

Roger Access Control System 5

Application note no. 042

Document version: Rev. A

RKD32 Key Cabinet

Note: This document refers to RACS v5.6.6 (VISO 1.6.6 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.

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. 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.)
- 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 local database according to AN006 application note or create recommended centralized database according to AN017 application note.
- Install RogerSVC software and select not only communication service but also license service and virtual controller service. If services are supposed to be operated on individual servers then install RogerSVC on each computer selecting required services. In RACS 5 system only single communication service can be operated.

Note: If license service and virtual controller service are supposed to be operated on individual servers then during installation of virtual controller the license service must be deselected. Only in such case it will be possible to indicate external license service when virtual controller service will be configured.

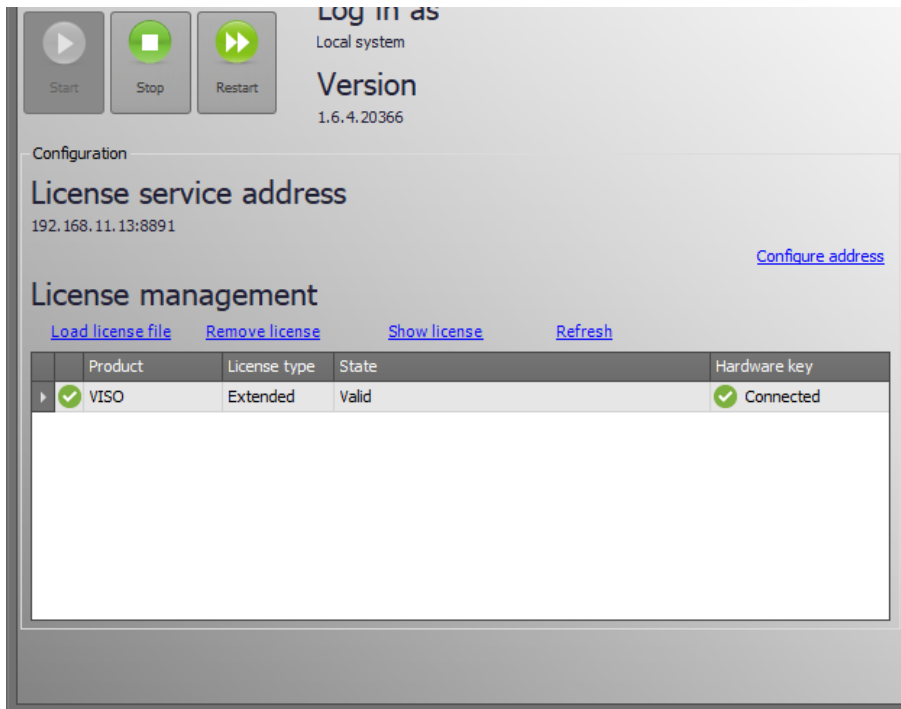
- Start RACS Services Manager selecting *Start->ROGER->RogerSVC* in Windows menu.
- Click the icon in Windows tray.



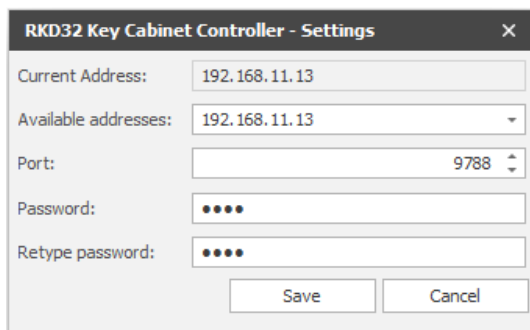
- In the manager window select *Database connection* tile and then *Configure connection* to indicate previously created RACS 5 database. Return to the main window.



- In the manager window select *Communication service* tile and then start the service. Return to the main window.
- Connect RUD-6-LKY hardware key to USB port of server with license service installed.
- In the manager window select *License service* tile, click *Configure address*, enter IP address of the computer with license service 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 service will be started and operated in the background whenever the computer is switched on even if the manager is closed.



- In the manager window select *Virtual controller service* tile, click *Configuration*, enter IP address of the computer with virtual controller service 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.

