

INFOWATCH

InfoWatch Device Monitor. User Guide

26/04/2024

© JSC “InfoWatch”

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

http://www.infowatch.com

Table of Contents

1 Who Should Read this Guide 6

2 Set of Documents 7

3 InfoWatch Device Monitor Functions 8

3.1 Operation in Safe Mode 11

4 Using Device Monitor Management Console 12

4.1 Management Console Overview 12

4.1.1 Authorization and Connecting to InfoWatch Device Monitor Server 12

4.1.2 Management Console Main Screen 14

Configuring Management Console Main Screen Elements 15

4.1.3 Management Console Sections 16

4.2 Managing Console Accounts 16

4.2.1 Viewing Management Console Account Details 18

Adding New Management Console Account 19

Editing Management Console Account 22

Locking or Unlocking Management Console Account 23

Deleting and Restoring Management Console Account 23

4.2.2 Roles of DM Console Users 24

Adding Role of the Management Console User 24

Editing Role of DM Console User 28

Deleting Role of Console User 28

4.2.3 Management Console Security Scheme Operation Activity Log 29

Viewing Audit Log 29

Log Records Filtering 31

Deleting Records from Log 36

Exporting Log Records 36

Analyzing Log Records in Microsoft Excel 36

4.3 General System Settings 37

4.3.1 General Settings for Agents 37

4.3.2 Corporate Network Control 40

4.3.3 Messengers Control 42

4.3.4 Network Traffic Control 43

Adding Servers to Exclusions 45

4.3.5 Device Monitor Server Settings. Connecting to Traffic Monitor Server 47

4.3.6 Device Monitor Server Settings. Connecting to Platform Server 50

Connection parameters 51

4.3.7 Active Directory Connecting and Synchronizing ... 52
Automatic Installation of Agent ... 57
4.3.8 Employee Notifications about Policy Violations ... 58
4.3.9 Exclusion of Application from Interception ... 60
4.3.10 Application Control and screenshots ... 63
4.3.11 Control of Keyboard Input ... 65
4.3.12 Event Storage ... 66
4.3.13 Synchronization of Traffic Monitor Policies ... 67
4.3.14 InfoWatch Device Monitor Server Manager ... 68
4.3.15 Setting Activity Status of Agents ... 69
4.3.16 Stopping and Starting Device Monitor Agent ... 71
Stopping agent remotely/starting agent ... 72
Stopping/starting agent locally ... 73
4.3.17 Configuring Agents distribution ... 73
4.3.18 Automatic Update of Agents ... 75
4.3.19 Setting Interception of Audio ... 76
4.3.20 Settings to Send Data to Products ... 78
4.4 Managing Security Scheme ... 80
4.4.1 Security Scheme Organization ... 81
Security Policies and Rules ... 81
Employees and Employee Groups ... 84
Computers and Computer Groups ... 84
Uploading Security Scheme to Managed Computers ... 85
4.4.2 Security Scheme Overview ... 85
Viewing Active Security Scheme ... 85
Viewing Old Security Scheme ... 86
Security Scheme Comments ... 87
Editing Security Scheme ... 88
Updating Security Scheme ... 90
Exporting/Importing Security Scheme ... 90
4.4.3 Security Scheme Setup ... 92
Security Policies ... 93
Rules ... 97
Employees ... 150
Computers ... 159
White Lists ... 174
Signatures ... 181
Application Protocol ... 184
Application Blockade ... 190
Resources ... 195
File Statistics ... 199
Junk Traffic Exceptions ... 205
4.4.4 Temporary Employee Access to Network ... 208

4.4.5 Temporary Employee Access to Devices ... 209
4.5 Viewing DM Events ... 211
4.5.1 Event Filters ... 221
4.5.2 Deleting Events ... 223
4.6 Agent Remote Installation, Updating and Uninstallation ... 224
4.6.1 Viewing Tasks ... 224
4.6.2 Preparing Primary Agent Installation. Distribution Agent ... 227
Enabling Shared Administrative Resources ... 228
Firewall Settings ... 228
4.6.3 Detecting Workstations to Install the Agents on ... 229
4.6.4 Creating Primary Distribution Task ... 230
4.6.5 Creating Update Task ... 234
4.6.6 Creating Uninstallation Password Reset Task ... 236
4.6.7 Creating Uninstallation Task ... 237
4.6.8 Launching, Pausing, Editing, and Deleting Tasks ... 238
4.6.9 Agent Installation Errors ... 239
4.6.10 Creating Installation Package ... 240
4.6.11 Creating template of distribution task ... 243
4.7 Additional Features ... 245
4.7.1 Filter Table Contents ... 245
Filtering by Date ... 246
Applying Standard Filters ... 246
Custom Filter ... 247
Editing Filters ... 248
Removing a Filter ... 249
4.7.2 Grouping or Sorting Entries ... 249
4.7.3 Hotkeys ... 250
5 End-user license agreement ... 254
6 Glossary ... 258

This guide contains information on how to work and perform tasks in InfoWatch Device Monitor.

InfoWatch Device Monitor (also referred to as the Module/System or Device Monitor) – software intended to intercept data in company information traffic.

1 Who Should Read this Guide

Information in this guide is intended for users who manage the System (perform the System configuration, analyze information objects, etc.).

This guide is intended for users familiar with the basics of Windows OS.

2 Set of Documents

InfoWatch Device Monitor documentation package includes the following:

- "InfoWatch Device Monitor. Installation, configuration and administration Guide". The document describes how to install, update, uninstall and configure the Module.
- "InfoWatch Device Monitor. User Guide". The document describes how to work in InfoWatch Device Monitor.

Associated documentation for InfoWatch Traffic Monitor includes the following:

- «InfoWatch Traffic Monitor. Installation Guide». The document describes how to install, configure and uninstall InfoWatch Traffic Monitor (further referred to as Traffic Monitor).
- «InfoWatch Traffic Monitor. Administration Guide». The document describes how to administer the System (database, server).
- «InfoWatch Traffic Monitor. User Guide». The document describes how to work in InfoWatch Traffic Monitor (configuration setting, export/import of data, creating policies to process objects).
- «InfoWatch Traffic Monitor. Configuration Files Guide». Describes the content of the configuration files.

Associated documentation for InfoWatch Activity Monitor includes the following:

- «InfoWatch Activity Monitor. Installation Guide». The document describes how to install, update, uninstall Activity Monitor.
- «InfoWatch Activity Monitor. Administration Guide». The document describes how to configure and prepare Activity Monitor for work.
- «InfoWatch Activity Monitor. User Guide». The document describes how to work in Activity Monitor.

3 InfoWatch Device Monitor Functions

InfoWatch Device Monitor is a module of InfoWatch Traffic Monitor for controlling data exchange on employee workstations. Collected data is sent to InfoWatch Traffic Monitor and Platform products for analysis.

The main functions of InfoWatch Device Monitor:

Function name	Related rule of security policy
Control of applications	Application Monitor Rule
Control of sound environment. Is used only by InfoWatch Activity Monitor	Audio Record Control Rule
Control of the clipboard	Clipboard Monitor Rule
Cloud storage control	Cloud Storage Monitor Rule
Control of access to external devices	Device Monitor Rule
Control of connection via Microsoft RDP or Citrix ICA	Device Monitor Rule
Control of copying files from/to removable devices, network resources and resources connected via terminal session	File Monitor Rule
Control of file reading and writing by applications	File Operations Monitor Rule
Control of traffic sent via FTP and FTPS	FTP Monitor Rule
Control of traffic sent via HTTP and HTTPS	HTTP(S) Monitor Rule
Control of instant messengers: Skype, Telegram, Facebook, WhatsApp, VK, Jabber (XMPP protocol), MMP protocol	IM Client Monitor Rule
Control of keyboard input	Keyboard Monitor Rule
Control of mail protocols (SMTP, IMAP, POP3, Outlook, HTTPS)	Mail Monitor Rule
Control of transferring data through network connections outside the corporate network	Network Monitor Rule
Monitoring print operations on controlled computers	Print Monitor Rule
Control of taking screenshots	ScreenShot Control Monitor Rule
Control of computer screen	ScreenShot Monitor Rule

Function name	Related rule of security policy
Control of employee activity and collecting statistics. Is used only by InfoWatch Activity Monitor and InfoWatch Prediction	Statistics Rule

Warning!

Incoming connections for server applications will only be intercepted on Device Monitor agents installed on workstations with Windows 8 and later.

Warning!

On computers with Astra Linux OS, RED OS and Alt Linux OS, the following control functions are supported:

Function name	Related rule of security policy	Note
Control of the clipboard	Clipboard Monitor Rule	Is not supported on Astra Linux OS
Cloud storage control	Cloud Storage Monitor Rule	–
Control of access to external devices	Device Monitor Rule	Only control of removable storage devices and MTP devices is supported
Control of copying files from/to removable devices, network resources and resources connected via terminal session	File Monitor Rule	–
Control of traffic sent via FTP and FTPS	FTP Monitor Rule	–
Control of traffic sent via HTTP and HTTPS	HTTP(S) Monitor Rule	–
Control of instant messengers: Skype, Telegram, Facebook, WhatsApp, VK, Jabber (XMPP protocol), MMP protocol	IM Client Monitor Rule	On workstations with one of the Linux familiy OS, you can control only desktop version of Telegram
Control of keyboard input	Keyboard Monitor Rule	Is not supported on Astra Linux OS

Function name	Related rule of security policy	Note
Control of mail protocols (SMTP, IMAP, POP3, Outlook, HTTPS)	Mail Monitor Rule	–
Monitoring print operations on controlled computers	Print Monitor Rule	–
Control of taking screenshots	ScreenShot Control Monitor Rule	Is not supported on Astra Linux OS
Control of employee activity and collecting statistics.	Statistics Rule	Is not supported on Astra Linux OS

Note:

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

Actions of employees are controlled on managed computers. For this, agent modules are installed on the controlled computer.

The agent module includes the following interceptors:

- Application Monitor
- Audio Record Control
- Clipboard Monitor
- Cloud Storage Monitor
- Device Monitor
- File Monitor
- File Operations Monitor
- FTP Monitor
- HTTP(S) Monitor
- IM Client Monitor
- Keyboard Monitor
- Mail Monitor
- Network Monitor
- Print Monitor
- ScreenShot Control Monitor
- ScreenShot Monitor
- Statistics

For more information on interceptors, see "Rules".

Note:

On computers with Astra Linux OS, operation of interceptors is supported in a limited mode (for details about operation of interceptors on different OS, see rule descriptions).

Intercepted data is analyzed on Device Monitor agents with the following detection technologies:

- Files formats
- Text objects

> **Note:**
>
> Names and values of document properties, which are extracted from PDF documents by Device Monitor agent, can be set as a Text object (see *Example 3* in "*Managing Text Objects*", "*Cases Solving in Traffic Monitor Management Console*", "*Traffic Monitor. User Guide*").

- Terms/content filtering base

3.1 Operation in Safe Mode

Some of InfoWatch Device Monitor features are still available in safe mode (with network features or without them). The following table lists the features available in safe mode.

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

4 Using Device Monitor Management Console

The Management Console is designed to address the following tasks:

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

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

- Management Console Overview. InfoWatch Device Monitor general actions (startup, interface configuration).
- Managing Console Accounts. How to perform InfoWatch Device Monitor administration tasks: managing InfoWatch Device Monitor Management Console accounts, working with log, etc.
- General System Settings. Defining global settings which are common for all rules and policies.
- Managing Security Scheme. How to use security scheme 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.
- Additional Features. Secondary functions enhancing InfoWatch Device Monitor Management Console user experience: records filtering, grouping and sorting, Management Console shortcuts.

4.1 Management Console Overview

Management Console basics are available in the following subsections:

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

4.1.1 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").

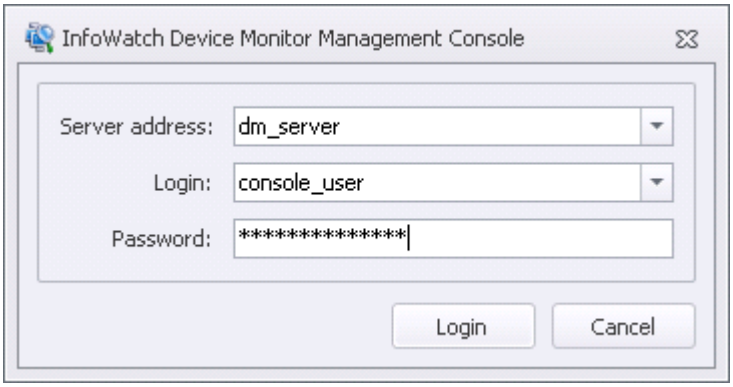
To start working with DM Management Console:

1. Start the Management Console. 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.



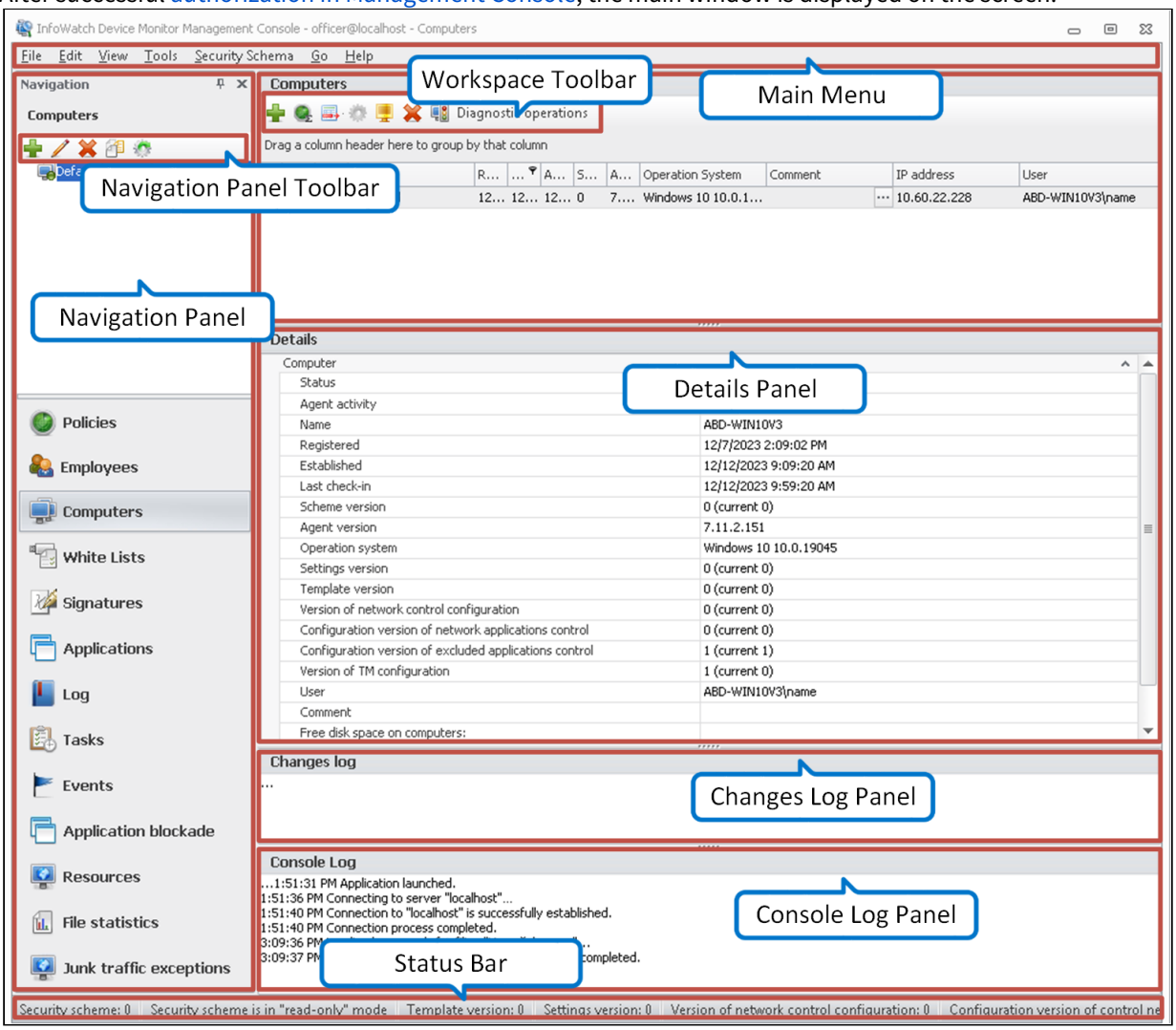
Parameter	Description
Server address	FQDN of the server, the Management Console is connecting to. Th default port for communication between the server and Management Console is 15003. If this port has been changed, enter the server address as follows: `dm_server:port`
Login	Name of the user account
Password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

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

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

4.1.2 Management Console Main Screen

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



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

The main screen contains elements required for working with Management Console:

- **Main Menu** contains commands that give you access to all Management Console essential features.
- **Navigation panel** allows you to switch between different sections of Management Console and manage elements of the selected section.
- **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. The toolbars are located on Navigation panel (for elements of the selected section) and in the workspace (for the selected element).
- **Details panel** displays extended information about properties of the selected element.
- **Changes Log panel** displays all changes made by the current user and not saved in the security scheme.
- **Console Log panel** 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 **Computers** section.

Configuring Management Console Main Screen Elements

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

Action	Steps
Hide pane	Click **View** in the Main Menu and click on the bar title you want to hide. To open the pane again, repeat this step. **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.
Return to the initial interface settings	Click **View** in the Main Menu and click on **Reset interface options**. After that DM concole should be restarted. **Note:** In this case the previously used columns order and grouping on the **Working area of the main window** will be returned as well as the initial **Navigation pane** settings.

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

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

4.1.3 Management Console Sections

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

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

- In 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** are designed for managing the security scheme, **Applications** section is for controlling the launching of applications, **Log** section is for monitoring security scheme 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
White Lists	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 scheme management activity log (logging administrating responsibility zones and configuring security scheme)
Tasks	InfoWatch Device Monitor Agents centralized installation, updating, and uninstallation on computers
Events	Viewing information on employee activities on managed computers using controlled means

4.2 Managing Console Accounts

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

The Management Console contains a pre-installed user, a **Superuser**, who has permissions for all operations in the Console. This user is not supposed to perform everyday operations. We recommend using this account for initial configuration of the Management Console, creating the Administrator account and then only in case of emergency.

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

The Management Console has the following preset roles:

- **Administrator** – a role for Console administrator who manages other Console accounts;
- **Security officer** – a role of Console end user who manages the security scheme and server settings;
- **Security officer of the group** – a role of Console end user who manages groups of employees and computers.

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

The list of available actions for preset roles:

Action	Administrator	Security officer	Security officer of the group
Viewing audit log		+	
Exporting log records		+	
Deleting records from log			
Viewing Management Console account details	+	+	
Adding, editing, deleting Management Console accounts	+		
Assigning/deleting Management Console account roles	+		
Locking/unlocking Management Console account	+		
Device Monitor Server Settings. Connecting to Traffic Monitor Server		+	
Device Monitor Server Settings. Connecting to Platform Server (for sending data to Activity Monitor and Prediction)		+	
Viewing security scheme versions		+	
Editing security scheme		+	

Action	Administrator	Security officer	Security officer of the group
Importing/exporting security policies and rules		+	
Viewing events		+	
Agent 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 white lists			+
Managing Agents		+	+

For more information on Management Console accounts management, see:

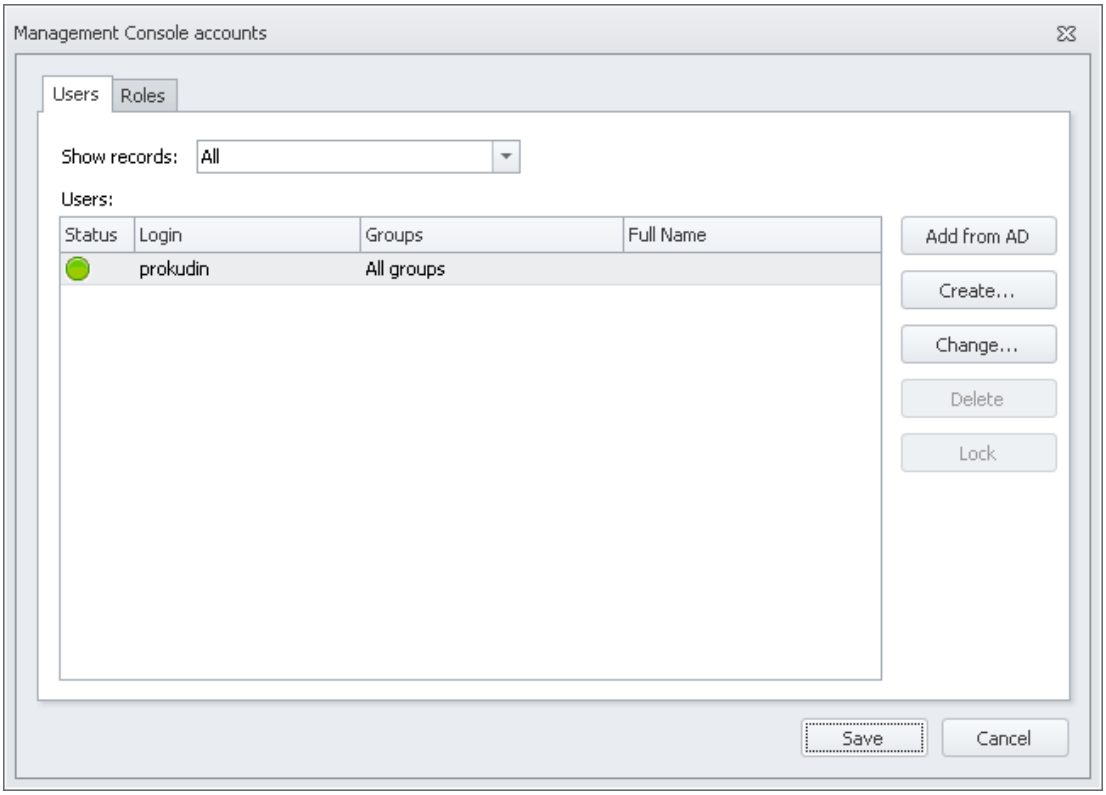
- Viewing Management Console Account Details
- Adding New Management Console Account
- Locking or Unlocking Management Console Account
- Editing Management Console Account
- Deleting and Restoring Management Console Account
- Management Console Security Scheme Operation Activity Log



4.2.1 Viewing Management Console 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 Account").
   - **Deleted**. List of deleted accounts. The System saves information about actions those users performed. Deleted accounts can be restored (see "Deleting and Restoring Management Console Account").

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

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.

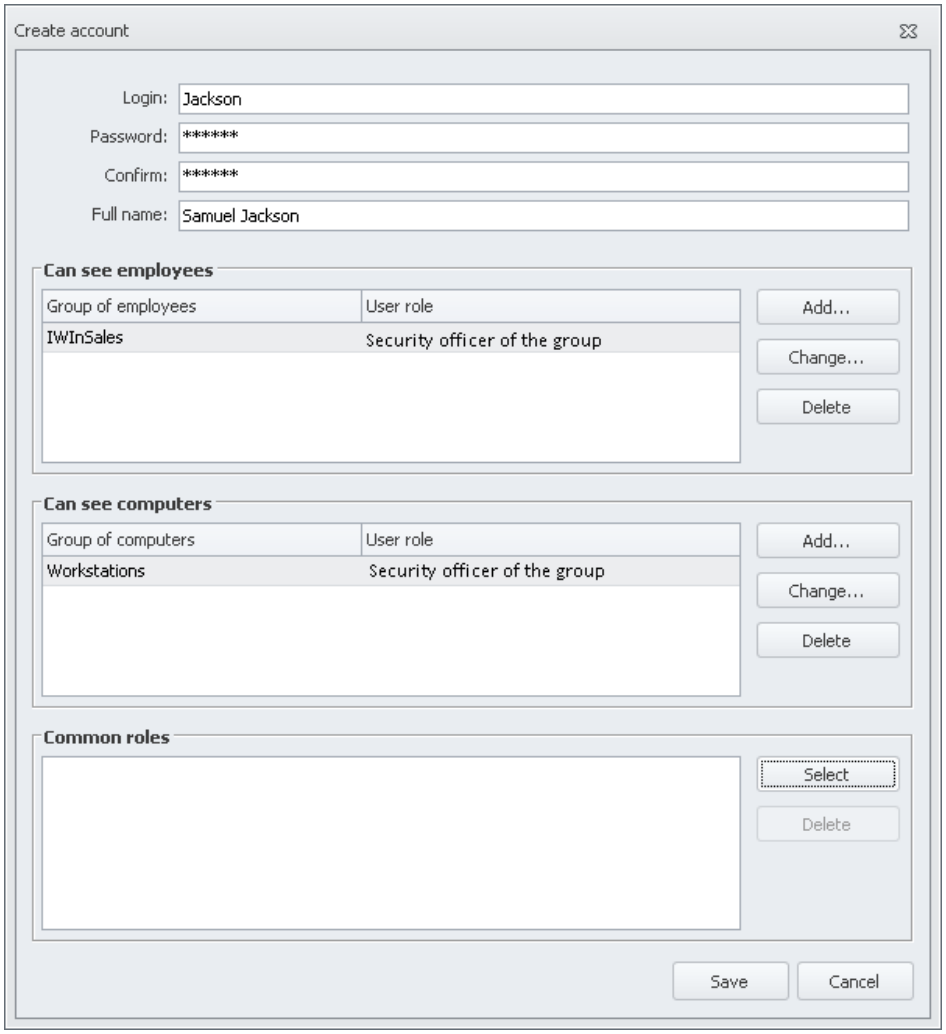
Login, password, role, and status are mandatory attributes. For a detailed description of roles, see "Roles of DM Console Users".

Adding New Management Console 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 Account").

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:

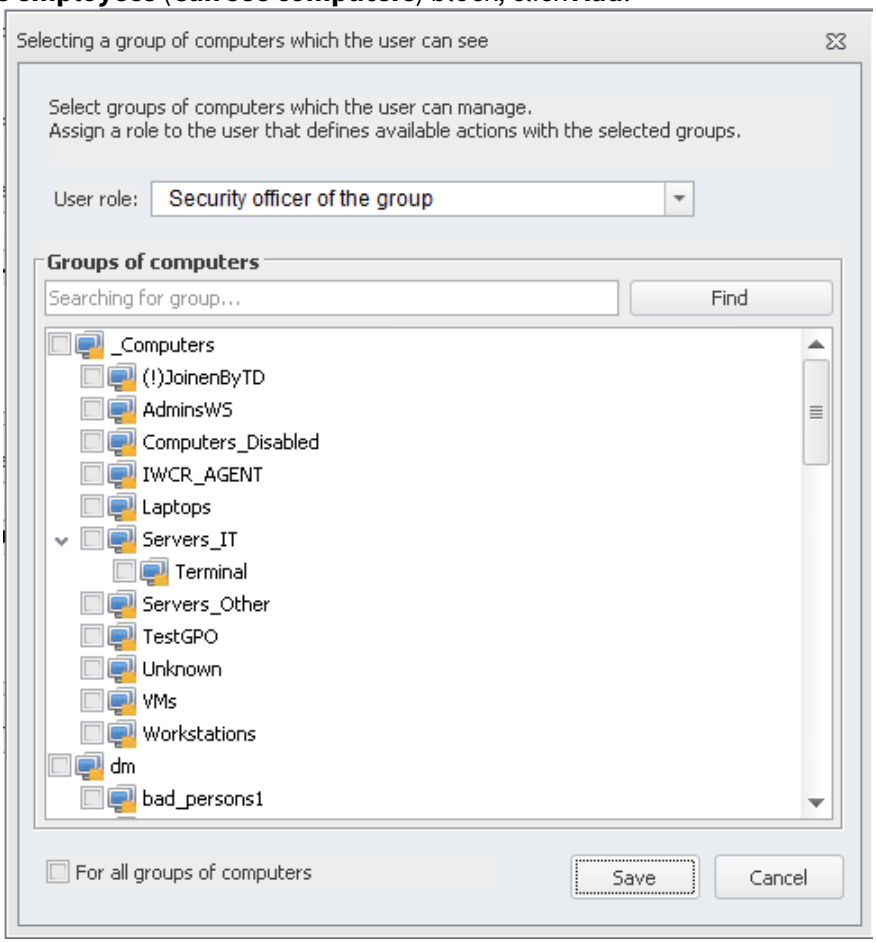
The login and full name that are displayed in the **Management Console Accounts** dialog box for the imported user will be filled automatically. The password matches the user password in AD.

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.

Editing Management Console Account

Warning!

If you edit a role that is currently authorized in the Management Console, 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 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.

Locking or Unlocking Management Console 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**.

- Click **Save** to apply changes.

Deleting and Restoring Management Console Account

After deletion, the account is moved to the list of deleted accounts. The account information remains in the database.

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

You can view deleted accounts in **Management Console Accounts** dialog box. To do this, select **Obsolete** in the **Accounts** drop-down list.

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.

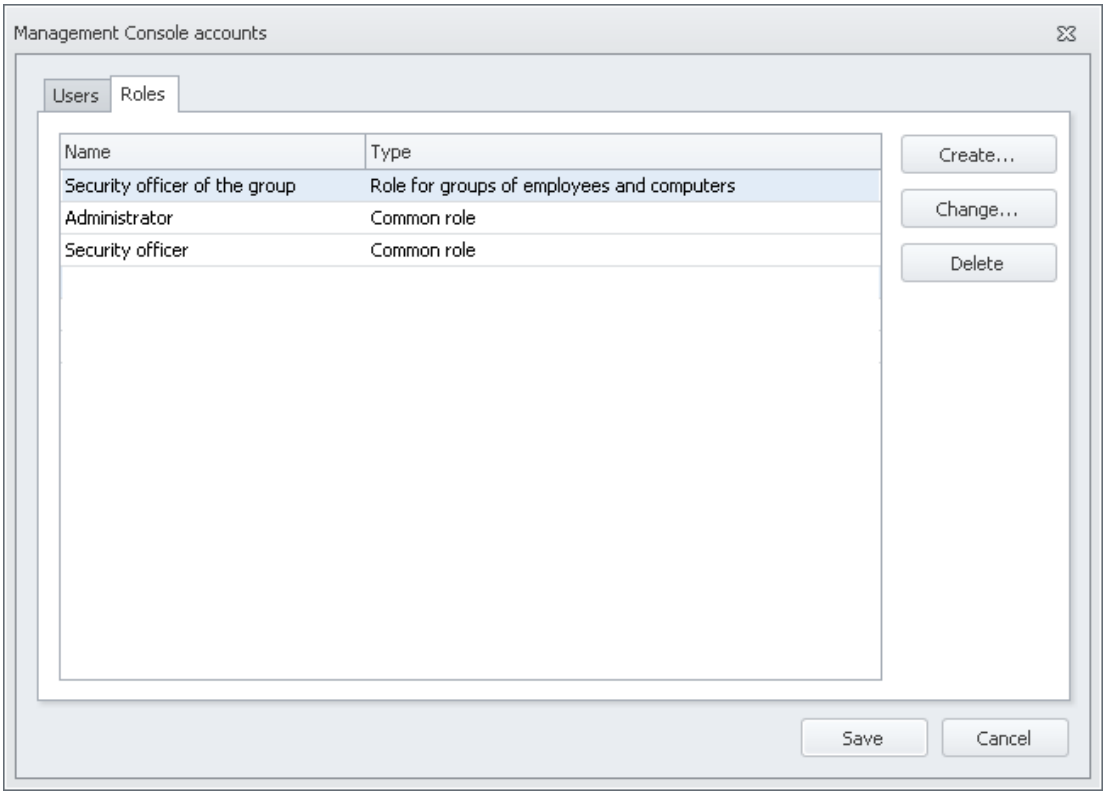
Restoring Account

To restore an account, add the account again with the same login (see "Adding New Management Console Account").

4.2.2 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 User".

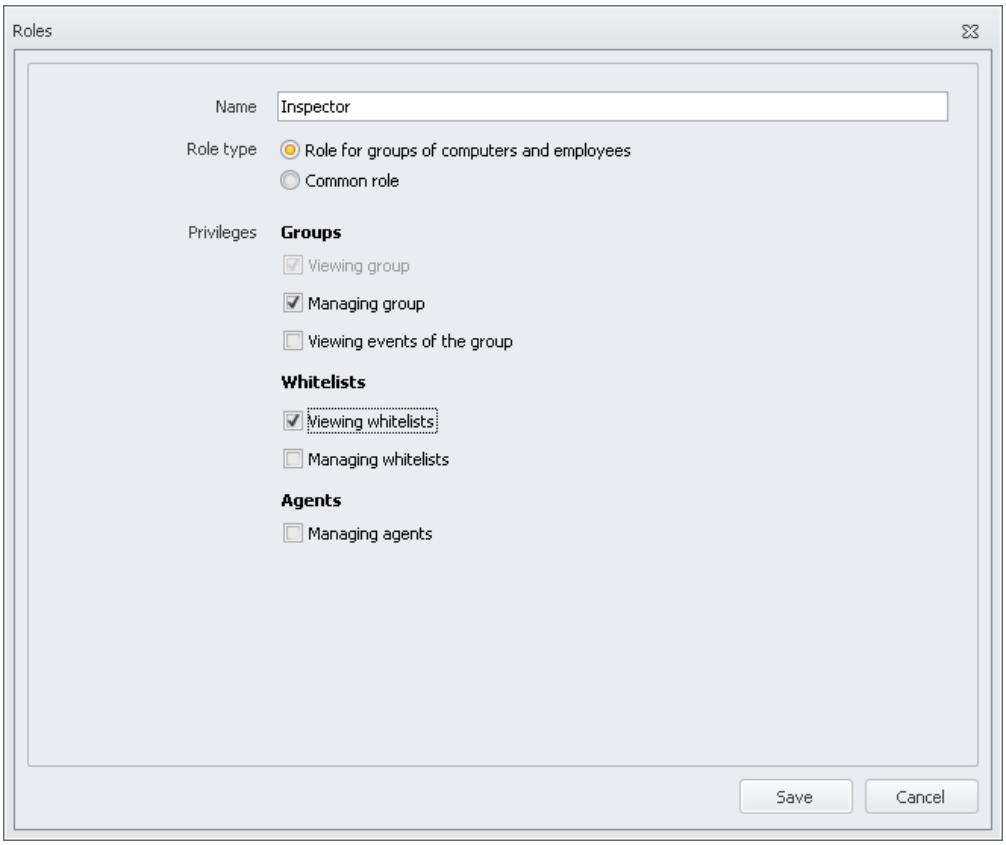
Adding Role of the Management Console User

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 • View the group parameters • View the list of computers/employees included in the group • View the effective policy for the computer/employee • 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 for reading or editing) • Add/delete computers/employees of the group • Copy computers, employees or subgroups of the group • Manage all subgroups of the group • Delete groups **Note:** adding this privilege enables the **View group** privilege.
View group events	View events received from workstations/employees of the group and its subgroups. **Note:** adding this privilege enables the **View group** privilege.
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 and its subgroups. **Note:** adding this privilege enables the **View whitelists** privilege.
Agents	
Manage agents	Add workstations from the group and its subgroups to the tasks to updating/deleting agents or changing the uninstallation password. **Note:** adding this privilege enables the **View group** 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 • Create new policy • 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) • Create new policy • Delete policy (available only to the owner)
Other privileges	
View audit log	Access to the "Log" section
Delete log entries	Delete entries from the audit log, clear the audit log. **Note:** adding this privilege enables the **View audit log** privilege.
Manage users	▪ View Console users and roles ▪ Create Console users and roles ▪ Edit Console users and roles ▪ Delete Console users and roles
Create groups	Create new groups of computers or employees. A new group is automatically added to the list of groups available to the user. The predefined role *Security officer of the group* is assigned to the group. **Note:** adding this privilege enables the **View all policies** privilege.
Manage agents on separate computers	• Add computers from the network environment and through connection to AD or ALD in the agent distribution task • Add computers through the file import or by name/IP in the agent distribution task • Create installation package • Delete agent from a mobile device
Manage settings	Manage global DM settings (except "Integration with AD" section in **Tools** -> **Settings** menu)
Sync with AD	Configure synchronization of workstations and employees with AD or ALD ("Integration with AD" section in **Tools** -> **Settings** menu)

Privilege	Available actions
Import/export of configuration	Import and export the security scheme and settings **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

Editing Role of DM Console User

Important!

If you edit a role that is currently authorized in the Management Console, 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 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.

Deleting Role of 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.

4.2.3 Management Console Security Scheme Operation Activity Log

Management Console operation involves various security scheme managing activities. Records related to activities that change database information (security scheme 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

Viewing Audit Log

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

Security scheme 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 is 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 panel. 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 panel.

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. See slector values interpretation in "Object Selector Values".
Field name	Object attribute changed by the action
Old value	Previous value of the attribute
New value	New value of the attribute
User	Name of Management Console account that initiated the transaction
Windows account	Account with credentials for Windows authorization
Computer	Name of the computer that initiated the action
Sequence number	Record number in the database

Note:

Change of Agent status via DM console will create a record containing the above listed attributes.

Some information from **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 10 corresponds to a change in security scheme. This was done in five steps. Steps 1-4 added *Floppy control* rule to *Device policy*. Each step configures a single rule parameter. For example, steps 1 and 2 define the time from which and until which the rule is active. Step 5 adds a comment on the security scheme change.

Transaction number 9 is associated with audit log records export. This transaction includes one step.

Transaction number 8 corresponds to a change in *CD/DVD Access* rule of *Device policy*. It includes two steps. Step 1 limits CD/DVD access to *Read Only* and step 2 adds a comment on the security scheme change.

Object Selector Values

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

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

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

The following are sample interpretations of **Object 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 policy was added to your security scheme.

Object Selector value interpretation

Transaction took place while version 2 of security scheme was active. A policy named *New Policy* was added.

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 changes the access right to CD/DVD from *Full Access* to *Read Only*.

Object Selector value interpretation

Transaction took place while version 3 of security scheme was active. Changes occured in *Device policy* for *CD/DVD Access* rule.

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.

Object Selector value interpretation

All records for operations on objects *Policy* and *Rules* were exported during this transaction.

Log Records Filtering

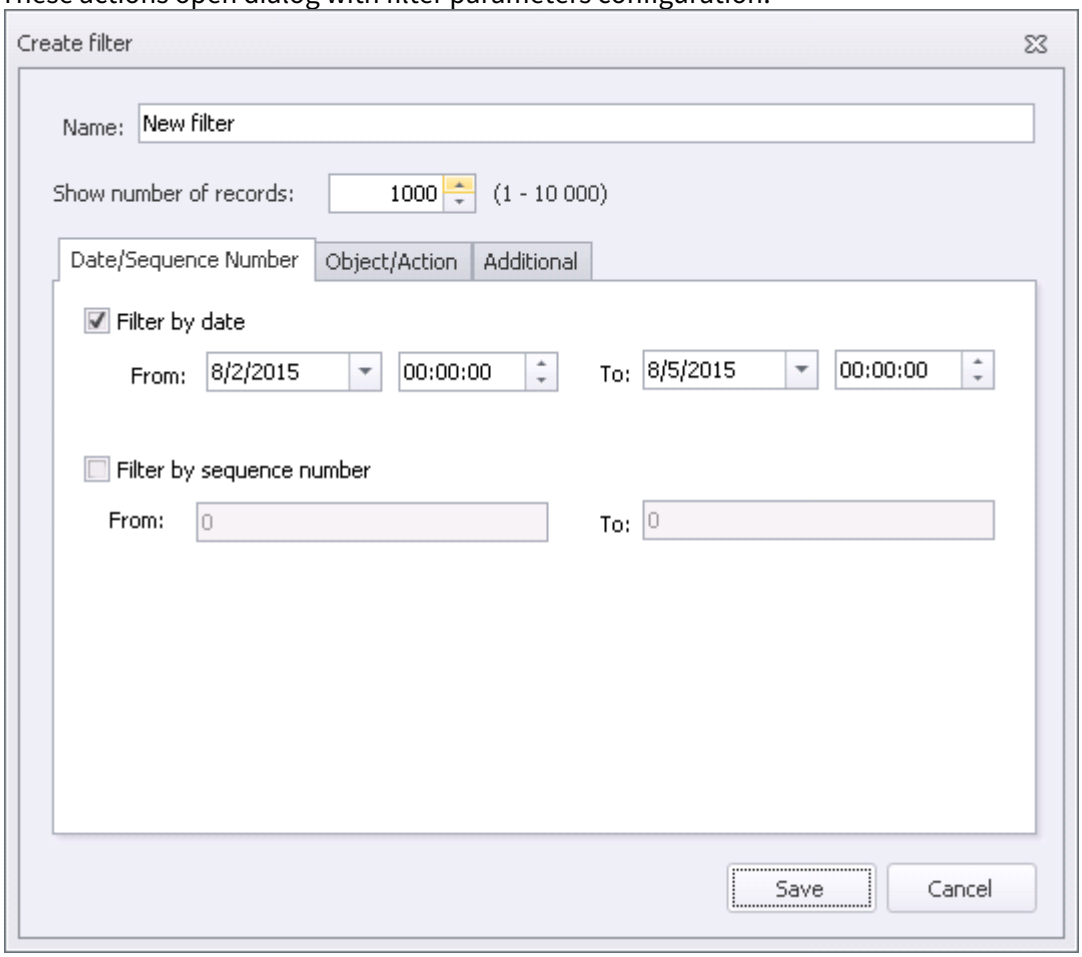
To access audit log records that meet certain criteria, you can use filters.

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

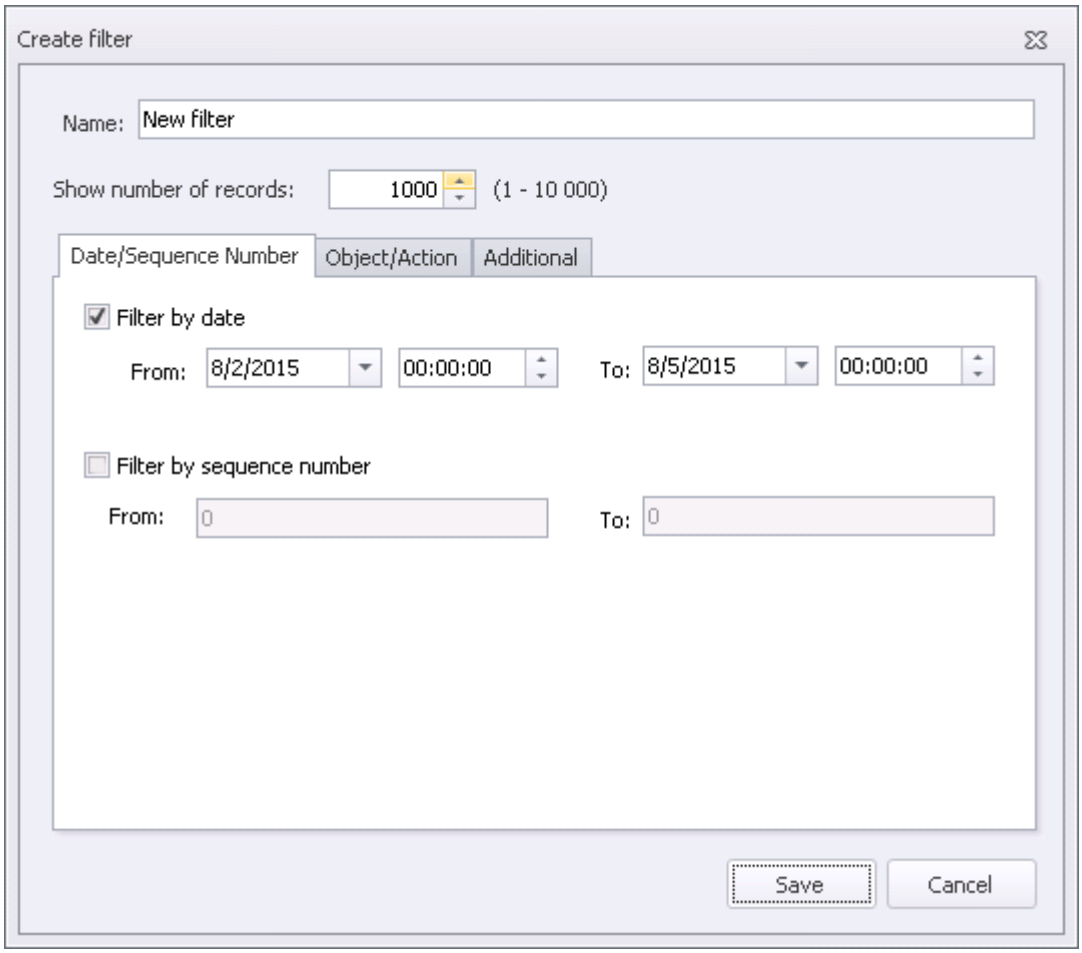
1. Go to **Log** section.
2. In the **Log** area of Navigation pane, select the name of the filter you want to remove.
3. Take one of the following steps:
   - in the Main Menu, select **Edit > Delete Filter**;
   - click  **Delete Filter** at the top of Navigation pane;
   - right-click the selected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

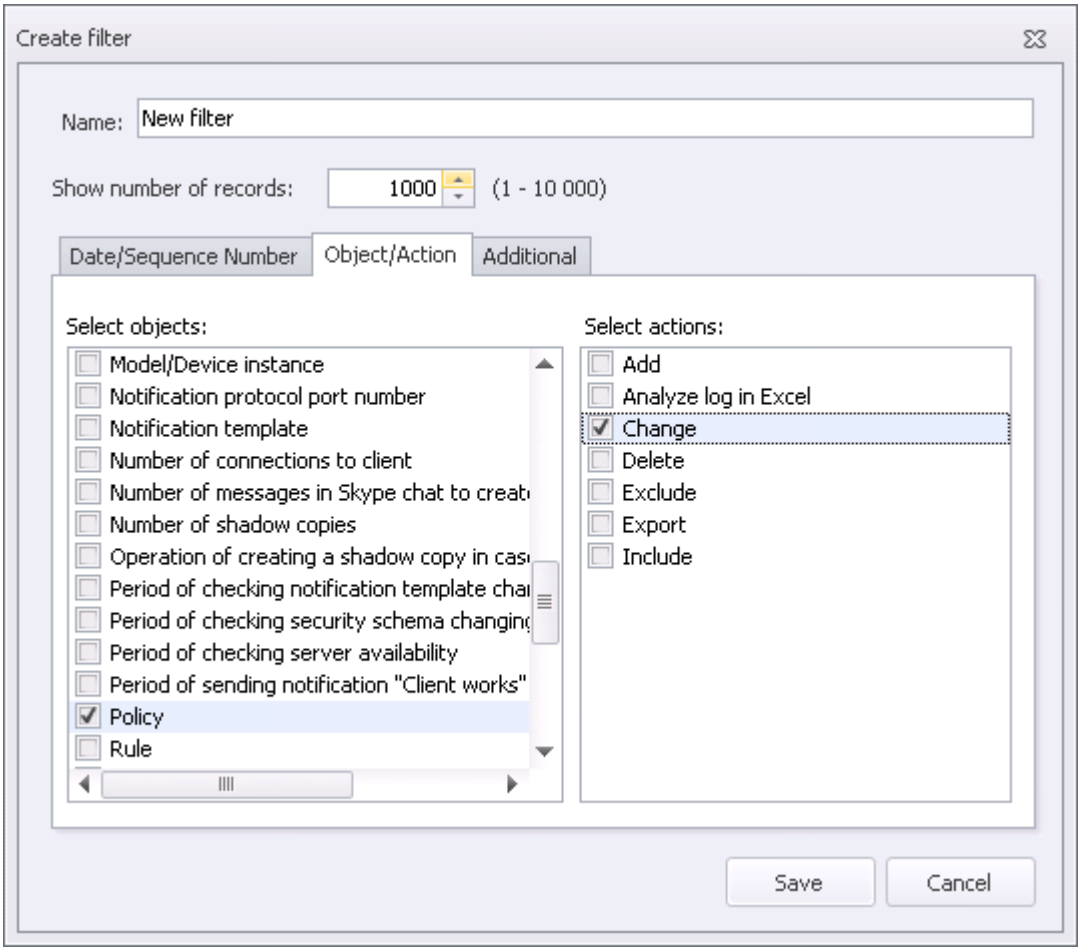
To filter by number:

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

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

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

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**.

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.

Analyzing Log Records in Microsoft Excel

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

To view Audit Log records in Excel:

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

This opens selected log in Microsoft Excel.

4.3 General System Settings

The System has a set of global settings that apply to all active policies and rules in Device Monitor. You can configure these settings in the **Tools > Settings** menu. For details, see the following articles:

- General Settings for Agents
- Corporate Network Control
- Messengers Control
- Network Traffic Control
- Device Monitor Server Settings. Connecting to Traffic Monitor Server
- Device Monitor Server Settings. Connecting to Platform Server
- Active Directory Connecting and Synchronizing
- Employee Notifications about Policy Violations
- Exclusion of Application from Interception
- Application control
- Control of Keyboard Input
- Event Storage
- Synchronization in Traffic Monitor Policies
- InfoWatch Device Monitor Server Manager
- Stopping and Starting Device Monitor Agents
- Setting Activity Status of Agents
- Configuring Agents distribution
- Automatic Update of Agents
- Setting Interception of Audio
- Settings to Send Data to Products

Modified settings apply after Agents are updated on controlled computers. Updating Agents is done as follows:

1. The Agent installed on the computer sends a request to the Server and checks the health of the Server, changes in the security scheme and changes in notification templates.
2. If there are any changes, the Agent receives a notification from the Server.
3. The Agent is updated.

4.3.1 General Settings for Agents

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

To configure common settings for Device Monitor agents operation:

1. In Main Menu select **Tools** > **Settings**.
2. In 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. Default value is 600 seconds.

Parameter	Description
Period of checking server availability	Interval (sec) with which the Agent checks Server availability. Default value is 2400 seconds.
Period of checking security scheme changing for active agent only	If the Agent operates in an active mode (the Agent itself polls the Server for security scheme modification), then this parameter sets the polling frequency (in seconds). Default value is 600 seconds.
Period of checking notification template changing for active agent only	If the Agent operates in an active mode (the Agent itself polls the Server for modifications of notification templates), then this parameter sets the polling frequency (in seconds). Default value is 1800 seconds. **Note**: For details on notification templates, see "Employee Notifications about Policy Violations".
Agent's disk space control	
Minimal free Agent's disk space	Minimal size of free disk space (%) of managed computer: when it is reached, shadow copies would not be created. Default value is 10%. I.e. if there is less free disk space than the parameter value, the System will not create a shadow copy or its part. 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 on 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 defined for employee/computer, then any actions controlled by security scheme could be denied. To deny, select **Operation will be blocked**. To allow all actions performed without 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 excessive 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 "Device

Parameter	Description
	Monitor Rule", "Cloud Storage Monitor Rule", "Viewing Events". The following options are available: • **None** – do not save events • **In case access denied** – events are created only if security policy violation is attempted; i.e. when device usage was denied, including blocking attempts of access level exceeding. The using of external devices which are not forbidden by policies, is not logged • **All** – all actions are logged (connection/usage of any devices, even from white lists)
Log connections outside of corporate network	Level of detailing when saving information about data transfer by network connections received by Network Monitor interceptor: see details in "Network Monitor Rule". The following options are available: • **None** – do not save events • **In case access denied** – events are created only if security policy violation is attempted; i.e. when connection attempt was denied
Agent activity on computer	
Show employee notifications	Indicates if an employee attempting to perform an action forbidden by security policy would receive a warning message. See details in "Employee Notifications about Policy Violations"
Hide the Agent presence	Indicates if Windows system tray of managed computer hides the Agent presence on the computer. 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. **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 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**

Parameter	Description
	and **Confirmation code** settings. Frequent update is not recommended.

4. To apply changes, click **Apply** and then **Save**.

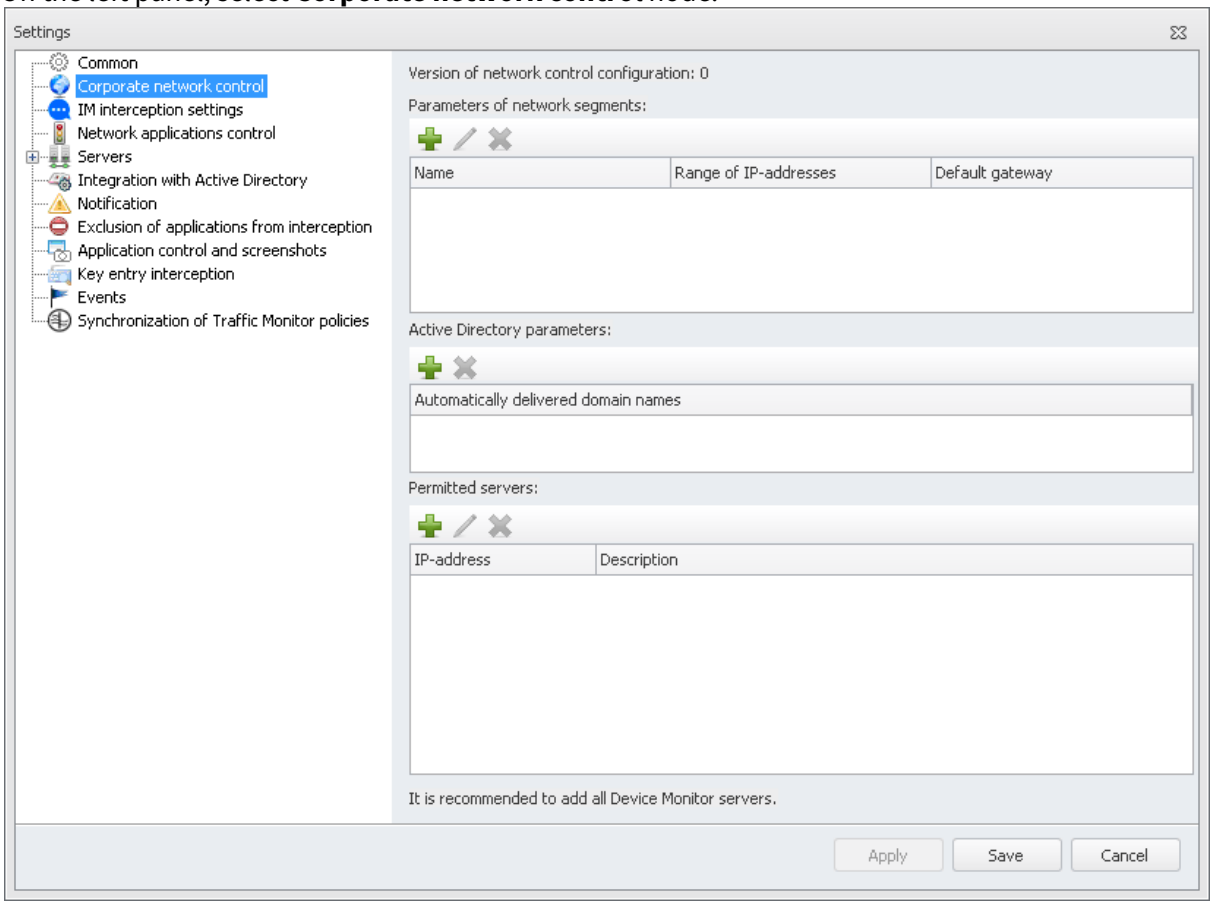
4.3.2 Corporate Network Control

To provide the data transfer control via network connections using **Network Monitor** (information on configuring the rule see in "Network Monitor Rule") you should specify the network segments to be considered the corporate network and which external addresses are permitted.

> **Note:**
>
> Permitting the external addresses can be required to provide the work with external resources when the Agent is outside the corporate network, such as VPN server or corporate network.

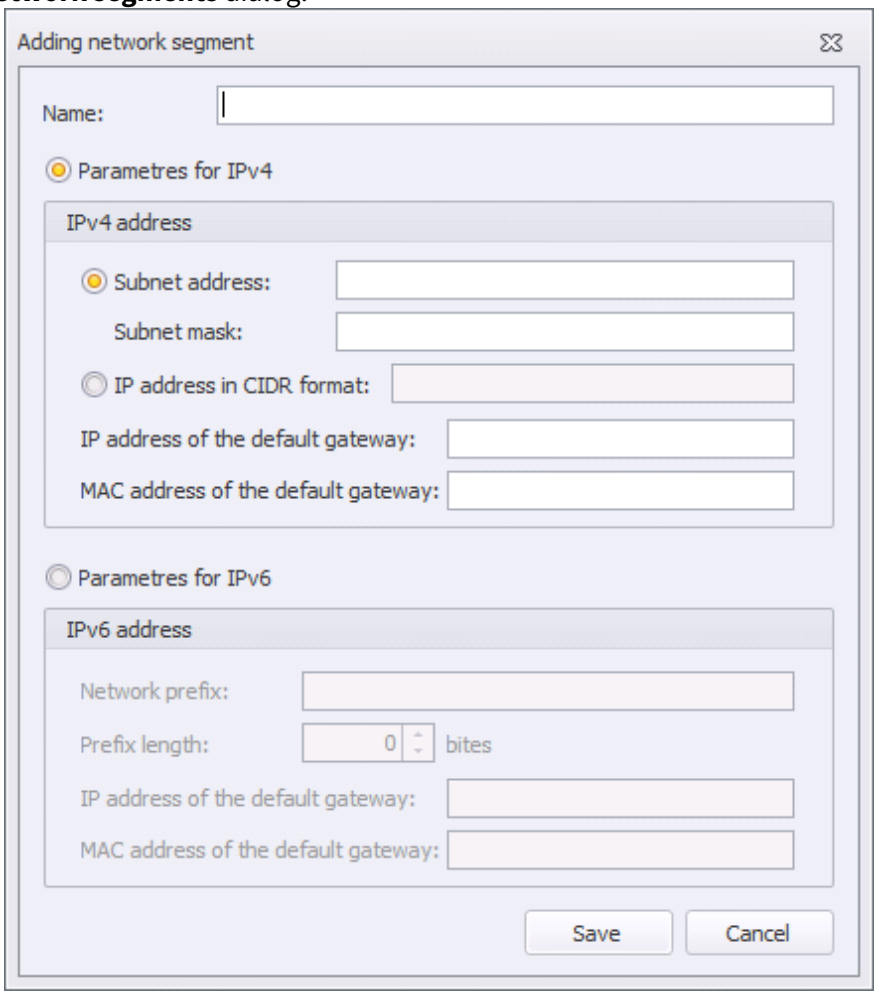
To configure corporate network settings:

1. In the Main Menu, select **Tools** > **Settings**.
2. On 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 have 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 have 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.

4. To define Active Directory parameters, click in the **Active Directory parameters** area. 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 **OK**.
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**.

How the System detects connections to the corporate network for different cases:

1. Only **Parameters of network segments** are specified. In this case, both domain and non-domain workstations are considered to be on the corporate network if:
   a. The IP address of the workstation is included in one of the specified segments.
   b. The IP address and MAC address of the default gateway correspond to the values specified for this segment.
2. Only **Active Directory parameters** are specified. In this case:
   a. A domain workstation is considered to be on the corporate network if:
      i. The network has a domain with the specified parameters.
      ii. It is possible to connect through a specific network adapter to a domain controller the workstation belongs to.
   b. A non-domain workstation is considered to be always on the corporate network.
3. Both **Parameters of network segments** and **Active Directory parameters** are specified. In this case:
   a. A non-domain workstation is considered to be on the corporate network if:
      i. The IP address of the workstation is included in one of the specified segments.
      ii. The IP address and MAC address of the default gateway correspond to the values specified for this segment.
   b. A domain workstation is considered to be on the corporate network if:
      i. The IP address of the workstation is included in one of the specified segments.
      ii. The IP address and MAC address of the default gateway correspond to the values specified for this segment.

   OR

      i. The network has a domain with the specified parameters.
      ii. It is possible to connect through a specific network adapter to a domain controller the workstation belongs to.

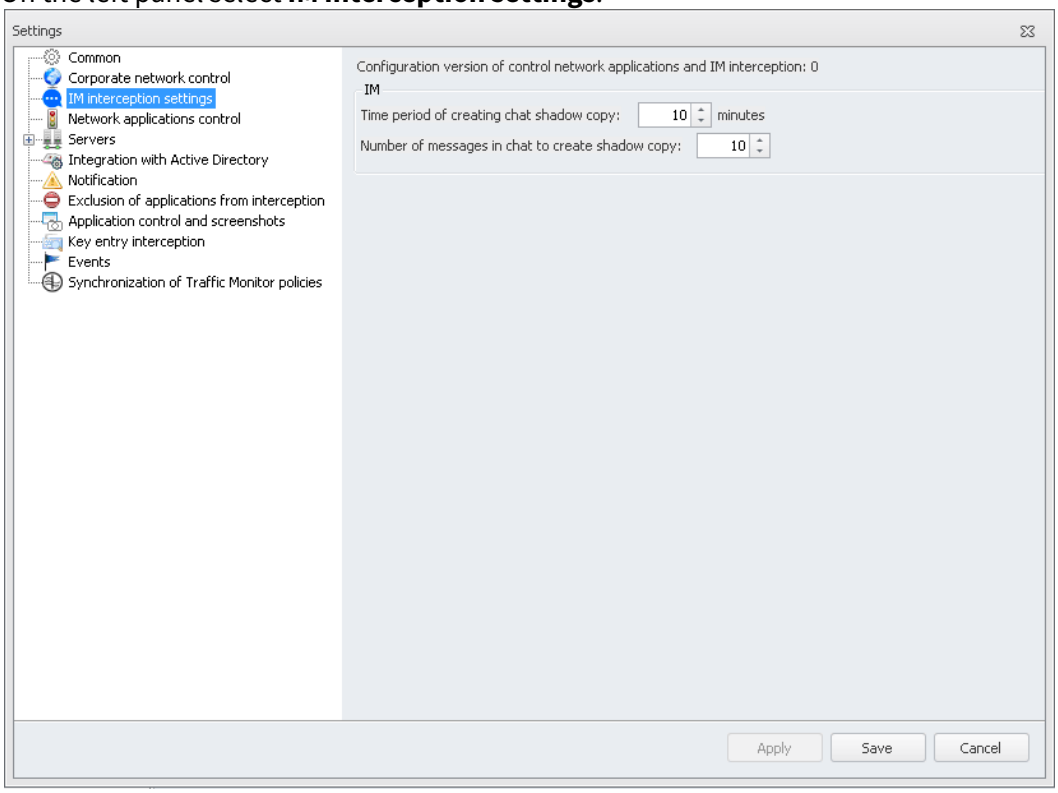
4.3.3 Messengers Control

When controlling the traffic, you can set additional settings for messengers (for more information on configuring this type of rules, please see IM Client Monitor Rule).

To configure the messengers control:

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

2. On the left panel select **IM interception settings**.



3. Specify the messengers control settings: set the assembling frequency for chat shadow copy to be sent for analysis to Traffic Monitor. You can specify the time frame (minutes), after expiration of which the shadow copy should be assembled (**Time period of creating chat shadow copy**), the number of messages, beyond which the shadow copy should be assembled (**Number of messages in chat to create shadow copy**). If the file sending is being processed within the chat, the shadow copy can be assembled before the period specified.

4.3.4 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, S/MIME, Outlook, 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.

Note:

If an employee uses Yandex.Browser on a workstation with Agent installed, the browser may show warnings when connecting to HTTPS resources.

