INFOWATCH

InfoWatch Data Access Tracker. Administration Guide

12/01/2026

© JSC “InfoWatch”

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

http://www.infowatch.com

Table of Contents

1 Who should read this guide 5

2 Set of documents 6

3 Technical support 7

4 Licensing 8

5 System Settings 9

5.1 System Status 9

5.1.1 Diagnostic data 11

5.2 Integrations 11

5.2.1 Integration with Active Directory 12

Information about integrations 14

5.2.2 Integration with InfoWatch Traffic Monitor 15

5.2.3 Editing or Deleting Integration 18

5.3 Users 18

5.3.1 Creating New User 19

5.3.2 Adding New User from LDAP 20

5.3.3 Editing User Account 20

5.3.4 Viewing User Profile 21

5.3.5 Changing User Password 21

5.3.6 User Activation and Deactivation 22

5.3.7 Deleting Users 22

5.4 Roles 22

5.4.1 Creating and Configuring a Role 23

5.4.2 Viewing, Editing and Copying User Roles 27

5.4.3 Revoking and Removing User Role 27

5.5 Audit 29

5.6 Password Settings 31

5.7 Global Settings 32

5.8 Filters 34

5.9 Mail Server 35

5.10 Email Notifications 36

6 Infrastructure Audit Settings 39

6.1 Connection to directory service 39

6.2 Connection to email service 40
6.3 Starting synchronization 40
6.4 Synchronization history 40
7 System Notifications 43
8 Adding User Certificate 44

This guide contains information on how to configure 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.

1 Who should read this guide

This guide is intended for users who configure, support, monitor, and analyze the System.

This guide is intended for users familiar with the basics of Linux and Microsoft Windows operating systems.

2 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.

3 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.

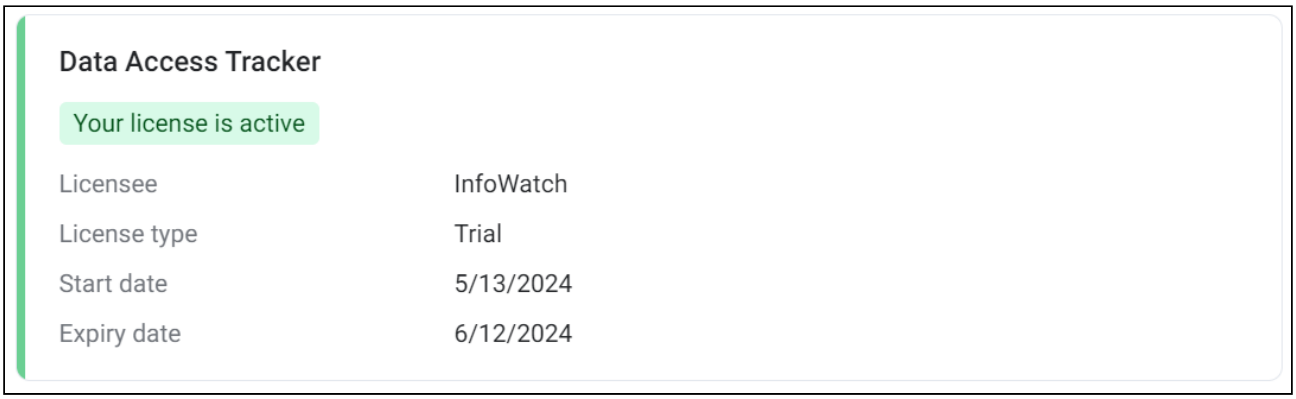
Technical Support Service is available to assist you Mon-Fri, 7 AM – 9 PM (Moscow time, GMT+3), except weekends and public holidays in the Russian Federation. You can also visit technical support section on our website: http://infowatch.com/support.

4 Licensing

You can manage licenses in the **Settings** → **Licensing** section.

To connect to the domain controller, you need an active license in the System.

By default, the System contains a one-month trial license. The trial period begins as soon as you install the product.



To add a license:

1. Click **+ Add**.
2. In the window that opens, add the license file.

To delete a license:

1. In the corner of the license tile, click .
2. Click **OK**.

5 System Settings

In **Settings** → **System Settings** section, you can find information about the following settings:

- System Status
- Integrations
- Users
- Roles
- Audit
- Password Settings
- Global Settings
- Filters
- Mail Server
- Email Notifications

> **Note:**
>
> Data Access Tracker does not use **Data for analysis** section, because the product does not store and use data in partitions.

5.1 System Status

The monitoring subsystem checks the operation of all System elements. It analyses availability of the distributed network elements, information about the main hardware components and status of all System services.

The **Settings** → **System status** section contains panels with information about servers of the Investigation Centre cluster. Each panel contains the following information:

Field	Description
Label (name)	Label and name of the node in the format: *label (name)*
Status	Status of the node: • *Ready* – available and ready to work • *Not Ready* – not ready to work • *Unknown* – registered, but not responding
Address	The IP address of product node
Latest healthcheck status update	Date and time when information on the node status was received
Kernel version	OS kernel version
Operating System	The operating system of product node

Field	Description
Memory	Server RAM: total and occupied size
CPU	Load of CPU on product server
*Disk space (ClickHouse) **	Total allocated and used disk space for storing ClickHouse database data
*Disk space (PostgreSQL) **	Total allocated and used disk space for storing PostgreSQL database data
*Disk space (Root) **	Total allocated and used space reserved for system data in the root directory
*Disk space (NATS) **	Total allocated and used disk space for storing NATS data
*Disk space (Datastorage) **	Total allocated and used disk space for storing binary data
The list of product node services	
Status	The service may have one of the following statuses: • *Running* – is running • *Stopped* – cannot get the status • *Not initialized* – is being launched • *Not found* – must be on the node, but is missing • *Error* – ended with an error
Name	Service name in the System (*containers*, *pods*)
Version	Service build version
View details	Displaying data on the service state, events, and internal messages

Note:

If other products of InfoWatch Investigation Centre are installed on the server, their services are also displayed in the list.

Note:

* If one of the partitions has 10 GB or less free space left, then the Investigation Centre web interface will display a warning that the disk space limit has been exceeded. This warning cannot be disabled.

If the limit is exceeded:

- On the **Platform office node**, then integrations configured on this node will be stopped;
- On the **Platform central node**, then all integrations in the cluster will be stopped.

To remove this restriction:

1. Go to the **Settings** → **System Status** section.
2. Identify the node and partition that has little space left.
3. Free up the partition using the OS or product.

5.1.1 Diagnostic data

All monitoring events in the System are logged.

To export diagnostic data, in the upper-right corner click **Export system log files**. Log files of the running services from all DAT nodes will be added to diagnostic data. Once diagnostic data has been generated, a ZIP archive that contains TXT files with the logs will be downloaded to your computer.

To download diagnostic data for a *separate* service, click next to the required service. A ZIP archive that contains TXT files with the service logs will be downloaded to your computer.

5.2 Integrations

In the **Settings** → **Integrations** section, you can configure integrations with data sources:

- Active Directory – to get company's up-to-date directory tree Active Directory and to create dossiers;
- InfoWatch Traffic Monitor – to upload events, which you can add to investigations, to the System, as well as to receive data used by other products.

The System uses sources for:

- generating employees' dossiers;
- obtaining the company structure;
- getting new events;
- obtaining directories from sources that are used in events. The sources can be security policies, protected objects, etc.

In the Settings → **System Settings** → **Integrations** section, you can configure integrations with the above source systems and manage them.

In this section, you can:

- Configure integration with Active Directory
- Configure integration with InfoWatch Traffic Monitor
- Edit or delete integrations

Important!

