

INFOWATCH

# InfoWatch Device Monitor for Linux. User Guide

12/11/2026
© JSC “InfoWatch”
Tel/Fax +7 (495) 229-00-22
http://www.infowatch.com

# Table of Contents


1 Who Should Read this Guide ..... 7

2 Set of Documents ..... 8

3 Technical Support ..... 9

4 Overview ..... 10

5 User Settings ..... 12

5.1 Users ..... 12

5.1.1 Creating a New User ..... 12

5.1.2 Viewing User Profile ..... 13

5.1.3 Editing an Account ..... 13

5.1.4 Changing User Password ..... 13

5.1.5 Activating and Deactivating a User ..... 14

5.1.6 Deleting a User ..... 14

5.2 Roles ..... 14

6 Global Settings ..... 15

6.1 Password Settings ..... 15

6.2 System Status Monitoring ..... 16

6.3 Integrations ..... 17

6.3.1 Integration with Active Directory ..... 18

6.3.2 Editing and Deleting Integration ..... 20

7 Configuring Device Monitor ..... 21

7.1 Servers ..... 21

7.2 Synchronization ..... 23

7.3 Excluding Applications from Interception ..... 26

7.4 Universal File Interceptor ..... 28

7.5 Interception Channels ..... 31

7.5.1 Hosts for VK+ ..... 33

7.6 Network Resources Control ..... 34

7.7 Notifications ..... 35

7.8 Agents ..... 37

7.9 Corporate Networks ..... 40

7.10 Sending Data to Products ..... 40

7.10.1 Sending events to This page has not yet been translated to English. and the Platform ..... 40

7.10.2 Example of data sending settings ..... 41
7.11 Configuration ..... 42
7.12 Event Diagnostics ..... 43
8 Administration Centre Interface (Device Monitor) ..... 45
8.1 "Policies" Section ..... 47
8.2 "Groups" Section ..... 48
8.3 "Tasks" Section ..... 49
8.4 "Resources" Section ..... 50
8.4.1 Web resources list ..... 50
8.4.2 Application lists ..... 50
Detected applications ..... 50
8.4.3 File categories ..... 51
8.5 "Agents" Section ..... 51
8.6 "File Statistics" Section ..... 51
9 Detection of Workstations for Installing Agents ..... 53
10 Primary Distribution and Updating Task ..... 55
11 Security Scheme Configuration ..... 58
11.1 Configuration Editing Modes ..... 58
11.1.1 Synchronous editing prohibition mode ..... 58
11.1.2 Automatic reset of unsaved configuration changes ..... 59
11.1.3 Description of the editing prohibition mode ..... 59
11.1.4 Restoring access to the blocked configuration ..... 59
11.1.5 Editing the configuration while synchronization with the directory service is running ..... 60
11.2 Creating Policies ..... 60
11.3 Adding a Rule ..... 61
11.3.1 Removable Device Control Rule ..... 63
11.3.2 Network Resource Control Rule ..... 64
11.3.3 Terminal Session Control Rule ..... 66
11.3.4 Print Control Rule ..... 67
11.3.5 External Device Control Rule ..... 68
11.3.6 FTP Control Rule ..... 68
11.3.7 HTTP(S) Control Rule ..... 69
11.3.8 Mail Control Rule ..... 70
11.3.9 Cloud Storage Control Rule ..... 71
11.3.10 Network Traffic Proxying Rule ..... 72
11.3.11 Clipboard Control Rule ..... 72
11.3.12 VK Messenger Control Rule ..... 74

11.3.13 Telegram Messenger Control Rule ... 74
11.3.14 Yandex Messenger Control Rule ... 76
11.3.15 WhatsApp Messenger Control Rule ... 76
11.3.16 MAX Messenger Control Rule ... 77
11.3.17 XMPP Protocol Control Rule ... 78
11.3.18 Screenshot Creation Control Rule ... 78
11.3.19 Screen Monitoring Rule ... 79
11.3.20 Keyboard Input Monitoring Rule ... 80
11.3.21 Employee Activity Monitoring Rule ... 81
Monitoring actions ... 81
11.3.22 Audio Environment Monitoring Rule ... 84
11.3.23 Screen Video Recording Rule ... 85
11.3.24 Application File Control Rule ... 86
11.4 Creating and Editing Application Lists ... 87
11.4.1 Creating an application list ... 87
11.4.2 Adding applications to the list ... 87
Manually adding an application to the list ... 88
Adding detected applications to the list ... 88
Copying and moving applications ... 89
11.4.3 Editing and deleting lists and applications ... 89
11.5 Creating and Editing Resource Lists ... 90
11.5.1 Creating a Resource List ... 90
Determining whether the visited resource matches a resource from the list ... 90
11.5.2 Editing a Resource List ... 91
11.5.3 Deleting a Resource List ... 92
11.6 Creating and Editing File Categories ... 92
11.6.1 Creating a file category ... 92
11.6.2 Changing the composition of the file category ... 93
11.6.3 Editing and deleting file categories ... 93
11.7 Working with Computer Groups ... 93
11.7.1 Creating and Editing Computer Groups ... 93
11.7.2 Setting up Computer Group Membership ... 94
11.7.3 Viewing Information about Computers ... 97
11.7.4 Viewing Computer's Result Policy ... 98
11.8 Working with Employee Groups ... 99
11.8.1 Creating and Editing Employee Groups ... 99
11.8.2 Setting up Employee Group Membership ... 100
11.8.3 Viewing Employee's Result Policy ... 103
11.9 Working with Agents ... 103
11.9.1 Viewing Information about Agents ... 104
Working with table data ... 105
Agent states ... 106

11.9.2 Filtering Entries ..... 107
11.9.3 Rebooting Computer ..... 111
11.9.4 Updating Configuration ..... 112
11.9.5 Agent Diagnostics ..... 112
11.9.6 Assigning the "Golden image" Status ..... 113
11.9.7 Starting and Stopping Agents ..... 113
11.9.8 Removing Agents ..... 114
11.9.9 Distribution Policies ..... 114
Working with policies ..... 114
11.10 Working with File Statistics ..... 116
11.10.1 Managing configuration parameters ..... 117
11.10.2 Including/excluding applications from file statistics ..... 117
11.10.3 Including/excluding files with specific extensions from interception ..... 118
11.10.4 Including/excluding files/folders located at a specific path from interception ..... 118
12 END-USER LICENSE AGREEMENT ..... 119

This guide contains information on how to work in the web console of InfoWatch Device Monitor for Linux (also referred to as the System or Device Monitor).

# 1 Who Should Read this Guide

This guide is intended for implementation engineers and security officers who will be working with the System and administering it. The guide is designed for users who are familiar with the basics of working with the Windows and Linux operating system environments.

# 2 Set of Documents

The documentation package includes the following:

- " InfoWatch Device Monitor for Linux. Installation Guide". Contains a description of the installation of the Server, Web console, and Agents included in the System.
- " InfoWatch Device Monitor for Linux. User Guide". Contains a description of how to work in the Web console to solve tasks.

Associated documentation for InfoWatch Traffic Monitor system (also referred to as Traffic Monitor) includes the following:

- " InfoWatch Traffic Monitor. Installation Guide". The document describes how to install, configure, and uninstall the InfoWatch Traffic Monitor system.
- " InfoWatch Traffic Monitor. Administration Guide". The document describes how to administer the InfoWatch Traffic Monitor 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". Contains explanations for commonly used configuration files.

In addition to the primary System User Guide and Administration Guide, a Knowledge Base is available at lk.infowatch.ru, which includes troubleshooting materials and answers to questions. If you do not have access to the Knowledge Base, please contact the InfoWatch technical support at support@infowatch.com

# 3 Technical Support

If you cannot resolve issues that arise when using the System or have questions regarding the use of the System, you can contact the Technical Support Service:

- If you purchased the product from an InfoWatch partner, contact the Technical Support Service of this partner company.
- If you purchased the product directly from InfoWatch, you can contact our Technical Support Service at support@infowatch.com.

You can also visit online support at our website: www.infowatch.ru/services/support.

# 4 Overview

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.
Main functions of InfoWatch Device Monitor:

| **Function name** | **Related rule of security policy** |
|---|---|
| Control of the clipboard | Clipboard Control Rule |
| Cloud storage control | Cloud Storage Control Rule |
| Control of access to external devices | External Device Control Rule |
| Control of copying files from/to removable devices | Removable Device Control Rule |
| Control of copying files from/to network resources | Network Resource Control Rule |
| Control of traffic sent via FTP and FTPS | FTP Control Rule |
| Control of traffic sent via HTTP and HTTPS | HTTP(S) Control Rule |
| Control of instant messengers: VK, Telegram, Yandex Messenger, WhatsApp, MAX, XMPP protocol | • VK Messenger Control Rule<br>• Telegram Messenger Control Rule<br>• Yandex Messenger Control Rule<br>• WhatsApp Messenger Control Rule<br>• MAX Messenger Control Rule<br>• XMPP Protocol Control Rule |
| Control of keyboard input | Keyboard Input Monitoring Rule |
| Control of mail protocols (SMTP, POP3, IMAP, HTTPS) | Mail Control Rule |
| Monitoring print operations on computers | Print Control Rule |
| Control of computer screen | Screen Monitoring Rule |
| Control of employee activity and collecting statistics | Employee Activity Monitoring Rule |
| Control of files in applications | Application File Control Rule |
| Control of sound environment | Audio Environment Monitoring Rule |
| Screen recording | Screen Video Recording Rule |

| Function name | Related rule of security policy |
| --- | --- |
| Network traffic proxying | Network Traffic Proxying Rule |

**Important!**

On computers with macOS, the following control functions are supported:

| Function name | Related rule of security policy |
| --- | --- |
| Control of traffic sent via HTTP and HTTPS | HTTP(S) Control Rule |
| Monitoring print operations on controlled computers | Print Control Rule |

# 5 User Settings

The section contains a directory of users – Security officers who can work in the System, as well as a description of the roles that define the user's competencies in the System.
An account is created in the web console for each user whose tasks include managing the security scheme. The account data is used for authorization in the System. Based on it, the set of permissions to perform certain actions is determined.
The web console has one pre-installed user – the **Superuser**, who has the complete set of permissions when working in it. Roles are used to distinguish user permissions. You can assign different roles in different groups for a single user. A set of permissions is defined for each role. Users cannot perform actions that go beyond the scope of the role assigned to them.
The following predefined roles are used in the web console:

- **Main security officer** is the administrator role that can manage other accounts;
- **Security officer** is a role that can manage the security scheme and Server settings.

## 5.1 Users

Wen installing the System, a pre-installed user "Main officer" is created. To log in to the System, select **InfoWatch Device Monitor** from the list of installed products and enter the default login and password:

| Login | Password |
|---|---|
| officer | xxXX1234 |

When logging in to the System for the first time, you will need to change your password to a permanent one (see Changing User Password).
The main page of the **Users** section contains a list of users authorized to work in the System:

- Main security officer;
- Security officer (SO) subordinate to them.

**Target actions:**

- Creating a New User
- Viewing User Profile
- Editing an Account
- Changing User Password
- Activating and Deactivating a User
- Deleting a User

### 5.1.1 Creating a New User

The Main officer can add new users who can also act as Security officers. To do this:

1. Go to the section **Settings -> Users**.
2. Click **+Create**.
3. Enter the parameters according to the table:

| Parameter | Required? | Description |
|---|---|---|
| *Photo* | No | User photo. |
| *Username* | Yes | Name of the new user (for name requirements, see Password Settings). |
| *Login* | Yes | User account name (see the requirements in Password Settings). The login is not case-sensitive. |

| Parameter | Required? | Description |
|---|---|---|
| *Password* | Yes | Account password (see the requirements in Password Settings). |
| *Confirm password* | Yes | Account password. |
| *Role* | No | Role of the user in the System. Only one role can be assigned to a user. |
| *Console language* | No | Language interface for the new user: *Russian* or *English.* |
| *Contacts* | No | Mobile phone number or email address. You can add one or more values. |

4. Click **Create**. The new user will be added to the System. Upon first login to the System, they must change their account password (see Changing User Password).

### 5.1.2 Viewing User Profile

The user profile contains the following tabs:

1. **Personal info**, with data specified when creating the profile:
   - user photo;
   - user name;
   - user login in the System;
   - the language used by the user in the System;
   - user status: – active, – deactivated;
   - contact details: phone numbers, email addresses;
   - log of recent activities with the account .
2. **Access rights**, with information about the user's rights in the System:
   - the role assigned to the user;
   - functions available to the user:
     - access that the user has to settings and products;
     - a set of data that the user has access to.

To remove or assign a new role, go to the account editing window (see Editing an Account).

**User actions:**

- Editing an Account
- Changing User Password
- Activating and Deactivating a User

### 5.1.3 Editing an Account

To make changes to a user account:

1. Go to **Settings** -> **Users**.
2. Click next to the user you need (or on the user profile page).
3. Select **Edit**.
4. In the window that opens, change one or more settings. Available settings include those defined when the user was created (see Creating a New User).
5. Click **Save**. The new settings will take effect.

### 5.1.4 Changing User Password

To change the password issued during the first login to the System, or a compromised one:

1. Do one of the following:

- in the section **Settings** -> **Users**, click  next to the required user;
- in the user profile, click ;
- go to the main menu of the user.

2. Select **Change password**.
3. Fill in the fields:

| Field | Description |
|---|---|
| *Old password* | Enter the current password. |
| *New password* | Enter the new password that meets the security requirements (see Password Settings*).* |
| *Confirm password* | Re-enter the new password. |

4. Click **Save**.

### 5.1.5 Activating and Deactivating a User

The Main officer can prohibit the selected user from performing any actions in the System. To do this:

1. Go to **Settings** -> **Users**.
2. Click  next to the required user (or  in the user profile).
3. Select **Deactivate**. The user's account will be blocked.

To unlock a previously blocked account:

1. Go to **Settings** -> **Users**.
2. Click  next to the required user (or  in the user profile).
3. Select **Activate**. The unlocked user can work in the System again.

The Main officer's account cannot be deactivated.

### 5.1.6 Deleting a User

The Main officer can delete user accounts. To do this:

1. Go to **Settings** -> **Users**.
2. Click  next to the required user (or  in the user profile).
3. Select **Delete**.
4. In the window that opens, click **OK**. The user account along with all its data will be deleted without the option to recover it.

The Main officer's account cannot be deleted.

## 5.2 Roles

System users can have different roles that determine their rights within the System. One user can have only one role. A user without an assigned role can't access the System.

The System has two predefined roles:

1. **Main security officer** has full access to all System data, its settings, and role management, including the creation of new users.
2. **Security officer** has full access to the System data, except for the **Settings** section.

This version of the System does not support the creation of new roles.

# 6 Global Settings

The section contains general settings that apply to the installed InfoWatch products and includes:

- Password Settings
- Monitoring System Status
- Integrations

## 6.1 Password Settings

To prevent unauthorized access to the System and to protect the user from compromising their account credentials as much as possible, you can set up rules for creating account passwords and their validity periods. To do this:

1. Go to **Settings** → **System settings** → **Password settings**.
2. In the window that opens, default settings are specified. To update the account password requirements, edit the following parameters:

| Parameter | Description |
|---|---|
| *Letters* | Uppercase and lowercase letters of the Russian and Latin alphabets that are used to create a password. You can set the following values:<br>- mandatory for input ( ☑ ) – the presence of letters in the password is mandatory;<br>- optional ( ☐ ) – a password without letters can be set. |
| *Digits* | Arabic numerals that are used to create a password. You can set the following values:<br>- mandatory for input ( ☑ ) – the presence of digits in the password is mandatory;<br>- optional ( ☐ ) – a password without digits can be set. |
| *Special symbols* | A list of special characters that can be included in a password. You can set the following values:<br>- mandatory for input ( ☑ ) – the presence of special characters in the password is mandatory;<br>- optional ( ☐ ) – a password without special characters can be set. |
| *Minimal length* | The minimum allowed password length in characters. |
| *Latest N passwords cannot be used* | To avoid compromise, prohibit the use of passwords from previous periods. |
| *Time before password expires* | The number of days the password is valid. The password should be changed before the specified period expires. |
| *Failed login attempts period* | The period (in minutes) during which the user can enter an incorrect password. |

| Parameter | Description |
|---|---|
| *Number of invalid input attempts* | The number of unsuccessful password entry attempts after which the account will be blocked. |
| *User blocking period* | Account blocking period (in minutes). |

3. Click **Save** to make the new settings take effect. If you need to return to the previous settings, click **Reset settings**.

**Example**

```
Failed login attempts period – 5.
Number of invalid login attempts – 4.
User blocking period – 15.
```

If the specified parameters are set, then the account will be blocked for 15 minutes after 4 unsuccessful password entry attempts within 5 minutes. After that, the user can try entering the password again.

**Requirements for usernames and logins**

The username must contain at least four characters.

The login:

- should start with a letter and not end with a period;
- may consist of letters of the Latin alphabet, Arabic numerals, and may contain special characters: "_", "-", "–", ".".

## 6.2 System Status Monitoring

The monitoring subsystem checks the operation of all nodes in the distributed network that are part of the System. It analyzes the node's availability, information from its main hardware components, and information about the status of all System services.

The section **Settings** → **System settings** → **System status** contains panels that reflect the status of network nodes, i.e. branches. Each panel contains the following information:

| Field | Description |
|---|---|
| *Label (name)* | Label and node name in the `label(name)` format. |
| *Status* | • *Ready* – available and ready to work;<br>• *Not Ready* – not ready to work;<br>• *Unknown* – registered, but not responding to requests. |
| *Address* | IP address of the InfoWatch Device Monitor node. |
| *Latest healthcheck status update* | Date and time when the node status information was received. |
| *Kernel version* | Version of the operating system kernel. |
| *Operating system* | Operating system of the InfoWatch Device Monitor node. |
| *Memory* | The total and occupied size of the server's RAM. |

| Field | Description |
|---|---|
| *CPU* | Usage of the InfoWatch Device Monitor server central processing unit. |
| *Disk space (NATS)** | The total allocated and used disk space for storing NATS data. |
| *Disk space (Datastorage)** | The total allocated and used disk space for storing Datastorage data. |
| *Disk space (PostgreSQL)** | The total allocated and used disk space for storing PostgreSQL data. |
| *Disk space (ClickHouse)** | The total allocated and used disk space for storing ClickHouse data. |
| *Disk space (Root)** | The total allocated and used disk space reserved for system data in the root directory. |
| List of services of the InfoWatch Device Monitor node | |
| *Status* | The service may have one of the following statuses:<br>• *Running* – running;<br>• *Unavailable* – could not retrieve status;<br>• *Not initialized* – in the process of being launched;<br>• *Not found* – should be on the node, but is missing;<br>• *Error* – completed with an error. |
| *Name* | Name of the service in the System. |
| *Version* | Service build version. |
| *View details* | Output of information about the status, events, and internal messages of the service. |

* If one of the System partitions (such as `/opt/data`) has 10 GB (or less) of free space remaining, a message will appear telling that the disk space usage limit has been exceeded. All integrations will be stopped.

To lift the restriction, go to **Settings** → **System settings** → **System status** and find the node and partition with insufficient space and free it up using the OS or product tools.
All monitoring events in the System are recorded in the log.

**To download the entire log:**

1. To collect data of all services and user activity, click **Export system log files** and wait for the download to complete.
2. Download the ZIP archive containing TXT files with logs and a CSV file with user activity data.

**To download diagnostic data for a specific service:**

1. In the list of the services, click next to the required service. The log file will be generated, followed by the download.
2. Download the ZIP archive containing TXT files with the service logs.

## 6.3 Integrations

To configure domain authorization in the Device Monitor server's web interface and retrieve information for distributing agents, you need to set up synchronization with Active Directory or Samba DC.

**Important!**

You can configure Samba DC as a secondary controller only. The primary controller is Active Directory. Configuring syncing with Samba DC is identical to configuring syncing with Active Directory.

This section contains:


- Integration with Active Directory
- Editing and Deleting Integration


## 6.3.1 Integration with Active Directory

**To add a new integration with Active Directory and run it:**

1. Go to **Settings** → **System settings** → **Integrations**.
2. Click **+Add**.
3. Select **Active Directory** and enter the parameters:

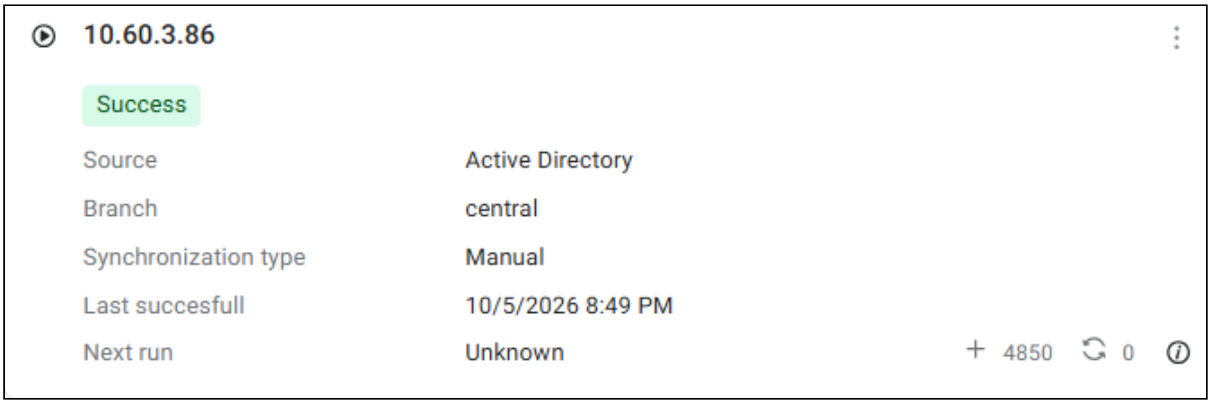
| Parameter | Description |
|---|---|
| *Integration name* | Integration name. |
| *Branch* | Node for connection: head office or branch. |
| *Source address* | Network address of the server with whose LDAP folders the syncing is performed. |
| *Connection type* | Selection of connection types:<br>• unsecure connection (Plain);<br>• secure connection via the LDAP protocol + StartTLS;<br>• secure connection via the LDAPS (TLS) protocol.<br>**Important!** A connection without certificates is not secure. |
| *Certificate* | Uploading a certificate file in PEM format for secure connections. |
| *Global port* | Port for connecting to the global LDAP folder. Depending on the connection type or when  is clicked, default values will be used:<br>• 3268 for an unsecure connection and secure connection via the LDAP protocol + StartTLS;<br>• 3269 for a secure connection via the LDAPS protocol. |
| *Port* | The port for connecting the local domain folder. Depending on the connection type or when  is clicked, default ports will be used:<br>• 389 for an unsecure connection and a secure connection via the LDAP protocol + StartTLS;<br>• 636 for a secure connection via the LDAPS protocol. |

| Parameter | Description |
|---|---|
| *LDAP query* | Filtering attributes that represent the full path to the specified folder. In this case, only one folder in the Active Directory organizational structure can be specified. To optimize the search, you can use individual levels of the base hierarchy:<br>`C-countryName`<br>`O-organizationName`<br>`OU-organizationalUnitName`<br>`DC-domainComponent`<br>`CN-commonName`<br>**Example:** to use the `Users` branch located in the company domain as the search base, you need to enter: `cn=users,dc=company,dc=com` |
| *Login* | Login for accessing the Active Directory server. |
| *Password* | Password for accessing the Active Directory server. |
| *Synchronization* | *Manual* or *Auto*. When using the second option, specify *Synchronization period* and *Repeat*. |
| *Synchronization period* | How often the synchronization will run: *Minutely, Hourly, Daily, Weekly.* |
| *Repeat* | Day of the week and time of the next synchronization. |

4. Click **Test connection** to check if the entered parameters are complete and correct. Wait for the message *Successfully connected* to appear.
5. Click:
   - **Save** – the new synchronization will wait to be started, with the status indicating that it has not yet been performed;
     or
   - **Save and start synchronization** to start syncing.

> **Note:**
>
> **Synchronization is performed with organizational units (Organizational units) and security groups (Security groups) in Active Directory.**

There is an option of sequential synchronization with several different LDAP folders. The list of servers whose LDAP folders are configured for synchronization is displayed in the central area. The bottom line indicates the number of persons added during the last synchronization (+) and the number of persons whose data was updated during the last synchronization ( ). The detailed information ( ) shows how many persons were added or updated during the last synchronization.




If you need to run a manual synchronization with the same parameters (such as when there was a change to the company's folder tree):

1. Click ▶.
2. Wait for the status to change from **Synchronizing** to **Success**. This process may take a long time (such as if the network bandwidth is low or if the volume of transferred data is large).
3. If you see the **Error** status, make sure the server is available and the credentials are correct.

**Important!**

We strongly recommended to perform the first synchronization with Active Directory at night because of the heavy load on Active Directory and the network during synchronization.

### 6.3.2 Editing and Deleting Integration

**To edit an already created integration:**

1. Click ⋮ in the top-right corner and select **Edit**.
2. Make changes.
3. Click:
   - **Save** – the synchronization will wait to be started;
     or
   - **Save and start synchronization** to start syncing.
4. If you have changed the key parameters of the integration, such as **Source address** or **LDAP query**, then click:
   - **Create a new one** to create a new integration with the specified settings instead of the current one. This will delete the current integration;
     or
   - **Continue with this**, if you need to edit some of the current integration parameters.

**To delete an integration:**

1. Click ⋮ in the top-right corner.
2. Select **Delete**, then click **Delete**.

**Note:**

The data obtained as a result of synchronization will not be deleted after the integration is deleted.

# 7 Configuring Device Monitor

This section contains:


- Servers
- Synchronization
- Agents
- Interception Channels
- Excluding Applications from Interception
- Network Resource Control
- Sending Data to Products
- Event Diagnostics
- Corporate Networks
- Notifications
- Universal File Interceptor
- Configuration


## 7.1 Servers

To send events for analysis to InfoWatch Traffic Monitor and/or Platform products, you need to configure:

- common parameters for all Device Monitor servers;
- storage and detection parameters for events;
- parameters for synchronizing policies;
- This page has not yet been translated to English.
  and/or Platform server connection parameters.

You can also disable the interaction of Device Monitor with Traffic Monitor by switching it to standalone mode.

**To configure common settings that apply to the Device Monitor main and all auxiliary servers:**

1. Go to **Settings** → **Device Monitor** → **Servers**.
2. Configure the following settings in the **Common** area:
   - **Number of shadow copies simultaneously received by server** – determines the number of copies that can be sent to the server at a time;
   - **Number of agents simultaneously processing notifications from server** – determines the number of agents that can receive notifications (for example, security policy) from the server at a time;
   - **DM agent version for installation and update** – determines the version for the Device Monitor agents distribution tasks. The same version is set by default for primary distribution and update tasks, if they are created manually (see Primary Distribution and Updating Task, Distribution Policies).

     **Note:**

     All available versions are located in the `/opt/iw/iwdistribution/bin/SetupPackages/` directory.

**To configure event storage and deletion parameters:**

1. Go to **Settings** → **Device Monitor** → **Servers**.
2. Configure the following settings in the **Event storage** area:
   - **Delete events with status "Sent to Traffic Monitor"** – to delete events sent to the Traffic Monitor server for further analysis. In this case, events with the **Processed** or **Sent to Traffic Monitor** status will be deleted once a day or when the server starts;
   - **Store events** – to determine the time during which an event will remain in the database and be displayed in the management console, including events with the **Failed to send to Traffic Monitor** or **No license** status. By default, the storage period of the event is 1 week. In this case, all events created before the specified period will be deleted;
   - **Divide by periods** – to split events into blocks by creation time to speed up access processes.

**Note:**

When the **Divide by periods** parameter is changed, partitions with the new parameters will be created in the database after the period of the last active event partition ends.

Example:
If you set the period to 6 months and then, after some time, change it to 3 months, these changes will take effect after the previously set period of 6 months ends.

If the deletion parameters are not set, events with **Processed** or **Sent to Traffic Monitor** status must be stored in accordance with the storage parameters, after which deletion must be performed.

**To configure synchronization with Traffic Monitor to receive policies:**

1. Go to **Settings** → **Device Monitor** → **Servers**.
2. Configure the following settings in the **Synchronization data protection policies on the agent** area:
   - **Traffic Monitor server address** – IP-address or the InfoWatch Traffic Monitor server name from which Device Monitor will retrieve the configuration version. The retrieved configuration deploys to Device Monitor agents;
   - **Traffic Monitor token** – token for connecting to API which is specified during the Device Monitor installation stage. You can get the current token from the Traffic Monitor administrator or generate it yourself in the Management Console.
3. Click **Save**.

**Note:**

The configuration obtained from Traffic Monitor is deployed from Device Monitor servers running RED OS, Alt OS or Astra Linux 1.7 to Device Monitor agents running RED OS, Alt OS, Astra Linux 1.7 or Windows family OS.
The version of the configuration used in Traffic Monitor is displayed in the Traffic Monitor Management Console (for details, see *InfoWatch Traffic Monitor. User Guide. Configuring the System*). If necessary, you can compare the version numbers in Traffic Monitor and Device Monitor to ensure that Device Monitor is using the current version.
To view the current version of the configuration used in Device Monitor, refresh the page.

**To view or configure Traffic Monitor and/or Platform server connection parameters:**

1. Go to **Settings** → **Device Monitor** → **Servers**.
2. By default, only the Device Monitor main server is installed. To go to the settings and select it in the **Device Monitor servers** area.