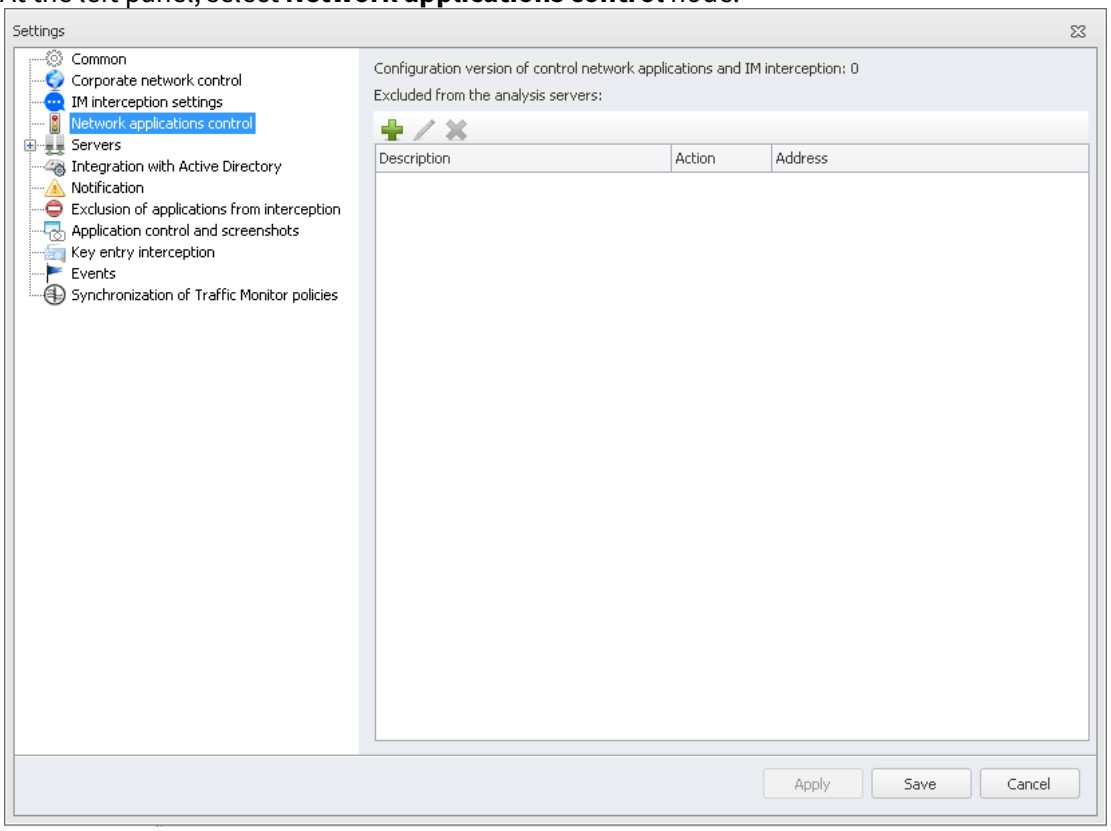
If the Agent intercepts HTTPS traffic for a resource, Yandex.Browser warns when connecting to the resource that:

- Device Monitor may have access to the information that the user views or enters on the resource;
- the connection may be unsafe.

When configuring the traffic control, you can specify additional parameters for mail systems (see "Mail Monitor Rule"), and FTP/FTPS traffic (see "FTP Monitor Rule"). 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 applications control** node.



3. You can specify a list of server IP addresses which protocols will not be controlled (i.e. traffic sent to those servers will not be redirected to internal proxy server) or will be compulsory controlled (to be redirected to internal proxy server).

> **Note:**
>
> Permitting external addresses can be required to provide work with external resources and update the programs installed, for example:
>
> - Firefox automatic update needs *.mozilla.com and *.mozilla.net in the list of permitted servers
> - Filezilla requires update.filezilla-project.org
> - Dropbox needs *.dropbox.com
> - Yandex Disk requires:
>   - oauth.yandex.ru
>   - webdav.yandex.ru
>   - clck.yandex.ru
>   - push.xmpp.yandex.ru
>   - etc.

To set a list of servers excluded from analysis:

a. In **Excluded from the analysis servers** area, click .
b. In **Add server to the list of excluded from the analysis** dialog, enter the server description. For more information on addresses that can be added, see "Processing Addresses Added to Exclusions".
c. Select an option: **Exclude from interception** или **Include into interception**.
d. Specify DNS name or IP address of a server and connection port.
e. If required, select **Address range** and set the spacing options between IP addresses.

> **Note:**
>
> When excluding server from interception, you can also select and enter **Domain from MitM interceptor**, which traffic is to be excluded from interception using SSL connection.

f. Click **OK**.
g. To change the server parameters, select it in the list and click .
h. To delete a server from the list of excluded ones, select it, click , then click **Yes** in the confirmation dialog.

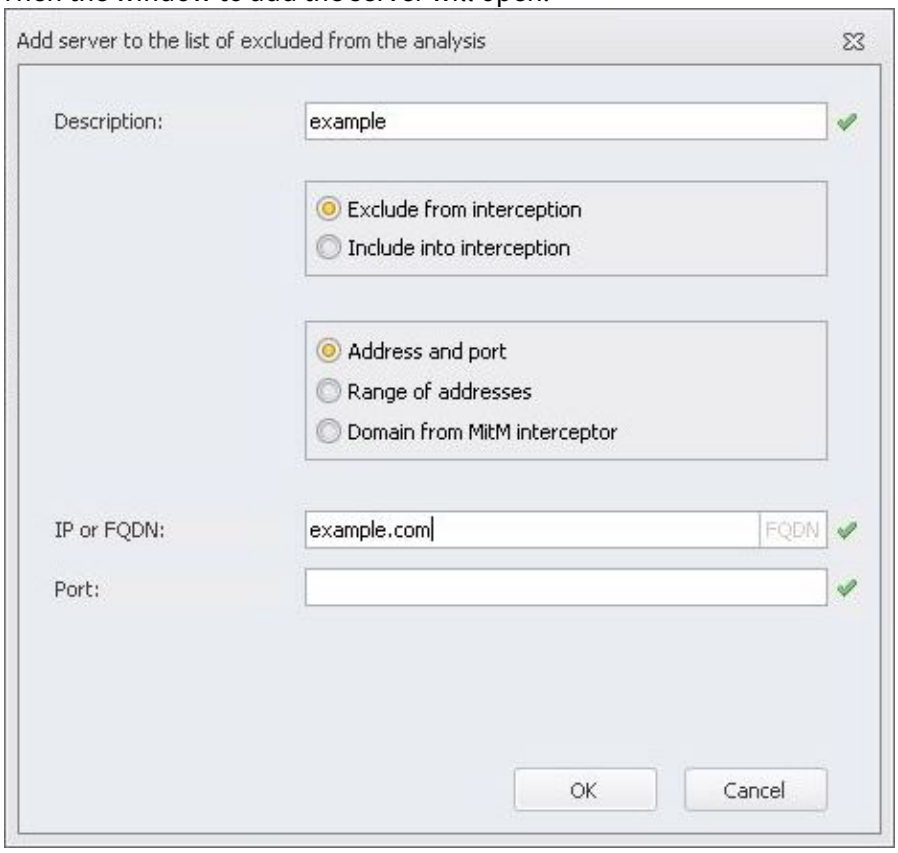
4. When all changes are made, click **Apply**.

Adding Servers to Exclusions

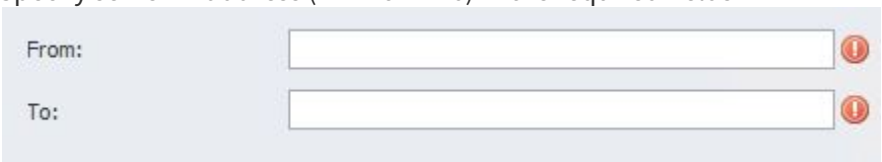
Adding server address to exclusions, (see "Network Traffic Control") it is required to specify the server IP address or FQDN.

To set the list of servers, permitted or forbidden:

1. In **Servers excluded from analisys** area press .
   Then the window to add the server will open:



2. In the window **Add server to the list of excluded from analysis** enter the server description:
   - To add a separate server port:
     a. Select the required action: **Exclude from interception** or **Include into interception**;
     b. Select the check box in the field **Address and port**;
     c. Specify FQDN or server IP address (IPv4 or IPv6) and connection port;
   - To add the addresses range:
     a. Select the required action: **Exclude from interception** or **Include into interception** ;
     b. Select the check box in the field **Range of addresses** ;
     c. Specify server IP address (IPv4 or IPv6) in the required fields



   - To add the resources group exclusion from interception via SSL/TLS connection template:
     a. Select **Exclude from interception**;
     b. Select the check box in the field **Domain from MitM interceptor**;
     c. Specify the domain



3. Click **OK**.

In the form of a text IPv4 address is speciified as nnn.nnn.nnn.nnn, where nnn has a value from 0 to 255 and each n letter means decimal figure. Zero with no value should not be specified.

In the form of a text IPv6 address is specified as xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, where each x letter is a hexadecimal figure, meaning 4 bits. Zero with no value should not be specified.

> **Note:**
>
> Including into interception has higher priority than exclusion.
>
> Exclusion template will operate in case the agent is connected via proxy server.
>
> 0.0.0.0 address is applied only together with a port, since it is a special address for all the exclusions with the port specified.

Example 1:

To exclude from interception the whole 10.128.0.2 traffic, except the one for port `8080`:

1. Exclude from interception the server with IP address `10.128.0.2` not specifying the port;
2. Include into interception the server with IP address `10.128.0.2,` specifying the port `8080.`

Example 2:

To exclude from interception a range of addresses `192.168.0.1` - `192.168.0.255` except one specific address `192.168.0.5`:

1. Exclude from interception a range of addresses `192.168.0.1` - `192.168.0.255`;
2. Include into interception the server with IP address `192.168.0.5.`

Example 3:

To exclude from interception the port `8080` on all the servers, exclude from interception the server with IP address `0.0.0.0`, specifying the port `8080`.

To change server configuration, select it in the list and click .

To remove server from the list of permitted ones, select the one required and click , then click **Yes** to confirm the removal.

4.3.5 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.

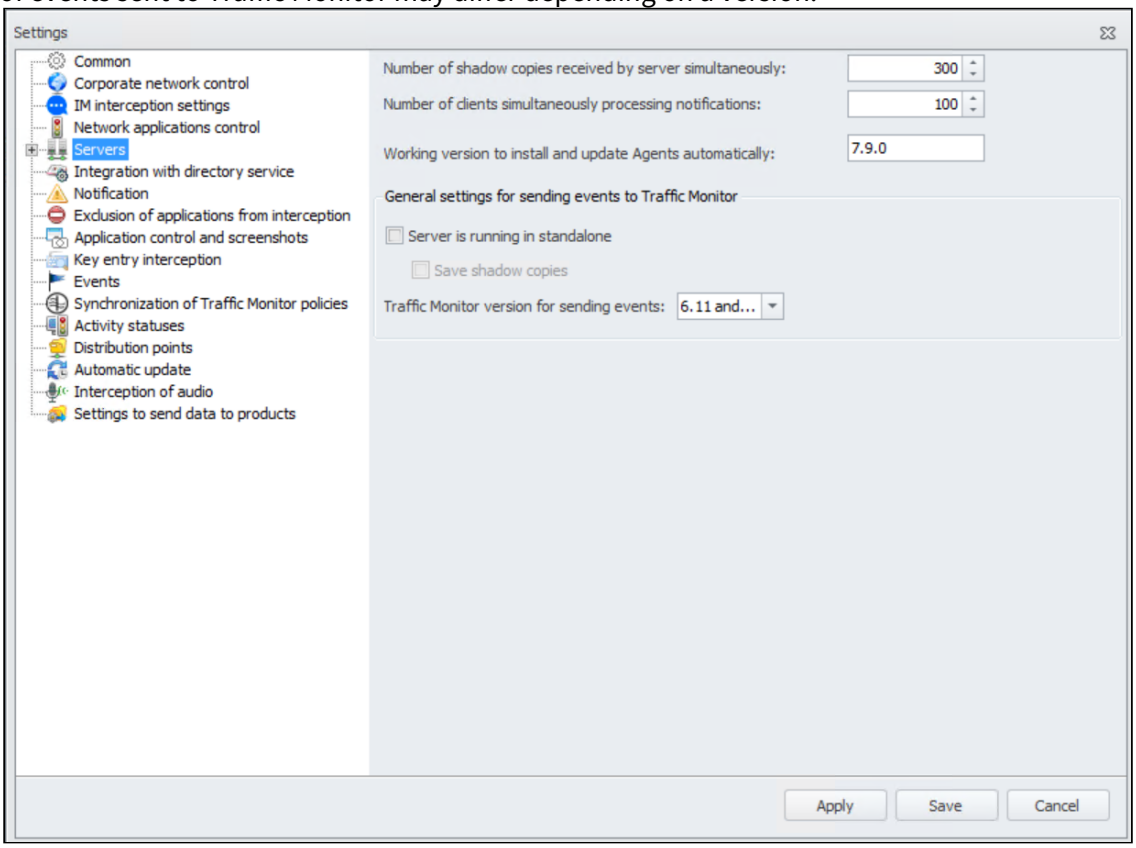
To view and set up Traffic Monitor connection parameters:

1. In Main menu, select **Tools -> Settings**.
2. In **Servers** node, set up the following parameters:
   - **Number of shadow copies received by server simultaneously** – determines the number of copies that can be sent to Traffic Monitor Server simultaneously.
   - **Number of clients simultaneously processing notifications** – determines the number of agents that can receive notifications (e.g. DM security policy) from the server at a time.

- **Working version to install and update Agents automatically** – determines the version to automatically install or update Device Monitor Agents. The version is displayed when creating a new primary distribution task. Specify the first three figures of the version, for example: 7.9.0.

> **Note:**
>
> You can view all available versions at `C:\ProgramData\InfoWatch\SetupPackages\`.

- **Server is running in standalone** – the server is running without integration with Traffic Monitor: events are stored on Device Monitor server and are not sent to Traffic Monitor.
  - **Save shadow copies** – shadow copies are saved locally in `ShadowCopyTempDir`.
- **Traffic Monitor version for sending events** – the current version of Traffic Monitor. Format of events sent to Traffic Monitor may differ depending on a version.



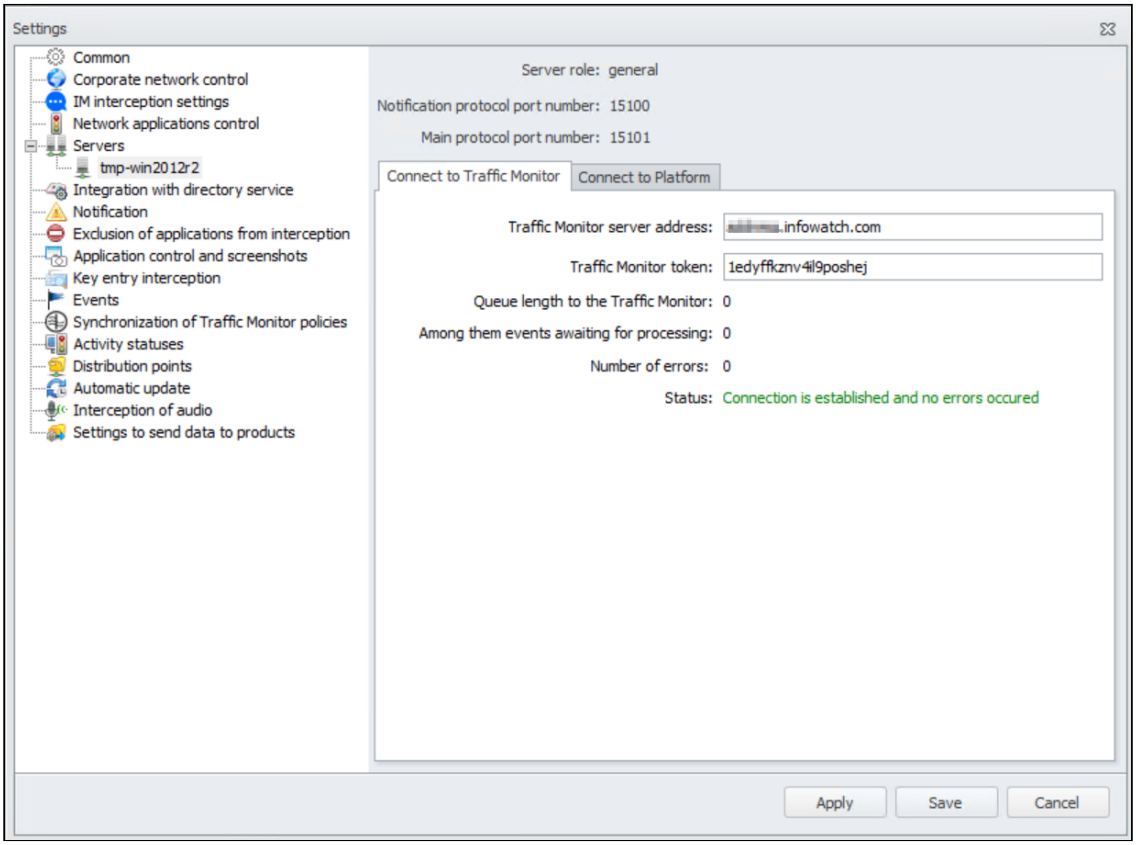
3. When selecting the connection server, the following connection parameters are displayed:
   - **Server role** – server role (primary or secondary) assigned to this server during installation: see "InfoWatch Device Monitor Server End Installation Procedure".
   - **Notification protocol port number**
   - **Main protocol port number**

> **Note:**

Changing server role (*General* or *Secondary*) as well as **Notification protocol port number** and **Main protocol port number** attributes are performed with InfoWatch Device Monitor Server Manager (see "InfoWatch Device Monitor Server Manager").

- **Traffic Monitor server address** – address of InfoWatch Traffic Monitor server to work in the Management Console. This server will receive events.
  Supported formats:
  - `host:port`
  - `protocol://host:port/`, where `protocol` should be `xml` for Traffic Monitor versions under 6.0 and `rcp` for Traffic Monitor versions 6.0 or higher
  - `host:port/`

  The address should be in the URI (Uniform Resource Identifier) format whose formal syntax is described in RFC 3986 http://tools.ietf.org/html/rfc3986.
  The *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** – the number of events pending submission to InfoWatch Traffic Monitor.
- **Among them events awaiting for processing** – the number of events pending processing before being sent to InfoWatch Traffic Monitor.
- **Number of errors** – the number of events in the error queue.
- **Status** – information on Traffic Monitor connection state.



When Device Monitor Server connects to Traffic Monitor Server, the remote server certificate is validated. For successful connection to the remote server, configure this validation. For

details, see "*InfoWatch Device Monitor. Installation, Configuration and Administration Guide*", "Configuring validation of the remote server certificates" article.
If the Traffic Monitor XAPI service certificate validation fails, then the **Status** parameter gets the *Certificate verification error* value.

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

4.3.6 Device Monitor Server Settings. Connecting to Platform Server

> **Important!**
>
> This functionality is used to interact with Activity Monitor and Prediction.

To be able to send events to the Platform, you need to configure Server – Platform connection parameters.

> **Note:**
>
> You can also send information about whitelisted devices to the Platform. For details, see the knowledge base article: "Sending data about devices from DM whitelists to the Platform".

To view Platform and Activity Monitor connection parameters:

1. In main menu, select **Tools > Settings**.
2. In the **Servers** node, select a server.
3. Select the **Connect to Platform** tab.

To configure connection with the Platform server:

1. In main menu, select **Tools > Settings**.
2. In the **Servers** node, select a server.
3. Select the **Connect to Platform** tab.
4. Specify the values of the **Platform server address** and **Platform token** parameters.
5. Click **Apply**.
6. Click **Save**.

To configure Activity Monitor connection:

> **Important!**
>
> The setting is required to connect to workstations of employees for online monitoring (online monitoring is available starting from DM 7.9.0).
>
> DM server – Activity Monitor connection should be configured only on the main server.

1. In main menu, select **Tools > Settings**.
2. In the **Servers** node, select a server.
3. Select the **Connect to Platform** tab.
4. Mark the checkbox  **Getting control commands from AM**.

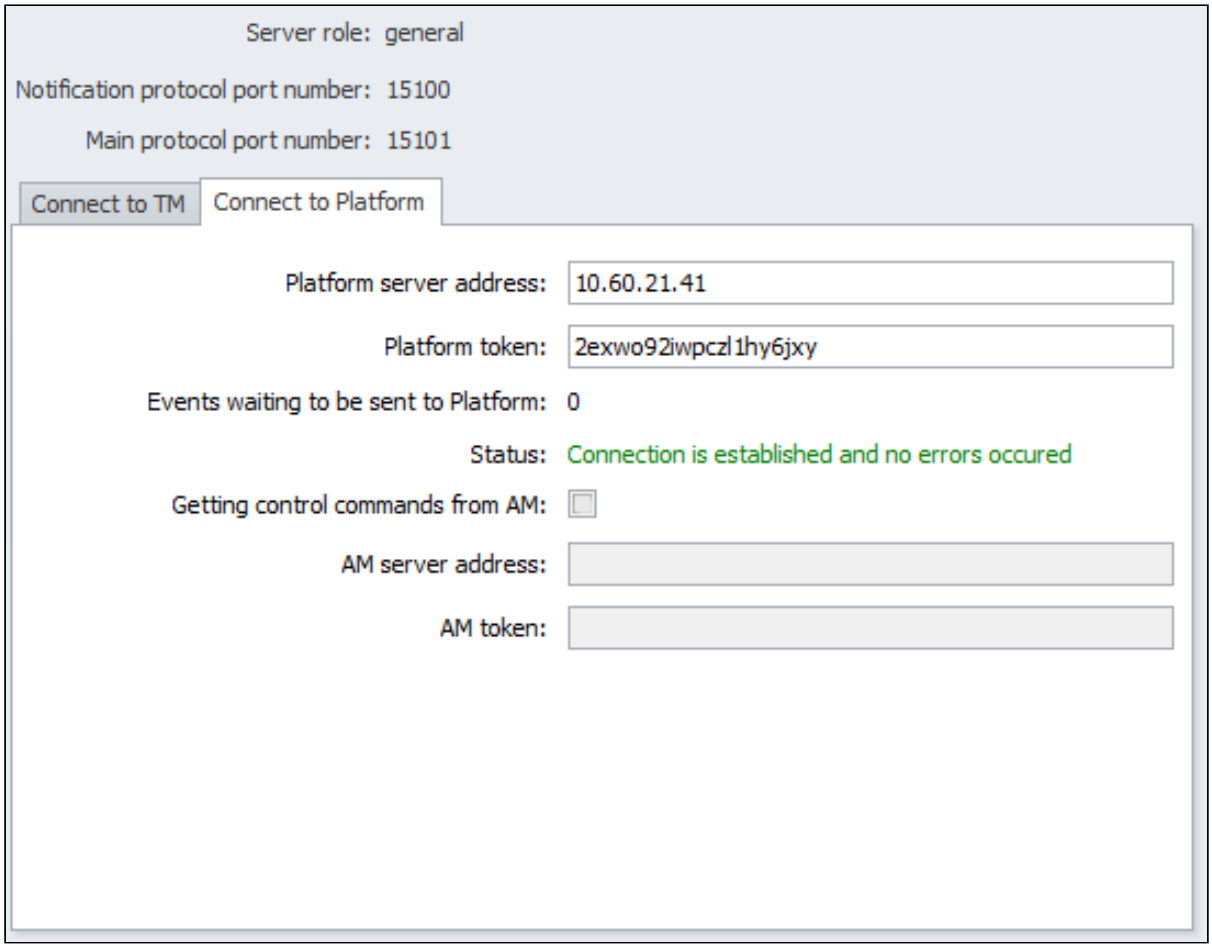
5. Specify the values of the **AM server address** and **AM token** parameters.
6. Click **Apply**.
7. Click **Save**.

Connection parameters

- **Server role** – server role (general or secondary) assigned to this server during installation (see "InfoWatch Device Monitor Server End Installation Procedure").
- **Notification protocol port number**.
- **Main protocol port number**.

> **Note:**
>
> Changing server role (General or Secondary) as well as **Notification protocol port number** and **Main protocol port number** attributes are performed with InfoWatch Device Monitor Server Manager (see "InfoWatch Device Monitor Server Manager").

- **Platform server address** – address of Platform server to work in the Management Console. This server will receive events. The connection string is to be filled in the format (server address):(port), where port is an optional value (default port to connect to Platform is 17104). Supported formats:
  - host
  - host:port
- **Platform token** – the token to connect to API. Required for Platform v. 1.5.0 or higher. You can get the actual token from the section Global settings of Activity Monitor (see details in "Infowatch Activity Monitor. Administration Guide", "Global Settings").
- **Events waiting to be sent to Platform** – the number of events pending submission to Platform.
- **Status** – information on Platform connection state.
- **Getting control commands from AM** – parameter that enables the connection between DM and Activity Monitor.
- **Activity Monitor server address** – address of Activity Monitor server to work in the Management Console. This server will receive events. The connection string is to be filled in the format (server address). Or (server address):(port), if you need to use a port different from the default port (default port of Activity Monitor server is 443). Supported formats:
  - host
  - host:port
- **Activity Monitor token** – the token to connect to API. Required for Platform v. 2.1.X or higher. You can get the actual token from the section Global settings of Activity Monitor (see details in "Infowatch Activity Monitor. Administration Guide", "Global Settings").



Note:

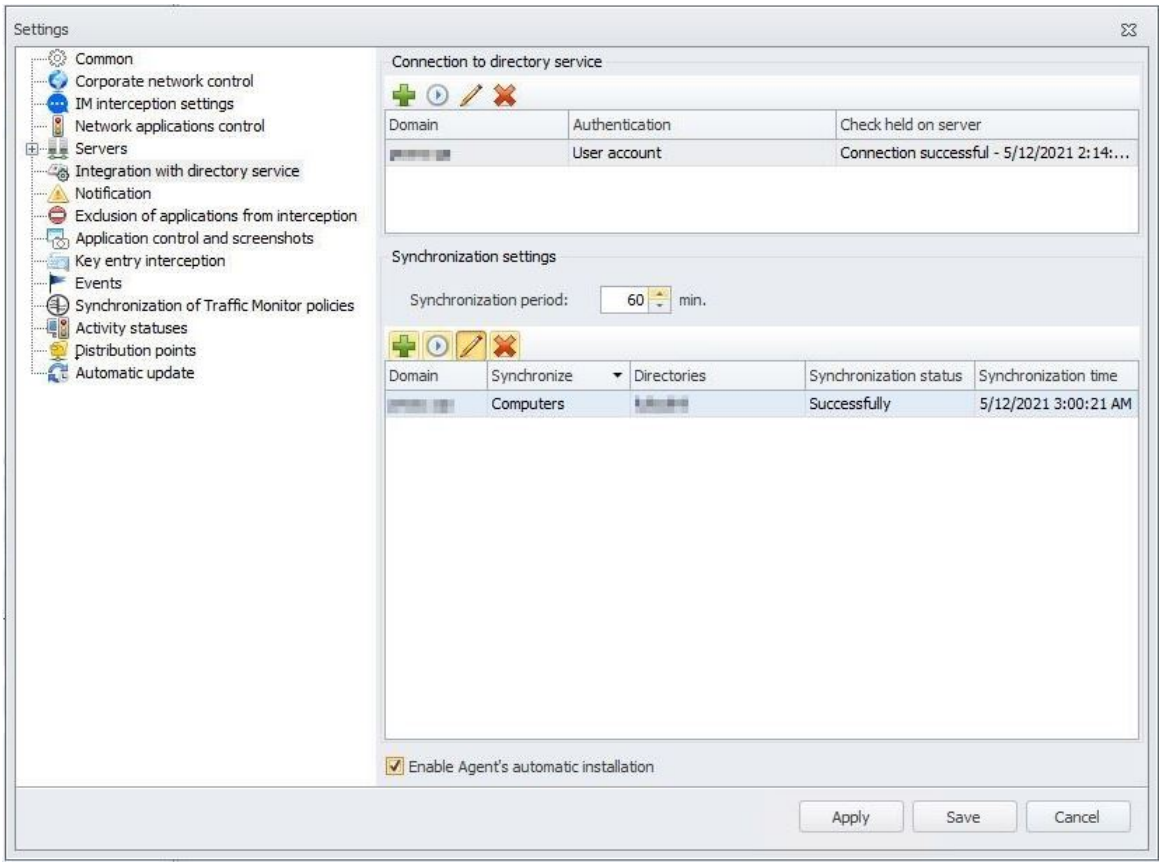
The **Getting control commands from AM**, **AM server address**, **AM token** parameters are not used in Activity Monitor version 2.0.x and lower.

Note:

When Device Monitor Server connects to Platform Server, the remote server certificate is validated. For details, see "*InfoWatch Device Monitor. Installation, Configuration and Administration Guide*", "Configuring validation of the remote server certificates" article.
If the Platform EPEVENTS service certificate validation fails, then the **Status** parameter gets the *Certificate verification error* value.

4.3.7 Active Directory Connecting and Synchronizing

You can specify all the attributes of synchronization and connection to directory service in settings. Indicate connection settings when connecting to LDAP using management console. To receive information about computers and employees from directory services, specify LDAP server connection parameters.



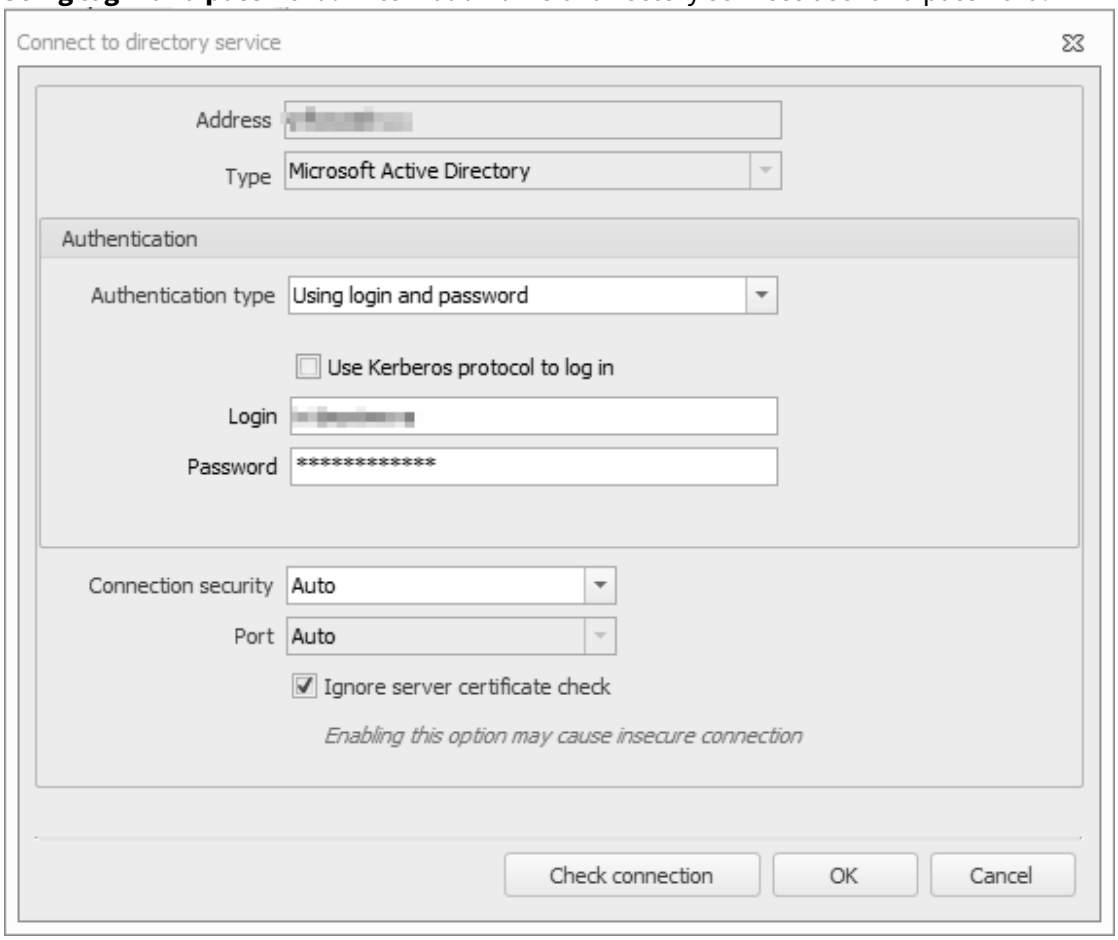
To configure synchronization parameters with LDAP server:

1. In main menu of management console (DM) select **Tools** > **Settings**.
2. Open **Integration with directory service**.
3. If you connect to directory service for the first time, click  in **Connection to directory service** section.
4. In **Address** field specify LDAP server domain name, IP address or click **Select domain from forest**. The forest should be selected in accordance with the user, who started the management console.
5. Specify directory service, if you know it or select **Auto**. After successful connection is confirmed, **Auto** type will be changed to this LDAP type.

   > **Warning!**
   >
   > Once the connection settings are saved, the type of directory service cannot be changed.

6. Specify Authorization details to connect to directory service:

- **Using login and password.** Enter valid name of directory services user and password.



- **User account.** Credentials of the current Windows session, that the System was started under, will be used for authorization.
- **Using client certificate.** Specify the full name of private key and certificate in `.p12` or `.pfx` format and the key password.
- **Anonymous.**

7. When selecting **User account** or **Using login and password**, you can also add Kerberos protocol support.
8. Click **Advanced** to establish secure connection and select from: **Auto**, **STARTTLS, LDAPS** or **Unprotected**. If you select Kerberos protocol support or **Using client certificate**, **Auto** will be applied.

> **Warning!**
>
> Synchronization using secure connection is supported for ActiveDirectory only.

9. Indicate the port, that will pespond to requests when the default port 389 is unavailable: **Auto**, **636**. If you select **Auto** or **Using client certificate**, or enable Kerberos protocol support, then **Auto** will be applied.
10. Enable the option **Ignore server certificate check**, if you don't need to check the certificate, that is sent from server while establishing secure connection.
11. Click **Check connection** and make sure that it is successfully established.
12. Click **OK**.

To check connection to previously created synchronizations:

1. In **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**.

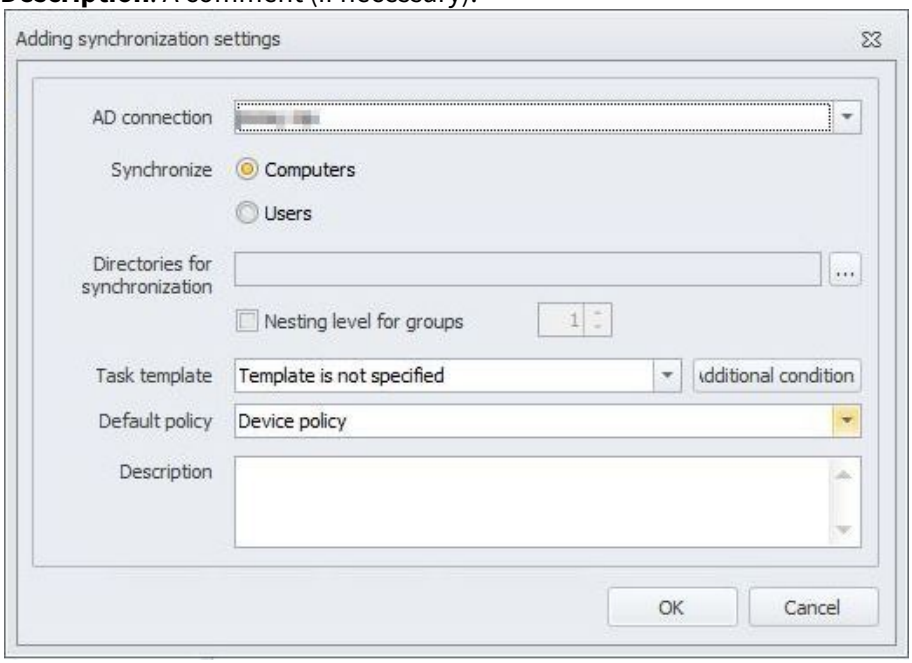
After configuring synchronization parameters, define what information directory services are required to provide and what policies are to be applied afterwards.

> **Note:**
>
> Synchronization is launched for Organizational units and Security groups of Active Directory

To add synchronization settings with Active Directory:

1. In **Synchronization settings** area, click .
2. In a dialog window, specify synchronization settings:

- **AD connection.** Name of the domain to which connection was installed before
- **Synchronize**. Synchronization objects - **Computers** or **Users**.
- **Directories for synchronization**. Directories in Active Directory, that must be synchronized. For synchronization:
    1. Click .
    2. In the tree, specify directories for synchronization.
    3. Click **Select**.
- **Nesting level for groups** (if necessary). The maximum nesting level is 100.
- **Task template**. Template for directory for synchronization is not specified by default.
- **Default policy**. A policy that will apply to synchronized groups after the first synchronization.
- **Description**. A comment (if necessary).



- Click **OK**.
- To apply changes, click **Apply** in the **Settings** window.
- Check the table with synchronization settings and results:

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

Note:

For users and computers the synchronization is to be configured separately. You can add several synchronization settings for the same domain.

To launch synchronization with Active Directory:

1. In **Synchronization settings** 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 (every 1 hour by default) and click **Apply**.

After each synchronization, including the first, a task of creating primary distribution on computers added to security scheme after synchronization, will be automatically created on condition that a synchronization template will be chosen (see details in the article "Automatic Agent Installation").

To edit Synchronization settings with Active Directory:

1. In **Synchronization settings** area, choose the desired row.
2. Click .
3. Edit synchronization settings.
4. Click **OK**.

To disable synchronization with Active Directory:

1. In **Synchronization settings** area, choose the required row.
2. Click .
3. In the confirmation window, click **Yes**.

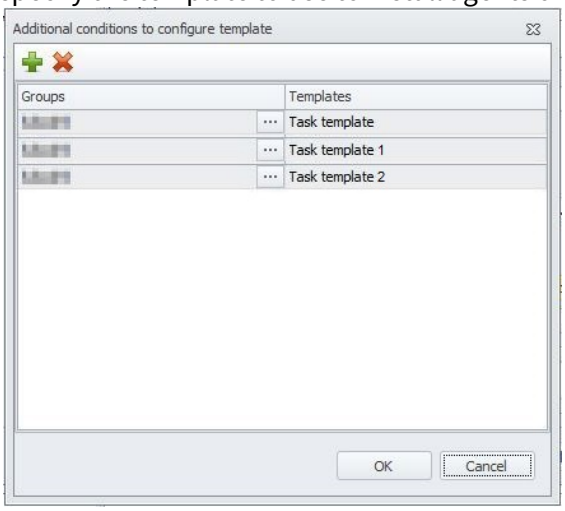
Warning!

When deleting synchronization settings, all groups of computers or user groups associated with this settings will be removed.

Automatic Installation of Agent

To configure automatic installation of agents on new computers or the ones of selected departments:

1. Create a new synchronization or choose one from already created, then open it for editing:
2. Select **Synchronize > Computers**
3. Specify Active Directory directories, for nested groups of which automatic installation of agents is required.
4. In settings of synchronization with Active directory, specify a task template if it was created earlier for distribution task. According to this template, the primary distribution task will be created and started after synchronization, if new computers will appear in the directories specified in step 3. Proceed to step 7.
5. To configure agent installation for nesting groups separately, you need to specify a different template for these groups. In this case, the task specified in additional conditions of synchronization will be created for the group and its subgroups. And otherwise, if using template option is excluded, then distribution task will not be created. Press **Additional conditions**.
6. In **Additional conditions of template setting** window**:**
   a. press , then
   b. select groups from directories, specified in step 3, press **Select**
   c. specify the template to use to install agents on the selected groups



   d. after specifying all additional conditions, press **OK**
7. Press **OK**
8. If the setting **Enable Agent automatic Installation** in **Tools > Settings > Integration with directory service** is disabled, then tasks will be created according to templates or computers will be added to already created tasks after synchronization. Installation task should be runned manually.
   Enabling the setting **Enable Agent automatic installation** will automatically start primary distribution task on new computers added after synchronization with Active Directory. Herewith, if a template is not specified, the setting does not change anything.
9. In **Settings,** press **Save**.

After the synchronization is complete, if there are new computers in OU a primary distribution task will be created according to the template:

- for each synchronization record
- for each template version
- for each working version.

If a task has been already created according to the template, then the new computers will be added to the existing task.

4.3.8 Employee Notifications about Policy Violations

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

- **Access to device denied** – Device Monitor rule which denies reading and writing to the device (see "Device Monitor Rule") was actuated.
- **Writing to device denied** – Device Monitor rule which denies writing to the device (see "Device Monitor Rule") was actuated.
- **Writing to open area denied** – Device Monitor rule which denies writing to unencrypted floppy drives and detachable devices (see "Device Monitor Rule") 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 (30000 events) and common settings have **Operation is blocked** option selected (see in "General Settings for Agents") then any operations controlled by current security policy are forbidden.
- **Data transfer via network protocols denied** – FTP Monitor, Mail Monitor or IM Client Monitor rule which denies data transfer through. FTP/FTPS/SMTP/S/MIME/POP3/Outlook/XMPP/MMP/YMSG/ Skype (see "FTP Monitor Rule", "Mail Monitor Rule", and "IM Client Monitor Rule") was actuated.
- **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 which prohibits applications to access the clipboard at the attempt to paste/copy data in the application was triggered.
- **Using clipboard is forbidden when a data protection policy is triggered** – is displayed if copying text is blocked because of applying a data protection policy.
- **Printing in applications is forbidden** – the rule 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.
- **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.
- **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. "General Settings for Agents"), then all operations controlled by the current security policy are forbidden.
- **Network connection forbidden** – Network Monitor rule which denies data transfer through any network connections except corporate network and specified permitted servers (see "Network Monitor Rule" and "Network Traffic Control") was actuated.

- **Network connection forbidden and request for 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 "Network Monitor Rule", "Network Traffic Control" and "Temporary Employee Access").
- **Request for 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 for temporary access to the device by email** – 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 which controls cloud storages agent usage (see "Cloud Storage Monitor Rule", Access Denied option) was actuated.
- **Prohibition of writing to cloud storage** – Cloud Storage Monitor rule which controls cloud storages agent usage (see "Cloud Storage Monitor Rule", Only download option) was actuated.
- **Prohibition of running application** – Application Monitor rule which controls user access to applications by means of white lists and blacklists (see "Application Monitor Rule") was actuated.
- **Prohibition of making screenshot** – ScreenShot Control Monitor rule which controls making screenshots (see "ScreenShot Control Monitor Rule") was actuated.
- **Prohibition of pasting data** - Clipboard Monitor rule which controls data paste from clipboard (see "Configuring Clipboard Monitor Rule") was actuated.

To disable notifications displaying 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**.

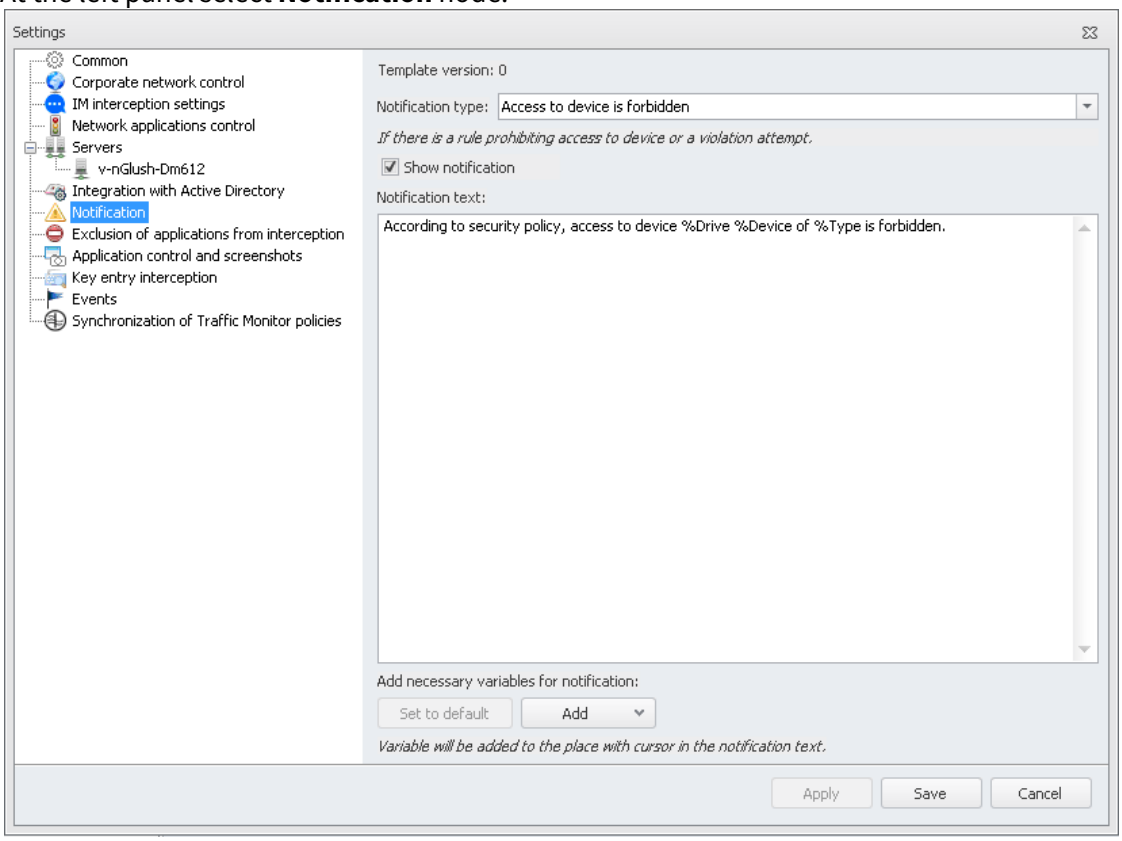
If required, you can change notification text or disable showing of any certain notification type or enable it back.

> **Warning!**
>
> If you have disabled notifications using the method described above, the notifications enabled using the method described below won't be 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**.

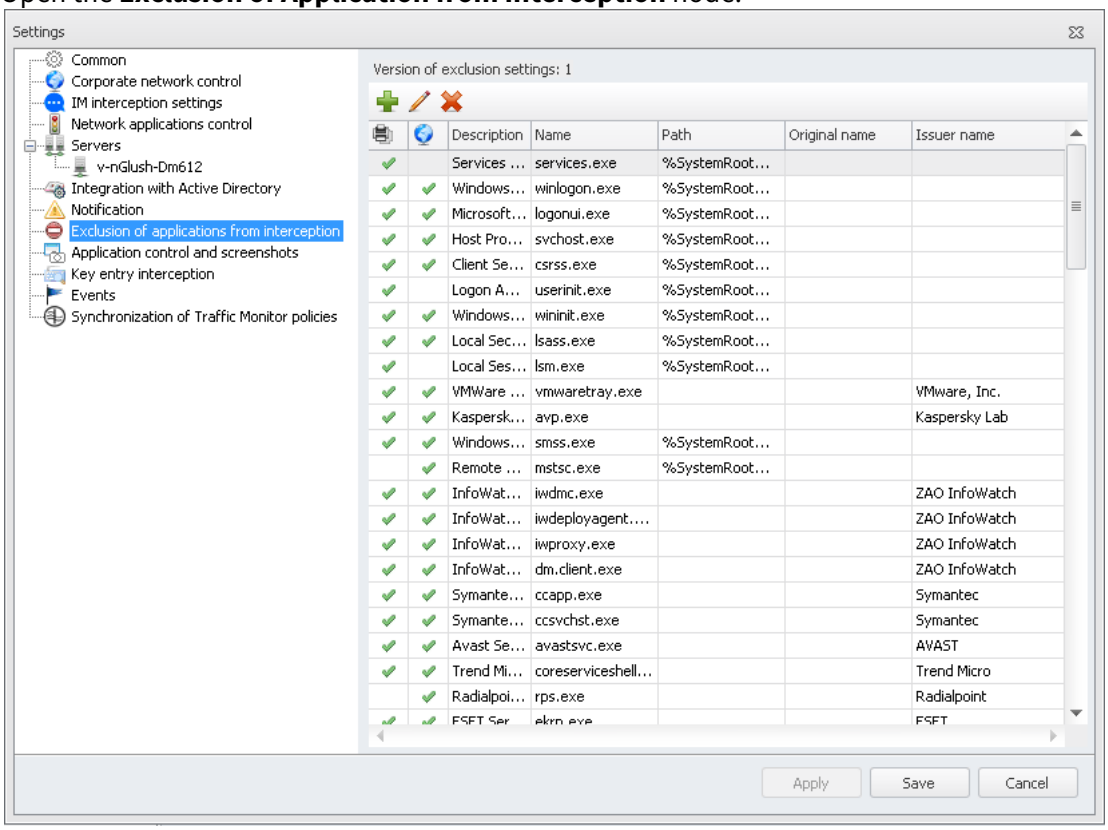
4.3.9 Exclusion of Application from Interception

You can configure parameters of applications that will be excluded from interception. These exceptional activities will become operative when Device Monitor policies are deployed over computers.

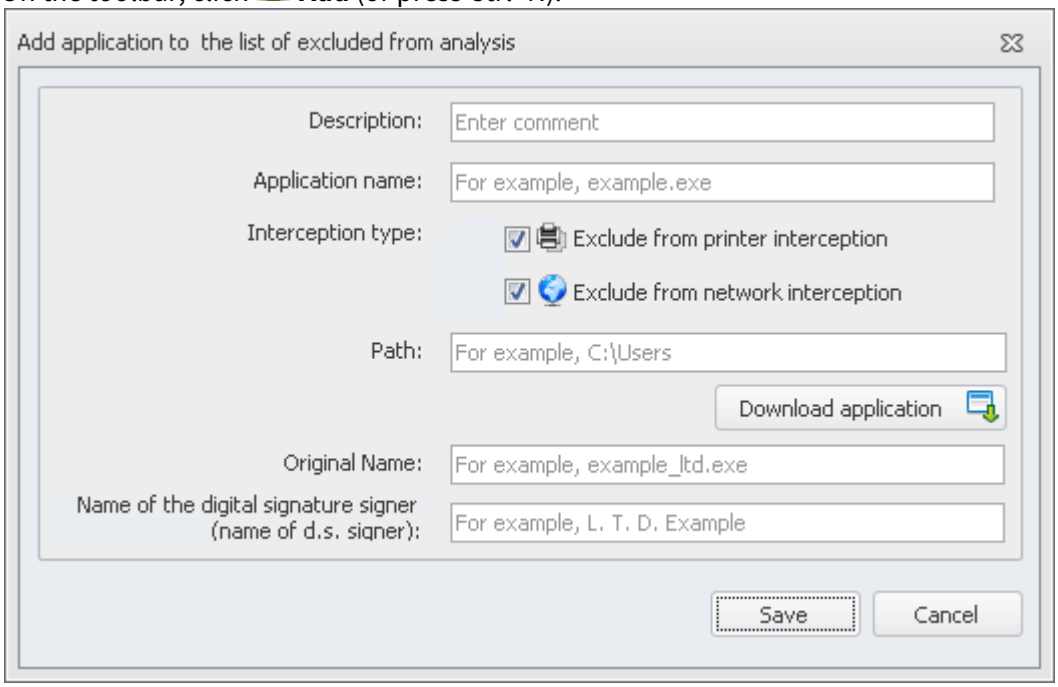
To view and configure parameters of excluding applications:

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

2. Open the **Exclusion of Application from Interception** node.



3. On the toolbar, click **Add** (or press Ctrl+N).



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 should be selected.

   > **Important!**
   >
   > Specifics of excluding **Outlook** from interception.
   >
   > When excluding Outlook from printer interception:
   >
   > - Intercepting Outlook mail (MAPI) will also be disabled. In this case, to intercept emails, configure rules for other protocols (see "Mail Monitor Rule").
   >
   > - Checking Outlook mail will also be disabled according to policies that are configured in the Traffic Monitor Management Console.

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: `%ProgramFiles%\Citrix`, then all applications in *.exe format located in the Citrix folder or any of its subfolders 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 file name** 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 the **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**. Excluding an application from interception, as well as canceling exclusion will be applied during the next run of the application. That is why you need to restart the application to apply the exclusions.

> **Note:**
>
> Applications with a built-in integrity check (e.g. SWIFT client) or the ones, containing debugger detections should be added to the printer interception exceptions list. Otherwise, they cannot be launched.

4.3.10 Application Control and screenshots

Device Monitor allows to control applications running on the managed computers via permitting or forbidding some applications. For this purpose there are two operation modes provided:

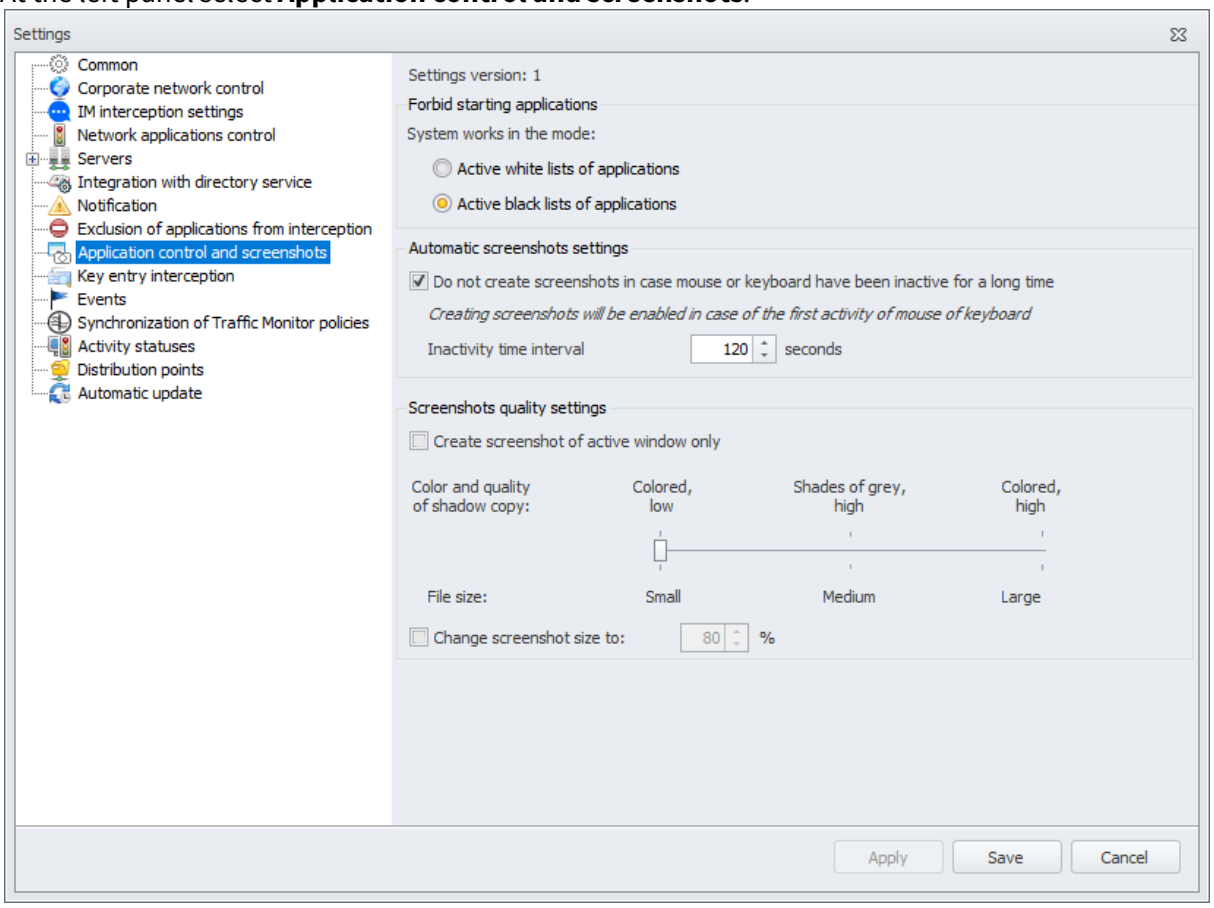
- **Active white lists of application**s - all applications from the lists selected in the Application Monitor rule from the resulting policy are allowed. Other applications are forbidden.
- **Active black lists of applications** - all applications from the lists selected in the Application Monitor rule 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 and Resultant White List for an Employee" and "Viewing Resultant Settings, Policy 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. 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 the value in **Inactivity time interval** field is reached and renewed at the first keyboard or mouse activity.
4. In **Screenshots quality settings** specify:
    - **Create screenshot of active window only**. If option is enabled, the System creates a screenshot of the active window instead of the entire screen.
    - **Colour and quality of shadow copy.** The following colour modes are available:
        - **Colored, low**. A colored file in a low resolution to be saved. Use this mode, in case you need files of small size.
        - **Shades of gray, high**. A file in greyscale mode in a high resolution to be saved.
        - **Colored, high**. A colored file in a high resolution to be saved. Use this mode, when you need high-quality images regardless of their size.
    - **Change screenshot size to**. If you need to reduce the image size while saving, select this option and specify the value (per cent, to be calcuted in accordance with initial file).
5. Change the mode if required.
6. Click **Save**.

Note:

The System receives screenshots created with the following rules (DM): **Rule for Keyboard Monitor** (creating screenshots is configured in the rule) and **Rule for ScreenShot Monitor**.

For more details on how to configure sending of screenshots to different products, see "Settings to Send Data to Products".

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

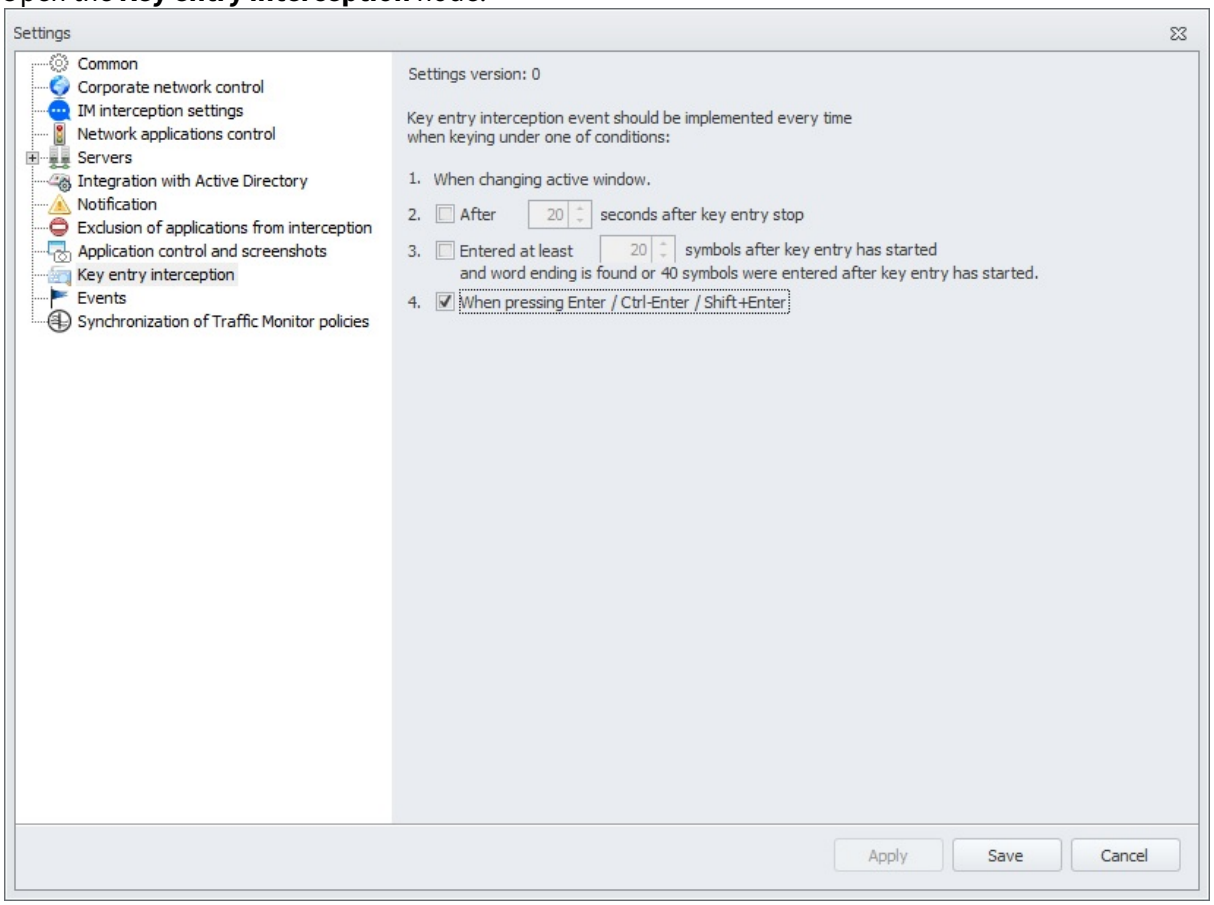
Restart controlled computers to apply a new version of applications and screenshots settings.

4.3.11 Control of Keyboard Input

On the **Key entry interception** tab, you can specify general conditions under which the rule is triggered.

For this:

1. In the main menu of the Management Console, select **Tools** > **Settings**.
2. Open the **Key entry interception** node.



3. If necessary, specify conditions, under which a new event is created:
   - the number of seconds which should pass after the user stops typing;
   - the minimum number of entered characters;
   - pressing Enter/Ctrl+Enter/Shift+Enter.

> **Note:**
>
> An event is always created when an active window changes.

4. Click **Apply**, then click **Save**.

Note:

For the keyboard input rule, the Security Officer can configure the list of resources for interception in DM Management Console. For details, see "Resources".

4.3.12 Event Storage

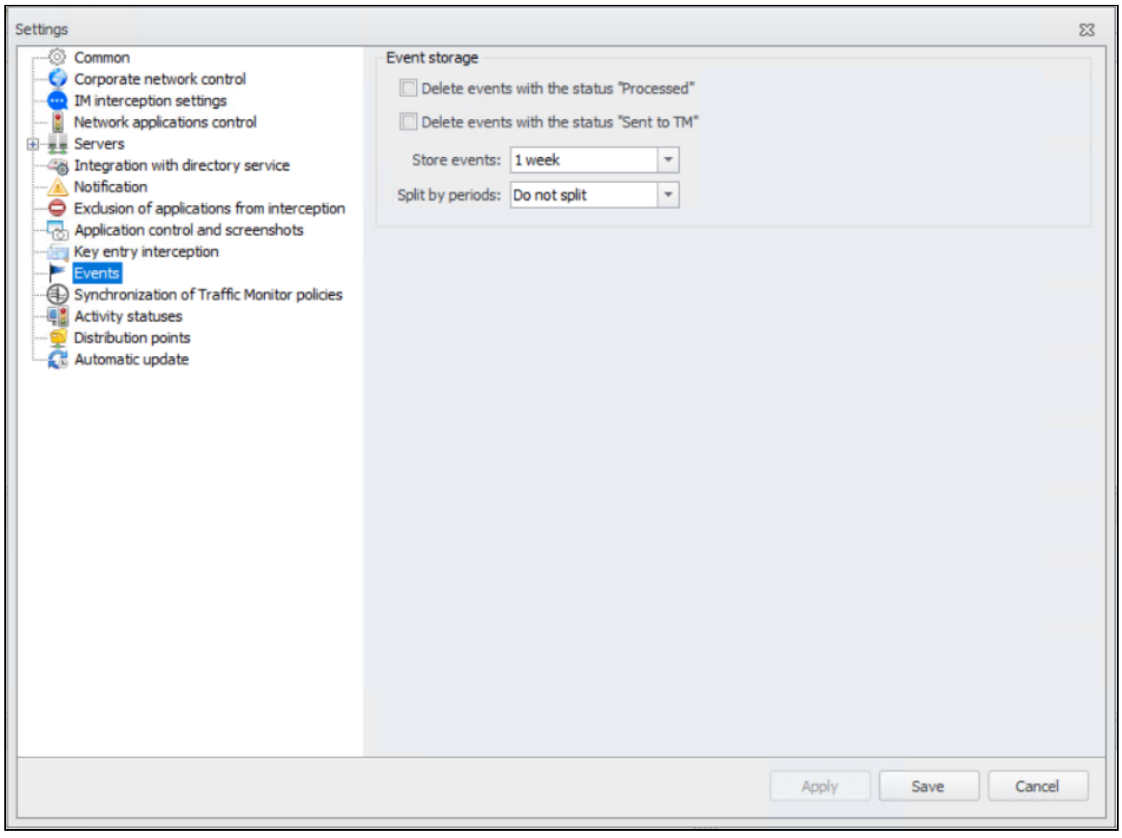
In the **Events** section, you can set parameters of automatic event storage and deletion.

