Rule (DM)

**FTP Monitor** interceptor allows you to control data transfer through FTP/FTPS protocol.

> **Note:**
>
> The rule applies on computers with Windows OS.

> **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 the file size is within specified range, then file transfer event will contain a shadow copy; otherwise, an 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;
   - press Ctrl+Shift+N.
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.

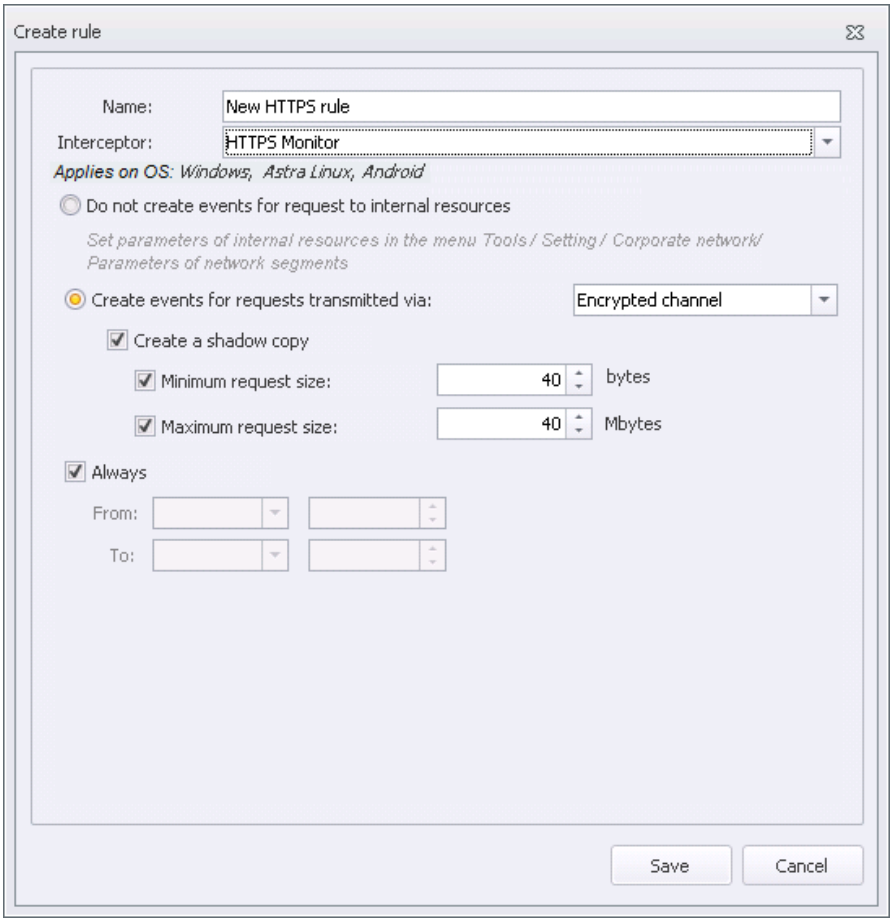
   > **Warning!**
   >
   > If FTP Monitor rule (DM) should create a shadow copy of file but there is less free system drive space left than required by the policy (DM) (see "Creating Shadow Copies and Blocking Operations Due to Free Space Shortage") then shadow copies of messages still will be created 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 a period, clear **Always** check box and specify dates and time in **From** and **To** fields.
9. When all parameters are configured, click **Save**.

## Configuring HTTPS Monitor Rule (DM)

**HTTPS Monitor** interceptor allows you to control data transfer through HTTP and HTTPS protocol.

## Note:

The rule applies on computers with MS Windows and Astra Linux OS and mobile devices on Android platform.




**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;
   - press Ctrl+Shift+N.
4. In **Create rule** dialog in **Interceptor** field, select **HTTPS Monitor**.
5. Enter rule (DM) name to the **Name** field.
6. Specify parameters of events which are created when traffic is intercepted. You can:

- disable interception of events to internal resources. For this, select the **Do not create events for request to internal resources** option. Requests within the corporate network (on configuring network segments, see "Settings of Corporate Network", **Parameters of network segments** group) will not be intercepted.

  > **Important!**
  >
  > If you select this mode, then creating a shadow copy in the rule will be unavailable. If you need to:
  >
  > - not create events for requests to internal resources
  > and
  > - create shadow copies
  >
  > then create two separate rules: a single rule for each requirement.

  > **Important!**
  >
  > For mobile devices, traffic to internal resources cannot be excluded from interception.

- configure data interception via encrypted channels or via all channels. For this, select the **Create requests for events transmitted via** option and from the drop-down list select:
  - **All Channels**
  - **Encrypted channel**

  If you want to save shadow copies of sent files, select the **Create shadow copy** option. You can also specify additional settings for shadow copies:
  - **Minimum request size**. If the check box is selected, shadow copies will be enabled only for files of 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.

  > **Important!**
  >
  > 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.

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**.

**Specifics of applying the rule on computers with Astra Linux OS:**

1. Connections via IPv6 protocol are not intercepted.
2. Requests related to webmail are intercepted similar to common HTTP requests.
3. Rules with the enabled setting **Do not create events for request to internal resources** are ignored.

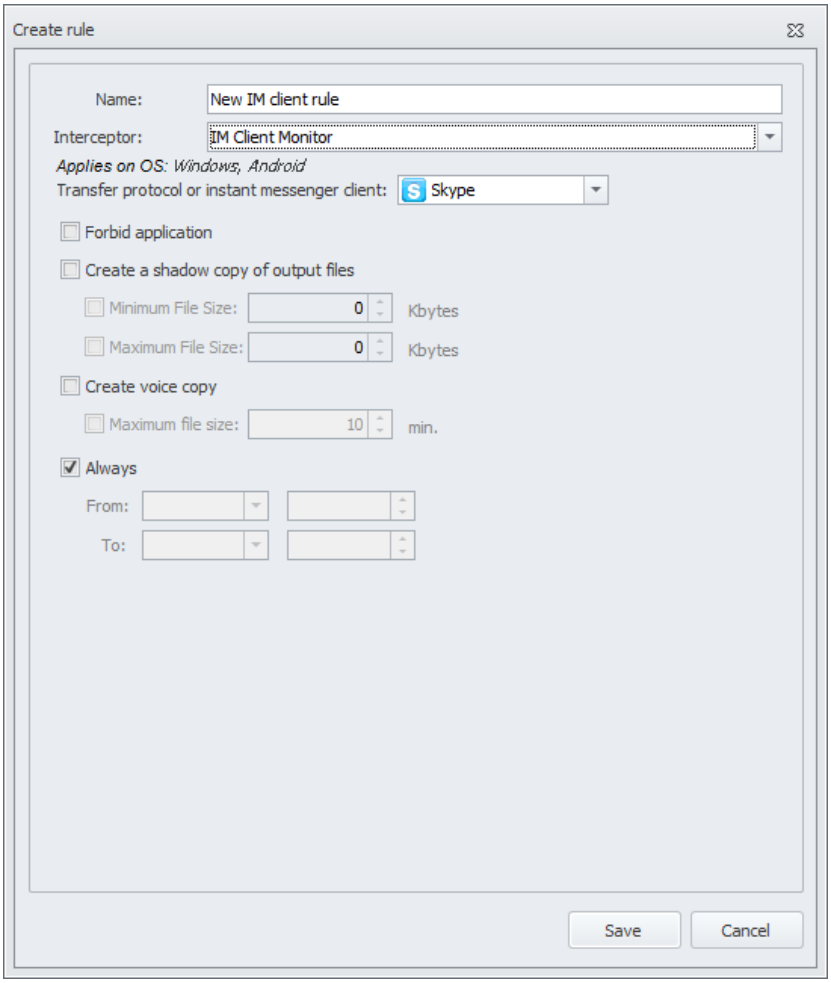
## Configuring IM Client Monitor Rule (DM)

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

> **Note:**
>
> The rule applies on computers with MS Windows and mobile devices on Android platform.

> **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**.

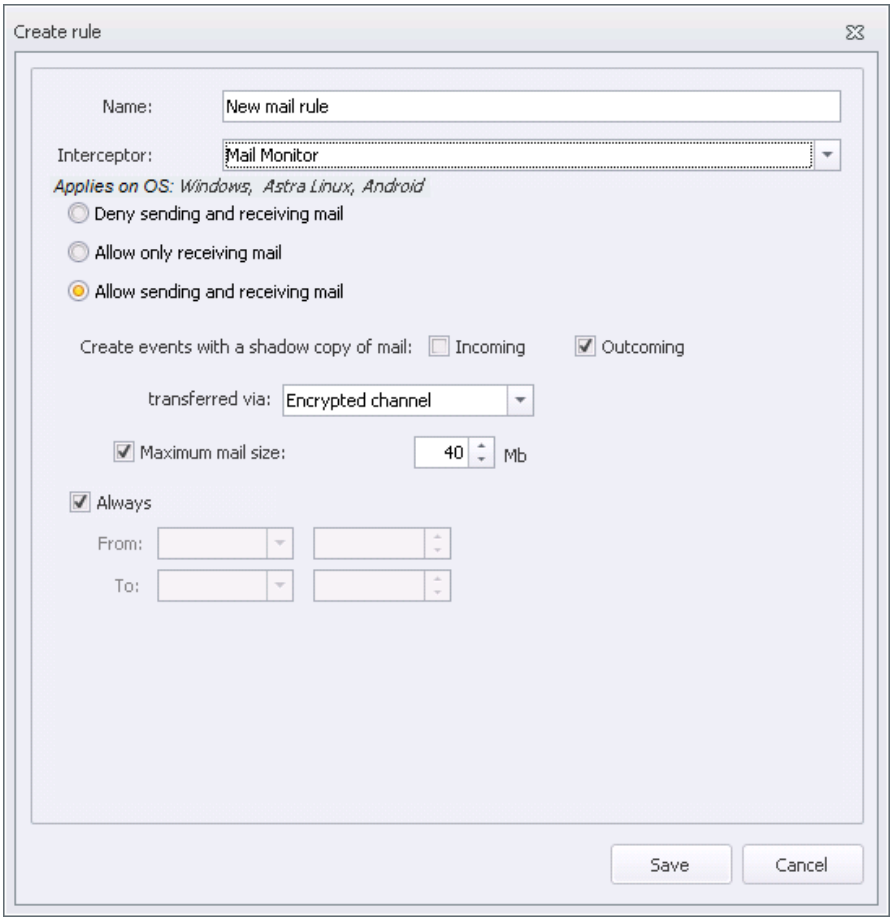
> **Warning!**
>
> In case shadow copy of message or chat must be created in accordance with an active IM Client Monitor rule (DM), but there is less free space on a computer, than it was defined by a policy (DM) (see "Creating Shadow Copies and Blocking Operations Due to Free Space Shortage"), then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

## 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.

> **Important!**
>
> The rule applies on computers with MS Windows and Astra Linux OS and mobile devices on Android platform.
>
> On computers with Astra Linux, the rule controls only SMTP, POP3, and IMAP 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;
   - press Ctrl+N.
4. In **Create rule** dialog in the **Interceptor** field, select **Mail Monitor**.
5. Enter the rule (DM) name to the **Name** field.
6. Choose the control level for sending and receiving emails:
   - **Deny sending and receiving mail**;
   - **Allow only receiving mail**;
   - **Allow sending and receiving mail**.

> **Warning!**

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

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

7. Configure creation of shadow copies. Select the **Incoming** or **Outcoming** checkbox in the **Create events with a shadow copy of mail** line.

> **Warning!**
>
> If the **Allow sending and receiving mail** option is enabled, then at least one mail direction (**Incoming** or **Outgoing**) should be selected, otherwise, the rule won't be saved.

You can also define additional parameters of shadow copies:

- **Transferred via**. Possible variants:
  - **All channels** - to create a shadow copy of emails sent through any channels;
  - **Encrypted channel** - to create a shadow copy of emails sent via encrypted channels.
- **Maximum mail size**. If the option is enabled, shadow copies will be created only for emails whose size is smaller or equal to the specified one.

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

8. Define a period of the 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.
9. 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.

## Configuring Network Monitor Rule (DM)

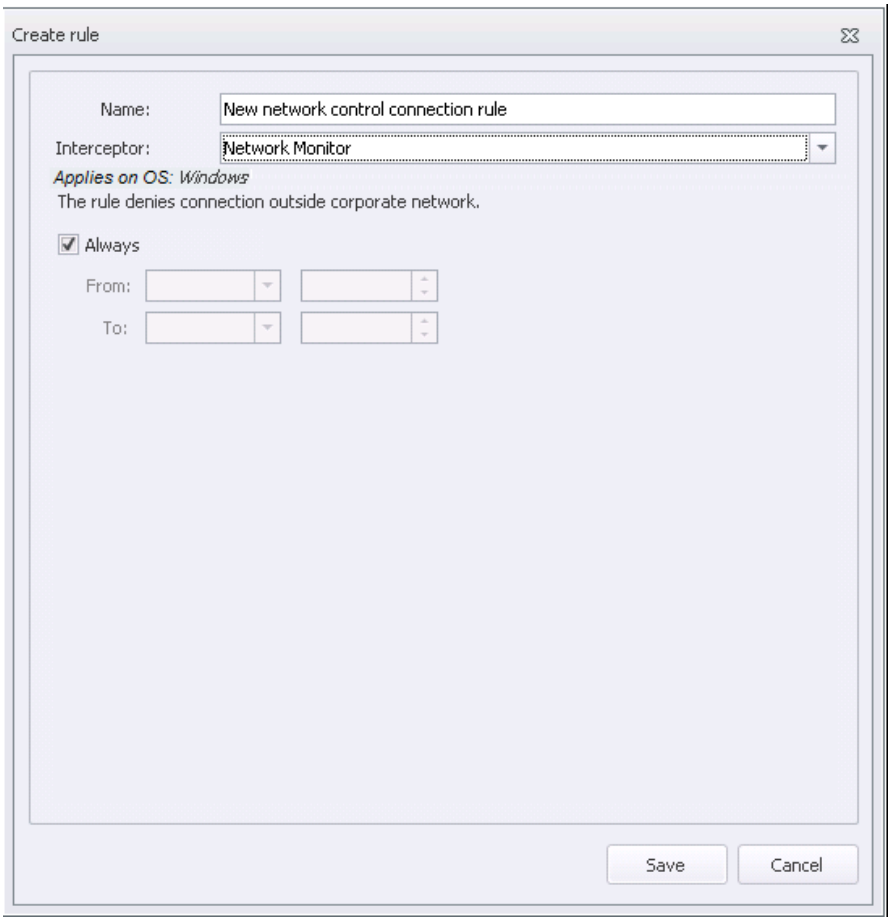
Network Monitor interceptor lets to deny transferring data by any network connections except connections with the corporate network or specified permitted servers. Configuring segments of the corporate network and permitted external addresses is performed as described in "Settings of Corporate Network".

### Note:

The rule applies on computers with MS Windows OS.

### 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").



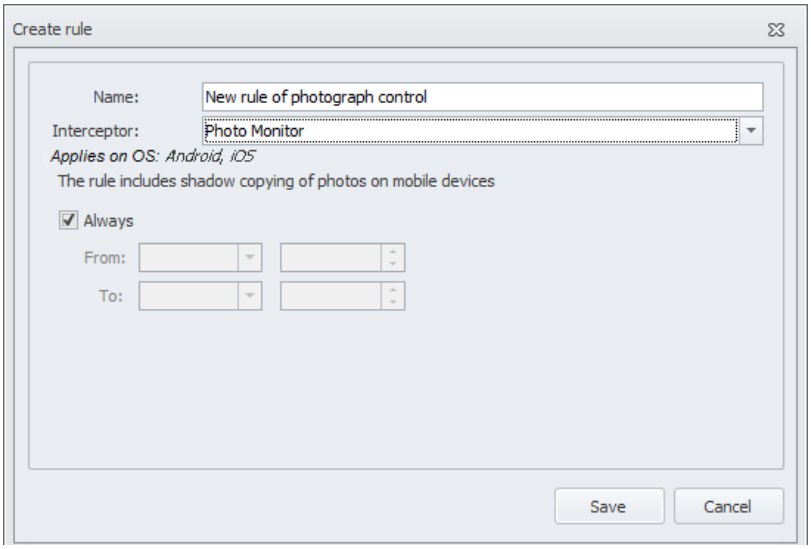

**To configure the rule, perform the following steps**:

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**.

## Configuring Photo Monitor Rule (DM)

Photo Monitor interceptor allows you to perform shadow copying of photos taken with cameras of controlled mobile devices.

> **Note:**
>
> The rule applies on mobile devices on Android and iOS platforms.




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

1. Go to the **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;
   - press Ctrl+Shift+N.
4. In the **Create rule** dialog in the **Interceptor** field, select **Photo Monitor**.
5. Enter rule (DM) name to the **Name** field.

