InfoWatch Data Access Tracker. User Guide

12/01/2026

© JSC “InfoWatch”

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

http://www.infowatch.com

Table of Contents

1 Set of documents 5

2 Technical support 6

3 Overview 7

4 Investigation Centre Interface 8

5 Main Page 11

5.1 Dashboards and Widgets 11

5.1.1 Dashboards 11

6 Single Filter 15

6.1 Filters 15

6.2 Managing Single Filter 22

6.2.1 Applying filters 22

6.2.2 Adding and removing filters 23

6.2.3 Filter values 23

6.2.4 Saving and loading filter sets 24

7 Events Section 26

7.1 Adding Events to the Investigation 28

7.2 Viewing and Exporting Event Data 29

7.2.1 Viewing contacts 29

7.2.2 Viewing data in a column 29

7.2.3 Filtering data 29

7.2.4 Exporting event data 30

7.3 Filtering Events by Persons and Contacts 31

8 Analytics Section 33

8.1 Statistics Widgets 33

8.2 Creating, Unloading and Printing Reports with Statistics Data 35

9 Infrastructure Section 37

9.1 Dashboard Tab 37

9.1.1 Widgets of Infrastructure Section 38

9.2 Directory Audit Tab 40

9.2.1 Reports 41

9.3 Group Changes Tab ... 44
9.4 Access to Mailboxes Tab ... 45
9.4.1 Reports ... 46
9.5 File and Folder Access Changes Tab ... 47
9.6 Viewing Reports ... 47
9.6.1 Hide tab menu ... 48
9.6.2 Full-screen mode ... 48
9.6.3 Event details ... 48
9.6.4 Event status ... 49
9.6.5 Grouping and sorting entries ... 49
Sorting entries ... 49
Grouping entries ... 51
9.7 Unloading Reports ... 52
9.7.1 Scheduled reports ... 53
10 Persons Section ... 55
10.1 "Personal Information" Tab ... 55
10.2 Person's Dossier Review ... 56
10.3 Creating, Editing, and Deleting Dossier ... 57
10.4 Dossier Merging ... 58
10.5 Adding Person's Contacts ... 58
10.6 Changing Person's Manager ... 59
10.7 Exporting Statistics from Person's Dossier ... 59
11 Investigation Section ... 60
11.1 Creating and Archiving Investigations ... 61
11.2 Adding Materials to Investigation ... 61
11.3 Collaborative Investigations ... 62
11.4 Editing, Exporting, Printing and Deleting Investigation ... 62
12 Reports Section ... 64
12.1 Tasks for Regular Sending ... 64
12.2 Reports Archive ... 64
13 End-user License Agreement ... 65
14 Glossary ... 69

This guide contains information on how to work with InfoWatch Data Access Tracker (also referred to as the System or DAT) and prepare it for operation. DAT software provides automatic audit results for directory service and mailbox access rights, as well as it enables you to track changes in access rights to filesystem objects.

Who should read this guide

This guide is intended for users who work with the System, that is who configure the System before use, analyze data, investigate cases, etc.

This guide is intended for users familiar with the basics of the Microsoft Windows operating system.

1 Set of documents

InfoWatch DAT documentation includes the following:

- "InfoWatch Data Access Tracker. Installation Guide". The document describes how to install, update and uninstall InfoWatch DAT.
- "InfoWatch Data Access Tracker. Administration Guide". The document contains information on how to configure and prepare InfoWatch DAT for operation.
- "InfoWatch Data Access Tracker. User Guide". The document describes how to work in InfoWatch DAT.

Related documentation for InfoWatch Traffic Monitor includes the following:

- "InfoWatch Traffic Monitor. Installation Guide". The guide describes how to install, configure, update, and uninstall InfoWatch Traffic Monitor.
- "InfoWatch Traffic Monitor. Administration Guide". The guide describes how to administrate InfoWatch Traffic Monitor (database, back end).
- "InfoWatch Traffic Monitor. User Guide". The guide describes how to work with InfoWatch Traffic Monitor (set up configuration, export/import data, create policies for processing objects).
- "InfoWatch Traffic Monitor. Configuration Files Guide". Provides explanations for frequently used configuration files.

2 Technical support

If you have any problems or questions related to the operation of the System, please contact our technical support service:

- If you purchased the product from InfoWatch partner, please contact the technical support service of the partner
- If you purchased the product from InfoWatch directly, please contact InfoWatch technical support at support@infowatch.com.

Technical Support Service is available to assist you Mon-Fri, 7 AM – 9 PM (Moscow time, GMT+3), except weekends and public holidays in the Russian Federation. You can also visit technical support section on our website: http://infowatch.com/support.

3 Overview

Investigation Centre is a web console designed to work with InfoWatch products. You can install one or multiple products in the cluster. Installing all the products allows you to get the most complete information about violations, persons, risks, etc.

DAT provides automatic audit results for directory service and mailbox access rights, as well as it enables you to track changes in access rights to filesystem objects. The product helps detecting potential security risks of your company, such as:

- Privileged group memebership changes;
- Long-term inactivity of accounts;
- Unsuccessful attempts to log into accounts;
- User access to several mailboxes;
- No requirement to periodically change account passwords;
- Disabled account blocking for unsuccessful login attempts;
- Changes in access rights to folders and files.

Besides, you can configure DAT to send notifications on changes of domain directory service groups.

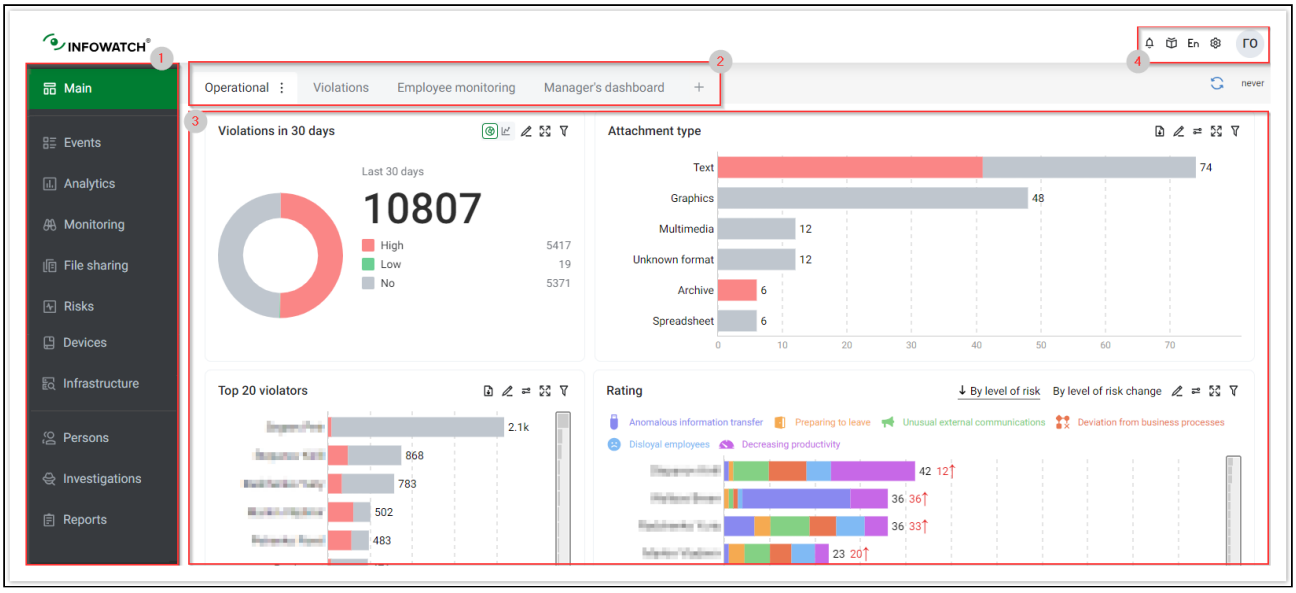
For visual assessment of unauthorized access risks, report-based widgets are available.

4 Investigation Centre Interface

Investigation Centre is a single graphical environment where you view and analyze data from different InfoWatch products you have installed:

- Data Access Tracker;
- Activity Monitor;
- Data Discovery;
- Prediction;
- Vision.

Investigation Centre interface contains several area. Below you can see **Main** page.



Interface elements:

Number in the picture	Window element	Element desription
1	Navigation panel	Working sections of the Investigation Centre. You can hide the Navigation panel by clicking « **Collapse menu** at the bottom.
2	Dashboard panel	The list of preinstalled dashboards
3	Working area	Here you can view widgets of InfoWatch products and work with them
4	User menu	User menu, where you can: • Edit your account • Change your password • Enable hot keys • Find out the contact details of the InfoWatch company and support service • Log out of the System

Number in the picture	Window element	Element desription
	Settings	The Settings section (for details, see "*InfoWatch Data Access Tracker. Administration Guide*")
	Notifications	Notification folder with system notifications for users (for details, see "*InfoWatch Data Access Tracker. Administration Guide*", "System Notifications")
	Change language	Selecting the interface language: *Russian* or *English*
	Guidebook	Investigation Centre Guidebook where you can find: • *System Use Scenarios* that describe how to use the product most efficiently; • *Administration Guide* that describes the product settings; • *User Guide* that describes how to work with the product; • Report on new features (*What's New*).

When working with the Investigation Centre, you can use the following sections:

Section	Description
Main	Contains preinstalled dashboards with widget sets. The widgets allow you to quickly get and display information about violations and violators. Information is displayed based on filters.
Events	This section contains a list of events according to set filters.
Analytics	This section contains statistical information about violations/violators according to set filter. This information is displayed on: • Widgets with graphs, diagrams and tables; • Connection graph with event visualization. *Violation statistics* tab is available to all products. *Connection graph* tab contains InfoWatch Vision functionality (see "*InfoWatch Vision. User Guide*"). *Activity statistics* tab contains InfoWatch Activity Monitor functionality (see "*InfoWatch Activity Monitor. User Guide*").
Monitoring	Monitoring employee activity as well as online monitoring of employee workstations The section of InfoWatch Activity Monitor (see "*InfoWatch Activity Monitor. User Guide*")

Section	Description
File sharing	Creating and running network resource scanning tasks, viewing and analyzing detailed information about files including file owners and searching for file duplicates The section of InfoWatch Data Discovery (see "*InfoWatch Data Discovery. User Guide*")
Risks	Calculation of employee ratings to predict information security risks The section of InfoWatch Prediction (see "*InfoWatch Prediction. User Guide*")
Devices	External storage devices control The section of InfoWatch Device Control (see "*InfoWatch Device Control. User guide*")
Infrastructure	Automatic audit of directory service and access to mailboxes; tracking changes in access rights to folders and files The section of InfoWatch Data Access Tracker
Persons	This section contains a catalog of persons in the company as well as external contacts
Investigations	This section allows you to carry out investigations using accumulated data on violations
Reports	The report directory where you can view the list of earlier created reports and export their files

5 Main Page

The Main Page of the Investigation Centre contains dashboards. These are tools that allow you to get up-to-date information about violations. Dashboards consist of a widget set of one or more InfoWatch products. You can create custom dashboards and add any available widgets to them or select preset dashboard with the most frequently used widgets. The set of available widgets depends on what InfoWatch products you have installed.

Preset dashboards:

- **Operative** – represents key indicators to monitor violations:
  - Graphs with the dynamics of violations for the last 3 days or the last 24 hours, charts with distribution by levels of violations,
  - Top violators among employees who send data,
  - Top most violated security policies,
- **Employee monitoring** – represents statistics of violations involving employees:
  - Top violators among employees who send data,
  - Employee rating (if InfoWatch Prediction is installed),
  - Employee under supervision,
- **Files** – represents the most common files in violations and audit of actions with them:
  - Top triggered protected objects,
  - Top files used in operations,
  - Top file types used in operations,
  - Statistics of actions with files (if InfoWatch Activity Monitor is installed)
- **Violations** – shows anomalies in employee actions, behavior changes, comparative statistics on violations:
  - Graphs with the dynamics of violations for a selected date or period of time, diagrams with distribution by violation levels,
  - Top most violated security policies,
  - Top violators among employees who send data,
- **Manager's dashboard** – presents statistics on employees' actions to the head of the department:
  - Graphs with the dynamics of violations for a selected date or period of time, diagrams with distribution by violation levels,
  - Top violators among employees who send data,
  - Top event types with violations,
  - User decision on events.

5.1 Dashboards and Widgets

5.1.1 Dashboards

Dashboards with widgets are avaialbe on the **Main** page. By default, the Main page contains the *Operative* template. On the working area, the Security Officer can place preset dashboards, create custom dashboards and then add widgets to them. You can use widgets of any installed InfoWatch product.

To add a widget:

1. On the dashboard panel, to the right of the *Operative* template tab, click .
2. Choose one of preset dashboards or **New dashboard**. If necessary, enter the new name and click **Save**. The dashboard will be added to the panel.
3. Click  and select **+ Add widget**.

4. The **Add** window will open. In the list on the left:
    - Specify which widgets and from which installed InfoWatch product you want to add,
    OR
    - Select **All**.

    To quickly find the desired widget by name, use the search bar.
5. Next to the needed widgets, click **+ Add** and specify their number. You can add up to 10 widgets of the same type to the dashboard.
6. If needed, select other widgets you want to add.
7. Click **Apply**. The selected widgets will be added to the working area.

Single Filter conditions specified in other sections of the Investigation Centre do not apply to dashboard widgets on the **Main** page. You can configre any widget regardless of others.

To configure a widget:

1. In the corner of the widget, click .
2. Set the filter values. If necessary, add additional filter attributes (see "Single Filter").
3. Click **Save**.

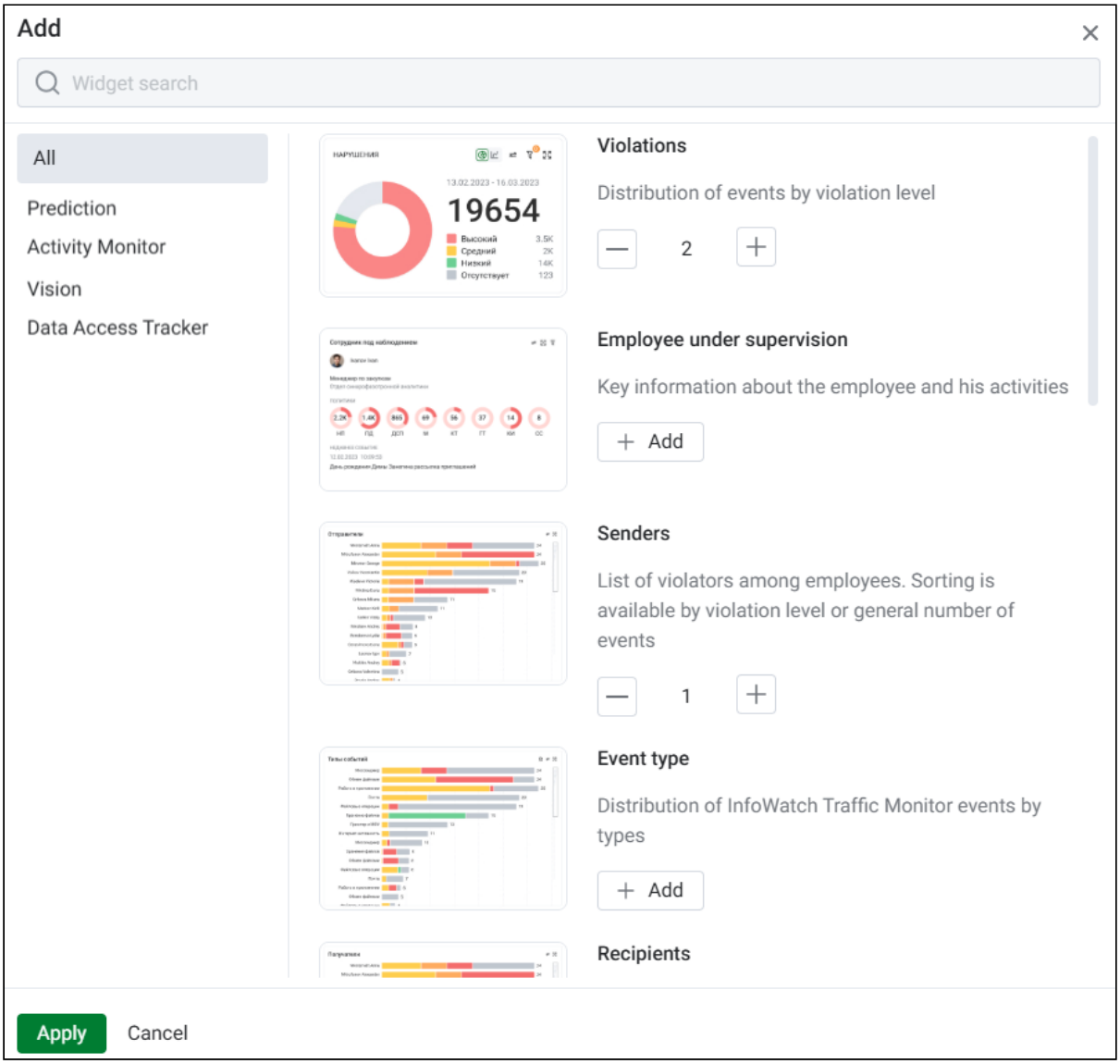
> **Note:**
>
> Data on widgets is updated according to the set interval. To set the update interval, select a value in the right upper corner. You can choose a value from 15 minutes to 1 hour. If you do not want to update the data, click **never**. You can also update data manually. For this, click . Please note that only widgets located in the visible area of the dashboard are updated. To update all data on all widgets, scroll through all widgets on the screen and click .

