BKT Elektronik - Headquarter
Poland, Lochowska 69 Str.
86-005 Biale Blota
Phone: +48 52 36 36 750
e-mail: export@bkte.pl

BKT ACBS

Access Control Bus System

- the access control system with RS485 bus interface

- installation and configuration manual
- version 7

Table of contents

1 INTRODUCTION

1.1 General information

The specification is owned and copyrighted by BKT Elektronik Sp. z o.o. Information contained herein may be changed at owner's discretion without any notice. BKT Elektronik may not be held liable for any possible inaccuracies and discrepancies in this document.

1.2 System characteristics

The access control system is designed to limit the access of unauthorized persons to sensitive parts of data centers, smaller server rooms, as well as to individual cabinets. BKT ACS (Access Control System) is a scalable access control system dedicated to 19'' frames. BKT Elektronik offers cabinets that are factory-adapted to the installation of an access control system. These cabinets have doors equipped with appropriate openings for mounting card readers and cable paths for arranging the wires. The BKT ACS system can also be applied to any teleinformation cabinets with a 19'' frame. It is then required to make appropriate openings in the door for card readers and to fasten the cables with, for example, cable ties. The BKT ACBS access control system (Access Control Bus System) uses devices (controllers and readers) that communicate using the RS485 bus. The controllers are placed in 1U casings adapted to be mounted in 19'' cabinets. A single controller, depending on the version, can supervise the operation of up to 16 doors. The number of controllers in the system is unlimited. In the same system, it is also possible to connect controllers supporting readers with Wiegand interface - BKT ACWS system (Access Control Wiegand System). Both systems use Roger RACS5 devices. This manual contains basic information sufficient to run the BKT ACBS access control system. More technical information about the devices used in the system can be found at www.roger.pl/en.

1.3 Basic system functionality

- Supports unlimited number of cabinets.
- Supports unlimited number of users, subject to a maximum of 8192 per controller.
- Supports different card standards depending on the reader used.
- The system may grant access to the door by presenting a card or entering a PIN code (or may require both actions at the same time). It is also possible to configure the so-called committee entry when two users have to present cards to open the door.
- Depending on the system, the readers may have an integrated keypad (BKT ACBS) or may be integrated in a cabinet handle (BKT ACWS). It is also possible to use any reader with a Wiegand interface.
- Archiving of events in the MS SQL Server/Express.
- Stand-alone operation of the system - without connection to a computer with a database. In such situation, up to 8 million events can be saved to the controller's internal memory, which will be sent to the computer during the next connection.
- Independent monitoring of the door status and the status of the handle.
- Free VISO ST application for system configuration and monitoring.
- Encrypted communication on the Ethernet network and on the RS485 bus.
- Email notifications about any chosen event.
- The system devices meet the requirements of security Grade 2 according to the EN 60839-11-1: 2013 standard
- The devices are adapted to be mounted in a 19'' frame. They are 1U high.
- Ease and speed of making connections thanks to the use of RJ45 connectors.
- BKT 4DC cabinets are available in a version adapted to the installation of access control devices. They have appropriate openings for the reader and dedicated cable paths on the door.

2 BKT ACBS and BKT ACWS SYSTEMS

The BKT ACS access control system is available in two variants:

- BKT ACBS (Access Control Bus System) - system based on the RS485 bus, which is used by controller to communicate with card readers.
- BKT ACWS (Access Control Wiegand System) - system that uses the Wiegand interface for communication between the controller and card readers.

Both versions use the same Roger MC16-PAC controller, so they can work in the same system managed by the same VISO ST application. The table below lists the main differences between the system variants.

	System structure	Interface between the controller and the reader	Supported standard of proximity cards	Possibility of connecting a handle with an integrated reader - AL301	Possibility of connecting any third party reader with Wiegand interface	1 controller (1 IP address) for many cabinet doors
BKT ACBS Bus System		RS485 bus	UNIQUE 125kHz or Mifare 13,56MHz (Ultralight and Classic)			Max 16 cabinet doors 
BKT ACWS System with Wiegand interface		Wiegand	Any standard dependent on the reader			Max 2 cabinet doors 

3 BKT ACBS SYSTEM COMPONENTS

3.1 AC100 controller

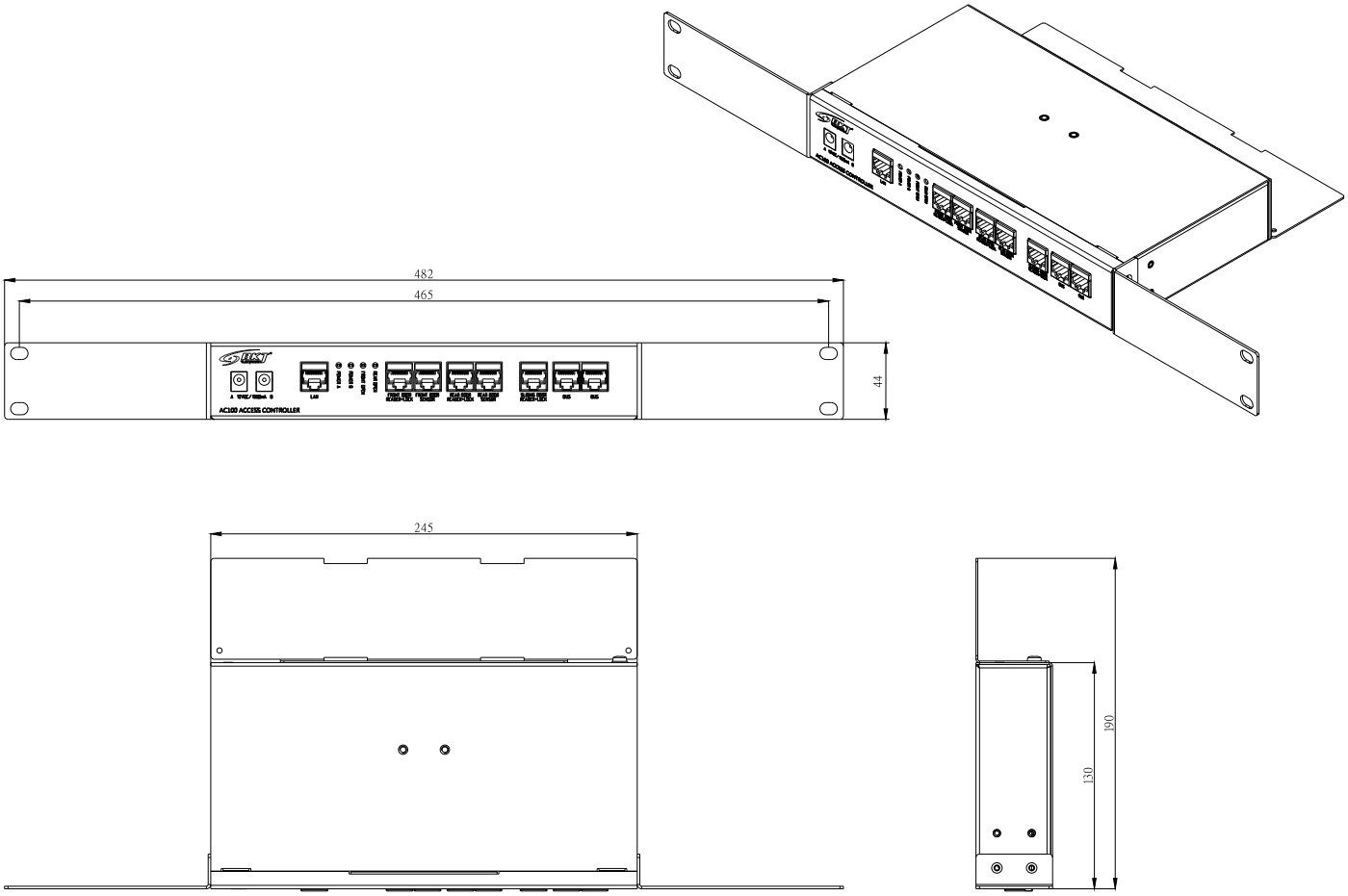
AC100 - Access controller in 1U 19'' enclosure, no power supply unit (122AA100015), no controller pcb (122AC102xxx). Designed to support readers with RS485 interface.

- The controller is the basic device of the system.
- Requires the Roger MC16-PAC-ST-x controller pcb. Depending on the used PCB of the controller, it can support from 1 door (MC16 PAC-ST-1) to 16 doors (MC16-PAC-ST-16)
- The controller has a 1U casing, adapted to be mounted in a 19'' cabinet.
- The number of controllers in the system is unlimited.
- The controller enables connection of two door sensors, two door readers, an additional reader for cold/hot aisle containment sliding door, LAN network and RS485 bus connecting slave sets. All connections to the controller are made with cables with RJ45 connectors.
- The controller has two configurable LEDs, which for example, can indicate the status of the front and rear doors of the cabinet.
- Two-way power supply possible.
- Requires one or two 12VDC 1.5A power supplies.

3.1.1 Technical data

Parameter	Value
Power supply voltage	Nominal 12V DC, allowed 12-15V DC
Average current consumption (with controller pcb and no external devices)	110 mA
Connectors	8 x RJ45 (for peripheries), 2 x DC 5,5/2,1 (for power supplies)
Dimensions	482 x 132 x 44mm (W x D x H)
Weight	1100g
Package dimensions	265 x 165 x 70mm
Package weight	1200g
Operating conditions	Temperature: 5°C - 40°C, Humidity: 10% - 95% RH (no condensation)
Storage conditions	Temperature: 0°C - 60°C, Humidity: 0% - 95% RH (no condensation)
Housing material	Steel
Housing colour	Black, RAL 9005
Housing protection rating	IP20
Compliance with directives	2014/35/EU (LVD), 2011/65/EU (RoHS)
Part number	122AC001000

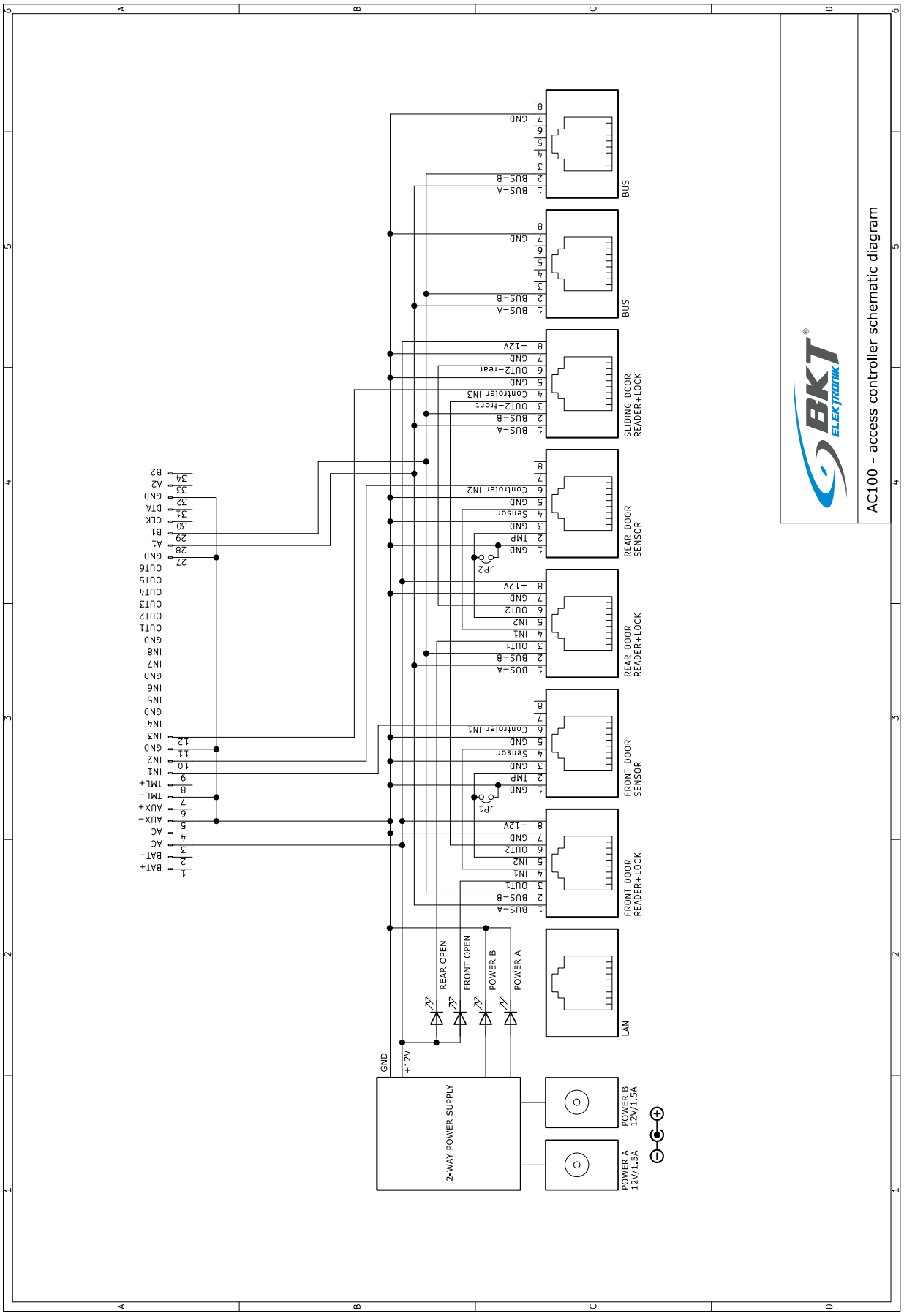
3.1.2 Dimensions



3.1.3 AC100 controller accessories

Product	Description	Part number
	MC16-PAC-ST-x - x door controller RACS5	122AC1021xx
	GST18A12-P1J - Power supply 18W 12VDC 1.5A; AC socket C14; DC plug 5.5/2.1; no AC cord	122AA100015
	Power cord, plug IEC 320 C13 10A, plug DIN 49441(unischuko) 16A, 3x1,0 mm2, black, 2m	11480784.2
	Power cord, plug IEC 320 C13 10A, plug IEC 320 C14 10A, 3x1,0 mm2 black, 2m	11480785.2

3.1.4 Controller wiring schematic



3.2 AB101 secondary set

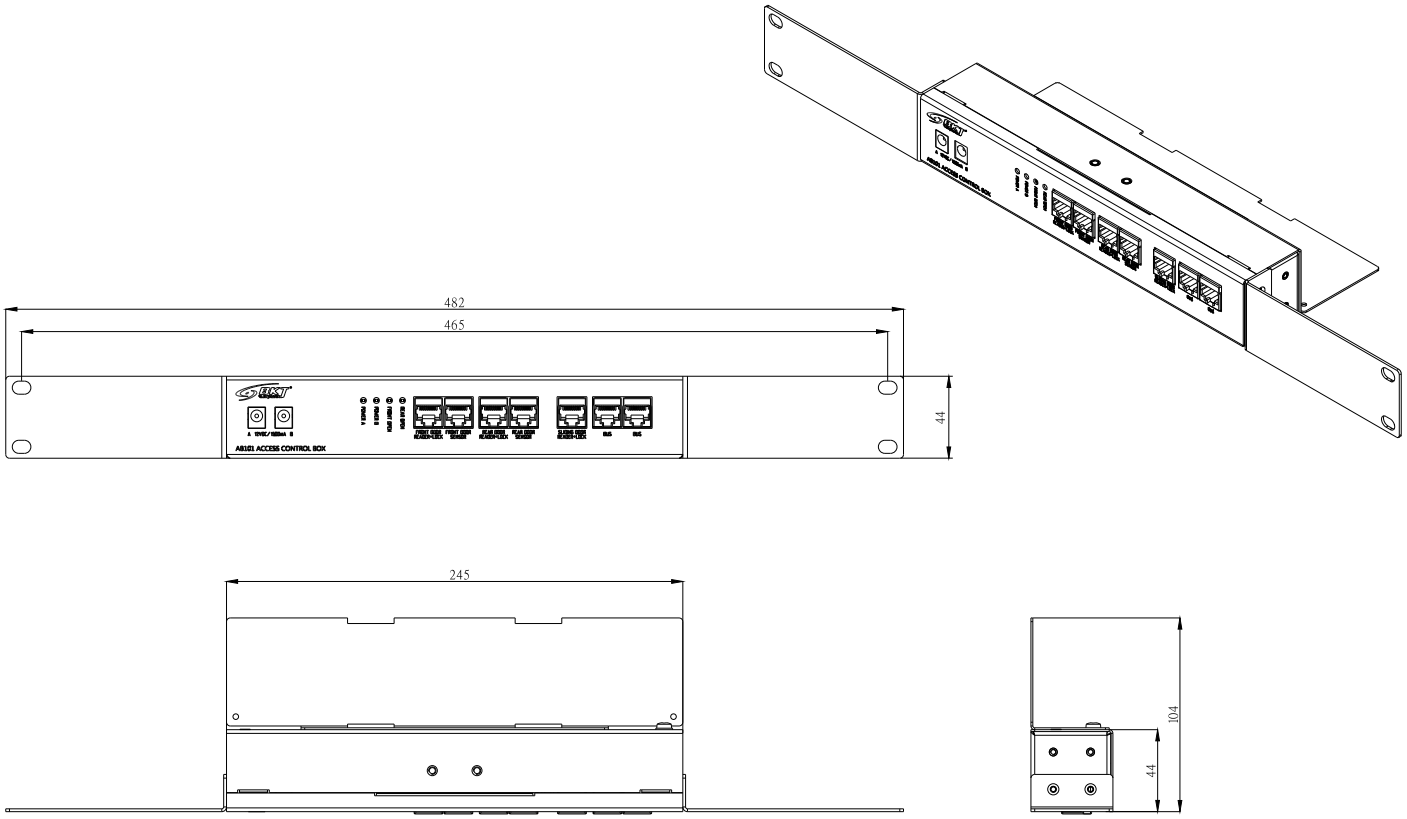
AB101 - Access control secondary set for 2 doors in 1U 19'' enclosure, no power supply unit (122AA100015). Works with the AC100 controller.

- The kit includes a connection system for devices for handling 2 doors.
- It has a 1U housing, suitable for mounting in a 19 "rack.
- The set works only with controller AC100.
- Designed for installation in subsequent cabinets.
- It enables connection of two door sensors, two door readers and an additional reader for cold/hot aisle containment sliding door, LAN network and RS485 bus connecting slave sets. All connections to the controller are made with cables with RJ45 connectors
- The controller has two configurable LEDs, which for example, can indicate the status of the front and rear doors of the cabinet.
- Two-way power supply possible.
- Requires one or two 12VDC 1.5A power supplies.

3.2.1 Technical data

Parameter	Value
Power supply voltage	Nominal 12V DC, allowed 12-15V DC
Average current consumption (with no external devices)	10 mA
Connectors	7 x RJ45 (for peripheries), 2 x DC 5,5/2,1 (for power supplies)
Dimensions	482 x 44 x 44mm (W x D x H)
Weight	800g
Package dimensions	265 x 165 x 70mm
Package weight	900g
Operating conditions	Temperature: 5°C - 40°C, Humidity: 10% - 95% RH (no condensation)
Storage conditions	Temperature: 0°C - 60°C, Humidity: 0% - 95% RH (no condensation)
Housing material	Steel
Housing colour	Black, RAL 9005
Housing protection rating	IP20
Compliance with directives	2014/35/EU (LVD), 2011/65/EU (RoHS)
Part number	122AB001011

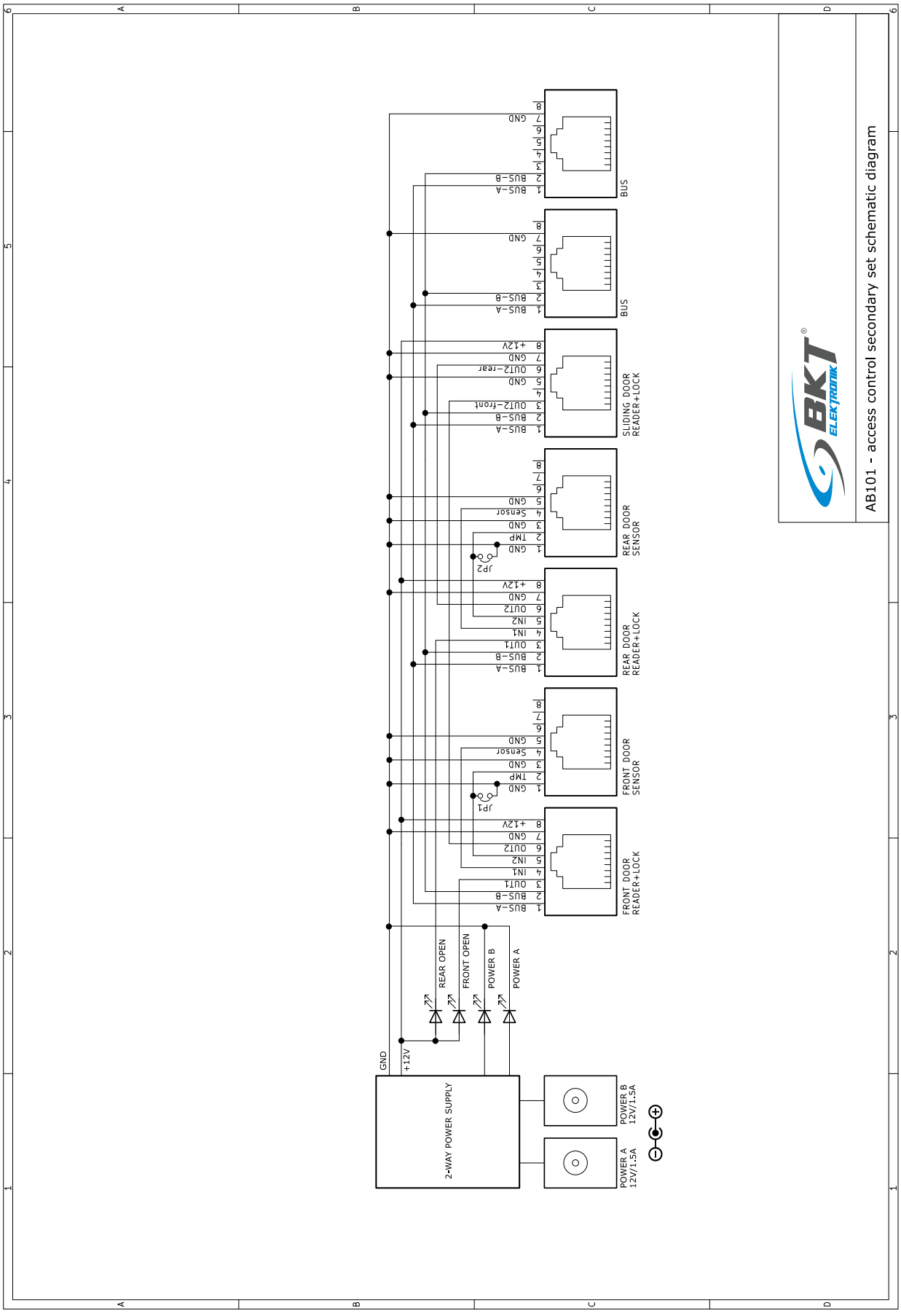
3.2.2 Dimensions



3.2.3 AB101 secondary set accessories

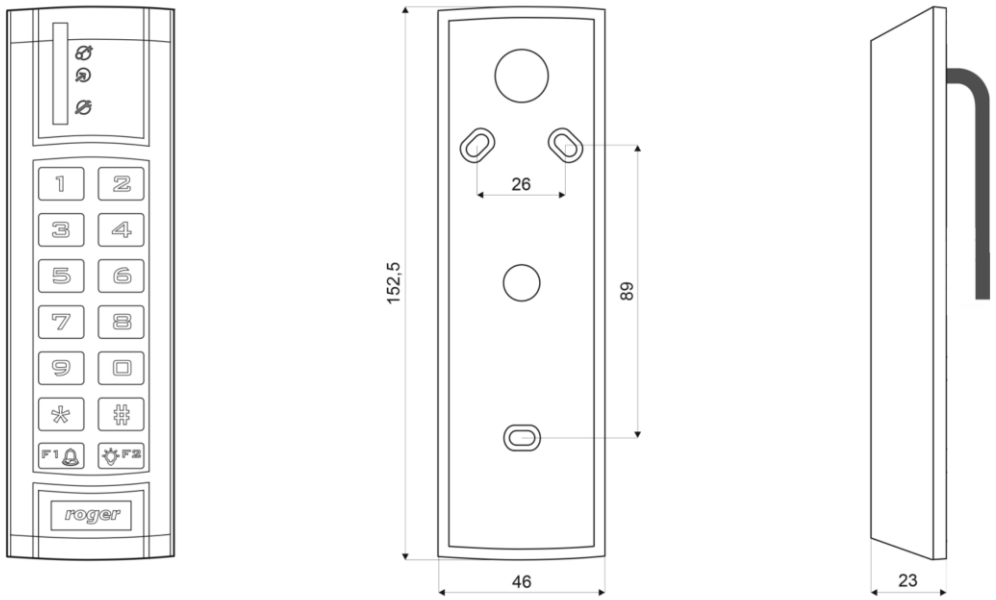
Product	Description	Part number
	GST18A12-P1J - Power supply 18W 12VDC 1.5A; AC socket C14; DC plug 5.5/2.1; no AC cord	122AA100015
	Power cord, plug IEC 320 C13 10A, plug DIN 49441(unischuko) 16A, 3x1,0 mm2, black, 2m	11480784.2
	Power cord, plug IEC 320 C13 10A, plug IEC 320 C14 10A, 3x1,0 mm2 black, 2m	11480785.2