To set up event storage:

1. In the Main Menu, select **Tools > Settings**.
2. Go to **Events**.
3. Select:
   - **Delete events with the status "Processed"** – to delete processed Device Monitor events or events of a standalone server. In the standalone mode, events with the **Processed** status cannot be sent to Traffic Monitor for analysis.
   - **Delete events with the status "Sent to TM"** – to delete events already sent to Traffic Monitor for analysis.

Note:

If options specifying deletion are not selected, events with **Processed** and **Sent to TM** statuses will be stored as specified in the **Store events** field.



4. From drop-down lists, select:
    - **Store events** – to set up time during which the event will be stored in the database and displayed in DM Management console. Also applies to events with **Error sending to TM** and **No license** statuses. The default value is **1 week**.
    - **Split by periods** – to split events into blocks according to their creation date to speed up connection process.

4.3.13 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.

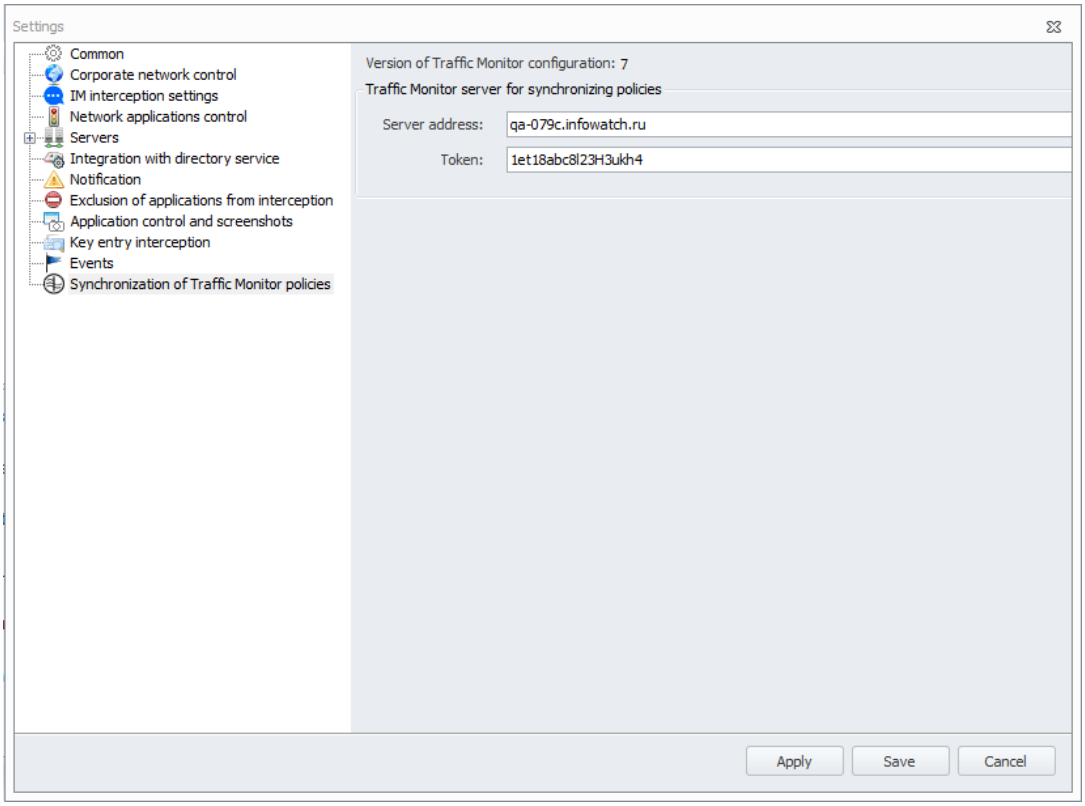
When synchronizing the policies, Device Monitor Server validates the Traffic Monitor certificate. For successful synchronization, configure the validation. See "Configuring validation of the remote server certificates".

> **Note:**
>
> The configuration version that is used in Traffic Monitor is displayed in TM console (for details, see "InfoWatch Traffic Monitor. User Guide", "Configuring the System" article). If necessary, you can compare version numbers in Traffic Monitor and Device Monitor to make sure that Device Monitor uses an actual version.

> **Note:**
>
> Configuration recived from Traffic Monitor is deployed to Device monitor agents running RED OS, Alt OS, Astra Linux OS 1.7 or Windows family operating systems.

To synchronize policies in TM:

1. From the Console main menu, choose **Tools** > **Settings**.
2. Open **Synchronization of Traffic Monitor Policies** node.
3. Enter the server address (host), on which you are going to work in the Management Console, and a token (see "Device Monitor Server Settings. Connecting to Traffic Monitor Server"). Make sure that you establish a connection with the Traffic Monitor server of the same version (see the Knowledge Base article "Compatibility among the versions of TM, DM and Agents").



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

4.3.14 InfoWatch Device Monitor Server Manager

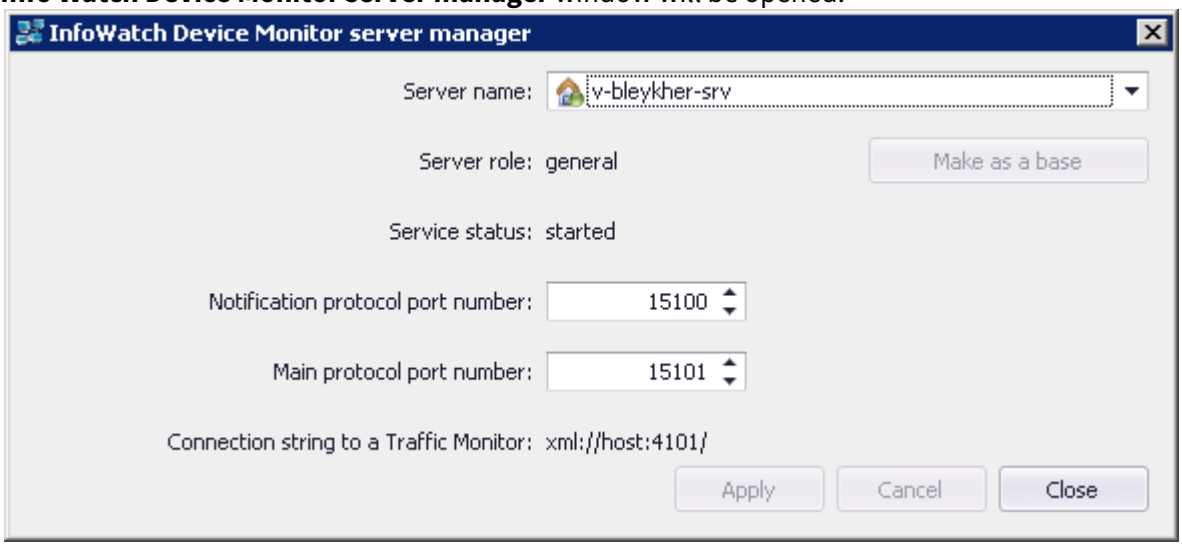
InfoWatch Device Monitor Server Manager is being used to define roles and change server settings.

> **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
> - server names must be successfully resolved through the customer's DNS service to the IP address (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.

> **Important!**
>
> If a base server is changed, go to administration console to enter again all passwords for tasks and synchronizations with Active Directory.

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**.

4.3.15 Setting Activity Status of Agents

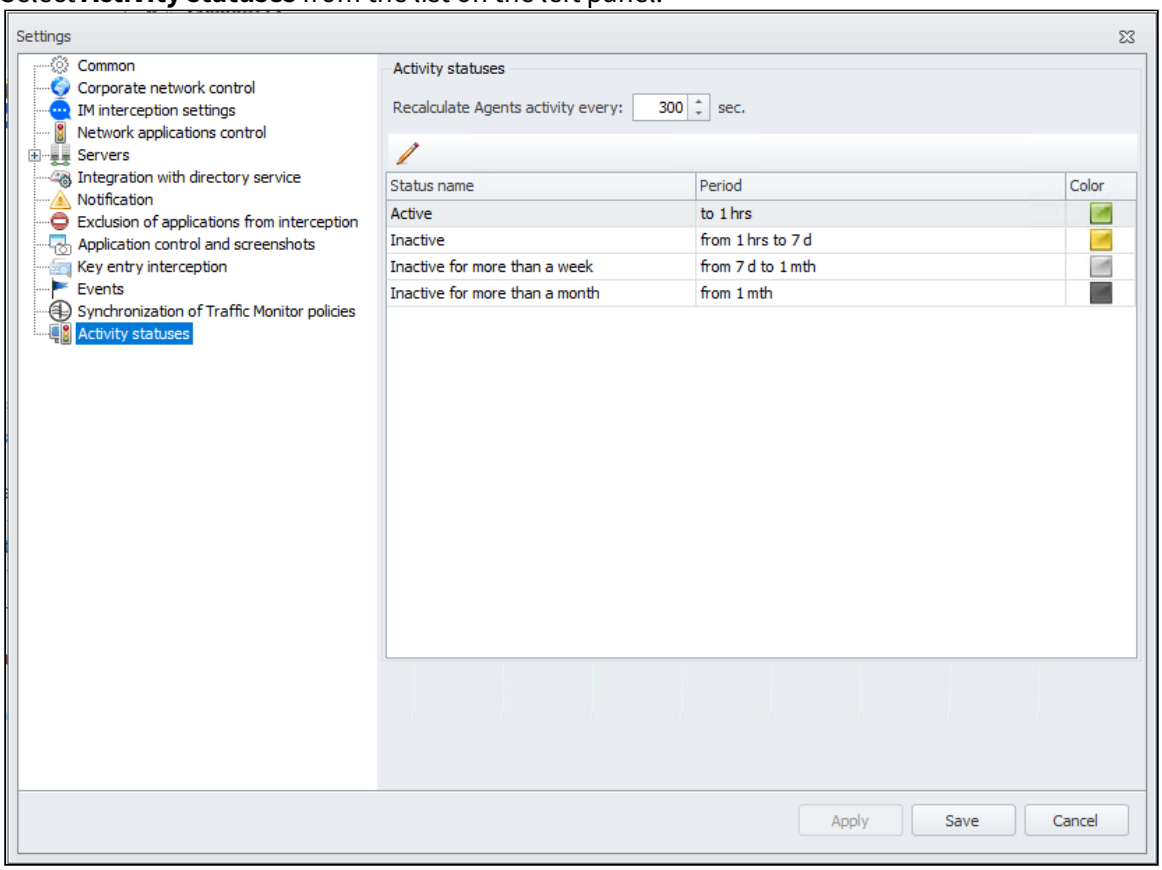
User can configure Agents activity statuses. To do this, define the following parameters:

- the period (seconds) to recalculate Agents activity;
- the name of status;
- the period since Agent last addressed to server.

To configure the parameters, complete the following steps:

1. In the main menu of DM Management console select **Tools** > **Settings**.

2. Select **Activity statuses** from the list on the left panel.



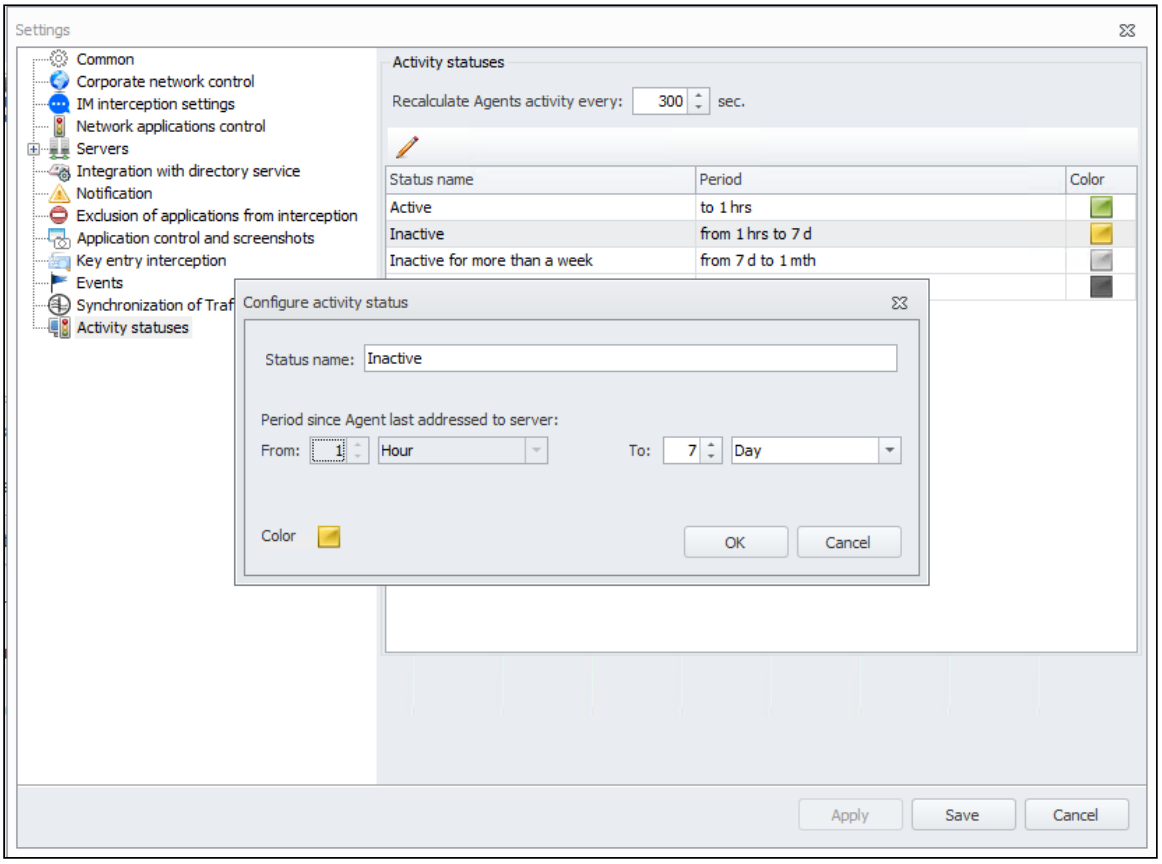
3. Using the button  define the period (seconds) to recalculate the Agents activity.

> **Warning!**
>
> We do not recommend to define the period since Agent last accessed to server **less**, than the one after which the Agent sends notification that Agent works to the server (default value – 600 seconds, see General Settings for Agents). Otherwise, the statuses of activity will be calculated and displayed wrongly in DM management console, as the value last access to server will be updated less frequently than the statuses of activity, which calculation depends directly on the last access to server.

4. Double click the status row and configure the status in the opened dialog window:
   a. Select the status name;
   b. Define the time period since the last addressing to server. The System will keep this status as current during this period.

> **Note:**
>
> If the status of Agent on a computer is **Not specified** then the status of Agent activity will be **Inactive**, and it will be calculated as configured in settings.

5. The color of each status is configured by default and cannot be changed.
6. To apply the changes, press **OK**. To cancel, press **Cancel**.



Note:

Statuses in DM Management console can be updated:

- automatically according to parameters configured in **Activity statuses** settings;
- manually, using Ctrl+F5.

When updated, the current statuses of activity are displayed in DM Management console. This means that the latest information from the DB is displayed in the console (the information is not collected from Agent, as no connection with Agent is being established at the moment).

4.3.16 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)
- If stopped agent is updated, it will be started after the update
- In case agent is hidden, it cannot be stopped locally

Important!

To avoid network failure, before you stop DM agent, please make sure that antivirus self-protect function is disabled on computers with antivirus software installed.

Restart computer after stopping/starting the agent.

Important!

It is highly recommended to use DM Management console to change the status of Agent from/to **Operates in diagnostic mode** and **Stopped** correctly.

Stopping agent remotely/starting agent

You can stop remote DM agent using 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).

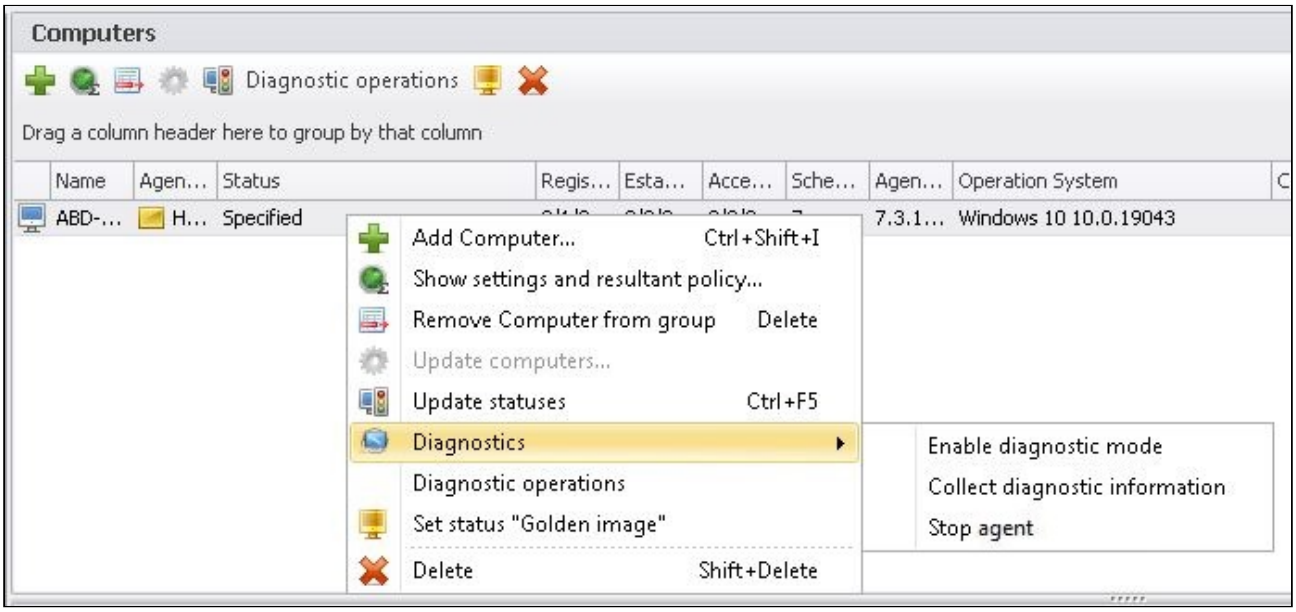
When choosing **Stop agent**, its operation will be suspended, agent status will change to **Stopped** and activity status will change to **Inactive**.

Note:

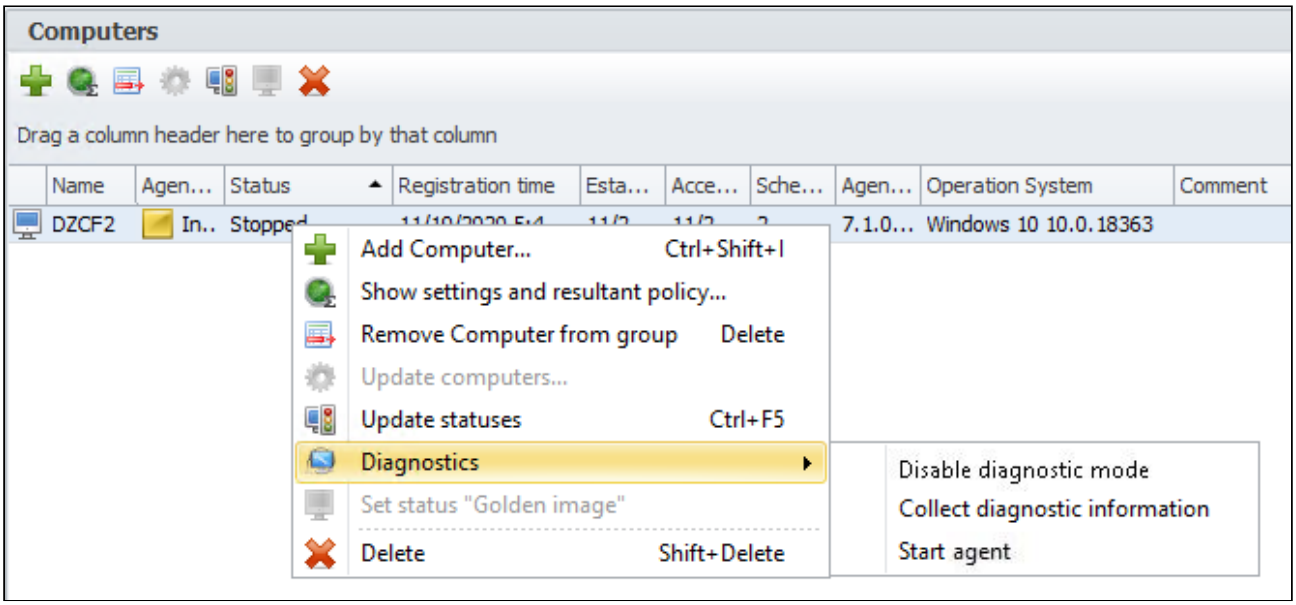
Stopped agent is available for update or deletion, but stopping is unavailable during update/deletion.
In case there is no connection with the agent, stop/start are unavailable.

After the Agent has been stopped:

- events are not intercepted
- actions are forbidden
- notifications and DM icon on the toolbar are not displayed



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



When selecting the option **Start agent**, its work will be resumed and the workstation status will go back to **Specified**.

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".

4.3.17 Configuring Agents distribution

To get quickly Agent's distribution kit to workstations you should use Distribution service. After the service is installed the directories containing distribution kits are created. These directories are registerd in the System and are the distribution points with InfoWatch protocol. The more distribution points the System has, the faster Agents distribution or update will be performed. The distribution points can be:

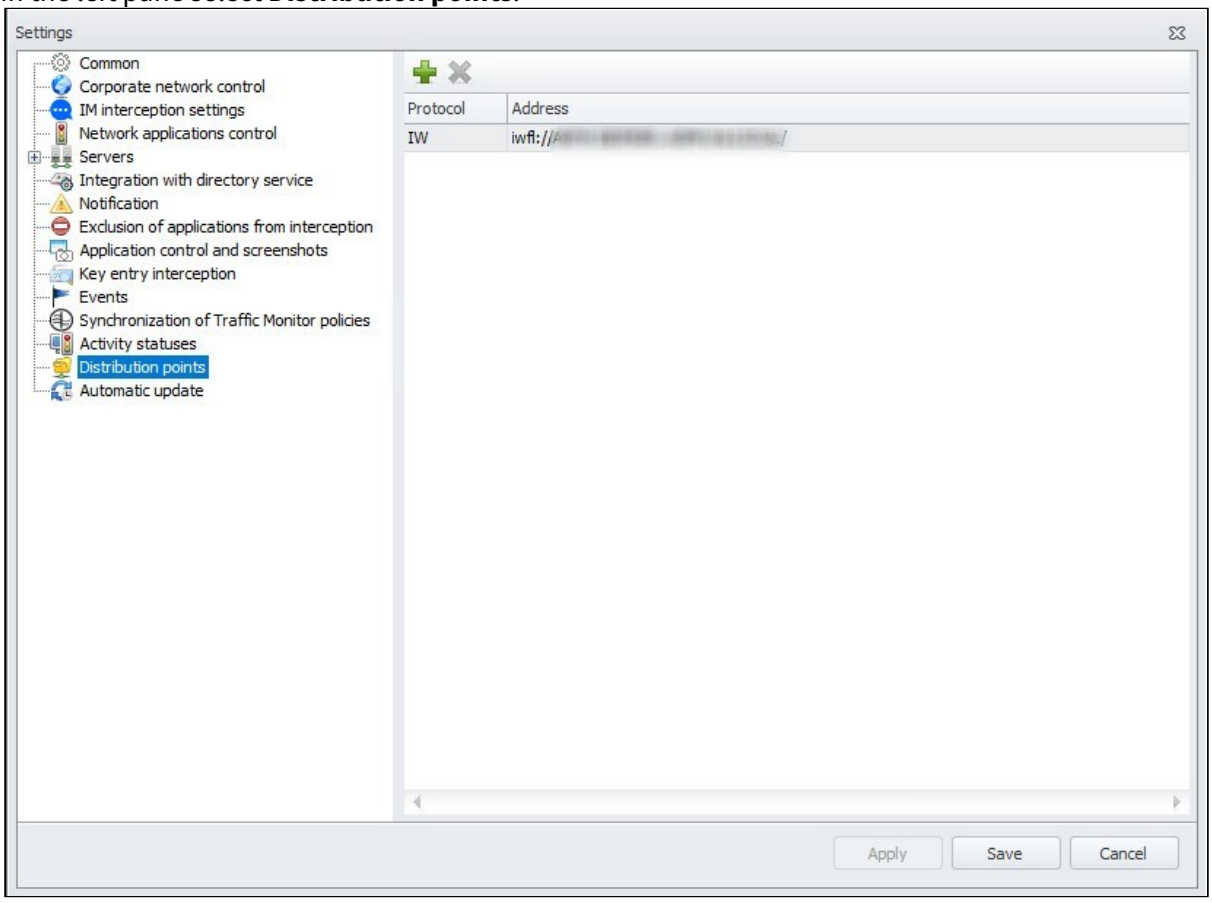
- FTP or SMB folder, where you can manually download the distribution kits.

> **Warning!**
>
> To use an SMB shared folder as a distribution point, configure the folder for anonymous access (to configure anonymous access in MS Windows family systems, see Windows Security Options).

- Any workstation, where Distribution service is installed. In this case the distribution point is created by default.

To add a new ditribution point:

1. Select in the main menu the command **Tools** -> **Settings**.
2. In the left pane select **Distribution points**.



3. Click  and select parameters as follows:
   - Protocol (to choose):
   - Windows network resources (SMB);
   - File Transfer protocol (FTP);
   - InfoWatch protocol (recommended to use).
     Note: InfoWatch protocol is displayed only for the records which were automatically added, e.g. on the workstations, where the Distribution service is installed.
   - Server, where the access to distribution folder is granted to;
   - Port (for FTP protocol use the default port number).
4. Click **Check connection** and make sure the distribution point is available.
5. Click **OK** and then **Save**. While saving, the System checks if the distribution point is available.

So, the list of distribution points is to be established. Then this list is sent to Agent together with task for installation or update. If you run the task on the Agent and then delete the distribution point, the new information will not be received by Agent. In this case Agent will receive the distribution from one of active distribution points.

All distribution points should have the structure of folders to publish the distributives:

- Version of Device Monitor (for example, "7.4.0")
  - OS 1 (supported: "Windows", "AstraLinuxSE-1.6", "AstraLinuxCE-2.12", "AstraLinux-1.7", "RedOS-7.3")
    - Platform (x86 or x64)
      - Agent distributive for the OS and platform

Warning!

Distribution point cannot be deleted in case it is related to any task.

Distribution points with InfoWatch protocol cannot be deleted. They will be removed automatically when removing a distribution service on the workstation.

4.3.18 Automatic Update of Agents

To configure Agents automatic update in accordance with server working version:

1. Go to menu **Tools** > **Settings** > **Servers**.
2. Specify required version in the field **Working version to install and update Agents automatically**.
3. Go to **Tools** section > **Settings** > **Automatic update**.
4. Enable automatic update and specify the period to check if update is required:
   - Each hour or each few hours;
   - Every day;
   - Every week on the following days: Monday, etc.

   Note:

   The first check every *n* hours (if configured) will be performed at the first start of the System, or at the moment of settings change when the setting was enabled, and then every *n* hours.

   Daily and weekly check is performed at 13:00 (the value is specified in the database).

5. Specify automatic update parameters:
   a. Specify the number of attempts to load the update.
   b. On **Removing computers** tab specify the workstations to be excluded from update, selecting them from catalogue or searching by name.
   c. On **Parameters of installation** tab specify:
      i. When the update is to be installed if available: *Right after the packages are downloaded*, *Every day*, *Every week on the following days*;
      ii. The most suitable time of the day to update;
      iii. If forced installation of the update is required after a number of attempts.
   d. On **Parameters of reboot** tab specify:
      i. How long to wait for reboot without notifying the employee: *Do not wait*, *Wait for n hours*, *Wait infinitely*;

ii. Notify the employee about the reboot necessity and wait for reboot.

> **Warning!**
>
> For the System to block removable devices correctly after Agent update on Linux family OS, reboot the workstation.
>
> Notification will not be displayed if **Hide Agents presence** is enabled on the computer.

6. Click **OK** and then click **Save**.

After saving the configuration, automatic update is started. In accordance with parameters specified (**Parameters of automatic update** tab), in menu **Results of automatic update** you can see the list of workstations with one of the following statuses:

- *Update is resolved* – Agent's distribution kit of required version is downloaded, update is required in accordance with configuration schedule;
- *Distribution kit download* – Agent's distribution kit is being downloaded from closest distribution point;
- *Update pending* – waiting for update in accordance with update installation schedule;
- *Product update* – it is time to install the update in accordance with schedule or an immediate update installation after download;
- *Update is complete* – successfully completed update;
- *Update complete with failures* – successful update cannot be performed, log contains errors;
- *Repeated update is resolved* – to start update after errors are corrected;
- *Reboot pending* – query to reboot the workstation manually or after the time is over according to update parameters.

User can:

- Filter workstations by the date of their creation in the list. To do this, create a filter by pressing on **Navigation** panel and specify the filter's parameters;
- Limit the total number of given records;
- View update parameters and go to **Settings** to apply them;
- View errors if they occur;
- Restart update if it failed.

4.3.19 Setting Interception of Audio

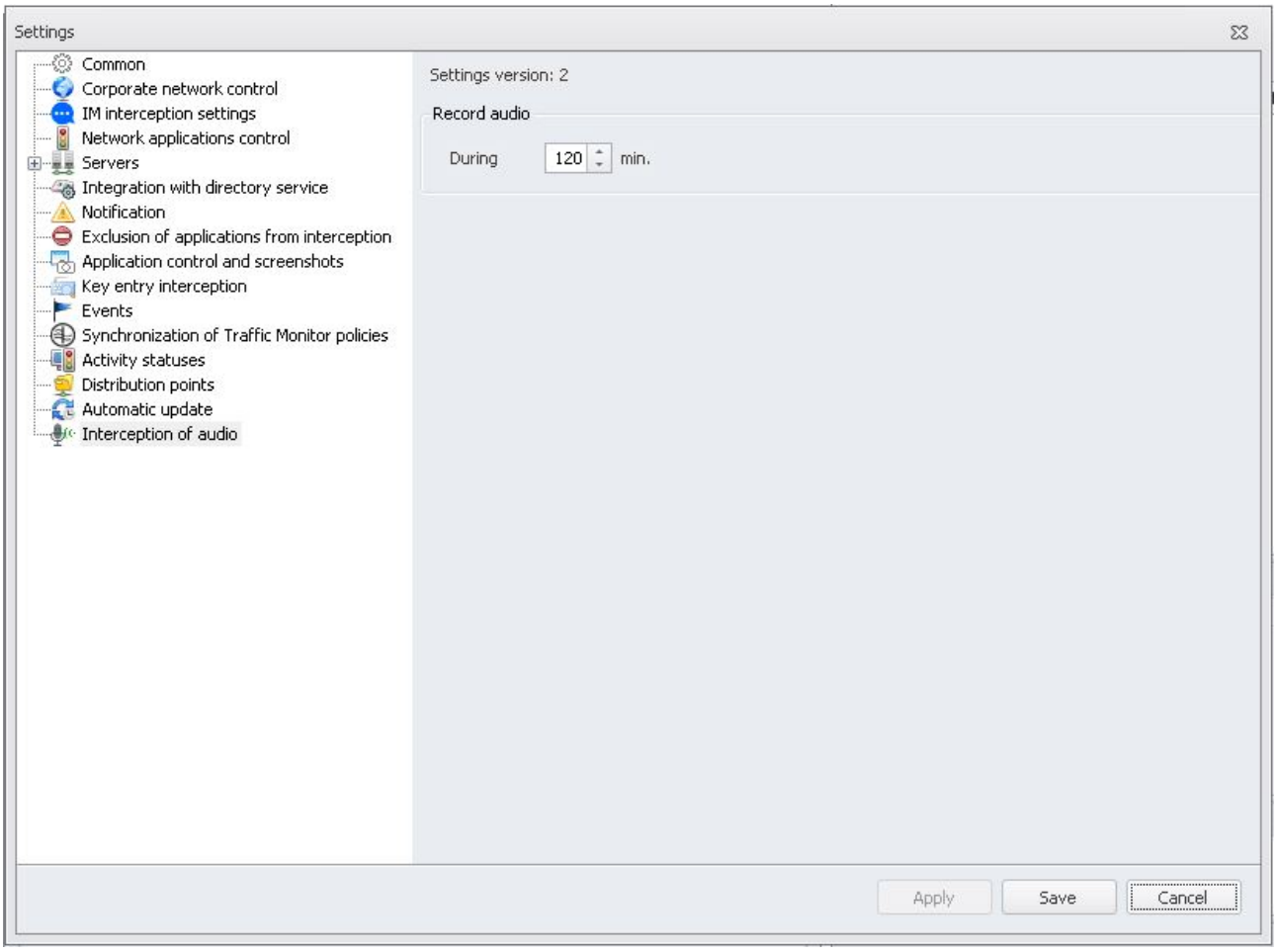
> **Warning!**
>
> The functionality is only for InfoWatch Activity Monitor.

Interception of audio is recording the sound around the employee's workstation when the rule "Audio Record Control" is triggered.

You can configure the setting for interception of audio. To do this:

1. Go to menu **Tools** > **Settings**.
2. On the left panel select **Interception of audio**.

3. Using the button , define the period from 1 to 120 minutes. During this time the System will record the sound around user's workstation. When the time ends, the recording will stop.
4. Click **Apply**, then click **Save**.



Важно!

On the Windows taskbar on the computer where Agent is running, the microphone icon will be hidden in the following cases:

- *Audio record control rule* is triggered;
- online recording of audio is started manually.

If before the recording the microphone was running (as some application was using it) and the microphone icon was displayed, then when the recording starts the System will hide the icon. Applied on Agents operating on OS Windows 10.

Note:

DM continuously records the sound around the user's workstation during the period specified in settings. When employee starts using the resource added to the **Audio record control** rule, DM activates audio recording. When the period specified in the settings is up, DM stops recording. If the user visites a number of resources specified in the rule, then when the they switches between these resources, DM continues recording.

Example 1

The rule specifies the resources for audio recording: https://example.ru/, https://example.com. The period for recording is 5 minutes. A user starts using the website https://example.ru/. DM activates audio recording and creates an event.

In 3 minutes after the recording started, the user leaves the resource and goes to the other resource https://example.com. This resource is also specified in the rule. DM continues recording, the 5 minutes period starts over.

When the 5 minutes period ends DM stops recording. As a result, Activity Monitor will have 2 events (one for each resource) containing 3 and 5 minutes audio records.

Example 2

The rule specifies the resources for audio recording: https://example.ru/, https://example.com. The period for recording is 5 minutes. A user starts using the website specified in the rule. The the person goes to some other website, which is not specified in the rule. After that they go back to the controlled resource.

The user goes to https://example.ru/. DM activates audio recording and creates an event. In 3 minutes after the recording started, the user leaves the resource and goes to the other resource https://example1.ru (not controlled by the rule) and uses the website for 4 minutes. DM continues recording.

Note: If whithin the period specified for recording (5 minutes in this example), the user leaves the controlled resource and starts using the resource that is not specified in the rule, then DM stops recording after 5 minute period ends.

Then the user comes back to the resource https://example.ru/. DM activates audio recording and creates an event. When the 5 minutes period ends DM stops recording. As a result, Activity Monitor will have 2 events containing 5 and 5 minutes audio records.

Example 3

The rule specifies the resources for audio recording: https://example.ru/, https://example.com. The period for recording is 5 minutes. A user starts using the website specified in the rule. The the person goes to some other website, which is not specified in the rule. After that they go back to the controlled resource.

The user goes to https://example.ru/. DM activates audio recording and creates an event. In 3 minutes after the recording started, the user leaves the resource and goes to the other resource https://example1.ru (not controlled by the rule) and uses the website for 1 minute. DM continues recording.

Then the user comes back to the resource https://example.ru/. DM continues audio recording and creates an event. When the 5 minutes period ends DM stops recording. As a result, Activity Monitor will have 2 events (one for each resource) containing 4 and 5 minutes audio records.

When the 5 minutes period ends DM stops recording. As a result, Activity Monitor will have 2 events containing 4 and 5 minutes audio records.

4.3.20 Settings to Send Data to Products

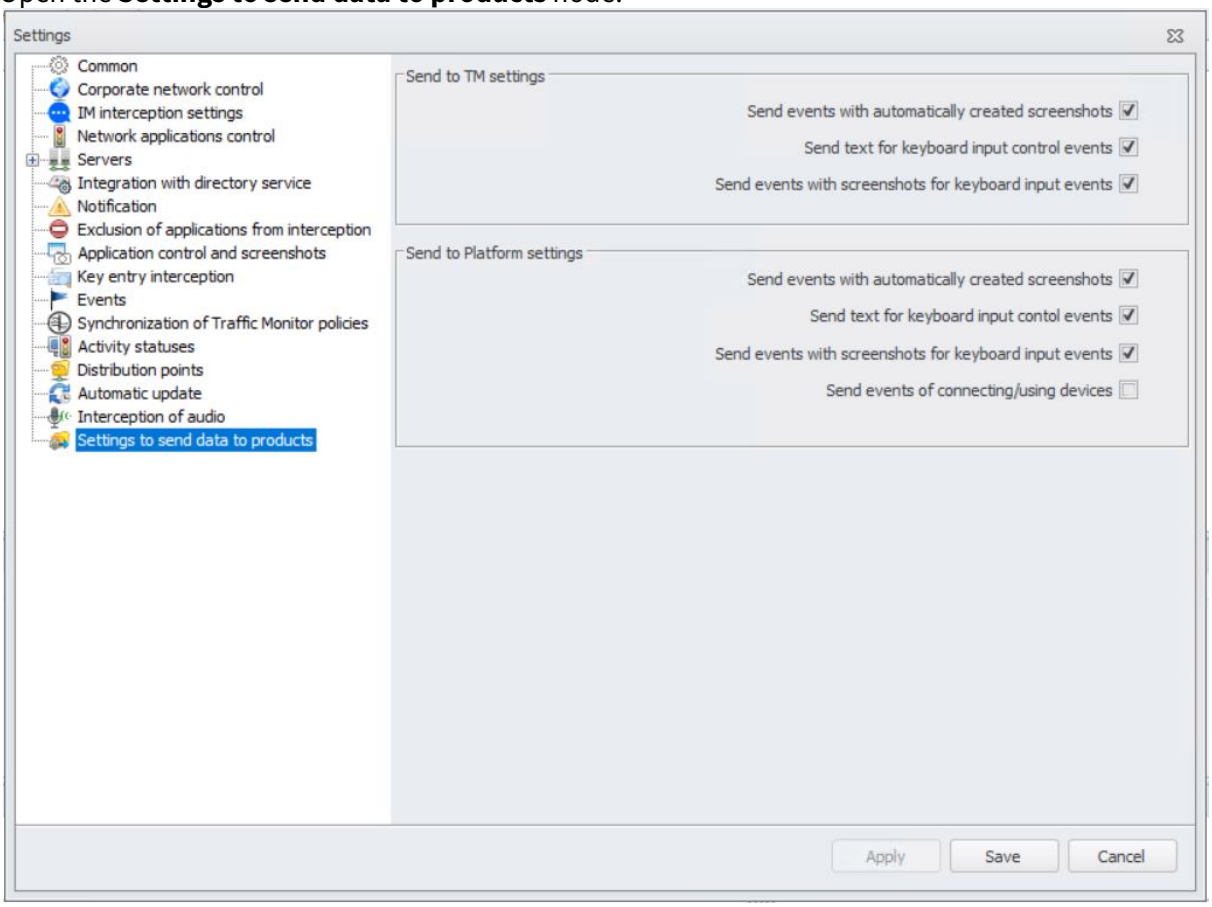
Processing screenshots is set up in the ScreenShot Monitor Rule and the Keyboard Monitor Rule.

Control of connecting and using devices is set up in the Device Monitor Rule.

Additionally, you can set up sending data to InfoWatch products. On the **Settings** tab, you can specify to which products you want to send data.

For this:

1. In the main menu of the Management Console, select **Tools** > **Settings**.
2. Open the **Settings to send data to products** node.



3. In the **Send to TM settings**, deselect the required option if you do not want to:
   - **Send events with automatically created screenshots** (monitoring events is configured in the ScreenShot Monitor Rule);
   - **Send text for keyboard input control events** (monitoring events is configured in the Keyboard Monitor Rule);
   - **Send events with screenshots for keyboard input events** (monitoring events is configured in the Keyboard Monitor Rule).
4. In the **Send to Platform settings**, deselect the required option if you do not want to:
   - **Send events with automatically created screenshots** (monitoring events is configured in the ScreenShot Monitor Rule);
   - **Send text for keyboard input control events** (monitoring events is configured in the Keyboard Monitor Rule);
   - **Send events with screenshots for keyboard input events** (monitoring events is configured in the Keyboard Monitor Rule).
5. In the **Send to Platform settings**, select the option if you want to:
   - **Send events of connecting/using devices** (monitoring events is configured in the Device Monitor Rule).

By default, sending of screenshots is configured for Traffic Monitor and the Platform. Events of connecting/using devices are not to be sent to the Platform by default.

Important!

For screenshots to be displayed in Activity Monitor, you should set up the Statistics rule.

Example

1. The *Keyboard Monitor rule* has been configured on a workstation and the **Take screenshot when creating an event** option has been enabled.
2. The following settings are specified:
   - **Send to TM settings** – not send screenshots for keyboard control input events;
   - **Send to Platform settings** – send screenshots for keyboard control input events.
3. When the rule is triggered:
   - screenshots are not sent to Traffic Monitor;
   - screenshots are sent to the Platform.

Important!

For events of connecting/using devices to be displayed in Activity Monitor:

- In General Settings for Agents, set the "**Log events of device and cloud storage interceptors**" parameter to the "**All**" or "**In case access denied**" value
- Set up the Device Monitor Rule

You can also add display of the **Send whitelists of devices** setting. By default, this setting is not displayed. To display the setting:

1. Open the **InfoWatch.DeviceMonitor.Gui.exe.config** configuration file of the Device Monitor Management Console.
2. Set the `ShowSendWhiteListToEpSettings` parameter to `True` (by default, the parameter is set to `False`).

Important!

Export and import of these settings are not supported.

When you update Device Monitor, settings specified in the DM Management Console configuration file are not saved.

4.4 Managing Security Scheme

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

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

4.4.1 Security Scheme Organization

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

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

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

Security scheme does not contain other entities of the System.

You can edit the security scheme multiple times. An updated security scheme is then saved as a new version of the existing scheme. Old security schemes are stored in the database. In DM Management Console, you may see policies and rules of any security scheme version.

This topic also contains:

- Security Policies and Rules
- Employees and Employee Groups
- Computers and Computer Groups
- Uploading Security Scheme to Managed Computers

Security Policies and Rules

A security policy is a set of rules that allow you to monitor transferring data to removable devices and network resources, sending documents to print, control network activity, and define access level to controlled peripherals.

When you assign a security policy to a group of employees or computers, please, mind the following:

- Each employee group and each computer group should have an assigned security policy.
  You can't add a new group without assigning a security policy to it. The security policy is selected from available policies. Therefore, you should create a security policy before adding a group;
- You can't assign more than one security policy to a group;
- The same security policy can be assigned to several groups. However, we recommend that you should assign an individual security policy to each group.

> **Note:**
>
> You can't remove a security policy from the security scheme if it is assigned to at least one group of employees or computers.

Accounts that are newly registered with Device Monitor are automatically added to "default" employee group. So, for a new employee, the System initially defines the access level by the security policy that is assigned to "default" group of employees and the security policy that is assigned to the computer group to which the employee's computer belongs. You can change the access level later by adding the employee to a different group.

> **Warning!**
>
> In case of multi-user type of access to a workstation and when it is impossible to define the process (event) initiator, the System does not take into consideration interception rules for employees. Only the interception rule for this specific workstation will be effective. In this case you should set up interception rules for the workstation with multi-user access, not only for employees.

Rules are restrictions and conditions according to which the System monitors data transfer to removable devices, network activity, sending documents to print and controls access to peripherals. A new set of rules is created for each security policy.

Each rule has a validity period during which the rule applies.

InfoWatch Device Monitor includes the following rule types:

- **Application Monitor Rule** allows you to control access to applications by means of black and white lists. You can also prohibit employees from:
  - Starting applications;
  - Using clipboard;
  - Printing.
- **Audio Record Control Rule** allows you to monitor actions of employees by controlling sounds around the empoyee's workstation.
- **Clipboard Monitor Rule** allows you to control pasting data from the clipboard. You can prohibit employees from pasting data to specified applications or to all applications of a terminal session.
- **Cloud Storage Monitor Rule** allows you to control web clients of a cloud storage.
- **Device Monitor Rule** allows you to control access of employees to selected peripherals.
- **File Monitor Rule** allows you to monitor the following actions with files on removable and network resources:
  - Copying files from network devices to a workstation;
  - Copying files to network resources using UNC (e.g., *Server**SharedFolder**Folder**File*);
  - Copying a file from a removable device to a workstation;
  - Creating a file directly on a removable device;
  - Copying/moving a file to a removable device from a controlled computer, another removable device, or a network resource;
  - Editing files directly on a removable device, including file renaming;
  - Copying files to media devices connected via MTP;
  - Copying files to a terminal session application;
  - Copying files from a terminal session to a workstation;
  - Copying files to resources connected via a terminal session. Redirection for network folders and virtual devices is supported.
- **File Operations Monitor Rule** allows you to control if applications read data from a file or write to a file. With this rule, you can also create a file shadow copy and a screenshot.
- **FTP Monitor Rule** allows you to control data exchange through the FTP/FTPS protocols. You can restrict or completely forbid using the protocol and create shadow copies of transferred files.
- **HTTP(S) Monitor Rule** allows you to control data exchange through the HTTP and HTTPS protocols. The System allows you to create shadow copies of transferred files.

- **IM Client Monitor Rule** allows you to control employee access to instant messengers: Skype, Telegram, XMPP, MMP, Facebook, WhatsApp, VK (VKontakte). The rule can block access to an application or just make copies of transferred files, messages, and chats. For Skype, voice messages can be recorded. It is also possible to create shadow copies of transferred files and messages.
- **Keyboard Monitor Rule** allows you to intercept text that is entered from the keyboard on workstations. Events are created:
    - When a user switches active windows or tabs in the browser;
    - When the time interval specified in settings expires. The interval is counted from the moment a user stops typing;
    - When the number of characters entered reaches the limit of characters specified in settings;
    - When a user presses Enter / Ctrl+Enter / Shift+Enter, if the corresponding setting is configured (see "Control of Keyboard Input").
- **Mail Monitor Rule** allows you to control incoming and outgoing mail. You can forbid/permit using email or permit only receiving emails. The System can also create shadow copies of transferred files.
- **Network Monitor Rule** allows you to forbid data transferring through any network connections except for the connection with the corporate network or with specified servers. You can determine the network segments that are considered the corporate network and create a list of allowed external addresses.
- **Print Monitor Rule** allows you to monitor sending documents to local and network printers. It is also possible to create shadow copies of print jobs.
- **ScreenShot Monitor Rule** allows you to automatically create screenshots on controlled computers.
- **ScreenShot Control Monitor Rule** allows you to control screenshots on Agent side.
- **Statistics Rule** allows you to collect statistics on employee activity and operations on controlled computers:
    - Entering/exiting a session (local, remote);
    - Locking/unlocking a session (local, remote);
    - Starting/stopping an application;
    - Getting/losing focus of an application active window;
    - Getting focus by a browser tab in Chrome, Yandex.Browser, Mozilla Firefox, Edge (Chromium), Opera, or IExplore;
    - Entering web search queries in Google or Yandex;
    - Using a mouse and a keyboard.

Note:

In case there are several rules configured for an employee or a computer, the System applies a resultant policy that consists of all rules configured for the employee or computer. For details on rule priority, see "Applying Rules".

Warning!

We do not recommend adding a default action to a data protection policy on Agent when there is a rule for the *Any sender – Any receiver* route. If there is a configured rule with the allowing verdict in the policy and a default rule with the blocking verdict and both of them are equal, the default action is to be applied.

Warning!

To enable correct interception of Google services (Gmail, Google Drive, etc.), we recommend disabling the experimental QUIC protocol in Google Chrome. For details, see the "Disabling QUIC protocol in Google Chrome" article in the knowledge base.

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" subsection.

Employees and Employee Groups

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

1. Each employee must belong to at least one employee group (the *default* group) as the security policy can not apply to individual employees.
   The *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 the "*Default*" group if the account is added to at least one employee group besides the Default group.
2. When the System is installed, the *Shadow copy policy* is assigned to the *default* employee group. The *Shadow copy policy* contains the 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**, **Telegram control**, **Facebook control**, **WhatsApp 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 an encrypted channel. Shadow copy is created, if the request size, transferred via an 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 an encrypted channel, when its size is not bigger than 40 MB.

Computers and Computer Groups

A computer registered in Device Monitor must belong to at least one computer group (the "default" group) as the security policy can not apply to an individual computer.

Note:

Last time logged in user is displayed in the field **User** in the section **Computers**.

User is not displayed for workstations running Linux.

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 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.

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 the security scheme to managed computers automatically in the following cases:

- When you save a new or edited security scheme;
- If you register an employee but do not identify their access level for current security scheme version. In this case, the employee is automatically added to "default" employee group, and the security scheme is updated.

If the managed computer is disconnected from the network where InfoWatch Device Monitor is deployed, policies 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 been connected to InfoWatch Device Monitor server, it automatically updates policies and sends shadow copies to the server.

4.4.2 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 Scheme Organization".

For information on the security scheme configuration, see "Security Scheme Setup".

Viewing Active Security Scheme

By default, the Management Console 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 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

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

To view information about a security scheme section:

1. Open the required section (see "Management Console 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.

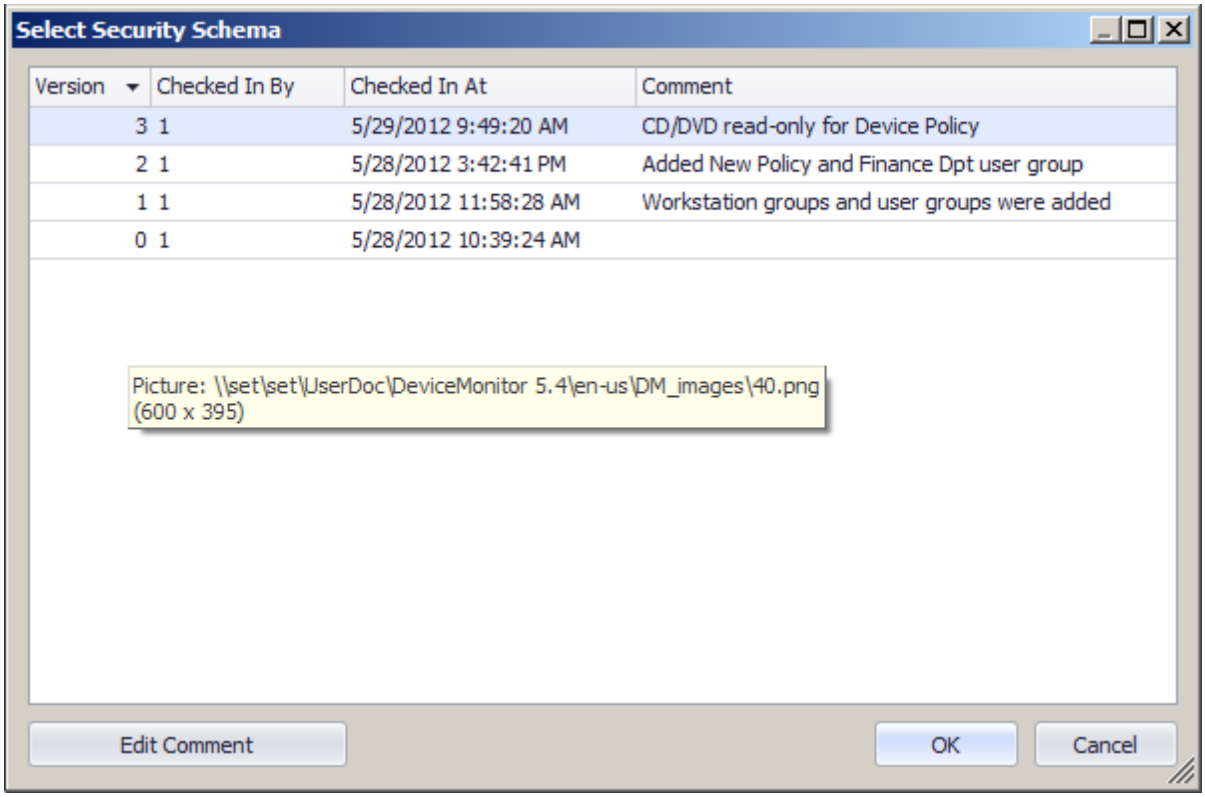
> **Note:**
>
> You can customize the main screen appearance (see "Main screen customization").

Viewing Old Security Scheme

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

To view older security scheme:

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



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 Scheme Comments"). Information on current Management Console security scheme (version number and comment) is displayed on the status bar.

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

Policies of the selected security scheme version and their rules will be loaded into Management Console. When working with an old version, the "*Old security scheme*" status is displayed.

To return to preview and active security scheme, open **Security Scheme** > **View Latest Security scheme** in Main Menu.

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.

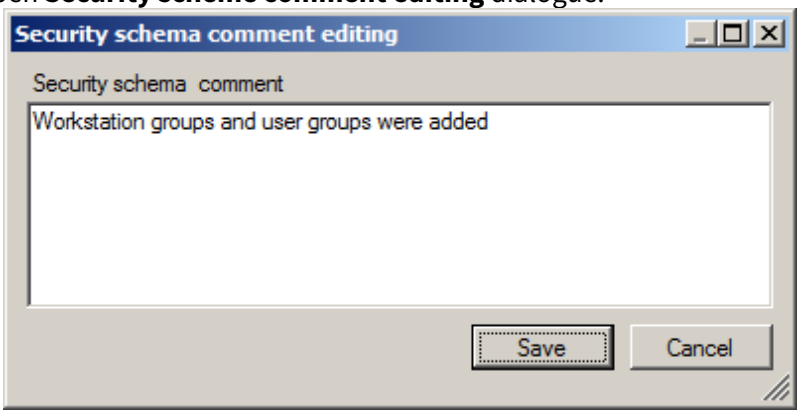
You can view comments for all security scheme versions in **Select Security Scheme** dialogue (see "Viewing Old Security Schemes").

> **Note:**
>
> You can add comments to security scheme 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 Scheme** > **Edit Current Security Scheme Comment**.
   - (*For any security scheme version except the current one*). In Main Menu, select **Security scheme** > **View Old Security Scheme**. This opens **Select Security Scheme** dialogue. In this dialogue, select the row containing the right security scheme version. Then click **Edit Comment**.

   These actions open **Security scheme comment editing** dialogue.



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

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

3. Click **Save**.

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 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, 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 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, workstations, employee accounts, device white lists, signature categories) while security scheme is being edited by another user:

1. Management Console displays warning message.
2. When another user saves or cancels changes, Windows system tray displays a notification: "***Security scheme 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 scheme 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 to 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 scheme, in Main Menu click **Security Scheme** > **Unlock**. All unsaved changes will be lost.

Updating Security Scheme

The system can be simultaneously operated by multiple users. To keep security scheme details in Management Console 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.

Exporting/Importing Security Scheme

You might need to save the existing settings of a security scheme. You might want to do this if you need to configure the 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, lists of resources) (see "Managing Security Scheme")
- **Applicaiton protocol** (see "Application Protocol")
- **Network control settings** (see "Corporate Network Control")
- **Servers excluded from analysis** (see "Network Traffic Control")

- **Applications excluded from interception** (see "Exclusion of Application from Interception")
- **Distribution points** (see "Configuring Agents distribution")
- **Automatic update configuration** (see "Automatic Update of Agents")
- **User and roles** (see "Managing Console Accounts")

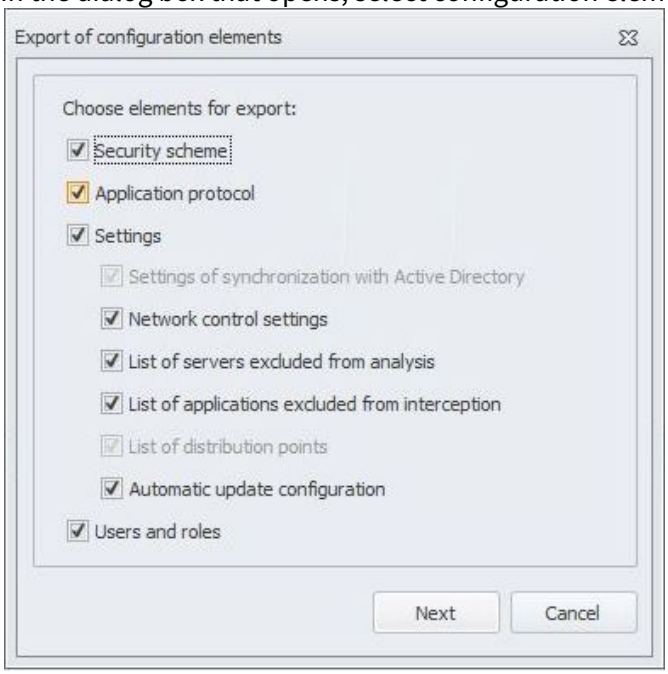
Important!

To Device Monitor version 7.2 you can import a configuration file of the same version only.

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**.

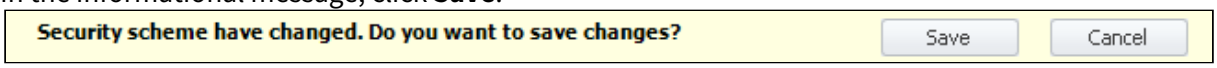
Important!

For a correct connection between roles and groups, the security scheme should be exported as well.

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

> **Note:**
>
> The status of Agent "Golden image" will remain irrespective of the computer security scheme after exporting /importing the configuration from/to the security scheme. For details about "Golden image" status, see Setting "Golden image" status on Agent.
>
> Computers with other statuses will have **Not specified** status of Agent after importing them to another security scheme.
>
> Computers that remain in the same security scheme will keep their statuses of Agents.

4.4.3 Security Scheme Setup

After System installation, you must configure your security scheme in the following order:

1. Configure "default" employee group and "default" workstation group.
2. Configure the rest of security settings.

Security scheme configuration principles:

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

Adding workstations to security scheme

There are two ways to add a managed workstation:

- Add a new workstation automatically during registration
- Add workstation manually via Management Console

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

Adding employee accounts to security scheme

You can add new account information manually or automatically. You can register a new employee while editing the security scheme. However, if an unknown employee who is not listed in the security scheme is registered on a workstation, the employee's account will automatically be added to the security scheme ("default" employee group).

Adding white lists to security scheme

Before you create a white list, add device models and instances to the device database. Then you should create a white list for a specific employee/employee group/workstation/workstation group and specify devices included in the list. These employees/workstations have access to whitelisted device models and instances regardless of assigned policies. When a white list record expires, access rights are distributed according to assigned policies.

For details on setting configuration parameters of the security scheme, see the following subsections:

- Security Policies
- Rules
- Employees
- Computers
- White Lists
- Signatures
- Application Protocol
- Application Blockade
- Resources
- File Statistics
- Junk Traffic Exceptions
- Temporary Employee Access to Network
- Temporary Employee Access to Devices

Security Policies

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

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

> **Note:**
>
> For recomendations on configuring the security policy, see "Security Policies and Rules".

Each security policy is a set of rules which allow you to monitor operations related to data transfer to removable devices, sending documents to print and network activity as well as to define access level to controlled peripherals.

Security policies are assigned to **employee groups** and **computer groups**. The security policy assigned to the employee group applies to all employees included in this group. The security policy assigned to a group of computers applies to all employees who work at managed computers included in this group.

Security policies 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, see:

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

Viewing Security Policies

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

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

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

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

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

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 name in the main screen workspace. This opens a table containing rule information on **Details** panel.

General information:

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

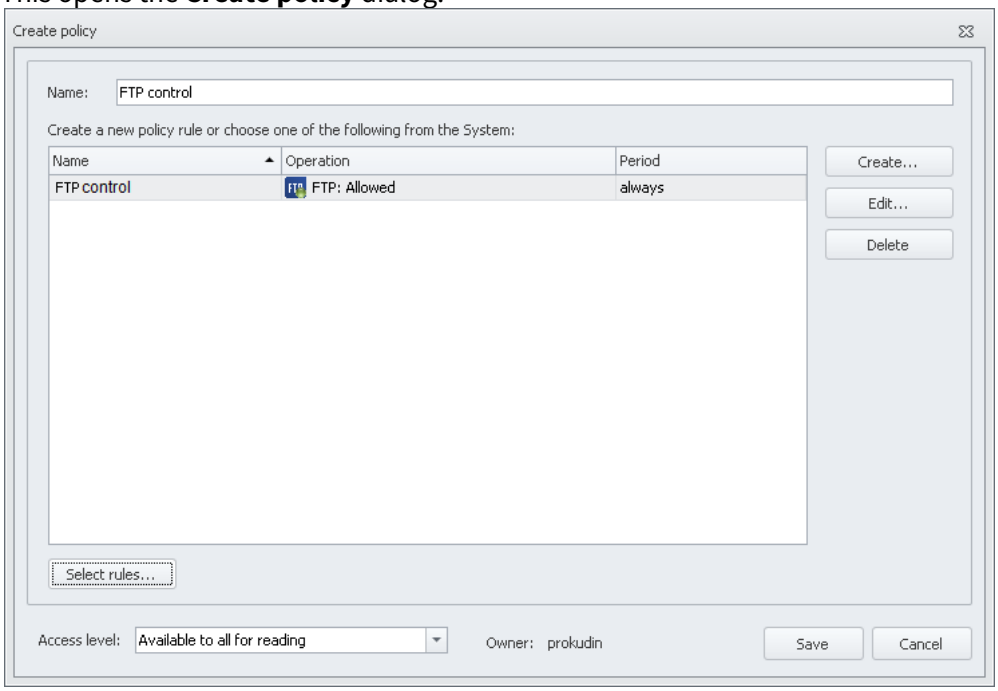
> **Note:**
>
> Information for some attributes is duplicated on the main screen.

