

# Roger Access Control System 5 v 2

Application note no. 039

Document version: Rev. A

## CompassPlus (OTIS) integration

Note: This document refers to RACS 5 v2.0.8 or higher

### *Introduction*

RACS 5 system enables software integration with CompassPlus elevator destination management system from OTIS company. The communication between both systems is provided in LAN and it requires installation and configuration of RACS 5 virtual controller. The integration is based on ICD v3 protocol from OTIS. The destination entry terminals (DEC) of elevator system can be equipped with OTIS readers or Roger readers connected to MC16 series controller. The integration requires VISO EX management software.

The integration enables centralized management of users and their access rights both on the level of RACS 5 doors and CompassPlus (OTIS) elevators. Particularly in case of elevators the integration enables to:

- Define Authorisations for selection floors and their sides (front, rear) by users on destination entry terminals (DEC).
- Define Authorisations for use of destination entry terminals (DEC) by users.
- Configure destination entry terminal operation mode (e.g. Default Floor)
- Define elevator call type for users (e.g. VIP, disability, etc.)
- Define default floor and side (front, rear) for users.
- Define allowed floors i.e. floors which can be selected by any user without identification.
- Register events related to users movement. Actions, notifications and other automatic reactions of RACS 5 system can be defined for such events.
- Monitor communication status with CompassPlus servers and terminals.

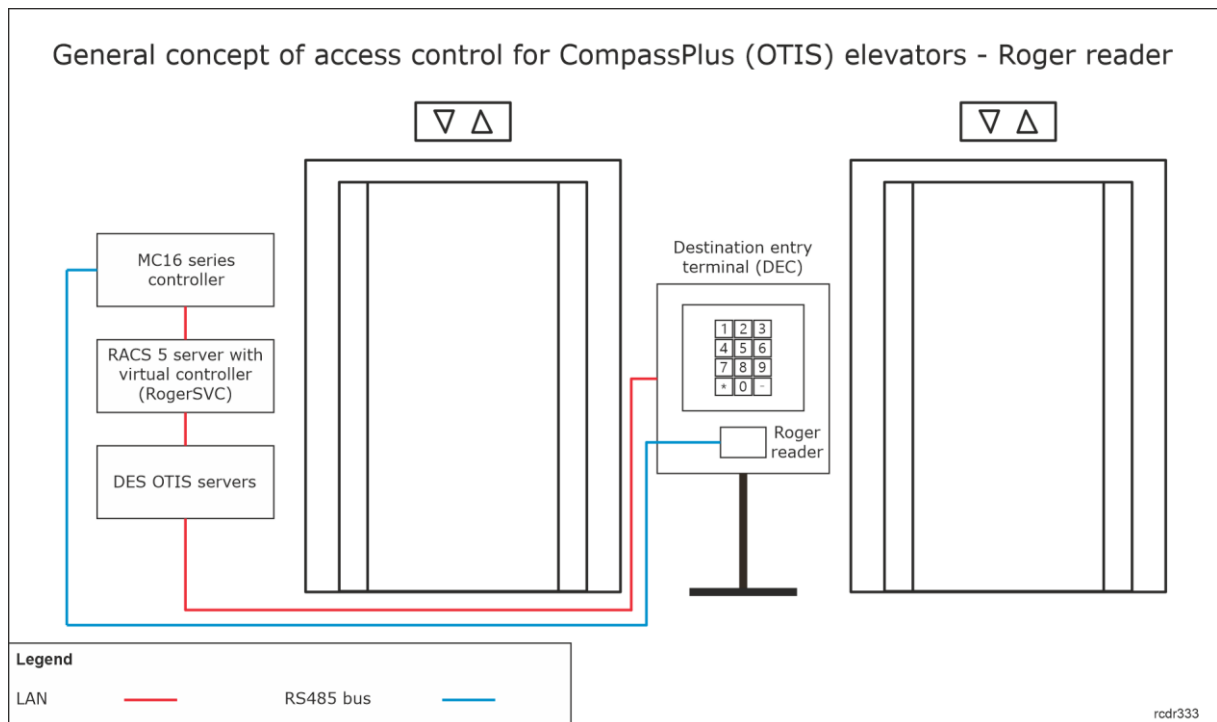
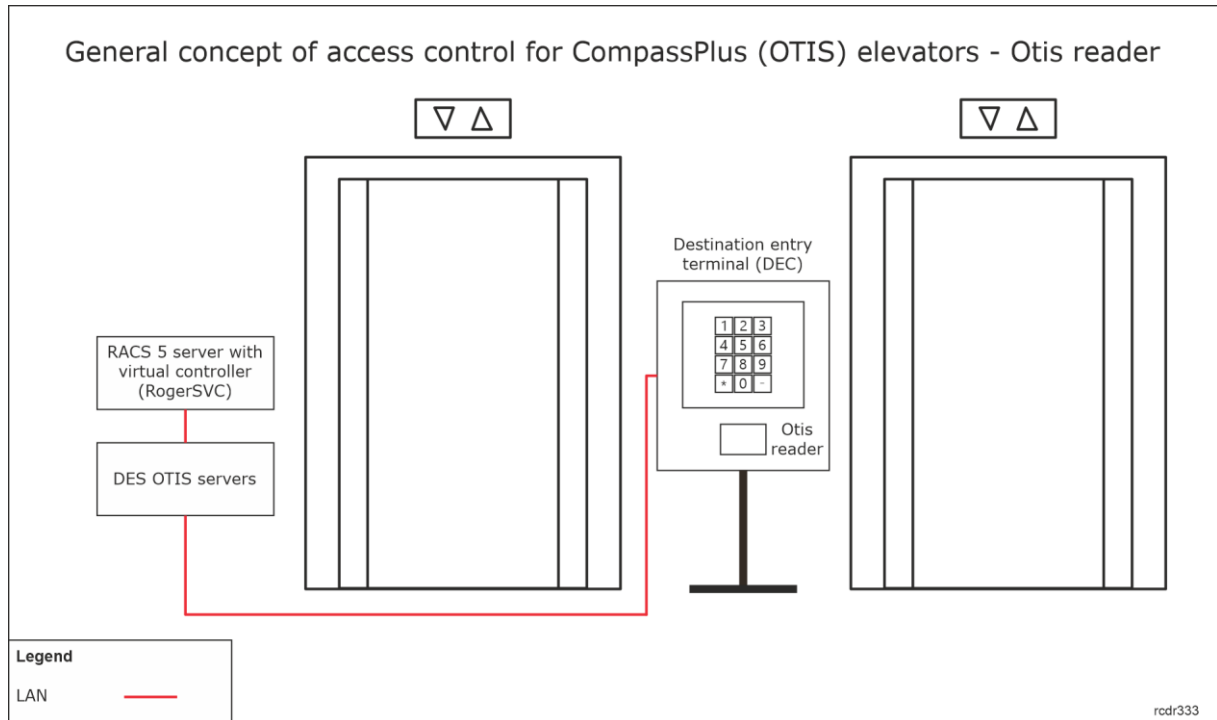
Authorisation can be limited to configurable period (e.g. 1 month) or it can be limited by weekly schedule (e.g. Mo-Fri 8am-4pm). In case of Schedules there can be configured Calendars to define exceptions on particular dates (e.g. holidays).