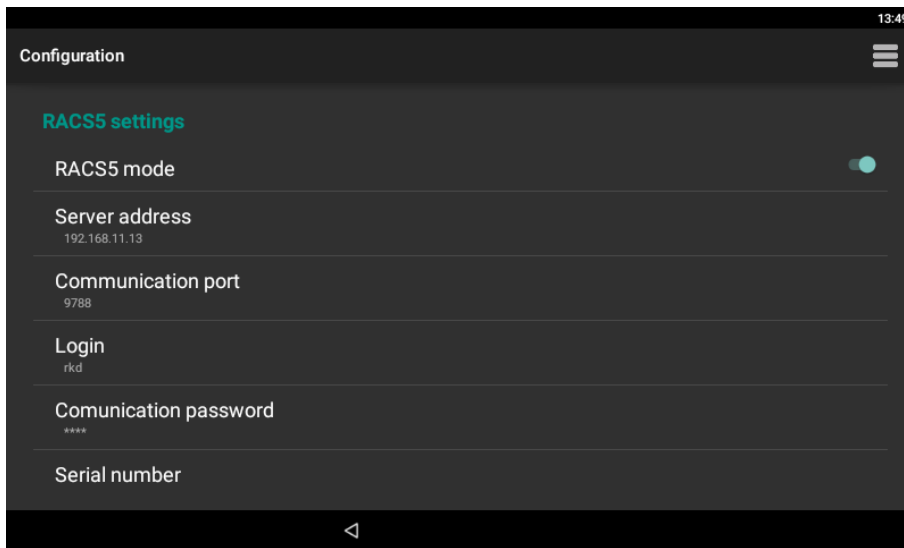


- Select *Start* and return to the main window. The service will be started and operated in the background whenever the computer is switched on even if the manager is closed.
- Start VISO software, in the top menu select *System*, then *Select Licensing Server* and indicate previously defined license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

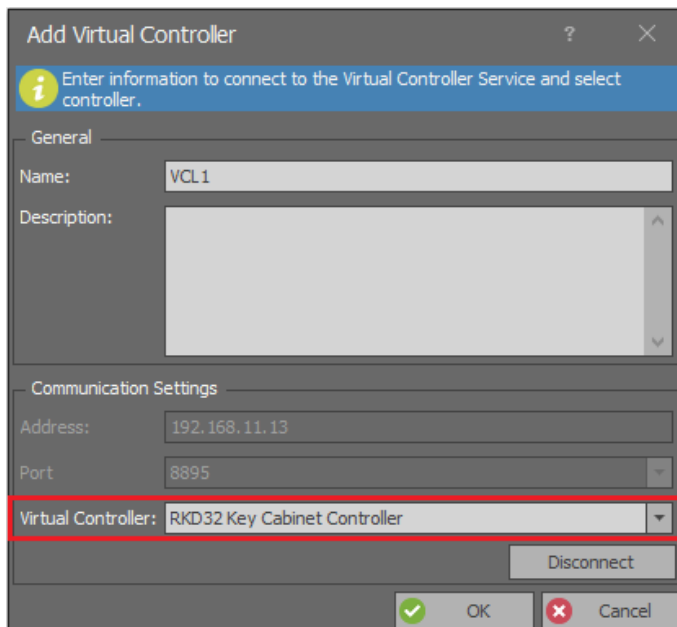
Note: The login must always be 'rkd'. Other values will not be recognized in RACS 5 system. The password can be defines as needed.



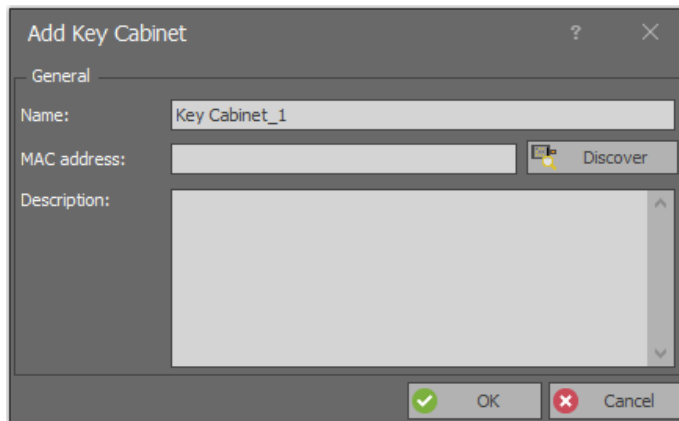
Connection with Key Cabinet

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.



