Roger Access Control System 5v2

Application note no. 021

Document version: Rev. C

Active Directory integration

Note: This document refers to RACS 5 v2.1.2 or newer

Introduction

RACS 5 system enables integration with directory services including Active Directory service, which is a hierarchical database containing information on users, user groups, computers and other company resources in computer network with Windows servers from Microsoft. Active Directory service enables to manage user in the network, to define their access to network resources and to configure computers.

The integration of RACS 5 system with Active Directory (AD) enables:

- VISO operator authentication by means of AD credentials
- Manual synchronisation of RACS 5 user list and AD user list
- Automatic synchronisation of RACS 5 user list and AD user list

The benefit of importing is such that user list in particular organization can be managed from one location (Active Directory) and modifications of such list can be propagated into RACS 5 access control system. Based on user's Organization Unit (OU) in AD an Access User Group with the same name is created in RACS 5 and the user is assigned to the group. Access User Groups can be assigned with Authorisations (access rights) in VISO software so the assignment of user to particular OU in AD will result in assignment of access rights in RACS 5 system.

Note: In RACS 5 system v2.1.2 the method Manual synchronisation of users is no longer available and its description is included in this note only for customer who operate older versions of RACS 5 system.

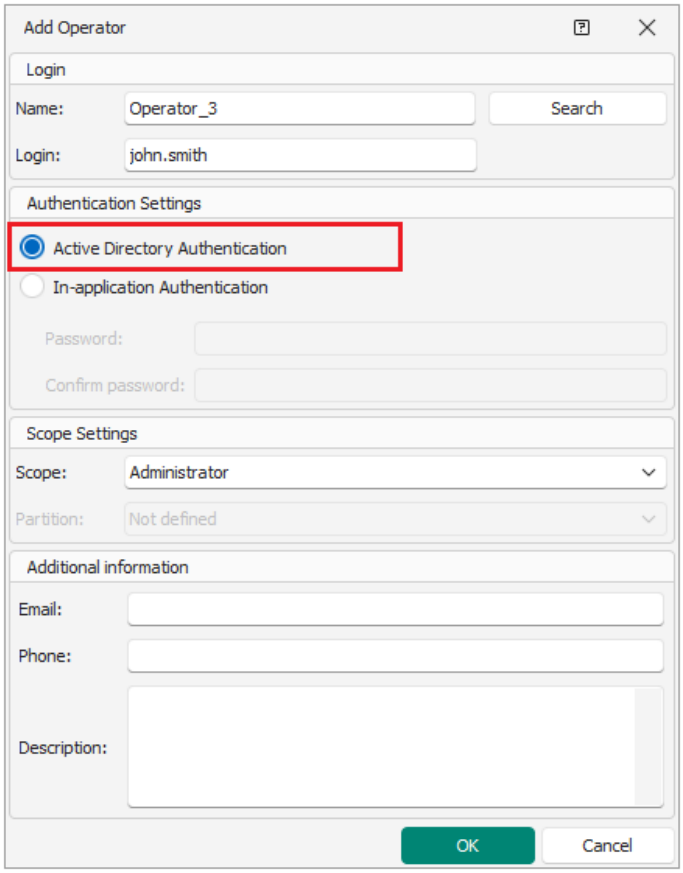
Operator authentication

'Admin' Operator is created automatically in VISO software as described in AN006 application note. According to AN040 application note it is possible to define multiple Operators in VISO software for management of RACS 5 system and for each Operator the access to various areas of VISO software can be defined (e.g. user management, access to monitors and maps, etc.)

Operator must enter valid login and password to start VISO software. Credentials can be stored in RACS 5 database or in Active Directory database. In the second scenario the Operator can use the same credentials for Windows system and VISO program and passwords for both systems can be managed from the level of the Active Directory. In order to configure authentication in VISO by means of Active Directory:

- Create a user in Active Directory domain
- Start VISO program and in the top menu select *Administration* and then *Operators*.
- In the opened window select *Add* to define new Operator or *Edit* to modify existing Operator.

- In the next window enter login of the user from Active Directory and select the option *Active Directory Authentication*.



