Roger Access Control System 5

Application note no. 042

Document version: Rev. C

RKD32 Key Cabinet

Note: This document refers to RACS 5 v2.0.4 or higher

Introduction

RKD32 Key Cabinet can be remotely configured and managed by means of VISO software from RACS 5 system. In such scenario the communication with cabinet is provided in Ethernet or W-fi network by means of virtual controller from RogerSVC software package. The virtual controller is Windows service which is operated on RACS 5 server and it can support multiple cabinets at the same time. Remote control of RKD32 Key Cabinets requires licensed VISO management software.

Key Cabinets in network mode can be centrally managed as another elements of access control system while users can have the same Authentication Factors (card, PINs) both for RACS 5 and RKD32. In case of RKD32, VISO operator can:

- Enrol users and define their Authorisations and Authentication Factors.
- Define keys for RKD32 cabinet.
- Monitor the cabinet in regard of alarms and failures including automatic alerts and notifications (email, mobile text).
- Monitor and control key statuses (Locked, Available, Dispensed.)
- Track keys including information who currently possesses particular key.
- Configure access denying for the user who exits the building without returning key to the cabinet.
- Generate reports based on events registered by RKD32.

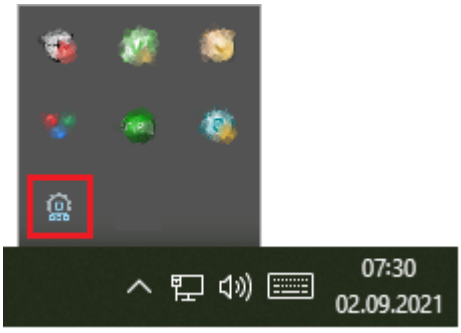
Preliminary configuration of RACS 5

In order to conduct preliminary configuration of RACS 5:

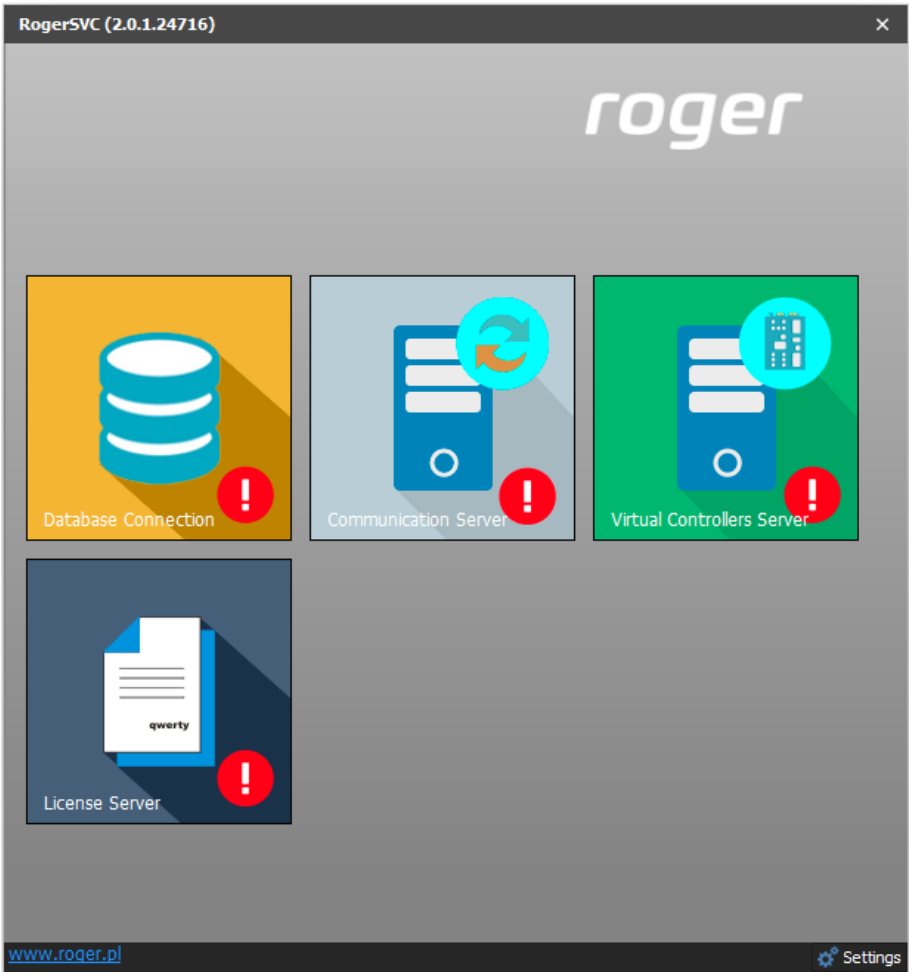
- Install VISO software and create centralized database according to AN017 application note.
- Install RogerSVC software and select not only Communication Server but also License Server and Virtual Controllers Server. If servers are supposed to be operated on individual computers then install RogerSVC 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.

