

Roger Access Control System 5v2

Application note no. 013

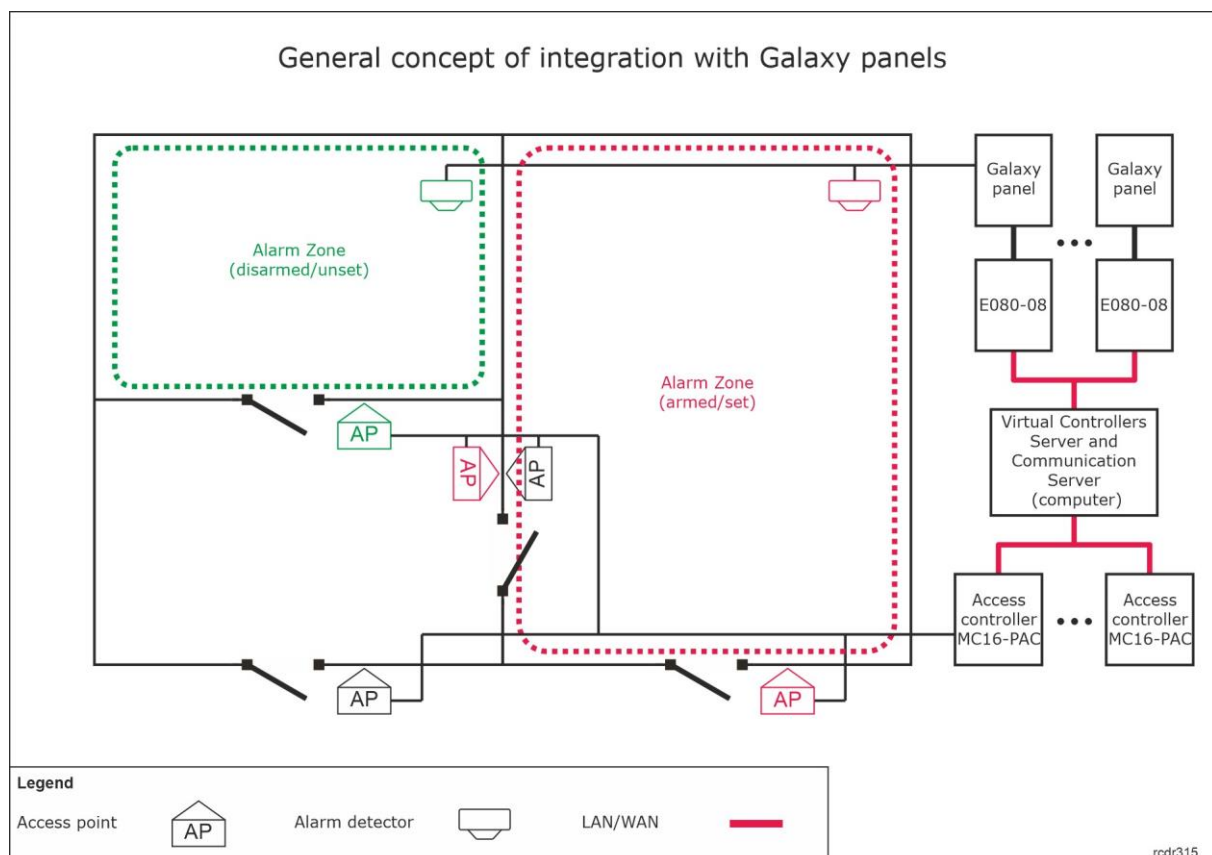
Document version: Rev. C

Galaxy (Honeywell) integration

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

Introduction

RACS 5 system enables not only universal hardware integration with intrusion alarm systems which is described in AN027 application note but also dedicated software integration with Galaxy Dimension series alarm control panels from Honeywell company. In such scenario the communication of access control system with alarm system is ensured by Virtual Controllers Server (Windows service) from RogerSVC software package. Alarm system can include multiple alarm control panels, each equipped with E080-08 module. The integration requires purchase of license.



Note: In Galaxy alarm system, Alarm zones are called Groups while inputs for connection of detectors are called Zones. In this note and in VISO software, Galaxy Groups and Zones are called respectively Alarm Zones and Input lines.

The concept of integration is based on logical connection of RACS 5 system Alarm Zones which include Access Points (readers) with Galaxy system Alarm Zones which include detectors. In practical application it means that the Armed mode of reader(s) and associated detector(s) is the same. Therefore the integration:

- Makes the management of both systems more convenient as Alarm Zones in both systems can be controlled from devices of one of the systems e.g. RACS 5 readers
- Allows to warn users about armed detectors in particular zone of alarm system as it can be presented on readers' LED indicators.
- Enables to avoid unnecessary alarms as the entry to the zone with armed detectors can be denied at access control readers because in such situation they would also be armed while getting into armed zone would require readers disarming which automatically results in detectors disarming.