Adding and Configuring New Security Policy

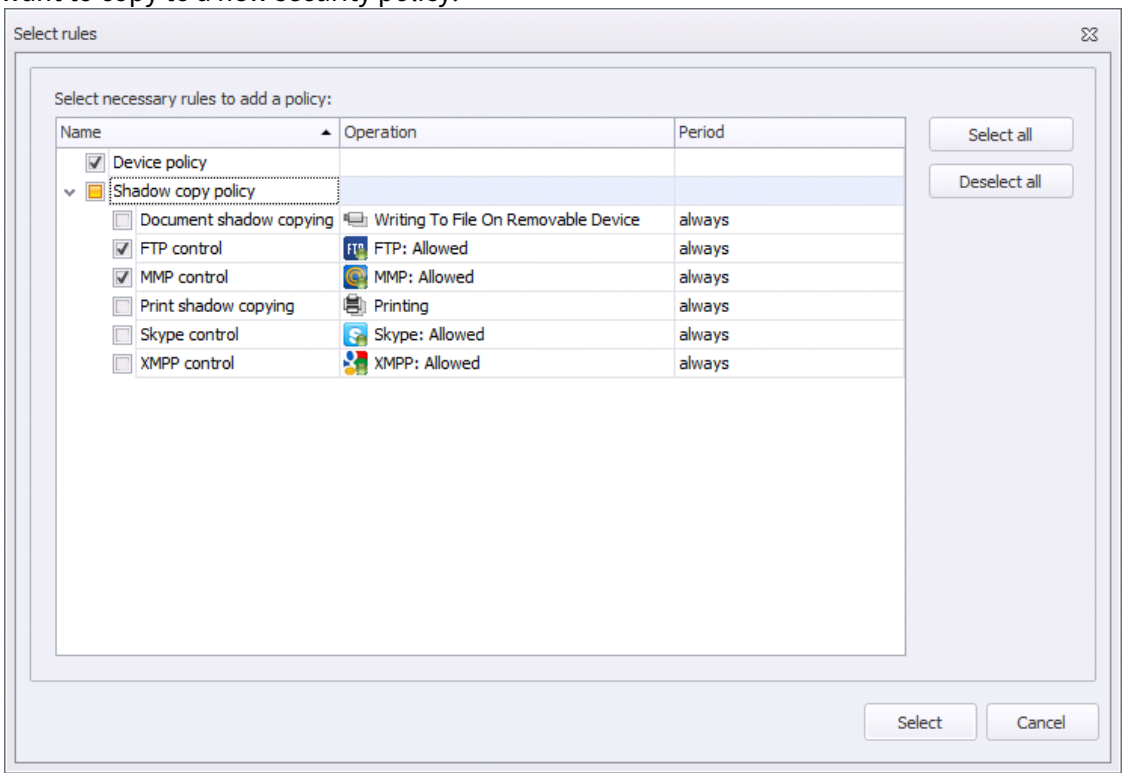
To create and configure a security policy:

1. Go to **Policies**.
2. Take one of the following actions:
    - Click **Create Policy** at the top of the Navigation panel
    - In the Main Menu, select **Edit** > **Create Policy**

- Use the **Ctrl+N** shortcut on the keyboard
  This opens the **Create policy** dialog.



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



   You can also select the whole policy. In this case, all the rules the policy contains will be added to a new security policy.
   After you flag all the rules, click **Select**.

- To create a new rule, click **Create** and specify the rule parameters as described:
  - Application Monitor Rule
  - Audio Record Control Rule
  - Configuring Clipboard Monitor Rule
  - Cloud Storage Monitor Rule
  - Device Monitor Rule
  - File Monitor Rule
  - File Operations Monitor Rule
  - FTP Monitor Rule
  - HTTP(S) Monitor Rule
  - IM Client Monitor Rule
  - Keyboard Monitor Rule
  - Mail Monitor Rule
  - Network Monitor Rule
  - Print Monitor Rule
  - ScreenShot Control Monitor Rule
  - ScreenShot Monitor Rule
  - Statistics Rule

  You can also edit or delete a policy rule by selecting it and clicking **Edit** or **Delete** respectively.
5. In the **Access level** drop-down list, specify permissions for reading and editing the policy.
6. After you define all the rules to be included in the policy, click **Save**.

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

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

Edit Security Policy

To edit security policy:

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

Warning!

A policy appointed to at least one employee group or workstation group cannot be deleted. To delete security policy, make sure that this policy is not appointed 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 panel, select security policy name.
3. Take one of the following steps:
   - In Main Menu select **Edit** > **Delete Policy**;
   - Click **Delete Policy** at the top of Navigation panel;
   - Use **Ctrl+D** shortcut.
4. In the following confirmation dialogue select **Yes** to confirm that you want to remove security policy.

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.

Rules

You can work with rules within the security policy in which they are created. Each security policy has an individual set of rules.

You can find information on rules in the following subsections:

- Adding Rule;
- Applying Rules;
- Configuring Device Monitor Rules to Collect Statistics and Intercept Events.

Adding Rule

To add a rule to a security policy:

1. Go to the **Policies** section.
2. In the **Policy** area of Navigation pane, select a security policy to which you want to add the rule.
3. Do either of the following:
   - in the main menu, click **Edit** > **Create Rule**;
   - click **Create Rule** at the top of the **Policies** area;
   - right-click in the **Policies** area and select **Create Rule** from the drop-down list;

- press **Ctrl+Shift+N**.

4. In the dialog box that opens, choose the rule type and specify other setting of the rule. Available rule types:
   - Application Monitor Rule
   - Audio Record Control Rule
   - Clipboard Monitor Rule
   - Cloud Storage Monitor Rule
   - Device Monitor Rule
   - File Monitor Rule
   - File Operations Monitor Rule
   - FTP Monitor Rule
   - HTTP(S) Monitor Rule
   - IM Client Monitor Rule
   - Keyboard Monitor Rule
   - Mail Monitor Rule
   - Network Monitor Rule
   - Print Monitor Rule
   - ScreenShot Control Monitor Rule
   - ScreenShot Monitor Rule
   - Statistics Rule
5. Once you have set all necessary parameters, click **Save**.

To edit the rule:

1. In the list of the policy rules, select the rule you want to edit.
2. Do either of the following:
   - in the main menu, click **Edit** > **Edit Rule**;
   - double-click the selected rule;
   - right-click the selected rule and select **Edit rule** from the drop-down menu;
   - click  **Edit rule** in the upper part of the **Policies** area;
   - press **Ctrl+Shift+E**.
3. In the dialog box that opens, edit the necessary parameters, then click **Save**.

To delete the rule:

1. In the list of the policy rules, select the rule you want to delete.

   > **Note:**
   >
   > To select multiple rules, use Shift or Ctrl keys. To select all rules, press Ctrl+A.

2. Do either of the following:
   - in the main menu, click **Edit** > **Delete Rule**;
   - click  **Delete rule** in the upper part of the **Policies** area;
   - right-click the selected rule and select **Edit rule** from the drop-down menu;
   - press **Delete**.
3. In the confirmation window, click **Yes**.

To copy the rule:

1. In the list of the policy rules, select the rule you want to copy. If you want to copy more than one rule, select all required lines.

2. Click the selected rule and holding the left mouse button drag the rule to the **Policies** area in the Navigation pane. Hover the mouse over the security policy to which you want to add the rule. When you see a yellow arrow to the left of the policy name, release the mouse.
   The rule will be copied to the selected policy.

You can also copy rules when editing the security policy. For this:

1. Start editing the selected policy.
2. Click **Select rules**. In the drop-down list, select rules, you want to copy to the policy. You can select the whole policy - in this case, all rules of the selected policy will be added to the policy being edited.
3. When you select all required rules, click **Select**.
4. Click **Save**.

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

Application Monitor Rule

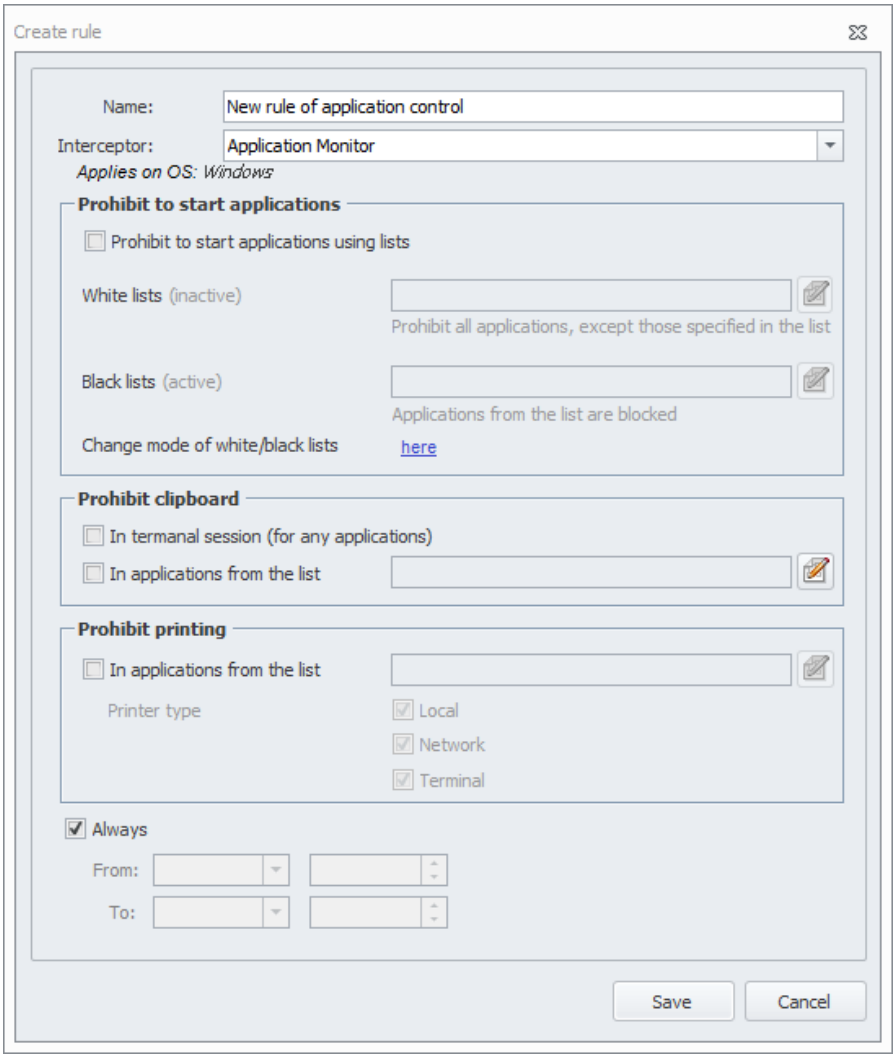
An employee can perform actions which can lead to the leakage of confidential information through third-party applications installed on a workstation and not controlled by InfoWatch Device Monitor.

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

- starting applications;
- using clipboard;
- printing.

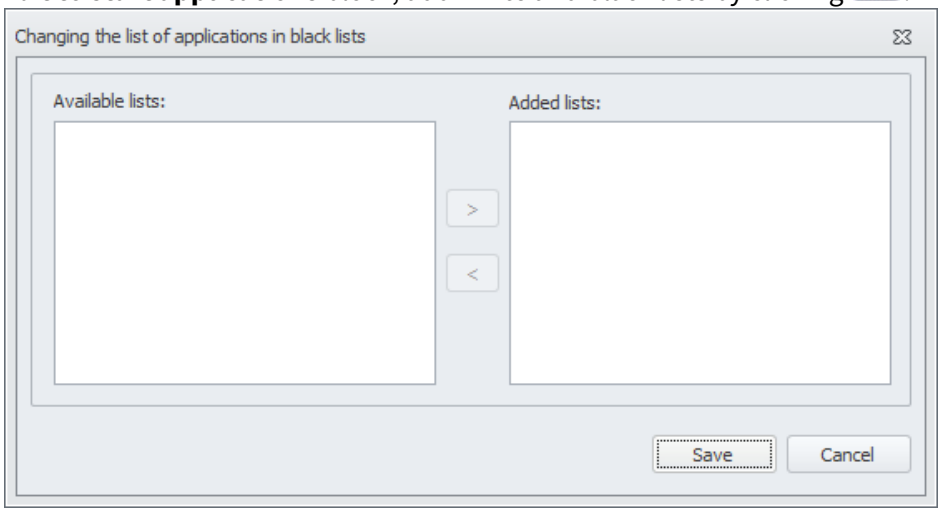
These prohibitions can be activated both separately and together.

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



To configure the rule:

1. Open the **Create rule** window (see "Adding Rule") and in the **Name** field, specify the rule name.
2. In the **Interceptor** field, select **Application Monitor**.
3. In the **Prohibit to start applications** block, add white and black 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".

4. In the window that opens, choose necessary types of available lists and move them to **Added lists** area by pressing >.
5. Click **Save**.
6. In the **Prohibit clipboard** block, select check boxes next to the application groups for which data copying should be prohibited. Possible choices:
   - **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.

7. In the **Prohibit printing** block, specify applications for which printing should be prohibited and choose 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.

8. Define a period when the rule applies. By default, the rule 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.
9. When all parameters are configured, click **Save**.

Audio Record Control Rule

> **Warning!**
>
> The functionality is for InfoWatch Activity Monitor only.

The **Audio record control** interceptor allows you to monitor actions of employees via possibility to control sound around the empoyee's workstation.

In the rule you can configure:

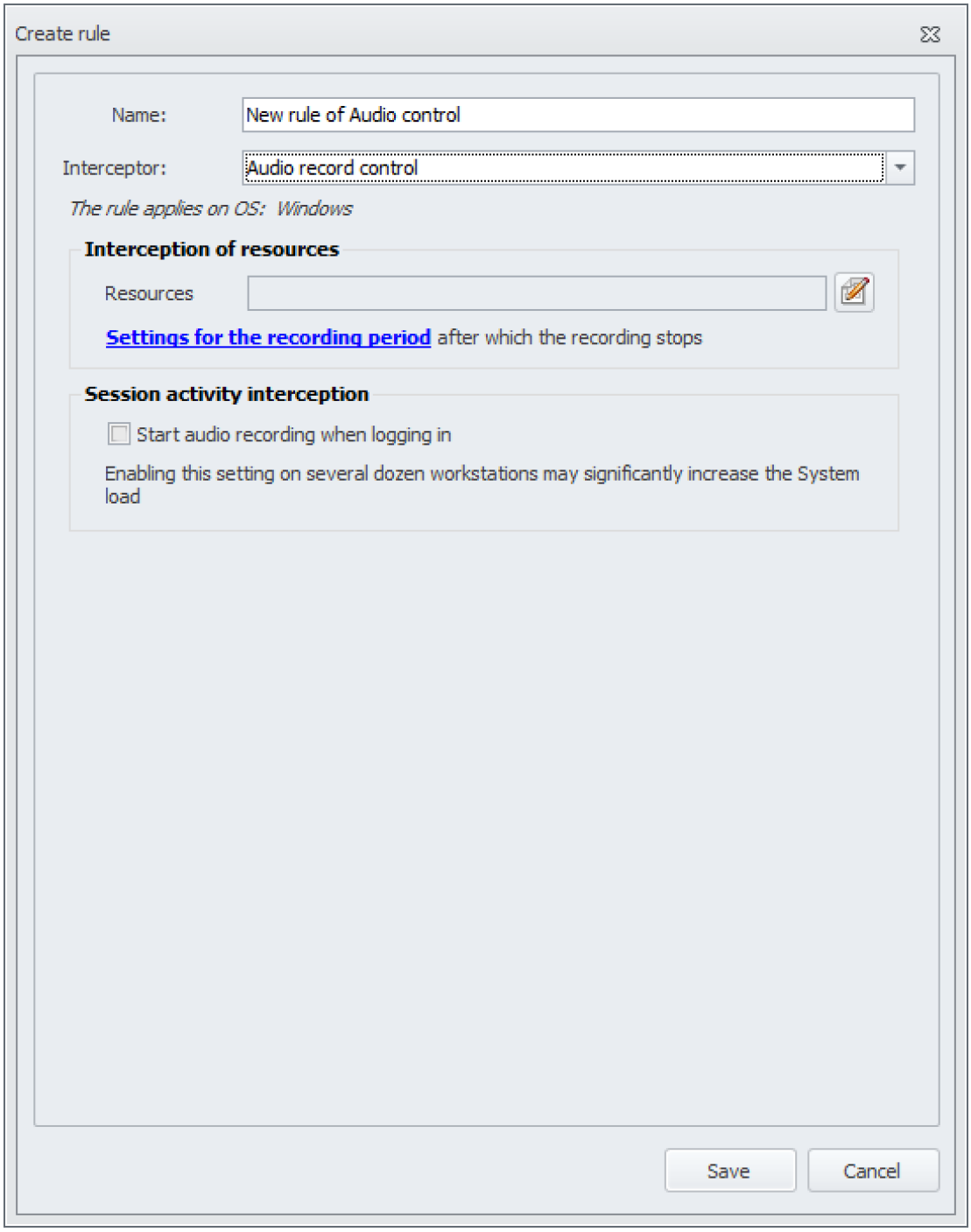
- **Resources interception** – audio recording when using the specified resources
- **Session activity interception** – audio recording throughout the entire period of work session, from user login to logout. When locking the workstation, recording is not interrupted.

Warning!

Resources interception applies starting from Device Monitor version 7.8.0.
Session activity interception applies starting from Device Monitor version 7.12.0.
Herewith the interception works if the version of Agent is not earlier than the version of Device Monitor server.

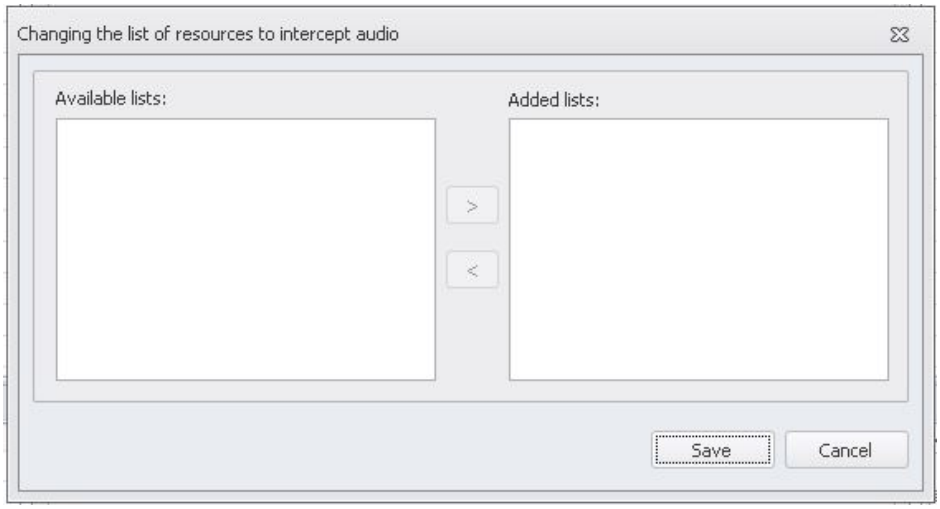
Note:

The rule applies on computers with Windows OS.



To configure the rule:

1. Open the **Create rule** window (see "Adding Rule") and in the **Name** field, specify the rule name.
2. In the **Interceptor** field, select **Audio record control**.
3. If you want to add resources for interception:
    a. Click .



b. In the window that opens, select from the **Available lists** the lists you need (when using these resources, audio recording is to start) and move them to the **Added lists** area by clicking > .
c. Click **Save**.
d. Click **Settings for the recording period** to specify the period throughout which you need the System to record audio. For details, see "Setting Interception of Audio".

4. If you want to enable session activity interception:
   a. Select the option **Start audio recording when logging in**.
   b. In the warning window that opens, click **Yes**.

> **Warning!**
>
> Regular session activity interception on several dozen workstations may cause the excessive growth of number of events and significantly increase the load on the network and on Device Monitor and Activity Monitor servers.

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

> **Warning!**
>
> The System verifies if the resource being visited by a user matches the one in the list of resources only if one of the browsers is used:
>
> - Chrome
> - Yandex.Browser
> - Mozilla Firefox
> - Edge (Chromium)
> - Opera

> **Note:**
>
> When logging out via the "Start" menu, the operating system forcibly terminates the process of audio interception. In this regard, the last chunk of audiodata cannot be intercepted. This chunk length is no more than one minute.

Note:

If when the rule is triggered, something that makes audio recording impossible happens (for example, the microphone malfunction), then the event may be containing a mute audio recording (you hear no sound when you play it).

Clipboard Monitor Rule

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

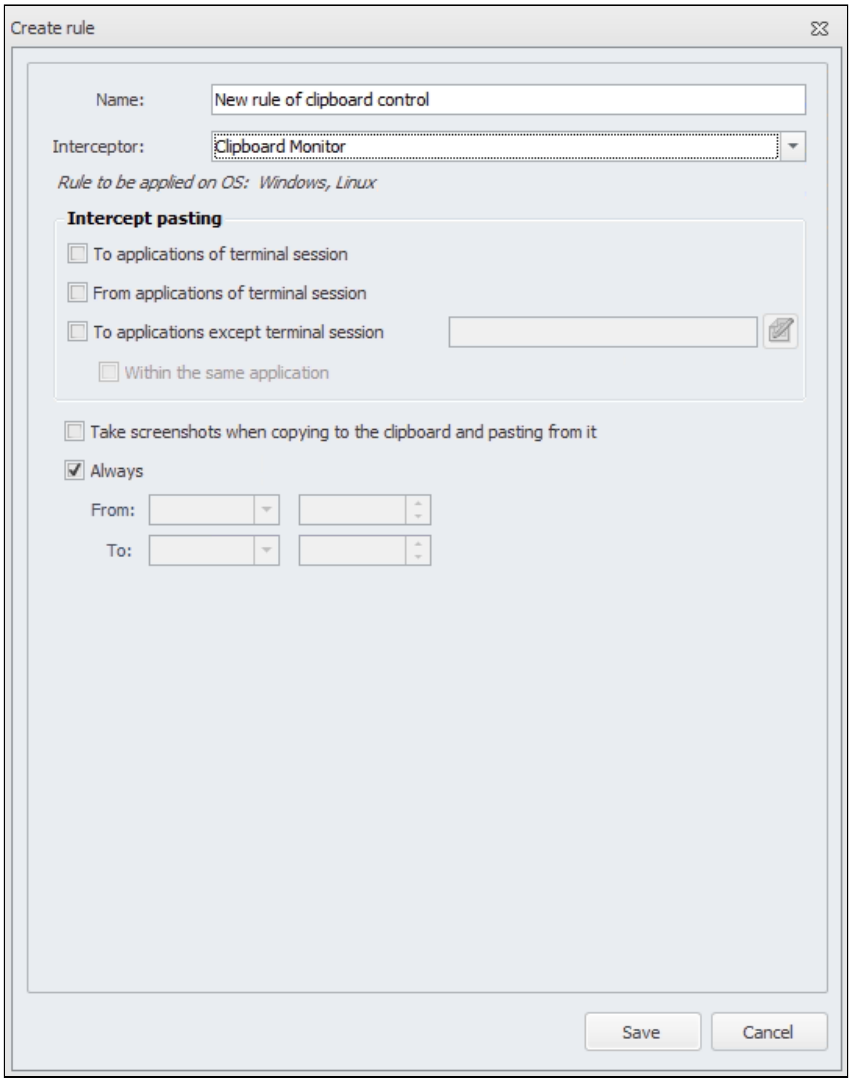
Warning!

Device Monitor intercepts only text data with this rule.

To control file copying, use the File Monitor rule (see "File Monitor Rule").

Note:

The rule applies on computers with Windows OS, RED OS and Alt Linux OS.



To configure the rule:

1. Open the **Create rule** window (see "Adding Rule") and in the **Name** field specify the rule name.
2. In the **Interceptor** field, select **Clipboard Monitor**.
3. In the **Intercept pasting from clipboard** area, specify when the rule applies:

> **Warning!**
>
> On computers with RED OS and Alt Linux OS, the following options are not supported:
>
> - **To applications of terminal session**
> - **From applications of terminal session**
>
> To configure the rule for RED OS and Alt Linux OS, select the **To applications except terminal session** option and choose the Linux list of applications.
> On computers with RED OS and Alt Linux OS, the **Within the same application** option is not supported.

- **To applications of terminal session**. If the option is selected, then the rule will be triggered when data is pasted to applications of a terminal session. Pasting data within a terminal session does not trigger the rule.

- **From applications of terminal session**. If the option is selected, then the rule will be triggered when data is pasted from 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 will be triggered 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 triggered when data is pasted to the application from which it has been copied, select the **Within the same application** option. Interception within a single application is supported only if the application uses system clipboard mechanisms.

4. Set flag next to the field **Take screenshots when copying to the clipboard and pasting from it** to select the corresponding option.

> **Warning!**
>
> On computers with RED OS and Alt Linux OS, taking screenshots in this rule is not supported.

5. Define a period of rule action. By default, the rule 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.
6. When all parameters are configured, click **Save**.

> **Note:**
>
> Blockage based on analysis performed in Traffic Monitor is supported only on Agents running Windows OS for operations when applications of terminal session are used.

Cloud Storage Monitor Rule

The **Cloud Storage Monitor** interceptor allows you to control web clients of the following cloud storages:

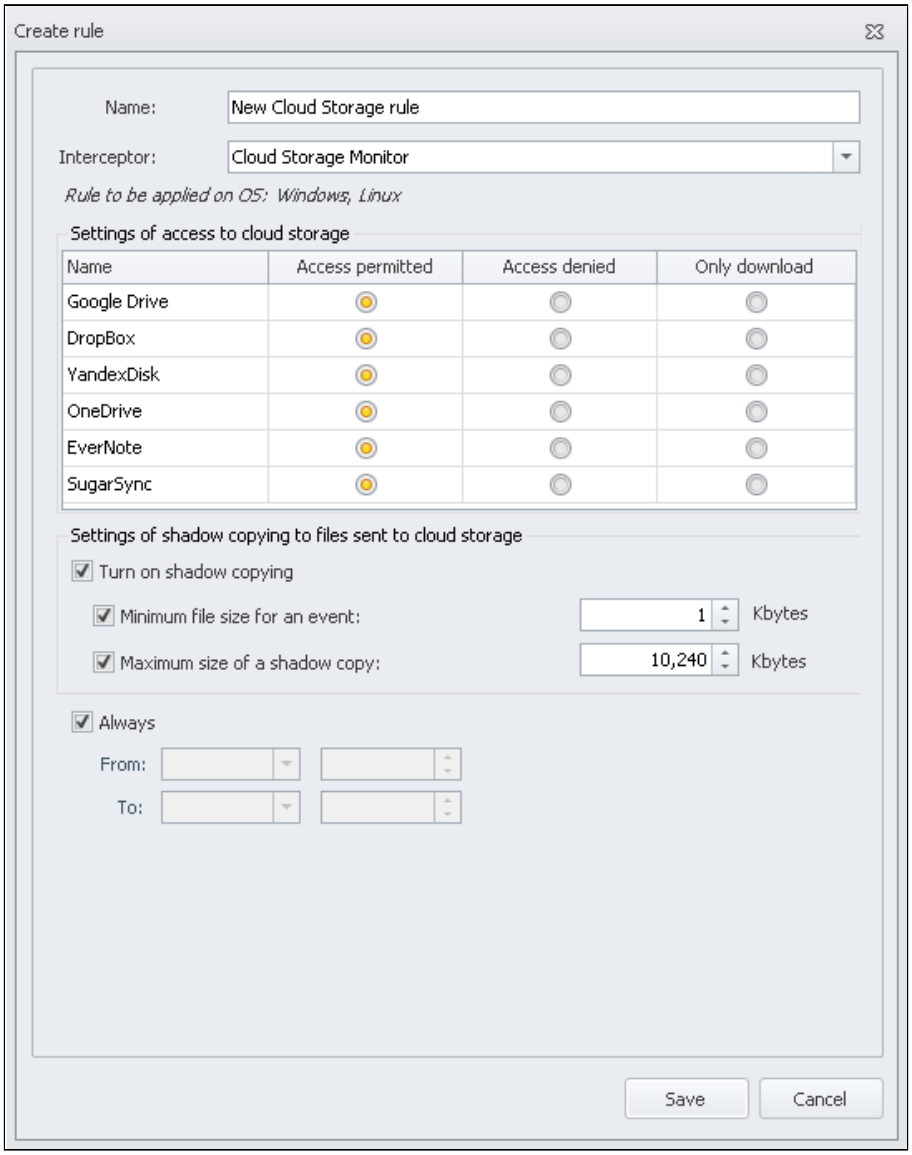
- Google Drive
- DropBox
- YandexDisk
- OneDrive
- EverNote
- SugarSync

For all cloud storages, the following restriction modes are available: **Access Denied** and **Only download**.

> **Warning!**
>
> In case access to Google Drive storage is denied, it may cause the incorrect operation and deny to other Google services using docs.google.com host. E.g., Google Docs, Google Tabs, Google Slides etc.

> **Note:**

The rule applies on computers with MS Windows, Astra Linux OS, Red OS and Alt Linux OS.



To configure the rule:

1. Open the **Create rule** window (see "Adding Rule") and in the **Name** field, specify the rule name.
2. In the **Interceptor** field, select **Cloud Storage Monitor**.
3. In the **Setting of access to cloud storage** area, mark the option for access limitation.
4. Define a period of the rule action. By default, the rule is always in effect (**Always** option is checked). To specify a period, clear **Always** checkbox and specify dates and time in **From** and **To** fields.
5. When all parameters are configured, click **Save**.

Note:

Blockage based on analysis performed in Traffic Monitor is supported only on Agents running Windows.

Device Monitor Rule

The **Device Monitor** interceptor allows you to control employee access to peripheral devices, mobile devices, and cameras connected to the computer as well as devices connected to thin and thick terminal clients.

Warning!

On computers with Linux OS only removable storage devices and MTP devices access setting and control are supported. The **Full access only to encrypted devices** option is unavailable.

When the device is blocked, it will be displayed in the OS but will not be available for usage.

You can configure appropriate control options for the following types of devices connected to the computer:

Full access only to encrypted devices / Read only / No access / Allowed to use	Read only / No access / Allowed to use	No access / Allowed to use
• Floppy • Removable storages (USB and IEEE 1394 devices)	• CD/DVD • MTP-compatible device (connected via MTP or PTP)*	• LPT port • COM port • Local Printer (with USB, IEEE 1394, SCSI connection, etc.) • Image Editing Devices (cameras and scanners) • Bluetooth Device • IrDA Device • Other USB Devices • FireWire • Modem • Smart Card Reader • Tape Drive • Multifunctional Device • PCMCI device • USB Adapter • Network printer • Pocket Computer (Windows Mobile and Palm OS pocket computers)

* – reading and removing actions are allowed

Note:

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

Mobile devices can be connected to the computer as:

- a removable storage;

- an MTP or PTP device;
- a USB network adapter.

Connection via MTP and PTP can be controlled for mobile phones on Android, iOS, Windows Phone/10 Mobile, and Blackberry 10 platforms.

A photo camera can be connected to the computer as:

- a removable device;
- a PTP device.

Important!

You can also use the File Monitor rule to control copying files to removable and MTP devices. Please note that the File Monitor rule allows you to monitor copying files, while the Device Monitor rule allows you to completely prohibit such operations. On how to solve conflicts if the event matches more than one rule, see "Applying Rules" and "Device Monitor Rules Application".

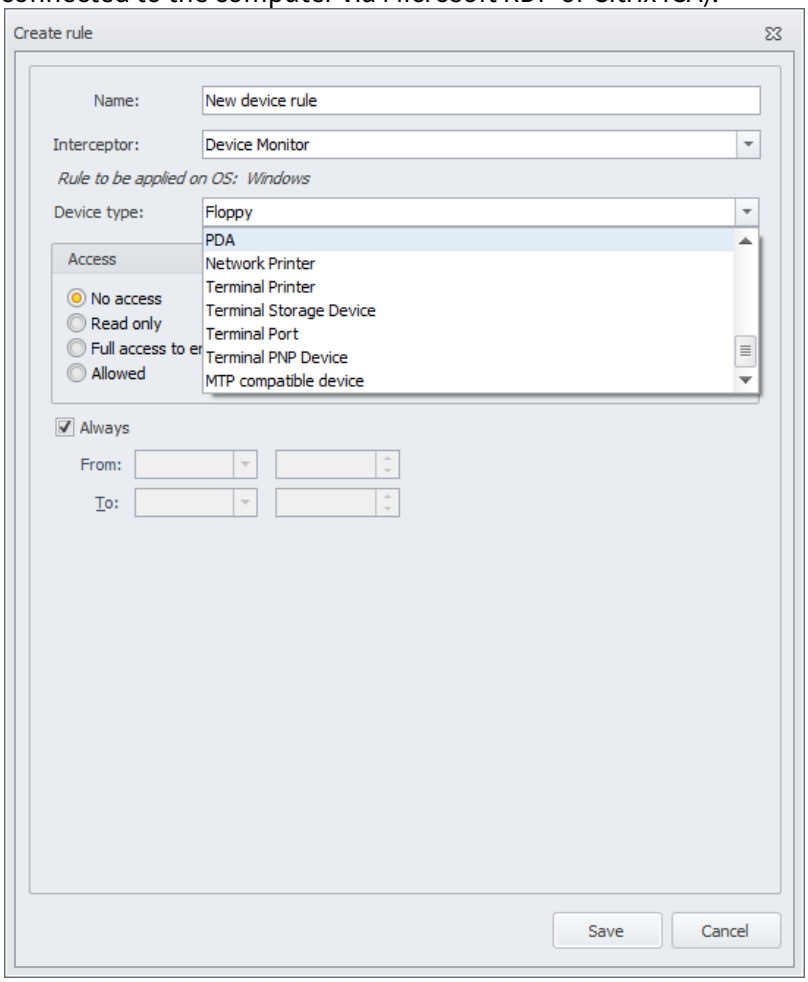
With this rule, you can also control the following types of devices which are connected via Microsoft RDP or Citrix ICA with the following restrictions:

Read only / No access / Allowed to use	No access / Allowed to use
• Terminal storage	• Terminal printer • Terminal port (thin client port) • Terminal Plug and Play devices

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).



To configure the rule:

1. Open the **Create rule** window (see "Adding Rule") and in the **Name** field, specify the rule name.
2. In the **Interceptor** field, select **Device Monitor**.
3. Select the device type controlled by this rule from the **Device type** drop-down list.
4. In the **Access** area, select the required access level. You can:
    - completely prohibit access to the device;
    - allow read-only access (only for **CD/DVD**, **MTP-compatible device**, **Floppy**, **Removable storage**, and **Terminal storage** types);

      Note:

      For **MTP-compatible device** type, the read-only access level also enables deleting files from devices.

    - allow full access only to encrypted devices (only for **Floppy** and **Removable storage** types).
    - allow full access to the device;
5. Define a period of the rule action. By default, the rule 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.
6. When all parameters are configured, click **Save**.

Note:

You can send events of connecting/using devices to Platform. For details, see "Settings to Send Data to Products".

Specifics of applying the rule on particular devices:

Mobile devices on BlackBerry 10 platform with "USB storage mode" setting enabled are treated by Device Monitor as two devices: *MTP-compatible device* and *Removable storage device*. To prevent copying data to the device, you should prohibit using *Removable storage device*.

Specifics of applying the rule during update:

After updating Agent to the current version, please, reboot the workstation to support the changes of denying access to MTP devices. In case of Agent instalation, no reboot is needed.

File Monitor Rule

The **File Monitor** interceptor allows you to monitor the following operations: copying files from/to removable storages and network resources (including network volumes), writing to the file on a removable device. The System registers only successful operations.

Note:

The rule applies on computers with MS Windows, Astra Linux OS, Red OS and Alt Linux OS.

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.

Using this rule, you can monitor the following actions of employees:

- Copying files to network resources using UNC (for example, *Server**SharedFolder**Folder**File*);
- Copying/moving files from/to a removable device. The System monitors operation of copying/moving from a controlled computer, another removable device or a network resource;
- Creating files directly on a removable device;
- Editing files directly on a removable device, including file renaming;
- Copying files from/to media devices connected via MTP;
- Copying files to a terminal session application;

> **Warning!**
>
> When copying file through terminal session using clipboard, only the short file name is known, not the full path.

> **Note:**
>
> To transfer data via RDP you are recommended to use disks "forwarding" mechanism to remote session instead of transfer via clipboard.

- Copying files to resources connected via terminal session (redirection for network folders and virtual devices is supported).

> **Warning!**
>
> Terminal session events cannot be created when copying files not across the terminal session border, but inside the local client remote connection. For example, when copying files via **Connection settings** -> **Open file**.

> **Warning!**
>
> On computers with RED OS and Alt OS, file copying to a network resource is not intercepted if the connection was established by entering the server name in the OS file manager search line.
>
> On computers with Astra Linux and RED OS, the following operations are not controlled:
>
> - Copying/moving files to resources connected via terminal session;
> - Writing to CD/DVD disks including those connected via USB ports.
>
> Blockage based on analysis performed in Traffic Monitor is supported:
>
> - Only on Agents running Windows, Alt, RED OS and Astra Linux 1.7 when copying files from/to removable storages and network resources.
> - Only on Agents running Windows OS when copying/moving files to resources connected via terminal session.

On computers running Linux family OS, copying a file from network resources to the workstation is intercepted only when sending the file via the SMBv1/CIFS protocol using one of the methods:

- Connecting to network resources and mounting to the file system: `mount -t cifs`
- Connecting to network resources with standard file explorers, built-in and third-party utilities

Blocked intercepted archives cannot be opened and blocked files are deleted.

The System opens archives and applies Traffic Monitor policies to them in one of the following cases:

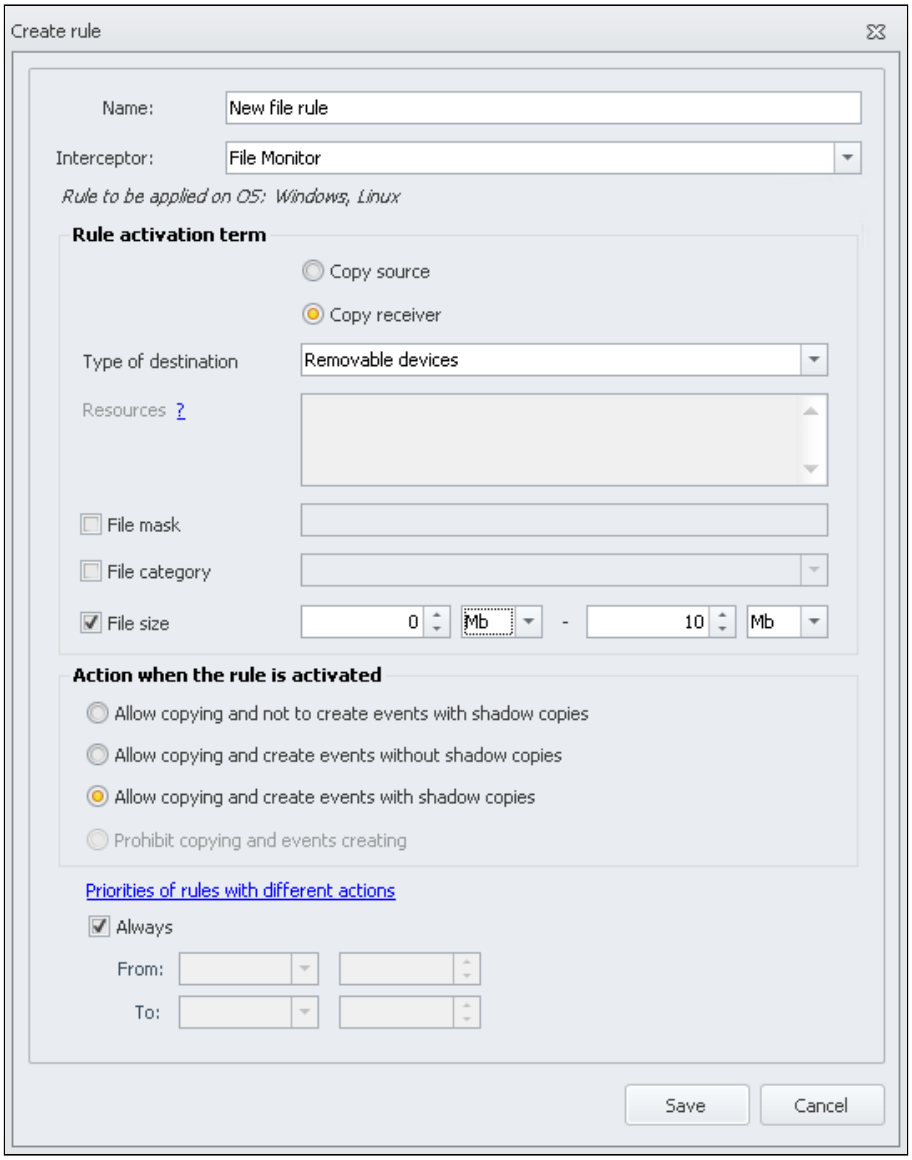
- An archive of 7Z, ZIP, TAR.GZ, AR, RAR or ISO format was intercepted on an Agent running Windows OS;
- An archive of 7Z, ZIP, TAR.GZ or AR format was intercepted on an Agent running Alt OS, RED OS or Astra Linux 1.7.

PDF file copying based on Traffic Monitor analysis can be blocked only on workstations running Windows OS or RED OS.

Warning!

You can also control access to removable and MTP-compatible devices with Device Monitor Rule which allows you to completely deny access to the device.

Information on cases when the rule matches several rules, see in "Applying Rules".



To configure the rule:

1. Open the **Create rule** window (see "Adding Rule") and in the **Name** field, specify the rule name.
2. In the **Interceptor** field, select **File Monitor**.
3. Specify **Rule activation term:**
   a. set the intercepted copy direction: C*opy source* or C*opy receiver;*
   b. specify the type of destination: *Removable devices*, *Network resources*, or *Terminal session*;
   c. if required, specify the Network resources, setting its addresses.
4. If required, you may restrict the list of controlled files, setting the file mask. To do this, mark the field **File mask** and specify the mask: you may use «?» to replace one symbol or use «*» to replace the range of symbols. For example, *.doc. The backspace is interpreted as a part of a filename.

> **Warning!**
>
> There should be only one mask for one rule. In case it is required to type in several masks, one should create a rule corresponding to the mask.

5. You can constrain controlled files by signature category (see "Signatures"). Flag **Category** checkbox and select a category from a drop-down list: the rule will be applied to files with the chosen signature type.

> **Note:**
>
> Signatures categories cannot be taken into consideration on the computers running Astra Linux, RED OS and ALT Linux OS; the rule is triggered if any file is being copied, regardless of the selected file category.

6. To control files by size, specify:
   - **Minimum File Size**. When checked, rule will be applied only to files larger or of the specified size.
   - **Maximum File Size**. When checked, rule will be applied only to files smaller or of the specified size.
7. Select the option for the rule, you may:
   a. Allow copying and not to create events with shadow copies;
   b. Allow copying and create events without shadow copies;
   c. Allow copying and create events with shadow copies;
   d. Prohibit copying and events creating.

> **Warning!**
>
> If the File Monitor rule enables shadow copying, but there is less free space on the hard drive than required by the policy (see "Creating shadow copies and blocking operations due to space problems"), then the file will be saved without a shadow copy.

> **Warning!**
>
> Events without shadow copies cannot be sent to Traffic Monitor.

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

For details, see the Knowledge Base article: "Intercepting Features and Restrictions when Copying Files from/to Removable Devices, Network Resources, FTP, when Sending Mail. Specifics of Configuring Rules in Data Protection Policies on Agents".

File Operations Monitor Rule

The **File Operations Monitor** interceptor allows you to control it if applications read data from files or write to files. With this rule, you can also create file shadow copies and screenshots.

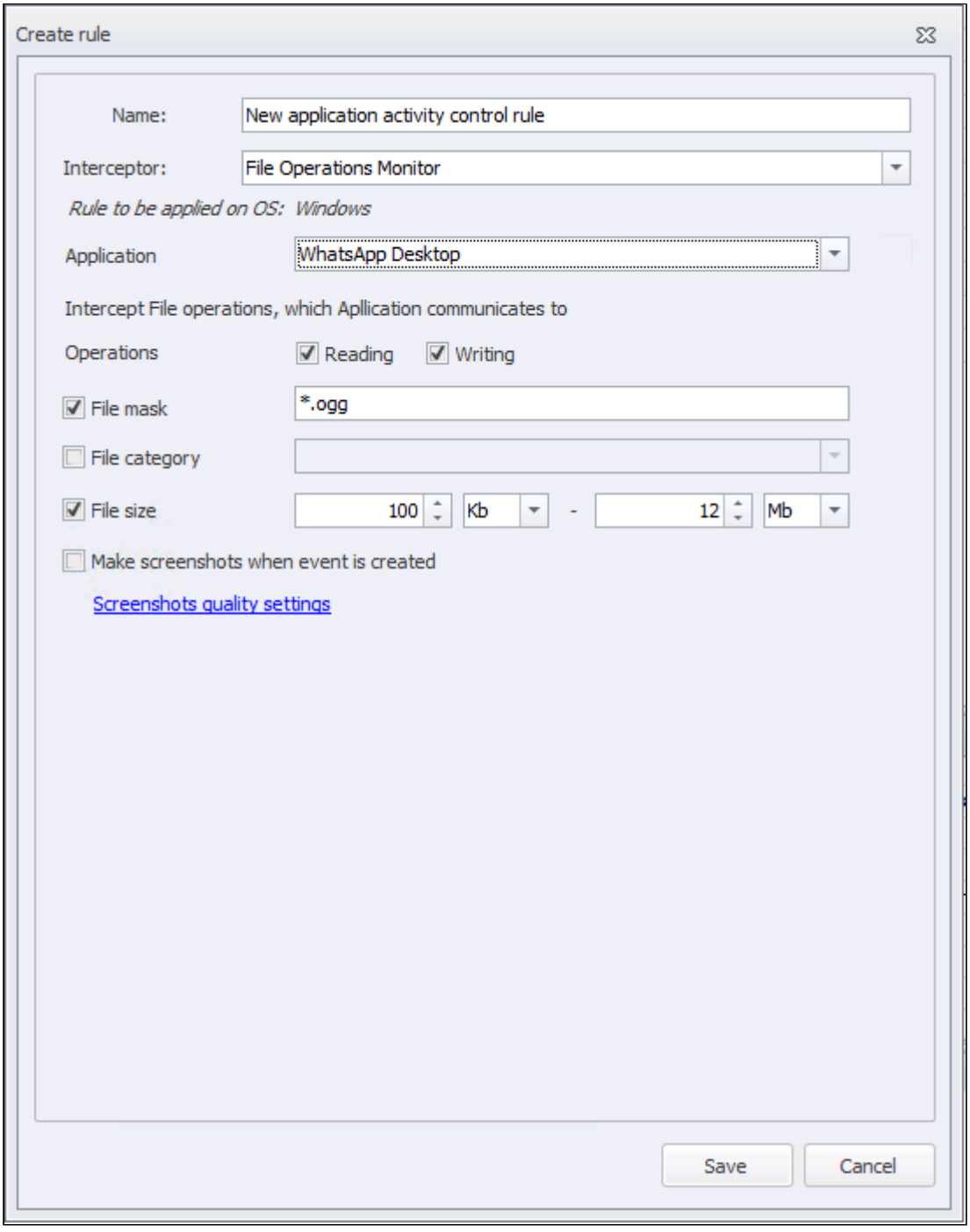
> **Important!**

By default, the rule is unavailable. In order to use the File Operations Monitor rule, add the Application Blockade configuration to the Device Monitor security scheme (see "Application Blockade").

Note:

The rule applies on computers with MS Windows OS.

The rule provides advanced control of applications:



To configure the rule:

1. Open the **Create rule** window (see "Adding Rule") and in the **Name** field, specify the rule name.
2. In the **Interceptor** field, select **File Operations Monitor**.
3. In the **Application** field, select the application you want to control.

> **Note:**
>
> The list of available applications is defined by the Application Blockade configuration.

4. In the **Operations** field, specify operations you want to control:
   - Reading
   - Writing
5. If necessary, you can limit the set of controlled files using a file mask. For this, select the **File mask** option and specify the mask using the following characters:
   - «?» - to replace a single character;
   - «*» - to replace a set of characters. For example, *.doc;
   - The space is treated as a part of the file name.

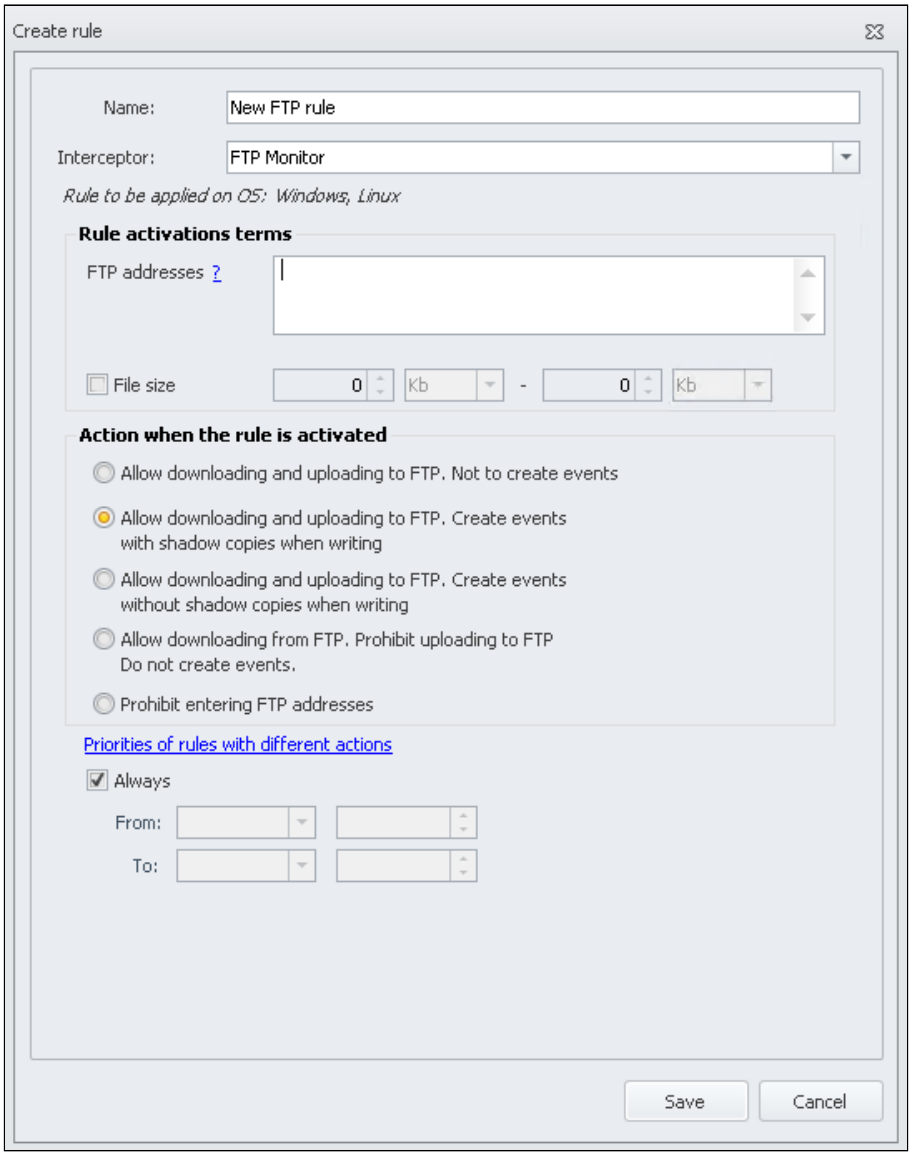
> **Important!**
>
> There can only be one mask for one rule. If you need to add several masks, you should create a separate rule for each mask.

6. You can also limit the application of the rule with a signature category (see "Signatures"). For this, select the **Category** field and choose a category from a drop-down list: the rule will apply to files if their type matches the selected category of signatures.
7. To limit the size of controlled files, select the **File size** field and specify :
   - Minimum file size. If the field is filled, then the rule will only apply to files whose size is greater than or equal to the specified value.
   - Maximum file size. If the field is filled, then the rule will only apply to files whose size is less than or equal to the specified value.
8. To create screenshots, select the **Make screenshot when event is created** option.
9. If necessary, specify image quality settings: see "Application Control and screenshots".
10. When all parameters are configured, click **Save**.

FTP Monitor Rule

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

> **Note:**
>
> The rule applies on computers with MS Windows, Astra Linux OS, Red OS and Alt Linux OS.



To configure the rule:

1. Open the **Create rule** window (see "Adding Rule") and in the **Name** field, specify the rule name.
2. In the **Interceptor** field, select **FTP Monitor**.
3. In **Rule activation terms** please specify **FTP addresses.** Clicking on **?** (question mark), you will know the details on how to fill in the field. You can also specify file size limitation, putting a check next to the File size tab. This parameter is available only when creating events with shadow copies and creating events without shadow copies when writing if there is less free space on the computer than it is required by the policy (see "Creating shadow copies and blocking operations due to space problems").
4. Select the control level for data exchange through the FTP protocol:
    - **Allow downloading and uploading to FTP. Not to create events**
    - **Allow downloading and uploading to FTP. Create events with shadow copies when writing**
    - **Allow downloading and uploading to FTP. Create events without shadow copies when writing**
    - **Allow downloading and uploading to FTP. Prohibit uploading to FTP. Do not create events**

- **Prohibit entering FTP addresses**

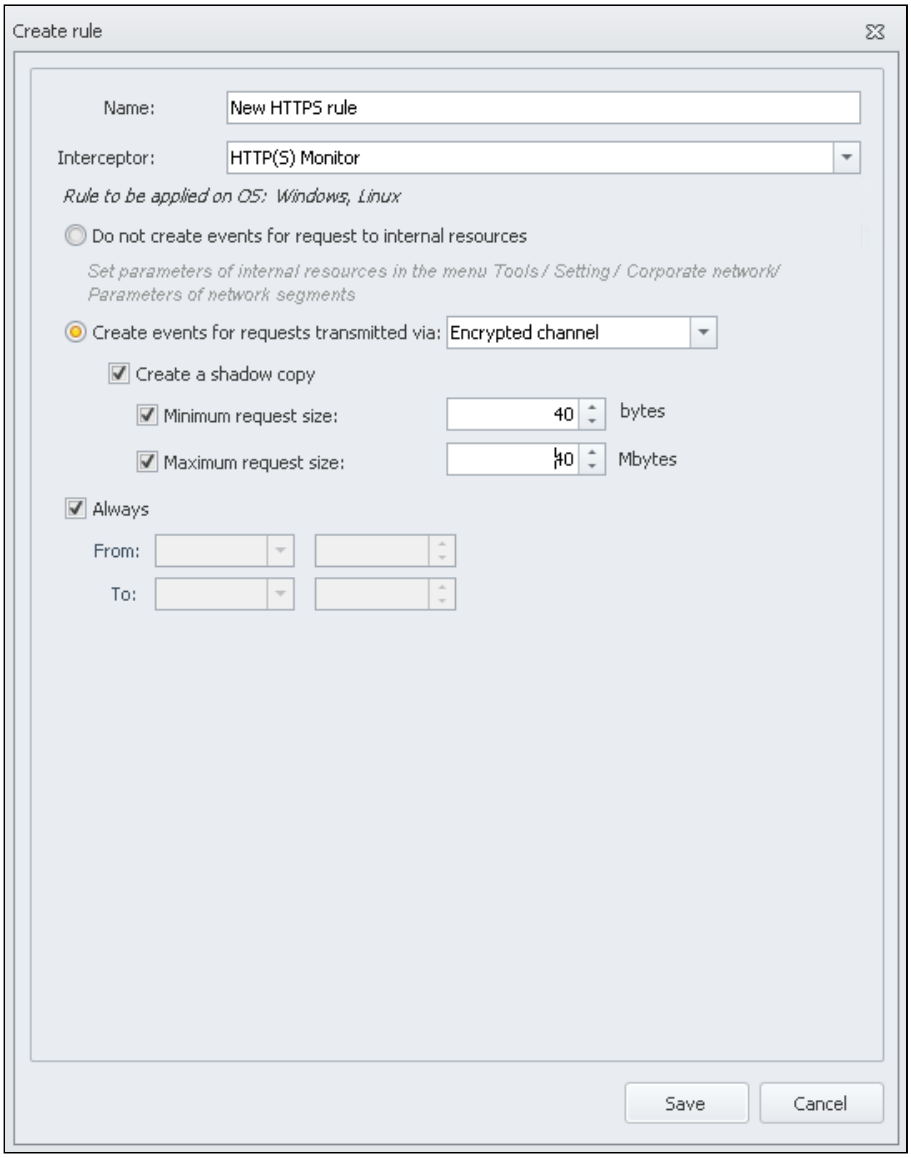
5. Define a period of rule action. By default, the rule is always in effect (the **Always** option is checked). To specify a period, clear the **Always** checkbox and specify dates and time in **From** and **To** fields.
6. When all parameters are configured, click **Save**.

> **Note:**
>
> Blockage based on analysis performed in Traffic Monitor is supported only on Agents running Windows.

HTTP(S) Monitor Rule

The **HTTP(S) Monitor** interceptor allows you to control data transfer through HTTP and HTTPS protocols.

> **Note:**
>
> The rule applies on computers with MS Windows, Astra Linux OS, Red OS and Alt Linux OS.



To configure the rule:

1. Open the **Create rule** window (see "Adding Rule") and in the **Name** field, specify the rule name.
2. In the **Interceptor** field, select **HTTP(S) Monitor**.
3. 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 "Corporate Network Control", **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.

- 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 a specified size or larger.
  - **Maximum request size**. If the check box is selected, shadow copies will be enabled only for files of a specified size or smaller.

Important!

If there is less free space on the computer than it is required by the policy (see "Creating shadow copies and blocking operations due to space problems"), then the event will be created without a shadow copy.

4. Define a period of the rule action. By default, the rule is always in effect (the **Always** option is checked). To specify rule duration, clear the **Always** check box and specify dates and time in **From** and **To** fields.
5. 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.
4. HTTP traffic can be blocked based on analysis performed in Traffic Monitor. This feature is supported only on Agents running Windows and RED OS.

Important!

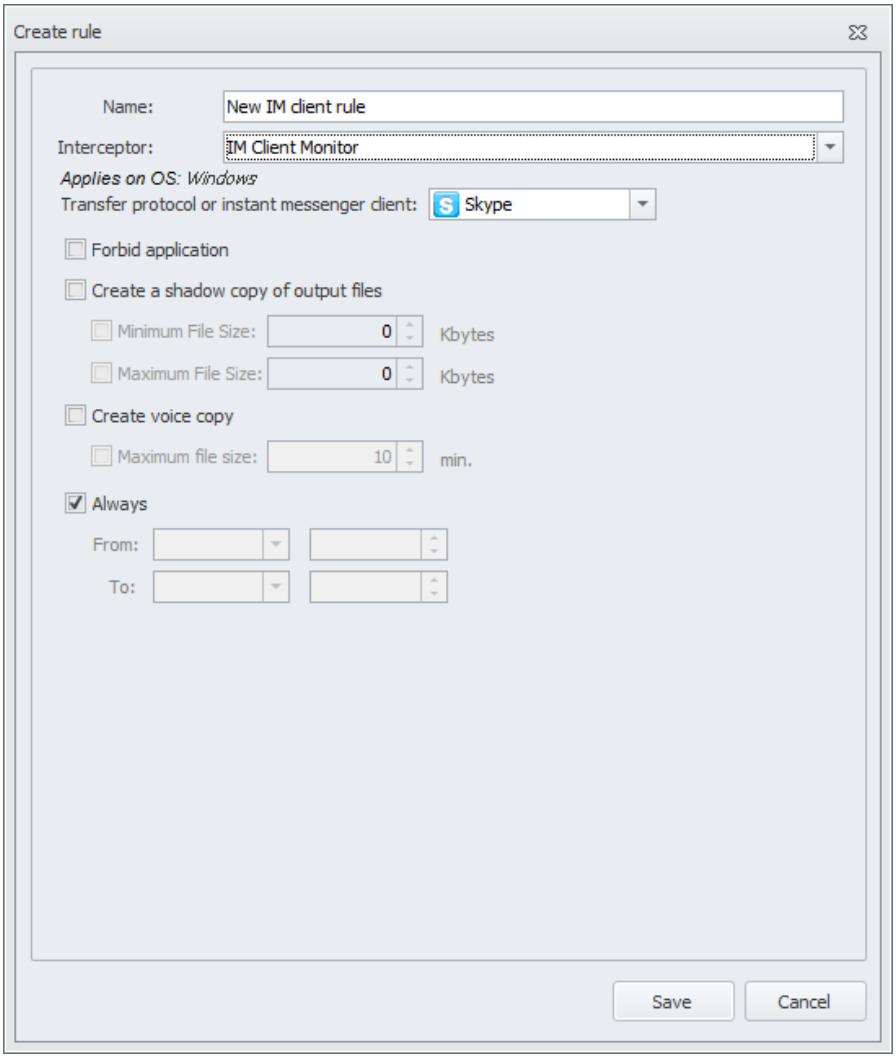
On computers running Astra Linux, RED OS and Alt OS:

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

HTTP traffic cannot be blocked on workstations running Astra Linux OS of versions 1.6 and 2.12.

IM Client Monitor Rule

The **IM Client Monitor** interceptor allows you to control employee access to instant messengers: Skype, Telegram, Jabber (XMPP protocol), Facebook, WhatsApp, VK (VKontakte), MMP protocol.



To configure the rule:

1. Open the **Create rule** window (see "Adding Rule") and in the **Name** field, specify the rule name.
2. In the **Interceptor** field, select **IM Client Monitor**.
3. In **Transfer protocol or instant messenger client** field, select messenger type which is controlled by this rule:
   - Skype - to control usage of Skype versions 7, 8 and Skype For Web;
   - XMPP - to control Jabber usage;
   - MMP - to control applications, using MMP protocol;
   - Telegram - to control Telegram;

> **Note:**

The rule allows to intercept the following Telegram versions:

- desktop version: the application from the official Telegram website (desktop.telegram.org) or from the Microsoft Store;
- web versions: K, Z and the earlier one (Legacy).

Web-based version interception has the peculiarities as follows:

- different web-based versions are defined as different applications;
- the start of interception can be delayed for 50 seconds after authorization is complete;
- Google Chrome and Mozilla Firefox browsers are supported.

- Facebook - to control Facebook usage;
- VK - to control VK usage ;
- WhatsApp - to control WhatsApp usage.

Note:

The rule allows to intercept the following WhatsApp versions:

- desktop version: the application from the official WhatsApp website (whatsapp.com) or from the Microsoft Store;
- web version in the browsers: Google Chrome, Mozilla Firefox, Microsoft Edge (Chromium), Yandex.Browser, Opera.

Intercepting the desktop version from the Microsoft Store has the following limitations:

- only text messages, images and attachments are intercepted;
- the following are not intercepted: citations, forwarded messages and attachment annotations;
- sender's phone number is not detected;
- if an employee sends a message to a group chat:
  - the recipients may be detected incorrectly;
  - event is sent to Device Monitor server with a delay of up to 10 minutes;
  - event time may be later than the actual message time;
- duplicates may appear and the order of messages may be incorrect.

Warning!

Interception will not be performed if the employee has logged into the web version of WhatsApp:

- when the Agent has not yet been installed;
- when the Agent has been stopped;
- when the Agent version lower than 7.8.0 was running.

In these cases, after starting a new version of Agent, you need to clear the browser cache.

4. If you need to intercept Skype voice messages and create events in Traffic Monitor, select the **Create shadow copy of output files** checkbox and, if necessary, specify file size (sound file will be saved in `*.ogg` format)
   - If the **Maximum File Size** option is selected, then several events with shadow copies will be created for talks, whose length exceeds the specified value.

5. If you want to completely prohibit using Client of this type, select the **Forbid application** checkbox (not available for **Telegram**, **Facebook**, **WhatsApp**, **VK**).