Integration with InfoWatch Traffic Monitor in the **Integrations** section is not related to DAT functionality.

On how to configure connection with domain controller and email server, see "Infrastructure Audit Settings".

5.2.1 Integration with Active Directory

To add an integration with Active Directory:

1. Go to the **Settings** → **System Settings** → **Integrations** section.
2. Click:
   - **+ Add integration** in the centre of the window, if there has been no integration configured before.
   - **+ Add** in the upper-right corner, if there has been another integration configured earlier.
3. Select **Active Directory**.
4. Specify values of the following parameters:

Parameter	Description
Integration name	The connection name, which is used in the Console
Branch	Label of the product node which is used for connecting to Active Directory
Source address	The network address of Active Directory server
Connection type	Select the type of connection to be established: • Unsecure connection (Plain) • Secure connection via LDAP protocol (StartTLS) • Secure connection via LDAPS protocol (TLS) **Warning!** Connection without certificates are not secure.
Certificate	Upload the certificate file in PEM or DER format The parameter is used if a secure connection type is selected
Global port	Port for connecting a global LDAP directory. By default, the following values are used: • 3268: • for unsecure connection (Plain); • for secure connection via LDAP protocol (StartLTS); • 3269 for secure connection via LDAPS protocol (TLS). To select default values, click .
Port	Port for connecting the domain local directory. By default, the following values are used: • 389: • for unsecure connection (Plain)

Parameter	Description
	• for secure connection via LDAP protocol (StartLTS) • 636 for secure connection via LDAPS protocol (TLS). To select default values, click .

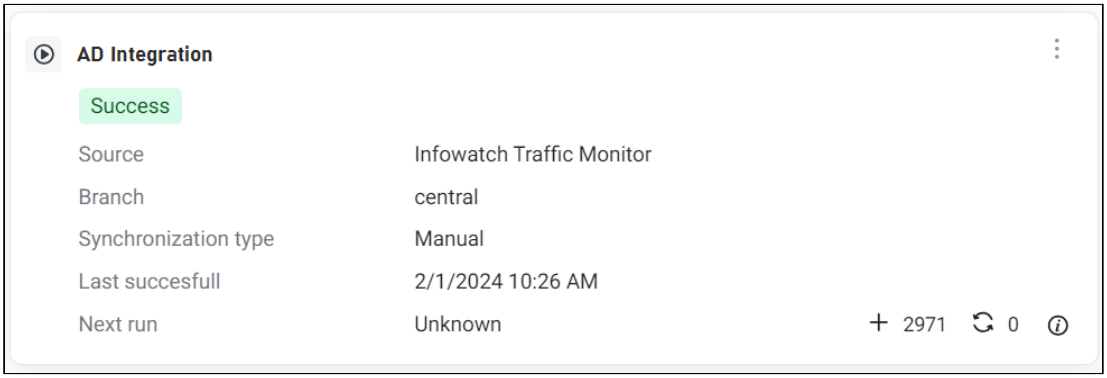
LDAP query	Directory service filtering attributes that are the full path to the specified domain directory. It is possible to specify only one directory in the organizational structure of Active Directory. You can use separate levels of the base hierarchy to optimize your search:
	`C – countryName`
	`O – organizationName`
	`OU – organizationalUnit`
	`DC – domainComponent`
	`CN – commonName`
	Example: To use `Users` branch, which is located in the company domain, as a search base, enter: `cn=users,dc=company,dc=com`

Login	Login to access the Active Directory server (the user must have read access to the directory)
Password	Password to access the Active Directory server
Synchronization	Two synchronization types are available: • *Manual*; • *Automatic*. When selecting *Automatic,* you should specify *Frequency* and *Repetition*. Example of nighttime syncronization setting in order to save time and minimize network load: • *Synchronization period: Daily*; • *Repeat: 12:00 AM*.
Synchronization period	How often to start the synchronization: *Minutely*, *Hourly*, *Daily*, *Weekly*
Repeat	The day of the week and/or time of the next synchronization

5. Click **Test connection** to make sure that all parameter values are specified correctly. Wait for the **Successfully connected** message. If you see the following status:
   - **Could not connect to server** – check if the address and port are correct;
   - **Login or password is incorrect** – check if the login and password are correct.
6. Click:
   - **Save** – to save the integration without starting the synchronization;
   - **Save and start synchronization** – to save the integration and start the synchronization.

Important!

Synchronization with Active Directory can create a high load on the domain servers and the network, so if you are running synchronization with Active Directory for the first time, we recommend doint it at night time.



To start the synchronization manually, click on the integration panel. The process may take some time.

Information about integrations

Synchronization with multiple LDAP directories is possible. Each integration is displayed in a separate panel.

The bottom line of the panel shows:

- – the number of persons, groups and workstations added during synchronizations;
- – the number of persons, groups and workstations whose data was updated during the last synchronization;
- – detailed information on the number of persons added or updated during the last synchronization.

The synchronization status is displayed for each integration:

Status	Description
Not synchronized	Integration is saved, synchronization has not been run yet
Synchronizing	Synchronization is in progress
Success	Synchronization completed successfully
Disconnected	Synchronization has been terminated by the user. The status also contains the date and time when the synchronization was stopped
Error	The status may indicate that: • an incorrect login, password, or address is specified; • product license has expired;

Status	Description
	• an error occurred during the synchronization.

5.2.2 Integration with InfoWatch Traffic Monitor

Integration with InfoWatch Traffic Monitor allows you to upload events, persons, groups and workstations to the Investigation Centre. For persons, you can create dossiers and initiate investigations. For details, see "*InfoWatch DAT. User Guide*", article "Creating, Editing and Deleting Dossier".

> **Note:**
>
> If Vision is installed in the Investigation Centre cluster, then integration with Traffic Monitor allows Vision to use information about protected objects and policies.

> **Important!**
>
> When planning the initial synchronization with InfoWatch Traffic Monitor, please keep in mind that a large number of events from the database can lower the channel capacity and general performance of the server and web console, so we recommend running synchronization with TM during non-working (night) hours.

When you log into the System for the first time, the integration list is empty.

To add a new synchronization with InfoWatch Traffic Monitor and start it:

1. Go to **Settings** → **System Settings** → **Integrations**.
2. In the right upper corner, click **Add**.
3. Click:
   - **+ Add integration** in the centre of the window, if there has been no integration configured before.
   - **+ Add** in the upper-right corner, if there has been another integration configured earlier.
4. Select **InfoWatch Traffic Monitor** and specify the following parameters:

Parameter	Description
Integration name	The integration name
Branch	Label of the product node which is used for connecting to Active Directory
Source address	The network address of a working TM server
Token	A token, which is required to receive data from the TM server (see "*InfoWatch DAT. Installation Guide*", "Traffic Monitor License and Plugin" article)

