Roger Access Control System 5v2

Application note no. 049

Document version: Rev. A

KCEGC (KONE) integration

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

Introduction

RACS 5 system enables software integration with Destination Controller System (DCS) from KONE company based on KCEGC elevator controllers. The integration can be implemented using:

- RCGIF v1.12 communication protocol
- GCAC v1.8 communication protocol
- Kone Access Rev. 8.5 communication protocol

The communication between both systems is provided in Ethernet network and it requires installation and configuration of virtual controller from RogerSVC software. Usually the server with virtual controller is equipped with two network adapters where one is used for communication with elevator system and the other is used for communication with MC16 access controllers. The integration requires licensed VISO EX management software.

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.

Integration – RCGIF protocol

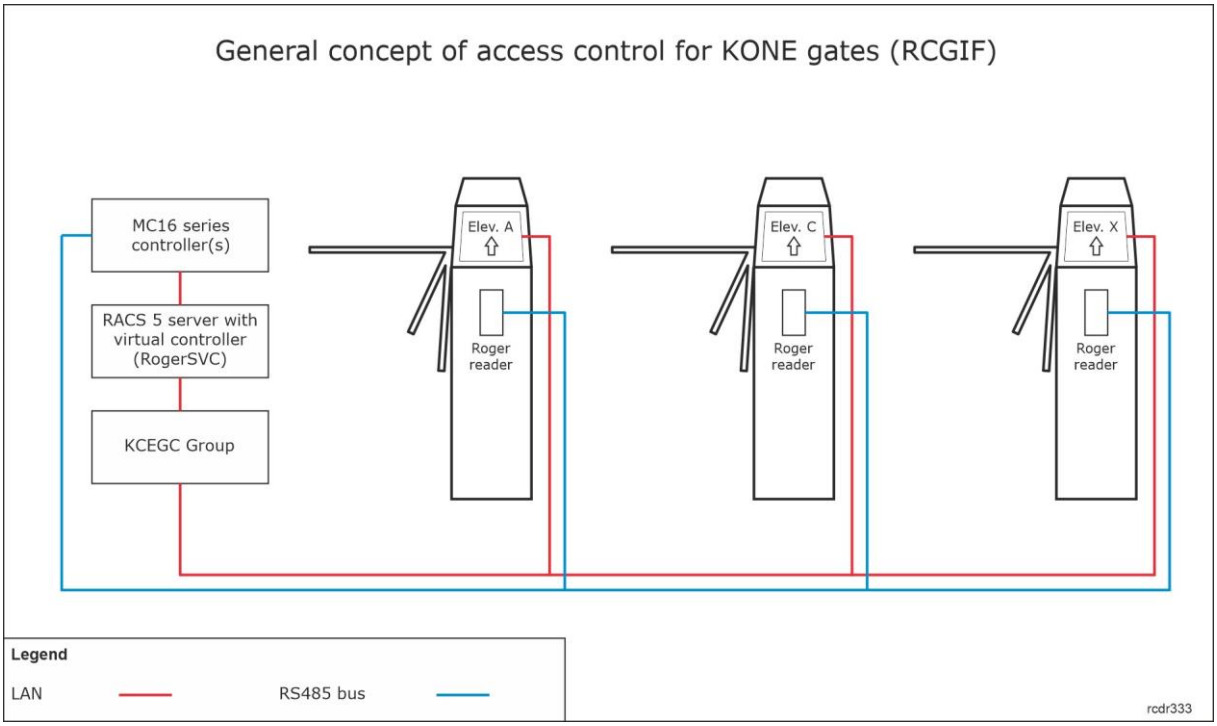
This integration is applied in such scenario where granting the access to a user at gate or turnstile is also supposed to call an elevator. When access is granted then elevator number is displayed on a screen at the gate. Floor is not selected by user manually because the system calls the elevator for previously defined home floor. This integration enables to define access rights including schedules, calendars and exceptions. This is online type integration so it requires stable and uninterrupted connection between access control system and elevator system.

The integration via RCGIF protocol can be applied in parallel with two other types of integrations but in practical applications it is much more often used with integration via GCAC protocol. The integration via Kone Access protocol enables by itself the calling of elevator to home floor but in case of integration via RCGIF protocol it is also possible to apply more advanced access control functions such as for example Global Anti-passback.

All types of readers which are supported by MC16 controller can be installed at turnstiles including MCT series readers which can recognise not only proximity cards abut also mobile factors (NFC/BLE) and QR codes. MC16 controller can also be connected with OSR series readers with OSDP protocol and third party readers with Wiegand protocol.

Note: For this integration it is recommended to apply 1, 2 and 3 door access controllers at turnstiles i.e. MC16-PAC-1, MC16-PAC-2 and MC16-PAC-3 controllers.

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



Integration – GCAC protocol

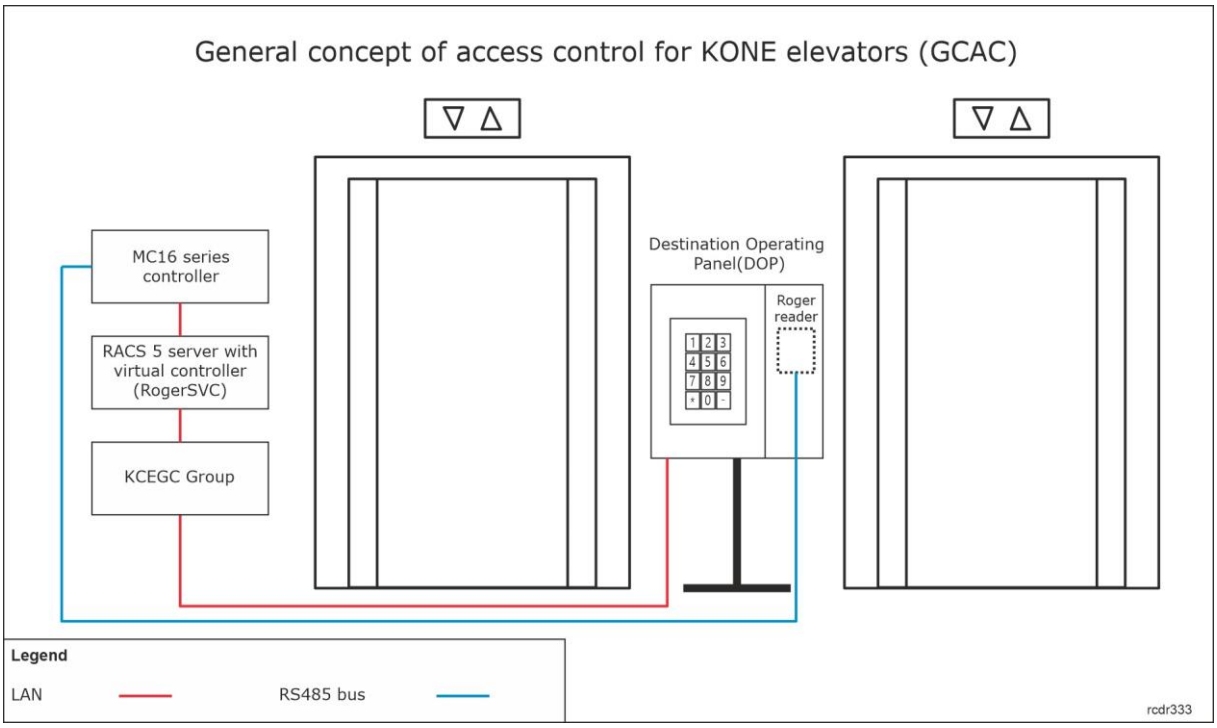
This integration mainly enables centralized management of users and their access rights both on the level of RACS 5 doors and Kone elevators. Particularly the integration enables to:

- Assign individual and group authorisations in RACS 5 system in order to define access rights in elevator system including schedules, calendars and exceptions.
- Define user validity end date.
- Define Authentication Factors (e.g. cards) for user
- Define elevator Call type for user (e.g. handicap, priority, etc.)
- Collect events form elevator system. Alerts, notifications and other automatic reactions of RACS 5 system can be defined for such events.

Integration via GCAC protocol is online type integration so it requires stable and uninterrupted connection between access control system and elevator system. It can be applied in parallel with integration via RCGIF protocol but it is not practical to apply it in the same building with integration via Kone Access because both offer similar functionalities.

All types of readers which are supported by MC16 controller can be installed inside elevator DOPs including MCT series readers which can recognise not only proximity cards abut also mobile factors (NFC/BLE) and QR codes. MC16 controller can also be connected with OSR series readers with OSDP protocol and third party readers with Wiegand protocol.

Note: For this integration it is recommended to apply 1, 2 and 3 door access controllers at DOPs i.e. MC16-PAC-1, MC16-PAC-2 and MC16-PAC-3 controllers.



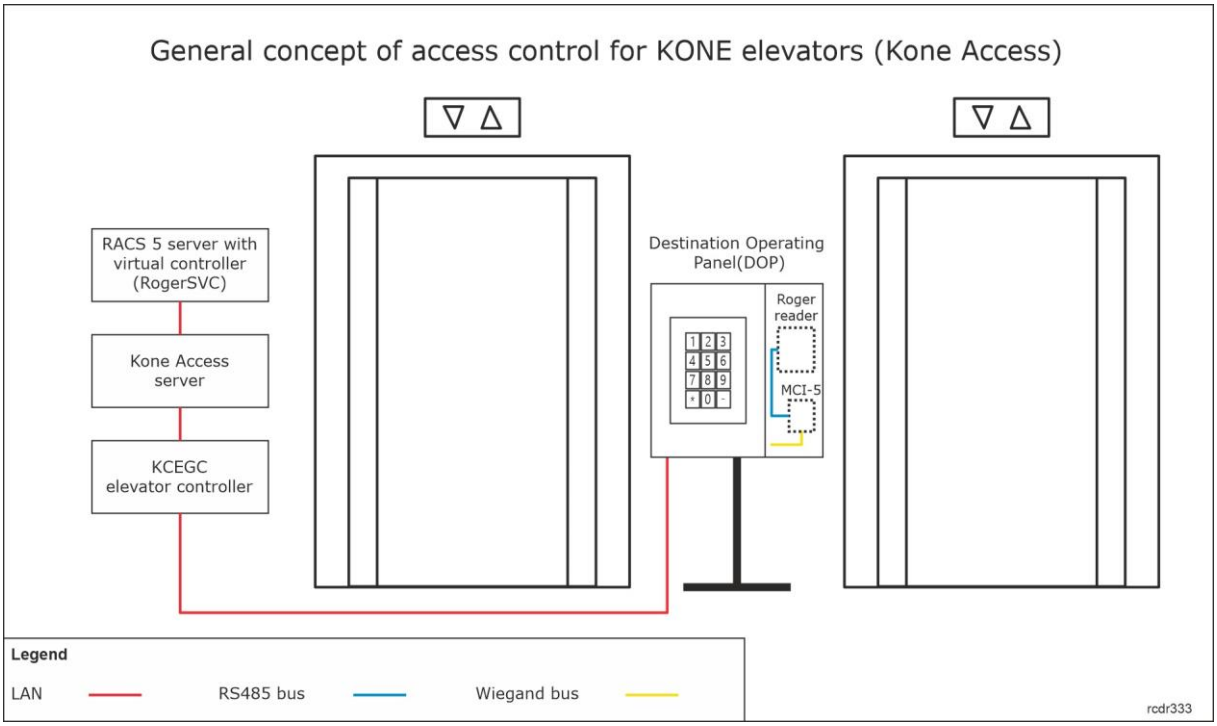
Integration – Kone Access protocol

This integration mainly enables centralized management of users and their access rights both on the level of RACS 5 doors and Kone elevators. Particularly the integration enables to:

- Assign individual and group authorisations which are defined in Kone Access system and they determine user rights in elevator system.
- Define user validity end date.
- Define Authentication Factors (e.g. cards) for user
- Define Home Floor for user
- Define elevator Call type for user (e.g. handicap, priority, etc.)
- Collect events form Kone Access system. Alerts, notifications and other automatic reactions of RACS 5 system can be defined for such events.