Widgets

You can place widgets of the **Analytics**, **Risks** and **Infrastructure** sections on dashboards.

> **Note:**
>
> For details on widgets of **Infrastructure** section, see "Dashboard Tab" article.

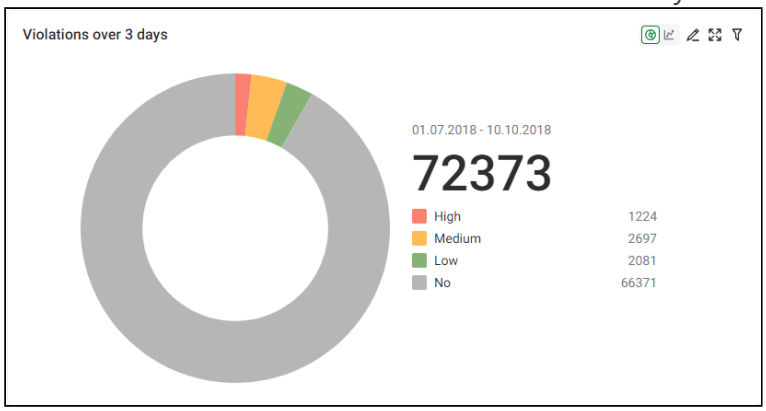
The set of widgets that can be added to dashboards depends on pruducts that are installed in the Investigation Centre cluster.



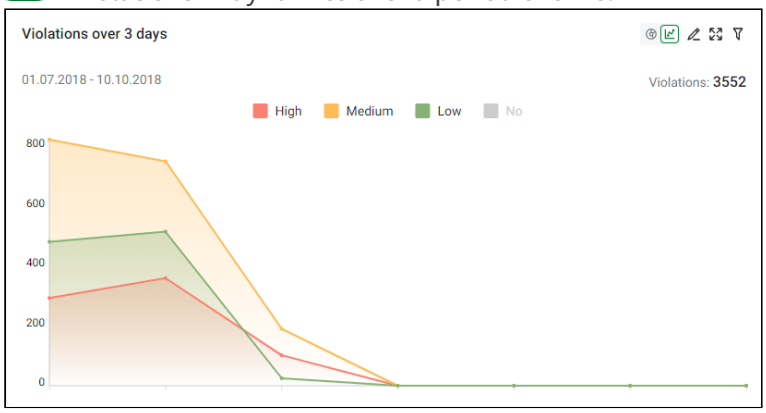
The **Violations** and **Employee under supervision** widgets are available only on the **Main** Page.

This **Violations** widget processes data received from Traffic Monitor and can display:

- – the total number of violations with distribution by their levels:



- – violations in dynamics over a period of time:



In both cases, you can customize the display. For this, use the legend where you can enable or disable graphs of violation levels:



The **Employee under supervision** widget collects information about an employee. Based on this information, the Security Officer can then start an investigation and start monitoring the employee more closely.

To set up the widget:

1. Click and specify attributes for filters that can apply to the widget.
2. In the **Person** filter, specify a person from the list of employees. If necessary, add other filters and specify their values.
3. Click **Save**. The widget will display:
   - Personal information about the employee and security policies, which include the employee. The widget can contain up to 8 policies with the most events with a high violation level,
   - The latest event related to the person, with the data, action and policy,
   - Other persons from events related to the employee.
4. Click if you want to change the widget display:
   - Employee photo size,
   - Diagrams of policies with high violation level.

6 Single Filter

A Single Filter is a universal tool that allows you to manage your searches and data display in InfoWatch Investigation Centre.

Using the Single Filter, you can:

- Save various sets of filters to quickly get required information;
- Exclude some data from analysis to get only specific information.

Important!

When working with the Single Filter, please keep in mind that:

- All settings of the Single Filter apply only within one browser tab,
- Clicking the **Back**/**Forward** browser tabs returns the filter to the state it was in at that step,
- When you log out of the System, all filter attributes are reset to their original state.

6.1 Filters

The Single Filter is a panel that contains a group of filters.

Note:

For details on filter panel configuration, see "Managing Single Filter".

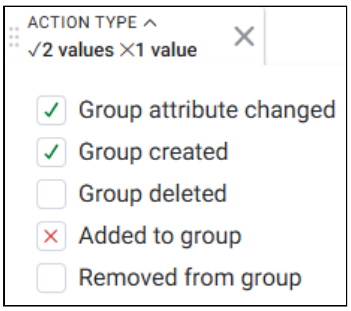
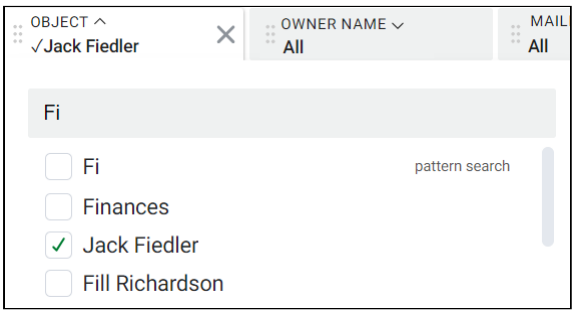
Filters on the tabs of the *Infrastructure* section

Note:

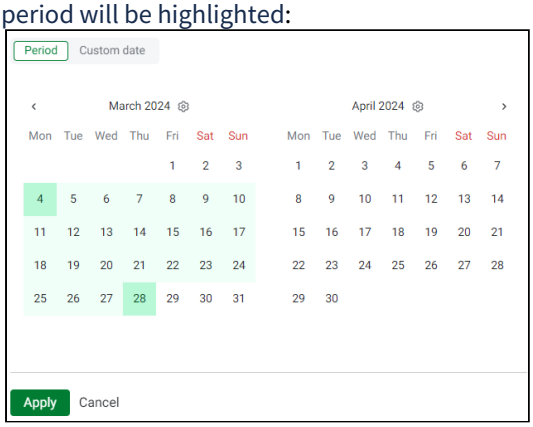
Data Access Tracker filters (except for *Date* filter) are unique and work only in **Infrastructure** section. Their values are not transferred when switching to other section and affect only Data Access Tracker data filtering.

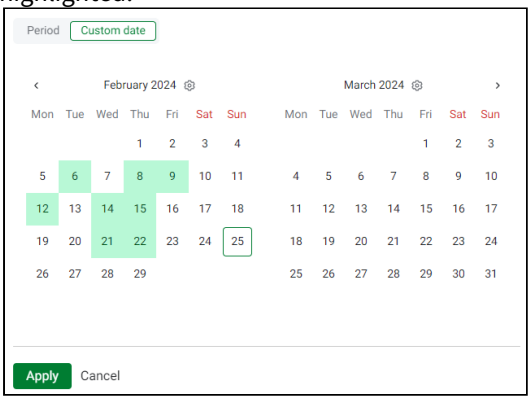
A user who has access to **Infrastructure** section can use Data Access Tracker filters without any additional settings.

Filter	Description	Setting values
Service account	Account used for execution of services or applications	You can leave only accounts with the specified value in the report. Available values: *No*/*Yes*
Viewed	Whether an acount has been marked as viewed	

Filter	Description	Setting values
Username	The name of a user whose account is included into the report	You can view entries which contain one or several values of an attribute, or, conversely, exclude entries with specific values. For attributes with multiple values, you can use the following flags: • ☐ – the value is not selected • ☑ – the value is included in filtering results • ☒ – the value is excluded from filtering results When specifying values for a filter attribute, you can combine conditions with different flags:  In case there are too many filter values, start entering the value you need into the searchbox and choose from selected options.  **Note:** Value search is available for the following filters: • On **Dashboard** tab: *Username*; • On **Directory audit** tab: *Changed by*, *Username*;

Filter	Description	Setting values
Computer name	Name of a computer on which edits were made	• On **Group changes** tab: *Changed by*, *Object*, *Group*; • On **Access to mailboxes** tab: *Mailbox address*, *Owner*, *Mailbox type*, *User/group*. • On **File and folder access changes** tab: *Changed by*, *Computer name*, *Network share*, *Local path*, *Account with access.*
Group	Name of a modified group	
Action type	Type of an action done with a directory service object	
Changed by	User account on whose behalf changes were made	
Object	Directory service object which was created, changed, added, removed from a group or deleted.	
Account with access	User (group/computer) whose access rights to a file/folder were changed. **Note:** Accounts or groups removed from Active Directory are displayed with gray font color.	
Access rights type	User's access level to the file/folder: *Filesystem* or *Network*	
Network share	Name of a network folder with updated access rights	
Local path	Path to the folder with updated access rights	
Logon error	Logon failure reason: You can adjust the table so that it displays only events with selected logon errors. Available values: • *No servers available* • *Invalid username* • *Invalid password* • *Invalid credentials* • *Unauthorized logon time* • *Unauthorized computer* • *Disabled account* • *Unavailable logon type* • *Netlogon service not started* • *Expired account* • *Logon blocked by firewall*	

Filter	Description	Setting values
	• *Password change required* • *Locked account* • *No account data in local store* • *System error* • *Insufficient system resources* • *Time out of sync* • *Expired password*	
Mailbox address	Address of a shared mailbox	
Owner	Active Directory user who owns the mailbox	
Mailbox type	MS Exchange mailbox type	
User/ group	Account/group that has access to other users' mailboxes	
Date of the directory service event	The time period for which you want to get data: • *Last 24 hours*; • *Current day;* • *Last 3 days;* • *Last 7 days;* • *Last 30 days;* • *Current month;* • *Last month;* • *Custom period* (you can select the start and end dates of the period or separate dates):	Select the time period or specify a custom period/ list of custom dates. • **To specify a custom period** 1. Use your mouse to select the start and end dates in the calendar. The selected time period will be highlighted:  2. Click **Apply**. **To specify one or more custom dates** 1. Use your mouse to select one or more dates in the calendar. The selected dates will be

Filter	Description	Setting values
Account **creation date** **Last logon date** **Previous logon date**		highlighted:  2. Click **Apply**.

After you select one or more attributes, the System will calculate the number of matching events. The following reports will be rebuilt:

- Tables and widgets in **Infrastructure** section;
- Diagrams, graphs, and tables in **Violation statistics** section;
- Event data table in **Events** section;
- A table with persons' data and widgets in **Persons** section.

Filters in the *Events* and *Analytics* → *Violation statistics* section

The table contains filters and widgets that are available in the **Events** and **Analytics** → **Event statistics** section.

Note:

The following widgets listed in the table below are available by default:

- *Date*
- *Senders*
- *Event types*
- *Violation level*
- *Recipients*

Note:

Value search is available for the following filters:

- In **Events** section: *Status*, *Department*, *Group, Event type, Protected object, Policy*, *Person*, *Perimetr*.
- In **Analytics** → **Violation statistics** section: *Status, Department, Group, Event type, Protected object, Policy, Person.*
- In **Persons** section: *Person*, *Job title*, *Status*, *Department*, *Group.*

Important!

To make data filtering available, make sure that the user role has access to **Events** and **Analytics** → **Violation statistics** section. For more information about configuring roles, see "*InfoWatch Data Access Tracker. Administration Guide*" document, "System Setting" section, "Roles" article.

Filter name	Description and possible values
Date	See Date filter in the table describing the **Infrastructure** section filters.
Violation level	The **Violation level** widget corresponds to this attribute. Select a violation level (complies with the similar one in Traffic Monitor): • *High* • *Medium* • *Low* • *No*
Event type	The **Event type** widget corresponds to this attribute. Create event type sampling. For this, select the event type in Traffic Monitor: • *Work with applications:* • *Clipboard* • *Keyboard input* • *Mail:* • *Mail on client* • *Webmail* • *Printer and MFD:* • *Printing* • *File storage:* • *Data Discovery* • *Web activity:* • *Web message* • *Messenger:* • *Facebook* • *ICQ* • *MS Lync* • *Mail.Ru Agent* • *MS Teams* • *Skype* • *Telegram* • *Viber* • *WhatsApp* • *VK* • *XMPP* • *Yahoo!* • *File exchange:* • *Cloud storage*

Filter name	Description and possible values
	• *Removable device* • *FTP* • *Network resource* • *Terminal session* • *File operations:* • *Read file* • *Write file* • *Others:* • *Photography* • *SMS*
Protected objects	The **Protected object** widget corresponds to this attribute. Select values from the list of protected objects created in Traffic Monitor.
Policy	The **Policies** widget corresponds to this attribute. Select values from the list of policies created in Traffic Monitor.
Contact type	The filter enables displaying contacts by different types of contacts used in the System. Select one or more values: • *Fired* – filter by events where one of participants is a former employee. If personal contacts of the employee were not automatically added during integration with other systems, they should be added manually (for details, see "Adding Person's Contacts"), • *External* – filter by events where at least one participant is not from an internal domain, • *Internal* – filter by events where at least one participant is from an internal domain, • *New* – filter by events where a given identified or unidentified contact received from Traffic Monitor appears for the first time on the exact date or during the time period specified in the ***Date*** filter, • *Personal* – filter by events containing messages sent to personal addresses, including emails sent by one employee to a personal address of another employee, • *Self sent* – filter by events where the sender and the recipient is the same person. When selecting *Personal* and *Self sent* at a time, then the System will display the events with emails sent by the employee to their own personal address
Perimeter, In perimeter, Out of perimeter	Select a perimeter from the list. Set a modifier, if needed: • *Perimeter* – search through all the events that have specified perimeters as their attributes, • *In perimeter* – search through the events that have specified perimeters in the **In perimeter** attribute, • *Out of perimeter* – search through the events that have specified perimeters in the **Out of perimeter** attribute.

Filter name	Description and possible values
	Selecting *Unknown perimeter* will find the events for which entering or leaving the perimeter was not identified in Traffic Monitor.
Person*, Sender*, Receiver*	The filter allows you to display events with specified persons as participants. You can specify either the employee's name or their contacts in the search bar. Additionally, you can set the filter using these modificators: • **Contains value** – events with at least one selected person are displayed; • **Exact match** – events containing all selected persons are displayed.
Group*, Group of receivers*, Group of senders*	The **Analytics by groups/persons** widget corresponds to this attribute. It creates a selection of AD and Traffic Monitor groups. Specify groups within the company hierarchical structure that are synchronized from Traffic Monitor and Active Directory.
Department*, Department of senders*, Department of receivers*	Specify all the company's departments synchronized from Traffic Monitor or AD you are interested in.
Status*, Status of senders*, Status of recipient*	Specify all the employee statuses synchronized from Traffic Monitor or AD you are interested in.
* – For person-related attributes, you can set the following modifiers: • *Any* • *Sender* • *Receiver* If you set the *Sender/Receiver* modifier, then selected persons, person groups or contacts will be considered as senders or recipients in events. If you set *Any*, all participants of the event will be selected: all persons, person groups and contacts.	

