

Roger Access Control System 5 v2

Application note no 047

Document version: Rev. B

Port Technology (SCHINDLER) **integration**

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

Introduction

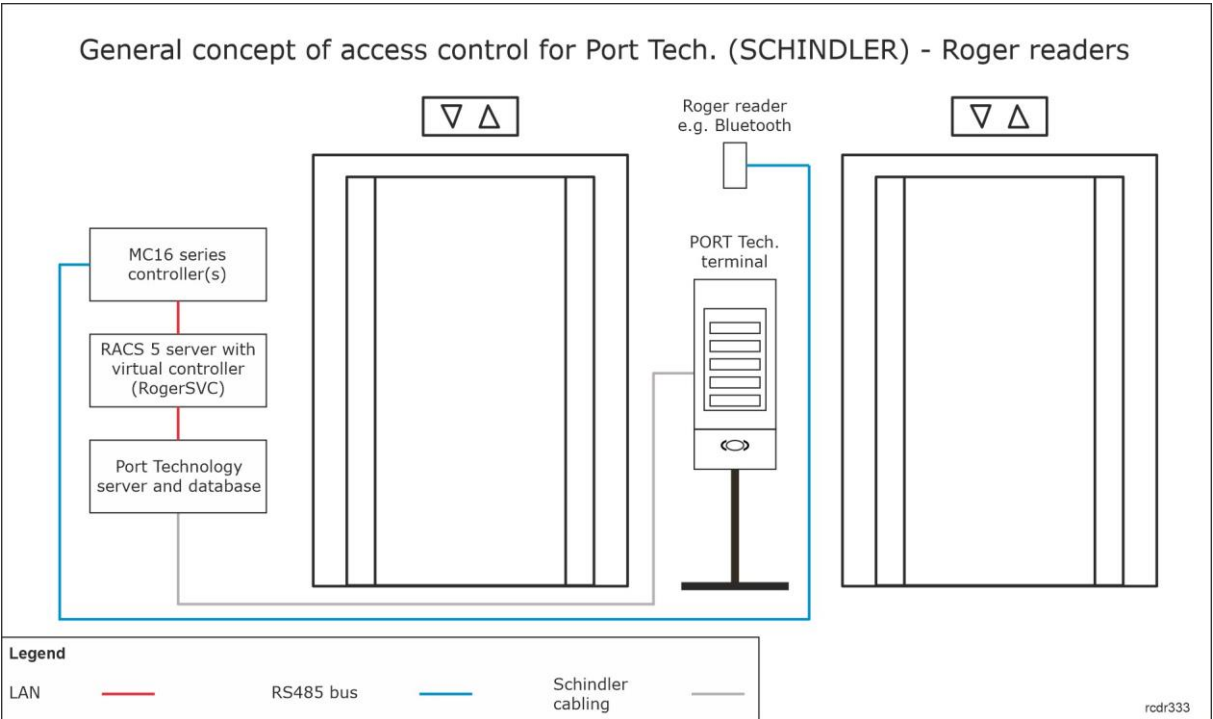
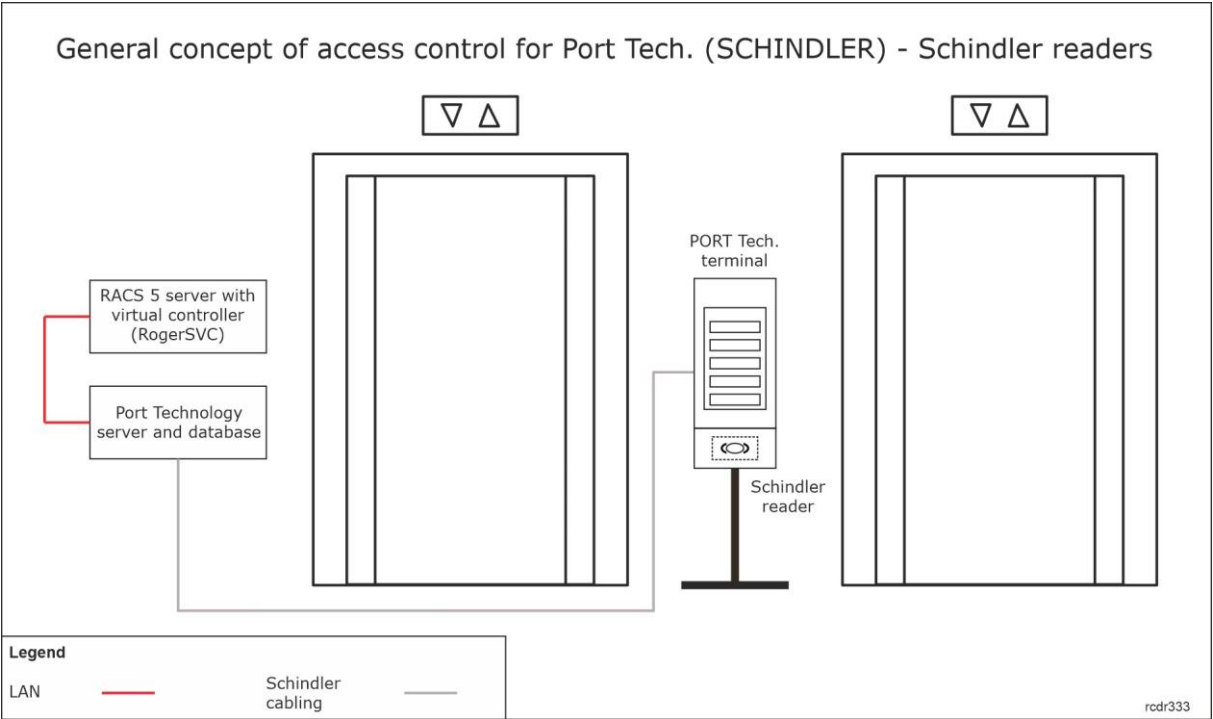
RACS 5 system enables software integration with Port Technology elevator system from SCHINDLER company. The communication between both systems is provided in LAN and it requires installation and configuration of RACS 5 virtual controller. The integration is based on Port Technology software v 1.3.371.1 or newer and it requires licensed VISO EX management software.