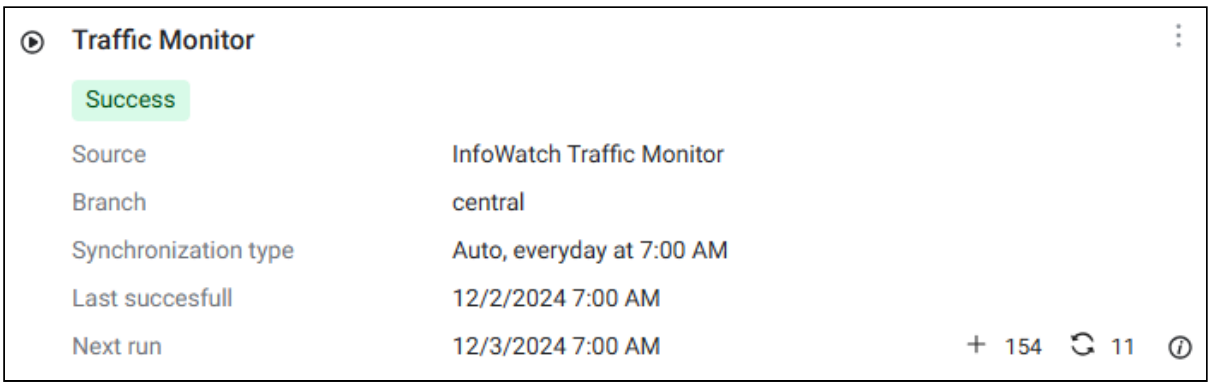
Parameter	Description
Number of download threads	The number of active threads used to upload events and directories from Traffic Monitor. Increasing the number of threads will result in a higher load on Traffic Monitor database. We recommend specifying the number of threads not greater than the number of Traffic Monitor server cores.
Events loading interval (minutes)	The time interval during which events occurred in Traffic Monitor. The data on these events will be loaded to the System as one thread. The default value is 120 minutes. Minimizing this parameter allows you to reduce the load on Traffic Monitor when sending data.
Use archiving options when downloading	If you enable this parameter, events for the last N weeks (the N value is set in the archiving settings) up to the current date will be loaded. The default value is 12 weeks. If the parameter is disabled, events for all the time will be loaded
Not to download LDAP data	Enable the parameter if you require downloading only data for analysis from Traffic Monitor while excluding downloading of persons, groups and workstations. In case the data has been already downloaded to Investigation Centre, enabling the parameter will not remove them.
Download events details	If the parameter is enabled, not only the main data but also event details will be loaded from Traffic Monitor.
Deferred loading	If the parameter is enabled, event details will be loaded at the specified time.
Time of deferred loading	Start time for detailed data loading
Synchronization	Two synchronization types are available: • *Manual*; • *Automatic*. When selecting *Automatic,* you should specify *Frequency* and *Repetition*. Example of nighttime syncronization setting in order to save time and minimize network load: • *Synchronization period: Daily*; • *Repeat: 12:00 AM*.
Synchronization period	How often to start the synchronization: *Minutely*, *Hourly*, *Daily*, *Weekly*
Repeat	The day of the week and/or time of the next synchronization

5. Click **Test connection** to check if you have specified all required parameters correctly. Wait until you see the "*Successfully connected*" message.
6. Click:
   - **Save** – in this case, the new synchronization will have the *Not synchronized* status and wait to start later;
     or
   - **Save and start synchronization** to start the synchronization.

In the central area, you can see the list of integrations with Traffic Monitor servers.

The bottom line of the panel indicates:

- – the number of persons, groups and workstations added during the last synchronization,
- – the number of persons, groups and workstations whose data was updated during the last synchronization,
- – detailed information on the number of persons, groups and workstations that were added or updated during the last synchronization.



If you need to run one more synchronization with the same parameters:

1. Click .
2. Wait until synchronization is complete. The process may take a long time (e.g., if the data transfer rate over the network is low or a large amount of data is transferred).
3. After successful synchronization with Traffic Monitor, go to the **Events** sections and make sure that the data is received and displayed in the table.

For each integration, its synchronization status is specified:

Status	Description
Not synchronized	The integration is saved, the synchronization has not been started yet
Synchronizing	The synchronization is in process
Success	The synchronization completed successfully
Disconnected	The synchronization was stopped by the user. The status also indicates when the synchronization was stopped (the date and time)

Status	Description
Error	The status may indicate that: • You have entered an incorrect login, password or address; • There is no plugin/license for using the Investigation Centre in TM; • A license for DAT has expired; • An error occurred during the synchronization.

5.2.3 Editing or Deleting Integration

To edit an existing integration:

1. In the upper-right corner, click  and select **Edit**.
2. Edit the integration.
3. Click **Save**.

To delete an integration:

1. In the upper-right corner, click .
2. Select **Delete** and then click **Ok**.

> **Note:**
>
> The data received as a result of synchronizations will not be deleted if you delete the integration.

5.3 Users

During the installation of the System, a pre-installed user is created. This user is called the Main Officer. To log into the System, use the default login and password:

Login	Password
officer	xxXX1234

When you first log into the System, you should change your password to a permanent one (see "Changing User Password").

The main page of the **Users** section contains the list of users who are allowed to work in the System:

- The Main Security Officer
- Other Security Officers who report to the Main Officer

User's actions:

- Creating New User
- Adding New User from LDAP
- Editing User Account
- Viewing User Profile

- Changing User Password
- User Activation and Deactivation
- Deleting Users

5.3.1 Creating New User

The Main Officer can add new users who can also be the Security Officers. For this:

1. Go to **Settings**  → **System settings** → **Users**.
2. In the right upper corner, click **Create**.
3. Select **Create user**.
4. Specify values as described in the table below:

Parameter	Description
Photo	User photo
*Username**	Name of the new user. It must contain at least four characters.
*Login**	Name of the user account: • Is not case-sensitive; • Must start with a letter and not end with a dot; • May consist of Latin letters, Arabic numerals and contain special characters: "_", "-", "_", "."
*Password**	Account password (for password requirements, see "Password Settings")
*Confirm password**	Account password
Role	User role in the System. Each user may have only one role
Console language	Interface language for the new user: *Russian* or *English*
Display functions of installed products only	Switcher which makes sections and widgets for not installed products invisible
Contacts	Mobile phone number. You can add multiple values

** – the parameter is required*

5. Click **Create**. The new user will be added to the System. When logging into the System for the first time, the user should change their account password (see "Changing User Password").

5.3.2 Adding New User from LDAP

The Main Officer can select new users from LDAP directory and grant them the rights of Security Officers. To add a new user from LDAP directory:

1. Go to **Settings** → **User settings** → **Users**.
2. In the right upper corner, click **Create**.
3. Select **Add from LDAP**.
4. Select an available LDAP server, integration with which has been configured in the System (see "Integration with Active Directory").
5. In the search bar, start typing a full name or login.
6. Select the user in search results and click **Add**.
7. Assign a role to the user (see "Editing User Account").

The user will be added to the list of the System users. The user can log into the System using the domain credentials. The account login has the following format: `domain\login` or `login@domain`. The account login is not case-sensitive.

> **Note:**
>
> The security requirements (see "Password Settings") do not apply to users added from LDAP directory. Users from LDAP directory cannot change their passwords in the System.

> **Important!**
>
> Changes to the account made in Active Directory will be available in the System only after you add the account again: delete the account and then add it to the System again.

5.3.3 Editing User Account

To edit the user account:

1. Go to **Settings** → **System settings** → **Users**.
2. Open the menu. For this:
   - in the **Users** section, click ⋮ in the user line, or
   - open the user's personal card and click ⋮ in the right upper corner.
3. Select **Edit**.
4. In the window that opens, edit one or more parameters. You can edit the parameters that were specified when creating the user ("Creating New User").
5. Click **Save**. The new settings will take effect.

To assign a role to the user:

1. Go to **Settings** → **System settings** → **Users**.
2. Select the user.
3. In the user personal card, open the **Access Rights** tab and click the Apply role link.

4. In the **Role** field, select a role from a drop-down list. Users without roles cannot work in the System.
5. Click **Save**.
6. To apply changes, the user with this role should log out of the System and then log in again. To force the user session to end, select **End users active sessions**.
7. Click **Apply** to confirm. The new role will be assigned to the user.