6.2 Managing Single Filter

6.2.1 **Applying filters**

To **apply** a filter, click  in the filter field and specify the value. The table will display only the lines which satisfy the value of the filter.

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

6.2.2 Adding and removing filters

You can use one or more filters on the filter panel.

To add a filter to the panel:

1. Click .
2. Select a filter from the list.
3. Click outside the filter list window.

The filter will be added to the filter panel.

To remove a filter from the filter panel:

1. Click .
2. Deselect the filter in the list.
3. Click outside the filter list window.

The filter will be removed from the filter panel.

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

To hide the Single Filter panel, click .

6.2.3 Filter values

You should select at least one value in the filter. If you do not select any value, the default value will be used.

> **Important!**
>
> When you log out from the System, filter values are reset. We recommend saving filters before logging out (see "Saving and loading filter sets").

A condition with multiple filters

If you set values for multiple filters, then the conditions of these filters are combined using logical "AND"

Example:

Set values for multiple filters:

- In the **Event date** filter, set the value: *Last month*;
- In the **Violation level** filter, set the value: *High*.

As a result, the table with events will display only entries with high violation level over the past month.

Including and excluding filter values

The following states are available for filter values:

-  – The value is not selected (default state),
-  – The value is included,

-  – The value is excluded.

To change the state of the value, click the state box.

You can include and/or exclude multiple values. In this case:

- Multiple included values are combined using logical "OR",
- Multiple excluded values are combined using logical "OR",
- A condition of multiple included values and a condition of multiple excluded values are combined using logical "AND".

Resetting filter values

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

To reset values for all filters, click .

6.2.4 Saving and loading filter sets

To be able to use specified filter values later, you can save them in catalogues of one of the type:

- *Personal* – the catalogues and their contents will be available only to the user who created them;
- *General* – the catalogues and their contents will be available to all users of the System.

To save a filter:

1. Set the required filter values and click .
2. In **Save filter** window, specify the filter name.
3. Select the type of the catalogue to which the System will save the filter: *Personal* or *General*.
4. Select a catalogue that will contain the filter or create a new one. To easily find a catalogue, search by its name.

   > **Note:**
   >
   > If you do not select a catalogue, the System will save the filter to the root directory of the specified catalogue type.

5. Click **Save**.

To use a previously created filter:

1. In the Single Filter area, click **Saved filters**.
2. Open the catalogue that contains the required filter.
3. Click the filter to activate it.

To edit catalogues and filters:

1. In the Single Filter area, click **Saved filters** or the name of the applied filter.
2. Click  above the filter list.
3. In **Set up filters and catalogues** window, you can:
   - Change the catalogue hierarchy by dragging;
   - In the catalogue type line:
     -  Create a catalogue;

- When hovering your mouse over the catalogue name:
  -  Rename the catalogue;
  -  Create a child catalogue;
  -  Delete the catalogue;
- Drag filters inside and between catalogues;
- When hovering your mouse over the filter name:
  -  Rename the filter;
  -  Record current filters under this name;
  -  Delete the filter.

Keep in mind that the Main Officer can edit and delete both personal and general catalogues and/or their contents, while other Security Officers can edit and delete only personal catalogues and/or filters.

7 Events Section

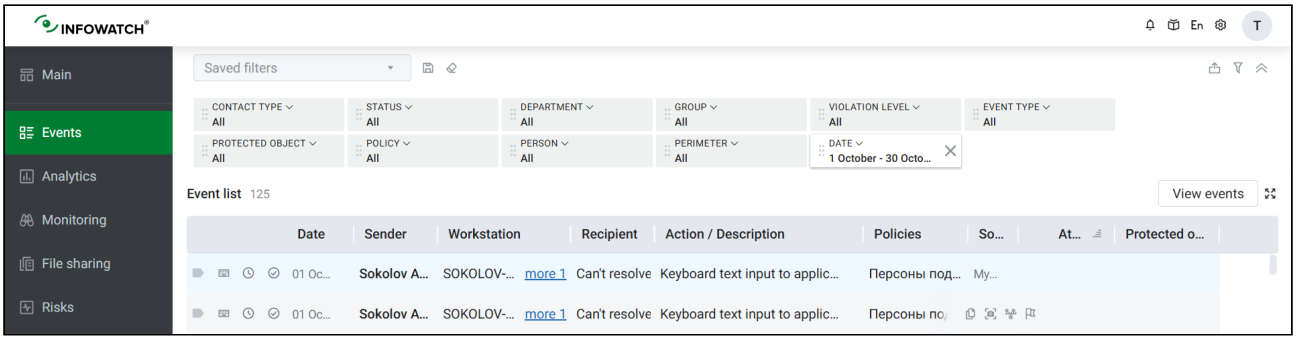
> **Note:**
>
> DAT does not use events from Traffic Monitor.

In this section, you can view data of events uploaded to the Investigation Centre after synchronization with Traffic Monitor:

- Violation level
- Event type
- Security officer's decision on the event
- The System's verdict on the event
- *Date* – event creation date in Traffic Monitor
- *Sender* – a person who committed the violation
- *Workstation* – computers involved in the event
- *Recipient* – persons who received data from the sender

> **Note:**
>
> The icon next to the *Sender* or *Recipient* indicates that this is a new contact who appeared in the System on the date/time period specified in the **Date** filter.

- *Attachments* – whether the event has files attached, their name and size
- *Action/Description* – sent data description and action taken
- *Policies* – policies that triggered on this violation type
- *Protected objects* – protected objects that were sent
- *Source/ID in source* – event ID in Traffic Monitor



Use the filters on the Single Filter panel to select the events you need. For details, see "Single Filter". Events are displayed as a table.

To get extended information or analysis of a selected event, you can:

- Click at the bottom of the event list. Together with the main data of the event, the System will display other data such as messages in the chat, message text, attached images. In event details, the System highlights words related to protected objects detected;
- Click to switch to the dialogue-viewing mode in messengers (available if you have Vision installed);

- Click  to add an event to a new or earlier created investigation;
- Click  to view event on the connection graph (available if you have Vision installed);
- Click  to copy the event ID to quickly find it in Traffic Monitor;
- Click  to open a new tab with the event screenshots (available if you have Activity Monitor installed);
- Click  to open a new tab with the event on the timeline of the person (available if you have Activity Monitor installed).

To view events in Traffic Monitor:

1. In the list, select events using:
   - ***Ctrl*** key to select required events one by one;
   - ***Shift*** key to select a range of events (from – to).
2. On the above panel, click:
   -  to build a specific connection graph with the selection (available if you have Vision installed);
   -  to start investigation with the selected event parameters (see "Adding Events to Investigation");
   - **View events** to open the **Events** section of Traffic Monitor for detailed analysis. The section will display only 300 events of all events filtered by the Investigation Centre. If events belong to several sources, then events for each source will open in a separate browser tab.

     To deselect events, click  **Reset selected events**.

Tip:

If you often switch between the Investigation Centre and Traffic Monitor, we recommend configuring pass-through authentication, which allows you to avoid re-entering your username and password. For details on how to configure it, see "*InfoWatch Traffic Monitor. Administration Guide*", section "*Configuring Single Sign-On in InfoWatch products*".

Note:

Table columns with events are displayed according to the role assigned to the user. So it is necessary to grant the user required access rights:

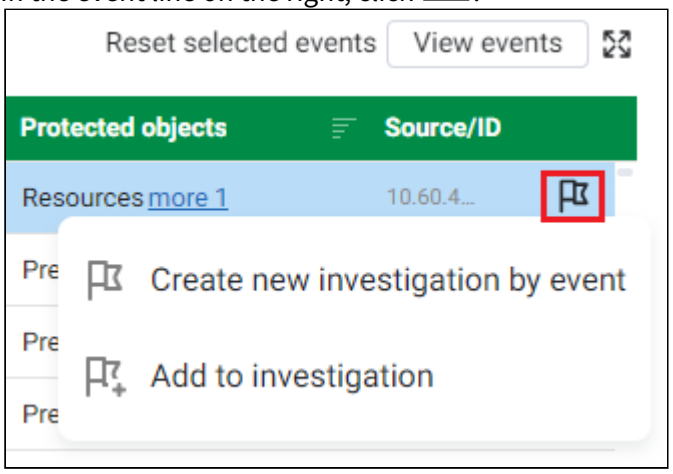
- to view the *Date*, *Event type*, *Sender*, *Recipient* columns, select the **Events** and **Violation statistics** checkmarks on the **Functions** tab of the role settings;
- to view *Description*, *Attachments*, *Source*, *Event ID* columns, enable **Event details**;
- to view *Violation level*, *User decision*, *Verdict* columns, enable **Violation details**;
- to view *Policies*, *Protected objects*, *Perimeters* columns, enable **Policies**, **Protected objects** and **Perimeters**.

7.1 Adding Events to the Investigation

You can add any events from the list to an investigation or creare a new investigation based on the events.

To add an event to an investigation:

1. Click on the required event in the list.
2. In the event line on the right, click .



3. Choose:
   - **Add to investigation**. Then:
     a. Start typing the name of the investigation to which you want to add the event.
     b. Choose the investigation from the drop-down list.
     c. Click **Add**.
     OR
   - **Create new investigation**. In this case, a new investigation will be created automatically.

To add one or more events to an investigation:

1. Select required events using *Ctrl* or *Shift* keys.
2. On the right side of the screen above the event table, click:
   - **Add to investigation**. Then:
     a. Start typing the name of the investigation to which you want to add the event.
     b. Choose the investigation from the drop-down list.
     c. Click **Add**.
     OR
   - **Create new investigation**. In this case, a new investigation will be created automatically.

Events that are involved in investigations are marked with . Such events can be added to new or already existing investigations.

To switch to an investigation from the event:

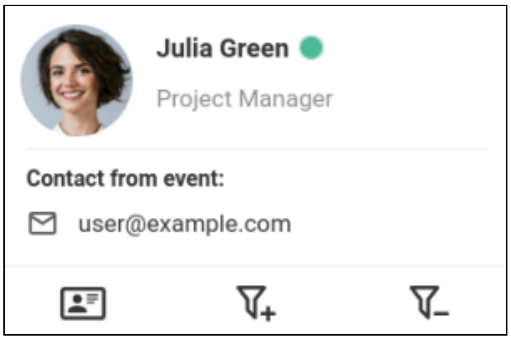
1. Click .
2. Select an event from the list. It will open on a new browser tab.

To view events that are included in investigations, use the **Investigations** filter (for details, see "Single Filter").

7.2 Viewing and Exporting Event Data

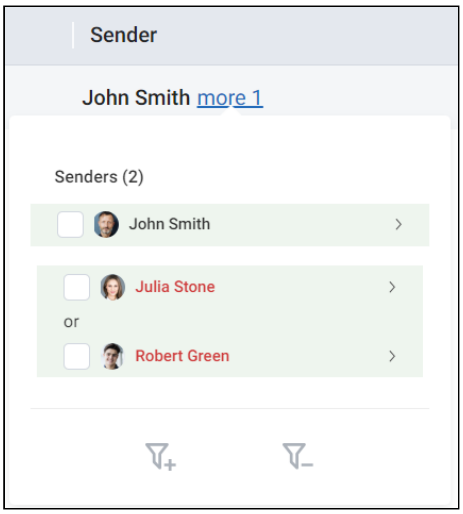
7.2.1 Viewing contacts

The person card in the **Events** section contains contacts of employees who were involved in the selected event:



7.2.2 Viewing data in a column

In case a column contains several objects, their list is collapsed. To expand the list, click **more**. You will see the list of all objects in this column:



7.2.3 Filtering data

You can add one or more objects to the filter. The list will include events with these objects only. For this, select the objects and click  to add them to the filter or  to exclude events with these objects from the list.

> **Note:**
>
> You can view data and filter it by column values only in the following columns: **Recipient**, **Sender**, **Attachments**, **Policies**, **Protected objects**.

Note:

For correct operation, you should allow pop-up windows from specified sources to open in the browser.

7.2.4 Exporting event data

Export event data if you need to report an incident, conduct an investigation or to make a compilation of events. You can export event data table to Excel or save it to the dossier. To export data:

1. In **Events** section, set values of the filter attributes. The event list will be updated.
2. At the top right of the screen, click  → **Unload report**.
3. Select what you want to add to the report and click **Save**.
4. Wait for the report to be generated.
5. Go to **Reports** section and click the link to download an XSLX report file.
6. Open the XLSX file. The **Additional information** sheet contains the date and time the report was created, applied filters and their values, as well as the link to the section where the report was created. The **Event list** sheet contains the event table. You can edit the table manually if necessary.

To set up regular sending:

1. Select values of the filter attributes. The event list will be updated.
2. Click  → **Configure regular sending**.
3. Select what to include in the report and specify the following parameters:

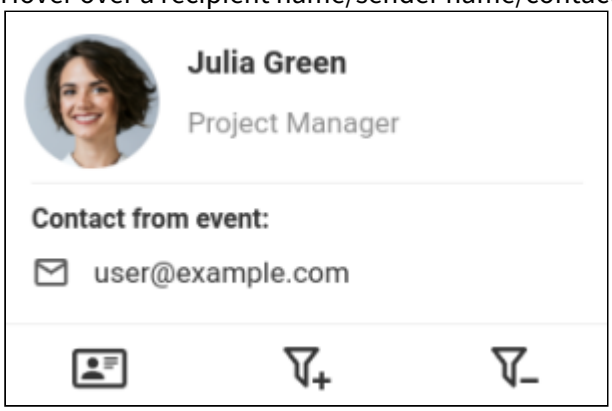
Parameter	Description
Report creation period	Specify a period for which to send the report: • Current day • Last 24 hours • Last 3 days • Last 7 days • Last 30 days
Receivers	Specify receivers of the report
Sending frequency	Specify how often the Security Officer will get reports: • Daily • Weekly • Monthly
Time	Specify the time when to send the report

4. Click **Save**. A task for regular sending reports will be created. You can view the list of such tasks on **Tasks for regular sending** tab of **Reports** section. For details, see "Tasks for Regular Sending".

7.3 Filtering Events by Persons and Contacts

To filter events by required recipients or senders:

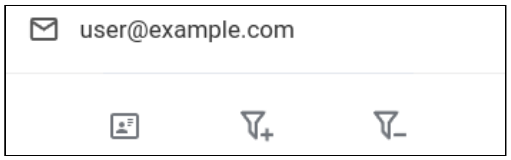
1. Hover over a recipient name/sender name/contact.



2. Click:
   -  – the recipient /sender will be added as an included attribute of the **Person** filter, and then the list of events will be updated;
     OR
   -  – the recipient /sender will be added as an excluded attribute of the **Person** filter, and then the list of events will be updated.

To filter events by undefined contacts:

1. Hover over an undefined contact in the event:



2. Click either of the following:
   -  – the contact will be added as an included attribute of the **Contacts** filter, and then the list of events will be updated;
     OR
   -  – the contact will be added as an excluded attribute of the **Contacts** filter, and then the list of events will be updated.

To assign an unidentified contact to a person:

1. Hover over an undefined contact in the event.
2. Click .
3. If you need to create a new dossier with this contact:
   a. Click **Create dossier**.
   b. Enter all required data as described in "Creating, Editing, and Deleting Dossier".
4. If you need to add the contact to an existing dossier:
   a. Click **Add to dossier**.

b. Select the dossier of the required employee and click **Add**.

8 Analytics Section

The **Analytics** section provides the Security Officer with visual statistics in the form of tables, charts and graphs. These are built according to specified conditions of the Single Filter and based on all events received from Traffic Monitor. The section contains the following tabs:

- **Incident statistics** – statistics widgets (see "Statistics Widgets");
- **Connection graph** – the Vision Connection Graph (see *"InfoWatch Vision. User Guide"*);
- **Activity statistics** – the Activity Monitor widgets (see *"InfoWatch Activity Monitor. User Guide"*).