   **Note:**

   To install the Device Monitor auxiliary server, follow the steps from *InfoWatch Device Monitor. Installation Guide. New Installation*.
3. The connection server settings page displays information on the following connection parameters:
   - **Server role** – server role (*main* or *auxiliary*) assigned during installation;
   - **Port number for notification protocol**. Default value is 15100;
   - **Port number for main protocol**. Default value is 15101.
4. On the **Traffic Monitor connection** tab, specify:
   - **Traffic Monitor server address** – IP-address or the InfoWatch Traffic Monitor server name to which events will be delivered. Possible entry formats: `host:port`. The address is specified during the Device Monitor installation stage. The `port` parameter specifies the InfoWatch Traffic Monitor server port through which events will be delivered. By default, the InfoWatch Traffic Monitor server port is 9100;
   - **Traffic Monitor token** – token for connecting to API which is specified during the Device Monitor installation stage. You can get the current token from the administrator or generate it yourself in the Management Console. The Traffic Monitor connection status will be displayed below;

5. On the **Platform connection** tab, specify the following:
   - **Activity Monitor server address** – IP-address or the Activity Monitor server name. Possible entry formats: `host:port`. The `port` parameter specifies the Activity Monitor server port (default value is 17104). If you do not specify the port, the default value will be used;
   - **Platform token** – token for connecting to the Platform API. You can get the current token in the Platform product management console, in the **Token for Device Monitor Server** field of the **Global settings** section. The Platform connection status will be displayed below;
   - **Getting control commands from Activity Monitor** – parameter for enabling the interaction setting between Device Monitor and Activity Monitor;
   - **Platform central node address** – IP-address or the Platform server name from which Device Monitor will receive Activity Monitor commands. Possible entry formats: `host:port`. The `port` parameter specifies the Platform web interface port through which Device Monitor will receive Activity Monitor commands. By default, the Platform web interface port is 443. If you do not specify the port, the default value will be used;
   - **Activity Monitor token** – token for connecting to the Activity Monitor API. You can get the current token in the **Global settings** section (for details, see *InfoWatch Activity Monitor. Administration Guide. Global Settings*).
6. If you need to establish a connection to another Traffic Monitor or Platform server, go to the required tab and change the server address or token.
7. Click **Save**.

When the Device Monitor server connects to the Traffic Monitor or Platform server, the remote server's certificate is verified. To successfully connect to the remote server, configure this verification. For details, see *InfoWatch Device Monitor for Linux. Installation Guide.* Configuring Validation of the Remote Server Certificates. If the certificate fails validation, the connection status will be *Certificate verification error*.

**To switch the Device Monitor server to standalone mode:**

1. Go to **Settings** → **Device Monitor** → **Servers**.
2. Activate the **Standalone mode of server operation** option in the **Send events to Traffic Monitor** area.
   Keep in mind that, after switching to standalone mode:
   - all events related to Traffic Monitor, including file shadow copies, will be deleted from the Device Monitor server's database. Events will be deleted the following day at 01:00;
   - the server will not save new Device Monitor events;
   - switching to standalone mode effects only the interaction with Device Monitor. Interaction with other products will not change.

## 7.2 Synchronization

**Important!**

Synchronization cannot be created, started or edited if you or another Security officer are modifying the configuration in the **Group** section of Administration Centre while the synchronous editing restriction is enabled. The edit buttons will be unavailable. Information on editing the configuration will become available at the top of the screen.
For more information about the synchronous editing restriction, see Configuration Editing Modes.

To retrieve information about computers or employees from the directory service, create a synchronization with a LDAP server and run it in the **Settings** → **Device Monitor** → **Synchronization** section.
In the central area of this section's workspace, all the created synchronizations, their parameters and statuses are displayed.
If you synchronize with computers, a new subgroup will appear in the **Imported** group within the **Computer** section of the Device Monitor web console. It will contain data on computers from the directory service, while preserving the source's hierarchical structure. Similarly, you can synchronize with employees.
Subsequently, synchronization occurs automatically at the interval specified in the **Synchronization period** field.
**To change synchronization period**, enter the required value in the field and click any place of the workspace. You can specify a value from 1 to 999 minutes. A single period is specified for all synchronizations.

**To create a new synchronization:**

1. If you configure a synchronization on a server running the Astra Linux OS, edit the LDAP client configuration file and restart the web API service. To do this, run the commands in the terminal:

```
echo "TLS_CACERT /etc/ssl/certs/ca-certificates.crt" > /etc/ldap/ldap.conf
systemctl restart iwdms_webapi
```

2. Go to the **Settings** → **Device Monitor** → **Synchronization** section.
3. Click **Add** on the upper-right part of the workspace.
4. In the window that opens, specify the parameters for a new connection:

| Parameter | Description |
|---|---|
| Source address | Domain name or LDAP server IP-address with which synchronization is performed. |
| Source type | The directory service type. It has a fixed *MS Active Directory* value. |
| Security type | The connection security type. Possible values:<br>• *STARTTLS*[1]<br>• *LDAPS*[2]<br>• *Kerberos*[3]<br>• *Insecure* (default value)<br>**Note:**<br>[1] Additional settings are required to work with the STARTTLS security level. Contact the InfoWatch support or partner from whom you purchased the product.<br>On the Device Monitor server installed with containerisation support, synchronization with the STARTTLS security level is not available.<br>[2] If the<br>This page has not yet been translated to English.<br>server was installed with containerisation support, to work with the LDAPS security level, you need to:<br>a. Import the root certificates at the path `/opt/iw/dmserver/cert` before creating the synchronization.<br>b. After installing certificates, restart the service `webapi`:<br>`systemctl restart iwdms_webapi`<br>[3] To work with the Kerberos security level:<br>• Prepare the server to work with Kerberos, as described in *InfoWatch Device Monitor. Installation Guide.* Preparing the Environment.<br>• Note the case sensitivity of the login used to access the synchronization server (see the description below in the table). |
| Port | Port for connecting to the synchronization server. You can select one of the preset values: *389* or *636*, or enter the value manually. |

| Parameter | Description |
| --- | --- |
| LDAP request | Filter attributes that represent the full path to the specified folder. In this case, only one folder in the Active Directory organizational structure can be specified.<br>**Note:** synchronization is performed with Active Directory Organization units and Security groups.<br>**Note:** you can also synchronize an object of the *Container* type by explicitly specifying the full path to it in the request. For example:<br>`cn=container_example,ou=ou_example,dc=company,dc=com`<br>If the object of the *Container* type is located inside the folder specified in the request, then there will be no data synchronization with this object.<br>**Note:**<br>The following characters can be used in the DC attribute:<br>• Numbers<br>• Letters (Cyrillic and Latin, case-insensitive)<br>• Symbol "-" (cannot be at the beginning or end of the attribute)<br>• Symbol "_"<br>The following characters can be used in the OU and CN attributes:<br>• Numbers<br>• Letters (Cyrillic and Latin, case-insensitive)<br>• Symbols * ( ) . & - _ [ ] ` ~ \| @ $ % ^ ? : { } ! '<br>• Space, if it does not appear at the beginning or end of the attribute value<br>• Reserved characters, escaped with a backslash "\":<br>  • \ # + < > , ; " =<br>  • Spaces at the beginning or end of the attribute value (such as "`OU=\ test`")<br>The length of в DC, OU, and CN attributes must be from 1 to 64 characters. |
| Login | Login for access to the synchronization server.<br>If you have selected the Kerberos security level, use uppercase letters for the domain part of the login. Example: *user@EXAMPLE.RU* |
| Password | Account password for accessing the synchronization server. This field is required. |
| Synchronization type | Synchronized objects. Select the *Computers* or *Employees* value. |
| Default policy | A policy that will be assigned to the synchronized groups after the first synchronization. |

| Parameter | Description |
|---|---|
| Nesting level | The nesting level to which tree nodes from the directory service are synchronized. Groups at this level include all computers or all employees of the included subgroups.<br>By default, the nesting level is not specified. In this case, *all* tree nodes from the directory service are synchronized. |

5. Click **Check connection** to verify that the entered parameters are complete and correct, and wait for the message "*Successfully connected*" to appear.
6. Click **Add**.

**To start the synchronization:**

1. On the synchronization tile, click  **Start synchronization**.
2. Wait for the synchronization to complete. The synchronization status will be set to **Success**.

> **Note:**
>
> If a synchronization error occurs on RED OS 8, make sure that you installed the `openldap-compat` package when preparing the server for Device Monitor installation. Otherwise, install it. For more information, see *InfoWatch Device Monitor for Linux. Installation Guide.* Preparing the Environment.

**To edit the synchronization:**

1. On the synchronization tile, click .
2. Select **Edit** from the drop-down list.
3. Make the required changes to the synchronization.

> **Note:**
>
> If **Default policy** is changed, the new policy will apply only to new groups created during synchronization.

4. Click **Save**.

**To delete the synchronization:**

1. On the synchronization tile, click .
2. Select **Remove** from the drop-down list.
3. Click **Confirm** in the window that appears.

> **Important!**
>
> When you delete a synchronization, all synchronized data associated with it will be deleted, except for:
> - the computers where the Device Monitor Agent is installed;
> - computers and employees that belong not only to imported groups, but also to Device Monitor groups.
>
> If a computer on which the Device Monitor Agent is installed belongs only to groups imported from directory services, it will be added to the default computer group when the synchronization is deleted.

## 7.3 Excluding Applications from Interception

You can specify the applications whose activity will not be intercepted by the System.

**To view and configure the parameters for excluding applications from interception:**

1. In the main menu, select **Settings** →
   This page has not yet been translated to English.
   → **Exclude applications from interception**.
2. To exclude applications on workstations running different operating systems, you need to use different tabs. Open the tab with the name of the corresponding OS family: **Windows, Linux, macOS**.
3. In the left part of the workspace, click .

4. Follow the instructions for the selected OS:

- **For Windows:**
  i. Enter the name of the application's executable file. Exclusion is performed by the name of the executable file. The field is required and not case sensitive.
  Instead of the application name, you can enter the symbol *. In this case, all applications located at the specified path or having the specified digital signature will be excluded from interception (see clauses *d, f*).
  ii. In the **Description** field, enter a custom description of the application.
  iii. In the **Interceptor type** field, select:
    - **Exclude application from network capture** if you need to exclude the application's network activity from interception;
    - **Exclude application from module injection** if you need to avoid creating events and shadow copies when printing from this application.

    > **Note:**
    >
    > You need to select at least one interceptor type.
    > Applications with built-in integrity checks (such as the SWIFT client) or containing anti-debugging methods must be added to the list of exceptions from module injection. Otherwise, they will not be able to run.

  iv. In the **Path** field, specify the folder on the computer with the Device Monitor Agent that contains the application's executable file, or the top-level folder (system variables can be used). The specified string must be at the beginning of the file path. For example, if the exception is specified as: `%ProgramFiles%\Citrix`, then all applications in the `*.exe` format in the `Citrix` folder, as well as in any of its subfolders, will be excluded from interception.
  v. In the **Original file name** field, specify the application name (in the context menu of the application's executable file, select **Properties**, the **Details** tab, the **Original filename** property).
  vi. In the **Name of person who's created the digital signature** field, specify the value from the executable file's properties (in the file's context menu, select **Properties**, the **Digital Signatures** tab, the **Signer name** attribute). You can specify the full name or part of the name. For example, if the exclusion is specified as `*Kaspersky`, all applications whose digital signature contains the substring `"Kaspersky"` will be excluded from interception.
- **For supported Linux operating systems**
  i. Enter the name of the application's executable file. Exclusion is performed by the name of the executable file. The field is required and not case sensitive.
  Instead of the application name, you can enter the symbol `*`. In this case, all applications located at the specified path will be excluded from interception (see clause *d*).
  ii. Enter a brief description. This field is required.
  iii. Specify the OS for which the exclusion is configured. To make the exclusion work on all supported Linux family OS, select the **Any Linux** option.
  iv. Specify the file location – the folder on the computer with the Device Monitor Agent that contains the application's executable file. Or the top-level folder (you can use system variables). The specified string must be at the beginning of the file path. For example, if the exception is specified as: `/opt/myapps`, then all applications in the `myapps` folder, as well as in any of its subfolders, will be excluded from interception.
- **For macOS:**

i. Enter the name of the application's executable file. Exclusion is performed by the name of the executable file. The field is required and not case sensitive.
Instead of the application name, you can enter the symbol `*`. In this case, all applications located at the specified path will be excluded from interception (see clause *c*).
ii. In the **Description** field, enter a custom description of the application.
iii. In the **Path** field, specify the folder on the computer with the Device Monitor Agent that contains the application's executable file, or the top-level folder (you can use system variables). The specified string must be at the beginning of the file path. For example, if the exception is specified as: `/opt/myapps`, then all applications in the `myapps` folder, as well as in any of its subfolders, will be excluded from interception.

5. Click **Add**.
6. Click **Apply**.

**Important!**

To apply an exception or a cancellation of such an exception, restart the application.

**To edit the exception configuration:**

1. At the end of the line of configurations, click  and select **Edit**.
2. Apply the changes and click **Save**.
3. Click **Apply**.

**To delete the exception configuration:**

1. At the end of the line of configurations, click  and select **Remove**.
2. Confirm the action in the dialog box.
3. Clock **Apply**.

**To delete several configurations at once:**

1. Check the boxes in the lines of configurations that should be deleted.
2. On the bottom panel, click . To reset the selection, click .
3. Clock **Apply**.

## 7.4 Universal File Interceptor

The system uses the added application profiles to intercept file read and write operations performed by applications, as well as to block these operations according to Traffic Monitor policies.
Information about application profiles is automatically synchronized with Traffic Monitor. For more details on configuring the corresponding Traffic Monitor rules, see *InfoWatch Traffic Monitor. User Manual. File Operations Rule*.

**Important!**

Blocking file read and write operations based on Traffic Monitor policies is available only on agents running supported Linux-family operating systems and only starting from Device Monitor version 7.20.4.

**Note:**

If several operations with a file are performed within 30 seconds, the System records them in a single interception event. In this case, if a blocking is configured, the System will block each attempt to perform an operation with a file during this time.

**To import the application profile:**

1. Go to **Settings** →
This page has not yet been translated to English.
→ **Universal file interceptor**.
2. Go to the tab **Applications**.
3. Click **Import** and, in the window that opens, select the application profile in the `.xml` format.
4. If the synchronous editing restriction is enabled, click **Save** on the information panel (see Configuration Editing Modes).

**Note:**

To obtain the required profile, contact the InfoWatch specialists.

**To delete the application profile:**

1. Click  on the required application profile and select **Remove**.
2. Confirm the action by clicking **Remove**.
3. If the synchronous editing restriction is enabled, click **Save** on the information panel (see Configuration Editing Modes).

**Important!**

The deleted application profile cannot be used when configuring policies in Traffic Monitor. If it was used in a policy previously, it will be corrupted.

**To edit the application interception settings:**

1. Click  on the required application profile and select **Edit**.
2. In the window that opens, make the necessary changes to the settings:

| Parameter name | Description |
|---|---|
| Executable files | Executable files that will be intercepted. They cannot be changed. |
| **Intercept all the files except those that match one of the exceptions** | |
| Files with extension | List of file extensions. The separator between extensions is ";", line breaks are not allowed. |
| Files located along the path | Specifying the file path:<br>• you can use masks.<br>• the separator is ";", line breaks are not allowed;<br>• the path must start with the standard file system path element separator character "\" or with a special character (such as "*");<br>• excluded paths must specify a relative file path, meaning that drive names are not allowed. |
| **Regardless the exclusion settings, always intercept files that match one of the criteria** | |
| Files with extension | List of file extensions. The separator between extensions is ";", line breaks are not allowed. |

| Parameter name | Description |
| --- | --- |
| Files located along the path | Specifying the file path:<br>• you can use masks.<br>• the separator is ";", line breaks are not allowed;<br>• the path must start with the standard file system path element separator character "\" or with a special character (such as "*");<br>• included paths must specify a relative file path, meaning that drive names are not allowed. |

3. After making the changes, click **Save**.
4. If the synchronous editing restriction is enabled, click **Save** on the information panel (see Configuration Editing Modes).

**To edit the OS profile interception settings:**

1. Go to the tab **General settings**.
2. Select the required OS profile and click  **Edit**.
3. In the window that opens, make the necessary changes to the settings:

| Parameter name | Description |
| --- | --- |
| **Intercept all the files except those that match one of the exceptions** | |
| Files with extension | List of file extensions. The separator between extensions is ";", line breaks are not allowed.<br>Default values:<br>Windows<br>.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;.URL<br>Astra Linux<br>.so;.o;.ko;.a<br>For RED OS and ALT OS, the default value is empty. |

| Parameter name | Description |
|---|---|
| Files located along the path | Specifying the file path:<br>• you can use masks.<br>• the separator is ";", line breaks are not allowed;<br>• the path must start with the standard file system path element separator character "\" or with a special character (such as "*");<br>• excluded paths must specify a relative file path, meaning that drive names are not allowed.<br>Default values:<br>Windows<br>\Recovery\;\System Volume Information\;\MSOCache\;\Windows\;\Program Files\;\Program Files (x86)\;\Users\\AppData\;\ShaderCache\<br>Astra Linux<br>/etc/\;/lib/\;/usr/lib/\;/usr/share/\;/.genisoimagerc\;/.mkisofsrc\;/tmp/*\<br>For RED OS and ALT OS, the default value is empty. |
| **Regardless the exclusion settings, always intercept files that match one of the criteria:** | |
| Files with extension | List of file extensions. The separator between extensions is ";", line breaks are not allowed.<br>The default value is empty for all operating systems. |
| Files located along the path | Specifying the file path:<br>• you can use masks.<br>• the separator is ";", line breaks are not allowed;<br>• the path must start with the standard file system path element separator character "\" or with a special character (such as "*");<br>• excluded paths must specify a relative file path, meaning that drive names are not allowed.<br>The default value is empty for all operating systems. |

4. After making changes, click **Save**.
5. If the synchronous editing restriction is enabled, click **Save** on the information panel (see Configuration Editing Modes).

## 7.5 Interception Channels

Set the interception parameters:

**To configure the frequency of receiving events with shadow copies of the chat for the messengers' control rule:**

1. In the main menu of the Management Console, select **Settings → Device Monitor → Interception channels**.
2. Specify how many minutes after the start of the chat conversation a shadow copy should be created.
3. Specify the number of messages in the chat at which a shadow copy should be created.

Each subsequent shadow copy is created based on the specified settings, depending on which setting was triggered first.

**To configure the conditions for the keyboard text entry rule, specify:**

1. How many seconds after the user stops typing on the keyboard should an event be created.
2. The minimum number of characters entered by the user that is sufficient to create an event.
3. The response to pressing Enter / Ctrl+Enter / Shift+Enter.

The interception event will be generated if at least one condition is met, as well as when the user changes the active window.

After setting the required values and selecting the conditions, click **Apply**. The settings will apply permanently.

**To configure the settings for screenshots[1], specify:**

1. The quality, size, and colour of the screenshots that need to be created:
   - low, minimal, colour;
   - average, minimum, grayscale;
   - high, maximum, colour.
2. By how much to adjust the screenshot size (in %, the default value is 80%).
3. The period from 120 to 1200 seconds, after which a screenshot does not need to be taken (the default value is 120 seconds).
4. If you need to take a screenshot of the active window only[2] [3].

**Important!**

[1] If there is not enough free space on the disk, screenshots are not created automatically.

[2] If the setting **Make screenshot of active window only** is enabled, screenshots taken on workstations running Alt 11 OS with the Wayland graphical shell will contain a black border.
On workstations running other Linux operating systems, only capturing the entire screen is supported.

[3] If, with the **Make screenshot of active window only** setting selected and an active window of on application, the user performs actions outside that application (for example, opens the context menu in the system tray on the workstation), only part of the active application window may be displayed in the screenshot.

**To configure the settings for recording the sound environment when the rule is triggered, specify the following in the *Audio recording* field:**

1. The duration of the recording in minutes. The minimum value is 1, the maximum is 120. The default value is 5 minutes.

**Note:**

When an employee uses a resource specified in the sound environment monitoring rule, Device Monitor continuously records the sound environment of the workstation for the period specified in the settings. Upon completion, the System stops the recording. If the employee has used several resources specified in the rule,
This page has not yet been translated to English.
resets the timer and starts the countdown anew when switching from one resource to another.

**Example 1**

The rule specifies the resources for which the sound environment should be recorded when they are visited: https://example.ru/, https://example.com. The recording duration is set to 5 minutes. The employee navigates to the resource https://example.ru/, and the System starts the recording. After 3 minutes, the employee leaves this resource and navigates to https://example.com, which is also monitored by the rule. The System continues to record the audio environment, restarting the 5-minute interval count.
After 5 minutes of using the resource, Device Monitor ends the recording and sends the events to Activity Monitor. As a result, an event will be created in Activity Monitor for this employee regarding the visit to 2 resources that lasted 8 minutes.

**Example 2**

The rule specifies the resources for which the sound environment should be recorded when they are visited: https://example.ru/, https://example.com. The recording duration is set to 5 minutes.

The employee uses the resource https://example.ru/, and after 3 minutes switches to https://example1.ru/ (not included in the list of controlled resources) and uses it for 1 minute. Device Monitor records the sound environment.
Then the employee returns to the monitored resource https://example.ru/. Device Monitor updates the timer for recording the sound environment for this resource. After 5 minutes, the System ends the recording. As a result, an event will be generated for this employee in Activity Monitor, indicating a visit to 1 resource lasting 9 minutes.
**Example 3**
The rule specifies the resources for which the sound environment should be recorded when they are visited: https://example2.ru/, https://example2.com. The recording duration is set to 120 minutes.
The employee uses the resource https://example2.ru/ for 20 minutes, then switches to https://example.ru/ (not included in the list of controlled resources) and uses it for 10 minutes. Throughout this time, Device Monitor records the sound environment.
Then the employee moves to the controlled resource https://example2.com/. Device Monitor updates the timer for recording the sound environment for this resource. After 120 minutes, the System ends the recording. As a result, an event will be generated in Activity Monitor for this employee regarding the visit to 2 resources lasting 150 minutes.

2. To prevent the System from recording silence, enable the **Record in case of speech only** setting. When this setting is activated, Device Monitor only sends events with recognized human speech to Activity Monitor.

   **Important!**

   To apply the setting, log out of the System and log back in.

   For details on recording audio, see Audio Environment Monitoring Rule.

**To configure the duration of screen recording when a rule is triggered, specify the value in the *Screen video* field.**
The value is set in minutes. The minimum value is 1, the maximum is 120 (the default value is 5 minutes).

**Note:**

Device Monitor records video from the workstation screen continuously during the period specified in the settings. At the moment when an employee starts using the resource specified in the recording rule,
This page has not yet been translated to English.
starts the workstation screen recording. Upon completion of the period specified in the settings, the System stops the recording. If an employee used several resources included in this rule, switching from one resource to another makes Device Monitor reset the timer and start the countdown anew.

**Important!**

When working with agents version 7.20 and earlier, only **Audio recording** is used as a setting for the duration of recording the sound environment and the screen of the workstation.
**Example**
Device Monitor version 7.21 is installed on the server, and the agent is running version 7.20. The agent is subject to rules for monitoring the sound environment and recording screen video.
The duration settings are configured as follows:

- for **Audio recording** – 2 minutes;
- for **Screen video** – 3 minutes.

When both rules are triggered, the recordings for both screen video and sound environment will last 2 minutes each.

**To intercept VK+ webmail, specify the hosts.** See Hosts for VK+.

### 7.5.1 Hosts for VK+

To intercept VK+ webmail, specify the hosts (see Mail Control Rule). You can do this on the **Hosts for VK+** tab in **Settings** → **Device Monitor** → **Interception Channels**.
**To add a host:**

1. In the top-right corner, click 

.
2. Enter the host name in the format <*scheme*>:<*host*>, such as *address.ru:15101* or *10.60.3.8:15101*.

3. Click **Add**.

**To edit a host:**

1. Next to the host, click  and then  **Edit**.
2. In the editing window, make the edits and click **Save**.

**To delete a host:**

1. Next to the host, click , and then  **Remove**.
2. In the window that opens, confirm the action by clicking **Remove**.

## 7.6 Network Resources Control

To control network traffic on the Device Monitor Agent, a transparent proxy server is implemented. All connections are redirected to this server, regardless of the used protocol. The Device Monitor Agent then parses the protocol and determines whether this protocol is one of the intercepted ones.
The following protocols are intercepted:

- FTP(S)
- POP3
- SMTP
- S/MIME
- HTTP(S)
- XMPP
- MMP

If the data stream is protected using the TLS\SSL protocol, the proxy server decrypts the traffic and determines whether the stream needs to be monitored.
You can specify a list of server addresses for which protocols are not monitored when connecting (the traffic to these servers is not redirected to the internal proxy server), or are forcibly monitored (the traffic is redirected to the internal proxy server).
When adding the server address to the exceptions, specify the IP-address or FQDN.

**To specify a list of prohibited or allowed servers:**

1. Select **Settings → Device Monitor → Network resources control** from the main menu.
2. Click  or **+ Add setting**.
3. Enter a description of the server in the **Add server to the list excluded from analysis** dialog box:
    - to add a *separate server port*:
        i. Select the required action: **Exclude** or **Intercept**.
        ii. Add **Description**.
        iii. Select **Address and port** in the **Type of addresses** field.
        iv. Specify FQDN or the server IP-address (IPv4 or IPv6).
        v. Specify the connection port in the **Port** field (may be empty).
    - to add an *address range*:
        i. Select the required action: **Exclude** or **Intercept**.
        ii. Add **Description**.
        iii. Select **Address range** in the **Type of addresses** field.
        iv. Specify the IP-addresses (IPv4 or IPv6) in the fields "from" - "to".
    - to add a *template for excluding a resource group from interception during SSL/TLS-connection*:
        i. Select the action **Exclude**.
        ii. Select **Domain from MITM Interception** in the **Type of addresses** field.
        iii. Specify the domain.
4. Click **Add** and then **Apply**.

In text format, a IPv4 address is written as `nnn.nnn.nnn.nnn`, where `nnn` ranges from 0 to 255 and each `n` represents a decimal digit. Nonsignificant zeros can be omitted.

In text format, a IPv6 address is written as `xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx`, where each `x` is a hexadecimal digit representing 4 bits. Nonsignificant zeros can be omitted.

**Important!**

Inclusion in the interception has a higher priority than exclusion.
A configuration with a specific address has a higher priority than an address range.

**To change the server parameters**, select it in the list and click **Edit**. After making changes, click **Save**, and then **Apply**.

**To remove the server from the list of allowed**, select it and click **Remove**. Confirm the action and click **Apply**.

## 7.7 Notifications

If an employee attempts to perform an action restricted by the security policy on a monitored computer, they will be displayed a notification about the restriction.
Depending on the operating system on the computer where the Device Monitor Agent is installed, the following notifications are displayed:

| Notification type | Reason for sending the notification | Windows | Linux |
|---|---|---|---|
| **Access to device is forbidden** | The rule prohibiting reading from and writing to the device was triggered (see Removable Device Control Rule). | + | + |
| **Writing to device is forbidden** | The rule prohibiting writing to the device was triggered (see Removable Device Control Rule). | + | + |
| **Writing to open area is forbidden** | The rule prohibiting writing to unencrypted floppy disk drives and removable devices was triggered (see Removable Device Control Rule). | + | - |
| **Copying/printing file is forbidden if there is not enough space for incidents** | If the Device Monitor Agent has been disconnected from the server for so long that the space allocated for storing information about events controlled by the rules (30,000 events) is exhausted, and the general agent settings for this case have the **Deny operations** parameter selected (see Agents), then any operations controlled by the current security policy are prohibited. | + | - |
| **Pasting from clipboard is forbidden when there is not enough space for events to store** | | + | - |
| **Data transfer via network protocols is forbidden when there is not enough space for incidents** | | + | - |

| Notification type | Reason for sending the notification | Windows | Linux |
|---|---|---|---|
| **Data transfer via network protocols is forbidden** | The rule prohibiting data exchange via the FTP(S) network protocol, mail, and messengers was triggered (see FTP Control Rule, Mail Control Rule, XMPP Protocol Control Rule and so on). | + | + |
| **Transferring data over network protocols is forbidden when data protection policy is triggered** | Displayed when data transmission via mail protocols, FTP, HTTP(S) is blocked as a result of applying the Traffic Monitor data protection policy. | + | + |
| **Using clipboard is forbidden when data protection policy is triggered** | Displayed when text copying is blocked as a result of applying the Traffic Monitor data protection policy. | + | - |
| **Printing is forbidden when data protection policy is triggered** | Displayed when copying a file to the printer as a print job is blocked as a result of applying the Traffic Monitor data protection policy. | + | - |
| **Copying a file to the removable device is forbidden when data protection policy is triggered** | Displayed when copying a file to a removable device is blocked as a result of applying the Traffic Monitor data protection policy. | + | + |
| **Prohibition of access to cloud storage** | A rule controlling the use of web clients for cloud storage was triggered (see Cloud Storage Control Rule, **Deny access** setting). | + | + |
| **Prohibition of writing to cloud storage** | The rule that controls the use of cloud storage web clients was activated (see Cloud Storage Control Rule, **Allow download only** setting). | + | + |
| **Prohibition of making screenshot** | The rule controlling the creation of screenshots was triggered (see Screenshot Creation Control Rule). | + | + |
| **Copying a file to the network resource is forbidden** | The rule that prohibits copying a file to network resources was triggered (see Network Resource Control Rule). | + | - |

| Notification type | Reason for sending the notification | Windows | Linux |
|---|---|---|---|
| **Writing is forbidden when data protection policy is triggered** | Displayed when writing or reading of a file for the specified profile is blocked (see Application File Control Rule). | + | + |
| **Reading is forbidden when data protection policy is triggered** | | + | + |

**To completely disable the display of notifications to employees or enable it again:**

1. In the Administration Centre, go to **Settings** → **Device Monitor** → **Agents**.
2. Deselect the **Show notifications to employee** box to disable the display of notifications to employees, or select it to enable notifications.
3. At the top-right, click **Apply**.

You can change the text of the notifications, as well as disable the display of any type of notification, or enable it again.

**Important!**

If you have disabled notifications using the method described above, then notifications enabled using the method described below will not be displayed.

**To change the notification text or enable/disable individual notifications:**

1. In the Administration Centre, go to **Settings** → **Device Monitor** → **Notifications**.
2. From the **Notification type** drop-down list, select the one you want to configure.
3. To enable/disable the display of the selected notification type, select or deselect the **Show employee a system notification** box.
4. In the **Notification text** field, enter the notification text.
   In the message, you can use variables that will be converted into actual data when displayed to the employee: for example, the type of the blocked device or the protocol the employee used to attempt to transmit data. To do this, place the cursor in the required location in the notification text, click + Add, and select the required variable from the drop-down list.

   To cancel the changes, click .

   To restore the system notification text, click .

   **Note:**

   By default, the notification text is in the language that was selected during the Device Monitor server installation. When changing the language of the web interface, the language of the notification text does not change.
5. After you have made the changes for the selected notification type, click **Save** in the top-right corner.
6. If necessary, change the settings for other types of notifications by repeating steps 2–5.

## 7.8 Agents

For the Device Monitor agent applications to work effectively, you need to set a number of general parameters.