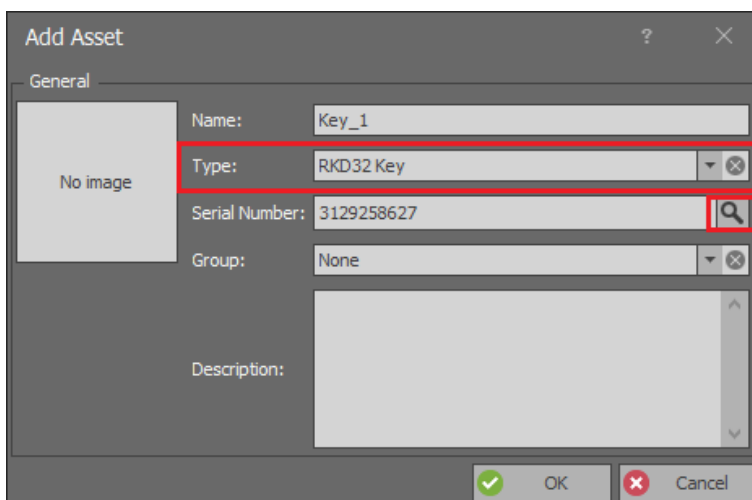
- In the navigation tree expand the virtual controller, right click *Key Cabinets* and then select *Add Key Cabinet*.
- In the opened window detect the cabinet with *Discover* button or enter its MAC address manually.



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.

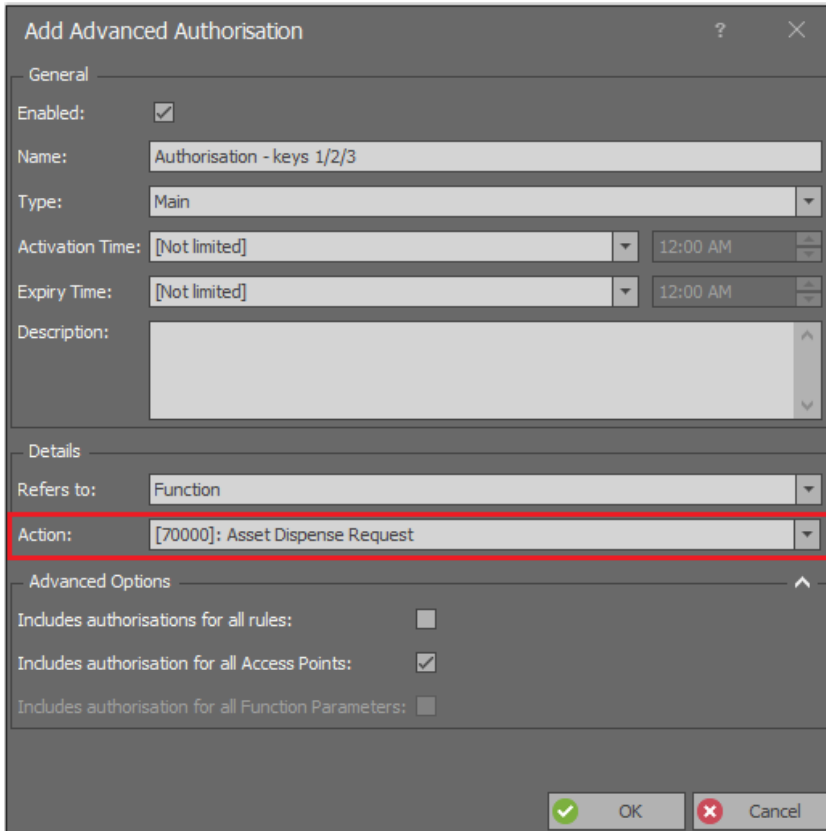
Authorisations

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.

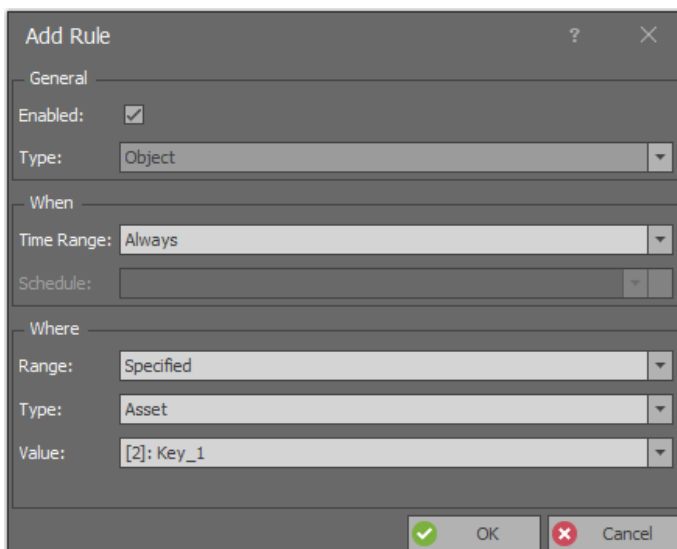
In order to define Authorisation for key collecting:

- 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.