5.3.4 Viewing User Profile

The profile page contains the user personal card with the following data:

1. The **Personal info** tab contains:
   - User photo;
   - Username;
   - User login in the System;
   - User language in the System;
   - Contact data: phone numbers, email addresses;
   - Log of recent actions with the account.
2. The **Access rights** tab contains information about the user rights in the System:
   - Role assigned to the user;
   - Available functions:
     - User access to products and settings;
     - Set of data the user may access.

   You can assign or revoke a role in the account editing window (see "Editing User Account").

User actions:

- Editing User Account
- Changing User Password
- User Activation and Deactivation

5.3.5 Changing User Password

The Main Security Officer can change a password for a user. Other Security Officers can change other users' passwords provided that the Security Officer has access to user settings.

To change a password that was provided for the first login or has been compromised:

1. Go to **Settings** → **System settings** → **Users** section.
2. Do either of the following to open the menu:
   - In the **Users** section, click in the user line;
   - Open the user personal card and click in the right upper corner.
3. Select **Change Password**.
4. Fill a new passowrd into *New password* and *Confirm password fields*.

   Important!

   The password must meet the security settings. See "Password Settings" for details.

5. Click **Save**.

5.3.6 User Activation and Deactivation

The Main Security Officer can deactivate users. Deactivated users cannot perform any actions in the System. Other Security Officers can deactivate users provided that the Security Officer has access to user settings.

To block the user account:

1. Go to **Settings** → **System Settings** → **Users** section.
2. Open the menu. For this, do either of the following:
   - In the **Users** section, click in the line of the user;
   - Open the user personal card and click in the right upper corner.
3. Select **Deactivate** depending on what you need.

To activate an earlier deactivated user, follow steps 1-2 of the previous instruction and then select **Activate**.

5.3.7 Deleting Users

The Main Officer can delete user accounts. For this:

1. Go to **Settings** → **System Settings** → **Users** section.
2. Open the menu. For this, do either of the following:
   - In the **Users** section, click in the line of the user;
   - Open the user personal card and click in the right upper corner.
3. Select **Delete**.
4. In the dialog box, click **Ok**. The user account and all its data will be permanently deleted from the System.

> **Note:**
>
> The account of the Main Officer cannot be deleted.

5.4 Roles

Users of the System may have different roles that define their rights in the System. Users without a role cannot access the System.

Each **User** working in the System can have only one **Role**. The **Role** includes **Functions** and **Data** with the following access types: ***full***, ***read-only*** and ***forbidden***.

The main page of the **Settings** → **System settings** → **Roles** section contains all roles that are used in the System. They include custom roles and two pre-installed ones:

1. The **Main Security Officer** has full access to all System data, System settings and role management including:
   - Creating new users;
   - Creating new roles and assigning them to users.
2. The **Security Officer** has full access to System data except for the **Settings** section.

You can find information about roles on the following tabs:

- **Functions** – access of the user with this role to products, their functions and settings;
- **Data** – access of the user with this role to data;
- **Users** – on this tab, the Main Officer can assign roles to users or revoke roles from them.

You can assign the role:

- When creating a new user;
- When editing a role;
- By adding it from the list of existing roles in the user card on **Access rights** tab.

User actions:

- Creating and Configuring a Role
- Viewing, Editing and Copying User Roles
- Revoking and Removing User Role

5.4.1 Creating and Configuring a Role

System user with the role **Main security officer** can create new user roles with different functions and work with data in accordance with role assigned.

If the set of functions changes, you can either:

- edit the role;
- create a new role and then assign this new role instead of the old one.

If all users have different functions, you should create a separate role for each user and create all required terms within the roles created.

To create a role:

1. Go to **Settings** → **System settings** → **Roles**.
2. Click **+ Create**.
3. In the opened window enter the role name and short description, if required.
4. Click **Save**.
5. On the **Functions** tab, specify the access level to products and settings for users with this role:
    a. In the list of **Functions**, select the checkmark as per products and sections the user should have full access to. By default, a user whose role does not contain open access can authorize in the System and work in **Main** and **Persons** sections.

> **Access to Platform functions**
>
> Access to *Events*, *Violation statistics* enables you to use functionality of **Events**, **Reports** and **Analytics** sections, including **Date**, **Senders**, **Recipients**, and **Event type** widgets.
>
> Access to *Investigations* enables you to work in this section.
>
> Access to *Event details* enables you to navigate to Traffic Monitor for additional event information, as well as use:
>
> - **File type**, **Top files**, **Event list** widgets
> - **Attachment name**, **Attachment existence**, **Attachment type**, **Email subject** filters

Access to *Violation details* enables you to unload data about details to the report and to use:

- **Violations**, **Violation level**, **Verdict**, **Statistics**, **User decisions** widgets, including corresponding filters
- Highliting and colouring of events by violation type

Access to *Policies, Protected objects and Perimeters* enables you to use:

- **Policies**, **Protected objects**, **Statistics** widgets, including corresponding filters
- Additional columns in **Events** section

Access to *Dossier status* enables you to use the filter's attribute and **Status** widget in a person's dossier.

Access to Platform products

Data Access Tracker

Access to *Infrastructure* enables you to use the tabs of **Infrastructure** section:

- Data Access Tracker widgets on **Dashboard** tab (as well as on **Main** page);
- Reports on statuses and changes of directory service objects on **Directory audit** and **Group changes** tabs;
- Reports on access to mailboxes on **Access to mailboxes** tab;
- Reports on changes in access rights to filesystem objects on **File and folder access changes** tab.

Activity Monitor

Access to *Analytics* enables you to use:

- Statistics and activity events in **Analytics** and **Monitoring** sections
- Activity events filter attributes corresponding to available widgets
- Activity Monitor widgets in **Persons** section and on **Main** page
- Report functionality in **Analytics**, **Monitoring** and **Reports** sections

Access to *Screenshots* enables you to:

- Display screenshots in **Monitoring** and **Persons** sections
- Display and filter corresponding events

Access to *Audio records* enables you to:

- Display data on audio recordings in **Monitoring** and **Persons** sections
- Display and filter corresponding events

Access to *Videos* enables you to:

- Display data on videos in **Monitoring** and **Persons** sections.

Access to *Monitoring* provides you with monitoring and timeline in **Monitoring** and **Persons** sections.

Access to *Online monitoring* enables you to:

- View a person's workstation display
- Listen to audio on a workstation
- Lock a person's session
- Request a list of processes running on a person's workstation

Access to *Input text* enables you to:

- Display entered text in connected events,
- Filter events by presence of entered text

Access to *Web search queries* enables you to:

- Display search queries in connected events
- Filter events by presence of search queries

Access to *File operations* enables you to:

- Display file operations and connected events in **Monitoring** and **Dossier** sections
- Filter events by file operations
- Unload reports in **Monitoring** section

Data Discovery

Access to *File sharing* enables you to:

- Work in **File sharing section**:
  - On **Scanning** tasks tab – to create and run scanning tasks;
  - On **File information** tab – to analyze scanning results;
- Work **in persons' dossiers on File sharing tab**, including the following sections:
  - **File owner**
  - **Available files**
- Unload reports with information from person's dossier subsections: **File owner** and **Available files**, as well as from the **File information** tab in **File sharing**

Prediction

Access to *Dossier, Rating* enables you to:

- Work with persons rating in **Risks** section;
- Work in person's dossier on **Risk groups** and **Pattern map** tabs;
- display widgets on the **Main** page on dashboards;
- unload reports in **Risks** section and on **Risk groups** tab in person's dossier.

Vision

Access to *Graph* enables you to use graph functionality.