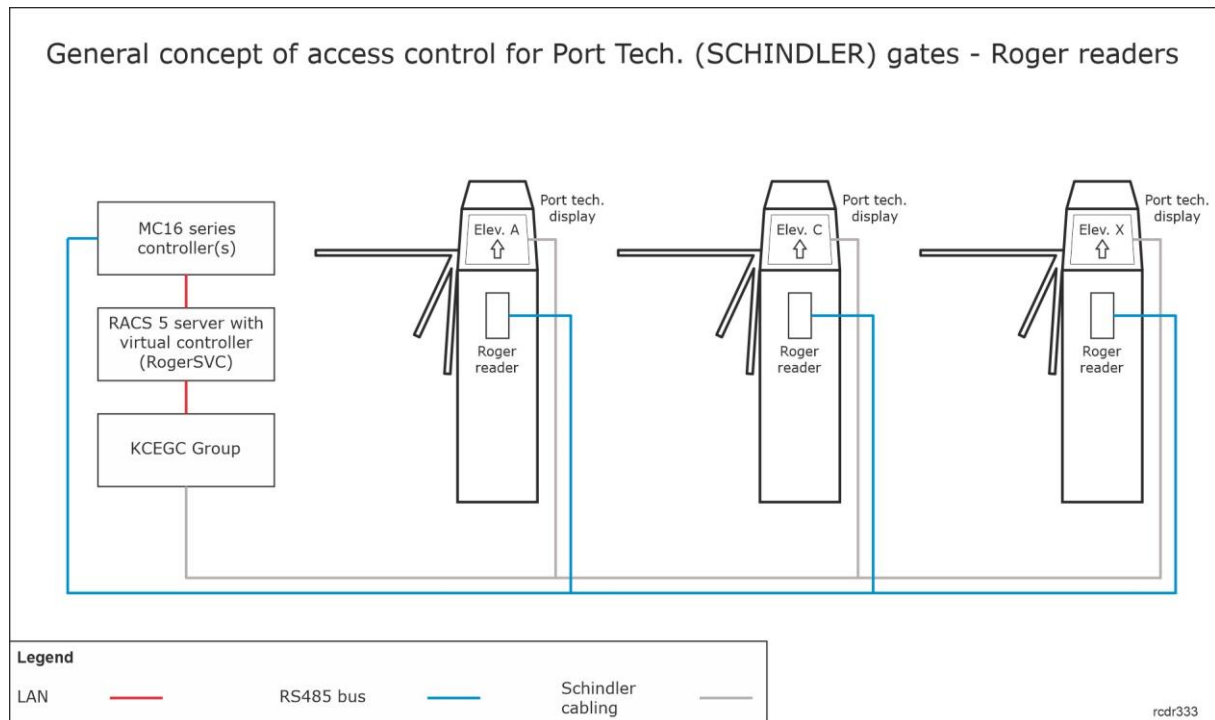
The integration is database type (3rd Party Database Interface) and it can be extended with the use of Roger readers (3rd Party Call Interface - Call by ID). In case of basic integration, only Schindler card readers installed inside PORT terminals can be used while in case of extended integration all kinds of Roger readers and controllers can be used to control access to elevators and at entry barriers/turnstiles. In case of Roger readers not only proximity cards but also mobile factors (BLE,NFC) and QR codes can be used to identify users. Additionally this method also allows to apply advanced access control functionalities such as antipassback, user counting, multistage user authentication, etc.