8.1 Statistics Widgets

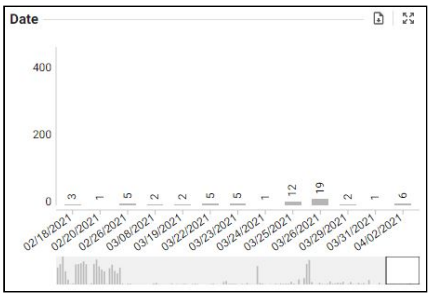
Widgets on the **Violation statistics** tab display the data from Traffic Monitor stored in the System.

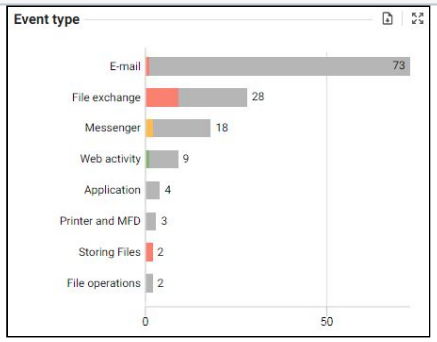
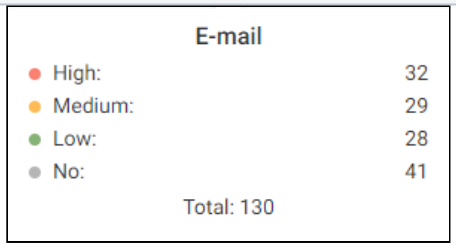
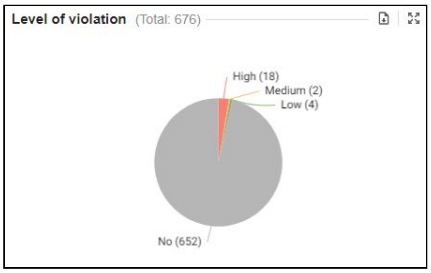
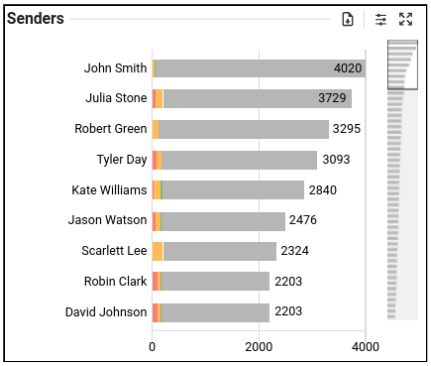
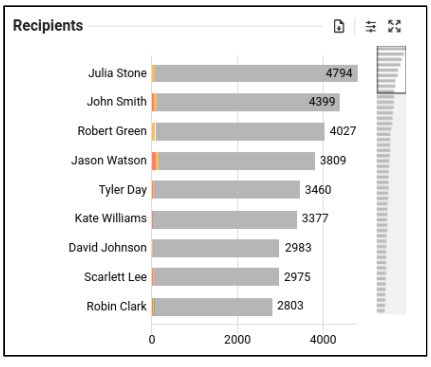
Note:

In the table below, you can find statistics widgets that are always available:

- date
- event type
- level of violation
- senders
- recipients

Other statistics widgets are available only if Vision is installed in the cluster.

Widget name	Description
Date 	Displays the events distribution by specified dates according to violation levels. You can specify one or more dates and filter events for the specified day
Event type	Displays the distribution of Traffic Monitor events with different violation levels by types. **To get extended information:** When hovering over a source name, detailed information on the number of events with different violation levels is displayed:

Widget name	Description
	
Level of violation 	Displays the distribution of events by violation level
Senders 	Displays the list of persons with the highest number of violations. The first 50 top violators sorted by events with highest violation levels are displayed. **To customize the widget display:** 1. In the corner of the widget, click ⇄. 2. In the window that opens, specify: a. the number of senders to be displayed: from *3* to *20*; b. how to sort them: *by violation level* or *by the total number of events* 3. Click **Save**.
Recipients 	Displays a list of recipients, identified or unidentified, who are involved in events. The first 50 most popular contacts are displayed. **To add a contact from the event to the filter:** 1. Select a contact in the event with a mouse pointer. 2. Click ⊽+. The selected contact will be added to the Single filter, and the data on the events will be rebuilt accordingly. To exclude a contact from filter, click ⊽−. **To add an unknown contact to a dossier:** 1. Hover over an unknown contact in the diagram.

Widget name	Description
	2. Click . 3. Enter the data as described in "Creating, Editing, and Deleting Dossier".

8.2 Creating, Unloading and Printing Reports with Statistics Data

You can export data from widgets as a report and configure regular sending of reports.

To create and export a report as an XLSX file:

1. Specify all required values of the filter attributes so that the System would display the necessary data.
2. Click  → **Unload report**. The report will be saved to the log. It will include data from all widgets that were in the working area when the report was being generated.
3. In **Report unloading** window, you can choose which data to include to **Detailed** report, which contains data from widgets in the form of tables.
4. If you want all widgets to be included in the report, set  next to **Pages to unload** option.
   If you need only specific widgets to be included in the report, set  next to their names.
5. Click **Save**. A message will appear on the screen indicating that the report is being saved.
6. Go to **Reports** → **Reports archive** section.
7. Click  next to the report. An XLSX file with the report will be saved to your computer's hard drive.

A downloaded report is an XLSX file with several sheets. On the **Additional information** sheet, you can find the date and time when the report was generated, applied filters and the link to open the section where the report was created. Each subsequent sheet contains text information from widgets that were displayed in the working area when the report was being created.

To set up regular sending:

1. Select values of the filter attributes. The event list will be updated.
2. Click  → **Configure regular sending**.
3. In **Report unloading** window, define what will be included in **Detailed** report. The report includes data from widgets in the form of tables.
   To include all widgets, set  next to **Select all** option.
   If you want to add only particular widgets to the report, click  next to their names.
4. Specify the following parameters:

Parameter	Description
Report creation period	Specify a period for which to send the report: • *Current day* • *Last 24 hours* • *Last 3 days* • *Last 7 days* • *Last 30 days*

Parameter	Description
Receivers	Specify receivers of the report
Sending frequency	Specify how often the Security Officer will get reports: • *Daily* • *Weekly* • *Monthly*
Time	Specify the time at which the System will send the report

5. Click **Save**. A task for regular sending reports will be created. You can view the list of such tasks on **Tasks for regular sending** tab of the **Reports** section. For details, see "Tasks for Regular Sending".

When preparing a report for the management, you may need to present data in paper or file format.

To save or print a report:

1. In **Violation statistics** section, configure the widgets required for the report.
2. Use filters to select a set of data.
3. Click  to hide the filter panel.
4. Scroll to the end of the page so that the widgets load and display all the data.
5. Click **Ctrl**+**P** or select **Print** in the browser menu.
6. In the print window:
   - select an installed printer
     or
   - click **Save as PDF** if you need to save the report as a file.
7. Select the layout: *Portrait* or *Landscape*.
8. To ensure that all widgets fit on the page, specify the scaling options on **More settings** tab. We recommend choosing the following parameters:
   - 50% for portrait layout
     or
   - 70% for landscape layout.
     Also you can use **Ctrl**++ and **Ctrl**+- keys to change the scale or the number of widgets on the page.
9. Depending on the action selected at step 5, click **Print** or **Save**.

9 Infrastructure Section

Infrastructure section contains functionality of InfoWatch DAT. In this section, you can view automatic audit results for domain directory service and access to mailboxes, track changes in access rights to files and folders.

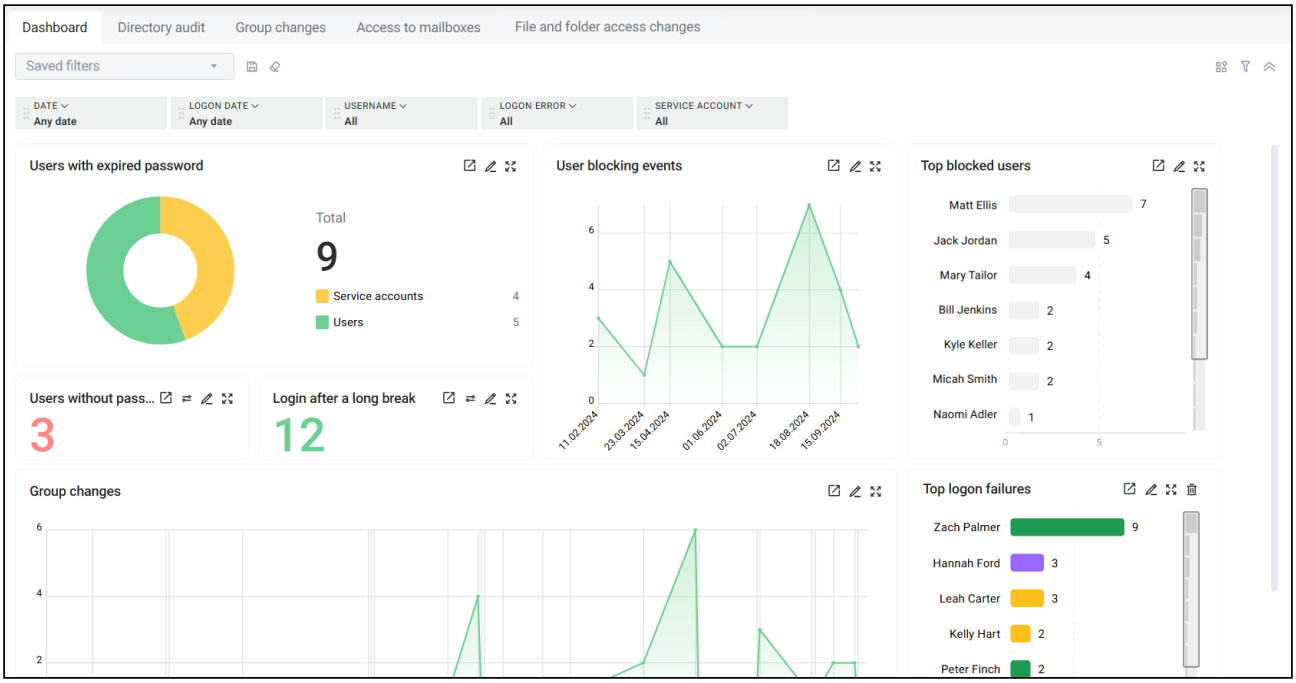
Five tabs are available:

- **Dashboard**, where you can view widgets which are based on the reports of this section;
- **Directory audit**, where you can view reports on sensitive accounts as well as on directory service events that can potentially lead to unauthorized access;
- **Group changes**, where you can track actions with directory service groups;
- **Access to mailboxes**, where you can monitor access to mailboxes;
- **File and folder access changes**, where you can track granting/revoking of user access rights to filesystem objects.

9.1 Dashboard Tab

For visual assessment of unauthorized access groups, **Dashboard** tab contains widgets based on reports from **Directory audit** and **Group changes** tabs:

- *Users with expired password*
- *User blocking events*
- *Top blocked users*
- *Top logon failures*
- *Login after a long break*
- *Users without password*
- *Group changes*
- *Privileged group changes*



When working with widgets, you can:

- Open a widget in full-screen view. In order to return to the regular view, click **Minimize**;

-  Go to the report connected to the widget. The report opens in a separate browser tab;
-  Rename the widget;
-  Edit the widget; Editing is available only for *Login after a long break*, *Users without password* and *Privileged group changes* widgets.

For description of reports and their settings, see "Widgets of Infrastructure Section".

Working area settings enables you to:

- Set the widget size;
- Select widgets and filters to be displayed on the tab;
- Select widget location in the working area.

To customize the display of widgets:

1. Click  **Setting widgets** in the upper-right corner of the working area.
2. Select a setting:
   - If you want to hide the widget from the working area, click  **Delete widget**.
   - If you want to move the widget, drag its name and drop it to any place in the working area.
   - If you want to resize the widget, press the mouse button and while keeping it pressed, move the widget borders.
3. Click  **Save** to apply changes.

To add a widget:

1. Click  **Setting widgets** →  **Add** in the upper-right corner of the working area.
2. In the dialogue, click **+ Add** opposite the widget.

   > **Note:**
   >
   > To quickly find the required widget, enter its name or a part of its name into the search box.

3. Specify the number of widget copies to display. You can add no more than 10 copies of a widget at a time.
4. Confirm by clicking **Apply**. The new widget will be displayed in the working area.
5. Click  **Save** to save changes and exit.

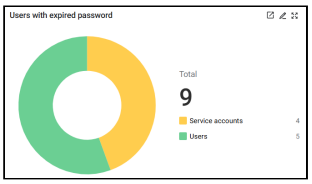
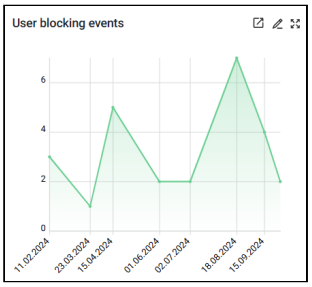
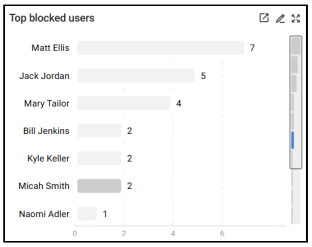
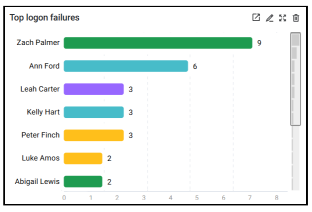
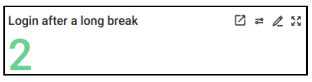
To filter data in widgets:

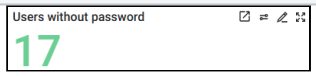
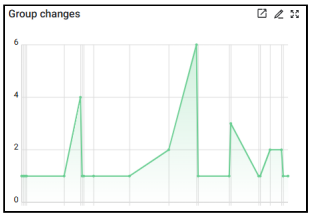
1. Adjust the filters displayed in the working area:
   a. Click  **Add/Delete filter** in the upper-right corner of the working area.
   b. In the filter list, check/uncheck the boxes next to the filters as needed.
2. Specify the values of the filters. The System will rebuild all widgets that use the specified parameters.

To **hide/show filter panel**, use  and  buttons.

9.1.1 Widgets of Infrastructure Section

Dashboard tab contains widgets based on reports from **Directory audit** and **Group changes** tabs:

Widget	Description
Users with expired password 	Pie-chart distribution of service and user accounts with expired password Based on *Users with expired password* report from **Directory audit** tab
User blocking events 	Distribution of user blocking events by dates Based on *User blocking events* report from **Directory audit** tab *Date* filter is available
Top blocked users 	List of most frequently blocked accounts Based on *User blocking events* report from **Directory audit tab** *Date* filter is available
Top logon failures 	List of accounts with the largest number of failed login attempts. Each failure type has its unique colour representation Based on *Failed login attempts* report from **Directory audit** tab *Date* and *Logon error* filters are available
Login after a long break 	Number of unviewed events of account login after a break of more than 30 days Based on *Login after a long break* report from Directory audit tab You can set a value that will determine a critical state, i.e. the colour of numbers equal to and greater than the value will turn to red *Logon date* filter is available
Users without password	Number of user accounts with "Password not required" attribute Based on *Users without password* report from **Directory audit** tab

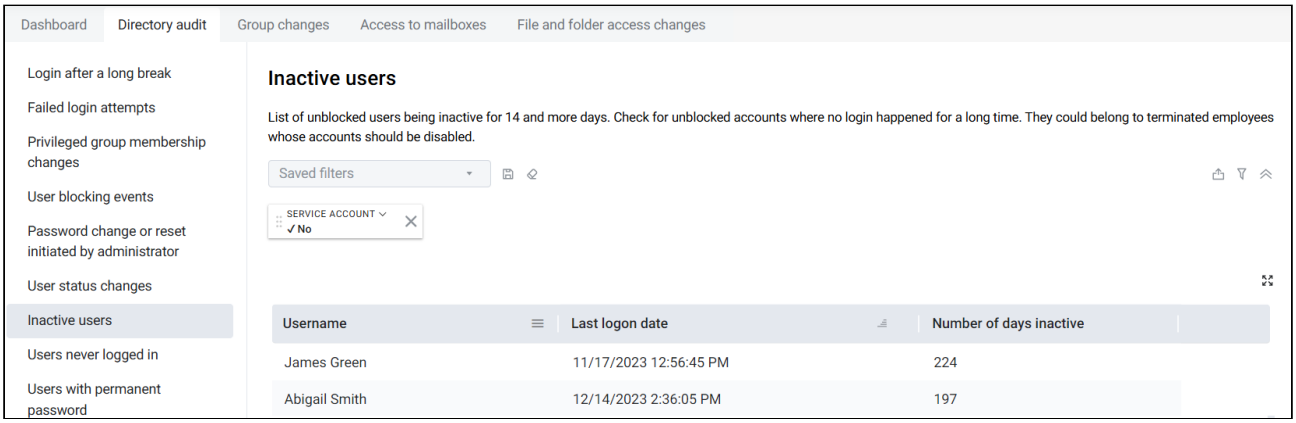
Widget	Description
	You can set a value that will determine a critical state, i.e. the colour of numbers equal to and greater than the value will turn to red *Service account* filter is available
Group changes 	Distribution of group change events by dates Based on data from **Group changes** tab *Date* filter is available
Privileged group changes 	Number of unviewed events of privileged group membership changes Based on *Privileged group membership changes* report from **Directory audit** tab You can set a value that will determine a critical state, i.e. the colour of numbers equal to and greater than the value will turn to red *Date* filter is available

To set a threshold value:

1. On the right to the widget name, press  **Edit widget**.
2. In **Edit widget** dialogue, enter the required number.
3. Click **Save**.