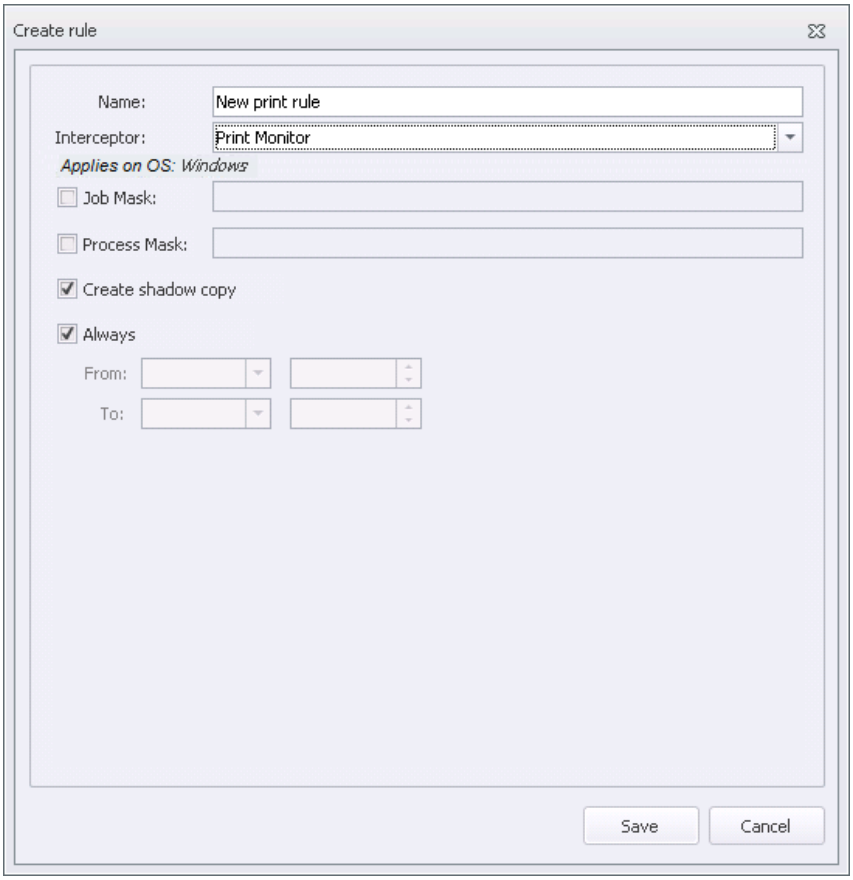
> **Warning!**
>
> If there is not enough free space on a workstation (see. "Creating Shadow Copies and Blocking Operations Due to Free Space Shortage"), a shadow copy will not be created.

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**.

## 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.

> **Note:**
>
> The rule applies on computers with MS Windows OS.




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

1. Go to the **Policies** section.
2. In the **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;
- press Ctrl+Shift+N.

4. In the **Create rule** dialog in the **Interceptor** field, select **Print Monitor**.
5. Enter rule (DM) name to the **Name** field.
6. If necessary, you can limit controlled print tasks using masks:
   - **Job Mask**. A mask is used for a task (document) which is sent to print. If you want to set the mask, select the checkbox and specify the mask.
     The print task name is formed by the application, from which document is sent to print. So, the name can be any text, not necessarily related to the type of the document.
     In the mask, you can use substitution symbols : «?» to replace one character or «*» to replace several characters. Spaces are treated as a part of the task name.
   - **Process Mask**. A mask is used for the process, which executes the print task. If you want to set a mask for a process, select the checkbox and specify the mask.
     The name (a full path) of the process is obtained for the process, in whose context rendering of the print task is performed. In some cases (local LPT- and COM-printers), printing subsystem can perform rendering in the context of the Print Spooler service. The path to the executable file of the service is `%SystemRoot%\system32\spoolsv.exe`.
     For the process name to be identified correctly, it is necessary to set the **Print directly to the printer** parameter in the printer properties (**P rinter properties** > **Additionally** ). Then, the task will be processed in the context of the application, from which the document is sent to print. However, in this case, printing will be synchronous, so you won't be able to work with the application until the document is printed .
     In the task mask, you can use substitution symbols : «?» to replace one character or «*» to replace character set. Spaces are treated as a part of the task name.
7. If you want to create shadow copies of printed documents and send them to Traffic Monitor, select the **Create shadow copy** checkbox.

   > **Warning!**
   >
   > If there is less free space on the computer than required by the policy (DM) (see "Creating Shadow Copies and Blocking Operations Due to Free Space Shortage"), then the document will be printed without creating a shadow copy.

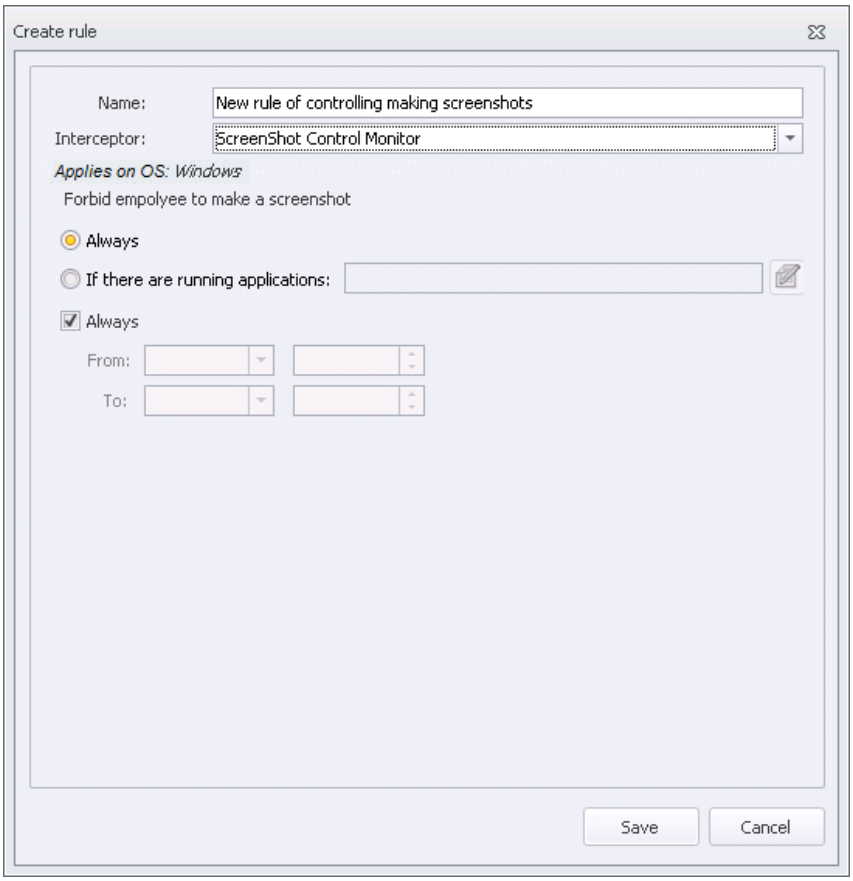
8. Define a period of rule (DM) action. By default, the rule (DM) is always in effect (**Always** option is checked). To specify rule (DM) duration, clear **Always** check box and specify dates and time in **From** and **To** fields.
9. When all parameters are configured, click **Save**.

## Configuring ScreenShot Control Monitor Rule (DM)

**ScreenShot Control Monitor** interceptor allows you to control screenshots on the agent side.

## Note:

The rule applies on computers with MS Windows OS.




**To configure the rule, 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 the **Name** field.
6. In **Forbid employee to make a screenshot** area, define a rule (DM) period::
   - **Always**. Has no time limit by default.
   - **If there are running applications**. Select this option to specify applications using button (see "Applications protocol").

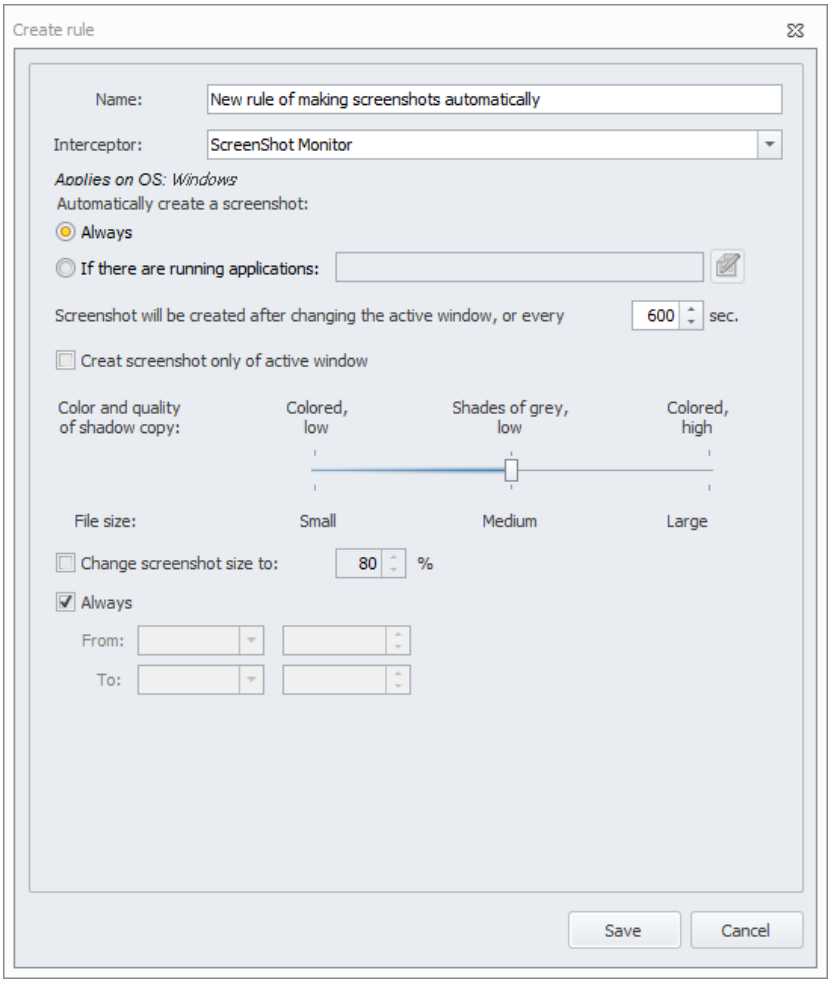
7. Define a period of rule (DM) action. By default, the rule (DM) is always in effect (**Always** option is checked). To specify rule (DM) duration, clear **Always** check box and specify dates and time in **From** and **To** fields.
8. When all parameters are configured, click **Save**.

## Configuring ScreenShot Monitor Rule (DM)

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

> **Note:**
>
> The rule applies on computers with MS Windows OS.

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

## 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.

## 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.

## 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 "Applying Rules (DM)".

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

Guidelines on account management is available in:

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

## Viewing Employee and Employee Groups Details

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

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

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

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

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

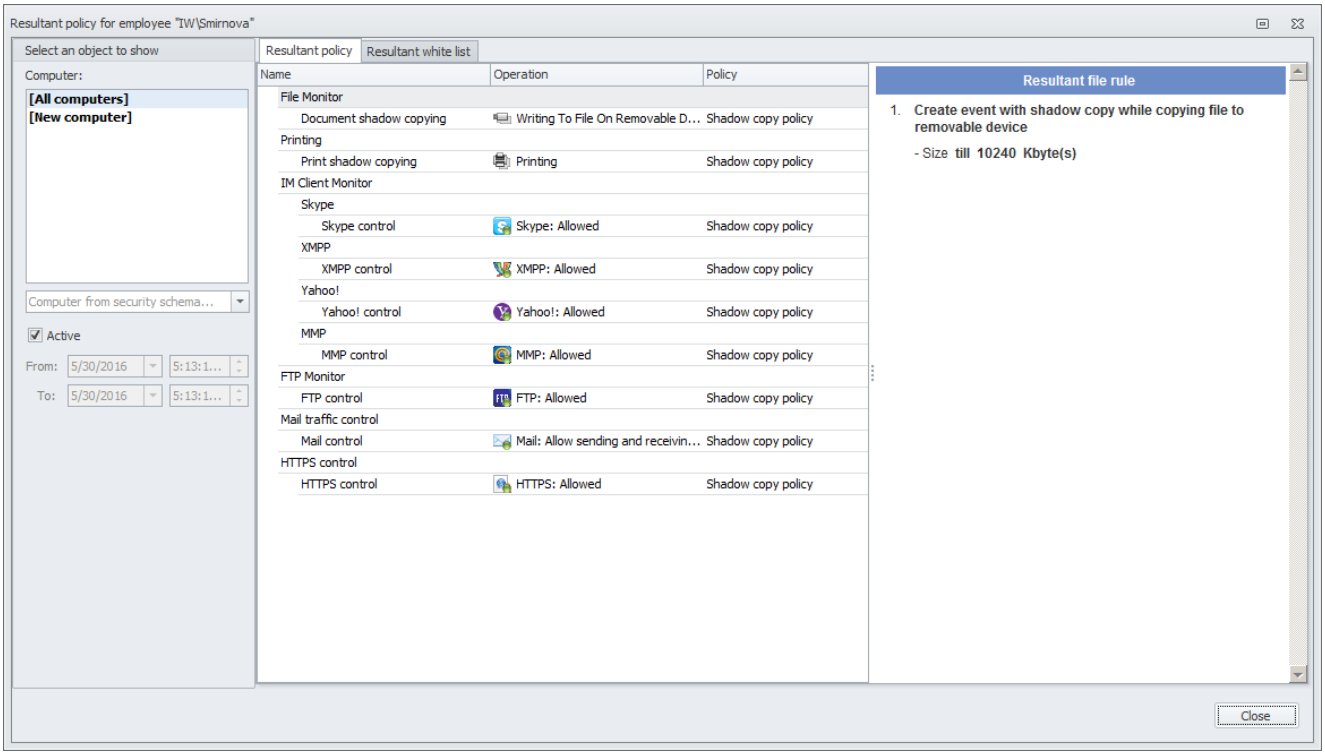
> **Note:**
>
> Some information on **Details** panel is duplicated in the main screen workspace.

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

**To view information about policy for an employee**:

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

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




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

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

**On a Workstation pane**:

- **All Workstations** - resulting policy (DM) for an employee account without attachment to a workstation.
  **Note**: to view resulting policy (DM) of an employee for a definite workstation, pick a workstation from Workstation pane or drop-down list Workstations from security schema.
- **New workstation** - resulting policy (DM) for an employee on a new workstation (it is not yet present in the security schema).
- To see resulting policy (DM) for chosen user on a definite computer:
  - from the **Computer** list, choose the name of the computer, on which chosen account is registered

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

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

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

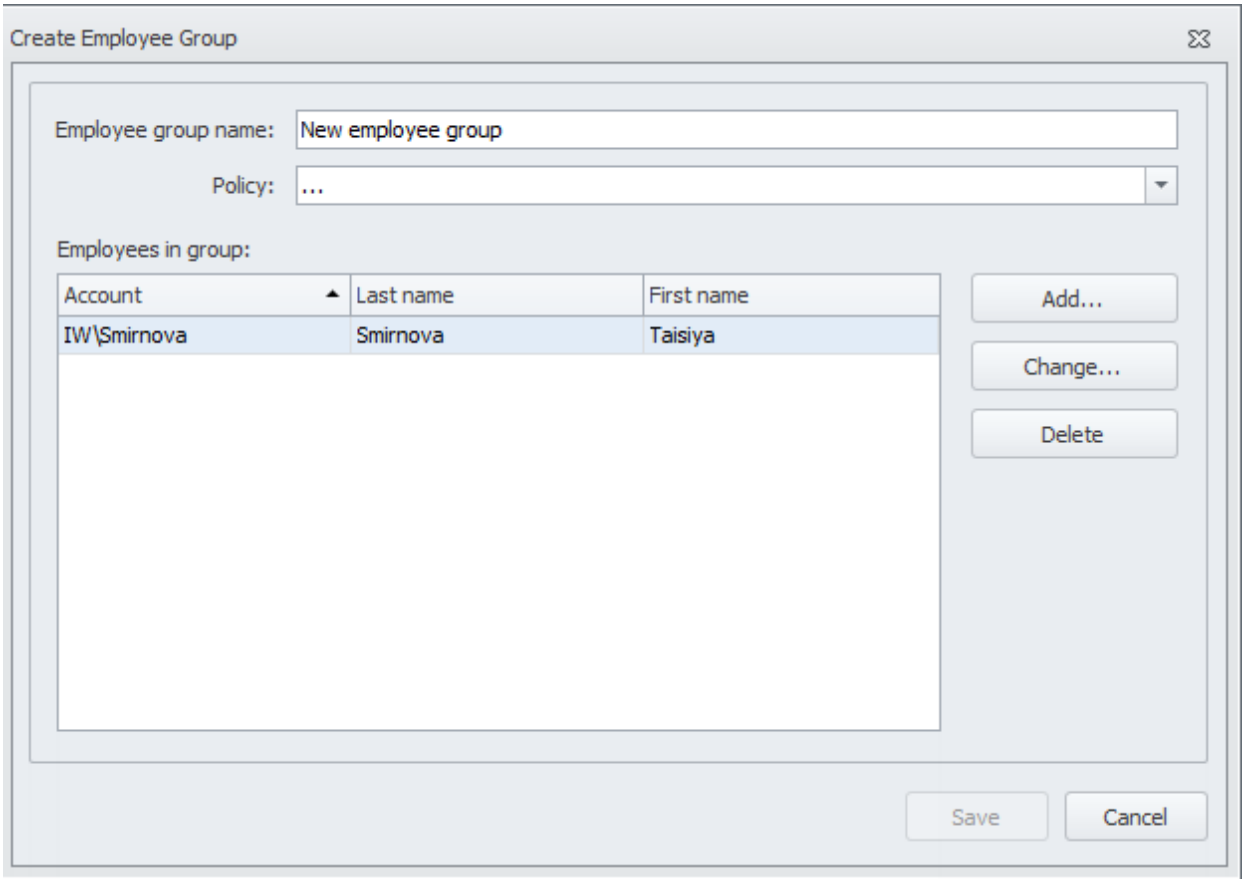
## Adding and Editing an Employee Group

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

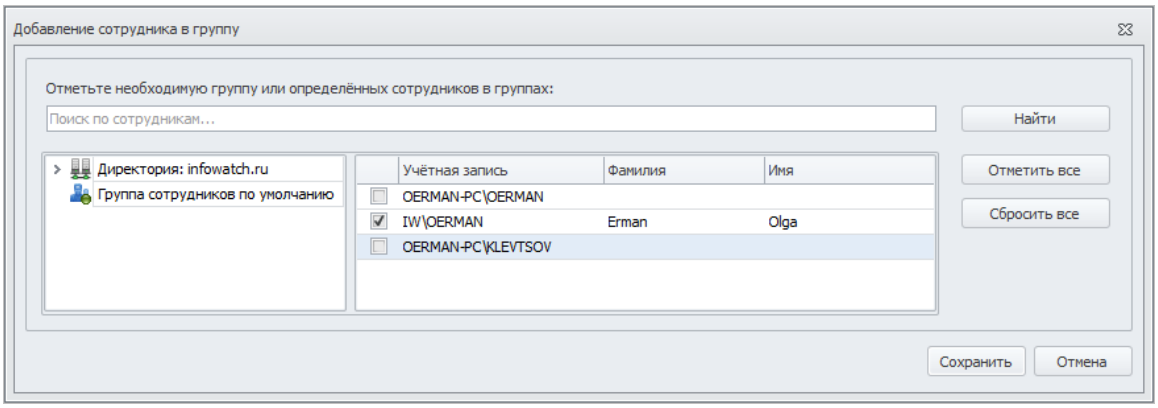
1. Go to **Employees** section.
2. Take one of the following steps:

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

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




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




   The **Add employee to the group** dialog displays a list of accounts imported from the directory service (see "Connecting to LDAP Server and synchronization with Active Directory and Astra Linux Directory") and already registered in the System (for example,

when Device Monitor Agent was installed to the workstation) and belonging to existing Device Monitor employee groups. To add an employee, in left pane select a node in groups tree, then flag accounts you want to add to the edited group. To flag all accounts of selected node, click Mark all. To clear selection, click Clear all.