Depending on selected destination entry terminals (DEC) and internally installed readers, users can be indentified with various types of proximity cards (e.g. EM125kHz UNIQUE, Mifare, iClass, etc.), with PINs and in case of Roger readers also with mobile factors (BLE, NFC) and QR codes.

---

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.

---



### ***Configuration of CompassPlus elevators***

The installation and configuration of elevators is done by their supplier. Prior to configuration of the integration it is necessary to determine IP addresses of destination entry terminals (DEC). In the integration it is assumed that destination entry servers (DES) are configured with typical IP addresses, respectively 192.168.1.250 and 192.168.1.251.

### ***Preliminary configuration of RACS 5***


In order to conduct preliminary configuration of RACS 5:

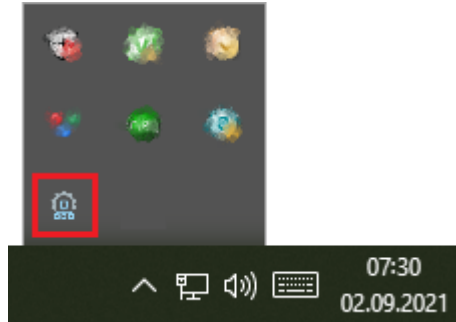
- Install VISO software and create database according to AN006 application note.
- Install RogerSVC software and select not only Communication Server but also License Server and Virtual Controllers Server. If servers are supposed to be operated on individual computers then install RogerSVC on each computer selecting required servers.