9.2 Directory Audit Tab

The tab presents automatic directory service audit results. You can view the account status reports and reports about directory service events.



9.2.1 **Reports**

Report type	Description	Available information	Available filter
Login after a long break	User accounts with over 30-day difference between the values of *LastLogonDate* attribute for the last and previous synchronizations. Among such users may be fired employees whose accounts have not been disabled.	• *Username* • *Logon date* • *Previous logon date* • *Number of days inactive*	• *Logon date* • *Viewed*
Inactive users	Unblocked users who have been inactive for 14 days or more. Accounts that have not logged in for a long time may belong to fired employees.	• *Username* • *Last logon date* • *Number of days inactive*	*Service account*
Inactive computers	Unblocked computers who have been inactive for 14 days or more.	• *Computer name* • *Operating system* • *Last logon date* • *Number of days inactive*	*Last logon date*
Users never logged in	Users whose accounts were created 14 or more days ago and have never been logged in. Such accounts may belong to attackers trying to gain unauthorized access to the system.	• *Username* • *User status* • *Date* of account creation	*Service account*
Computers never logged in	Computers whose accounts were created 14 or more days ago and have never been logged in. Attackers may use such computers for unautharized access to the system.	• *Computer name* • *Computer status* • *Creation date*	*Creation date*
Users with permanent password	Users with accounts that do not have a password change deadline. Specifying a password change deadline is optional for service accounts. Make sure that other accounts have a password change deadline.	• *Username* • *User status* • *Creation date* • *Last logon date*	*Service account*
Users without password	User for whom *Password Not Required* attribute is selected. May include users with a blank password.	• *Username* • *User status* • *Creation date*	*Service account*

Report type	Description	Available information	Available filter
		• *Last logon date*	
Blocked users	Automatically blocked users. May include users who tried to guess a password or gain unauthorized access in another way.	• *Username* • *Last logon date*	*Service account*
Users with expired password	Users with accounts for which the password change period has expired. For such accounts, the risk of password guessing or gaining unauthorized access in another way is increased.	• *Username* • *Last password change date* • *Creation date* • *Last logon date*	*Service account*
Failed login attempts	Failed authorization attempt events. May include password guessing incidents or attempts to gain unauthorized access in another way.	• *Username* • *Date* of an event • *Computer IP address* • *Computer name* • *Logon error*	• *Date* • *Logon error*
Privileged* group membership changes	Changes to groups with increased access rights. Any changes in the composition of such groups may indicate possible security incidents.	• *Modified group name* • *Date* of an event • *Action type* • *Added or removed user/ group name* • *Changed by*	• *Date* • *Viewed*
User blocking events	Events of automatically blocked users. Such users may include those who tried to guess a password or gain unauthorized access in another way.	• *Username* • *Date* of an event • *Last logon date*	• *User* • *Date*
Password change or reset initiated by administrator	Users whose password was changed by the administrator. Password resets for users with increased privileges may indicate attacker activity. **Note:** A password change event is created in audit events each time when a new user is created. This event usually does not indicate suspicious activity.	• *Username* • *User status* • *Date* of an event • *Changed by*	*Date*

Report type	Description	Available information	Available filter
User status changes	Report on administrator actions with user accounts: • Creating an account; • Deleting an account; • Disabling an account; • Enabling an account; • Unlocking an account. These changes may indicate suspicious activity.	• *Username* • *Date* of an event • *Changed by* • *Action type*	• *Username* • *Date* • *Changed by* • *Action type* • *Viewed*

You can:

- Hide the tab menu;
- View reports full-screen;
- Mark events as viewed;
- View event details.

For instructions, see "Viewing Reports" article.

- Filter, group and sort entries in reports.

Besides, you can **filter** your reports by columns listed in **Available filter** column of **Reports** table. The filters are described in "Single Filter" article.

You can also **group** entries by the values of the following columns:

- *User status*;
- *Modified group name*;
- *Username*;
- *Computer IP address*;
- *Computer name*;
- *Added or removed user/group name*;
- *Action type*;
- *Changed by*;
- *Status*.

Sorting entries is available by values of all columns excluding:

- Number of days inactive;
- Computer name.

* **Privileged groups**

List of Active Directory service groups, actions with which are presented in **Privileged group membership changes** report:

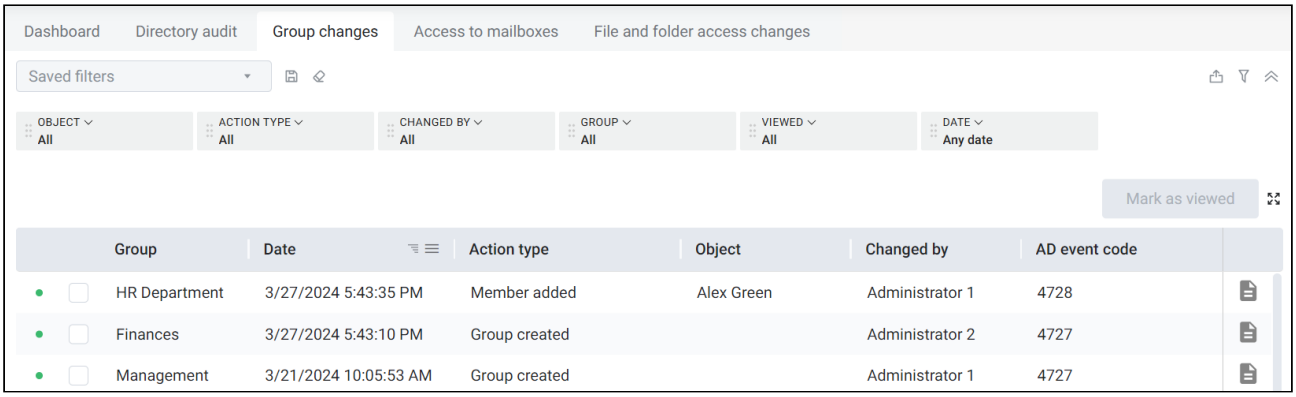
- *Account Operators*
- *Administrators*
- *Backup Operators*
- *Certificate Authority Server*
- *Delegated Setup*

- *DHCP Server*
- *Discovery Management*
- *DNS Server*
- *DNSAdmins*
- *Domain Admins*
- *Domain Controllers*
- *Enterprise Admins*
- *Enterprise Read-only Domain Controllers*
- *Exchange Organization Administrators*
- *Exchange Public Folder Administrators*
- *Exchange Recipient Administrators*
- *Exchange Servers*
- *Exchange Trusted Subsystem*
- *Exchange View-Only Administrators*
- *Group Policy Creator Owners*
- *Incoming Forest Trust Builders*
- *Managed Availability Servers*
- *Microsoft Exchange Server*
- *Microsoft Exchange Servers*
- *Network Configuration Operators*
- *Organization Management*
- *Power Users*
- *Print Operators*
- *Public Folder Management*
- *Read-only Domain Controllers*
- *Replicators*
- *Schema Admins*
- *Server Operators*
- *View-Only Organization Management*
- *WSUS Administrators*

9.3 Group Changes Tab

On the tab, you can view all group-changing events. Find the data in a table with the following columns:

- **Group** which has changed;
- **Date** of an event;
- **Action type**: group attribute change, creating/deleting a group, adding/removing a member;
- **Object** of the event – name of a user/group added to a group or deleted from it;
- **Changed by** – name of a user which has made edits;
- **AD event code**;
- **Event details**.



You can:

- View reports fullscreen;
- Mark events as viewed;
- View event details.

For instructions, see "Viewing Reports" article.

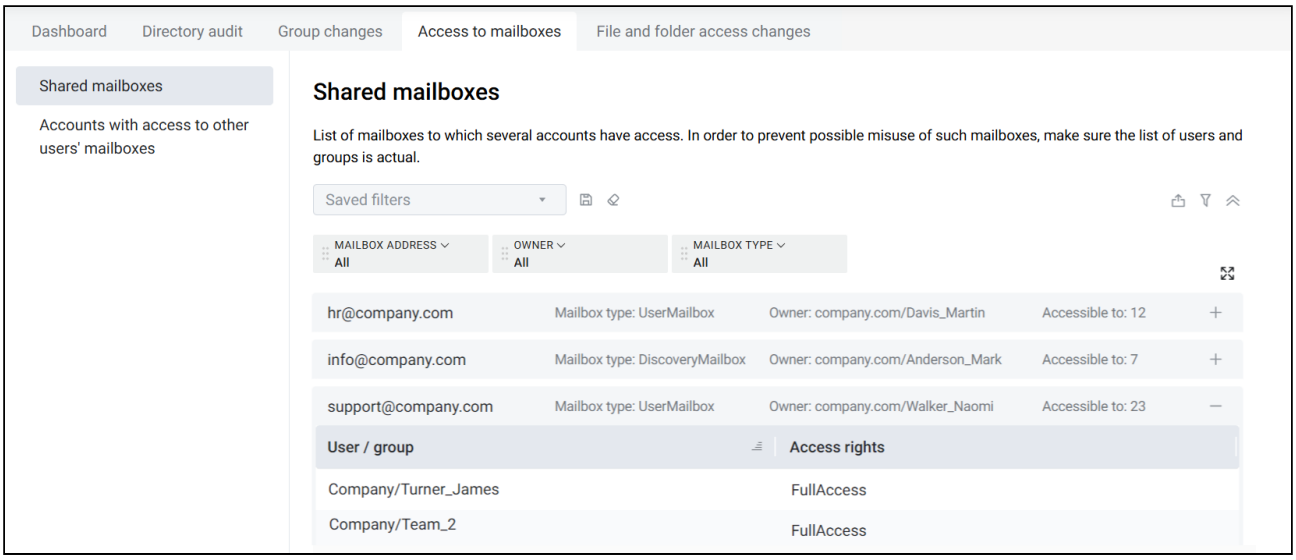
Besides, you can **filter** entries by the following columns: *Changed by*, *Object*, *Group*, *Action type*, *Viewed*, *Date*. The filters are described in "Single Filter" article.

You can **sort** and **group** entries by values of the following columns:

- *Group*;
- *Changed by*;
- *Object*;
- *Action type*.

9.4 Access to Mailboxes Tab

On the tab, find reports on access rights to Microsoft Exchange mailboxes. When clicking any report line, an additional level of the report opens.



9.4.1 Reports

Report type	Description	Available information	Filters
Shared mailboxes	List of mailboxes to which several accounts have access. In order to prevent possible misuse of such mailboxes, make sure the list of users and groups is actual.	Main level: • **Mailbox address**; • **Mailbox type**, for example: *DiscoveryMailbox*, *UserMailbox*; • **Owner**; • **Accessible to** – number of users/groups who have access to the mailbox. Additional level: • **User/group** – list of all users/groups with access to the mailbox; • **Access rights** – access level to the mailbox for each user/group.	• **Mailbox address** • **Owner** • **Mailbox type**
Accounts with access to other users' mailboxes	List of users and groups which have access to other users' mailboxes. In order to prevent possible misuse of mailboxes, make sure a user or group has only necessary access rights.	Main level: • **User/group**; • **Number of mailboxes** to which the account has access. Additional level: • **Mailbox address**; • **Mailbox type**; • **Owner** of the mailbox; • **Access rights**.	• **User/group**

Data in reports is divided into pages. Using the panel under a report, you can:

- Select the page by number;
- Navigate to the first, last, previous and next pages;
- From the drop-down list, select the number of entries to display on the page: 25, 50, 75 or 100.



For easier viewing of reports, you also can:

- Hide the tab menu;
- Open reports fullscreen;
- Sort entries in reports.

For instructions, see "Viewing Reports" article.

You can also **filter** entries by columns listed in *Filters* column of **Reports** table. The filters are described in "Single Filter" article.

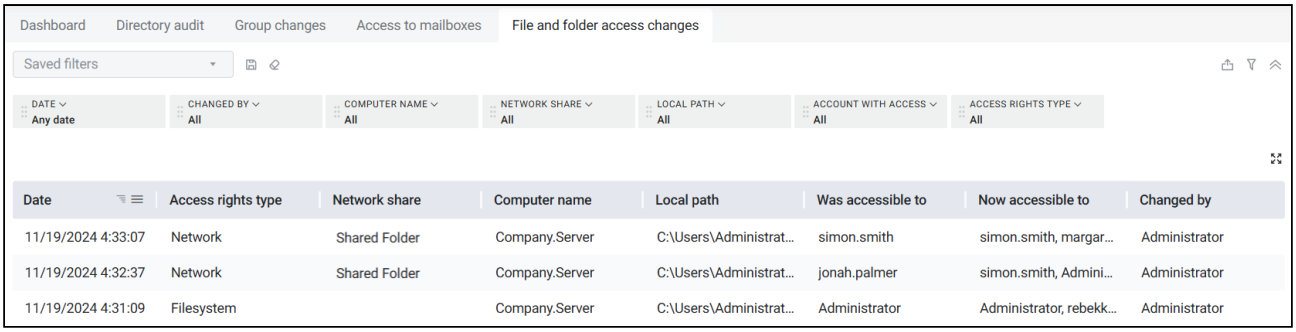
9.5 File and Folder Access Changes Tab

The tab contains a report on changes of lists of accounts and groups which have access to certain filesystem objects. Find the data in a table with the following columns:

- **Date** of an event;
- **Access rights type**: *Filesystem* (Active Directory event code 4670) or *Network* (event code 5143);

> **Note:**
>
> An account/group has access to a file/folder only in case it was granted access rights of both filesystem and network types. Granting access rights of one of the types does not provide access to the object. That is why the factual date of receiving rights is considered the date when the account/group received rights of both types.
>
> Note that an account/group might have received rights of one of the types before IW Data Access Tracker started tracking access rights changes. DAT will not display such an event.

- **Network share** – name of a network share (displayed only for *Shared network* events);
- **Computer name** – name of a computer on which edits were made;
- **Local path** to the folder;
- **Was accessible to** – list of accounts/groups which had access to the object before the changes were applied;
- **Now accessible to** – list of accounts/groups which received access to the object after the changes were applied;
- **Changed by** – name of a user which made the edits.



You can view the table fullscreen (see "Viewing Reports").

Besides, you can **filter** entries in the table by the values of the following columns: *Date*, *Changed by*, *Computer name*, *Network share*, *Local path*, *Account with access*, *Access rights type*. For description of filters, see "Single Filter" article.

Entries in the table can be also **sorted** by the values of **Date** column.

9.6 Viewing Reports

When working with reports, you can:

- Hide the tab menu;

- View reports full-screen;
- View event details;
- Mark events as viewed;
- Group and sort entries.