You can also make a search of account by all available elements: enter a part of account name to the field at the top and click Find. After you selected all needed accounts, click Save to close Add employee to the group dialog and return to a dialog box with group parameters. To edit account parameters, select it from the list of employees belonging to the group and click Change (see "Editing Employee Account").

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

5. Click **Save**.

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

## Deleting Employee Group

**To delete employee group**:

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

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

## Adding Employee Account to a Group

After InfoWatch Device Monitor Agent is installed on the workstation (see document "*InfoWatch Traffic Monitor. Installation guide*" "InfoWatch Device Monitor Agent Setup" article), data on all employees registered at it is automatically added to the Device Monitor security scheme, "Default" employee group. Therefore the policy (DM) assigned to "Default" employee group will be applied to all newly registered employees. In prospect security policy (DM) for an employee is defined by including its account to different employee groups.

**To move an employee account from one group to another:**

1. Go to **Employees** section.
2. In **Employees area** of Navigation pane select a group containing employee's entry.
3. In **Employees** area of the main screen, select an account which you want to add to another group. Left-click and hold the selected row and drag it to **Employees** area of Navigation pane. Move the cursor over the name of the group you want to add an account to. When a yellow arrow appears at the left of selected group, release left mouse button.

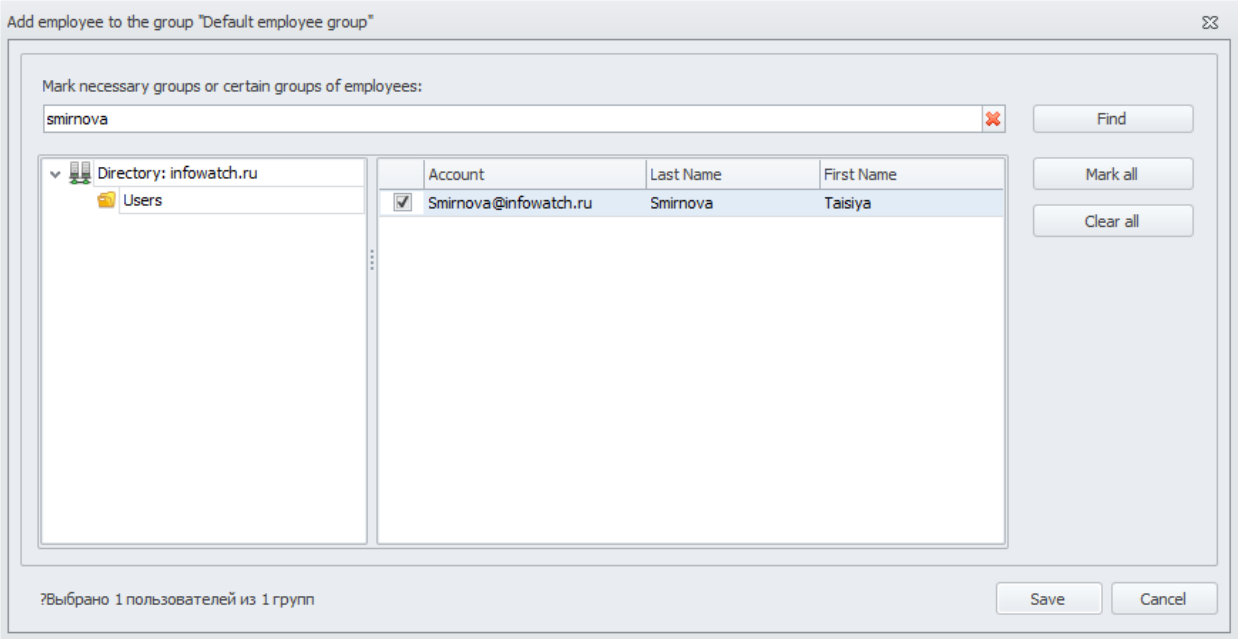
This adds an account to the selected group.

You can also manually import an information on the employee from directory service (see connection configuring description in "Connecting to LDAP Server and synchronization with Active Directory and Astra Linux Directory"). Then after this employee is registered at the workstation where InfoWatch Device Monitor Agent installed, this employee will be subject of policy (DM) of a group where the employee is added to.

**To add one or several accounts to employee group**:

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

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




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

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

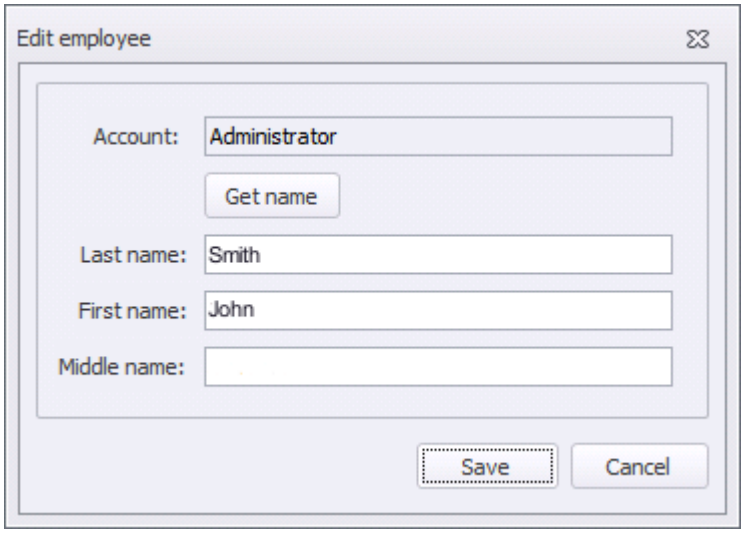
## Editing Employee Account

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

**To edit an employee account**:

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

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




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

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

## Removing Employee Account from Employee Group

**To remove an account from employee group**:

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

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

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

This removes employee account from selected employee group.

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

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

### Deleting Employee Account from Security Schema

**To remove employee account from security schema**:

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

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

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

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

## 4.3.4 Computers

In InfoWatch Device Monitor, a computer is a controlled computer where InfoWatch Device Monitor Agent is installed.

General principles of managing computers are described in "Computers and Computer Groups" section.

Active security policies (DM) can be applied only to a computer group. You can define a security policy (DM) for a certain computer by including it to a computer group.

> **Warning!**
>
> To each computer, both a security policy (DM) of the computer group and a security policy (DM) of the employee who is currently authorized on the computer apply. For information on resolving conflicts between rules (DM), see "Rules Application".

To go to Management Console (DM) section where you can manage computers, click **Computers** button on Navigation pane.

For more information on working with controlled computers, see:

- Viewing Computer Details
- Viewing Computer Effective Policy
- Adding and Editing a Computer Group
- Deleting Computer Group
- Adding Computer to a Group
- Removing Computer from a Group
- Deleting Computer from Security Schema
- Updating Agents on managed computers
- Diagnostics

On how to install the Agent on a mobile device or uninstall it, see "Mobile devices".

## 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: a list of computers included in the group will be displayed in the working area.

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

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

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

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

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

- **Type.** Type of computer - displayed only for stationary or mobile computers.
- **Model name**. Model of mobile device - displayed for mobile 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 Agents at managed computers.

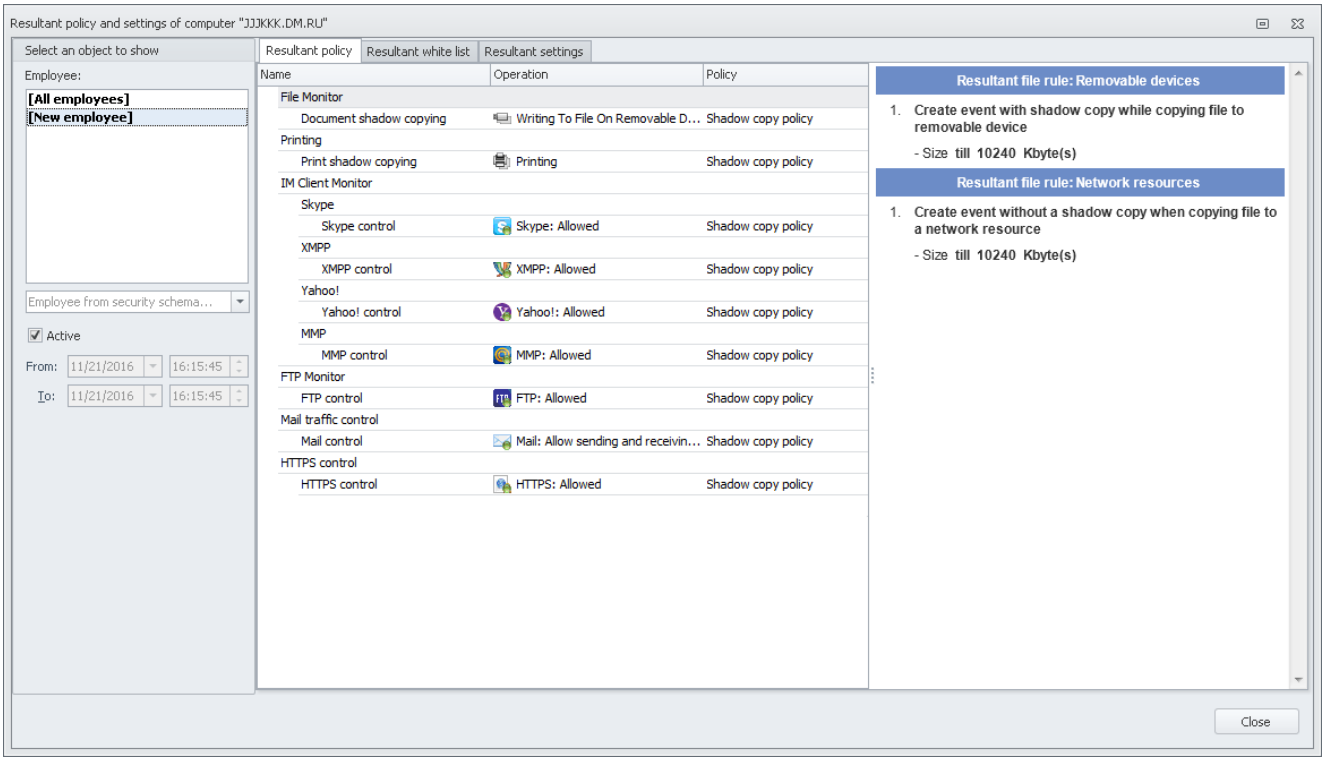
For more information on installing and deleting Agents for mobile devices see "Mobile devices".

## 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 resultant policy**.
   - on **Computers** pane, click **Show settings and resultant policy**.

As a result, a window **Show settings and resultant policy <computer name>** will be displayed**:** where by default 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 the 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 the computer (see "White lists"). To see detailed information about the device, select it from the list: detailed information will be displayed on the panel on the right.
- **Resultant settings** - settings of Sending data to the agent speed and Control disk space on agent, which are resultant on the computer, are displayed. Resultant settings consist of default settings and settings for computer group, which includes the selected computer. (see " Common Settings for Agents" and "Adding and Editing an Employee Group").

On the **Employee** pane, you can choose object for review:

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

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

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

- 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.

## Adding and Editing a Computer Group

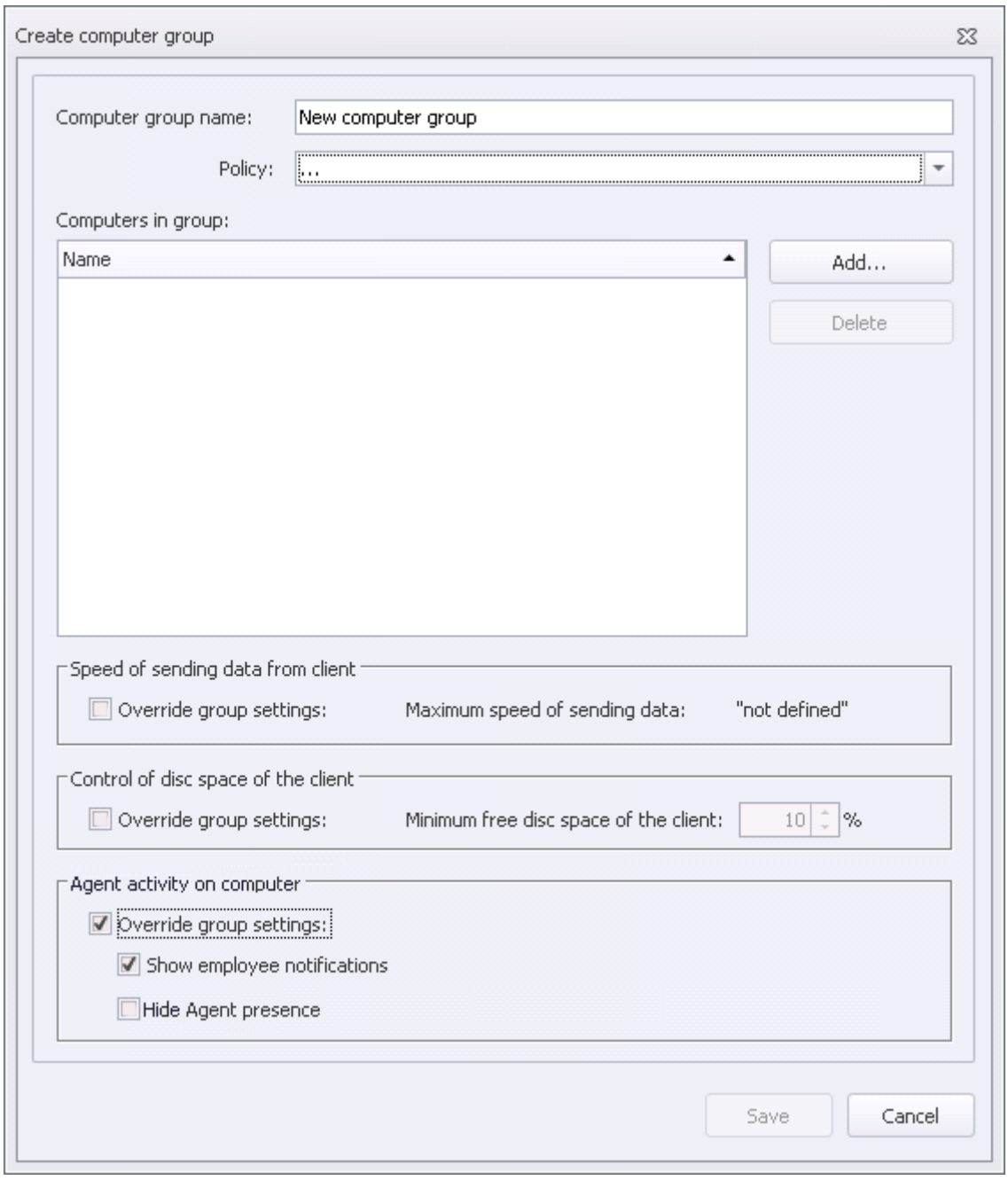
> **Important!**
>
> When you register a new computer, information on this computer is automatically added to the security scheme (to the "default" computer group).