Integration via Kone Access protocol is a database type where users are configured in RACS 5 system and then they are uploaded to elevator system on operator request or automatically with specified frequency. Therefore the communication between both system is necessary only when configuration is sent because later the elevator system can make decision on access granting by itself. This integration can be applied in parallel with integration via RCGIF protocol but it is not practical to apply it in the same building with integration via GCAC protocol because both offer similar functionalities.

All types of MCT can be installed inside elevator DOPs including the ones which can recognise not only proximity cards abut also mobile factors (NFC/BLE) and QR codes. Additionally it is necessary to install MCI-5 device inside each DOP as it requires Wiegand interface.



Configuration of integration – RCGIF and GCAC

Configuration of elevator system

The installation and configuration of elevators is made by their supplier. Prior to configuration of the integration it is necessary to determine following parameters of Kone elevator system:

- IP addresses of KCEGC controllers
- Ports for RCGIF and GCAC interfaces (by default 2004 and 2005)
- DOP Terminal IDs for elevator panels
- DOP Terminal IDs for displays installed at turnstiles

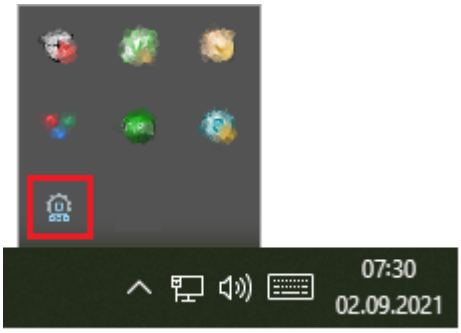
Preliminary configuration of RACS 5

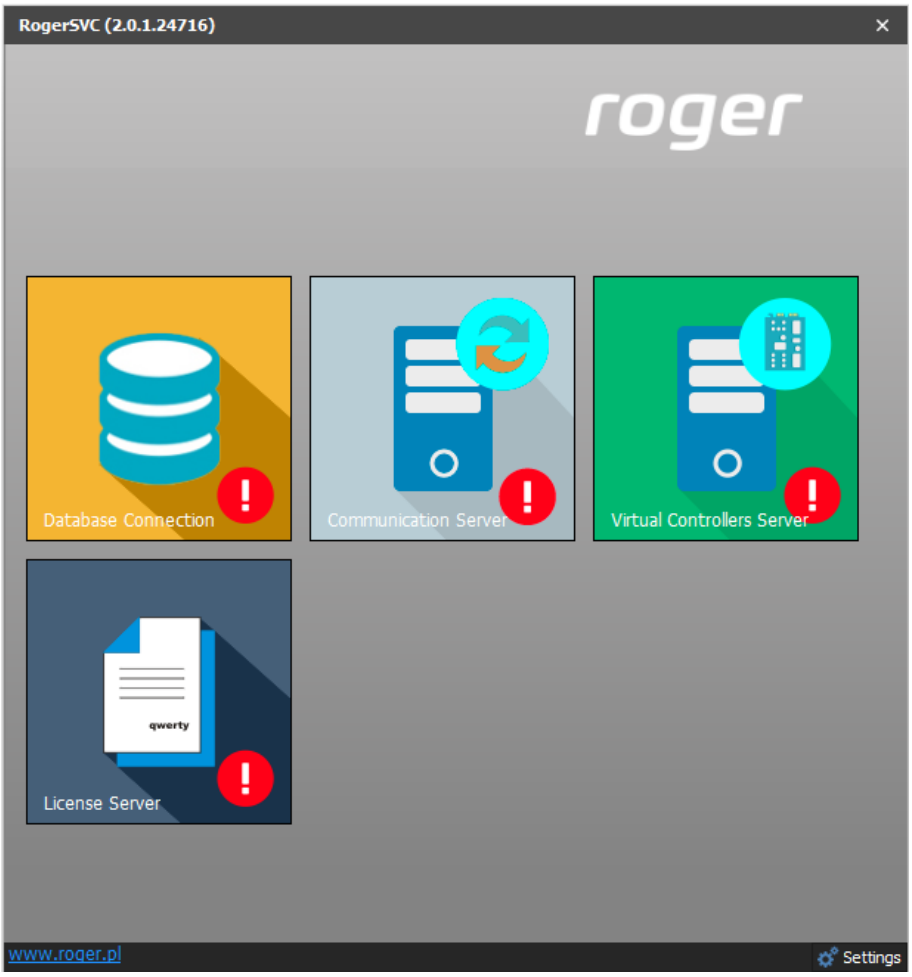
In order to conduct preliminary configuration of RACS 5:

- 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.

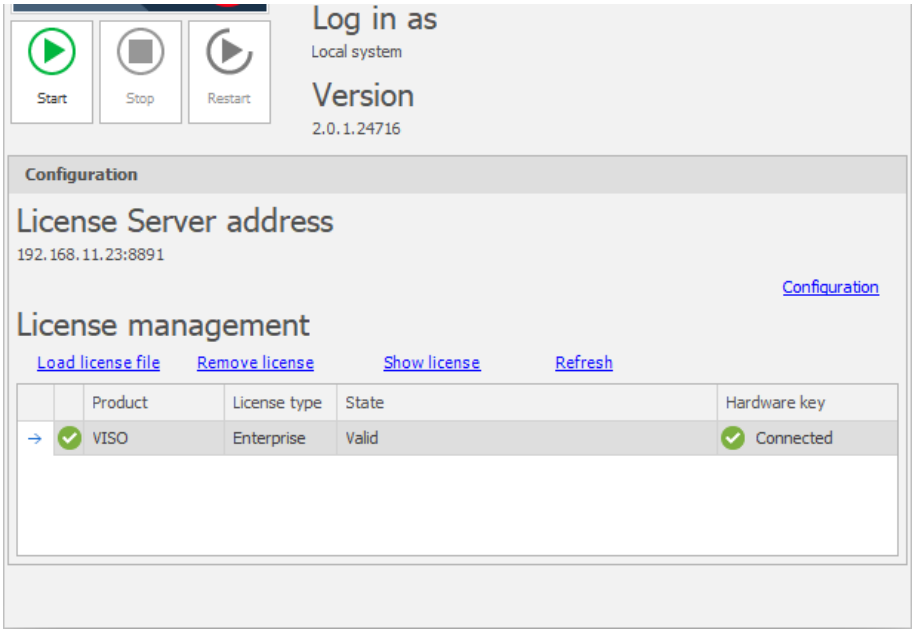
Note: If License Server and Virtual Controllers Server are supposed to be operated on individual computers then during installation of Virtual Controllers Server, the License Server must be deselected. Only in such case it will be possible to indicate external License Server when Virtual Controllers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