Additionally the integration enables monitoring and remote control of Galaxy alarm system in VISO management software by means of available monitors, Maps and remote commands. The integration can also be applied in VISO SMS (Security Management System) as explained in AN055 application note.

Configuration of alarm system

Integration settings

Configure alarm system according to manufacturer's instructions and manuals. Printscreens below present parameters which are essential in regard of the integration. They were taken from Galaxy Remote Servicing Suite (RSS) software. Additionally numbers of the parameters are shown in red. They can be used for manual configuration of Galaxy panel by means of keypad e.g. CP037.

The screenshot displays the 'System Users' configuration window in the V6 Application software. The window is titled 'System Users' and has a 'General' tab selected. The interface is divided into several sections for configuring different user roles:

- Manager:** Fields for Name (MGR), PIN, Menu Choice (*), Group Choice, Tag Number, Menu Option (12=TIMED SET), Keypad (**), Dual Focus, Dual Access, Tag Link, Duress (#), Serial Number, PA, RF Mode (Alpha), and Alarm Group (A1-).
- Authority:** Fields for Name (AUTOR), PIN, Menu Choice (*), Group Choice, Tag Number, Serial Number, PA, RF Mode (Alpha), and Alarm Group (A1-).
- Engineer:** Fields for Name (INZ), PIN, and Dual.
- Remote:** Fields for Name (REMOTE) and PIN (*****). This section is highlighted with a red box, and red text labels '42.1.3' and '42.1.1' are placed next to the Name and PIN fields respectively.

The left sidebar shows a navigation tree with categories like Users, Zones, Outputs, Groups, Links, and Communications. The 'Users' category is expanded, showing 'System Users' as the selected item.

In the *Remote* area, remote communication password can be changed into own 6 digit password. In this note the default PIN=543210 will be applied.

V6 Application

File Edit View Connect Panel Communications Logs Help

Navigation Window

Users

User Codes

System Users

Zones

Assemble Zones

Outputs

RIO Outputs

Keypad Outputs

Schedule Output

Header Outputs

Groups

Group Mode

Group Parameters

Group Communications

Links

Communications

Internal Telecomms

External Telecomms

ISDN

Ethernet

Internal RS232

External RS232

Ethernet

General Remote Access Reporting Triggers

Module Config

IP Address 192 . 168 . 11 . 123 56.4.1.1

Gateway IP Address 192 . 168 . 11 . 1 56.4.1.3

Network Mask 255 . 255 . 255 . 0 56.4.1.4

Site Name TW-460(1)

Autotest

Hours 0

Minutes 0

Interval 0 hours

Heartbeat

Hours 0

Minutes 1

ISOM

Enable

Server URL https://isom.galaxy.mymaxproc

Server Port 443

Proxy IP / URL

Comm Fail

Number Of Attempts 3

Line fail

Network Available

Signal Primary

Encrypt

Alarm Report Alarm Mon

Remote Access SIA Control

Backup Module Off

SIA Control

SIA IP Address 192 . 168 . 11 . 13 56.4.8

GPRS Network

Access Point Name

Login

Password

In *Module Config* area, there are entered parameters of E080-08 module which is used for communication with alarm panel via Ethernet. In *SIA IP Address* it is necessary to enter IP address of computer with Virtual Controllers Server from RogerSVC software package of RACS 5 system.