**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**;<br>• click  **Create Computer Group** at the top of Navigation pane. |
| Edit computer group | a. In **Computers** area of Navigation pane select workstation group name.<br>b. Take one of the following steps:<br>• in the Main Menu select **Edit > Edit**;<br>• click  **Edit** at the top of Navigation pane;<br>• double-click selected workstation group name. |

This opens a dialog box with group parameters.




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

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

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

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

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

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

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

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

**Warning!**

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

## Deleting Computer Group

**To edit or delete computer group**:

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

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

5. Click **OK**.

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

## Adding Computer to a Group

When installing InfoWatch Device Monitor Agent (see the document "*InfoWatch Traffic Monitor. Installation Guide*", "InfoWatch Device Monitor Agent Setup" article), the computer is added to "default" computer group. To all computers within the "default", the policy assigned to this group will apply. Further on, you can assign security policies (DM) to the computer by adding it to various computer groups.

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

1. Go to **Computers**.
2. In **Computers** area of Navigation pane, select computer group that contains the computer.

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

You can also add information about computers without InfoWatch Device Monitor Agent manually. Computer information is imported from directory service (connection configuring settings see in "Connecting to LDAP Server and synchronization with Active Directory and Astra Linux Directory") 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. The main screen will display a list of all computers inside the group.
3. Take one of the following steps:
   - in the main menu select **Edit > Add computer**;
   - click **Add computer** located at the top of **Computers** area;
   - right-click in the workspace and select **Add computer** from the drop-down menu.

   In the opened dialog you can select computers:
   - imported from directory service (for example Active Directory);
   - received from Microsoft Windows Network;
   - from ALD tree;
   - 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.
   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 information on selected computers to the computer group.

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

## Removing Computer from a Group

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

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

**To exclude computer from computer group**:

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

This removes computer from the group.

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

## Deleting computer from security schema

You can remove a computer from the list of registered computers (for example, computer discontinued operation). Computer information will not be deleted, but it will be marked as **Inactive** due to Agent deactivation.

If you don't want to save inactive computer information, you can delete its record.

**To remove computer from the security scheme**:

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

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

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

## Updating Agents on managed computers

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

**To update Device Monitor Agents on all managed computers of the group**:

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

**To update Device Monitor Agents on selected computers**:

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

This creates and runs the update task for the selected computers.

### Diagnostics of the Workstation

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

> **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 Agent supports mobile devices specified in the document "*InfoWatch Traffic Monitor. Installation Guide*", the page "Hardware and Software Requirements".

> **Note:**

InfoWatch Device Monitor Mobile Lite application can be downloaded from Google Play and provides the following functionality:

- Control of incoming and outgoing SMS messages;
- Control of cloud storages: YandexDisk, Google Drive, DropBox;
- Control of Skype text chats;
- Control of photos;
- Possibility to replace GPS coordinates.

**Important!**

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 Agent, the following requirements should be met:

- USB Debugging mode must be 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 Agent 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

## 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 Agent, you should:

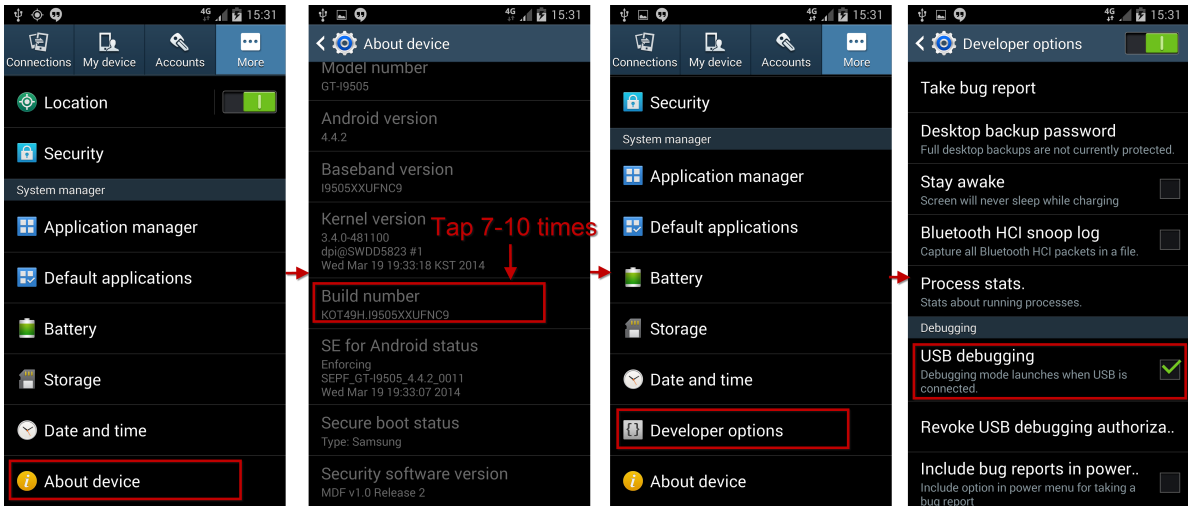
1. Enable "**USB debugging**" mode on the device: see example below.
2. Via a USB-wire connect this device to the computer where Device Monitor Management Console is running.
3. If necessary (for example, for some builds of Samsung), install additional drivers.

### Step 1. Enabling "USB debugging" mode

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

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

1. Enable developer mode: **Settings -> About device -> Build number**; tap the build number several times (7-10).
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 the **Settings** menu. Select **Developer options** which appeared near **About device** section.
5. Select **USB debugging**.

You can disable the debugging mode when the installation, updating or deleting the InfoWatch Device Monitor Agent 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 computer.

### Step 2. Connecting to the computer

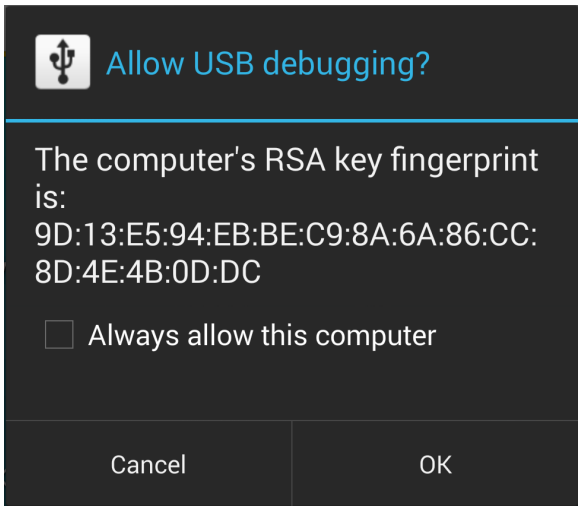
To install or update the InfoWatch Device Monitor Agent, you should connect the mobile device to the physical workstation where Device Monitor Management Console is running, via the USB-wire.

> **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 Agent 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.




### 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.

## 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 Agent, you should:

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

#### Step 1. Jailbreaking the mobile device

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

### Note:

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

#### Step 2. Installing iTunes

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

#### Step 3. Connecting to the computer

To install or update InfoWatch Device Monitor Agent, 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 the installation of Device Monitor Agent 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**).

**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**.

## 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 Agent, 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.

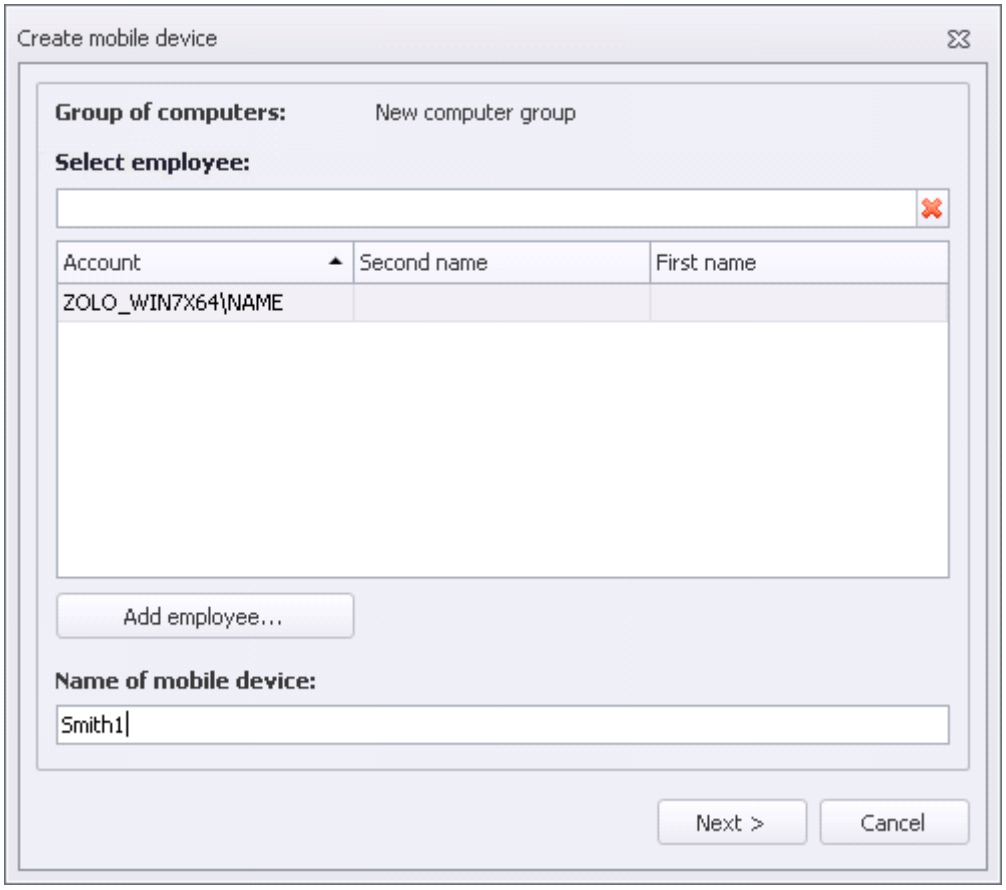
Details see in "Preparing a Mobile Device" and "Preparing a Mobile Device on iOS Platform".

**To add a mobile device to the computers group and install the InfoWatch Device Monitor Agent 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 Agent 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 Agent 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".

## 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 Agent, there should be:

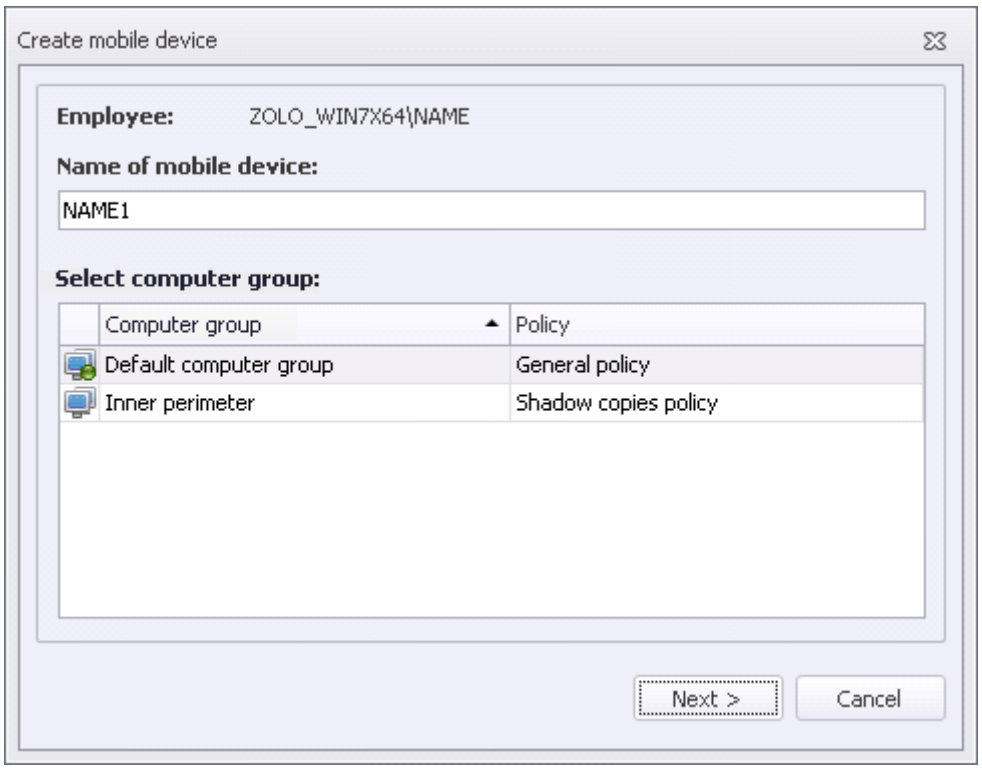
- USB Debugging mode enabled on the mobile device and all required drivers installed (for devices on Android platform only);
- the Management Console (DM) running on the physical workstation (using virtual machines or remote desktop connections is not recommended; using of the Microsoft Windows XP is 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 employee group and install the InfoWatch Device Monitor Agent 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 Agent 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 Agent 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".

## Deleting the Mobile Device

The removing the mobile device from the security scheme without uninstalling the InfoWatch Device Monitor Agent 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 Agent, 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);
- the 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 scheme and uninstall the InfoWatch Device Monitor Agent 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 Agent from the mobile device and delete the entry of a new mobile device from the computer group and security scheme.

### 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".

#### Viewing White List Details

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

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

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

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

**Details** panel displays properties table including the following information:

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

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

## Adding White List

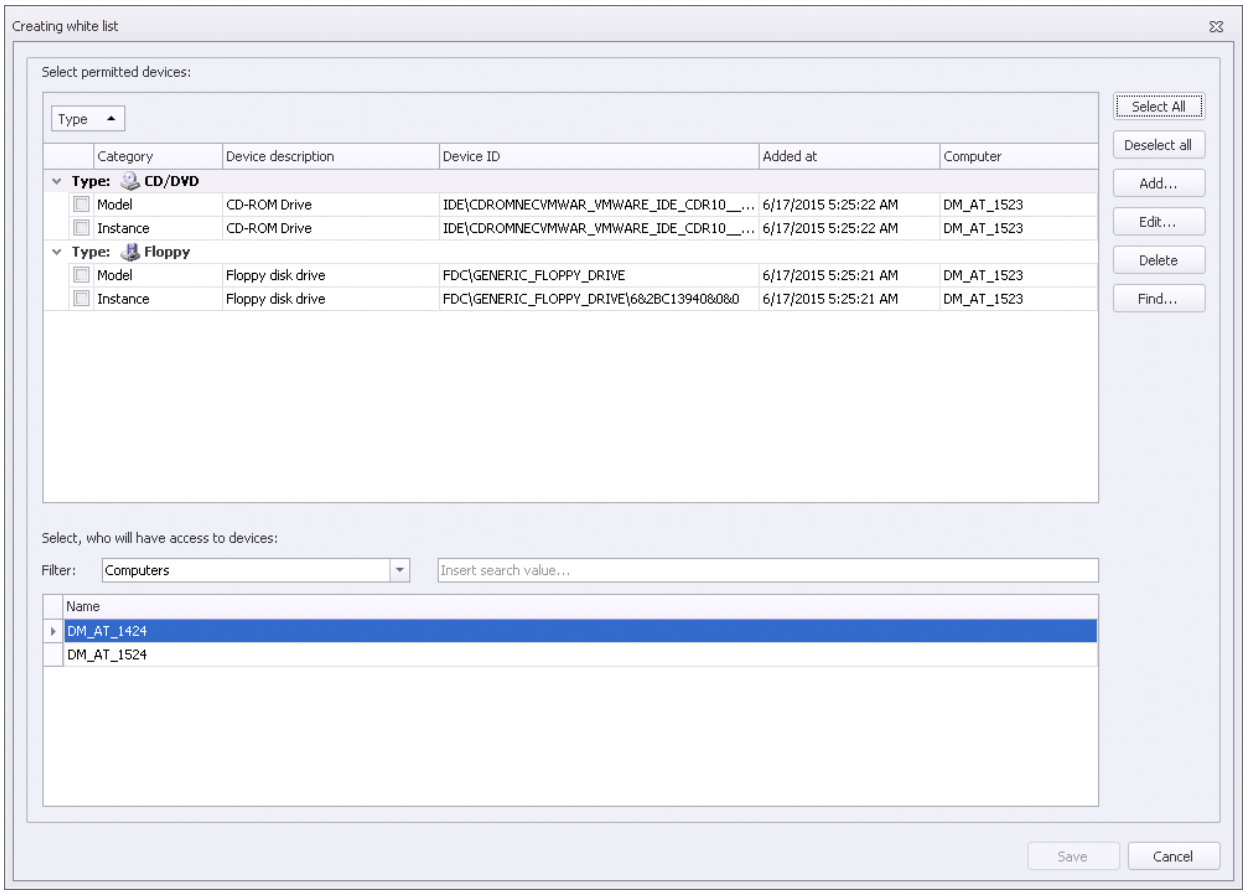
White list affects selected objects: employees, employee groups, computers or computer groups.

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

**To add white list**:

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

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




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

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

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

- computers
- computer groups

The list of entries will appear below.
You can also use a search string by entering a name or its part.

5. Select employee / employee group / computer / computer group that will have full access to selected
devices.
6. Click **Save**.