Access to *Violation statistics* enables you to work with:

- Statistics in **Analytics** and **Persons** sections, as well as to unload reports
- Widgets in Vision on **Main** page
- Report files in **Reports** section

Access to *Comments and files in the Dossier* enables you to:

- Use **Comments** and **Files** in a person's dossier
- Create an unloading or a screenshot of a widget or a graph and save it in the dossier

b. In the list of settings, you should select:
   - , if the user should have full access (view and editing) to settings in the  section. By default, access is denied;
   - , if the user should have view-only rights for selected sections;

- ☐, if you should restrict access to specific sections.
  Regardless of the selected access level, a user always has full access to personal information in their own profile.

6. On the **Data** tab, you can specify access restrictions for the user. To change the user access level to specific data, specify data categories: *Persons*, *Groups*, *Branches*, *Departments*, *Contacts*, *Policies*, *Protected objects*. You can:
   a. ☐ – restrict access to selected data;
   b. ☑ – provide access to selected data;
   c. ☒ – prohibit access to selected data.

> **Example:**
>
> If you mark a *Person* with ☒, this role will prohibit access to any data in the System for the user.
>
> If you mark a *Person* with ☑ (or leave by default ☐ for all *Persons*), this role will grant the user a full access to person's data: events, dossier, in *Single filter*, displaying on *Graph* and widgets.
>
> If you mark a *Person* with ☐ with simultaneous selection of other *Persons*, this role will grant user access to its events with participants allowed (☑), but with no access to *Graph* displaying, widgets and *Single filter*.

> **Note:**
>
> Main security officer should carefully monitor which conditions were added, since you may narrow available data when using AND instead of expansion which is required when using different role elements.
>
> **For example:**
>
> a. Access was given to *Group-1* OR *Group-2*.
>
> b. Then access was added to *Person-1*, *Person-2*, *Person-3*.
>
> As a result, the quantity of available data decreased, since you get a condition: (*Group-1* OR *Group-2*) AND (*Person-1* OR *Person-2* OR *Person-3*).
>
> To set up one general restriction for groups and persons, Security offcier should create an integrated group including all required groups and persons and use this group in access settings.
>
> Correct visibility scopes and exceptions adding shoud be verified in *Single filter*, when setting the same conditions and checking the results with widgets used.

7. If you need to deny access to all data, select ☑ **Deny access to data**.
8. On the **Users** tab, the Main officer can select a user without a role and assign the created role to this user. For this:
   a. Click **+ Add**.
   b. In the **Users** field, select a user.

c. Click **Assign**. The role will be assigned to the user.

9. After you have specified all settings, click **Apply**.
10. For the changes to be applied, users should log out of the System and get authorized again. Until the logout, former rules of role access will apply. To forcibly end the session for users with this role, in the dialogue box that opens, select ☑ **End users active sessions**, then click **Apply**.

5.4.2 Viewing, Editing and Copying User Roles

The Main Officer can view and edit roles assigned to users in the users' profiles. For this:

1. Go to **Settings** → **System Settings** → **Roles**.
2. Click the user whose profile you want to view. On the profile page, you can see the user card with the personal data.
3. Open the **Access rights** tab. The tab contains information about the user role. You can also find there:
   - Functions – if the user has access to the product settings;
   - Data (visibility scopes) – the set data the user has access to.
4. To change the user role, click ⋮ and select **Edit**.
5. In the window that opens, remove the current role by clicking ×.
6. Assign a new role by clicking ▾ and selecting the required role from the list.
7. Click **Save**.
8. For the changes to be applied, the user should log out of the System and get authorized again. To forcibly end the session for users with this role, select ☑ **End users active sessions**, and then click **Apply**.

To copy a user role, e.g., when expanding the staff or for auditing:

1. Go to **Settings** → **System settings** → **Roles**.
2. Click ⋮ on the tile of the role you need to copy and select **Copy role**. The following role parameters will be copied:
   - **Name** – each copying adds the **Copy** word to the original name until the name of the role becomes unique:

     > ⓘ **Example:**
     > After copying, the *Officer* name will change to *Officer copy*. To rename the role, you should edit it.

   - **Description**;
   - **Access settings** – all settings (function and data elements) are copied;
   - **Creation date** – the current date and time are specified.

The list of users to whom the role is assigned is not copied.

5.4.3 Revoking and Removing User Role

The user cannot have more than one role at the same time. So, if you need to assign a new role to a user, you should first revoke the current role. You can do it either in the user card or in the role card.

To revoke a role in the role card:

1. Go to **Settings** → **System settings** → **Roles**.
2. Select a role you want to revoke.
3. Open the **Users** tab.
4. Select next to users from whom you want to revoke the role.
5. Click **Delete**. The role will be revoked from selected users and you will be able to assign a new role to these users.
6. Click **Apply**.

To revoke a role in the user card:

1. Go to **Settings** → **System settings** → **Users**.
2. Do either of the following:
   - Click on the panel of the user from whom you want to revoke the role.
   - Select the user and then click in the user's card.
3. In the menu, select **Edit**.
4. In the **Roles** field, revoke the role by clicking .
5. Click **Save**.

> **Note:**
>
> For the changes to be applied, the user should log out of the System. To forcibly end sessions for this user, select **End users active sessions**.

6. Click **Apply** to confirm. The role will be revoked from this user and you will be able to assign a new one.

> **Note:**
>
> The Main Officer can remove all roles except for preset ones.

To remove a role from the System:

1. Go to **Settings** → **System settings** → **Roles**.
2. Do either of the following:
   - Click on the panel of the role you want to remove.
   - Select the role and then click .
3. In the menu, select **Delete**.

> **Note:**

For the changes to be applied, users with this role should log out of the System. To forcibly end sessions for these users, select ☑ **End users active sessions**.

4. Click **Remove** to confirm. If the role has been assigned to some users, it will be revoked from those users and removed from the list of roles. Then you will be able to assign new roles to the users.

5.5 Audit

The section displays the log of users' actions in the System. Only the user who has access to the section can view its data (for more information, see "Roles").

The log contains the following information:

- **User** who performed an action;
- **Action in the system** performed with an object;
- **Object type**: user, integration, dossier, role;
- **Event object** with which the action was performed (for example, a role or integration);
- **Branch** – the name of the branch where the audit event was detected;
- **Date** and time when the audit event was created.

Note:

The System keeps audit logs indefinitely. They cannot be deleted.

The following actions are audited:

Users	• Log in • Log out • Create • Change • Delete • Password change • Block user
Roles	• Create • Change • Delete
Integrations	• Create • Change • Delete • Run manually
Dossier	• View • Create • Change • Delete • Combine

In **Audit** section, you can:

- Unload audit events in CSV format;
- Move columns in the table;
- Sort columns content (by default, events are sorted by date, from the latest to the earliest);
- Switch to a user card in **User** section, when you click on the user;
- Add a filter to the panel or remove it;
- Sort events by selecting filters;
- Copy content of cells.

By default, the following filters are displayed:

- *Date*;
- *Action in the system*;
- *Event object*;
- *User*;
- *Object type*;
- *Branch*.

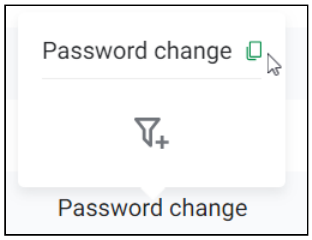
To manage filters on the panel, use the **Add/delete filter** button . Select the checkbox , to add the filter to the panel. Or deselect the checkbox to remove the filter.

To sort events, select a filter attribute:

- On the panel above the table;
- In the table. For this:
  a. Point the cursor to the cell.
  b. Press **Add to filter** . The table content will be sorted according to the selected filter.

To copy the content of a table cell:

1. Point the cursor to the cell content.
2. Point the cursor to the line with the content, then press **Copy** .



In the **Date** column, **Copy** button is displayed when you point the cursor on a cell content.

