

INFOWATCH

InfoWatch Data Discovery. Administration Guide

25/10/2024

© 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

4.1 Trial license 8

4.2 Actions with licenses 8

5 System Settings 9

5.1 System Status 9

5.2 Integrations 11

5.2.1 Integration with Active Directory 12

Information about integrations 15

5.2.2 Integration with InfoWatch Traffic Monitor 15

5.2.3 Editing or Deleting Integration 18

5.3 Users 19

5.3.1 Creating New User 19

5.3.2 Adding New User from LDAP 20

5.3.3 Editing User Account 21

5.3.4 Viewing User Profile 21

5.3.5 Changing User Password 22

5.3.6 User Activation and Deactivation 22

5.3.7 Deleting Users 23

5.4 Roles 23

5.4.1 Creating and Configuring Role 24

5.4.2 Viewing and Editing Role 27

5.4.3 Revoking and Removing User Role 28

5.5 Audit 29

5.6 Password Settings 30

5.6.1 Requirements for the account name 32

5.7 Global Settings 32

5.7.1 Collect statistical data 32

5.8 Notification Services 32

6 Zones and servers 35

6.1 Managing zones 35
6.1.1 Creation 35
6.1.2 Renaming 35
6.1.3 Deletion 35
6.1.4 Adding servers to zone 36
6.1.5 Data export to Traffic Monitor 36
6.2 Managing servers 37
6.2.1 Selecting zone and removing from zone 38
6.2.2 Configuring storage 39
7 Notifications 41
8 Configuring Autodeletion of Data Discovery Events in Traffic Monitor 42
9 Adding User Certificate 43
10 Log File Rotation 44
10.1 Scanning task services 44
10.2 Discoperator service 44
10.3 TPS Agent 44
10.4 Log file rotation 44
10.5 Configuring rotation with logrotate and crontab 45

This guide contains information on how to configure InfoWatch Data Discovery (also referred to as the System or Data Discovery), software designed to search for confidential information on shared network resources, workstations, servers, and in document storages.

1 Who should read this guide

This guide is intended for deployment engineers and security officers who are going to work with the System and administrate it. This guide is intended for users familiar with the basics of the Linux operating system and PostgreSQL DBMS.

2 Set of documents

The documentation includes:

- "InfoWatch Data Discovery. Installation Guide". The document describes how to install, update, and uninstall the System.
- "InfoWatch Data Discovery. Administration Guide". The document contains information on how to configure the System.
- "InfoWatch Data Discovery. User Guide". The document describes how to work with scanning tasks.

Related documentation for InfoWatch Traffic Monitor (also referred to as Traffic Monitor) includes:

- "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, prepare 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

In the **Settings** → **Licensing** section you can manage licenses.

Scanning tasks can be launched only if the System has an active license.

4.1 Trial license

By default, the System has a one-month trial license. The product installation date is the start date for this license.



4.2 Actions with licenses

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. Select **Delete**;
3. Click **Ok**.

5 System Settings

The **Settings** → **System settings** section includes information on the following settings:

- **System Status**
- **Integrations**
- **Users**
- **Roles**
- **Audit**
- **Password Settings**
- **Global Settings**
- **Notification Services**

> **Note:**
>
> Data Discovery does not use the following sections:
>
> - **Data for analysis** – Data Discovery does not store and use data in partitions;
> - **Email notifications** – Data Discovery does not send email notifications;
> - **Filters** – Data Discovery uses separate filters which are not used by other products sections.

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 state of all System services.

The **Settings** → **System status** section contains panels with information about nodes of the Investigation Centre. 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 Data Discovery 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 Data Discovery node

Field	Description
Memory	Server RAM: total and occupied size
CPU	Load of Data Discovery server CPU
Disk space (Clickhouse)	Total allocated and used disk space for storing Clickhouse DB data
Disk space (PostgreSQL)	Total allocated and used disk space for storing PostgreSQL DB 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 services of Data Discovery node	
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.

If Data Discovery is executing scanning tasks, then the list will also display services related to the running tasks.

Services of scanning tasks have a number of features:

- The service name includes the number of the scanning task the service belongs to. For example, for task number 42: `puller-42`, `sender-42`.

- Multiple services of the same type that belong to the same task will appear in the list with the same name.
  For example: If, to execute scanning task number 42, Data Discovery starts three `puller` services, then the list will display three `puller-42` entries.
- The list does not diplay services that has not started or stopped working.

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 stop working;
- on the **Platform** `central` **node**, then all integrations in the cluster will be stopped.

To remove this restriction, in the **Settings** → **System Status** section, identify the node and partition that has little space left and free it up using the OS or product.

In Data Discovery, you can set a storage limit for scanned files (the default directory is `/mnt/disctps`). For details, see "Zones and servers".

If there is little free space left in the storage, you can speed up sending files to Traffic Monitor. For this, in the scanning task settings, reduce the number of scanners (`puller`) and increase the number of transmitters (`sender`).

All monitoring events in the System are logged.

To export the diagnostic data:

1. Click **Export system log files**. Log files of the running services and log files of the running scanning tasks from all Data Discovery nodes will be added to the diagnostic data. Exporting will begin once the diagnostic data has been generated.

   Note:

   If you need to get log files for a scanning task (e.g., log files of the Puller service instances), then before exporting the diagnostic data, make sure that the task is running.

2. Download the ZIP archive that contains TXT files with the logs.

To download diagnostic data for a separate service:

1. Click next to the required service. The log file will be generated and then loaded.
2. Download the ZIP archive that contains TXT files with the service logs.

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 load events, which you can add to investigations, to the System, as well as to receive data used by other products.

With Active Directory integration, you can:

- **Add new users to the System from LDAP directories**
  Users added from LDAP directories can log into the System using domain credentials. For details on adding users from LDAP directory, see "Adding New User from LDAP".
  Adding a new user from the LDAP directory does not require synchronization.

- **Add hosts from directories to scanning tasks** (see "InfoWatch Data Discovery. User Guide", "Adding and Configuring Hosts")

- **Add persons and groups from LDAP directories to the System**
  - The list of persons will be uploaded to the **Dossier** section where you will be able to view information about each person;
  - Persons added from LDAP directories will have a SID contact type;
  - The System will be able to identify persons and groups by their SIDs. Their names will be displayed in the table with information about files (see "InfoWatch Data Discovery. User Guide", "Table with File Information").