Manual synchronisation of users

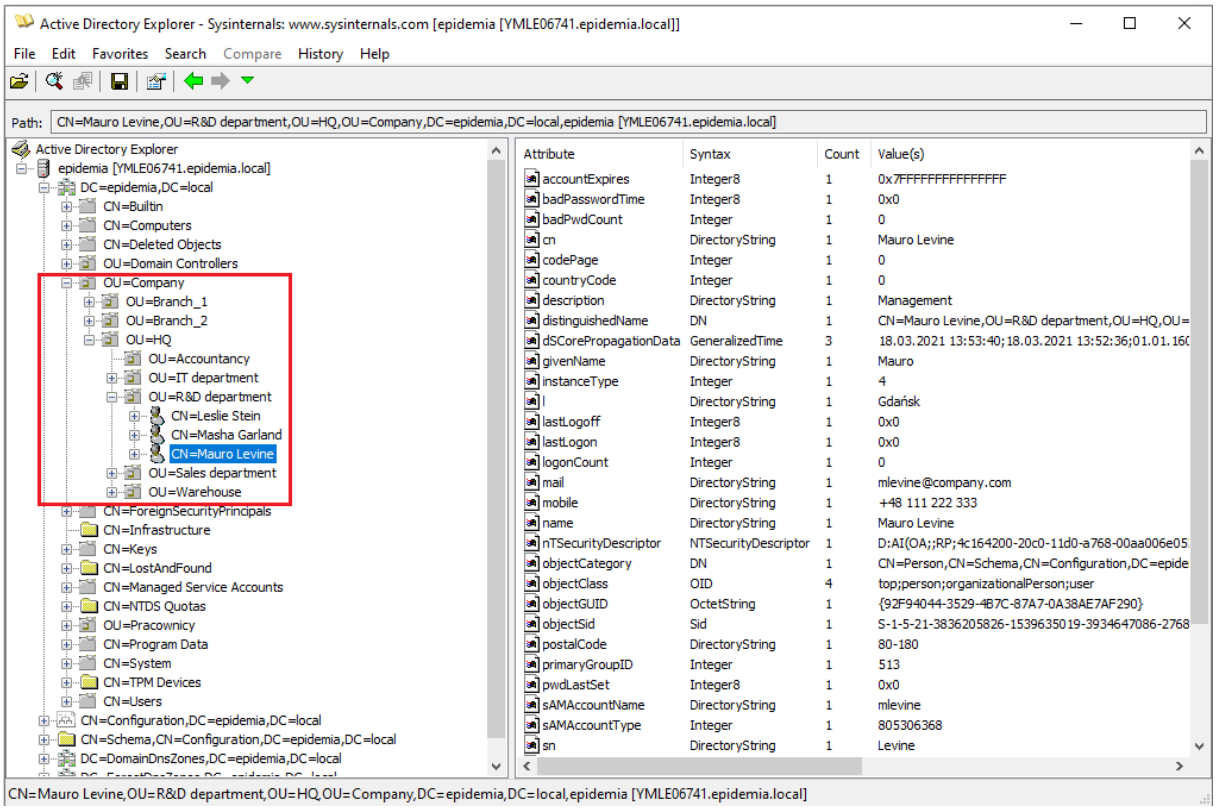
Note: Manual synchronisation method is not available in RACS 5 system version 2.1.2 or newer.

Manual AD synchronisation enables to import users from directory service (AD) on request of VISO Operator. The import concern AD attributes listed in *VISO->Tools->Attribute Mappings*. It is also possible to define own mappings as explained further in this note.

Users importing

In order to import users:

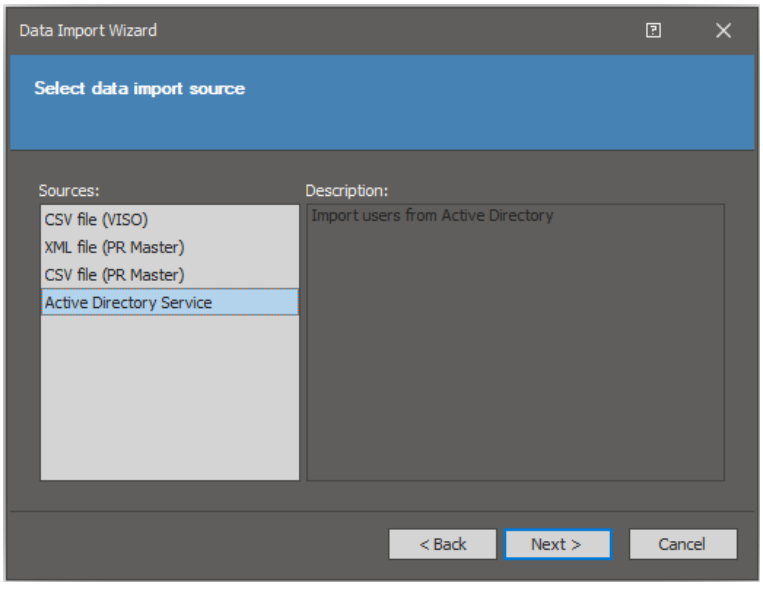
- Configure RACS 5 system in regard of Communication Server, database, controllers, Access Doors, Authorisations, etc. according to AN006 application note.
- Create users in Active Directory domain and organize them in such containers as organization units (OU) as in example below. Later, during the import it will be possible to select units for data import.
- Define such details for users as first name, last name and optionally email, phone, address, description and other.



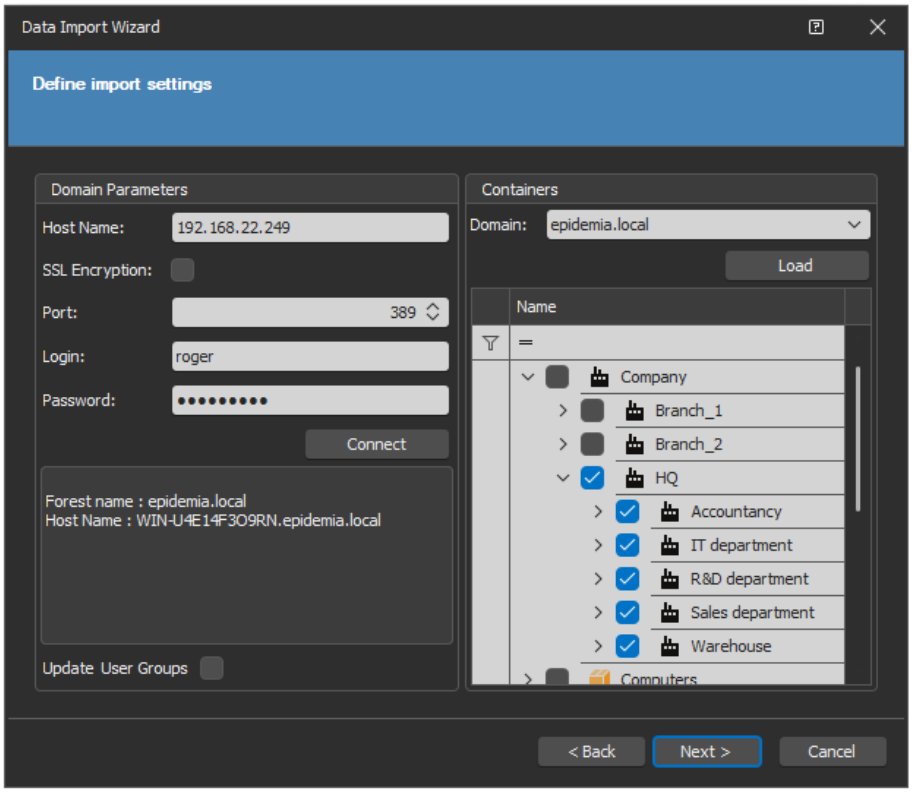
- Start VISO program and in the top menu select *System* and then *Import…*

