

INFOWATCH

InfoWatch Vision 2.0. Administration Guide

06/07/2019

© JSC “InfoWatch”

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

http://www.infowatch.com

Table of Contents

1 Who Should Read this Guide 4

2 Set of Documents 5

3 Technical Support 6

4 Managing integrations 7

4.1 Integrating with LDAP catalogues 7

4.2 Integrating with Infowatch Traffic Monitor 9

4.2.1 Installing plugin to InfoWatch Traffic Monitor 11

5 Managing users 12

5.1 New user creation 12

5.2 Account editing 13

5.3 User activation and deactivation 13

5.4 Deleting user 13

6 Managing data for analysis 14

6.1 Filter creation 14

6.2 Events storage 15

6.3 Manual archiving and restoring partitions 15

7 Security management 17

8 License management 19

9 Managing organizational chart download 20

9.1 Display settings 20

9.2 Internal domains 21

10 Notifications 22

This guide will provide with information on setup and configuration of InfoWatch Vision 2.0 for proper operation. This software is intended to visualize the investigations of incidents based on data provided by InfoWatch Traffic Monitor.

1 Who Should Read this Guide

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

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

2 Set of Documents

InfoWatch Vision 2.0 documentation package includes the following:

- "InfoWatch Vision 2.0. Installation Guide". The document describes how to install, configure, update and uninstall InfoWatch Vision 2.0.
- "InfoWatch Vision 2.0. Administration Guide". The document contains information on how to configure and prepare the System for proper operation.
- "InfoWatch Vision 2.0. User Guide". The document describes the working procedures and tasks facilitating by InfoWatch Vision 2.0.

Related documents on InfoWatch Traffic Monitor includes as follloows:

- "InfoWatchTraffic Monitor. Installation Guide". The document describes how to install, configure, update, and uninstall the InfoWatch Traffic Monitor.
- "InfoWatch Traffic Monitor. Administration Guide". Contains information on System administration (database, server-end).
- "InfoWatch Traffic Monitor. User Guide". The document describes operation with InfoWatch Traffic Monitor: configuration setting, data export/import, creating policies for objects processing.
- "InfoWatch Traffic Monitor. Configuration files guide". The document describes the frequently used configuration files.

3 Technical Support

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

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

Technical Support Service is available to assist you Mon-Fri, 7 AM – 9 PM (Moscow time, GMT+3), except weekends and public holidays in Russian Federation.

You can also visit online support at our website at: http://infowatch.com/support.

Before contacting the Technical Support Service, please refer to the Knowledge Base at our web-site: https://kb.infowatch.com/. The knowledge base may already contain the answer to your question or a description of the problem you are having.



4 Managing integrations

To investigate incidents the System should be provided with data from source systems. For this purpose you should configure the integration with the following systems:

- LDAP Integration - to get actual catalogues tree for company's Active Directory and to create a dossier;
- Infowatch Traffic Monitor - to get data for analysis required to perform investigation.

Sources are used in the System to:

- create employees dossiers;
- get company's structure;
- get new events;
- get directories from sources, used in events such as security policies, protected objects, etc.

Clicking **Settings** section -> **Integrations** you can configure the integration with source systems specified above and manage these integrations.

Targeted actions:

- Integrating with LDAP catalogues
- Integrating with Infowatch Traffic Monitor

4.1 Integrating with LDAP catalogues

Integrating with LDAP catalogues is required to download the company's catalogues tree into the System: groups and persons. The dossiers are to be accordingly created (see "Dossier creation, editing and deletion") to become a subject of investigation.

When you enter the System for the first time, the list of integrations is empty.

To add a new integration with Active Directory and run it please do the following:

1. Go to **Settings** -> **Integrations**.
2. Click **+Create**.
3. Select **LDAP Integration** and enter the parameters as follows:

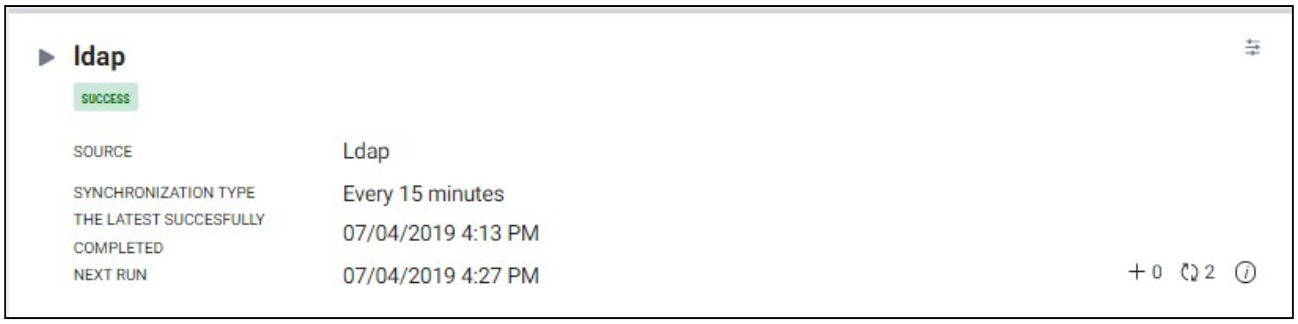
Parameter	Description
Integration name	Name of connection, used in management console.
Source address	Network server address, which LDAP catalogues are integrated with.
Global port	Port used to connect gloal LDAP Catalogue.
Port	Port used to connect local domain catalogue.

LDAP query	Domain (LDAP base), where the search of AD data is performed. Example To use `Users` branch as a search base, which is located in `Company` domain, enter a string of a type: cn=users,dc=company,dc=com
Login	Login used to access Active Directory server.
Password	Password used to access Active Directory server.
Synchronization	*Manual* or *Auto.* When using *Auto* synchronization, please specify *Synchronization period* and *Repeat*.
Synchronization period	Synchronization frequency: *Minutely*, *Hourly*, *Daily*, *Weekly*.
Repeat	Day of the week and time, when synchronization should be run.

4. Click **Test connection** to check the data you've input are correct. Wait until you see the message "Successfully connected".
5. Click :

- **Save** - the new synchronization will be later running with NOT SYNCHRONIZED status or
- **Save and start synchronization** to start the synchronization process.

You can synchronize the System with few LDAP catalogues at the same time. The list if servers, which were synchronized are displayed in the central part of **Integrations** tab. The lower line contains information about the number of persons added during the latest synchronization (+) and the number of persons whose data were updated during the latest synchronization ( ). Detailed information ( ) displays the type of synchronization and the number of persons and workstations were adeed/updated during the latest synchronization.



If you require to perform manual synchronization using the same parameters (for example, when changing the company's catalogues tree):

1. Click to run the synchronization.
2. Wait until SUCCESS status occurs. This process may take a long time 9for example, when data transfer speed is low).
3. If the status is error, please check is the server is available and data you've input are correct.
4. Go to **Dossier** section and make sure the data were transferred and are displayed in the table.

Note:

Due to high workload of Active Directory and network we recommend performing the first synchrization with Active Directory at night.

4.2 Integrating with Infowatch Traffic Monitor

Integration with InfoWatch Traffic Monitor is required to download events into the System as well as the groups, persons, protected objects and policies. Dossiers are created for persons monitoring (see "Dossier creation, editing and deletion") and investigations are to be accordingly initiated.

When entering the System for the first time the integrations list is empty.

Note:

Before processing the integration with InfoWatch Traffic Monitor you should specify the organization's internal domains (see "Internal domains"). In this case the downloaded events will be correctly classified by internal and external contacts.

To add a new synchronization with InfoWatch Traffic Monitor and run it please do the following:

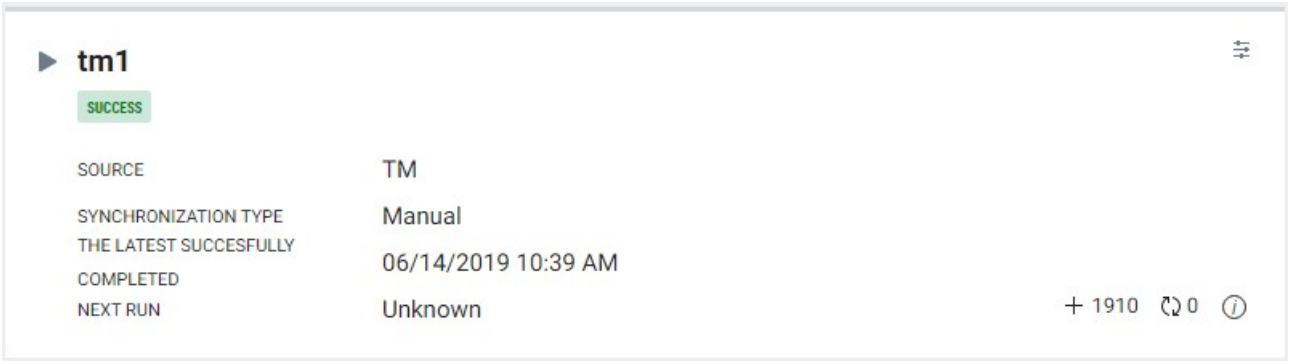
1. Go to **Settings** section and follow **Integrations**.
2. Click on **+Create**.
3. Select **InfoWatch Traffic Monitor** and specify the parameters as follows:

Parameter	Description
Integration name	Name of connection to be used in management console
Source address	TM server network address
Token	Key used to provide data from TM server (см. "Installing plugin to InfoWatch Traffic Monitor")
Synchronization	*Manual* or *Auto.* When selecting *Auto*, *Syncronization period* and *Repeat* should be specified as well.
Synchronization period	How often the integration should be run: Как часто необходимо запускать синхронизацию: *Minutely*, *Hourly*, *Daily*, *Weekly*
Repeat	Day of the week and time for the next synchronization to be run

4. Click on **Test connection** to check the data you've input are correct. Wait until you see the message "Successfully connected".
5. Press:

- **Save** - however, a new synchronization will be expecting the later running in NOT SYNCHRONIZED status.
- **Save and start synchronization** - to start synchronization process.

In the central part you may find the list of integrations with Traffic Monitor servers. In the lower line you will find the number of entities added during the latest synchronization (+) and the number of entities which data were updated during the latest synchronization ( ). Detailed information ( ) is used to display the number of groups, persons, protected objects and policies which were added and updated during the latest synchronization.



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

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

> **Note:**
>
> When planning the first synchronization with InfoWatch Traffic Monitor please take into consideration the big amount of events may load the network thus influencing the operational speed of server and management console. So, we would recommend running the synchronization in non-business hours (at night).

If you require running one more synchronization with the same parameters (for example, if the changes were implemented in the policies):

1. Click on **Start synchronization**.
2. Wait until you see the status **synchronized** => **successfully**. This process may take some time (for example, due to data export low speed or due to big data).
3. If you see **error** status, check if the data you've entered are correct.
4. After the synchronization has been successfully completed the System will create a directory. Go to **Events** and make sure the data have been exported and displayed via table.

To assess the violations level within the company branches it is required synchronizing with Traffic Monitor installed in the branches:

1. Create few integrations with Traffic Monitor, installed in different branches.
2. Start synchronization.
3. After the synchronization with few TM servers has been successfully completed, you may analyze events separately in accordance with specific branch. To do this:

a. Set up filtration parameters in System ci=onfiguration (see "Single filter - Source").
b. In **Statistics** section add required widget in the working area (see "Statistics widgets - Source").

4.2.1 Installing plugin to InfoWatch Traffic Monitor

To connect to Traffic Monitor server and provide data extraction from it you shouild install InfoWatch Vision plugin using Traffic Monitor management console. Plugin file is a `.json` file provided together with InfoWatch Vision distribution kit.

To install the plugin:

1. Log into Traffic Monitor server management console as Security officer.
2. Go to **Administration** -> **Plugins**.
3. In **Plugins** section click .
4. In the opened window clock **Download**.
5. Add plugin file, using file manager.

After the plugin was successfully added, its information is available in **Administration** -> **Plugins**. For further data export from Traffic Monitor a token is required. This token is automatically created and is available in **Administration** section -> **Plugins** -> **Tokens**. Copy the token data and enter it to **Token** field in InfoWatch Vision managemen console, when setting up an integration.

5 Managing users

Once the System installed a default user is also installed it is called - Главный офицер (Main officer). To log into System Main officer uses the default login and password. When entering the System for the first time officer should change passwordto his/her permanent one. To do this:

1. Go to **Settings** section -> **Users**.
2. On *Главный офицер* (*Main officer*) tab click to select **Change password**.
3. Enter an active password (default one), then the new one, which meets the security requirements (please see Security management), confirm the new password is correct and click **Save**.