9.6.1 Hide tab menu

In order to free up space to view reports, you can hide the menu of **Directory audit** and **Access to mailboxes** tabs.

To do this, click « **Collapse menu** under the list of reports.

9.6.2 Full-screen mode

To view reports on tabs in full-screen mode, click **Open fullscreen** .

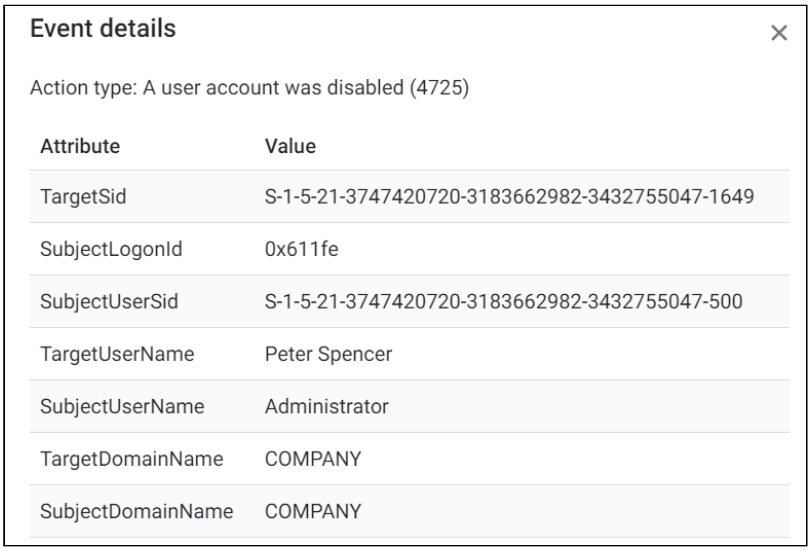
To leave full-screen mode, click **Minimize** .

9.6.3 Event details

You can view event details:

- In the report on **Group changes** tab;
- In reports on **Directory audit** tab:
  - **Privileged group membership changes**;
  - **User status changes**;
  - **User blocking events**;
  - **Password change or reset initiated by administrator**;
  - **Failed login attempts**.

To view detailed information from the directory service, click **Event details** at the end of the line. You will see a window with the Microsoft Active Directory event attributes and their values, including the event ID:



To exit the detail view mode, click or click outside the window.

9.6.4 Event status

You can view event details:

- In the report on **Group changes** tab;
- In reports on **Directory audit** tab:
  - **Login after a long break**;
  - **Privileged group membership changes**;
  - **User status changes**.

The System indicates an event's status with green or grey colour in the beginning of the event's line:

- – unviewed events;
- – viewed events.

By default, each event is unviewed:



Group	Date	Event type	Object	Changed by	AD event code
HR Department	5/5/2024 11:12:30 AM	Add	Alex Green	Administrator 2	4728

To mark an event as viewed, click the indicator. The colour will change and the event will be displayed as viewed:



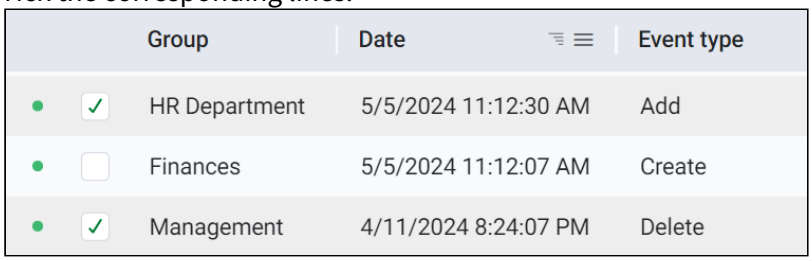
Group	Date	Event type	Object	Changed by	AD event code
HR Department	5/5/2024 11:12:30 AM	Add	Alex Green	Administrator 2	4728

Similarly, you can set the event back as unviewed:



To mark several events as viewed:

1. Tick the corresponding lines:



Group	Date	Event type
HR Department	5/5/2024 11:12:30 AM	Add
Finances	5/5/2024 11:12:07 AM	Create
Management	4/11/2024 8:24:07 PM	Delete

2. Above the table to the right, click **Mark as viewed**.

9.6.5 Grouping and sorting entries

Sorting entries

You can sort data in the columns in ascending/descending order. The columns with sorted entries have or icon to the right of them.

To sort entries:

1. Click the name of the column by which you want to sort the entries.
2. By clicking the icon, select the sorting order:
   - Ascending 
     or
   - Descending 

Entires in the table will be sorted by the values of this column:

Username	Changed by	User status	Date	
Barbara Brown	Administrator 1	Enabled	3/27/2024 2:41:23 PM	
David Jackson	Administrator 4	Enabled	4/29/2024 4:30:28 AM	
Joseph Smith	Administrator 1	Enabled	4/28/2024 12:44:49 AM	
Keith Lee	Administrator 2	Enabled	3/29/2024 10:46:14 AM	

To sort values by two and more columns:

1. Sort values by a priority column.
2. Keep pressed **Ctrl** on the keyboard and sort the entries in another column.

Example:

Entries in the report are sorted by the priority column (as it is on the left) named **Changed by**. Entries in the second column are sorted relatively to the first column.

Changed by	Username	User status	Date	
Administrator 1	Barbara Brown	Enabled	3/27/2024 2:41:2...	
Administrator 1	David Jackson	Enabled	4/29/2024 4:30:2...	
Administrator 1	Joseph Smith	Enabled	4/28/2024 12:44:...	
Administrator 2	Anthony Flowers	Enabled	3/29/2024 10:46:...	

To reset sorting:

1. Hover your cursor over the column name.
2. Click the  icon that appears.
3. Select **Reset columns**.

Примечание:

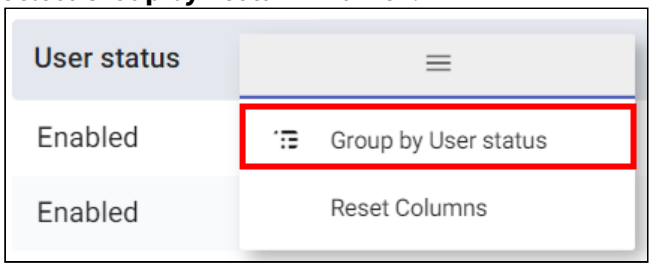
Multiple sorting and **Reset columns** button are not available for tables in the report on **Access to mailboxes** tab.

Grouping entries

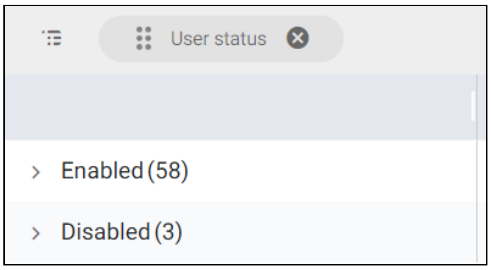
You can apply grouping to entries on **Directoy audit** and **Group changes** tabs.

To group entries:

1. Hover over the column name.
2. Click on the  icon that appears.
3. Select **Group by <column name>**:



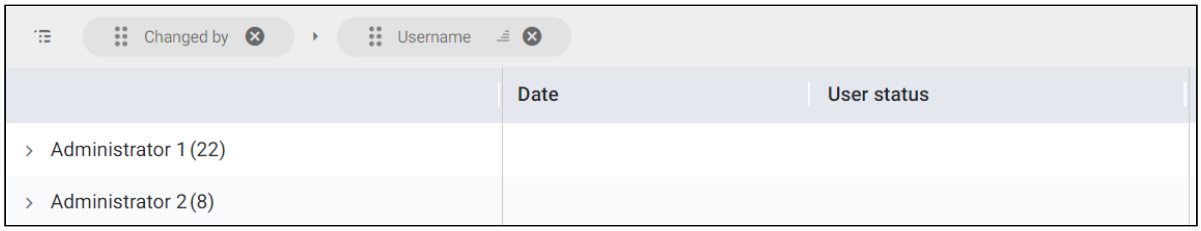
As a result, all events will be divided into groups:

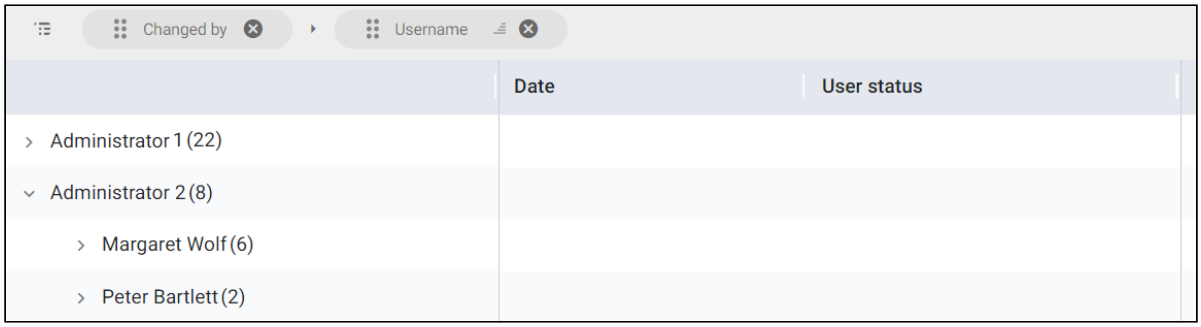


Multiple grouping

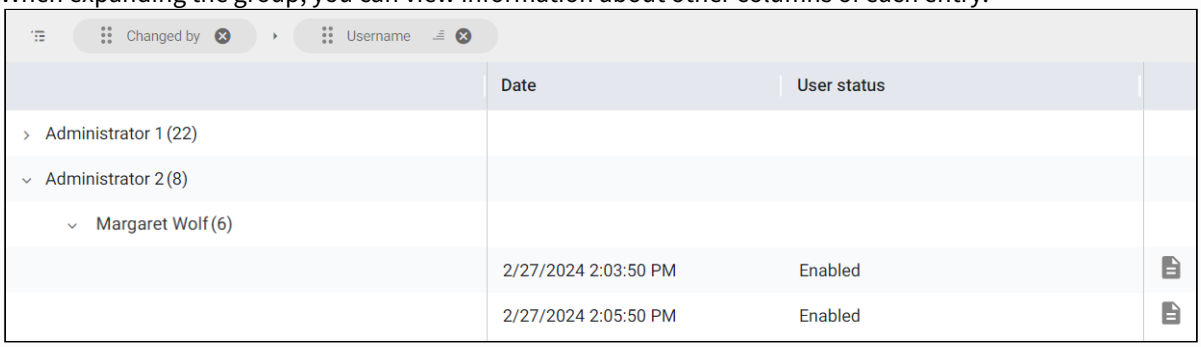
You can group entries in some reports by multiple columns. For this, you should determine column priority and apply grouping to each column.

> **Note:**
>
> The column priority is determined from left to right. You can change the column order by dragging them.

> **Example:**
>
> Entries in **Password change or reset initiated by administrator** report of **Directory audit** tab are grouped by **Changed by** column: *Administrator 1* and *Administrator 2*. The number of entries is specified in brackets:
>
> 
>
>
> Entries within the group whose accounts were changed by *Administrator 1* are grouped by the **Username** column:



When expanding the group, you can view information about other columns of each entry:



To reset grouping:

- On the column name panel above the table, click 
  or
- Click  icon, which appears when you hover your cursor over a column name, and select **Reset columns**.

9.7 Unloading Reports

Data represented on the following tabs of **Infrastructure** section is available for unloading as an XLSX report and saving on your computer:

- **Directory audit**
- **Group changes**
- **Access to mailboxes**
- **File and folder access changes**

You can also schedule emails with report files.

To export data:

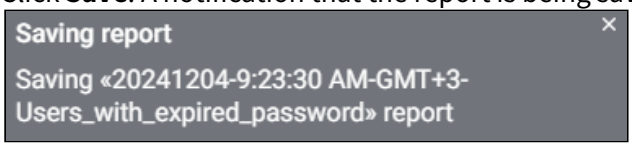
1. If required, configure filters and sort entries. The System will export data to the report in the configured view.

   Note:

In case the table contains more than 10,000 entries after filtering (on **Access to mailboxes** tab – including entries of the additional level), the System will add only the first 10,000 entries to the report.

On **Access to mailboxes** tab, entries from the selected page only are added to the report.

2. In the upper-right region above the report, click .
3. Click **Unload report**.
4. In **Report unloading** window, define the file contents:
   a. To add a sheet with additional information to the report, select **Additional information** in the list. The sheet contains:
      - Date and time of report generation;
      - Filter settings;
      - Link to the Management Console.
   b. Add main report data by selecting the report name.
   c. Click **Save**. A notification that the report is being saved appears:



5. Go to **Reports** → **Reports archive** section to download the report. For details, see "Reports Section".
6. Click  on the line corresponsing to the report file.

9.7.1 Scheduled reports

You can set up regular emails with report files:

- On **Directory audit** tab for reports:
  - *Login after a long break*;
  - *Failed login attempts*;
  - *Privileged group membership changes*;
  - *User blocking events*;
  - *Password change or reset initiated by administrator*;
- For the report on **Group changes** tab.

For this:

1. If required, configure filters and sort entries. The System will export data to the report in the configured view.

> **Note:**
>
> In case the table contains more than 10,000 entries after filtering, only the first 10,000 entries are added to the report.

2. In the upper-right region above the report, click .
3. Click **Set up regular sending**.
4. In **Report unloading** window, define the file contents:

a. To add a sheet with additional information to the report, select **Additional information** in the list. The sheet contains:
   - Date and time of report generation;
   - Filter settings;
   - Link to the Management Console.

b. Add main report data by selecting the report name.

5. Configure sending parameters:

Parameter	Description
Report creation period	Specify the period for which to create a report: • *Last 24 hours* • *Current day* • *Last 3 days* • *Last 7 days* • *Last 30 days*
Recipients	Specify recipients of the report.
Sending frequency	Specify the frequency with which the Officer should recieve the report: • *Every day* • *Every week* You can select days of the week when the System should send reports. • *Every month* The System will send the report on the first day of the month following the reporting month.
Time	Specify the report sending time.

6. Click **Save**. A task for regular sending will be created. You can view the task list in **Reports** → **Tasks for regular sending** section. For details, see "Tasks for Regular Sending".

Important!

For the System to send regular reports, configure the connection with the mail server in Investigation Centre. For details, see "*InfoWatch Data Access Tracker. Administration Guide*" document, "Notification Services" article.

Note:

You can also configure email notifications (without reports):

- On domain directory service group changes, to be sent daily;
- On privileged group membership changes, to be sent instantly.

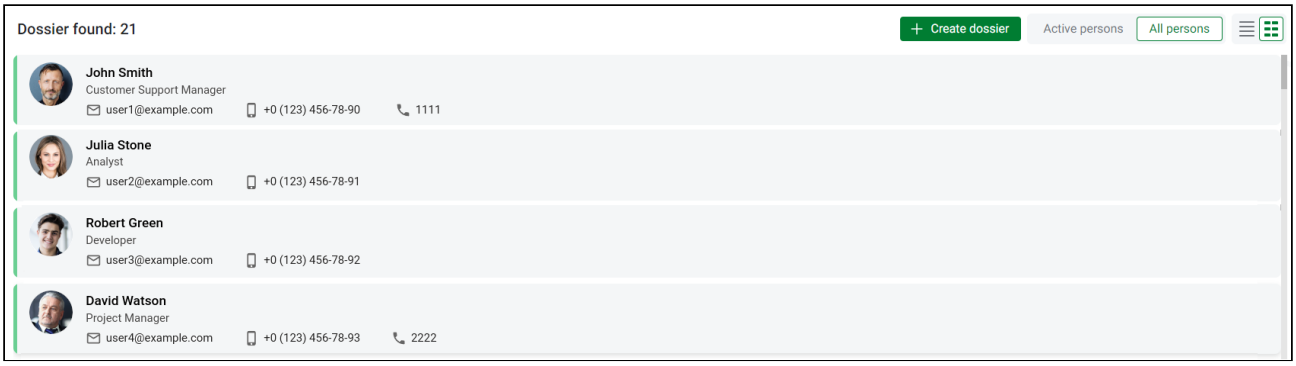
For details, see *"InfoWatch Data Access Tracker. Administration Guide"* document, "Email Notifications" article.