Note: The computer with installed VISO software must be logged in Active Directory domain in order to collect data from this domain. Detailed range of data for collection depends on assigned AD rights.

- In the opened window select *Next*, then *Active Directory* and *Next* again.

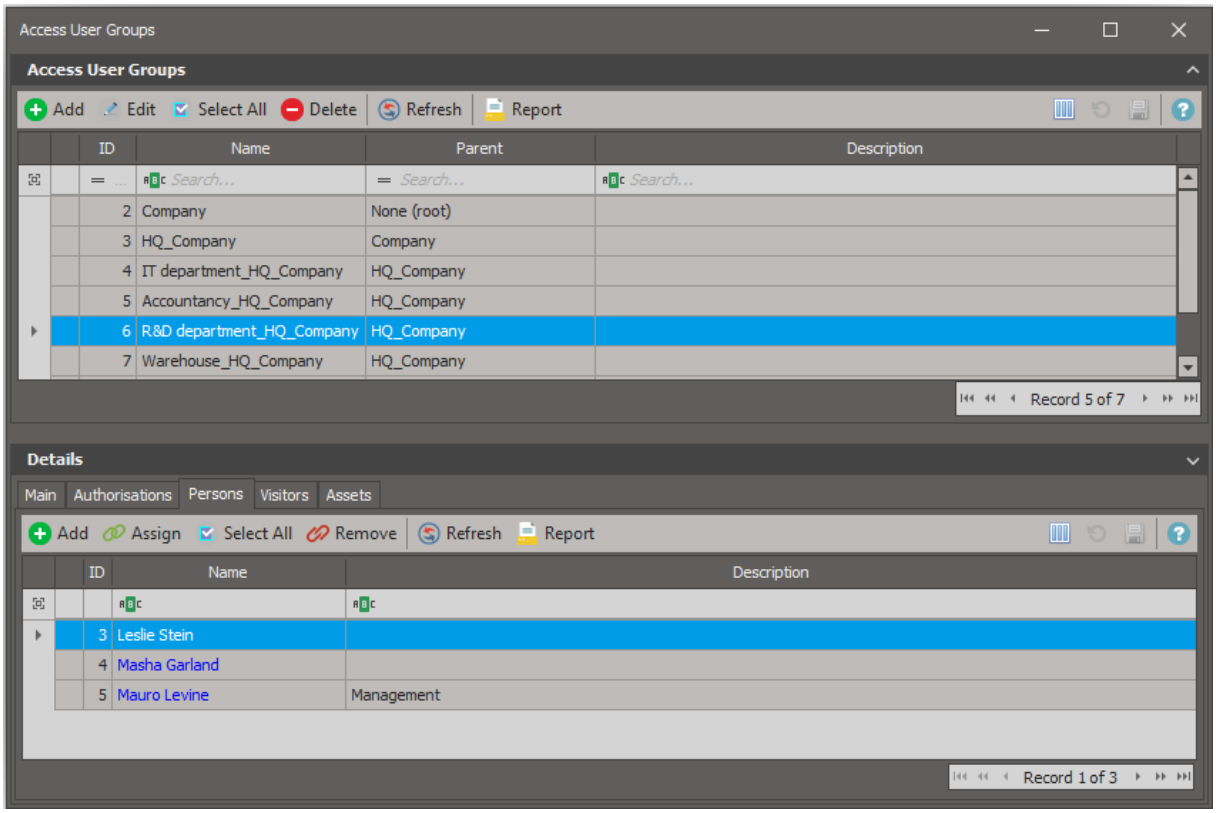


- In the next window enter domain parameters, click *Connect* and then select domain and click *Load*. Select OU containers on the list in order to import users from these OU containers. If the option *Update User Groups* is enabled then users who were imported previously and then manually moved to other Groups in VISO software now will be updated according to their OU in AD.