---

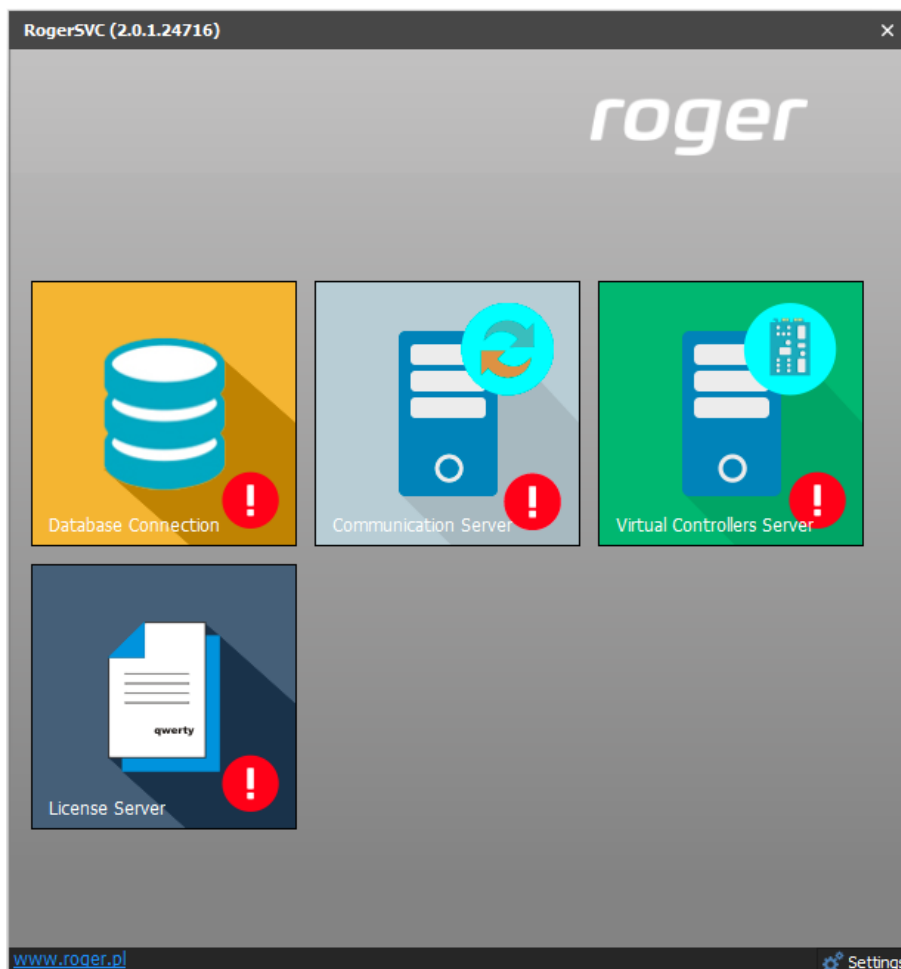
Note: If License Server and Virtual Controllers Server are supposed to be operated on individual computers then during installation of Virtual Controllers Server, the License Server must be deselected. Only in such case it will be possible to indicate external License Server when Virtual Controllers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

---

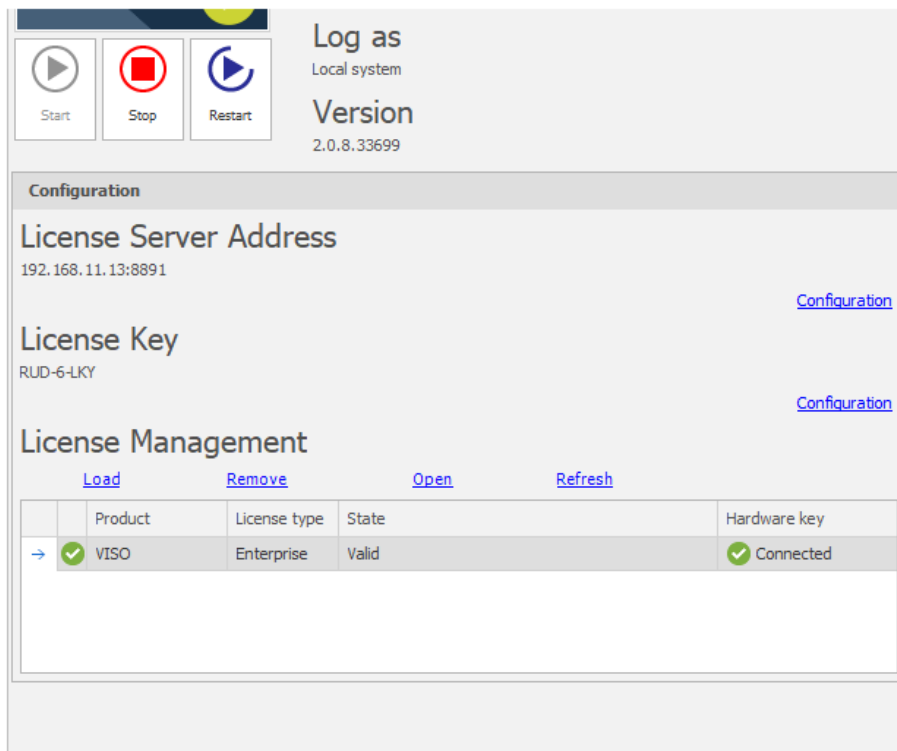
- When RogerSVC is launched then its icon is displayed in Windows tray. Click the icon . The RogerSVC icon in tray can also be launched from Windows menu *Start -> Roger -> RogerSVC*.