10 Persons Section

About this section:

This section contains a catalog of contacts uploaded into the System when synchronizing with the sources (Active Directory and Traffic Monitor) as well as manually added persons.

To review a specific person's dossier, left-click on it. To return to the list of persons, click  in the top left corner of the working area.



The list of persons displays only those persons that satisfy conditions of the Single filter. To customize how dossiers with persons are displayed, use the toolbar on the right side of the working area:

- **Active persons** – to display only dossiers of employees with active account in Active Directory and at least one event:

> **Note:**
>
> If person does not have any event or they are blocked/deleted from AD, then this person is considered unactive and displayed on **All persons** tab.
>
> Use filters to view the list of active persons. If no value is selected in any filter, then active persons list cannot be displayed.

- **All persons** – to display dossiers of all the persons, including ex-employees of the company;
-  – to display data as a list;
-  – to display data as a table.

User actions in this section:

- Person's Dossier Review
- Reviewing and configuring personal information
- Dossier creation, editing and deletion
- Dossiers merging
- Adding Person's Contacts
- Changing Person's Manager
- Exporting Statistics from Person's Dossier

10.1 "Personal Information" Tab

The widgets on the **Personal information** tab allow to view all the information about person in the System.

WIdget name	Description
Manager	Displays a list of the person's managers and allows specifying the manager manually
Contacts	Allows you to manage the person's contacts and displays contacts loaded from connected sources
General information	Displays the person's information provided by different sources: date of hiring, period of employment, date of leaving
Statuses	Displays a list of statuses assigned to the person in Traffic Monitor
Description	Displays description of person, allows to add and edit it manually

To expand widget, press .

To edit data on widget, press .

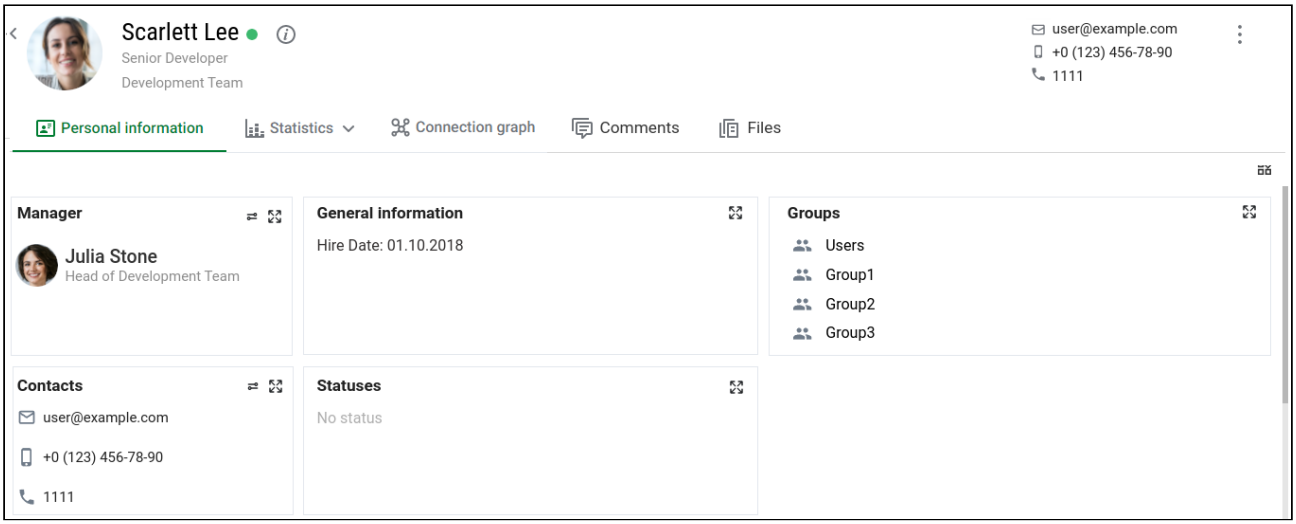
10.2 Person's Dossier Review

A dossier is a tool intended to collect data for a specific person.

On the page of the person's dossier, you can find the employee's personal data:

- Employee's full name;
- Job title;
- Department;
- Contacts: account in AD *login@company.com*, personal and working contacts including email, telephone number, mobile phone number.

> **Note:**
>
> All persons added during integration with Active Directory have the type of contact – SID, which is used to identify the persons.



The colour indicator is displayed on the right of person's name:

- –for active employees including manually created and the ones with expired Active Directory accounts, but with active status in AD;
- – for employees disabled in Active Directory or with undefined status.

Click on the right of the person's name to see the following data:

- date of the dossier's creation;
- date of the dossier's last update;
- the dossier's owner – the System or Security officer (for manually created dossiers).

To change the dossier's data, use button in the right part of the working area (for details, see "Creating, Editing, and Deleting Dossier").

The information in persons' dossier is displayed on two tabs:

- **Personal information** – you can find widgets of dossier specific for this person: **General information**, **Manager**, **Contacts**, **Statuses**, **Description** (see "Personal Information" Tab");
- **Violation statistics** – statistics widgets of the person (see "Statistics Widgets").

> **Note:**
>
> Above described tabs are available when DAT is installed.
>
> The set of person's dossier tabs depends on products installed in the cluster of the Investication centre.

To go back to the list of persons, press in the top left corner of the working area.

10.3 Creating, Editing, and Deleting Dossier

To create a dossier for a new person or an additional dossier for an existing person:

1. Go to the **Persons** section.

2. Click **+ Create dossier**.
3. Specify personal information as follows:
    - Person name
    - Job title within the organization
    - Department the person is assigned to
    - Additional description
4. Add person's photo.
5. Add person's contact data. It can be a personal or working phone number, e-mail address, or a social network account.
6. Click **Create dossier**. The new dossier will become available in the list of employees' dossiers.

To edit the dossier:

1. Open the required dossier.
2. Click  in the right upper corner and select **Edit**.
3. Make your changes and click **Save**.

To delete a dossier:

1. Open the required dossier.
2. Click  in the right upper corner and select **Delete**.
3. Click **OK**. The dossier will be deleted permanently.

10.4 Dossier Merging

It can be convenient for a Security officer to merge two or more dossiers into one. The new dossier will include all data from the initial dossiers. For this:

1. Open the first dossier which you need to merge.
2. Click  and select **Merge dossiers.**
3. In the opened window select the second dossier or several dossiers in the field **Merge with**.
4. Click **Merge**.

10.5 Adding Person's Contacts

When synchronizing with Traffic Monitor or Active Directory, the person's contacts become available: work and personal phone numbers, email addresses, social network accounts (in case of synchchronization with TM), etc. You can also add more contacts manually. For this:

1. Go to the person's dossier.
2. On the **Personal information** tab on the **Contacts** widget, click .
3. You will see a window with all contacts that were automatically added from other systems during the integration. By default, for the following contact types, only one contact is displayed: login in the domain, phone number, email, mobile phone number. Click **Add contact**.
4. Specify the contact type (for example, a personal phone number) and enter its value. You also can:
    - add several items;
    - comment on the contact .
5. Click **Save**. The new contacts will become available in the dossier. For contacts with comments, the  icon is displayed next to the contact. To view the comment, click the icon.

10.6 Changing Person's Manager

The **Manager** widget of the tab **Personal information** displays the person's manager. This information is retrieved from the person's card during synchronization with a source: ActiveDirectory or Traffic Monitor.

The Security Officer can change the manager manually. Manager added from the system source cannot be changed.

To change the manager:

1. Cick .
2. The **Change manager** window will open, In the *Manually added* field, choose the new manager from the list of persons registered in the System. You can enter multiple names.
3. Click **Save**. The selected managers will be displayed on the **Manager** widget.

To open the dossier of a person's manager, left-click the manager's name on the **Manager** widget.

10.7 Exporting Statistics from Person's Dossier

In a person's dossier, you can export statistics on the person's activities (widgets on **Violation statistics** tab of **Analytics** section) as an XLSX file. For this:

1. In the dossier of a person for whom you need to create a report, open **Violation statistics** tab.
2. Select widgets and set up filters, so that the System would display the required data.
3. In the upper right corner of the screen, click  and **Unload report**.
4. In **Report unloading** window, choose the widgets to include:
   - To include all widgets to the report, click  **Select all**.
   - If you need to add only particular widgets, select them in the list by clicking .
5. Click **Save**. You will see a message indicating that the report is being saved.
6. Open the **Reports** section.
7. Select the report and unload it to your computers. The report file will be saved to **Downloads** folder.

The downloaded report is a file with several sheets – a separate sheet for each widget. For more information about data that is represented in reports, see "Creating, Unloading and Printing Reports with Statistics Data".

11 Investigation Section

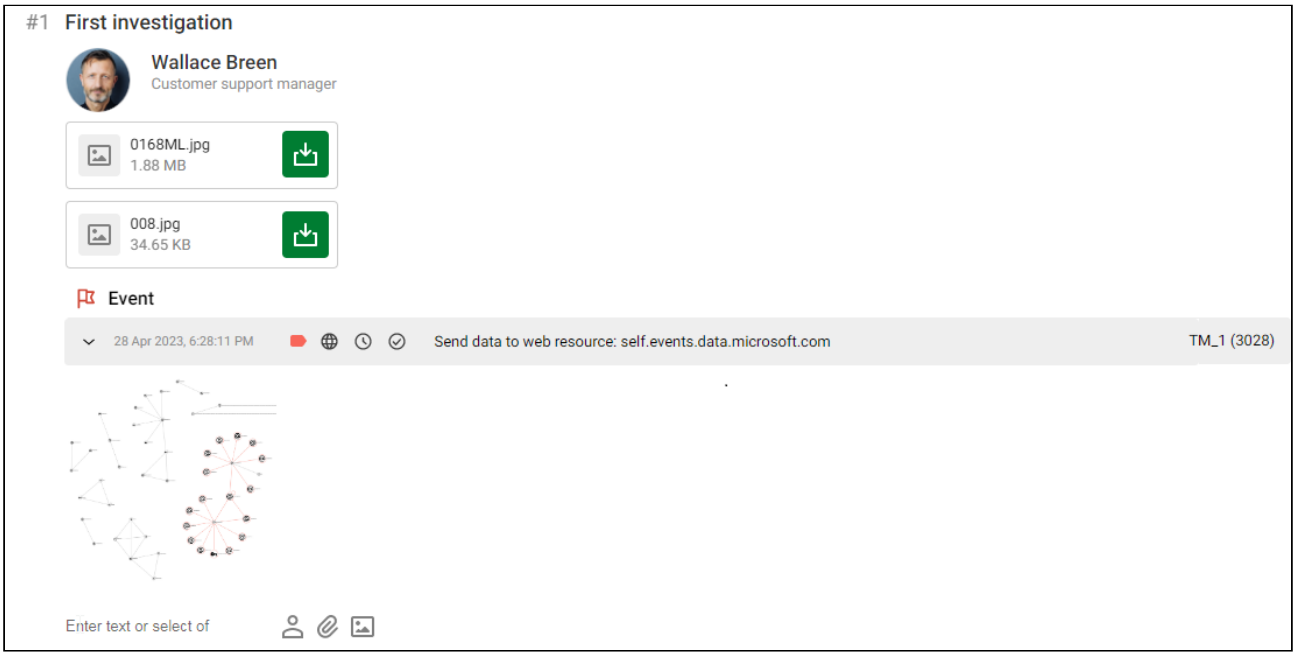
In this section, you can accumulate data collected from different sources and combine it into investigations. You can use this data for making decisions and creating reports. The order of collecting materials and conducting investigations is as follows:

1. The System represents facts of policy violations in the form of events.
2. A Security Officer manually adds such events to an investigation. If necessary, the Security Officer adds descriptions, attaches files, screenshots and dossiers of persons that are suspected of violating.
3. Other Security Officers join the investigation, add their comments and attach other materials. Thus, they can promptly exchange information.
4. The Security Officers represent the accumulated data as a report.

On the navigation bar, you can find a list of all open investigations and an archive – this is a base of investigations with which Security Officers are not currently working.

In the working area, you can see a card of the selected investigation. This card may include:

- Links to dossiers of persons involved in the investigation,
- Cards of the Traffic Monitor event from the **Events** section,
- Attachments in different formats,
- Graphic files,
- A free-form text comment.



To learn more about the attached materials, you can:

- Click on the dossier link and go to the **Persons** section,
- Click  and download the attached file to your hard drive,
- Open the event card and view detailed information on the event,
- View graphic files.

For your convenience, you can reorder materials in the investigation card. For this, hold  and drag the item to the right place. To delete an obsolete item, click  next to it and select **Delete**.

To update the state of the investigation card, click .

User's actions:

- Creating and Archiving Investigations
- Adding Event to Investigation
- Adding Materials to Investigation
- Collaborative Investigations
- Editing, Exporting, Printing and Deleting Investigation

11.1 Creating and Archiving Investigations

To create an investigation:

1. On the navigation bar on the left, click .
2. In the window that will open, enter the investigation name.
3. Click **Save**. A card of the new investigation will open and you will be able to add materials to it.

While you are working on the investigation, other users can accidentally edit the investigation data. To prevent it, we recommend archiving the investigation. We also recommend that you should archive the investigation when it is over.

To move the investigation to an archive:

1. On the navigation bar, open the required investigation.
2. Click .
3. In the window that will open, click **Move to archive**. Archived investigations can be viewed, but they cannot be edited.

To get back to working on an archived investigation:

1. Select the required archive.
2. Click .
3. In the window that will open, click **Unarchive**. Now you can edit the investigation.

11.2 Adding Materials to Investigation

To conduct an investigation, you should collect materials as fully as possible. For this:

1. On the navigation bar, open the investigation card.
2. In the working area, you can add different kinds of materials to the investigation:
    - **Text comment** – for this:
        a. Enter a free-form comment.
        b. If necessary, format the comment text using built-in standard tools. Double-click the comment text to access the tools.
        c. Click **Enter** to save the comment.
    - **A link to the person's dossier** – for this:
        a. Click .
        b. In the window that will open, choose the required dossier and click **Accept**.
    - **Attachments** – for this:
        a. Click .

b. On your computer's hard drive, select one or more files of any format and click **Open**. The process may take some time and depends on the size of the files. You can upload up to 10 files at a time with a total size of up to 100 MB. Selected files will be attached to the investigation. These files can be viewed after a Security Officer who is admitted to the investigation downloads them to a hard drive.

- **Graphic files** – for this:
  a. Click .
  b. On your computer's hard drive, select one or more graphic files with the following extenstions: jpg, jpeg, png, webp, gif and click **Open**. These files will be displayed in the card in preview mode.
- **A link to the Traffic Monitor event** (for details, see "Adding Event to Investigation")

11.3 Collaborative Investigations

Collaborative work on investigations is one of the main ways to achieve high efficiency. For this purpose, we have implemented co-editing of investigations. Herewith, you need to consider features of co-editing investigations:

Actions	System response
If a Security Officer opens an investigation for viewing and at the same time another Security Officer adds new material	The first Security Officer gets a notification that the investigation has been modified. The first Security Officer will be able to save their changes and changes made by both Security Officers will be merged.
If a Security Officer is trying to save changes to the investigation that has already been deleted by another Security Officer	The first Security Officer will get a notification saying that the removed material is unavailable and changes cannot be saved.

11.4 Editing, Exporting, Printing and Deleting Investigation

To change the investigation name:

1. Open the investigation card.
2. Click .
3. Enter a new name and click **Save**.

To export/print the investigation card:

1. Open the investigation card.
2. Click .
3. Choose either of the following:
   - Print PDF document. Information from the card will be printed using standard browser tools.
   - Save an archive to a hard drive. The archive includes a PDF document with text data on the investigation and attachments.