3.2.4 Secondary set wiring



3.3 Card readers

3.3.1 Dimensions



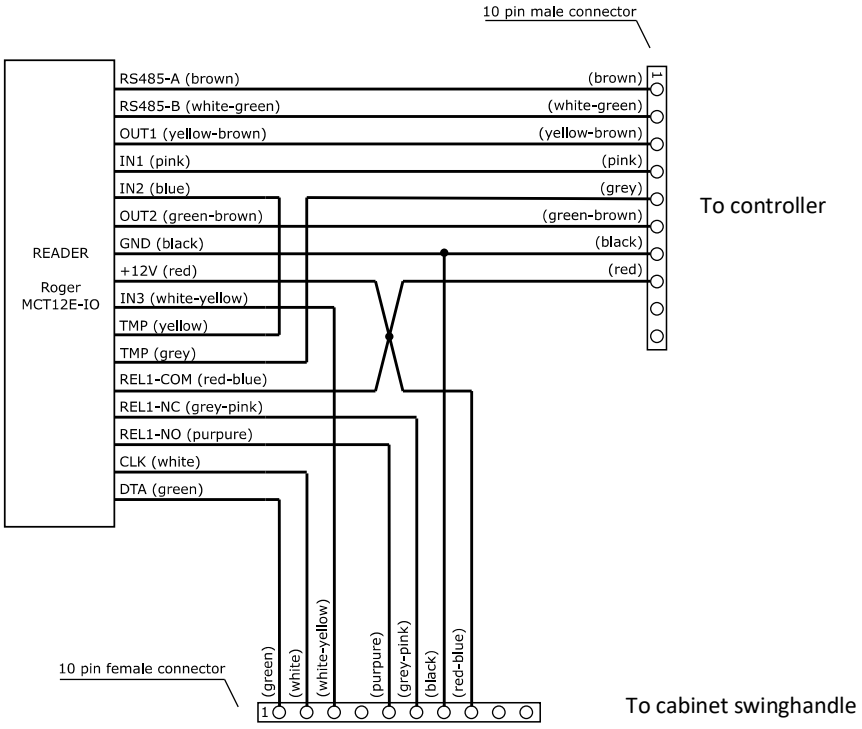
3.3.2 Card reader accessories

Product	Description	Part number
	**AW111** – Reader to controller connection cable, 5m • The cable is used to connect the reader AR121, AR122, AR131, AR132 to AC100 controller or AB101 secondary set. • Length: 5m, terminated with RJ45 and 10-pin female connectors.	244AW001110
	**AW113 -** Reader to housing sliding door controller connection cable, 5m • The cable is used to connect the reader AR122, AR132 to sliding door controller • Length: 5m, terminated with RJ45 and 10-pin male connectors.	244AW001130
	Electrical junction box 86mm x 86mm x 39mm, wall mount, black, IP55	122AA100006
	**RUD-1** - USB-RS485 interface/programmer	122AA101000
	**EMC-1** - UNIQUE EM 125 kHz thin proximity card	122AA101004
	**MFC-2** - MIFARE Classic 1k 13.56 MHz thin proximity card	122AA101011

3.3.3 AR121 Unique card reader with keypad

Product	Description	Part number
	**AR121** (MCT12E-IO) – Unique 125kHz card reader with keypad for cabinet door • Roger MCT12E-IO reader was used • Reader adapted to control the cabinet door. It has a 15cm long cable terminated with multi-pin connectors to connect to the lock and cabinet controller. • It reads EM Unique 125kHz proximity cards, reading range up to 7 cm. • Three LED indicators, buzzer with adjustable sound level, keyboard with backlight, two function buttons, detection of housing opening and detachment from the surface. • 12V, 50mA power supply from a controller or a slave set. • Dimensions: 153 x 46 x 23 (HxWxD) • More information can be found at www.roger.pl	244AR001210

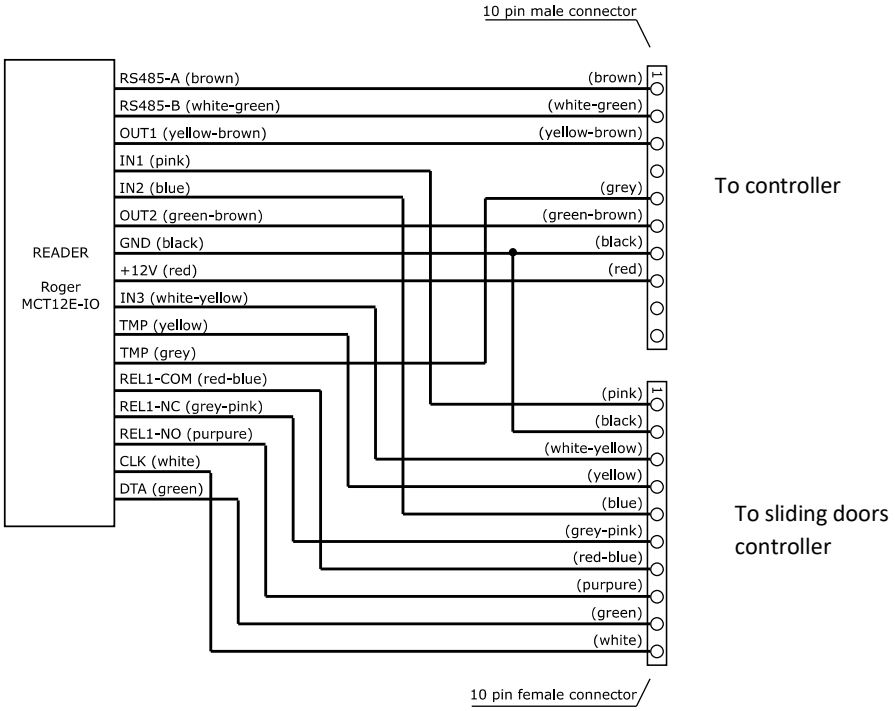
3.3.4 AR121 card reader wiring schematic



3.3.5 AR122 Unique card reader with keypad

Product	Description	Part number
	**AR122** (MCT12E-IO) - Unique 125kHz card reader with keypad for cabinet housing sliding doors • Roger MCT12E-IO reader was used • The reader is designed to control the sliding doors of the cabinet housing. It has a 40cm long cable terminated with multi-pin connectors to connect to the sliding door controller and to the system controller. The wiring arrangement is different than in the AR121 reader. • It Reads EM Unique 125kHz proximity cards, reading range up to 7 cm. • Three LED indicators, buzzer with adjustable sound level, keyboard with backlight, two function buttons, detection of housing opening and detachment from the surface. • 12V, 50mA power supply from a controller or a slave set. • Dimensions: 153 x 46 x 23 (HxWxD) • More information can be found at www.roger.pl	244AR001220

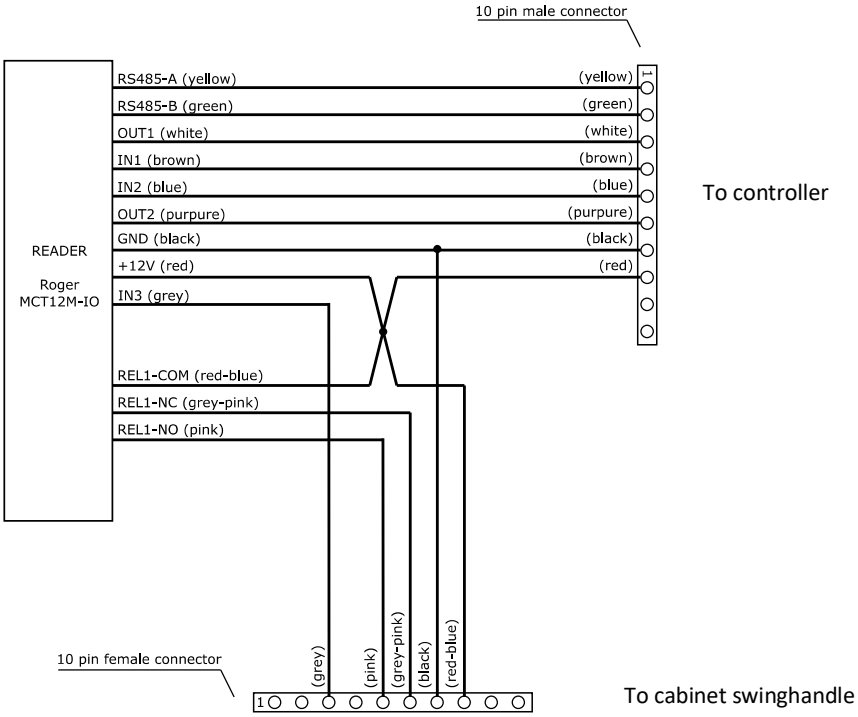
3.3.6 AR122 Card reader wiring schematic



3.3.7 AR131 Mifare card reader with keypad

Product	Description	Part number
	**AR131** (MCT12M-IO) - Mifare 13,56 MHz card reader with kepad for cabinet door • Roger MCT12M-IO reader was used • Reader adapted to control the cabinet door. It has a 15cm long cable terminated with multi-pin connectors to connect to the lock and cabinet controller. • It reads Mifare 13.56MHz proximity cards, reading range up to 7 cm. • Three LED indicators, buzzer with adjustable sound level, keyboard with backlight, two function buttons, detection of housing opening and detachment from the surface. • 12V, 85mA power supply from a controller or a slave set. • Dimensions: 153 x 46 x 23 (HxWxD) • More information can be found at www.roger.pl	244AR001310

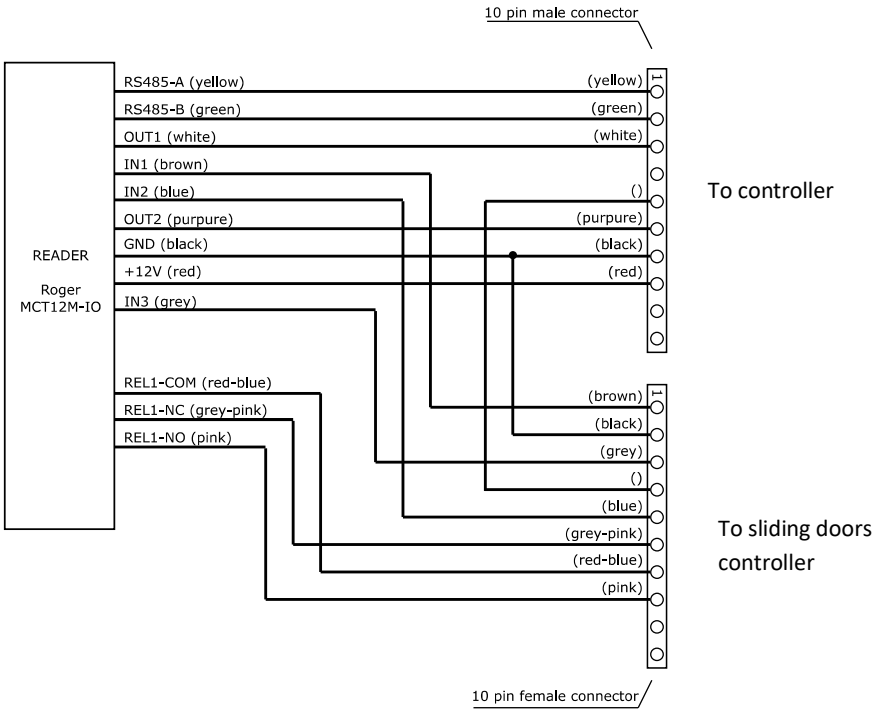
3.3.8 AR131 Card reader wiring schematic



3.3.9 AR132 Mifare card reader with keypad

Product	Description	Part number
	**AR132** (MCT12M-IO) - Mifare 13.56MHz card reader with keypad for cabinet housing sliding doors • Roger MCT12M-IO reader was used • The reader is designed to control the sliding doors of the cabinet housing. It has a 40cm long cable terminated with multi-pin connectors to connect to the sliding door controller and to the system controller. The wiring arrangement is different than in the AR121 reader. • It reads Mifare 13.56MHz proximity cards, reading range up to 7 cm. • Three LED indicators, buzzer with adjustable sound level, keyboard with backlight, two function buttons, detection of housing opening and detachment from the surface. • 12V, 85mA power supply from a controller or a slave set. • Dimensions: 153 x 46 x 23 (HxWxD) • More information can be found at www.roger.pl	244AR001320

3.3.10 AR132 Card reader wiring schematic

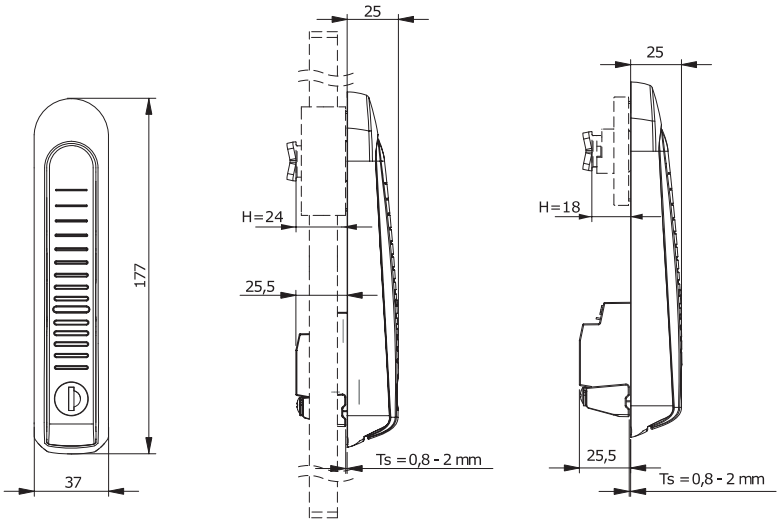


3.4 Cabinet swinghandles

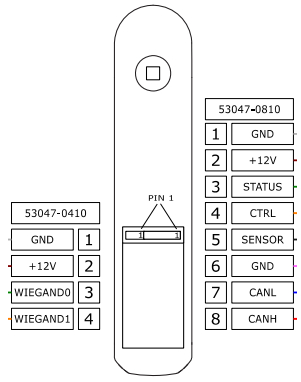
3.4.1 AL200 swinghandle

Product	Description	Part number
	**AL200** - Electronic locking & monitoring swinghandle with mechanical override • Installation in a standard 150x25mm cut out. • Can be installed in a single and multi-point locking system. • Three-color LED signalling the operation status of the swinghandle. • Monitoring the status of the handle and the ability to transfer information to the access control system. • Emergency key override. • Nominal current consumption during lock operation: 180mA • Quiescent current consumption: 30mA • Dimensions: 177 x 37 x 51 (H x W x D)	122AL002000

3.4.2 AL200 Dimensions



3.4.3 AL200 connectors



		8-pin socket (53047-0810)
1	GND	Power supply input: GND.
2	+12V	Power supply input: +12V.
3	STATUS	Handle status (active low, when handle open)
4	CTRL	Handle control (+12V or GND to open the handle)
5	SENSOR	Do not connect
6	GND	Do not connect
7	CANL	Do not connect
8	CANH	Do not connect
		4-pin socket (53047-0410)
1	GND	Do not connect
2	+12V	Do not connect
3	WIEGAND 0	Do not connect
4	WIEGAND 1	Do not connect

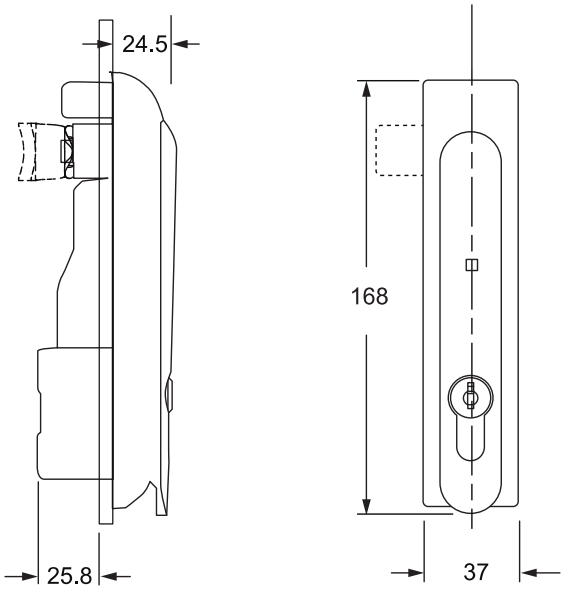
3.4.4 AL200 accessories

Product	Description	Part number
	**AW212** - AL200 swinghandle to AR121 or AR131 reader connection cable, 0.55m • The cable is used to connect the reader AR121, AR131 to AL200 swinghandle. • Length: 0.55m, terminated with 10-pin male and 8-pin female connectors.	122AW002120

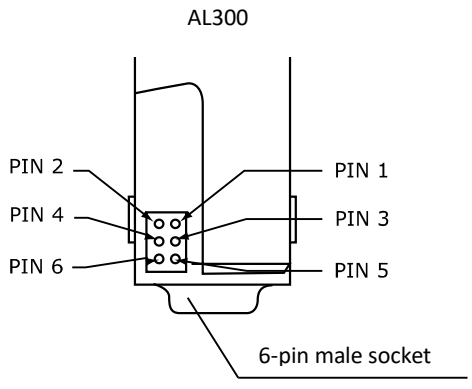
3.4.5 AL300 swinghandle

Product	Description	Part number
	**AL300** (H3-EM-60-100) - Electronic locking & monitoring swinghandle with mechanical override • Standard 150x25mm mounting cutout. • Supports single and multi-point locking. • Opening signalled by a built-in LED. • Monitored status of the handle and the ability to pass information to the access control system. • The lock can be opened with a key in the event of a power failure. • Nominal current consumption during lock operation: 200mA • Quiescent current of the handle: 50mA • Dimensions: 168 x 37 x 50 (HxWxD)	122AL103001

3.4.6 AL300 Dimensions



3.4.7 AL300 connectors



1 – Power supply GND
2 - Power supply +12V
3 – N/C
4 – Control (+12V, to open handle)
5 – Electrical status (active low, when handle is open)
6 – Mechanical status (active low, when handle is open)

3.4.8 AL300 accessories

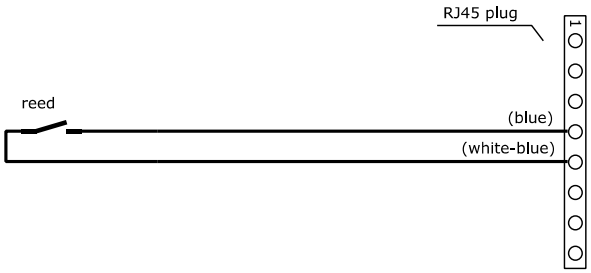
Product	Description	Part number
	**AW112** – AL300 swinghandle to AR121 or AR131 reader connection cable, 0.55m • The cable is used to connect the reader AR121, AR131 to AL300 swinghandle. • Length: 0.55m, terminated with 10-pin male and 6-pin female connectors.	244AW001120

3.5 Door sensors

3.5.1 AD101 Single leaf door sensor

Product	Description	Part number
	**AD101** – Single leaf door reed sensor with 5m cable • Sensor normally open (NO) • 5m long wire terminated with an RJ45 plug to connect to the controller. The set has a metal bracket that fixes the reed switch to the cabinet frame.	244AD001010

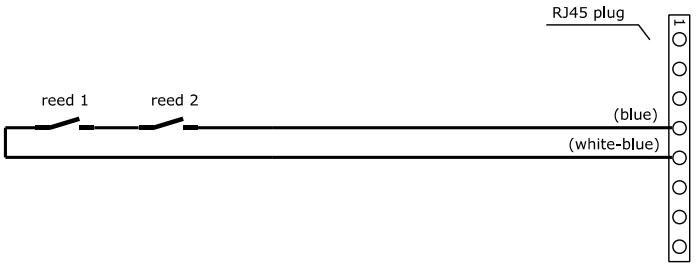
3.5.2 AD101 Door sensor wiring



3.5.3 AD102 - Double leaf door sensor

Product	Description	Part number
	**AD102** – Double leaf door reed sensor with 5m cable • Sensors normally open (NO) • 5m long wire terminated with an RJ45 plug to connect to the controller. • The set has a two metal brackets that fixes the reed switches to the cabinet frame.	244AD001020

3.5.4 AD102 Door sensor wiring

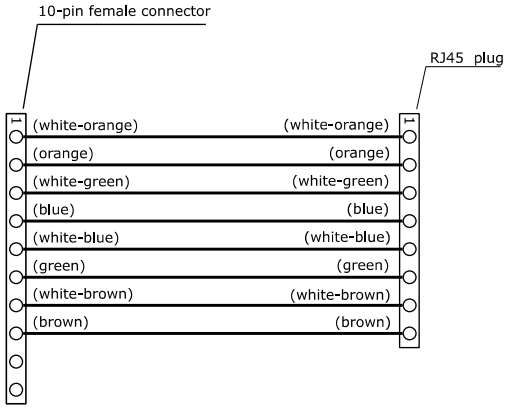


3.6 Connection cables

3.6.1 AW111 cable

Product	Description	Part number
	**AW111** – Reader to controller connection cable • The cable is used to connect the reader AR121, AR122, AR131, AR132 with the AC1xx controller. • 5m long, terminated with RJ45 plug and a 10-pin female connector.	244AW001110

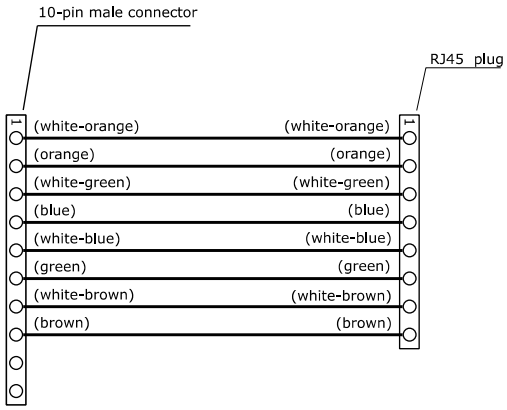
3.6.2 AW111 cable wiring



3.6.3 AW113 cable

Product	Description	Part number
	**AW113** - Reader to housing sliding door controller connection cable • The cable is used to connect the reader AR121, AR122, AR131, AR132 with the cold/hot aisle containment sliding door controller. • 5m long, terminated with RJ45 plug and male 10-pin connector.	244AW001130

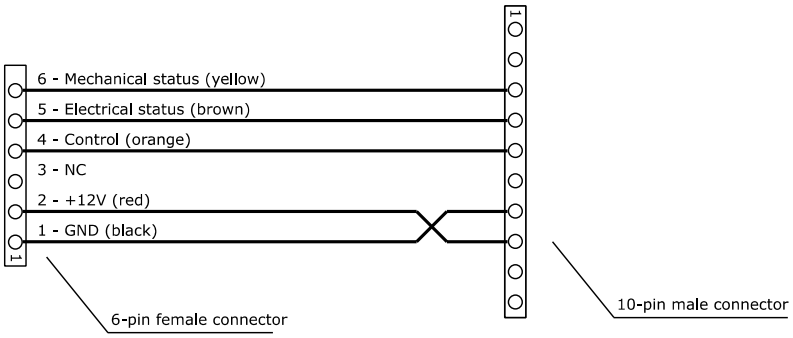
3.6.4 AW113 cable wiring



3.6.5 AW112 cable

Product	Description	Part number
	**AW112** - AL300 swinghandle to AR121 or AR131 reader connection cable, 0.55m • The cable is used to connect the reader AR121, AR131 to AL300 swinghandle. • Length: 0.55m, terminated with 10-pin male and 6-pin female connectors.	244AW001120