V6 Application

File Edit View Connect Panel Communications Logs Help

Navigation Window

Users

User Codes

System Users

Zones

Assemble Zones

Outputs

RIO Outputs

Keypad Outputs

Schedule Output

Header Outputs

Groups

Group Mode

Group Parameters

Group Communications

Links

Communications

Internal Telecomms

External Telecomms

ISDN

Ethernet

Internal RS232

External RS232

Ethernet

General Remote Access Reporting Triggers

Remote Access

Times Any Time 56.4.3.1

Mode Direct Access 56.4.3.2

Call IP Address 1

Port Number 1 0

Call IP Address 2

Port Number 2 0

Call IP Address 3

Port Number 3 0

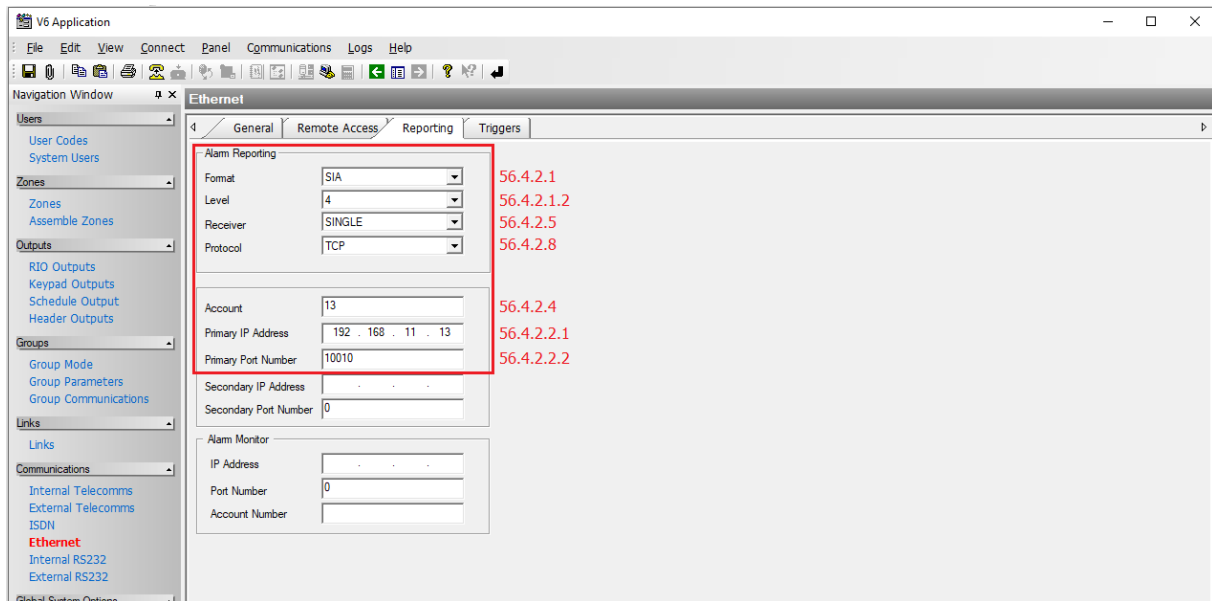
Call IP Address 4

Port Number 4 0

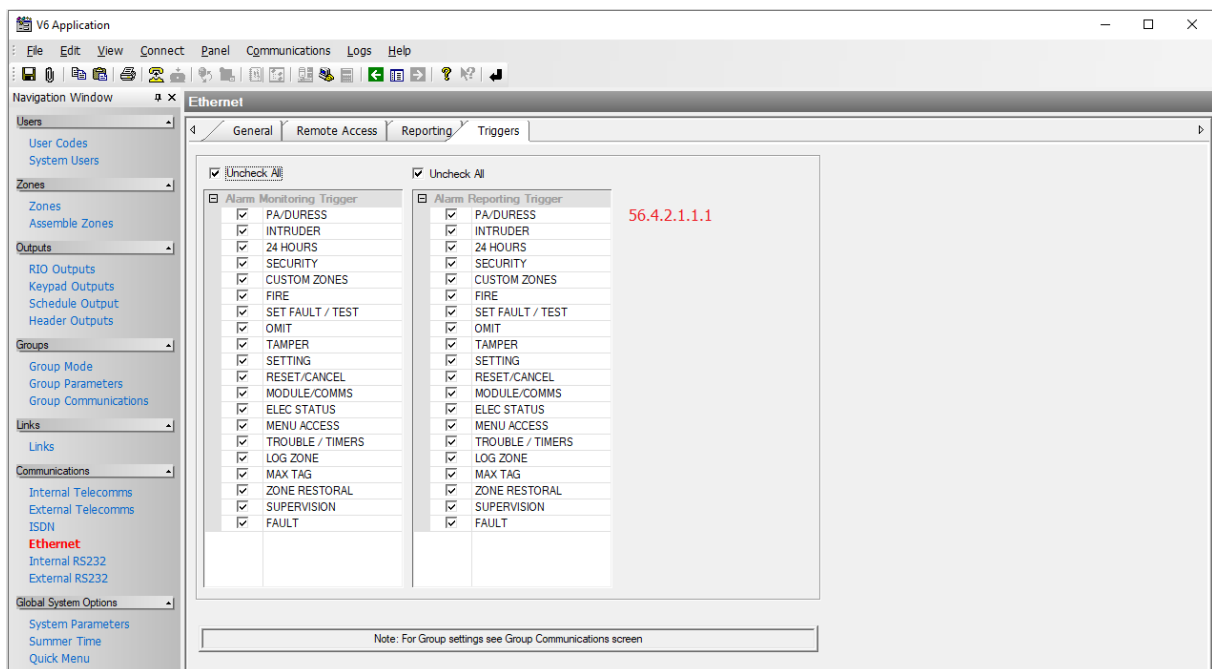
Call IP Address 5