The integration enables centralized management of users and their access rights both on the level of RACS 5 doors and Port Technology (SCHINDLER) elevators. Particularly the RACS 5 system enables to:

- Assign Access Profiles which are defined in Port Technology system and they determine user rights in elevator system.
- Define user validity end date.
- Define Authentication Factors (e.g. cards) for user.
- Define default floor/zone for user:
 - from any floor/zone
 - from specified floor/zone
- Apply Master Groups and User Templates to user.
- Monitor connection status with Port Technology server.

Note: RACS 5 system enables also universal access control in elevators offered by various manufactures. This solution is based on MCX8-BRD expanders and it is explained in AN030 application note.

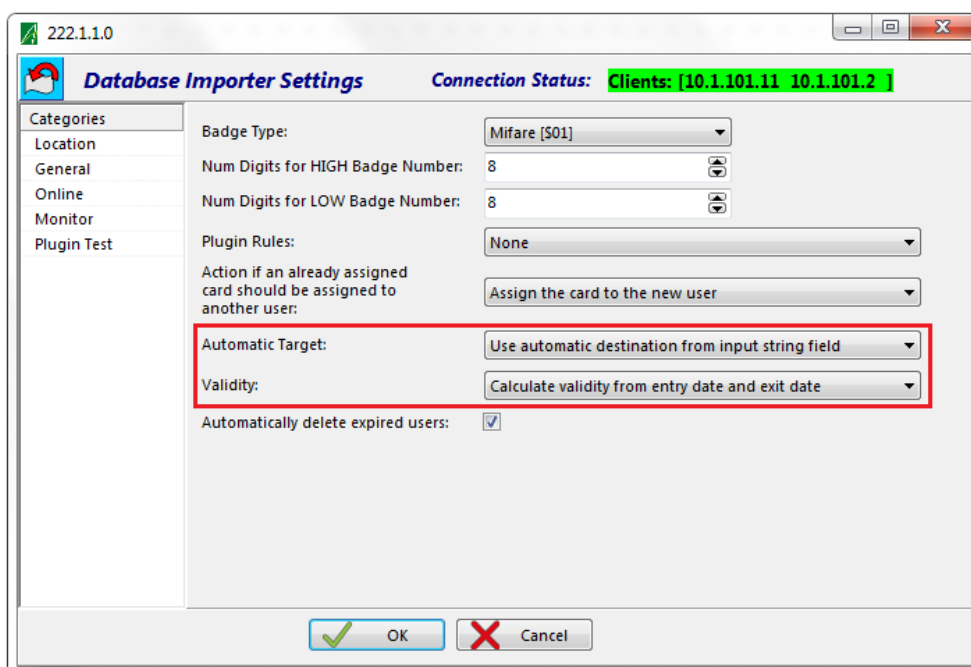




Note: Additional information on general installation and configuration of turnstiles is given in AN019 application note.

Configuration of Port Technology elevators

The installation and configuration of elevators is done by their supplier. It concerns number of elevators, arrangement of floors and zones as well as Access Profiles which include floor access rights. Prior to configuration of the integration it is necessary to obtain list with the names of Access Profiles as well as floor and zone numbering in Port Technology system so the data could be used in RACS 5 system. The list of Master Groups and User Templates can also be obtained if they are supposed to be used within the integration.




Additionally it is necessary to configure import settings in Port Technology system particularly in regard of such parameters as *Automatic Target* and *Validity* so the settings from VISO software could actually be received and applied in Port Technology system.