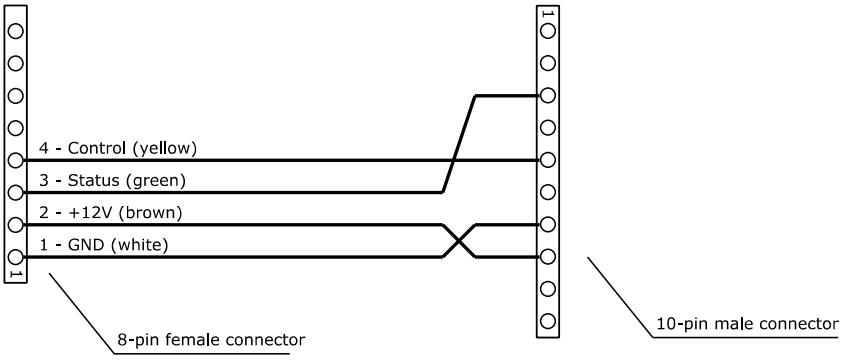
3.6.6 AW112 cable wiring



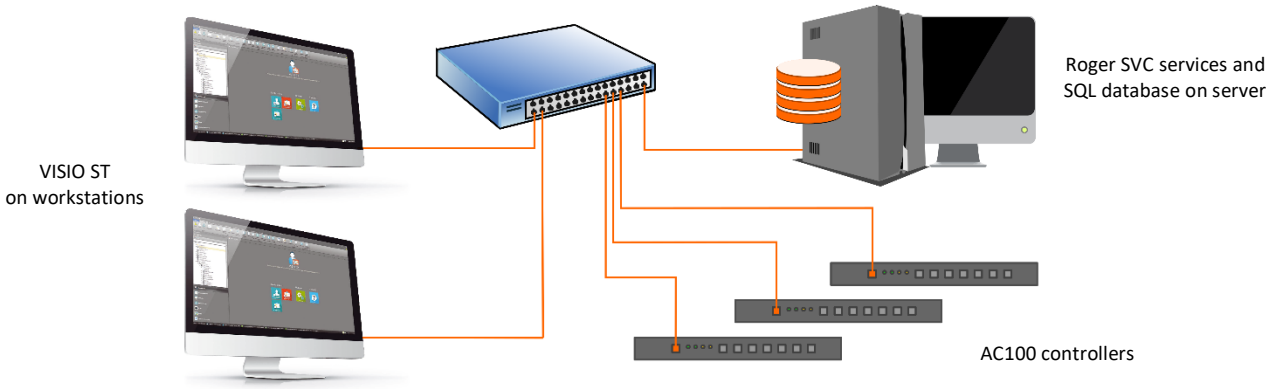
3.6.7 AW212 cable

Product	Description	Part number
	**AW212** - AL200 swinghandle to AR121 or AR131 reader connection cable, 0.55m • The cable is used to connect the reader AR121, AR131 to AL200 swinghandle. • Length: 0.55m, terminated with 10-pin male and 8-pin female connectors.	244AW002120

3.6.8 AW212 cable wiring



3.7 System software



RogerSVC is a free package of Windows system services, the main task of which is to:

- Communicate with access controllers
- Perform configured system tasks
- Save system events to the database
- Requires continuous operation, if events are to be written to the database online, otherwise the events will be saved in the controllers memory and will be transferred to the database after RogerSVC is restarted.
- The software is available for download at www.roger.pl

Hardware requirements for RogerSCV:

Systems for up to 5 controllers	Systems from 5 to 50 controllers	Systems of over 50 controllers
4GB RAM, Intel Core i3 / i5 (2 cores) or equivalent, 500 MB HDD	4GB RAM, Intel Core i5 / i7 (4 cores) or equivalent, 500MB HDD	8GB RAM, Intel XEON (8 cores) or equivalent, 500MB HDD

VISO is a Windows application for configuring and managing the access control system. It is available in two versions VISO ST (Standard, also as a free version up to 16 doors) and VISO EX (Enterprise for installations over 128 doors). Basic program functions:

- MS SQL Express / Server database
- Management from multiple workstations
- Encrypted communication with system devices and system servers
- Configurable rights for system operators
- Operator's actions recorded in logs.
- Unlimited number of system users
- Monitoring the current operation of the system in text (table) and graphical (maps) modes
- Monitoring of any state of the facility with the use of automation nodes
- Configurable event types for selected logical automation nodes
- System control using remote commands
- Automatic system reactions for selected events
- Configurable alerts for selected events
- E-mail notifications
- Support for system administrator reader
- Wizards for quick system configuration
- The software is available for download at www.roger.pl

Hardware requirements for VISO ST:
RAM: 4 GB (8 GB for systems with more than 50 controllers), CPU: Intel Core i5 or equivalent (Core i7 for systems with more than 50 controllers), HDD: 500 MB for VISO, minimum screen resolution 1280x1024

3.7.1 Software versions and licenses

Version comparison

Parameter	VISO ST		VISO EX
	Free version	Maximum version	Maximum version
Controller supported	MC16-PAC-ST	MC16-PAC-ST	MC16-PAC-EX
Number of doors	16	128	Unlimited
Number of users	500	Unlimited	Unlimited
Operator stations	1	3	Unlimited
USB dongle for license	Not required	RUD-6-LKY	RUD-6-LKY

VISO ST licenses

VISO ST licenses	Part number
LIC-VISO-START-ST - License for the management program for the RACS 5 system; starter version; no license or dongle required; free version limitations: - up to 16 doors - up to 500 users - 1 operator station	122AS102100
RUD-6-LKY - USB dongle for license	122AS102099
LIC-VISO-BASE-ST - License for the management program for the RACS 5 system; basic version; requires a license and dongle; basic version limitations: - up to 32 doors (max 128) - up to 1000 users (max unlimited) - 1 operator station (max 3)	122AS102101
LIC-VISO-ST-16AD -License for additional 16 doors (VISO-ST Standard system)	122AS102102
LIC-VISO-ST-32AD -License for additional 32 doors (VISO-ST Standard system)	122AS102103
LIC-VISO-ST-64AD -License for additional 64 doors (VISO-ST Standard system)	122AS102104
LIC-VISO-ST-100U - License for additional 100 users (VISO-ST Standard system)	122AS102111
LIC-VISO-ST-500U - License for additional 500 users (VISO-ST Standard system)	122AS102112
LIC-VISO-ST-1000U - License for additional 1000 users (VISO-ST Standard system)	122AS102113
LIC-VISO-ST-1WS- License for 1 additional operator station of VISO program (VISO-ST Standard system)	122AS102121
LIC-VISO-ST-WEB- License for VISO Web application (VISO-ST Standard system)	122AS102122
LIC-VISO-ST-MOB- License for the VISO Mobile application (VISO-ST Standard system)	122AS102123

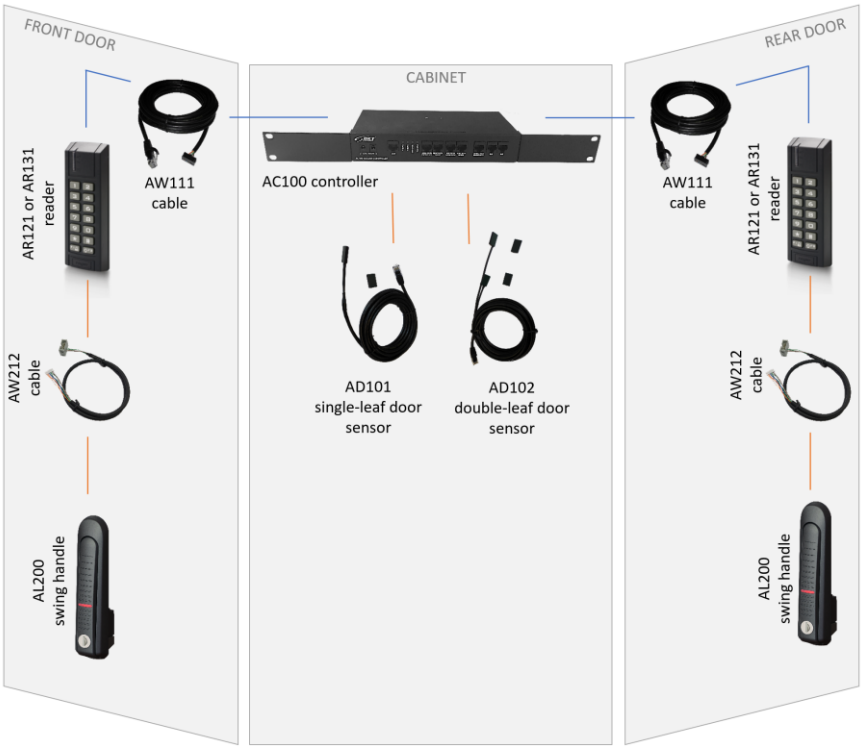
VISO EX licenses

VISO EX licenses	Part number
RUD-6-LKY - USB dongle for license	122AS102099
LIC-VISO-BASE-EX - License for the management program (VISO-EX Enterprise) for the RACS 5 system; basic version, includes a license to use VISO Web and VISO Mobile; requires a license and dongle; Basic version limitations: - up to 32 doors (max unlimited) - up to 1000 users (max unlimited) - 2 operator stations (max unlimited)	122AS102201
LIC-VISO-EX-16AD -License for additional 16 doors (VISO-EX Enterprise system)	122AS102202
LIC-VISO-EX-64AD -License for additional 64 doors (VISO-EX Enterprise system)	122AS102204
LIC-VISO-EX-128AD -License for additional 128 doors (VISO-EX Enterprise system)	122AS102205
LIC-VISO-EX-100U - License for additional 100 users (VISO-EX Enterprise system)	122AS102211
LIC-VISO-EX-500U - License for additional 500 users (VISO-EX Enterprise system)	122AS102212
LIC-VISO-EX-1000U - License for additional 1000 users (VISO-EX Enterprise system)	122AS102213
LIC-VISO-EX-1WS- License for 1 additional operator station of VISO program (VISO-EX Enterprise system)	122AS102221

4 BKT ACBS SYSTEM STRUCTURE

4.1 System structure in a single cabinet

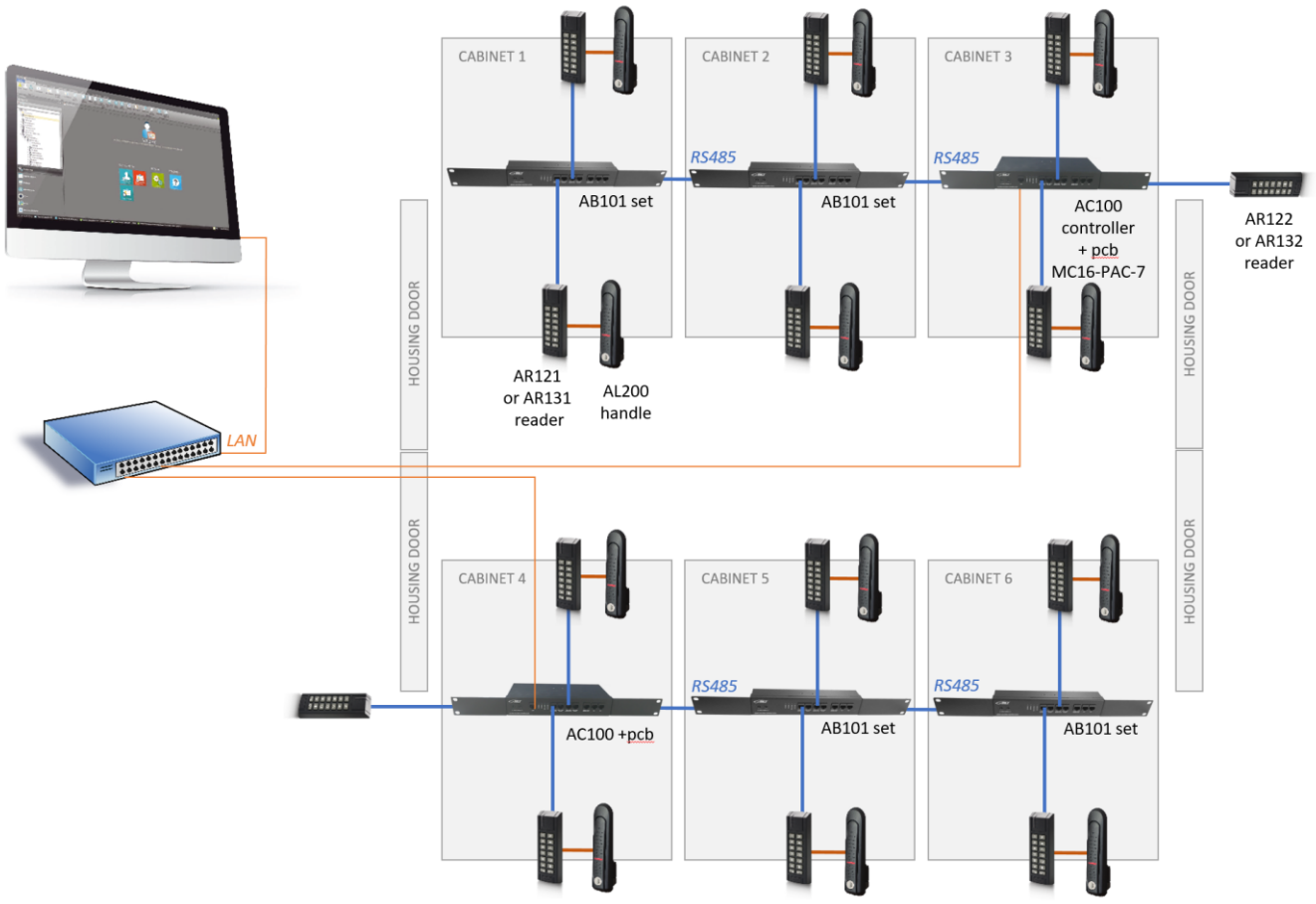
The figure below shows the connections between system components in one cabinet. Each cabinet in the system has a controller or a slave set in a 1U 19'' enclosure that powers the devices. The 1U 19'' enclosure has a set of RJ45 sockets allowing connection of two door sensors, two cabinet door readers and an optional cold/hot aisle containment sliding door reader. Connections are made using dedicated wires terminated from the controller's side with RJ45 plugs.



4.2 System structure in cold/hot aisle containment

One controller can handle up to 16 doors. It should be installed in one of the cabinets. The controller should be connected to the local network via the LAN connector. Other cabinets are equipped with AB101 secondary sets, also in 1U 19'' enclosures. The secondary sets are connected to the controller using UTP Cat5e patch cords, which form the RS485 bus for the subsystem of a maximum of sixteen doors. The RS485 bus can be up to 1000m long.

The figure below shows an example of the connection layout for a cold/hot aisle containment made of six cabinets. The system has been divided into two identical subsystems, one for each row of cabinet - a subsystem for cabinets 1 - 3 and a subsystem for cabinets 4 - 6. One of the cabinets has an AC100 controller installed with the MC16-PAC-ST-7 controller pcb that supports up to 7 doors . The remaining cabinets are equipped with AB101 secondary sets. The secondary sets are connected to the controller with UTP kat5e patchcords, which form the RS485 bus for the 7-door subsystem. Two card readers and handles are connected to the AC100 controller or the AB101 set in each cabinet. Additionally, a third reader for the cold/hot aisle containment sliding door is connected directly to the controller. The controller is connected to the local LAN network, which is accessed by a computer with system configuration and management software.

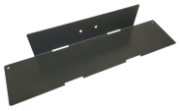


5 INSTALLATION OF CABINET DOOR DEVICES

Note: The installation of the devices should be performed by a skilled person or a person instructed by a skilled person.

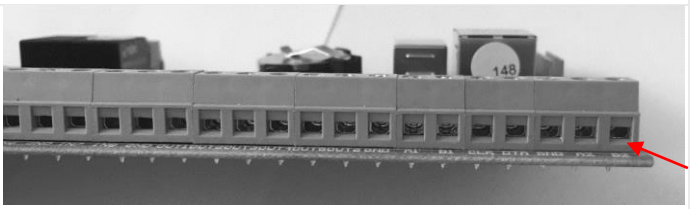
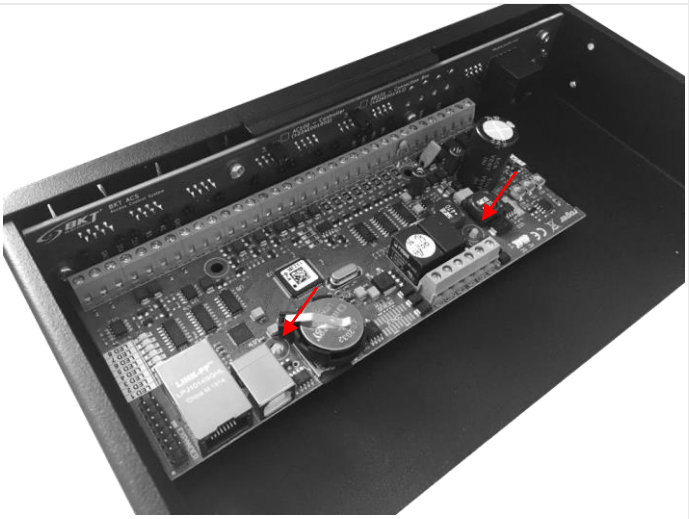
5.1 AC100 controller installing

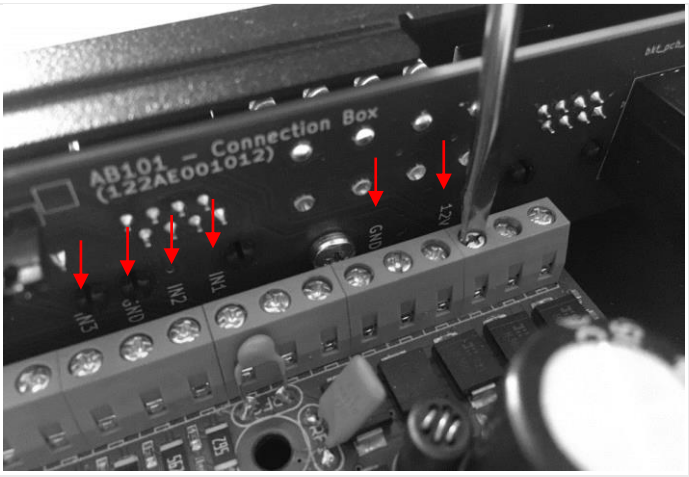
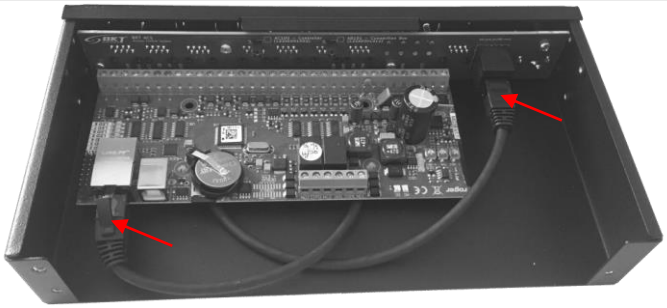
5.1.1 Package contents

				
AC100 housing	1U 19’’ bracket	Power supplies bracket	Bolts set	Quick Start Guide

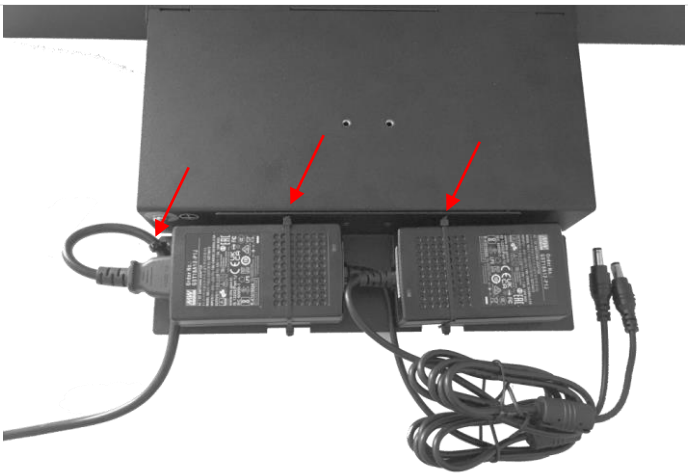
5.1.2 Controller pcb mounting

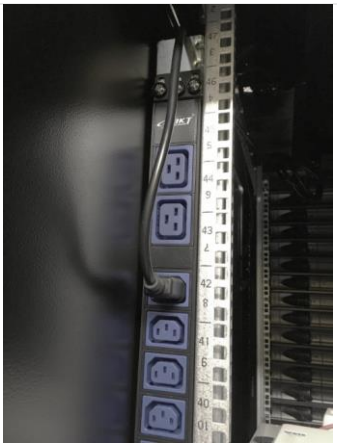
Before installing the controller in the cabinet, install the Roger MC16-PAC-ST-x pcb, where "x" means the number of doors supported by the controller. Versions are available from MC16-PAC-ST-1 (for one door) to MC16-PAC-ST-16 (for 16 doors). The assembly of the pcb board should be performed in an environment free from electrostatic charges. Hold the board only by its edges. More information about the controller pcb itself can be found on the website www.roger.pl

Open the controller housing cover by unscrewing the three screws.	
Make sure that all connectors on the terminal block are unscrewed on the controller pcb.	
Place the controller pcb inside the housing, starting by placing the controller terminal blocks on the pin strip located on the pcb inside the housing. Then press the controller onto the two plastic spacers located on the bottom plate of the housing.	

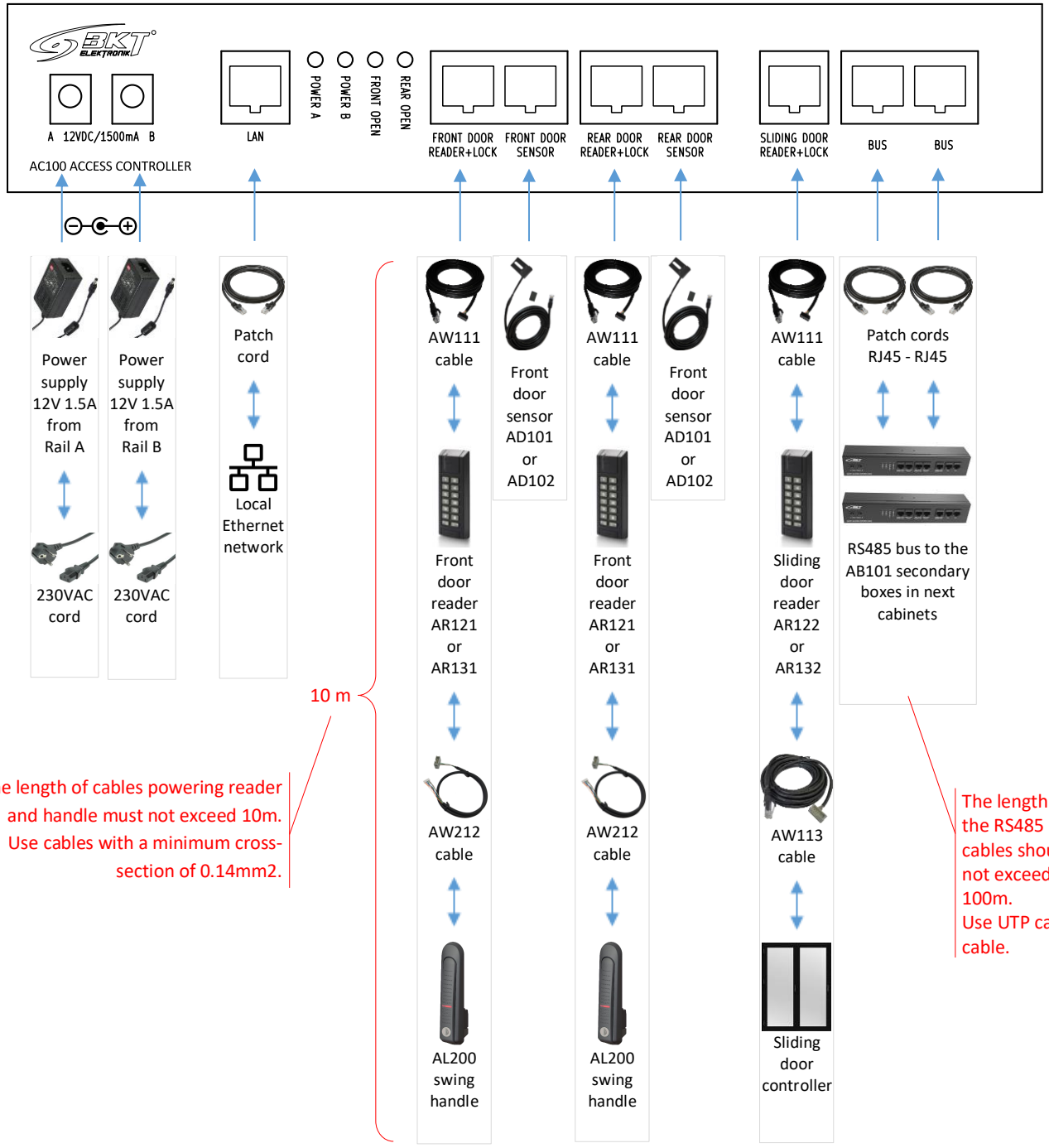
Carefully tighten the connectors on the terminal block. It is enough to tighten only the connectors with the white description on the pcb, the others are not used.	
Connect the LAN connection patchcord.	
Put the housing cover and tighten the screws.	