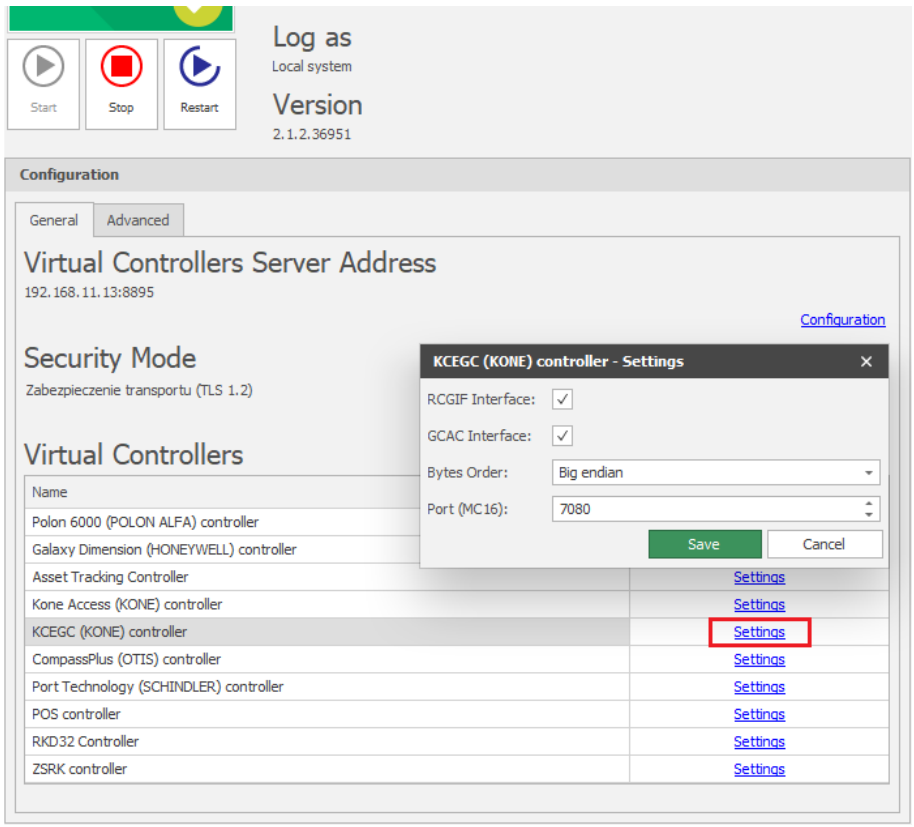




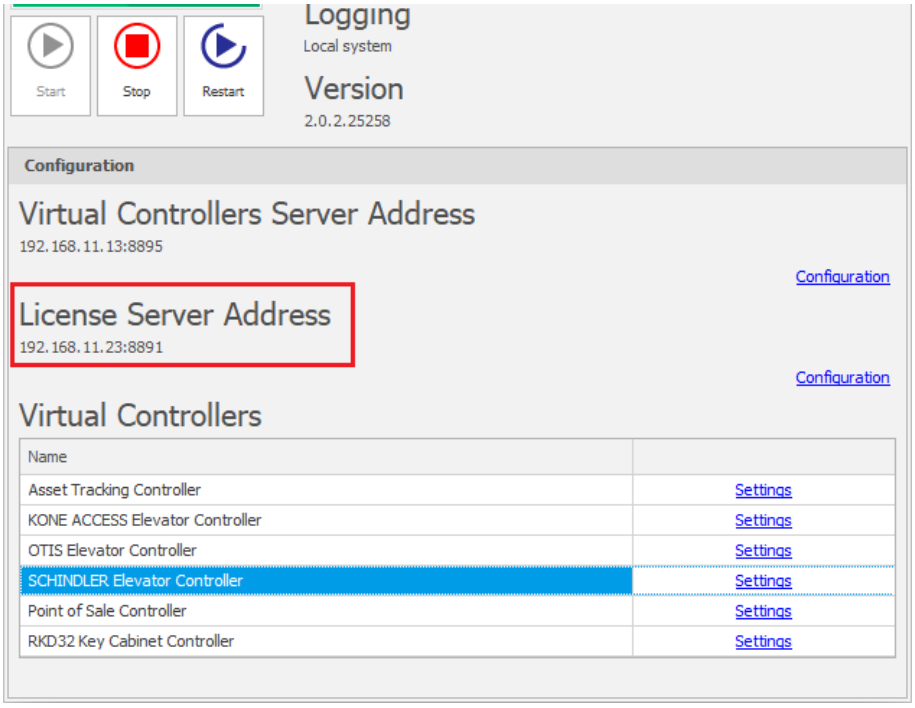
- In the RogerSVC window select *Database Connection* tile and then *Configuration* to indicate previously created RACS 5 database. Return to the main window.
- In the RogerSVC window select *Communication Server*, click *Configuration,* enter IP address of the computer with the server installed e.g. 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).
- Select *Settings* for *KCEGC (KONE) controller* and in the opened window enable RCGIF and/or GCAC interfaces.



- 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 controllers

MC16 controllers with readers installed inside DOPs and at turnstiles/gates require not only typical low level configuration with RogerVDM or VISO v2 but also additional 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 which is communicating with readers used in elevator system.
- 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)

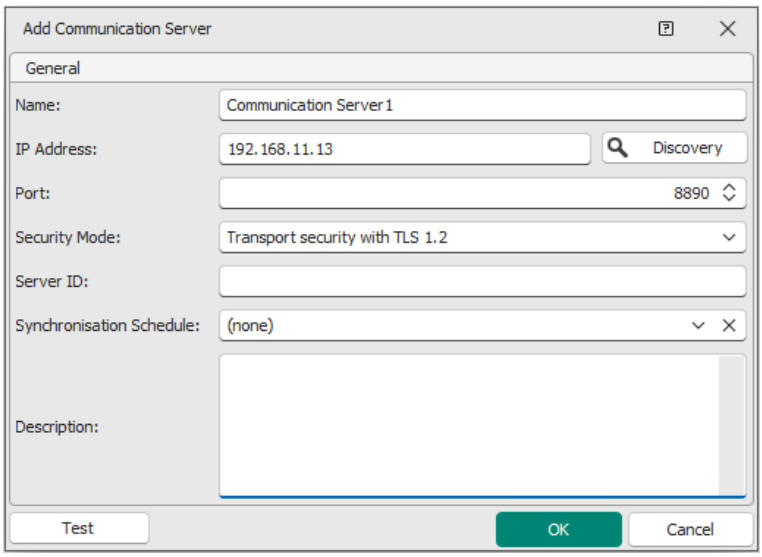
Alternatively, both ETI and EPI parameters can be configured on MC16 memory card in DEBUG.CFG file.

Connection with elevator system

In order to configure virtual controller:

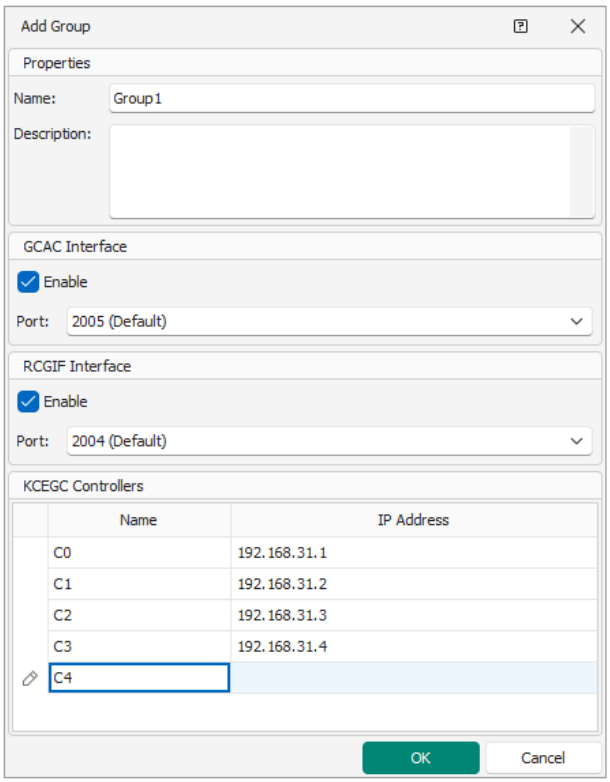
- If Communication Server is not already configured in VISO software then in the navigation tree of VISO software right click *Networks* command and select *Add Communication Server*.

- 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.



- If not already done, then according to AN006 application note add MC16 controllers and discover their hardware resources including connected readers. This step concerns all readers which are connected to DOPs (GCAC) and installed at turnstiles (RCGIF).
- In case of integration via RCGIF protocol define Access Door for each turnstile and assign respective readers. It is recommended to use Add Access Door wizard for that purpose.
- In case of integration via GCAC protocol for each reader installed inside DOP create Access Point. This can be done by expanding particular MC16 access controller in the navigation tree of VISO software, double clicking *Access Points* and selecting *Add*. Then name particular point, close the window with *OK* button, in the bottom select *Access Terminals* tab and use *Add* button to assign particular reader to the Access Point.
- 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 *KCEGC (KONE) 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 *Floors*. In the opened window define floors which will be managed in the building. They will be later used among others to define access rights.
- In case of integration via GCAC protocol within the virtual controller double click *DOPs.* In the opened window define elevator DOPs which are installed in the elevator system and assign them with previously configured Access Points i.e. readers installed inside DOPs. Additionally indicate their Kone Terminal IDs which are configured in the elevator system and indicate floor where they are installed. The parameter *Opening Timeout* defines how long floor numbers are displayed for a user after identification.
- In case of integration via RCGIF within the virtual controller double click *Turnstile Displays.* In the opened window define displays installed at turnstiles and assign them with previously configured Access Points i.e. readers installed at turnstiles. Additionally indicate their Kone Terminal IDs which are configured in the elevator system as well as indicate floor and side where they are installed.
- After configuration of Floors, DOPs and Turnstile Displays double click *Groups* within the virtual controller. In the opened window select *Add* and in the next window enable RCGIF and/or GCAC

interfaces indicating IP addresses of KCEGC devices within particular elevator group. Close the window with *OK* button.



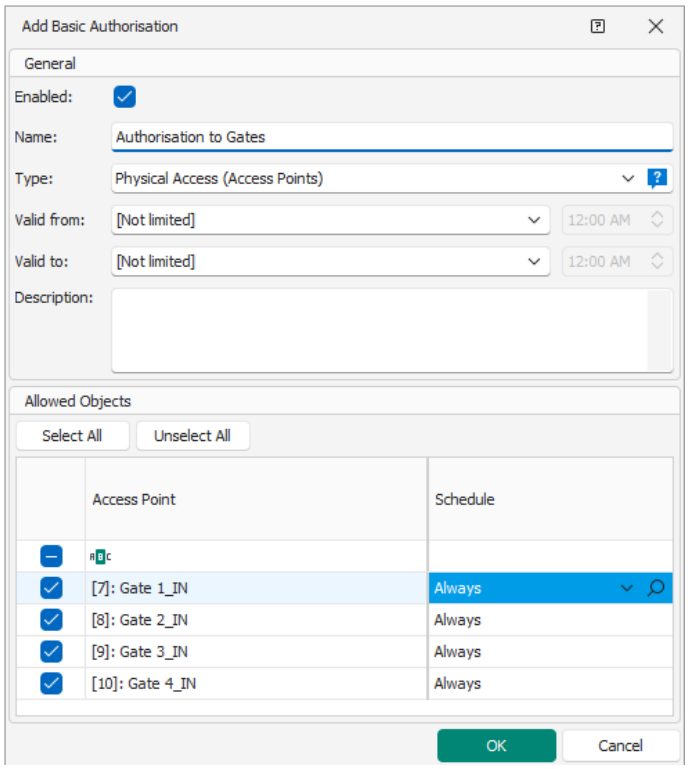
- In the bottom select *Floors*, *DOPs* and *Turnstile Displays* tabs and assign respective elements for the created elevator group in accordance with the actual arrangement of elevator system.
- Define more Groups with KCEGC elevator controllers if they exist in the elevator system.

Authorisations (RCGIF)

Authorisations are access rights which are assigned to users of access control system. If Access Doors at turnstiles/gates were defined with Add Access Door wizard as mentioned in the previous section then Basic Authorisations for Access Points at these turnstiles were created automatically. User who is supposed to call elevator for home floor during identification at a turnstile must be assigned with Authorisation to the Access Point (reader) installed at the turnstile.

If Access Doors and Access Points were defined manually and not with the wizard then in the navigation tree of VISO software define Basic Authorisations with *Physical Access (Access Points)* type indicating adequate Access Points or define Advanced Authorisations with function *[151]* indicating Access Points within Positive Rules. It is possible to define single Authorisation for multiple gates or individual Authorisations for each gate.

In case of integration via RCGIF protocol there is no need to define Authorisations for particular floors because default home floor is used when elevator is called.