> **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 prohibit using Telegram, Facebook, WhatsApp and VK, use Application Monitor Rule (see "Application Monitor Rule").

6. If you want to create shadow copies of transferred files and send them besides event, to Traffic Monitor, select the **Create shadow copy of output file** checkbox. In this case, you can also define additional parameters for shadow copies:
   - **Minimum File Size**. When checked, shadow copies will be created only for files of larger or equal size.
   - **Maximum File Size**. When checked, shadow copies will be created only for files of smaller or equal size.
7. If you want to create shadow copies of voice messages and send them besides event, to Traffic Monitor, select the **Create voice copy** option and specify the maximum length of a voice file. For this, in the **Maximum file size** field, specify the required value in minutes.
8. Define a period of the rule action. By default, the rule is always in effect (the **Always** option is checked). To specify the rule duration, clear the **Always** checkbox and specify dates and time in **From** and **To** fields.
9. When all parameters are configured, click **Save**.

> **Warning!**
>
> Values specified in the **Minimum File Size** and **Maximum File Size** fields apply only to creating shadow copied. If the file size is within the specified range, then the event will contain a shadow copy. Otherwise, the event will be created without a shadow copy. The event can be created without a shadow copy also in the case if there is less free space on the computer than it is required by the policy (see "Creating shadow copies and blocking operations due to space problems").
>
> If there is an active IM Client Monitor rule, then shadow copies for chats and messages are created regardless of the **Create shadow copy of output file** and **Create voice copy** settings. Shadow copies for chats and messages are configured in the " Network Traffic Control " section.

> **Important!**
>
> When sending messages to a Skype group chat, the list of recipients in the event includes also the chat ID.
>
> If sending a file is the first message in the group chat, then the list of recipients in the event will contain only the chat ID.

You can use the chat ID in queries to search for events (see "Creating Queries"). When entering the ID, use the mask *. For example: d57efb0b486c4*.

Important!

In Telegram version 2.4.3 and later when sending a message to a group chat as a group administrator, the senders are not identified.

Keyboard Monitor Rule

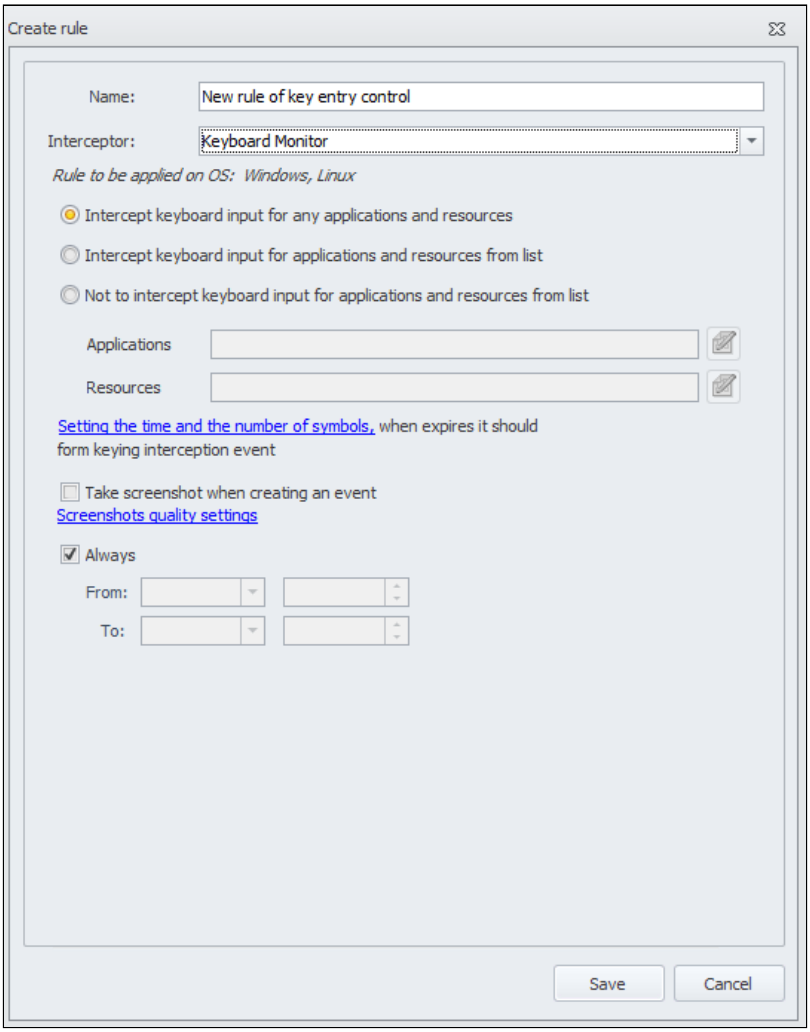
The **Keyboard Monitor** interceptor allows you to intercept text that is entered from the keyboard on workstations. Events are created:

- When a user switches active windows or tabs in the browser (for Agents on RED OS and OS Alt Linux Workstation 10 – only when active windows are switched).
- When the time interval specified in the settings expires. The interval is counted from the moment a user stops typing.
- When the number of characters entered reaches the limit of characters specified in the settings.
- When a user presses Enter / Ctrl+Enter / Shift+Enter, if the corresponding setting is configured (see "Control of Keyboard Input").

Note

The rule is applied on workstation operating MS Windows, OS Alt Linux Workstation 10 and OS Red OS.

Events which are created from intercepted data are then sent to Traffic Monitor for analysis and further processing.



To configure the rule:

1. Open the **Create rule** window (see "Adding Rule") and in the **Name** field, specify the rule name.
2. In the **Interceptor** field, select **Keyboard Monitor**.
3. Specify in which case the rule will apply:
   - **Intercept keyboard input for any applications and resources**;
   - **Intercept keyboard input for applications and resources from list**;

     > **Note:**
     >
     > Using lists is supported only for OS MS Windows.

   - **Not to intercept keyboard input for applications or resources from list**.

   To choose the applications and resources where the rule should apply, click  : see "Application Protocol" and "Resources".
4. If required, specify additional conditions for creating events: see "Control of Keyboard Input ".
5. If required, specify the screenshots quality settings: see "Application Control and screenshots".

To receive screenshots, it is also necessary that you should set up sending screenshots in the **Settings to send data to products** section (by default, sending screenshots is enabled).

If the rule specifies that screenshots should be taken, however, sending screenshots is disabled in the **Settings to send data to products** section, then screenshots will not be sent. For details, see "Settings to Send Data to Products".

Important!

On workstations running RED OS, ALT Workstation 10 taking screenshots in this rule is not supported.

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

Important!

The System verifies if the resource being visited by a user matches the one in the list of resources only for Agents on Windows OS and only if one of the following browsers is used:

- Chrome
- Yandex.Browser
- Mozilla Firefox
- Edge (Chromium)
- Opera
- IE

Important!

For an Agent on Windows OS, configurations applied in the rules ScreenShot Monitor and Keyboard Monitor are independent and do not influence each other. Therefore, when creating screenshots the System does not consider possible overlap of the attributes and lists of applications and resources in the two rules. For example, if the option **Create screenshot of active window only** is disabled in ScreenShot Monitor rule, then the information from the applications and resources excluded in Keyboard Monitor (but not in ScreenShot Monitor rule) rule can appear on screenshots.

Important!

Keyboard input interception works correctly for the Russian and the English languages. If you add other languages, you need to restart the workstation.

Mail Monitor Rule

The **Mail Monitor** interceptor allows you to control incoming and outgoing email.

The Mail Monitor rule provides control of SMTP, IMAP, POP3, HTTPS protocols, and Outlook. For HTTPS, the System controls emails sent via the following services:

- Gmail
- Yandex
- Mail.ru
- Yahoo
- Rambler
- Outlook.com

Important!

The rule applies on computers with MS Windows and Astra Linux OS, RED OS and Alt OS.

On computers running Astra Linux OS, Alt OS and RED OS, the rule does not control Outlook.com.

Important!

On workstations running Linux-family operating systems, only outgoing traffic (SMTP protocol and web mail) can be blocked. On computers running Astra Linux OS of versions 1.6 and 2.12, blockage based on analysis performed in Traffic Monitor is not supported.

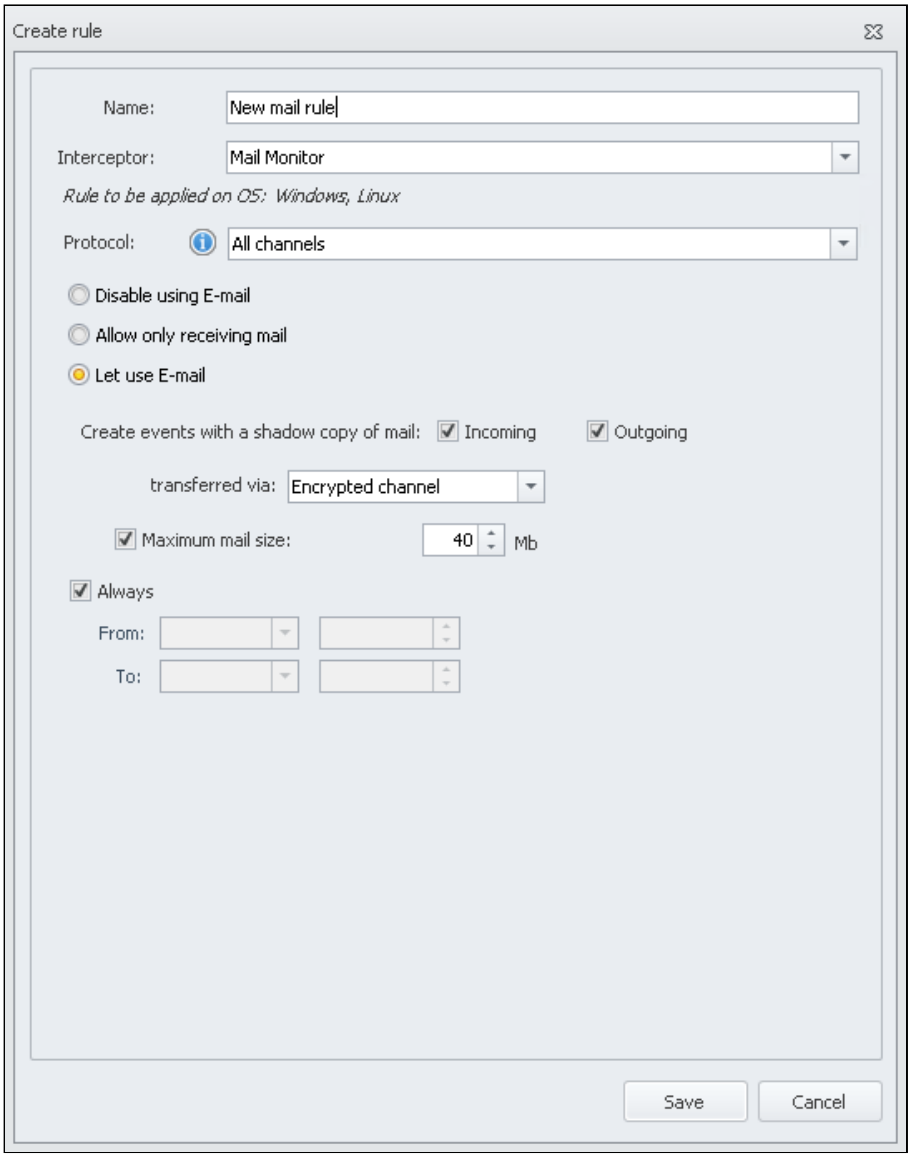
Important!

The System opens archives and applies Traffic Monitor policies to them in one of the following cases:

- An archive of 7Z, ZIP, TAR.GZ, AR, RAR or ISO format was intercepted on an Agent running Windows OS;
- An archive of 7Z, ZIP, TAR.GZ or AR format was intercepted as an email attachment sent via SMTP protocol on an Agent running Alt OS, RED OS or Astra Linux 1.7.

PDF file blockage is supported in one of the cases:

- The Agent is running Windows OS;
- The Agent is running RED OS and the file is sent as an email attachment via SMTP protocol.



To configure the rule:

1. Open the **Create rule** window (see "Adding Rule") and in the **Name** field, specify the rule name.
2. In the **Interceptor** field, select **Mail Monitor**.
3. In the **Protocol** field, choose the channel that will be controlled by the rule. Possible values:
   - **All channels**;
   - **SMTP** – only for outgoing mail;
   - **POP3** – only for incoming mail;
   - **Outlook** – both for incoming and for outgoing mail;
   - **IMAP** – only for incoming mail;
   - **HTTPS** – only for outgoing mail.
4. Choose what actions with mail are allowed for the user. Possible values:
   - **Forbid using email**;
   - **Allow only receiving mail** – is available only if *Outlook* or *All channels* value is selected in the **Protocol** field;
   - **Allow using email**.
5. In the **Create events with a shadow copy of mail** line, specify for what emails shadow copies should be created. Depending on the channel selected in step 6 the following values are available:

- For **POP3** and **IMAP** channels – only the **Incoming** direction;
- For **SMTP** and **HTTPS** – only the **Outgoing** direction;
- For **Outlook** and **All channels** – both **Incoming** and **Outgoing** directions are available. You can choose one value or both.

> **Warning!**
>
> If the **Allow using email** 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:

- In the **transferred via** field, specify if shadow copies should be created for emails sent via all channels or only via encrypted ones;

  > **Note:**
  >
  > For HTTPS protocol, the **All channels** value is unavailable.

- **Maximum mail size**. If the option is enabled, shadow copies will be created only for emails which 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 space problems"), a shadow copy will not be created.

  > **Important!**
  >
  > Shadow copy of web email will contain only the data from intercepted traffic. For example, the events will contain the email attributes except attachments, in the following cases:
  > - Person sends the email from templates after the event has been sent to Traffic Monitor, because the timeout after the last activity with the email was reached;
  > - Person sends the email from the templates created on another workstation;
  > - Person sends the email again (it has been sent earlier).

6. Define a period of the rule action. By default, **Always** option is active. To specify the rule duration, clear **Always** checkbox and specify dates and time in **From** and **To** fields.
7. When all parameters are configured, click **Save**.

> **Warning!**
>
> If the rule has the following attributes:
> - **Allow using mail**;
> - **Create events with a shadow copy of mail: Incoming and Outcoming, transferred via: All channels**.

and the mail program is configured to store data on the server (e.g., in MS Outlook, the **Save sent items to the next folder on the server** option is enabled in the **Internet E-mail Settings** dialogue box, **Sent** tab), then each mail sending event will generate two interception objects: one of the **Outcoming** type and the other one of the **Incoming** type. Depending on the mail program, the option name may differ.

Example:

To intercept Outlook emails via IMAP, SMTP, POP3 protocols at the network level:

1. Cancel excluding **Outlook** from network interception (for details, see "Exclusion of Application from Interception"). By default, this option is enabled.
2. Create a rule, activating interception for these protocols, as described above.
3. Delete the rule for Outlook/MAPI protocol.

Important!

When Outlook is included in network interception, operation with MS Exchange server may be incorrect.

Network Monitor Rule

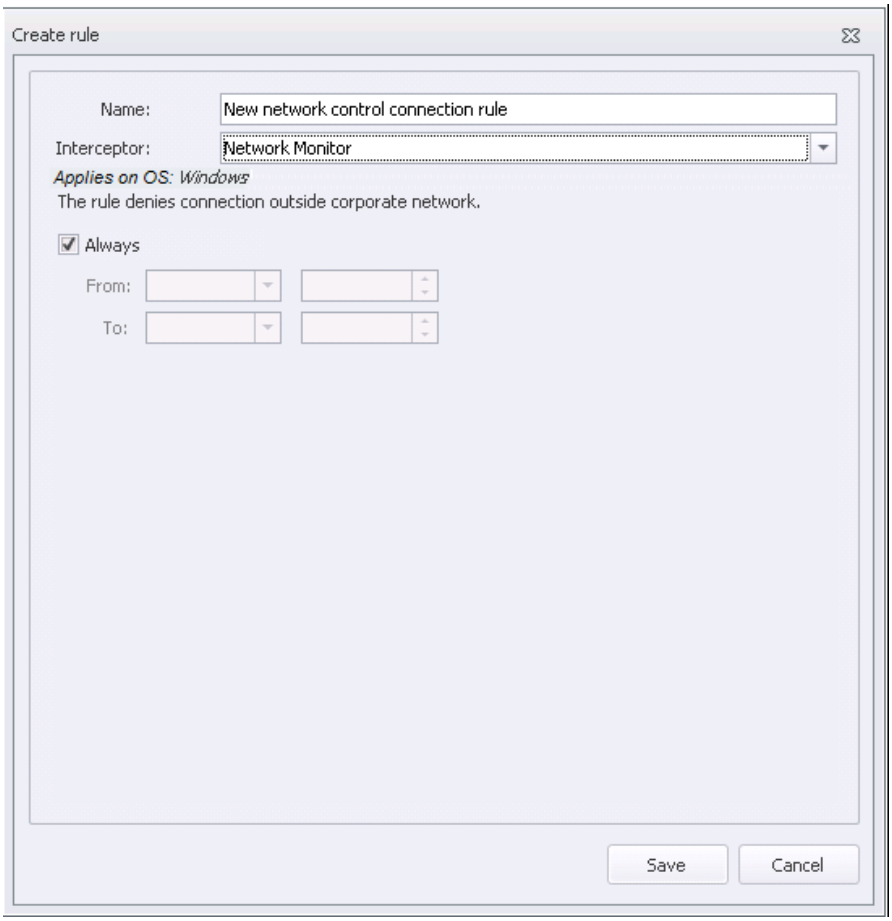
The **Network Monitor** interceptor allows you to prohibit data transfer over any network connections except connections with the corporate network or specified authorized servers. On how to define segments of the corporate network and authorized external addresses, see "Corporate Network Control".

Note:

The rule applies on computers with MS Windows OS.

Warning!

If there is at least one active Network Monitor rule, Device Monitor Agent installed on the computer tries to resolve the DNS names of Internet pages being opened. To avoid problems with external connections, you should configure forwarding servers on the corporate DNS server (for details, see the Internet article "Configure a DNS Server to Use Forwarders").



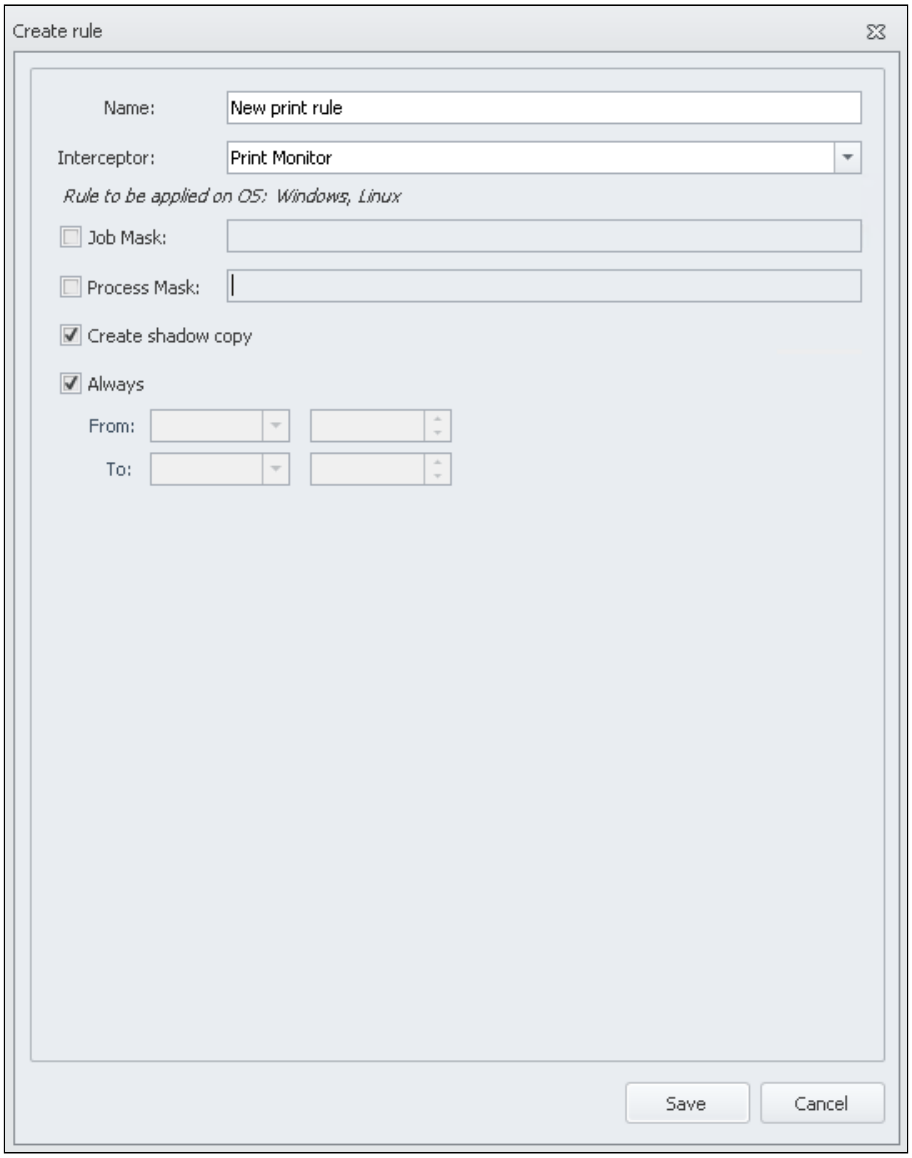
To configure the rule:

1. Open the **Create rule** window (see "Adding Rule") and in the **Name** field, specify the rule name.
2. In the **Interceptor** field, select **Network Monitor**.
3. Define a period of the rule action. By default, the rule is always in effect (the **Always** option is checked). To specify the rule duration, clear the **Always** check box and specify dates and time in **From** and **To** fields.
4. When all parameters are configured, click **Save**.

Print Monitor Rule

The **Print Monitor** interceptor allows you to monitor operations related to printing documents on local and network printers.

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



To configure the rule:

1. Open the **Create rule** window (see "Adding Rule") and in the **Name** field, specify the rule name.
2. In the **Interceptor** field, select **Print Monitor**.
3. If necessary, you can specify restrictions for 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 wildcards: «?» to replace one character or «*» to replace several characters. Spaces are treated as a part of the task name.

> **Important!**
>
> The title for printing task is being generated by the application, where from the document is sent for printing. That's why the title may be any tex and not the one that is a document title.

- **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 (**Printer 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 wildcards: «?» to replace one character or «*» to replace character set. Spaces are treated as a part of the task name.

4. 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 (see "Creating shadow copies and blocking operations due to space problems"), then the document will be printed without creating a shadow copy.

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

Example:

To intercept the printing task file with `.txt` extension, in `notepad.exe`:

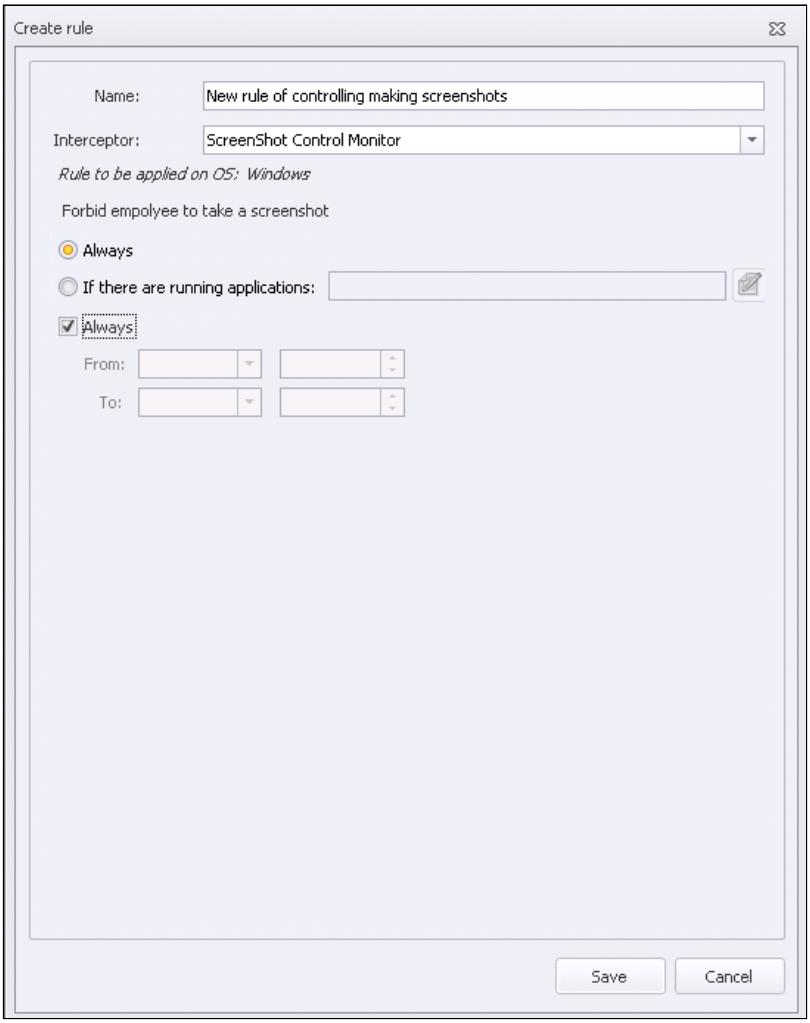
1. In Process Mask line enter *.txt*
2. In Process Mask line enter *nodepad.exe

> **Important!**
>
> The printing tasks are to be intercepted in case the user OS displays the files extension (In Folder options unmark **Hide extension for registered file types**).

ScreenShot Control Monitor Rule

The **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:

1. Open the **Create rule** window (see "Adding Rule") and in the **Name** field, specify the rule name.
2. In the **Interceptor** field, select **ScreenShot Control Monitor**.
3. In the **Forbid employee to take a screenshot** area, specify the condition. Possible choices:
   - **Always**;
   - **If there are running applications**. If you select this option, click  to specify applications (see "Applications protocol").
4. Define a period of the rule action. By default, the rule is always in effect (the **Always** option is checked). To specify rule duration, clear the **Always** check box and specify dates and time in the **From** and **To** fields.
5. When all parameters are configured, click **Save**.

ScreenShot Monitor Rule

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

> **Note:**
>
> The rule applies on computers with MS Windows OS, RED OS and Alt Linux OS.

Note:

Configure the Statistics rule (see "Statistics Rule") to send events with screenshots to InfoWatch Activity Monitor.

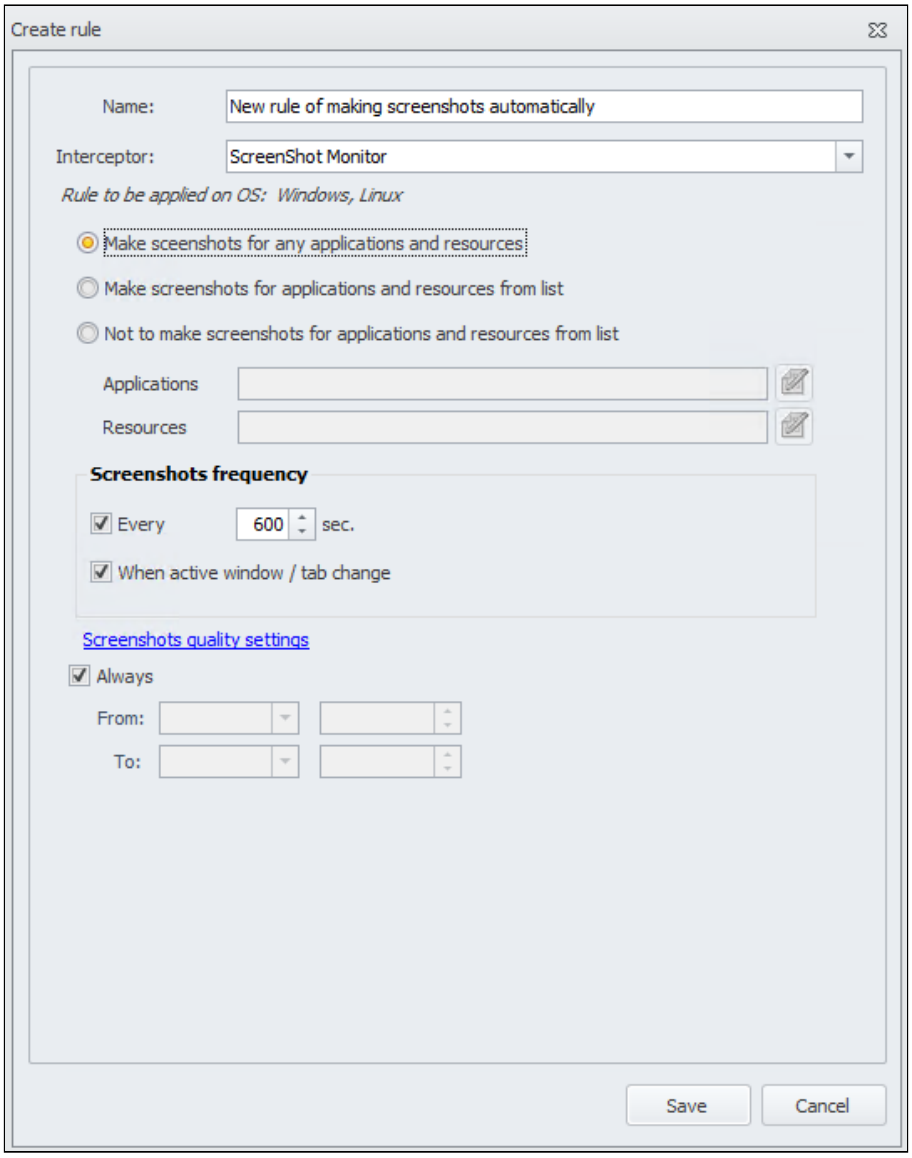
Important!

To create screenshots when data is copied to the clipboard or pasted from the clipboard use the Clipboard Monitor rule (see "Application Monitor Rule").

To create screenshots when intercepting text input from keyboard on workstations use the Keyboard Monitor rule (see "Keyboard Monitor Rule").

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 "Application Control and screenshots").



To configure the rule:

1. Open the **Create rule** window (see "Adding Rule") and in the **Name** field, specify the rule name.
2. In the **Interceptor** field, select **ScreenShot Monitor**.
3. Define in which case the rule is valid. Possible choices:
    - **Make screenshots for any applications and resources**;
    - **Make screenshots for applications and resources from list**;
    - **Not to make screenshots for applications and resources from list**.

> **Important!**
>
> To receive screenshots, it is also necessary that you should set up sending screenshots in the **Settings to send data to products** section (by default, sending screenshots is enabled).
>
> If the rule specifies that screenshots should be taken, however, sending screenshots is disabled in the **Settings to send data to products** section, then screenshots will not be sent. For details, see "Settings to Send Data to Products".

To specify applicaitons and resources, click  (see "Application protocol" and "Resources").

> **Warning!**
>
> The System verifies if the resource being visited by a user matches the one in the list of resources only if one of the following browser is used:
>
> - Chrome
> - Yandex.Browser
> - Mozilla Firefox
> - Edge (Chromium)
> - Opera
> - IE

> **Important!**
>
> On worstations running RED OS, only the **Make screenshots for any applications and resources** option is available. Lists of applications and resources are not supported.

4. In **Screenshots frequency** field specify the periodicity of screenshots creation:
   - **Every n seconds**;
   - **When active window / tab change**.
5. If required, specify the screenshots quality settings: see "Application Control and screenshots".
6. Define the period of rule action. By default, the rule is always in effect (the **Always** option is checked). To specify the rule duration, clear the **Always** check box and specify dates and time in the **From** and **To** fields.
7. When all parameters are configured, click **Save**.

> **Warning!**
>
> Screenshot is created during 5 seconds after the active window is changed. If changing the active window happens faster than one time every 5 seconds, then a screenshot will not be created.

> **Warning!**
>
> Configurations applied in the rules ScreenShot Monitor and Keyboard Monitor are independent and do not influence each other. Therefore, when creating screenshots the System does not consider possible overlap of the attributes and lists of applications and resources in the two rules. For example, if the option **Create screenshot of active window only** is disabled in ScreenShot Monitor rule, then the information from the applications and resources excluded in Keyboard Monitor (but not in ScreenShot Monitor rule) rule can appear on screenshots.

> **Note:**
>
> See more information about how the System prioritizes the rules when making screenshots in the article "Defining priorities of rules when making screenshots according to ScreenShot Monitor rule".

Statistics Rule

To collect statistics on actions of persons with files/folders, you need to configure settings in Device Monitor. For this, you can use the Device Monitor rule for Statistics. The **Statistics** interceptor allows you to collect statistics about user activity and actions with files/folders on monitored computers.

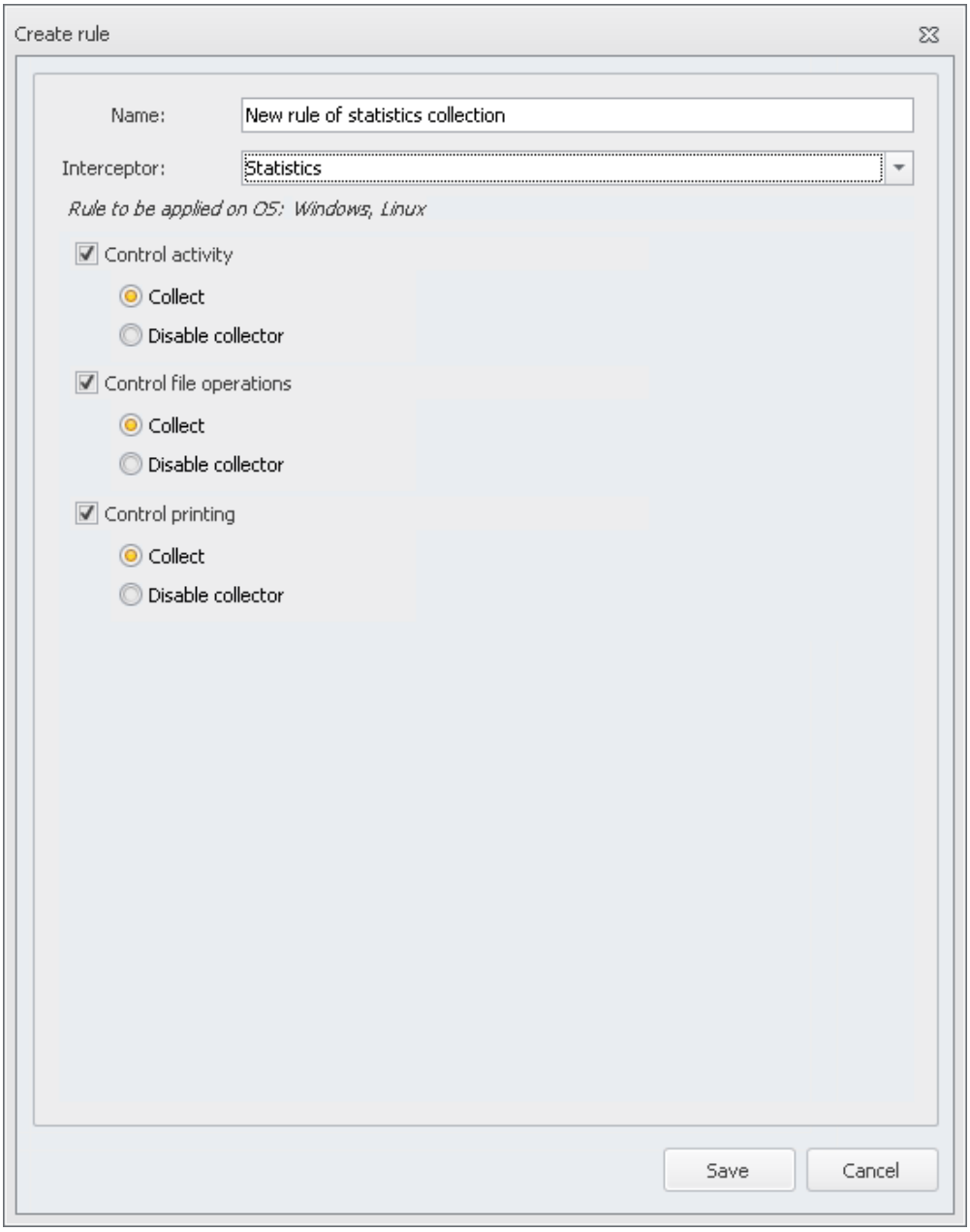
Note:

The rule applies on computers with Windows OS and supported Linux family operating systems.

Important!

The functionality is for InfoWatch Activity Monitor and InfoWatch Prediction only.

The rule applies starting from Device Monitor version 7.6.0. Herewith the rule works if the version of Agent is not earlier than the version of Device Monitor server.



You can select which type of statistics to collect according to this rule. For example, to collect statistics on user activity and not to collect statistics on file operations. If the parameters **Control activity** / **Control file operations** / **Control printing** are not selected, then these types of statistics are not collected.

Activity control

The System controls the following operations of user in the System:

- Entering the session (local, remote)
- Exiting the session (local, remote)
- Blocking the session (local, remote)
- Unblocking the session (local, remote)
- Running the application
- Stopping the application
- Getting focus of the application active window
- Losing focus of the application active window

- Getting focus by the browser tab. The following browsers are supported:
  - Chrome
  - Yandex.Browser
  - Mozilla Firefox
  - Edge (Chromium)
  - Opera
  - IExplore
- Web search events. The following browsers are supported:
  - Google
  - Yandex
- Events of using a mouse and keyboard

Note:

The statistics on using a mouse and keyboard is created every 15 minutes (the value cannot be changed) or when the focus of active window changes. If no action has happened within the 15 minutes period, then the event is not created.

If user keeps a button pressed and then stops, the Agent generates many events of pressing the button and one event of releasing it.

Note:

The System controls the following operations of user on Agents with RED OS:

- Entering the session (local)
- Exiting the session (local)
- Blocking the session (local)
- Unblocking the session (local)
- Getting focus of the application active window
- Losing focus of the application active window
- Events of using a keyboard
- Getting focus by the browser tab (for the browser Edge (Chromium)

Note:

- If URL address was changed (without applying changes using **Enter** or cancelling changes using **Esc**), then the event of switching a browser tab is created on Agents, operating on RED OS.
- If a website was added to favorites, then an event of switching tabs is created on Agents, operating on RED OS.
- If URL address was changed, then a number of events of switching the browser tab may be created on Agents, operating on RED OS.
- The event of *Exiting the session (local)* on RED OS may not be created in the following cases:
  - Workstation was restarted/shut down with the **Restart**/**Shut down** buttons of the **Start** menu.

- Workstation was restarted/shut down using the console with the commands shutdown, reboot, etc.

File operations control

Collecting statistics on files operations is performed on:

- Computer
- Removable devices
- Network devices
- Terminal session

Important!

Collecting file statistics is not supported for FTP, HTTP, Cloud Storage.

The System controls the following operations:

- Creation of file
- Opening of file
- Renaming of file
- Relocation of file/folder
- Copying of file/folder
- Deletion of file/folder
- Relocation of file/folder to recycle bin
- Recovery of file/folder from recycle bin
- Deletion of file/folder from recycle bin

Note:

- If the operation of copying/deleting/moving file was initiated and then cancelled, the event may still be created.
- If Agent is started after user logged in, then for this user no event of *Entering the session* is created, only the event of *Exiting the session/Blocking the session* is created.
- If several users logged in to a workstation, then when the workstation is turned off/ restarted, the event of *Exiting the session* will be created only for the user that logged in first.
- If "ScreenShot Control Monitor Rule" and collecting statistics are configured at the same time, then when user presses the **Print Screen** button, only the event for releasing the button will be created.
- The events of getting/losing focus for UWP applications (Universal Windows Platform) may not be created.
- For events with websites and web search the attribute *site* may have the value "about:blank", if the URL does not correspond to the site domain or IP address.
- If the System cannot define the original file name when deleting it from a recycle bin, then the file name displayed in the bin will be specyfied in the event. The original file name is the one it has before being moved to recycle bin (if OS changes the file name while moving there).
- Events for subfolders and empty folders are not created.

Example:
A folder contains 4 files and a subfolder with 2 files. When user works with the parent folder, an event for this parent folder and 6 events for the files will be created. No separate event for the subfolder will be created.

Printing control

The System collects statistics for the following printer types:

- Local
- Network
- Terminal

Important!

Printing control is supported on Agents running Windows OS only.

The System collects the number of copies of a document sent for printing as well as the number of pages for each copy.

Note:

The number of copies might sometimes not be detected precisely.

To configure the rule:

1. On Device Monitor Management Console, select the section **Policies**.
2. Open **Create rule** window (see "Adding Rule").
3. In **Name** field, specify the rule name.
4. In **Interceptor** field, select **Statistics**.
5. Select **Control activity** to activate user activity collection (enabled by default).
6. Specify if the System should **Collect** the data or **Disable collector** (enabled by default).
7. Select **Control file operations** to activate the control of user activity with files (enabled by default).
8. Specify if the System should **Collect** the data or **Disable collector** (enabled by default).
9. Select **Control printing** to activate the control of files sent for printing by user (enabled by default).
10. Specify if the System should **Collect** the data or **Disable collector** (enabled by default).
11. Click **Save**.

Important!

Rules of security policies created for a computer and employee are combined. The rules with different types of statistics and paremeters of enabling/disabling are combined too. If in one rule you have control of activity enabled and in the other the control of operations with files enabled, then both rules will be applied on this computer and the System will control user activity and their actions with files.

Select **Disable collector** if you need to forbid collecting statistics (for example, for a certain group of persons of computers). Herewith, in the resulting rule the collecting will be forbidden because all the rules for persons and computers are combined and the rule that has this parameter disabled prevails over others.

Example 1

Collecting statistics is enabled for a group of computers. But, if a person from a group for which the collecting of statistics is disabled logs in on a computer of the group, then the events will not be created.

Example 2

A number of rules are configured for a user.

In the rule 1

- Control of activity is activated
- Collection of activity is enabled
- Control of operations with files is not activated

In the rule 2

- Control of user activity is disabled
- Control of file operations is enabled
- Collecting of statistics with files is disabled

In the rule 3

- Control of activity is activated
- Collecting of activity is enabled
- Control of operations with files is activated
- Collecting of operations with files is enabled

In the resulting rule, collection of statistics on user activity will be performed on this computer, and file statistics will not be collected on this computer.

For more information on Device Monitor security policies, see "Security Scheme Setup".

How to configure collecting of file statistics, see the section "File Statistics".

Note:

File size is defined after an application has finished working with the file (at the moment of an event creation). For operation of file deletion, its size is defined at the moment of the file opening.

The data of the file size is received from the context of the file object. If the System cannot receive the data, the value of the file size will be 0. The events will not be created for original files that have the size 0.

Important!

On versions of Agents earlier than 7.6.0 the rules of collecting statistics will be operating only for computers. The rules created for a group of employees will be ignored.

Applying Rules

The event satisfies a rule if all conditions of the rule are satisfied.

If the event matches several rules at a time, then the rule priority is determined as follows:

1. An excluding rule (the **Exclude from interception option** is available for File Monitor rule) has the highest priority.
2. A full access rule overrides the forbidding one, while the forbidding rule overrides the permission to read-only and to access encrypted devices.
   Example 1. *Allowed to use* rule for Device Monitor overrides *No access* restriction, which overrides on its part the rule permitting *Read only*, the one that is accordingly more preferred than a rule with *Full access to encrypted devices* option.
3. *Example 2*. If there are several HTTP(S) Monitor rules, then a rule with the *Do not intercept requests to internal resources* is superior to the same rule without this option.
4. The rule where the **Create a shadow copy** option is selected overrides a rule without shadow copies.

See also:

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

Creating shadow copies and blocking operations due to space problems

A shadow copy of a file, document, message or chat is created when the following conditions are met:

1. A rule which applies to the file enables creating shadow copies and the file size is within the specified range.
2. There is more free space on the controlled computer than the value specified in the **Free clients' disk space** parameter (see "General Settings for Agents"). The default value is 10%.
3. There is more free space on the controlled computer than it is needed to create a shadow copy.

> **Note:**
>
> If a rule enables shadow copying, but there is less free space on the computer than it is defined by the policy or than it is needed to save the file, then the event will be created without a shadow copy. Such events are displayed in the Management Console with the *Error of copy creating* state (see "Viewing Events").

> **Warning!**
>
> Shadow copies for printing files exceeding 512 Mb **cannot** be made.

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

- Device Monitor Agent has not connected with Device Monitor Server for a long time and has than 30000 events
  and
- in common settings for agents the **If there is not enough disk space to save shadow copy, the operation will** parameter has the **Operation is blocked** value,

then any employee's actions controlled by the current security policy will be blocked.

Device Monitor Rules Application

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

Employee access rights are defined based on:

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

When the Agent is installed, controlled devices are fully accessible by default. Therefore, all forbidden operations with the device must be set explicitly as DM rules.

Each newly registered computer is added to the Default group. This group has a "Shadow copy policy" which contains no rules. Rules regulating access to devices are not defined for employees by default. Thus, the System always allows access to all controlled devices after the installation.

Example:
There is a rule that prohibits writing to CD/DVD drive to members of *A* computer group. A computer *PC* belongs only to the group *A*. Employee Smith belongs only to the employee group *B* with no device rules and his computer belongs to the group *A*. Employee Smith tries to view a CD on the computer *PC*. In this case, the employee won't be able to view CD contents of the disk or write new data to it.

You can assign multiple rules, in the same or in different policies, with various access levels to the same device. In this case, a rule which is allowed to use is superior to other rules (see the table below).

Device type	Access in descending order of priority
All devices, except CD/DVD, Floppy drives, and removable storage devices	1. Allowed to use 2. Using is prohibited
CD/DVD	1. Allowed to use 2. No access 3. Read-only
Floppy drives and removable storage devices	1. Allowed to use 2. No access 3. Read-only 4. Full access to encrypted devices only
Cloud storages	1. No access 2. Read-only 3. Allowed to use

Example:

> There is a rule for the employee group *E* that allows read-only access to a removable storage device. There is a rule for the employee group *F* that grants full access only to encrypted removable storage devices. An employee Smith who belongs to both groups can only get read-only access to both encrypted and not encrypted devices (the rule with a lower priority is not applied at all).

For some types of devices controlled by Device Monitor interceptor, rules can overlap (see the table below). Please, keep it in mind when configuring access to a controlled device.

Rule	Overlapping rules	Notes
Floppy	No	
CD/DVD	No	
Parallel port (LPT)	Local printer (LPT) Imaging devices (LPT)	If there is no access to LPT port, the device connected to this port will be unavailable
Serial port (COM)	Modem Local printer (COM) Imaging devices (COM)	A modem connected to COM port is only accessed basing on COM port rule If there is no access to COM port, the device connected to this port will be unavailable
Removable Storage (USB and IEEE 1394 devices)	FireWire (IEEE 1394)	If there is no access to FireWire (IEEE 1394) port, the device connected to this port will be unavailable
Local Printer (with USB, IEEE 1394, SCSI connection, etc.)	FireWire (IEEE 1394) Serial port (COM) Parallel port (LPT)	If there is no access to FireWire (IEEE 1394), COM, LPT port, the device connected to this port will be unavailable
Image-processing Devices (cameras, scanners)	FireWire (IEEE 1394) Serial port (COM) Parallel port (LPT)	If there is no access to FireWire (IEEE 1394), COM, LPT port, the device connected to this port will be unavailable
Bluetooth Device	No	
IrDA Device	No	
Other USB Devices	No	
FireWire	Removable storage device (IEEE 1394) Local printer (IEEE 1394) Imaging devices (IEEE 1394)	If there is no access to FireWire (IEEE 1394) port, the device connected to this port will be unavailable
Modem	Serial port (COM)	Modem access rules do not affect modems connected to COM port. A modem connected to COM port is only accessed basing on COM port rule
Smart Card Reader	No	

Rule	Overlapping rules	Notes
Tape Device	No	
Multifunctional Device	No	
PCMCI device	No	
USB Network Adapter	MTP-compatible device	When a mobile device is connected to the computer, it can be treated either as an MTP device or as a USB network adapter
Pocket Computer (Windows Mobile and Palm OS pocket computers)	No	
MTP-compatible device	USB Network Adapter	When a mobile device is connected to the computer, it can be treated either as an MTP device or as a USB network adapter

Configuring Device Monitor Rules to Collect Statistics and Intercept Events

Important!

Statistics data can be used by InfoWatch Activity Monitor and InfoWatch Prediction.

To enable collecting statistical events by means of InfoWatch Device Monitor, configure the following rules in InfoWatch Device Monitor Management Console:

- Keyboard Monitor Rule
- ScreenShot Monitor Rule
- Statistics Rule

Note:

Intercepting statistics on keyboard events and interception of keyboard typing are different events that are configured and can work both separately and together. Collecting statistics on keyboard events is needed for calculating active working time of the user. Keyboard typing events are needed to intercept the text being typed.

Statistical events collected by Device Monitor:

- User session events:
  - Entering the session (local, remote)
  - Exiting the session (local, remote)
  - Blocking the session (local, remote)

    - Unblocking the session (local, remote)
- Events of working in the application:
    - Running the application
    - Stopping the application
    - Getting focus of the application active window
    - Losing focus of the application active window
- Events of working in the browser;
    - Getting focus by the browser tab
- Web search events
- Events of using a mouse and keyboard
- File actions

Important!

For RED OS only the following statistical events are collected:

- Entering the session (local)
- Exiting the session (local)
- Blocking the session (local)
- Unblocking the session (local)
- Getting focus of the application active window
- Losing focus of the application active window
- Events of using a keyboard

In rare cases to shut down or restart the workstation using the shut down or restart buttons may end in loss of the event - local exit of session.

To shut down or restart the workstation using the commands (shutdown, reboot, etc.) in OS management console will in most cases end in loss of the event - local exit of session.

Important!

If control of network connections (traffic interception) is disabled in Device Monitor, then browser events are treated as follows: the System gets events of getting focus by the browser tab and does not get web search events.

Employees

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

Warning!

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

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

Guidelines on account management is available in:

- Viewing Employee Details;
- 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 Scheme.

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:

Property	Description
Account	Account name
Last Name	Account owner's last, first and middle name.
First Name	
Middle Name	
Sid	Account identifier **For MS Windows workstations**: • Device Monitor gets account data from the operating system. • Getting SID for a domain account from Active Directory is supported.

Property	Description
	For Linux workstations: • Getting SID for a domain account from Active Directory is supported only if all the following conditions are met: • The workstation is running RED OS (SID may be determined incorrectly on workstations running other operating systems). • The workstation joined an Active Directory domain using SSSD (System Security Services Daemon). • If it is not possible to get SID for a domain account, Device Monitor identifies the account as local.

Warning!

Getting domain SID from Active Directory on Linux workstations is supported from version 7.8.0:

- Device Monitor version lower than 7.8.0 identifies domain account as local account.
- After updating Agent to version 7.8.0 or higher:
  - For accounts that were identified as local before the update, a domain SID can be determined. If there is no employee with this SID in the System, a new employee will be added.
  - If a domain SID is determined on a workstation, the rules that are configured for the employee with the domain account will be used.

Note:

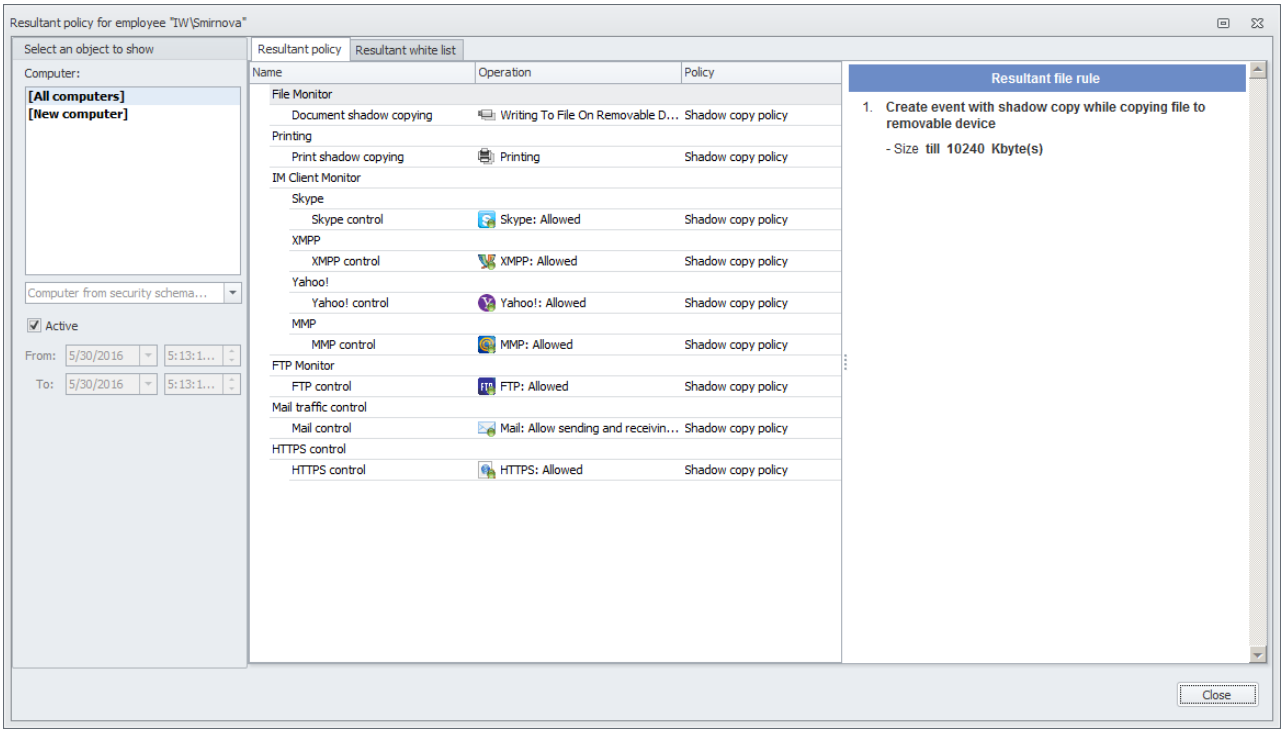
Some information on **Details** panel is duplicated in the main screen workspace.

Viewing Resultant Policy (DM) and Resultant White List for an Employee

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

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

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



The main window **Resultant policy for employee <computer name>** area contains two tabs:

- **Resultant policy** displays the rules (DM) that are resultant on a computer. Resultant policy (DM) consists of rules (DM) configured by default, rules (DM) applied to this computer and rules (DM) for computer users (see "Device Monitor Rules 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 a computer (see "White lists"). To see detailed information about a device, select it from the list: detailed information will be displayed on the panel on the right.

On the **Computer** panel, you can choose an object to view:

- **All computers** object displays the resultant policy (DM)/white list for an employee regardless of a computer.
- **New computer** object displays the resultant policy (DM) for an employee on a new computer, which is not yet present in the security scheme.
- To see the resultant policy (DM) for a chosen user on a definite computer:
    - From **Computer** list, choose the name of the computer on which the chosen account is registered

  or
- From **Computer from seciruty scheme** drop-down list, choose any account which is registered with the System (see "Computers").

You can choose time period for a resultant policy/white list:

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

Adding and Editing an Employee Group

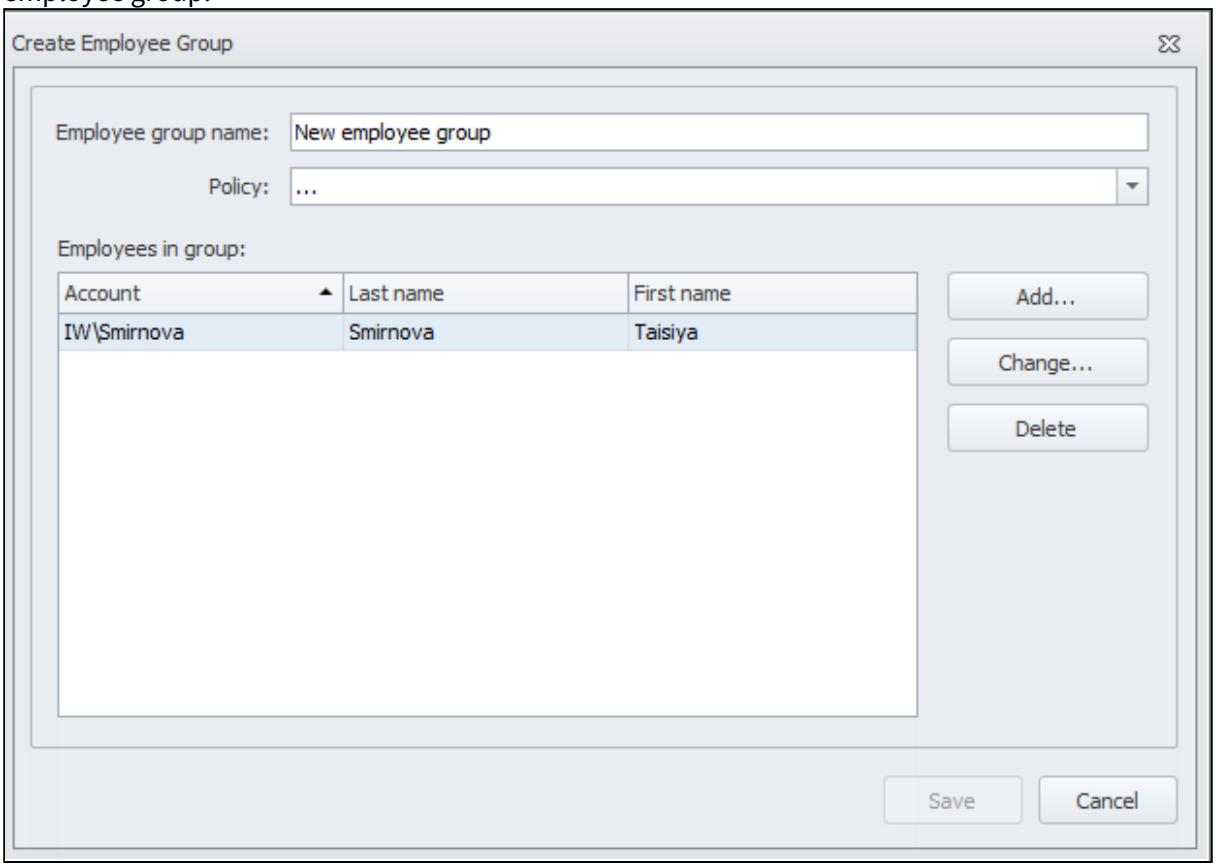
To add or edit an employee group:

1. Go to **Employees** section.

2. Take one of the following steps:

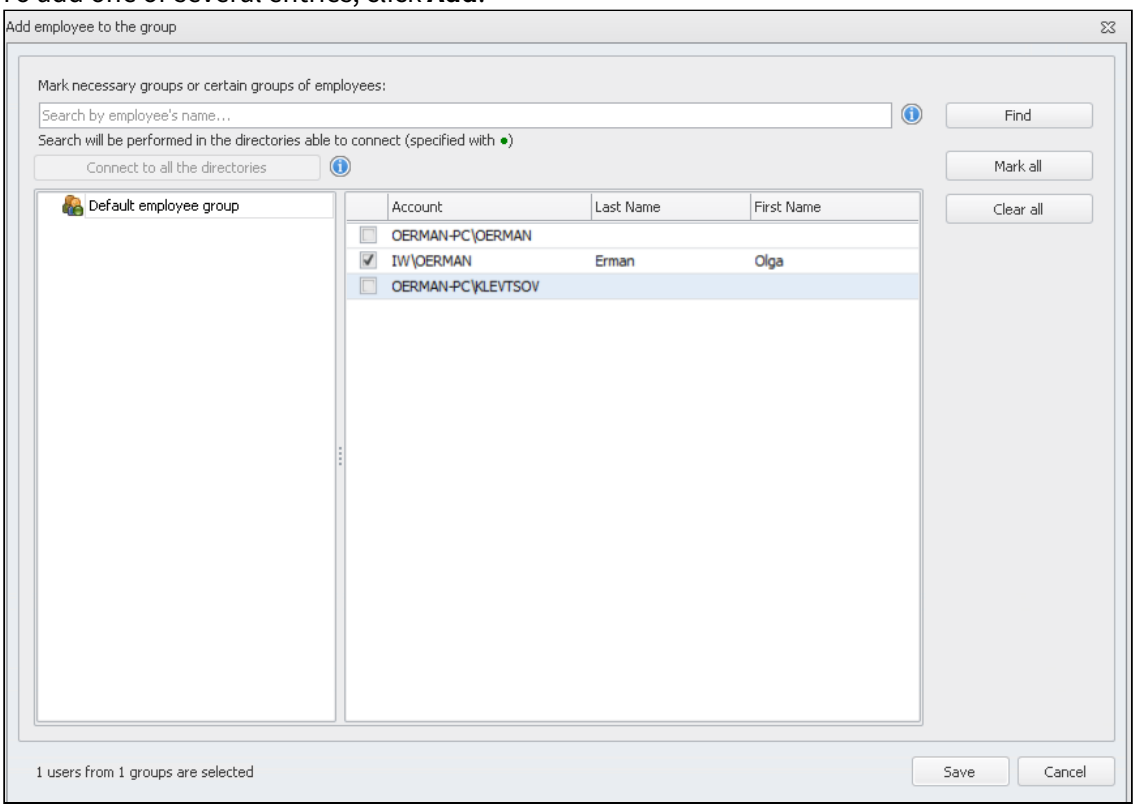
Action	Steps
Add an employee group	• Select **Edit** > **Create Employee Group** in Main Menu; • Click **Create Employee Group** at the top of Navigation panel.
Edit an employee group	a. In **Employees** area of Navigation panel select the employee group name. b. Take one of the following steps: • In Main Menu, click **Edit** > **Edit Employee Group**; • Click **Edit Employee Group** at the top of Navigation panel; • Double-click the selected employee group name.

As a result of any of these actions, a dialogue window will appear to define parameters of the employee group.



3. Specify the following parameters:
   - **Employee group name**. Name of the employee group.
   - **Policy**. From the drop-down list, choose a security policy 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** dialogue displays a list of accounts imported from directory service (see "Active Directory Connecting and Synchronizing") and already registered with 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 group tree, then flag accounts you want to add to the edited group. To flag all accounts of the 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 have selected all needed accounts, click **Save** to close **Add employee to the group** dialogue and return to the dialogue 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 scheme, 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 Main Menu;
    - Click **Delete Employee Group** at the top of Navigation Panel;
    - Right-click the group and select **Delete** in the context menu;
    - Press **Ctrl+D**.
4. Click **Yes** in the confirmation box to confirm that you want to remove the employee group.

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.

Adding Employee Account to a Group

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

To move employee account from one group to another:

1. Go to **Employees** section.
2. In **Employees** area of Navigation panel, select a group containing the 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 panel. Move the cursor over the name of the group you want to add the account to. When a yellow arrow appears at the left of the selected group, release left mouse button.

This adds the account to the selected group.