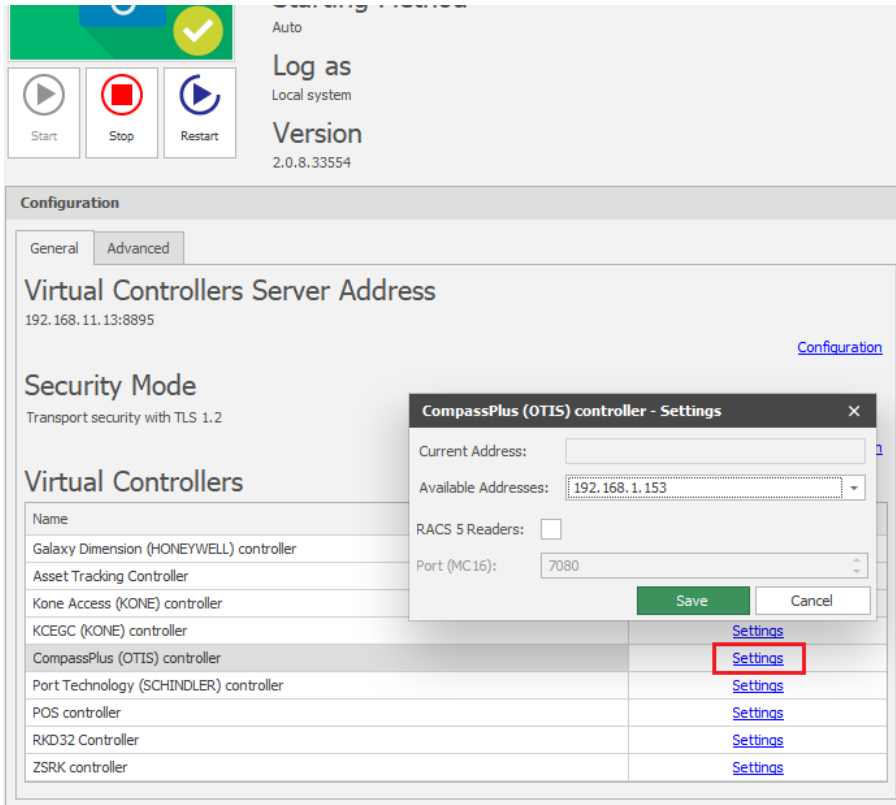
- In the RogerSVC window select *Database Connection* tile and then *Configuration* to indicate previously created RACS 5 database. Return to the main window.



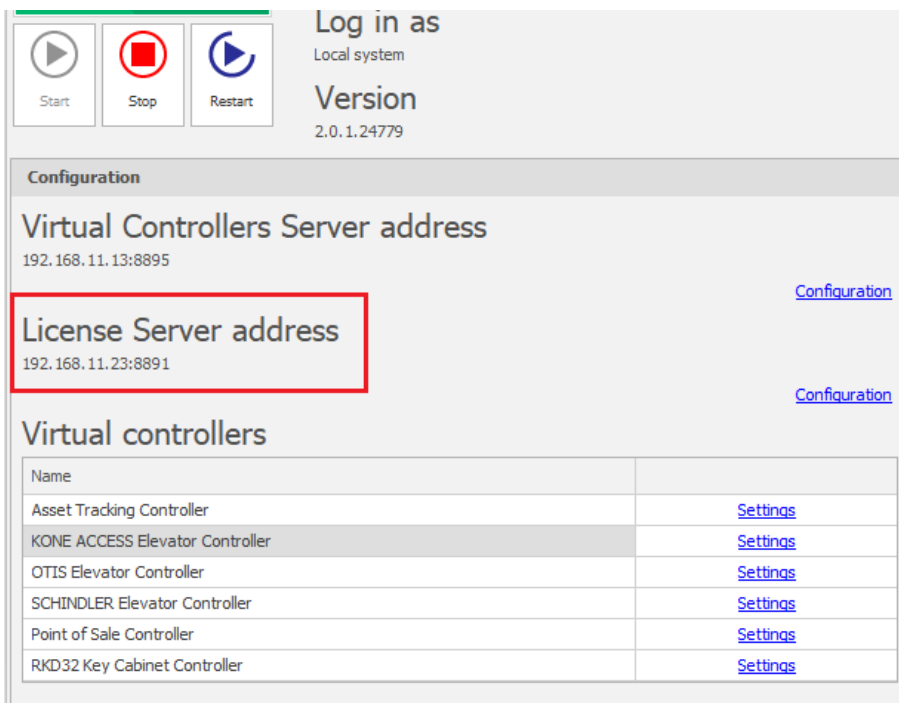
- In the RogerSVC window select *Communication Server*, click *Configuration*, enter IP address of the computer with the server installed e.g. 192.168.11.13 and define port (8890 by default).
- Select *Start* and return to the main window. The server will be started and operated in the background whenever the computer is switched on even if RogerSVC window is closed.
- 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).
- Connect RUD-6-LKY hardware key to USB port of computer with License Server installed or connect RLK-1 hardware key to LAN and define its IP address in RogerSVC.
- Select *Load license file* and indicate purchased license file for the hardware key.
- Select *Start* and return to the main window. The server will be started and operated in the background whenever the computer is switched on even if RogerSVC window is closed.