Basic operations:

- New user creation
- Account editing
- User activation and deactivation
- Deleting user

5.1 New user creation

Main officer (Главный офицер) is able to add new users to perform the duties of Security officer. To do this the following actions are to be taken:

1. Go to Settings section -> Users tab.
2. Click +Create.
3. Enter the value in accordance with table below:

Parameter	Mandatory parameter	Description
Photo	No	User photo
Username	Yes	New user name (for details please see Настройки безопасности)
Login	Yes	User account (for details please see Настройки безопасности)
Password	Yes	Password for user account (for details please see Настройки безопасности)
Confirm password	Yes	Additional confirmation of password
Console language	No	Interface language for a new user: Russian or English
Contacts	No	Mobile phone number or e-mail address. Few values are allowed.

4. Click Create. A new user will be added to the System. When logging into System for the first time the user should change his/her password.

5.2 Account editing

To edit a user account, take the following actions:

1. Go to **Settings** section -> **Users**.
2. Select required user and click ... opposite his/her name and select **Edit**.
3. In the opened window change one or few settings required.
4. Click **Save**. The new settings will be applied.

5.3 User activation and deactivation

Main officer (Главный офицер) can prevent a selected user from taking any actions in the System. To do this he/she should:

1. Go to **Settings** section -> **Users**.
2. Opposite required user click  and then select **Deativate**. User account will be blocked.

To unlock previously blocked account click the following actions are to be taken:

1. Go to **Settings** section -> **Users**.
2. Opposite the blocked user click  and select **Activate**. The user can continue working in the System.

5.4 Deleting user

Main officer (Главный офицер) can delete user accounts. To do this, the following actions are to be taken:

1. Go to **Settings** section -> **Users**.
2. Select required user and click  opposite his/her name, then select **Delete**.
3. In the opened window click **OK**. User account with all related data will be permanently deleted from the System.

Main officer (Главный офицер) account cannot be deleted.

6 Managing data for analysis

Events available in the System are stored via partitions. Two types of partitions are created in the System:

- events with violations;
- events without violations.

In **Setting** section -> **Data for analysis** contains the list of partitions, each of them are created in the System every day. Partitions parameters are as follows:

Parameter	Description
Creation date	Partititon creation date. Filled in automatically.
Status	*Active partition or Archived partition.*
Date of archiving	Partition archiving date. Filled in automatically when creating an archive with partition.
Violations	If there events with violations in parttiton.
Week	Week dates of partitions creation. **Note:** If there were no events intercepted during a week, this week will be missed in partition.
Year	Partition data creation year.

To reduce the amount of data processing, the following options are available for Security officer:

- Filter creation;
- Events storage
- Manual archiving and restoring partitions.

6.1 Filter creation

Filtering events let you download specific events from partitions to be analyzed, thus significally saving the resources.

Note:

Filtering events can be performed in partitions in case any synchronization with source system took place.

To set up a filter the following actions are to be taken:

1. Go to **Settings** section -> **Data for analysis**.
2. Click **Filtering settings** and then **+Add filter**. You can filter data as follows:
   a. by *Event type*;

b. by *Violation level*;
c. or you can apply both filters.

3. Specify the violation type to get the events with this type as filtering results. Possible values (one or few values can be selected) are as follows:
   a. *No* violation;
   b. *Low*;
   c. *Medium*;
   d. *High*.
4. Specify the data source to get the events with these types as filtering results:
   a. *Skype;*
   b. *Web message;*
   c. *FTP;*
   d. *Webmail;*
   e. *Work e-mail;*
   f. *Messengers (Yahoo!, Jabber, WhatsApp, Viber,Telegram, Mail.Ru Агент, ICQ);*
   g. *Social network (VK, Facebook);*
   h. *Cloud storage;*
   i. *SMS;*
   j. *Photo;*
   k. *Network resources;*
   l. *Terminal session;*
   m. *Crawler;*
   n. *Keyboard input;*
   o. *Printing;*
   p. *Screenshots;*
   q. *Removable devices;*
   r. *Clipboard*, etc.
5. Click **Apply**. Filters application process can take a long time. The first you will see the events which were extracted before, then the new events in accordance with filters specififed.
6. **Data for analysis** table will display the partitions according to applied filters.