To delete the investigation:

1. Open the investigation tab.

2. Click .
3. In the window that opens, click **Delete**. The investigation can be deleted only by its author.

12 Reports Section

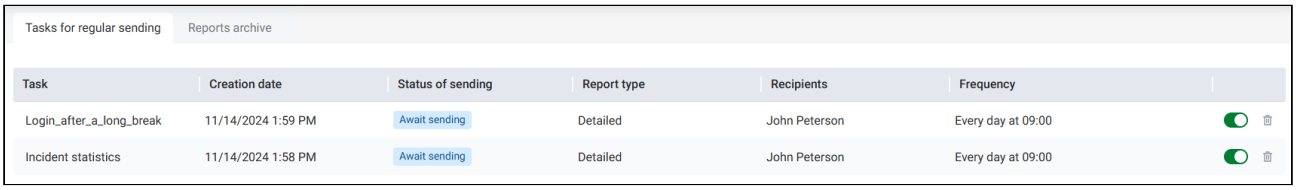
In this section, you can:

- view the reports list and download reports on **Reports archive** tab;
- view and edit tasks for regular sending on **Tasks for regular sending** tab.

12.1 Tasks for Regular Sending

The list of tasks for regular sending contains the following fields:

- **Task** – name of the report for which the task is created;
- **Creation date** – date and time when the task is created;
- **Status of sending**;
- **Report type** – detailed;
- **Recipients** – Security Officer who gets the report;
- **Frequency** – days of the week and time when the Security Officer gets the report.



On **Tasks for regular sending** tab, you can:

- **Change the task name**. For this, click on the current name and enter a new one.
- **Disable the report sending** for a certain period. For this, use the button.
- **Delete a task**. For this:
  1. In the task line, click .
  2. In the window that opens, click **OK**. The task will be deleted.

12.2 Reports Archive

The tab represents a table with files for all reports created in the Investigation Centre.

For each report, you can view its data:

- Name;
- Size;
- Date and time when the report was created.

To download the report, click next to it. The report will be saved to **Downloads** folder of your computer. For details on exporing reports, see "Creating, Unloading and Printing Reports with Statistics Data" and "Viewing and Exporting Event Data".

The archive may contain reports from different InfoWatch products, but for one user only. The list includes the last 500 reports. You can download files within 30 days after they are generated. If the number of files in the list exceeds 500, the System will remove earlier files.

For easy viewing, you can change the width of the table columns.

13 End-user License Agreement

ATTENTION! Please read the terms and conditions of this End-User License Agreement (hereinafter referred to as the "Agreement") carefully before using the Software. Installation and/or use of the Software shall constitute your full and unconditional acceptance of all the terms and conditions of this Agreement.

If you do not accept to the terms and conditions of this Agreement, or if you enter into this Agreement on behalf of a legal entity, but you do not have such authority, you must interrupt the installation and/or stop using the Software and delete any copies of the same.

1. Grant of License

1.1. This End-User License Agreement shall constitute a standard form contract entered into by and between the End User and Laboratory InfoWatch LLC, Taxpayer Identification Number (INN) 7734583888 (hereinafter referred to as the "Copyright Holder").

1.2. You shall be granted hereunder a personal, non-transferable and non-exclusive license granting you the rights to use the Copyright Holder's software (hereinafter referred to as the "Software"), namely the rights to download, install, backup and use the Software for its intended purpose, as set forth in the Software Documentation (User's Guide, Administrator's Guide, Installation Guide), this Agreement and your Licensing Agreement. The Software Documentation shall be an integral part hereof.

1.3. If you have received, downloaded and/or installed the Software for information, you may use the Software only for informational purposes and only during the trial period. Any use of the Software for any other purposes or after the trial period shall be prohibited.

1.4. If you use different Software versions or Software versions for different languages, or if you receive the Software on several media, or if you otherwise receive several copies of the Software or receive the Software as part of a package of other software, the total number of your licenses shall not exceed the number specified in your Licensing Agreement.

1.5. You may make a copy of the Software, provided that such a copy is intended only for archival purposes or to replace a duly purchased copy in cases where the original is lost, destroyed or becomes unusable. This copy may not be used for any other purposes and shall be destroyed, if the possession of the Software copy ceases to be legitimate.

1.6. You shall be solely responsible and ensure compliance with the applicable export and import laws, as well as applicable trade sanctions and embargo with regard to the transfer of rights and use of the Software.

2. Terms and Conditions of Use

2.1. The Software is intended solely for use in analyzing and checking corporate information, and specifically for detecting and preventing unauthorized use of confidential data.

2.2. You shall use the Software exclusively in accordance with the applicable statutory requirements of the Russian Federation or any other countries, including but not limited to:

- legislation on personal data;
- legislation on trade secrets;
- legislation on combating the misuse of insider information;
- anti-corruption legislation;
- legislation on critical information infrastructure;
- legislation on state information systems;
- National Payment System data protection legislation;
- statutory provisions of the Labor Code of the Russian Federation;
- and any other applicable sources of law.

2.3. You may not use the Software for any purpose or in any manner that violates applicable law, this Agreement and/or any third-party rights. The Copyright holder shall not be liable for your breach of this Clause.

2.4. If you are not a resident of the Russian Federation, you shall use the Software in full compliance with applicable law, including laws and regulations on personal data and trade secrets.

2.5 In order to avoid your violation of Articles 138, 138.1 of the Criminal Code of the Russian Federation, Article 23 of the Constitution of the Russian Federation or any other legal regulations, before using the Software, you are recommended to inform your employees in writing that:

- this Software is used on the workstation computer, and you should inform your employees about the features of this Software and data that may be obtained as a result of using the same;
- the workstation computer and the communication channels used (e-mail, local corporate network, telephony and IP-telephony, etc.) are your property and are provided to such employees for temporary use so that they could perform their official duties;
- all information created on the workstation computer is your property and is subject to inspection and logging on a legal basis.

2.6. Please note that you need to obtain the consent of the persons whose data will be processed when using the Software to the relevant collection, storage, use, processing, distribution or any other form processing of such data.

2.7.We remind you that installing a program on another person's computer without prior authorization from such a person, obtaining personal data of any third party without his/her consent, violating privacy, breaching confidentiality of correspondence, telephone conversations, telegraphic or any other types of messages shall constitute a criminal offense and shall be prosecuted, as prescribed by the current legislation of the Russian Federation.

2.8. The Copyright Holder shall not have access to the data created and/or obtained as part of your use of the Software. You shall have exclusive access to such data. In view of the foregoing, the Copyright Holder shall not collect, or store, or use, or distribute such data.

2.9. You shall be held fully and solely liable if the information created and/or obtained as part of your use of the Software contains unethical and/or illegal data, computer viruses or programs (or links thereto) that may interrupt or disrupt the standard features of computer equipment, software or telecommunication facilities of any persons.

2.10. You shall not:

- edit, change, adapt, translate, decompile, disassemble, reverse engineer, create or recreate source code, modify the Software, whether in full or in part, or attempt to do so in respect to the Software, or create derivative works based on the Software and/or Documentation;
- integrate the Software into any third-party website or software product, except where such integration is expressly authorized by the Copyright Holder and the copyright holder of such a third-party website or software product. The Software may be integrated into a third-party software product only through the built-in API module within the features of such a module;
- remove or modify any notice of copyright, proprietary rights to the Software and/or its elements;
- let on lease, rent out or assign for temporary use, sublicense, distribute the Software or otherwise grant any rights with respect to the Software and/or Documentation to any person or entity, or disclose the results of development testing of the Software, except as expressly permitted by this Agreement;
- allow or provide access to the license key to any third party in violation of this Agreement and your Licensing Agreement;
- collect, systematize, store or disseminate confidential and/or personal information in violation of law;
- use the Software for unauthorized remote access to any third-party computer, or changing the configuration of the computer so that such features can appear in third-party software;
- use the Software to collect, store, use, process or distribute any information or data that violates the applicable laws or the rights and legitimate interests of any third party.

2.11. The license key shall constitute confidential information. The Copyright Holder shall reserve the right to use the means to verify the authenticity of the license key you have installed.

3. Disclaimer of Warranties and Liability of the Copyright Holder

3.1. The Software shall be provided "AS IS" in accordance with generally accepted international business practice. The Copyright Holder shall not be responsible for any issues arising during the operation of the Software, including those related to compatibility with other software products (packages, drivers, etc.) or those arising from ambiguous interpretation of the Software Documentation, or for failure of the Software to meet your expectations, etc.).

3.2. You confirm that you are aware of the features of the Software licensed hereunder, and you shall be held fully and solely liable if the Software or the results of using the same do not meet your individual needs or expectations.

3.3. The Copyright Holder makes no warranties, whether expressed or implied, and hereby disclaims all warranties.

The Copyright Holder makes no representations or warranties regarding the fact that the Software is flawless, uninterrupted, fast or accurate, and shall not be resposible for any direct or indirect consequences of using the Software, including those arising from potential errors in the Software or typos in the Software and/or the Documentation attached thereto or further provided.

The Copyright Holder makes no representations or warranties and shall not be held liable in the event of any changes in a third-party software that occurred after the installation/deployment of the Software and resulted in a loss of the Software features (including, but not limited to, a change in the data transfer protocol, data storage format, logic of a third-party software, an update of a software that ceases to support the Software). The Copyright Holder makes no warranties or representations and sets no conditions or provisions (whether expressed or implied) in respect of any matters, including but not limited to infringement of third-party rights, merchantability, integration or fitness for a particular purpose.

3.4. Any data that becomes available in the course of using the Software, including any file, link, image or text, shall be the sole responsibility of a disclosing person or entity and shall be the property of such a person or entity. This Agreement shall not grant any rights to such data. You accept responsibility for any potential consequences, security risks or any losses caused by such data viewed or obtained by using the Software.

3.5. The Copyright Holder shall not be liable for any loss or damage, regardless of the reasons for such a loss or damage (including, but not limited to, direct or indirect damage, lost profits, interruption of commercial or business activities, loss of business information, negligence, or any other losses) arising from the use or failure to use the Software, even if the Copyright Holder has been notified of eventual losses. The Copyright Holder's liability shall be at any time limited to reimbursement for documented actual damage of up to Three thousand rubles (RUB 3,000). The Copyright Holder shall be held liable only for actions or omissions for which the Copyright Holder is at fault.

4. Intellectual Property Rights

4.1. You hereby agree that the exclusive rights to any intellectual property embodied in the Software and /or any documentation provided to you shall be vested in the Copyright Holder. The Software shall not be assigned or sold hereunder, but shall be granted under a limited non-exclusive license. Nothing in this Agreement grants you any rights to the said intellectual property other than those conferred under your Licensing Agreement.

4.2. You agree that the source code and the license key for the Software shall be the property of the Copyright Holder.

5. Rights to Information Accessed in the Course of Performance of this Agreement

5.1. You hereby agree that you do not have any rights to any information that is not subject to intellectual property, as set forth in Section 4, accessed by you in the course of performance hereof.

5.2. Such information may include, but shall not be limited to, any system, method of work or any other information.

5.3. You may use the above information only for the purpose of exercising the rights to the Software granted under this Agreement and the Licensing Agreement. You may not use this information for your own benefit or beyond the scope of this Agreement or the Licensing Agreement.

6. Open Source Software

You are aware that the Software contains open source software distributed under certain licenses, available in the licenses.inf license.info file, provided together with the Software as part of the distribution kit.

7. Miscellaneous

7.1. This Agreement shall come into force immediately upon installing the Software and shall be valid throughout the period of use.

7.2. In the event that you violate any of the provisions of this Agreement and/or your Licensing Agreement, or in the event that the performance of this Agreement and/or your Licensing Agreement violates or may result in violation of the applicable laws, the Copyright Holder shall have the right to repudiate and terminate this Agreement (including, but not limited to, by blocking the license key, terminating the grant of rights) at any time without prior notice. To the extent set forth above in this Clause, you shall not be reimbursed for the cost of the Software/the amount of the Software license fee, or any eventual losses arising under this Agreement and/or your Licensing Agreement.

7.3. Upon termination or expiration hereof, the End User shall destroy all copies of the Software installed.

7.4. You are hereby notified that when the usage statistics collection function is enabled in the Software, the Software may collect and record anonymized information on:

a) hardware, operating system of the device on which the Software is installed and operated, as well as other technical data containing information on the use of hardware, hardware load and processing speed of the Software;

b) end user's activities in the user interface of the Software.

The Copyright Holder may use the specified data to make decisions on the development of features and improvement of the operational characteristics of the Software.

The Copyright Holder shall ensure the confidentiality of the data obtained and shall not disclose or transfer such data to any third party.

7.5. This Agreement, as well as any disputes arising out of or in connection with this Agreement, shall be governed by and construed in accordance with the laws of the Russian Federation.

7.6. All disputes and disagreements arising during the performance hereof shall be resolved through negotiations, if possible. In case of failure to reach an agreement, disputes shall be settled in court in the Arbitration Court of Moscow.

7.7. This Agreement may be amended by the Copyright Holder at any time without prior notice. The amended Agreement shall enter into force once it is posted at the address specified below in this Clause. The current version of the Agreement is always available at https://kb.infowatch.com/display/EULA/. By continuing to use the Software, you accept the amendments and/or additions made to this Agreement. If you do not accept the terms and conditions of such amended Agreement, you shall immediately discontinue the use of the Software.

8. Contact Details of the Copyright Holder

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

Sales Department: sales@infowatch.com

Technical Support: support@infowatch.com

Web site: www.infowatch.ru

14 Glossary

Term	Description
Administrator	Administrator is a user of the System who installs, configures and maintains the System. See also: Main Security Officer, User
Main Security Officer	In the Management Console: the preset user role that has privileges for all actions in the System. See also: Security Officer, User
User interface	A set of means and methods by which the user interacts with the System
Management Console	Graphical user interface for managing DAT (administrating and configuring the System, viewing audit results for directory service and mailbox access rights, tracking changes in access rights to filesystem objects)
Domain controller	A server designed to manage network access within a domain. Directory service information is physically stored on one or more equivalent domain controllers. Each domain controller maintains a read-write copy of directory service data. Changes made on one controller are synchronized to all domain controllers. However, records on object changes are not synchronized between domain controllers. See also: Directory service
License	The right to use the System. The right is obtained by purchasing the System and defines allowed actions with the System
Directory service object	A single directory service entity, such as a user or computer. See also: Directory service, Active Directory
Security Officer	The main user of the Management Console. Also, a preset user role in the Management Console with privileges for all actions in the System, except for administrative ones
Person	An account of the company employee or an external contact that is stored in the directory of the System. Such an account makes it possible to process all account-related data as one whole as well as to display account-related events in a user-friendly form
Platform	Principal design of the product. This is a set of parts, subsystems, interfaces and production processes. The product Platform is the

Term	Description
	basis for deploying the product family and assembling finished products from standardized components
User	A user of DAT: an Administrator, a Security Officer, etc. See also: Administrator, Security Officer
Privileged Group, Critical Group	A group of accounts that are granted rights, privileges, and permissions to perform virtually any activity in the directory service and domain-joined systems. See also: Directory service, Person
Workstation/Computer	In terms of the System, a controlled workstation or terminal device
ClickHouse service	Distributed analytical columnar DBMS designed for real-time analysis of stored data. A component of the product Platform
PostgreSQL service	DBMS that is used in the DAT to store directory service events. A component of the product Platform
Directory service	A means of hierarchical representation of an organization's resources (staff, material and network resources, etc.) and information about these resources. See also: Active Directory, Domain controller
Active Directory (AD)	LDAP-compatible implementation of Microsoft's intelligent directory service for Windows NT family operating systems See also: Directory service, Domain controller
Exchange	Corporate email service by Microsoft
FTP	Network data transfer protocol
InfoWatch Traffic Monitor (InfoWatch TM)	Traffic Monitor is a software package designed to control different types of traffic (SMTP, IMAP, POP3, HTTP, HTTPS, IMAP, XMPP, ICQ, NRPC) and shadow copies of data that are copied to removable media and sent for printing
Kubernetes	Containerized application orchestration software. Orchestration includes automation of application deployment, scaling and coordination in a cluster environment
NATS	Messaging system for components
SMB (Server Message Block)	Network protocol for remote access to files, printers and other network resources. Is also used for interprocess communication

Term	Description
SSH (Secure Shell)	A network protocol that allows remote control of the operating system and tunneling of TCP connections (for example, for sending files)