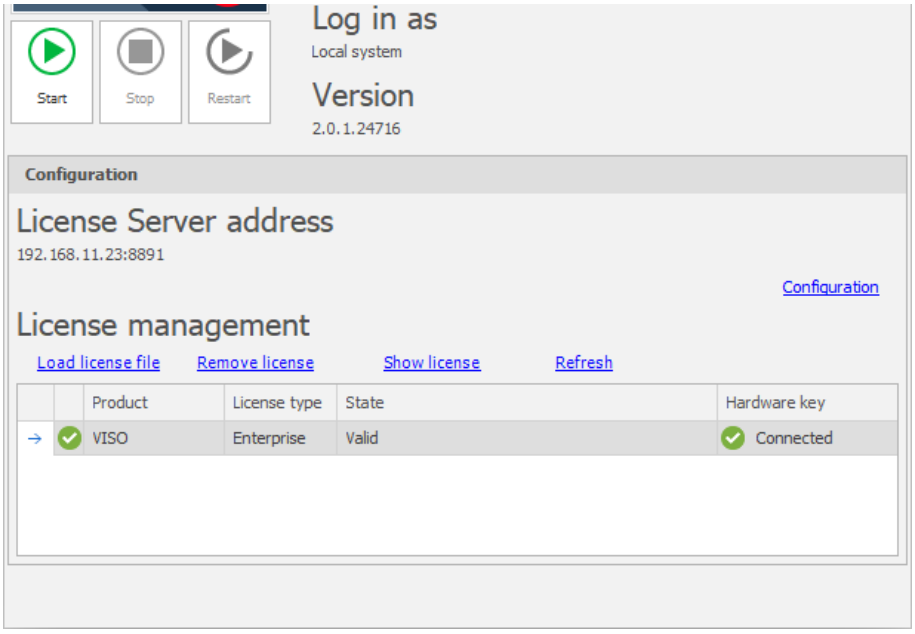
- Start RogerSVC program selecting *Start->ROGER->RogerSVC* in Windows menu.
- Click RogerSVC icon  in Windows tray ( in older versions).



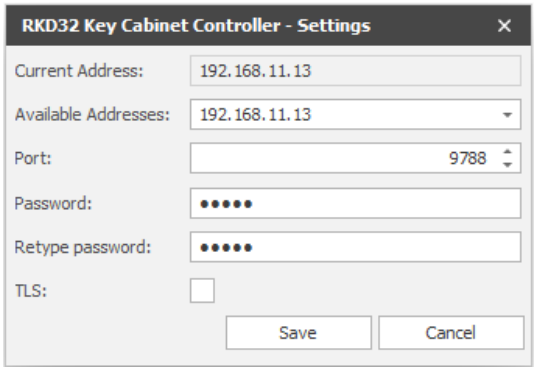
- In the RogerSVC window select *Database Connection* tile and then *Configuration* to indicate previously created RACS 5 database. Return to the main window.



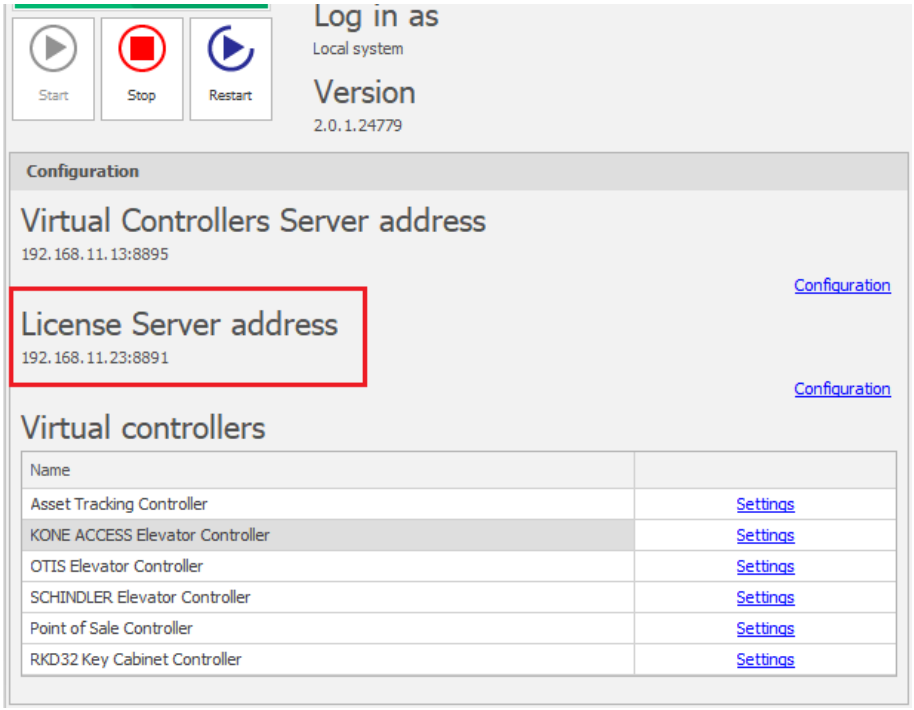
- In the RogerSVC window select *Communication Server*, click *Configuration,* enter IP address of the computer with the server installed e.g. 192.168.11.13 and define port (8890 by default).
- Select *Start* and return to the main window. The server will be started and operated in the background whenever 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.
- 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 RUD-6-LKY 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).
- Additionally in the line of *RKD32 Key Cabinet Controller* select *Settings* and in the opened window configure the controller. The same settings will be further used in configuration of the RKD32 Key Cabinet. Close the window with *Save* button.



- 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.