Port Number 5 0

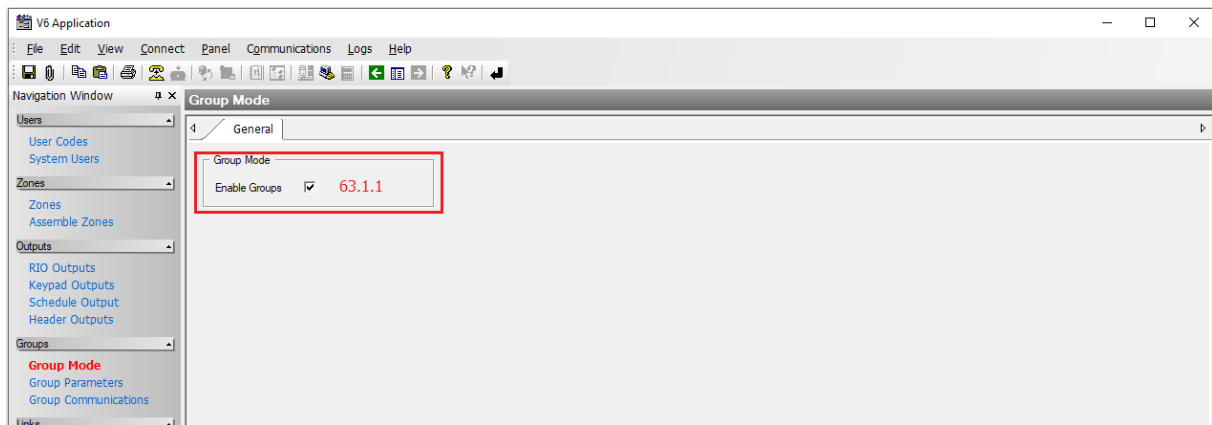
In *Remote Access* tab the limits for remote access to alarm panel are configured. It is recommended to define unrestricted access as in the window above.



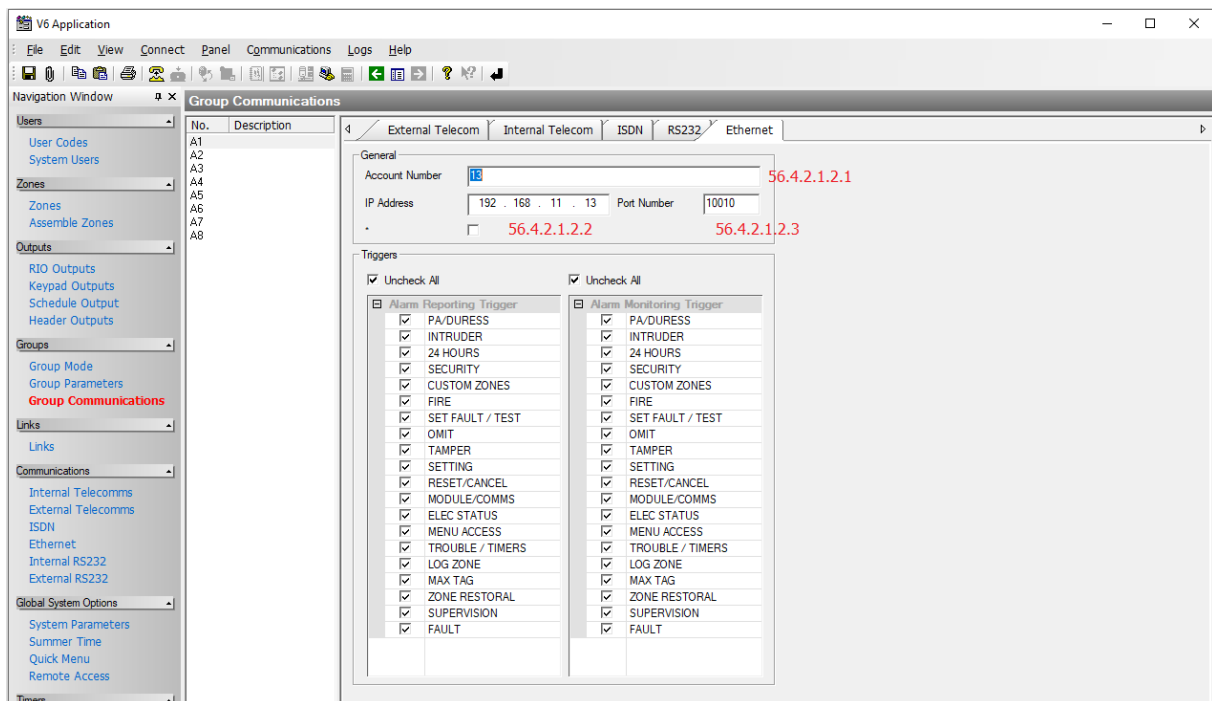
In this tab, communication parameters and format of events transmitted by alarm panel are configured. The parameter *Account* is necessary and it is used to distinguish Galaxy panels. The value 13 is exemplary. In *Primary IP address* it is necessary to enter IP address of computer with Virtual Controllers Server from RogerSVC software package of RACS 5 system. The port 10010 is exemplary and the same port must be entered when integration connection is defined in RACS 5 system.