5.1.3 Installing in the cabinet

Attach the 19'' brackets to the housing using the provided four M3 screws (two on each side).	
Attach the power supply bracket to the housing using the provided two M3 screws.	
Attach the power supplies using plastic cable ties or Velcro ties. Connect the 230VAC power cables and secure against disconnection by attaching a cable tie to the power supply holder.	
Connect the 12VDC plugs of the power supplies to the sockets on the front panel. Pay attention to the Rail A and Rail B markings.	

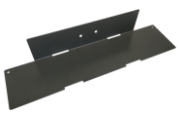
Install the AC100 controller in the rack. Suggested position - at the top at the back of the cabinet.	
Screw the protective grounding conductor from the cabinet grounding bar to the device housing.	
Connect the power supply cables to the power strips in the rack. Pay attention to the proper connection to Rail A and Rail B.	 
Make connections of the other devices according to *5.1.4 Connecting devices to the AC100 controller*.	

5.1.4 Connecting devices to the AC100 controller



5.2 AB101 secondary set installing

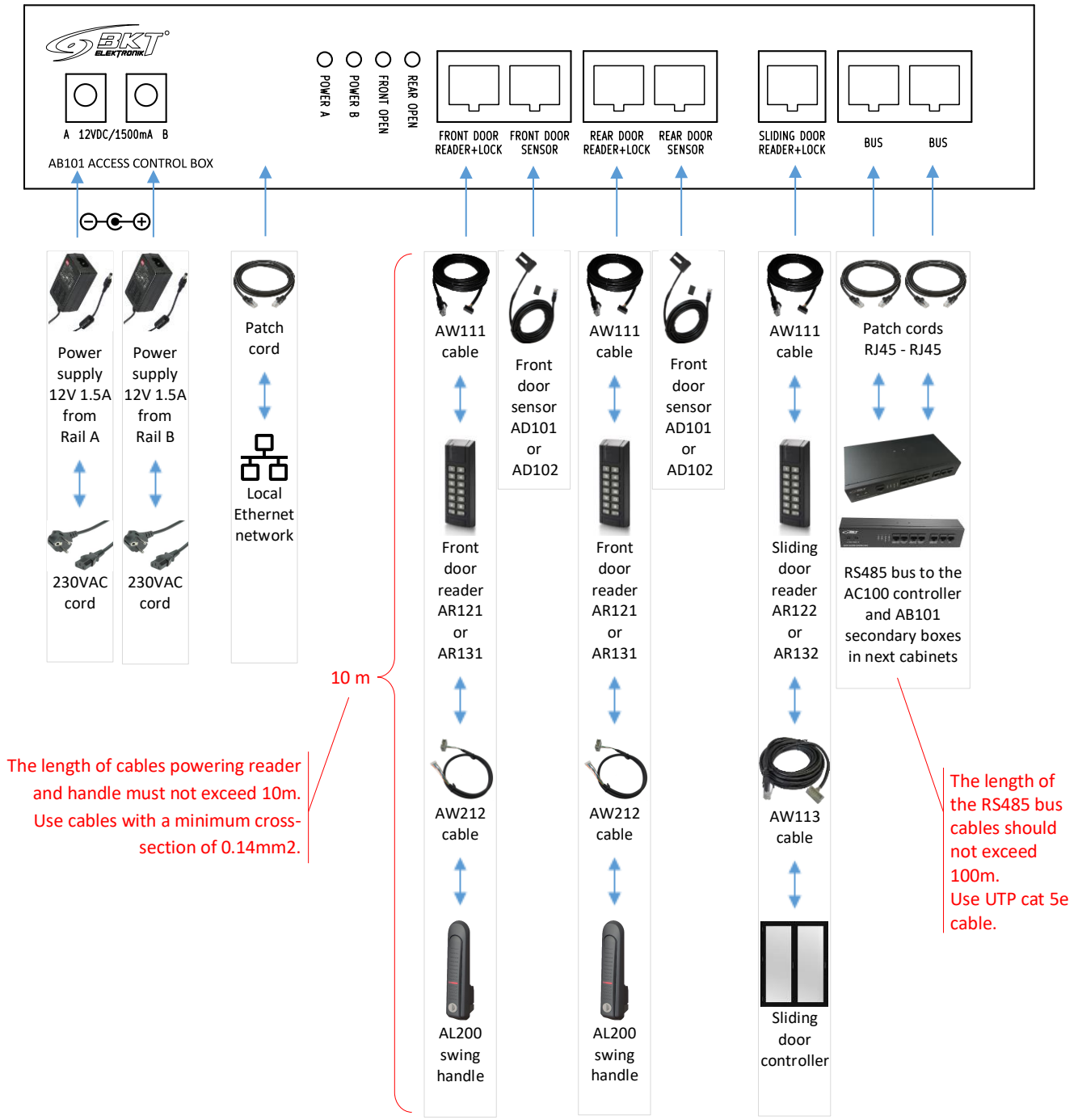
5.2.1 Package contents

				
Obudowa AB101 housing	1U 19'' bracket	Power supplies bracket	Bolts set	Quick Start Guide

5.2.2 Installing in the cabinet

Install the set in the same way as the controller (see *5.1.3 Installing in the cabinet*).

5.2.3 Connecting devices to the AB101 set



5.3 AR121, AR131 readers installing

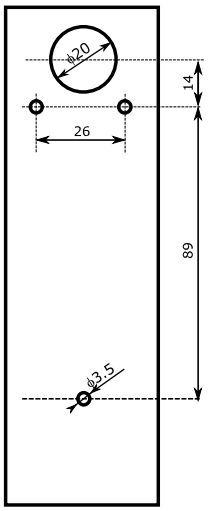
5.3.1 Package contents

	
Reader	3 M3 screws with nuts

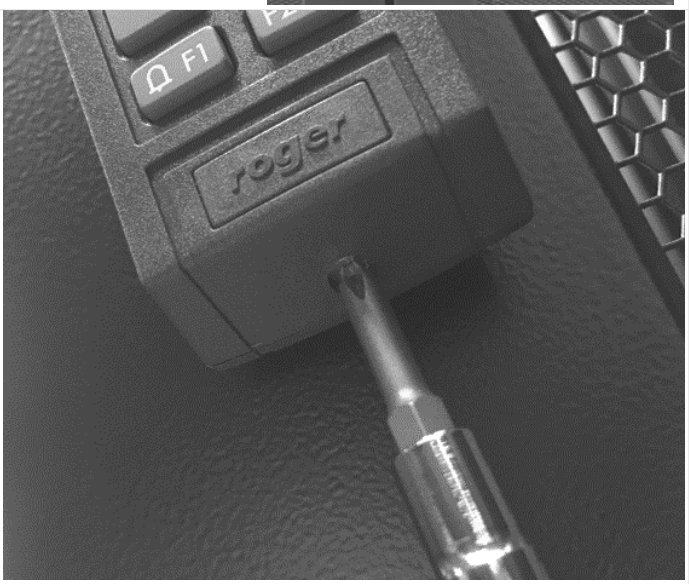
NOTE: Before installing the AR131 reader (Mifare) you need to perform a low-level configuration (see chapter *7.2 Card reader low level configuration*)

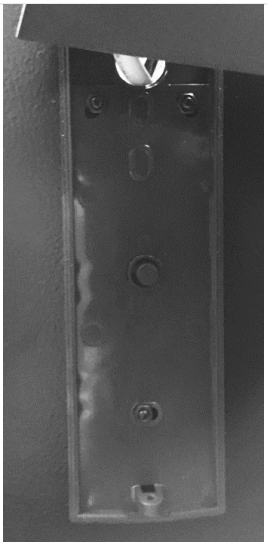
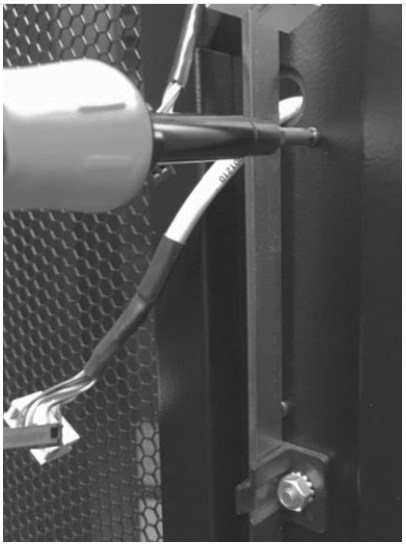
5.3.2 Installing on the cabinet door

Install the AR121 (Unique) or AR131 (Mifare) reader on the cabinet door in a designated place. If the cabinet does not have a door dedicated to access control, make the mounting holes as shown in the picture on the right.



Open the reader casing by unscrewing the screw at the bottom.



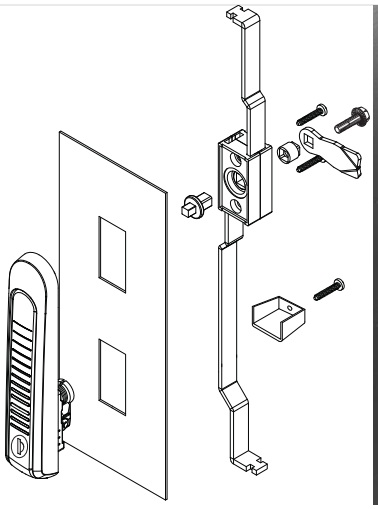
Attach the reader base to the outside of the door using the three provided M3 screws. The screw head should be on the inside of the door. Then close the reader casing by tightening the screw unscrewed earlier from the bottom.	 
Connect the reader with the controller and the door handle (see *5.7 Installation of cabinet door wiring*)	

5.4 AL200 swinghandle installing

5.4.1 Package contents

		
AL200 swingahndle	Fastening element with a screw	Quick Start Guide

5.4.2 Installing on the cabinet door

If the cabinet does not have an AL200 electronic handle pre-installed, install it in place of the mechanical handle. Depending on the type of mechanical handle used, additional mechanical elements may be required. More information on this subject can be found in the AL200 handle manual available on the website www.bkte.pl.	 

Unscrew the cam, cylinder housing, and then the cogwheel mechanism and remove the handle.

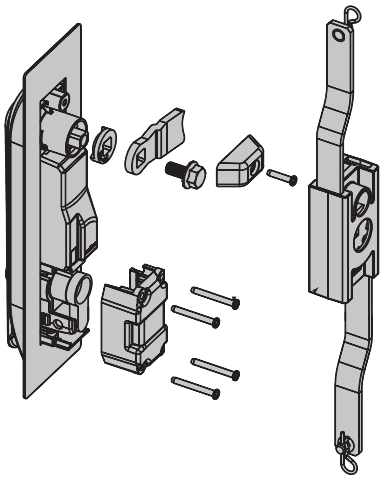



Pull out the rods so that in the closed position of the handle, the rods are extended to the maximum. Then place the electronic handle in the cut-out in the door.
Screw in all the elements you just unscrewed.


Check if the handle mechanically closes the door properly.

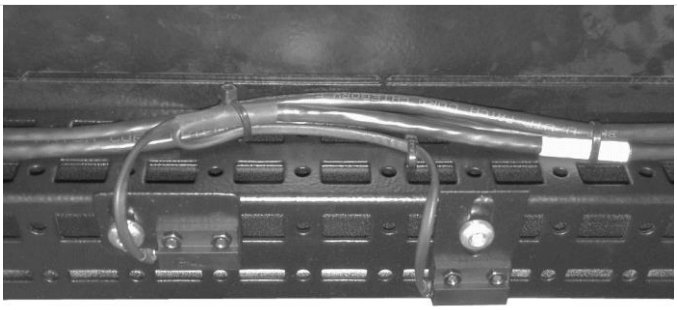
5.5 AL300 swinghandle installing

Installation of the AL300 handle is similar to the AL200 handle. Additional mechanical components, including a cogwheel mechanism, may be required.



5.6 Door sensors installing

Install the door sensors on the upper part of the cabinet frame by screwing the metal holders that secure the reed switches. Attach the reed switch magnets to the cabinet door using the enclosed self-adhesive double-sided tape. The end of the cable should be connected to the door sensor socket in the AC100 controller or the AB101 set. The door sensor cable can be shortened to the required length and reterminated with an RJ45 plug or its spare rolled up and fixed in such a way that it does not interfere with other devices in the cabinet.



5.7 Installation of cabinet door wiring

Connect the reader to the controller with the AW111 cable. On the door, hide the cable in dedicated cable paths. Fix the cables in the cabinet using cable ties.

Leave a spare cord between the door and the cabinet frame to allow the door to be opened.

The AW111 reader cable can be shortened to the required length and reterminated with an RJ45 plug or its spare rolled up and fixed in such a way that it does not interfere with other devices in the cabinet.

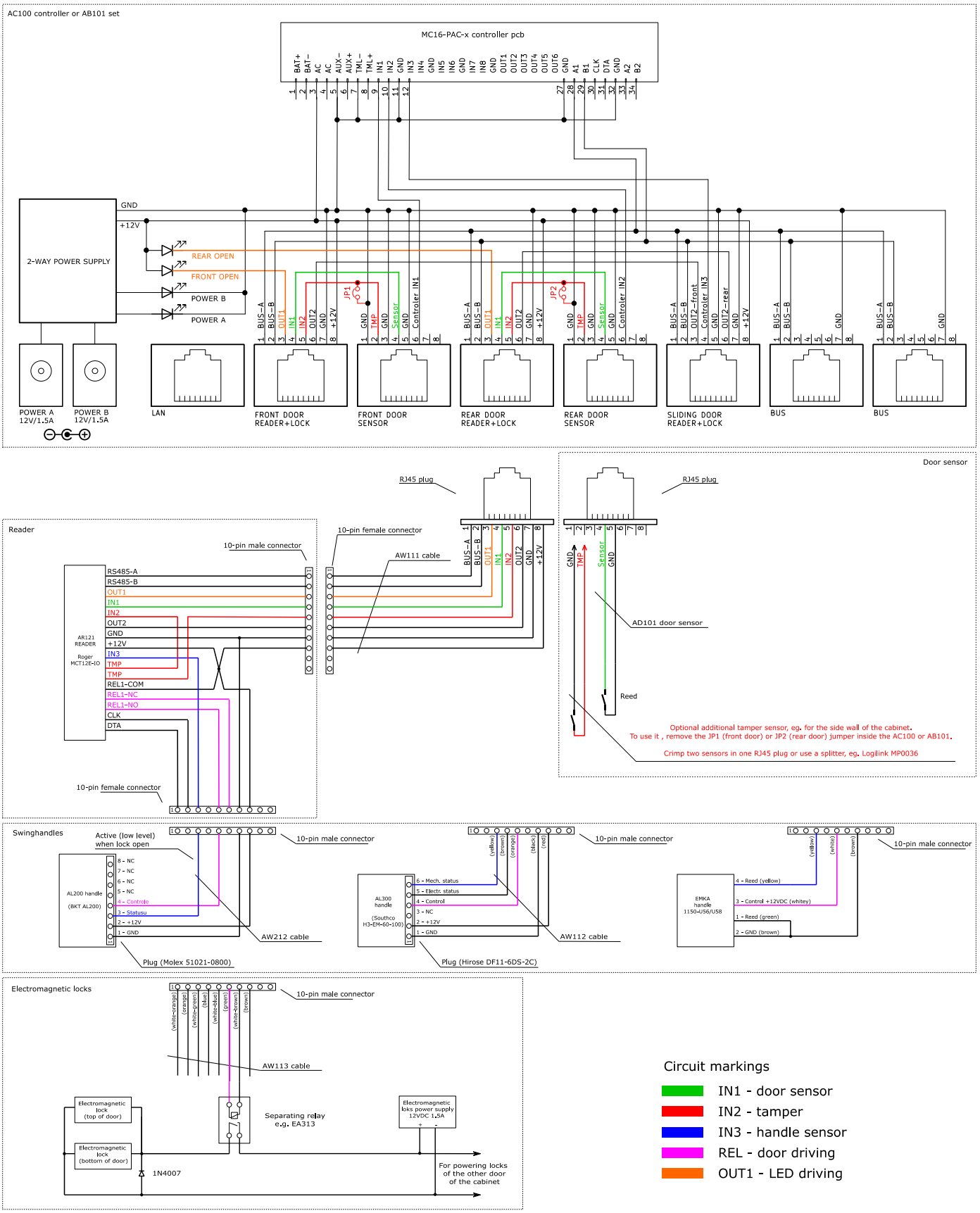
Connect the AL200 handle to the reader using the AW212 cable or the AW112 cable (for the AL300 handle).

Connect the cables to the reader and arrange them carefully. Secure them with electrical tape.

Screw on the reader connector cover.	

5.8 Diagram of functional circuits for operating the cabinet door

Wiring diagram for operating the cabinet door



6 INSTALLATION OF COLD/HOT AISLE CONTAINMENT SLIDING DOOR DEVICES

Note: The installation of the devices should be performed by a skilled person or a person instructed by a skilled person.

6.1 AC100 controller installing

The controller already installed in the cabinet should be used - see chapter *5.1 AC100 controller installing*.

6.2 AR122, AR132 readers installing

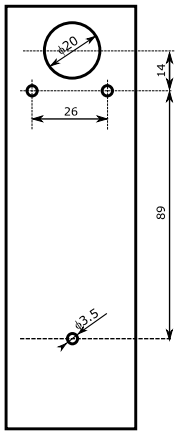
6.2.1 Package contents

	
Reader	3 M3 screws with nuts

NOTE: Before installing the AR132 reader (Mifare) you need to perform a low-level configuration (see chapter *7.2 Card reader low level configuration*)

6.2.2 Installing reader next to the sliding door

Install the AR122 or AR132 reader in a dedicated place on the side wall of the cold/hot aisle containment. If the containment wall does not have dedicated holes, make the mounting holes as shown in the picture on the right. Make sure that the reader installation location will not interfere with the sliding doors.
Connect the reader to the AC100 controller or the AB101 set located in the nearest cabinet. Use the AW111 cable. The cable must be connected to the "SLIDING DOOR READER + LOCK" socket of the controller (see *5.1.4 Connecting devices to the AC100 controller*.).
Install the electrical junction box inside the cabinet and hide the reader connectors in it.



6.3 Installing exit button and emergency button

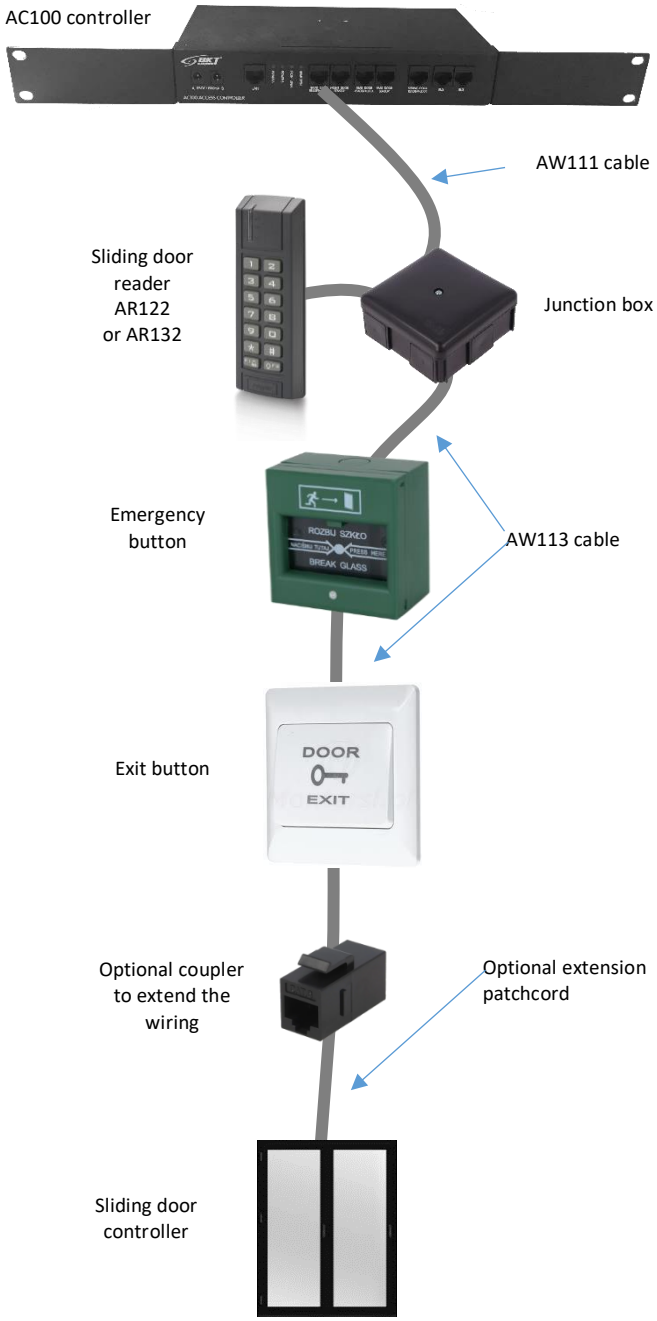
Fix the buttons in dedicated places on the beam above the sliding door, as shown in the photo, or on the optional frame installed behind the sliding doors.

6.4 Installing optional exit buttons

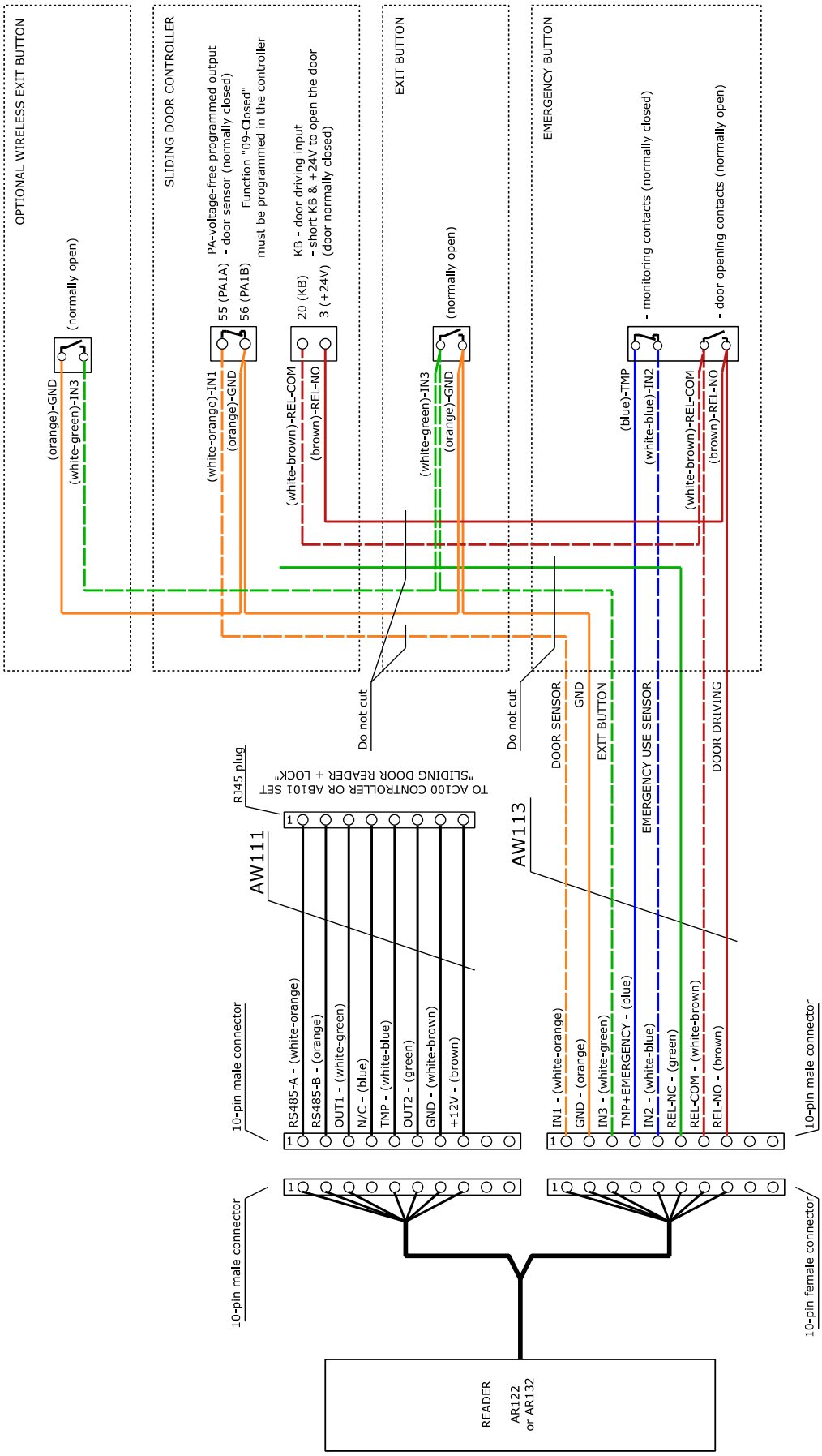
The wireless exit button and / or foot exit button must be connected in parallel with the exit button above the sliding door.