**To specify the general Device Monitor agent operation settings:**

1. Select **Settings** → **Device Monitor** → **Agents** in the main menu.
2. Change the parameters:

| Parameter | Description |
|---|---|
| **Connect** | |
| Send notifications on agent operation to server | The frequency with which the agent sends notifications about its operation to the server, in seconds. The default value is 600 sec. |
| Check server health every | The frequency with which the agent checks the server availability, in seconds. The default value is 2400 sec. |
| Check for security scheme changes every | If the agent is operating in active mode (meaning that it asks the Server itself for changes to the security scheme), the check will be performed at the specified frequency, in seconds. The default value is 600 sec. |
| **Disk space control** | |
| Low disk space | The minimum amount of free space (GB) on the monitored computer, below which shadow copies will not be created. The default value is 10 GB. |
| Warning threshold | When this threshold is reached (GB), the system will use color indication to show that the disk space required for the system to create shadow copies without interruption may soon run out. The default value is 20 GB. |
| If maximum number of events on agent has been exceeded | On the disk of the monitored computer where the Device Monitor Agent is installed, space is allocated that is sufficient to store information about 30,000 events. If the Device Monitor Agent has been disconnected from the server for so long that more than 30,000 events controlled by the rules defined for the employee/computer have accumulated, any actions controlled by the current security policy may be prohibited. To prohibit, select **Deny operations**. To allow all actions to be performed uncontrolled, select **Allow operations**. |
| **Speed of sending data from agent** | |
| Limit data sending speed | In the case of a low bandwidth, to avoid overloading it, you can adjust the speed at which shadow copies are sent to the server. To do this, enable the setting and specify the upper speed limit, in KB/s. |
| **Event log** | |

| Parameter | Description |
|---|---|
| Log events from device and cloud storage interceptor | The level of detail when saving information about working with external devices and cloud storages. To learn more, see External Device Control Rule and Cloud Storage Control Rule. One of the following options is possible:<br>• **Always log** – events are always created and contain information about all actions, including the connection and use of devices included in white lists;<br>• **Never log** – events are not saved;<br>• **If access denied** (default value) – events are generated only when there are attempts to violate the Device Monitor security policies, i.e. when the use of a device or cloud storage is blocked, including blocking attempts to exceed the access level. The use of external devices and cloud storages not prohibited by the policies is not saved. |
| **Agent's behavior on computers** | |
| Hide agent's presence on computer | A sign that the System will hide the Agent's presence on computers.<br>If this setting is not selected, an icon  will be displayed in the notification area of the Windows taskbar on the computer where the Agent is installed. Clicking this icon will provide information about the Agent's work, as well as a list of currently monitored devices.<br>**Important!** If antivirus protection is enabled on the monitored computer, the antivirus may detect the operation of Device Monitor: for example, in the list of processes running on the monitored computer or in the list of programs initiating the monitoring.<br>**Note:** supported for agents running Windows. |
| Show notifications to employee | If the box is selected, the employee will receive a notification when they attempt to perform an action prohibited by the security policy.<br>You can configure the display of individual notification types in the section Notifications. |

3. To apply the changes, click **Save**.

**Note:**

For Agents running Astra Linux 1.7, RED OS, and Alt OS, sending events about connecting or using external devices via USB is supported. At the same time:

- the user account name used to connect the device may not be identified;
- the device identifier may be missing if it is not set in this device by the manufacturer.

To send such events, you need to specify the value **Always log** for the **Log events from device and cloud storage interceptor** parameter.

## 7.9 Corporate Networks

To avoid creating events for requests to internal resources when the HTTP(S) traffic control rule works, you can exclude the segments of the corporate network. To do this:

1. Go to **Settings → Device Monitor → Corporate networks**.
2. In the upper-right part of the workspace, click **Add**.
3. In the window that opens, specify the:
    - network name;
    - subnet address in CIDR format, such as:
        - `182.0.7.1/21` (IPv4 protocol)
        - `2001:4f8:3:ba::/64` (IPv6 protocol)
4. Click **Add**.

> **Note:**
>
> If you define the segments, the information about the location of adapters in the corporate network will be displayed incorrectly in the parameters of agents running on Windows.

## 7.10 Sending Data to Products

In **Settings → Device Monitor → Sending data to products**, you can specify
This page has not yet been translated to English.
products the data should be sent to.

### 7.10.1 Sending events to

This page has not yet been translated to English.

### and the Platform

1. Under **Configure sending data to Traffic Monitor**, deselect the box if you do not want to:
    - **Send events with automatically created screenshots**
    - **Send text for keyboard input control events**
    - **Send events with screenshots for keyboard input events** (the setting is available if sending events with text according to this rule is enabled)
2. Under **Configure sending data to Platform**, deselect the box if you do not want to:
    - **Send events with automatically created screenshots**
    - **Send text for keyboard input control events**
    - **Send events with screenshots for keyboard input events** (the setting is available if sending events with text according to this rule is enabled);
    - **Send events of connecting/using devices**

> **Note:**
>
> Event control settings are configured in the following rules:
> - Screen Monitoring Rule
> - Keyboard Input Monitoring Rule
> - Employee Activity Monitoring Rule
>
> To display events related to device usage/connection in InfoWatch Activity Monitor:
> - Under **Settings**, in the **Agents** section, for the **Log events from device and cloud storage interceptor** parameter, set the value to **Always log** or **If access denied**. See Agents.
> - Configure the removable device control rule.

# Sending events to Activity Monitor directly from agents

To ensure that user activity events (such as work in applications and on websites, text input from the keyboard, mouse usage, and so on) are sent to Activity Monitor directly from the agents rather than via the **Device Monitor** server, in the **Send from agent to Activity Monitor** area, activate the **Send events directly** switch and specify the parameters:

- **Server address** – Activity Monitor server address. If you do not specify a port, the default port number will be 11008;
- **Token** – Activity Monitor server token. You can get the current token in the Investigation Centre management console, under **Global settings**, in the **Token for Device Monitor Server** field;
- **Send events every** – the interval between sending events from the agent in seconds;
- **Maximum number of simultaneously sent events** – the maximum value is 1000.

If required, deselect the box **Do not break the connection after the connection is established**.

**Important!**

Sending events to Activity Monitor directly is only possible from agents running Windows OS.
We strongly recommend to avoid the simultaneous use of direct (from the agent to Activity Monitor) and indirect (via the Device Monitor server to Activity Monitor) event sending, as it may lead to the following scenario:
If the account of the same person is used on agents with different event sending settings:

- an agent running Windows OS, on which direct sending is configured,
- and an agent running Linux, where only indirect sending is configured,

in this case, events of the person from the agent on Linux will not reach Activity Monitor.
We recommend to take this scenario into account when planning the retrieval of data from agents running both Windows and Linux, as well as from agents with a version that does not support direct sending (such as agents with older versions – 7.14 and earlier).
When enabling direct event sending, you need to change this setting simultaneously (within a short period of time) **on all** Device Monitor servers from which data is transmitted to the
This page has not yet been translated to English.
server. We do not recommend to return the setting to its original state (sending via the Device Monitor server) later, as this will require additional changes.
In case you still need to do this, follow these steps:

1. Restrict data from being received directly on the Activity Monitor server by closing the TCP port 11008 (optional action). To learn more about configuring network connections, see
   This page has not yet been translated to English.
   . *Installation Guide. Configuring Network Access Rules*.
2. Disable the direct sending to Device Monitor.
3. On each Activity Monitor node in the cluster, delete the data from ClickHouse that was generated during direct sending. To do this, use the following commands:

```
kubectl scale deployment --replicas=0 datacollector-NODENAME -n infowatch
crictl exec -it $(crictl ps | grep click | awk '//{print $1;}') clickhouse-
client --user default
truncate table datacollector.activityMonitorObjects
kubectl scale deployment --replicas=1 datacollector-NODENAME -n infowatch
```

   where NODENAME is the name of the Activity Monitor in the cluster.
   After clearing the table, the list of employees in the *Monitoring* section will also be reset until the first event appears for the person.

If you choose to send statistics directly to Activity Monitor, the *Mixed* activity type will not be generated. To learn more about activity types, see *InfoWatch Activity Monitor. Administration Guide. Product Settings. Directories. Activity Types*.

## 7.10.2 Example of data sending settings

The following rules are configured for the workstation:

- the rule for monitoring text input from the keyboard, for which the option **Take screenshot when creating an event** is enabled;
- the rule for monitoring employee activity. Activity statistics collection was selected.

The following settings are also configured:

- **Send to Traffic Monitor settings** – do not send events with screenshots according to the keyboard text input control rule;

- **Send to Platform settings** – send events with screenshots according to the keyboard text input control rule;
- **Send from Agent to Activity Monitor settings** – send events directly to Activity Monitor.

The result when the event occurs:

- screenshots are not sent to Traffic Monitor;
- screenshots are sent to the Platform;
- user activity events are sent by the agent directly to Activity Monitor.

## 7.11 Configuration

In the **Settings** → **Device Monitor** → **Configuration** section, you can:

- export/import the configuration;
- set the time for automatic resetting of unsaved configuration changes.

**To export the configuration:**

1. Click **Export** .
2. In the windows that opens, select  the items for exporting and click **Export**.
3. The configuration archive file will be saved to the **Downloads** folder of your computer.

**To import the configuration:**

1. Click **Import** .
2. In the windows that opens, drag the configuration file into the field or select the file from your computer.
3. Select  the items for importing and click **Import**.
4. Click **Import**.
   As a result, elements from the configuration file will be added to the System. The old elements will not be removed. If the names match, a number will be added to the name of the imported element, such as *"Device policy (1)"*.
   No duplicates of computers and employees will be created.

You can export/import the following configuration elements:

- **Security scheme**
  When selecting a security scheme, the **Synchronization settings with Active Directory** element will also be automatically selected.
- **Application protocol**
  Only the **Detected** application list will be exported/imported (see "Resources" Section).

  > **Important!**
  >
  > When importing the application protocol, you also need to import the security scheme. If, after import, there is no connection between the application from the protocol and the workstation where it was detected, this application will not be added to the System.

- **Settings**
  - Corporate networks settings
  - Network resource control settings
  - List of applications excluded from interception
  - Interception channels settings – Hosts for VK+

If you select the **Security scheme** element, the following will be exported/imported as part of the configuration:

- Rules:
  - Removable device control rule
  - Network resource control rule
  - Terminal session control rule
  - Print control rule
  - FTP control rule
  - HTTP(S) control rule
  - Mail control rule

- Clipboard control rule
- Cloud storage control rule
- VK messenger control rule
- Telegram messenger control rule
- Yandex Messenger control rule
- WhatsApp messenger control rule
- MAX messenger control rule
- Screenshot creation control rule
- Screen monitoring rule
- Keyboard input monitoring rule
- Employee activity monitoring rule
- Audio environment monitoring rule
- Application file control rule

**Important!**

If the import file contains the *Application file control* rule for a certain profile, but that profile is not present on the computer where the configuration is being imported, then this rule will be missing in the system after the import.
To learn more about profiles, see Universal File Interceptor.

To learn more about rules, see Adding a Rule.

- Computer groups (see *Groups Section*);
- Employee groups (see *Groups Section*);
- Resources:
  - Web resources list;
  - Application lists;
  - File categories.

To learn more about resources, see "Resources" Section.

**To set up automatic reset of unsaved configuration changes:**

1. In the *Automatic discard of unsaved configuration changes* field, specify the time between 00:05 and 23:59, after which unsaved changes should be reset.
2. Click **Save**.

**Important!**

If you change the automatic reset time while editing the configuration, the changes will take effect only after the configuration is applied/reset. To learn more about editing the configuration, see Configuration Editing Modes.

## 7.12 Event Diagnostics

In this section, you can download a report with Agent events according to the specified filters. To do this:

1. Go to **Settings → Device Monitor → Event diagnostics**.
2. In the **Start of the period** and **End of the period** filters, select the date and time for which you need to export the report. By default, the report includes events from 00:00 to 23:59.
3. To select a user, click **Select user**.
4. In the window that opens, click the required group and select a user, or use the search field. User search is available only by their ID.
5. Click . The  icon will appear next to the user who has been added. To remove the user from the list of selected, hover over their username and click .
6. Click **Apply**.
7. To select a computer, click **Select computer**.
8. In the window that opens, click the required group and select the computer, or use the search field.

9. Click . The  icon will appear next to the computer that was added. To remove the computer from the list of selected, hover over its name and click .
10. Click **Apply**.
11. Specify the number of events in the export in the **Maximum number of events per upload** field. By default, the export contains 10,000 events; the maximum number of events in the export is 1,000,000.
12. Click **Download report**.

The report in CSV format will be downloaded to the Downloads folder of your computer. It will contain the following fields:

- *Event Date*
- *Workstation*
- *Username* (the field may be empty)
- *Application* (the field may be empty)
- *RuleName* – the name of the rule according to which the event was created (the field may be empty)
- *Operation* – the action defined in the rule
- *Event Type* – the performed operation
- *Event Status* with possible values:
    - unknown
    - waiting to be processed
    - processed
    - waiting to be sent
    - sent
    - no license
    - waiting to be sent to Traffic Monitor
    - sent to Traffic Monitor
- *Security Schema Version*
- *Operation Verdict* (the field may be empty)
- *Event Id*

For events involving the use of devices, the report also includes these fields:

- *Device Type*
- *Device Instance Id*
- *Device Description*

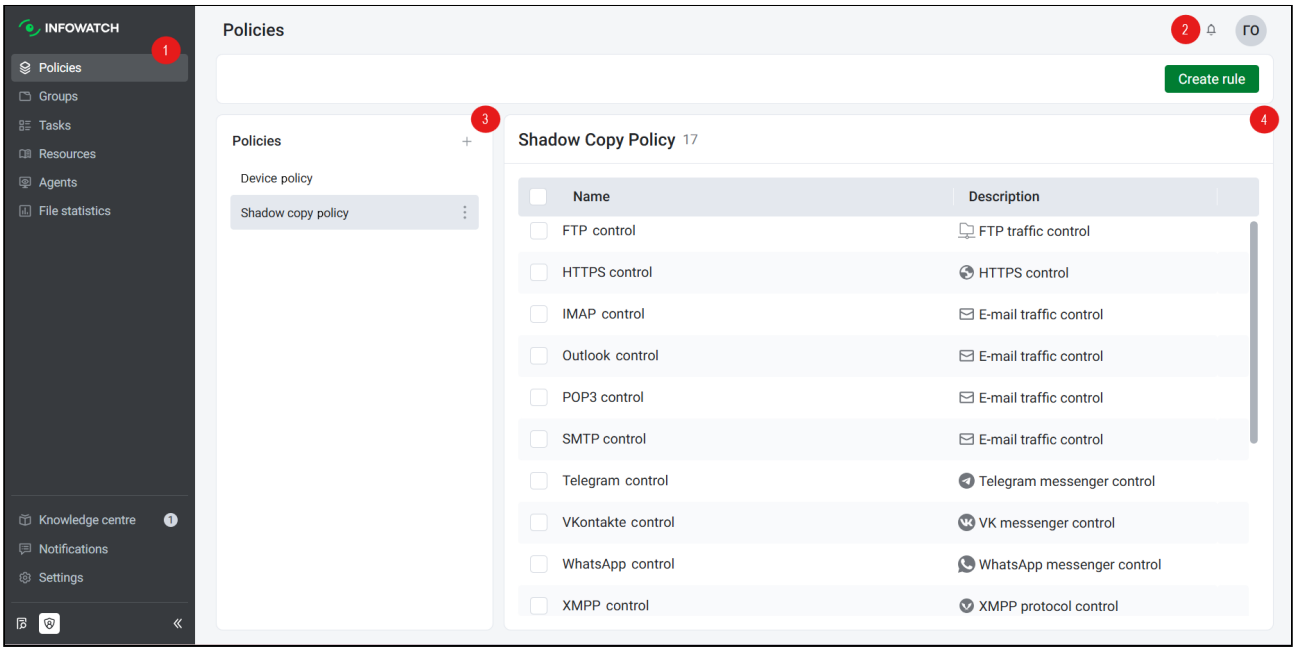
The data in the report is sorted in descending order by the date and time of the events.

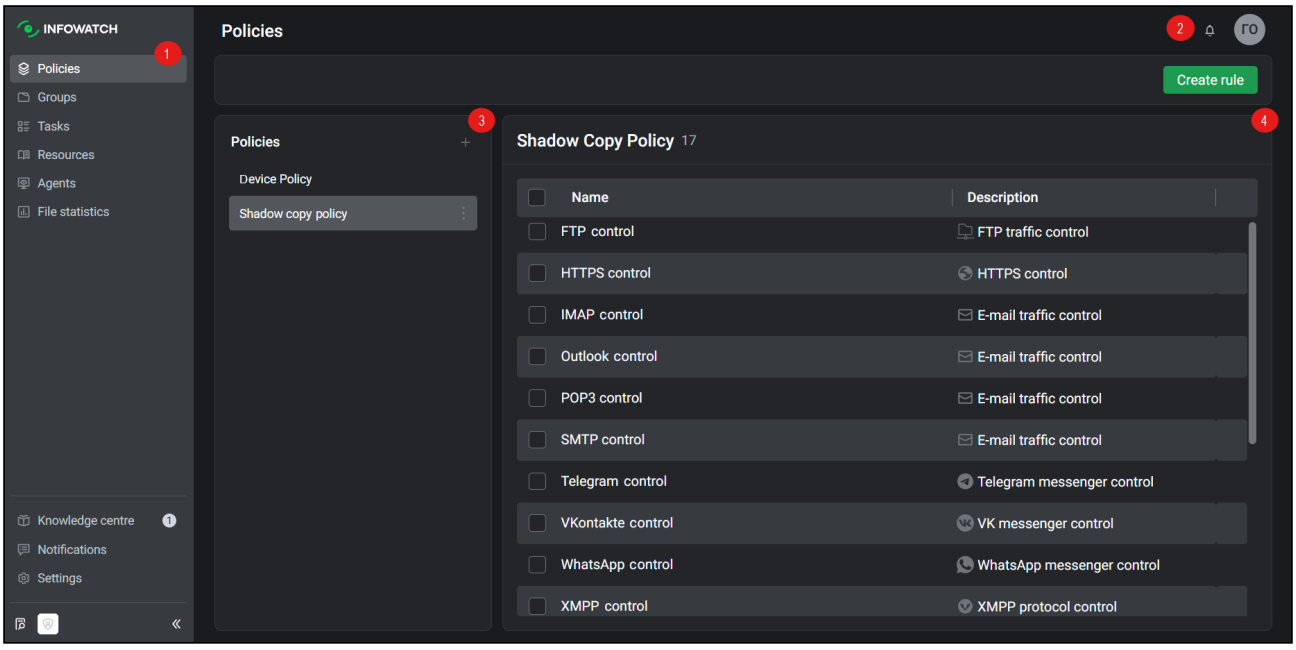
# 8 Administration Centre Interface (Device Monitor)

The Administration Centre web console ( Device Monitor) is designed to solve the following tasks:

- access control to the InfoWatch Device Monitor system;
- centralized installation and updating of Device Monitor Agents on workstations;
- configuration of the monitoring system for computers, employees, and devices;
- access control to computers and devices.

The Administration Centre interface contains several areas with settings and data (for example, the **Policies** section).




Interface elements:

| Number on the image | Window element | Purpose of the element |
|---|---|---|
| 1 | Navigation panel | Sections of the Administration Centre ( Device Monitor):<br>• Creating Policies – Device Monitor policy management: creating policies, configuring rules for each policy;<br>• "Groups" Section – management of employee records and employee groups (**Employees** tab), management of controlled computers: creating computer groups, distributing controlled computers across groups (**Computers** tab);<br>• "Tasks" Section – centralized installation, updating, and removal of InfoWatch Device Monitor Agents on computers;<br>• "Resources" Section – management of lists of web resources, applications, and file categories for use in rules;<br>• "Agents" Section – monitoring the status of Agents on workstations;<br>• File Statistics Section – management of the user file statistics configuration;<br>• **Knowledge Centre** section with documentation and a knowledge base;<br>• **Notifications** section for configuring and viewing user notifications;<br>• **Settings** section (see User Settings, Global Settings, Configuring Device Monitor).<br>You can hide the navigation panel by clicking .<br>To switch between the Investigation and the Administration Centre, click  or . |
| 2 | User menu | The user menu, where you can:<br>• select a light or dark screen display theme;<br>• edit your account;<br>• change your password;<br>• get help with hotkeys;<br>• find out about the version, view the contact details of InfoWatch and support service;<br>• select the interface language: Russian or English;<br>• log out of the System. |
| |  | The folder of system notifications containing messages received by the user in automatic mode. |

| Number on the image | Window element | Purpose of the element |
|---|---|---|
| 3–4 | Work areas | Displaying the elements of the selected section of the Administration Centre ( Device Monitor) and working with them. |

## 8.1 "Policies" Section

The **Policies** section is located in the Device Monitor Administration Centre. To access it, click  at the bottom-left of the navigation panel.
A **policy** is a set of rules according to which the analysis and processing of intercepted objects are performed.
The policy is assigned to a group of computers in accordance with the following principles:

- each group of computers must be assigned a policy;
  Adding a new group of computers is impossible if no policy has been assigned for that group. Therefore, you need to first create a policy, then create the group and select a policy for it.
- a group of computers cannot be assigned more than one policy;
- the same security policy can be assigned to multiple groups of computers, but we recommend that each group of computers is assigned its own security policy.

**Important!**

In case of multi-user access to a workstation and if it is impossible to determine the initiator of the process (event), the interception rules for employees will not be taken into account. The interception rules will only apply to this workstation. Therefore, you need to configure the interception rules not only for employees but also for the workstation that supports multi-user access.

**Rules** are a set of restrictions and conditions under which operations related to transferring files to removable devices and network resources, network activity, and sending documents to print are monitored. Each policy has its own set of rules.
There are the following types of rules in Device Monitor:

- **Monitoring of removable devices**. Allows you to track file activities on removable devices:
  - creating a file directly on a removable device;
  - copying/transferring a file to a removable device. In this case, operations involving copying/moving a file from a monitored computer, another removable device, or network resources are tracked.
- **Network resource control**. Allows you to track activities involving network resources:
  - copying a file to network resources using UNC (for example, `\\Server\SharedFolder\Folder\File`);
  - interception of file copying from network resources;
  - prohibits copying files to network resources.
- **Terminal session control**. Allows you to monitor file copying operations into the terminal session application and file copying to resources connected via the terminal session.
- **Print control**. Allows you to track actions related to printing documents on local and network printers. You can also create a shadow copy of the print job.
- **External devices control**. Allow, restrict access, and prohibit the use of removable storage devices.
- **FTP control**. Allows you to control data exchange via the FTP/FTPS protocol. You can restrict or completely prohibit the use of the FTP/FTPS protocol, as well as to create shadow copies of the transmitted files.
- **HTTP control**. Allows you to control data exchange via HTTP and HTTPS protocols. The system enables you to create shadow copies of the transmitted files.

- **Mail control**. Allows you to control the sending and receiving of emails. The system enables you to completely prohibit or allow the use of email, or to allow only the receipt of email, as well as to create shadow copies of transmitted files.
- **Cloud storage control**. Allows you to control the receipt and sending of any data to cloud storage and access to their web clients.
- **Screen control**. Allows you to take screenshots of the computer screen.
- **Clipboard control**. Allows you to control the pasting of data using the clipboard via the terminal session application.
- **VK messenger control**. Allows you to control employees' access to the VK instant messaging service. The system enables you to make a copy of the chat and create shadow copies of outgoing files.
- **Telegram messenger control**. Allows you to control employees' access to the Telegram instant messaging service: the exchange of new, forwarded, or edited chat messages (including group messages), outgoing files, and voice messages.
- **Yandex Messenger control**. Allows you to control employees' access to the Yandex Messenger instant messaging service: the exchange of new, forwarded, or edited chat messages (including group chats), as well as outgoing files.
- **WhatsApp messenger control**. Allows you to control employees' access to the WhatsApp instant messaging service: the exchange of new, forwarded, or edited chat messages (including group chats), as well as outgoing files.
- **MAX messenger control**. Allows you to control employees' access to the MAX instant messaging service: chat message exchange (including group chats) and outgoing file transfers.
- **XMPP control**. Allows you to control the exchange of incoming and outgoing text messages via the XMPP protocol, as well as outgoing files.
- **Keyboard text input control**. Allows you to intercept keyboard input in the window of any application on workstations and generate events when the active window changes.
- **Employee activity control**. Allows you to collect statistics on an employee's activity on a monitored computer.
- **Sound environment control**. Allows you to monitor an employee's activities by controlling the sound environment of their workstation.
- **Video interception control**. Allows you to monitor an employee's actions by recording the screen video of the workstation.
- **Screenshot creation control**. Allows you to prohibit employees from taking screenshots.
- **File control in applications**. Allows you to intercept file reading and/or writing events in the application.

**Important!**

Control of the Skype messenger is not supported starting from version 7.19.

For information on configuring policies, see:

- Creating Policies
- Adding a Rule

## 8.2 "Groups" Section

The **Groups** section is located in the Device Monitor Administration Centre. To access it, click  on the navigation bar. The **Groups** section contains the following subsections:

- **Computers**
- **Employees**

By "computers" in the Device Monitor system, we mean monitored computers on which Device Monitor Agents are installed.

Active policies can only be assigned to a group of computers. To define a policy for an individual computer, you need to include the computer in a group.

The computer registered in Device Monitor must be part of at least one computer group (**the default computer group**). This is because a security policy cannot be assigned to an individual computer.
The **default computer group** includes all computers for which no other computer groups have been defined:

- computers first registered in Device Monitor;
- computers excluded from all other groups.

After installing the System, a **policy for devices** is assigned to the **default computer group**.
You can exclude a computer from the **default computer group**, provided that the computer is added to at least one other computer group.
To learn about working with monitored computers, see Working with Computer Groups.
Registration of monitored users (employees) in the System is performed in accordance with the following principles:

- Each employee must be a member of at least one employee group (the "default" group). This is because a security policy cannot be assigned to an individual employee.
  The "default" group includes the accounts of all employees for whom no other employee groups have been defined: employees who have been registered in Device Monitor for the first time, employees who have been excluded from all other employee groups.
  You can exclude an employee from the "default" group provided that the employee's account has been added to at least one employee group other than the "default" group.
- After the System is installed, the "default" group of employees is assigned a **shadow copy policy** containing the following rules:
  - FTP control
  - HTTPS control
  - IMAP control
  - Outlook control
  - POP3 control
  - SMTP control
  - Telegram control
  - VKontakte control
  - WhatsApp control
  - XMPP control
  - Webmail control
  - Cloud storage control
  - Yandex Messenger control
  - Shadow copying of documents
  - Shadow copying of documents in a terminal session
  - Shadow copying of documents to network resources
  - Shadow copying of printing

To learn more about the rules, see "Policies" Section.
To learn more about working with monitored employees, see Working with Employee Groups.

## 8.3 "Tasks" Section

**Important!**

The **Tasks** section will be disabled in later versions. Installation, update, and removal management is available in a new section with enhanced control and prioritization capabilities. We recommend navigating to **Distribution policies** in the **Agents** section to continue working. See Distribution Policies.

The **Tasks** section is located in the Device Monitor Administration Centre. To access it, click  on the navigation bar. This section displays a list of all tasks created by the user. These can be primary distribution or update tasks. The workspace of the main window shows a list of workstations for which the selected task is being performed. The **Details** panel displays the parameters specified when creating the selected task. To hide the panel, click .
To create and run a task, see the article Primary Distribution and Updating Task.

## 8.4 "Resources" Section

The **Resources** section is located in the Device Monitor Administration Centre. To access it, click  on the navigation bar.
The **Resources** section contains the following subsections:

- Web resources list
- Application lists
- File categories

### 8.4.1 Web resources list

In the **Web resources list** subsection, you can create resource lists to be used use in the automatic screenshot creation rule. Using the lists, you can specify which web resources the rule should monitor or exclude from monitoring.
To learn more about working with resource lists, see Creating and Editing Resource Lists.

### 8.4.2 Application lists

The subsection contains lists of applications that you can use in rules to make monitoring more precise.
You can use application lists in:

- the keyboard input monitoring rule (see Keyboard Input Monitoring Rule);
- the clipboard control rule (see Clipboard Control Rule);
- the screen monitoring rule (see Screen Monitoring Rule).

The list of applications contains the following information:

- *Application name*
- *Description*
- *Product name* *
- *Issuer* *
- *Executable file path*

**Note:**

* The *Product name* and *Issuer* columns are available only for Windows applications.

You can change the width of a column in a table and move it.
To learn about creating lists and adding applications to them, see Creating and Editing Application Lists.

#### Detected applications

The **Detected** list contains a table with information about applications that were launched on monitored workstations running Windows.
After installing the InfoWatch Device Monitor Agent on workstations running Windows and restarting them, the System automatically begins to receive information about the applications being launched. Information about all launches and installations forms the list of detected applications.
The table contains the following information about the applications:

- *Date added*
- *Workstation*
- *User*
- *Description*
- *Product name*
- *Issuer*
- *Executable file path*

You can move the columns in the table and change their size.
From the table, you can add applications to lists for Windows. To learn about creating lists and adding applications to them, see Creating and Editing Application Lists.

**Note:**

To reduce the load on the CPU, the database table containing records of application launches is added to the regular cleanup queue. To learn more, see Deleting Records of Device Monitor Application Log (decreasing CPU load).

**Important!**

The list of detected applications is required so that the Security officer cannot prohibit an application without which the computer will stop functioning properly.

### 8.4.3 File categories

The **File categories** section contains a list of file extensions that Device Monitor can recognize. For ease of use, the extensions are grouped **by category**:

- CAD systems
- Archives
- Audio-video
- Databases and tables
- Graphical data
- Documents (office files, PDF)
- Other files
- Protected data (encrypted, PKI elements, password stores)
- Executable files
- Images (virtual machines, disk images, memory dumps)
- Mobile device data formats

For the following rules, you can specify which file category they will apply to:

- Removable Device Control Rule
- Network Resource Control Rule
- Terminal Session Control Rule

You can create your own file categories from the preinstalled extensions. To learn more about working with file categories, see Creating and Editing File Categories.

## 8.5 "Agents" Section

The **Agents** section is located in the Device Monitor Administration Centre. To access it, click  on the navigation bar. The section contains the **Status** tab, where you can monitor the status of Agents on workstations.
To learn about viewing information about Agents and assigning statuses to them, see Working with Agents.

## 8.6 "File Statistics" Section

The **File statistics** section is located in the Device Monitor Administration Centre. To access it, click  on the navigation bar. In this section, you can edit the preset user file statistics configuration.
**File statistics configuration** is a set of application inclusion/exclusion rules, file extensions, file paths, and other parameters for configuring user file statistics.