  To add the data to the System, synchronization is required.

For details on configuring integrations, see the following articles:

- "Integration with Active Directory";
- "Integration with InfoWatch Traffic Monitor";
- "Editing or Deleting Integration".

Warning!

Integration with InfoWatch Traffic Monitor in the **Integrations** section is not relevant to this release of Data Discovery.

For information on how to configure data export to Traffic Monitor, see "Zones and servers".

5.2.1 Integration with Active Directory

To add a new integration with Active Directory:

1. Go to **Settings** → **System settings** → **Integrations**.
2. Click + Add.
3. Select **Active Directory**.
4. Set parameter values:

Parameter	Description
Integration name	Connection name which is used in the Console

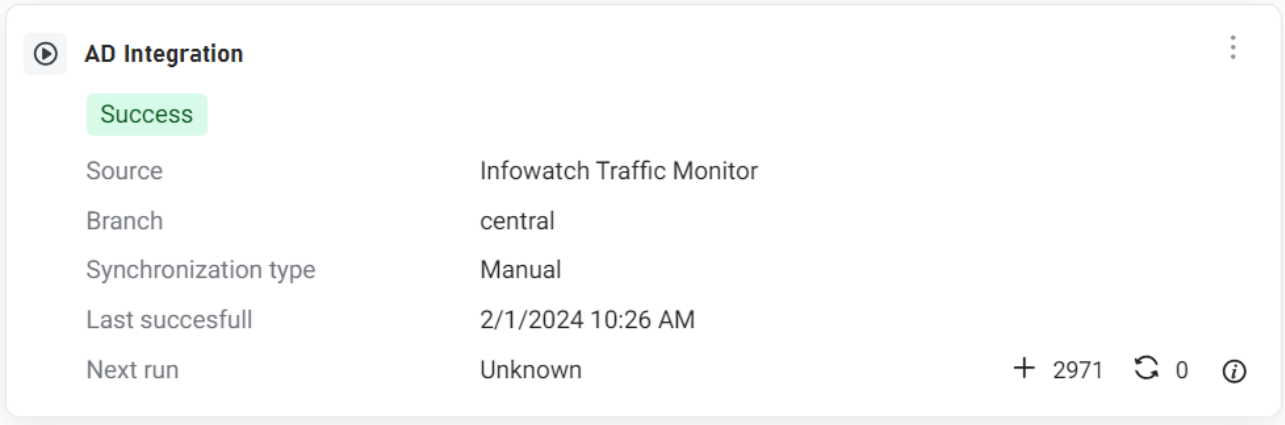
Parameter	Description
Branch	Label of the Data Discovery node, which is used for connecting to Active Directory
Source address	The network address of Active Directory server
Connection type	Select the type of connection to be established: • Unsecure connection (Plain) • Secure LDAP connection (StartTLS) • Secure LDAPS connection (TLS) **Warning!** A connection without certificates is not secure.
Certificate	Upload the certificate file in PEM or DER format Parameter is used if secure connection type is selected
Global port	Port for connecting the global LDAP directory. By default the following values are used: • 3268: • for unsecure connection (Plain); • for secure LDAP connection (StartLTS); • 3269 for secure LDAPS connection (TLS). Click  to set default values.
Port	Port for connecting the domain local directory. By default the following values are used: • 389: • for unsecure connection (Plain) • for secure LDAP connection (StartLTS) • 636 for secure LDAPS connection (TLS). Click  to set default values.

LDAP query	Filtering attributes that are the full path to the specified 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 the Users branch located in the company domain as a search base, enter:
	`cn=users,dc=company,dc=com`

Parameter	Description
Login	Login to access the Active Directory server (user must have read access to the directory)
Password	Password to access the Active Directory server
Synchronization	Type of synchronization: manual or automatic. If automatic synchronization is selected, it is necessary to specify the values in the **Synchronization period** and **Repeat** parameters
Synchronization period	Interval of automatic synchronization. For example, if the **Synchronization period** parameter value is **Hourly** and the **Repeat** parameter value is **2**, then the synchronization starts every 2 hours.
Repeat	

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.

> **Warning!**
>
> Synchronization with Active Directory can create a high load on the domain servers and the network so we recommend running the first synchronization with Active Directory at night.



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

Information about integrations

It is possible to synchronize with several LDAP directories. Each integration is displayed in a separate panel.

The bottom line of the panel shows:

-  – number of persons, groups and workstations added during synchronizations;
-  – 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 user. Status also contains information on date and time of termination
ERROR	The status can indicate that: • an incorrect login, password, or address is specified; • an error occurred during synchronization.

5.2.2 Integration with InfoWatch Traffic Monitor

Integration with InfoWatch Traffic Monitor (also referred to as TM) allows you to load events, groups and persons into the Investigation Centre. For persons, you can create dossiers and initiate investigations (see "*InfoWatch Data Discovery. User Guide*", article "Creating, Editing and Deleting Dossier").

> **Note:**
>
> Data Discovery does not use data on Traffic Monitor events. Other products installed in the Investigation Centre cluster can use this functionality.
>
> Vision product installed in the Investigation Centre cluster, once integrated, can use information on protected objects and policies.