6.5 Installing sliding doors wiring

Connect the AW113 cable (see *3.6.3 AW113 cable*) to the sliding door reader, and then route it (without cutting it) to the emergency button, exit button, and sliding door controller. Cut and terminate only the wires of the cables that need to be connected to the device. Place and clamp the ferules on the ends of the cables before connecting them. Make connections as shown in the diagram *6.6 Connection diagram of sliding kiosk door control devices*.

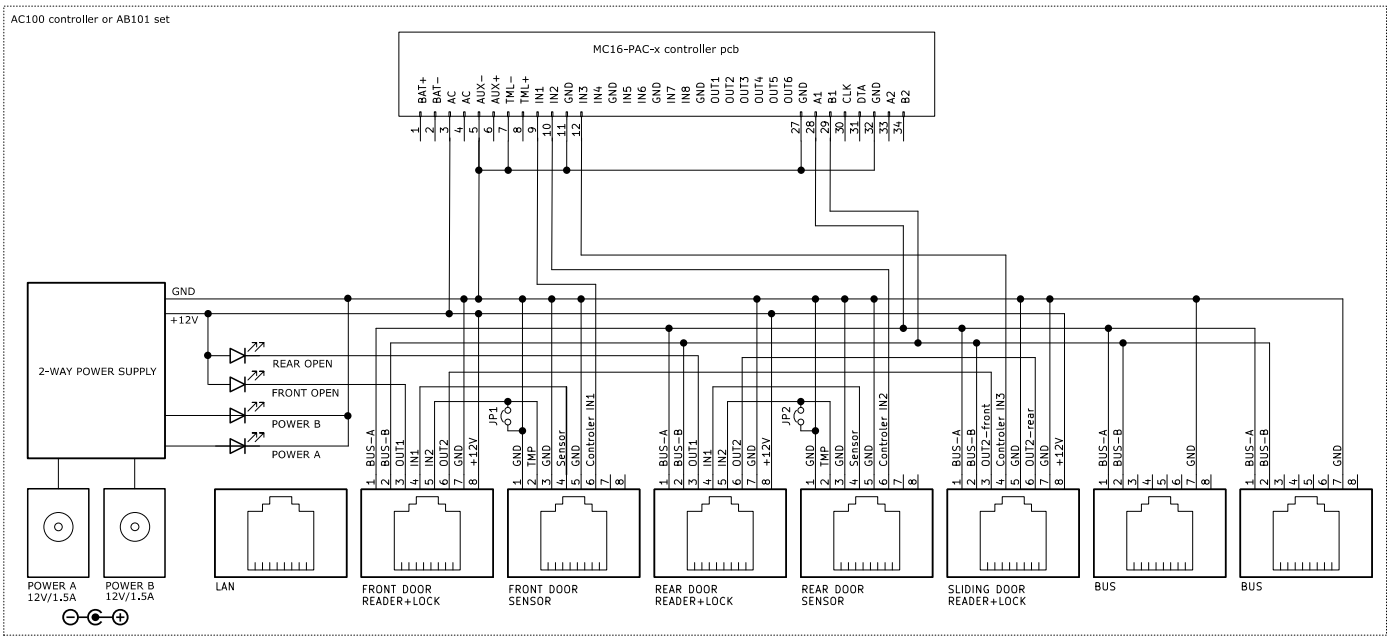


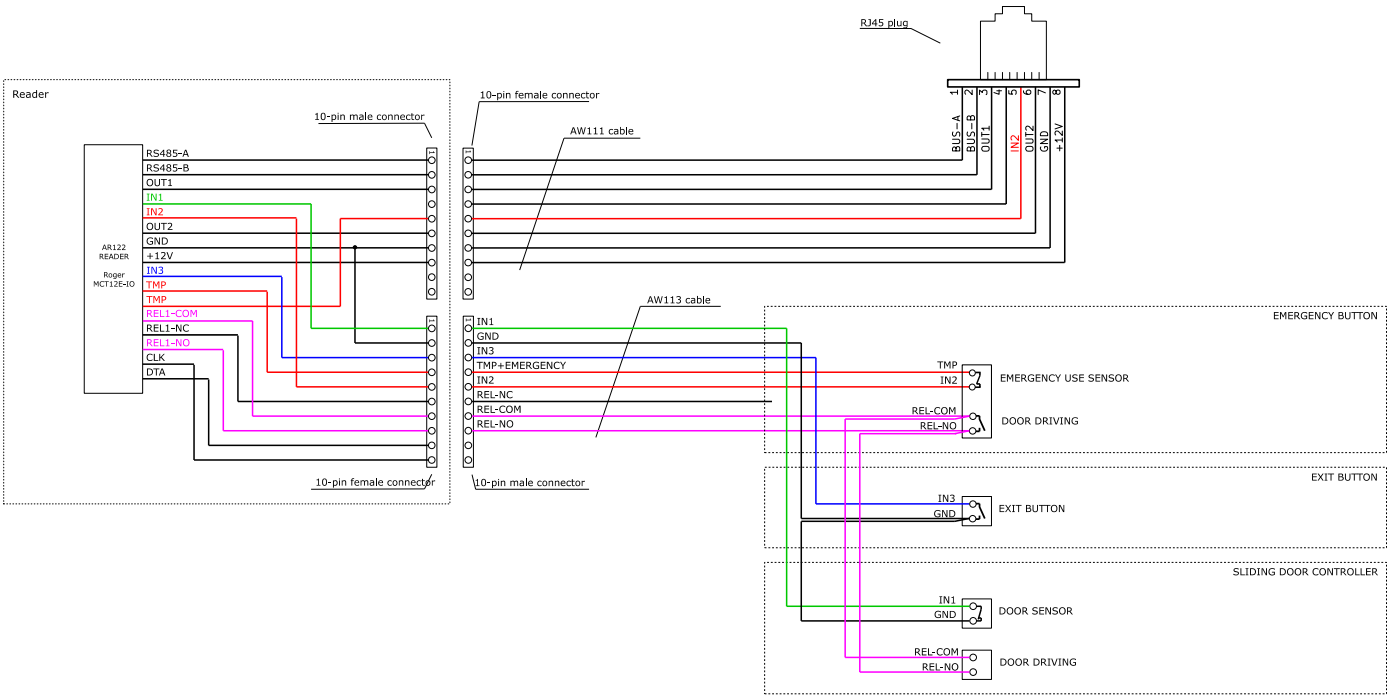
6.6 Connection diagram of sliding kiosk door control devices



6.7 Diagram of functional circuits for operating the sliding door

Wiring diagram for operating the sliding door





Circuit markings

- IN1 - door sensor
- IN2 - tamper + emergency use sensor
- IN3 - exit button
- REL - door drivingi

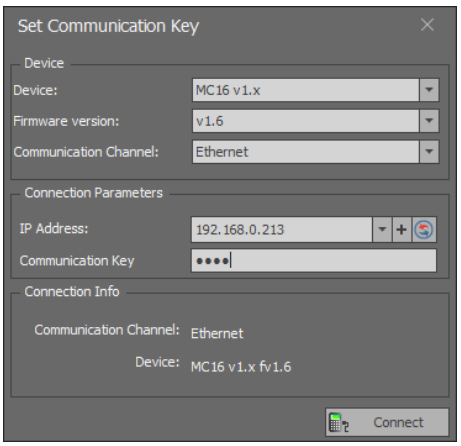
7 DEVICE LOW LEVEL CONFIGURATION

Before starting the configuration in the VISO ST software, the devices must be pre-configured. Roger VDM software is used for a low-level configuration. Roger VDM software can be downloaded from www.roger.pl.

7.1 Controller low level configuration

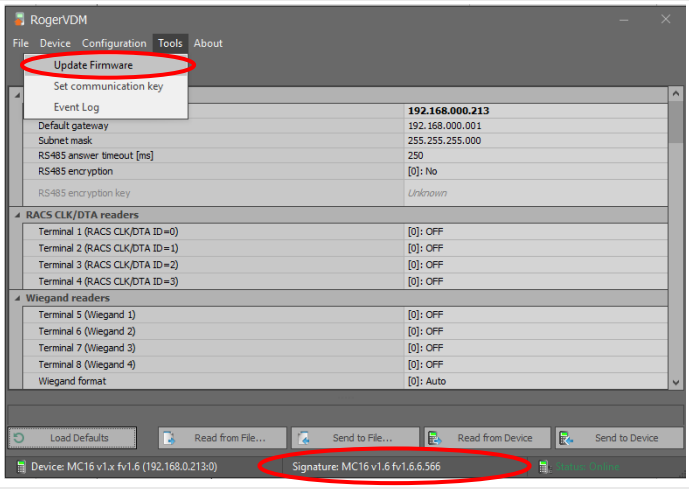
Connecting to the controller

1. Connect the LAN port of the controller to the computer from which the configuration will be performed. Remember to configure the network parameters of the computer properly.
2. Run the Roger VDM software.
3. In Roger VDM, select *Device->New*.
4. Select the device model (MC16 v1.x), firmware version, communication channel (Ethernet).
5. Enter the IP address of the MC16 (factory default IP address: 192.168.0.213).
6. Enter the communication key (factory default password is "1234"). In controllers with version older than 1.4, the factory password is empty.
7. Click *Connect*, the program will connect to the controller and automatically go to the *Configuration* tab.



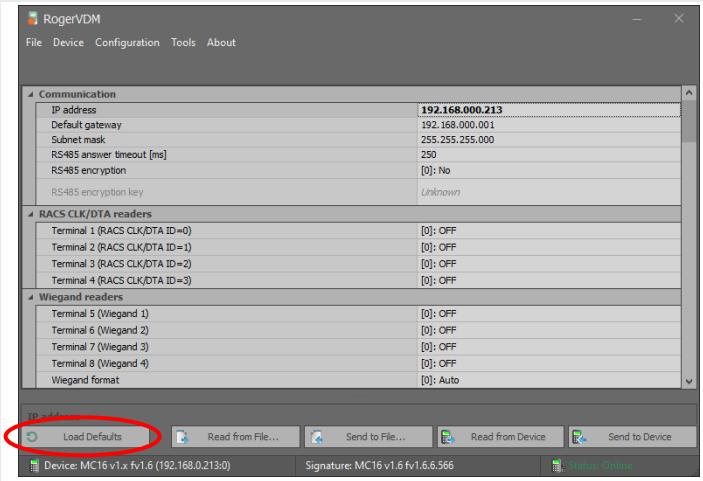
Firmware update

1. Make sure that the device has the newest firmware. The version currently installed on the device is displayed in the bottom bar of the application window. The latest versions of firmware can be downloaded from the website www.roger.pl
2. To run the firmware update on your device, select *Tools-> Update firmware* from the menu.

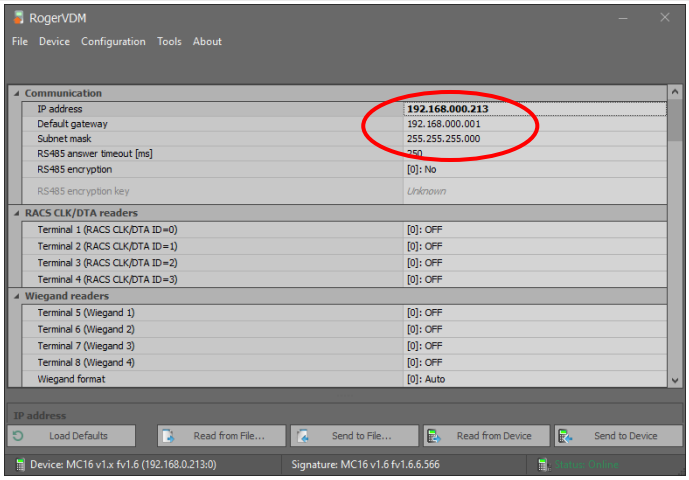


Configuring the controller

It is recommended to start a new configuration from restoring all default values.

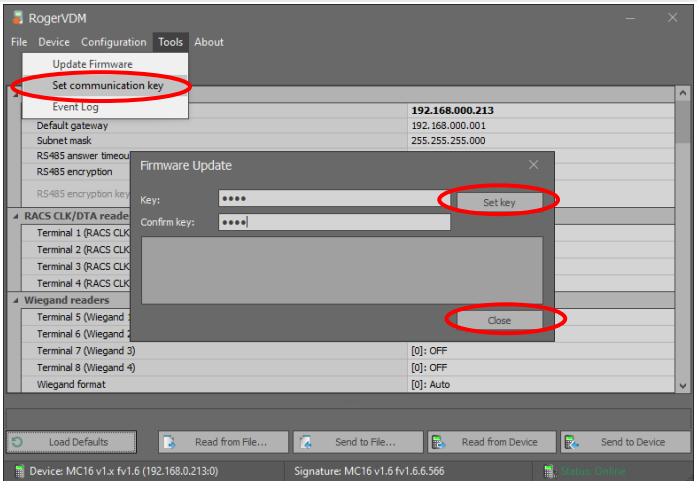


Set the controller's network parameters.

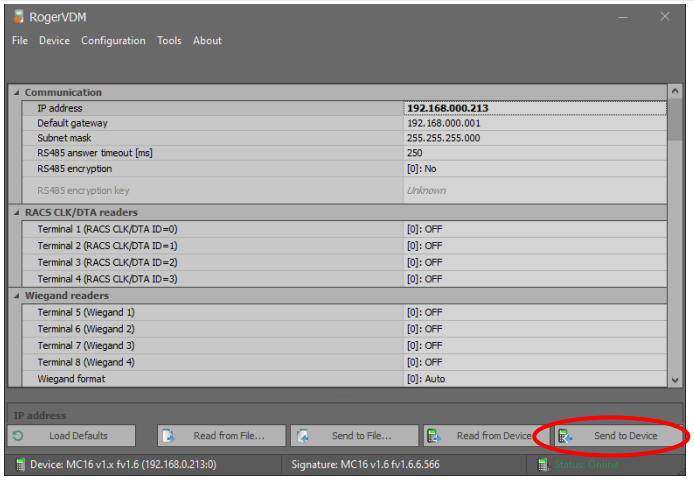


It is necessary to set the communication key. This is a kind of password to access the controller.

1. Select *Tools->Set communication key* from menu.
2. Enter key. You can use only hex signs (0-9, A, B, C, D, E, F).
3. Write the key down, as it will be needed at high level configuration of the system.
4. Click *Set key* button.
5. Click *Close* button.



Send settings to the device - click *Send to Device* button.



Ending the controller low level configuration

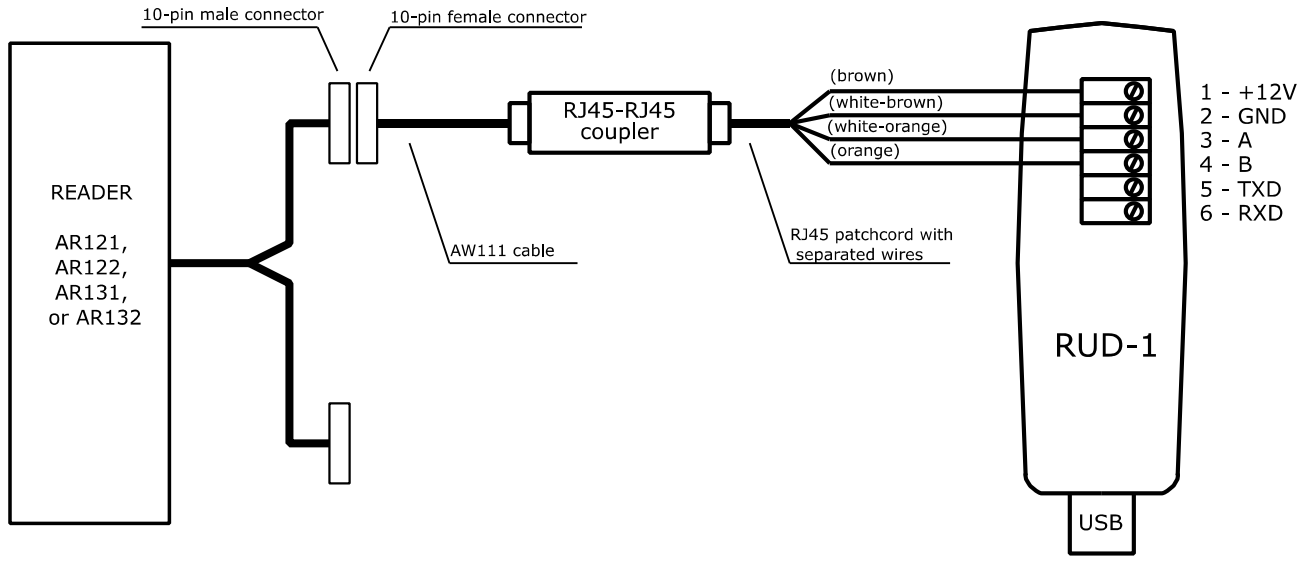
1. In Roger VDM menu select Device-> Disconnect.
2. The controller will be rebooted.

7.2 Card reader low level configuration

Connecting the reader

For low-level configuration, the reader should be connected to the computer via the RUD-1 interface. If the reader is already installed on the cabinet door, then:

1. Disconnect the reader's AW111 cable from the controller by unplugging the RJ45 connector.
2. Connect the RJ45 plug of the AW111 cable to the RUD-1 interface as shown in the figure below.

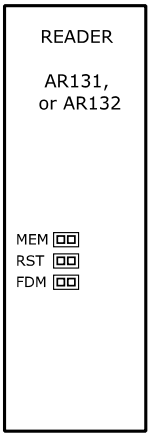


Putting the reader into the service mode

AR121 and AR122 readers (UNIQUE readers) do not require any additional steps.

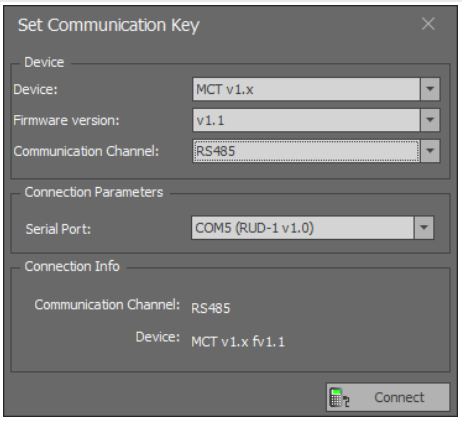
In AR131 and AR132 readers (Mifare readers) you should:

1. Remove the MEM jumper on the reader
2. Restart the reader (turn off and turn on the power or short RST jumper for a moment) - orange LED SYSTEM reader will start to flash
3. Within 5 seconds put back the MEM jumper - reader orange LED SYSTEM will start to flash
4. The reader is ready for low-level configuration



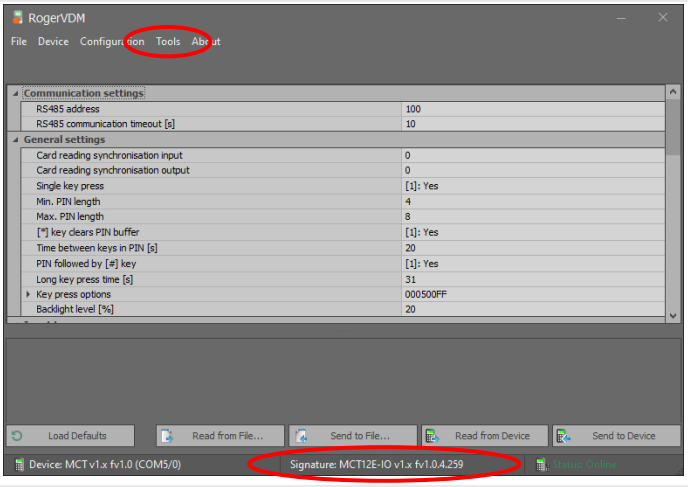
Connecting to the reader

1. Run the Roger VDM software.
2. In Roger VDM, select *Device->New*.
3. Select the device model, firmware version, communication channel COMx (RUD-1).
4. Click *Connect*, the program will connect to the reader and automatically go to the *Configuration* tab.



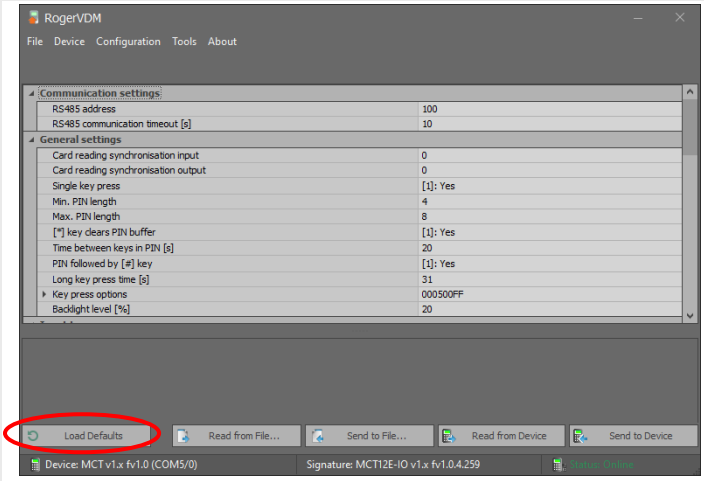
Firmware update

1. Make sure that the device has the newest firmware. The version currently installed on the device is displayed in the bottom bar of the application window. The latest versions of firmware can be downloaded from the website www.roger.pl.
2. To run the firmware update, disconnect (Device-> Disconnect), and then select Tools-> Update Firmware from the menu. For the UNIQUE readers (AR121 and AR131) to update firmware use RogerISP software available at www.roger.pl.

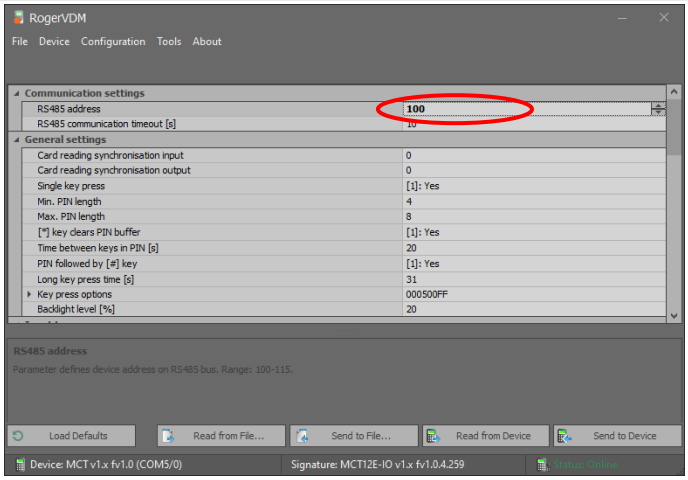


Configuring the reader

It is recommended to start a new configuration from restoring all default values.

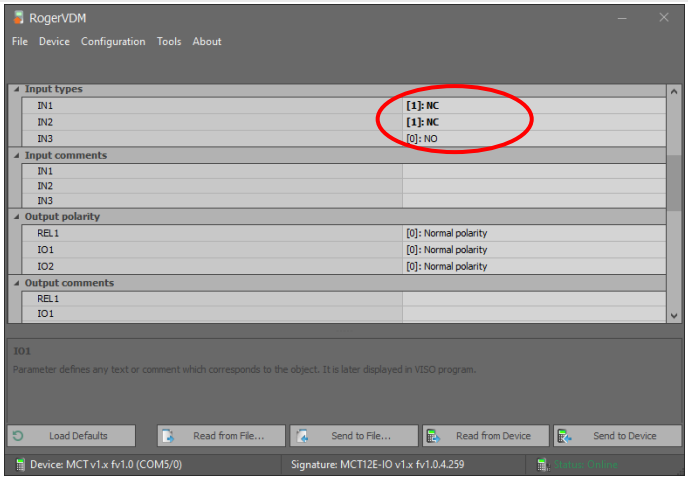


Each reader connected to the same controller (also via secondary sets AB101) must have a unique address. Each reader should be given an individual address in the range of 100 - 115, which gives the maximum number of 16 readers connected to the controller.