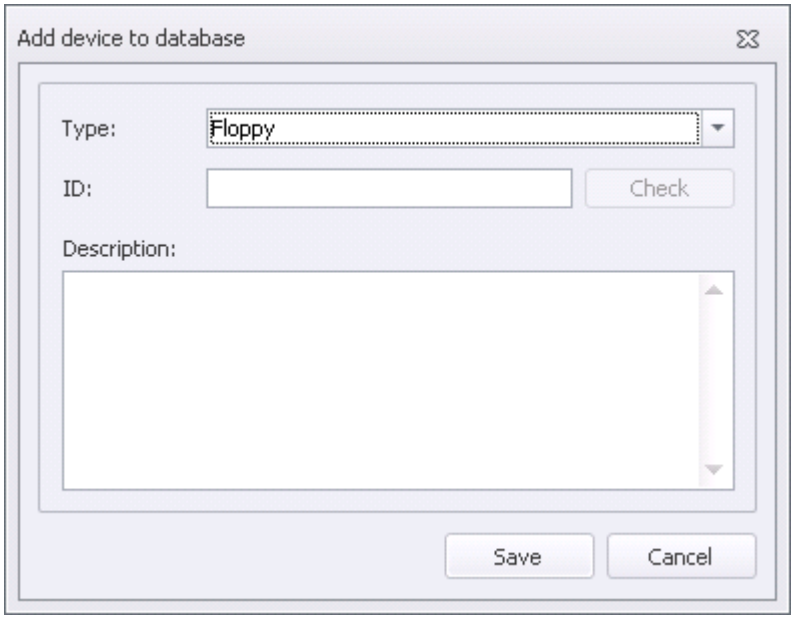
## Adding Device Entry

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

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

**To add device information manually**:

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




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

> **Note:**

To retrieve device instance string, connect the device and use standard Windows tools (for example, **Device Manager**) to view its properties. Device instance string is displayed on Information tab.

Device instance string is displayed as XXX\YYY\ZZZ where XXX is device type (usually, connection type, such as USB, IDE or ACPI), YYY is device model string (Vendor ID), and ZZZ is device instance string (Product ID).

Model ID is displayed as XXX\YYY where XXX is device type and YYY is model ID string (VID).

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

**Warning!**

When using instance code, take into account that some devices do not have unique ID: ID can be changed dynamically and differed even when connecting to different ports of the same computer.

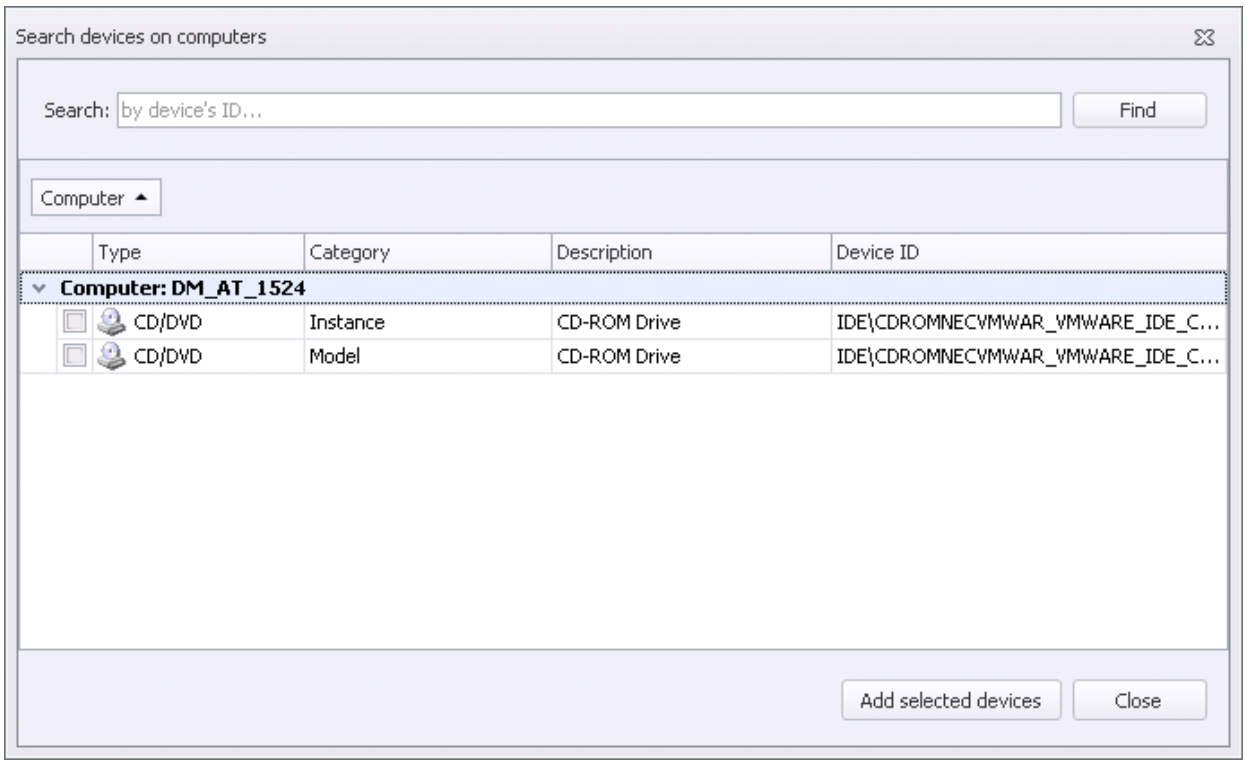
In such case using device model code is recommended.

- enter description into **Description** box.

4. Click **Add**.

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

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




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

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

## Deleting Device Entry

**To remove device entry from database**:

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

## Defining Entry Validity Period

Each device instance or model from the white list has an access permission displayed separately. This item's
(permission's) default validity period is practically infinite (from 01.01.1753 to 31.12.9999). You can

limit full access
period for this device. This device will be subject to general rules (DM) that apply to this device type before and after the
specified period.

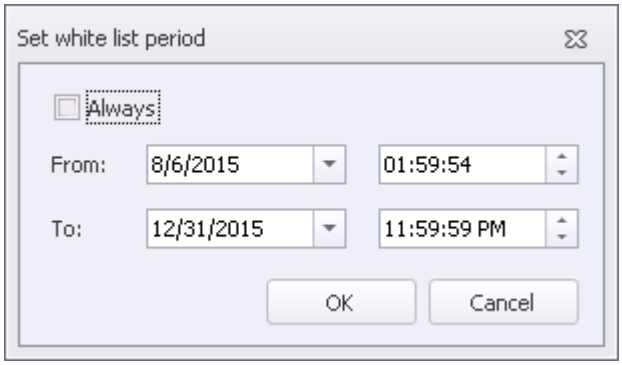
**To set white list entry period**:

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

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

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

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




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

## Editing White List

**To edit white list parameters**:

1. Go to **White Lists**.

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

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

## 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:

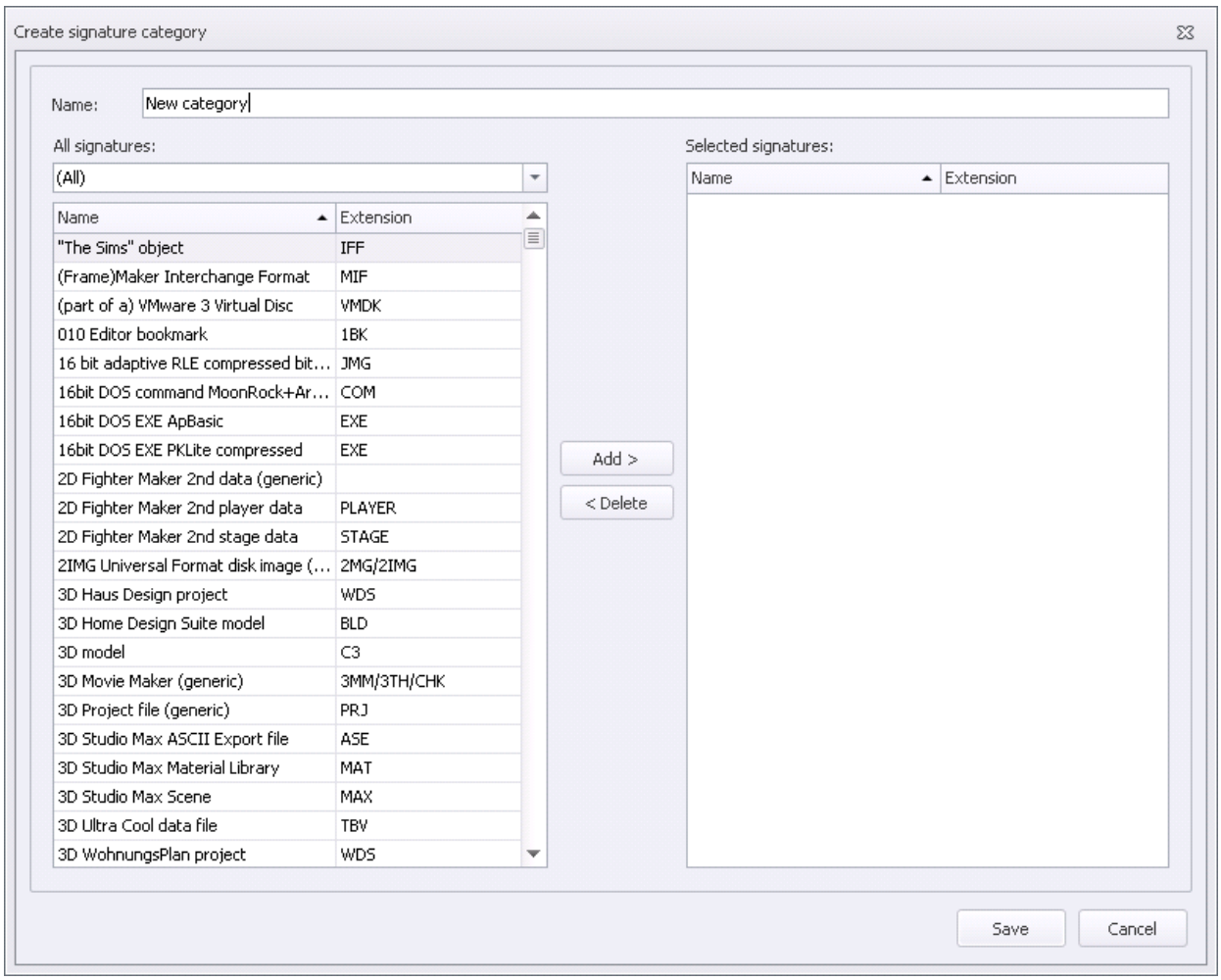
- create signature categories;
- fill created categories by copying predefined signatures;
- delete your signature categories, if they are not used by any rule.

## Adding Signature Category

**To add signature category:**

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

   **Create signature category** dialog appears.




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

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

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

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

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

## Editing Signature Category

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

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

or

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

**To copy a signature from one category to another**:

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

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

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

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

## Deleting Signature Category

> **Warning!**
>
> The following categories cannot be deleted:
>
> - signature categories used by any File Monitor rule (DM)
> - predefined signature categories.

**To delete a signature category:**

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

**Warning!**

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

### 4.3.8 Application Protocol

After the InfoWatch Device Monitor Agent is installed on 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 into two groups in this section: **List of applications** and **Applications Protocol**:

- The **List of applications** group contains lists used to control employee's access to applications:
  - forbid launching applications in one of two modes: white lists and black lists. See details in "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 details in "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.

## Creating an Application List and Adding Applications

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

**To create an empty application list**:

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

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

and "Adding Application to List Manually".

**To select an application from the list**:

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

**To edit application in the list**:

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

**To delete application from the list**:

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

in List of applications group menu click Create list of applications

## Creating and Editing the Application Protocol Filter

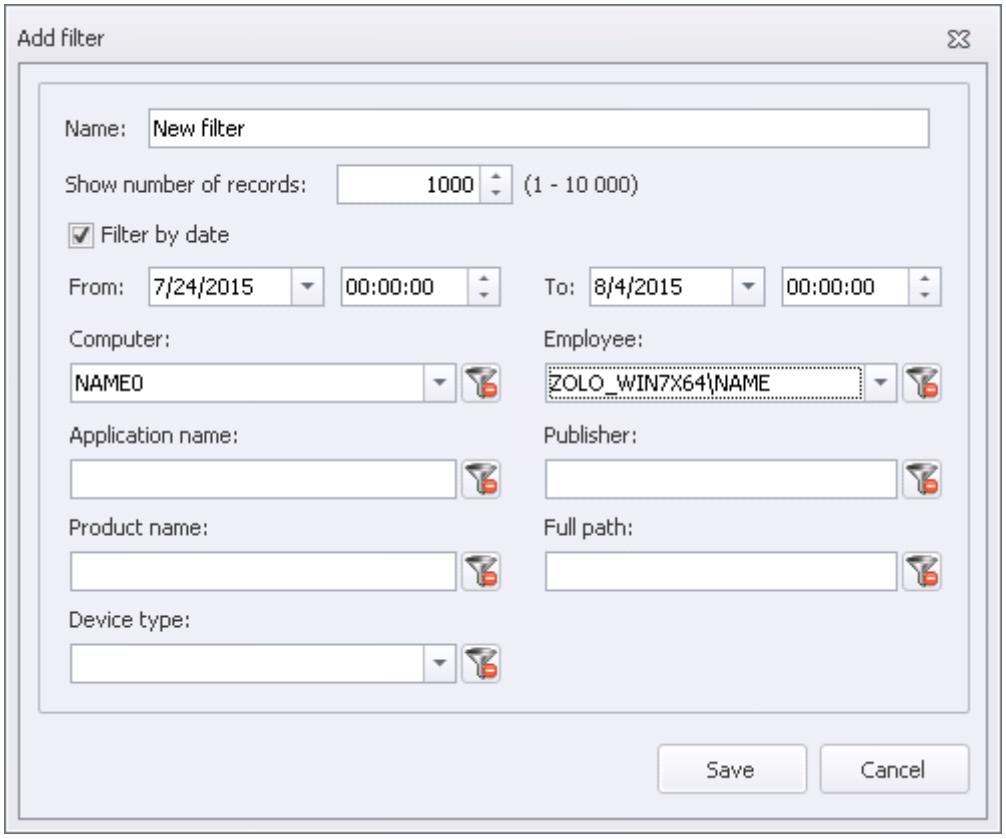
Filters allow you to configure the application protocol (see "Application protocol") to display information on applications that meet specified conditions.

> **Warning!**
>
> A preset **Today** filter shows applications which have been started on a particular day since initial installation of the Agent.
> The **All** filter shows applications which have been started right upon the Agent installation.

**To create a new filter**:

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

   This opens a dialog box with filter parameters.



3. Enter the name of the filter in **Name** field.
4. In the **Show number of records** field, enter the number of records you want to see in the protocol.
5. To set up period for the records to be displayed flag the **Filter by date** option and specify parameters **From** and **To**.
6. If needed, specify additional filter conditions:
   - in **Computer** field select employee's computer which protocol you need to view;
   - in **Employee** field select account of an employee who launches applications;
   - in **Application name** field type in the name of the application you want to see information about;
   - in **Publisher** field type in the program publisher;
   - in **Product** name field pick the name of the product;
   - in **Full path** specify the path to the application location;
   - 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 the filter.
7. Click **Save**.

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

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

## Adding Application to List Automatically

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

**To add application to the list automatically**:

1. Go to **Applications** section.
2. On the Navigation pane select the needed filter in the **Application protocol** group.
3. On the **Application protocol** pane select one or several entries. To select several entries click at them
   while pressing **Shift** or **Ctrl** button.
4. Take one of the following steps:
   - on the **Application protocol** pane click  **Add application to list automatically**;
   - select **Edit > Add application to list automatically** command in the main menu;

- right-click in the **Application Protocol** pane and select **Add application to list automatically**
  manually from the drop-down list.