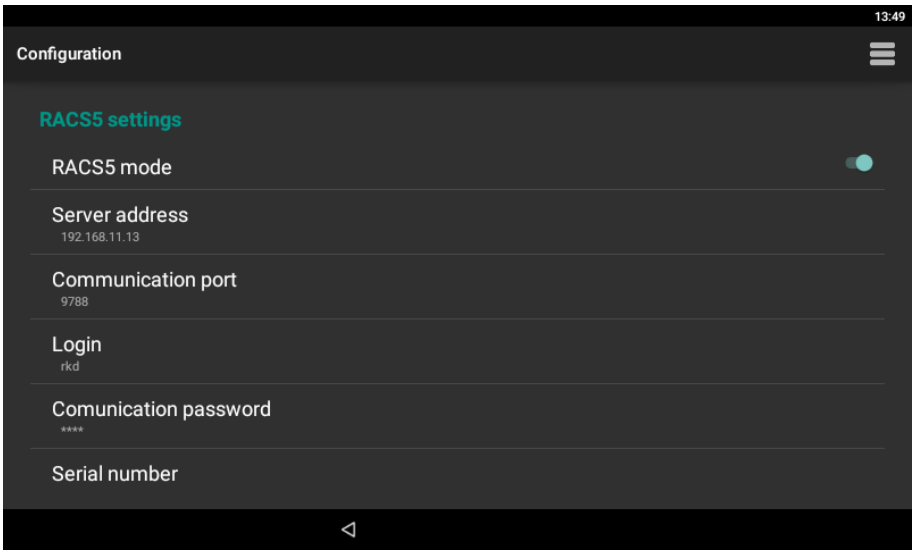


- Select *Start* and return to the main window. The server will be started and operated in the background whenever the computer is switched on even if RogerSVC window is closed.
- Start VISO software, in the top menu select *System*, then *Select License Server* and indicate previously defined License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

Key Cabinet configuration

The configuration of Key Cabinet is done by means of its MD70 touch panel. Based on RKD Operating Manual it is necessary to configure parameters in the section *RACS 5 settings* (table 2 in the manual) according to previous configuration of virtual controller. It is also recommended to note MAC address as it may be later required to detect and distinguish Key Cabinets in VISO software.

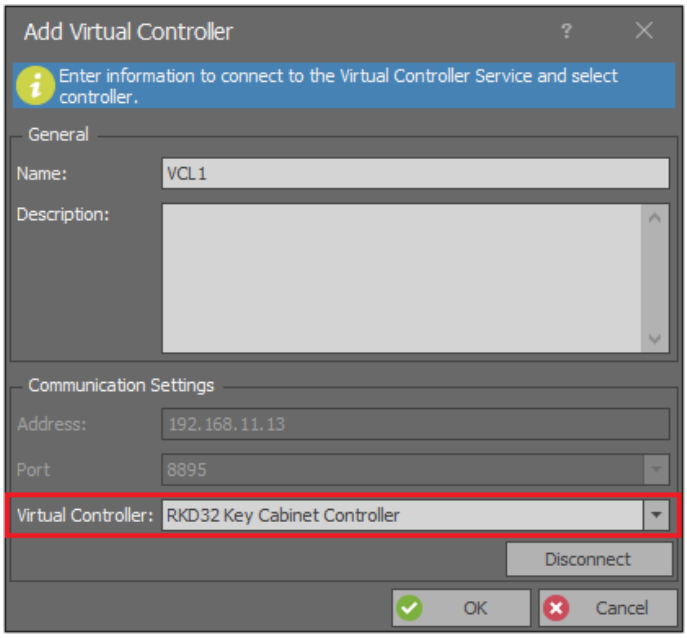
Note: The login must always be 'rkd'. Other values will not be recognized in RACS 5 system. The password can be defines as needed.



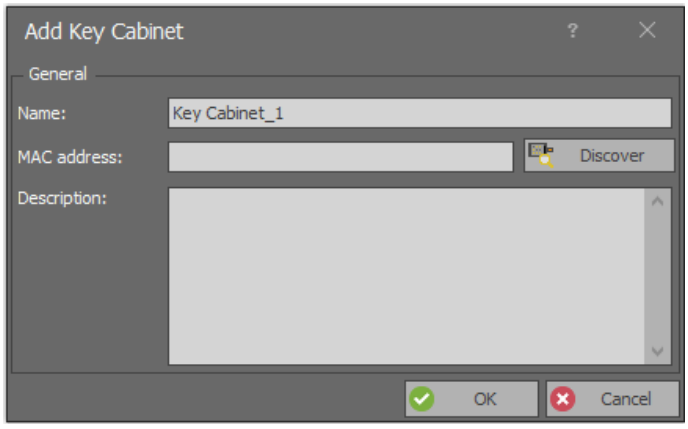
Connection with Key Cabinet

In order to configure virtual controller:

- In the navigation tree of VISO software right click *Virtual controllers* command and select *Add Virtual Controller*.
- In the opened window enter the IP address and port of previously configured virtual controller service.
- Click *Connect.*
- Select *RKD32 Key Cabinet Controller* and close the window with *OK* button.



- In the navigation tree expand the virtual controller, right click *Key Cabinets* and then select *Add Key Cabinet*.
- In the opened window detect the cabinet with *Discover* button or enter its MAC address manually.