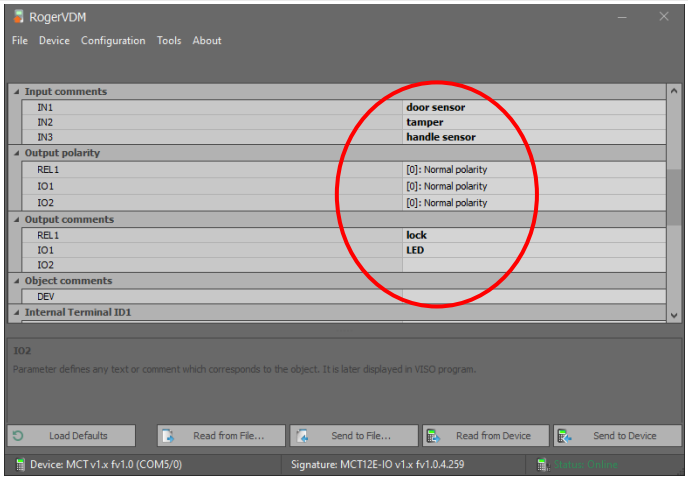
Set the IN1, IN2 and IN3 input type. Depending on the reader, these inputs are for the door sensor, tamper, door handle sensor, exit button and escape button sensor for the sliding door.
See these diagrams:
5.8 Diagram of functional circuits for operating the cabinet door
6.7 Diagram of functional circuits for operating the sliding door

AR121 & AR131 – for cabinet door	**AR122 & AR132 – for cold/hot aisle containment sliding door**
Input IN1 – NC	Input IN1 – NC
Input IN2 – NC	Input IN2 – NC
Input IN3 – NO	Input IN3 – NO

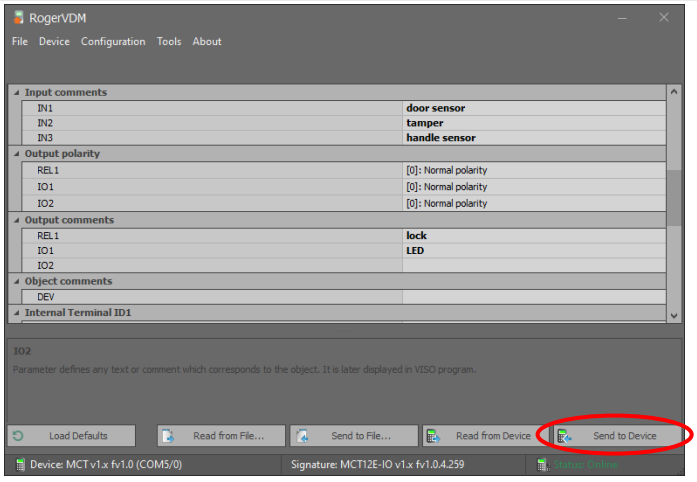


Describe the reader's inputs and outputs. These descriptions will be visible in the high-level VISO ST software, which can help you navigate between inputs and outputs during system configuration.

AR121 & AR131 – for cabinet door	**AR122 & AR132 – for cold/hot aisle containment sliding door**
Input IN1 – door sensor	Input IN1 – door sensor
Input IN2 – tamper	Input IN2 – emergency
Input IN3 – handle sensor	Input IN3 – exit button
Output REL – lock	Output REL – lock
Output IO1 - LED	Output IO1 - LED



Send settings to the device - click *Send to Device* button.



Ending the reader low level configuration

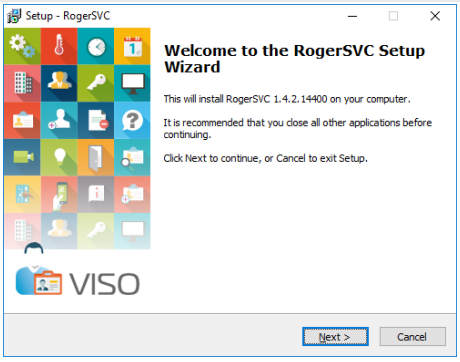
1. In Roger VDM menu select Device-> Disconnect.
2. Put the MEM jumper on the reader (only in AR131 and AR132)
3. Connect the reader back to the controller or slave set in the cabinet.

8 SOFTWARE

The Roger SVC software must be installed for the system to function properly. Once installed, the software runs as Windows service. The software is responsible for communication with system controllers and writing information to the database. The service package must be installed only on one computer, e.g. on a server.

8.1 SVC software installation

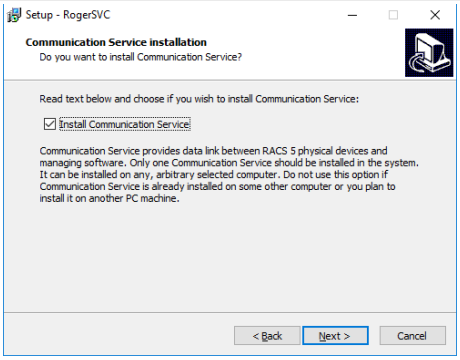
Download from http://www.roger.pl/en/and run the file RogerSVCSetup.exe. Then follow the windows that appear.



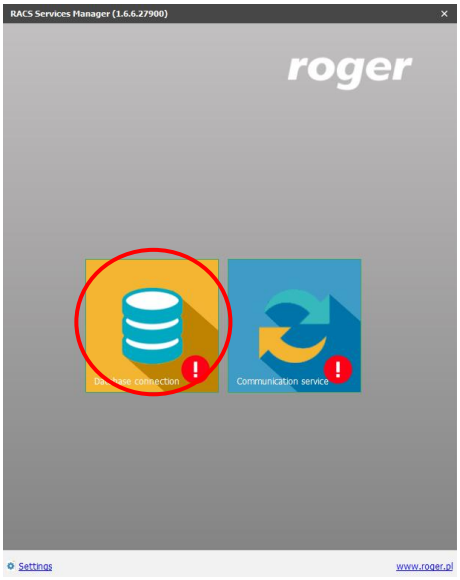
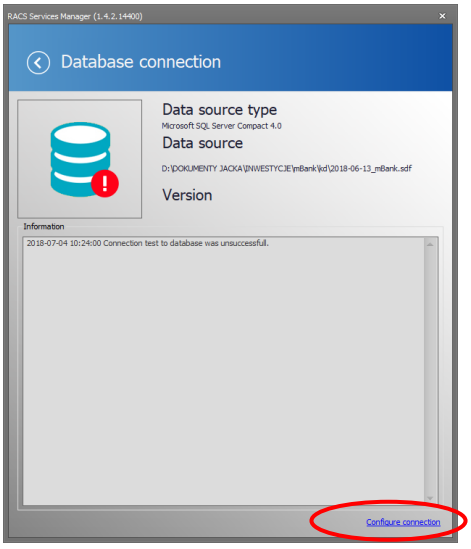
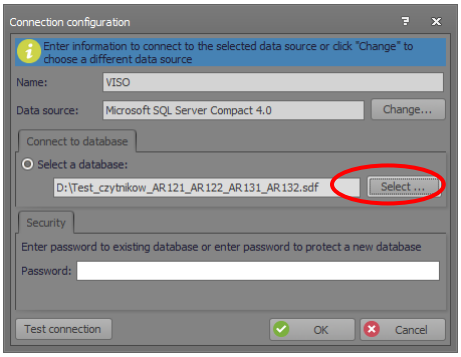
It is necessary to select *Install communication service*
Installing:

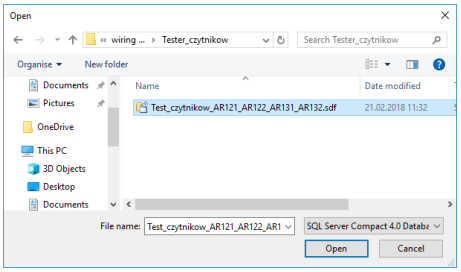
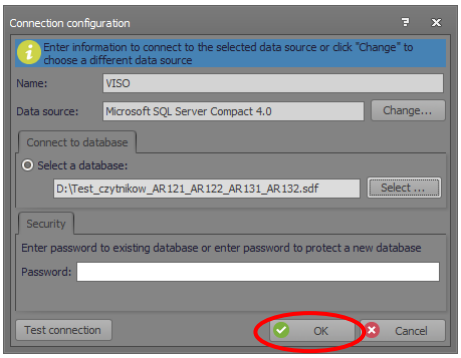
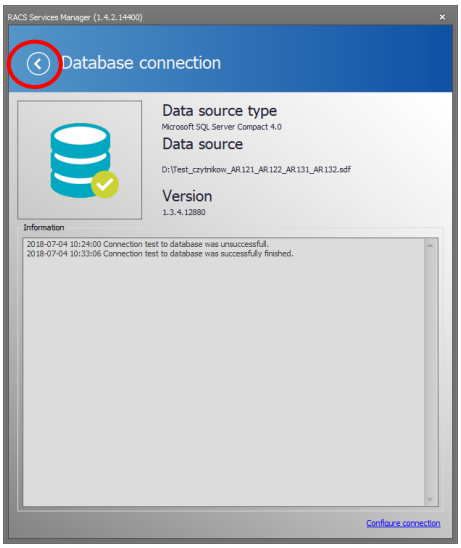
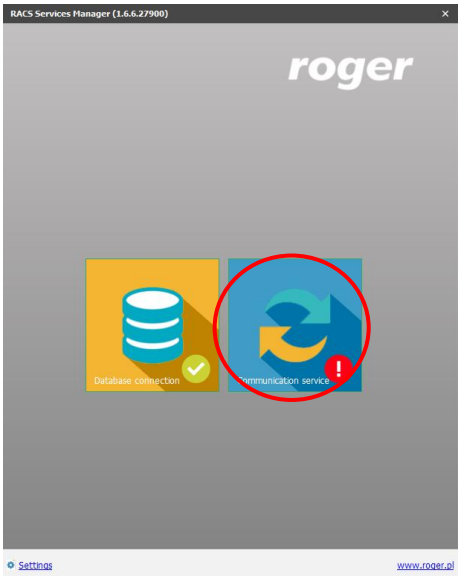
- *Licence service*
- *Integration service*
- *Virtual controller service*

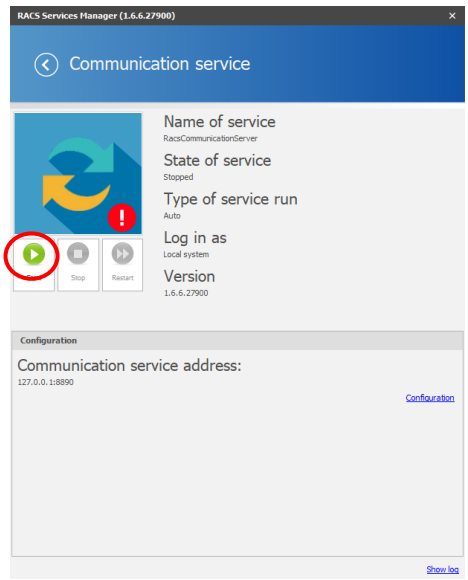
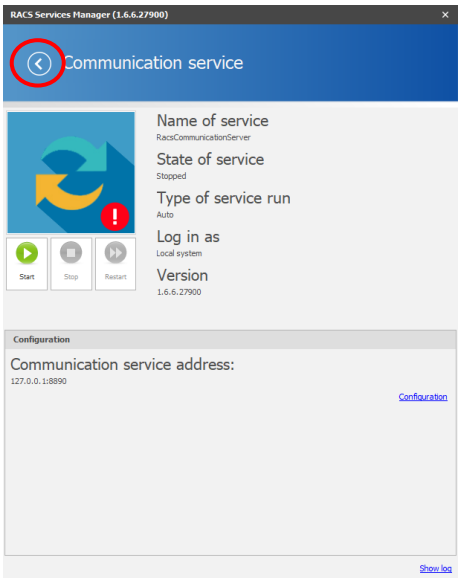
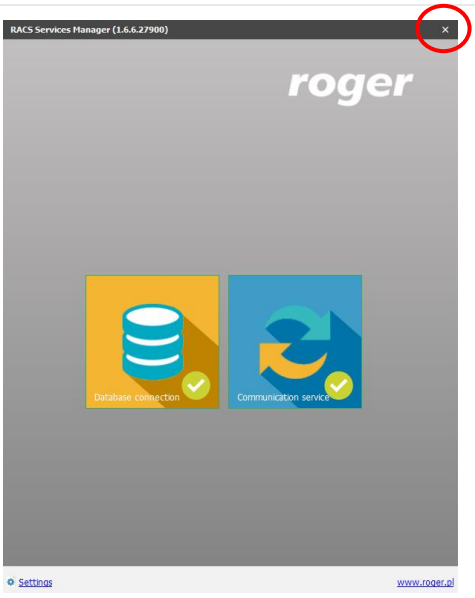
is not needed.



8.2 SVC software configuration

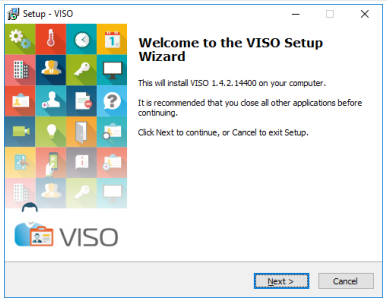
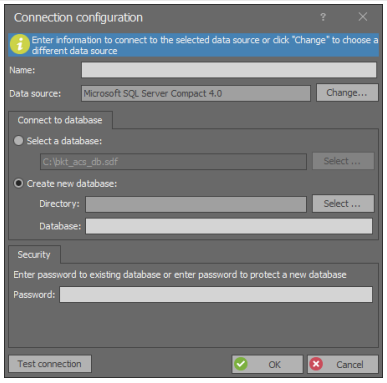
Open the service management application from the taskbar shortcut.	
Click on *Database connection*.	
Click on *Configure connection*.	
Click on *Select database*.	

Select the file with the database created in the VISO software and confirm. See section 8.4 Database configuration.	
Enter the database password if it was created and click *OK*.	
Go back to the main window.	
Click on *Communication service*.	

Click *Start*	
Go back to the main window.	
Services have been configured. Close the window.	

8.3 VISO ST software installation

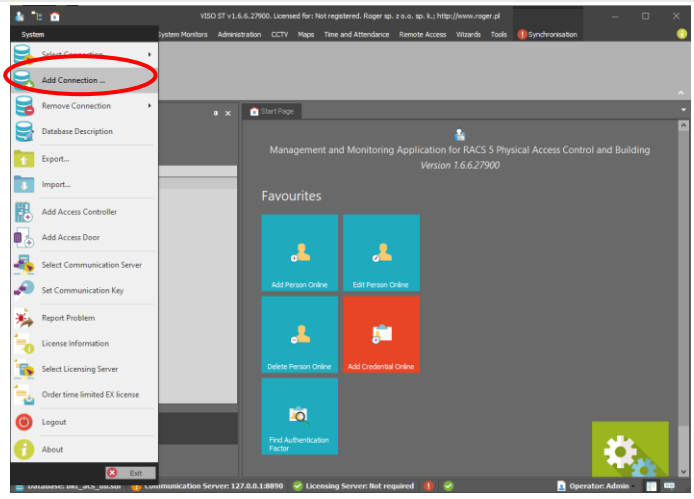
Roger VISO ST software is used to configure and manage the RACS5 access control system. In the case of multi-user work, the software must be installed on every computer from which the system will be managed

Download from www.roger.pl/en/ and run the VISOSetup.exe file. Then follow the windows that appear.	
After installation, the first time you run the program, you must configure the database access. See section 8.4 Database configuration.	

8.4 Database configuration

The database stores information including system configuration, system users data and events occurring during system operation.

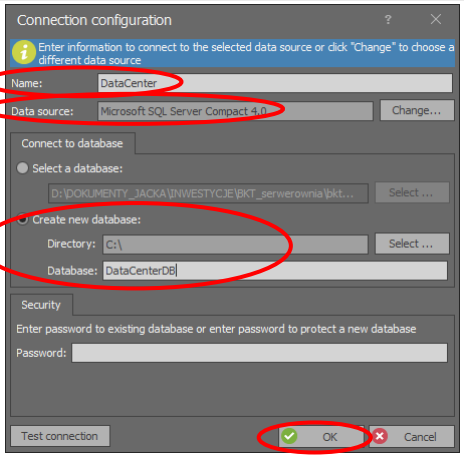
NOTE: from version 2.0, the VISO program works only with the MS SQL Express/Server database.

To add a new connection to the database, select *System->Add Connection* If this is the first time you run VISO, go to the next step.	

File database configuration:

NOTE: from version 2.0, the VISO program works only with the MS SQL Express/Server database.

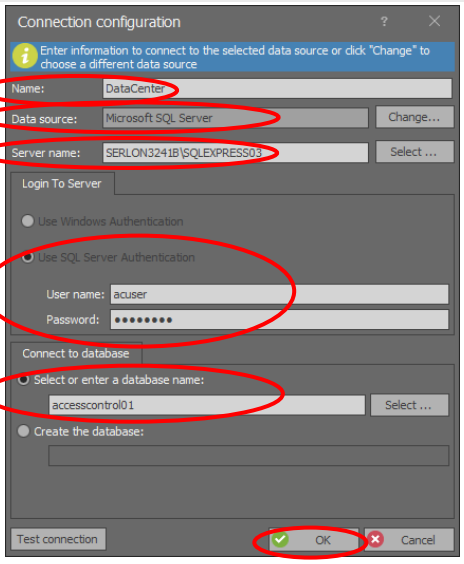
- Enter the name of the connection to the database in the *Name* field.
- Select *Create new database*.
- Select *Directory* where you want to save the database file.
- Enter the name of the database file in the *Database* field.
- Optionally enter a password to protect access to the database.
- Confirm by clicking OK.



Configuration of the server database:

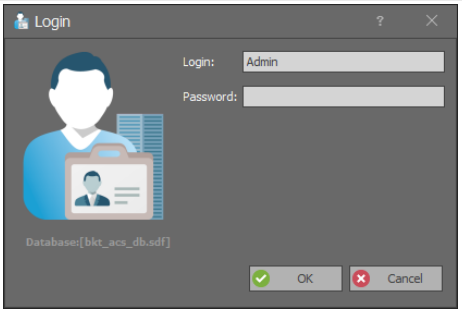
The database and its user should be previously created on the SQL server.

- Enter the name of the connection to the database in the *Name* field.
- Select an SQL server.
- Check *Use SQL Server database authentication* and enter database user details.
- Check *Select or enter a database name* and enter the database name you created earlier.
- Confirm by clicking OK.



After configuration, the software will restart using the created database.

In the newly created database, the administrator's access password is empty.



8.5 Migration from file to server database

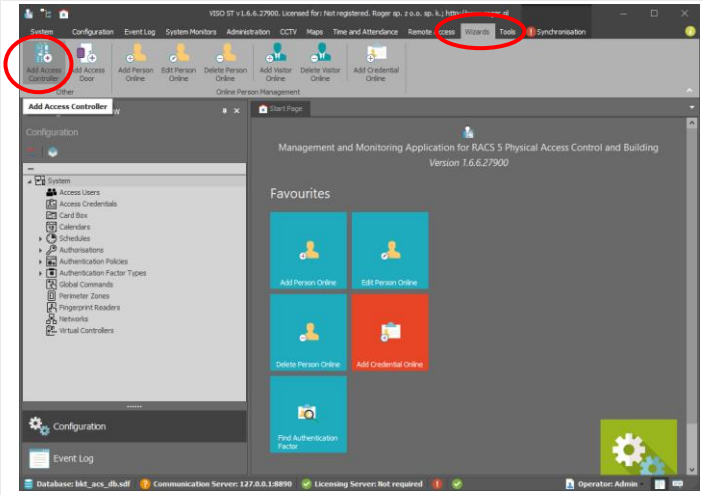
It is possible to transfer data from a file database to an MS SQL server database. This procedure is described in the application note AN-017 available on the website www.roger.pl.

9 SYSTEM CONFIGURATION

9.1 Controller configuration

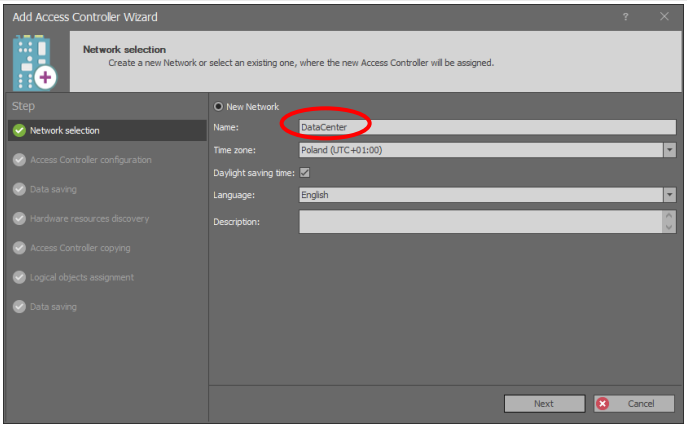
The system configuration should be started by adding a new controller.

- Choose Wizards->Add Access Controller.

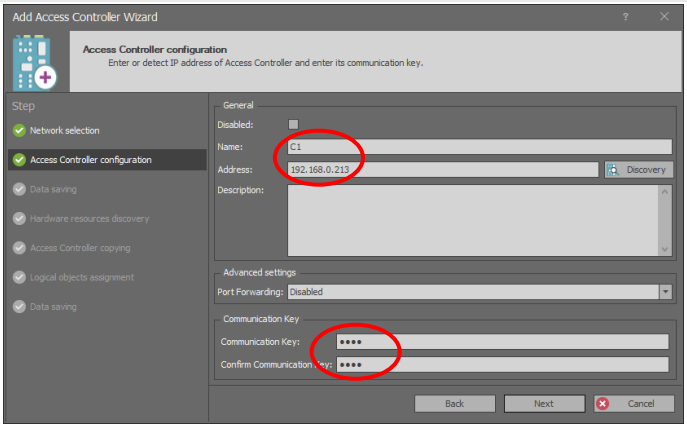


The controller can be assigned to a subsystem. Such dividing works well with large systems.

- Enter the name of the subsystem to which the controller will belong - eg. Server room or DataCenter.
- Click *Next*.

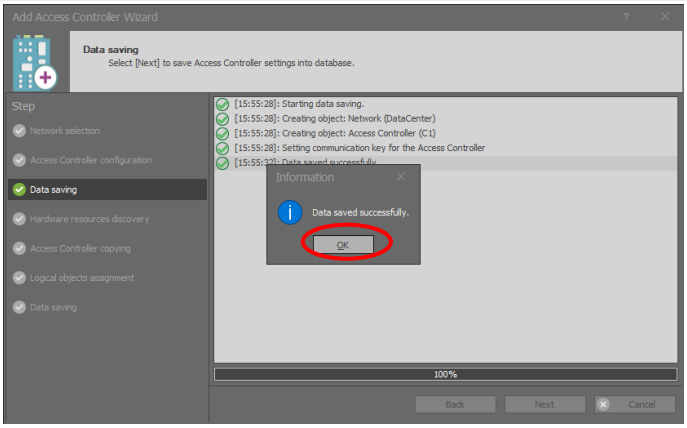


- Enter the name of the controller, e.g. C1.
- Enter IP address of the controller or click *Discovery*.
- Enter the communication password that was created during the low-level configuration of the controller. See section *7.1 Controller low level configuration*.
- Click *Next*.



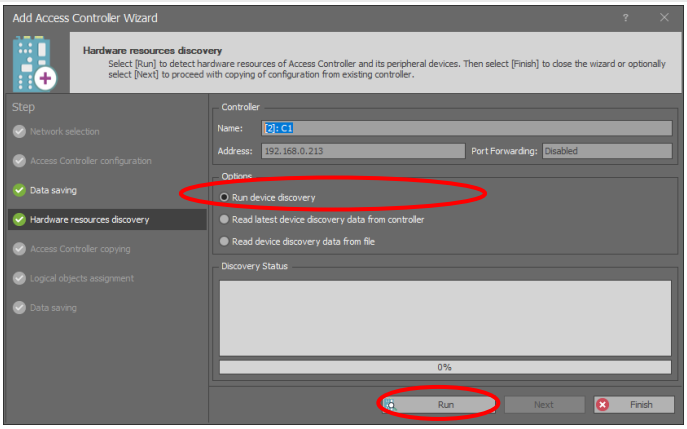
Settings are being saved to the database

- Then on the confirmation window click OK



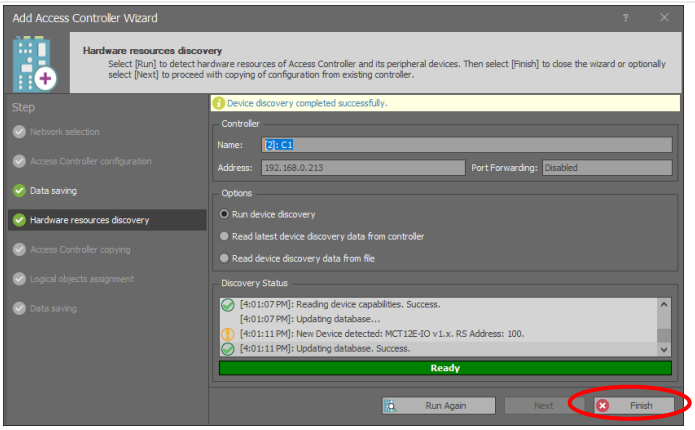
The controller will now search for readers that have been connected to the bus.