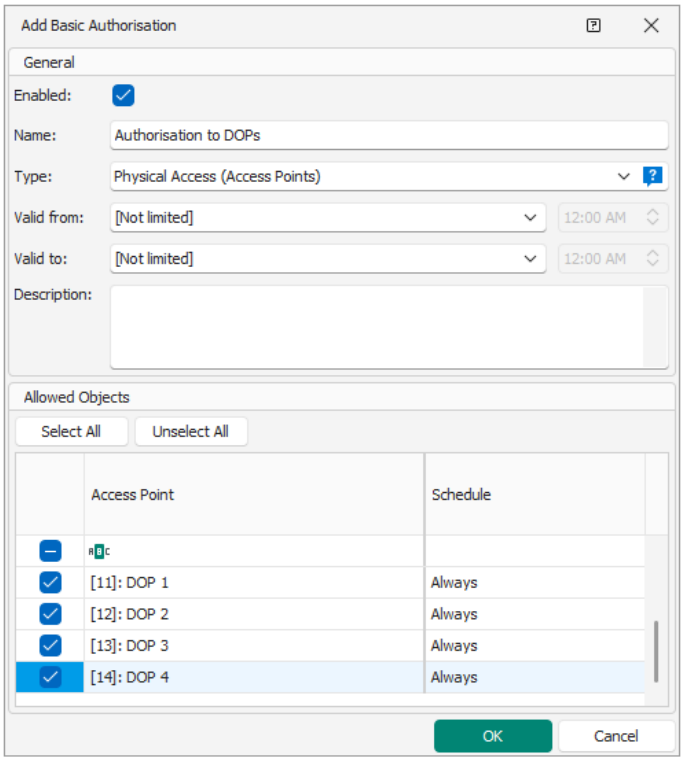


Authorisations (GCAC)

Authorisations are access rights which are assigned to users of access control system. In case of integration via GCAC protocol it is necessary to define Authorisations to Access Points (readers) and Authorisations to Floors which could be selected by user at elevator DOP.

Authorisations to Access Points

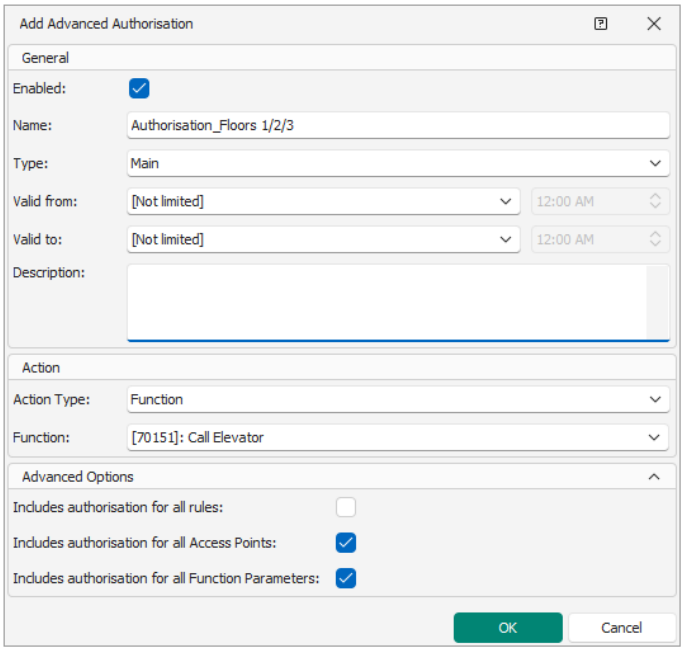
Authorisation to Access Points can be defined using Basic Authorisations with *Physical Access (Access Points)* type or Advanced Authorisations with function *[151]*. It is possible to define single Authorisation for multiple DOPs or individual Authorisations for each DOP. Authorisation are configured in the navigation tree of VISO software.



Authorisation to Floors

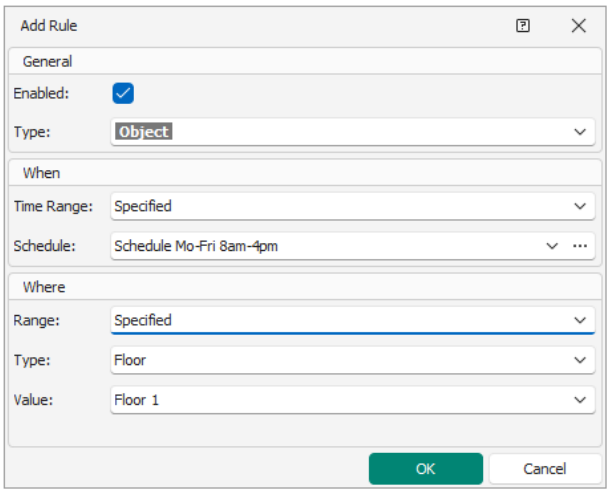
Authorisation to Floor is defined as Advanced Authorisation with function *[70151]: Call Elevator*. In order to define such Authorisation:

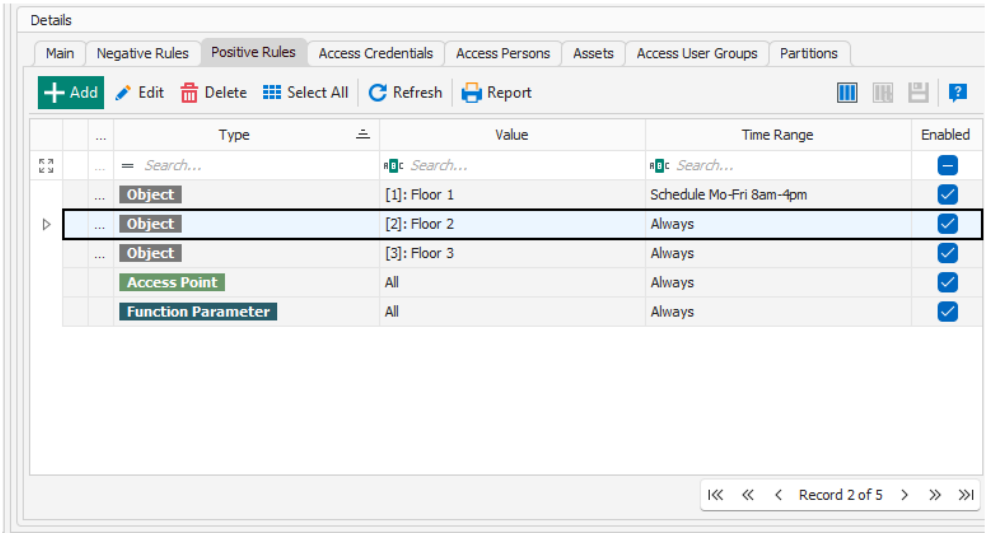
- In the navigation tree of VIOS software expand *Authorisations* and then double click *Advanced Authorisations*.
- In the opened window select *Add,* in the next window name the Authorisation and select the function *[70151].* If the Authorisation is supposed to cover all floors for both sides (front and rear) and be valid from all DOPs then enable the option *Include authorisation for all rules*. In such case there is no need to define Positive Rules as explained in the next steps. Close the window with *OK* button.



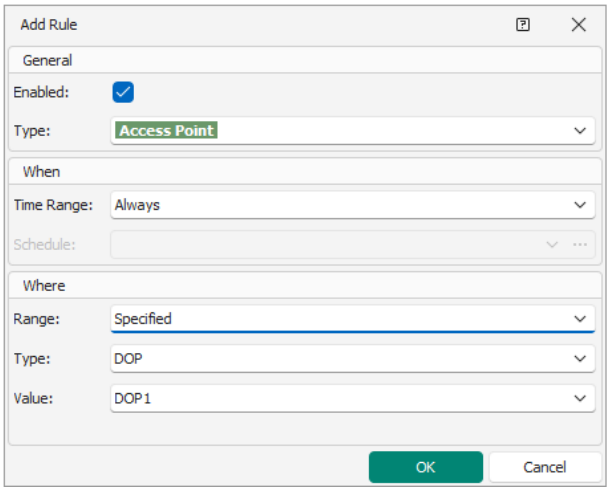
- In the bottom select *Positive Rules* tab and then click *Add*.
- In the opened window define as below in order to define rule for floor 1. Time range and Schedule are optional and Schedule must be earlier defined in the navigation tree of VISO software. It is possible to define up to 64 rules within single Authorisation. Therefore it is possible to define individual Authorisation for each floor or define group Authorisation for multiple floors by defining multiple rules for such Authorisation. Close the window with *OK* button.

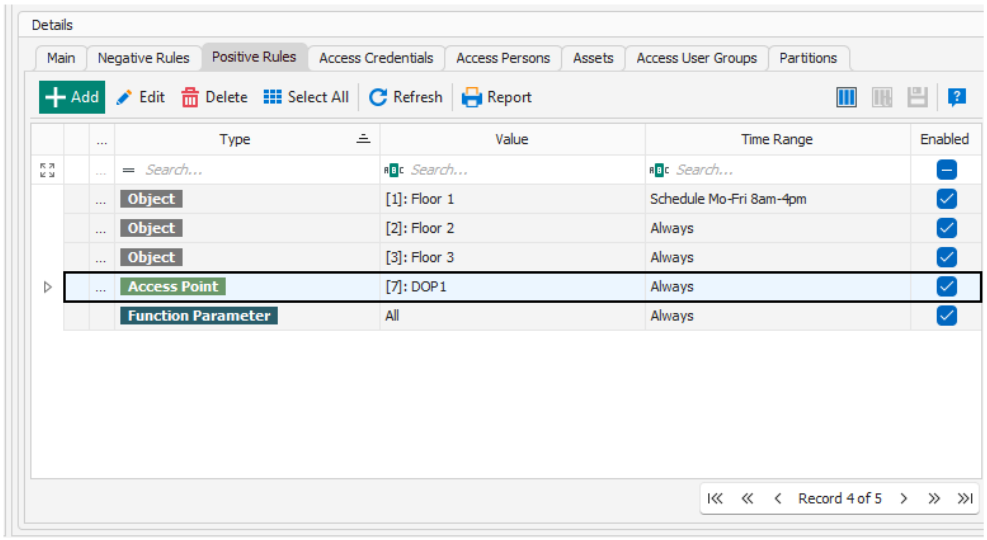
Note: In further steps all Authorisations can be grouped by expanding *Authorisations* command in the navigation tree and then selecting *Authorisation Groups*. When user is enrolled in the system then both Authorisations and Authorisations Groups e.g. for doors and floors can be assigned.