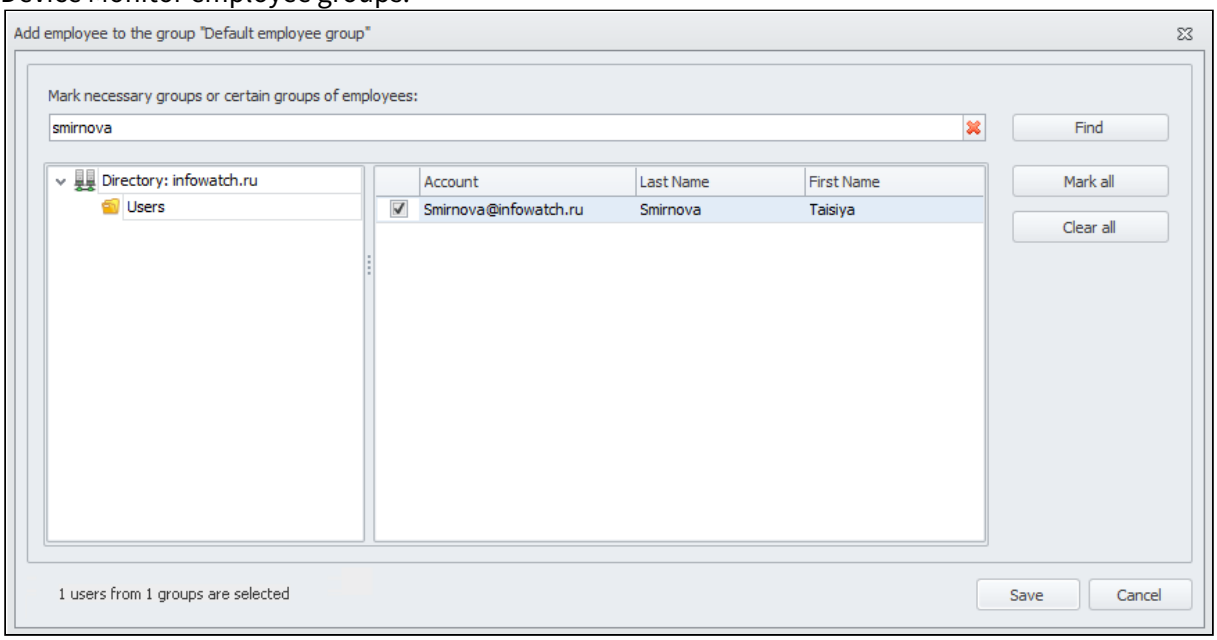
You can also manually import information on the employee from directory service (see how to configure connection in "Active Directory Connecting and Synchronizing"). After this employee is registered at the workstation where InfoWatch Device Monitor Agent is installed, this employee will be subject to the policy of a group where the employee is added to.

To add one or several accounts to employee group:

1. Go to **Employees** section.
2. In **Employees** area of Navigation panel, select a group to which you want to add the employee's account.
3. Take one of the following steps:
    - In 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 directory service (see "Active Directory Connecting and Synchronizing") and already registered with 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 the group tree, then flag the accounts you want to add to the edited group.
   To flag all accounts of the 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 the account name to the field at the top and click **Find**.
5. After you select all accounts, click **Save** to close **Add employee to the group** dialog and return to the dialog box with group parameters.
6. Click **Save**.

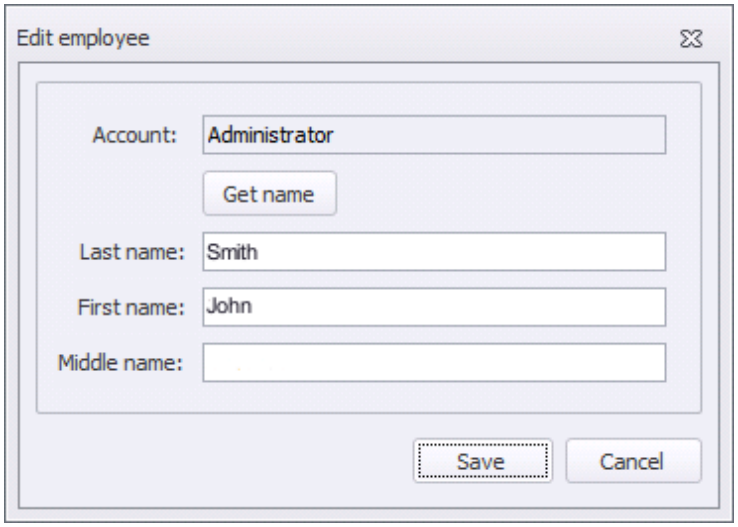
> **Warning!**
>
> To apply changes, you have to save current security scheme (see "Editing Security Scheme"). If you don't save your security scheme, all changes will be discarded.

Editing Employee Account

Parameters of an employee account can be imported from directory service or while installing InfoWatch Device Monitor Agent 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 panel, 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 Main Menu, click **Edit** > **Edit Employee**;
   - Click **Edit Employee** at the top of **Employees** area;
   - Double-click the selected row.



5. In **Edit employee** dialog 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 scheme, 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 the Navigation panel, select the 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 employees' accounts you want to exclude from this group. To select multiple rows, use **Shift** or **Ctrl**. To select all rows, press **Ctrl+A**.

4. Take one of the following steps:
   - In Main Menu, click **Edit** > **Remove employee from group**;
   - Click **Remove employee from group** at the top of **Employees** area;
   - Right-click the row and select **Remove employee from group** in the context menu;
   - Press **Delete** keyboard button.

This removes the employee account from the selected employee group.

> **Note:**

If an employee account belongs to a single employee group, it will be automatically added to "default" employee group after exclusion.

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.

Deleting Employee Account from Security Scheme

To remove an employee account from security scheme:

1. Go to **Employees** section.
2. In **Employees** area of Navigation panel, select the 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 scheme, select all rows that contain the accounts you want to remove.

4. Take one of the following steps:
   - In Main Menu, click **Edit** > **Delete employee from security scheme**;
   - Click  **Delete employee from security scheme** at the top of **Employees** area;
   - Right-click the row and select **Delete employee from security scheme** in the context menu;
   - Press **Shift+Delete**.
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 scheme (see "Editing Security Scheme"). If you don't save your security scheme, all changes will be discarded.

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 can be applied only to a computer group. You can define a security policy for a certain computer by including it to a computer group.

Warning!

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

To go to the Management Console section where you can manage computers, click **Computers** button on Navigation panel.

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 Scheme;
- Updating Agents on Managed Computers;
- Diagnostics;
- Updating Statuses of Agents on Managed Computers;
- Setting "Golden image" status on Agent.

Viewing Computer Details

Computers area of Navigation panel 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 panel.

Information on computers is displayed as a table. The table columns contain basic properties of the computer. You can adjust the order of columns and hide columns you do not need.

The table contains the following basic information:

- **Name**. Domain name of the computer.
- **Status**. Agent status. This parameter may have the following values:
  - **Not specified**. Agent has never been installed on the computer, it was added to the security scheme.
  - **Specifed**. Agent was installed via primary distribution task or a computer with Agent was added to the security scheme.
  - **Stopped**. Agent is installed. Stopped via DM console.

    Note:

    If stopped agent is updated, it will be started after the update.

    - **Works in diagnostic mode**. Agent is installed. A diagnostic mode is enabled via DM console.
    - **Golden image**. Agent is specified. "**Golden image"** status is set.
    - **Removed**. Agent is removed via primary distribution task or using tools of the computer.
- **Agent activity**. Activity status of Agent. This parameter may have the following values:
    -  **Active**. Agent regularly connects to the server and transfers data.
    -  **Inactive**. Agent does not regularly connect to the server or it is disabled.
    -  **Inactive for more than a week**. Agent does not connect to the server over a week.
    -  **Inactive for more than a month**. Agent does not connect to the server over a month.

User can configure parameters of Agent activity statuses (see details in the article "Setting Activity Status of Agents").

- **Registered**. Date and time when computer was added to the database.
- **Established**. Date and time of Agent launch on the computer. If computer has **Not specified** status of Agent, **Agent not specified** will be displayed.
- **Last check-in**. Date and time of computer Agent's last access to the Server. If computer has **Not specified** status of Agent, **Agent not specified** will be displayed.
- **Scheme version**. Agent's current security scheme 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.

> **Note:**
>
> User is not displayed for workstations running Linux.

> **Note:**
>
> Workstation comment is to be saved immediately while editing with no changes within security scheme. Thus, the following restrictions should be taken into consideration:
>
> - When changing a comment on an exisiting workstation, the comment is stored immediately in the database even if security scheme is being edited;
> - When changing a comment on a newly added workstation, the comment is saved only when security scheme is saved.

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:

- **Settings version**. Common security policy settings version number (see "General System Settings").
- **Template version**. Version of templates for notifications to be displayed to employees.
- **Version of network control configuration**. Data transmission through network connections with the help of Network Monitor control version (see "Corporate Network Control").

- **Configuration version of network applications control**. Version of network traffic control configuration using protocols YMSG,XMPP, MMP, FTP, FTPS, SMTP/S/MIME/Outlook/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.
- **Version of TM configuration**. The last version of TM configuration that was delivered to the workstation.
- **Free disk space on computers**. Free space size on disks, where shadow copies are saved (also in percentages).

> **Warning!**
>
> If there is at least one valid rule that allows shadow copying, and there is less free space on the host drive than specified by the policy (see "Creating shadow copies and blocking operations due to space problems"), no data will be printed or written to removable media: even if these steps aren't covered by any rule.

> **Warning!**
>
> If Agent sends an event to Device Monitor server, Agent deletes the event data from the disk.
>
> In some cases, data deletion is not supported on Agents running Linux OS. The file with event metadata may remain on the Agent disk even if Agent has sent the event.

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

Each registered workstation is automatically added to "default" workstation group. At the same time, "default" workstation group security policy is assigned to the new workstation.

You can do the following as you work:

- Manage 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 scheme;
  - Update Agents on managed computers.

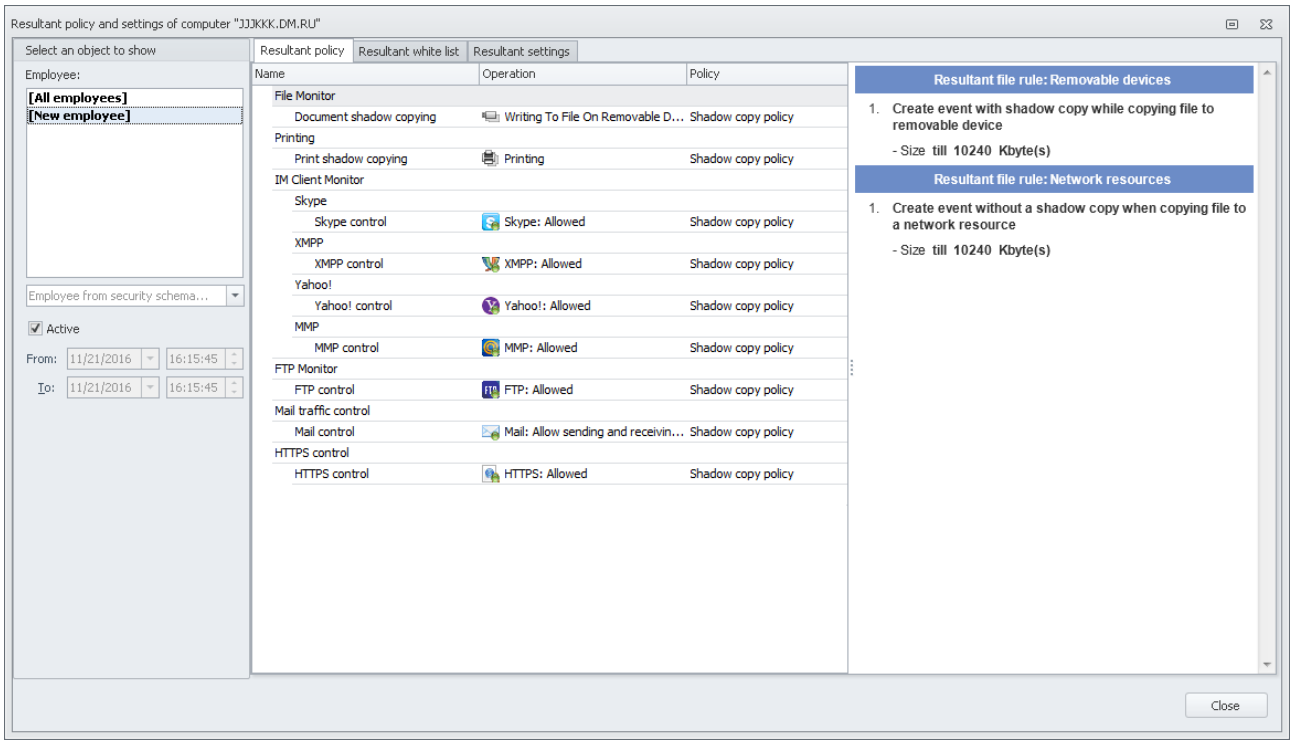
Viewing Resultant Settings, Policy and Resultant White List for Computer

To view information about settings, policy and white list 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 resulting policy for all employees on the chosen computer is displayed.



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

- **Resultant policy** - rules are displayed, that are resulting on the computer. Resulting policy consists of rules, configured by default, rules, applied for this computer and rules for computer's users (see "Device Monitor Rules Application"). To see detailed information about a rule, 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 a new employee (which is not yet registered in security scheme) are displayed.
- To view resulting policy\white list\settings for a specific 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:

- by default, **Active** setting is enabled, and current resultant policy/white list/settings for an employee are displayed;
- untick **Active** box and specify the period, to view resultant policy/white list/settings for the period.

Adding and Editing a Computer Group

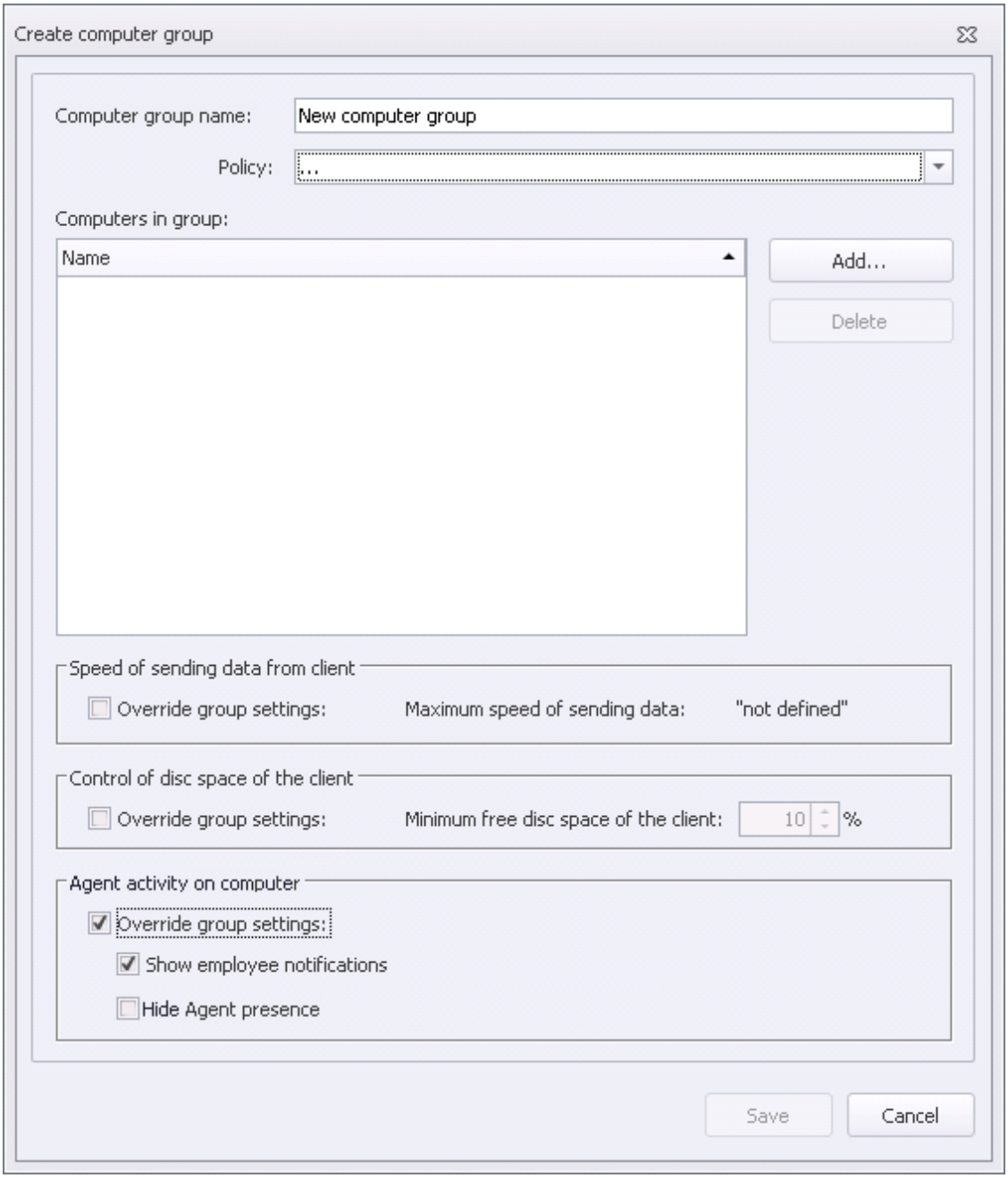
> **Warning!**
>
> When you register a new computer, information on this computer is automatically added to the security scheme (to "default" computer group).

To create a computer group:

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

Action	Steps
Add a computer group	• In Main Menu, click **Edit** > **Create workstation group**; • Click **Create Computer Group** at the top of Navigation panel.
Edit a computer group	a. In **Computers** area of Navigation panel select workstation group name. b. Take one of the following steps: • In Main Menu, select **Edit** > **Edit**; • Click **Edit** at the top of Navigation panel; • Double-click selected workstation group name.

This opens a dialogue box with group parameters.



3. In this dialogue, specify the following parameters:
    - **Workstation group name**.
    - **Policy**. From the drop-down list, select security policy that will be assigned to this computer group.
4. Define a list of computers in a group:
    - To add one or several computers, click **Add**. In **Add computer to the group** dialogue, you can select computers from:
        - Microsoft Windows Network;
        - AD and/or ALD tree;
        - Computers registered with the 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, enter a part of a

computer name to the upper field and click **Find**.
When all needed computers are selected, click **Save**: this closes **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 Agents for computers belonging to the group (configuring a common value is described in "General Settings for Agents", **Limit the speed of sending data** setting). To do this:
   a. In **Speed of sending data from agent** area, select **Override group settings**;
   b. In **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 minimal free disk space (when it is reached on the managed computer, shadow copies would not be created) for computers belonging to the group (configuring a common value is described in "General Settings for Agents", **Minimal free agents' disk space** setting). To do this:
   a. In **Control of disk space of the agent** area, select **Override group settings**;
   b. In **Minimal free agents' disk space** 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 "General Settings for Agents", **Hide Agent presence** 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 scheme, all changes will be discarded.

Deleting Computer Group

To edit or delete computer group:

1. Go to **Computers**.
2. In **Computers** area of Navigation panel, select computer group name.
3. Take one of the following steps:
   - In Main Menu, select **Edit** > **Delete**;
   - Click **Delete** at the top of Navigation panel.
4. In the following confirmation dialogue, 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 scheme (see "Editing Security Scheme"). If you don't save your security scheme, 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 "default" group, the policy assigned to this group will apply. Further on, you can assign security policies 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 panel, 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 panel. 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 a selected computer group.

You can also add information about computers without InfoWatch Device Monitor Agent manually. Computer information is imported from directory service (see connection configuring settings in "Active Directory Connecting and Synchronizing") or your network environment. After InfoWatch Device Monitor installation, this computer (see "Creating Primary Distribution Task") will be affected by the policy of the group it was added to.

Warning!

It is not recommended to add computers with similar names. These computers will be registered with InfoWatch Device Monitor System as a single computer, affected by the same policies, registering the same events, etc.

To add a computer to a group:

1. Go to **Computers**.
2. In **Computers** area of Navigation panel, 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 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 dialogue you can select computers:
   - Received from Microsoft Windows Network;

- From AD and/or ALD tree;
- Among previously registered with the System. For this, type computer name in the search line and click **Find**.

> **Warning!**
>
> Connection or search of a computer is limited by connected directories (marked).

4. Flag computers or computer groups ( ).
   a. Minimized groups are marked with an icon ; expanded – . Double-click a group, to expand or collapse it.
   b. You can also specify computer name in the line at the bottom of the dialogue box. When listing names, separate them with semicolons.
   c. Select **Connect all directories**. Herewith, all directories will be consistently connected after indicating authorization data.
5. Click **Save**.

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

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

Removing Computer from a Group

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

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

To exclude computer from computer group:

1. Go to **Computers**.
2. In **Computers** area of Navigation panel, 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 Main Menu select **Edit** > **Remove Computer From Group**;
   - Click **Remove Computer From Group** 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 scheme (see "Editing Security Scheme"). If you don't save your security scheme, all changes will be discarded.

Deleting Computer from Security Scheme

You can remove a computer from the list of registered computers (for example, computer discontinued operation). Computer can be deleted irrespective of status of Agent. 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 panel, 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 Main Menu, click **Edit** > **Delete Computer From Security Scheme**;
   - Click **Delete Computer From Security Scheme** located at the top of **Computers** area;
   - Right-click computer row and select **Delete Computer From Security Scheme**;
   - Press **Shift+Delete** at the keyboard.
5. In the following confirmation dialogue 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

Важно!

Updating Agents on Astra Linux OS is not supported for the versions earlier than 7.0.

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").

Before starting the update, make sure that the correct new version for automatic update and installation is specified in Device Monitor server settings (for details, see "Device Monitor Server Settings. Connecting to Traffic Monitor Server").

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 information from workstations. You can get diagnostic information via DM Management console. Diagnostic information is requested through DM server, which accesses Agents. TLS protocol with two-way authentication is used for secure connection between server and Agents.

> Agents of versions lower than 7.3 are connected to server through an insecure channel. We recommend updating Agents to the most recent version.

Agent starts collecting diagnostic information if you switch it into diagnostic mode.

To enable diagnostic mode:

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 > Enable diagnostic mode**.

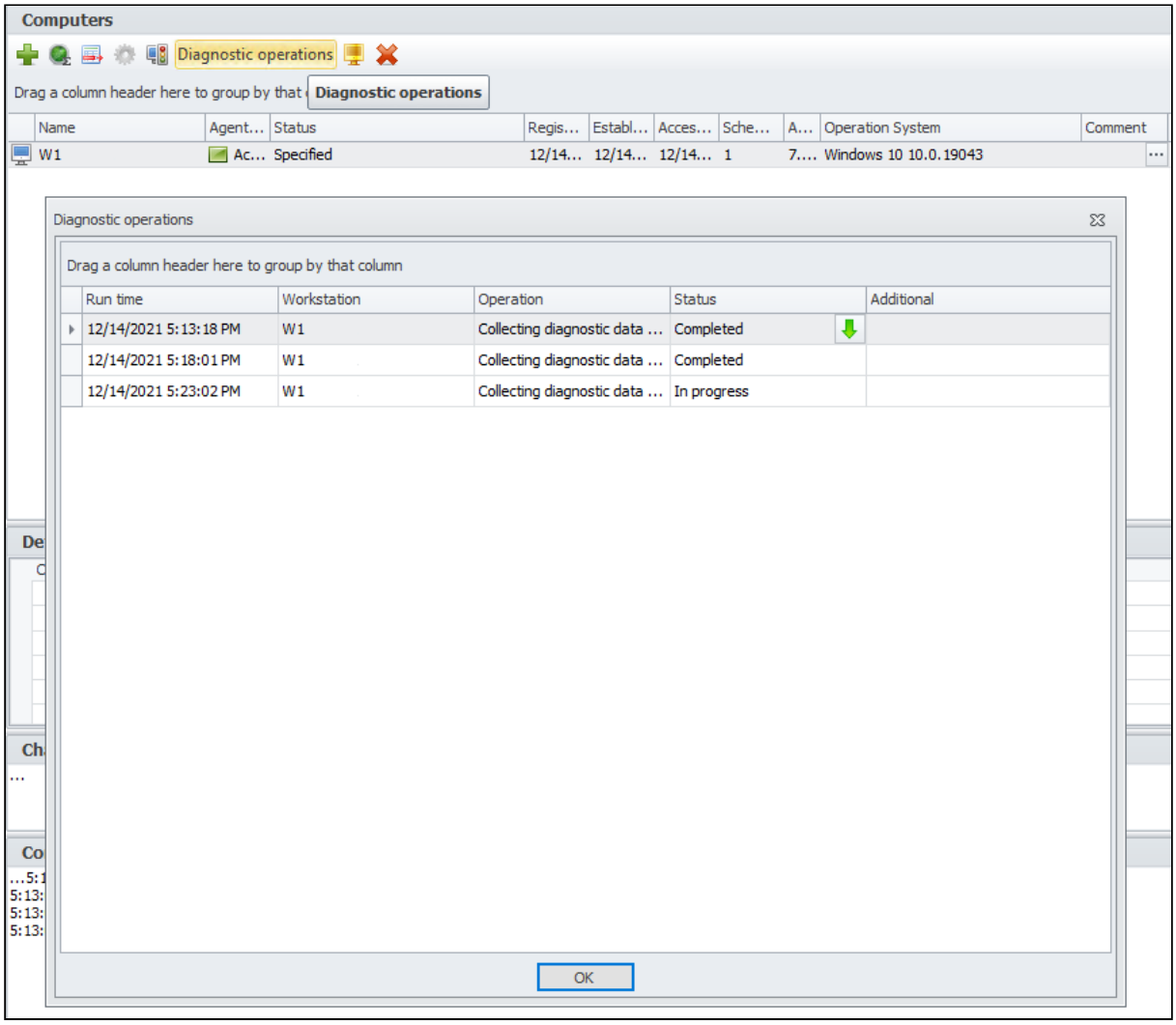
To disable diagnostic mode:

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 > Disable diagnostic mode**.

You can download an archive file with collected diagnostic information.

To get the archive that contains all provided diagnostic information:

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 > Collect diagnostic information**.
4. In toolbar, press **Diagnostic operations.**
   Diagnostic operations window will open, which contains history of diagnostic information requests made during the session.



Collected diagnostic information is stored on server as long as the connection of DM Management console to DM server is active. If the session ends or is interrupted, all collected diagnostic information is deleted for security reasons.

When multiple users are connected at the same time, each user has access only to the information collected in that user's session.

While workstation is collecting diagnostic information, it is not possible to make the same request from a different session.

Before being downloaded from server, diagnostic information is stored in the directory `C:\Program Files\InfoWatch\Device Monitor\Server\AgentLogs`. By default, access to the directory is restricted to:

- user named System;
- users from Administrator group;
- user on behalf of whom the service makes the request to collect information.

5. Wait for status of request to change to **Completed**.
6. To download results of completed request, press .

7. In the opened **Specify a directory to save an archive with the diagnostic information** dialog, specify the directory and the archive name, then press **Save**.

   > Once the archive is saved, it cannot be downloaded again. Diagnostic information collected on the request is deleted from server.

8. To close **Diagnostic operations** window, press **OK**.

> **Note:**
>
> If the status of Agent is **Not specified** or **Removed** then when selecting **Diagnostics**, the System will display the error that Agent is not specified.

> **Note:**
>
> When enabling the diagnostic mode the status of Agent will be displayed as **Works in diagnostic mode**. If user stops the Agent working in this mode, the status of Agent will change to **Stopped**. After resuming the diagnostic mode, the status of Agent will also change to **Works in diagnostic mode**.

> **Warning!**
>
> To change the status from/to **Works in diagnostic mode** and **Stopped** correctly, it is highly recommended to use DM Management console.
>
> If stopping or enabling diagnostic mode is performed on Agent locally via utility, the new status of Agent will not be sent to server. To display the current status, select **Diagnostics** from the menu of DM Management console. In that case the console addresses the Agent directly, receives its current status, records it into the DB and updates within the console itself.

Updating Statuses of Agents on Managed Computers

Statuses of Device Monitor Agents on managed computers can be simply updated by using one button or a key combination.

To update statuses of 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. Take one of the following steps:
   - click **Update statuses** button located at the top of **Computers** area;
   - right-click computer row and select **Update statuses**;
   - press **Ctrl+F5** on the keyboard.

To update statuses of 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. Take one of the following steps:
    - click **Update statuses** button located at the top of **Computers** area;
    - right-click computer row and select **Update statuses**;
    - press **Ctrl+F5** on the keyboard.

Setting "Golden image" status on Agent

Virtualization systems have the option of creating computer's image in order to create new virtual computers (for example, servers of the same type or workstations used for the same type of tasks). The image is a computer that has OS and SW installed. Device Monitor Agent can be installed along with the other SW. Security Officer should manually set "**Golden image**" status on Agent, so the computer with Agent which has this status will not be renamed; and the new computers deployed from it will be registered in the same group with it. The status "**Golden image**" can be set only on Agent with the status **Specified**. "**Golden image**" status can not be set automatically.

There are two ways to set "**Golden image**" status on Agent:

1. Select **Computers** from the left navigation panel of DM Management console;
2. Select the computer on which you need to set the status of Agent "**Golden image**";
3. Click **Set status "Golden image"** on the top pane;
4. Confirm the action by clicking **Yes** in the opened dialog window. "**Golden image**" status is set on this Agent.

or

1. Select **Computers** from the left panel of DM Management console;
2. Right click on the row of the computer on which the status of Agent "**Golden image**" should be set;
3. Select **Set status "Golden image"** from the opened list;
4. Confirm the action by clicking **Yes** in the opened dialog window. "**Golden image**" status is set on this Agent.

Removing "**Golden image**" status from Agent is also possible in either of two ways:

1. Select **Computers** from the left navigation panel of DM Management console;
2. Select the computer on which you need to remove the status "**Golden image**" from the Agent;
3. Click **Remove satus "Golden image"** on the top pane;
4. Confirm the action by clicking **Yes** in the opened dialog window. "**Golden image**" status is removed from this Agent.

or

1. Select **Computers** from the left navigation panel of DM Management console;
2. Right click on the row of the computer on which the status "**Golden image**" should be removed from the Agent;
3. Select **Remove satus "Golden image"** from the opened list;
4. Confirm the action by clicking **Yes** in the opened dialog window. "**Golden image**" status is removed from this Agent.

Warning!

In case there is need to rename the computer with "**Golden image**" status on Agent, the System will operate according to the same scheme, as if a new computer was deployed from it. Thus, its old name of the computer will remain and will be displayed in DM Management console, from where Officer should delete it manually.

If security scheme does not contain the new name registered, then:

- This computer will be registered with the new name, its status of Agent will be **Specified**
- Officer should set "**Golden image**" status on Agent on this computer
- The renamed computer will be added to the same group of security scheme as the one with "**Golden image**" status of Agent.

If the new name has been already registered in security scheme, then Agent will receive the information that computer with this name is registered.

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 Settings, Policy and Resultant White List for Computer".

Note:

You can send information about whitelisted devices to the Platform. For information on how to configure this, see the knowledge base article: "Sending data about devices from DM whitelists to the Platform".

Viewing White List Details

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

Note:

You can make a search in the white list index: type the name of the list in the search box below the index on the Navigation pane.
You can adjust the displaying of the 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 a 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 the 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**.
- **Comment**.
- **Device type**.
- **Category**. Model or instance.
- **Period**. Full access period starting and expiry date and time.
- **Detected on computer**. Name of the computer where the device was detected.
- **Added to database at**. Date of device information submission to the database (see "Adding Device to Database").

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

Adding White List

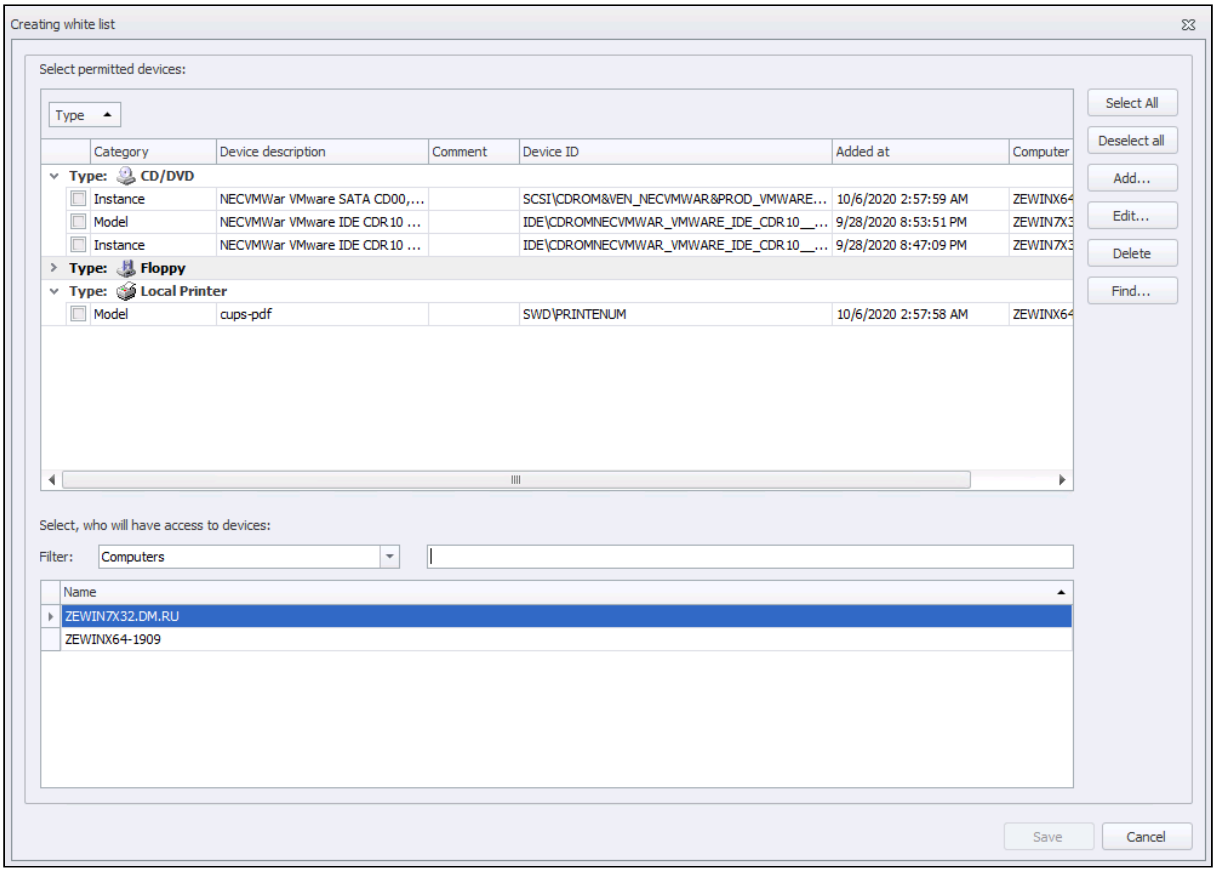
White list affects selected objects: employees, employee groups, computers or computer groups.

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

To add a 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;
   - right-click in the **White Lists** are and select **Create white list** from the drop-down list.

   This opens the **Creating White List** dialog with a table which contains all devices registered in the System.



3. In the table, select models and instances access to which must be unconditionally allowed.

> **Important!**
>
> You can find information on how to modify the list of registered models and device instances in the following sections:
>
> - Adding Device Entry
> - Deleting Device Entry

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

   The list of entries matching the selected filter will appear below.
   You can also use a search string by entering a name or its part.
5. Select the employee / employee group / computer / computer group that will be included in the white list.
6. Click **Save**.

Adding Device Entry

You can add to white lists only device models and instances which were previously registered in the System.

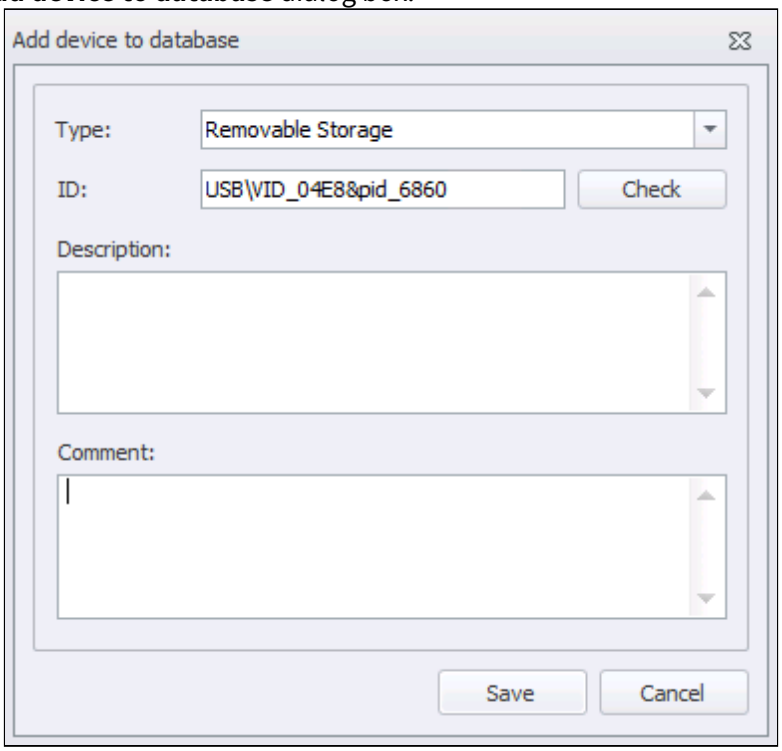
Device information is added in two ways:

- manually (if device ID is provided)

- via the search engine (if the device is connected to the monitored computer).

To add device information manually:

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



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

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

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

> **Warning!**

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

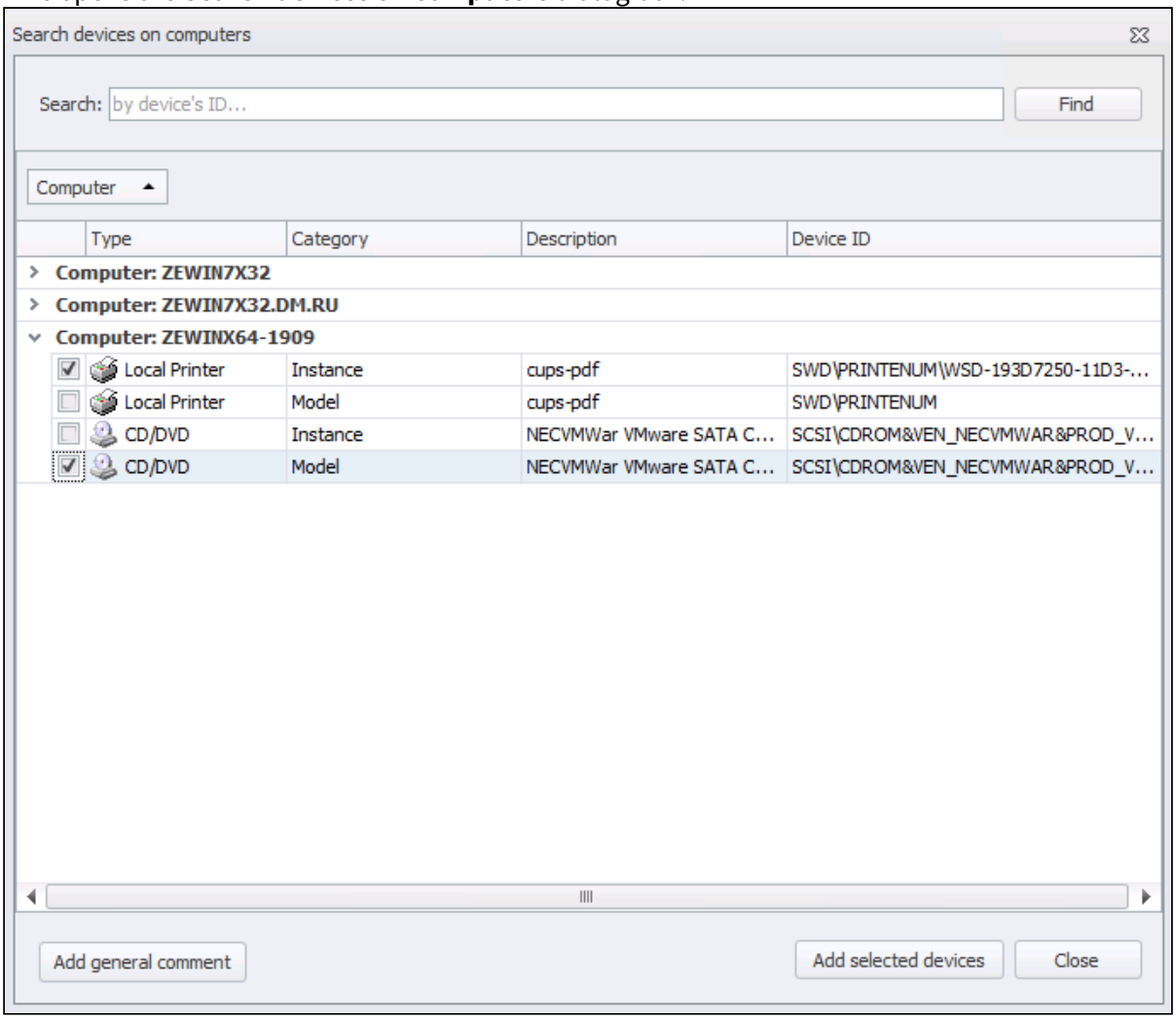
In this case, we recommend using the device model code.

- if necessary, enter the description in the **Description** field.
- if necessary, add a commend to the device in the **Comment** field.

4. Click **Add**.

To add device information by searching for devices connected to monitored computers:

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



Note:

In this window, you can see computers running all supported OS, except OS Astra Linux 1.6 and OS Astra Linux 2.12.

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

   You will see a list of devices that were connected to the selected computer during the time of Device Monitor Agent operation.

   > **Note:**
   >
   > If the computer with Device Monitor Agent was not connected to Device Monitor Server and, during this period, the device was connected and disconnected, then this device will not be on the list.

   > **Note:**
   >
   > For computers running one of the Linux family OS, only USB devices will be displayed.

   > **Note:**
   >
   > Please note that devices connected to the computer are highlighted in white, while disabled devices are greyed out.

4. Select the devices you want to add.

   > **Note:**
   >
   > The **Add general commend** becomes active if you select multiple devices. Clicking this button opens a dialog box where and can specify a common comment for all selected devices.

5. Click **Add selected devices**.

Deleting Device Entry

To remove the entry about a device registered in the System:

1. Open the **Creating White List** dialog box (see "Adding white list").
2. Do either of the following:
   - in the table with registered devices, right-click the selected device instance or model and select **Delete device** from the drop-down menu.
   - press Ctrl+D.
3. In the confirmation window, click **Yes**.

   > **Note:**
   >
   > When deleting a device, a commend added to this device is also deleted.

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.

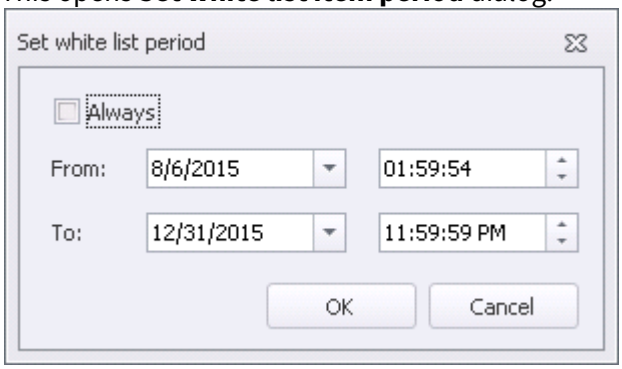
To set white list entry period:

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 parameters of a white list:

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

- Right-click the name of the selected white list and select **Edit** from the drop-down menu;
- Press Ctrl+E.

These actions open **Edit white list <List Name>** dialogue box. This dialogue box is similar to **Creating white list** dialogue box, but **Select, who will have access to devices** area is unavailable.

4. If necessary, you can add or remove devices from the list of devices registered with the System (see "Adding Device to Database" and "Removing Device from Database").
   You can also change the description of a previously registered device: to do this, select the device in the list and click **Edit** at the right of the window. In the window that opens, edit the description text or comment and click **Save**.
5. In the list of registered devices, select or deselect check-boxes to change the list of models and device instances included in the white list.
6. Click **Save**.

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

Deleting White List

To delete a 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 Main Menu;
   - Click **Delete** at the top of Navigation panel.
4. In the confirmation box, click **Yes** to confirm that you want to remove the white list.

> **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.

Signatures

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

To view available signatures:

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

Warning!

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

You can do the following:

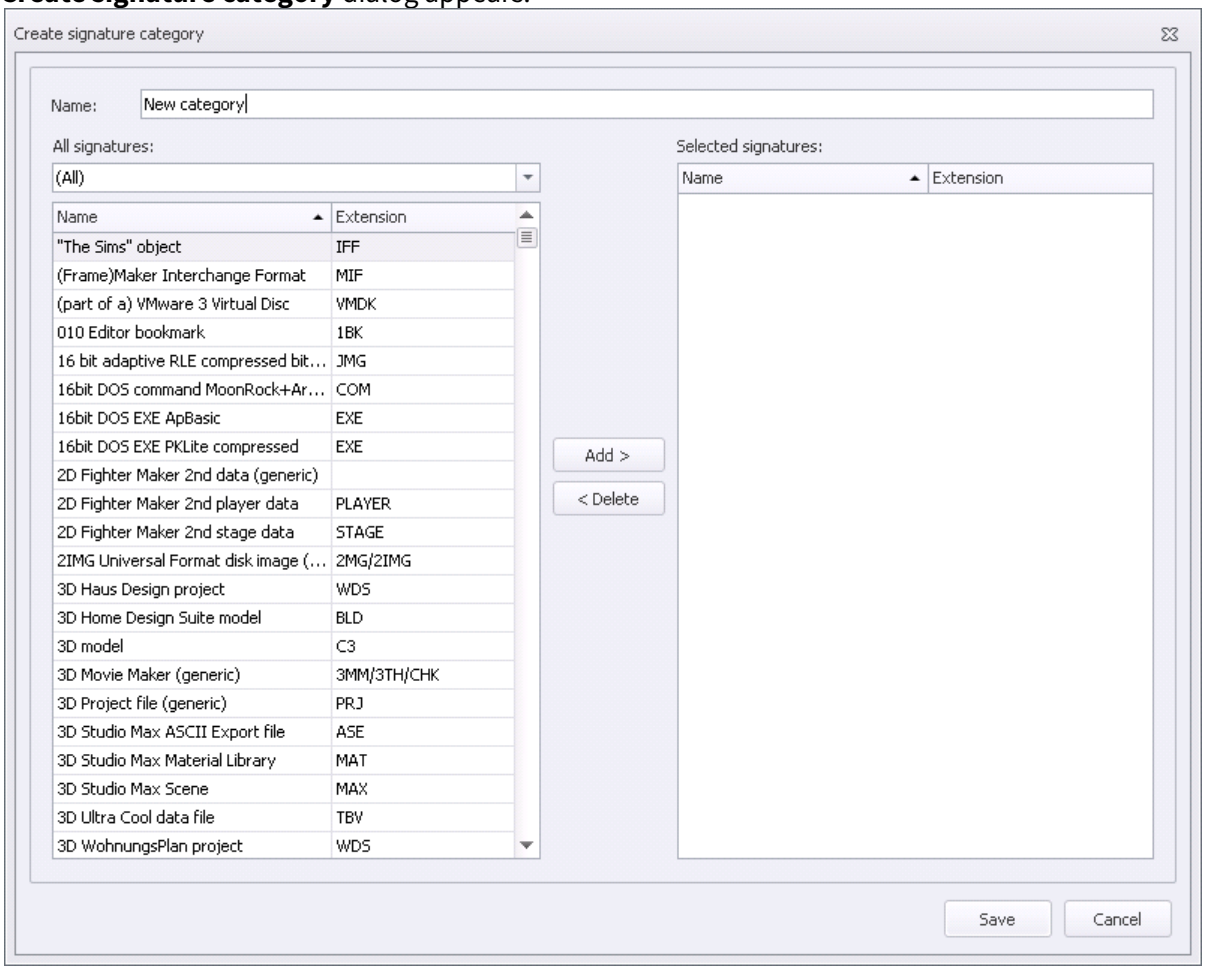
- create signature categories;
- fill created categories by copying predefined signatures;
- delete your signature categories, if they are not used by any rule.

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 signatures** 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;
> - 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 Main Menu select **Edit** > **Delete**;
    - Click **Delete** at the top of Navigation panel;
    - Right-click the name of the selected category and select **Delete**;
    - Press Ctrl+D.
4. In the next confirmation dialogue, select **Yes** to confirm that you want to remove the signature category.

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.

Application Protocol

To go to the **Applications** 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**
- **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 "Application Monitor Rule".
- forbid screenshots creating. See details in "ScreenShot Control Monitor Rule";
- automatic creating the screenshots by the System. See details in "ScreenShot Monitor Rule";
- pasting to clipboard. See details in "Clipboard Monitor Rule".

In the **Applications Protocol** group you can use filters for viewing data on all applications launched on managed workstations running MS Windows OS. In this group, you can add applications to lists for MS Windows OS.

After the InfoWatch Device Monitor Agent is installed on workstations running MS Windows OS and they are rebooted, the System automatically starts to receive data on applications launched on managed workstations.

Note:

To decrease the CPU load, the database table containing records on application launches is added to the regular cleaning queue. See the Knowledge Base article: "Deleting Records of Device Monitor Application Log".

Data on all launches and installations produces an *application protocol*.

Warning!

Application protocol aim is that one can not forbid the application, which absence is obstructive for computer proper operation.

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;
- Exporting Application Protocol.

Creating an Application List and Adding Applications

Lists are used to permit or forbid application usage on computers.

To manage white and black application list, the System offers application lists creation from the **Application protocol** (see "Application protocol").

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.
   - press Ctrl+N.
3. In the **List Name** field enter a name for a list you create.
4. In the **Operation System** field enter one of the OS:
   - **Windows** - the list will have the icon
   - **Linux** - the list will have the icon

   > **Note:**
   >
   > You can use the Linux lists of applications only in the Clipboard Monitor rule.

5. Click **Save**.

When the list is created, add applications to it.

Add applications to list

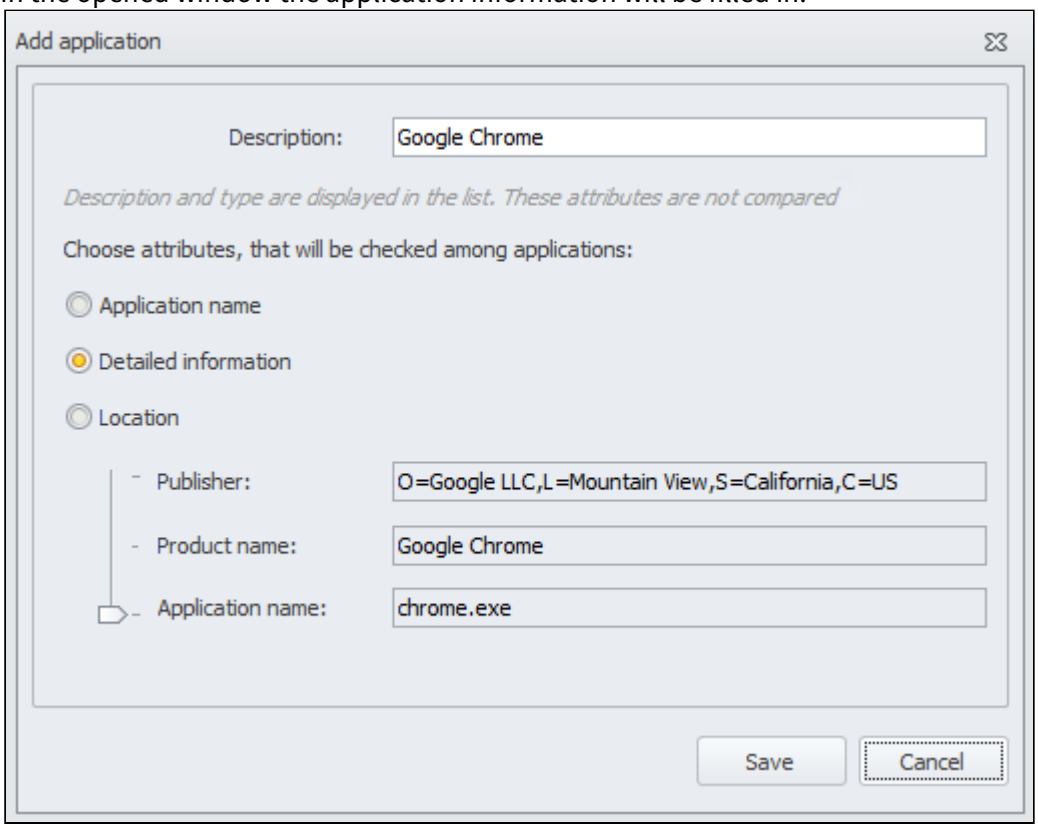
You can:

- Add application via executable file (available only for list of applications for **MS Windows OS**);
- Add application to the list manually;
- Add application to list automatically from the application protocol (available only for list of applications for **MS Windows OS**);
- Add application from another list.

Add application via executable file
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. In the opened window specify the executable file of application.

5. In the opened window the application information will be filled in.



6. Click **Save**.

To add application to list manually

1. Go to **Applications** section.
2. In the top left area in the **List of applications** group select the list of applications you would like to add to.
3. On the **List of applications** panel click ;
4. In **Add application** window you can set parameters for application correspondence check:
   - **Application name**
     Enter the full name of the application file
   - **Detailed information**
     Filtering application by detailed information of **Publisher**, **Product Name**, **Application Name**.

     > **Note:**
     >
     > **Detailed information** is available only for lists of applications for **MS Windows OS**.

   - **Location**
   - Filtering application by detailed information of **Location** to **Application name**.

     > **Note:**

Do not specify file name in the **Location**, only path to directory.

5. Click **Save**.

You can also add applications to the list manually from the **Applications protocol**. Available for **MS Windows OS** only.

For this:

1. Go to **Applications** section.
2. On the Navigation pane select the needed filter in the **Application protocol** group (see details in the article "Creating and Editing the Application Protocol Filter").
3. On the **Application protocol** panel select one or several entries. To select several entries click on them
   while pressing **Shift** or **Ctrl** button.
4. Take one of the following actions:
   - on the **Application protocol** panel click **Add application to list manually**;
   - select **Edit > Add application to list manually** command in the main menu;
   - right-click in the **Application Protocol** panel and select **Add application to list manually**
     manually from the drop-down list.
5. In **Add application** window you can set parameters.
6. Click **Save**.
7. If you have selected several entries, repeat steps 5 and 6 for other entries.
8. Click **OK**.

Add to application list automatically from the application protocol
The System allows to fill application lists automatically using data received from the application protocol. Only for **MS Windows OS** application lists.

To add application/s to the list automatically from the application protocol:

1. Go to **Applications** section.
2. On the Navigation pane select the needed filter in the **Application protocol** group (see details in the article "Creating and Editing the Application Protocol Filter").
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** from the drop-down list.
5. In the opened 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**.

Add application from another 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 the application from list/lists and click **Add application to list**.
5. From the list select **Add application to list automatically** or **Add application to list manually**.

> **Note:**
>
> Adding applications from a different OS family is not supported. It means that you cannot add a Windows application to a list for Linux, and vice versa.

Editing and deleting application from the list

To edit application in the list:

1. Click button on the  **List of applications** group or right-click the application and in the context menu select **Edit**.
2. You can edit details which will be used to filter the application (see "Add application to the list manually").

To delete application from the list:

1. Click  button on the **List of applications** group or right-click the application and in the context menu select **Edit**.
2. Click **Yes** to delete application from the security scheme.

Creating and Editing the Application Protocol Filter

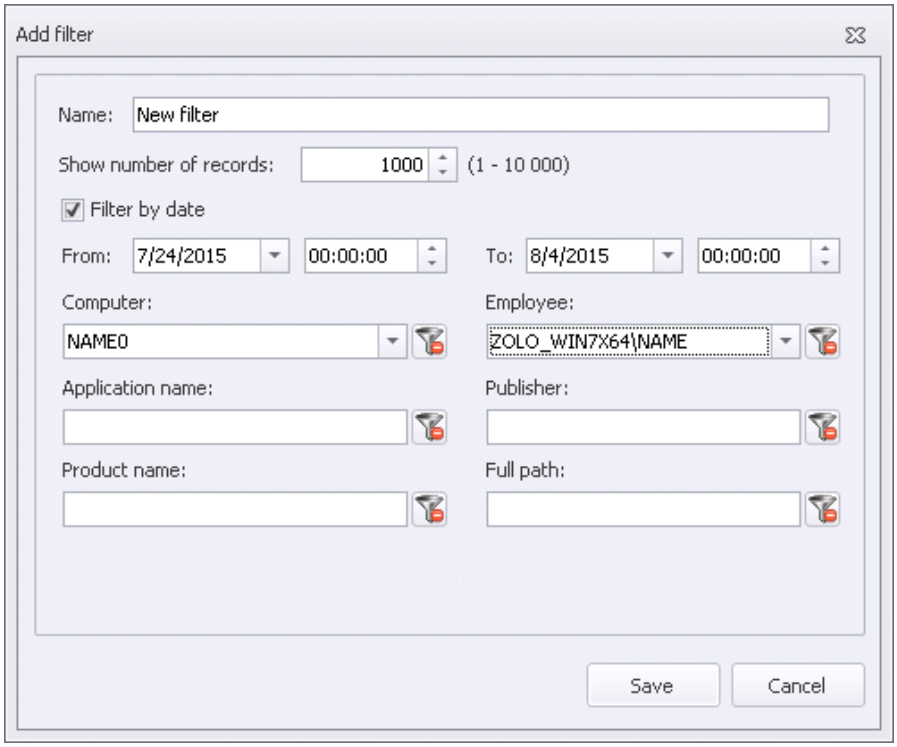
Filters allow you to configure the application protocol (see "Application protocol") to display information on applications that meet specified conditions.

> **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.

    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.

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.

Application Blockade

Application Blockade is functionality using which Device Monitor intercepts file reading/writing performed by applications. For this, Device Monitor uses the File Operations Monitor module.
Device Monitor sends interception events to Traffic Monitor that analyzes them according to its security policies.

In order to use the File Operations Monitor rule (see "File Operations Monitor Rule"), **be sure to add** the Application Blockade configuration to the Device Monitor security scheme.

> **Note:**
>
> If you do not add the Application Blockade configuration, the File Operations Monitor rule will be unavailable.

The configuration consists of application profiles and OS profiles. Application profiles are used for configuring the interception rule. During interception, both profile types are used.

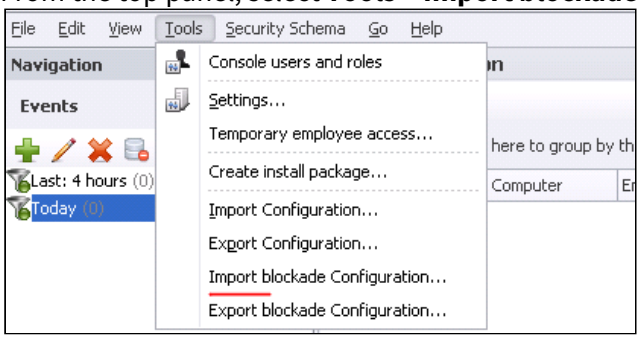
You can add profiles manually or import a prepared configuration from file.

> **Important!**
>
> We recommend using a prepared Application Blockade configuration from files. To get the configuration, please contact the InfoWatch company.
>
> For Device Monitor to be able to send Application Blockade events, you need to add a license to Traffic Monitor.
>
> Importing and editing the Application Blockade configuration is considered modifying the security scheme. After applying changes, distribute the new scheme to Device Monitor Agents.

Importing and exporting the Application Blockage configuration

To import a prepared Application Blockade configuration:

1. From the top panel, select **Tools > Import blockade configuration**.



2. In the window that opens, choose the configuration file in XML format.
   You can view and edit the imported configuration on the **Application blockade** tab.

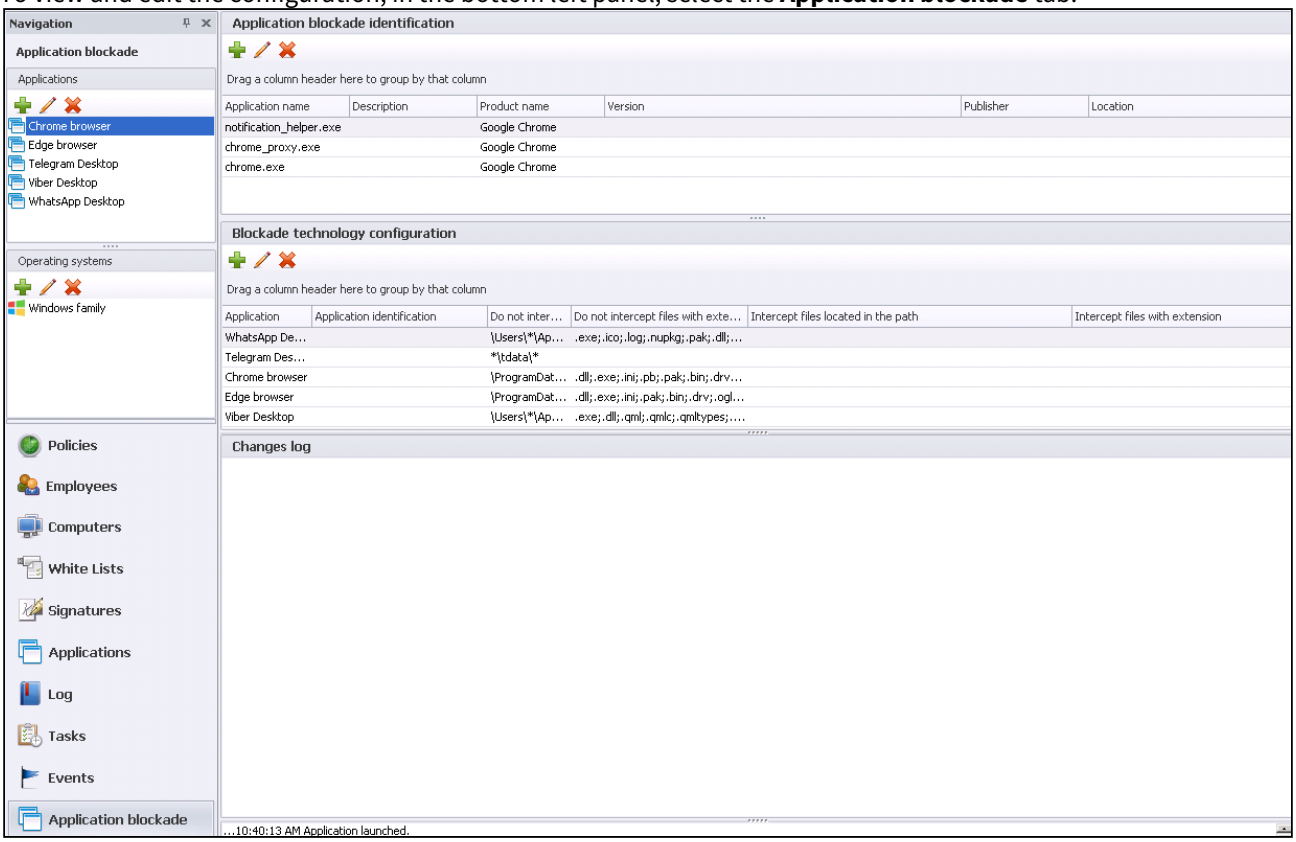
Also, you can export the current Application Blockade configuration and use it on another Device Monitor server.

To export the Application Blockade configuration:

1. From the top panel, select **Tools > Export blockade configuration**.
2. In the window that opens, specify the name and location of the configuration file and click **Save**. The configuration file in XML format will be saved to your computer.

Editing configuration and adding profiles manually

To view and edit the configuration, in the bottom left panel, select the **Application blockade** tab.