To unload a report on audit events:

1. Press **Save report** .
2. Go to the **Downloads** folder of your computer.

If you moved columns in the table, keep in mind that unloadings preserve the default order of columns.

To view the report in Excel, you need to enable the UTF-8 encoding. For details, see "How to enable UTF-8 encoding in Excel" article in Knowledge Base.

5.6 Password Settings

The Security Officer can set rules for generating account passwords and password expiration dates. This is needed to prevent unauthorized access to the System and protect users from compromising their account data to third parties. To set these rules:

1. Go to **Settings** → **System settings** → **Password settings**.
2. You can see the default password settings. To set new requirements for passwords, modify the following parameters:

Parameter	Description
Letters	Uppercase and lowercase letters of the Russian and Latin alphabets that can be used in the password. You can set the following values: ☑ – the password must include letters ☐ – you can use passwords without letters
Digits	Arabic numerals that can be used in the password. You can set the following values: ☑ – the password must include numbers ☐ – you can use passwords without numbers
Special symbols	A list of special characters the password may include. You can set the following values: ☑ – the password must include special characters ☐ – you can use passwords special characters
Minimal length	The minimum password length
Latest N passwords cannot be used	Select the option if you want to forbid using passwords from previous periods as they could be compromised
Time before password expires	How long the password is valid. The user should change the password before the expiration date
Failed login attempts period	For how many minutes the user can enter invalid passwords
Number of invalid input attempts	The number of unsuccessful input attempts after which the account is blocked
User blocking period	For how many minutes the user account is blocked

> **Note:**
>
> If necessary, you can change the required sets letters, digits and special characters in corresponding fields.

3. Click **Save** to apply new parameters. If you need to restore original settings, click **Reset to default settings**.

> **Example:**
>
> *Failed login attempts period – 5.*
>
> *Number of invalid input attempts – 4.*
>
> *User blocking period – 15.*
>
> If you set these settings, then, after 4 unsuccessful attempts to enter the password within 5 minutes, the user account is blocked for 15 minutes. In 15 minutes the user can enter the password again.

5.7 Global Settings

In the **Settings** → **Global settings** section, you can:

- Configure the session settings;
- Configure the period for which the data is displayed;
- Manage the tokens;
- Create the name template;
- Manage statistical data collection.

> **Note:**
>
> The following settings are not supported in the current version of the product (System):
>
> - **Token for Data Storage User**;
> - **Use a proxy server**.

Session settings

You can set the session lifetime – the timeout for the user activity in the Console. If during the specified period of time the System does not detect any activity (mouse movement and keystrokes on the keyboard), the Console will automatically exit. In this case, to continue working, the user must re-authorize in the System.

To configure these settings:

1. In the **Session lifetime** field, specify the required value (in minutes, any number under 100000).
2. In the right upper corner, click **Save**.

Displaying data over a period of time

This setting allows you to set the period for the **Date** attribute of the Single Filter. Select the required parameter in the drop-down list:

- *Any date*;
- *Last 24 hours*;
- *Current day*;
- *Last 3 days*;
- *Last 7 days*;
- *Last 30 days*;
- *Current month*;
- *Last month*.

The default period is 30 days.

Managing tokens

You can connect components to the System using tokens. For this, you need to get a token and specify this token in the component you are connecting. In this version of the System, you can connect the Device Monitor server. The token is created during System installation and has a form of a text string. For details on configuring the Device Monitor server, see the InfoWatch Device Monitor documentation (for the Windows server): "*InfoWatch Device Monitor. User Guide*", "Working in Device Monitor Management Console. General System settings. Configuring Device Monitor server" section, the "Connecting to the Platform server" article.

You can view the token or copy it to clipboard. To copy the token, click  in the **Token for Device Monitor Server** field.

If the token has been compromised, click  to generate a new one.

Creating template name

You can create a template that display the main information about the person using the following attributes:

- First name;
- Middle name;
- Last name;
- Full name;
- Displayed name;
- Name is required;
- Initials;
- Login.

To create a template:

1. Click  and add attributes to the field. You can add all specified atttibutes.
2. Click **Save**. After some time, the changes will be displayed in the System sections.

To modify the template:

1. Remove unnecessary attributes from template string. For this, do either of the following:
   - Remove them manually in the template field;
   - Click  to clear the template;
   - Click  to restore the template original form: *First and Last Name.*
2. Click **Save**.

The display type will apply to all persons in the System that appeared after synchronization with Active Directory.

Collecting statistical data

The statistics collection system accumulates and summarizes data about the user's work in the Console. At the user's discretion, this data can be downloaded and sent to InfoWatch for processing. This is done to improve the quality of the product, assess the demand for a particular functionality and develop new work scenarios.

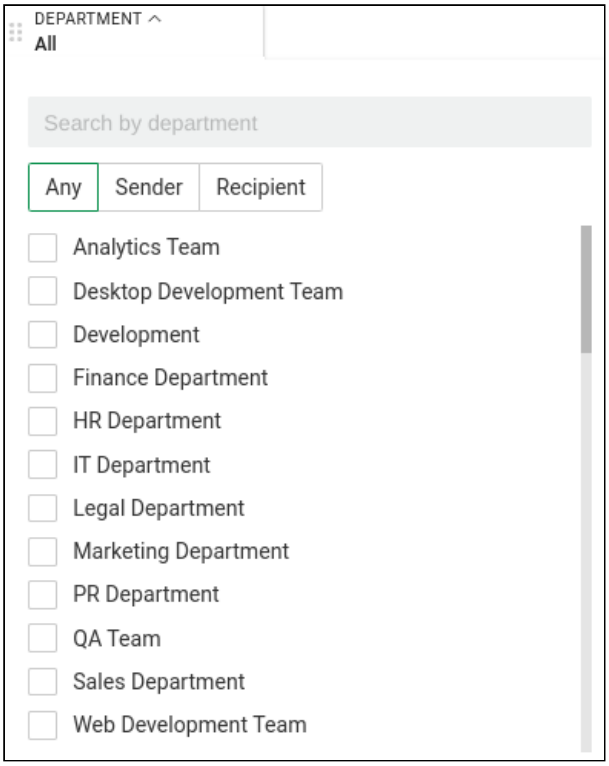
Statistics collection is enabled by default. To disable it, deselect the **Enable** option and click **Save**.

> **Note:**
>
> The statistics collection system does not accumulate, analyze or transmit personal data. All full names of users and employees are replaced with internal system ID numbers.

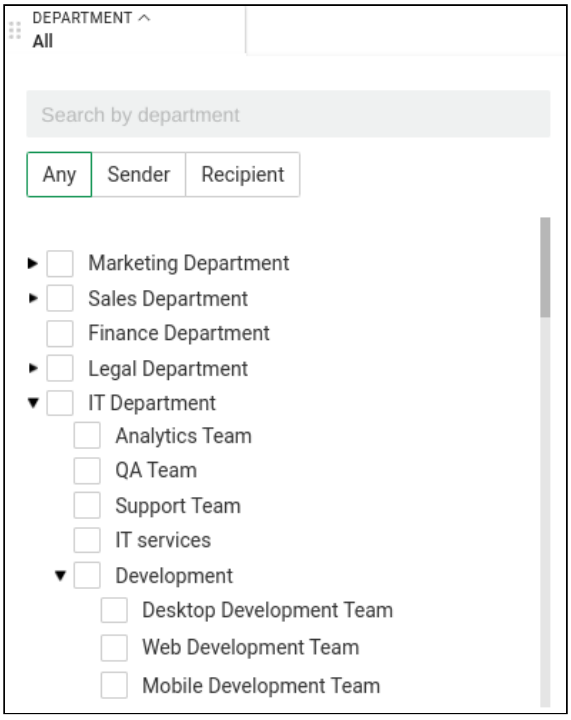
5.8 Filters

When synchronizing with the directory service, the System receives a list of departments. You can customize the display of this list in the Single Filter:

Flat – all departments are displayed at the same level in the list



Hierarchy – departments are displayed as a tree



If you need to load departments without employees, select the ☑ **Upload empty departments** option.