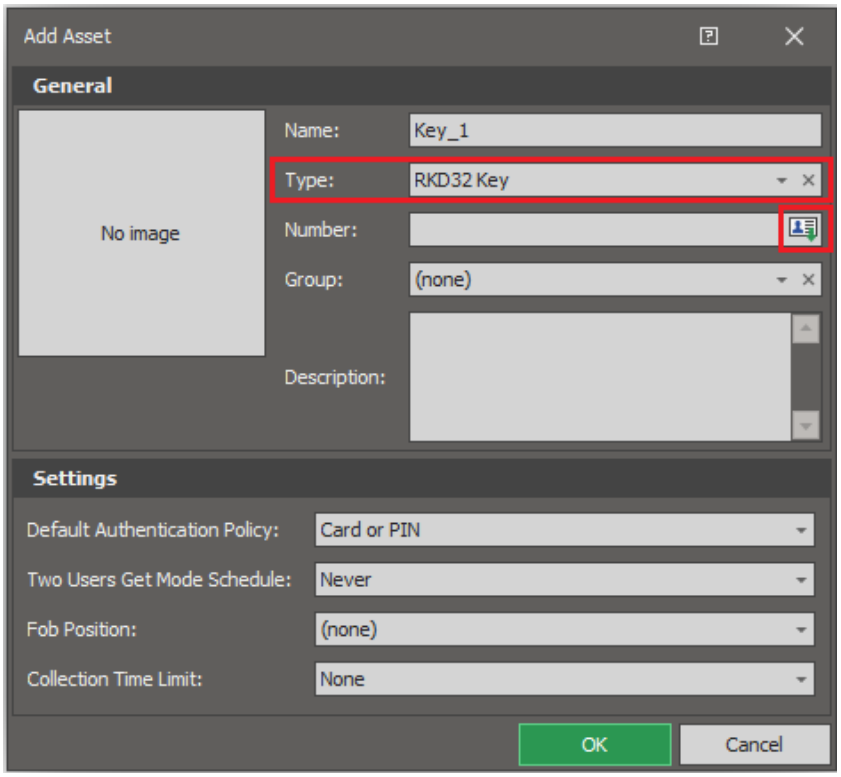
Note: For the communication of VISO and RKD32 cabinet it may be necessary to add rule in Windows firewall in regard of ICMP protocol using following exemplary command:

```
netsh advfirewall firewall add rule name="ICMP Allow incoming V4 echo request" protocol=icmpv4:8,any dir=in action=allow
```

Keys

In order to define key under control of Key Cabinet:

- In the top menu of VISO software select *Configuration* and then *Assets*.
- In the opened window select *Add* and in the next window define key with fob. Fob number can be read at RUD administrator reader (e.g. RUD-3) which is connected to computer's USB port. RUD settings should be default ones (CSN reading). Close the window with *OK* button.
- Add remaining keys.



Note: Key cannot be uploaded to Key Cabinet unless at least single Authorisation for such key is defined in the system.

When key is created then additional settings can be defined. The parameter *Default Authentication Policy* can be set to *Card and PIN*. In such case a user must identify with proper card or PIN to open the cabinet and then identify once more respectively with proper PIN or card (depending on what was used in the first step) to collect particular key. The parameter *Two Users Get Mode Schedule* enables to define when key collecting requires identification by two users, each with proper rights. Required General Purpose Maintained type Schedule can be defined by means of *Schedules* command in the navigation tree of VISO software. The parameter *Fob Position* can be used to select dedicated slot for the key. The parameter is valid only if the RKD32 is operated in *Fixed fob position* operating mode which can be selected on the panel when the RKD32 is started for the first time (if operating mode need to be changed later then it is necessary to stop and clear all data for RAACA app on MD70 terminal). The parameter *Collection Time Limit* enables to define maximal time for key collecting. The limit can be till particular time (e.g. 5:00 PM) or for particular time (e.g. 10 h). When the limit is exceeded then alarm event is generated in RACS 5 system.

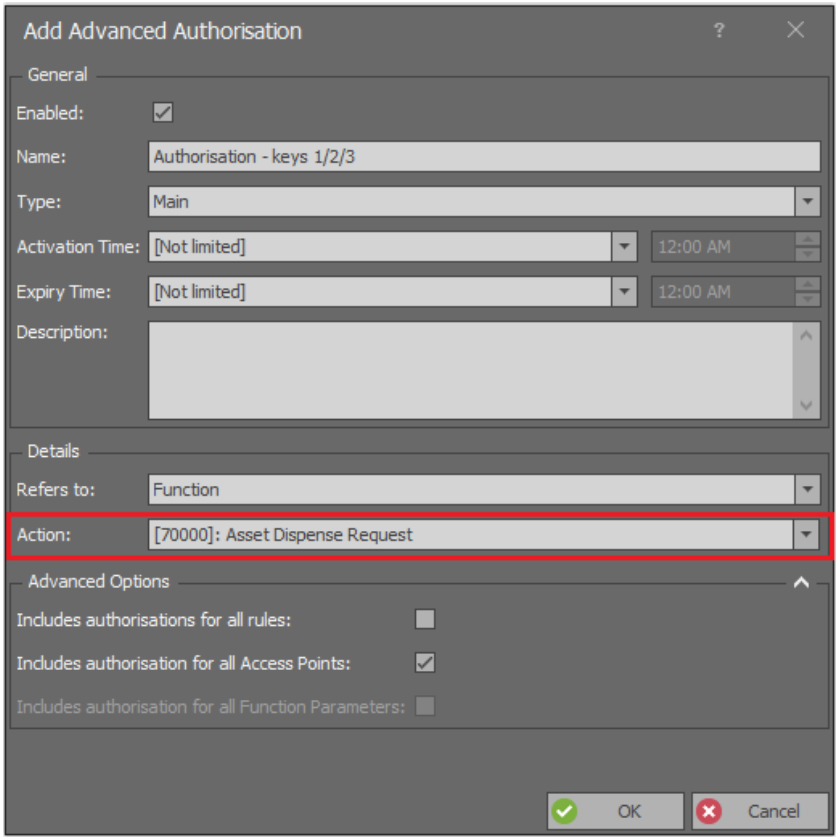
Authorisations

It is possible to define Authorisations not only to particular keys but also in regard of Key Cabinet management i.e. access to settings, access to event log, access to key status and authorisation for overriding reserved key blocking.