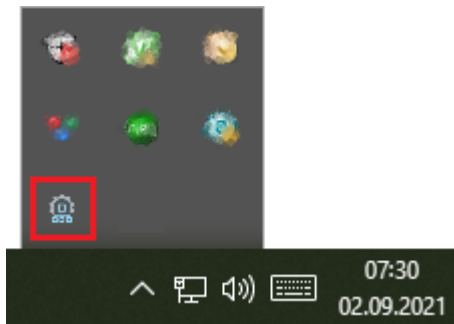
Preliminary configuration of RACS 5

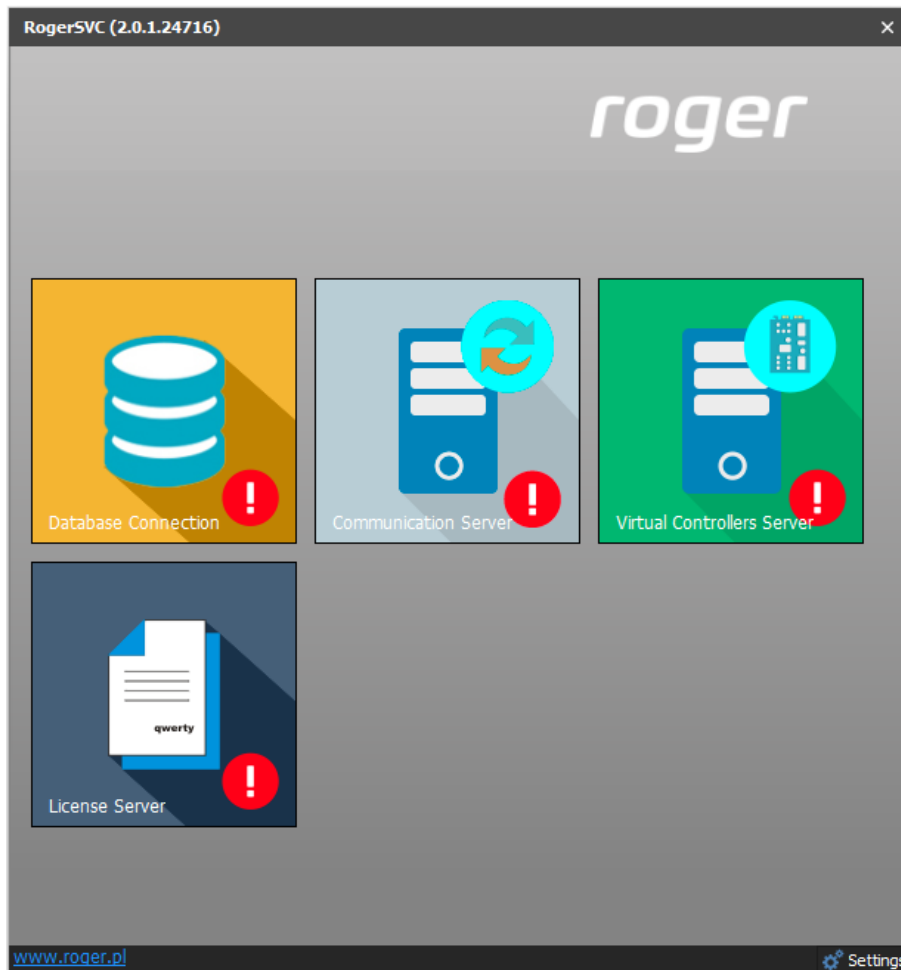
In order to conduct preliminary configuration of RACS 5:

- 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.

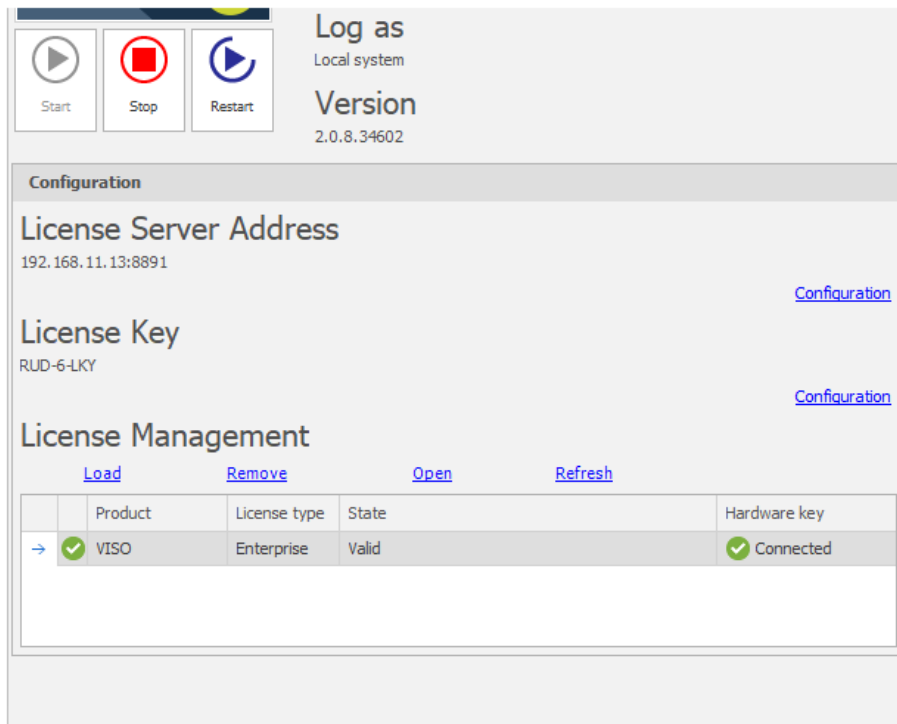
Note: If License Server and Virtual Controllers Server are supposed to be operated on individual computers then during installation of Virtual Controllers Server, the License Server must be deselected. Only in such case it will be possible to indicate external License Server when Virtual Controllers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