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. Click .
3. Select **InfoWatch Traffic Monitor** and specify the following parameters:

Parameter	Description
Integration name	Connection name
Branch	A node for connection: main office or a branch
Source address	The network address of a working TM server
Token	A token required to receive data from the TM server (see the document "*InfoWatch Data Discovery. Installation Guide*", article "Traffic Monitor License and Plugin")
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 (min.)	Time interval during which events occurred in Traffic Monitor. Data of these events will be loaded to the System as one thread. By default, 120 minutes. Minimizing this parameter allows you to reduce load on Traffic Monitor when sending data.
Use archiving options when downloading	When the parameter is enabled, 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. Enabling the parameter will exclude the download of data on persons, groups and workstations to Investigation centre from Traffic Monitor. In case the data has been already downloaded to Investigation centre, enabling the parameter will not remove them.
Download events details	When the parameter is enabled, all details will be further loaded to main data received from Traffic Monitor. The parameter allows you to enable a deferred loading.
Deferred loading	When the parameter is enabled, loading of detailed data is to be done at the time specified below
Time of deferred loading	Time to start loading of detailed data

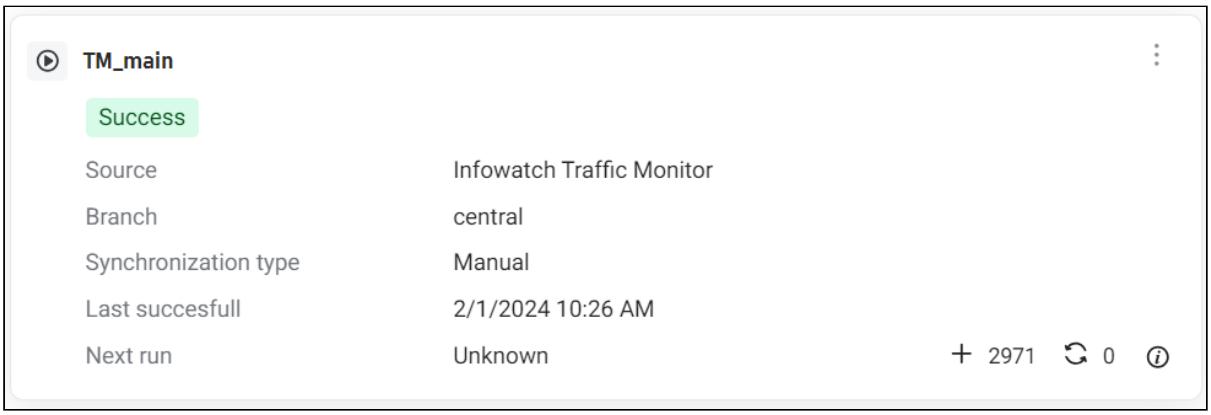
Parameter	Description
Synchronization	*Manual* or *Automatic*. When selecting *Automatic,* you should specify *Frequency* and *Repetition*
Synchronization period	How often to start synchronization: *Minutely*, *Hourly*, *Daily*, *Weekly*
Repeat	Day of the week and time of the next synchronization

4. Click **Test connection** to check if you've specified all required parameters correctly. Wait until you see the message "*Successfully connected*".
5. Click:
   - **Save** – a new synchronization will wait for running with the NOT SYNCHRONIZED status
   or
   - **Save and start synchronization** to start the synchronization process.

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

In the lower line, you will find:

- – the number of entities added during the latest synchronization
- – the number of entities whose data was updated during the last synchronization
- – detailed information on synchronization results.



To set up auto synchronization on schedule (for example, at night in order to reduce time costs and network load):

1. Click and select **Edit**.
2. Select synchronization type: **Auto**.
3. Specify synchronization period: **Daily**.
4. Specify the time to repeat: **0:00**.
5. Click **Save**. The System will run synchronization in accordance with schedule.

Important!

When planning the initial synchronization with InfoWatch Traffic Monitor, 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 outside of working hours (at night).

If you require running one more synchronization with the same parameters:

1. Click .
2. Wait until synchronization is complete. The process can 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 TM, go to **Events** sections and make sure that the data is received and displayed in the table.

Possible synchronization statuses and their description:

Synchronization status	Description
NOT SYNCHRONIZED	Synchronization has been saved and can be started later
SYNCHRONIZING	Synchronization in process
SUCCESS	Synchronization completed successfully
DISCONNECTED	Sunchronization has been terminated by user. Status also contains information on date and time of termination
ERROR	This status can indicate that: • You have entered an incorrect login name, password or address; • There is no plugin/license for using the product in TM; • An error occurred during synchronization.

5.2.3 Editing or Deleting Integration

To edit an existing integration:

1. In the upper-right corner, click  and select **Edit**.
2. Make the changes.
3. Click **Save**:
   - To create a new integration with the specified settings instead of the current one, click **Create a new one**. The current integration will be deleted.
   - If you need to change the settings of the current integration, click **Continue with this**.

To delete an integration:

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

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

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 a list of users who are allowed to work in the System:

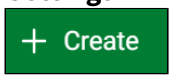
- the Main Security Officer
- other Security Officers who report to the Main Officer

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 Security Officers. For this:

1. Go to **Settings**  → **System settings** → **Users**.
2. Click .
3. Select **Create user**.
4. Specify values as described in the table below:

Parameter	Is required	Description
Photo	No	User photo

Parameter	Is required	Description
Username	Yes	Name of the new user (for username requirements, see " Password Settings").
Login	Yes	Name of the user account (for login requirements, see "Password Settings"). Login is not case-sensitive
Password	Yes	Account password (for password requirements, see "Password Settings")
Confirm password	Yes	Account password
Role	No	User role in the System. A user may have only one role.
Console language	No	Interface language for the new user: *Russian* or *English*
Display functions of installed products only	No	Switcher which makes sections and widgets of uninstalled products invisible
Contacts	No	Mobile phone number. You can add one or more values
	No	Email address. You can add one or more values

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 the 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. Click + Create.
3. Select **Add from LDAP**.
4. Select an available LDAP server, integration with which is configured in the System (see "Integration with Active Directory").
5. In the search bar, start typing user 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 domain credentials. Account login has the following format: `domain\login` or `login@domain`. Account login is not case-sensitive.

> **Note:**
>
> 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.

> **Warning!**
>
> Changes to the account made in Active Directory will be available in the System only after the account is re-added: 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. Click next to the user or in the upper-right corner of the user profile page.
3. Select **Edit**.
4. Edit required settings. Available settings are described in the "Creating New User" article.
5. Click **Save**. The new settings will be applied.