**Note:**

The default configuration includes the following exceptions:

- file extensions: 000; .386; .adv; .ani; .ann; .automaticdestinationsms; .bcd; .bin; .bio; .bk1; .bk2; .bmk; .bud; .cab; .cat; .chg; .chs; .cht; .ci; .clb; .cnt; .cpi; .cpl; .cur; .cust omdestinations-ms; .dat; .desklink; .deskthemepack; .dev; .devicemetadatams; .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; .itemdat a-ms; .js; .job; .jpn; .kbd; .kor; .libraryms; .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; .reg trans-ms; .rs; .scf; .scr; .searchconnectorms; .shd; .spl; .spx; .str; .swp; .sys; .theme; .trx_dll; .uce; .vga; .vx_; .vxd; .wdf; .wer; .wsf; .wsh; .xrmms; .zone.identifier; .tmp; .crdownloads; .thumbs.db
- file paths: \Recovery\;\System Volume Information\;\MSOCache\;\Windows\;\Program Files\;\Program Files (x86)\; \Users*\AppData\

The following subsections are displayed in the workspace:

- **General** – editing the configuration of file statistics and the list of applications that are included in or excluded from the interception;

- **Interceptions** – configuring inclusion and exclusion of file extensions and file paths.

  **Important!**

  Including/excluding extensions and paths applies only to the files and folders that are directly affected by the action.

  **Example 1**

  If files with the `.docx` extension are configured in the exceptions, then when a user works with a folder that contains files with this extension, an event for the action with the `*.docx` file is generated and sent to the Platform.

  **Example 2**

  *Folder 2*, which is a subfolder of *folder 1*, is configured in the exceptions:

  - if the action is performed with *folder 1*, then events for all files located in *folder 2* will be generated and sent to the Platform;
  - if the action is performed with *folder 2*, it falls under the exceptions, and no folder event is generated on the agent side.

To learn about editing the configuration, see Working with File Statistics.

# 9 Detection of Workstations for Installing Agents

The  Device Monitor server installation distribution kit includes a utility for scanning a range of IP addresses. It is installed automatically with the Device Monitor management console. The scan result is a text file with a "IP-address or domain name – operation system" list for workstations on which the Device Monitor Agent is not installed.

The utility has no graphical interface and is launched from the command line. The parameters that need to be specified or can be specified during launching are described below. To view their description, open the help: `Iw.Util.MachineDiscovery -- help`.

| | |
|---|---|
| `--mode arg (=icmp)*` | Network scanning mode (required parameter):<br>• `nmap` – scanning the network using the `nmap` utility that can additionally determine the type of operation system based on heuristic algorithms;<br>• `icmp` – scanning the network by ICMP protocol. |
| `--ip-range arg` | The IP-address range in one of the formats valid for `nmap` (required parameter). For example: "`--ip-range 10.60.3-35.1-254`". |
| `--ip-cidr-range arg` | The IP-address range in CIDR format (required parameter). For example "`--ip-cidr-range 10.60.3.4/24`". |
| `--ipv6-cidr-range arg` | The IPv6-address range in CIDR format (required parameter if the IPv6 protocol is used). For example: `"--ipv6-cidr-range fe80::98b9:ec9:f9a9:9104/120"`.<br>**Warning!** Only the CIDR format is supported for IPv6-addresses. |
| `--threads arg (=2)` | The number of threads for processing asynchronous network scanning requests. |
| `--icmp-attempts arg (=2)` | The number of attempts to contact the IP-address via the ICMP protocol to determine that it is unavailable. Since the ICMP protocol does not guarantee packet delivery (unlike TCP), packets may be lost, and several attempts are required to be more confident that the addressee is unavailable. |
| `--icmp-timeout arg (=5000)` | The time to wait for a response from the addressee for each attempt to check its availability. |
| `--deploy-agent-port arg (=15505)` | The distribution agent's port, on which it listens to the network. You need to leave the default value. |
| `--output-file arg` | The path to the file containing the utility's result. |

| | |
|---|---|
| `--nmap-path arg (nmap mode)` | The path to the cross-platform `nmap` utility when using the `nmap` mode. |
| `--nmap-os-info arg (=1)` | Whether to determine (=1) or not to determine (=0) the operation system of a workstation when scanning in the `nmap` mode. |
| `--nmap-save-output-to-file arg (=1)` | Save `stdout` and `stderr` from `nmap` to the file `Nmap_output_%Y-%m-%d_%H-%M-%S.log` |
| `--nmap-timing arg (=3)` | Scanning frequency by `nmap`:<br>• from 0 – the slowest and the most accurate scan;<br>• to 5 – the fastest and the least accurate scan. |
| `--nmap-min-hostgroup arg (=16)` | The minimum group size for parallel scanning by `nmap`. |
| `--nmap-max-hostgroup arg (=16)` | The maximum group size for parallel scanning by `nmap` (to 1024). |
| `--nmap-min-parallelism arg (=10)` | The minimum number of requests for a group of hosts (from 1). |
| `--nmap-max-parallelism arg (=10)` | The maximum number of requests for a group of hosts. |
| * – the default value is indicated in brackets. | |

To run the utility:

1. In the command line of the workstation with the Device Monitor console, go to the directory with the `Iw.Util.MachineDiscovery` utility using the `cd` command:

   ```
   cd  <path_to_utility>
   ```

2. Run the utility, making sure to specify the range of IP-addresses, and other parameters, if needed. For example:

   ```
   Iw.Util.MachineDiscovery --ip-range 10.60.3-35.1-254
   ```

3. Wait for the scan to complete.
4. When the scan is complete, the results will be saved to the `iw_machine_discovery.output.txt` text file in the directory where the utility is located. Use the obtained data to create a list of computers for Agent installation (see Primary Distribution and Updating Task).

# 10 Primary Distribution and Updating Task

**Important!**

The **Tasks** section will be disabled in subsequent versions. Installation, update, and removal management is available in a new section with enhanced control and prioritization capabilities. We recommend navigating to the **Distribution policies** in the **Agents** section to continue working. See Distribution Policies.

Follow the sequence of actions:

1. Create a primary distribution task.
2. Generate a list of workstations for installing the Agents..
3. Run the task.
4. If there are errors, review information about them or download the log.

**To create a primary Agents distribution task:**

1. In the left part of the workspace, click .
2. Select the operating systems of the workstations to which you need to distribute the Agents: *Windows*/*Linux*.
3. Enter the name of the new task.
4. Deselect the box **Install the network traffic interception component** if you do not want this component to be installed.
5. Starting from **Device Monitor version 7.18.5, during the initial installation of the Agent**, the installer checks whether the list of applications that should be excluded from interception has been received. If the list of exclusions is not received, the installation of this Agent will be stopped. In this case, an entry will be added to the error log:
   - for Linux – `ERROR: exclusions not received (rc=255); abort install (exit 2)`
   - for Windows – `CustomAction GetExclusionsFromServerWithCheck returned actual error`

   The check is enabled by default. If you want to disable it, deselect the box **Cancel the installation if receiving the list of applications excluded from interception fails**.
6. If needed, add a description of the task.
7. Specify the number of task runs and their frequency in minutes.
8. Specify the Agent distribution point that was previously configured on the Device Monitor server (see New Installation, step 30). Or select the **Use all available distribution points** box.
9. The latest available version of the Agents whose distribution kits need to be installed is displayed in the **Version** field (see Servers).

   **Note:**

   All available versions are located in the directory `/opt/iw/iwdistribution/bin/SetupPackages/`
10. Specify the number of attempts to download the package. The default value is 10.
11. Click **Add**. The new task will be displayed in the task list.

**To update the version of the Agents on workstations running Linux:**

1. Open the created task for editing by clicking .
2. In the **Version** field, specify the new version of the Agent whose directory is located at the distribution point. If the task specifies a computer with an older version of the Agent installed, it will be updated after the task is completed.
3. Click **Add**.

**Important!**

To ensure proper blocking of removable devices, make sure to restart the workstation after updating the Agent.

**To create a list of workstations:**

Add computers in one of the following ways:

1. To add a computer manually, click  in the selected task.
2. In the window that opens, enter the IP address or DNS name of the computer, separated by a semicolon or a line break (the computer name can consist of any characters from any alphabets specified in Unicode).
3. Click **Add**.

or

1. To add computers from the list, click **Set up task composition** :
2. In the window that opens, a list of computers from the available integration with Active Directory or previously added computers of the Device Monitor group will be displayed (see Setting up Computer Group Membership), along with the full name for installing Agents. Select the workstations in the **Computers** area and click . When adding a group, only computers from the selected group are added, excluding computers in subgroups. You can use the search field to quickly find the required computer and add it to the task. Enter at least 3 and no more than 64 characters.
3. Click **Apply**. The area with the task name will display a list of computers with the full name specified for installing the Agents. If the Agents were not previously installed on the specified computers, or if the Agents' versions are lower than the version specified in the task, then after the task is launched, the Agents will be installed or updated.
4. To delete erroneously added addresses, select them and click .

**To run the task**:

1. Select the task with the added workstation addresses or click  next to the required task in the list on the left.
2. Click **Run** .
3. In the window that opens, enter the credentials of the user on the remote workstation on whose behalf the task is being run.
4. If you are running a task to distribute agents to workstations running Linux operating systems:
   a. Select the mechanism for escalating the privileges `sudo` / `su`.
   b. If you have selected the `su` privilege escalation mechanism:
      - enter the credentials of the user on whose behalf the agents will be distributed.
      or
      - select **Use specified credentials** to distribute agents on behalf of the user specified in step 3.
5. Click **Run**.
6. Wait for the task to complete.

For each workstation that the task applies to, the following parameters are displayed in the workspace of the main window:

| Parameter | Description |
|---|---|
| Name | The IP address or domain name of the workstation. |

| Parameter | Description |
|---|---|
| Task status | The current status of the task for this workstation. Possible values:<br>• **Error**<br>• **Ignored**<br>• **Scheduled**<br>• **Installation in progress**<br>• **Executed** |
| Agent version | The version of the Agent installed on the workstation. |
| Operating system | The operating system installed on the workstation. |
| Operating system digit | The bitness of the operating system on the workstation. |
| Number of connections | The number of attempts made to connect to an unavailable workstation. |
| Last access time | Date and time of the last connection to the workstation. |

If the task is completed with the status **Error**, you can go to the error log and view the detailed information.

**To view information about errors during the installation of Agents and to export the logs:**

1. Select the row in the table with the task status **Error**.
2. Click . General information and error descriptions will be displayed.
3. Click  to export the logs in TXT format.

> **Note:**
>
> If an error occurs during the installation of the Agent, you can only download the error log from the last task run.

To return to the list of workstations, click .

# 11 Security Scheme Configuration

The
This page has not yet been translated to English.
**security scheme** is a set of configuration parameters that regulate the monitoring of the actions of the monitored employees. The security scheme is created during the Server installation process 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**, each with its own assigned security policy;
- **Computer groups** with a security policy assigned to each of them.
- **Lists of applications** permitted or prohibited for use in the rules;
- **File categories** that can be used to extend the rules for controlling removable devices to specific file formats;
- **File statistics configuration** for setting up control over an employee's file activities.

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

The remaining entities of the System are not included in the security scheme.
You can edit the security scheme multiple times. The edited security scheme will be saved as a new version of the existing security scheme. The old versions of the security scheme are not deleted but are stored in the database. In the Investigation Centre, you can view the policies and the rules they contain for any version of the security scheme.
You can find the detailed information about configuring the scheme in these subsections:


- Configuration Editing Modes
- Creating Policies
- Adding a Rule
- Creating and Editing Application Lists
- Creating and Editing Resource Lists
- Creating and Editing File Categories
- Working with Computer Groups
- Working with Employee Groups
- Working with Agents
- Working with File Statistics


## 11.1 Configuration Editing Modes

In the current version of Device Monitor, two configuration editing modes are available in the Device Monitor **Universal file interceptor** settings and in the **Groups**, **Policies**, and **Resources** sections of the Administration Centre:

- **Synchronous editing**. In this mode, all users can edit the configuration simultaneously. Configuration editing will be unavailable only when synchronization with the directory service is running;
- **Synchronous editing prohibited** (default). At any given moment, only one user can edit the configuration. All changes made by the user take effect only after the configuration is saved. Other users cannot edit the configuration at that time. Editing will also be blocked for all users when synchronization with the directory service is running.

### 11.1.1 Synchronous editing prohibition mode

The synchronous editing prohibition mode is enabled by default.
To configure the synchronous editing prohibition mode, add the `"SandboxSettings"` parameter to the configuration. To do this:

1. Open the configuration file `/opt/iw/dmserver/webapibin/webapi.appsettings.json`
2. In the latest configuration, find the line:

```
"ConnectionString":
"Server=<server_name>;Port=<port>;Database=<database_name>;User
Id=<user_id>;Password=<password>;",
```

and after it, add:

```
"SandboxSettings":
{
    "UseSandbox": "False",
}
```

where:

- `UseSandbox` is the setting to prohibit synchronous editing. To disable the editing mode, set the value to `False`. For further configuration or to enable the mode, set the value to `True`.

3. If necessary, add the `ResetTimeMinutes` setting to the parameter, which allows any user to reset the configuration that is currently being edited. The value is set in minutes. The minimum value is 5, the maximum is 999.
4. Restart the service using the command:

```
systemctl restart iwdms_webapi.service
```

### 11.1.2 Automatic reset of unsaved configuration changes

If the user is inactive for the set period of time, the configuration editing is automatically reset. By default, the configuration is reset after 20 minutes of user inactivity.
To change the reset time, go to **Settings** > **Configuration** (see Configuration).

**Important!**

If you change the automatic reset time while editing the configuration, the changes will take effect only after the configuration is applied/reset.

### 11.1.3 Description of the editing prohibition mode

All your configuration changes are available only in the current browser session until they are saved.
After editing the configuration, you can save the changes or reset them by clicking the corresponding buttons on the information panel at the top of the screen.




If the configuration is already being edited by another user, editing actions become unavailable or are hidden. A message will appear at the top of the screen telling that the configuration is being edited by another user. If you try to change a locked scheme, a save error message will appear.
You can reset another user's configuration only after the time specified in the parameter has elapsed.

**Important!**

If the configuration editing results in an error, the System still considers it locked.
When resetting another user's configuration, all changes in unfinished sessions will be lost.

Actions that do not change the configuration do not block it. For example, when you edit information about one computer/employee, the ability to edit the configuration will not be blocked for other users.
If the user does not interact with the Management Console within the time specified in the parameter, the changes made will be automatically reset and the configuration will be unlocked.

### 11.1.4 Restoring access to the blocked configuration

During work, a situation may arise where none of the users are editing the configuration, but it still locked. This is possible if the configuration editing process was completed incorrectly (for example, when the user changes the browser or clears the browser cache during editing).

The configuration will be automatically unlocked after the time specified in the parameter if the user who made the changes does not interact with the Management Console during this time.
To restore access before automatic unlocking, restart the `iwdms_webapi.service` service using the command:

```
systemctl restart iwdms_webapi.service
```

**Important!**

When restarting the `iwdms_webapi.service`, all changes in unfinished sessions will be lost.

### 11.1.5 Editing the configuration while synchronization with the directory service is running

When synchronization with the directory service is started (see Synchronization), editing actions become unavailable or are hidden. At the top of the screen, the message appears telling that the synchronization process is running and editing the configuration is prohibited.
This functionality is enabled by default.

## 11.2 Creating Policies

**Important!**

When upgrading the
This page has not yet been translated to English.
server to version 7.15 or higher, agents connected to this server running version 7.13 or earlier will stop receiving data about changes to the security scheme. Therefore, to ensure that agents can receive rules, policies, computers, employees, etc., you need to also upgrade the agents to version 7.14 or later.

On Device Monitor Agents, policies are applied in the following order:

1. Prohibitive policies.
2. Data protection policies on agents created in Traffic Monitor.
3. Shadow copy policy.

Each security policy consists of a set of rules that are used to monitor operations related to transferring files to removable devices and network resources, sending documents to print, and network activity, and to determine the level of access to controlled peripheral devices.
Policies are assigned to **employee groups** and **computer groups**. A policy assigned to a group of employees applies to all employees included in that group. A security policy assigned to a group of computers applies to all employees working on the monitored computers included in that group.
You can work with security policies in the **Policies** section. To go to this section, click **Policies** on the navigation panel.
After installing the Administration Centre ( Device Monitor), two policies are created by default – **Shadow copy policy** and **Device policy**.
The **shadow copy policy** contains the following rules:

- FTP control
- HTTPS control
- IMAP control
- Outlook control
- POP3 control
- SMTP control
- Telegram control
- VKontakte control
- WhatsApp control
- MAX control
- XMPP control
- Webmail control
- Cloud storage control
- Yandex Messenger control

- Shadow copying of documents
- Shadow copying of documents in a terminal session
- Shadow copying of documents to network resources
- Shadow copying of printing

The default **device policy** does not contain any rules.

**To create a new policy:**

1. In the left part of the workspace, click .
2. In the **Name** field, enter the policy name.
3. Click **Create**.
4. If the synchronous editing prohibition is enabled, click **Save** in the information panel (see Configuration Editing Modes).

After creating the policy, add one or more rules to it. To learn more about applying the rules, see Adding a Rule.

**To edit a policy:**

1. In the left part of the workspace, select a policy.
2. Click  next to the selected policy.
3. In the drop-down list, click  **Edit policy**.
4. In the **Name** field, specify the new name of the policy.
5. Click **Save**.
6. If the synchronous editing prohibition is enabled, click **Save** on the information panel (see Configuration Editing Modes).

**To delete a policy:**

1. In the left part of the workspace, select a policy.
2. Click  next to the selected policy.
3. Click  **Delete policy**.
4. Confirm the action.

   **Note:**

   If a security policy is assigned to at least one employee group or a computer group, it cannot be removed from the security scheme.
5. If the synchronous editing lock is enabled, click **Save** on the information panel (see Configuration Editing Modes).

## 11.3 Adding a Rule

**To add a rule to a security policy:**

1. Go to the **Policies** section of the Administration Centre.
2. On the left of the working area, select a security policy to which you want to add the rule.
3. Press  next to the selected policy. In the drop-down list, click  **Create Rule**.

   or

   In the upper-right of the working area, click **Create Rule**.
4. In the window that opens, specify the rule's parameters. Available rules:
   - Data transmission channel control:
     - Removable Device Control Rule
     - Network Resource Control Rule
     - Terminal Session Control Rule
     - Print Control Rule
     - External Device Control Rule
     - FTP Control Rule
     - HTTP(S) Control Rule

        - Mail Control Rule
        - Cloud Storage Control Rule
        - Network Traffic Proxying Rule
        - Clipboard Control Rule
    - Messenger control:
        - VK Messenger Control Rule
        - Telegram Messenger Control Rule
        - Yandex Messenger Control Rule
        - WhatsApp Messenger Control Rule
        - MAX Messenger Control Rule
        - XMPP Protocol Control Rule

        **Important!**

        Skype messenger monitoring is not supported starting from the version 7.19.
    - User activity monitoring:
        - Screen Monitoring Rule
        - Keyboard Input Monitoring Rule
        - Employee Activity Monitoring Rule
        - Audio Environment Monitoring Rule
        - Screen Video Recording Rule
    - Usage control:
        - Screenshot Creation Control Rule
    - Application control:
        - Application File Control Rule
5. Once you have set all necessary parameters, click **Create**. The rule will be added to the policy.
6. In case if synchronized editing is prohibited, click **Save** on the information panel (see Configuration Editing Modes).

**Note:**

Device Monitor allows you to intercept the actions of an employee connected to a workstation through a terminal session:

- on **OS Linux only through xRDP**. The details of this type of interception are specified separately for each rule;
- on **OS MS Windows through RDP**, without limitations.

To view detailed information about a rule, select it. The rule information will be displayed on the panel on the right.

To hide the panel, press  in the upper-right corner or click on the rule again.

**To edit the rule:**

1. Go to the **Policies** section of the Administration Centre.
2. Select a policy.
3. Select the rule you need to edit.
4. Press  next to the selected rule.
5. Press **Edit**.
6. Make changes.
7. Press **Save**.
8. In case if synchronized editing is prohibited, press **Save** on the information panel (see more in Configuration Editing Modes).

**To delete the rule:**

1. Go to the **Policies** section of Administration Centre.
2. Select a policy.

3. If you need to remove a rule, click  next to it and select **Remove**.

   If you need to remove several rules, select them on the left  and click  on the panel at the bottom.

   If you need to remove all the rules in the policy, select them  in the table header, then click  on the panel at the bottom.
4. Confirm the action.
5. In case if synchronized editing is prohibited, click **Save** on the information panel (see Configuration Editing Modes).

### 11.3.1 Removable Device Control Rule

The rule allows you to track the following operations:

- copying files to/from removable devices;
- creating new files on removable devices;
- modifying and renaming files on removable devices;
- copying files to/from media devices that use the MTP protocol for connection;
- copying files on removable devices (for example, from one folder on a USB device to another).

Removable devices include:

- devices connected via USB and IEEE 1394 ports (FireWire, i-Link);
- floppy disk drives (Floppy-disk, ZIP);
- optical discs (CD, DVD, BD) in Live File System mode;
- media devices.

**Important!**

On computers running Linux-based operating systems, write operations to CD/DVD discs, including those connected via USB ports, are not monitored.

**To configure the rule:**

1. Open the rule creation window and enter the rule name in the **Name** field.
2. In the **Interception channel** field, open the drop-down list and select **Control data transmission channels** -> **Removable storage**.
3. Select the direction of the copy interception: **To device** or **From device**. The event will be created as a result of copying the file in the selected direction.
4. Under **Action type**, select the System's response to file copying:
   - **Create event** to create an event with a shadow copy;
   - **Exclude from interception** – allow the copying, no event will be created. To create a rule, fill in at least one of the following fields below: **File mask** or **File category**.
5. Select **Create a shadow copy** if you need to create a shadow copy in the event (this setting is available when you select **Create event** in the **Action type** field).

   **Note:**

   In Traffic Monitor, an event without a shadow copy displays the file name and size.
6. Specify the conditions for event generation:
   a. Select and specify the **File mask** to apply the rule to files that match it. You can use wildcard characters:
      - ? – one unknown character;
      - * – any number of characters.
   b. You can limit the application of the rule to a specific file category by clicking **File category** and selecting the required category from the drop-down list.

      **Note:**

You can familiarize yourself with the file categories in the "Resources" Section, as well as in the knowledge base article Intercepted file extensions in Device Monitor (for rules with File category selection).
If you specify both a file mask and a category, both specified conditions must be met for the rule to be triggered.
On computers running Linux, extension categories are not taken into account – the rule will be triggered for copying any files, regardless of the specified file categories.

c. Specify the **File size** to limit the size of files subject to monitoring. Specify the range of values for the minimum and maximum file size and the unit of measurement. If both fields are filled in, the rule will apply only to files whose size is within the specified range.
By default, the condition is enabled, and the file size is set to 0 to 10 MB.
If the conditions are not enabled, the event will be generated without taking them into account.

7. After you have configured all the required parameters, click **Create**. The rule will always be in effect and will allow copying with the creation of an event with shadow copies. Subsequently, such events are sent for analysis to Traffic Monitor.

**Important!**

On workstations running Linux, when copying is blocked:

- copied files are deleted (with the possibility of recovery, provided that special software is used);
- if the removable device was ejected forcibly, the file copying block based on the analysis results may not be triggered;
- when copying files from a workstation to a removable device, the file path is not detected. Therefore, policies configured to use the path as the source of copying may not work;
- there is no blocking based on the analysis results when copying files to media devices connected via the MTP protocol;
- if a file is blocked based on the analysis results when it is moved or a *cut-paste* operation is performed on it, the file may be deleted from the source and missing from the receiver.

  The `move` operation is not supported:
  - in RED OS 8 when using the *Dolphin* file manager (*KDE* graphical environment);
  - in Astra Linux when using the *Fly* file manager;
  - in the *Midnight Commander* file manager;
  - via Bash commands.

  The move operation is supported:
  - in RED OS, when using the *Caja* file manager (*MATE* graphical environment). If the operation is prohibited by policies, *Caja* displays the `error.png` message;
  - in ALT OS 11.1, when using the *Nautilus* file manager (*GNOME* graphical environment).

The system unpacks the archives and applies Traffic Monitor policies to them if:

- an archive in the 7Z, ZIP, TAR.GZ, AR, RAR, or ISO format has been intercepted on the Agent running Windows;
- an archive in the 7Z, ZIP, AR, or TAR.GZ format has been intercepted on the Agent running ALT OS, RED OS, or Astra Linux 1.7.

To learn about the specifics of how the rule works, see 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*.

### 11.3.2 Network Resource Control Rule

The rule controls actions with network resources and allows you to:

- intercept copying files to network resources using UNC (for example, *Server**SharedFolder**Folder**File*);
- intercept copying files from network resources;

- prohibit copying files to network resources.

**Important!**

Copying a file from network resources to a workstation running Linux can be blocked only when transferring via the SMBv1/CIFS protocol using one of the following methods:

- connecting to network resources with mounting to the file system:

```
mount -t cifs
```

- connecting to network resources using standard file explorers, built-in utilities, and third-party tools.

The system unpacks the archives and applies Traffic Monitor policies to them if:

- an archive in the 7Z, ZIP, TAR.GZ, AR, RAR, or ISO format has been intercepted on the Agent running Windows;
- an archive in the 7Z, ZIP, AR, or TAR.GZ format has been intercepted on the Agent running ALT OS, RED OS, or Astra Linux 1.7.

**Important!**

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

- when copying files to network resources, only the final destination path is known, and when copying from a network resource, only the source path is known;
- copying a file to a network resource is not intercepted if the connection was established by entering the server name in the search bar of the OS file manager.

On a workstation running Linux, when connecting to a terminal session via xRDP, the event attribute **Network address of a terminal Agent** may contain the IP address of the remote computer.

**To configure the rule:**

1. Open the rule creation window and enter the rule name in the **Name** field.
2. In the **Interception channel** field, open the drop-down list and select **Control data transmission channels -> Network share**.
3. Select the copy interception direction: **To resource** or **From resource**. The event will be created as a result of copying the file in the selected direction.
4. You can select the **Prevent copying** mode. The prohibition is available only when copying is directed to a resource. In this case, the **Action type** field will be set to **Create event** and will be unavailable for editing. The **File mask**, **File category**, and **File size** fields will also be unavailable.
5. In the **Action type** field, select the System's response to file copying:
   - **Create event** to create an event with a shadow copy;
   - **Exclude from interception** – allow the copying, no event will be created. To create a rule, fill in at least one of the following fields below: **File mask** or **File category**.
6. Select **Create a shadow copy** if you need to create a shadow copy in the event (this setting is available when you select **Create event** in the **Action type** field).

   **Note:**

   In Traffic Monitor, an event without a shadow copy displays the file name and size.
7. If required, specify the **Resources** by setting their addresses. To view the rules for specifying, hover the cursor over .
8. If required, you can limit the set of monitored files by setting a file mask. To do this, check the **File mask** field and specify the mask. You can use the following characters: **?** to replace a single character or ***** to replace a set of characters. For example, `*.doc`. The space character is interpreted as part of the file name.

   **Important!**

   There can be a single mask for a single rule. If you need to enter several masks, create one rule for each of the masks.

> **Note:**
>
> On computers running Astra Linux or RED OS, file masks are not taken into account.

9. You can limit the application of the rule to a specific file category by clicking **File category** and selecting the required category from the drop-down list.

> **Note:**
>
> You can familiarize yourself with the file categories in the Resources Section, as well as in the knowledge base article Intercepted file extensions in Device Monitor (for rules with File category selection).
> If you specify both a file mask and a category, both specified conditions must be met for the rule to be triggered.
> On computers running Linux, extension categories are not taken into account – the rule will be triggered for copying any files, regardless of the specified file categories.

10. To limit the size of files subject to monitoring, specify the range of values for the minimum and maximum file size and the unit of measurement. If both fields are filled in, the rule will apply only to files whose size falls within the specified range.
    By default, the condition is enabled and the file size is set to 0 to 10 MB.
11. After you have defined all the necessary parameters, click **Save**. The rule will apply permanently.

To learn about the specifics of how the rule works, see 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*.

### 11.3.3 Terminal Session Control Rule

The rule allows you to track the following operations:

- copying a file to the application of the terminal session[1];
- copying a file to resources connected via the terminal session (redirection for network folders and virtual devices is supported)[1 2].

> **Important!**
>
> [1] A terminal session refers to the corresponding Microsoft and Citrix technologies.
> When copying a file via a terminal session using the clipboard, only the short file name will be known, not the full path.
> For the event to include the IP address of the node to which the data was copied, the Device Monitor Agent must be present on the remote computer for which the terminal session is open.
> If the Device Monitor Agent is installed only on the computer from which the connection to the terminal session is established, the event will contain information only about the application through which the data was copied, without indicating the recipient's IP address.
> To transfer files when using terminal access tools, we recommend to use the mechanism of "disk forwarding" to the remote session instead of transferring files via the clipboard.
> [2] Terminal session events will not be generated when copying files not across the terminal session boundary, but within the local remote connection client. For example, when a user copies files in the **Connection parameters -> File open** window.
> For Agents on workstations running Linux, interception of file operations with devices connected via a terminal session is not supported.

**To configure the rule:**

1. Open the rule creation window and enter the rule name in the **Name** field.
2. In the **Interception channel** field, open the drop-down list and select **Control data transmission channels** -> **Terminal session**.
3. Select the direction of the copy interception: **To session** or **From session**. The event will be created as a result of copying the file in the selected direction.
4. Under **Action type**, select the System's response to file copying:
   - **Create event** to create an event with a shadow copy;
   - **Exclude from interception** – allow the copying, no event will be created. To create a rule, fill in at least one of the following fields below: **File mask** or **File category**.

2. Select **Create a shadow copy** if you need to create a shadow copy in the event (this setting is available when you select **Create event** under **Action type**).
3. Specify the conditions for event creation:
    a. Select **File mask** and specify the mask to apply the rule to files that match it. You can use wildcard characters:
        - ? – one unknown character;
        - * – any number of characters.
    b. You can limit the application of the rule to a specific file category[4] by clicking **File category** and selecting the required category from the drop-down list.
    c. Specify the **File size** to limit the size of files subject to monitoring. Specify the range of values for the minimum and maximum file size and the unit of measurement. If both fields are filled in, the rule will apply only to files whose size is within the specified range.
    By default, the condition is enabled, and the file size is set to 0 to 10 MB.
    If the conditions are not enabled, the event will be generated without taking them into account.
4. After you have configured all the required parameters, click **Create**. The rule will always be in effect and will allow copying with the creation of an event with shadow copies. Subsequently, such events are sent for analysis to Traffic Monitor.