6.2 Events storage

To reduce the volume of data stored Security officer can specify the period to store the partitions. To do this, the following actions are to be taken:

1. Go to **Settings** section -> **Data for analysis**.
2. Click **Archive settings**.
3. In the opened window you should specify the number of weeks to store events with violations and the ones without violations. However, please take into consideration the following:
   a. If the value was not specified, all the partitions for all the periods will be saved.
   b. Partitions with events beyond the specified period will be automatically archived.
4. Click **Apply**.

6.3 Manual archiving and restoring partitions

To reduce the volume of data downloaded into the Stystem, Security officer can archive partitions manually. The folowing actions are to be taken to do this:

1. Go to **Settings** section -> **Data for analysis**.

2. Specify the partitions to be archived ( ).
3. Click **Action** and select **To archive a partition**.
4. Make sure the selected partitions status was changed to Archived. Events from specified partitions will not be analyzed.

To restore a partition:

1. Specify an archived partition( ).
2. Click **Action** and select **To restore partition from archive**.
3. Make sure the partition status has changed to *Active*. Events from specified partition will become available for analysis.

7 Security management

To prevent unauthorized access to the System and to protect user from compromizing his/her account data to third parties, Security officer can regulate the password management policies. To do this the following actions are to be taken:

1. Go to **Settings** section -> **Password settings**.
2. In the opened window you can see the default settings. To enter new password requirements, the following paramenets can be changed:

Parameter	Description
Letters	Uppercase letters of Russian and Latin alphabets to be used in password:- obligatory (☑) - optional (☐)
Digits	Arabic numerals to be used in password: - obligatory (☑) - optional (☐)
Special symbols	List of special symbols which can be used in password: - obligatory (☑) - optional (☐)
Minimal length	Minimal length of password (symbols).
Latest N passwords cannot be used	To avoid compromoizing previous passwords cannot be used.
Time before password expires	Number of days when password is active. Password should be changed before the date specified.
Failed login attempts period	Period (minutes) when user can enter invalid password.
Number of invalid input attempts	Number of invalid input attempts, before the account is blocked.
User blocking period	Account blocking period in days.

3. Click **Save** to implement changes. If you require to get back to previou settings, click Reset to default settings.

Example

Failed login attempts period - 30

Number of invalid input attempts - 4

User blocking period - 3

If you use the parameters specified, then after 4 invalid input attempts in 30 minutes the user account will be blocked for 3 days. User may enter the password after 3 days.

User accpount requirements:

- Username should consist of two symbols minimum;
- System login should contain 2 symbols minimum.

8 License management

In order to to work with a System you should have an active license. When entering the System for the first time a prompt trial license will be installed6 it is active for active for one month.



To install a new license please take the following actions:

1. Go to **Licensing** section.
2. Click **+Add**.
3. In the opened window specify the path to the file with active license.

To delete the lisence:

1. Click  in the right top corner of license tab and select **Delete**.
2. in the opened window confirm the action by clicking **OK**.

Note:

Before deleting the license you previously used, make sure you have a file with a new active license. The System operation cannot be performed without license. After the license has been changed, we would recommend performing integrations with source systems again.

Note:

When a prompt trial license expires, data export from source systems will be terminated.

9 Managing organizational chart download

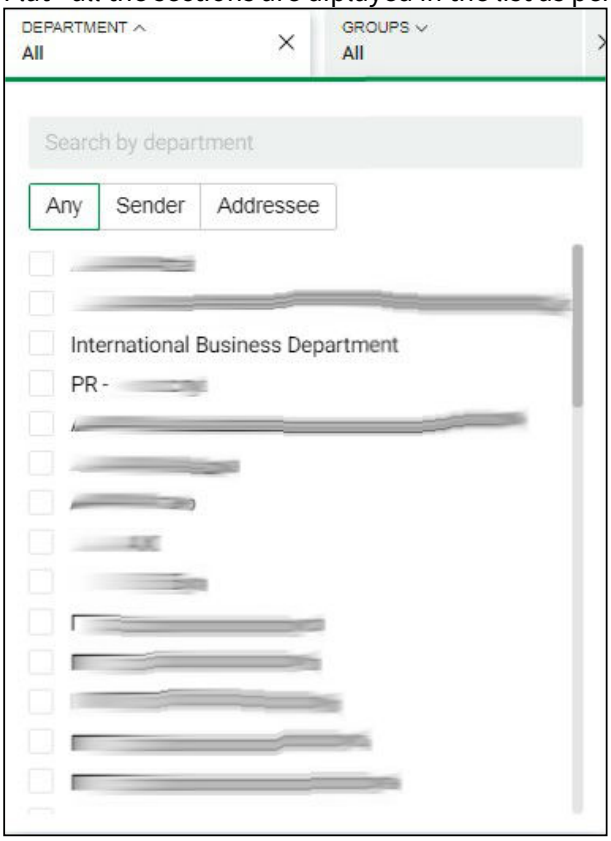
This section contains the System download settings:This section contains System download settings:

- Display settings;
- Internal domains.