To assign a role to the user:

1. Go to **Settings** -> **System settings** -> **Users**.
2. Select a 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 includes a user personal card with the following data:

1. The **Personal info** tab displays the following data:
   - User photo;
   - Username;
   - User login name in the System;
   - User language in the System;
   - Contact data: phone numbers, email addresses;
   - Log of recent account activity.
2. The **Access rights** tab displays the user rights in the System:

- Role assigned to the user;
- Available functions:
  - User access to products and settings;
  - 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

To change your 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:
   - Click next to the user;
   - Open the user's profile and click in the upper-right corner.
3. Select **Change Password**.
4. Fill in the following fields:

Field	Description
Old password	Enter your current password
New password	Enter a new password. The password must match the security settings (see "Password Settings")
Confirm password	Re-enter the new password

5. Click **Save**.

5.3.6 User Activation and Deactivation

The Main Officer can prevent the selected user from performing actions in the System. For this:

1. Go to **Settings** → **System settings** → **Users**.
2. Do either of the following:
   - Click next to the active user;
   - Click in the upper-right corner of the user's profile.
3. Select **Deactivate**. The user account will be blocked.

To unblock a previously blocked user account:

1. Go to **Settings** → **System settings** → **Users**.
2. Do either of the following:
   - Click next to the blocked user;

- Click  in the upper-right corner of the user's profile.

3. Select **Activate**. The unblocked user can now work in the System.

If other Security officers have access to user settings, they also can deactivate users.

5.3.7 Deleting Users

Main officer can delete user accounts. To do this:

1. Go to **Settings**  → **System settings** → **Users**.
2. Do one of the following:
   - Click  next to the active user;
   - Click  in the upper-right corner of the user's profile.
3. Select **Delete**.
4. In the opened window, click **Ok**. User account and all its data will be permanently deleted from the System.

> **Note:**
>
> Main officer's account cannot be deleted.

5.4 Roles

System users can have different roles which define users' rights in the System. Users without a role cannot access the System.

A **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***.

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

1. **Main security officer** has full access to all System data, System settings and can mange roles including:
   - Creating new users;
   - Creating new roles and assigning roles to users.
2. **Security officer** has full access to System data except for the **Settings** section.

Find information about roles on the tabs:

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

Role can be assigned:

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

User actions:

- Creating and Configuring Role
- Viewing and Editing Role
- Revoking and Removing User Role

5.4.1 Creating and Configuring Role

The *Main Security Officer* role allows the user with this role to create new roles and assign them to users. If all users have different responsibilities, the Main Officer should create a separate role for each user. If user responsibilities change, you should either edit the role, or create a new role and assign it to the user instead of the obsolete one.

To create a role:

1. Go to **Settings** → **User Settings** → **Roles**.
2. Click **+ Create**.
3. Enter the role name. If necessary, add a description.
4. Click **Save**.
5. In 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 Investigation Centre 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**, **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 functions of other products**
>
> **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 *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 Access Tracker

Access to *Infrastructure* enables you to review reports of accounts statuses and changes in AD groups in the **Infrastructure** section.

Data Discovery

Access to *File sharing* enables you to:

- Work in **File sharing section**:
  - On **Tasks** tab – to create and run scanning tasks;
  - On **File information**, **Duplicate files** and **Similar files** tabs – to analyze scanning results and grouping files by duplicates and similar ones;
- 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**, **Duplicate files** and **Similar files** tabs in **File sharing** section.

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 **Settings** list, select:
   - ☑ to provide full access to settings. By default, access is denied;
   - 👁 to provide access to selected sections only;
   - ☐ to deny access to separate sections .

     Regardless of the selected access level, a user always has full access to personal information in their own profile.

6. In the **Data** tab, you can allow or restrict user access to data. To change user access rights to selected data, specify it in the following categories: *Persons*, *Groups*, *Branches*, *Contacts*, *Departments*. You can:
   a. ☐ – restrict access to selected data;
   b. ☑ – allow access to selected data;
   c. ☒ – deny access to selected data.

Examples:

If you set ☒ next to a person, the role will prevent the user from accessing any information on this person in the System.

If you set ☑ next to a person (or leave the default ☐ option for all persons), then the role will give the user full access to the person's data.

If you set ☐ next to a person and select other persons at the same time, this role will give the user access to information related to allowed participants (☑).

Note:

The Main Officer should be careful when adding conditions as using different elements may result in narrowing of the available data instead of expanding it. This may happen when using logical AND between different categories.

Example:

a. The Main Officer configures access to *Group-1* OR *Group-2*.

b. The Main Officer configures access to *Person-1*, *Person-2*, and *Person-3*.
Now the user can access less data as the resulting condition is as follows:
(*Group-1* OR *Group-2*) AND (*Person-1* OR *Person-2* OR *Person-3*).

To configure a shared limitation for both groups and persons, create a cumulative group in Traffic Monitor, which would include all the groups and persons needed. Use it in the access settings.

To test the correctness of newly added visibility scopes, assign similar conditions in *Single filter* and then check results with the widgets used.

7. If you want to deny access to all data, select  **Prohibit access to data**.

> **Note:**
>
> For correct work with Data Discovery, do not prohibit access to data for a user.

8. In the **Users** tab, select a user without a role to whom the role should be assigned. For this:
   a. Click **+ Add**.
   b. From the **Users** field, select the required user.
   c. Click **Grant**. The role will be assigned to the user.
9. After you specify all the settings, click **Apply**.
10. For the changes to be applied, the user should log out of the System and then log in again. To forcibly end sessions for users with this role, select the  **End users active sessions** option and then click **Apply**.

5.4.2 Viewing and Editing Role

The Main Officer can view and edit roles assigned to users in their 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 user's 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) – data to which the user has access.
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 the field and selecting the required role from the list.
7. Click **Save** to apply changes.
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**.

You may need to copy a role, for example, when staff is increasing or for audit purposes:

1. Go to  **Settings** → **System settings** → **Roles**.

2. Click on the panel 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 becomes **Officer copy**.
    - **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.

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. Now you can 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**.
6. For the changes to be applied, the user with this role should log out of the System and then log in again. To forcibly end sessions for this user, select **End users active sessions**.
7. Click **Apply** to confirm. The role will be revoked from this user.

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**.

4. For the changes to be applied, the user with this role should log out of the System and then log in again. To forcibly end sessions for this user, select ☑ **End users active sessions**.
5. 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.