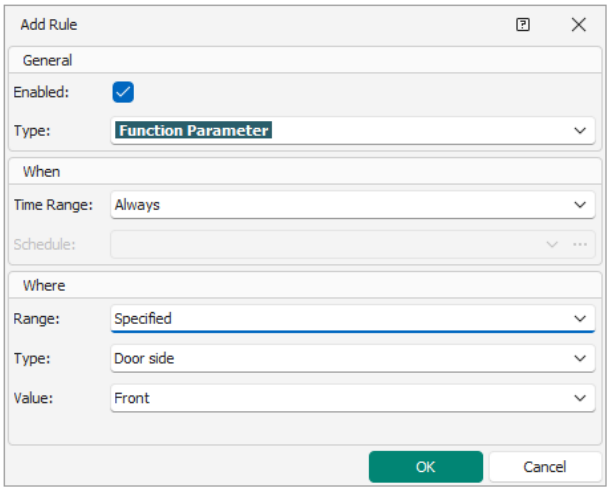


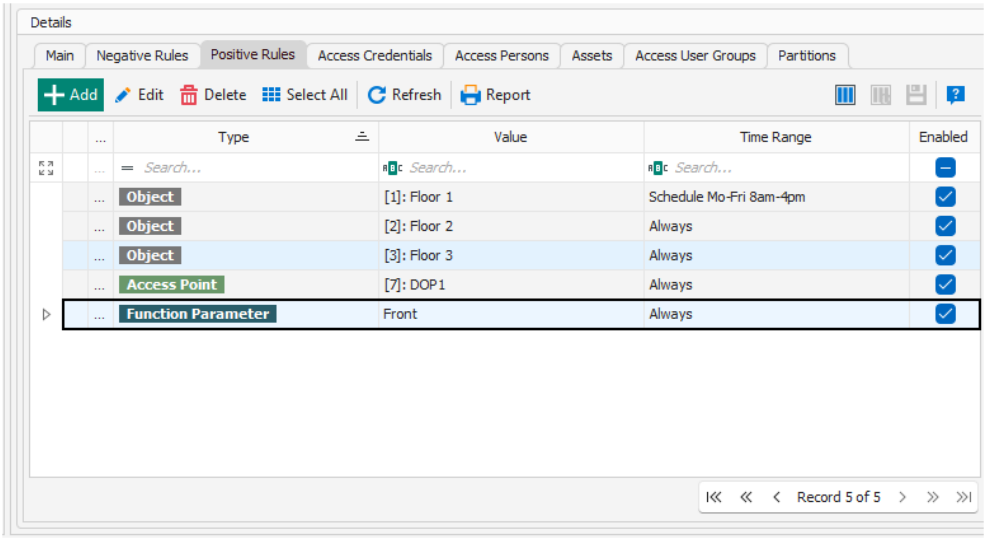
- When Authorisation is created and the option *Includes authorisations for all Access Points* is deselected then Access Point type rule can be created and then the Authorisation can be limited to specific destination operating panels (DOP). Similarly as in case of Object type rule the Access Point type rule can be limited in time and there can be defined multiple rules of this type within the Authorisation.





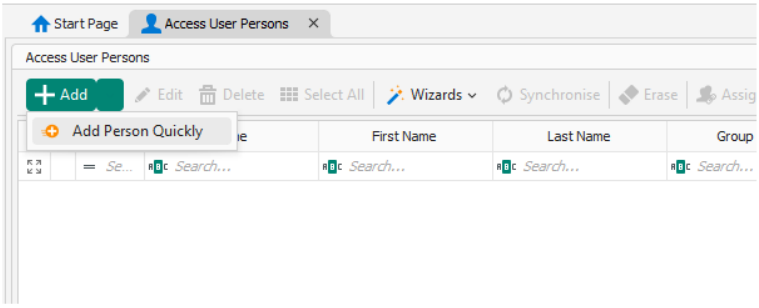
- When Authorisation is created and the option *Includes authorisations for all Function Parameters* is deselected then Function Parameter type rule can be created and then the Authorisation can be limited to specific side of floor. Similarly as in case of Object type rule the Function Parameter type rule can be limited in time and there can be defined multiple rules of this type within the Authorisation.





Users

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 as explained in AN006 Application note. There is also Add User Quickly wizard which can be started by selection of *Configuration->Access User Persons->Add* in the top menu of VISO software.

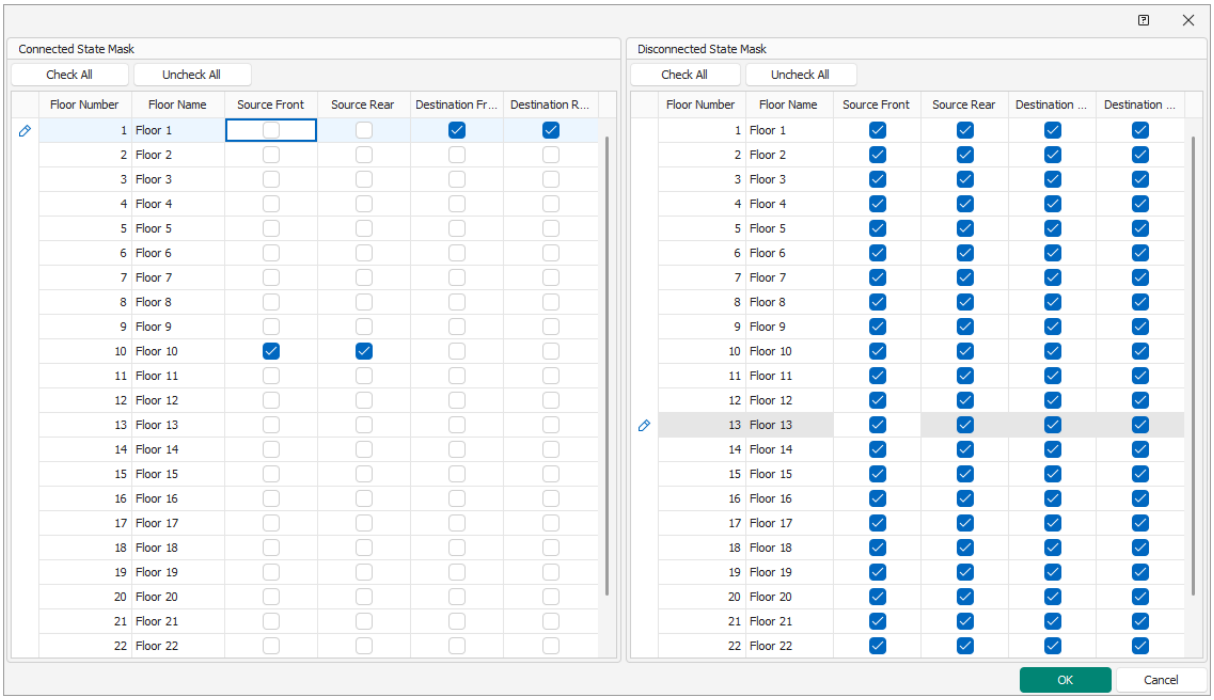


Masks

Masks are used to determine which floors can be accessed by everyone regardless of their Authorisations. User does not have to identify at a reader when selecting floors which are enabled in a mask. There are Global masks which are defined on the level of the whole elevator system and there are masks on the level of individual DOPs. Additionally there are Connected State Masks which are applied when there is stable connection between RACS 5 and elevator system and there are Disconnected State Masks which are applied in case of emergency resulting from failed communication. Masks are optional and they concern only integration via GCAC protocol.

Global masks

Global mask for particular Group of KCEGC controllers are defined in *Masks* tab when such group is defined in VISO. Floors must be created and assigned to particular Group before they can be selected in a mask. In the example below when there is communication failure and Disconnected State Mask is applied then it is possible to travel from all floors to all floors on all sides without user identification. In case of proper communication when Connected State Mask is applied then everyone can travel to floor 1 (on both sides) from all floors and from floor 10 (on both sides) it is possible to travel to any floor.

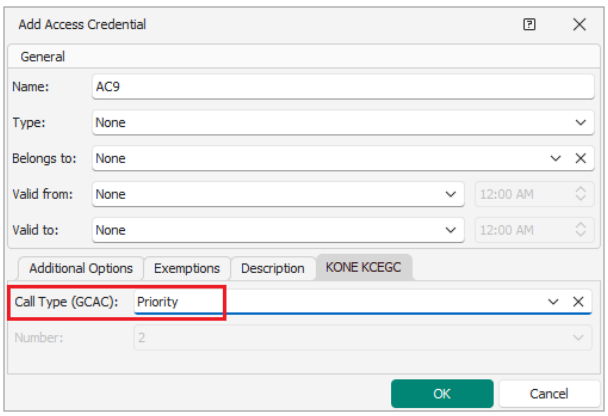


DOP masks

DOP masks are used to configure exceptions for Global mask. They are defined when DOP is configured and the same rules apply as in case of Global mask with the exception then only destination floors are selected.

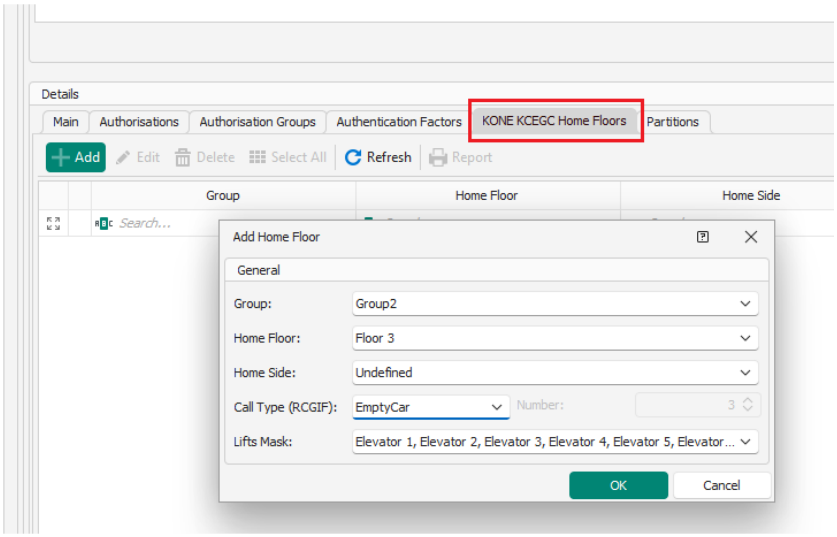
Call Types (GCAC)

Call Type is used to specify if particular user should be treated differently, usually as privileged one by elevator system when identified at DOP. Call Types are optional and they are defined in the properties of Access Credential belonging to a Person. They can be defined manually or within Add Person online wizard.



Home Floors and Call Types (RCGIF)

Home Floors are the most essential element of integration via RCGIF protocol. Additionally it is possible to define Call Type which specifies if particular user should be treated differently, usually as privileged one by elevator system when identified at a turnstile. Both parameters are defined in *KONE KCEGC Home Floors* tab within Access Credential belonging to a Person. The parameter *Lifts Mask* can be used to exclude some elevators from calling.



Configuration of integration - Kone Access

Configuration of elevator system

The installation and configuration of elevators is made by their supplier. Prior to configuration of the integration it is necessary to determine following communication parameters of Kone Access system:

- Server IP Address.
- API key.
- Login and password.