- Select *Run Device Discovery Process.*
- Click *Run*.



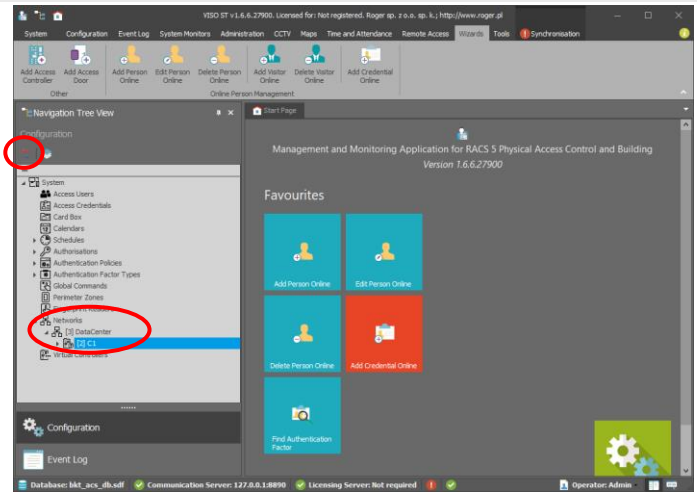
The controller and all the readers connected to it should appear on the list.

- Click *Finish.*



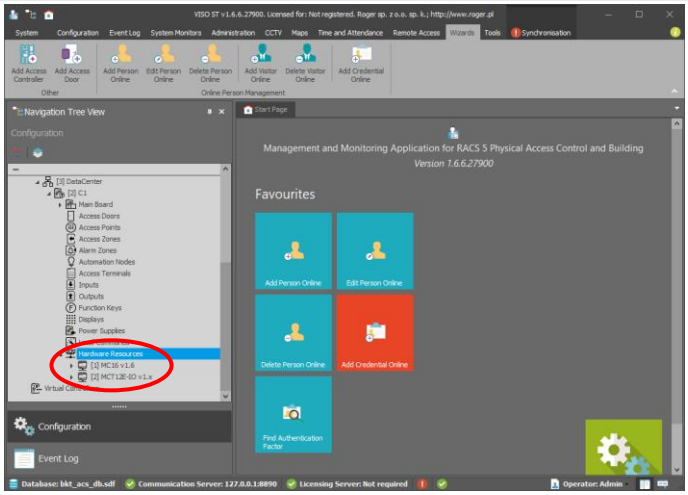
In the system tree view of main application window, the DataCenter subsystem should appear with the C1 controller, which just have been added. The system tree may need to be refreshed.

- In the tree view, expand *System->Networks.*



All system readers connected to the controller should appear in the system tree view.

- In the tree view, expand *System->Networks-> ->DataCenter->C1->Hardware Resources*



The above configuration should be sent to the controller. See chapter 9.3 Data synchronising.

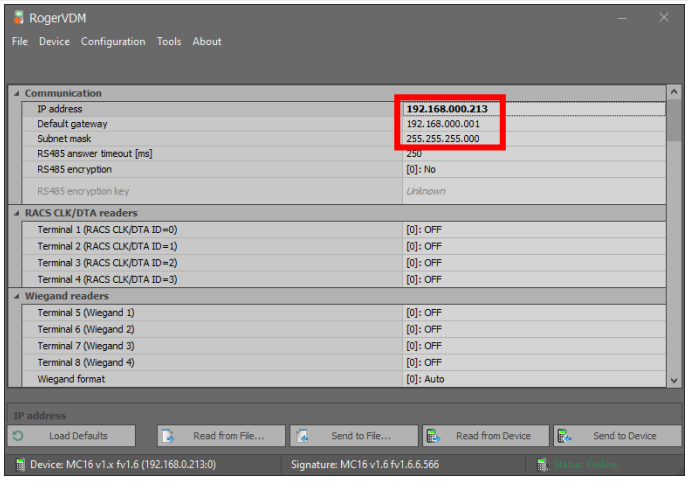
9.2 Changing the controller IP address

Changing the IP address of the controller is done in two stages. First you need to change the address during low level programming and then update it in the VISO application.

Carry out low-level configuration of the controller using RogerVDM software. Enter a new IP address. Follow the instructions in the chapter *7.1 Controller low level* configuration.

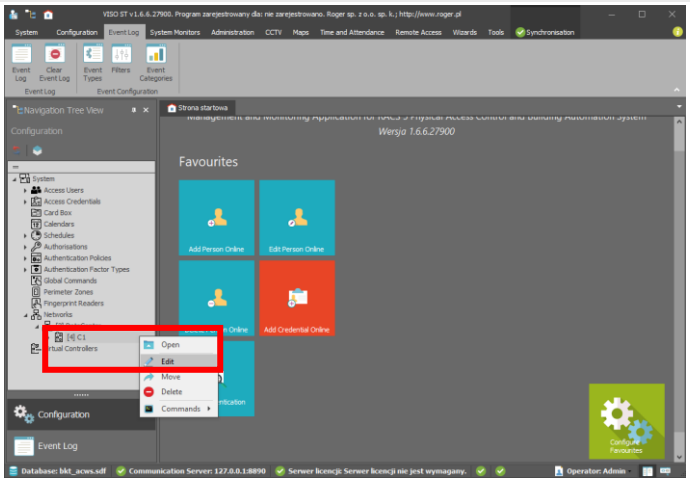
Make sure that the configuration process has been completed by restarting the device. To do this:

- In RogerVDM, select *Device->Disconnect*.
- The controller will restart.

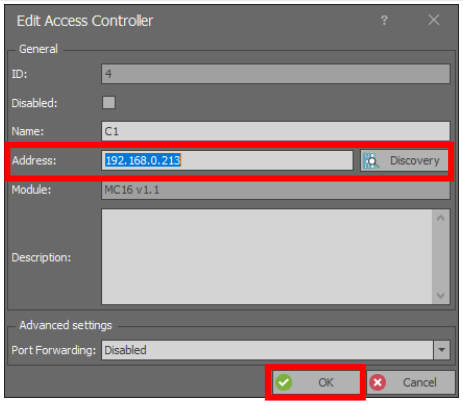


Update the data in the VISO program. For this purpose:

- In the tree view, right click *System->Networks->DataCenter->C1->Edit*

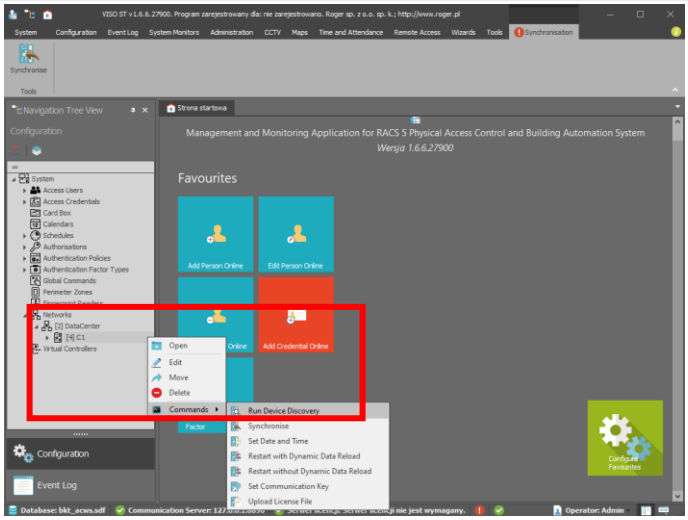


- In the popup window, enter a new IP address
- Click *OK*

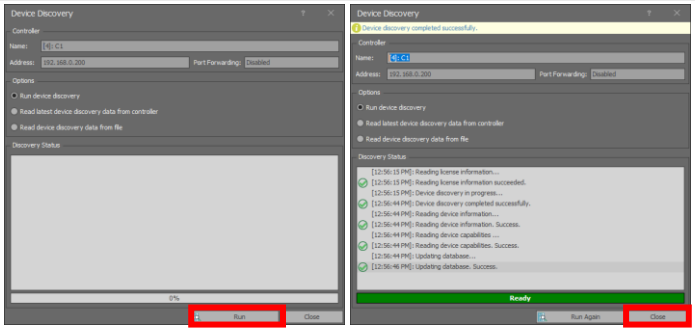


It is still necessary to discover devices again.

- In the tree view, right-click *System->Networks->DataCenter->C1->*Commands-> *->Run Device Discovery*



- Click *Run*
- Then *OK* when finished

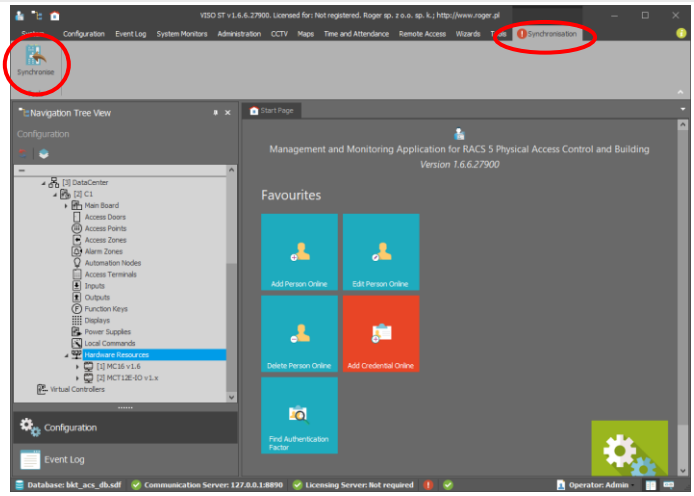


- Perform data synchronization. See chapter 9.3 Data synchronising.

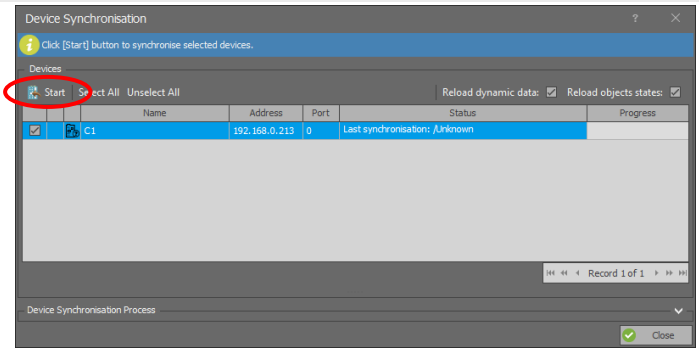
9.3 Data synchronising

Data synchronisation is an uploading to the system controllers the configuration created in the VISO software. For this purpose:

- Choose *Synchronisation* tab.
- Then click *Synchronise.*

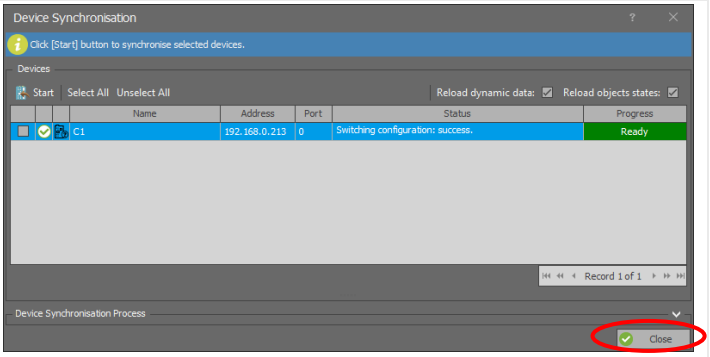


- In the pop up window, you can select the controllers to participate in the synchronisation.
- Then click *Start.*



Correctly completed process of data synchronisation with controllers is indicated by a green field next to each of them.

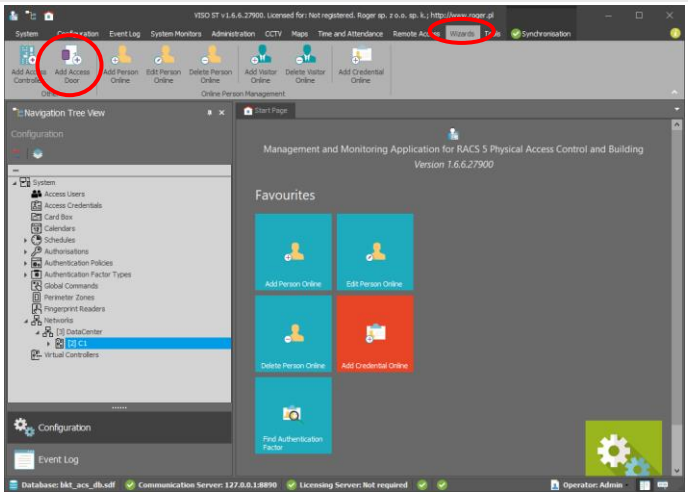
- Click *Close.*



9.4 Cabinet door configuration

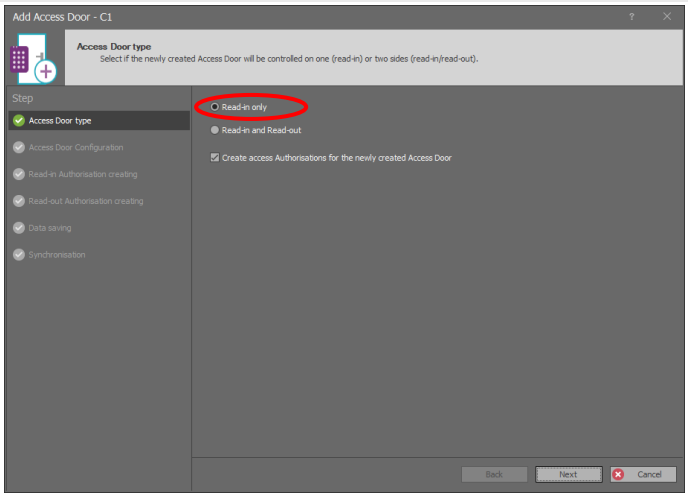
To start the door configuration::

- Choose *Wizards->Add Access Door.*

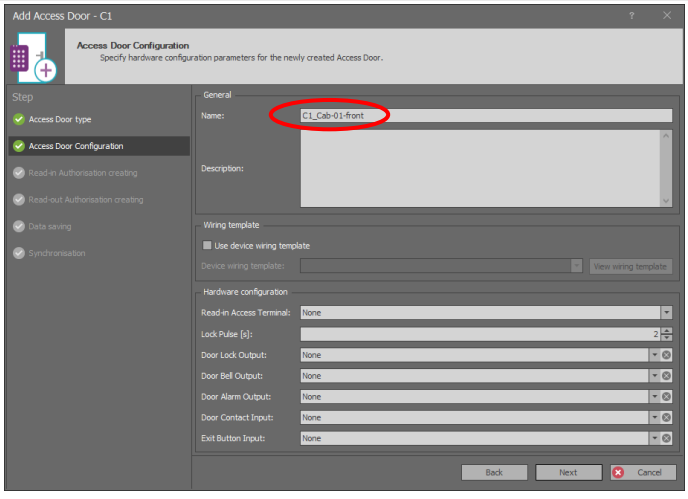


In the pop up windows:

- Choose Read-in only (the door with card reader on one side).
- Click *Next.*

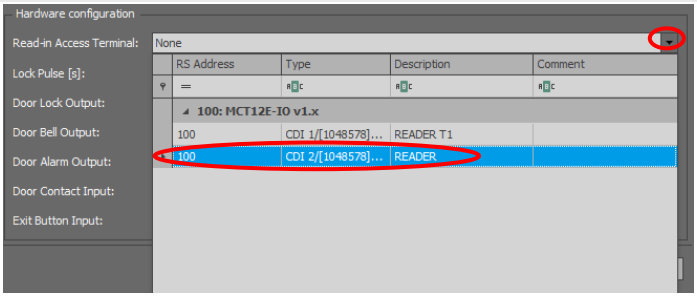


- Enter the door name eg. *C1_Cab-01-front*

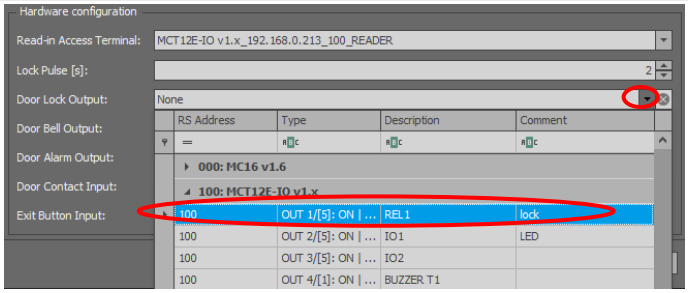


The hardware configuration of the door should be assigned: door reader, door sensor and a door lock control relay. For this purpose it is necessary to know which address has the reader installed on the configured cabinet door. In this example, only one reader with address 100 is displayed.

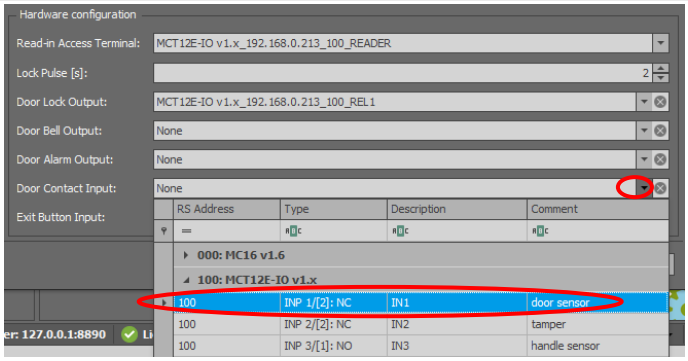
- Drop down the *Read-in Terminal* list and select *READER* from the appropriate card reader.



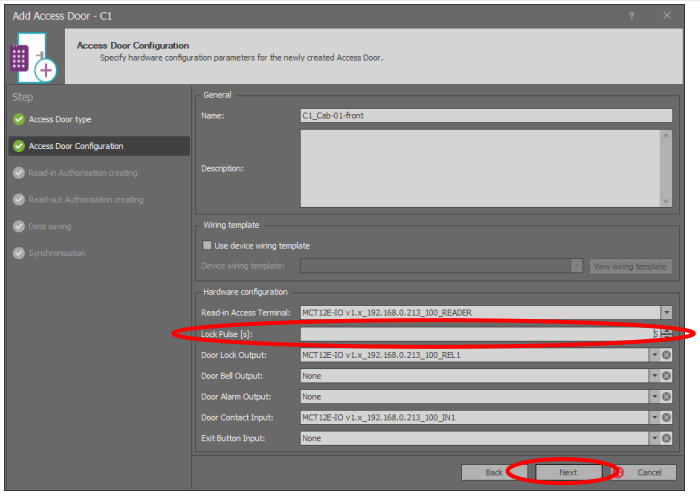
- Drop down the *Door Lock Output* list and select *REL1* from the appropriate card reader.



- Drop down the Door Contact Input list and select *IN1* from the appropriate card reader.

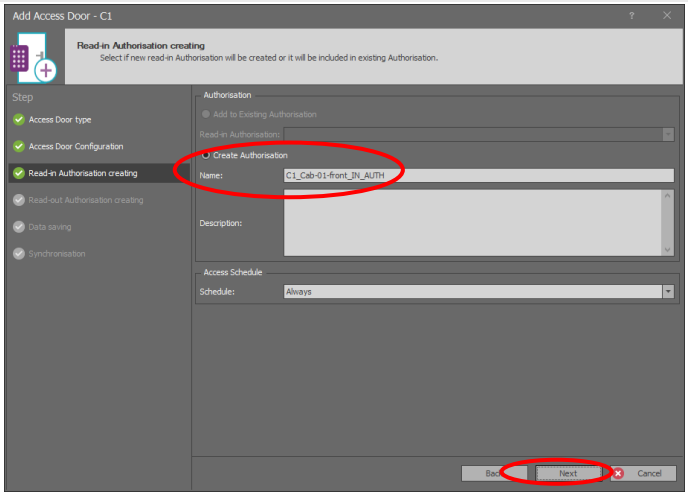


- Set the time to unlock the lock for 6s. This is the optimal unlocking time for cabinet electronic handles.
- Click *Next*

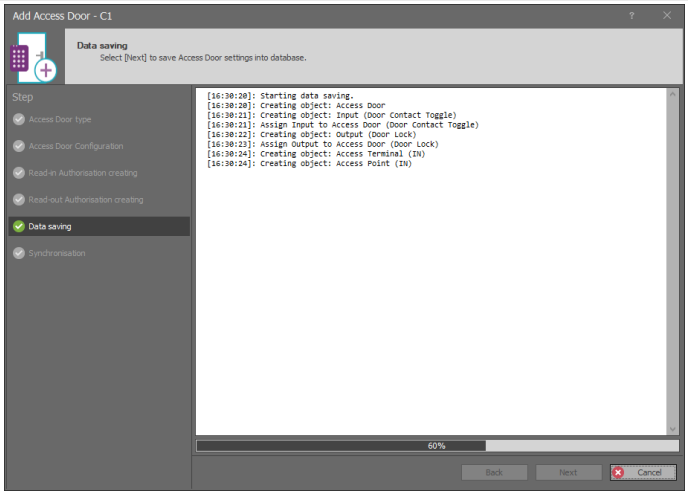


Create a new access authorization for this door. This authorization you will later be able to assign to a user group, so they could open that door. The program will suggest a name (C1_Cab-01-front_IN_AUTH).

- Choose *Create new Authorisation.*
- Click *Next.*

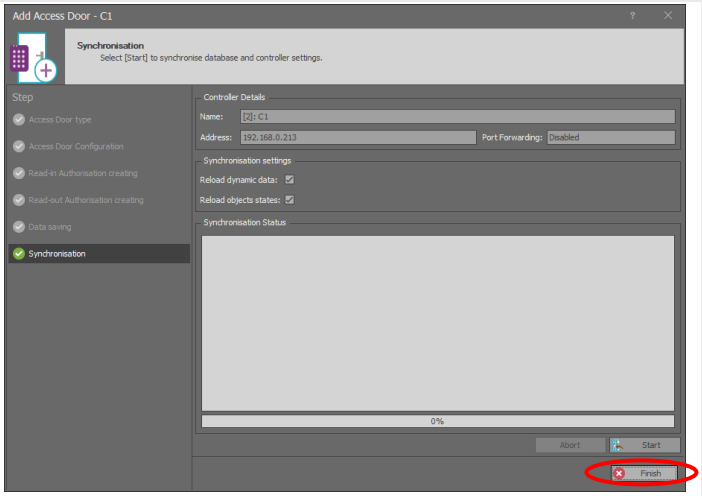


System saves the settings to the database.



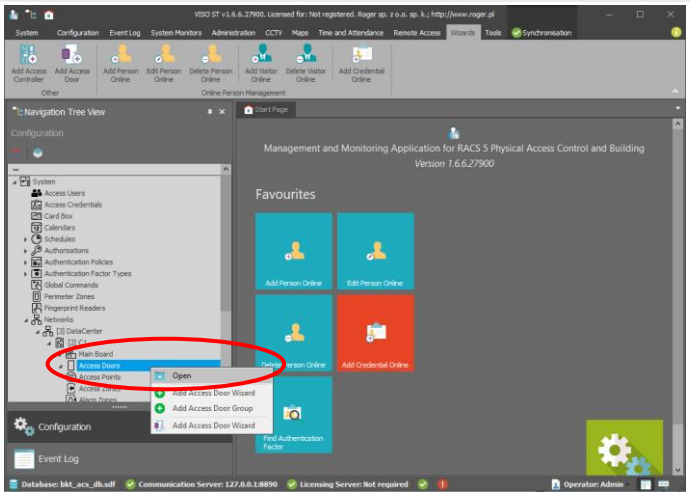
Do not perform synchronisation, yet (uploading settings to the controller).