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

The following actions are audited:

Users	- log in - log out - create - change - delete - change password - block user
Roles	- create - change - delete
Integrations	- create - change - delete - run manually
Dossier	- view - create - change - delete - combine

In the section you can:

- move columns in the table;
- sort columns content (by default the events are sorted by date, from the latest to the earliest);
- switch to user card in the User section, when you click on the user;
- add filter to the panel or remove it;
- sort events by selecting filters;
- unload audit events (in .csv format);
- copy content of cells.

By default all filters are added to the panel:

- *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.

You can sort events by:

- selecting the filter attribute on the panel above the table;
- selecting the filter attribute in the table.

To select the filter attributes in the table:

1. Point cursor to the cell.
2. In the window that opens, press **Add to filter** . The table content will be sorted according to the selected filter.

To copy the content of table cell:

1. Point the cursor on the cell content.
2. In the window that opens, point the cursor on the content in the row, then press **Copy** .

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

To unload the report of audit events:

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

If you moved columns in the table, the unloading will still have the columns order by default. To view the report in Excel, you need to enable the UTF-8 encoding. For more details, see the article "How to enable UTF-8 encoding in Excel" in our 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 a rule:

1. Go to **Settings**  → **System settings** → **Password settings**.
2. You can see 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: - required ☑ – the password must include letters - optional ☐ – letters in the password are not required
Digits	Arabic numerals that can be used in the password. You can set the following values: - required ☑ – the password must include digits - optional ☐ – digits in the password are not required
Special symbols	A list of special characters the password can include. You can set the following values: - required ☑ – the password must include special characters - optional ☐ – special characters in the password are not required
Minimal length	The minimum password length
Latest N passwords cannot be used	Select the option to forbid using previous passwords 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

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.

5.6.1 Requirements for the account name

The username should contain at least four characters.

The user login name:

- Must start with a letter and not end with a dot
- May consist of Latin letters, Arabic numerals and contain special characters: "_", "-", "–", "."

5.7 Global Settings

In the **Settings** → **Global settings** section, you can manage the collection of statistical data.

Warning!

The other settings in this section are not used for Data Discovery.

5.7.1 Collect statistical data

The statistics collection system collects and aggregates data on user activity in the Management Console. By user's decision this data can be downloaded and sent to the InfoWatch company to be processed. This is done to improve the quality of the product, to assess the need for functionality and to create new work scenarios.

Statistical data collection is enabled by default. To disable data collection, uncheck **Enable** and click **Save**.

Note:

The statistics collection system does not collect, analyse or transfer any personal data. All users' and employees' full names are replaced with internal system IDs.

5.8 Notification Services

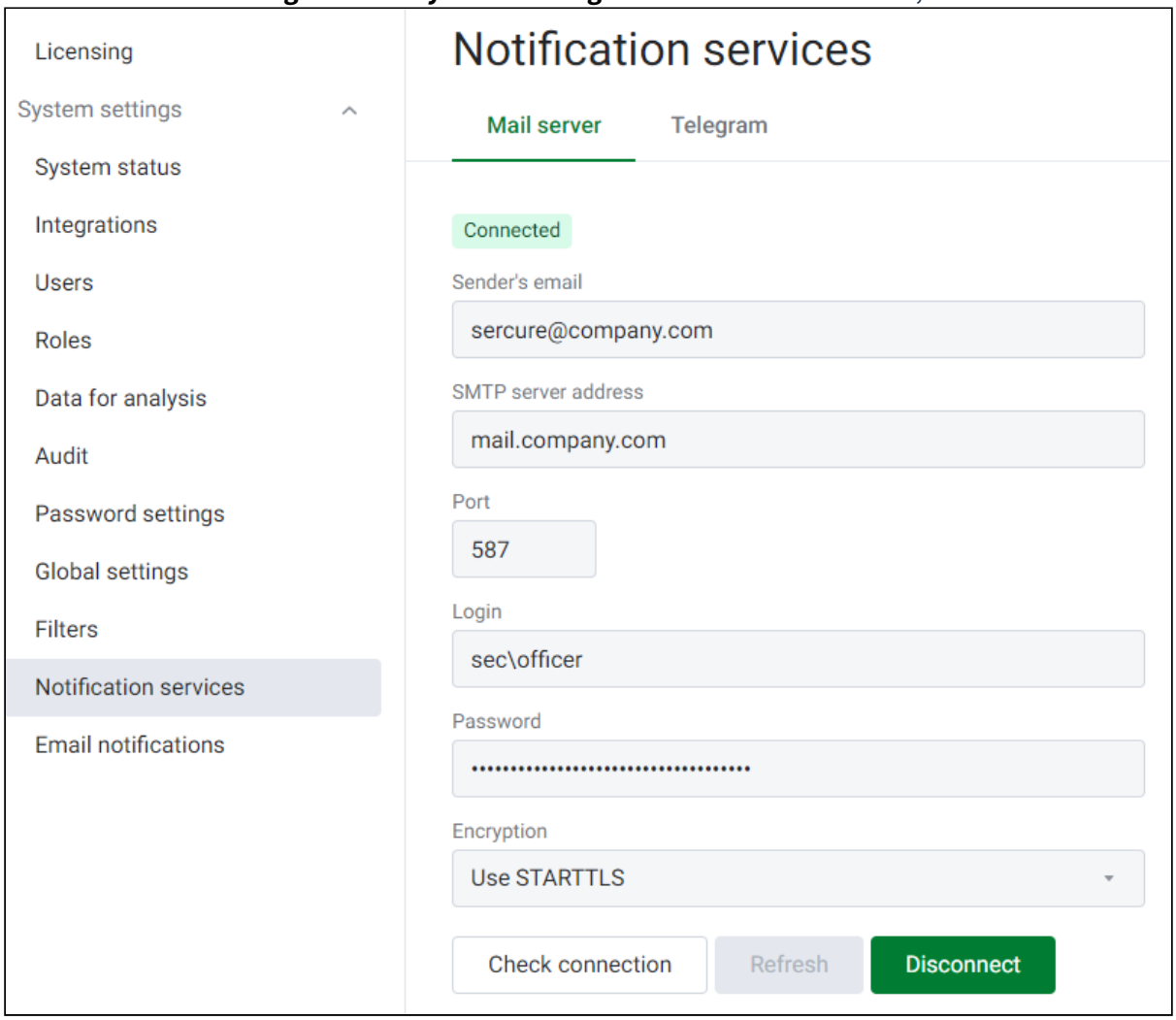
Data Discovery uses mail server for regular report sending.