Note: Default port for communication with Kone Access server is 443.

Note: It is recommended to configure card number length to 16 HEX bytes for Medium UID type Media Definition in the elevator system.

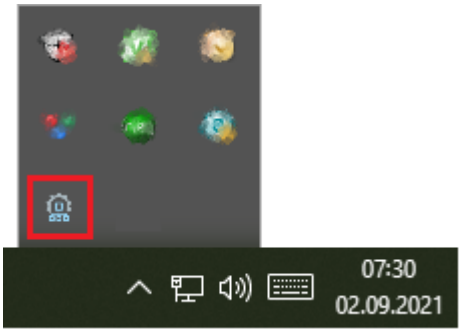
Preliminary configuration of RACS 5

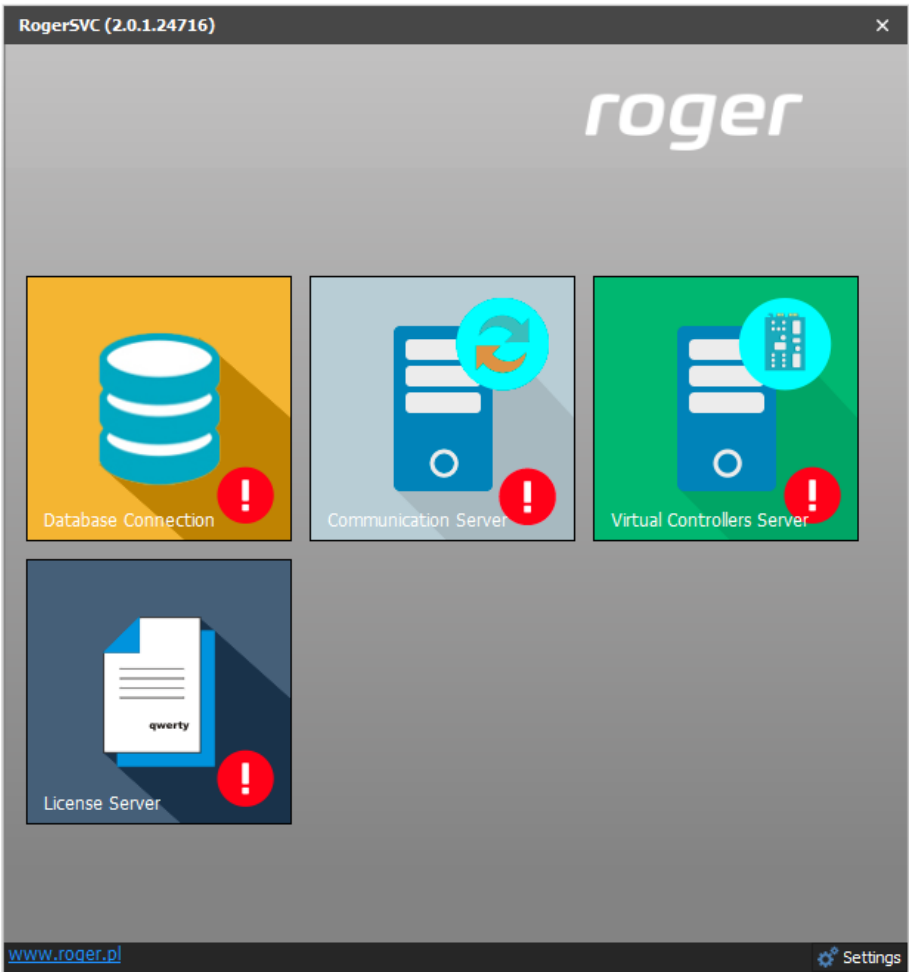
In order to conduct preliminary configuration of RACS 5:

- 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.

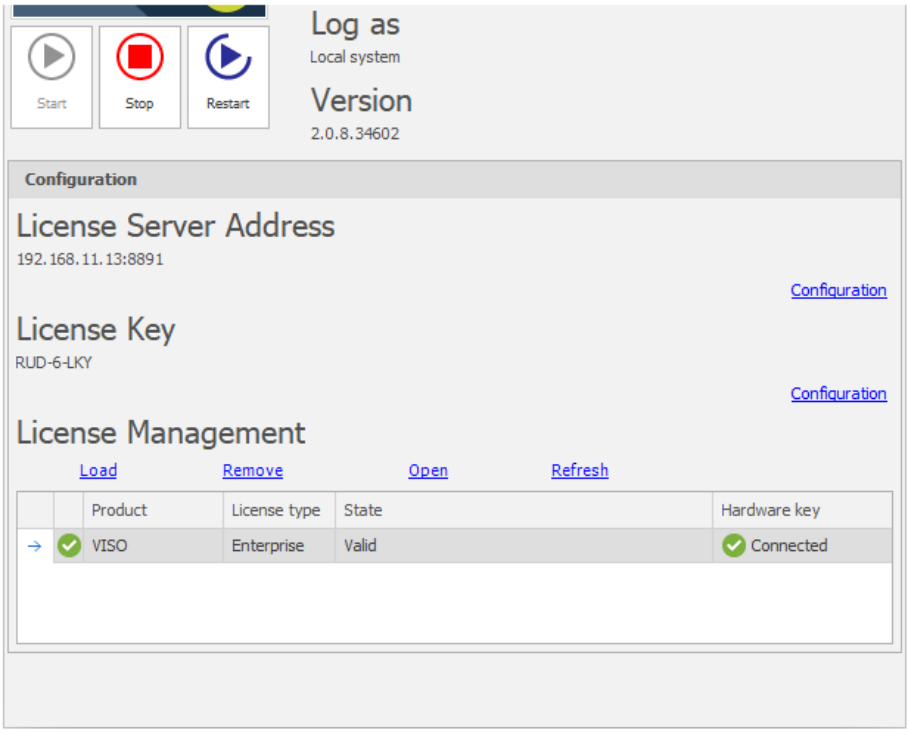
Note: If License Server and Virtual Controllers Server are supposed to be operated on individual computers then during installation of Virtual Controllers Server, the License Server must be deselected. Only in such case it will be possible to indicate external License Server when Virtual Controllers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

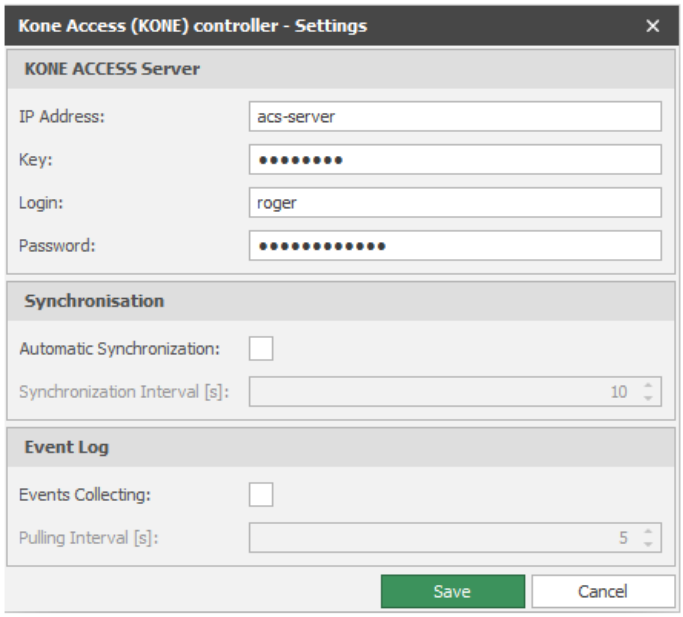




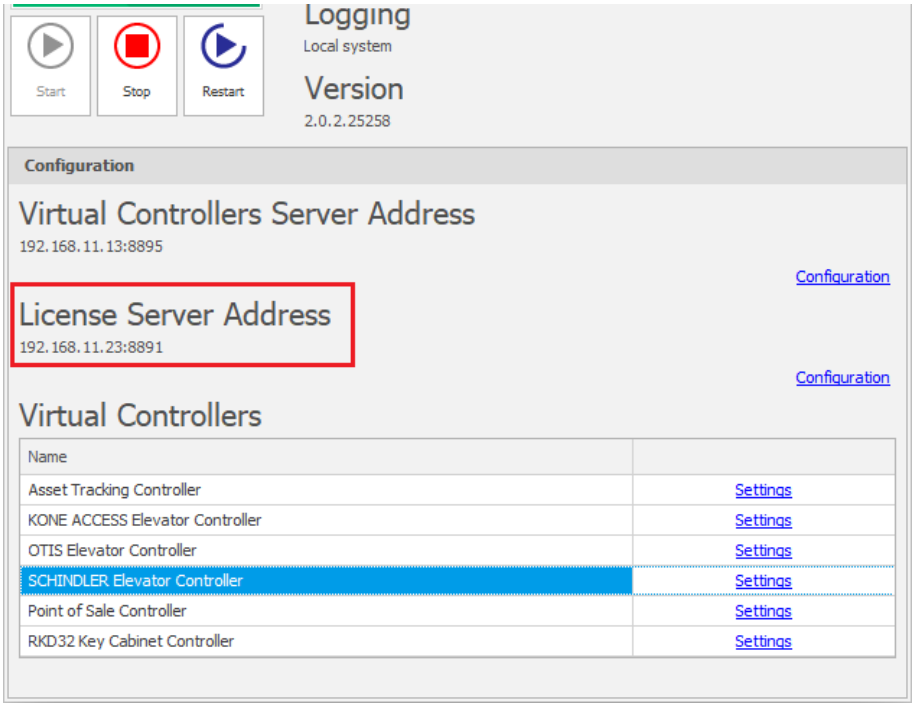
- In the RogerSVC window select *Database Connection* tile and then *Configuration* to indicate previously created RACS 5 database. Return to the main window.
- In the RogerSVC window select *Communication Server*, click *Configuration,* enter IP address of the computer with the server installed e.g. 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).
- Select *Settings* for *Kone Access (KONE) controller* and in the opened window enter communication parameters acquired from elevator supplier. Optionally enable automatic synchronization so settings could be uploaded to elevator system automatically by RACS 5 system and not only on VISO operator request. Optionally enable the option *Events Collecting* if events from elevator system are supposed to be downloaded and presented in VISO log.



- 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.