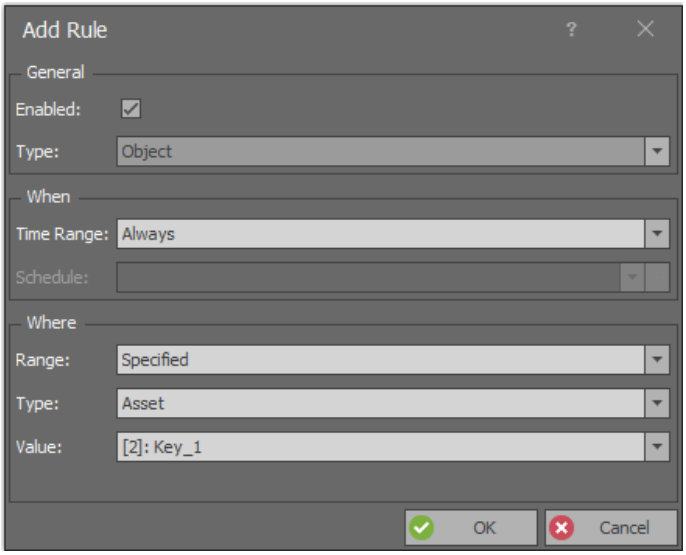
Advanced Authorisations (keys)

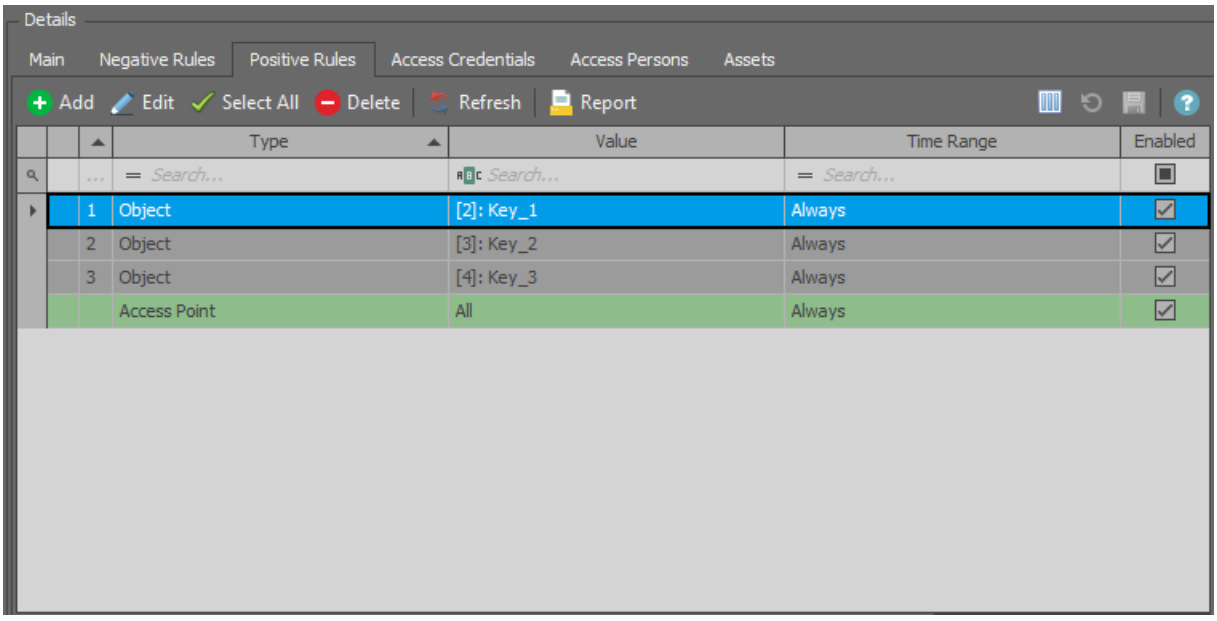
In order to define Advanced Authorisation for key collecting:

- In the navigation tree of VISO software expand *Authorisations* command and double click *Advanced Authorisation* command.
- In the opened window select *Add*, then in the next window name the Authorisation and select the function *[70000].* If the option *Include authorisation for all rules* is enabled then the Authorisation will allow to collect all keys from all Key Cabinets without further defining of Positive rules.



- In the bottom select *Positive Rules* tab and then *Add*.
- In the opened window select *Object* as *Type*, *Specified* as *Range* and specific key as *Value*. This rule will allow to collect *Key_1* from any RKD32 cabinet. Optionally the rule can be limited in time by assigning a General Purpose Maintained schedule. Such schedules are created by selecting *Schedules* command in the navigation tree of VISO software. There can be up to 64 rules included in the Authorisation. Therefore in the system there can be defined individual Authorisations for each key and there can also be defined collective Authorisation for multiple keys using multiple rules within single Authorisation. Close the window with *OK* button.