Note:

Sending via **Telegram** is not supported in the current version.

To connect to the mail server:

1. Go to the section **Settings** → **System Settings** → **Notification Services**, **Mail server** tab.



2. Specify connection parameters:

Parameter	Description
Sender's email	The email address that will be used to send the notifications
SMTP server address	Mail server address that uses SMTP protocol. Specify the domain name or the IP address
Port	Port that is used to connect to the mail server
Login	Name of the account that has access to the mail server
Password	Password to log in to the mail server

Parameter	Description
Encryption	Specify the encryption protocol to connect to the mail server. Available protocols: • STARTTLS • TLS

All parameters are required.

3. After you have specified connection parameters, click **Connect** on the bottom.
   In case of a successful connection, the status will change its value to **Connected**.
   To check the availability of the server, you can click **Check connection** on the bottom.

To change connection settings or connect to a different mail server, make your changes and click **Refresh** on the bottom.

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

6 Zones and servers

In **Settings** → **Product settings** → **Zones and servers** you can manage Data Discovery zones and servers.

A zone is a group of Data Discovery servers. Dividing servers into zones allows you to:

- Run task services only on specific servers. A zone can include several servers from the System cluster. Each server can be only in one zone.
- Configure data export to Traffic Monitor for each server group. Each zone has its own settings for data export.

You can select the zone of a scanning task in the task settings (see "InfoWatch Data Discovery. User Guide", "Creating, Configuring and Running Tasks").

6.1 Managing zones

In the **Zones** tab:

- The list of zones is displayed on the left.
- The workspace on the right displays the settings for exporting data to Traffic Monitor and the list of zone servers.

6.1.1 Creation

To create a zone:

1. Go to the **Zones** tab.
2. Click + Create zone.
3. Enter the zone name.
4. Click **Create**.

6.1.2 **Renaming**

To rename a zone:

1. Go to the **Zones** tab.
2. The list of zones is displayed on the left. Click next to the zone name.
3. Select **Rename**.
4. Enter a new name.
5. Click **Save**.

6.1.3 Deletion

If you delete a zone, the servers are removed from the zone. The System on the servers is not be deleted.

You cannot delete a zone if the zone is selected in tasks. Change zone in the task settings or delete such tasks.

You cannot delete the preinstalled **Default** zone.

To delete a zone:

1. Go to the **Zones** tab.
2. The list of zones is displayed on the left. Click next to the zone name.
3. Select **Delete**.
4. Click **Delete**.

6.1.4 Adding servers to zone

To add servers to a zone:

1. Go to the **Zones** tab.
2. The list of zones is displayed on the left. Select the zone.
3. Click **Add server** in the workspace on the right.
4. The window that opens displays servers that are not added to any zone. Select servers.
5. Click **Add**.
6. Restart the tasks in the zone so that the task services can run on the added servers.

6.1.5 Data export to Traffic Monitor

To send file copies and information about files to Traffic Monitor for analysis while executing a scanning task, configure the data export. Traffic Monitor license and plugin are required to export data (see "Installing the License and Plugin").

To configure date export:

1. Go to the **Zones** tab.
2. The list of zones is displayed on the left. Select the zone.
3. Expand the **Data export to Traffic Monitor** panel.
4. Specify values for the parameters:
    a. **TM Version:**
    Traffic Monitor version on the server that you need to connect to. You can select **Version 6.10** or **Version 7.1 and above**.

    > **Note:**
    >
    > To get TM version number, open **Security Officer** → **About** section of Traffic Monitor Management Console.

    b. **XAPI Address:**
    XAPI addresses of the Traffic Monitor servers. The servers must be in the same Traffic Monitor cluster. Data Discovery sends data to the servers from the list.
    - To add an address:
        i. Enter the address in IPv4 IP address format: "xxx.xxx.xxx.xxx".
        ii. Press Enter.
    - You can specify multiple addresses.

> **Note:**
>
> To distribute the load and not to fill up only the first specified Traffic Monitor server, Data Discovery uses the Round-robin distribution algorythm: the first file in the queue is sent to the first specified Traffic Monitor server, the second file is sent to the next server etc.

If one address is unavailable, the System automatically starts using the next specified address.

- Traffic Monitor version 7.7 or higher reports if there is not enough space on the server to receive data from Data Discovery (see "Traffic Monitor. Configuration Files Guide", the `FreeSpaceThresholdMountPoint` и `FreeSpaceThresholdGb` parameters in **xapi.conf**). In this case, Data Discovery switches to the next XAPI address or tries to send data again after 1 minute.

c. **Token:**
Connection token.

> **Note:**
>
> To copy a connection token:
>
> i. In the Traffic Monitor Management Console, go to **Administration** -> **Plugins** section.
> ii. At the top left of the screen, select a preset plugin:
> - "InfoWatch Crawler" for Traffic Monitor version 7.3 and lower;
> - "InfoWatch Data Discovery" for Traffic Monitor whose version is higher than 7.3.
>
> iii. Copy the token by clicking .

5. You can check availability of Traffic Monitor servers using the **Check connection** button.
6. Click **Apply**.
7. Restart the tasks in the zone. The tasks will get new data export settings when started.

6.2 Managing servers

The  **Servers** tab displays a list of all Data Discovery servers. The list of servers for each zone is displayed on the  **Zones** tab.

Server panel displays the following information:

Server data	Description
 Name	Label and name of the server in the format: `label (name)`
 Zone	The zone to which the server is added. There is no value if the server is not added to a zone.

Server data	Description
	• Server with Data Discovery in `central` mode is automatically added to the **Default** zone. • Servers with Data Discovery in `office` mode are not automatically added to zones.
 Role	In the current version of the System, all servers have the **Scanner and sender** role
 Storage	Data about the server storage space

6.2.1 Selecting zone and removing from zone

Note:

You cannot change the server zone if the server storage has task files.