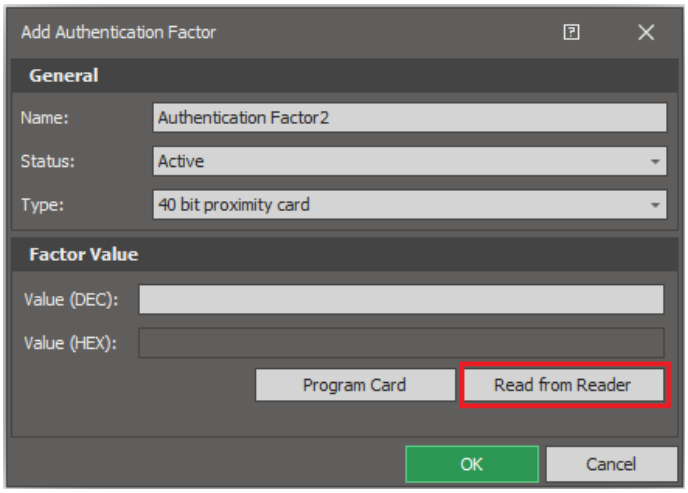


Note: Users will be imported only from selected units and it will be only users directly listed in the unit. For example if *HQ* unit is selected but *IT department* unit is not selected then only users who are directly listed in *HQ* unit will be imported while users listed in *IT department* unit will not be imported until this unit is selected.

- In the next windows select *Next* and in the last window select *Finish* to import users. During the import only users i.e. objects with attribute sAMAccountType=805306368 are imported while others as for example printers are omitted.
- In the top menu of VISO software select *Configuration* and then *Access User Groups*. If no groups were earlier created in RACS 5 with the same names as AD units then they will be created automatically during the import and users will be assigned to them.
- In the bottom select *Authorisations* tab and then assign previously created Authorisations to particular group. All Persons belonging to the group will have the same rights to doors and other objects in the system.
- Optionally select *Persons* tab, then select particular Person and in the opened window in *Authorisations* tab assign individual Authorisations to the Person. In such scenario the Person will have rights resulting from group it belongs to and additionally own rights.

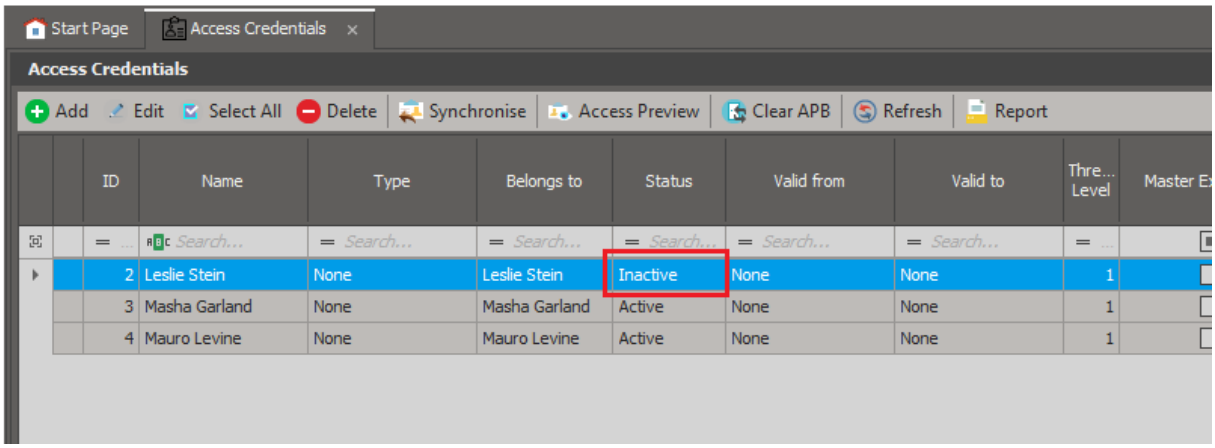


- In the top menu of VISO software select *Configuration* and then *Access Credentials*.
- For the Access Credential of particular Person, in the bottom select *Authentications Factors* tab and then *Add* to define card, PIN or other factor type which will be used for Person identification at RACS 5 readers. Card number can be read at RUD series administrator reader connected to computer's USB port or any other reader installed in the system.



Users disabling and removing

Every time users are imported from AD then they will be updated in RACS 5 system. If user account is disabled in AD then after the import, the Access Credential of corresponding Person in VISO will also be disabled. If user account is removed from AD then after the import corresponding Person and Access Credential will be removed from RACS 5 database.



Synchronisation with MC16 controllers

After the synchronisation of RACS 5 database with MC16 controllers, Persons with inactive Access Credentials and deleted Persons lose the possibility of identification on RACS 5 readers.

Such synchronisation in RACS 5 system can be started on request by right clicking Communication Server and then *Synchronise* in the navigation tree of VISO software or automatically based on synchronisation schedule, which can be defined by selection of *Schedules* command in the navigation tree of VISO software. Synchronisation schedule is assigned within Communication Server.

Automatic synchronisation of users

Automatic AD synchronisation enables to import users list from directory service (AD) in the background with defined frequency. Such synchronisation is ensured by virtual controller from RogerSVC software package and it requires license on the level of VISO software. Imported users data (attributes) are the same as in case of previously mentioned manual synchronisation.