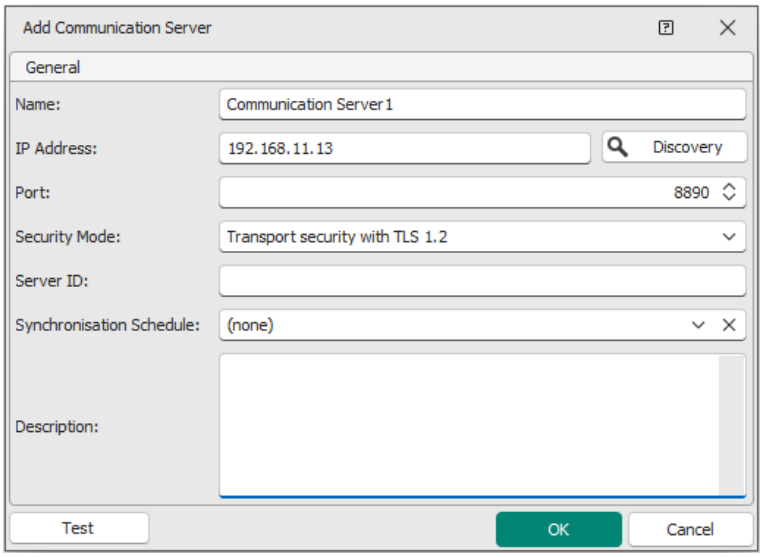
Low level configuration

The purpose of low level configuration of such devices as MCT terminals and MCI-5 converters is to define basic operational parameters. Make low level configuration according to manuals of these devices prior to their connection to Wiegand interface of elevator panel.

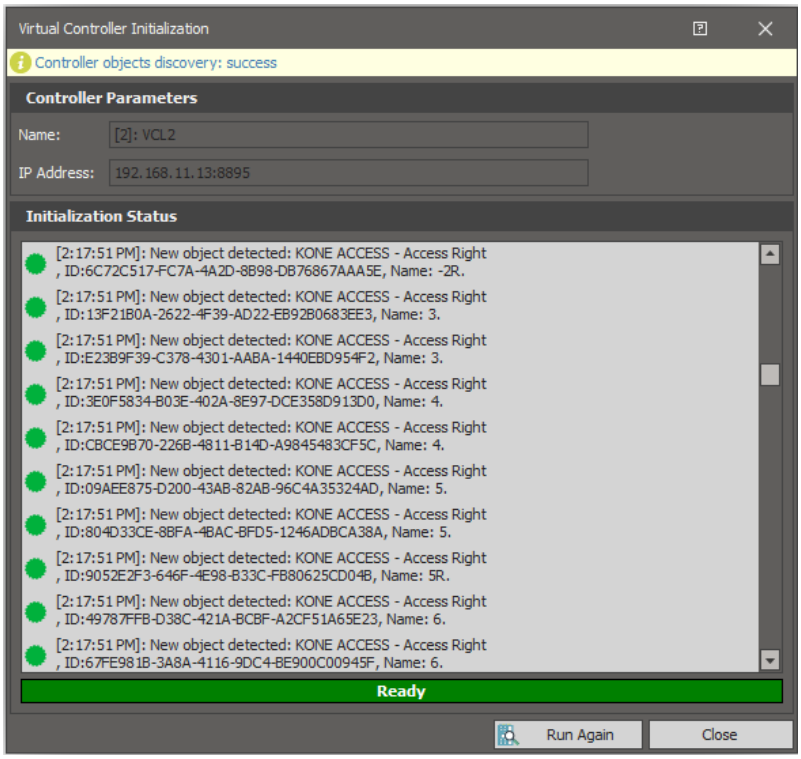
Connection with elevator system

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.



- 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 *Kone Access (KONE) 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.
- Right click created virtual controller and select *Run Discovery*.
- In the opened window select *Run* to start downloading of such objects from Kone Access server as Access Rights, Person Categories, Home Floors, Call Types, Time Zones and Factor Types. They will be further used in configuration of users.



Note: It is possible to define maximal number of simultaneous connections in Kone Access system. The integration with RACS 5 can be operated within single connection both for settings uploading and events downloading.

All objects downloaded from Kone Access server are assigned with original names but it is possible to assign them with own names and descriptions in VISO software. For example in order to change Home Floor name:

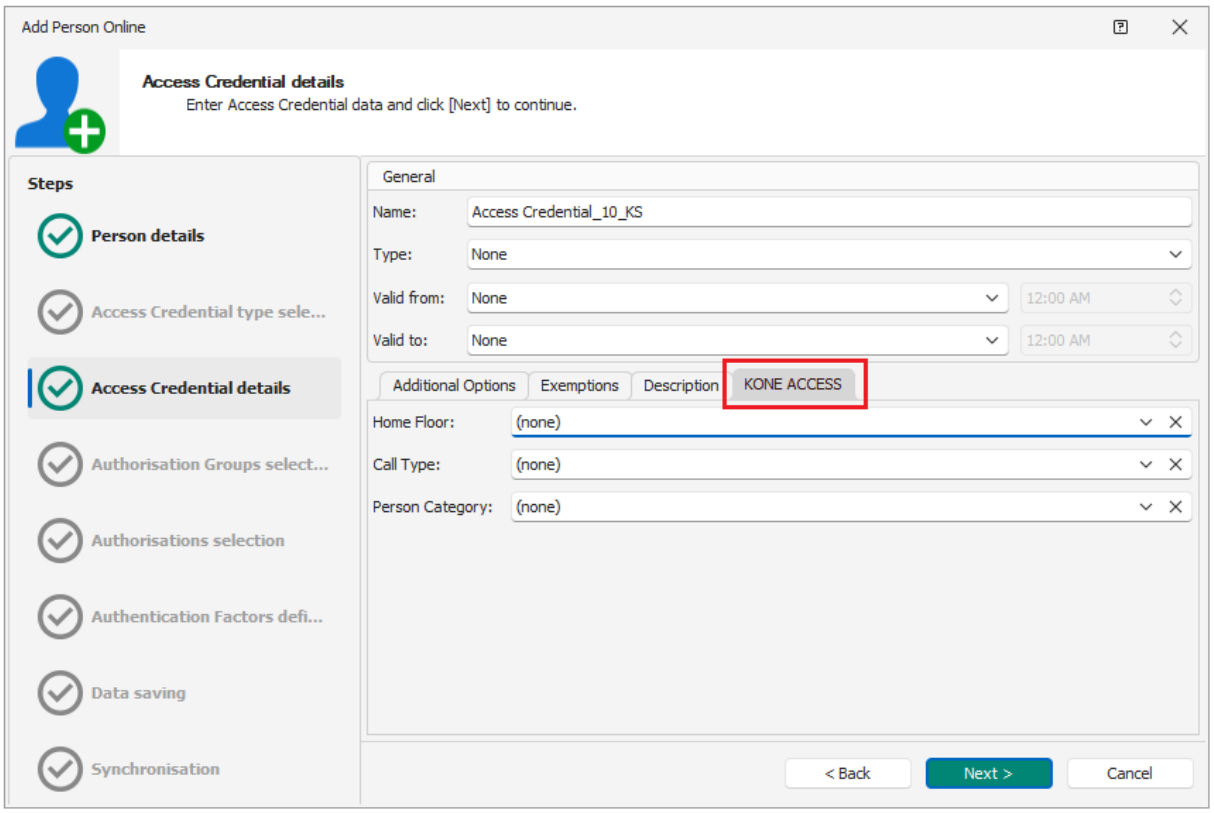
- Double click *Home Floors* in the navigation tree of VISO software.
- In the opened window select particular floor and then *Edit*.
- In the opened window enter own name and description for the object.

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 wizard is explained in AN006 Application note.

In regard of users, wizards enable to:

- Define validity date for user's Access Credential with *Valid to* parameter. Kone Access system does not support start date i.e. *Valid from* parameter.
- Define home floor for user which is default elevator floor.
- Define elevator call type for user e.g. handicap, priority, etc.
- Define person category for user
- Define Authentication Factors for user (e.g. cards, NFC/BLE mobile factors).



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

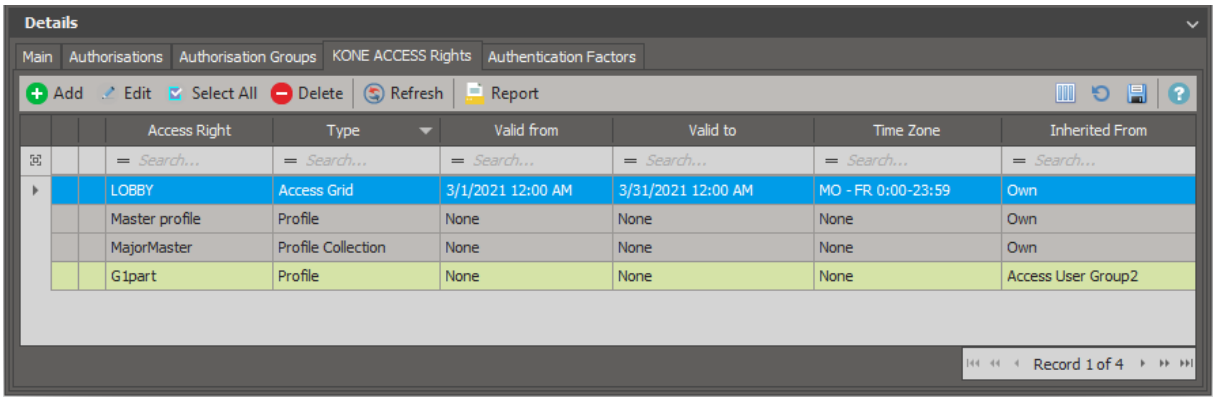
Note: It is possible to configure default values for all users e.g. default Person Category by selection of *Tools* in the top menu of VISO software, then *Default Values* and *Edit* on the level of Access Credential.

Access Rights Assignment

Access Rights in regard of elevator system are defined in Kone Access software by means of such objects as Profiles, Profile Collections and Access Grids which are later imported to VISO software. Then these rights can be assigned to user's Access Credential. Kone recommends to use Profiles and Profile Collections instead of Access Grids.

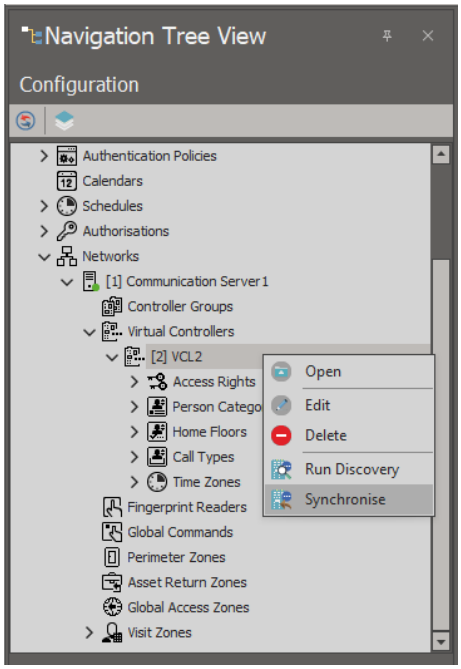
In order to assign Kone Access Rights:

- 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 *KONE ACCESS Rights* tab and then *Add*. In the opened window assign Access Grids and/or Profiles to define user rights in elevator system.