In *Triggers* tab the operator can select which events will be transmitted by alarm system and consequently registered in RACS 5 system. It is recommended to select all events.



In this window the operator can enable Groups. The integration is based on association of Alarm zones from RACS 5 system with Groups (Alarm zones) from Galaxy systems. If Groups with their Zones (detectors) are not defined then within the integration it will not be possible to arm/disarm particular detectors but only all detectors.



When Galaxy system is divided into Groups (Alarm zones) then it is necessary to define which events are to be transmitted for particular Groups by alarm system and consequently registered in RACS 5 system. It is recommended to select all events for all Groups.

Note: Virtual Controllers Server and RSS software cannot be used at the same time for communication with Galaxy as they will interfere with each other.

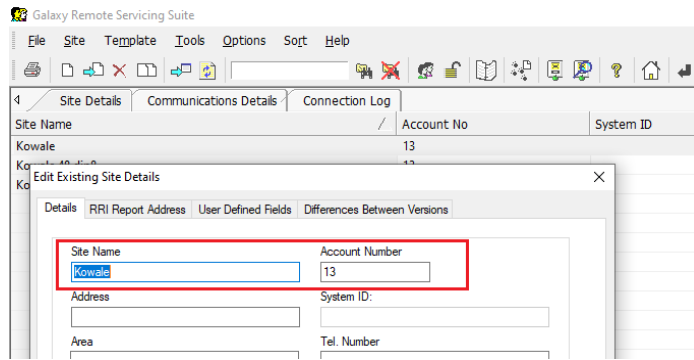
Export

After connection of detectors and other required devices and configuration of intrusion alarm system according to manufacturer's instructions and manuals it is necessary to export the configuration so it could be later imported into RACS 5 system. In order to export the configuration:

- Start Galaxy Remote Servicing Suite (RSS) software.

- In the top menu select *File->Export->All Galaxy Dimension Panels* and export setting into txt files.

Note: Account number which is configured in the panel must also be configured in the properties of site as below. Otherwise it will not be exported into files and it will result in error during import to VISO software.




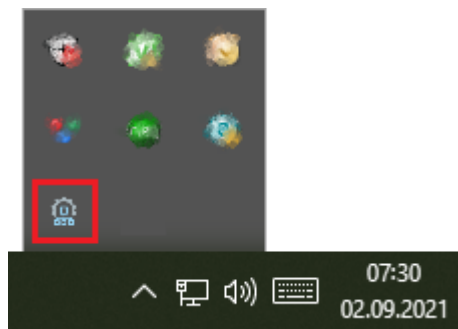
Preliminary configuration of RACS 5

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.

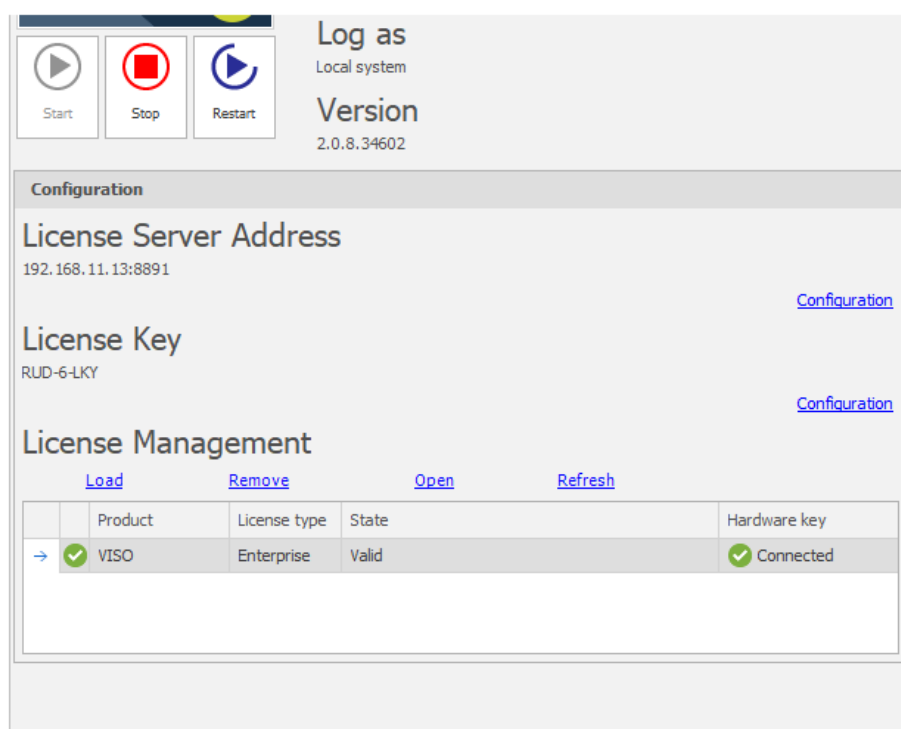
- When RogerSVC is launched then its icon is displayed in Windows tray. Click the icon . The RogerSVC icon in tray can also be launched from Windows menu *Start-> Roger-> RogerSVC*.