**Note:**

[3] In Traffic Monitor, the event without a shadow copy displays the file name and size.

[4] You can familiarize yourself with the file categories in the Resources Section, as well as in the knowledge base article Intercepted file extensions in Device Monitor (for rules with File category selection).
If you specify both a file mask and a category, both conditions must be met for the rule to be triggered.
On computers running Linux, file extension categories are not taken into account – the rule will apply to copying any files, regardless of the specified file categories.

### 11.3.4 Print Control Rule

The rule allows you to monitor the operations of document printing on local and network printers, including printing via terminal session.

**To configure the rule**:

1. Open the rule creation window and enter the rule name in the **Name** field.
2. In the **Interception channel** field, open the drop-down list and select **Control data transmission channels** -> **Print**.
3. If needed, deselect the **Create a shadow copy** option, then the event will be saved without a shadow copy. The option is enabled by default.
    For Agents on workstations running Windows, you can block printing based on the analysis results. For this, you need to configure the data protection policy on agents in Traffic Monitor.
4. When all parameters are configured, click **Create**. The rule will apply permanently.

**Important!**

In some cases, the Agent on Astra Linux OS, RED OS, and macOS may create several events when intercepting print events. This can happen, if the print event is transferred through several print servers and it was intercepted on these servers with big intervals.
If the print server and Device Monitor Agent are installed on Linux OS:

- the user who sent a file to print is not detected;
- the number of pages in a shadow copy is not determined;
- interception of documents sent to print via the terminal session is not performed;
- shadow copy format of intercepted print events can be changed. Herewith:
    - single-page EXCEL document is divided in fragments and each fragment is converted to JPEG format;
    - multiple-page PDF document is divided by pages, and each page is converted to JPEG format;

- WORD document is converted to a number of JPEG files, where each page is a separate JPEG file.

If Device Monitor Agent is installed on Linux OS:

- print events are not generated for printing to a file, and on Agents on Astra Linux OS print events are also not generated for the preinstalled printer.

If Device Monitor Agent is installed on RED OS:

- print job sent from some applications (for example, the Pluma editor) to a remote print server are not intercepted if printing is configured only for a local CUPS server (i.e. when `ServerName` directive is missing in `/etc/cups/client.conf`).

If Device Monitor Agent is installed on macOS:

- print interception may stop working, if while the Agent is working, the CUPS print system has been reconfigured so that copies of printed files are not created;
- events can be created in case if print was cancelled.

**Important!**

If, under the current rule, the printing process from a network printer takes longer than usual, add the printer's IP address to the exceptions list for network interception. Make sure the address is static.

### 11.3.5 External Device Control Rule

**Important!**

Starting from Device Monitor 7.15, the rule is available in Device Control (the "Devices" section of the Investigation Centre) and unavailable in Device Monitor. See *InfoWatch Device Control*. *User Guide*. Updating Device Monitor Server.

### 11.3.6 FTP Control Rule

The rule allows you to control data transfer through FTP/FTPS protocol, including:

- allow or prohibit the transfer of information via the FTP protocol;
- intercept traffic via the FTP protocol with the creation of shadow copies;
- restrict access to FTP resources.

**Important!**

On computers running RED OS and Alt OS, copying a file to an FTP server is not intercepted if the connection was established by entering the server name in the search bar of the OS file manager.

**To configure the rule**:

1. Open the rule creation window and enter the rule name in the **Name** field.
2. In the **Interception channel** field, open the drop-down list and select **Control data transmission channels -> FTP(S)**.
3. Under **Action**, select the System's response during data exchange:
   - **Create events for FTP write cases** – writing to the specified FTP resources will be allowed, but an event will be created in this case;
   - **Exclude operations on specified FTP servers** – operations on the specified servers will be excluded from interception, meaning they will be allowed;
   - **Disable writing to FTP**;
   - **Deny FTP addresses visiting.**
4. Select **Create a shadow copy** if you need to create a shadow copy in the event (this setting is available when you select **Create events for FTP write cases** in the **Action** field).

   **Note:**

   In Traffic Monitor, an event without a shadow copy displays the name and the size of the file.
5. Fill in the **FTP address** field. Hover the mouse over **?** (question mark) to see the rules for filling it in. If no addresses are specified, the rule will be applied to all addresses.

   **Note:**

   Take the following into account:
   - allow rules for specific addresses take precedence over deny rules;

- allow rules without specifying addresses are less prioritized than any deny rules;
- if only the server address is specified as the address for a deny rule, access to all folders on that server will be denied;
- if the server address and subfolders are specified as the address for a deny rule, transitions between folders on that server will be allowed, but access to copying files will be denied only for the specified folder.

6. If required, specify the file size limit:
   a. Select **File size**.
   b. Indicate the range of values and the units of measurement.
   If both fields are filled in, the rule will apply only to files whose size falls within the specified range.
   By default, the condition is enabled and the file size is set to be between 0 and 10 MB.
   This parameter is available only when creating events with shadow copies of the sent files and when creating an event without shadow copies for write cases if there is less free space left on the computer than is defined by the policy.
7. When all parameters are configured, click **Create**. The rule applies permanently.

### 11.3.7 HTTP(S) Control Rule

The rule allows you to control data transfer through HTTP and HTTPS protocols.

**To configure the rule:**

1. Open the rule creation window and enter the rule name in the **Name** field.
2. In the **Interception channel** field, open the drop-down list and select **Control data transmission channels** –> **HTTP(S)**.
3. In the **Action** field, select:
   - *Create events for resources from lists;*
   - *Do not create events for resources from lists;*
   - *Do not create events for internal resources* – in this case, add the corporate network segments to exclusions. See more in Corporate Networks*;*
   - *Create events for all resources.*
4. In case you select one of the actions for resources from the lists, specify one or more previously created lists. See more in Creating resource list.
5. Specify the request size, for which a shadow copy will be created. To do this, activate the:
   a. **Minimum** request size, specify the value and the units of measurement. If the setting is configured, shadow copying will be performed only for requests whose size is greater than or equal to the specified value. The default value: 40 B.
   b. **Maximum** request size, specify the value and the units of measurement. If the setting is configured, shadow copying will be performed only for requests whose size is less than or equal to the specified value. The default value: 40 MB.
6. When all parameters are configured, click **Create**. The rule will apply permanently.

**Important!**

Interception of network traffic from the HTTPS proxy server is not supported.

**Important!**

On computers running Linux:

- connections via IPv6 protocol are not intercepted;
- requests related to webmail are intercepted similar to common HTTP requests.

**Important!**

When working with Device Monitor server running Linux, Device Monitor Agent running Windows will transfer incorrect data about the adaptors' presence in the corporate network to the server. The reason is that to correctly determine the location within the corporate network, the network segments should be correctly specified, including gateway addresses.

**Important!**

**When migrating from a Device Monitor server running Windows to a Linux OS**
If only one HTTP rule was configured on Device Monitor running Windows, which excluded the interception of requests to internal resources, then after switching to a Linux OS, this rule will mean that events will be generated for all resources except internal ones. For example: in Device Monitor running Windows, there was a rule stating *Do not create events for internal resources.* After migrating to Linux OS, the rule will mean *Create events only for external resources.*
In Device Monitor running Windows, there is a rule *Create events for requests transmitted via some channels*, with the request size specified. After migration to Linux OS, the rule will mean *Create events for all resources*, with the same request size.

### 11.3.8 Mail Control Rule

The mail control rule allows you to intercept email receipt via POP3, IMAP, and email sending via SMTP, HTTPS, as well as to prohibit sending web mail via HTTPS.

**Important!**

Message interception via the HTTPS protocol is supported only when using web mail services: Gmail, Yandex, Mail.ru, Yahoo, Rambler, Outlook.com, VK+ (VK WorkSpace).
Mail interception via the HTTPs protocol is not supported via Outlook Web App when using an MS Exchange server.

**To configure the rule:**

1. Open the rule creation window and enter the rule name in the **Name** field.
2. In the **Interception channel** field, open the drop-down list and select **Control data transmission channels –> E-mail**.
3. Select which actions with the email should be available to the user:
   - *Allow e-mails using*
   - *Deny e-mails using*
4. In the **Protocol** field, select the channel that should be controlled by the rule:
   - *All protocols*
   - *SMTP* – for outgoing mail only
   - *POP3* – for incoming mail only
   - *IMAP* – for incoming mail only
   - *HTTPS* – only for outgoing mail from the following services: Gmail, Yandex, Mail.ru, Yahoo, Rambler, Outlook.com, VK+ (VK WorkSpace)

     **Note:**

     To intercept VK+ mail, you need to specify the hosts in the menu **Settings > Device Monitor > Interception channels > Hosts for VK+**.
   - MAPI/Outlook – for incoming and outgoing mail.
5. Select if you need to create events with a shadow copy for:
   - *Incoming e-mails*, if *POP3* or *IMAP* is selected in the **Protocol** field;
   - *Outgoing e-mails*, if *SMTP* or *HTTPS* is selected in the **Protocol** field;
   - both values, if *All protocols* or *MAPI/Outlook* is selected in the **Protocol** field.

     **Important!**

     If the rule specifies **Allow e-mails using**, a shadow copy must be created for at least one of the email directions: *Incoming e-mails* or *Outgoing emails*.
6. If required, configure the **Maximum e-mail size**. To do this, enter its value and the units of measurement. In this case, shadow copying will be performed only for emails whose size is less than or equal to the specified value.
   By default, the condition is enabled and the maximum file size is set to 40 MB.
   To create an event with shadow copying for emails of any size, deselect the box.
7. After you have defined all the necessary parameters, click **Create**. The rule will apply permanently.

**Applying of Traffic Monitor policies**

- On workstations running Linux, only outgoing traffic (SMTP protocol and webmail) is blocked. At the same time, files transmitted via web mail are not analyzed.
- The system unpacks the archives and applies Traffic Monitor policies to them if:
    - an archive in the 7Z, ZIP, TAR.GZ, AR, RAR, or ISO format was intercepted on the Agent running on Windows;
    - an archive in the 7Z, ZIP, AR, or TAR.GZ format, transmitted via the SMTP protocol as an email attachment, was intercepted on the Agent running Alt OS, RED OS, or Astra Linux 1.7.

**Interception events**

Features of creating events for intercepting email messages:

- The set of attributes for a webmail interception event depends on the specific implementation details of the particular web application.
- In the shadow copy of the web mail event, only the data that was in the intercepted traffic will be present. For example, the events will contain all the attributes of the email, except for attachments, in cases where:
    - the employee sends the email from the drafts after the event has already been sent to Traffic Monitor, following the timeout from the last time the employee was active with the email;
    - the employee sends an email from drafts created on another workstation;
    - the employee forwards a previously sent email.

### 11.3.9 Cloud Storage Control Rule

The rule allows you to control the sending and receiving of any data, as well as access to the web clients of the following cloud storage services:

- Dropbox
- Evernote
- Google Drive
- OneDrive
- SugarSync
- Yandex Disk

**Important!**

If access to the Google Drive storage is restricted, other Google services that use the docs.google.com host may function incorrectly or be unavailable. For example, Google Docs, Google Tabs, Google Slides, and so on.

**To configure the rule**:

1. Open the rule creation window and enter the rule name in the **Name** field.
2. In the **Interception channel** field, open the drop-down list and select **Control data transmission channels** –> **Cloud storage**.
3. In the **Action** field, select the action to apply. For all cloud storages, the following options are available:
    - **Deny access**
    - **Allow download only**
    - **Intercept file upload**
4. Select one or several file storages to monitor.
5. While intercepting file upload, shadow copies will be created. In this case, you can additionally specify the:
    - **Min. file size to create an event**, by setting a value and a measurement unit. If this field is filled in, the rule will create an event only for files whose size is greater than or equal to the specified value.
      The default value is 1 KB.
    - **Max. shadow copy size**, by setting a value and a measurement unit. If this field is filled in, the shadow copy will be created only for files whose size is less than or equal to the specified value.

The default value is 10 MB.

6. When all parameters are configured, click **Create**. The rule will apply permanently.

### 11.3.10 Network Traffic Proxying Rule

The rule of network traffic proxying allows you to configure applications to be excluded from interception.

> **Important!**
>
> Network traffic proxying works only on computers running Windows.
> In case if a running application has been excluded from network interception using this rule, removing it from the rule later does not cancel the exclusion. To start interception, restart the application.

**To configure the rule:**

1. Open the rule creation window and enter the rule name in the **Name** field.
2. In the **Interception channel** field, open the drop-down list and select **Control data transmission channels** –> **Proxying network traffic**.
3. In the **Exclude applications from interception** area, select lists in the **Select application lists** field (to learn about creating lists, see Creating and Editing Application Lists). You can use the search bar to select the lists.
4. When all parameters are configured, click **Create**. The rule will apply permanently.

### 11.3.11 Clipboard Control Rule

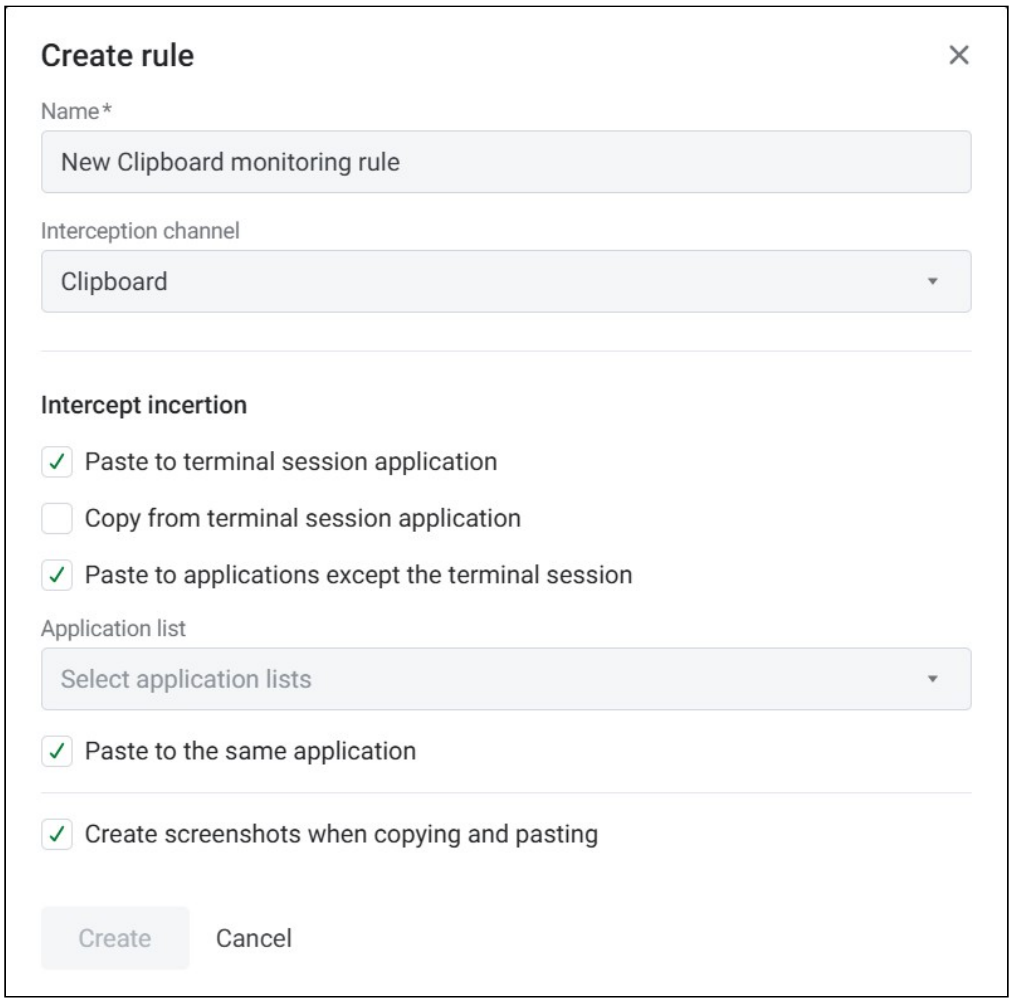
The rule allows you to control access of employees to the clipboard.

> **Important!**
>
> The rule applies to computers running Windows or Linux.
> Device Monitor intercepts only text data with this rule.

**To configure the rule**:

1. Open the rule creation window and enter the rule name in the **Name** field.
2. In the **Interception channel field**, open the drop-down list and select **Control data transmission channels** -> **Clipboard**.
3. In the **Intercept insertion** area, specify when the rule should work. At least one of the options should be selected:
   - **Paste to terminal session application**[1]. 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.
   - **Copy from terminal session application**[1]. 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.
   - **Paste to applications except the terminal session**. Select this option, if the rule should be triggered only when data is pasted to specified applications. The rule also applies to data copied from a terminal session.
     To use the option, select the lists in the **Application list** field (to learn about creating application lists, see Creating and Editing Application Lists). To select the lists, you can use

the search bar.




- If you need the rule to be triggered when data is pasted to the application from which it has been copied, select **Paste to the same application**[2].
  Interception within a single application is supported only if the application uses the system clipboard mechanisms.
- To create screenshots when the rule is triggered, select **Create screenshots when copying and pasting**[3].

4. When all parameters are configured, click **Create**. The rule will apply permanently.

**Important!**

[1] Application of a terminal session is a client or system application from server software providing terminal access:

- client applications:
  - Microsoft RDS and the following client software (for connecting to a terminal server): Remote Desktop Connection (mstsc.exe), SysInternals RDCMan, MobaXterm;
  - Remote Desktop Connection Manager;
  - Citrix Receiver.
- system applications are supported according to the version of OS or Citrix.

On workstations running Linux, only interception of pasting into applications other than terminal sessions is supported. The **Paste to the same application** option is not available. To configure the rule for Linux, select the **Paste to applications except the terminal session** option and specify the Linux list of applications.

On a Linux-based workstation, when there is a connection to a terminal session using xRDP, the IP address of the remote computer may be recorded in the **Network address of a terminal Agent** event attribute.

[2] Pasting within the same application is not supported on workstations running Astra Linux.

[3] In this rule, screenshot generation is supported only on workstations running Windows.

**Note:**

In case the System intercepts a text in Latin characters with length less than 10 symbols, or a text in Cyrillic characters with length less than 5 symbols, the text of this event will not be displayed in Traffic Monitor.

### 11.3.12 VK Messenger Control Rule

The rule allows you to control chat messaging and any types of outgoing files in the web version of VK (VKontakte) instant messaging system. Herewith, the whole correspondence history will be intercepted on a corporate computer, including the period before the Device Monitor Agent installation.

**Important!**

The interception of the following is not supported:

- files, downloaded from a computer without Device Monitor Agent installed;
- posts on walls;
- messages with geolocation;
- edited messages history.

**To create and configure the rule**:

1. Open the rule creation window and enter the rule name in the **Name** field.
2. In the **Interception channel** field, open the drop-down list and select **Messengers** –> **VK**.
3. If you want to create shadow copies of transferred files and send them to Traffic Monitor besides the event, select the **Create shadow copy of outgoing files** checkbox. In this case, you can also define additional parameters for shadow copies:
   a. **Minimum file size**, specify a value and a measurement unit. When enabled, shadow copies will be created only for files of larger or equal size.
   b. **Maximum file size**, specify a value and a measurement unit. When enabled, shadow copies will be created only for files of smaller or equal size.
   These fields are taken into account only when creating a shadow copy: if the file size falls within the specified range, the event will contain a shadow copy. Otherwise, the event will be created without a copy.

   **Note:**

   To specify conditions of event generation, go to **Settings > Interception channels** (see Interception Channels).
4. When all parameters are configured, click **Create**. The rule will apply permanently.

### 11.3.13 Telegram Messenger Control Rule

The rule allows you to control new, forwarded, or edited messages in chat, including group chat, outgoing files and audio messages in desktop or web version of Telegram. Herewith, the whole correspondence history will be intercepted on a corporate computer, including the period before the Device Monitor Agent installation.

**To create and configure the rule**:

1. Open the rule creation window and enter the rule name in the **Name** field.
2. In the **Interception channel** field, open the drop-down list and select **Messengers** –> **Telegram**.
3. If you want to create shadow copies of transferred files and send them to Traffic Monitor besides the event, select the **Create shadow copy of outgoing files** checkbox. In this case, you can also specify additional parameters for shadow copies:
   a. **Minimum file size**, specify a value and a measurement unit. When enabled, shadow copies will be created only for files of larger or equal size.
   b. **Maximum file size**, specify a value and a measurement unit. When enabled, shadow copies will be created only for files of smaller or equal size.

These fields are taken into account only when creating a shadow copy: if the file size falls within the specified range, the event will contain a shadow copy. Otherwise, the event will be created without a copy.

> **Note:**
>
> To specify conditions of event generation, go to **Settings > Interception channels** (see Interception Channels).

4. When all parameters are configured, click **Create**. The rule will apply permanently.

**Important!**

Use prohibition is not supported.
Interception is not supported for:

- stickers
- GIF-animation
- contacts
- geolocation
- channels
- audio calls
- surveys
- text attached as a link

For a group chat:

- at the moment of message sending in chat, an event contains only the chat identifier and its name; the chat participants are unknown, but may become available if the monitored employee has viewed the chat participants list;
- a participant removal can be detected only if the monitored employee removed them. In events of this chat received from other employees, the chat participants list will stay the same.

For Telegram on computers running **Linux**:

- the rule allows you to intercept the following Telegram versions:
  - desktop version, even when the executable module (Telegram.exe) is renamed;
  - web versions: A, K, Z, and obsolete (Legacy).
- intercepting web versions has a number of specific features:
  - the System defines different versions as different applications;
  - there is a delay of interception start – up to 50 seconds from the authentication time;
  - supported browsers:
    - Google Chrome;
    - Mozilla Firefox;
    - Yandex Browser.
- the system call `ptrace()` needs to be enabled for interception;
- Flatpak-application interception is not supported.

For Telegram on computers running **Windows**:

- the rule allows you to intercept the following Telegram versions:
  - desktop version – application from the official Telegram website (desktop.telegram.org) or Microsoft Store. The interception is supported even when the executable module (Telegram.exe) is renamed;
  - web versions: A, K, Z, and obsolete (Legacy).
- intercepting web versions has a number of specific features:
  - the System defines different versions as different applications;
  - there is a delay of interception start – up to 50 seconds from the authentication time;
  - supported browsers:

- Google Chrome;
- Microsoft Edge;
- Mozilla Firefox;
- Opera;
- Yandex Browser.

### 11.3.14 Yandex Messenger Control Rule

The rule allows you to control messaging in web and desktop version, and outgoing files in the web version of Yandex Messenger. The rule allows to intercept new, forwarded. and edited chat messages (including group chats). The System intercepts the correspondence history on a corporate computer, starting from the Device Monitor Agent installation and the rule creation.

**Important!**

Yandex web version interception is supported in the following browsers:

- Google Chrome
- Microsoft Edge
- Mozilla Firefox
- Opera
- Yandex browser

Prohibition of audio messages use and interception are not supported.
The group call events do not contain the information about the participants (recipients) who did not sent messages in the group chat.
In case if a one-on-one call is changed to a group call, then no event will be created either for individual or group calls.
In case of outgoing file interception in a group chat, the event will not contain the chat name.
The events for edited messages of group chats may not contain the chat name.
When sending messages to a group chat, the event will contain the chat identifier, and it also may contain the chat name.
Interception of Yandex Messenger desktop version is not supported on Agents running Linux.

**To create and configure the rule**:

1. Open the rule creation window and enter the rule name in the **Name** field.
2. In the **Interception channel** field, open the drop-down list and select **Messengers** –> **Yandex messenger**.
3. If you want to create shadow copies of transferred files and send them to Traffic Monitor besides the event, select the **Create shadow copy of outgoing files** checkbox. In this case, you can also specify additional parameters for shadow copies:
   a. **Minimum file size**, specify a value and a measurement unit. When enabled, shadow copies will be created only for files of larger or equal size.
   b. **Maximum file size**, specify a value and a measurement unit. When enabled, shadow copies will be created only for files of smaller or equal size.
   These fields are considered only when creating a shadow copy: if the file size falls within the specified range, the event will contain a shadow copy. Otherwise, the event will be created without a copy.

   **Note:**

   To specify conditions of event generation, go to **Settings > Interception channels** (see Interception Channels).
4. When all parameters are configured, click **Create**. The rule will apply permanently.

### 11.3.15 WhatsApp Messenger Control Rule

The rule allows you to control messaging and outgoing files in web and desktop version of the WhatsApp messenger. The rule allows you to intercept new, forwarded, and edited chat messages (including group chats). The System intercepts the correspondence history on a corporate computer, starting from the Device Monitor Agent installation and the rule creation.

**Important!**

WhatsApp web version interception is supported in the following browsers:

- Google Chrome
- Microsoft Edge
- Mozilla Firefox
- Opera
- Yandex Browser

Prohibition of use is not supported.
Interception is not supported for:

- audio- and video calls;
- contact meta information (nickname);
- files transferred between chats;
- text attached as a link.

Interception is not supported in case if an employee logs in to the WhatsApp web version:

- when the Agent has not been installed;
- when the Agent has been disabled.

In this case, after starting a new version of the Agent, you need to clear you browser cash.
If the Agent is activated while WhatsApp is already running, it may terminate WhatsApp processes so that the interception can be integrated into WhatsApp when it is launched again. Interception will not be performed until WhatsApp is restarted.
When the analysis server (IWProxy process) starts, all detected WhatsApp processes may be forcibly terminated.
When photos and video files are intercepted, the event may contain a preview of the file rather than the original file. In this case, the file name will have the format `"Embedded <Content type: image/video> <Time of data sending in milliseconds>".`
If multiple messages with the same text and sender are intercepted within approximately 3 second gap, a single event will be generated for them.
When sending messages to a group WhatsApp chat, the event will contain the chat identifier and the chat name.
The events for edited messages in group chats may not contain the chat name.
Files interception is not supported on Agents running Linux.

**To create and configure the rule**:

1. Open the rule creation window and enter the rule name in the **Name** field.
2. In the **Interception channel** field, open the drop-down list and select **Messengers > WhatsApp**.
3. If you want to transfer shadow copies of outgoing files to Traffic Monitor besides the event, select the **Create shadow copy of outgoing files** checkbox. In this case, you can also define additional parameters for shadow copies:
   a. **Minimum file size**, specify a value and a measurement unit. When enabled, shadow copies will be created only for files of larger or equal size.
   b. **Maximum file size**, specify a value and a measurement unit. When enabled, shadow copies will be created only for files of smaller or equal size.
   These fields are taken into account only when creating a shadow copy: if the file size falls within the specified range, the event will contain a shadow copy. Otherwise, the event will be created without a copy.

   **Note:**

   To specify conditions of event generation, go to **Settings > Interception channels** (see Interception Channels).
4. When all parameters are configured, click **Create**. The rule will apply permanently.

### 11.3.16 MAX Messenger Control Rule

The rule allows to control messaging and file exchange in the desktop and web version of the MAX messenger.

**Important!**

Interception is not supported for:

- edited messages;
- reply messages (i.e. attached to initial message);
- audio messages;
- incoming files;
- files forwarded between chats;
- messages history;
- surveys.

If there are no incoming messages after outgoing ones, the current messenger user is displayed as the recipient in the event.
If an employee uploads a file but does not send it, the System generates a file upload attempt event when the messenger is closed. The current messenger user is specified as both the sender and the recipient.
If an employee attempts to upload a file that is not supported by the messenger, the System generates an event indicating an attempt to upload the file with an incomplete shadow copy when the messenger is closed. The current messenger user is specified as both the sender and the recipient.

**To create and configure the rule:**

1. Open the rule creation window and enter the rule name in the **Name** field.
2. In the **Interception channel** field, open the drop-down list and select **Messengers** –> **MAX**.
3. If you want to create shadow copies of transferred files and send them to Traffic Monitor besides the event, select the **Create shadow copy of outgoing files** checkbox. In this case, you can also define additional parameters for shadow copies:
   a. **Minimum file size**, specify a value and a measurement unit. When enabled, shadow copies will be created only for files of larger or equal size.
   b. **Maximum file size**, specify a value and a measurement unit. When enabled, shadow copies will be created only for files of smaller or equal size.
   These fields are taken into account only when creating a shadow copy: if the file size falls within the specified range, the event will contain a shadow copy. Otherwise, the event will be created without a copy.

   > **Note:**
   >
   > To specify conditions of event generation, go to **Settings > Interception channels** (see Interception Channels).

4. When all parameters are configured, click **Create**. The rule will apply permanently.

### 11.3.17 XMPP Protocol Control Rule

The rule allows you to control incoming and outgoing messages exchange via the **XMPP** protocol.

**To create and configure the rule**:

1. Open the rule creation window and enter the rule name in the **Name** field.
2. In the **Interception channel** field, open the drop-down list and select **Messenger > XMPP**.
3. In the **Action** field, **Intercept messages** is selected by default. In case you want to prohibit messages exchange via the XMPP protocol on a workstation with the Device Monitor Agent, select **Deny usage**.

   > **Note:**
   >
   > To specify conditions of event generation, go to **Settings > Interception channels** (see Interception Channels).

4. When all parameters are configured, click **Create**. The rule will apply permanently.

### 11.3.18 Screenshot Creation Control Rule

The rule allows you to prohibit screenshot creation by employees.

**To configure the rule**:

1. Open the rule creation window and enter the rule name in the **Name** field.
2. In the **Interception channel** field, open the drop-down list and select **Usage control > Disable screenshots**.
3. In the **Prevent employee from taking screenshot** block, select when the rule should be triggered. To create the rule, one of the options needs to be selected:

- **Always**;
- **If applications are running**. In case you select this option, the rule will work for the specified applications.

4. If you have selected the trigger when applications are running, specify these applications in the **Application lists** field.

> **Note:**
>
> Only Windows applications can be added.

5. When all parameters are configured, click **Create**. The rule will apply permanently.

> **Note:**
>
> Screenshot prohibition using PrtScr button or a combination of PrtScr+Alt buttons is supported.

### 11.3.19 Screen Monitoring Rule

The rule allows you to create screenshots in PNG format when the application active window is switched. The screenshots are created for all monitors connected to unblocked monitored computer.

> **Note:**
>
> The rule applies to computers running Windows and Linux.
> On a Linux workstation, when there is a connection to a terminal session using xRDP, the IP address of the remote computer may be recorded in the **Network address of terminal client** event attribute.