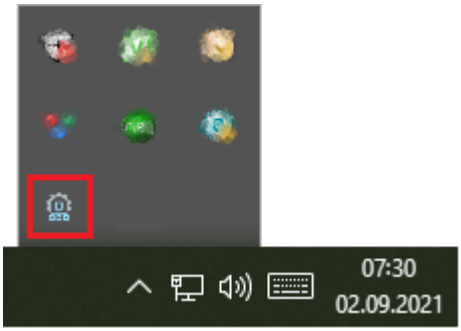
Preliminary configuration of RACS 5

In order to conduct preliminary configuration of RACS 5:

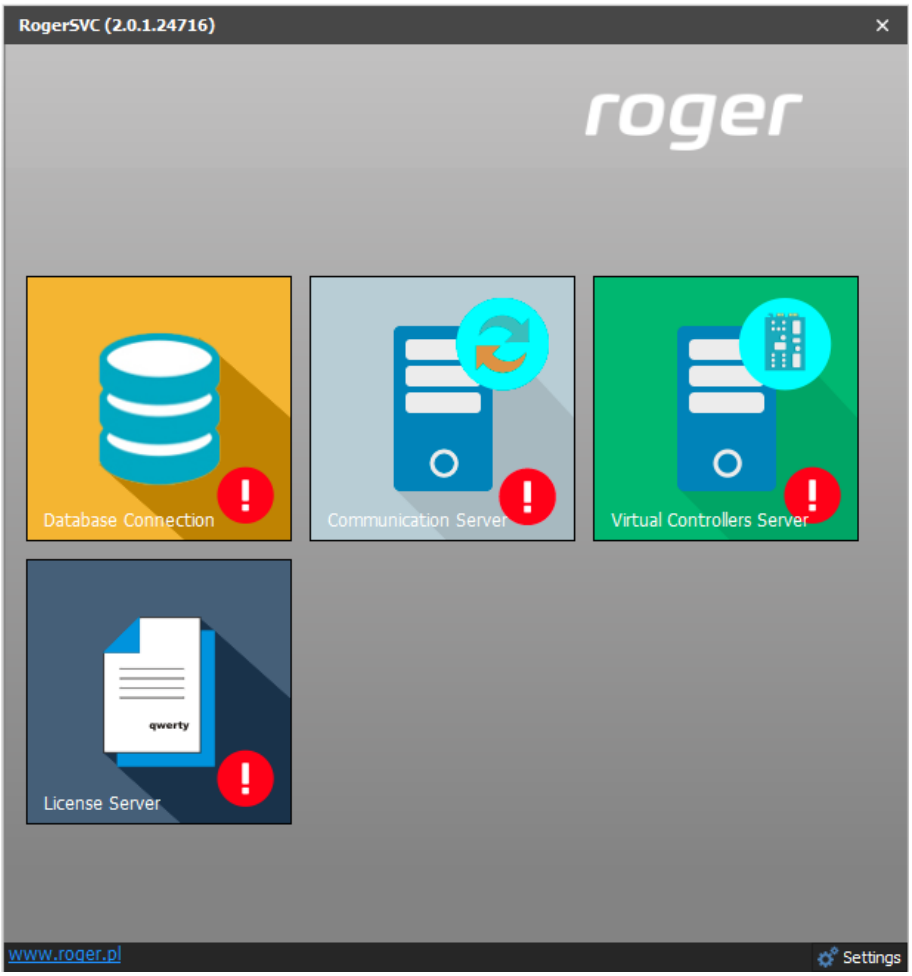
- Install VISO software and create database according to AN006 application note.
- Install RogerSVC software and select not only Communication Server but also License Server and Virtual Controllers Server. If servers are supposed to be operated on individual computers then install RogerSVC on each computer selecting required servers.

Note: If License Server and Virtual Controllers Server are supposed to be operated on individual computers then during installation of Virtual Controllers Server, the License Server must be deselected. Only in such case it will be possible to indicate external License Server when Virtual Controllers Server is configured.

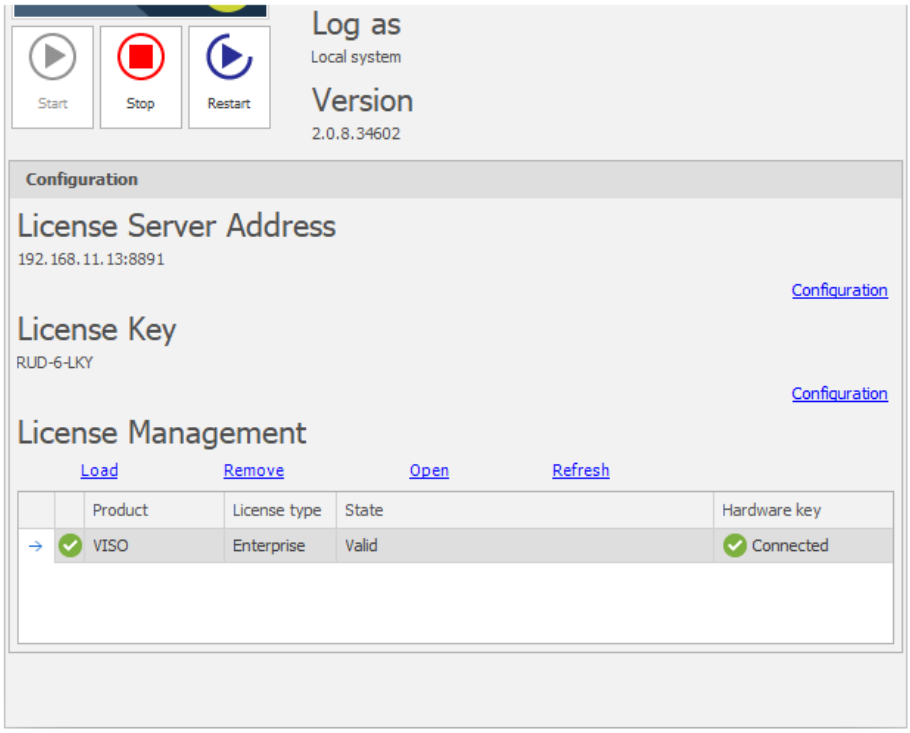
- When RogerSVC is launched then its icon is displayed in Windows tray. Click the icon . The RogerSVC icon in tray can also be launched from Windows menu *Start-> Roger-> RogerSVC.*