- In the RogerSVC window select *Virtual Controllers Server* tile, click *Configuration*, enter IP address of the computer with the server installed (e.g. 192.168.11.13) and define port (8895 by default).
- If there are two network adapters on the server with virtual controller installed e.g. one for communication with VISO software and MC16 controllers and another one for communication with OTIS servers then two communication channels can be applied. In the example below the communication with OTIS servers is done via network adapter with 192.168.1.153 IP address. Additionally if Roger readers are supposed to be used instead of Otis readers then enable the option *RACS 5 Readers*.



- If contrary to previously presented configuration steps, the License Server is installed on a computer with exemplary 192.168.11.23 address while Virtual Controllers Server is installed on computer with exemplary 192.168.11.13 address then it is possible to indicate external License Server for virtual controllers as below.



- Select *Start* and return to the main window. The server will be started and operated in the background whenever the computer is switched on even if RogerSVC window is closed.

- Start VISO software, in the top menu select *System*, then *Select License Server* and indicate previously defined License Server from RogerSVC software in order to start the VISO program in licensed version.

### ***Additional low level configuration of MC16 controller***

If Roger readers are supposed to be used instead of Otis readers then it is necessary to make additional low level configuration of each MC16 controller using its memory card. Therefore:

- Switch off the power supply of MC16 controller.
- Press memory card and remove it from the socket under CR2032 battery on controller's board.
- Insert card into standard Flash memory card reader and connect it to computer's USB port.
- Add following exemplary settings to DEBUG.CFG file:

```
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)

### ***Connection with CompassPlus system***

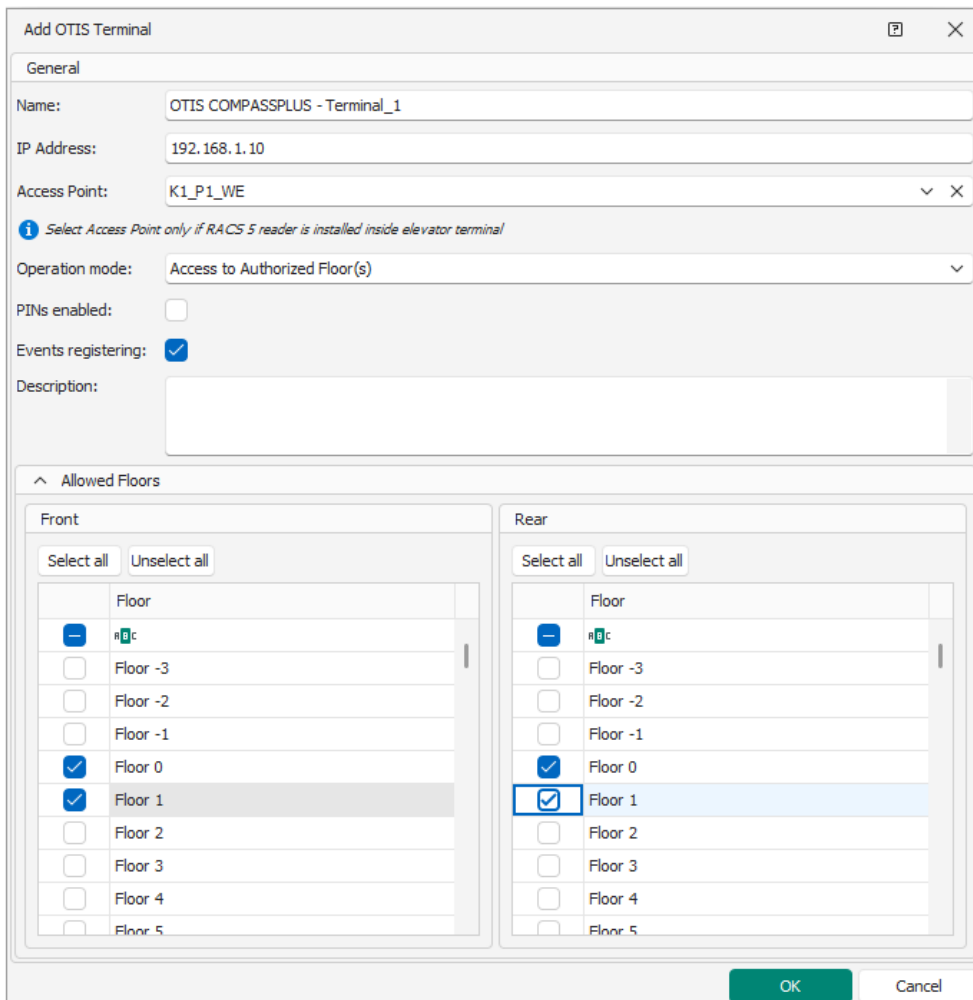
In order to configure virtual controller:

- 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 Roger readers are supposed to be installed instead of Otis readers then for each Roger reader which is mounted inside DEC and connected to MC16 controller it is necessary to create Access Point expanding the controller in the navigation tree of VISO software then double clicking *Access Points* and selecting *Add*. When Access Point is created then select *Access Terminals* tab in the bottom, select *Add* and indicate physical reader for 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 *CompassPlus (OTIS) 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.
- Expand the controller in the navigation tree and double click *Floors*. When the virtual controller is created then all possible floors are automatically created. In order to make system configuration more clear and simple it is recommended to remove floors which actually do not exist in the building. When *SHIFT* key is used then multiple floors can be selected and removed at once.