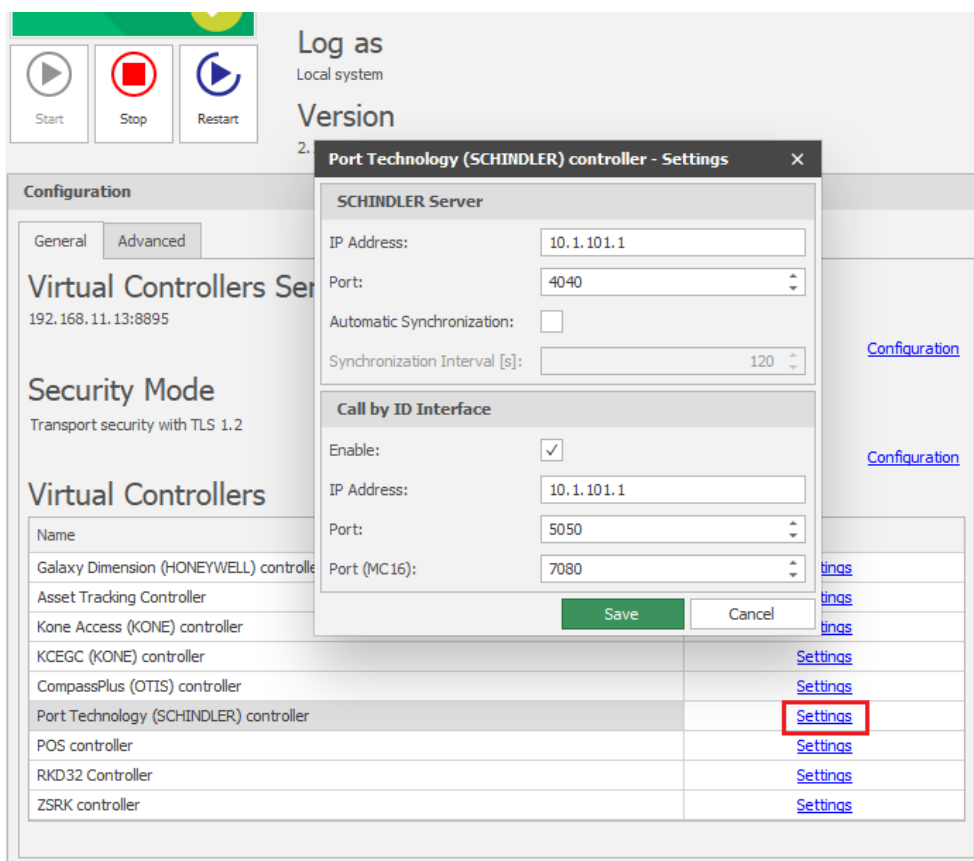




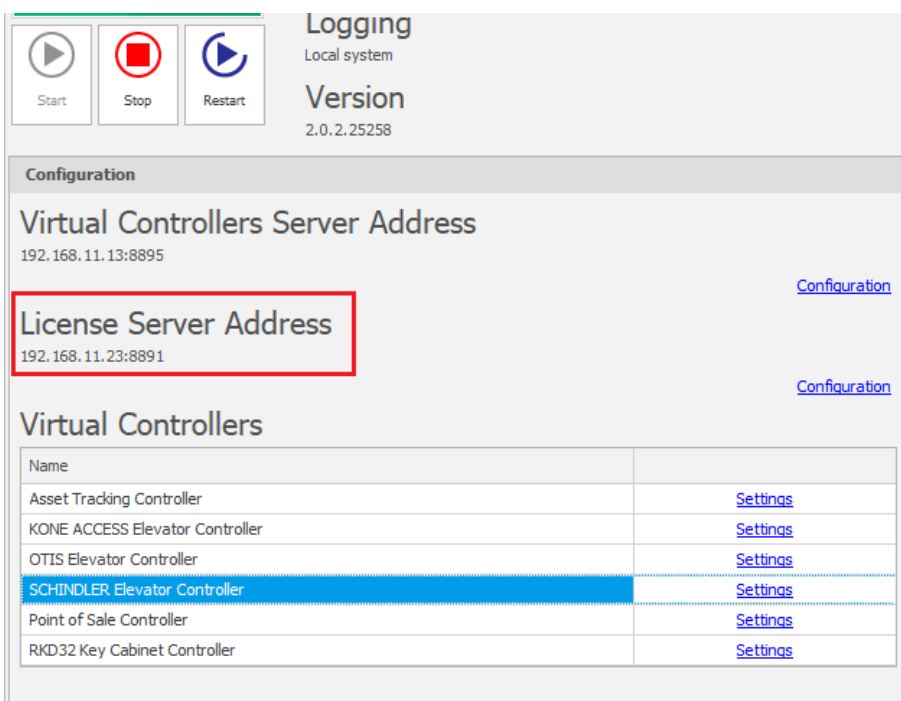
- In the RogerSVC window select *Database Connection* tile and then *Configuration* to indicate previously created RACS 5 database. Return to the main window.
- In the RogerSVC window select *Communication Server*, click *Configuration*, enter IP address of the computer with the server installed e.g. 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 there are two network adapters on the server with virtual controller installed e.g. one for communication with VISO software and MC16 controllers and another one for communication with Port Technology server then two communication channels can be applied. In the example below, the communication with SCHINDLER servers is done via network adapter with 10.1.101.1 IP address. Enabling of Call by ID interface is optional and it depends on the applied scenario of operation. Additionally it is possible to enable automatic synchronisation (update) of users in Schindler database with specified frequency.