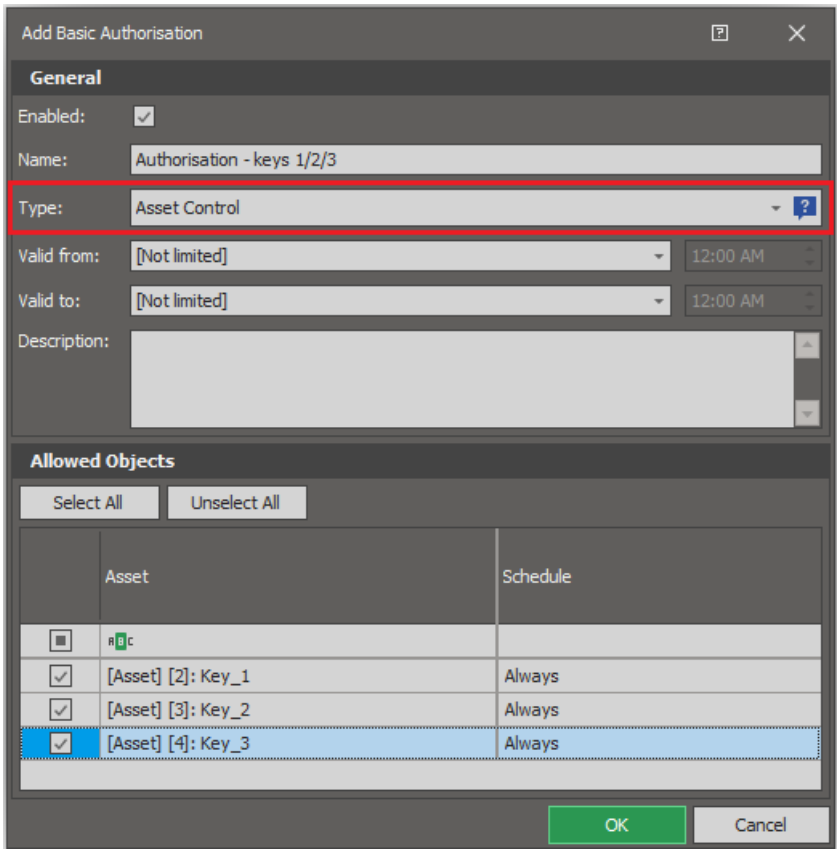




Note: In further steps all Authorisations can be grouped by expanding *Authorisations* command in the navigation tree and then selecting *Authorisation Groups*. When user is enrolled in the system then both Authorisations and Authorisations Groups e.g. for typical keys.

Standard Authorisations (keys)

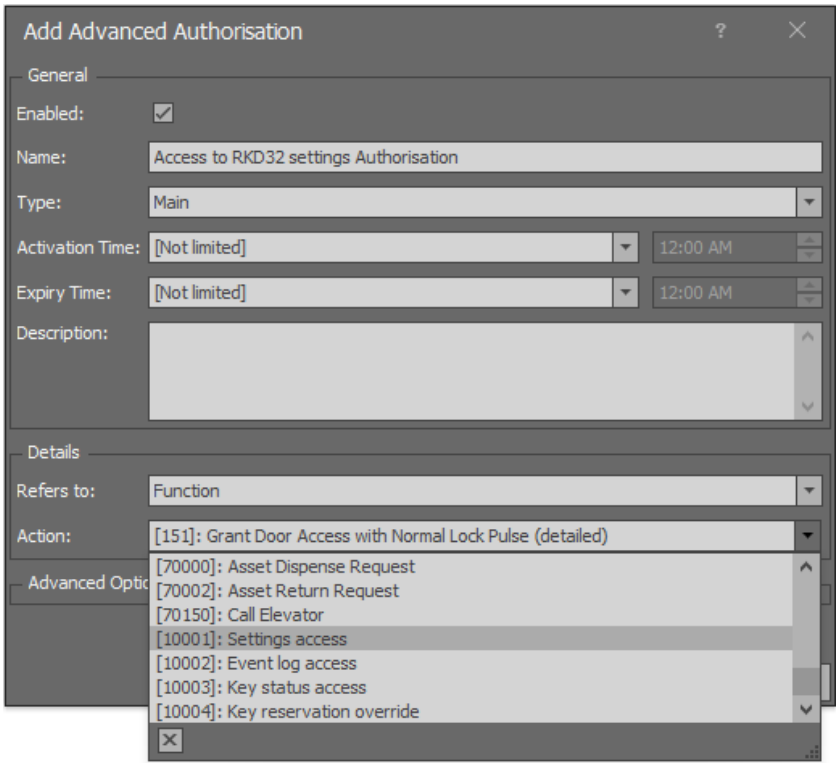
In RACS 5 v2 system it is possible to define Basic Authorisations for key collecting. Both types of Authorisation i.e. Advanced and Basic can be used in the same system.



Advanced Authorisations (management)

In order to define additional Authorisations in regard of RKD32 management:

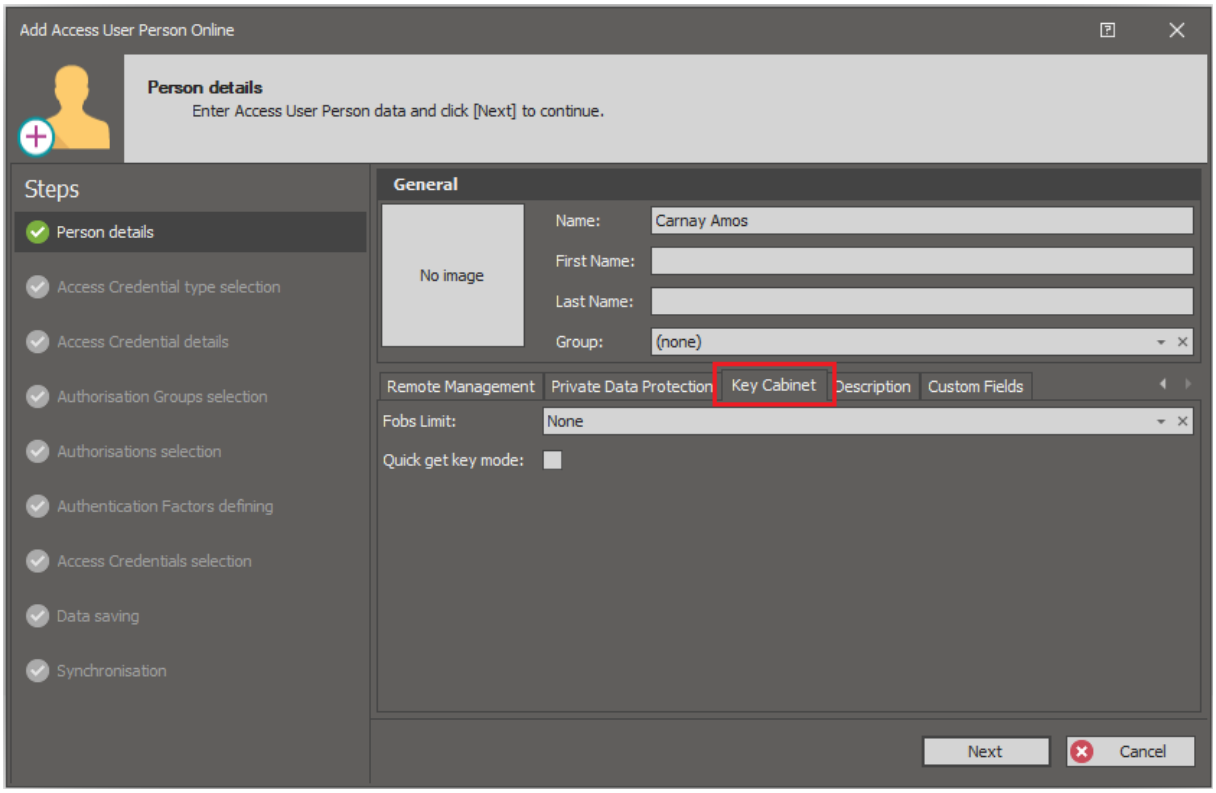
- In the navigation tree of VISO software expand *Authorisations* command and double click *Advanced Authorisation* command.
- In the opened window select *Add*, then in the next window name the Authorisation and select the function in range of *[10001]..[10004].*
- Define Authorisation for each function. Positive rules are not required for these Authorisations.