- In the navigation tree double click *Terminals* and then *Add* to define DEC in VISO software.
- In the next window name the terminal, enter IP address, select operation mode and indicate allowed floors i.e. floors which can be selected by everyone on the terminal (DEC) as they would not require Authorisation. If Roger readers are supposed to be installed instead of Otis readers then additionally indicate Access Point i.e. reader installed inside DEC. If needed, enable PINs for users on this terminal.



The terminal can be operated in following operation modes which are explained in detail in OTIS documentation:

Default Floor – in this mode user selects allowed floor or authorized floor. In the second case, proximity card or PIN must be used so the system could verify user access to selected floor. Alternatively a user in the first step can use proximity card or PIN instead of selecting a floor and

then default floor will be automatically selected for the user by the system. In such case a user must be assigned with default floor and with Authorisation for this floor.

Access to Authorized Floors(s) – in this mode user must swipe card or enter PIN. Then floor can be selected and the system will verify if it is allowed floor or authorized floor. In this mode, default floor cannot be selected automatically.

User Entry of Destination Floor – this mode works in the same way as Default floor but it is not possible to use card or PIN in the first step for automatic selection of default floor.

Default Floor or User Entry of Destination Floor – in this mode user must use card or PIN and wait till default floor is selected automatically by the system on condition the user is assigned with such floor and assigned with Authorisation for such floor. Before the default floor is selected automatically the user can override this selection and select floor manually. The system will verify if allowed or authorized floor is selected manually. The time for manual selection of floor is defined during configuration of CompassPlus system and it usually equals to a few seconds.

- Configure remaining destination entry terminals (DEC), which are installed in the CompassPlus system.

---

Note: All settings related to virtual controllers including users and their Authorisation do not require manual synchronisation by VISO operator. They are applied within a few seconds when entered.

---

## ***Authorisations***

In order to define Authorisations for floors in CompassPlus system:

- 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 [70150]. If the Authorisation is supposed to allow access to all floors on both sides (front, rear) and from all destination entry terminals (DEC) then select the option *Includes authorisations for all rules*. Close the window with *OK* button.



- In the bottom select *Positive Rules* tab and then *Add*.
- In the opened window select *Object* as *Type*, *Specified as Range* and specific floor as *Value*. This rule will allow to select floor 1 from all destination entry terminals (DEC). 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 floor and there can also be defined collective Authorisation for multiple floors 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 common doors and floors can be assigned.