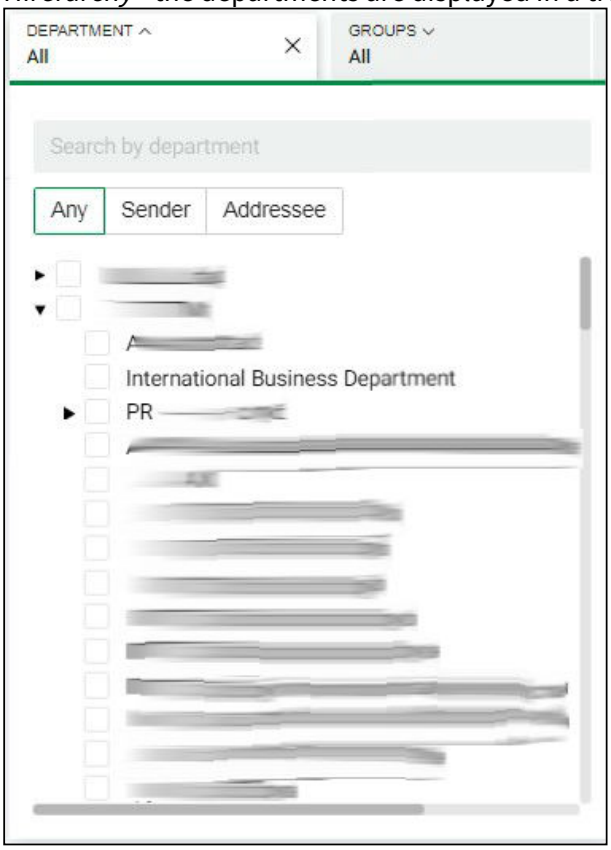
9.1 Display settings

When synchronising with Active Directory, the System is provided with a list of company's departments. Security officer can manage the display of this list as per Single filter:

- *Flat* - all the sections are diplayed in the list as per one level;



- *Hirerarchy* - the departments are displayed in a tree view.



If you require downloading departments without employees, specify opposite **Load empty departments**.

9.2 Internal domains

Security officer ois able to create a list of domains, contacting these domain will be considered as internal contacts.

To add internal domain please do the following:

1. Click **Add new** within **Settings** tab.
2. Enter domain names in *companyname.ru format.*
3. Click **Save**. Further contacts with specified domain will be considered by System as internal one.

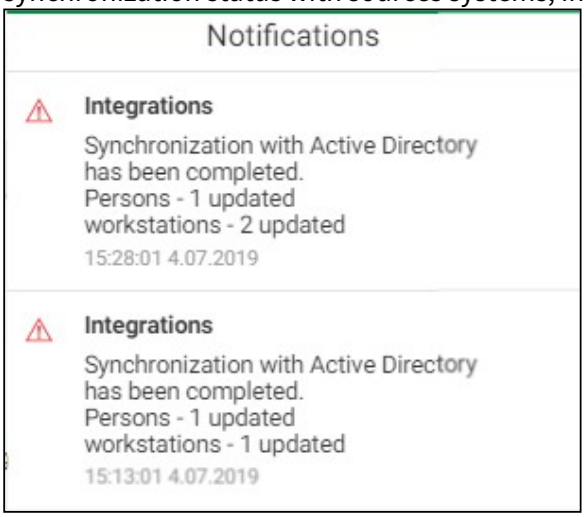
To delete internal domain, the following actions are to be taken:

1. Click opposite the domain name.
2. Click **OK** in the opened window.

10 Notifications

You can see all the notifications by clicking  on the navigation panel. Notifications are used to inform users about:

- synchronization status with sources systems, initiated by this user;



- limitations of data export from source systems in accordance with active license.