Details

Main Negative Rules Positive Rules Access Credentials Access Persons Assets

+ Add Edit Select All Delete Refresh Report

	Type	Value	Time Range	Enabled
1	Object	[2]: Key_1	Always	<input checked="" type="checkbox"/>
2	Object	[3]: Key_2	Always	<input checked="" type="checkbox"/>
3	Object	[4]: Key_3	Always	<input checked="" type="checkbox"/>
	Access Point	All	Always	<input checked="" type="checkbox"/>

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.

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.

Add Advanced Authorisation

General

Enabled:

Name: Access to RKD32 settings Authorisation

Type: Main

Activation Time: [Not limited] 12:00 AM

Expiry Time: [Not limited] 12:00 AM

Description:

Details

Refers to: Function

Action: [151]: Grant Door Access with Normal Lock Pulse (detailed)

Advanced Options

- [70000]: Asset Dispense Request
- [70002]: Asset Return Request
- [70150]: Call Elevator
- [10001]: Settings access
- [10002]: Event log access
- [10003]: Key status access
- [10004]: Key reservation override

Users

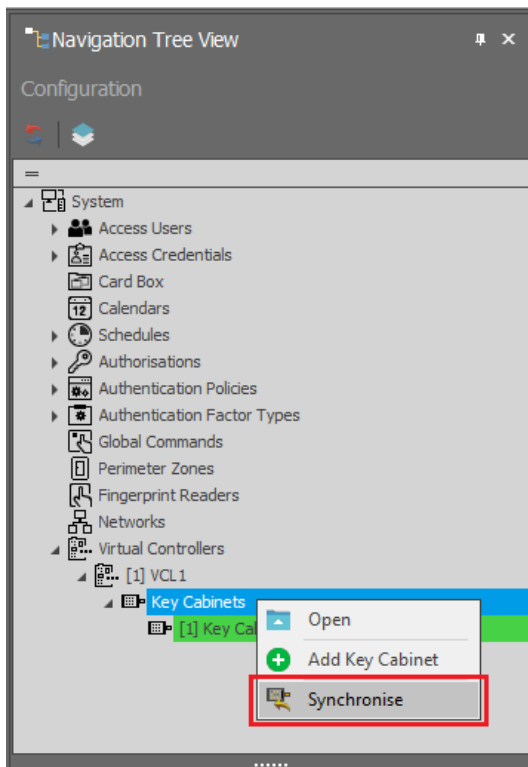
The management of users in the system can be done with wizards, which are accessed by selection of *Wizards* command in the top menu of VISO software. New user can be enrolled with *Add Person Online* wizard. The use of wizard is explained in AN006 Application note.

When user is defined then *Quick get key mode* can be enabled and 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.

The screenshot shows the 'Add Access User Person Online' wizard at the 'Person details' step. The title bar reads 'Add Access User Person Online'. Below the title bar is a header area with a person icon and the text 'Person details' and 'Enter Access User Person data and click [Next] to continue.' A 'Steps' sidebar on the left lists various steps, with 'Person details' highlighted. The main area is divided into 'General' and 'Contact Information' tabs. Under 'General', there are fields for 'Name' (Carnay Amos), 'First Name', 'Last Name', and 'Group' (none). Under 'Contact Information', there are fields for 'T&A ID', 'Information Reference', and 'Credit' (0). A red box highlights the 'Quick get key mode' checkbox, which is currently unchecked. At the bottom right, there are 'Next' and 'Cancel' buttons.

The screenshot shows the 'Add Access User Person Online' wizard at the 'Access Credential details' step. The title bar reads 'Add Access User Person Online'. Below the title bar is a header area with a person icon and the text 'Access Credential details' and 'Enter Access Credential data and click [Next] to continue.' A 'Steps' sidebar on the left lists various steps, with 'Access Credential details' highlighted. The main area is divided into 'General' and 'Additional Options' tabs. Under 'General', there are fields for 'Name' (Access Credential_2_Carnay Amos), 'Group' (None), 'Valid from' (None, 12:00 AM), and 'Valid to' (None, 12:00 AM). Under 'Additional Options', there are checkboxes for 'Master Exemption', 'Anti-passback Exemption', 'Occupancy Count Exemption', 'Occupancy Count Limit Exemption', and 'Perimeter Zone Exemption'. A red box highlights the 'Master Exemption' checkbox, which is currently unchecked. At the bottom right, there are 'Back', 'Next', and 'Cancel' buttons.