> **Note:**
>
> Set up the Employee Activity Monitoring Rule to send events with screenshots to InfoWatch Activity Monitor.

**To configure the rule**:

1. Open the rule creation window and enter the rule name in the **Name** field.
2. In the **Interception channel** field, open the drop-down list and select **Monitoring user activity > Automatic screenshots**.
3. Specify when the rule should work. Possible values:
   - **Create screenshots for any applications or resources**
   - **Create screenshots for applications or resources from the list**
   - **Do not create screenshots for applications or resources from the list**
4. If you select the action where the application or resources lists are taken into account, select them in the fields below.
   To learn more about lists creation, see "Resources" Section.

> **Important!**
>
> 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 browsers is used:
> - Chrome
> - Yandex Browser
> - Mozilla Firefox
> - Edge (Chromium)

5. Specify when the screenshots should be created, or select both conditions:
   - **When changing active window** – applies to all applications, but browser tab switching is not taken into account;
   - **Every n seconds** – time between screenshots creation.

> **Important!**
>
> You can also specify the rule's work depending on activity on monitored computers. For this, in the interception channels settings, select the **Do not make screenshot in case mouse/keyboard are inactive more than**... parameter (see Interception Channels).
> On workstations running Linux, the System registers changing a browser tab only for Yandex Browser, Edge (Chromium) and Mozilla Firefox.

On workstations running Astra Linux 1.7 and 1.8, the System does not identify opening a new document in office multi-window applications, such as LibreOffice.

6. When all parameters are configured, click **Create**. The rule will apply permanently.

**Important!**

Screenshot of the entire screen is created during 5 seconds after the active window/tab is changed. If changing the active window happens faster than one time every 5 seconds, then a screenshot will not be created.

**Note:**

The configuration and application of the screenshot monitoring rule and keyboard input monitoring rule are performed independently from each other.

**Note:**

To learn more about how the System prioritizes the rules when making screenshots, see Defining priorities of rules when making screenshots according to ScreenShot Monitor rule.

## 11.3.20 Keyboard Input Monitoring Rule

The rule allows you to intercept text input from the keyboard and keyboard shortcuts in the window of any application on workstations and generate events when the active window changes. Subsequently, events containing shadow copies of the data entered from the keyboard will be sent to Traffic Monitor for processing and analysis.

**Note:**

The rule is available for workstations running Windows and Linux.
On a Linux workstation, when there is a connection to a terminal session using xRDP, the IP address of the remote computer may be recorded in the **Network address of terminal client** event attribute.

By default, text input and/or keyboard shortcuts are intercepted on workstations:

- when the active window is changed;
- after 20 seconds from the end of input;
- when 100 characters are accumulated in a single word or 200 characters are entered from the keyboard;
- when pressing Enter / Ctrl+Enter / Shift+Enter.

**To create the rule:**

1. Open the rule creation window and enter the rule name in the **Name** field.
2. In the **Interception channel** field, open the drop-down list and select **Monitoring user activity > Keyboard text input**.
3. Choose one of the rule's actions:
   - **Intercept text input in all applications and resources**;
   - **Intercept text input for applications and resources in the list** – Device Monitor will create an event when text is entered in the window of the active applications from the list;
   - **Do not intercept text input for applications and resources in the list** – Device Monitor will **not** create an event when text is entered in the window of the active applications from the list.

     **Note:**

     Only lists for Windows are supported.
4. If you select an action that takes into account the lists of applications and resources, specify them in the fields that appear.
   To learn more about creating lists of applications and resources, see Creating and Editing Application Lists, Creating and Editing Resource Lists.
5. If required, enable the option **Make screenshot when creating an event**. Configuring and applying the keyboard text input monitoring rule and the screen monitoring rule are independent of each other.
6. Click **Create**.

To configure the conditions for event generation, go to **Settings > Interception channels** (see Interception Channels).

**Important!**

- Keyboard text interception works correctly for Russian and English. Adding other languages requires restarting the workstation.
- For the Agent on a workstation running Linux, changing a tab in the browser is ignored. **Example:** an application is open, and text input from the keyboard is being intercepted there. The employee switches between tabs and enters text into them. The system will generate one event for text input in the application, not for each tab.
- For the Agent on a workstation running **Alt 11** (with the Wayland graphical shell) or **Astra Linux**, if the user holds down a character while entering text, the System intercepts that character in a single instance.
  **Example:** the text "*exaaample*", in which the repeated character was entered not by successive keystrokes but by holding down the key, will be intercepted as "*example*".
- For the Agent on a workstation running **Astra Linux**, the System does not intercept text entered into the standard text manager if the text starts with a slash, such as "*/sample/text*".
- For the Agent on a workstation running **Alt 11** (with the Wayland graphical shell), after updating to version 7.21 or later, interception is available only after restarting the user session.

### 11.3.21 Employee Activity Monitoring Rule

The rule allows you to collect statistics on an employee's activity on a monitored computer, generate events, and send them to Activity Monitor.

**Note:**

The rule is available for workstations running Windows and Linux.

**To configure the rule:**

1. Open the rule creation window and enter the rule name in the **Name** field.
2. In the **Interception channel** field, open the drop-down list and select **Monitoring user activity > Employee activity**.
3. In the **Types of statistics** section, select which user actions need to be monitored (see the list of monitored actions for each type below):
   - **Control activity**
   - **Control actions with files**
   - **Control printing**
4. If you do not need to collect statistical data when monitoring any user actions, select **Disable collection**. Events generated in Device Monitor will not be sent to the Platform.
5. Click **Create**. The rule will apply permanently.

To make sure that statistical data is successfully sent to Activity Monitor, make sure that a connection to the Platform is established (see Servers – Connecting to the Platform).

**Note:**

If you want certain events (such as screenshot events according to the Screen monitoring rule) to be sent to the Platform even if statistics collection is disabled, set the value of the `SEND_EVENT_TO_PLATFORM_WITH_CHECK` field in the Settings table of the database to `False`. By default, this field is set to `True`.

On a workstation running Linux, when connecting to a terminal session using xRDP, the IP address of the remote computer may be written in the **Network address of terminal client** event attribute.

#### Monitoring actions

Monitoring activity

The System monitors the following user actions:

- session logon (local, remote);

- session logoff (local, remote);
- locking a session (local, remote);
- unlocking a session (local, remote);
- launching an application;
- stopping an application;
- getting and losing focus on the active window;
- switching between applications;
- switching between browser tabs. The following browsers are supported:
  - Chrome
  - Yandex.Browser
  - Mozilla Firefox
  - Edge (Chromium)
- performing search queries. The following search engines are supported:
  - Google
  - Yandex
- using a mouse and a keyboard.

**Note:**

- 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.
- The events of getting/losing focus for UWP applications (Universal Windows Platform) may not be created.
- For events with websites and web search, the *site* attribute may have the "about:blank" value, if the URL does not correspond to the site domain or IP address.
- If Screenshot Creation Control 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 statistics on using a mouse and a 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 a user keeps a button pressed and then releases, the Agent generates many events of pressing the button and one event of releasing it.

**Important!**

On workstations running Linux, the following user actions in the system are monitored:

- local session logon;
- local session logoff;
- local session unlocking;
- local session locking;
- getting the focus – active application window;
- losing the focus – active application window;
- using the keyboard;
- browser tab gets focus (for the following browsers: Edge (Chromium), Yandex Browser and Mozilla Firefox);
- performing search queries (for the following browsers: Edge (Chromium) and Mozilla Firefox).

For the Agent on a workstation running **Alt 11** (with the Wayland graphical shell) after upgrading to version 7.21 or later, intercepting application window switching is available only after restarting the user session.

**Note:**

On workstations running RED OS:

- 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.
- If a website was added to favorites, then an event of switching tabs is created.
- If URL address was changed, then a number of events of switching the browser tab may be created.
- The event of *Exiting the session (local)* 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.

Monitoring actions with files

**Important!**

Monitoring actions with files is supported on Agents running Windows OS only.

The system monitors the following user actions:

- creating a file;
- opening a file;
- renaming a file;
- moving a file/folder;
- copying a file/folder;
- deleting a file/folder;
- moving a file/folder to the trash;
- restoring a file/folder from the trash;
- deleting a file/folder from the trash.

**Note:**

- If the operation of copying/deleting/moving file was initiated and then cancelled, the event may still be created.
- If the System cannot determine the original file name when deleting a file from the trash, the event will indicate the file name displayed in the trash. The original file name is the file name before it was moved to the trash (if the OS changes it during the move).
- 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.
- The file size data is extracted from the file object context. If the System has not received this data, the file size value will be set to 0.

Statistics on file operations are collected for the following sources:

- computer;
- removable devices;
- network resources;
- terminal session.

**Important!**

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

Monitoring printing

**Important!**

Monitoring printing is supported on Agents running Windows OS only.

The system controls the sending of files to print for the following types of printers:

- local;
- network;

- terminal.

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.

## 11.3.22 Audio Environment Monitoring Rule

The rule allows you to monitor an employee's actions by controlling the sound environment of the employee's workstation, generate events, and send them to Activity Monitor.
In the rule, you can configure the:

- **Sound source** – you can choose one or two types of sound source for the environment: microphone and/or speakers;
- **Intercept from resource list** – recording the sound environment when using the selected resources;
- **Intercept session activity** – recording of the surrounding sound throughout the entire work session, from the moment the user logs in to the moment they log out. If the workstation is locked, the recording of the surrounding sound is not interrupted.

> **Important!**
>
> To generate and send audio environment recording events to Activity Monitor, you also need to configure the Employee Activity Monitoring Rule.

> **Note:**
>
> The rule applies to agents running Windows.

**To configure the rule:**

1. Open the rule creation window and enter the rule name in the **Name** field.
2. In the **Interception channel** field, open the drop-down list and select **Monitoring user activity > Sound environment**.
3. Choose which type of source to use for recording the surrounding sound:
   - *Microphone*
     and/or
   - *Speakers*
     If several devices of the same type are connected to the workstation, the one with the highest audio signal amplitude will be selected for recording.
4. If necessary, add resources for interception to the **Resource lists** field.
   You can adjust the recording duration in the settings. See Interception Channels.
5. If you want to enable session activity interception, select the option **Record sound environment when logging in**.

   > **Important!**
   >
   > Recording the sound environment on several dozen workstations can significantly increase the load on the system.
6. After you have defined all the necessary parameters, click **Create**. The rule will apply permanently.

You can also adjust the recording duration and exclude the periods of silence from the recording. To learn more, see Interception Channels.

> **Note:**
>
> - the same record can relate to several events simultaneously. If a user sequentially visits several different resources for which a rule is triggered, the record is kept continuously, but separate events are created for the different resources;
> - during the conference, the recording made not for the voice, but for the sounds around the workstation;

- if something happened during the rule's activation that prevents sound recording (for example, the microphone turned off), the event may contain an audio recording without sound (you'll hear silence when playing it);
- the check for the correspondence between the visited resource and the resource from the list is performed only if the user is working in the following browsers:
  - Chrome
  - Yandex Browser
  - Mozilla Firefox
  - Edge (Chromium)
  - Opera
- when logging out of the system via the *Start* menu, the audio environment interception process is forcibly terminated by the operating system. As a result, the last fragment of the audio data cannot be intercepted. The duration of this fragment is no more than 1 minute;
- the sound environment recording is performed when the session is locked;
- for agents running Windows 11 and later, the fact that audio is being recorded will be hidden from the user. The microphone icon will be hidden even if the microphone is already in use by another application;
- other applications cannot capture the microphone in exclusive mode;
- if the user uses a Bluetooth headset to play audio, intercepting the sound via the headset's microphone may cause the playback to stop. Further audio playback during the interception will be available in lower quality via the Hands-Free Profile (HFP) or Headset Profile (HSP).

### 11.3.23 Screen Video Recording Rule

The rule allows you to track the following employee actions by recording the screen video of the workstation:

- logging in to the website specified in the rule;
- use of the application specified in the rule;
- use of the clipboard in the application specified in the rule;
- text input in the application specified in the rule.

When the rule is triggered, the System generates events and sends them to Activity Monitor.

**Important!**

To generate and send video recording events to Activity Monitor, you also need to configure the Employee Activity Monitoring Rule.

**Note:**

The rule applies to computers running Windows.
The rule does not work on an agent running Windows 7.

**To configure the rule:**

1. Open the rule creation window and enter the rule name in the **Name** field.
2. In the **Interception channel** field, open the drop-down list and select **Monitoring user activity > Screen record video**.
3. In the **Resource lists** field, select the resources that should trigger the rule (see Creating a Resource List).
4. Next, select the conditions for the rule to be triggered in the application:
   - **Use application**
   - **Text input**
   - **Use clipboard**
5. In the **Application lists** field, select the applications that should trigger the rule when they're used (see Creating and Editing Application Lists).
6. After you have defined all the required parameters, click **Create**. The rule will apply permanently.

You can adjust the recording duration in the settings. See Interception Channels.

**Note:**

- due to the specific features of the video capture technology used in the agent, the duration of the screen recording may be shorter than the specified time;
- the video capture start offset may not correspond to the duration of the previous video;
- video recording is performed from all available screens;
- the same video recording can relate to multiple events simultaneously. If a user sequentially visits several different resources for which a rule is triggered, the recording is continuous, but separate events are created for the different resources;
- when the rule is triggered, only video recording is performed. Recording of the workstation's sound environment is not available;
- video recording begins when the user logs in to the session or unlocks the screen, and continues until the user logs out the session or locks the screen;
- when intercepting using the clipboard, recording is triggered by any request from the application to the clipboard. That is, if the application can independently write information to the clipboard or retrieve it from it, this will be recognized as a user action, and recording will begin;
- when entering text in the application, the recording starts with the first character and continues until the focus is moved out of the application or until the maximum recording time is reached;
- **If you have selected the application interception with the "Text input" option**

| the record is performed when pressing in the input field: | the record is not performed when pressing in the input field: |
|---|---|
| • combinations of the Ctrl key and letters, for example, Ctrl+a, Ctrl+t, and so on;<br>• function keys, such as Esc, Backspace, Enter, Tab, and so on;<br>• keys without entering anything into any field. | • navigation keys, such as PgUp, PgDown, Home, and so on;<br>• F1-F12 keys;<br>• Delete key;<br>• key combinations that do not request the application, such as Alt + F4. |

## 11.3.24 Application File Control Rule

The rule allows you to intercept file read and/or write events in the application if the Security officer has created at least one interception rule.

**Important!**

When reading and writing events for the same file are intercepted simultaneously, the write operation takes precedence.

**Note:**

- file interception will be performed based on the extension specified in the application profile, even if the file path is included in the exceptions (see Universal File Interceptor);
- file interception will be performed based on the path specified in the application profile, even if the file extension is included in the exceptions (see Universal File Interceptor).

**To configure the rule**:

1. Open the rule creation window and enter the rule name in the **Name** field.
2. In the **Interception channel** field, open the drop-down list and select **Universal file interceptor > File control in applications**.
3. In the **Application** field, select the application profile from the list (see Universal File Interceptor).
4. Select **Make a screenshot when creating an event** and/or **Create a shadow copy**, if you need these actions during the events interception.

> **Note:**
>
> If the **Create a shadow copy** action was not selected, but the size of the file sent in the application exceeds 50 MB, then events for sending such files are created without a shadow copy.

5. Specify the conditions for event generation:
   a. Select the **Read** and/or **Write** operation.
   b. Select and specify the **File mask** to apply the rule to files that match it. You can use wildcard characters:
      - ? – one unknown character;
      - * – any number of characters.
   c. You can limit the application of the rule to a specific file category by enabling the **File category** and selecting the one you need from the drop-down list.

      > **Note:**
      >
      > You can familiarize yourself with the file categories in the "Resources" Section, as well as in the knowledge base article Intercepted file extensions in Device Monitor (for rules with file category selection).
      > If you specify both a file mask and a category, both conditions must be met for the rule to be triggered.
      > On computers running Linux, file extension categories are not taken into account – the rule will apply to copying any files, regardless of the specified file categories.

   d. Specify the **File size** to limit the size of files subject to monitoring. Specify the range of values for the minimum and maximum file size and the units of measurement. If both fields are filled in, the rule will apply only to files whose size is within the specified range.
      By default, the condition is selected, and the file size is set to between 0 and 10 MB.
      If the conditions are not selected, the event will be generated without taking them into account.
6. After you have defined all the required parameters, click **Create**. The rule will apply permanently and will allow copying with the creation of an event with shadow copies. Subsequently, such events are sent for analysis to Traffic Monitor.

## 11.4 Creating and Editing Application Lists

To ensure more precise operation of the Agents on monitored workstations, you can use application lists.

### 11.4.1 Creating an application list

To create an application list:

1. Go to the Administration Centre by clicking  on the navigation bar.
2. In the **Resources** section, open the **Application lists** tab.
3. On the left, in the **Application list** section, click. .
4. In the **Create an application list** window:
   a. In the **Name** field, enter the name of the list.
   b. In the **Operation system** field, select one of the OS families:
      - **Windows** – the list will be marked with the icon 
      - **Linux** – the list will be marked with the icon 
5. Click **Create**.
6. If the synchronous editing prohibition is enabled, click **Save** on the information panel (see Configuration Editing Modes).

### 11.4.2 Adding applications to the list

To fill out the list, you can:

- Add the application manually
- Add the detected application to the list (only to the lists for Windows)

- Move or copy the application from another list

### Manually adding an application to the list

To add an application to the list:

1. Go to the Administration Centre by clicking  on the navigation bar.
2. In the **Resources** section, open the **Application lists** tab.
3. On the left, in the **Application list** section, click the list to which you want to add an application.
4. Click **Create an application**:
   - in the top-right corner;
   - in the list window, if the list is empty.
5. In the **Create an application** window, provide the following information:
   - **Description**;
   - For Windows:
     - **Application name** – the name of the executable file with the extension, such as *notepad.exe*;
     - **Location of executable file** – the absolute (full) path to the folder containing the executable file, such as *C:\Windows\System32*. When specifying the path, you can use environment variables;
     - **Issuer** – Organization (O), Location (L), State (S), Country (C) from the properties;
     - **Product name –** an optional parameter. The field is available if the **Issuer** is specified.
   - For Linux:
     - **Application name** – the name (without additional characters) that corresponds to the process being launched, such as *pluma*;
     - **Location of executable file** – the absolute (full) path to the folder containing the executable file, such as */usr/bin/*. When specifying the path, you can use environment variables.
6. After filling in the fields, click **Create**.
7. If the synchronous editing prohibition is enabled, click **Save** on the information panel (see Configuration Editing Modes).

**Note:**

To add an application to the list, the **Description** field and one of the following fields must be filled in: **Application name**, **Location of executable file**, or **Issuer**.
To determine whether the launched application matches the application from the list, the attribute values are compared:

- **Application name**
- **Location of executable file**
- **Issuer**

The verification process differs depending on the operating system of the monitored workstation.

- Windows – **not** case sensitive;
- Linux – case sensitive.

Take this into account when specifying the attributes of the applications.
If the attribute field is not filled in the list of applications, it will be checked.
**Example**: if you add an application to the list that contains only the **Description** and **Issuer** fields, it will match all applications from that issuer, regardless of the name or location of the executable file.

### Adding detected applications to the list

You can only add detected applications to lists **for Windows**.

**To add a detected application:**

1. In the  Device Monitor Management Console, go to **Resources > Application lists**.
2. Open the **Detected** list.
3. Select one or more applications .

4. On the pop-up window that appears at the bottom of the screen, click **Add to application list**.
5. In the dialog box that opens, select the list to which you want to add the application.
6. Click **Save**. In the top-right corner, the System will display a notification stating that the applications have been added.
7. If the synchronous editing prohibition is enabled, click **Save** on the information panel (see Configuration Editing Modes).

or

1. In the list of applications, hover over the application row on the right and click **Add application to list**.
2. In the dialog box that opens, select the list to which you need to add the application.
3. Click **Save**. In the top-right corner, the System will display a notification stating that the application has been added.
4. If the synchronous editing prohibition is enabled, click **Save** on the information panel (see Configuration Editing Modes).

> **Note:**
>
> If an application without a description is added from the list of detected applications, its name will be displayed in the **Description** field for that application.

### Copying and moving applications

You can copy and move applications from one list to another.

> **Note:**
>
> Moving or copying an application to a list for an OS of a different family is not supported. That is, you cannot copy or move an application from the list for Windows to the list for Linux, and vice versa.

**To copy the applications:**

1. Click next to the app, and then select **Copy**
   or
   select one or more applications and click at the bottom of the workspace.
2. In the **Copy application** window, select the list to which you want to copy the applications.
3. Click **Copy to list**.
4. If the synchronous editing prohibition is enabled, click **Save** on the information panel (see Configuration Editing Modes).

To move the applications:

1. Click next to the application and select **Move**
   or
   select one or more applications and click at the bottom of the workspace.
2. In the **Move application** window, select the list to which you want to move the applications.
3. Click **Move**.
4. If the synchronous editing prohibition is enabled, click **Save** on the information panel (see Configuration Editing Modes).

## 11.4.3 Editing and deleting lists and applications

**To edit** a list or an application:

1. Select the required element.
2. Click next to it, and then select **Edit**.
3. In the editing window, make the edits and click **Save**.

4. If the synchronous editing prohibition is enabled, click **Save** on the information panel (see Configuration Editing Modes).

**To delete** a list or applications:

1. Click  next to the element you want to delete, and then select  **Remove**
   or
   select one or more applications  and click  at the bottom of the workspace.
2. In the window, confirm the action by clicking **Remove**.
3. If the synchronous editing prohibition is enabled, click **Save** on the information panel (see Configuration Editing Modes).

> **Note:**
>
> The list of applications cannot be deleted if it is used in a policy rule.

## 11.5 Creating and Editing Resource Lists

For more precise operation of Agents on monitored workstations, you can use resource lists.
See the information on how to work with them in the sections:

- Creating a Resource List
- Editing a Resource List
- Deleting a Resource List

### 11.5.1 Creating a Resource List

**To create a resource list:**

1. Go to the Administration Centre by clicking  on the navigation bar.
2. Go to the **Web resources list** tab in the **Resources** section.
3. On the left, in the **Resource lists** area, click .
4. Enter the name of the resource list.
5. Click **Create**.
6. If the synchronous editing prohibition is enabled, click **Save** on the information panel (see Configuration Editing Modes).

**To add resources to the created list:**

1. Click .
2. Select the identification type: **Domain**, **URL**, or **URL includes**. To view help on identification types, hover over  in the **Identification type** field.
3. Enter the resource and its description.
4. Click **Create**.
5. If the synchronous editing prohibition is enabled, click **Save** on the information panel (see Configuration Editing Modes).

#### Determining whether the visited resource matches a resource from the list

The System determines whether the visited resource matches a resource from the list according to the following principle:

1. For the **Domain** type:

A check is performed for an exact match of `<host>`, including subdomains. Case is not taken into account.

*Example*: if the list contains the resource *example.com*, then the resources *one.example.com* or *ExamPle.com* will be considered matching the resource from the list. However, the resource example1.com will not match the value specified in the list.

2. For the **URL** type:

- if the URL in the list contains only a domain, an exact match check is performed for *<host>*, without taking subdomains into account;
- if the URL in the list contains parameters and an anchor (there are delimiters /, ?, #), an exact match check is performed for *<host> <port>* and *[/<URL path>][?<parameters>][#<anchor>]*;

- if the URL in the list contains a port, an exact match check is performed taking the port into account;
- if the URL in the list does not contain a port, only an exact match check is performed.

The case is taken into account everywhere except for the *<host>* part.
*Example*: if the list contains the resource *example.com/example?example#example*, then the resource *EXAMPLE.com/example?example#example* will be considered to match the resource from the list. However, the resources *one.example.com*, *one.example.com/example*, and *example.com:8080/example?example#example* will not match the value specified in the list.
3. For the **URL includes** type:
A check is performed to match the text entered in the list with the text in any part of the URL (by substring) *<host>[:<port>]][/<URL path>][?<parameters>][#<anchor>]*, including subdomains. Case is not taken into account.
*Example*: if the resource *example* is specified in the reference, then the resource *one.com/example?example#example* will be considered matching the resource from the list. However, the resource *one.com/one?onet#o* does not match the value specified in the list, as the URL does not contain the substring *example*.

**Important!**

Determining the matching of resources has the following features:

- The technologies for determining the URL of a resource displayed in the currently active tab of a supported application (internet browser) are based on the analysis of the application's graphical interface elements. Therefore, the determined URL may not fully match the actual URL of the resource which the application has requested.
- There is no conversion of the resource name to an IP address.
- There is no reverse transformation of the resource name if it was specified as an IP address.
- There is no conversion of characters encoded using the Punycode scheme (https://tools.ietf.org/html/rfc3492).
- The System determines whether the visited resource matches the resource from the list only if the user works in the following browsers:
  - Chrome
  - Yandex Browser
  - Mozilla Firefox
  - Edge (Chromium)
  - Opera
  - IE

## 11.5.2 Editing a Resource List

To change the list of resources, go to the **Web resources list** tab in the **Resources** section.

**To edit the name of the resource list:**

1. In the **Resource lists** area, select the list you want to edit by left-clicking it.
2. Next to the selected list, click  and select **Edit**.
3. In the window that opens, edit the list name.
4. Click **Save**.
5. If the synchronous editing prohibition is enabled, click **Save** on the information panel (see Configuration Editing Modes).

**To edit a resource from the list:**

1. In the **Resource lists** area, select the list you need.
2. Select the resource you want to edit by left-clicking it.
3. Next to the selected list, click  and select **Edit**.
4. In the window that opens, make the required edits.
5. Click **Save**.
6. If the synchronous editing prohibition is enabled, click **Save** on the information panel (see Configuration Editing Modes).

**To copy/move a resource from one list to another:**

1. In the **Resource lists** area, select the list that contains the required resource.
2. Select the resource you want to copy/move.
3. Next to it, click  and select **Copy**/**Move**.
   or
   click  /  at the bottom of the central area.
4. In the window that opens, select the list to which you need to copy/move the resource.
5. Click **Copy**.
6. If the synchronous editing prohibition is enabled, click **Save** on the information panel (see Configuration Editing Modes).

You can also copy/move several resources at once by selecting them and clicking  / .

**To remove a resource from the list:**

1. In the **Resource lists** area, select the list you need.
2. Select the resource you want to delete.
3. Next to it, click  ans select **Remove**
   or
   click  at the bottom of the central area.
4. In the window that opens, confirm the deletion.
5. If the synchronous editing prohibition is enabled, click **Save** on the information panel (see Configuration Editing Modes).

You can also delete several resources at once by selecting them and clicking .

### 11.5.3 Deleting a Resource List

**To delete a resource list:**

1. Go to the **Resources** section –> **Web resources list** tab.
2. In the **Resource lists** area, select the list you need to delete by left-clicking it.
3. Next to the selected list, click  and select **Remove**.
4. In the window that opens, confirm the action.
5. If the synchronous editing prohibition is enabled, click **Save** on the information panel (see Configuration Editing Modes).

## 11.6 Creating and Editing File Categories

When configuring file operation control rules, you can specify a file category as a condition for event creation. To view the existing categories, go to "Resources" Section **> File categories** and select the one you need from the **File categories** area. The workspace will display a list of extensions that are part of the selected category.

> **Important!**
>
> The preset file categories cannot be edited or deleted. Creating file extensions is not supported.

### 11.6.1 Creating a file category

**To create a file category:**

1. Go to the Administration Centre by clicking  on the navigation bar.
2. In the **Resources** section, open the **File categories** tab.
3. On the left, in the **File Categories** area, click .
4. Enter the name of the file category.
5. Click **Add**.
6. If the synchronous editing prohibition is enabled, click **Save** on the information panel (see Configuration Editing Modes).

7. To add file extensions to the created category, copy them from the predefined or other file categories you have created.

### 11.6.2 Changing the composition of the file category

**To copy extensions from one category to another:**

1. Select the category that contains the extensions you need to copy.
2. In the workspace, hover over the extension, click , then  **Copy**
   or
   select one or more extensions  and click  at the bottom of the workspace.
3. In the window that opens, select a category from the drop-down list.
4. Click **Select**.
5. If the synchronous editing prohibition is enabled, click **Save** on the information panel (see Configuration Editing Modes).

**To exclude extensions from the file category:**

1. Select the category from which you need to exclude extensions.
2. In the workspace, hover over the extension, click , then  **Remove**.
   or
   select one or more extensions  and click  at the bottom of the workspace.
3. In the window that opens, confirm the deletion.
4. If the synchronous editing prohibition is enabled, click **Save** on the information panel (see Configuration Editing Modes).

### 11.6.3 Editing and deleting file categories

**To edit the name** of a file category:

1. Select the category you want to change by left-clicking it.
2. Click , then  **Edit**.
3. In the editing window, make the edits you need and click **Save**.
4. If the synchronous editing prohibition is enabled, click **Save** on the information panel (see Configuration Editing Modes).

**To delete** a file category:

1. Select the category you want to delete by left-clicking it.
2. Click , then  **Remove**.
3. In the window that opens, confirm the deletion.
4. If the synchronous editing prohibition is enabled, click **Save** on the information panel (see Configuration Editing Modes).

## 11.7 Working with Computer Groups

You can assign security policies to computer groups. Working with computer groups is carried out in the **Groups** section of the Administration Centre and includes:

- Creating and Editing Computer Groups
- Setting up Computer Group Membership
- Viewing Information about Computers
- Viewing Computer's Result Policy

### 11.7.1 Creating and Editing Computer Groups

**Important!**

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

**Note:**

To retrieve information about computers from the directory service, you can perform synchronization with a LDAP server. To learn more, see Synchronization.

**To add a computer group:**

1. Go to the **Administration Centre** by clicking  on the navigation panel.
2. Go to **Groups > Computers**.
3. On the **Groups** panel, click .
4. Specify the following parameters:
   - group **Name**;
   - **Policy**. Select a policy to be assigned to this computer group from the drop-down list.
5. Click **Add**. A new computer group will be created and you can add computers to it.
6. If the synchronous editing prohibition is enabled, click **Save** on the information panel (see Configuration Editing Modes).

**To edit a computer group:**

1. Select the computer group and click  on the right from its name.
2. Select **Edit** and make the changes.
3. Click **Save**.
4. If the synchronous editing prohibition is enabled, click **Save** on the information panel (see Configuration Editing Modes).