Contact type

You can create a list of domains whose contacts will be considered internal contacts.

To add an internal domain:

1. Click **+ Add domain**.
2. Enter the domain name in the ***companyname.com*** format. The System will consider further contacts with this domain as internal.

Add other domains as needed.

To remove an internal domain:

1. Click  next to the domain name.
2. In the window that opens, click **Ok**.

To apply the new settings, click **Save** and then click **Yes**.

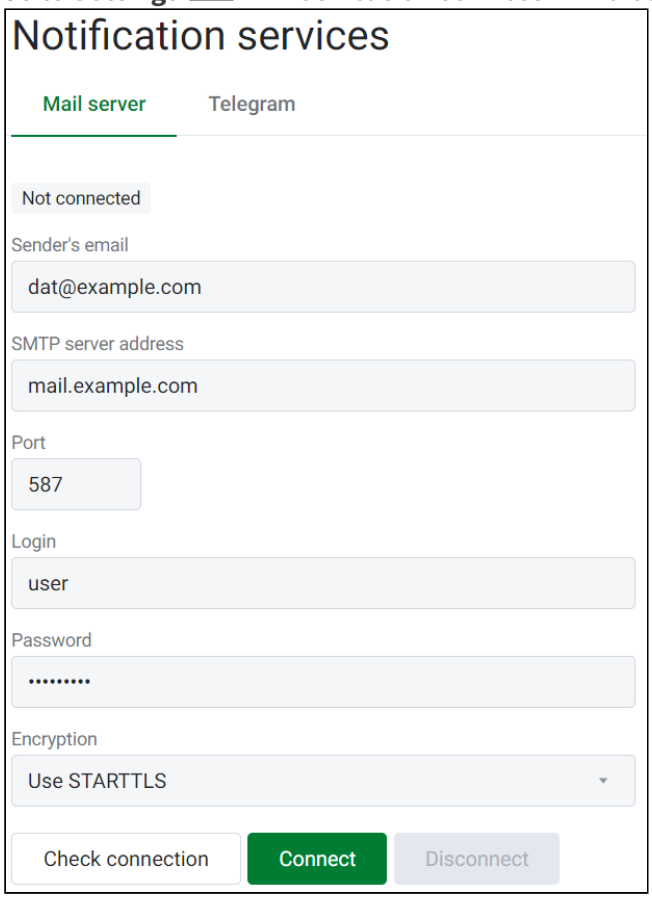
5.9 Mail Server

You can configure the System to send emails containing:

- Notifications on directory group changes. See "Email Notifications" for details;
- XLSX files with reports from **Infrastructure** section. See *"InfoWatch Data Access Tracker. User Guide"* document, "Infrastructure Section" → "Reports Unloading" article for details.

For this set up a connection to a mail server. For this:

1. Go to **Settings**  → **Notification services** → **Mail server**.



2. Specify connection parameters:

Parameter	Desctiption
Sender's email	Email address from which notifications will be sent
SMTP server address	The address of the mail server that operates using the SMTP protocol. Enter the domain name or IP address

Parameter	Desctiption
Port	Mail server connection port
Login	Name of the account that has access to the mail server
Password	Password of the account that has access to the mail server
Encryption	Specify the encryption protocol that will be used when connecting to the mail server. Available protocols: • STARTTLS • TLS

Note:

All parameters are required.

3. To check the availability of the server, click **Check connection**.
4. In case of a successful connection check, click **Connect**.

To change your connection settings or connect to a different mail server, make your changes and click **Update**.

To disconnect from the mail server, click **Disconnect**.

Note:

Working with functionality on **Telegram** tab is not supported in Data Access Tracker version 2.1.

5.10 Email Notifications

You can notify users when directory service groups change including changes in the membership of privileged groups.

Important!

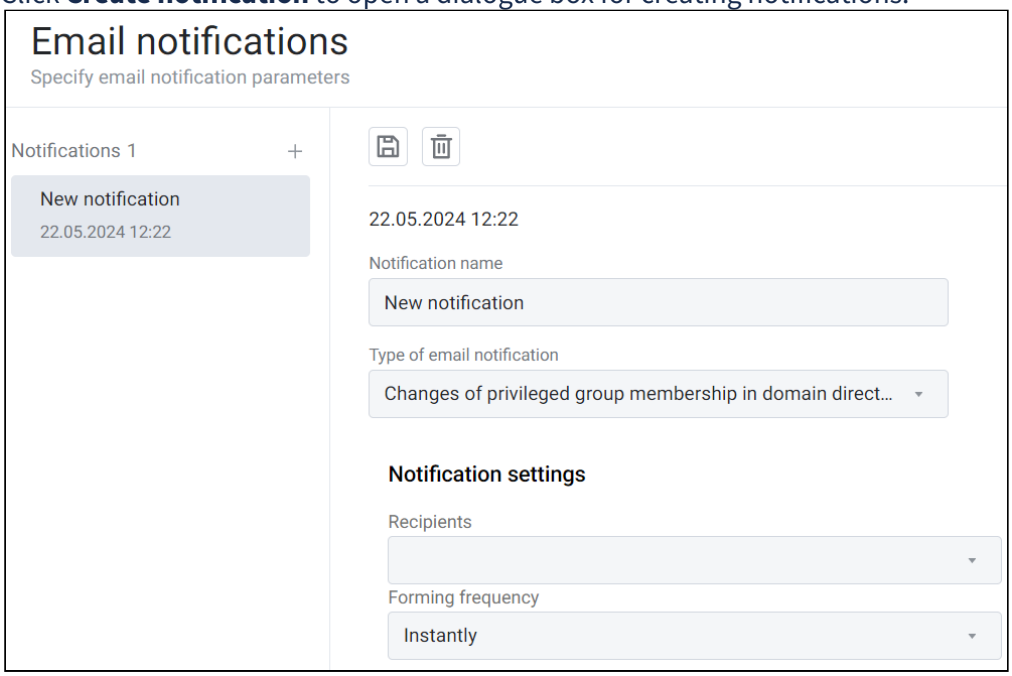
To be able to send notifications, make sure that you have configured connection to mail server. For details, see "Mail Server".

Note:

Notification emails do not contain reports. In order to recieve XLSX files with reports generated by DAT, configure report sending on schedule. For details, see *"InfoWatch Data Access Tracker. User Guide"* document, "Infrastructure Section" → "Unloading Reports" article.

To create email notifications:

1. Go to **Settings** → **Email notifications**.
2. Click **Create notification** to open a dialogue box for creating notifications:



3. Specify the **Notification name**.
4. Select the **Type of email notification**:
   - *Changes to the membership of the privileged groups in the domain directory service* – to get an instant notification whenever someone edits a privileged group;
   - *Changing groups in a domain's directory service per day* – to receive daily reports on all group-related events occured within 24 hours.
5. In the **Receivers** field, click to open the list of available users and select users who need to get the notifications.

> **Note:**
>
> You can select only those users whose contacts contain an email address.

6. The frequency of sending notifications is set automatically:
   a. *Instantly* – for notifications about changes in the composition of privileged groups;
   b. *Daily* – for notifications about changes in the domain directory service per day.
7. In case of *Changing groups in a domain's directory service per day* report, specify the time to send daily report. Default time is 7:00.
8. To save the notification, click at the top.