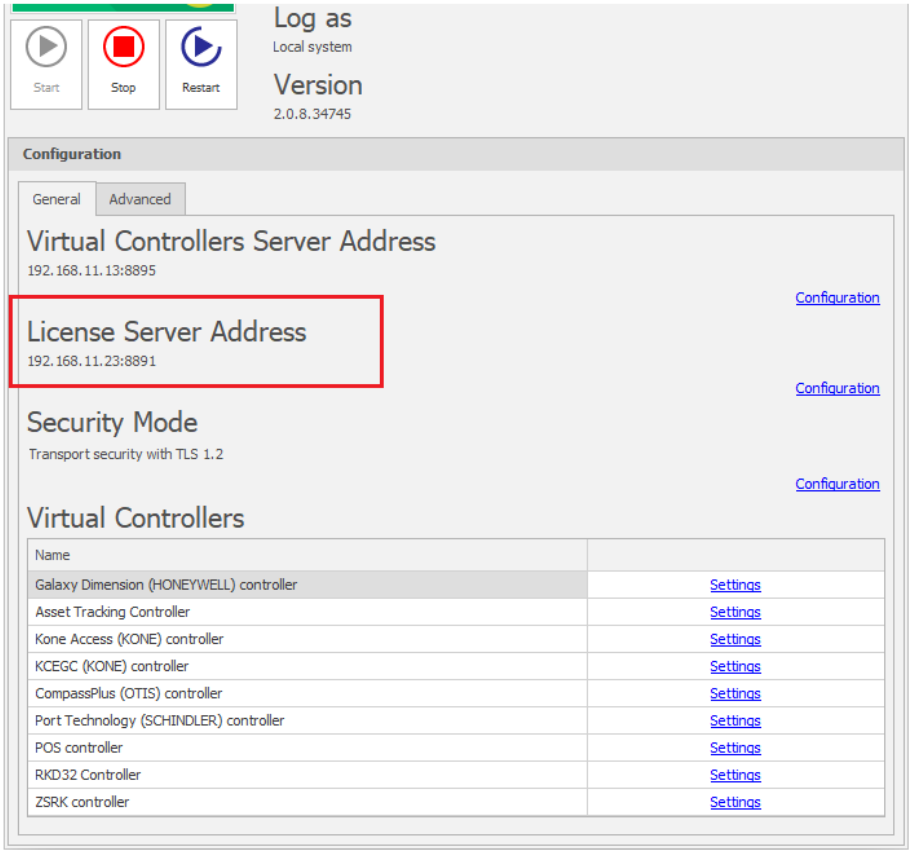
- In the RogerSVC window select *Database Connection* tile and then *Configuration* to indicate previously created RACS 5 database. Return to the main window.



- In the RogerSVC window select *Communication Server*, click *Configuration,* enter IP address of the computer with the server installed e.g. 192.168.11.13 and define port (8890 by default).
- Select *Start* and return to the main window. The server will be started and operated in the background whenever the computer is switched on even if RogerSVC window is closed.
- Connect RUD-6-LKY hardware key to USB port of computer with License Server installed or connect RLK-1 hardware key to LAN and enter its IP address.
- In the RogerSVC window select *License Server* tile, click *Configuration,* enter IP address of the computer with the server installed e.g. 192.168.11.13 and define port (8891 by default).
- Select *Load license file* and indicate purchased license file for the hardware key.
- Select *Start* and return to the main window. The server will be started and operated in the background whenever the computer is switched on even if RogerSVC window is closed.



- In the RogerSVC window select *Virtual Controllers Server* tile, click *Configuration*, enter IP address of the computer with the server installed (e.g. 192.168.11.13) and define port (8895 by default).
- If contrary to previously presented configuration steps, the License Server is installed on a computer with exemplary 192.168.11.23 address while Virtual Controllers Server is installed on computer with exemplary 192.168.11.13 address then it is possible to indicate external License Server for virtual controllers as below.



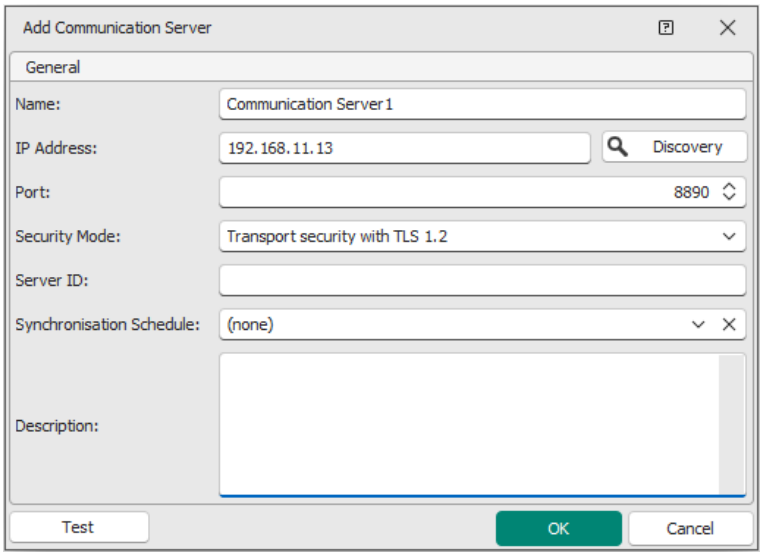
- Select *Start* and return to the main window. The server will be started and operated in the background whenever the computer is switched on even if RogerSVC window is closed.
- Start VISO software, in the top menu select *System*, then *Select License Server* and indicate previously defined License Server from RogerSVC software in order to start the VISO program in licensed version.