**To search for a computer or a computer group:**

1. In the upper part of the workspace, enter a search query of at least 3 characters in the search bar. The drop-down list will display the first 5 computers and the first 5 computer groups whose parameters include the entered text.
2. Select the search results to display:
   - To view all items matching the query, press **Enter** or click **View all results**. The results will be displayed as a hierarchical list in the left pane, with the found groups highlighted in blue. If one of the search results is a group, all items included in it will be shown, including those that do not match the search criteria.
   - To go to a specific item, click a group or a computer. The workspace will open the selected group or the group containing the selected computer.

**Important!**

If a search using Cyrillic characters does not return results, make sure that the Russian locale ( `ru_RU.utf8` ) is set for the database Device Monitor server interacts with. To learn more, see Check and change PostgreSQL DBMS locale.

To reset the filter applied via search, click  in the search bar.

**To delete a computer group:**

1. Select the group to delete and click  on the right of its name.

   **Note:**

   The "default" computer group cannot be deleted.
2. Click **Remove**. The group you are deleting may contain computers that are not included in other groups. In this case, the computers will be automatically added to the "default" computer group.
3. In the window that opens, click **Remove**.
4. If the synchronous editing prohibition is enabled, click **Save** on the information panel (see Configuration Editing Modes).

## 11.7.2 Setting up Computer Group Membership

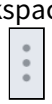
When installing InfoWatch Device Monitor Agent on a computer, a record for the computer is automatically created in the System. This record is added to the "default" group. The policy assigned to this group will apply to all

computers included in it. Later, these policies are to be assigned to a computer by adding it to different computer groups.

**To configure the membership of a computer group:**

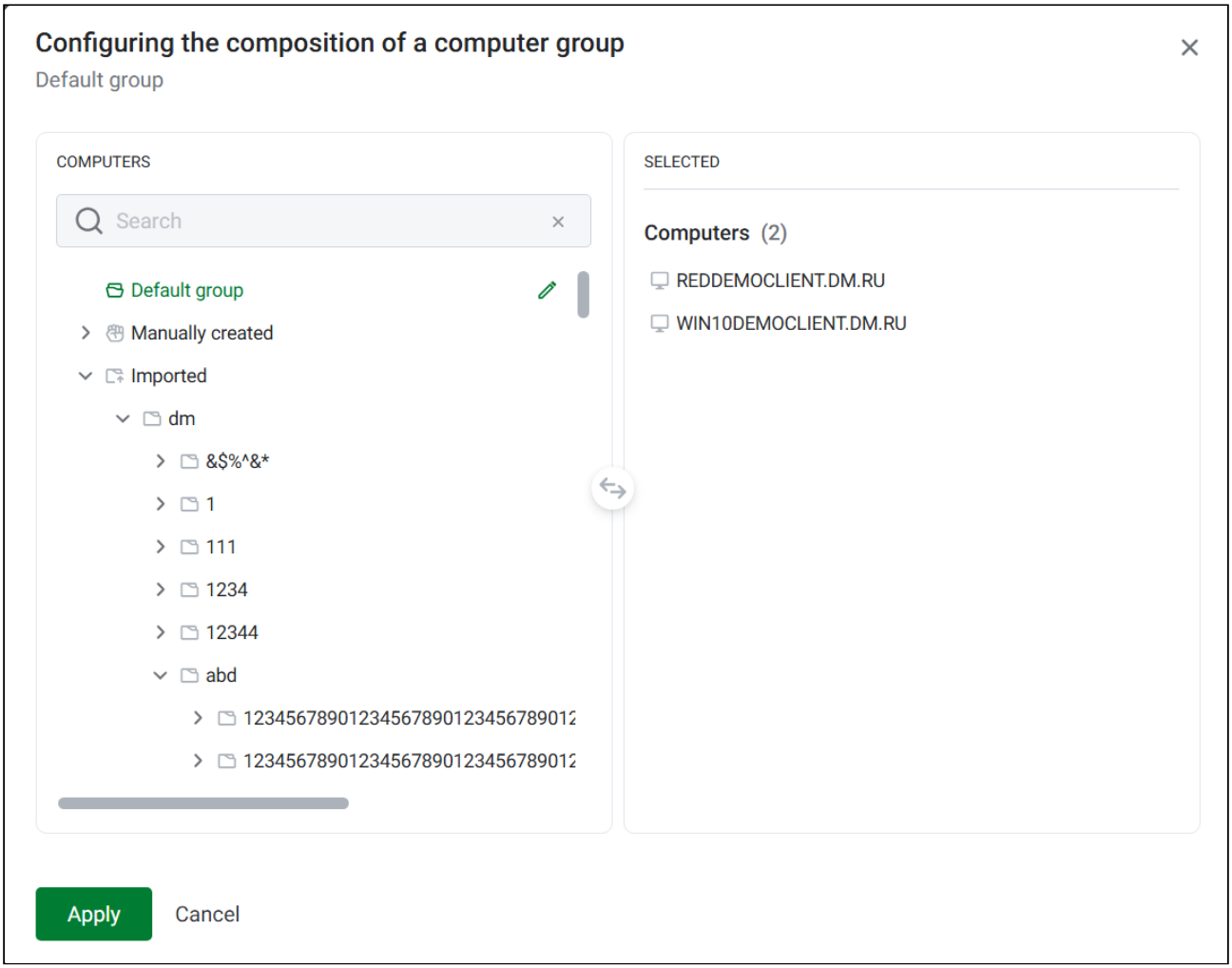
1. Click  on navigation panel to go to Administration Centre.
2. Open the **Computers** tab in the **Groups** section.
3. In the left part of the workspace, select the name of the required group. The workspace of the main window will then display a list of all computers already included in the group.

   > **Note:**
   >
   > To find a group in the list, you can use search. To learn more, see Creating and Editing Computer Groups.

4. Open the **Configuring the composition of a computer group** window in one of the following ways:
   - in the upper-right corner of the workspace, click  **Set up group membership**;
   - on the right of the group name, click  >  **Set up group membership**.

5. In the left pane, browse the **Computers** list. It displays computers previously registered in the System, meaning the computers with the Agent installed, from the "default" group and other groups.

   To expand or collapse a group, click .
   To find a computer or a group, enter a search query of at least 3 characters in the search bar. The results will be displayed as a hierarchical list in the left pane, highlighted in blue. If one of the search results is a group, all the items included in it will be shown, including those that do not match the search criteria.
6. To add computers to a group, in the left pane hover the cursor over the computer or group and click  **Add computers to "<Computer group name>"**. The  icon will appear next to the added group or computer. If a computer name is very long, you can view it using the scroll bar at the bottom of the window.
7. To remove an entry from the group, hover the cursor over the entry and click  **Remove computers from "<Computer group name>"**. You can do this both in the right pane and in the left pane.
8. Click **Apply**.
9. If the synchronous editing prohibition is enabled, click **Save** on the information panel (see Configuration Editing Modes).



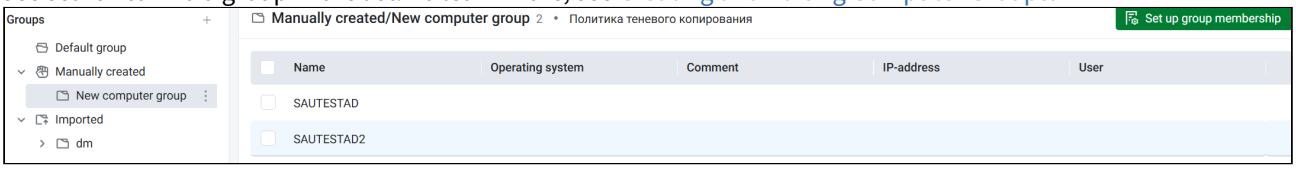

**Note:**

If you add a computer group that contains subgroups, the computers from those subgroups will not be automatically added to the selected group. You can add them separately.

If a computer is included in a specific computer group, the policies of that group will be assigned to it. To revoke the effect of any security policy on a computer, exclude it from the group to which that policy is assigned.

Within a computer group, you can work with the list of computers: edit, exclude, and delete computers from the System.

Use search to find a group in the list. To learn more, see Creating and Editing Computer Groups.




**Note:**

For imported computer groups the only action available within the group is editing.

**To exclude a computer from a computer group:**

1. In the row with the computer name, click ⋮.
2. Select — **Exclude from group**.
3. Click **Exclude**. If the computer was a member of only one group, it will be automatically added to the "default" computer group upon exclusion.

4. If the synchronous editing prohibition is enabled, click **Save** on the information panel (see Configuration Editing Modes).

**To exclude several or all computers from a group:**

1. Select the required computers using the checkboxes.
2. Select  **Exclude from group**.
3. In the dialog box that opens, click **Exclude**. If a computer was a member of only one group, it will be automatically added to the "default" computer group upon exclusion.
4. If the synchronous editing prohibition is enabled, click **Save** on the information panel (see Configuration Editing Modes).

**To add a comment to a computer:**

1. In the row with the computer name, click .
2. Select  **Edit**.
3. In the **Comment** field, add your comment and click **Save**.

If necessary, you can delete computers from the list of registered ones (for example, if a workstation is no longer in use).

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

1. In the row with the computer name, click .
2. Select  **Remove from security scheme**.
3. In the dialogue window that opens, select **Remove**.
4. If the synchronous editing prohibition is enabled, click **Save** on the information panel (see Configuration Editing Modes).

**To remove several or all computers from a group:**

1. Select the required computers using the checkboxes.
2. Select  **Remove from security scheme**.
3. In the dialogue window that opens, select **Remove**.
4. If the synchronous editing prohibition is enabled, click **Save** on the information panel (see Configuration Editing Modes).

**Important!**

Deleting a computer from a security scheme will also remove it from all groups and policies.

## 11.7.3 Viewing Information about Computers

The left part of the workspace displays the list of computer groups. The right part shows the list of computers included in the selected computer group.

Information about computers is presented as a table. The columns display the main properties of the computers. You can change the order of the columns, as well as hide the columns that you do not need to display.

The table contains the following main information:

- **Name**. Workstation domain name;
- **Operating system**. Version of operating system;
- **Comment**. Field for entering a comment. The same comment for the workstation is displayed on the **Status** tab of the **Agents** section;
- **IP-address**. IP address of the workstation;
- **User**. The username of the person who last logged in to the workstation.

  **Note:**

  The user is not displayed for workstations running Linux.

Extended information about the computer properties is displayed in the **Details** panel. To view the properties of a specific computer, in the workspace of the main window click the row with the description of the required computer.

The **Details** panel will display a table of properties containing additional information about the selected computer:

- **Schema version**. The version number of the security scheme uploaded to the Agent;
- **Network resource control settings version**. The version of the settings for controlling network traffic transmitted via the XMPP, MMP, FTP, FTPS, SMTP/S/MIME/Outlook/POP3, and HTTPS protocols;
- **Excluded applications settings version**. The version of the settings for excluding applications from interception. The number of the last applied version is specified in brackets;
- **Settings version**. The version of the general security policy settings ( Device Monitor) (see Configuring Device Monitor);
- **TM configuration version**. The latest configuration version of Traffic Monitor delivered to this workstation;
- **Network control settings version**. The version of the settings for controlling data transfer over network connections;
- **Template messages version**. The version of notification templates displayed to the user.

> **Note:**
>
> When the Agent sends an event to the Device Monitor server, the Agent deletes the data of this event from the disk.

> **Important!**
>
> In some cases, data deletion on Agents is not supported. The file with event metadata may remain on the Agent's disk even if the Agent has sent the event.

The information displayed for some properties is duplicated in the workspace of the main window.
Each registered computer is automatically added to the "default" computer group. The security policy ( Device Monitor) defined for the "default "computer group is assigned to it.

### 11.7.4 Viewing Computer's Result Policy

The result policy is a set of rules that are effective on the computer. The result rules consist of the rules configured by default and the rules specified for this particular computer.

**To view the result policy in effect on a computer:**

1. Go to the **Administration Centre** by clicking  on the navigation panel.
2. Open the **Computers** tab in the **Groups** section.
3. In the **Groups** pane, select the group that contains the computer you need. The workspace will display a list of all computers included in the group.
4. In the row with the name of the required computer, click .
5. Select  **Result policy**.

The **Result policy** window will open, where you can view the resulting rules on this computer. To view detailed information about a rule, in the **Interceptors** pane, select the interception channel you need.
You can view the following resulting rules:

- Data transfer channel control:
  - Removable Device Control Rule
  - Network Resource Control Rule
  - Terminal Session Control Rule
  - Print Control Rule
  - FTP Control Rule
  - HTTP(S) Control Rule
  - Mail Control Rule
  - Cloud Storage Control Rule
  - Clipboard Control Rule
- Messenger control:
  - VK Messenger Control Rule
  - Telegram Messenger Control Rule

        - Yandex Messenger Control Rule
        - WhatsApp Messenger Control Rule
        - MAX Messenger Control Rule
        - XMPP protocol Control Rule
    - User activity monitoring
        - Screen Monitoring Rule
        - Keyboard Input Monitoring Rule
        - Audio Environment Monitoring Rule
        - Screen Video Recording Rule
    - Usage control
        - Screenshot Creation Control Rule
    - Application control
        - Application File Control Rule

**Note:**

In the **Result policy** window, resource lists are also displayed for the **Keyboard input monitoring** and **HTTP(S) control** rules (to learn more about resource lists, see Keyboard Input Monitoring Rule, HTTP(S) Control Rule).

To view the policy assigned to the default computer group, select **New computer** in the **Computer** field.
You can additionally view the resulting policy for an employee associated with the selected computer. To do this, select the object to view in the **Employee** field:

- **New employee** — the rule assigned to the default employee group is displayed;
- **Known employees** — the rule for the selected employee from the list of users who have ever been registered on this computer is displayed.

The field provides search across all employees. If you select an employee who is not associated with the computer, the value in the **Computer** field is reset.

**Note:**

Similarly, for an employee you can select the computers associated with them. To learn more, see Viewing Employee's Result Policy.

## 11.8 Working with Employee Groups

You can assign security policies to employee groups. Working with employee groups is performed in the **Groups** section of the **Administration Centre** and includes:

- Creating and Editing Employee Groups
- Setting up Employee Group Membership
- Viewing Employee's Result Policy

### 11.8.1 Creating and Editing Employee Groups

You can manage the employees' accounts and monitor them in the **Employees** section.

**Important!**

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

**Note:**

To retrieve information about employees from the directory service, you can perform synchronization with a LDAP server. To learn more, see Synchronization.

**To add an employee group:**

1. Go to the Administration Centre by clicking  on the navigation panel.
2. Go to **Groups > Employees**.
3. On the **Groups** panel, click .
4. Specify the following parameters:
    - group **Name**;
    - **Policy**. Select a policy to be assigned to this employee group from the drop-down list.

5. Click **Add**. A new employee group will be created and you can add employees to it.
6. If the synchronous editing prohibition is enabled, click **Save** on the information panel (see Configuration Editing Modes).

**To edit an employee group**:

1. Select the employee group and click  to the right of its name.
2. Select  **Edit** and make the changes.
3. Click **Save**.
4. If the synchronous editing prohibition is enabled, click **Save** on the information panel (see Configuration Editing Modes).

**To search for an employee or an employee group:**

1. In the upper part of the workspace, enter a search query of at least 3 characters in the search bar. You can search an employee by their identifier, surname, name or patronymic.
   The drop-down list will display the first 5 employees and the first 5 employee groups whose parameters include the entered text.
2. Select the search results to display:
   - To view all items matching the query, press **Enter** or click **View all results**. The results will be displayed as a hierarchical list in the left pane, with the found groups highlighted in blue. If one of the search results is a group, all items included in it will be shown, including those that do not match the search criteria.
   - To go to a specific item, click a group or an employee. The workspace will open the selected group or the group containing the selected employee.

**Important!**

If a search using Cyrillic characters does not return results, make sure that the Russian locale ( `ru_RU.utf8` ) is set for the database Device Monitor server interacts with. To learn more, see Check and change PostgreSQL DBMS locale.

To reset the filter applied via search, click  in the search bar.

**To delete an employee group:**

**Note:**

You cannot delete the default employee group.

1. Next to the group you need, click .
2. Click  **Remove**. The group you are deleting may contain employees that are not included in other groups. In this case, the employees will be automatically added to the "default" employee group.
3. In the window that opens, click **Remove**.
4. If the synchronous editing prohibition is enabled, click **Save** on the information panel (see Configuration Editing Modes).

## 11.8.2 Setting up Employee Group Membership

When installing InfoWatch
This page has not yet been translated to English.
Agent on a computer, the records for the employees are automatically created in the System. These records are added to the default group. The policy assigned to this group will apply to all employees included in it. Later, these policies are to be assigned to an employee by adding it to different employee groups.

**To configure the membership of an employee group:**

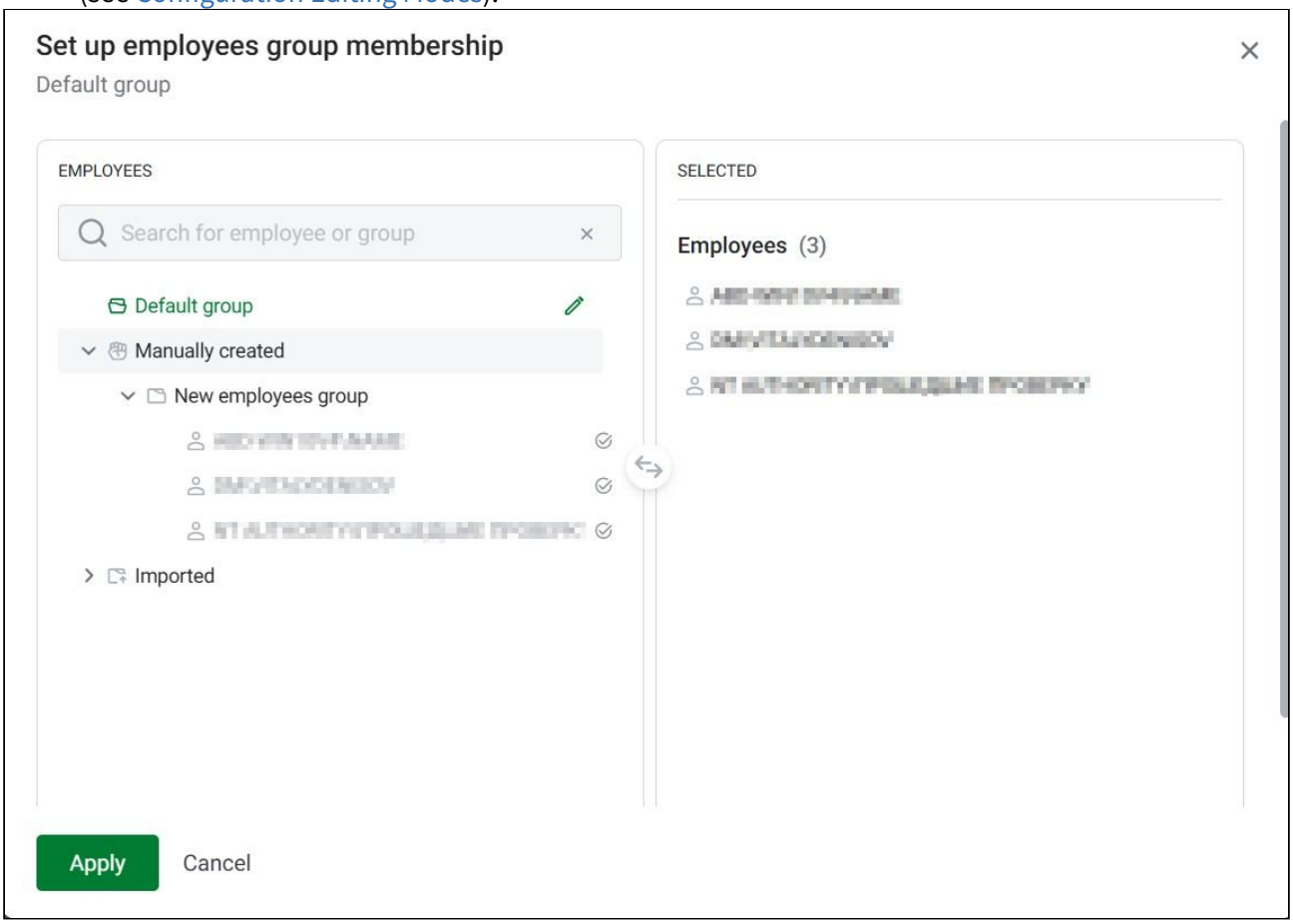
1. Go to the **Administration Centre** by clicking  on the navigation panel.
2. Open the **Employees** tab in the **Groups** section.
3. In the left part of the workspace, select the name of the group you need. The workspace of the main window will then display a list of all employees already included in the group.

**Note:**

To find a group in the list, you can use search. To learn more, see Creating and Editing Employee Groups.

4. Next to the group, click , then select **Set up group membership** or select the group and, in the upper-right corner of the workspace, click **Set up group membership**.
   A dialogue window will open. In its left area, the list of employees previously registered in the System, will be displayed.

   To expand or collapse a group of employees, click .
   To find an employee or a group, enter a search query of at least 3 characters in the search bar. Only search by identifier is available. The results will be displayed as a hierarchical list in the left pane, highlighted in blue. If one of the search results is a group, all the items included in it will be shown, including those that do not match the search criteria.
5. To add an employee to a group, in the left pane, hover the cursor over the employee or group and click **Add employee to "<Employee group name>"**. The icon will appear next to the added group or employee.
6. To remove an entry from the group, hover the cursor over the entry and click **Remove employee from "<Employee group name>"**. You can do this either in the right pane or in the left pane.
7. Click **Apply**.
8. If the synchronous editing prohibition is enabled, click **Save** on the information panel (see Configuration Editing Modes).



**Note:**

If you add an employee group that contains subgroups, the employees from those subgroups will not be automatically added to the selected group. You can add them separately.

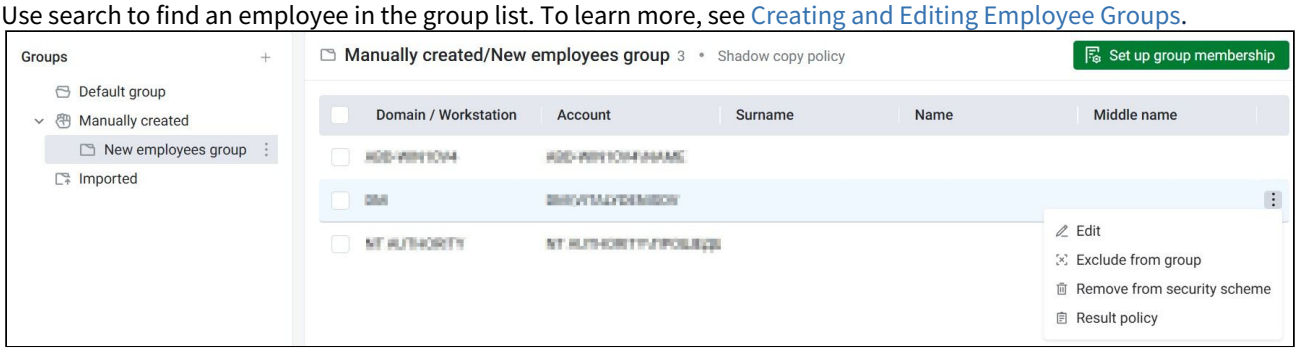
If an employee is included in a specific employee group, the policies of that group will be assigned to them. To revoke the effect of any security policy on an employee, exclude them from the group to which that policy is assigned.

**Important!**

If an employee has never logged in on a computer with an Agent (for example, they were using connection via SSH), then the policy assigned to them will not be triggered. In this case, the interception will be performed in accordance with the rules in the default policy. If the default policy has no rules, the interception will not be performed.

Within an employee group, you can work with the list of employees: edit, exclude, and delete employees from the System.

Use search to find an employee in the group list. To learn more, see Creating and Editing Employee Groups.




**Note:**

For imported employee groups, the only action available within the group is editing.

**To edit an employee record**:

1. In the row with the employee name, click ⋮.
2. Select ✎ **Edit**.
3. If the employee record is created during the directory service synchronisation, click **Get name** to retrieve the up-to-date data for the employee.
4. You can also manually change the employee's **Name**, **Surname**, and **Middle name**.
5. When all the changes are made, click **Save**.

**To exclude an employee from a group:**

1. In the row with the employee name, click ⋮.
2. Select − **Exclude from group**.
3. In the dialogue window that opens, confirm the action by clicking **Exclude**. If the employee was a member of one group only, they will be automatically added to the "default" employee group upon exclusion.
4. If the synchronous editing prohibition is enabled, click **Save** on the information panel (see Configuration Editing Modes).

**To exclude several or all employees from a group:**

1. Select the required employees using checkboxes.
2. Select ⛶ **Exclude from group**.
3. In the dialog box that opens, click **Exclude**. If an employee was a member of one group only, they will be automatically added to the "default" employee group upon exclusion.
4. If the synchronous editing prohibition is enabled, click **Save** on the information panel (see Configuration Editing Modes).

If needed, you can delete employees from the list of registered ones.

**To remove an employee from the security scheme:**

1. In the row with the employee name, click .
2. Select  **Remove from security scheme**.
3. In the dialogue window that opens, select **Remove**.
4. If the synchronous editing prohibition is enabled, click **Save** on the information panel (see Configuration Editing Modes).

**To remove several or all employees from the security scheme**:

1. Select the required employees using the checkboxes.
2. Select  **Remove from security scheme**.
3. In the dialogue window that opens, select **Remove**.
4. If the synchronous editing prohibition is enabled, click **Save** on the information panel (see Configuration Editing Modes).

**Important!**

Removing an employee from a security scheme will also remove them from all groups and policies.

### 11.8.3 Viewing Employee's Result Policy

The result policy is a set of rules that are effective for the employee. The effective rules consist of the rules configured by default and the rules specified for this particular employee.

**To view the result policy in effect for an employee:**

1. Go to the **Administration Centre** by clicking  on the navigation panel.
2. Open the **Employees** tab in the **Groups** section.
3. In the **Groups** pane, select the group that contains the employee you need. The workspace will display a list of all employees included in the group.
4. In the row with the name of the employee you need, click .
5. Select  **Result policy**.

The **Result policy** window will open, where you can view the effective rules for this employee. To view detailed information about a rule, in the **Interceptors** pane, select the interception channel you need. To learn more about all effective rules available for viewing, see Viewing Computer's Result Policy.

You can view the policy of another employee by selecting them from the **All** list in the **Employee** field. If necessary, use search. You can search an employee by their identifier, last name, first name, or patronymic.

To view the policy assigned to the default employee group, select **New employee**.

You can additionally view the result policy of the computer associated with the employee. To do this, select the object to view in the **Computer** field:

- **New computer** – the rule assigned to the default computer group is displayed;
- **Known computers** – the rule for the computer selected from the list of computers previously used by the user is displayed.

The field provides search across computers.

**Note:**

Similarly, for a computer, you can select the employees associated with it. To learn more, see Viewing Computer's Result Policy.

## 11.9 Working with Agents

You can work with Agents in the **Agents** section of the Administration Centre. Information about working with Agents is available in the following subsections:

- Viewing Information about Agents
- Filtering Entries
- Rebooting Computer

- Updating Configuration
- Agent Diagnostics
- Assigning the "Golden image" Status
- Starting and Stopping Agents
- Removing Agents
- Distribution Policies

### 11.9.1 Viewing Information about Agents

Information about Agents is displayed as a tabular list. The columns display the main properties of workstations. You can change the order of the columns.

The tabular list contains the following basic information:

- **State**. State of the Agent installed on the computer. See the list below.
- **Disk space**. Data on the capacity of the disk with the Agent displayed in the following format: Free space/Total space. Possible values:
  -  – there is enough space (meaning that it is greater than or equal to the value specified for the *Warning threshold* option in the **Disk space control** block. To learn more, see Agents).
  -  – space is about to run out (remaining space is less than the *Warning threshold* value or equal to the value specified for the *Low disk space* parameter).
  -  – space has run out, shadow copies are not being collected (remaining disk space is less than the value specified for the *Low disk space* parameter).

  If an Agent running Windows has multiple disks, the information is displayed for the disk with the maximum free space.
- **Workstation**. Workstation domain name.
- **IP address**. Workstation IP address.
- **Last call**. Date and time of the last call to the server of the Agent installed on the workstation.
- **Connection**. Date and time of the connection to the server of the Agent installed on the workstation.
  Connection is established when the client starts. Also, for load balancing, the Agent periodically reconnects to the pool of servers. With each successful connection, the date and time in the **Connection** field change. When the Agent is started after being stopped, a connection to the server is established and the value of the **Connection** field is updated.
- **Registration**. Date and time of the workstation registration (adding to database).
- **Agent version**. The version number of the Agent installed on the workstation.
- **Operating system (OS)**. Version of the operating system.
- **User**. The name of the last user who logged in at the workstation. The user is not displayed for workstations running Linux.
- **Comment**. Comment entered on the **Computers** tab of the **Groups** section.
- **Agent activity**. The activity of the installed Agent is displayed using a colour indicator at the beginning of the row:
  -  – *Inactive for over an hour*, meaning that the Server cannot establish a connection with it;
  -  – *The Agent is active*;
  -  – *Inactive for more than one day*;
  -  – *Inactive for more than two weeks*;
  -  – *Inactive for over a month*.
- **Schema version**. The version number of the security schema loaded onto the Agent. For a computer with the **Not installed** installation state, the value "0" should be displayed.
- **TM configuration version**. The last version of the Traffic Monitor configuration delivered to this workstation.

- **Settings version**. Version of the general settings of the security policy. The number of the last version applied on the Agent is indicated in parentheses.
- **Template version**. Version of notification templates that can be displayed for the user.
- **Network control settings version**. Version of the settings for controlling network traffic transmitted over protocols: XMPP, MMP, FTP, FTPS, SMTP/S/MIME/Outlook/POP3, HTTPS.
- **Network resource control settings version**. Version of the data transfer control settings for network connections.
- **Excluded applications settings version**. Version of the settings for excluding applications from interception on the server. The number of the last version applied on the Agent is indicated in parentheses.

## Working with table data

When working with the table, you can:

- change the column display:
  - reorder columns and add new ones
  - sort values
  - group Agents
  - filter entries, see Filtering Entries
- view detailed information
- refresh data

### Table column display

By default, you can see the following columns:

- Agent activity
- State
- Workstation
- IP address
- Last call
- Agent version
- OS
- Comment

You can configure the display of columns in the table. For this:

1. In the upper-right corner, click .
2. From the list, select  the columns to add to the table.
3. To enable the default column display in the table, click **Revert system settings**.