---

Details

Main Negative Rules Positive Rules Access Credentials Access Persons Assets

+ Add Edit Select All Delete Refresh Report

	Type	Value	Time Range	Enabled
13	Object	Floor (OTIS) 1	Schedule Mo-Fri 8am-4pm	<input checked="" type="checkbox"/>
14	Object	Floor (OTIS) 2	Schedule Mo-Fri 8am-4pm	<input checked="" type="checkbox"/>
15	Object	Floor (OTIS) 3	Schedule Mo-Fri 8am-4pm	<input checked="" type="checkbox"/>
	Access Point	All	Always	<input checked="" type="checkbox"/>
	Function Parameter	All	Always	<input checked="" type="checkbox"/>

- 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 entry terminals (DEC). 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.

Add Rule

General

Enabled:

Type: Access Point

When

Time Range: Always

Schedule:

Where

Range: Specified

Type: OTIS Terminal

Value: OTIS Terminal\_1

OK Cancel

Details

Main Negative Rules Positive Rules Access Credentials Access Persons Assets

+ Add Edit Select All Delete Refresh Report

	Type	Value	Time Range	Enabled
13	Object	Floor (OTIS) 1	Schedule Mo-Fri 8am-4pm	<input checked="" type="checkbox"/>
14	Object	Floor (OTIS) 2	Schedule Mo-Fri 8am-4pm	<input checked="" type="checkbox"/>
15	Object	Floor (OTIS) 3	Schedule Mo-Fri 8am-4pm	<input checked="" type="checkbox"/>
16	Access Point	OTIS Terminal_1	Always	<input checked="" type="checkbox"/>
	Function Parameter	All	Always	<input checked="" type="checkbox"/>

- 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 floor side (front, rear). Similarly as in case of Object type rule the Function Parameter type rule can be limited in time.

Add Rule

General

Enabled:

Type: Function Parameter

When

Time Range: Always

Schedule:

Where

Range: Specified

Type: Door side

Value: Front

OK Cancel

Details

Main Negative Rules Positive Rules Access Credentials Access Persons Assets

+ Add Edit Select All Delete Refresh Report

	Type	Value	Time Range	Enabled
13	Object	Floor (OTIS) 1	Schedule Mo-Fri 8am-4pm	<input checked="" type="checkbox"/>
14	Object	Floor (OTIS) 2	Schedule Mo-Fri 8am-4pm	<input checked="" type="checkbox"/>
15	Object	Floor (OTIS) 3	Schedule Mo-Fri 8am-4pm	<input checked="" type="checkbox"/>
16	Access Point	OTIS Terminal_1	Always	<input checked="" type="checkbox"/>
17	Function Parameter	Front	Always	<input checked="" type="checkbox"/>

### 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 elevators the wizard enables to:

- Define validity period e.g. 1 month for user’s Access Credential.
- Define default floor and default side.
- Define elevator call type e.g. VIP (all call types are explained in CompassPlus system manuals).
- Assign Authorisation Groups and Authorisations.
- Define Authentication Factors (cards, PINs).

Add Access User Person Online

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

Steps

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

General

Name: Access Credential\_4\_Madrid Derrick

Group: None

Valid from: None 12:00 AM

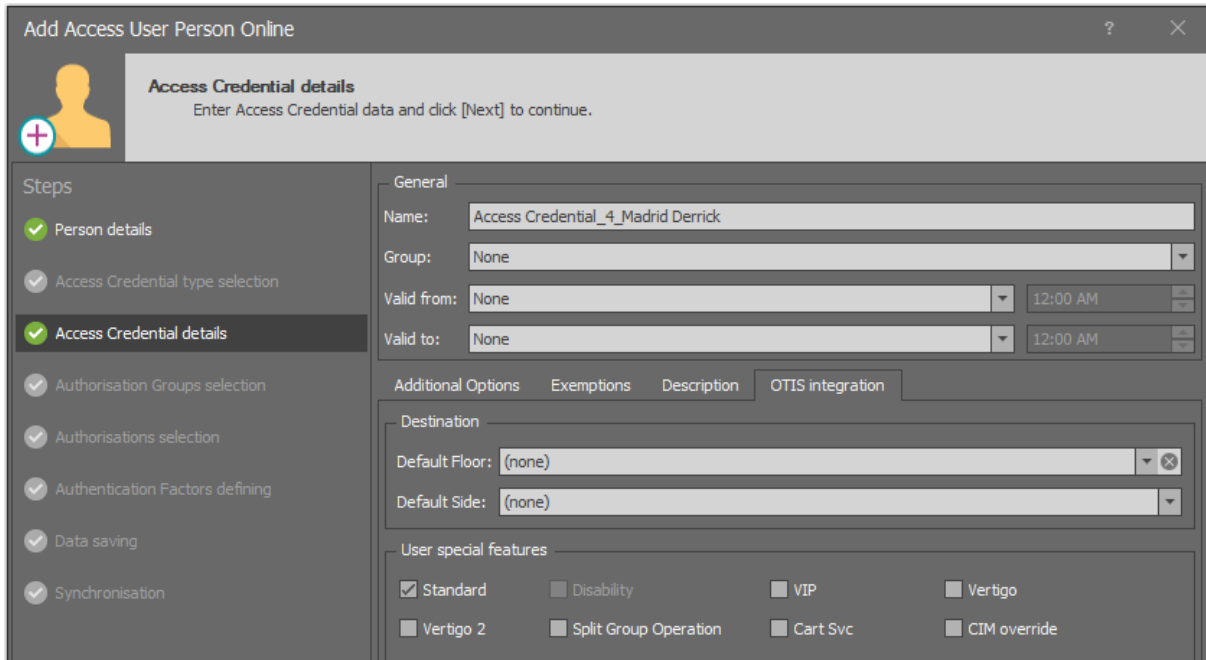
Valid to: None 12:00 AM