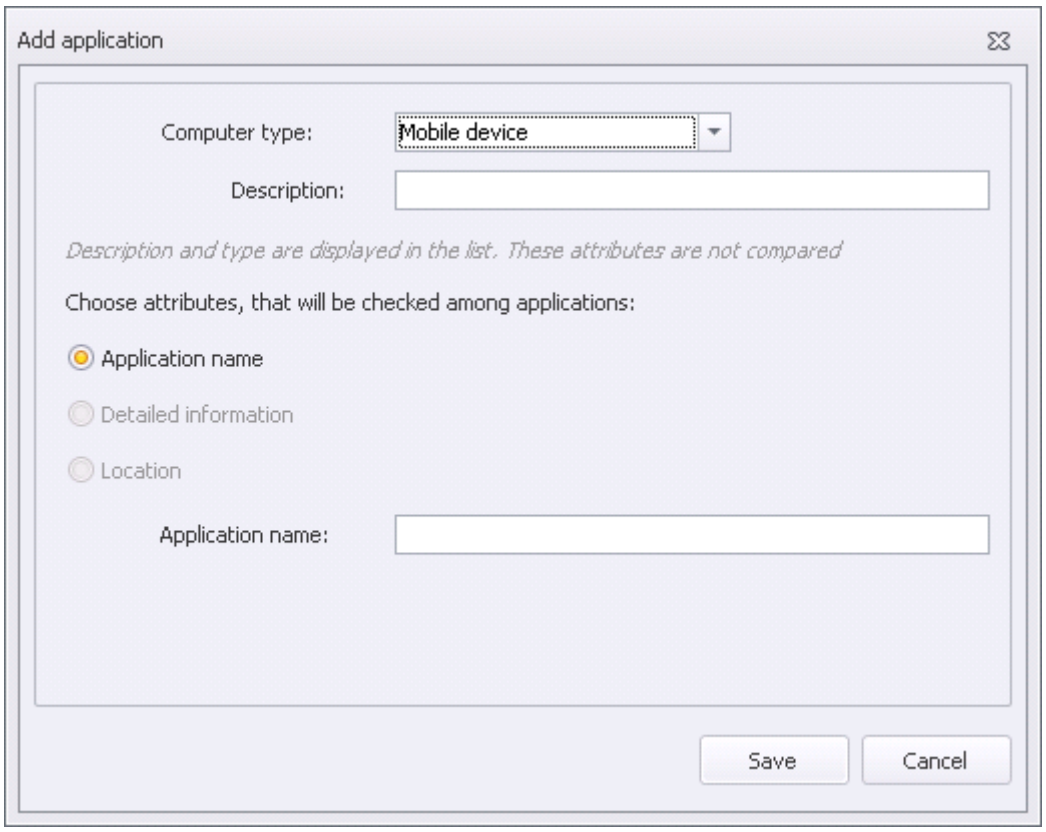
5. In the appeared window:
   - select existing list

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

## Adding Application to List Manually

**To add application to the list manually**:

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

### 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 Agent menu, **Network control** command.

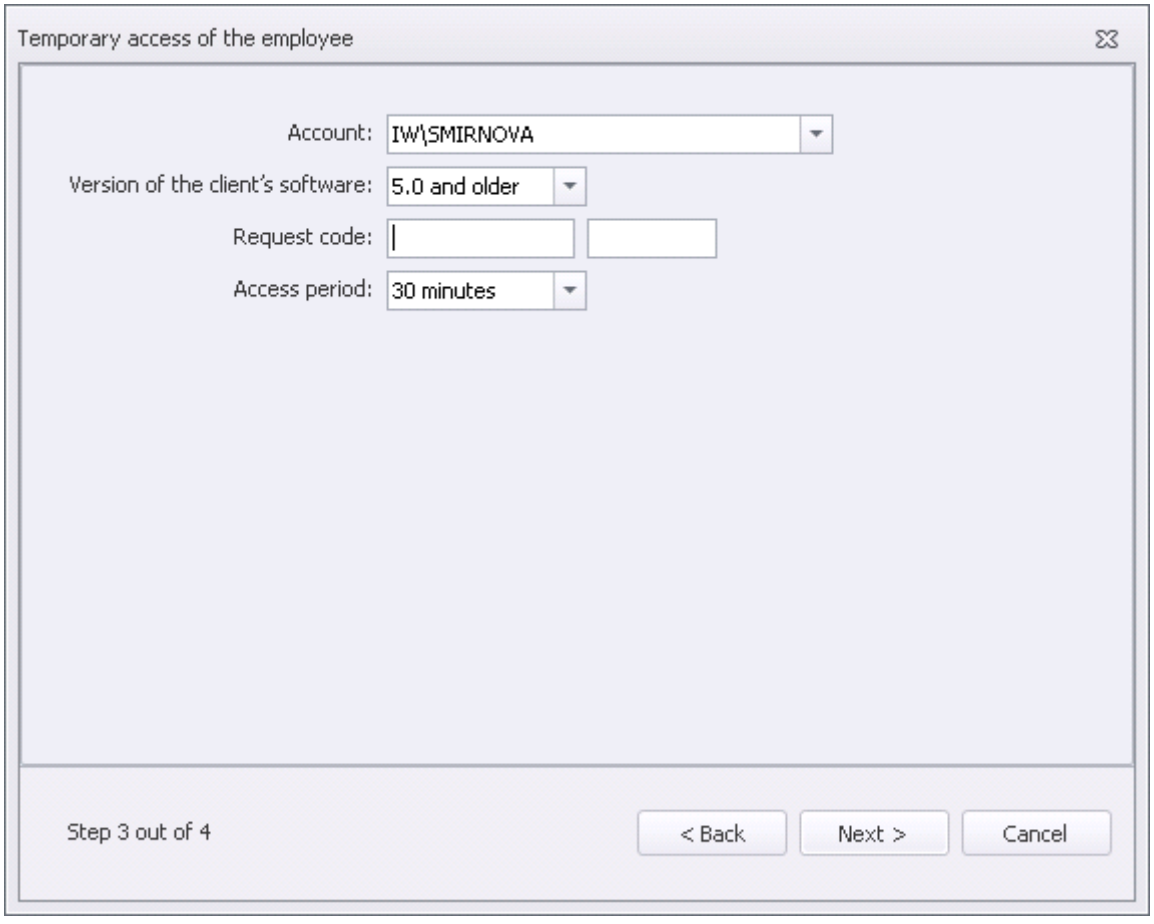
## Warning!

An employee can request access only if the **Show tray icon** interface option is selected (see "Common Settings for Agents"). The way how to configure text displayed to an employee is described in "Employee Notifications about Policy (DM) Violations", **"Network connection forbidden. Detailed"** notification type.

An employee should send the received request code to the security officer.

**To grant access to external connections for employee**:

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




4. From **Account** drop-down list, select an account of the employee to which a temporary access should be granted.
5. In **Version of client's software**, choose the version of Device Monitor Agent installed on employee's computer.
6. In **Request code** field, enter a code sent by the employee.
7. From **Access period** drop-down list, select the time period for which temporary access should be granted.

8. Click **Next**.
   The code which should be sent to the employee is displayed in **Response code** field.
9. Click **Close**.

# 4.5 Temporary Employee Access to Devices

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

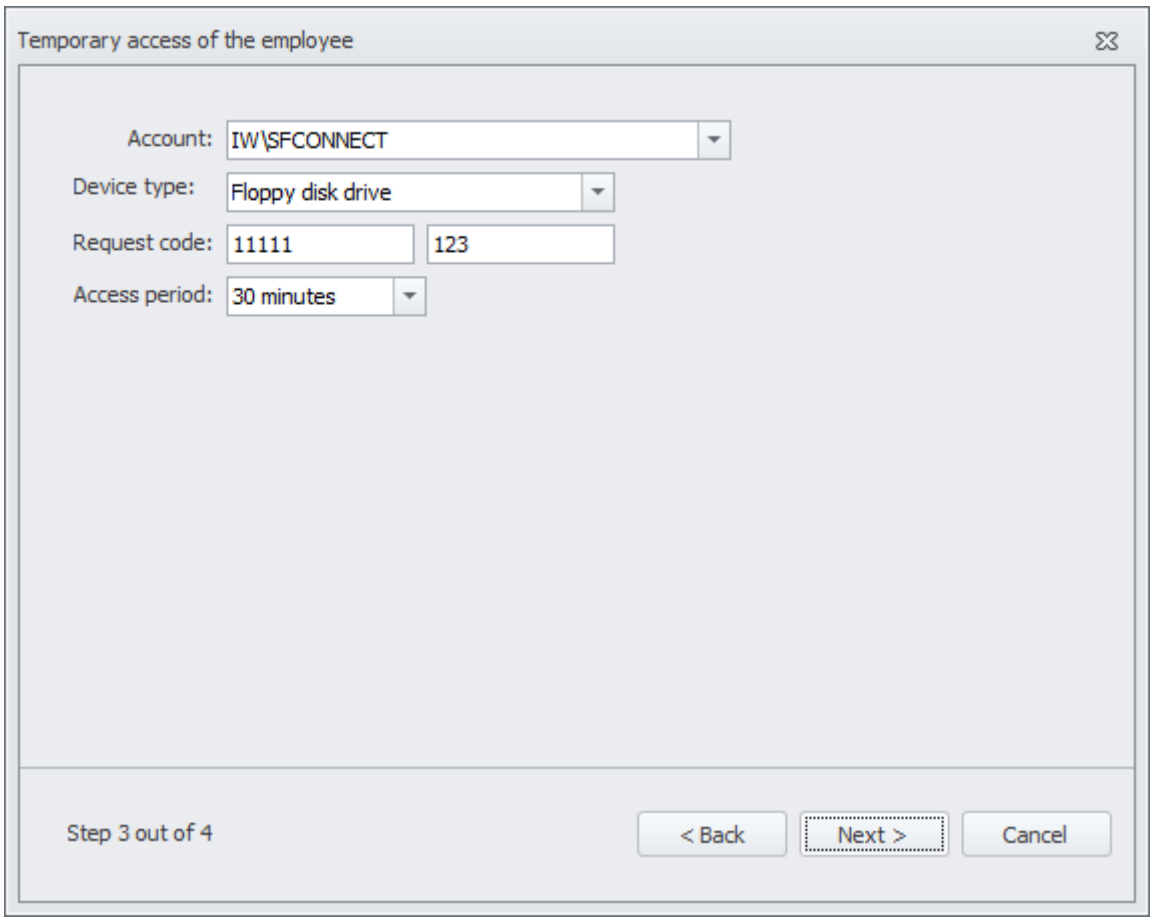
> **Warning!**
>
> An employee can request access only if the **Show tray icon** option is selected (see "Common Settings for Agents"). On to configure the text displayed to the employee, see "Employee Notifications about DM Policy Violations", "**Access to device denied**" notification type.

The employee should send a received request code to the security officer.

You can communicate with the employee using phone or e-mail.

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

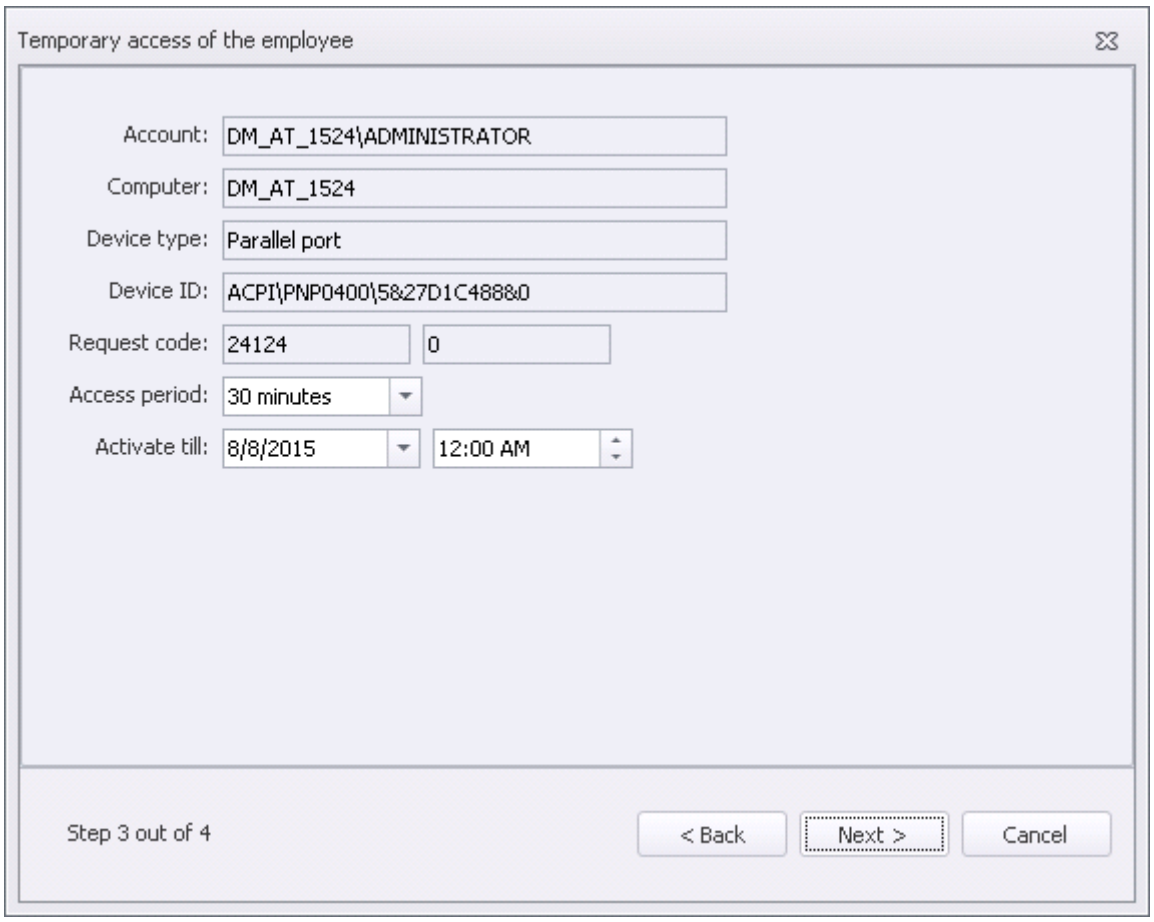
1. In Main Menu select **Tools > Temporary employee access**.
2. Select **Dictated by phone**, click **Next**.
3. Select **To the device**, click **Next**.




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

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

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




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

# Viewing DM Events

InfoWatch Device Monitor Agents installed on controlled 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 Agents".

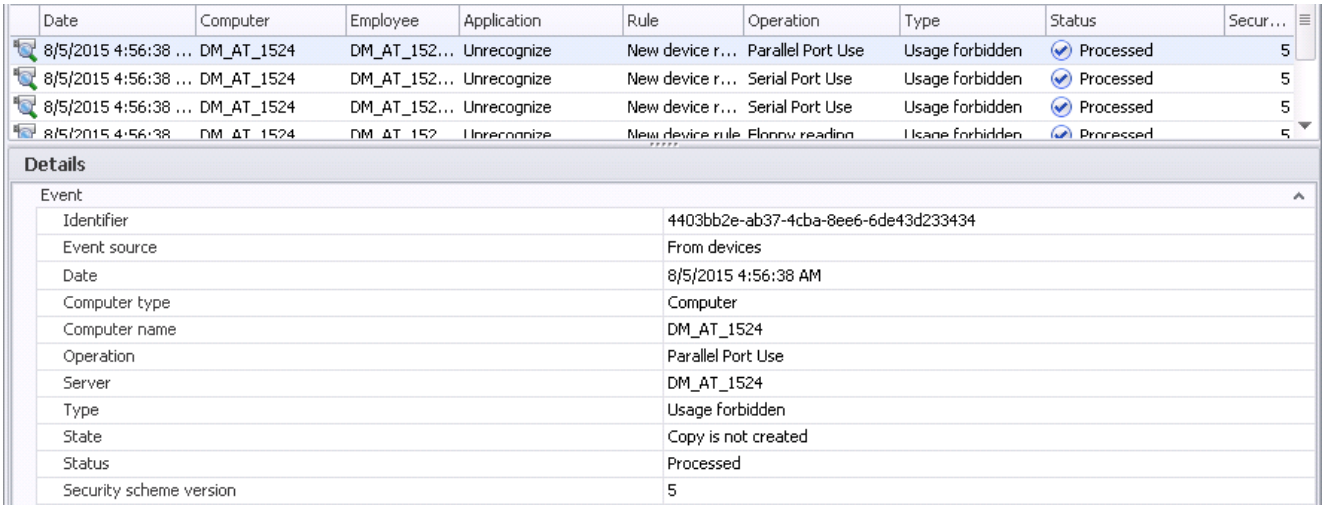
You can view events in **Events** section. To go to this section, click **Events** button on Navigation pane.