Connection and import

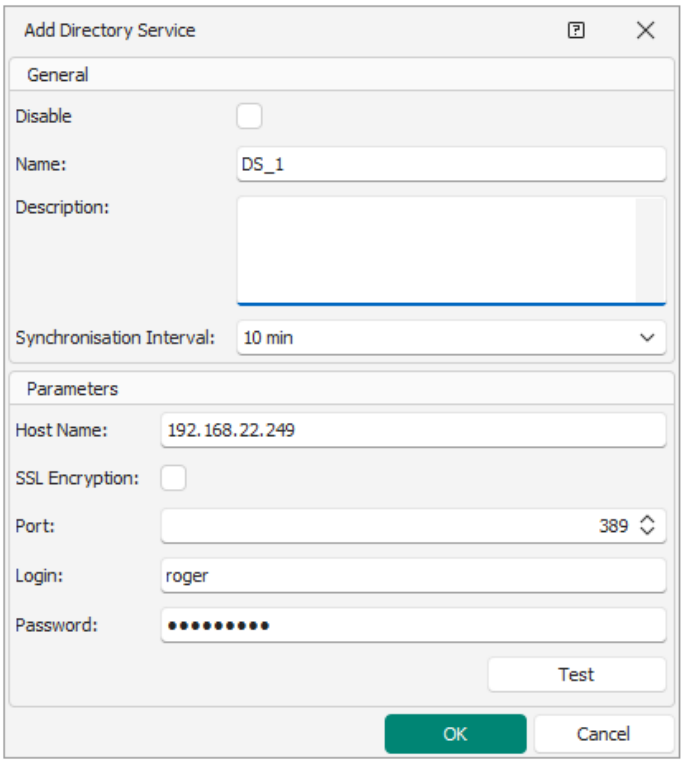
Note: If the integration with Active Directory is applied along with the integration with fire alarm systems (it concerns OPC integration i.e. Bosch. Schrack Seconet and Esser Honeywell fire panels) then it might be necessary to install OPC Core Components 3.0 Redistributable (x86 or x64) drivers and to add following entry in setttings.config file which is by default located in C:\Program Files\ROGER\RogerSVC.
<add key="OpcLabs.EasyOpc.Internal.OpcPSBoxing.EnableOpcCorePSBoxer" value="false"/>

In order to configure virtual controller:

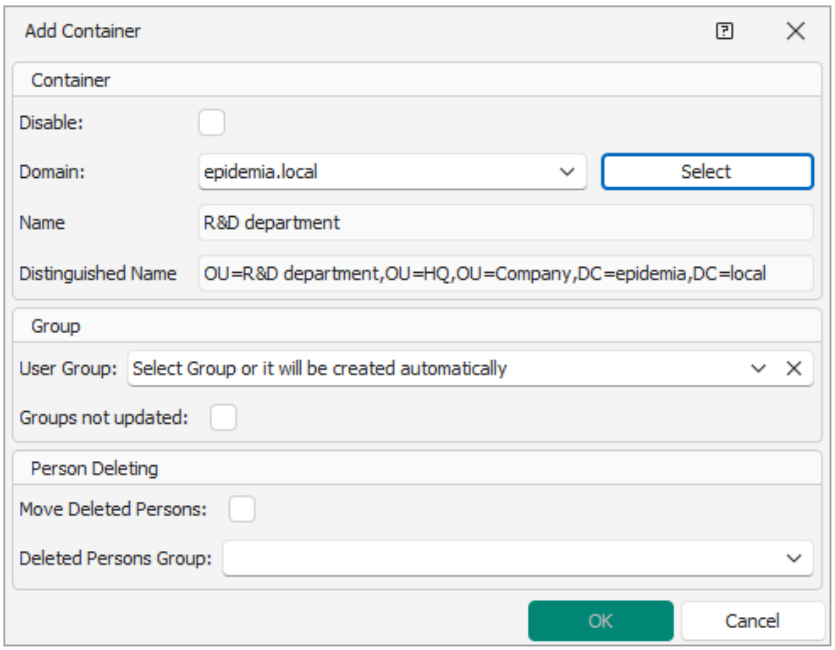
- In the opened window enter parameters of Communication Server previously configured in RogerSVC program and close the window with *OK* button. It is recommended to apply TLS 1.2 mode to encrypt the communication.



- In the navigation tree right click *Virtual Controllers Server* and select *Add Server*. In the opened window enter parameters of Virtual Controllers Server previously configured in RogerSVC program and click *OK*. It is recommended to apply TLS 1.2 mode to encrypt the communication.
- In the navigation tree right click the server and select *Add Virtual Controller*. In the section *Other Systems* select *Directory Service Controller*. If the controller is not on the list then most probably there is license error on the level of VISO software or RogerSVC software. Close the window with *OK* button.
- In the navigation tree double click *Directory Service Controller* and in the opened window select *Add*.
- In the opened window define parameters for connection with Active Directory service. Automatic synchronisation interval can be defined in range from 1 minute to 24 hours. Close the window with *OK* button.