To move a column:

1. On the upper panel, select the column to move.
2. Hold the mouse button and drag the column.

### Sorting values in columns

The following sorting principle is applied in the table:

- Ascending/Descending: *Activity*, *Disk space*, *IP address*
- Ascending/Descending alphabetical order: *Workstation*, *Comment*, *OS*, *User*
- From latest to earliest: *Agent version*, *TM configuration version*, *Settings version*, *Excluded applications settings version*, *Network control settings version*, *Network resource control settings version*, *Schema version*, *Template version*, *Connection*, *Last call*, *Registration*

For the *State* column, sorting is implemented as follows: since an Agent can have multiple states at the same time, sequential sorting is applied from the first state in the list to the last one, meaning that the System first sorts by the first displayed state, then by the second one, and so on.

To change the sorting:

1. In the column you need, click the cell with the name of that column.
2. Click the  **Sort** button that appears.
3. To change the sort order, click the button again.

Grouping Agents

You can also group Agents by column values.

> **Important!**
>
> Grouping is available only for columns that have the corresponding button.

To group Agents:

1. In the column you need, click the cell with the name of that column.
2. Click the  **Group** button that appears.

When grouping, the System creates groups of Agents with matching values in the selected column. The column name is displayed above the table with Agents. To disable grouping, click  next to the column name or the **Reset** button in the upper-right corner.

The **Empty** group is a group with Agents with empty value in the column.

You can group Agents by multiple columns. Grouping is performed hierarchically: first, Agents are split by the first selected column; then, within each group, they are split by the second column, and so on. To change the order, drag the column name to the required position in the hierarchy above the Agents table.

Viewing detailed information

You can see extended information about the Agent's state on the **Details** panel. It appears when you click on an Agent row.

In addition to the data presented in the table, the panel displays the **Versions** section with the following information:

- **Schema version**
- **Agent version**
- **TM configuration version**
- **Settings version**
- **Template version**
- **Network resource control settings version**
- **Network control settings version**
- **Excluded applications settings version**

To hide the panel, click  to the right of its name.

> **Note:**
>
> If an Agent sends an event to the Device Monitor server, the Agent deletes data of the event from the disk. In some cases, deleting data on Agents is not supported. The event metadata file may remain on the Agent's disk even if the Agent has sent the event.

Refreshing data

You can refresh data in the Agents table by clicking . In this case, the selected filter, sorting, and grouping values are preserved. These values are also preserved when switching tabs.

## Agent states

Agent can have the following **states**[1]:

- *Not installed*. An Agent was never installed on the workstation, or the workstation was added to the security schema without an Agent;
- *Installed*. The Agent is installed on the workstation via primary distribution task, or the workstation was added to the security schema with the installed Agent. This state is not displayed when the Agent has other states;
- *Works with limitations*. The Agent is installed on the workstation but is partially operational. For example, the Agent has this state after it starts, when checking the loading and compatibility of the required OS kernel drivers;
- *Stopping*. A stop process is running on the Agent;
- *Stopped*[2]. The Agent is installed on the workstation and stopped via the Device Monitor Console;
- *Starting*. A start process is running on the Agent;
- *Starting the diagnostic mode*. The Agent is switching to the diagnostic mode;

- *Diagnostic mode*. The Agent is installed on the workstation and switched to the diagnostic mode via the Device Monitor Console;
- *Leaving the diagnostic mode*. The Agent is exiting the diagnostic mode;
- *Golden image*[3]. The Agent is installed on the workstation that has the *Golden image* state – a computer image that serves as the basis for creating new virtual machines (for example, to create similar servers or workstations for users solving similar tasks);
- *Uninstalled*[4]. The Agent is deleted from the workstation via product uninstallation task or by means of the workstation.

**Note:**

[1] When migrating the Device Monitor for Windows server to Device Monitor for Linux, the Agents' state is overwritten with the pre-installed settings in Device Monitor for Linux.

[2] If the stopped Agent is updated, then it will be started after the update is completed.

[3] When the name of a workstation with the *Golden image* state is changed, the System creates a new entry for the workstation with the new name, thus identifying it as cloned. If you actually renamed the workstation (and did not clone it):

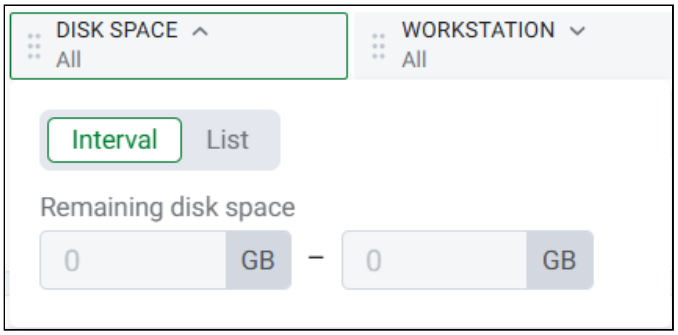
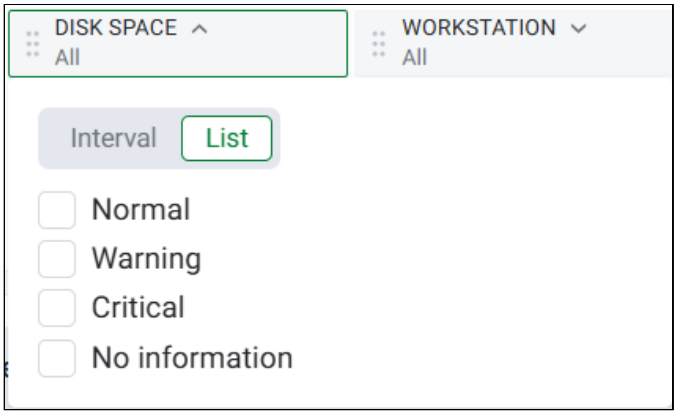
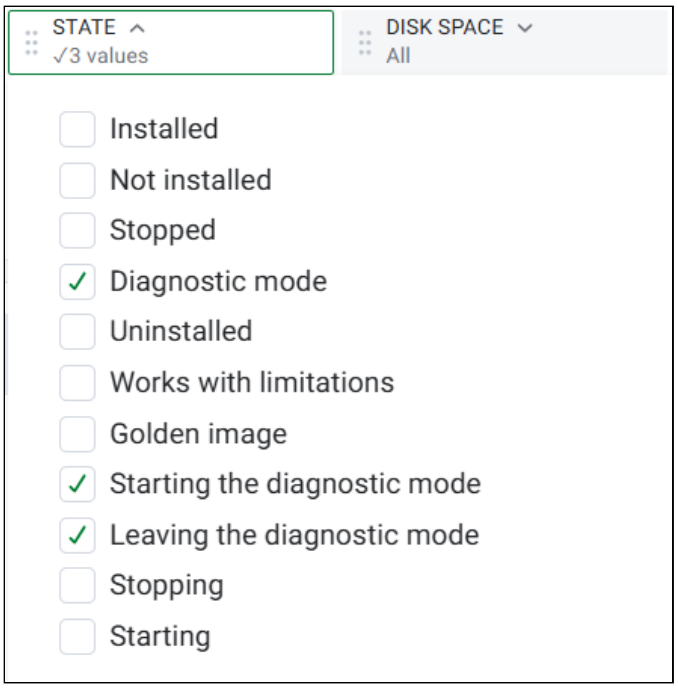
1. In the **Groups** > **Computers** section, delete the entry with the old name.
2. In the **Agents** section, assign the *Golden image* state to the entry with the new name.

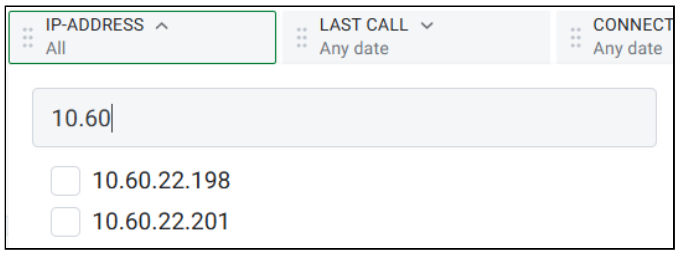
[4] When deleting Device Monitor, the Agent sends information about its state via UDP protocol that does not guarantee delivery.
Moreover, the Agent sends a notification when a session has already been established with the Device Monitor server. The Agent sends the message to the server that it is currently communicating with.

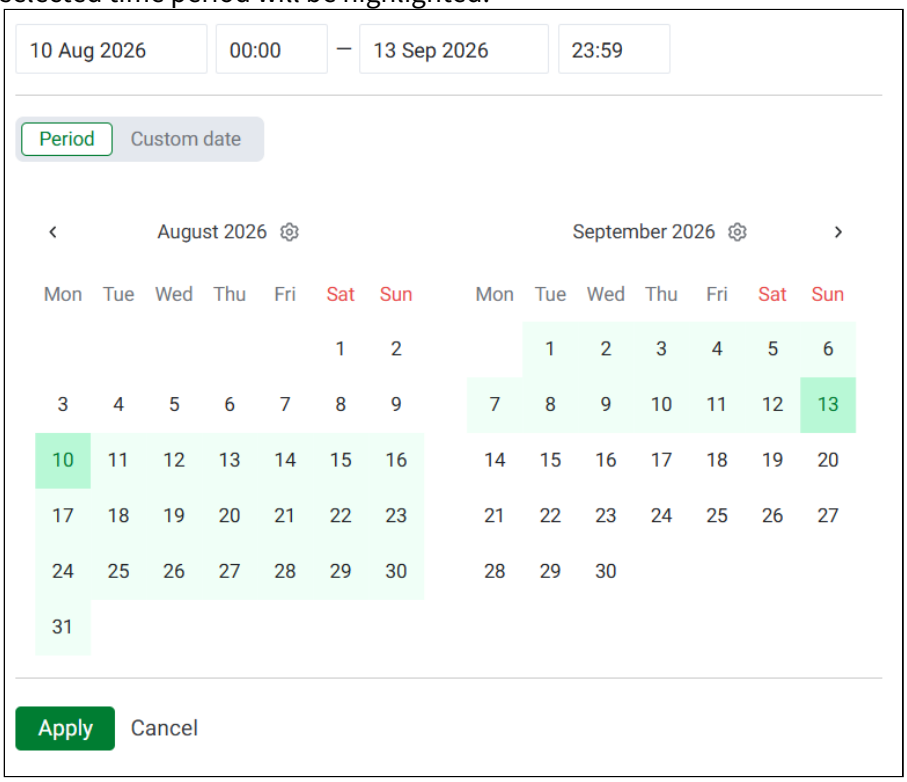
### 11.9.2 Filtering Entries

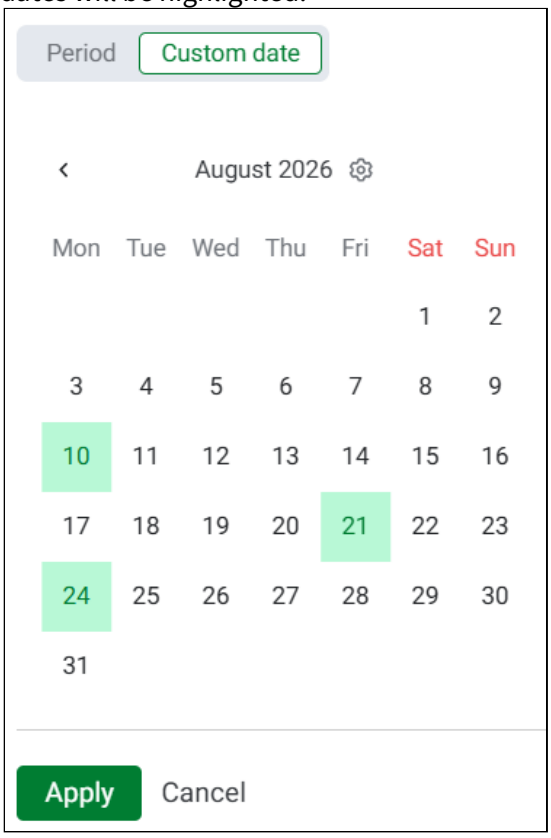
A filter panel is located above the Agents table. Using the panel, you can exclude part of the data from the analysis to hide unnecessary information.
You can filter the entries in the **Agents** section by the values of the following columns:

| Column | Setting filter values |
|---|---|
| **Activity** | • *Active*<br>• *Inactive for over an hour*<br>• *Inactive for more than one day*<br>• *Inactive for more than two weeks*<br>• *Inactive for over a month*<br>• *No information* |

| Column | Setting filter values |
| --- | --- |
| **Disk space** | You can specify the value as an interval (in GB):<br><br>or as a list of attributes:<br><br>For Agents with version 7.18.x and earlier, the *No information* value is displayed. |
| **State** | Select the checkboxes next to all required values:<br> |

| Column | Setting filter values |
| --- | --- |
| **Agent version**<br>**Schema version**<br>**TM configuration version**<br>**Settings version**<br>**Excluded applications settings version**<br>**Network resource control settings version**<br>**Network control settings version**<br>**Template version**<br>**OS**<br>**Comment**<br>**IP address** | When the *Comment* and *IP address* filters have many values, use search. To do this, start entering a value in the filter field and select one of the suggestions:<br> |
| **Workstation**<br>**User** | Selecting values is similar to adding computers/employees to groups. See Setting up Computer Group Membership and Setting up Employee Group Membership. |

| Column | Setting filter values |
| --- | --- |
| **Last call** | Select the time period for which you want to get data:<br>• *Last 24 hours*<br>• *Current day*<br>• *Last 3 days*<br>• *Last 7 days*<br>• *Last 30 days*<br>• *Current month*<br>• *Last month*<br>• *Custom period* (you can select the start and end dates of the period or separate dates):<br>To specify a custom period:<br>a. Use your mouse to select the start and end dates in the calendar. The selected time period will be highlighted:<br><br><br>You can also specify dates in the fields above.<br>b. If needed, specify the start and end time of the period.<br>c. Click **Apply**.<br>To specify one or more custom dates: |

| Column | Setting filter values |
|---|---|
| **Connection**<br>**Registration** | a. Use your mouse to select one or more dates in the calendar. The selected dates will be highlighted:<br><br><br>b. Click **Apply**. |

Values within the same column are combined with logical *OR*; columns are combined with logical *AND*.

**To reset the values of the filter**, on the filter panel, click . The filter will be set to its default value.

**To hide the filter panel**, click in the upper-right corner of the panel.

**To remove a filter from the panel**, click in the upper-right corner of the panel and clear the filter checkbox.

**To move a filter to a different location on the panel,** hold down next to the selected filter and drag it to another place.

**Note:**

When working with filters, keep in mind that:

- all filter settings apply only within a single browser tab;
- when the page is refreshed or you log out of the System, all user filter attributes are preserved.

## 11.9.3 Rebooting Computer

To remotely reboot the computer with the installed Agent:

1. In the **Agents** section, hover over the row with information about the Agent.
2. At the end of the row, click .
3. Select **Reboot PC**.

**Important!**

Workstation reboot is not available for Agents with the *Not installed* and *Uninstalled* statuses.

### 11.9.4 Updating Configuration

To update the configuration and settings of the Agent:

1. In the **Agents** section, hover over the row with information about the Agent.
2. At the end of the row, click .
3. Select **Update the configuration and agent settings**.

> **Note:**
>
> For a successful configuration update via the Device Monitor Console, at least 5 minutes must pass between the moment of the last configuration edits in the Console and the request to update the configuration on the Agent.

### 11.9.5 Agent Diagnostics

You can remotely collect diagnostic data from workstations. The data is requested from the Administration Centre via the Device Monitor server that communicates with the Agents.

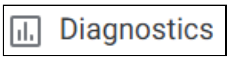
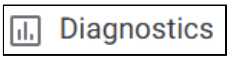
For the Agent to start collecting diagnostic information, you need to switch it to diagnostic mode.

**To enable the diagnostic mode:**

1. Go to the **Agents** section. Select one of the methods:
   - If you need to enable the mode for a single Agent:
     i. Hover over the row with the Agent and click  at the end of the row.
     ii. Click **Enable diagnostic mode**.
   - If you need to enable the mode for several Agents:
     i. Select  the Agents you need. Or click  on the tile at the top of the Agents list to select all Agents at once. At the bottom of the screen, a panel will appear. It contains the number of selected Agents and control buttons.
     ii. Click  **Enable diagnostic mode**.
     iii. To hide the tile, click .

You can download collected diagnostic data as an archive with files.

**To get an archive with diagnostic data:**

1. Enable the diagnostic mode for all the Agents you need.
2. Collect diagnostic data in one of the following ways:
   - If you need to collect data for a single Agent:
     i. In the **Agents** section, hover over the row with the Agent and click  at the end of the row.
     ii. Click **Collect logs**.
     iii. In the upper-right corner, click .
   - If you need to collect data for several Agents:
     i. In the **Agents** section, select  all Agents or the Agents you need.
     ii. Enable the diagnostic mode.
     iii. In the upper-right corner, click .
     iv. In the **Manage diagnostics** window, at the beginning of the Agent row, click .
3. Wait until the data is collected and the  status appears for the selected Agents.
4. At the beginning of the Agent row, click  **Download logs**.
5. To close the **Manage diagnostics** window, click  in the upper-right corner.

Before you download diagnostic data from the server, it is stored in the `/opt/iw/dmserver/AgentLogs` directory. Access to the directory is restricted.

**To disable the diagnostic mode**:

1. Go to the **Agents** section.
2. Select all Agents or the Agents you need.
3. On the panel that appears in the bottom of the screen, click **Disable diagnostic mode**.

or

1. Go to the **Agents** section.
2. Hover over the row with the Agent and click at the end of the row.
3. Click **Disable diagnostic mode**.

**To delete diagnostic data**:

1. Hover over the row with the Agent and click at the end of the row.
2. Click **Delete logs**.

**Note:**

You can delete only verbose diagnostic data and only for Windows Agents. In this case:

- data of Device Monitor processes is not deleted;
- to successfully delete data of other applications, the application processes must be terminated;
- diagnostic data is unavailable for download if a policy is running.

### 11.9.6 Assigning the "Golden image" Status

To assign the *Golden image* status to the Agent:

1. In the **Agents** section, hover over the row with information about the Agent.
2. At the end of the row, click .
3. Select **Assign Golden image status**.

To remove the *Golden image* status, repeat the steps and in step 3, select **Remove Golden image status**.

### 11.9.7 Starting and Stopping Agents

**Important!**

You can start and stop Agents installed on workstations running the following OS: Windows, macOS, and Linux.
The System may not intercept processes launched before the Agent was restarted. For correct operation, you need to restart the computer with the Agent.

**To stop the Agents:**

1. Hover over the row with the Agent and click at the end of the row.
2. Click **Stop agent**.

or

1. In the **Agents** section, select the Agents you need. Or click on the tile at the top of the list to select all Agents at once.
2. On the panel that appears in the bottom of the screen, click .

**To start the Agents again:**

1. Hover over the row with the Agent and click at the end of the row.
2. Click **Start agent**.

or

1. In the **Agents** section, select the Agents you need. Or click on the tile at the top of the list to select all Agents at once.
2. On the panel that appears in the bottom of the screen, click **Start agents**.

**To reboot the computer with the Agent:**

1. Hover over the row with the Agent and click  at the end of the row.
2. Click **Reboot PC**.

### 11.9.8 Removing Agents

To remove an Agent from the security schema:

1. Hover over the row with the Agent and click  at the end of the row.
2. Click **Remove from system**.

The Agent will be removed from all groups and policies.

**Important!**

Removal is not available, if:

- the Agent was added as a result of synchronization. Such Agents can only be removed when the synchronization is removed;
- the configuration is being edited by at least one of the System users;
- synchronization with Active Directory is running.

### 11.9.9 Distribution Policies

In the **Agents** section on the **Distribution** tab, you can manage installation, update, and removal. You can apply policies to selected computers and groups, start them manually, and run them until stopped. If multiple policies are distributed to a single computer, the policy with the higher priority takes effect.

#### Working with policies

To **create** and **run** a policy:

1. In the upper-right corner, click **+ Create policy**.
2. In the **Create policy** window:
   - select policy type: *Install and update* or *Delete*;
   - enter the policy name.
3. Click **Create**. The policy will be displayed on the left in the **Distribution policies** list.
4. Click the policy in the list. On the right, you will see a panel with the following tabs:
   - Configuring policies:
     - Policy parameters
     - Composition
     - Launch options (available only for the installation and update policy)
   - viewing the workstation list, the policy execution status, and details:
     - Computers
5. After completing the policy configuration, click **Save** and **Run**.

To **edit** a policy, select it in the list, make changes, and click **Save**.

To **run**/**stop** or **delete** a policy:

- select the policy name in the list, click  to the right of the name, and select the required action; or
- open the policy editing window by clicking its name in the list, and on the top panel select the required action.

**Note:**

If the task execution results in the **Error** status, you can view detailed information by opening the `/var/log/iwdms/webapi-<date>.txt` log file on the server. `<date>` is the task start date. To get records in the log, make sure that the `Verbose` logging level is set in the `MinimumLevel` section of the `/opt/iw/dmserver/webapibin/webapi.appsettings.json` file.

**Note:**

Policy priority is determined as follows:

- deletion policies have higher priority than installation and update policies;

- to increase/decrease the priority of an installation and update policy, move it to the beginning/end of the list.

"Policy Parameters" Tab

Enter the policy name and add a description.

For installation and update policies: by default, the System distributes the last available Agent version. To specify an earlier version, turn off the **Latest version** toggle and enter the version in the field on the right.

> **Note:**
>
> All available versions are located in the `/opt/iw/iwdistribution/bin/SetupPackages/` directory.

"Composition" Tab

On the **Composition** tab, add workstations and/or groups to which the policy should be distributed. To do this, click **Manage policy membership** and select the method:

- *Set up list*
  In the window that opens, you can see the computer list for installing the Agents. The list displays computers from the available integration with Active Directory or from previously added computers of the Device Monitor Group (see Setting up Computer Group Membership). The computers are displayed with their full names.
  a. Select the workstations in the *Computers* area and click . When adding a group, only computers from the selected group are added, excluding computers in subgroups. You can use the search field to quickly find the computer and add it to the task. Enter at least 3 and no more than 64 characters.
  b. Click **Apply**. In the area with the task name, the list of computers will be displayed with their full names specified for installing Agents. If the Agents were not previously installed on the specified computers, or if the Agent versions are lower than the version specified in the task, then after the task is started, the Agents will be installed or updated.
  c. To delete mistakenly added addresses, hover over them and click .
- *Add manually*
  In the window that opens, enter the computer DNS name and click **Add**.
  The computer name can consist of any characters from any alphabets specified in Unicode. To enter multiple names, use a semicolon or a line break as a separator.

To clear the computer list, click **Exclude all computers**.

To quickly check whether the policy contains the specific computer/group, use the search field above the list of added computers.

"Launch Options" Tab

For installation and update policy, specify parameters in four subsections.

"Main" subsection

In the **Main parameters** subsection, specify the login and password of the user on whose behalf the task will be launched.

By default, the System uses all distribution points. To specify particular points, click the **All distribution points** toggle and select points from the drop-down list.

"Operating System" Subsection

The subsection contains operating system parameters of workstations to which you plan to distribute the policy. If you do not need to apply the policy to workstations running one of the operating systems, deactivate the **Set parameters** toggle for this OS.

- **Windows**
  Default installation directory: `%ProgramFiles%\Infowatch\DeviceMonitor\Client`. You can change the location of the Agent files.
- **Linux**
  Specify the SSH port. The default value is 22. The minimum value is 1, the maximum value is 65535.
  Specify the privilege escalation mechanism: **sudo** or **su**.

If necessary, for the **su** mechanism, specify the credentials of the user on whose behalf distribution is performed.
If you do not need to enter the credentials, deselect the **Use launch login and password** checkbox.

"Reboot" subsection

Specify whether to wait for a reboot without notification:

- *Do not wait*;
- *Wait*. In this case, specify the number of hours to wait;
- *Wait infinitely*.

Also specify whether to notify the employee about the need to reboot, how often, and with what message.

"Additional" Subsection

If necessary, enter the password to protect against Agent removal (available for workstations running Windows).

The default unique name for the Device Monitor proxy server certificate (Issuer Distinguished name, Proxy Root Issuer DN): `CN=InfoWatch Transparent Proxy Root,C=RU,O=ZAO InfoWatch,OU=TechDep,ST=Moscow`. You can change its parameters. The name must contain the CN (Common Name) field. Fields within the name must be comma-separated.

Using checkboxes, determine whether the following is required:

- install the network traffic interception component;
- cancel installation if receiving the list of applications excluded from interception fails[1].

**Note:**

[1] Starting from Device Monitor version 7.18.5, during the initial installation of the Agent, the installer checks whether the list of applications that should be excluded from interception has been received. If the exclusion list is not received, the installation of this Agent will be stopped.
The check is enabled by default. You can disable it.

"Computers" Tab

The tab displays a list of workstations with the versions of the Agents installed on them and dynamically updated icons of the policy execution status.

You can **filter** workstations by the policy execution status. To do this, select the required values in the **State** filter:

- *Error*
- *Ignored*
- *Planned*
- *Installation is in progress*
- *Success*

You can view the Agent installation log if the policy execution completed with the *Error* status. To download the log, click  **Download error log** in the row of the required workstation.

**Important!**

You can download only the most recent log.
When a computer/policy is deleted, the logs are also deleted.

When you click a workstation, a panel with the following **detailed information** opens:

- policy execution status;
- task type;
- current version and version to install;
- IP address, operating system, and OS bitness;
- error log download button if the policy execution completed with the *Error* status.

## 11.10 Working with File Statistics

To configure control over an employee's actions with files, manage the file statistics configuration.

In the **File statistics** section, you can:

- manage the parameters of the user file statistics configuration;
- include/exclude an application from the user file statistics;
- include/exclude files with specific extensions from interception;

- include/exclude files/folders located at a specific path from interception.

When the rule is triggered, the System generates events and sends them to Activity Monitor.

> **Important!**
>
> To generate and send events to Activity Monitor, you need to set up the Employee Activity Monitoring Rule → *Control actions with files*.
> After the file statistics configuration is changed, it must be distributed to the Agents. To lean more, see Distribution Policies.
> To download/upload a new configuration to the System, go to the **Settings** → **Device Monitor** → **Configurations** section. To lean more, see Configuration.

### 11.10.1 Managing configuration parameters

In the **General** area, you can **configure the following parameters of file statistics**:

1. *Create events for alternate file streams*. The parameter is disabled by default.
   If an application and/or a file system uses not the main (monitored) data stream but alternative ones (metadata related with a file system object), events may not be generated. The System uses this setting to generate information collection events for alternative file streams. For example, to detect an intruder who attaches a file with sensitive information to an allowed file and copies it outside.
2. *Monitor only applications explicitly included in monitoring list*. The parameter is disabled by default.
   Enable the setting if you need to track only the applications that are included in monitoring.
3. *Cumulative session time*. The default value is 30 seconds.
   The setting allows you to control the timing of event generation (in seconds). If Activity Monitor receives many low-level events that do not correspond to user actions, you can increase the cumulative session time. The default value can also be reduced; in this case, the number of events may increase.
4. *Percentage of read data*. The default value is 0.
   Use the setting to reduce the number of system file-open events in Activity Monitor. The higher the value, the fewer such events the System generates.

After making changes, click **Save** in the upper-right corner. If the synchronous editing prohibition is enabled, click **Save** on the information panel (see Configuration Editing Modes).

### 11.10.2 Including/excluding applications from file statistics

**To include/exclude an application from the user file statistics**:

1. In the **General** area, click **Add application**.
2. In the window that opens, select an action with the application: **Exclude** or **Include**.
3. Specify the following parameters:
   - Application name (required parameter)
   - Description
   - Minimum version
   - Maximum version
   - Product name
   - Publisher
   - Path
4. Click **Add**.
5. After making changes, click **Save** in the upper-right corner. If the synchronous editing prohibition is enabled, click **Save** on the information panel (see Configuration Editing Modes).

**To edit an application in the list**:

1. Hover over the application and click .
2. Make changes and click **Add**.
3. After making changes, click **Save** in the upper-right corner. If the synchronous editing prohibition is enabled, click **Save** on the information panel (see Configuration Editing Modes).

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

1. Hover over the application and click .
2. After making changes, click **Save** in the upper-right corner. If the synchronous editing prohibition is enabled, click **Save** on the information panel (see Configuration Editing Modes).

### 11.10.3 Including/excluding files with specific extensions from interception

**To exclude files with specific extensions from interception**, add the extension to the **Do not intercept files with extension** field in the **Interceptions** area.

**To include files with specific extensions to interception**, add the extension to the **Intercept files with extension** field in the **Interceptions** area.

### 11.10.4 Including/excluding files/folders located at a specific path from interception

**To exclude files/folders located at a specific path from interception**, specify the path in the **Do not intercept files located along the path** field in the **Interceptions** area.

Enter folder paths separated by ";" (semicolon). Standard search characters are also supported:

- ? (question mark) – replaces a single unknown character;
- * (asterisk) – replaces any number of characters.

The field value must not contain more than 4000 characters.

**To include files/folders located at a specific path to interception**, specify the path in the **Intercept files located along the path** field in the **Interceptions** area.

Enter folder paths separated by ";" (semicolon). Standard search characters are also supported:

- ? (question mark) – replaces a single unknown character;
- * (asterisk) – replaces any number of characters.

**To avoid collecting information when actions are performed on a folder**, select the **Disable collection if a folder is in use** checkbox. The parameter is disabled by default.

# 12 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. The Software is only for use in your current operational activities. 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:

- fully or partially edit, change, adapt, translate, decompile, disassemble, reverse engineer, create or recreate source code, modernize, correct obvious errors, modify the Software and/or its components, whether in full or in part, or attempt to do so in respect to the Software and/or its components, or create derivative works based on the Software and/or Documentation;
- to use the Software in excess of the licensed number of accounts stipulated in the agreement with your direct licensor;
- 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;
- to use the Software for the purpose of making a profit, let on lease, rent out or assign for temporary use, to provide a subscription to the Software, provide outsourcing services using the Software, 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 or by the written consent of the Copyright Holder;
- allow or provide a link to the distribution copy or a license key to any third party in violation of this Agreement and your Licensing Agreement;
- use the Software to create data or code intended for use by other Software products;
- independently install additional Software applications, replace Software components;
- 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, and its unauthorized transfer to third parties is prohibited. 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.**
You agree that the Software components developed by third-party developers are provided without guarantees of access to updated versions of the components and to other programs, equipment, training certificates or services of third-party developers.

**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:

1. 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;
2. 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