- 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.

Additional low level configuration of MC16 controller

Additional configuration is necessary only if Call by ID method is applied in the system. In such case MC16 controllers which are connected with Roger readers used for elevator system require not only typical low level configuration with RogerVDM or VISO v2 but also defining of certain parameters in their configuration files. In order to configure these parameters:

- Start RogerVDM software.
- According to its installation manual establish the connection with MC16 controller.
- In the top menu select *Tools->Configuration file*.
- In the opened window configure following parameters:

ETI=192.168.11.13
ETP=7080

where:

ETI – IP address of computer with Virtual Controllers Server from RogerSVC software.

ETP – port for communication of MC16 controller with Virtual Controllers Servers which is configured in RogerSVC software (by default 7080)

Alternatively, both ETI and EPI parameters can be configured on MC16 memory card in DEBUG.CFG file.

Connection with Port Technology system

In order to configure virtual controller:

- If Communication Server is not already configured in VISO software then in the navigation tree of VISO software right click *Networks* command and select *Add Communication Server*.
- 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.

The screenshot shows a window titled "Add Communication Server" with a "General" tab. The fields are as follows:

- Name:** Communication Server 1
- IP Address:** 192.168.11.13 (with a "Discovery" button next to it)
- Port:** 8890 (with a dropdown arrow)
- Security Mode:** Transport security with TLS 1.2 (with a dropdown arrow)
- Server ID:** (empty field)
- Synchronisation Schedule:** (none) (with a dropdown arrow and a close button 'X')
- Description:** (empty text area)

At the bottom, there are three buttons: "Test", "OK", and "Cancel".

- 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 *Elevator Systems* select *Port Technology (SCHINDLER) 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 expand the virtual controller and double click *Profiles*.
- In the opened window select *Add* to create Profile in RACS 5 system.
- In the next window name the Profile in the field *Name (RACS 5)* – this will be used in VISO software when Profile which represents elevator access rights is assigned to user. In the field *Name (SCHINDLER)* enter the name of Access Profile which was previously defined in Port Technology system.

Note: Profile name in *Name (SCHINDLER)* field must be exactly the same as Access Profile name in Port Technology system including lowercase and uppercase characters.

- Define remaining Profiles in VISO for each Profile created in Port Technology system.

- Optionally, in the same way define Master Groups and Templates if they are supposed to be used on the level of Access User Groups.

General configuration of integration

Users management

The management of users in the system can be done with wizards, which are accessed by selection of *Wizards* command in the top menu of VISO software. New user can be enrolled with *Add Person Online* wizard. The use of wizards is explained in AN006 Application note.

In regard of users, wizards enable to:

- Define validity date for user's Access Credential e.g. for 1 month.
- Define destination floor/zone.
- Define boarding floor/zone
- Define Authentication Factors for user (e.g. cards, NFC/BLE mobile factors).

Add Person Online

Access Credential details
Enter Access Credential data and click [Next] to continue.

Steps

- Person details
- Access Credential type selection
- Access Credential details**
- Authorisation Groups selection
- Authorisations selection
- Authentication Factors defining
- Data saving
- Synchronisation

General

Name: Access_Credential_4_KS

Type: None

Valid from: 10/29/2020 12:00 AM

Valid to: 11/5/2020 12:00 AM

Facility Code Type: ☐

Additional Options | Exemptions | Description | SCHINDLER integration

Destination Floor: None

Destination Zone: None

Boarding Floor: None

Boarding Zone: None

Note: Port Technology (SCHINDLER) system does not accept *Valid from* date and time which are earlier than current date and time.

Note: During assignment of destination and boarding floors/zones to Access Credential it is necessary to know their IDs which are defined in Port Technology software.

Note: The option *Master exemption* which in general perspective gives all Authorisations to user in RACS 5 system does not concern Port Technology system.

Access Rights Assignment

Access Rights in regard of elevator system are defined in Port Technology software by means of Profiles. For each such Profile an equivalent must be created in VISO software and then elevator access rights are defined in VISO software by assignment of such Profiles to users.

In order to assign Port Technology rights:

- In the top menu of VISO software select *Configuration* and then *Access Credentials*.
- In the opened window the list of Access Credentials belonging to previously created users is displayed.
- For particular Access Credential in the bottom select *SCHINDLER Profiles* tab and then assign previously created Profile(s) as needed to define user rights in elevator system.