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 in VISO navigation tree.

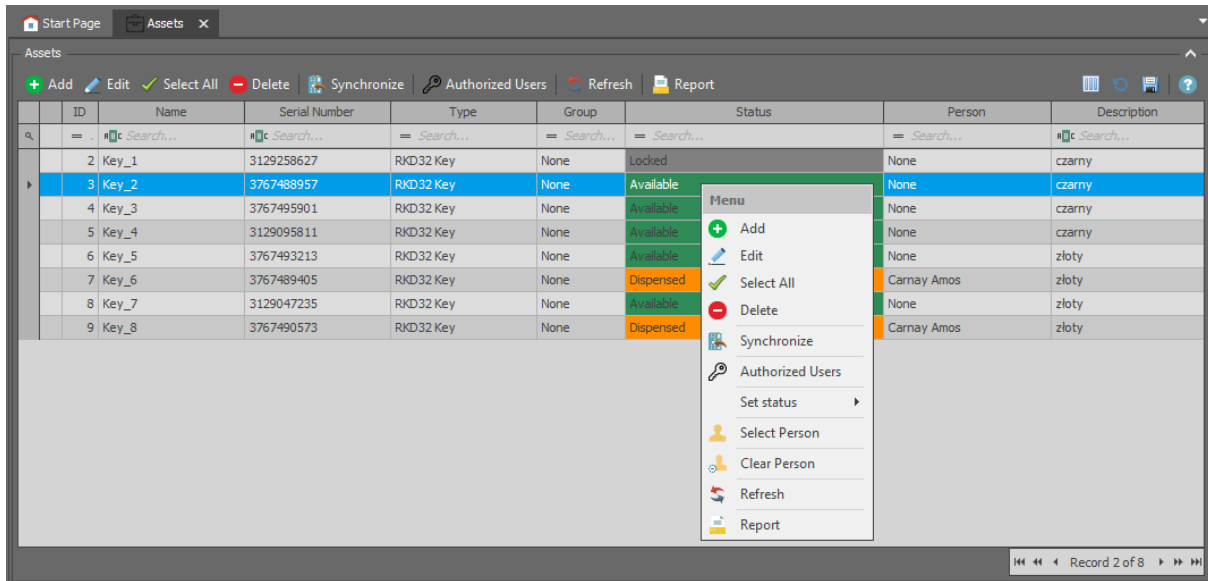


Monitoring

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

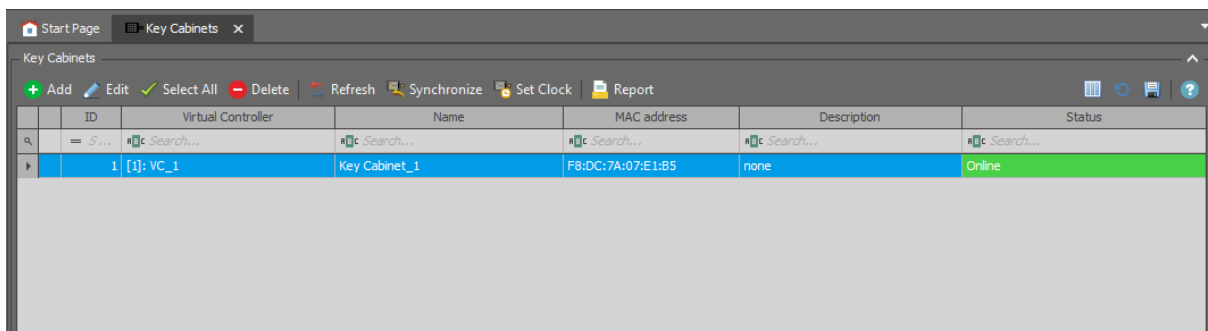
Assets window presents statuses of particular keys and includes information on persons who collected keys. *Available* and *Dispensed* statuses are updated automatically when keys are returned and collected. Additionally it is possible to lock/unlock a key. Locked key cannot be collected from Key Cabinet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