- In the bottom select *Containers* tab and then *Add*.
- In the opened window click *Select* in order to choose organizational type (OU) container in particular domain. If previously created Access User Group is selected in the window then imported users will be assigned to the group. If no group is selected then it will be created automatically during import and its name will be based on the name of selected organizational units.
  If the option *Groups not Updated* is enabled then users who were manually moved to other groups by VISO Operator after synchronisation, will not be moved back to their original groups after the next synchronisations. In other words actions of VISO operator will not overwritten/reverted.
  If the option *Move Deleted Persons* is enabled then users deleted in Active Directory will not be deleted in VISO during synchronisation but they will be moved to the group indicated with the option *Deleted Persons Group*. Close the window with *OK* button.



- Define more containers within the same directory service and if needed define more directory services with their containers in other domains.
- In the top select *Import* in order to start importing of users or wait till users are imported automatically according to *Synchronisation Interval* (every 10 minutes by default). During the import only users i.e. objects with attribute sAMAccountType=805306368 are imported while others as for example printers are omitted.
- Similarly as in case of manual AD synchronisation, assign Authorisations on the level of Access User Groups and Persons as well as define Authentication Factors (e.g. cards) on the level of Access Credentials belonging to Persons.

Note: It is not recommended to apply automatic synchronisation and previously described manual synchronisation as it may result in conflicts. In case of automatic synchronisations users can be imported on request by selection of *Import* button in the window of directory services.

Users disabling and removing

In case of automatic synchronisation, users disabling and removing functions in the same way as in case of previously mentioned manual synchronisation. Users who are removed in AD will be removed in RACS 5 and users who are disabled in AD will be disabled in RACS 5.

Synchronisation with MC16 controllers

In case of automatic synchronisation, the synchronisation with MC16 controllers functions in the same way as in case of previously mentioned manual synchronisation. Controllers can be configured on request or automatically based on schedule which is configured by selection of *Schedules* in the navigation tree of VISO software.

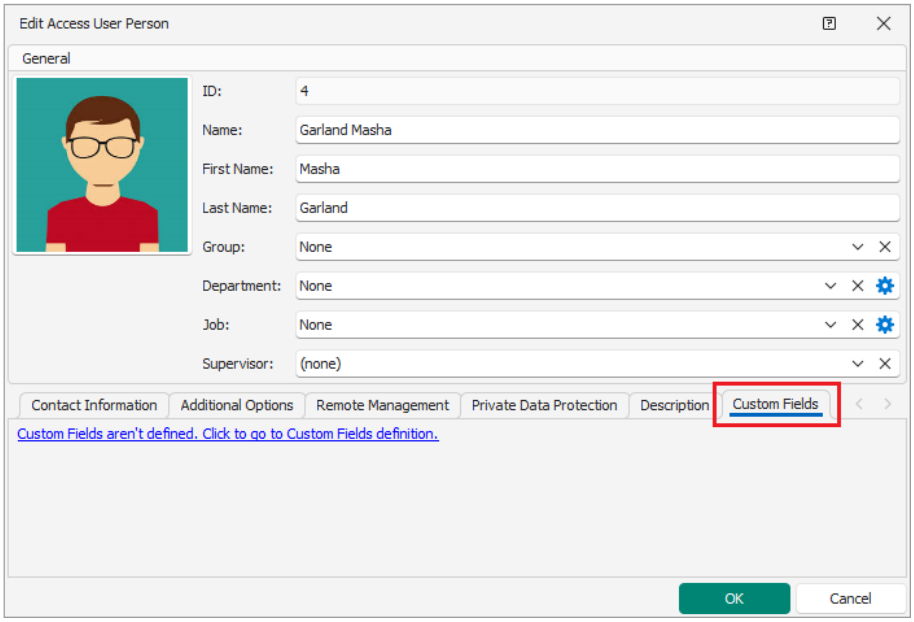
Attribute mappings

It is possible to map attributes in VISO software i.e. define what user data is imported from AD to VISO software and where it is saved. Mappings are defined after selection of *Tools-> Attribute Mappings* in the top menu of VISO software. The list of predefined mappings includes:

- Name (name)
- First name (givenname)
- Last name (sn)
- Description (description)

- Email address (mail)
- Phone number (telephonenumber)
- Address (streetaddress)
- City (l)
- Postal code (postalcode)
- Job (title)
- Department (department)
- Supervisor (manager)
- Access Credential deactivation (useraccountcontrol)
- Access Credential validity (accountexpires)

It is possible to edit these mappings and define own ones. Mappings can target not only built-in Person fields in VISO such as for example first or last name but it is also possible to define custom fields by selection of *Tools-> Person Custom Fields* in the top menu of VISO software and then define mapping which will import user parameter from AD to such Person Custom Field. When Person Custom Field is defined then it is visible in the tab *Custom Fields*.



Contact:
Roger sp. z o.o. sp.k.
82-400 Sztum
Gościszewo 59
Tel.: +48 55 272 0132
Fax: +48 55 272 0133
Tech. support: +48 55 267 0126
E-mail: support@roger.pl
Web: www.roger.pl