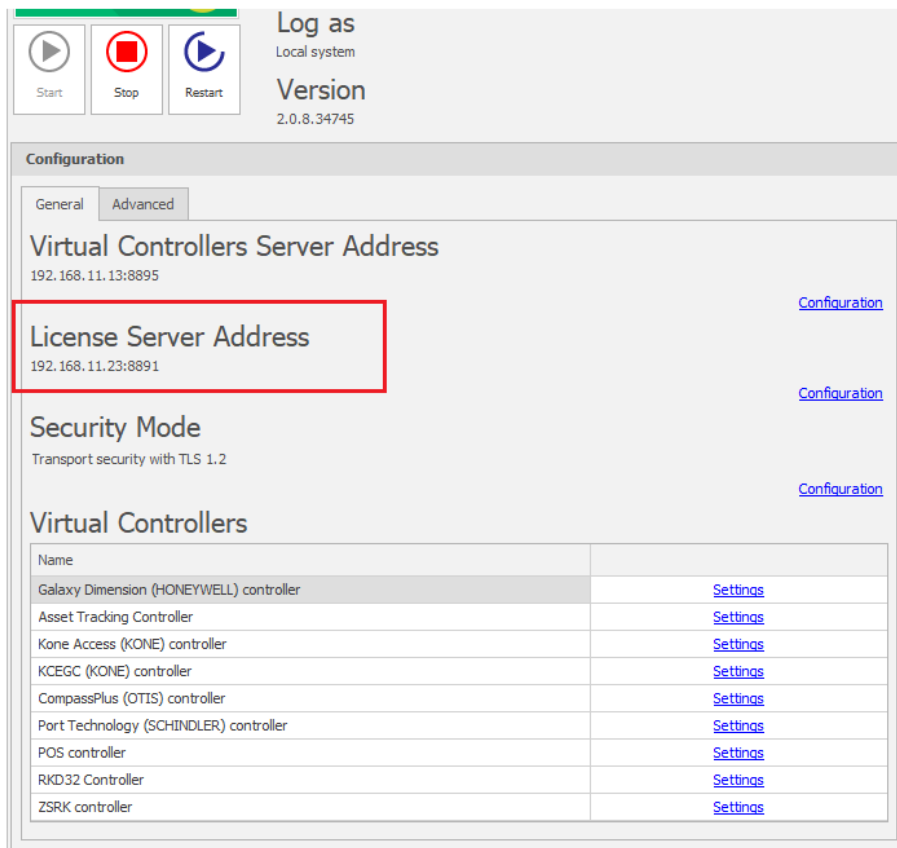
- In the RogerSVC window select *Database Connection* tile and then *Configuration* to indicate previously created RACS 5 database. Return to the main window.



- 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).
- On the list of controllers select *Settings* for *Galaxy Dimension (HONEYWELL) controller* and in the next window indicate folder with previously exported configuration files from panels.
- 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.

Configuration of RACS 5 Alarm Zones

RACS 5 system enables configuration of Alarm Zones, each within single RS485 bus including MC16 access controller and its peripheral devices such as readers and expanders. Alarm Zone includes Access Points (readers) called Arming Points which are armed/disarmed concurrently which means that all Arming Points of particular zone are always in the same Armed mode. In order to create Alarm Zone:

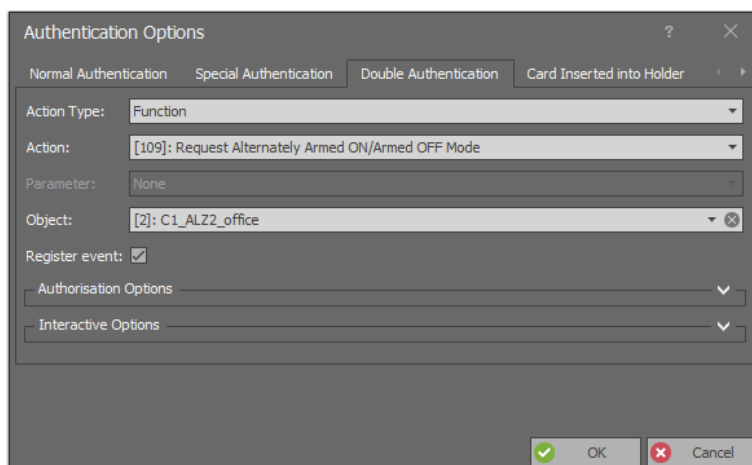
- Configure access control system according to AN006 Application note in regard of Access Doors, Access Points, Users and their Authorisations.
- In the navigation tree of VISO software within particular MC16 access controller double click *Alarm Zones* command.
- In the opened window click *Add* button and optionally enter zone's name.
- Enable the option *Disable physical access when zone armed*, if Access Points of armed zone are supposed to deny access to users with valid access rights till zone disarming.
- Click *OK* button.
- In the bottom select *Arming Points* tab and assign Access Points to the Alarm Zone. These points (readers) will be armed/disarmed concurrently within their zone.
- Upload settings to controller. Red LED SYSTEM indicators on readers signify armed zone while green LED SYSTEM indicators signify disarmed zone.

Alarm Zone and assigned readers can be armed/disarmed with card, PIN, input, function key and remote command. These methods are described in detail in AN027 Application note which is

available at www.roger.pl. The integration works in both directions which means that arming/disarming of Alarm Zone in RACS 5 results in arming/disarming of associated zone in alarm system while arming/disarming of zone in alarm system e.g. from its keypad results in arming/disarming of associated Alarm Zone in RACS 5 system.

In case of integration with Galaxy, arming/disarming can be initiated in RACS 5 only with functions which request arming/disarming. The concept of integration is such that RACS 5 system sends request to alarm system and if arming/disarming occurs in alarm system then based on a feedback it also occurs in RACS 5 system. Therefore in case of this integration, input functions [107]..[109] must be applied and functions [101]..[106] cannot be used. Consequently there is no need to use output functions as in hardware integration because in case of communication with Galaxy panels no outputs are used. All mentioned functions are listed and described in AN027 Application note which is available at www.roger.pl.

The image below presents exemplary settings in *Authentication Options* tab of Access point to enable arming/disarming by double card reading or PIN entering. In such case a user must be also assigned with Advanced Authorisation for function [109] as shown in AN027 Application note. At the same time, single card reading or PIN entering can still be used for access granting.



Configuration of communication between systems

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.

Add Communication Server

General

Name: Communication Server 1

IP Address: 192.168.11.13 Discovery

Port: 8890

Security Mode: Transport security with TLS 1.2

Server ID:

Synchronisation Schedule: (none)

Description:

Test OK 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 *Intruder Alarm Systems* select *Galaxy Dimension (HONEYWELL) 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 of VISO software double click *Galaxy Dimension Controller* and select *Add* in the opened window.
- In the next window enter such parameters as E080-08 module IP address, communication port (10005 is necessary), PIN i.e. Galaxy remote password (543210 by default), Galaxy account number, and Galaxy monitoring port. The option *Events collecting* does not concern state events i.e. [151000]..[151005] as they are always generated in VISO. Close the window with *OK* button.

Add Alarm Panel

General

Name: Galaxy Panel_1

IP Address: 192.168.21.23

Communication port: 10005

PIN:

Description:

Settings

Events collecting: ☒

Time synchronisation: ☒ Synchronisation Interval [min]: 30

Monitoring

Account no: 13

Monitoring port: 10010

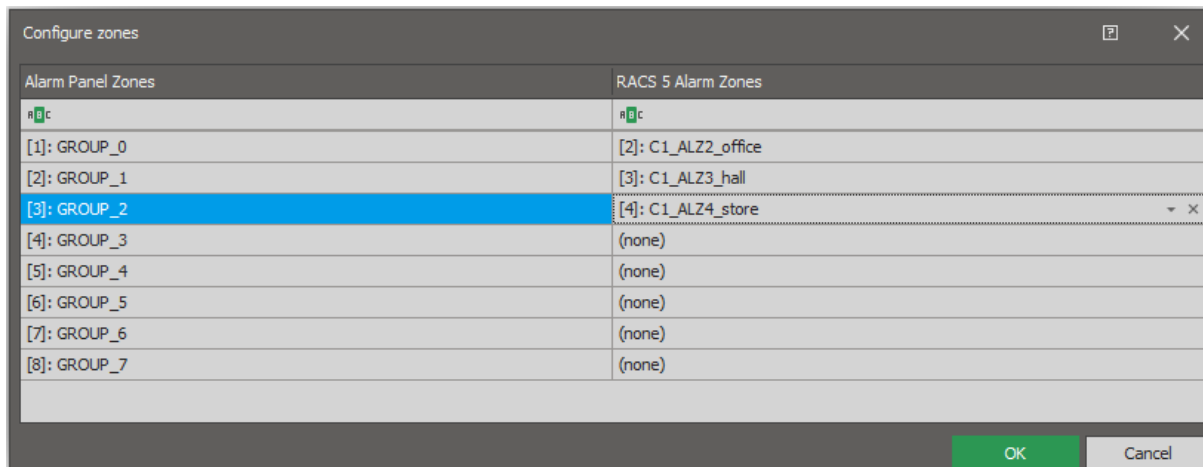
OK Cancel

- Select *Initialize* and then *Run* in the opened window to download Alarm Zones , inputs, outputs and users of Galaxy panel from previously indicated files. Close the window.

Note: If detection of Galaxy configuration fails then unblock TCP ports in the firewall of computer with Virtual Controllers Server. Following ports are used in the integration: 10001, 10002, 10005 and monitoring port which according to previous descriptions was set to 10010.

Note: If incorrect PIN is entered then the panel can disable the communication and it may be necessary to restart Galaxy panel by power supply switching off and on.

- Select *Configure zones* and in the opened window associate alarm zones of both systems. Alarm zones from both systems can be linked in 1:1 relation.



Additional information

The integration enables bidirectional arming and disarming of alarm zones in RACS 5 system and Integra intruder alarm system. All events generated by Integra are downloaded, displayed and recorded in RACS 5 database. Additionally events [151000]..[151005] are generated in VISO based on states detected in the Integra panel.

The integration can be used in VISO SMS which is system for monitoring and visualisation of security systems in a facility. More information on this subject is given in AN055 application note.

Arming and disarming

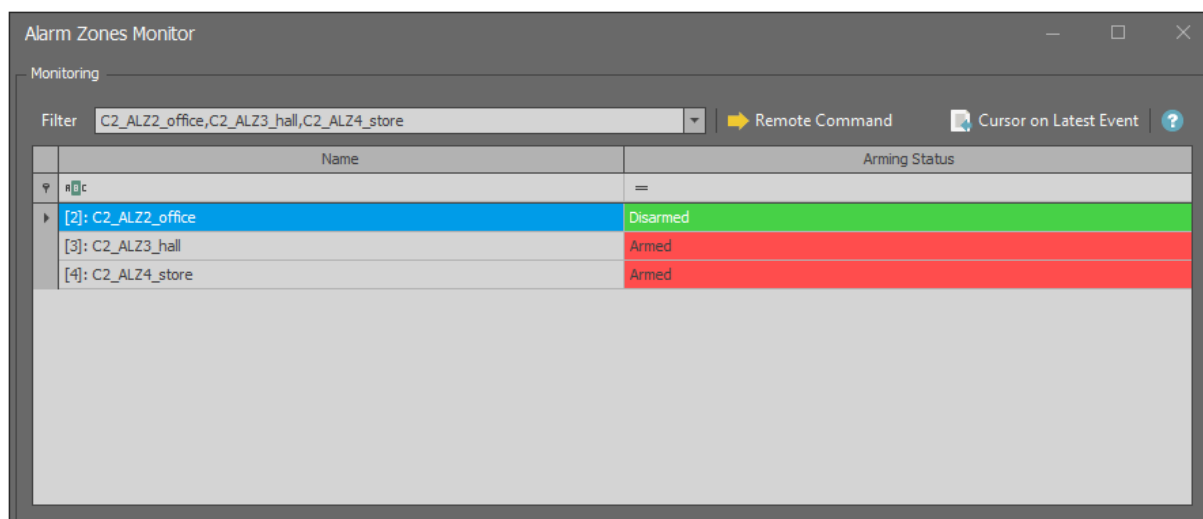
According to the description in AN027 application note, Alarm Zones in RACS 5 system can be armed and disarmed by means of Authentication Factors (card, PIN, etc.) on the level of Access Points (reader) and by means of Inputs, Function Keys and Remote Commands. The integration is bidirectional so Alarm Zones in both systems can also be armed and disarmed by means of Galaxy keypads and schedules.

Actions

When event is registered in RACS 5 software then actions can be started automatically. The action could among others consist in email or mobile text (SMS) sending. More information on actions is given in AN041 application note.

Alarm Zones Monitor

When *System Monitors* command in the top menu of VISO software is selected then Alarm Zones Monitor can be started. The monitor displays status list of Alarm Zones in RACS 5 and it can be used to remotely arm and disarm.



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