**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;<br>• **Devices** – Device Monitor;<br>• **Printer** – Print Monitor;<br>• **Skype, XMPP, MMP, WhatsApp, SMS** – IM Agent Monitor;<br>• **FTP/FTPS** – FTP Monitor;<br>• **HTTP/HTTPS** – HTTP(S) Monitor;<br>• **Mail** - Mail Monitor;<br>• **Network** – Network Monitor; |

| Attribute name | Description | Available values |
|---|---|---|
| | | • **Mobile device camera** - Photo Monitor;<br>• **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 the computer. Device Monitor server keeps an event in UTC, and Management Console (DM) displays it according to the local time of a computer where Console (DM) installed | |
| Computer type | Indicates if the computer where the event arisen is the workstation or mobile device | • Workstation<br>• 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 Agent transmits event information to | |
| Application | Executable file name and/or name of the process responsible for the action, if detected | |
| Type | Action-based event type | • **Record** – adding or changing data (including renaming) on external device; sending files via messenger; sending print jobs to printer; sending data via FTP/FTPS.<br>• **Use** – connecting an external device that allows unmonitored read/write operations or sending messages;<br>• **Violation** – IM Agent interceptor user-initiated violation;<br>• **Warning** – user-initiated a ban or didn't give consent to use IM Agent plug-in, while monitoring is required by security policy (DM).<br>• **Usage forbidden** – attempt of sending data via forbidden channel. |
| Status | Status of event processing on the server and sending to Traffic Monitor server | • **New** |

| Attribute name | Description | Available values |
| --- | --- | --- |
| | | • **Awaiting for proceeding**<br>• **Awaiting for sending to TM**<br>• **Sent to TM**<br>**Note**: If the Server is in standalone mode then the event has the **Processed** status only |
| Security schema version | Number of security schema version that was active on the computer when the event was registered | |
| Operation verdict | Attribute of allowed action. For Devices events (**Device Monitor** rule) the blocking is also available. | • **Allowed**<br>• **Forbidden** – only for Devices events<br>• **Unprotected data copying is disabled** – only for Devices events<br>• **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 agent | Terminal agent name, if detected | |
| Network address of a terminal agent | Terminal agent IP, if detected | |
| **For events with *File* source** | | |
| Assign | Full target file name | |
| File size | Target file size | |
| Object status | Shadow copy of transferred data | • **no copies created** - rule (DM) does not require shadow copying |

| Attribute name | Description | Available values |
|---|---|---|
| | | • **copy created** - shadow copy created successfully<br>• **copying error** - for example, if there is no free space on the agent |
| Device description | Target device instance or model ID | |
| **For events with *Devices* source** | | |
| Device type | For supported device types list see "InfoWatch Device Monitor Functions" | |
| Device instance or model identifier | Model identifier (VID) and serial number (PID) of external device or printer used for the operation | |
| Device description | Device description received from OS of the computer where the Agent is installed | |
| **For events with *Skype, XMPP, MMP, 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<br>• **copy created** - shadow copy created successfully<br>• **copying error** - for example, if there is no free space on the agent |
| 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 | |

| Attribute name | Description | Available values |
|---|---|---|
| File size | Transferred file size | |
| Shadow copy | File, message or chat shadow copy | • **No** - no shadow copy was created<br>• **Yes** - shadow copy created successfully |
| **For events with *Printer* source** | | |
| Document | Full name of the file sent to print | |
| Printer | Name of target network printer | |
| Object status | Result of creating a shadow copy of the print job | 1. Shadow copy of print job was successfully created. The job contained graphic and text data.<br>2. Shadow copy of print job was not created. The job contained no graphic or text data.<br>3. An error occurred while creating a shadow copy of print job.<br>4. Shadow copy of print job was successfully created. The job contained only graphic data.<br>5. The shadow copy should not have been created.<br>6. Shadow copy of print job was partially created. Graphic data were fully processed. Text data were partially processed.<br>7. Shadow copy of print job was partially created. Graphic data were partially processed. Text data were fully processed.<br>8. Shadow copy of print job was successfully created. The job contained only text data.<br>9. Shadow copy of print job was partially created. Graphic data were partially processed. The job contained no text data.<br>10. Shadow copy of print job was partially created. The job contained no graphic data. Text data were partially processed. |
| Object status | Result of creating shadow copy of transferred data | • • **no copies created** - rule (DM) does not require shadow copying |

| Attribute name | Description | Available values |
|---|---|---|
| | | • **copy created** - shadow copy created successfully<br>• **copying error** - for example, if there is no free space on the agent |
| **For events with *FTP/FTPS* source** | | |
| Object status | Result of creating shadow copy of transferred data | • **no copies created** - rule (DM) does not require shadow copying<br>• **copy created** - shadow copy created successfully<br>• **copying error** - for example, if there is no free space on the agent |
| 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<br>• **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 |

| Attribute name | Description | Available values |
| --- | --- | --- |
| | | • **copy created** - shadow copy created successfully<br>• **no free space on disk** - agent does not have enough free space<br>• **copying error** - for example, if there is no free space on the agent |
| 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<br>• **copy created** - shadow copy created successfully<br>• **no free space on disk** - agent does not have enough free space<br>• **copying error** - for example, if there is no free space on the agent |
| 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 | |

| Attribute name | Description | Available values |
|---|---|---|
| Transmission type | Used protocol | |
| Message type | Mail direction | • **Incoming**<br>• **Outgoing** |
| Size, bite | Size in bites | |
| Channel type | Encrypted or not encrypted | • **All channels**<br>• **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 - the port number used for connection attempts. | |
| **For events with *Mobile* device camera source** | | |
| Photo size | Size of photo a 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

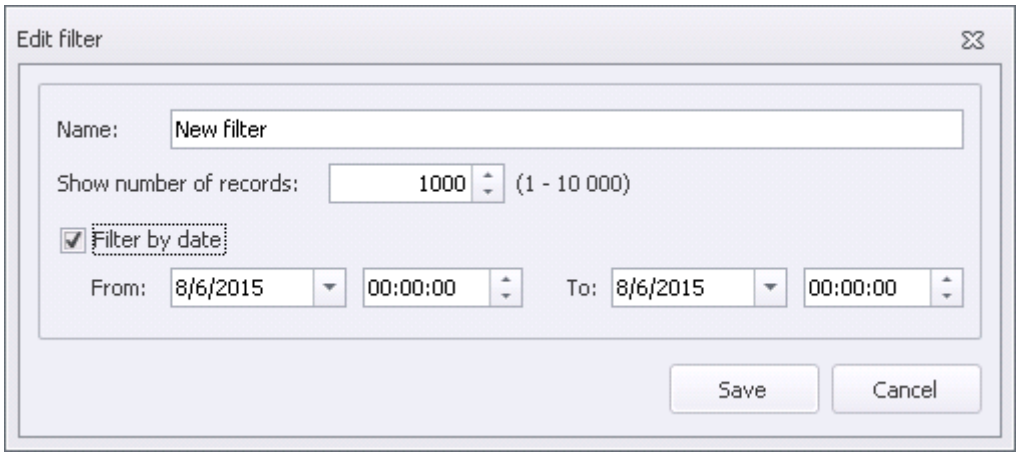
In addition to predefined filters you can create custom filters to view event information.

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

These actions open Edit filter dialog.




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

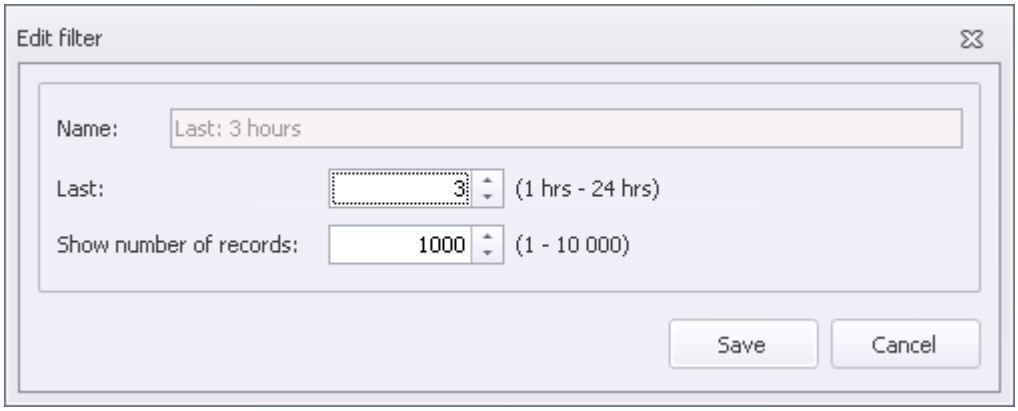
> **Note:**
>
> For the predefined filters **Filter Name** and **Filter by date** parameters cannot be edited.

4. Click **Save**.

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

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

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




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

# 5.2 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.

# Agent Remote Installation, Updating and Uninstallation

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

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

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

> **Note:**

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

To go to Management Console (DM) task section, use **Tasks** button on Navigation pane.

Tasks management guidelines are available in:

- View Tasks;
- Preparing Primary Agent Installation;
- Creating Primary Distribution Task;
- Creating Update Task;
- Creating Uninstallation Password Reset Task;
- Creating Uninstallation Task;
- Launching, Pausing, Editing, and Deleting Tasks;
- ClienAgent Installation Errorst Installation Errors.

You can also install and upgrade your Agent with software distribution tools (for example, via Microsoft Active Directory group policies (DM)). For more information see the document "*InfoWatch Traffic Monitor. Installation guide*", "Agent Installation via Software Distribution Tools" article. To run these operations, use installation package that was created as described in "Creating Installation Package".

# 6.1 Viewing Tasks

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

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

| Parameter | Description |
|---|---|
| Name | Original name of the task |
| Description | Original description of the task |
| Type | One of the following task types:<br>• Primary distribution<br>• Change password<br>• Update<br>• Uninstall |

| Parameter | Description |
|---|---|
| Status | Current task status. Possible values:<br>• Executing<br>• Stopped<br>• Completed |
| Restart period, min | Intervals between task launches on the computer, if the previous attempt failed, in minutes. Counted from ending the last workstation proceeding in previous task launch. If the task fails, it won't be launched again. |
| Number of restart trials | The maximum number of retries to restart distribution task on the computer. If all attempts have been used, **Task status** parameter value will be set to **Error** (for further details, see "Agent Installation Errors"). |
| **For primary distribution tasks** | |
| Show employee notifications | Indicates that employee's attempt to perform a banned action will trigger a warning. For further details, see "General System Settings", "Creating Installation Package" and "Employee Notifications about Policy (DM) Violations" |
| Hide presence of agent on workstation | Indicates if Windows system tray of managed computer hides Agent presence on the computer. Otherwise, Windows system tray of the computer where Agent installed will display  icon. By clicking this icon, information on DM Agent operation and list of currently controlled devices are displayed.<br>**Warning!** If there is an antivirus protection enabled on the managed computer then the antivirus program can reveal the operation of Device Monitor: for example, in the list of processes running on the managed computer or in the list of programs that initiate a control. |
| Install the component of network connections control | Indicates if `iw_proxy` component is installed. |
| Install the component of network connections control | Indicates if Network Monitor interceptor is installed. |
| Uninstallation product password | Shows if the password requested from the employee who attempts to remove Device Monitor Agent. |
| Proxy Root Issuer DN | The unique name of Device Monitor proxy server certificate, issuer distinguished name. |

| Parameter | Description |
|---|---|
| **For primary distribution and update tasks** | |
| Installation directory | Installation directory for Device Monitor Agent at target computers. |
| Installation login | Name of the Console (DM) user that launches the task on computers. |
| Waiting fir restart duration, hours | Computer reboot waiting period (in hours); if the computer is not restarted manually during this period, the System will notify the employee (if notifications are enabled), and force operating system restart. |
| Duration of restart notifications, hours | Period of displaying requests for rebooting the computer, in hours. |
| Restart notifications rate, min | Time intervals between repeated reboot requests, in minutes. |
| Reboot messages | Text displayed to the employee in reboot request. |
| Show a warning before forced reboot | Indicates if a notification about forced reboot will be displayed when reboot wait durations are expired but the employee did not reboot the computer. |
| **For change password tasks** | |
| Uninstallation product password | Shows if the password requested from a user who attempts to remove Device Monitor Agent. |

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

| Parameter | Description |
|---|---|
| Address | Computer IP address or domain name |
| Status | Current status of task for the relevant computer. Possible values:<br>• NEW **Not running** |

| Parameter | Description |
|---|---|
| | •  **Prepare to start**<br>•  **In progress**<br>•  **Waiting for reboot** (only for installation and upgrade tasks)<br>•  **Error** (for further details, see "Agent Installation Errors")<br>•  **No access**<br>•  **Completed** |
| Agent version | Agent version currently installed on the computer. |
| Operation system | Computer operating system. |
| System type | Type of operating system on the computer: x64 or x32. |
| Connections count | Number of connection attempts to the unavailable computer. |
| Time | Date and time of the last connection to the computer. |

# 6.2 Preparing Primary Agent Installation. Distribution Agent

Remote agent installation is carried out by InfoWatch Device Monitor special **Distribution Agent**.

For correct remote installation of agents, workstations should meet hardware and software requirements: see the document "*InfoWatch Traffic Monitor. Installation guide*", "InfoWatch Device Monitor Agent Hardware and Software Requirements" article.

Besides, for workstations installed on Windows OS, the following conditions should be met:

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

Additional requirements vary depending on the distribution method:

**Method 1**:

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

**Method 2**:

For workstations installed on Windows OS, perform actions required for transmitting the Distribution agent through shared administrative resources:

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

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

### 6.2.1 Enabling Shared Administrative Resources

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

- If a workstation 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`.
- Shared administrative resources (like `\\computername\admin$`) must be enabled on workstations (in Windows Vista and Windows 7, they are disabled by default). To enable them:
    1. Make sure that sharing of files and printers is enabled. In Control Panel, open **Network and sharing Center -> Change advanced sharing settings**. In the desired profile, enable file sharing and printer sharing.
    2. In the registry, in `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System` path, add **DWORD (32-bit)** parameter named **LocalAccountTokenFilterPolicy**. Set its value to **1**.

> **Note:**
>
> After you add the parameter in the registry, you need to log into the System again.

### 6.2.2 Firewall Settings

Firewall settings requirements:

| Application protocol | Transport protocol | Port |
|---|---|---|
| RPC | TCP | 135 |

| Application protocol | Transport protocol | Port |
|---|---|---|
| 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 Agent using installation **agents**. Installation agent is an executable file. It is passed on to computers and starts automatically during task execution, receiving Agent updates from the server.

**Warning!**

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

- all target computers
- a computer where Management Console (DM) is running
- a 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 Agent installation package (see "*Traffic Monitor. Installation guide* ", article "Creating Installation Package") and install it by other means (see "*Traffic Monitor. Installation guide*", article "Standard InfoWatch Device Monitor Agent Setup" and "Agent 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 Agent. See internet article "How to enable /disable self-defense in Kaspersky Internet Security" internet article.

**To create a primary InfoWatch Device Monitor agent 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 the task name, select **Initial deployment task** (to install the agent on computers with Windows OS) or **Initial deployment task (Linux)** (to install the agent on computers with Astra Linux OS) and enter the task description, then click **Next**.
4. Create a list of computers which you need to install Device Monitor Agent to. To add a computer (or several computers):
   a. Click **Add Select computer** dialog will display a list of computers from:
      - from a directory;
      - Microsoft Windows Network;
      - from ALD tree;
      - ones registered before (for example, after manual Agent 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.
   You can also specify computer names or IP addresses:
      - in the line at the bottom of dialog box. When listing addresses, separate them with semicolons;
      - 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 Agent installation directory ( %Program Files%\Infowatch\DeviceMonitor\Agent 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 agent installation 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 the 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 Agent 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 the text of the message displaying in reboot notification.
   - **Show a warning before forced reboot**. If this check box is flagged, then the Agent displays a notification about forced reboot and allows 5 minutes to end operations. 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 if neither **Wait while employee reboots computer** setting, nor **Show a warning before force reboot** setting is flagged, or their wait durations are expired but the employee did not reboot the computer.

   Click **Next**.
8. Configure Agent settings:
   - To protect Agent application from deleting by an employee, enter the password that will be requested when trying to uninstall the Agent and confirm it.

- **Show employee notifications** - if employee attempts to perform an action restricted by security policy (DM), a warning will be displayed. For further details, see "Employee Notifications about Policy (DM) Violations".
- **Hide Agent presence** - indicates if Windows system tray of managed computer hides Agent presence on the computer.

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

  > **Important!**
  >
  > Hiding/notifying settings apply on the Agent up to the first call to the server. On calling to the server, the Agent 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 Agent is installed will display  icon. By clicking this icon, information on DM Agent operation and the list of currently controlled devices is displayed.
- **Install the component of network traffic interception** - installs **iw_proxy** component on a computer.
  The 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. The 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

> **Warning**
>
> You need to update agents with a primary distribution task (see. Article "Creating Primary Distribution Task") when updating the DM to version 6.7, otherwise errors may occur. When upgrading to all other versions, the procedure described in this article is used.

Updating InfoWatch Device Monitor Agents is required after updating InfoWatch Device Monitor server: for details, see the document "*InfoWatch Traffic Monitor. Installation guide*", "Updating InfoWatch Device Monitor Server End" article.

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

**To create and schedule an update task for InfoWatch Device Monitor Agents**:

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. At step1, select **Update task** (to update computers with Windows OS) or **Update task (Linux)** (to update computers with Astra Linux OS), enter the task name and description and click **Next**.
4. At step 2, create a list of computers where Device Monitor Agents should be updated. To add a computer (or several workstations):
    a. Click **Add**. The **Select computers** dialog, **DM server computers** node, contains the list of computers where Device Monitor Agent version does not match Device Monitor Server version but can be automatically updated (agent software version should be 4.0.651 and higher).
    b. Flag computers or computer groups. Minimized groups are marked with an icon ; expanded - with . Double-click a group, to expand or collapse it.
    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. At step 3, specify parameters of restarting computers:
    - **Wait for reboot without notifying.** The Agent can**:**
        - Notify immediately (*Do not wait* parameter),
        - Notify after specified time period (*Wait for hour(s)* parameter - you need to specify the time before notification),
        - Do not notify the employee (*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 Agent 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 not notify (*Do not notify*). When necessary, change length and frequency and specify the text of the message, which will be displayed along with the 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. At step 4, specify:
    - Task retry parameters: they will be used in case the task wasn't launched at the first attempt; if launching failed, the task won't be launched again. Specify the number of attempts and their intervals, in minutes.
    - To launch a task immediately after saving, 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 computer has the Kaspersky Internet Security installed then you need to disable its self-protection function for successful InfoWatch Device Monitor Agent 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 agent update task**:

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

   These actions open **Deployment task wizard** dialog.
3. Select **Change uninstall password task**, enter task name and description and click **Next**.
4. Create a list of computers that need their uninstallation passwords to be changed on **Deployment target computers** screen. To add a computer (or several computers):
   a. Click **Add**. The **Select computers** dialog, **DM server computers** node, contains the list of computers where Device Monitor Agent is installed.
   b. Flag computers or computer groups. Minimized groups are marked with an icon ; expanded - . Double-click a group to expand or collapse it. Use **Filter by computer name** field to specify the computer. Click **Find**.
   c. After you specify the computers you want to add, click **ЬISelect**. The **Select computers** dialog will be closed.
   Selected computers will be displayed in the **Task target computers list** area.
   To remove a computer from the list, select it and click **Remove**.

   When you specify all required computers, click **Next**.
5. Specify:
   - **Password** which is required to delete Device Monitor Agent. In the **Confirm** field, retype the password.