Details

Main | Authorisations | Authorisation Groups | **SCHINDLER Profiles** | Authentication Factors

Assign | Select All | Remove | Refresh | Report

ID	Name	Inherited From (Object Type)	Inherited From (Object Name)
1	SCHP_1	Own	
2	SCHP_2	Own	
3	SCHP_3	Access User Group	Access User Group2

- In the navigation tree of VISO software right click previously created virtual controller and select *Synchronise*.
- In the opened window select *Start* to upload users to the elevator system.

	Access Credential	User First Name	User Last Name	Card 1	Valid from	Valid to	Boarding/D...	Pending operation	Status
<input checked="" type="checkbox"/>	2 Access_Crede...	Miles	Porter	00000000C25EAF0	1/1/2000 12:00 AM	1/1/2038 12:00 ...		+ Add	None
<input checked="" type="checkbox"/>	4 Access Creden...	Mauro	Connors	00000000CE7D156A	1/1/2000 12:00 AM	1/1/2038 12:00 ...	1_1_2_2	+ Add	None
<input checked="" type="checkbox"/>	5 Access Creden...	Levine	Mauro	000000008384D440	1/1/2000 12:00 AM	1/1/2038 12:00 ...		+ Add	None

Note: There is option in RogerSVC software within virtual controller which enables automatic synchronisation of users with a specified frequency.

Schindler Profiles can be also assigned on the level Access User Groups and then Persons can be assigned to groups so they can acquire those rights in elevator system by being part of a group. Person can be assigned to particular group also on the level of Add Person Online wizard.

Particular Access User Group can also be assigned with Master Group and Template if they are defined in both system. They facilitate user management in particular scenarios of operation.

Templates

The application of Templates is optional and at first they must be configured in elevator system where they are used to facilitate the configuration of users. User who is assigned to a Template can inherit access rights, validity period and other parameters included in the Template.

In order to apply Templates in VISO:

- In the navigation tree of VISO software expand the virtual controller and double click *Templates*.
- In the opened window select *Add* and then enter the name of a Template previously configured in elevator system. Additionally enter the Template name to be used in VISO software. Repeat the same steps for all required Templates.
- In the top menu of VISO software select *Configuration* and then *Access User Groups*.
- Create new group or edit existing one.
- In the next window assign one of the Templates to the User Group.

Master Groups

The application of Master Groups is optional and at first they must be configured in elevator system where they are used to divide users into groups which correspond to companies, departments, etc. Particular Master Group is managed by particular Master or Supermaster operator.

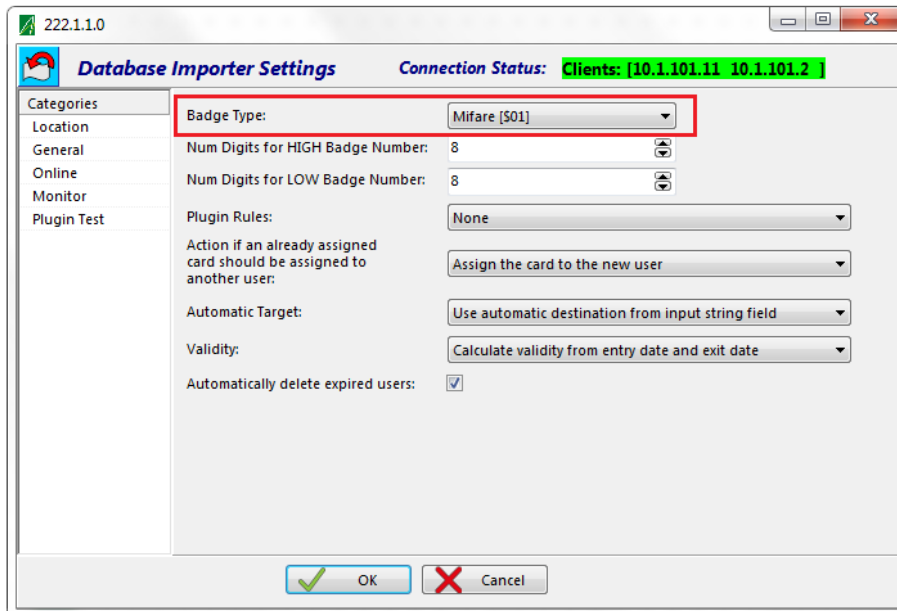
In order to apply Master Groups in VISO:

- In the navigation tree of VISO software expand the virtual controller and double click *Master Groups*.
- In the opened window select *Add* and then enter the name of a Master Group previously configured in elevator system. Additionally enter the Master Group name to be used in VISO software. Repeat the same steps for all required Templates.
- In the top menu of VISO software select *Configuration* and then *Access User Groups*.
- Create new group or edit existing one.
- In the next window assign one of the Master Group to the User Group.

Note: If no Master Groups are defined in VISO software then every user uploaded to elevator system by default will be assigned to Master Group 0.