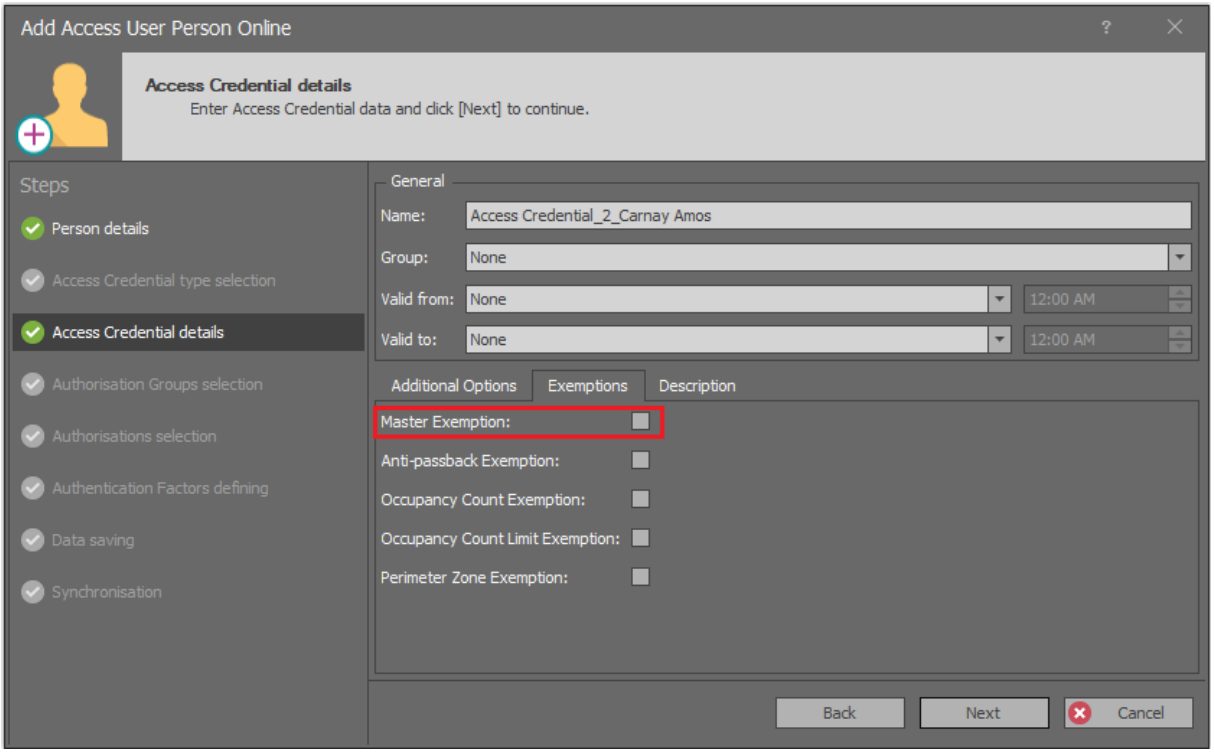


Users

The management of users (Persons) in the system can be done with wizards, which are accessed by selection of *Wizards* command in the top menu of VISO software. It is recommended to create new user by means of *Add Person Online* wizard because then Access Credential and Person are created as a pair. When only Access Credentials are defined without Persons then functionalities of the system in regard of key collecting are limited because some functions are executed on the level of Persons. The use of wizard is explained in AN006 Application note.

When user is defined then *Quick get key mode* can be enabled and the maximal number of keys for collection by user can be defined. When user's Access Credential is defined and the option *Master exemption* is enabled then such user will be granted unlimited Authorisation in the system including access to all doors, keys, and RKD32 settings.





Note: In current version of the system, users can be defined with wizards but in order to upload them to RKD32 Key Cabinets it is necessary to make full synchronisation. This can be done for example by right clicking *Networks* in the navigation tree of VISO software and then selecting *Synchronise*.