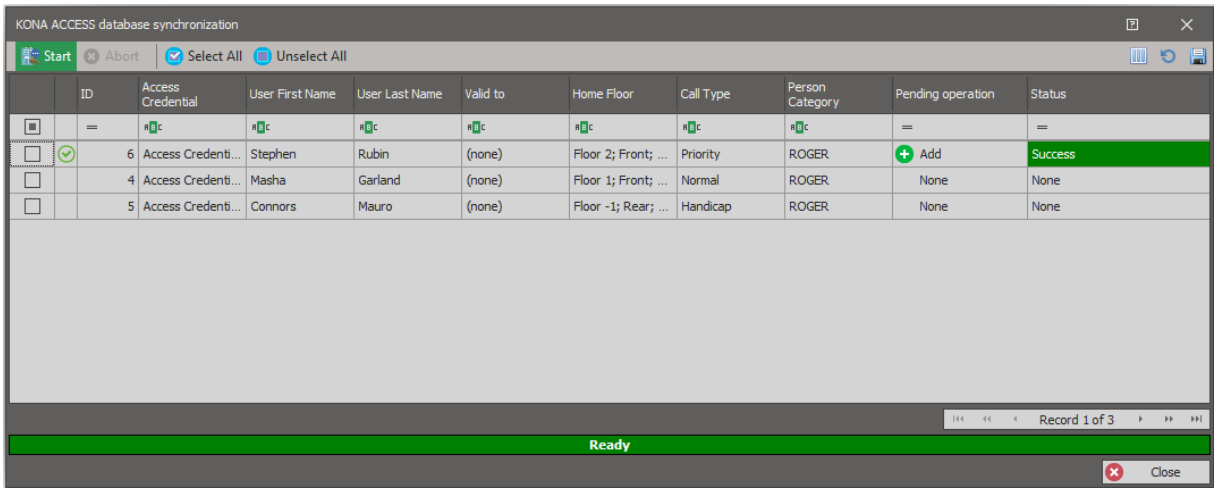


Note: In case of assignment of Access Grid it is necessary to select Time Zone from proper domain.

- If during earlier configuration of virtual controller in RogerSVC software the automatic synchronisation was not enabled then in the navigation tree of VISO software right click the virtual controller and select *Synchronise*.



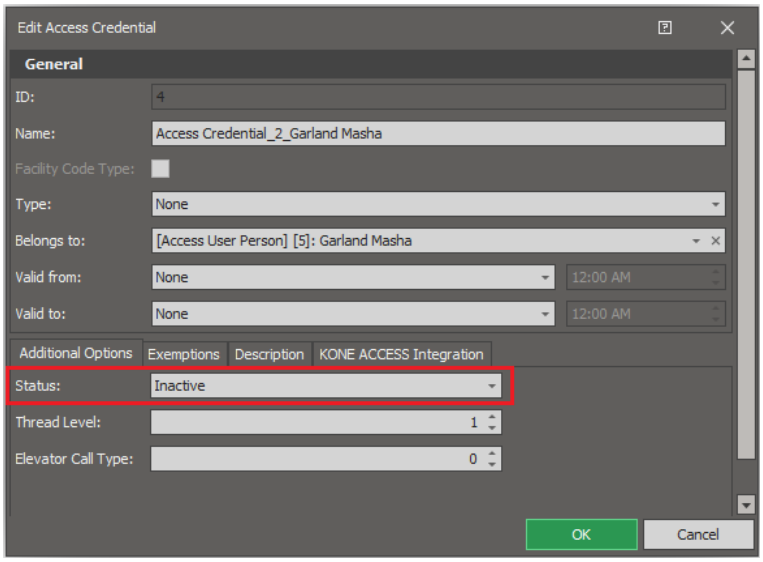
- In the opened window select *Start* to upload users to the elevator system.



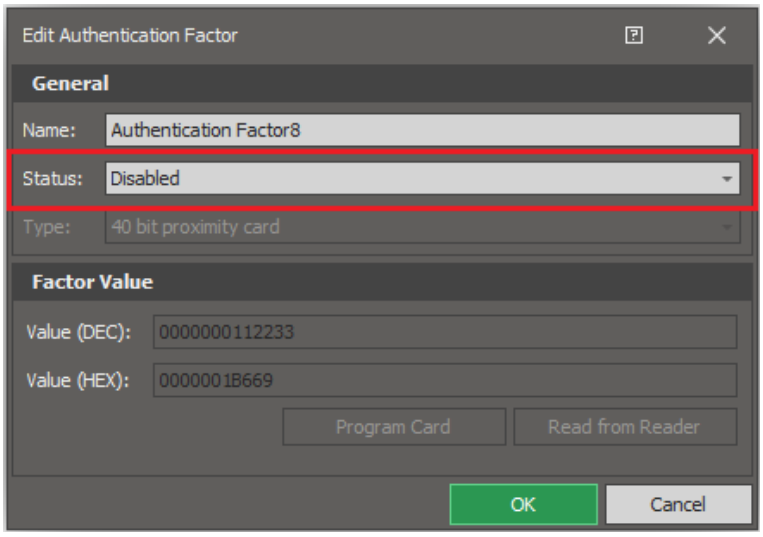
Kone Access Rights can be also assigned on the level Access User Groups and then Persons can be assigned to groups so they can acquire those rights in elevator system by being part of a group. Profiles and Profile Collections can be assigned on the level of Access User Groups while Access grids cannot. Person can be assigned to particular group also on the level of Add Person Online wizard.

Users can be blocked in RACS 5 and Kone Access systems. In order to block a user:

- In the top menu of VISO software select *Configuration* and then *Access Credentials*.
- In the opened window select Access Credential belonging to particular user and then select *Edit*.
- In the opened window select *Additional Options* tab, set *Inactive* and close the window with *OK* button.
- Synchronise settings with Kone Access system.



When user is blocked in Kone Access then all Authentication Factors (cards) belonging to such users are also blocked but it is possible to block selected Authentication Factors (cards) without blocking the whole user. In such case edit particular Authentication Factor belonging to user's Access Credential and change its status as below.



Factor Mappings

Factor mappings allows to make association between Authentication Factor Types in VISO software (e.g card types) and Factor Types (Media Definitions) in Kone Access elevator system. In order to define a mapping:

- In the navigation tree of VISO software expand *Kone Access Controller*.
- Double click *Factor Mappings*.
- In the opened window select *Add*.
- In the next window define mapping selecting RACS 5 Factor Type e.g. *40 bit proximity card* and Kone Factor Type (Media Definition) which must be defined in Kone system and downloaded during the initialization.

Factor mapping is optional and useful when multiple types of cards and/or mobile factors are used in the whole system. It allows to translate factor types between access control system and elevator system. It is possible to use predefined Authentication Factor Types and define own types be selection of *Authentication Factor Types* in the navigation tree of VISO software.

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

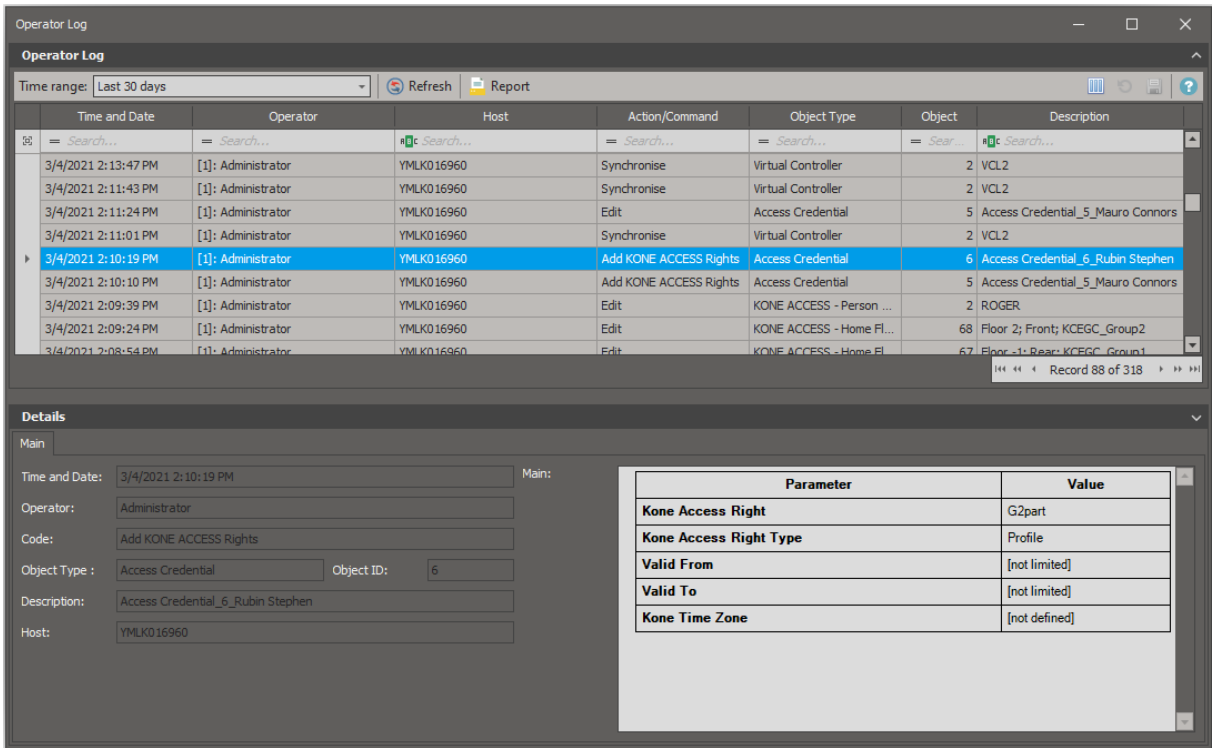
The connection between virtual controller and Kone Access server is established when it is needed for the purpose of users uploading or events downloading. Therefore the connection is not monitored constantly. In case of communication problem events and warnings are generated.

Users

RACS 5 system registers events related to access granting. RACS 5 system can collect events from Kone Access if it is enabled on the level of virtual controller in RogerSVC.

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.



Alerts and notifications

Automatic reaction of the system for event can be defined by selection of *Event log* in the top menu of VISO software and them *Event types* icon and *Actions* tab in the bottom. Typical actions are alert displaying for operator acknowledgement, mobile text (SMS) sending and email sending. In case of mobile texts and emails it is necessary to configure SMTP Account(s) and SMS Gateway(s) by selection of *Tools* in the top menu of VISO software. More information on alerts and notifications is given in AN041 application note.

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