Factor Mappings

In the typical integration, *Mifare [\$01]* badge type is selected in Schindler software while *40bit proximity card* Authentication Factor Type is used for user cards in VISO software.



If *None [\$00]* badge type is selected in Schindler software then various card technologies such as Mifare Classic, Mifare DesFire, etc. can be applied at the same time. In such case the elevator system expects that each uploaded user card number will be preceded with a header defining its type. In such scenario it is necessary to define mappings in VISO software i.e. define link between Authentication Factor Types from VISO software and badge types from Schindler system. It is possible to use predefined Authentication Factor Types and define own types by selection of *Authentication Factor Types* in the navigation tree of VISO software.

Additional configuration for Call by ID integration

According to previous description in case of Call by ID method a Person calls elevator by means of Roger reader connected to MC16 controller instead of Schindler reader. Such scenario requires additional configuration in RACS 5 system. Therefore it is necessary not only to configure virtual controller in RogerSVC program and make additional low level configuration of MC16 controller but it is also required to define Access Points as Schindler terminals and define Authorizations for Access Doors with these Access Points as follows:

- In the top menu of VISO software select *Wizards* and then *Add Access Door*.
- According to AN006 application note define read-in door and point Roger reader which will be used to call elevators. The wizard will create also Authorization for such door. A Person which calls elevator should be assigned not only with Profile(s) but also with Authorization for the door with the Access Point. If the reader is supposed to control gate or turnstile then it is also necessary to indicate output which will be activated when access is granted.
- In the navigation tree of VISO software within Port Technology virtual controller double click *PORT Terminals*.
- In the opened window select *Add* and then assign previously defined Access Points with Schindler terminal IDs so the elevator system could know from where the elevator is called by a Person. The list of possible Schindler Terminal IDs can be acquired from the installer/supplier of elevator system.

Note: Additional information on general installation and configuration of turnstiles is given in AN019 application note.

Monitoring

In RACS 5 system events are generated for various actions and conditions. Events can be browsed after selection of *Event log* in the top menu of VISO software and then *Event log* or they can be monitored in real time after selection of *System Monitors* in the top menu of VISO software and then *Event Monitor*. In both cases events can be filtered.

Communication

The communication with Port Technology server is monitored and respectively [70004] and [70005] events are generated both for lost and restored communication. Additionally for all events in RACS 5 system it is possible to define alerts and notifications (mobile text, email) in accordance with AN041 application note.

Users

Events related to user access granting and denying are registered only in Port Technology system.

Operators

Operator actions in VISO software are registered in log which can be accessed by selection of *Administration* in the top menu of VISO software and then *Operator Log*. More information on Operators is given in AN040 application note.

The screenshot displays the 'Operator Log' window in the VISO software. The window has a title bar and standard window controls. Below the title bar, there's a 'Time range' dropdown set to 'Last 30 days', a 'Refresh' button, and a 'Report' button. The main area is a table with columns: Time and Date, Operator, Host, Action/Command, Object Type, Object, and Description. The table contains several rows of log entries. The second row is highlighted in blue. Below the table, there's a 'Details' section with a 'Main' tab. This section contains fields for Time and Date, Operator, Code, Object Type, Object ID, Description, and Host. To the right of these fields is a large text area titled 'Added Users Identifiers' and 'Changed Users Identifiers'.

Time and Date	Operator	Host	Action/Command	Object Type	Object	Description
5/25/2021 10:19:53 AM	[1]: Administrator	YMLK016960	Synchronise	Virtual Controller	2 VCL1	
5/25/2021 10:19:53 AM	[1]: Administrator	YMLK016960	Synchronise	Virtual Controller	2 VCL1	
5/25/2021 10:16:32 AM	[1]: Administrator	YMLK016960	Log in	Operator	1 Administrator	
5/25/2021 10:16:11 AM	[1]: Administrator	YMLK016960	Log out	Operator	1 Administrator	
5/25/2021 10:16:09 AM	[1]: Administrator	YMLK016960	Edit	System Options		NFC/BLE authentication factor encr...
5/25/2021 10:16:09 AM	[1]: Administrator	YMLK016960	Edit	System Options		Navigation tree sorting method
5/25/2021 10:16:09 AM	[1]: Administrator	YMLK016960	Edit	System Options		PIN digits
5/25/2021 10:16:09 AM	[1]: Administrator	YMLK016960	Edit	System Options		PIN fixed length
5/25/2021 10:16:09 AM	[1]: Administrator	YMLK016960	Edit	System Options		Only unique PINs

Record 2 of 485

Details

Main

Time and Date: 5/25/2021 10:19:53 AM

Operator: Administrator

Code: Synchronise

Object Type: Virtual Controller

Object ID: 2

Description: VCL1

Host: YMLK016960

Added Users Identifiers

6,8

Changed Users Identifiers

7

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