To get the number of task files in the server storage:

1. Connect to the server SSH console. Task files are stored in **`PATH/NUMBER`** directories, where:
   - **`PATH`** is the server storage path, by default: **`/mnt/disctps`**;
   - **`NUMBER`** is the task number.
2. Run the **`ls PATH/NUMBER -1 | wc -l`** command for each task. Example: **`ls /mnt/disctps/7 -1 | wc -l`**

To delete files from the storage, perform one of the actions for each task in the storage:

- Send the task files to Traffic Monitor:
  1. In the task settings:
     - Enable the **Send files to Traffic Monitor for analysis** parameter.
     - Specify the following values in the task settings:
       - **0** for the **Pullers count** parameter;
       - **N** for the **Senders count** parameter, where **N** is greater than or equal to the number of Data Discovery servers in the task zone.
  2. Start the task. The System sends files to Traffic Monitor and deletes them from storages, but does not download new files to zone storages.
  3. Wait until there are no task files left in the storage.
  4. Stop the task.
- Delete the task. Task files will be deleted and will not be sent to Traffic Monitor.

To add a server to a zone / to change the server zone:

1. Click  on the server panel.
2. Select **Select zone**.
3. Select a zone from the list.
4. Click **Apply**.
5. Restart the tasks in the zone so that the task services can run on the server.

To remove a server from the zone:

1. Click ⋮ on the server panel.
2. Select 🗑 **Remove from zone**.
3. Click **Remove**. The System on the server will not be deleted.

6.2.2 Configuring storage

Each Data Discovery server has a storage for the scanned files. All servers have the same storage path (by default, `/mnt/disctps`). The storage path is specified when you install the System in the central office.

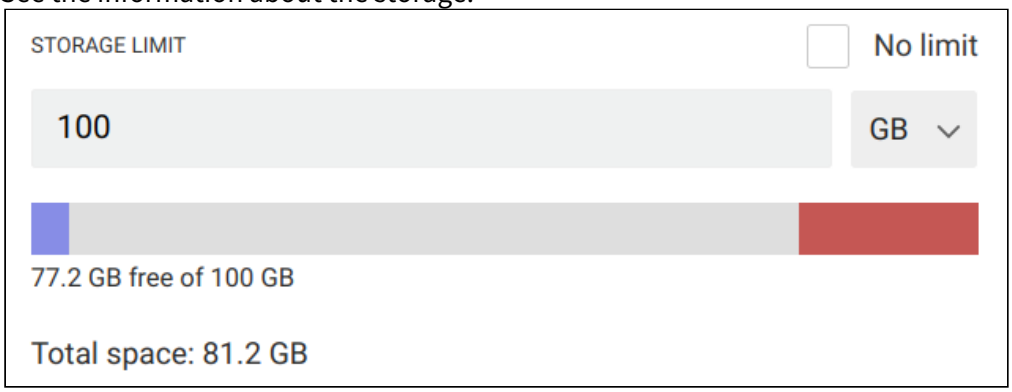
> **Note:**
>
> We recommend that you place the server storage on a separate partition or disk.

> **Warning!**
>
> Only the files and directories that are added by the System must be in the storage. If you place other files or directories in the storage, the System may not function correctly.

During scanning, the System downloads a file to one of the zone storages. The System sends the file to Traffic Monitor and then deletes the file from storage.

To configure a storage:

1. Click ⋮ on the server panel.
2. Select ⚙ **Set up roles.**
3. See the information about the storage:



   - The **Storage limit** field contains the current storage limit.
   - If the **No limit** setting is enabled, the storage limit is not used.
   - **Total space** = free disk space + space that is used by Data Discovery files.
4. To view detailed information about the storage space, hover your cursor over the storage space indicator:



- **Used by Data Discovery** is the space that is used by Data Discovery files.
- **Available for Data Discovery** is the free disk space that Data Discovery can use.
- **Unavailable** is displayed if the limit exceeds **Total space**.

5. Configure the limit:

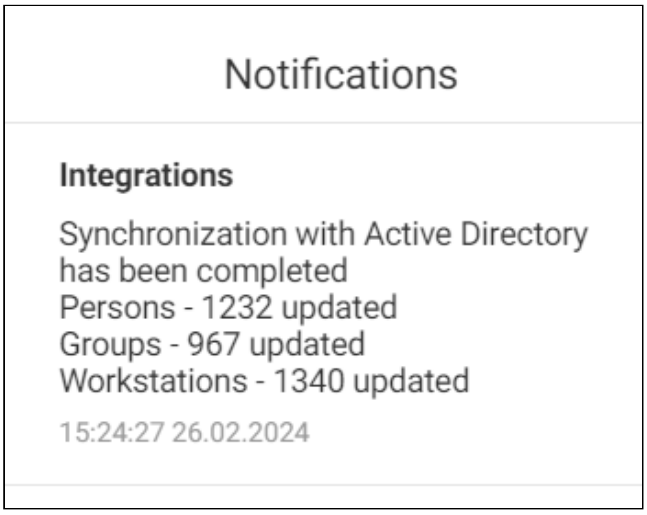
> **Warning!**
>
> Set a storage limit if the System and storage are located in the same partition. We recommend that you set the limit so that 10 GB are always available in the partition.
>
> The System may not function correctly if there is not enough free space in the partition.

   - To set a limit:
     a. Disable the **No limit** setting.
     b. Specify the limit in the **Storage limit** field and select the unit of measurement. The System stops downloading files to the storage if the used space in the storage reaches the limit. If space becomes available, the System continues downloading.
   - If a limit is not required, enable the **No limit** setting. The System stops downloading files to the storage if the free space on the disk runs out. If space becomes available, the System continues downloading.

6. Click **Apply**. The System will start using the new storage settings.

7 Notifications

To view Investigation Centre notifications, click .



Notification may contain the following information:

- The status of synchronization with sources initiated by user;
- Adding a license;
- Removing a license;
- The current number of dossiers loaded to the System;
- Possible disk space overflow;
- Soon password expiration.

8 Configuring Autodeletion of Data Discovery Events in Traffic Monitor

Traffic Monitor applies an atigarbage filter to Data Discovery events. **By default**, the filter removes Data Discovery events which have not triggered Traffic Monitor policies or which do not contain protected objects.