Note:

When you specify extensions and paths in profile settings, the following rules apply:

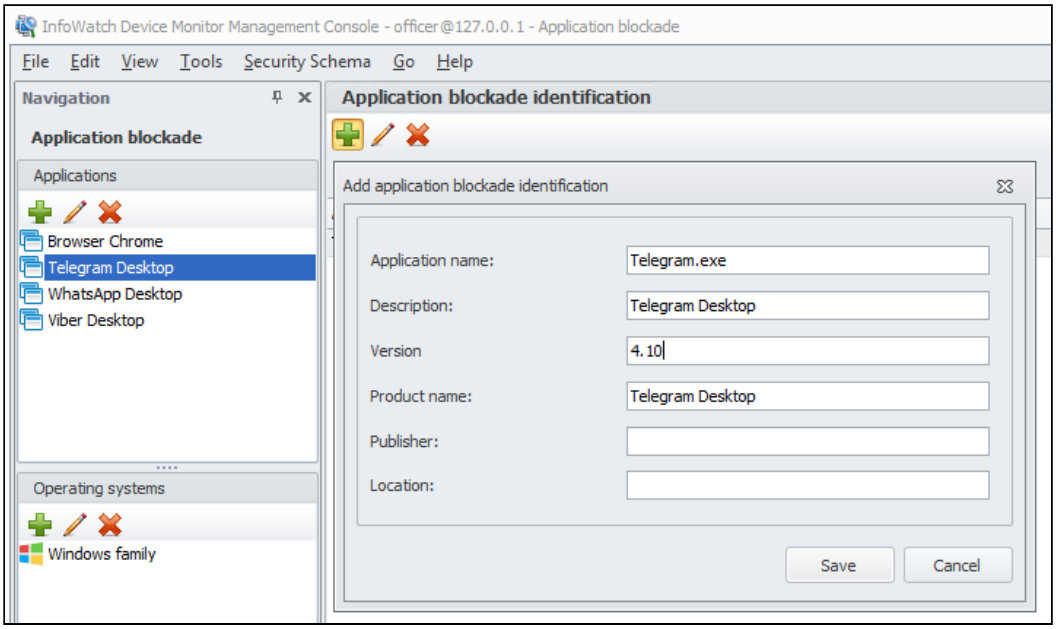
- Using masks is allowed
- The delimiter should be " ; "
- The path must begin with the standard file system path separator "\" or with a special character (for example, *)
- Excluded/included paths must specify a relative path to the file, that is, drive names are not allowed

To edit the configuration elements, use the  button.

Configuring application profile

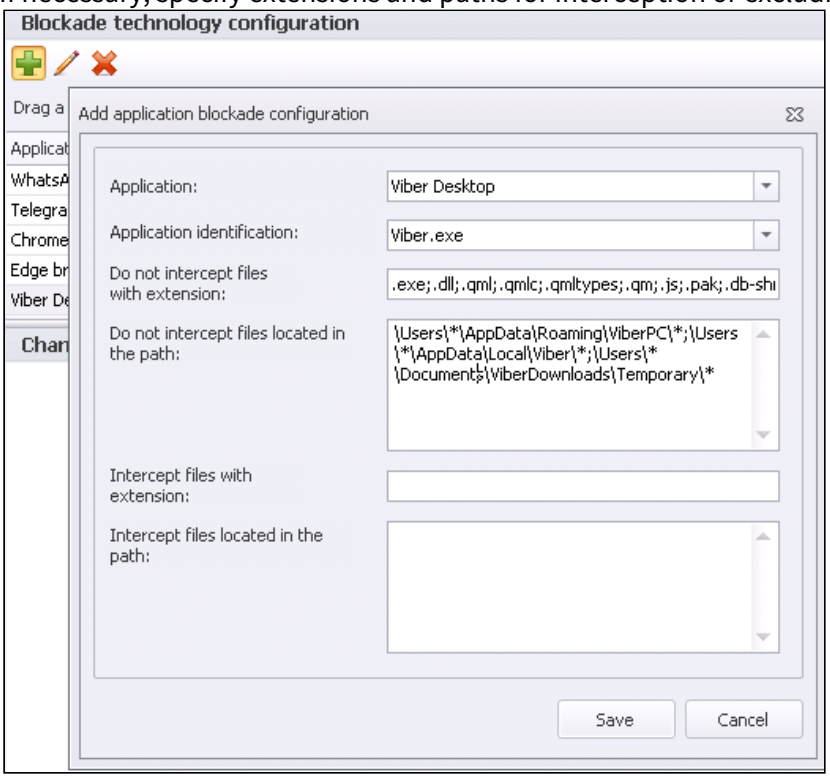
To configure the application profile:

1. To add an application profile, click  in the **Applications** area and specify the name of the new profile.
2. Select a custom profile and fill in the **Application blockade identification** area.
    a. Click  and specify application identification parameters:
        - **Application name** – original name of the executable file
        - **Description** – the file description
        - **Version** – the application version (version range)
        - **Product name**
        - **Publisher**
        - **Location**



    b. You can specify multiple controlled applications in the same profile.
3. Add technology configurations for the blockade:
    a. In the **Application** field, choose the profile name from the list.
    b. In the **Application identification** field, select the product version from the list related to the selected profile. Or you can leave the field empty – in this case, the configuration will apply to the whole profile.

c. If necessary, specify extensions and paths for interception or excluding from interception.



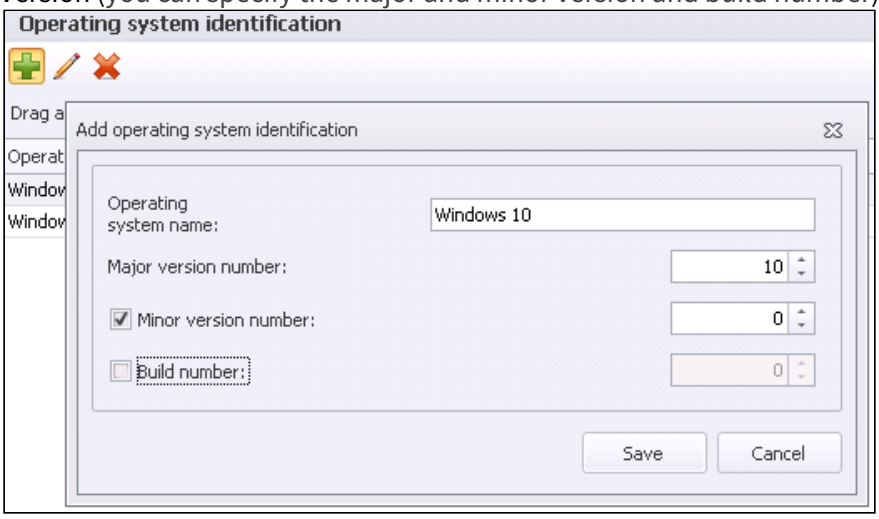
Configuring OS profile

1. To add an OS profile, click  in the **Operating systems** area and specify the name of the new profile.

> **Note:**
>
> Only work with the MS Windows OS family is supported.

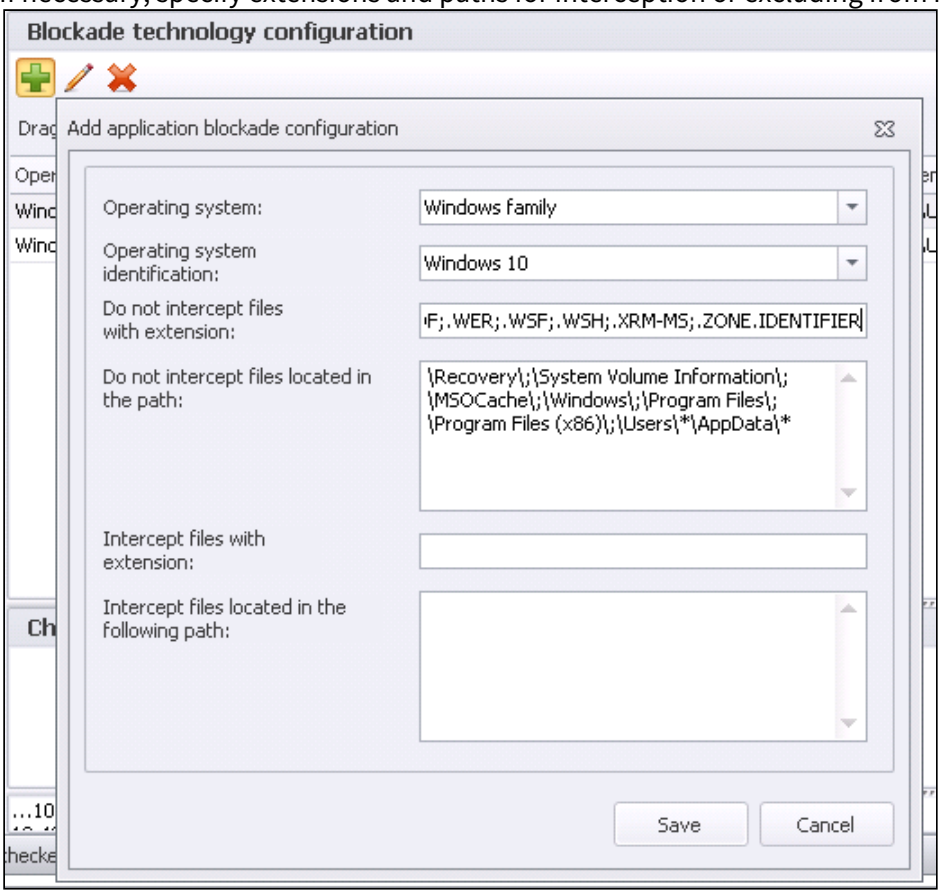
2. Choose a custom profile and fill in the **Operating system identification** area:
   a. Click  and specify OS identification:
      - OS name

- Version (you can specify the major and minor version and build number)



- You can specify multiple operating systems in the same profile

3. Add the blockade technology configurations:
   a. In the **Operating system** field, choose the OS profile name from the list.
   b. In the **OS identification** field, choose the OS version from list related to the selected profile. Or you can leave the field empty – in this case, the configuration will apply to the whole profile.
   c. If necessary, specify extensions and paths for interception or excluding from interception.



Application blockade events

Events sent to Traffic Monitor contain the following data about the file operation:

- File operation type:
  - Reading
  - Writing
- Data about the application in which the operation was performed
- Active browser tab data (if the file operation was performed in the browser). The URL of the active tab is displayed in TM events for Traffic Monitor version 7.6.0 and later

> **Note:**
>
> The System creates an event and stores data about an active tab when the application reads/writes a file. The tab may be defined incorrectly if the user has switched to another tab before the screenshot is taken.

- File information
- File shadow copy
- Screenshot (if taking screenshots is configured in the rule).

You can also view Application blockade events in the **Events** section of the Device Monitor Management Console (see "Viewing DM Events").

Resources

For Screenshot Monitor rule and Keyboard Monitor rule Security officer can specify which resources to control or exclude from control. To do this, Security officer can create a list of these resources.
You can manage resources in **Resources** section. To go to this section, use the button **Resources** on Navigation pane.

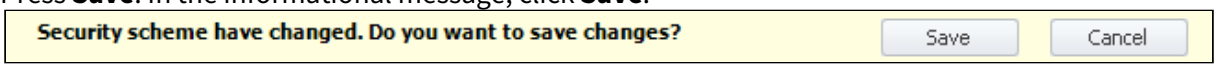
For more information on resources see:

- Adding list of resources
- Editing list of resources
- Deleting list of resources
- Creating list of resources from file
- Unloading list of resources to file

Adding list of resources

To add a list of resources:

1. Go to **Resources** section.
2. Click on **Add list of resources** on navigation pane.
3. Enter the list name.
4. Press **Save**. In the informational message, click **Save**.

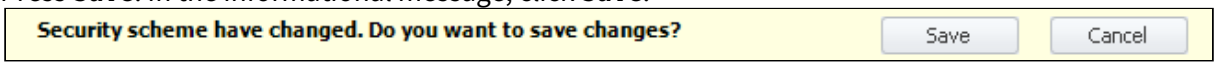


The list of resources will be created.

To add resources to the list:

1. Go to **Resources**.

2. Click on **Add resource** in **Resource** area.
3. Select the type of resource: Domain, Url, Url contains. To see a tip on resource type, mouse over the icon in the **Type** field.
4. Enter the resource and its description in the correspondent fields.
5. Press **Save**. In the informational message, click **Save**.



The resource will be added to the list of resources. Details about it will be displayed in **Details** area.

Note!

Below you can see the principle of how the System verifies if the resource being visited by a user matches the one in the list of resources:

Domain type

The System verifies if there is an exact match for *<host>,* including subdomains. Registry is not considered.

Example: If the list of resources contains *example.com*, then *one.example.com* or *ExamPle.com* will be considered matching it. But *example1.com* will not be considered matching the resource from the list.

URL type

- if URL in the list of resources contains only domain, then the System verifies if there is an exact match with *<host>,* subdomains not considered
- if URL in the list of resources contains parameters and ancor (there are delimiters /,?, #), then the System verifies if there is an exact match with *<host> <port> and [/<URL-path>][?<parameters>][#<ancor>]*;
- if URL in the list of resources contains port, the System verifies if there is an exact match with consideration of the port;
- if URL in the list of resources does not contain port, then the System verifies if there is an exact match.

Registry is considered (except for the *<host>*).

Example: If the list of resources contains *example.com/example?example#example,* then *EXAMPLE.com / example?example#example* will be considered matching it. But *one.example.com* or *one.example.com/ example* or *example.com:8080 /example?example#example* will not be considered matching the resource from the list.

URL contains type

The System verifies if there is a match with a text in the list in any part of substring *<host>[:<port>]][/<URL-path>][?<parameters>][#<ancor>]*, including subdomains. Registry is not considered.
Example: If the list of resources contains *example*, then *one.com/example?example#example* will be considered matching it. But *one.com/one?onet#o* will not be considered matching the resource from the list, as the url does not contain *example*.

Warning!

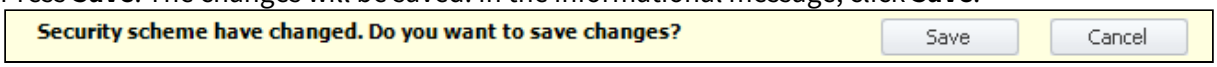
- Technologies defining URL resource that is displayed in the current active tab of the supported application (browser) are based on elements analysis of the application graphic

interface. So the URL detected by the System may not completely match the actual URL of the resource addressed by the application
- Resource name will not be transformed into IP address
- Resource name added as an IP address will not be transformed back into the resource name
- Symbols will not be transformed if encoded with Punycode (https://tools.ietf.org/html/rfc3492)
- The System verifies if the resource being visited matches the one in the list of resources only when the following browsers are used:
  - Google Chrome;
  - Yandex browser;
  - Mozilla Firefox;
  - Edge (Chromium);
  - Opera;
  - IE.

Editing list of resources

To edit a list of resources:

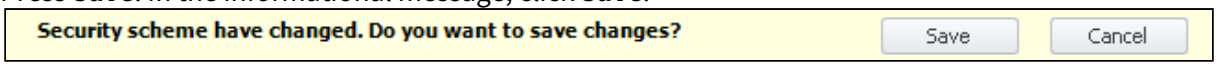
1. Go to **Resources** section.
2. Click on **Edit list of recources** on the top of navigation pane.
3. In the window that opens, edit the list name.
4. Press **Save**. The changes will be saved. In the informational message, click **Save**.



The changes will be saved.

or

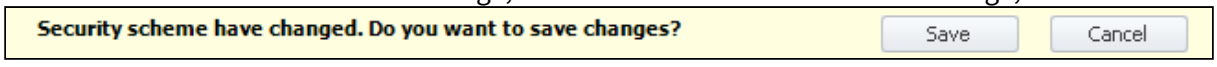
1. Go to **Resources** section.
2. On navigation pane, double click on the list you need to change.
3. In the window that opens, edit the list name.
4. Press **Save**. In the informational message, click **Save**.



The changes will be saved.

To edit a resource from the list:

1. Go to **Resources** section.
2. On the right, in **Resources** area click on the resource you need to edit.
3. Click on **Edit resource** on **Resources** area pane.
4. In the window that opens, make changes you need.
5. Press **Save**. In the informational message, click **Save**. In the informational message, click **Save**.

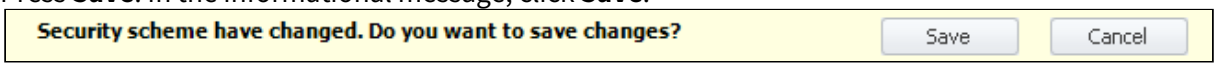


The changes will be saved. Detailed information about the resource will be displayed in **Details** area.

or

1. Go to **Resources** section.
2. On the right, in **Resources** area double click on the resource you need to change.

3. In the window that opens make changes you need.
4. Press **Save**. In the informational message, click **Save**.

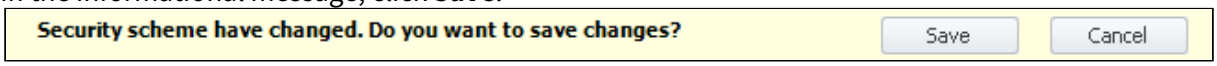


The changes will be saved. Detailed information about the resource will be displayed in **Details** area.

Deleting list of resources

To delete a list of resources:

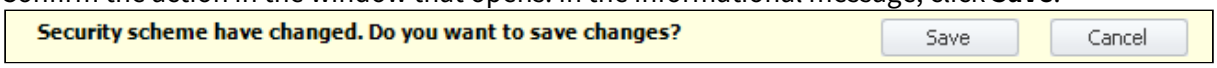
1. Go to **Resources** section.
2. Press **Delete list of resources** on the top of navigation pane.
3. Confirm the action in the window that opens.
   In the informational message, click **Save**.



The list of resources will be deleted.

To delete a resource from the list:

1. Go to **Resources** section.
2. On the right, in **Resources** area tap on a resource you need to delete from the list.
3. Press **Delete resource** on the pane in **Resources** area.
4. Confirm the action in the window that opens. In the informational message, click **Save**.



The resource will be deleted.

Creating list of resources from file

If needed, Security officer can create a list of resources from file. You may use this option to migrate data faster or to deploy a new Device Monitor server. The file you upload should:

- have the extension .txt;
- have the encoding UTF-8;
- the row should have the content:
  - resource type: domain/URL/URL contains;
  - resource;
  - description.
- use tab as a separator;
- have the structure: one line in the file is one record in the list of resources.

Note:

Name of the uploaded file will become the one of list of resources. If the System already has a file with the same name, then (n+1) will be added to such name, where n - is a number that is used in the name of previous list of resources. In case the uploaded file contains a double record of a resource (the one that does not contain the unique combination type + resource), then such record will not be uploaded in the System.

To create a list of resources from file:

1. Go to **Resources** section.

2. Click on **Create list of resources from file** on navigation pane.
3. Select the file with resources that you need to add to the System. In the informational message, click **Save**.



The list of resources will be added.

Note:

If an error occurs while uploading the file, then the System will display a message about it, specifying what line contains the error. The list of resources will not be created.
The type of errors can be as follows:

- created line is invalid (for example, tab is not used as a separator or some required value is missing);
- unknown resource type (the type differs from the ones that should be specified: domain, URL, URL contains);
- type does not match the resource (for example, domain is specified as a type, but the resource corresponds to URL type).

Unloading list of resources to file

To unload a list of resources to file:

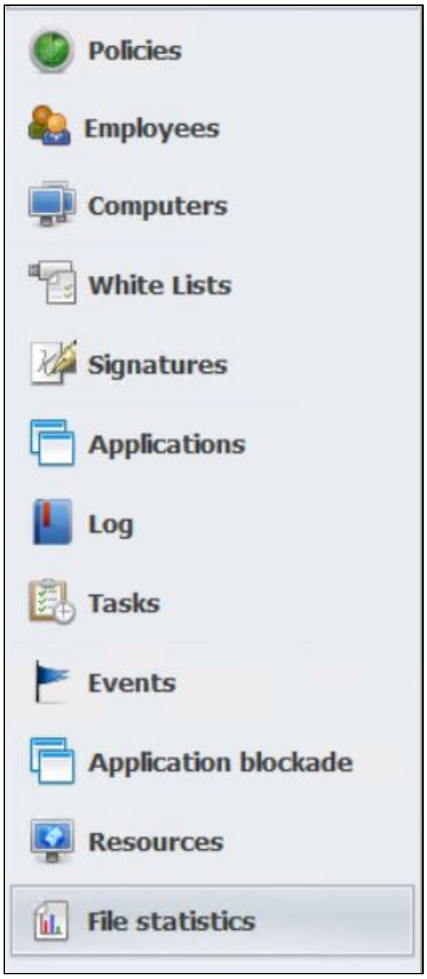
1. Go to **Resources** section.
2. Click on **Unload list of resources** to file on navigation pane.
3. Select where to unload the list. Press **Save**. The list of resources will be saved into the directory you selected.

File Statistics

Important!

The functionality is to be used only in InfoWatch Activity Monitor and InfoWatch Prediction.

File statistics allows to monitor actions of persons with files. To work in the section, press **File statistics** on the left of the Navigation panel.



You can manage file statistics and configure it in the section **File statistics**. Interception of files reading and recording is to be set in **Statistics** rule (for more details, see "Statistics Rule").

To add application or edit application of file statistics:

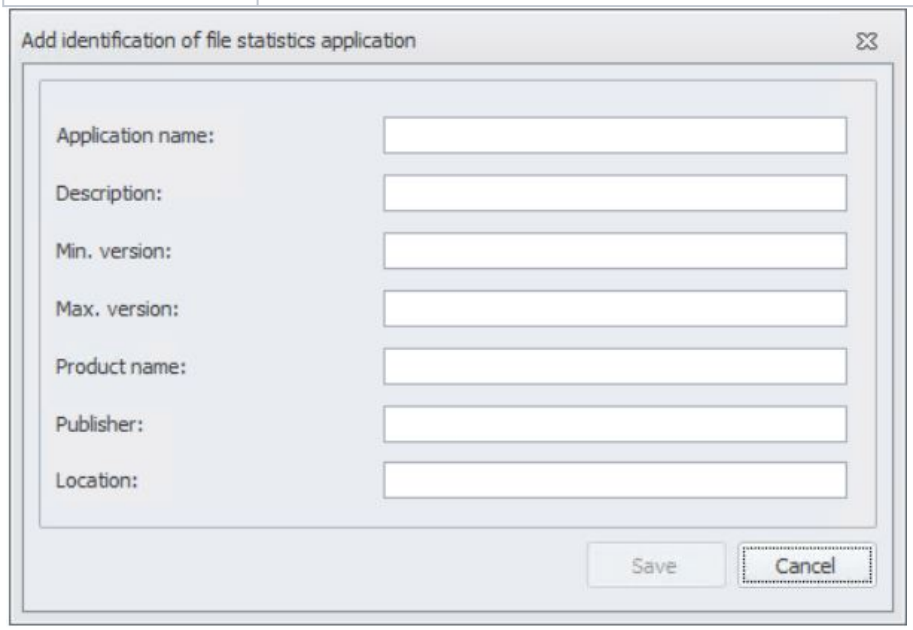
Important!

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.

1. In Device Monitor Management Console, select the section **File statistics**.
2.

Operation	Steps
Add application of file statistics	In **File statistics applications** area of Navigation panel, press **Add application** on the top panel of Navigaion panel.
Edit application of file statistics	a. In the area **File statistics applications** of Navigation panel, select the application you need.

Operation	Steps
	b. Press **Edit application** on the top of Navigation panel, or double left-click on the application. The dialogue window opens:



3. Specify the following parameters:
   - **Application name** (example: Outlook.exe)
   - **Description** (example: Outlook)
   - **Min. version** (example: Outlook 2016)
   - **Max. version** (example: Outlook 2021)
   - **Product name** (example: Outlook 2016)
   - **Publisher** (example: Microsoft)
   - **Location** (example: C:\Program Files)
4. Press **Save**.
5. Confirm modification of security scheme by pressing **Save**.

To delete application of file statistics:

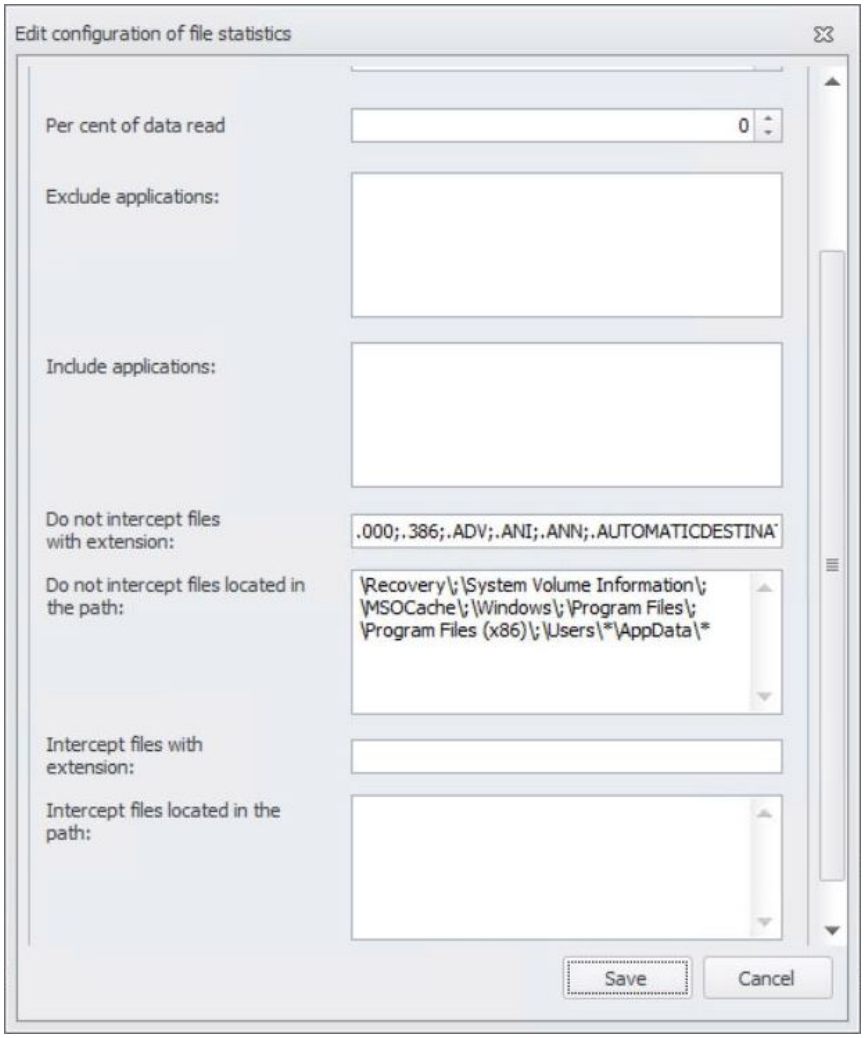
1. Go to **File statistics** section.
2. Select an application you need to delete.
3. Press **Delete application** on the top of Navigation panel. Or double left-click on the application you need to delete and in the window that opens select **Delete application**.
4. Press **Save**.
5. Confirm modification of security scheme by pressing **Save**.

To edit configuration of file statistics:

Important!

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.

1. In the area **File statistics configuration**, press **Edit configuration of file statistics**. The dialog window with parameters of configuration opens:



2. Select the parameters:
   - **Generate events for alternative file streams**.
     If application and/or file system uses not the main data stream (controlled), but the alternative data stream (metadata, associated with object of file system), then events may not be created. Enable the setting if you need to create events for alternative file streams. For example, to detect the violator who attaches a file with sensitive information to a normal allowed file, then copies that file outside the perimeter. By default, the setting is disabled.
   - **Monitor applications, which are running in system session**.

     Important!

     The setting is disabled without possibility to enable. Applications running in the system session are not monitored.

   - **Monitor only the applications clearly added to monitoring**. Enable the setting if you need to monitor only the applications specified for monitoring. Disabled by default.

3. Specify the parameters value:
    - **Cumulative session time, sec**. The parameter allows to set the moment of events creation. If Activity Monitor receives a big amout of low-level events, which do not match user activity, then you can increase the time of the session. Default value is 30 seconds. The defualt value can be decreased, but then the number of events can increase.
    - **Per cent of data read**. The setting allows decreasing in Activity Monitor the number of system events of file opening. The higher the value, the lower the number of such events. Value by default is 0.
4. **Exclude applications**. Specify the applications you need to exclude from monitoring.
5. **Include applications**. Specify the applications you need to include in monitoring.
6. If you do not need to not intercept files with a specific extension, fill in the extension in the field **Do not intercept files with extension**.

> **Important!**
>
> By default, the following extensions are excluded:
>
> .000; .386; .adv; .ani; .ann; .automaticdestinations-ms; .bcd; .bin; .bio; .bk1; .bk2; .bmk; .bud; .cab; .cat; .chg; .chs; .cht; .ci; .clb; .cnt; .cpi; .cpl; .cur; .customdestinations-ms; .dat; .desklink; .deskthemepack; .dev; .devicemetadata-ms; .dit; .dll; .dmp; .drv; .ebd; .etl; .evt; .evtx; .exe; .ffa; .ffl; .ffo; .ffx; .fid; .grl; .group; .grp; .h1s; .hdmp; .hhc; .hhk; .hiv; .hlp; .hpj; .hsh; .hve; .icl; .icn; .ico; .iconpackage; .idx; .ime; .inf; .inf_loc; .ini; .itemdata-ms; .js; .job; .jpn; .kbd; .kor; .library-ms; .lnk; .manifest; .mbr; .mdmp; .mem; .mlc; .msc; .msi; .msp; .msstyle; .msstyles; .mtz; .mui; .mum; .nfo; .nls; .nt; .ntfs; .pdr; .pfx; .pol; .ppd; .ppm; .prf; .printerexport; .ps1; .ps2; .pwl; .reg; .reglnk; .regtrans-ms; .rs; .scf; .scr; .searchconnector-ms; .shd; .spl; .spx; .str; .swp; .sys; .theme; .trx_dll; .uce; .vga; .vx_; .vxd; .wdf; .wer; .wsf; .wsh; .xrm-ms; .zone.identifier; .tmp; .crdownloads; .thumbs.db

7. If you do not need to intercept files/folders located in a particular path, fill in the path in the field **Do not intercept files located in the path**.

> **Important!**
>
> By default, the following paths are excluded:
>
> \Recovery\;\System Volume Information\;\MSOCache\;\Windows\;\Program Files\;\Program Files (x86)\;\Users*AppData*\

8. If you do not need to intercept files with a specific extension, fill in the extension in the field **Intercept files with extension**.
9. If you do not need to intercept files/folders located in a particular path, specify the path in the field **Intercept files located in the path**.

> **Important!**
>
> Interception/no interception paths and extensions is performed only with the folders and files with which the user operates directly.
>
> Example:

If *Do not intercept files with .docx extension* is selected, then when the user operates with the folder containing files with this extension, the event for the file *.docx is created and sent to the Platform.

If *Do not intercept* is selected for the folder 2, which is a subfolder for the folder 1:

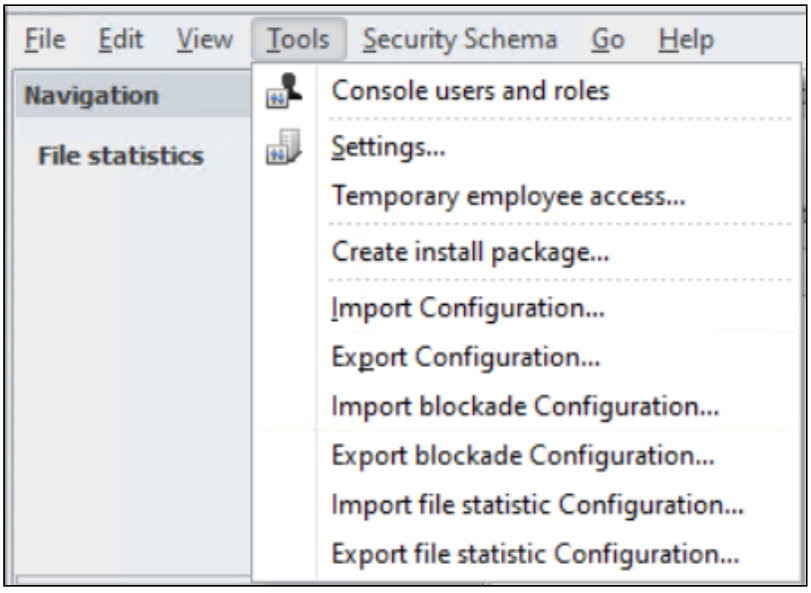
- When an operation is performed with the folder 1: for all the files from the folder 2 the events are created and sent to the Platform.
- When an operation is performed with the folder 2: the event is not created by Agent, as *Do not intercept* option is selected for the folder.

10. If you do not need to collect information about operations with folder content, then select the option **Disable event generation for operations**, **where folder content listing is required**. The parameter is disabled by default.

> **Important!**
>
> When moving a folder to recycle bin, restoring it from there or moving a folder within volume, the file system considers these operations as low-level operation of changing name. However, if these files are numerous and an event should be created for each of them, then the system load may increase considerably.
>
> For example, when moving a folder containing 1000 files, in Activity Monitor 1000 events are created for each file. The setting allows to disable collecting statistics of these operations and to desrease load on system. If collecting statistics for operation with folders is disabled, then the system does not create the events for the files inside the folders, in case the files are being moved within volume, or being moved to recycle bin or being restored from there.

11. Press **Save**.
12. Press **Save** to confirm modification of security scheme.

To import configuration of File statistics:



1. On the top of the panel select **Tools** > **Import file statistic configuration**.
2. In the window that opens, select the file you need to import. Press **Open**.
3. On the top of the panel press **Save** to save your changes in security scheme.

To export configuration of file statistics:

1. On the top of Navigation panel, select **Tools** > **Export file statistics configuration**.
2. In the window that opens, select the directory where you need to export the file. Press **Save**.

Junk Traffic Exceptions

Exception allows to specify the URL addresses, which should not be intercepted in HTTP/HTTPS traffic. If HTTP/HTTPS request is sent for the excepted URL address, the System does not create an event and a shadow copy.

Lists of exceptions are sent to Agents within the security scheme and are applied to all Agents. The Agent verifies the URL address to which the request is sent. URL address contains a host name and a resource request.

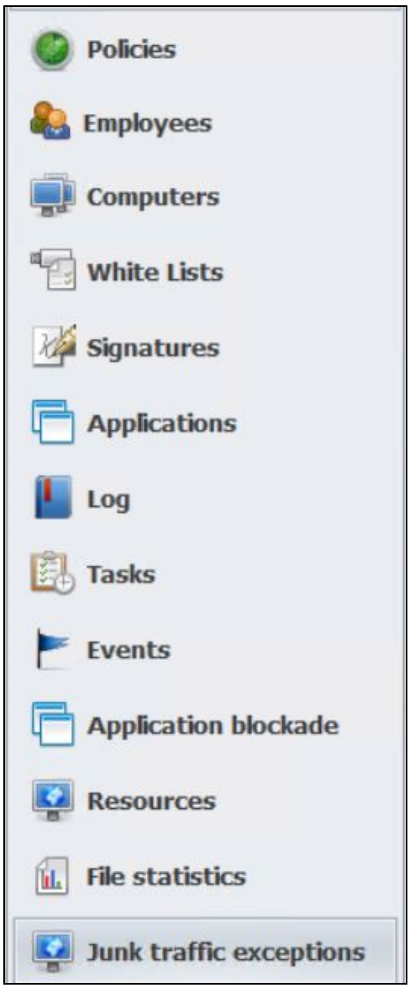
Example:

Host name: `www.google.ru`

Request to resource: `/log?format=json&hasfast=true`

The Agent verifies URL address: `www.google.ru/log?format=json&hasfast=true`

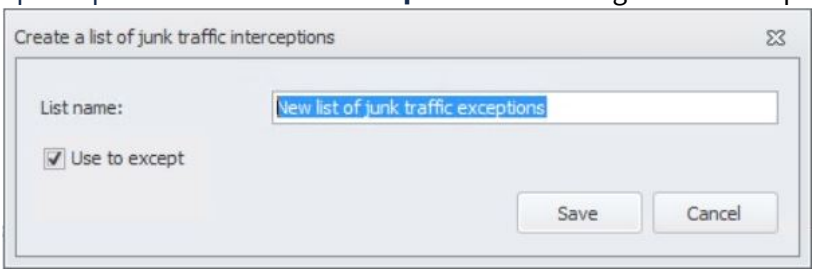
You can configure lists of exceptions in the section **Junk traffic exceptions** of navigation panel.



To add list of junk traffic interceptions

1. On the navigation panel of Device Monitor Management console press **Junk traffic exceptions**.

2. On the top of the panel press **Add list of exceptions**. The dialogue window opens:



3. Specify the list name. Select **Use to except**, to make the list active.
4. Press **Save**.
5. Confirm modification of security scheme by pressing **Save**.

The list can have one of two statuses:

- Active : the list is being used to exclude traffic
- Unactive : the list is not being used to exclude traffic

To activate the list, when you add or edit it, enable the parameter **Use for exception**.

To edit list of junk traffic interceptions

1. In the area **Junk traffic exceptions** on the top of the navigation panel select the list you need to edit.
2. Press **Edit list of exceptions** on the top of the navigation panel.
3. In the window that opens, make your changes.
4. Press **Save**.
5. Confirm modification of security scheme by pressing **Save**.

To delete list of junk traffic interceptions

1. In the area **Junk traffic exceptions** on the top of the navigation panel select the list you need to delete.
2. Press **Delete list of exceptions** on the top of the navigation panel.
3. Press **Yes**.
4. Confirm modification of security scheme by pressing **Save**.

To import list of junk traffic interceptions

1. In the area **Junk traffic exceptions** on the top of the navigation panel press **Import list of exceptions** .
2. Select the file you need to import.
3. Press **Open**.
4. Confirm modification of security scheme by pressing **Save**.

To export list of junk traffic interceptions

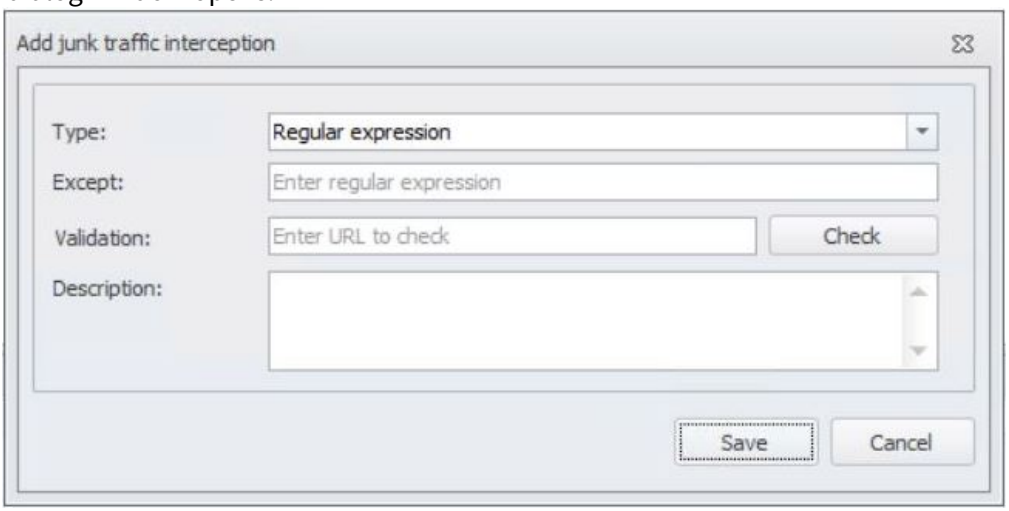
1. In the area **Junk traffic exceptions** on the top of the navigation panel press **Exmport list of exceptions** .
2. Press **Save**.
3. Confirm modification of security scheme by pressing **Save**.

You also can import/export list of exceptions within the security scheme.

You can configure exceptions in the selected list.

To add exception in the list of junk traffic

1. In the area **List of junk traffic interceptions** on the top of the area select press **Add exception** . The dialog window opens:



2. Specify:

Parameter	Description
Type	Only regular expression type of exclusion is available **Note**: If URL address matches the regular expression, then the System makes it exception from interception. The dialect to use for regular expressions – ECMAScript
Exception	Regular expression to be an exception For example, to exclude any URL address containing the string "google", specify: .*google.*
Description	Description of exception

3. Press **Save**.
4. Confirm modification of security scheme by pressing **Save**.

To edit exception in the list of junk traffic

1. In the area **List of junk traffic interceptions** on the top of the area select an exception you need to edit.
2. Press **Edit exception** on the top of the area.
3. Make your changes in the dialog window that opens.
4. Press **Save**.
5. Confirm modification of security scheme by pressing **Save**.

To delete exception in the list of junk traffic

1. In the area **List of junk traffic interceptions** on the top of the area select an exception you need to delete.
2. Press **Delete exception**  on the top of the area.
3. Press **Yes**.
4. Confirm modification of security scheme by pressing **Save**.

4.4.4 Temporary Employee Access to Network

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

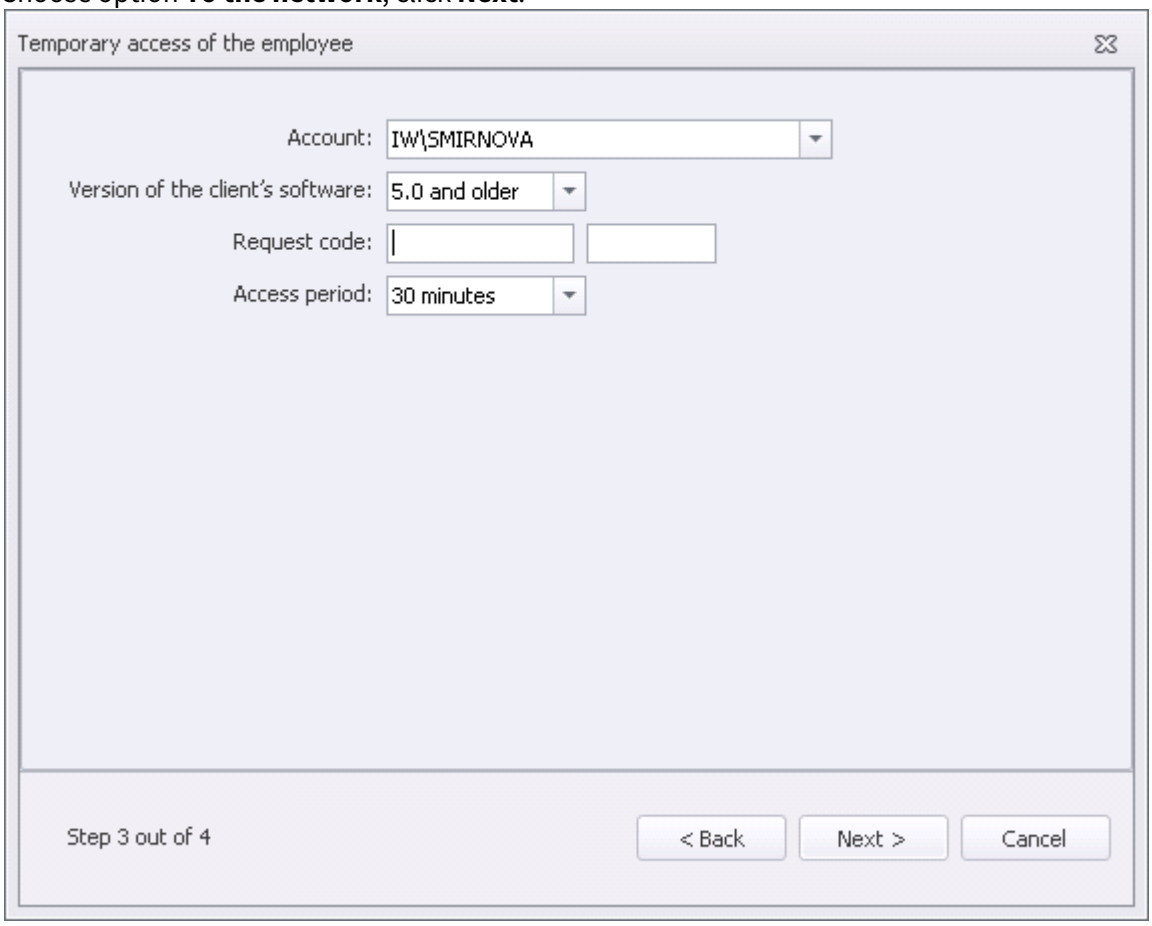
> **Warning!**
>
> An employee can request access only if the **Show tray icon** interface option is selected (see "General Settings for Agents"). The way how to configure text displayed to an employee is described in "Employee Notifications about Policy Violations", **"Network connection forbidden.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

An employee should send 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**.

4.4.5 Temporary Employee Access to Devices

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

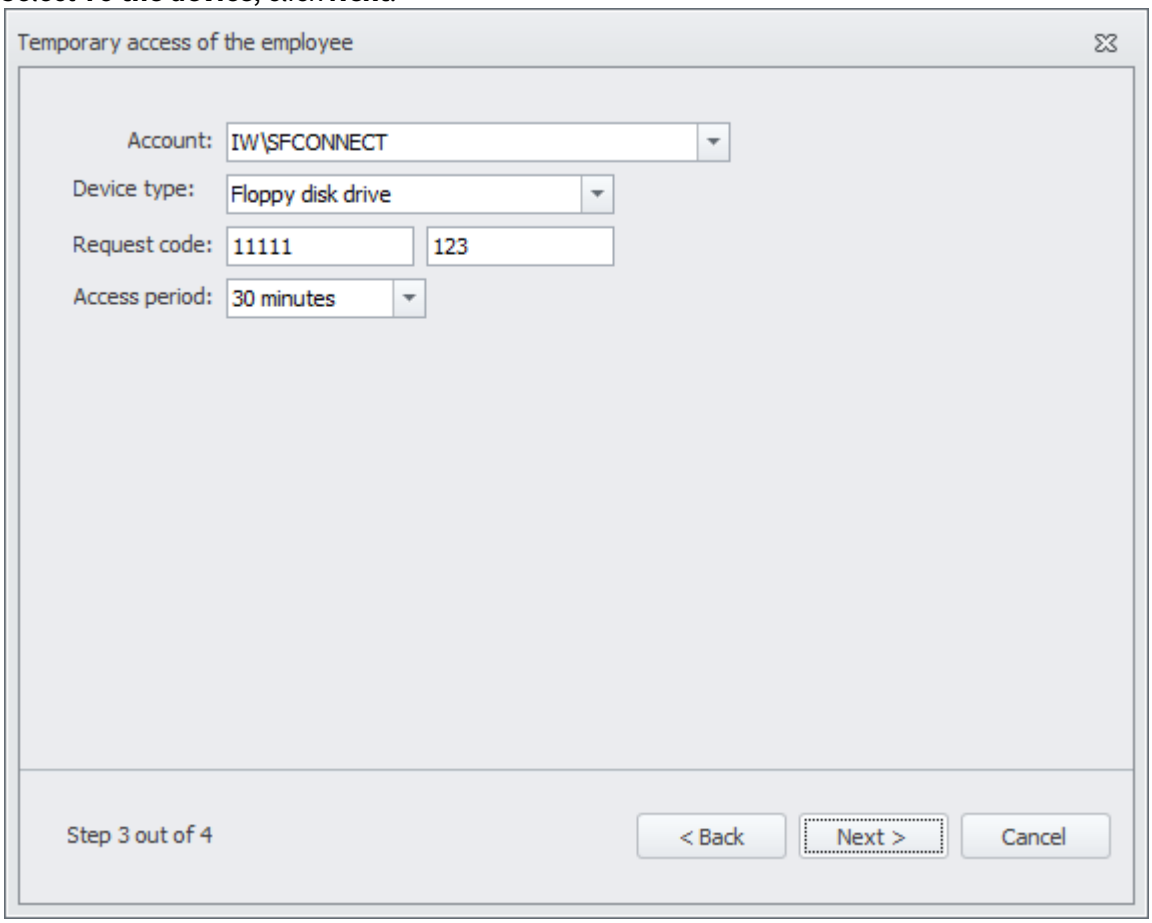
> **Warning!**
>
> An employee can request access only if the **Show tray icon** option is selected (see "General Settings for Agents"). On to configure the text displayed to the employee, see "Employee Notifications about DM Policy Violations", "**Access to device denied**" notification type.

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**.

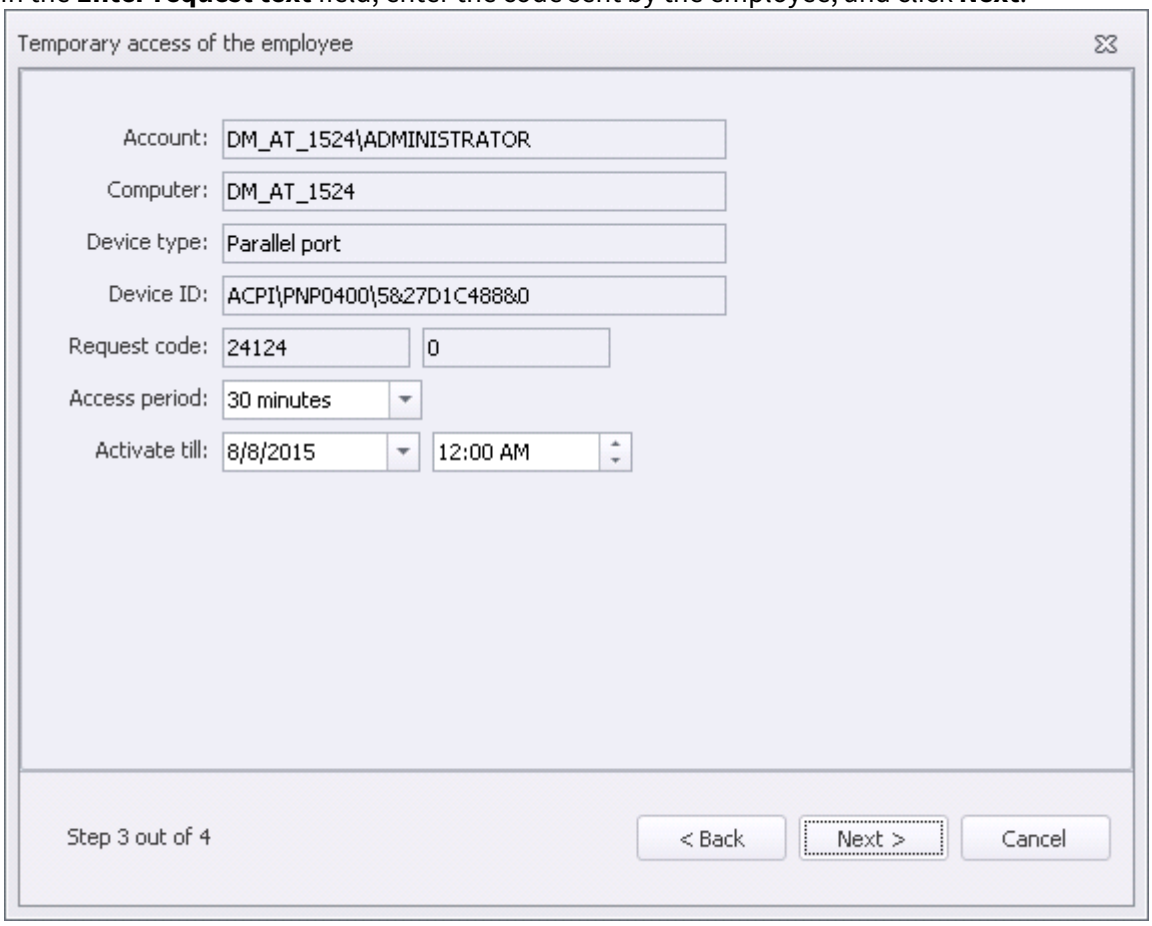


4. From the **Account** drop-down list, select an account of the employee to which temporary access should be granted.
5. From the **Device type** drop-down list, select the necessary device type.
6. In the **Request code** field, enter the code dictated by the employee.
7. From the **Access period** 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**.

4.5 Viewing DM Events

Data obtained by InfoWatch Device Monitor Agents on controlled computers is stored as **events** and transferred to InfoWatch Device Monitor servers along with shadow copies. Events (unlike shadow copies) are registered with InfoWatch Device Monitor database and are available from Management Console.

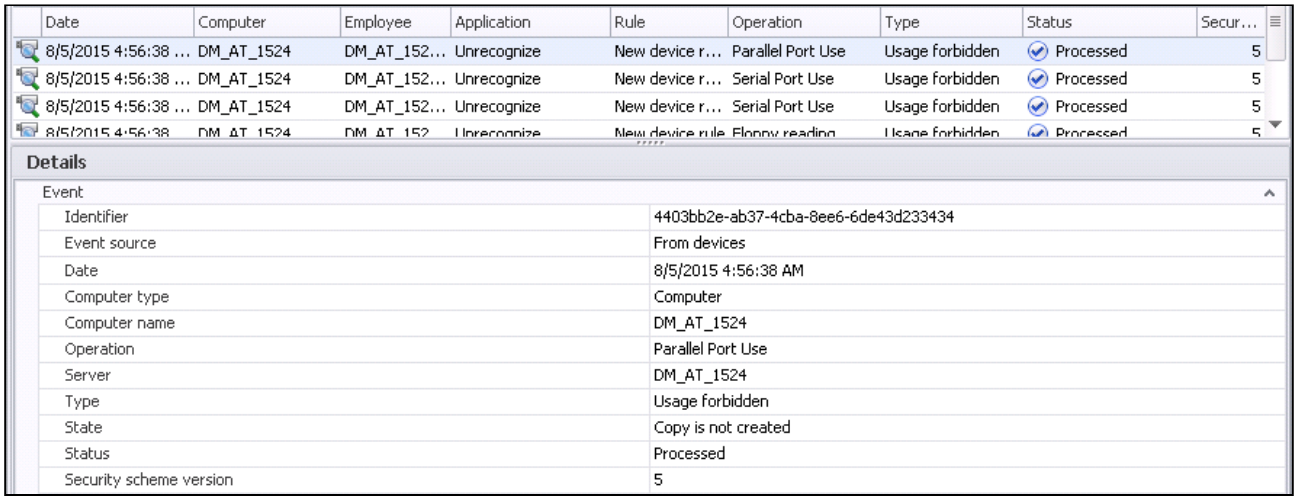
You can define the logging level (save information on all attempts of access, on policy violations only or do not save anything) in general settings of the security scheme: for details, see "General Settings for Agents".

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

To view events, choose the required filter in the list. You can choose a preset filter or create a new one as described in "Event Filters". Preset filters:

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

Event data is displayed as a table. Extended information on each record is available in **Details** panel.



Attribute name	Description	Available values
Common attributes		
Identifier	Unique event number	
Event source	Interceptor-based event type	• **File** – File Monitor; • **Devices** – Device Monitor; • **Clipboard** – Clipboard monitor; • **Application** – File operations monitor; • **Printer** – Print Monitor; • **Skype**, **XMPP**, **MMP**, **Telegram**, **WhatsApp** – IM Agent Monitor; • **FTP/FTPS** – FTP Monitor; • **HTTP/HTTPS** – HTTP(S) Monitor; • **Cloud Storage** – Cloud Storage Monitor; • **Mail** – Mail Monitor; • **Network** – Network Monitor; • **Screenshot** – ScreenShot Monitor; • **System** – event is created when the disk space for saving shadow copies is running out. *Such an 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 displays it according to the local time of a computer where Console is installed	

Attribute name	Description	Available values
Computer name	Name of the computer that registered the event	
Operation	Description of an action or an action attempt performed by the employee	
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	If an application cannot be detected in **Screenshot** event, the value is **Not specified**. In this case, the event is not sent to Activity Monitor.
Type	Action-based event type	• **Record** – adding or changing data (including renaming) on an external device; sending files via messenger; sending print jobs to printer; sending data via FTP/FTPS. • **Use** – connecting an external device that allows unmonitored read/write operations or sending messages. • **Violation** – IM Agent interceptor user-initiated violation. • **Warning** – user initiated a ban or didn't give consent to use IM Agent plug-in, while monitoring is required by security policy. • **Usage forbidden** – attempt of sending data via forbidden channel.
Status	Status of event processing on the server and sending to Traffic Monitor server	• **Unknown** • **Waiting for processing** • **Processed** • **No license** • **Waiting for sending to TM** • **TM sending error** • **Sent to TM** **Note:** If the Server is in standalone mode then the event has the **Processed** status only.
Security scheme version	Number of security scheme version that was active on the computer when the event was registered	

Attribute name	Description	Available values
Operation verdict	Attribute of allowed action. For Devices events (**Device Monitor** rule), blocking is also available.	• **Allowed** • **Forbidden** – only for events from devices • **Unprotected data copying is disabled** – only for events from devices • **Allowed (in white list)** - for whitelisted events from devices
Employee	Name of the domain (computer name outside the domain) and user login used for event registration or operating system reference for events outside user sessions	
Rule	Name of policy rule managing the event	
For events with *File, Devices, Application, Printer, FTP/FTPS, HTTP/HTTPS, Cloud Storage, Network, System* sources		
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 does not require shadow copying • **copy created** – shadow copy created successfully • **no free space on disk** – if there is no free space on the Agent • **copying error** – if an error occurred while creating a copy

Attribute name	Description	Available values
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 *Clipboard* source		
Copying via terminal session	Attribute showing that data crossed the terminal session line	• **Yes** • **No**
Data type	The type of pasted data	
Application receiver	Subheading describing the attributes of the application receiver to which the data is pasted from the clipboard	
Application source	Subheading describing the attributes of the source application that placed the data to the clipboard	
Application name	Name of the source application or application receiver	
Description	Description of the source application or application receiver	
Product name	Product name of the source application or application receiver	

Attribute name	Description	Available values
Issuer	Issuer of the source application or application receiver	
Location	Location of the source application or application receiver	
File version	File version of the source application or application receiver	
Product version	Product version of the source application or application receiver	
Terminal session application	If the application is on the list of supported virtualization systems	• **Yes** • **No**
Screenshot pasted into application	The attribute showing if the screenshot was saved while pasting from the clipboard	• **Yes** • **No**
Screenshot pasted from application	The attribute showing if the screenshot was saved while copying to the clipboard	• **Yes** • **No**
For events with *Application* source		
Path	Full path to thfile on workstation	
File size	File size in bytes	
Screenshot	Shows if the System saved a screenshot	• **Yes –** screenshot was saved; • **No –** screenshot was not saved.
For events with *Skype, XMPP, MMP, Telegram, WhatsApp*		
IM user ID	UIN of the user authorized in the messenger on the computer	
Object status	Shadow copy of transferred data	• **no copies created** – rule does not require shadow copying

Attribute name	Description	Available values
		• **copy created** – shadow copy created successfully • **no free space on disk** – if there is no free space on the Agent • **copying error** – if an error occurred while creating a copy
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 a transferred file	
File size	Transferred file size	
Shadow copy	File, message or chat shadow copy	• **No** – no shadow copy was created • **Yes** – shadow copy created successfully
For events with *Printer* source		
Document	Full name of the file sent to print	
Printer	Name of a target network printer	
Printing 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. 2. Shadow copy of print job was not created. The job contained no graphic or text data. 3. An error occurred while creating a shadow copy of print job. 4. Shadow copy should not have been created. 5. Shadow copy of print job was partially created. Graphic data were fully processed. Text data were partially processed. 6. Shadow copy of print job was partially created. Graphic data were partially processed. Text data were fully processed. 7. Shadow copy of print job was successfully created. The job contained only text data. 8. Shadow copy of print job was successfully created. The job contained only graphic data.

Attribute name	Description	Available values
		9. Shadow copy of print job was partially created. Graphic data were partially processed. The job contained no text data. 10. Shadow copy of print job was partially created. The job contained no graphic data. Text data were partially processed.
Object status	Result of creating shadow copy of transferred data	• **no copies created** – rule does not require shadow copying • **copy created** – shadow copy created successfully • **no free space on disk** – if there is no free space on the Agent • **copying error** – if an error occurred while creating a copy
For events with *FTP/FTPS* source		
Object status	Result of creating shadow copy of transferred data	• **no copies created** – rule does not require shadow copying • **copy created** – shadow copy created successfully • **no free space on disk** – if there is no free space on the Agent • **copying error** – if an error occurred while creating a copy
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 a 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)	

Attribute name	Description	Available values
Starting point	When file is transferred by piecemeals, position which starts the current part transfer.	
Shadow copy	Result of creating file shadow copy	• **No** – shadow copy was not created • **Yes** – shadow copy created successfully
For events with *HTTP/HTTPS* source		
State	Result of creating shadow copy	• **no copies created** – rule does not require shadow copying • **copy created** – shadow copy created successfully • **no free space on disk** – if there is no free space on the Agent • **copying error** – if an error occurred while creating a copy
Reciever DNS	DNS name of a computer	
Receiver IP	IP-address of a computer	
Request size	Size of a request in Kbps	
Rule	Name of policy rule managing the event	
For events with *Cloud storage* source		
Name of cloud storage	Name of the cloud storage where data is uploaded	• Google Drive • DropBox • YandexDisk • SkyDrive • EverNote • SugarSync
File name	Target file name	
File size	Size (in bytes) of the file to be sent to the cloud storage	
For events with *Terminal session* source		

Attribute name	Description	Available values
Path	Short name of file being copied	
Device name	Device name, if detected	
Device ID	Device ID, if detected	
For events with *Mail* source		
State	Result of creating shadow copy	• **no copies created** – rule does not require shadow copying • **copy created –** shadow copy created successfully • **no free space on disk** – if there is no free space on the Agent • **copying error** – if an error occurred while creating a copy
List of senders	DNS name of a sender computer	
List of recipients	Receiver addresses	**Note:** For events with a large number of senders, you should remember that 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).
Rule	Name of policy rule managing the event	
For events with *Network* source		
Time of ban removal starts	For *Temporary ban removal* operation. Corresponds to the start of temporary access period. See details in "Temporary Employee Access".	
Time of ban removal ends	For *Temporary ban removal* operation. Corresponds to the end of temporary access period. See details in "Temporary Employee Access".	

Attribute name	Description	Available values
Connection server	For *Connection forbidden* operation. Corresponds to the address or name of forbidden server which was attempted to gain access to.	
Port	For *Connection forbidden* operation. Corresponds to the port number used for connection attempts.	

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

> **Note:**
>
> Agents on RED OS support sending to Device Monitor server events when reading from external device and reading/recording from/to external device are forbidden.

> **Note:**
>
> Agents on Astra Linux OS 1.7, RED OS and Alt Linux OS support sending to Device Monitor server events of connecting/using external devices via USB. In this case:
>
> - the account name of the user that connected the device might not be detected.
> - the device ID might not be detected, if it is not specified in the device by manufacturer.
>
> For sending the events, you should specify the "**All**" value for the " **Log events of device and cloud storage interceptors** " parameter in General Settings for Agents.