Asset Return Zones

Asset Return Zones are introduced in RACS 5 v2 system. Their functionality is ensured by Communication Server and they enable to deny user the exit from zone if key(s) collected by the user is/are not returned to RKD32 Key Cabinet. In order to define zone:

- In the navigation tree of VISO software within particular Communication Server double click *Asset Return Zones*.
- In the opened window select *Add*, name the zone and optionally select Schedule to define time when the limits of zone are enforced. The required General Purpose Maintained type Schedule can be defined by selection of *Schedules* in the navigation tree of VISO software. Close the window with *OK* button.
- In the bottom select *Access Points* tab and then *Assign* to select exit points (readers) for the zone. Close the window with *OK* button.
- Select the tab *Assets* and then select keys which will be affected by the zone limits.
- Optionally select the tab *Exempt Persons* in order to select Persons who are not limited by the zone.
- Synchronise settings with Key Cabinet(s) and controller(s).

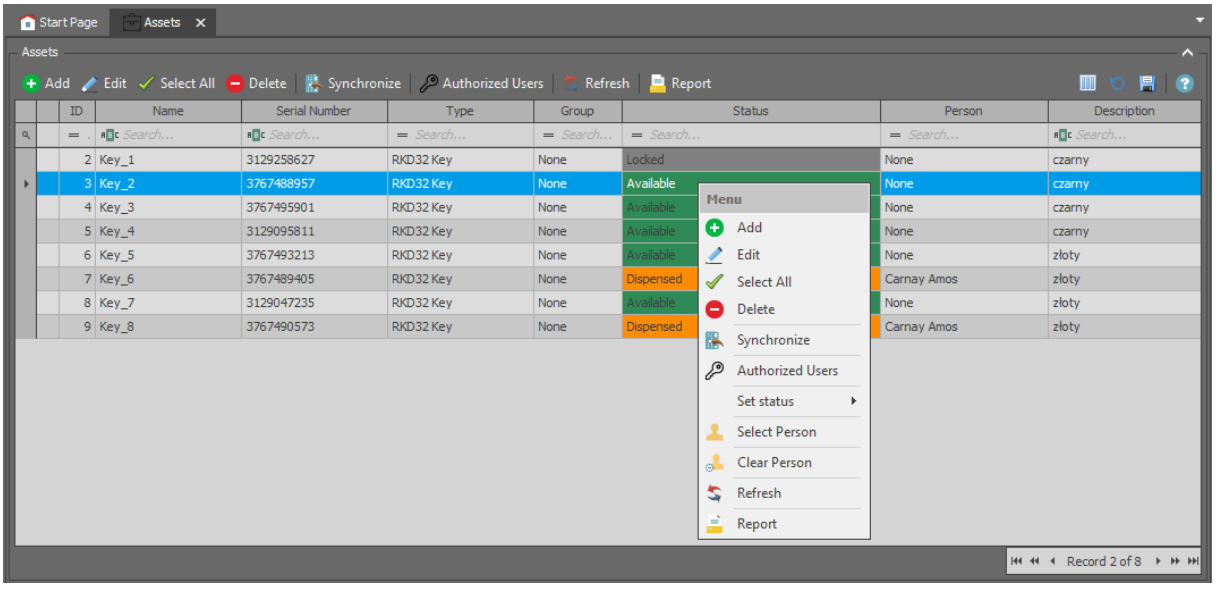
Note: In case of Asset Return Zones the External and Machine Authorisation monitoring process must be enabled within Communication Server in VISO software.

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.

Key statuses

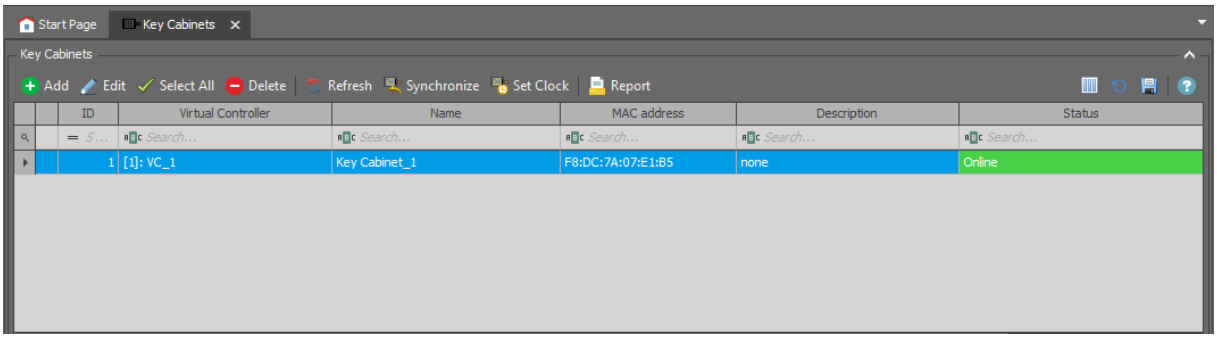
Assets window presents statuses of particular keys and includes information on persons who collected keys. *Available* and *Dispensed* statuses are updated automatically when keys are returned and collected. Additionally it is possible to lock/unlock a key. Locked key cannot be collected from Key Cabinet until its status is set to *Available* on the level of VISO software.



Note: In current version of the system, when key is locked/unlocked on the level of VISO software then full synchronisation must be done to affect the cabinet.

Communication

The communication with RKD32 Key Cabinets is monitored and events are generated both for lost and restored communication. Additionally, current status of connection with Key Cabinets is presented on the list of cabinets in VISO software. Lost connection is reported within a few seconds from its occurring.



Users and alarms

RACS 5 system registers events related to user logging as well as key collecting and returning. Additionally various alarm events related to door forced open, tamper, door open too long are also registered in the system.

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