You can configure Data Discovery events deletion in `/opt/iw/tm5/etc/luaengined.conf` configuration file.

To define operation modes of the antigarbage filter, set a value for `DeleteDDEventsWithoutPolicy` parameter:

- `true` – to save only events which have triggered policies;
- `false` (default) – to save events which contain protected objects or which have triggered policies.

In case you want to disable deletion of Data Discovery events for certain servers, specify the servers in `DisableDeleteDDEventsForServers` parameter.

To apply changes:

1. Save the file.
2. Restart `iw_luaengined` service:

```
iwtm restart luaengined
```

Example:
You do not wish to apply the filter to events from *MainDD* and *DDcompany* servers, and, for the other servers, you want to save only events which have triggered policies.

Parameter values for luaengined.conf configuration file of the example:

```
"DeleteDDEventsWithoutPolicy": true,
"DisableDeleteDDEventsForServers": ["MainDD", "DDcompany"],
```

9 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 web service. You can add a 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. Navigate to the directory to which you unpacked the distribution archive during the installation.
3. Run the command as a user with *root* privileges:

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

    In our example:
    - `/folder/test.crt` is the full path to the certificate file;
    - `/folder/test.key` is the full path to the private key file.

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

10 Log File Rotation

10.1 Scanning task services

To perform scanning tasks, the System uses the services: Puller, Sender, Ripper, Contents Processor, Task Execution Controller. Log files of service instances are stored in subdirectories of the `/var/log/infowatch/disc` directory on the server where the scanning task services were running.

Each time the task is started, the System adds a subdirectory to the `/var/log/infowatch/disc` directory for each service instance involved in the task execution. Log files of a service instance are added to the subdirectory. Each subdirectory has a unique identifier in its name.

10.2 Discoperator service

Log files of the Discoperator service are stored on the node with Data Discovery that is installed in the central mode, in the `/var/log/infowatch/disc` directory. This service is used for operation of the web interface.

Discoperator is constantly running and adds entries to the log file. If the service has been restarted, the System adds a subdirectory to the `/var/log/infowatch/disc` directory for the new service instance.

10.3 TPS Agent

The `/var/log/infowatch/disc` directory on each server stores the TPS Agent service log files. This service is used to manage the server storage.

The service is constantly running and adds entries to the log file. If the service has been restarted, the System adds a subdirectory to the `/var/log/infowatch/disc` directory for the new service instance.

10.4 Log file rotation

Services instances add a large number of entries to log files. The size of log files constantly increases, which leads to a decrease in free disk space.

You can free up disk space in the following ways:

- Stop all scanning tasks in Management Console, then delete subdirectories and log files manually from the `/var/log/infowatch/disc` directory. When you run the task again, the System:
  - creates new subdirectories with new identifiers;
  - creates log-files in subdirectories, to which entries about the task execution will be added.

> **Warning!**
>
> If you delete log files of a running task, entries will not be saved in the System until the task is stopped and started again.

> **Warning!**

It is not recommended to manually delete the directories and log files of the running Discoperator and TPS Agent services. The directories of these services have names like the following:

- `discoperator-central-5c5769b58d-77rq2`
- `tps-agent-f85x8`

- Configure log file rotation.

For regular and automatic deletion of outdated entries, it is recommended to configure log file rotation. Log file rotation is an automatic process for managing log files. During rotation, depending on the settings:

- New file is created that is a version of the original log file. Entries from the original log file are moved to the new file.
- Files that are versions of the original file are compressed.
- Outdated files are deleted.

10.5 Configuring rotation with logrotate and crontab

It is required to configure rotation on each Data Discovery server.

To configure the rotation of log files on the server:

Warning!

Perform all actions as a user with root privileges.

1. Configure the **logrotate** utility:
   a. Check the contents of the **`/etc/logrotate.conf`** configuration file. The configuration file must contain the following line:

   ```
   include /etc/logrotate.d
   ```

   If the line is missing, add the line to the configuration file.
   b. In the **`/etc/logrotate.d`** directory, create a file for Data Discovery logrotate configuration (in our example, the file name is **`iwdd`**).
   c. Open the created file for editing and enter the following configuration:

   iwdd

   ```
   /var/log/infowatch/disc/*/*.log {
       daily
       copytruncate
       rotate 7
       notifempty
       compress
       missingok
   }
   ```

   Configuration description

Content	Description
/var/log/infowatch/disc/*/*.log {	rotate log files in the subdirectories of the `/var/log/infowatch/disc` directory
daily	perform daily rotation
copytruncate	at each rotation create a version of an original log file, then move all entries from the original file to the created version
rotate 7	keep the last 7 versions of each original log file, delete older versions of the log file
notifempty	do not rotate if there are no entries in the original log file
compress	compress each version of the original log file
missingok	do not report an error if the original log file was not found
}	

d. Save the changes you made. By default, `logrotate` runs automatically.
e. To check if the configuration is correct without performing a rotation, run the command:

```
logrotate -d /etc/logrotate.d/iwdd
```

2. If the service instance was restarted, the new instance adds entries to a new log file in a new subdirectory. The old file will become empty after one rotation and will no longer be rotated. Configure automatic deletion of unused files and subdirectories using the **crontab** file:
   a. Open the `crontab` file of root user for editing by running the command:

```
crontab -u root -e
```

   b. Add the line to the configuration file:

```
30 5 * * * find /var/log/infowatch/disc/ -mtime +7 -name "*.log*" -delete > /dev/
null 2>&1; find /var/log/infowatch/disc/ -empty -type d -delete > /dev/null 2>&1
```

   The script runs every day at 5:30. The script sequentially performs the following actions:
      i. Deletes log files and versions of log files from subdirectories. Log files and versions of log files that were modified more than 7 days ago are deleted.
      ii. Deletes empty subdirectories.
   c. Save the changes you made. The script will run automatically every day using cron.

As a result of the configuration:

- `logrotate` regularly rotates Data Discovery log files and deletes outdated versions of log files;
- the script specified in the `crontab` regularly deletes unused files and empty subdirectories.