4.5.1 Event Filters

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

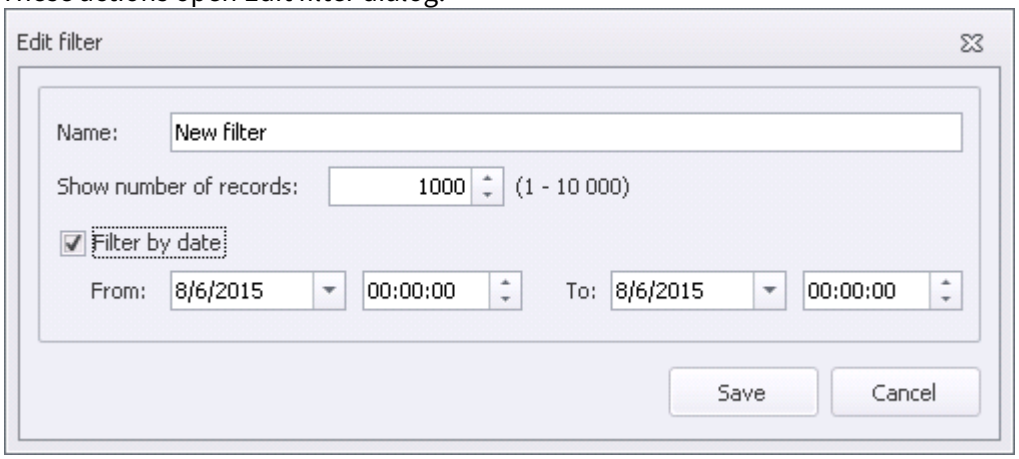
To add or edit a filter:

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

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

Action	Steps
	- in Main Menu click **Edit > Edit Filter**; - click **Edit Filter** at the top of Navigation pane; - double-click selected filter name and in the menu press **Edit**; - press Ctrl+E.

These actions open Edit filter dialog.



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

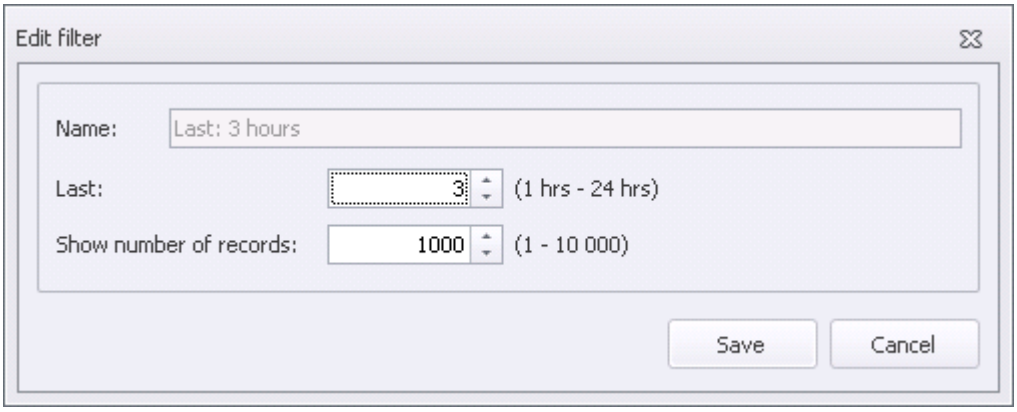
   > **Note:**
   >
   > For the predefined filters **Filter Name** and **Filter by date** parameters cannot be edited.

4. Click **Save**.

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

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

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



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

4.5.2 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.

4.6 Agent Remote Installation, Updating and Uninstallation

To perform the remote Agent management tasks a special distribution Agent is used, which is sent onto agent workstations. To operate correctly the Agent should be provided with the following conditions: You can install, update, or delete InfoWatch Device Monitor Agents centrally from a computer via InfoWatch Device Monitor Management Console. These operations are performed through **tasks**. You can run tasks to install, update or remove agent software, change uninstallation password, or monitor these processes.

- Target computers must meet hardware and software requirements: see the document "*InfoWatch Traffic Monitor. Installation guide*", "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 task section, use **Tasks** button on Navigation pane. Tasks management guidelines are available in:

- View Tasks
- Preparing Primary Agent Installation
- Detecting Workstations to Install the Agents on
- Creating Primary Distribution Task
- Creating Update Task
- Creating Uninstallation Password Reset Task
- Creating Uninstallation Task
- Launching, Pausing, Editing, and Deleting Tasks
- Agent Installation Errors
- Creating Template of Distribution Task.

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

4.6.1 Viewing Tasks

Tasks area of Navigation panel displays a list of all created, executed and outstanding tasks, as well as templates for automatic creating primary distribution task. Main workspace window displays a list of workstations for which the selected task is being performed.

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: • Initial deployment • Change uninstall password • Update • Uninstall
Status	Current task status. Possible values: • Created • Executing • Stopped • 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.
For primary distribution tasks	
Show employee notifications	Indicates that employee's attempt to perform a banned action will trigger a warning. For further details, see "General System Settings", "Creating Installation Package" and "Employee Notifications about Policy Violations"
Hide 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. **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.

Parameter	Description
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, is specified.
Proxy Root Issuer DN	The unique name of Device Monitor proxy server certificate, Issuer Distinguished Name.
For primary distribution and update tasks	
Installation directory	Installation directory for Device Monitor Agent at target computers.
Installation login	Name of the Console user that launches the task on computers.
Waiting for 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 (5 min) are expired, but the employee did not reboot the computer.
Uninstallation product password	Shows if the password, requested from a user who attempts to remove Device Monitor Agent, is specified.

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: • NEW **Not running**

Parameter	Description
	•  **Prepare to start** •  **In progress** •  **Waiting for reboot** (only for installation and upgrade tasks) •  **Error** (for further details, see "Agent Installation Errors") •  **No access** •  **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.

4.6.2 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.

Enabling Shared Administrative Resources

To transfer InfoWatch Device Monitor distribution agent to target computers with Windows OS through shared administrative resources, make sure that the following requirement is met:

Shared administrative resources (like `\\computername\admin$`) must be enabled on workstations (in Windows Vista, Windows 7, Windows 8, Windows 10 and Windows 11 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.

Firewall Settings

Firewall settings requirements:

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

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

4.6.3 Detecting Workstations to Install the Agents on

The distributive of Device Monitor server contains the utility that scans a range of ip addresses. It is installed atomatically together with Device Monitor management console. The result of scanning is a text file with a list of ip addresses or domain name - OS of the workstations on which the Agent was not installed.

As the utility does not have a graphic interface, you can run it using a command line. The table below contains the parameters you need or can specify when you run the utulity. You can see their description by entering the command: `Iw.Util.MachineDiscovery.exe -- help`.

`--mode arg (=icmp)*`	Network scanning mode (mandatory parameter): • `nmap` - scans the network using nmap utility which can additionally recognize the type of the OS with the help of heuristic algorithms • `icmp` - scans the network using icmp protocol
`--ip-range arg`	A range of ip addresses in one of the formats valid for nmap (mandatory parameter). Example: "`--ip-range 10.60.3-35.1-254`"
`--ip-cidr-range arg`	A range of ip addresses in CIDR format (mandatory parameter). Example "`--ip-cidr-range 10.60.3.4/24`"
`--ipv6-cidr-range arg`	A range of IPv6 addresses in CIDR format (mandatory parameter if IPv6 protocol is being used). Example: "`--ipv6-cidr-range fe80::98b9:ec9:f9a9:9104/120`" **Warning!** For Ipv6 addresses only CIDR format is supported
`--threads arg (=2)`	Number of threads to process acynchronous requests of network scanning.
`--icmp-attempts arg (=2)`	The number of attempts to request an ip address using icmp protocol, before the address is recognized anavailable. As icmp protocol, unlike tcp protocol does not guarantee packages delivery, then the packages may be lost. So to be sure that the address is anavailable, there is need to have several attemps.
`--icmp-timeout arg (=5000)`	Timeout for address response for each attempt that checks its availability.
`--deploy-agent-port arg (=15505)`	Port of deploy agent which it uses to listen the network. Recommended to not change
`--output-file arg`	Path to the file with utility's work results.
`--nmap-path arg (nmap mode)`	Path to cross-platform nmap utility when the mode is "nmap".

`--nmap-os-info arg (=1)`	Recognize (=1) or not (=0) the OS of workstations while scanning in "nmap" mode
`--nmap-save-output-to-file arg (=1)`	Save stdout and stderr Nmap'a in the file Nmap_output_%Y-%m-%d_%H-%M-%S.log
`--nmap-timing arg (=3)`	How often to scan using nmap: • from 0 - the slowest and the most exact • up to 5 - the fastest and the least exact
`--nmap-min-hostgroup arg (=16)`	Minimum size of group to be scanned simultaneously by nmap.
`--nmap-max-hostgroup arg (=16)`	Maximum size of group to be scanned simultaneously by nmap (up to 1024).
`--nmap-min-parallelism arg (=10)`	Minimum number of requests for a group of hosts (from 1).
`--nmap-max-parallelism arg (=10)`	Maximum number of requests for a group of hosts.
* - the value in brackets is the default one	

To start the utility:

1. Using the command line on the workstation with Device Monitor console, enter the command `cd` to go to directory containing the utility Iw.Util.MachineDiscovery.exe:
   cd <path_to_utility>
2. Run the utility, herewith you are required to specify a range of ip addresses and other parameters, if needed. As per our example:
   `Iw.Util.MachineDiscovery.exe --ip-range 10.60.3-35.1-254`
3. Wait till the scanning process ends.
4. When the scanning is finished, the results will be recorded in the text file `iw_machine_discovery.output.txt` in the directory where the utility is stored `C:\Program Files\InfoWatch\Device Monitor\Management Console\Utils`. Load the file to the primary distribution task when creating a list of computers to install Agents on (see "Creating Primary Distribution Task").

4.6.4 Creating Primary Distribution Task

Primary distribution (installation from DM Management Console) of InfoWatch Device Monitor Agent is performed using **installation agents**. The installation agent is an executable file. During the task execution, it is sent to workstations and starts automatically. The current Agent version is received from the server.

Warning!

If the account under which the server is running doesn't have administrator rights on all target computers, then the primary Device Monitor Agent distribution will require credentials of an account with administrator rights for:

- All target computers;
- A computer where Management Console is running;
- A computer where Device Monitor server is running.

If the password of Windows account is expiring (Windows displays a warning that the password expires in 3 days and needs 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 "Creating Installation Package") and install it by other means (see "*InfoWatch Device Monitor. Installation, Configuration and Administration Guide*", article "Standard InfoWatch Device Monitor Agent Setup" and "Agent Setup via Software Distribution Tools").

Warning!

If Kaspersky Internet Security is installed on the workstation, then you need to disable its self-protection to install the InfoWatch Device Monitor Agent. For details, see the Internet article "How to enable or disable Self-Defense in Kaspersky Internet Security".

To create a primary distribution task for InfoWatch Device Monitor Agent:

1. Go to **Tasks**.
2. Take one of the following steps:
   - In the Main Menu, select **Edit** -> **Create Task**;
   - Click **Create Task** at the top of the Navigation panel.

   The **Deployment task wizard** will open.
3. Select **Initial deployment task** (to install Agent on computers with Windows OS), enter the task name, select **Initial deployment task** and enter the task description, then click **Next**.
4. Task creation master will display:
   - Storage addresses which are points of Agent distribution to workstations;
   - The version of Agent on the distribution points, which is specified in general system settings. See "Device Monitor Server Settings. Connecting to Traffic Monitor Server" for details.

   If needed, you can change these parameters and set a different number of attempts to download update.
   Click **Next**.

   Note:

   You can view all available versions at `C:\ProgramData\InfoWatch\SetupPackages\`.

5. Create a list of computers to which you want to install Device Monitor Agent. To add a computer (or several computers):
   a. Click **Add**. You can select computers:
      - By a name typed in search string in the directories connected ()
      - By a directory;
      - From Microsoft Windows Network;
      - From ALD tree;

- From computers that have already been registered (for example, after manual Agent installation) and belong to existing computer groups (**DM computer groups** node).

b. Click **Connect to all the categories**, if you need to select computers from directories that are not connected yet.

c. Select computers or computer groups. Collapsed groups are marked with ▶, expanded ones are marked with ▼. Doubleclick a group to expand or collapse it.
You can also specify computer names or IP addresses:
   - In the line at the bottom of dialogue box. When listing addresses, separate them with semicolons;
   - By clicking **Import** and downloading a text file with listed IP addresses or DNS names of computers. Each entry should begin with a new line; blank lines are not allowed. You can create the file using a scanning utility (see "Detecting Workstations to Install the Agents on").

d. After you specify all computers you want to add, click **Select**. The dialogue box will close and the **Task target computers list** area will display selected computers. To remove a computer from the list, select it and click **Remove**. When the list of computers is ready, click **Next**.

6. The **Deployment task wizard** displays servers registered with the System. You can change the Agent installation directory (by default, it is `%Program Files%\InfoWatch\DeviceMonitor\Client`).

> **Warning!**
>
> Path to the catalogue may contain the following characters: 0-9, a-z, A-Z, ":", ".", "_", "-", "\", " ". If the path includes other characters, the Agent will not be installed properly.

   Click **Next**.
7. A unique name of Device Monitor proxy server certificate (Issuer Distinguished name, Proxy Root Issuer DN) will be displayed. You can change it in accordance with X.509 standard, CN (Common Name) field is required, fields inside the name should be separated by commas. Click **Next**.
8. Configure Agent settings:
   - To prevent deleting Agents by employees, enter a password that is required to uninstall the Agent and confirm the password.
   - **Hide agent's presence on computer until the configuration from DM server is received** – the System will hide the Agent's presence on the computer until a connection with the DM server is established.

> **Warning!**
>
> The fact that you do not notify users about interceptors running on their computers may contradict the applicable laws of your country.

> **Warning!**
>
> Hiding/notifying settings apply on the Agent until the first call to the server. Once the workstation addresses the server, the Agent starts using settings of the workstation group it belongs to.

> **Warning!**
>
> If an antivirus system is enabled on the computer, it can reveal the presence of Device Monitor: for example, in the list of running processes or in the list of programs that initiate 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 interception** – installs **iw_proxy** component on the computer.
  The component will not be installed if you leave the checkbox empty.
- **Install the component of network control** – installs **Network Monitor** interceptor on the computer. The component will not be installed if you leave the checkbox empty.

> **Warning!**
>
> We do not recommend installing the component of network perimeter control to the image that will be used as the base image of VDI framework under control of Citrix Provisioning Services, as it will affect the technology and the performance of the whole scheme.

- Specify task restart parameters: they will be used if the task wasn't launched at the first attempt. Specify the number of attempts and their intervals, in minutes. If the first launch ended with an error, the task will not be launched again.
- To launch the task immediately after saving, select the **Run task immediately** option.
- Enter the credentials for the account that launches the task. This account must have administrator rights on all target computers.

> **Warning!**
>
> The user launching the primary distribution task must have a password. Otherwise, the launch is not possible.
>
> The System does not save passwords for the accounts that are used to launch tasks.
>
> If a new task is not launched immediately, you will need to enter the password the next time to launch the task from the Management console.
>
> If a password of the Windows user account is expiring (Windows displays a warning that the password expires in 3 days and needs to be changed), then primary distribution task cannot run on behalf of this user.

Click **Next**.

9. Specify options of the computer reboot.

> **Note:**

If at the previous step, you have selected the **Hide agent's presence on computer until the configuration from DM server is received** option, then these options are unavailable.

Possible values:

- **Wait for reboot without notifying the employee**. The Agent can:
  - Start notifications immediately (*Do not wait* option);
  - Start notifications after the specified time (*Wait for* option – specify the time after which to start notifications);
  - Not show notifications at all (*Wait infinitely* option).
- **Notify the employee about reboot necessity and wait for reboot**. When waiting in the "silent" mode (the **Wait for reboot without notifying the employee** option) ends or immediately after the installation, Device Monitor Agent starts notifying the employee that reboot is required:
  - During a specified time period (*Notify within* option);
  - Permanently (*Notify infinitely* option);
  - Not show notifications at all (*Do not notify* option).

  If needed, change the duration and frequency of notifications and enter the message text that is displayed in the notification. The message can contain not more than 255 characters.
- **Show a warning before forced reboot**. If the option is selected, then the Agent displays a notification about forced reboot. The computer will be restarted in 5 minutes during which the employee can finish operations. If the option is not selected, then the forced reboot (if required according to settings) will be performed without notifying the employee.

  Warning!

  Forced reboot is performed if neither the **Wait while employee is rebooting computer** setting, nor the **Show a warning before force reboot** option is selected, or if the waiting time has expired but the employee has not restarted the computer.

Click **Next**.

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

4.6.5 Creating Update Task

Warning!

When upgrading Device Monitor from versions below 7.2 you should update the agents using the primary distribution task only (please see "Creating Primary Distribution Task" article). When upgrading from version 7.2 and above you should follow the instructions described in this article.

You should update Device Monitor Agents after you update InfoWatch Device Monitor server end: 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 use the automatic creation of update tasks for selected computers as described in the document "*InfoWatch Traffic Monitor. Installation guide*", "Updating Agents at Managed Computers" article.

To create an update task for InfoWatch Device Monitor Agents, go to **Tasks** and take one of the following steps:

- in the Main Menu, select **Edit** -> **Add Task**;
- click  **Add Task** at the top of the Navigation pane.

In the **Deployment task wizard** that opens, take the following steps.

1. 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**.
2. Task creation master will display the storage addresses which are Agents distribution points to workstations and the latest version of Agent installed to workstations. If required you can change these parameters and set a different number of attempts to download update.
   Click **Next**.
3. Create a list of computers where Device Monitor Agents should be updated. To add a computer (or several computers):
   a. Click **Add**. The **Select computers** dialog, **DM server computers** node, will display the list of computers where Device Monitor Agent version does not match Device Monitor Server version and they can be automatically updated (agent software version should be 4.0.651 or higher).
   b. Select computers or computer groups. Collapsed groups are marked with , expanded ones are marked with . Double-click a group to expand or collapse it.
   c. You can also use the **Filter by computer name** field to find a computer. To start the search, click **Find**.
   d. After you specify the computers you want to add, click **OK**. The **Select computers** dialog will be closed and the **Task target computers list** area will display selected computers. To remove a computer from the list, select it, and click **Remove**.
   When the list of computers is ready, click **Next**.
4. Task creation master will display the unique name of certificate for Device Monitor proxy server (Issuer Distinguished name, Proxy Root Issuer DN). If required you can change these parameters; but the name should comply with X.509 standard, contain CN field (Common Name), fields should be separated by comma.
   Click **Next**.
5. Specify parameters of restarting computers:
   - **Wait for reboot without notifying.** The Agent can**:**
     - notify the employee immediately (*Do not wait* parameter),
     - notify the employee after the specified time period (*Wait for hour(s)* parameter - you need to specify the time before notification),
     - not notify the employee (*Wait infinitely* parameter).
   - **Notify the employee about reboot necessity and wait for reboot.** When waiting in the "silent" mode (the **Wait for reboot without notifying the employee** option) ends or when the update process is complete, Device Monitor Agent starts notifying the employee that reboot is required during a specified time period (*Notify within hour(s) within: minutes* parameter) or infinitely (*Notify infinitely every x minutes*), or it does not notify the employee (*Do not notify*). If needed, change the duration and frequency of notifications and enter the message text that is displayed in the notification. The message can contain not more than 255 characters.

- **Show a warning before reboot** - if the option is selected, then a notification about a forced reboot will be displayed (the employee can complete current tasks within 5 minutes before the forced reboot). Otherwise, a forced reboot will be performed without notifications.

> **Warning!**
>
> If the **Hide Agent presence** option is enabled on the workstation, notifications are not displayed.

6. Specify the task run parameters: they will be used if the task wasn't launched at the first attempt. Specify the number of attempts and their intervals, in minutes. If the first launch ended with an error, the task will not be launched again.
   If necessary, select the **Run task immediately** option to launch the task immediately after saving.
   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 Kaspersky Internet Security is installed on the computer, then you need to disable its self-protection function before updating InfoWatch Device Monitor Agents.
>
> See details in the Internet article "How to enable/disable self-defense in Kaspersky Internet Security".

4.6.6 Creating Uninstallation Password Reset Task

To create task to reset password required to uninstall InfoWatch Device Monitor:

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.
   c. After you specify the computers you want to add, click **Select**. 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**.

4.6.7 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".

4.6.8 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 launching tasks of distributing/updating/deleting Agents on Astra Linux or RED OS, the System will require login and password to authorize on workstations. Herewith the user whose login and password are entered to launch, should be in the list of `sudo users` on the workstations specified in the tasks.

Note:

To install Agent on ALT Workstation 10 for the user under the name of which the task is launching, you need: Для установки агента на ОС Альт Рабочая станция 10 для пользователя, под учетной записью которого будет выполняться запуск задачи необходимо:

- manually enable access to the workstation via SSH by running the command: `service sshd start`
- uncomment the string `Per mitRootLogin` in the file `/etc/openssh/sshd_config`

Action	Steps
Start task	• in the Main Menu select **Edit > Perform** task • click **Perform task** located at the top of Navigation pane • right-click the task and select **Perform** in the context menu
Stop task	• in the Main Menu select **Edit >Stop task** • click **Stop task** at the top of the Navigation pane • right-click the task and select **Stop** in the context menu
Edit list of computers in task	• at the top of **Task execution result** panel, click **Add computer** or **Exclude computer from task**

Action	Steps
	• right-click the computer row and select **Add computer** or **Exclude computer from task** • press Ctrl+Shift+N to add the computer to the task or Delete to exclude the computer from the task **Warning!** You can't remove a computer if the task is running and not completed.
Edit task	• in the Main Menu, select **Edit > Edit** • click **Edit** at the top of the Navigation pane • right-click on task name and select **Edit** • double-click the task name • press Ctrl+E Specify the task parameters, as it is done while creating a task (see "Creating Primary Distribution Task", "Creating Updating Task", "Creating Uninstallation Password Reset Task", "Creating Uninstallation Task")
Delete task	• in the Main Menu, select **Edit > Delete** • click **Delete** at the top of the Navigation Pane • right-click on task name and select **Delete** • press Ctrl+D **Warning!** You can't delete a task if it includes computers with running tasks.
View computer error log	• at the top of **Task execution result** panel, click **Computer log** • right-click the computer row and select **Computer log** • press Ctrl+L

4.6.9 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".

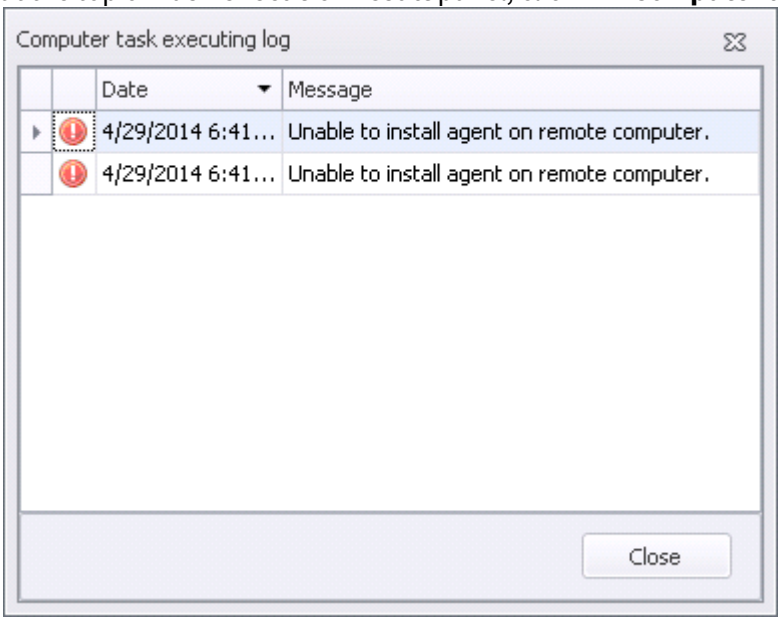
To view task errors:

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 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:
   - error description;
   - error code;
   - log entries in error's description.

> **Warning!**
>
> Log entries are available only for the error with the latest date of occurrence.

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.

4.6.10 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 installation 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. 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, a warning will be displayed. For further details, see "Employee Notifications about Policy Violations".
   - **Hide Agent presence** - indicates if Windows system tray of managed computer hides 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.

   Warning!

   If "Hide Agent presence" is activated on the computer, notification about computer reboot will not be displayed.

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**.

5. 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. The message can contain not more than 255 characters.
   - **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**.
6. Look through the task summary. If you need to change any settings click **Back** to return. If all settings are correct, click **Finish**.

The folder you've specified during the first step will contain InfoWatch Device Monitor Agent original installation packages together with supplying scripts to be used to launch as per parameters you've set when forming the packages. Scripts names are formed as follows: "<Name of msi package>.msi.cmd". The script content includes the

command line for msiexec, to be used to launch a specific package. In case the third party distribution system can specify the distribution parameters, the script file data can be used to be send to distribution system. Unless its not provided, the launch should be performed as script manual running.

> **Warning!**
>
> When launch the package with no parameters specified or with no script used, the installation is to be run with default values (as specified above). In accordance with installation context this may result in Agent's launch, which is connected to none InfoWatch Device Monitor server.

4.6.11 Creating template of distribution task

To create a primary distribution task for InfoWatch Device Monitor Agent :

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

   Create distribution task template wizard will open.
3. Enter the task name (should be unique) and its description, then click **Next**.
4. Create distribution task template wizard will display default installation parameters of InfoWatch Device Monitor Agent:
   a. Specify the directory where Agent should be installed (by default it is `%ProgramFiles%\Infowatch\DeviceMonitor\Client`).

   > **Warning!**
   >
   > Path to the catalogue may contain the following characters: 0-9, a-z, A-Z, ":", ".", "_", "-", "\", " ". If the path includes other characters, the Agent will not be installed properly.

   b. Specify distribution point - the storage address where Agent distributive is to be loaded:
      i. Click **Change**,
      ii. If needed, select another distribution point from previously specified (for more details, see "Distribution points").
   c. Specify the number of attempts to load the update.

   Click **Next**.
5. The **Deployment task wizard** will display a unique name of Device Monitor proxy server certificate (Issuer Distinguished name, Proxy Root Issuer DN). You can change it with accordance to X.509 standard, CN (Common Name) field is required, fields inside the name should be separated by commas.
   Click **Next**.
6. Configure Agent's settings:
   - To prevent deleting Agents by employees, enter a password that is required to uninstall the Agent and confirm the password.
   - **Hide agent's presence on computer until the configuration from DM server is received** - the System will hide the Agent presence on the computer until a connection with the DM server is established.

> **Warning!**
>
> The fact that you do not notify users about interceptors running on their computers may contradict the applicable laws of your country.

> **Important!**
>
> Hiding/notifying settings apply on the Agent until the first call to the server. Once the workstation addresses the server, the Agent starts using settings of the workstation group it belongs to.

> **Warning!**
>
> If an antivirus system is enabled on the computer, it can reveal the presence of Device Monitor: for example, in the list of running processes or in the list of programs that initiate 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 the 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 the computer. The component will not be installed if you leave the checkbox empty.

> **Warning!**
>
> We recommended not installing the component of network perimeter control to the image that will be used as the base image of VDI framework under control of Citrix Provisioning Services as it will affect the technology and the performance of the whole scheme.

- Specify task restart parameters: they will be used if the task wasn't launched at the first attempt. Specify the number of attempts and their intervals, in minutes. If the first launch ended with an error, the task will not be launched again.
- To launch the task immediately after saving, select the **Run task immediately** option.
- 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 a new task is not launched immediately, you will need to enter the password the next time to launch the task from the Management Console.
> If a password of the Windows user account is expiring (Windows displays a warning that the password expires in 3 days and needs to be changed), then primary distribution task cannot run on behalf of this user.

Click **Next**.

7. Specify options of the computer reboot.

   > **Note:**
   >
   > If at the previous step, you have selected the **Hide agent's presence on computer until the configuration from DM server is received** option, then these options are unavailable.

   Possible values:
   - **Wait for reboot without notifying the employee**. The Agent can:
     - start notifications immediately (*Do not wait* option),
     - start notifications after the specified time (*Wait for option* - specify the time after which to start notifications),
     - not show notifications at all (*Wait infinitely* option).
   - **Notify the employee about reboot necessity and wait for reboot**. When waiting in the "silent" mode (the **Wait for reboot without notifying the employee** option) ends or immediately after the installation, Device Monitor Agent starts notifying the employee that reboot is required:
     - during a specified time period (*Notify within* option);
     - permanently (*Notify infinitely* option);
     - not shows notifications at all (*Do not notify* option).

     If needed, change the duration and frequency of notifications and enter the message text that is displayed in the notification. The message can contain not more than 255 characters.
   - **Show a warning before forced reboot**. If the option is selected, then the Agent displays a notification about forced reboot. The computer will be restarted in 5 minutes during which the employee can finish operations. If the option is not selected, then the forced reboot (if it required by already specified settings) will be performed without notifying the employee.

     > **Warning!**
     >
     > Forced reboot is performed if neither the **Wait while employee reboots computer** setting, nor the **Show a warning before force reboot** setting is selected, or if the waiting time has expired but the employee has not restarted the computer.

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

4.7 Additional Features

You can use the following functions to enhance your Management Console experience: filtering, grouping and sorting table entries.
Certain functions can be also accessed with hotkeys.

4.7.1 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;

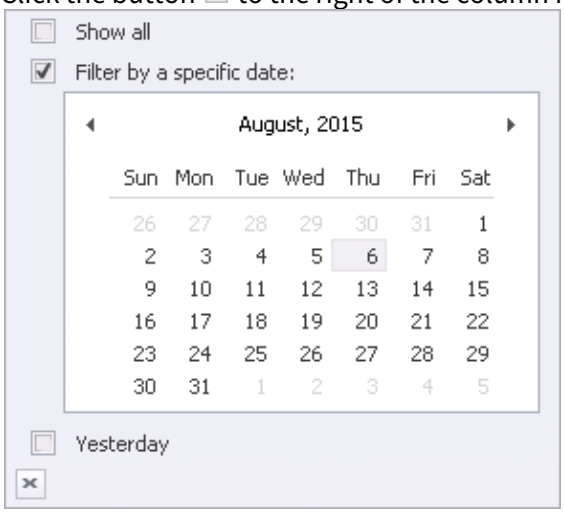
- Applying Standard Filters;
- Custom Filter;
- Editing Filters;
- Removing a Filter.

Filtering by Date

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

To view the records for specific date or period:

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



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

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").

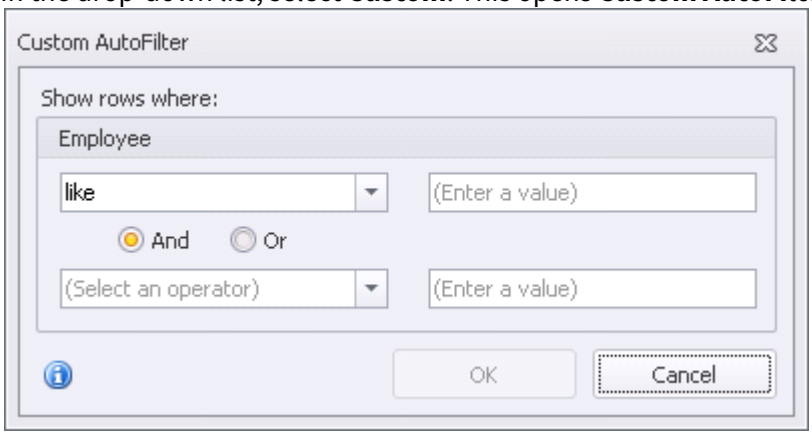
The table will only display filtered values.

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.

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.

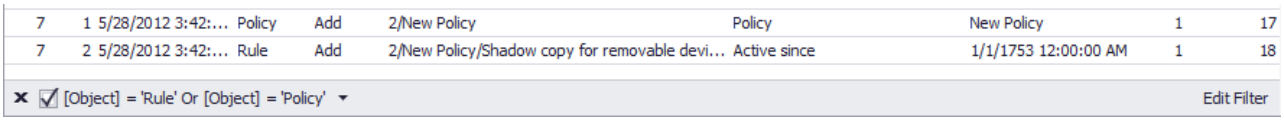
     > **Note:**
     >
     > You can use comparison operators to limit filtering criteria: *equal, not equal, greater than, greater than*
     > *or equal to, less than, less than or equal to; values empty (blank) and nonempty (non-blank field)*; or
     > text filter with a mask. To get a text filter syntax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

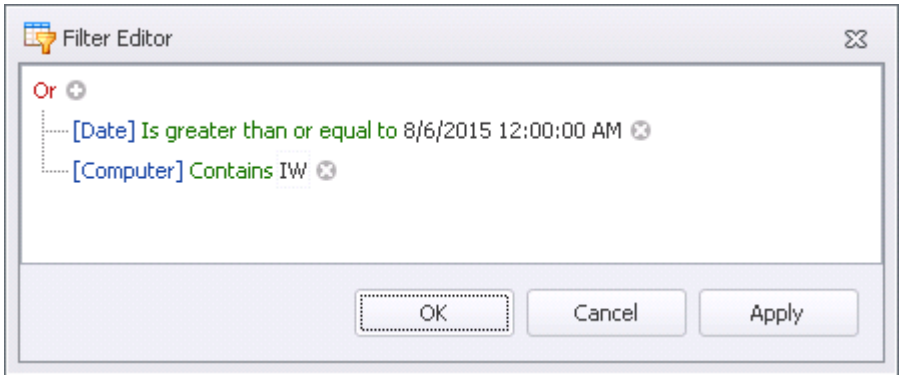


To remove filter and view all items, clear the check box in filter string. To apply the filter again, select the check box. To re-use a filter, click the filter string and select filter from drop-down filter history list. Custom filters are stored until you close the window with filtered content.

Editing Filters

To edit active filter:

1. Click **Edit Filter** at the end of the filtering conditions string. The following dialog box displays **Filter Editor**.



2. Edit filtering criteria. Available actions:

Action	Steps
Edit an attribute, attribute value or operator	1. Click attribute/value name of attribute/operator 2. Select the value from the drop-down list or enter the value to the field
Add a simple condition	Click the button ⊕ to the right of the logical operator or Click **Add Condition** in logical operator menu
Delete condition	Click the button ⊕ at the end of condition string

Action	Steps
Add criteria group	1. Click the logical operator name 2. Select **Add Group** in the menu
Delete criteria group	1. Click the name of operator criteria group 2. Select **Delete Group** in the menu
Delete all criteria	Click **Clear All** in logical operator menu

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

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.

4.7.2 Grouping or Sorting Entries

Grouping function is intended for managing table entries according to selected scheme. Group scheme is displayed on the group panel over the column title row. Contents are grouped basing on a single attribute (table column) or more.

To group contents basing on an attribute:

1. In table 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 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 an 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 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.

4.7.3 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
Get help	
Open offline documentation, PDF format	F1
Open online documentation	Ctrl+F1
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
Go to White Lists	Ctrl+4
Go to Signatures	Ctrl+5
Go to Applications	Ctrl+6

Feature name	Hotkeys
Go to Log	Ctrl+7
Go to Tasks	Ctrl+8
Go to Events	Ctrl+9
Manage security scheme (overview)	
Go to security scheme editing mode	F11
Save security scheme	F12
Cancel security scheme saving	Shift+F11
Unblock security scheme (Superuser only)	Ctrl+Shift+U
Update security scheme	F5
Go to the latest security scheme version (when viewing an earlier version)	F9
Manage security policies	
Add security policy	Ctrl+N
Edit security policy	Ctrl+E
Delete security policy	Ctrl+D
Manage rules	
Add rule	Ctrl+Shift+N
Edit rule	Ctrl+Shift+E
Delete rule	Delete
Manage employee groups	
Add new employee group	Ctrl+N
Edit employee group	Ctrl+E

Feature name	Hotkeys
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 scheme	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 scheme	Shift+Delete
Manage white lists	
Add white list	Ctrl+N
Edit white list	Ctrl+E
Delete white list	Ctrl+D
Edit white list entries	Ctrl+Shift+E
Manage signatures	
Add signature category	Ctrl+N
Edit signature category	Ctrl+E

Feature name	Hotkeys
Delete signature category	Ctrl+D
Remove signature from category	Delete
Configure filters for Audit Log and Event Viewer	
Add filter	Ctrl+N
Edit filter	Ctrl+E
Delete filter	Ctrl+D
Manage Agent remote installation and update 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

5 End-user license agreement

ATTENTION! Please read the terms and conditions of this End-User License Agreement (hereinafter referred to as the "Agreement") carefully before using the Software. Installation and/or use of the Software shall constitute your full and unconditional acceptance of all the terms and conditions of this Agreement.

If you do not accept to the terms and conditions of this Agreement, or if you enter into this Agreement on behalf of a legal entity, but you do not have such authority, you must interrupt the installation and/or stop using the Software and delete any copies of the same.

1. Grant of License

1.1. This End-User License Agreement shall constitute a standard form contract entered into by and between the End User and Laboratory InfoWatch LLC, Taxpayer Identification Number (INN) 7734583888 (hereinafter referred to as the "Copyright Holder").

1.2. You shall be granted hereunder a personal, non-transferable and non-exclusive license granting you the rights to use the Copyright Holder's software (hereinafter referred to as the "Software"), namely the rights to download, install, backup and use the Software for its intended purpose, as set forth in the Software Documentation (User's Guide, Administrator's Guide, Installation Guide), this Agreement and your Licensing Agreement. The Software Documentation shall be an integral part hereof.

1.3. If you have received, downloaded and/or installed the Software for information, you may use the Software only for informational purposes and only during the trial period. Any use of the Software for any other purposes or after the trial period shall be prohibited.

1.4. If you use different Software versions or Software versions for different languages, or if you receive the Software on several media, or if you otherwise receive several copies of the Software or receive the Software as part of a package of other software, the total number of your licenses shall not exceed the number specified in your Licensing Agreement.

1.5. You may make a copy of the Software, provided that such a copy is intended only for archival purposes or to replace a duly purchased copy in cases where the original is lost, destroyed or becomes unusable. This copy may not be used for any other purposes and shall be destroyed, if the possession of the Software copy ceases to be legitimate.

1.6. You shall be solely responsible and ensure compliance with the applicable export and import laws, as well as applicable trade sanctions and embargo with regard to the transfer of rights and use of the Software.

2. Terms and Conditions of Use

2.1. The Software is intended solely for use in analyzing and checking corporate information, and specifically for detecting and preventing unauthorized use of confidential data.

2.2. You shall use the Software exclusively in accordance with the applicable statutory requirements of the Russian Federation or any other countries, including but not limited to:

- legislation on personal data;
- legislation on trade secrets;
- legislation on combating the misuse of insider information;
- anti-corruption legislation;
- legislation on critical information infrastructure;
- legislation on state information systems;
- National Payment System data protection legislation;
- statutory provisions of the Labor Code of the Russian Federation;
- and any other applicable sources of law.

2.3. You may not use the Software for any purpose or in any manner that violates applicable law, this Agreement and/or any third-party rights. The Copyright holder shall not be liable for your breach of this Clause.

2.4. If you are not a resident of the Russian Federation, you shall use the Software in full compliance with applicable law, including laws and regulations on personal data and trade secrets.

2.5 In order to avoid your violation of Articles 138, 138.1 of the Criminal Code of the Russian Federation, Article 23 of the Constitution of the Russian Federation or any other legal regulations, before using the Software, you are recommended to inform your employees in writing that:

- this Software is used on the workstation computer, and you should inform your employees about the features of this Software and data that may be obtained as a result of using the same;
- the workstation computer and the communication channels used (e-mail, local corporate network, telephony and IP-telephony, etc.) are your property and are provided to such employees for temporary use so that they could perform their official duties;
- all information created on the workstation computer is your property and is subject to inspection and logging on a legal basis.

2.6. Please note that you need to obtain the consent of the persons whose data will be processed when using the Software to the relevant collection, storage, use, processing, distribution or any other form processing of such data.

2.7.We remind you that installing a program on another person's computer without prior authorization from such a person, obtaining personal data of any third party without his/her consent, violating privacy, breaching confidentiality of correspondence, telephone conversations, telegraphic or any other types of messages shall constitute a criminal offense and shall be prosecuted, as prescribed by the current legislation of the Russian Federation.

2.8. The Copyright Holder shall not have access to the data created and/or obtained as part of your use of the Software. You shall have exclusive access to such data. In view of the foregoing, the Copyright Holder shall not collect, or store, or use, or distribute such data.

2.9. You shall be held fully and solely liable if the information created and/or obtained as part of your use of the Software contains unethical and/or illegal data, computer viruses or programs (or links thereto) that may interrupt or disrupt the standard features of computer equipment, software or telecommunication facilities of any persons.

2.10. You shall not:

- edit, change, adapt, translate, decompile, disassemble, reverse engineer, create or recreate source code, modify the Software, whether in full or in part, or attempt to do so in respect to the Software, or create derivative works based on the Software and/or Documentation;
- integrate the Software into any third-party website or software product, except where such integration is expressly authorized by the Copyright Holder and the copyright holder of such a third-party website or software product. The Software may be integrated into a third-party software product only through the built-in API module within the features of such a module;
- remove or modify any notice of copyright, proprietary rights to the Software and/or its elements;
- let on lease, rent out or assign for temporary use, sublicense, distribute the Software or otherwise grant any rights with respect to the Software and/or Documentation to any person or entity, or disclose the results of development testing of the Software, except as expressly permitted by this Agreement;
- allow or provide access to the license key to any third party in violation of this Agreement and your Licensing Agreement;
- collect, systematize, store or disseminate confidential and/or personal information in violation of law;
- use the Software for unauthorized remote access to any third-party computer, or changing the configuration of the computer so that such features can appear in third-party software;
- use the Software to collect, store, use, process or distribute any information or data that violates the applicable laws or the rights and legitimate interests of any third party.

2.11. The license key shall constitute confidential information. The Copyright Holder shall reserve the right to use the means to verify the authenticity of the license key you have installed.

3. Disclaimer of Warranties and Liability of the Copyright Holder

3.1. The Software shall be provided "AS IS" in accordance with generally accepted international business practice. The Copyright Holder shall not be responsible for any issues arising during the operation of the Software, including those related to compatibility with other software products (packages, drivers, etc.) or those arising from ambiguous interpretation of the Software Documentation, or for failure of the Software to meet your expectations, etc.).

3.2. You confirm that you are aware of the features of the Software licensed hereunder, and you shall be held fully and solely liable if the Software or the results of using the same do not meet your individual needs or expectations.

3.3. The Copyright Holder makes no warranties, whether expressed or implied, and hereby disclaims all warranties.

The Copyright Holder makes no representations or warranties regarding the fact that the Software is flawless, uninterrupted, fast or accurate, and shall not be resposible for any direct or indirect consequences of using the Software, including those arising from potential errors in the Software or typos in the Software and/or the Documentation attached thereto or further provided.

The Copyright Holder makes no representations or warranties and shall not be held liable in the event of any changes in a third-party software that occurred after the installation/deployment of the Software and resulted in a loss of the Software features (including, but not limited to, a change in the data transfer protocol, data storage format, logic of a third-party software, an update of a software that ceases to support the Software). The Copyright Holder makes no warranties or representations and sets no conditions or provisions (whether expressed or implied) in respect of any matters, including but not limited to infringement of third-party rights, merchantability, integration or fitness for a particular purpose.

3.4. Any data that becomes available in the course of using the Software, including any file, link, image or text, shall be the sole responsibility of a disclosing person or entity and shall be the property of such a person or entity. This Agreement shall not grant any rights to such data. You accept responsibility for any potential consequences, security risks or any losses caused by such data viewed or obtained by using the Software.

3.5. The Copyright Holder shall not be liable for any loss or damage, regardless of the reasons for such a loss or damage (including, but not limited to, direct or indirect damage, lost profits, interruption of commercial or business activities, loss of business information, negligence, or any other losses) arising from the use or failure to use the Software, even if the Copyright Holder has been notified of eventual losses. The Copyright Holder's liability shall be at any time limited to reimbursement for documented actual damage of up to Three thousand rubles (RUB 3,000). The Copyright Holder shall be held liable only for actions or omissions for which the Copyright Holder is at fault.

4. Intellectual Property Rights

4.1. You hereby agree that the exclusive rights to any intellectual property embodied in the Software and /or any documentation provided to you shall be vested in the Copyright Holder. The Software shall not be assigned or sold hereunder, but shall be granted under a limited non-exclusive license. Nothing in this Agreement grants you any rights to the said intellectual property other than those conferred under your Licensing Agreement.

4.2. You agree that the source code and the license key for the Software shall be the property of the Copyright Holder.

5. Rights to Information Accessed in the Course of Performance of this Agreement

5.1. You hereby agree that you do not have any rights to any information that is not subject to intellectual property, as set forth in Section 4, accessed by you in the course of performance hereof.

5.2. Such information may include, but shall not be limited to, any system, method of work or any other information.

5.3. You may use the above information only for the purpose of exercising the rights to the Software granted under this Agreement and the Licensing Agreement. You may not use this information for your own benefit or beyond the scope of this Agreement or the Licensing Agreement.

6. Open Source Software

You are aware that the Software contains open source software distributed under certain licenses, available in the licenses.inf license.info file, provided together with the Software as part of the distribution kit.

7. Miscellaneous

7.1. This Agreement shall come into force immediately upon installing the Software and shall be valid throughout the period of use.

7.2. In the event that you violate any of the provisions of this Agreement and/or your Licensing Agreement, or in the event that the performance of this Agreement and/or your Licensing Agreement violates or may result in violation of the applicable laws, the Copyright Holder shall have the right to repudiate and terminate this Agreement (including, but not limited to, by blocking the license key, terminating the grant of rights) at any time without prior notice. To the extent set forth above in this Clause, you shall not be reimbursed for the cost of the Software/the amount of the Software license fee, or any eventual losses arising under this Agreement and/or your Licensing Agreement.

7.3. Upon termination or expiration hereof, the End User shall destroy all copies of the Software installed.

7.4. You are hereby notified that when the usage statistics collection function is enabled in the Software, the Software may collect and record anonymized information on:

a) hardware, operating system of the device on which the Software is installed and operated, as well as other technical data containing information on the use of hardware, hardware load and processing speed of the Software;

b) end user's activities in the user interface of the Software.

The Copyright Holder may use the specified data to make decisions on the development of features and improvement of the operational characteristics of the Software.

The Copyright Holder shall ensure the confidentiality of the data obtained and shall not disclose or transfer such data to any third party.

7.5. This Agreement, as well as any disputes arising out of or in connection with this Agreement, shall be governed by and construed in accordance with the laws of the Russian Federation.

7.6. All disputes and disagreements arising during the performance hereof shall be resolved through negotiations, if possible. In case of failure to reach an agreement, disputes shall be settled in court in the Arbitration Court of Moscow.

7.7. This Agreement may be amended by the Copyright Holder at any time without prior notice. The amended Agreement shall enter into force once it is posted at the address specified below in this Clause. The current version of the Agreement is always available at https://kb.infowatch.com/display/EULA/. By continuing to use the Software, you accept the amendments and/or additions made to this Agreement. If you do not accept the terms and conditions of such amended Agreement, you shall immediately discontinue the use of the Software.

8. Contact Details of the Copyright Holder

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

Sales Department: sales@infowatch.com

Technical Support: support@infowatch.com

Web site: www.infowatch.ru

6 Glossary

Term	Glossary
Active Directory	LDAP-compatible Microsoft directory services for the Windows NT operating systems family
Active policy	A policy included into a configuration that is uploaded to a host. See also: Policy, Host
Administrator	A preset role and user account in Management Console. An Administrator can modify other accounts and their rights. It is also a System user who installs, configures and maintains the System. See also: User role, Security officer, User
AJAX	Asynchronous JavaScript and XML is a group of interrelated Web development techniques used on the client-side to create asynchronous Web applications
Attachment	File attached to the intercepted event at any nesting level. See also: Event
Audit	Controlling of actions fulfilled by Management Console users: creating and managing the security scheme, System administrating. See also: Audit log, Management Console accounts
Blanks	Technology of searching the filled blanks of forms: questionnaires, receipts, etc. Blanks are stored in the System as digital prints, their text is not available for viewing to either users or System administrators. See also: Technologies, Technology element
Case-sensitive	Term setting: if the term is case-sensitive, the text search will detect only word forms which completely match upper- and lower-case letters defined in a term. See also: Term
Catalogues of persons, computers, and groups	Information about users, workstations, groups of users, and groups of computers imported from Active Directory, Domino Directory or Astra Linux Directory or created using Management Console. Used to simplify work with the events information.
Categories and terms	Technology of searching the words and phrases in the event text. The event where the term is found is referred to the category which this term belongs to. Old synonyms: Classifier, CFB. See also: Event, Term, Category, Technologies, Protected object

Term	Glossary
Category	Named term group characterizing some theme. If the System detects any term from the category in the text of the intercepted event, it associates the event with this category. See also: Term
Citation index	A measure of how close the sample document matches the text of the document being analyzed. See also: Sample document, Quote
Computer	A managed computer: workstation or terminal device. See also: Workstation, Terminal device
Configuration	A group of settings required to check events for data monitoring and analyzing. See also: Event, Technologies, Lists, Policy
Configuration version	A fixed state of the configuration designed to monitor changed settings of the event analysis. The configuration version is committed after uploading to a host. The configuration version can be active (currently used), editable (the last version with up-to-date modification) and saved (having changes and editable for users). See also: Configuration
Consul agent	Consul cluster member. It can be server or client.
Controlled persons	Set of persons, groups of persons and person's statuses which detection in the event results in associating this event to the person control policy which defines this set. See also: Persons, Person group, Person status, Person control policy
Copy mode	One of IW TM transport modes. In this mode, the actual traffic does not pass through the System. The copy of traffic is analyzed. In this mode, the traffic cannot be filtered by the System. See also: Transport mode
Copy rule	The rule that regulates copying and printing protected data. See also: Rule, Protected data, Data protection policy
Corporate security policy	A set of technical, organizational, administrative, legal, and physical measures, methods, rules, and guidelines that cover all security aspects in a company
Dashboard	Management Console section that displays on widgets the statistical information on the violations and violators. See also: Management Console, Widget, Violation
Data interception	A process of acquiring, parsing, categorizing, and converting data (or a copy) into context. It is possible to intercept data transferred using the following protocols: SMTP, HTTP, ICQ/OSCAR, Skype, IXP, XMPP, MMP, FTP. See also: Interceptor, Event context

Term	Glossary
Data interception channel	A data interception environment that includes technical appliances, software tools, and communication protocols. The System supports the following data interception channels: email (SMTP, IMAP, and POP3), Web (HTTP), instant messaging services (ICQ and Skype), shadow copies of files, connected/disconnected workstation events, and print jobs.
Database	A collection of data stored in accordance with a data scheme. Contains all information needed for the System.
Database unloadings	Technology of searching the quotes in the database. Database unloadings may be lists of salaries, other personal data, etc. See also: Technologies
Decision	The security officer’s conclusion on whether the event violates the corporate security policy or not. Possible values: "No decision", "Violation" and "No violation". See also: Security officer, Corporate security policy, Event, Event attributes, Violation, Policy, Verdict
Delivery status	Event attribute that specifies the possibility of event delivery to recipients after the analysis. If the event delivery has been allowed, then the attribute value represents the delivery tracking (completed or failed). See also: Event attributes
Digital print	A method of storing a sample document in the database in the form of a set of quotes. See also: Sample document, Quote
Document shadow copy	A copy of printed document received from the print job initiated on the managed computer. See also: InfoWatch Device Monitor
Domino Directory	IBM Lotus Domino Directory is a directory of information about users, servers, and groups. The Domino Directory is also a tool that administrators use to manage the Domino system.
Event	Objects of traffic interception (SMTP and IMAP and POP3 mail, HTTP requests, ICQ and Skype messages), shadow copies of files and print jobs. Generated by the System as a result of the data exchange between employees and others, including publication in media, copy to external devices and printing.
Event analysis	The procedure of processing of the attributes, attached files, and text of the intercepted events and of assigning additional attributes to the event. See also: Event, Policy, Event attributes
Event attributes	Structured data extracted from the events and assigned according to the processing results. See also: Event, Policy, Verdict, Decision, Transport mode

Term	Glossary
Event context	Internal representation of an intercepted event in the System. XML data (attributes, text) extracted from the event and its attachments. After processing the analysis results and the decision are added to the context. See also: Event, Technologies, Decision
Event text	Text information extracted from the event body and its attachments. Contains no formatting or markup. Used for analysis and search. See also: Event, Event body
File shadow copy	A copy of file recorded to a removable device. The copy is created only if the file is successfully saved on the removable storage device. See also: InfoWatch Device Monitor
File signature	A constant integer value that uniquely identifies a file of a certain type.
FTP	File Transfer Protocol is a network protocol used to transfer computer files from one host to another host over a TCP-based network, such as the Internet.
Graphical object	Technology of searching the images (passports, bank cards, etc) in the text and attachments of the intercepted events. See also: Technologies, Event, Protected object
Group of persons and computers	Group aggregating data on organization's users and computers and on external contacts. The groups can be AD Groups (imported from Active Directory) or TM Groups (created using IW TM). See also: Person, Computer, Contact
GTalk	Google Talk is an instant messaging service that provides both text and voice communication.
Headers	Supplemental data placed at the beginning of a block of data being stored or transmitted. Used for creating the event entity in the System and for determining the attribute values of this event. See also: Event, Event attributes
HTTP	HyperText Transfer Protocol, an application-tier protocol used to transfer the data in the text format. See also: HTTPS, HTTP(S) Monitor
HTTP query	A request formed according to the HTTP standards (POST request, GET request etc.) See also: HTTP, Event

Term	Glossary
HTTPS	Hypertext Transfer Protocol Secure is a network protocol for secure communication over a computer network. See also: HTTP, HTTP(S) Monitor
ICAP	Internet Content Adaptation Protocol is a lightweight HTTP-like protocol that allows you to control the incoming and outgoing HTTP traffic. It also makes it possible to modify the content of the HTTP requests.
ICQ	An Internet instant messaging service. Uses OSCAR protocol.
ICQ message	A message sent through the ICQ-OSCAR protocol. See also: Event
IMAP	Internet Message Access Protocol is a protocol for e-mail retrieval and storage
InfoWatch Activity Monitor	A software designed for monitoring employees' activity
InfoWatch Device Monitor	IW DM is software appliance designed to control the user access to peripherals and to monitor operations (data either copied to removable media and network storages or sent to print, network activity, applications usage) and intercepting messengers traffic (Skype, GTalk and Jabber) and so on.
InfoWatch Prediction	A software designed as a predictive and behavioral analytics tool
InfoWatchTraffic Monitor	IW TM software suite is designed to control various types of traffic (SMTP, IMAP, POP3, HTTP, HTTPS, IMAP, XMPP, ICQ, NRPC) and shadow copies of the data copied to the removable media and sent to printing.
Initiators	A person whose actions led to the event creation
Inline mode	IW TM system deployment mode which may block mail outgoing from the perimeter, followed by dispatching. IW TM Server is used as a relay server.
IW Lync Adapter	Interceptor of data communication events through MS Lync servers installed in the company infrastructure
Jabber	Messaging and information exchange system based on the open XMPP protocol
LAN	Local Area Network

Term	Glossary
License	Right to the System usage. Gained when buying the System and defines available users number, used technologies and interceptors and so on. See also: Technologies, Interceptors
Lists	Lists the similar data generated by Management Console to be used in policies creating. See also: Configuration, Policy
Lotus Adapter	Interceptor installed on the IBM Lotus server to redirect emails to IW TM for analysis. See also: Interceptor
Lotus Domino	IBM mail server whose messages are intercepted by Lotus Adapter
Management Console (TM)	A graphical user interface. Designed to manage InfoWatch Traffic Monitor (administration, configuring settings, event analysis, etc.).
Management Console (DM)	GUI element. It is designed to control InfoWatch Device Monitor (System administration, security scheme configuration, etc.).
Management Console user	User who manages the System. Each user has a role assigned basing on corporate security policy.
MAPI	Messaging Application Programming Interface is a messaging architecture and a Component object model based API for Microsoft Windows
Mask	A search pattern of characters and wildcards used to match folder and file names
Monitor	See: Interceptor
Morphology	Term setting: if morphology is used, the text search will detect all word forms of this term. See also: Term
MS Lync	Microsoft instant messaging client for corporate environments
MTProto	A cryptographic protocol used in the messaging system to encrypt user correspondence
Normal transport mode	A traffic analysis and filtering mode. In this mode, it’s possible to block the traffic forbidden by the System. See also: Transport mode, Inline mode
Notification	E-mail sent in case if the policy triggers on the event. Sent via Management Console to notify Management Console users,

Term	Glossary
	employees or third parties. Contains a summary on the intercepted events and attached message. See also: Policy, Event
Occurrence threshold	A number of text objects found in the event enough to detect the protected object where this occurrence threshold is defined. See also: Event, Text objects, Protection object
Perimeter	A container of company infrastructure elements and contact information. The perimeter is used to logically divide a company into structural elements and track the traffic of every element. See also: Group of persons and computers
Person	Account of employee or external contact that is contained in the System catalogue and allows to process the data belonging to this account as a whole and to user-friendly display data referring to it. See also: Group of persons and computers
Persons control policy	A policy to add rules controlling persons, person groups, and person statuses. See also: Policy, Person control rule, Person, Person status
Persons control rule	Rule that assigns attributes to the event of specified violation level and whose senders or recipients contain persons specified in the policy which includes this rule. Allows to re-assign person's status and to send notifications. See also: Rule, Event attributes, Person, Violation level, Person status, Notification, Person control policy
Placement rule	The rule that regulates storing protected data. See also: Rule, Protected data, Data protection policy
Platform	A set of components, subsystems, interfaces and production processes. The Platform acts as a base for deploying InfoWatch products and assembling ready-to-use software decisions from standardized components
Policy	A set of rules according to which the event analysis and processing facilities are performed. See also: Policy, Active policy, Rule
Policy of DM	A set of file monitoring rules for removable devices, network activity, printing, configuring peripherals access level etc. You can only assign security policy to a group (of employee or workstations). See also: DM Rule
POP3	Post Office Protocol Version 3 is an application-layer network protocol used by local e-mail clients to retrieve e-mail from a remote server over a TCP/IP connection

Term	Glossary
POST query	A query method designed to request that a web server accepted the data enclosed in the request message body for storage. Often used for file downloading of filled web-form representing
Privilege	Entity defining user's ability to perform some action (set of actions) when managing the System
Protected data	A set of protected objects, their catalogues and file formats whose detection in the event allows to characterize this event as fallen under the data protection policy where this set is defined. See also: Protected object, File format, Data protection policy
Protected object	The set of technology elements whose presence in the event allows the System to determine that this event belongs to a particular type of business documents (catalogue of protected objects). Protected objects are used in defining of data protection policies. See also: Technology element, Data protection policy
Proxy Server	The service that allows indirect requests to other network services. Proxy forwards all requests of the client programs to the network, and, having received the reply, sends it back to the client.
Quotation threshold	A percent of the sample document found in the event as quotes, enough to associate the event with this sample document. See also: Event, Sample document, Quote
Quote	A quote from the sample document found in the event text. See also: Sample document
Reference hash sum	Unlike the current hash sum, keeps the representative state of System files. See also: Integrity control
Relay server	A server which allows anyone on the Internet to send e-mail through it, not just mail destined to or originating from known users
Report	Selection providing a visual display of event statistic data. See also: Management Console, Event
Rule	Entity defining System's actions in response to any actions which persons do with secured data. A rule is a set of conditions to test the event with and actions performed when those conditions are fulfilled or not. See also: Event, Policy, Protected object, Person control rule, Copy rule, Transfer rule, Placement rule

Term	Glossary
Rule of DM	Set of restrictions and conditions that monitor file operations on removable devices, network activity, printing, configure access to managed peripherals etc. Each interceptor features a separate rule type. A rule can be only applied within its policy. See also: Policy of DM
Sample documents	Technology of searching the quotes from sensitive documents: memos, financial reports, contracts, and others. Sample documents are stored in the System as digital prints, their text is not available for viewing to either users or System administrators. See also: Technologies, Technology element, Digital print, Quote
Security officer	A basic user of the Management Console. Also, pre-installed role of the Management Console user that has privileges for all the actions in the System except administrative. See also: Management Console, User, User role, Privilege, Administrator
Skype	A voice-over-IP service and instant messaging client
SMB	Server Message Block operates as an application-layer network protocol mainly used for providing shared access to files, printers, serial ports, and miscellaneous communications between nodes on a network
SMTP	Simple Mail Transfer Protocol is a networking protocol used to send the email in TCP/IP networks
S/MIME	A standard for public key encryption and signing of MIME data
SMTP mail	An e-mail formed according to SMTP standards. See also: SMTP, Event
SPAN	Switched Port Analyzer is a technology that allows to mirror the network traffic from one port to another
SPAN copy	A variety of the "Copy" transport mode. In this case the traffic passes through a CISCO switch. The copy of the traffic is sent to Traffic Monitor Server for analysis. See also: SPAN
SSL	Secure Sockets Layer is a cryptographic network protocol developed for transmitting private documents via the Internet.
Status	Characteristics of persons and computers allowing to divide them onto groups for convenient analysis and activity control and to display them on dashboards and reports with special colour indicating. See also: Persons, Computers, Dashboard, Report

Term	Glossary
Stop word	Numbers, letters and words, whose presence in cells does not trigger these cells. Stop words are used to eliminate false triggering.
Tag	The text label giving a brief description of the event. See also: Event attributes
Technologies	Set of analysis tools searching for defined elements in the events' context and adding characterizing attributes to the event. See also: Technology element, Event context, Categories, Terms, Sample documents, Blanks, Database unloadings, Text objects, Graphical objects
Technology element	A part of the System technologies settings. Samples of confidential data. Can be categories and terms, sample documents, blanks, database unloadings, text and graphical objects. See also: Technologies, Categories and terms, Sample documents, Blanks, Database unloadings, Text objects, Graphical objects, Protected object
Telegram	A messenger for smartphones which allows you to send text messages, images, audio and video files; uses MTProto protocol
Term	One of the set of words and phrases together defining a topical area. See also: Category
Term Weight	How the term is characterized for the given category; an integer between 1 and 10. If a term with a higher weight is detected in event, then this event will be more likely associated with the category of this term. See also: Term
Text object pattern	Unified description of all possible text objects with the typical structure: passport numbers, credit card numbers, phone numbers, medical codes etc. See also: Text objects
Text objects	Technology of matching the data from the events' text with defined patterns (rules of generating bank card numbers). See also: Technologies, Event, Technology element, Text object pattern
Transfer rule	The rule that regulates sending and receiving protected data. See also: Rule, Protected data, Data protection policy
Transport mode	Event attribute that defines the level of control when the object is delivered to the recipients. Assigned by the analysis and decision engine during the object analysis. Together with the "Verdict" attribute determines if the object can be delivered further on. See

Term	Glossary
	also: Event attributes, Verdict, Copy mode, Normal transport mode, Delivery status
User	IW TM users: administrator, security officer etc. See also: Administrator, Security officer, Person
User interface	The complex of tools and methods by means of which the user interacts with the System
User role	A set of privileges that define a set of actions available for the user. See also: Administrator, Security officer, Management Console, Privilege
Verdict	An event attribute with the conclusion about the presence (or absence) of violations in an event. Together with the Transport Mode attribute determines if the event can be delivered further on. See also: Event, Transport mode, Delivery status, Event attributes
Verdict reason	Event attribute that describes the reason why a certain verdict was assigned to the event. See also: Event attribute, Verdict
Violation	The value of the "Decision" attribute; means that the corporate security policy has been violated. See also: Decision, Corporate security policy
Violation level	Event attribute indicating (by the colour tag) the level of threat to corporate security policy. See also: Event, Event attributes, Violation
Visibility scope	The way to divide intercepted events to restrict Management Console user access to them. Events satisfying criteria of some visibility scope will be visible to those users who have an access to this scope only (given that user has privileges to view or/and manage events). See also: Event, Privilege
Widget	Interface element in the form of an isolated area that displays the specified statistic information on violations and violators. See also: Management Console, Violation, Violator
WhatsApp	A messenger for smartphones which allows you to send text messages, images, audio and video files; uses its own protocol
Workstation	Computer type: desktop or notebook with OS of Windows, Linux or Mac family. See also: Computer

Term	Glossary
XMPP	Extensible Messaging and Presence Protocol is a communications protocol for message-oriented middleware based on XML