You can edit or delete an existing email notification.

To edit a notification:

1. Select the notification you want to edit.
2. Make your changes.
3. Click .

To delete a notification, select the list and click  at the top.

6 Infrastructure Audit Settings

In **Infrastructure audit settings** section, you can configure connection with directory and email services, start a synchronization as well as view running and completed synchronizations.

> **Warning!**
>
> Before connecting a domain controller, make sure you have configured it for interaction with DAT. For details, see «InfoWatch Data Access Tracker. Installation Guide», "Setting Up Domain Controller in Active Directory", "Configuring Active Directory Account", "MS Exchange Server Setup" articles.

6.1 Connection to directory service

To add an integration with directory service:

1. Go to **Settings** → **Products settings** → **Infrastructure audit settings**.
2. On **Directory service** tab, select one of the options:
   - **Add controller manually**:
     a. Specify all parameter values:
        - *Controller address* – IP address or domain name of domain controller server;
        - *Login* for authorization on the server (the user should have read access to the directory);
        - *Password* for authorization on the server.
   - **Detect automatically**:
     a. In **Detect controllers automatically** dialogue, specify the parameter values:
        - *Domain* – domain name of the server;
        - *IP address of DNS server* (optional) – explicit indication of DNS server address in case of incorrect default settings.
     b. Click **Search**. The list of detected addresses will be displayed.
     c. Review the address list. If needed, remove certain addresses by clicking ✕ on the right to the address.
     d. Click **Add controllers**.
     e. In **Connection settings for domain controllers** section, specify connection parameters for each server:
        - *Login* for authorization on the server (the user should have read access to the directory);
        - *Password* for authorization on the server.
3. In the upper-right corner, click **Save**.
4. In order to connect to another domain controller, click **+ Add controller** and specify its parameters.

> **Important!**
>
> Connect all domain controllers from which system security log events need to be sent to DAT. Synchronization will be performed simultaneously with all connected servers.

To delete a connection, on **Directory service** tab click  on the right to the line you want to delete.

6.2 Connection to email service

To add an integration with directory service:

1. Go to **Settings**  → **Products settings** → **Infrastructure audit settings**.
2. On **Email service** tab, specify parameter values:
    - *Controller address* – IP address or domain name of domain controller server;
    - Email server address – domain name of email server;
    - *Login* for authorization on the server (the user should be added to *View-Only Organization Management* group);
    - *Password* for authorization on the server.
3. In the upper-right corner, click **Save**.

To delete a connection, on **Email service** tab click  on the right to the line you want to delete.

6.3 Starting synchronization

Synchronization runs for all configured connections simultaneously. For example, if you added three domain controllers and an email server, synchronization will run for all four connections. You can start a synchronization manually or configure an automatic one.

To start a synchronization manually:

1. Go to **Synchronization history** tab.
2. In the upper-right corner, click **Start synchronization manually**.

To set up an automatic synchronization:

1. Go to **Automatic synchronization** tab.
2. Click the switcher .
3. From **Synchronization period** drop-down list, select the synchronization interval value: *5*, *15*, *30* or *60* minutes.
4. In the upper-right corner, click **Save**. Next synchronization start time will appear under the list.

To disable automatic synchronization:

1. On **Automatic synchronization** tab, click the switcher .
2. In the upper-right corner, click **Save**.

To change automatic synchronization interval:

1. On **Automatic synchronization** tab, select a new value from **Synchronization period** drop-down list.
2. In the upper-right corner, click **Save**.

6.4 Synchronization history

Synchronization history tab contains a list of all running and completed synchronizations and their attributes:

- *Start date and time*;
- *Completion date and time*;

- *Status* (*Completed*, *In progress, Error, Exited with errors);*
- *Type* of loaded events (*Audit events*, *Active Directory objects, Access to Exchange mail*);
-  – detailed information:
  - for *Audit events* type – on the number of event records loaded during synchronization with the specified servers. For example:

Domain controller	Uploaded records
10.60.44.35	265
10.60.44.168	11

  - for *Active Directory objects* – on the numbers of discovered/deleted accounts of users and computers, as well as organizational units. For example:

Domain controller	Users		Computers		Organizational units	
	Discovered	Deleted	Discovered	Deleted	Discovered	Deleted
10.60.44.174	102	0	16	0	38	0

  - for *Access to Exchange mail* – on the numbers of discovered/deleted mailboxes and permissions:

Domain controller	Mailboxes		Permissions	
	Discovered	Deleted	Discovered	Deleted
10.60.3.63	57	0	1464	0

By default, lines of more recent synchronizations are displayed at the top the table. You can sort data in the columns in ascending/descending order. The columns with sorted data have  or  icon on the right to them .

To sort records:

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

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

Completion date and time	Start date and time	Status	Type
5/23/2024 11:11:42 AM	5/23/2024 11:08:57 AM	Done	Audit events
5/23/2024 11:09:02 AM	5/23/2024 11:08:57 AM	Done	Active Directory obje...
5/23/2024 10:59:20 AM	5/23/2024 10:56:27 AM	Done	Audit events

To sort values by two and more columns:

1. Sort values by the first column.

Note:

Column priority is defined from left to right. You can change the order of columns by dragging them.

2. Keep **Ctrl** keyboard button pressed and sort the lines in another column.

Example:

Records in the table are sorted by the priority column named **Type** (as it is on the left). Records in the second column are sorted relatively to the first column.

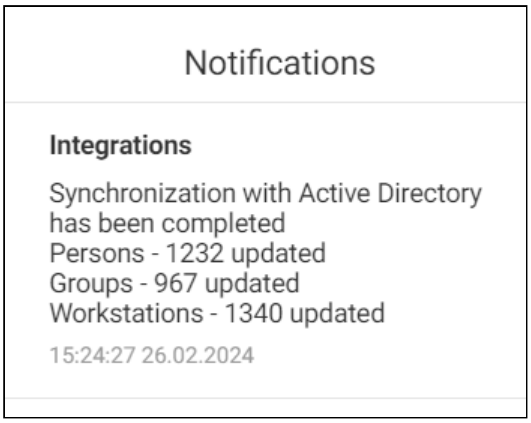
Type	Status	Completion date and time	Start date and time
Audit events	In progress		5/23/2024 11:46:38 AM
Audit events	Done	5/23/2024 7:54:57 AM	5/23/2024 7:52:42 AM
Audit events	Done	5/23/2024 11:11:42 AM	5/23/2024 11:08:57 AM
Audit events	Done	5/23/2024 10:59:20 AM	5/23/2024 10:56:27 AM
Active Directory objects	Done	5/23/2024 11:46:42 AM	5/23/2024 11:46:37 AM

To reset sorting:

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

7 System Notifications

To view the Investigation Centre notifications, click .



Notification may contain the following information:

- The status of user-initiated synchronizations with sources;
- Adding a license;
- Removing a license;
- The current number of dossiers loaded into the System;
- Possible lack of hard disk space;
- Soon password expiration.

8 Adding User Certificate

To prevent unauthorized access to the System and to increase the security of the data transmission channel, you can add a new user certificate for the web service. You can add the certificate via command line at any time while using the System. To add a certificate:

1. Place two PEM files on the disk:
    - A certificate file (e.g., `test.crt`);
    - A private key file (e.g., `test.key`).
2. In the directory with the `setup.py` file, run the command as a user with *root* privileges. Be sure to specify the full name of the files with the certificate and private key:

```
./setup.py setwebkeys --certificate=test.crt --privatekey=test.key
```

The last added certificate is considered valid. After adding or replacing a certificate, you should manually reload all browser tabs used by the System.