Additional Options Exemptions Description OTIS integration

Status: Active

Thread Level: 1

Elevator Call Type: 0

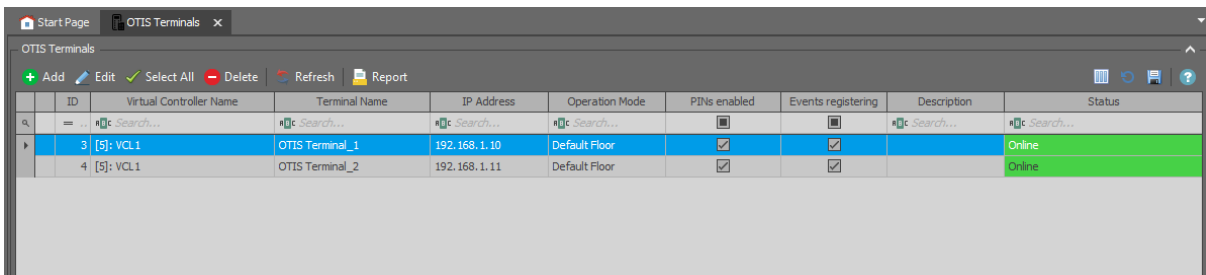


### Monitoring

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 *Events Monitor*. In both cases events can be filtered.

### Communication

The communication with servers and terminals of CompassPlus system is monitored and events are generated both for lost and restored communication. Additionally, current status of connection with destination entry terminals (DEC) is presented on the list of terminals in VISO software. Lost connection is reported within a few seconds from its occurring.



### Users

RACS 5 system registers events related to access granting and access denying when floor is selected. For obvious reasons events are registered only when user is identified with proximity card or PIN. Additional information on elevator related events is available in event details.

The screenshot displays the VISO software interface for viewing event logs. The top part is a table listing events, and the bottom part is a detailed view of a specific event.

Time and Date	Event	Controller	Location	Source	Access User Person	Option
12/20/2019 12:...	Access granted (OTIS elevator)	VCL1	[1148]: Floor (OTIS) 4	[4]: Access Credential_4_M...	Madrid Derrick	Przód
12/20/2019 12:...	Access granted (OTIS elevator)	VCL1	[1148]: Floor (OTIS) 4	[4]: Access Credential_4_M...	Madrid Derrick	Przód
12/20/2019 12:...	Authentication Factor Read	VCL1	[3]: OTIS Terminal_1	[4]: Access Credential_4_M...	Madrid Derrick	Przód
12/20/2019 12:...	Authentication Factor Read	VCL1	[3]: OTIS Terminal_1	[4]: Access Credential_4_M...	Madrid Derrick	Przód
12/20/2019 12:...	Access granted (OTIS elevator)	VCL1	[1148]: Floor (OTIS) 4	[4]: Access Credential_4_M...	Madrid Derrick	Przód
12/20/2019 12:...	Access granted (OTIS elevator)	VCL1	[1148]: Floor (OTIS) 4	[4]: Access Credential_4_M...	Madrid Derrick	Przód
12/20/2019 12:...	Access denied (OTIS elevator)	VCL1	[1148]: Floor (OTIS) 4	[4]: Access Credential_4_M...	Madrid Derrick	Przód
12/20/2019 12:...	Access denied (OTIS elevator)	VCL1	[1148]: Floor (OTIS) 4	[4]: Access Credential_4_M...	Madrid Derrick	Przód
12/20/2019 12:...	Authentication Factor Read	VCL1	[3]: OTIS Terminal_1	[4]: Access Credential_4_M...	Madrid Derrick	Przód
12/20/2019 12:...	Access denied (OTIS elevator)	VCL1	[1148]: Floor (OTIS) 4	[4]: Access Credential_4_M...	Madrid Derrick	Przód

The details view for the selected event shows the following information:

- Event: [70000]: Access granted (OTIS elevator)
- Time (UTC): 12/20/2019 11:35:18
- Event ID: 176
- Action status: OK
- Severity: Medium
- Category:
- Function: Call Elevator
- Details: Group ID: 1, Car ID: 8, Direction designation: 315
- Description: Access granted (OTIS elevator)
- Network: None
- Controller: VCL1
- Location: [1148]: Floor (OTIS) 4
- Source Type:
- Source: [4]: Access Credential\_4\_Madrid Derrick
- Access User Person: Madrid Derrick
- Asset: None
- Group: None
- Comment:

## 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](mailto:support@roger.pl)**  
**Web: [www.roger.pl](http://www.roger.pl)**