- **Task running parameters**: they will be used in case the task wasn't launched at the first attempt; if launching failed, the task won't be launched again. Specify the number of attempts and their intervals, in minutes.
- To launch a task immediately after saving, select the **Run task immediately** check box.

Click **Next**.

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

# 6.6 Creating Uninstallation Task

**To create a centralized task that removes InfoWatch Device Monitor agents:**

1. Go to **Tasks**.
2. Do either of the following:
   - from the main menu, choose **Edit** > **Add task**;
   - use  **Add task** button which is located at the top of the **Tasks** section.

   The **Deployment task** wizard dialog box will appear.
3. At step 1, select **Uninstall task** (to delete the agent from a computer with Windows OS) or **Uninstall task (Linux)** (to delete the agent from a computer with Astra Linux OS), enter the task name and description, then click **Next**.
4. At step 2, create a list of computers, from which you want to uninstall Device Monitor Agent. To add computers:
   a. Click **Add**. The **Select computers** dialog box will open. The **DM server computers** node contains the list of computers, where Device Monitor Agent is installed. You can also use the search field **Filter by computer name**. Enter the computer name and click **Find**.
   b. Flag required computers or computer groups. Minimized groups are marked with ; expanded ones are marked with . To expand or collapse a group, double-click its name.
   You can also list computer names or IP addresses:
      - manually in the row at the bottom of the dialog box; items in the list should be separated by a semicolon;
      - by clicking **Import** and loading a text file with IP addresses or DNS names of computers: each entry should start with a new line; there should be no empty lines in the file.

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

To remove a computer from the list, select its name and click **Remove**.
If all required computers are present in the list, click **Next**.

5. At step 3, specify restart options for the task: they will be used if, for some reasons, the task was not started at the first attempt; if the task start failed with an error, the task will not be started again. Specify the number of attempts and the interval between attempts in minutes.
To launch the task immediately after saving, select **Run task immediately** check box.
Click **Next**.
6. View the task summary. If you need to change some settings, click **Back**. If all settings are specified correctly, click **Finish**.

> **Important!**
>
> If Kaspersky Internet Security is installed on a computer, then, before uninstalling InfoWatch Device Monitor Agent applications, you should disable self-defense in Kaspersky Internet Security.
>
> For more details, see "How to enable/disable self-defense in Kaspersky Internet Security".

# 6.7 Launching, Pausing, Editing, and Deleting Tasks

If you flagged **Launch task immediately** when creating a task, it will start immediately. Otherwise, you will need to launch the task manually. You may need this option if for some reason you had to stop the task and want to start it again.

For instructions, see the table below.

To perform any of these actions, you must first select a task from the list on the **Tasks** panel.

> **Important!**
>
> When you run a task of deploying/updating/deleting agents on Astra Linux, you need to enter a login and a password to get authorized on workstations. The user whose login and password are used for launching the task must be in the `sudo users` list on workstations specified in the task.

| Action | Steps |
|---|---|
| Start task | • in the Main Menu select **Edit > Perform** task;<br>• click **Perform task** located at the top of Navigation pane. |
| Stop task | • in the Main Menu select **Edit >Stop task**;<br>• click **Stop task** at the top of Navigation pane. |

| Action | Steps |
|---|---|
| Edit list of computers in task | • at the top of **Task execution result** panel click  **Add computer** or  **Exclude computer from task**<br>• right-click computer row and select  **Add computer** or  **Exclude computer from task**.<br>**Warning!** You can't remove a computer if the task is running and not completed. |
| Edit task | • in the Main Menu select **Edit > Edit**;<br>• click  **Edit** at the top of Navigation pane.<br>• right-click on task name and select  **Edit**.<br>Specify new settings for the task like it is done for a new task (see "Creating Primary Distribution Task", "Creating Updating Task", "Creating Uninstallation Password Reset Task", "Creating Uninstallation Task") |
| Delete task | • in the Main Menu select **Edit > Delete**;<br>• click  **Delete** at the top of Navigation Pane.<br>• right-click on task name and select  **Delete**.<br>**Warning!** You can't remove a task with computer that has a running task. |
| View computer error log | • at the top of **Task execution result** panel click  **Computer log**<br>• right click computer row and select **Computer log** |

# 6.8 Agent Installation Errors

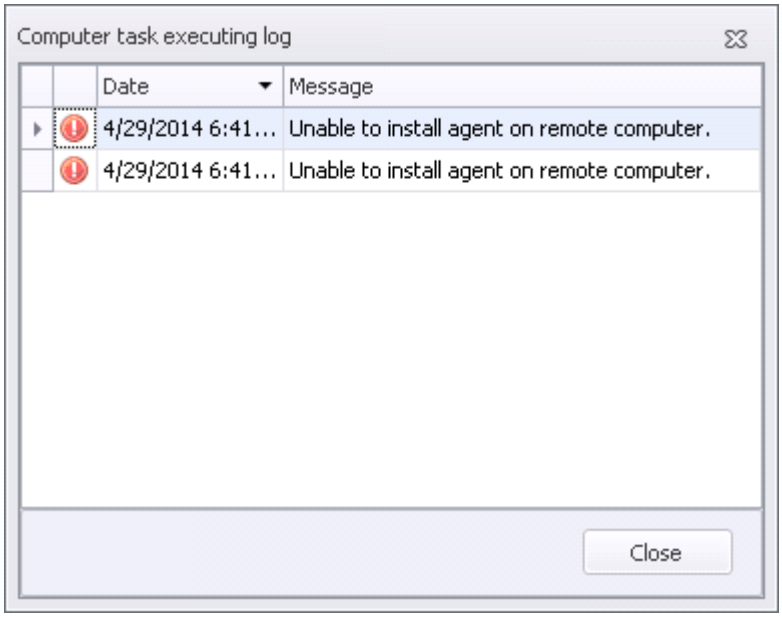
You may encounter problems during remote installation of InfoWatch Device Monitor agents to computers. This will be indicated by Task status value in the list of tasks: see "Viewing Tasks".

**To view task errors**:

1. Go to **Tasks**.
2. On **Tasks** panel select the task you want to review.
3. In **Status** column select filter value **Error** (for more information on filters see "Applying Standard Filters").

> **Note:**
>
> Status  **No access** indicates that computer is not available (switched off or disconnected from network)

4. In the row of the target computer, do one of the following:
    - right-click the row and select **Computer Log;**
    - double-click the target computer row;
    - at the top of **Task execution result** panel, click **Computer log**.




5. To view detailed error information, click the row. This opens a screen with Windows error description.

For detailed information on the error see its description, error code, or log in error's description. In particular, the errors may be caused by the following things:

- the computer is not available (switched off or disconnected from the network);
- the installation process or reboot is blocked by another task or user (common description could be "*Other task is running*");
- target computer does not allow administrative resources;
- the account in use doesn't have enough rights on the target computer.

If all remote Agent installation conditions in "Preparing Primary Agent Installation. Distribution Agent" are met and the task is not blocked by the user, but the error persists, please contact InfoWatch technical support at support@infowatch.com and attach error description and log.

# 6.9 Creating Installation Package

Supplied InfoWatch Device Monitor Agent installation package contains the following default settings:

- Agent installation directory on computer system drive - `%Program Files%\Infowatch\DeviceMonitor\Client`.
- There is no uninstallation password.

- After installation Device Monitor Agent starts to remind an employee that a reboot is required. Message text - "*Please reboot your computer as soon as possible*". Reminders are displayed infinitely, with 10 min intervals.

To change these settings create your own installation package. When you run it, it will use the settings specified when installation package created: no other parameters are needed to specify.

**To create InfoWatch Device Monitor Agent installation package**:

1. In the Main Menu select **Tools > Create install package**.
   This opens distribution task manager dialog box.
2. The InfoWatch Device Monitor servers currently registered in the System are displayed. Agent will use them for primary installation.
   If necessary, change Agent installation directory at computers.
   Specify local or network directory where to the installation packages will be saved.
   Click **Next**.
3. The unique name of Device Monitor proxy server certificate (Issuer Distinguished name, Proxy Root Issuer DN) will be displayed. You can change it with accordance to X.509 standard, CN (Common Name) field is mandatory, all fields comma-separated. Click **Next**.
4. Specify options of computer reboot:
   - **Wait for reboot without notifying the employee**. The Agent can:
     - start notifications immediately (*Do not wait option*),
     - start notifications in specified time (*Wait for option* - please specify time period to start notifications),
     - do not notify at all (*Wait infinitely option*).
   - **Notify the employee about reboot necessity and wait for reboot**. Upon completing reboot waiting in "silent" mode (see **Wait for reboot without notifying the employee** setting) or immediately after installation ends, Device Monitor Agent starts to notify employee on reboot necessity:
     o during specified time period (*Notify within* option)
     o permanently (*Notify infinitely* option)
     o do not notify at all (*Do not notify* option).
     If needed, change continuance and frequency of notifications appearance and enter text of the message displaying in reboot notification.
   - **Show a warning before forced reboot**. If this check box is flagged, then the Agent displays a notification about forced reboot and allows 5 minutes to end operations. If the option is not checked then the forced reboot (if it should be made according your settings) will be performed unexpectedly for the employee.

     **Warning!**

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

Click **Next**.

5. Define Agent settings before it connects to the server for the first time:

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

     **Warning!**

     Not notifying the user about interceptor operation may contradict the applicable laws of your country.

     **Warning!**

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

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

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

     **Warning!**

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

Click **Next**.

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

Agent installation package will be saved in the folder you specified at the first step.

# 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:

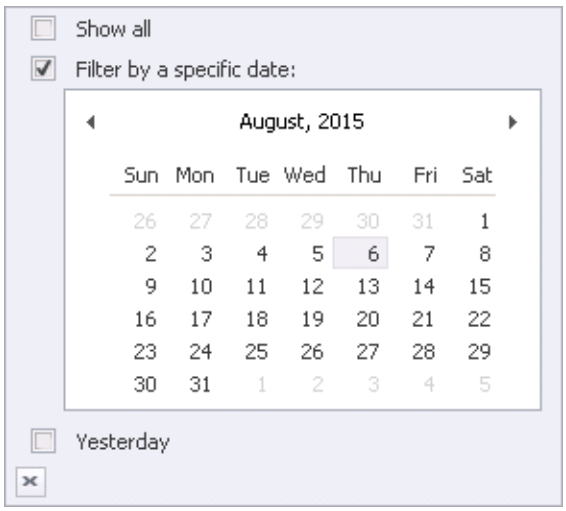
- Filter by Date;
- Applying Standard Filters;
- Custom Filter;
- Editing Filters;
- Removing a Filter.

### 7.1.1 Filtering by Date

If the table shows temporary parameter characteristics (for example, Agent installation date and time, Console (DM) log
time, last computer access, registered event date, etc.), you can filter the column against the desired date or
period.

**To view the records for specific date or period**:

1. Move the pointer over the time/date attribute in the column header.
2. Click the button ▾ to the right of the column header.




3. Select one of the following filters:
   - **Show all** - select this check box to view all records regardless the date.
   - **Filter by a specific date** - select the date in the calendar.
     To select a period, select it holding the mouse button.
     To go from date to month or year display, click the month/year.
     Use arrows to go forward or backward.
   - **Today; Yesterday; Last week; Earlier this week; Earlier this year** fields depend on column values: for
     example, if there are no records for the date, **Today** field won't be displayed. Check this box to display
     only the records inside specific date range.
4. Click ✖ to apply the filter and close the form.

## 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").

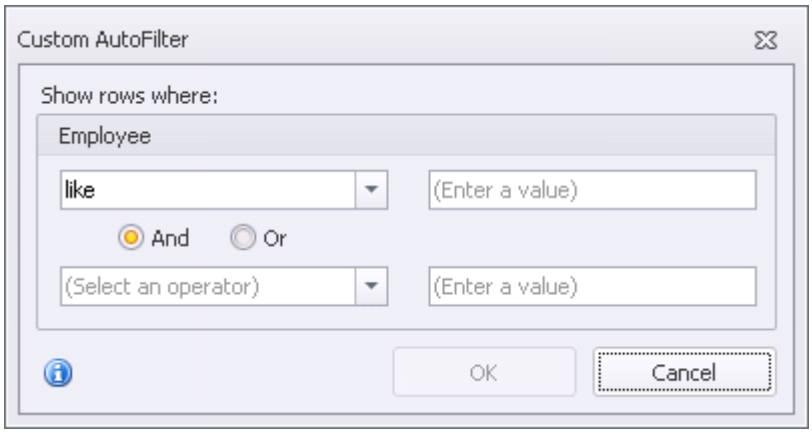
The table will only display filtered values.

**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.

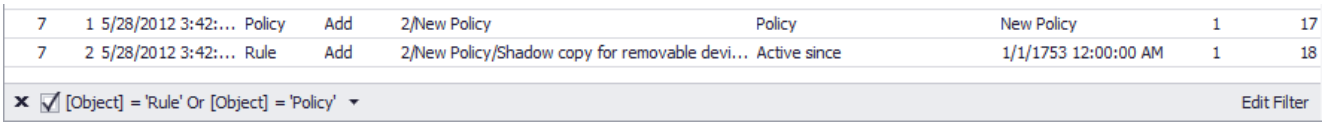
     > **Note:**
     >
     > You can use comparison operators to limit filtering criteria: *equal, not equal, greater than, greater than or equal to, less than, less than or equal to; values empty (blank) and nonempty (non-blank field)*; or
     > text filter with a mask. To get a text filter syntax tip,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

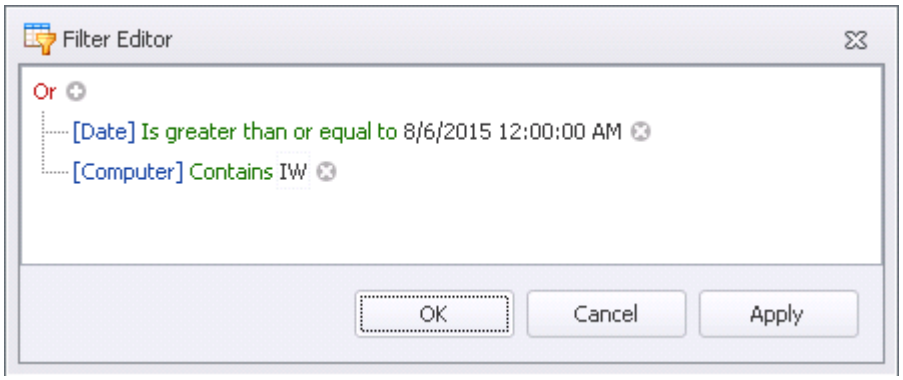



To remove filter and view all items, clear the check box in filter string. To apply the filter again, select the check box.
To re-use a filter, click the filter string and select filter from drop-down filter history list. Custom filters are stored until you close the window with filtered content.

## 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<br>2. Select the value from the drop-down list or enter the value to the field |
| Add a simple condition | Click the button to the right of the logical operator<br>or<br>Click **Add Condition** in logical operator menu |
| Delete condition | Click the button at the end of condition string |
| Add criteria group | 1. Click the logical operator name<br>2. Select **Add Group** in the menu |
| Delete criteria group | |

| Action | Steps |
| --- | --- |
| | 1. Click the name of operator criteria group<br>2. Select **Delete Group** in the menu |
| Delete all criteria | Click **Clear All** in logical operator menu |

3. Click **Apply** and view the filtered results without closing **Filter Editor** screen.
4. Click **OK**.

### 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+1 |
| Go to Employees | Ctrl+2 |
| Go to Computers | Ctrl+3 |

| Feature name | Hotkeys |
| --- | --- |
| Go to White Lists | Ctrl+4 |
| Go to Signatures | Ctrl+5 |
| Go to Applications | Ctrl+6 |
| Go to Log | Ctrl+7 |
| Go to Tasks | Ctrl+8 |
| Go to Events | Ctrl+9 |
| Manage security schema (overview) | |
| Go to security schema editing mode | F11 |
| Save security schema | F12 |
| Cancel saving security schema | Shift+F11 |
| Unblock security schema (Superuser only) | Ctrl+Shift+U |
| Update security schema | F5 |
| Go to the latest security schema version (when viewing an earlier version) | F9 |
| Manage security policies | |
| Add security policy | Ctrl+N |
| Edit security policy | Ctrl+E |
| Delete security policy | Ctrl+D |
| Manage rules | |
| Add rule | Ctrl+Shift+N |
| Edit rule | Ctrl+Shift+E |

| Feature name | Hotkeys |
| --- | --- |
| 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 |

| Feature name | Hotkeys |
| --- | --- |
| Edit white list | Ctrl+E |
| Delete white list | Ctrl+D |
| Edit white list entries | Ctrl+Shift+E |
| Manage signatures | |
| Add signature category | Ctrl+N |
| Edit signature category | Ctrl+E |
| Delete signature category | Ctrl+D |
| Remove signature from category | Delete |
| Configure filters for Audit Log and Event Viewer | |
| Add filter | Ctrl+N |
| Edit filter | Ctrl+E |
| Delete filter | Ctrl+D |
| Manage Agent remote installation and upgrade tasks | |
| Add task | Ctrl+N |
| Edit task | Ctrl+E |
| Delete task | Ctrl+D |
| Add computer to selected task | Ctrl+Shift+N |
| Remove computer from selected task | Delete |
| Display target computer error log | Ctrl+L |