- Click *Finish.*

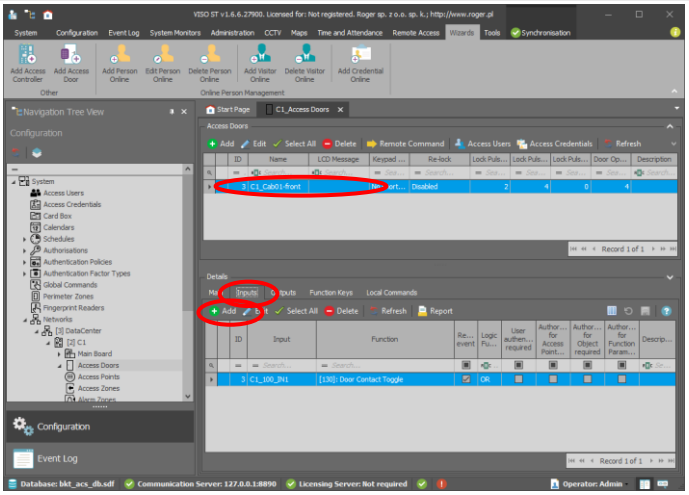


As the door sensor, only one input IN1-door sensor has been assigned to the door. It is necessary to assign the IN3 input - sensor of the handle. In this way, the system will recognize the door status as open when either door or handle is open.

- In the tree view, right-click on *System->Networks-> DataCenter->C1->Access Doors* and select *Open*.

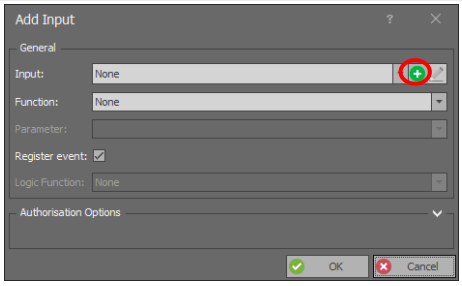


- Click on the door, which just has been added to the system – *C1_Cab-01-front.*
- Choose *Inputs* tab.
- Click *Add.*



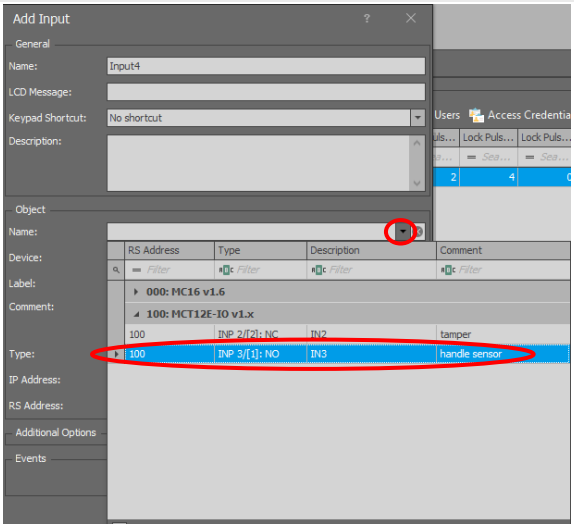
In the pop up window:

- Click on + in the field *Input.*



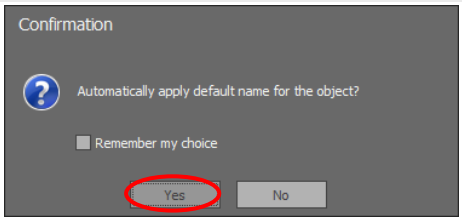
In the next pop up window select the input line where the swinghandle sensor is connected.

- Click on the drop down list in the field *Object->Name.*
- Select *IN3* input of the card reader MCT12x-IO which belongs to currently configured door.

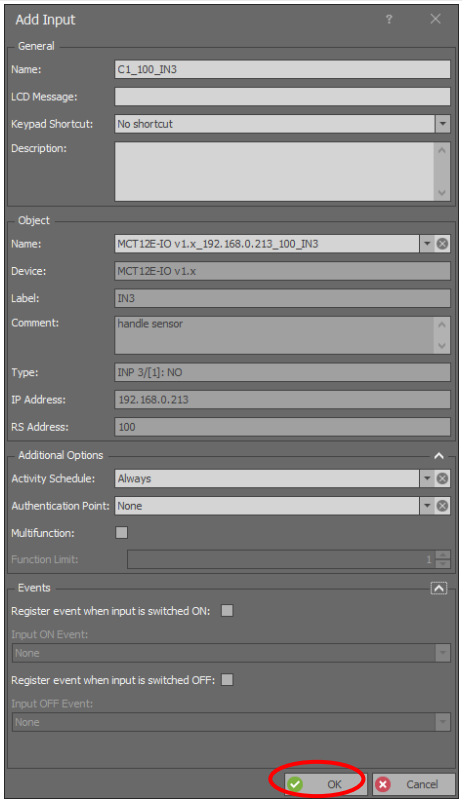


The program will propose a name for the selected object

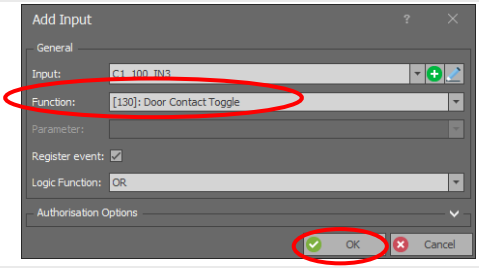
- Confirm the suggestion by clicking *Yes*



- Confirm the input line by clicking *OK*

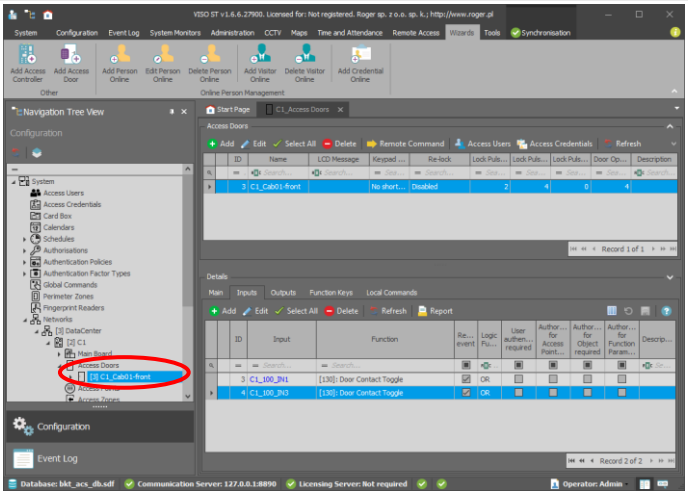


- In the *Function* field, select the function *[130]: Door Contact*
- Click *OK*



The cabinet doors have been configured and should appear in the system tree view.

- In the tree view expand *System->Networks->*
  ->DataCenter->C1->Access Doors

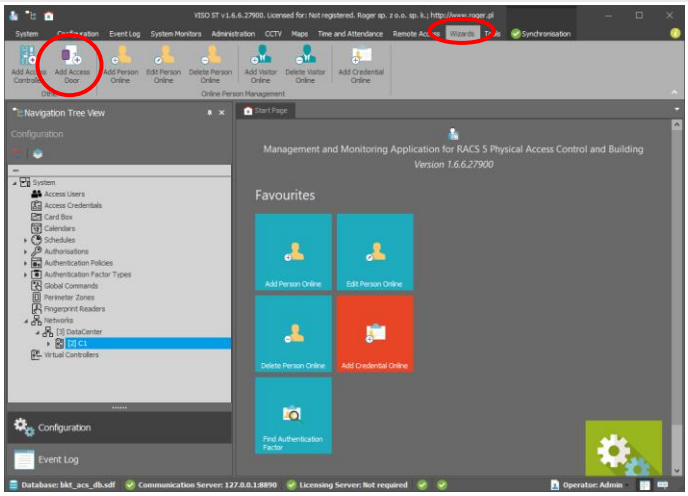


The above configuration should be sent to the controller. See chapter 9.3 Data synchronising.

9.5 Cold/hot aisle containment sliding door configuration

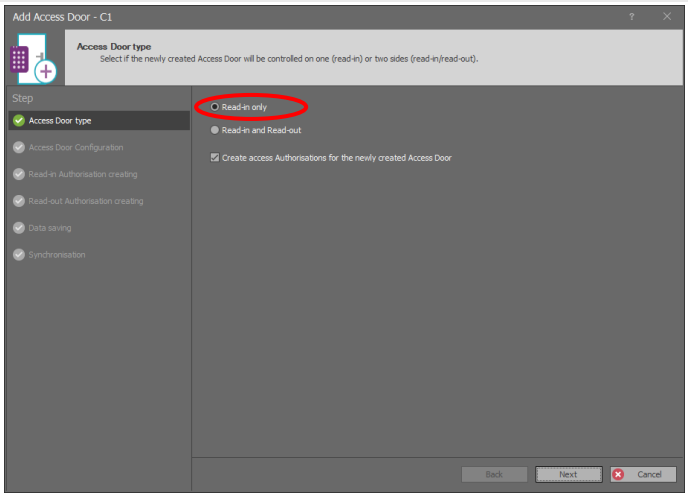
To start the door configuration::

- Choose *Wizards->Add Access Door.*

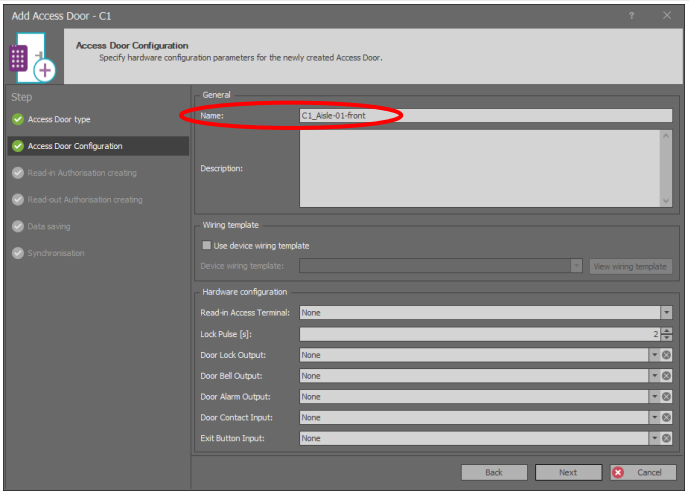


In the pop up windows:

- Choose Read-in only (the door with card reader on one side).
- Click *Next.*

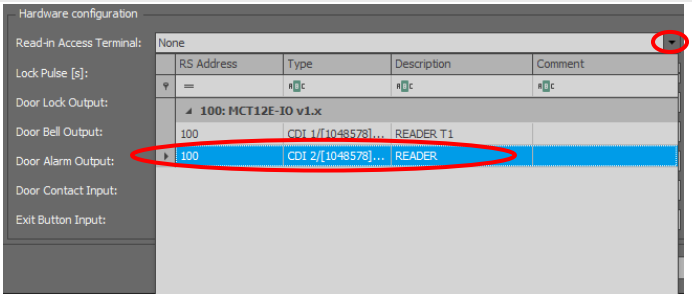


- Enter the door name eg. *C1_Aisle-01-front*

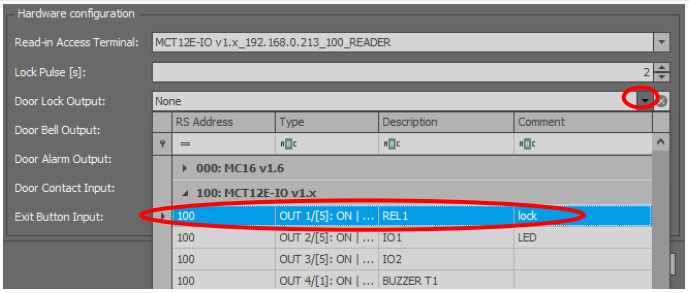


The hardware configuration of the door should be assigned: door reader, door sensor, door lock control relay and exit button. For this purpose it is necessary to know which address has the reader installed on the configured sliding door. In this example, only one reader with address 100 is displayed.

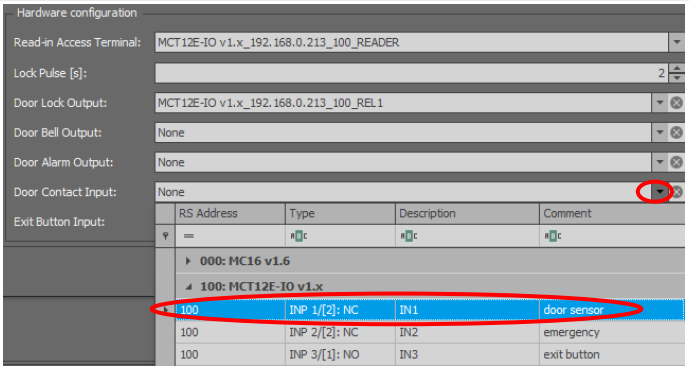
- Drop down the *Read-in Terminal* list and select *READER* from the appropriate card reader.



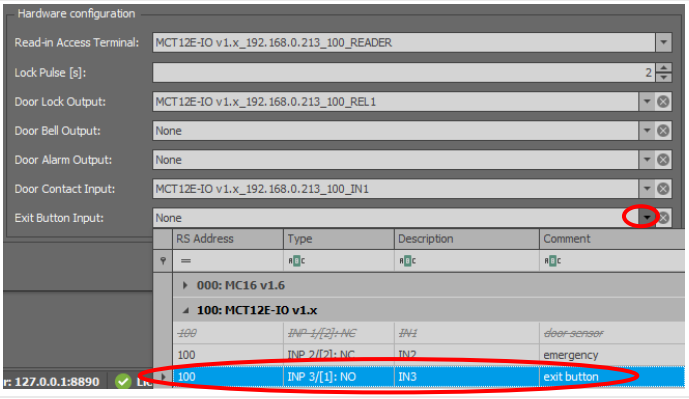
- Drop down the *Door Lock Output* list and select *REL1-lock* from the appropriate card reader.



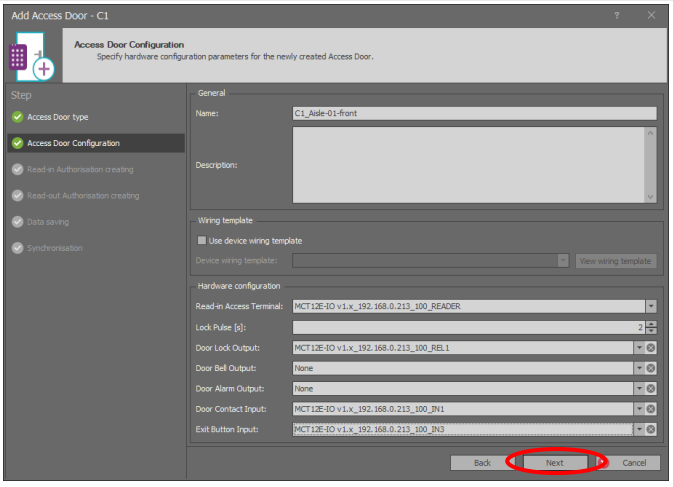
- Drop down the *Door Contact Input* list and select *IN1-door sensor* from the appropriate card reader.



- Drop down the *Exit Button Input* list and select *IN3-exit button* from the appropriate card reader.

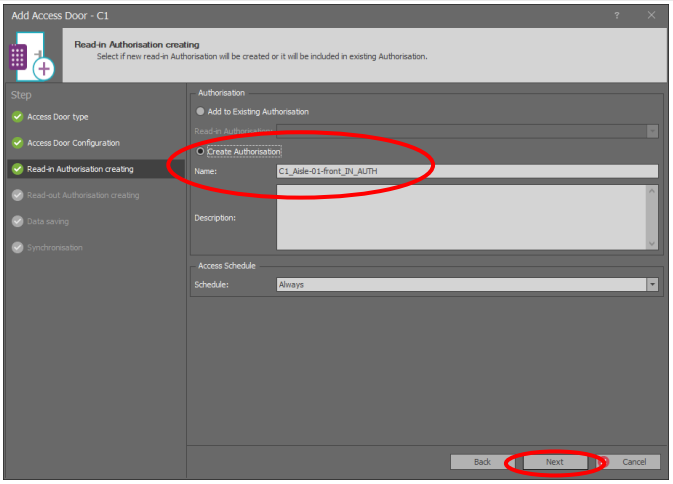


- Click *Next*.

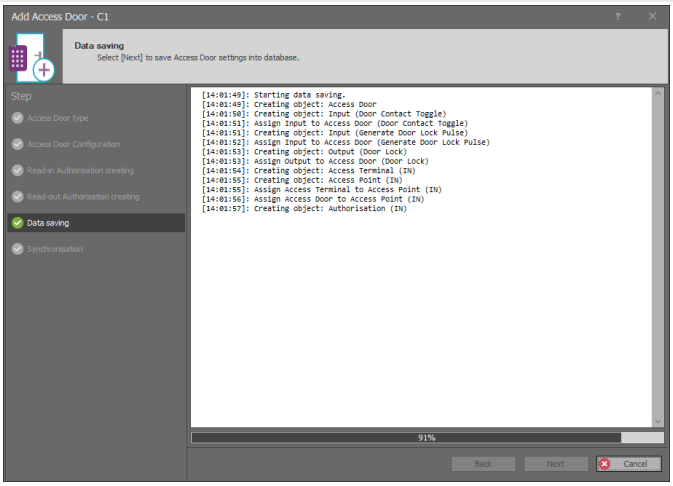


Create a new authorisation to access this door. This authorisation will then be assigned to the user so that he can open the door. The program will propose the name (*C1_Aisle-01-front_IN_AUTH*).

- Choose *Create new Authorisation*.
- Click *Next*.

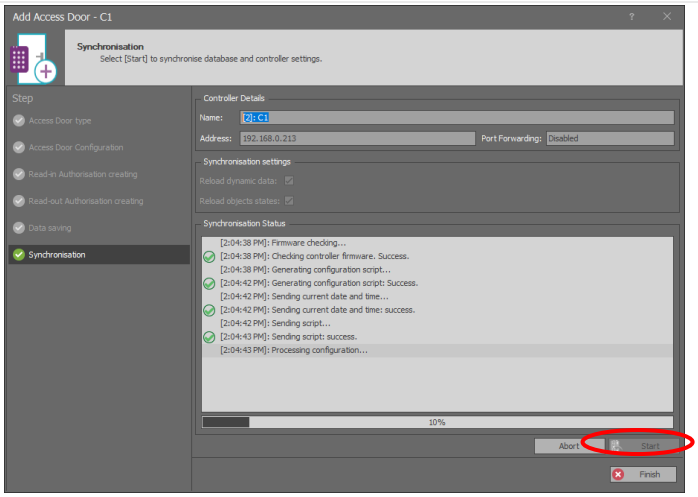


System savs the settings to the database.



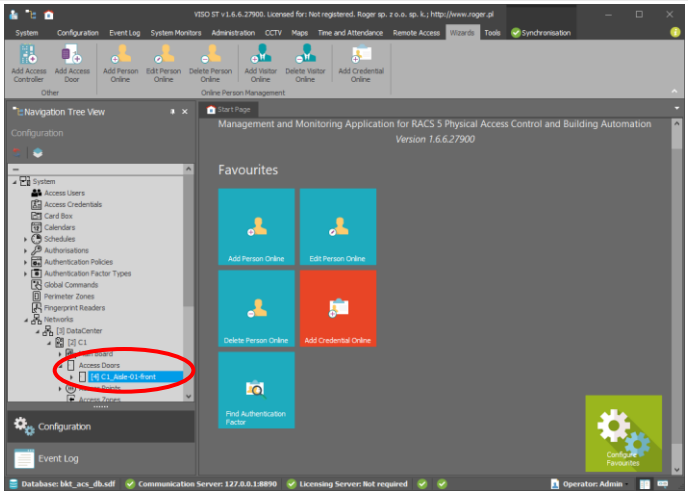
Upload the configuration to the device, that is, synchronise the controller.

- Click *Start*.
- After synchronisation click *Finish*.



The cold/hot aisle containment sliding door has been configured and should appear in the system tree view.

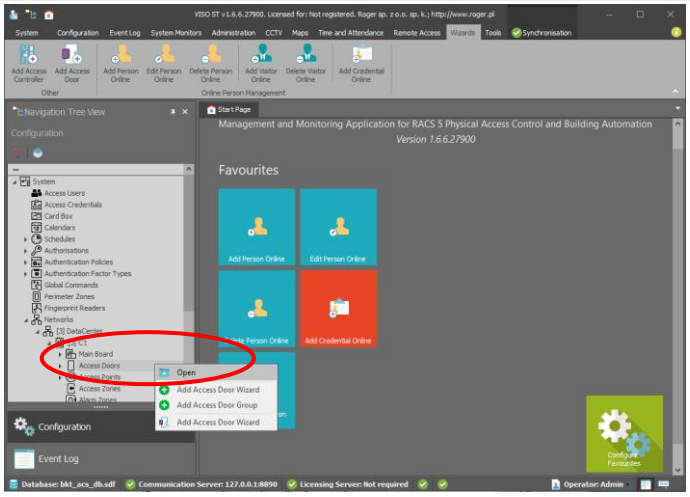
- In the tree view expand *System->Networks-> ->DataCenter->C1->Access Doors*



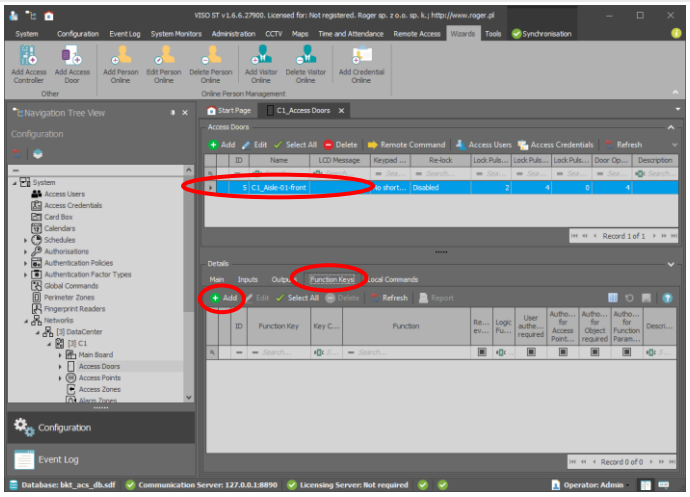
9.6 Permanent opening of the cold/hot aisle containment sliding door

Sometimes, while working in the server room, it is necessary to block the entrance door to the cold/hot aisle containment in a permanently open position. Pressing the F1 button on the door reader keypad and then applying the authorized user card will open the door and lock it in the open position. To close the door, press F1 and again apply the card.

- In the system tree view, click right on *System->Networks-> ->DataCenter (configurable name)> C1 (configurable controller name)-> Access Doors* and select *Open*

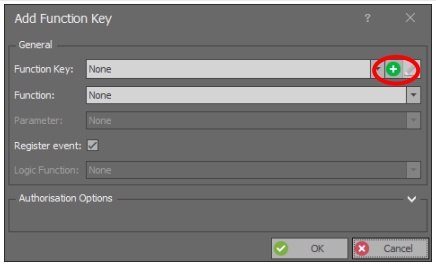


- Select the door of the aisle eg. *C1-Aisle-01-front.*
- Select *Function Keys* tab.
- Click *Add*.



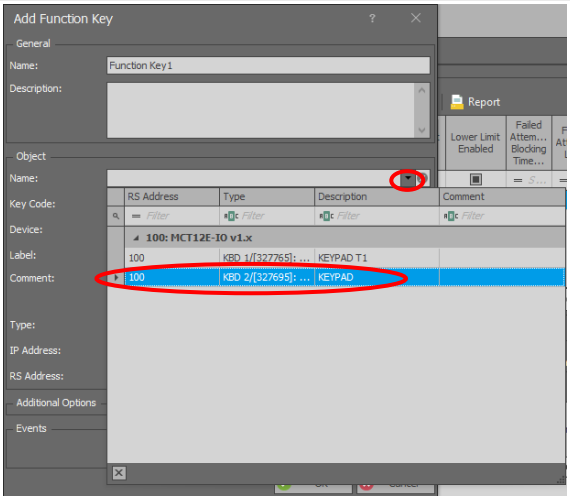
In the pop up window:

- Click on + in *Function Key* field



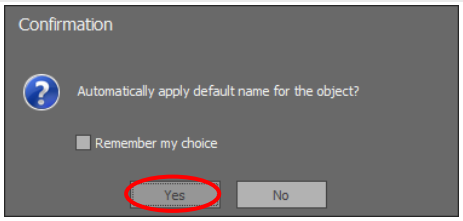
In the next window that opens, select the keypad of the cold/hot aisle containment front door reader:

- Drop down the *Object->Name* list and select *KEYPAD* of the reader, which controls aisle door.

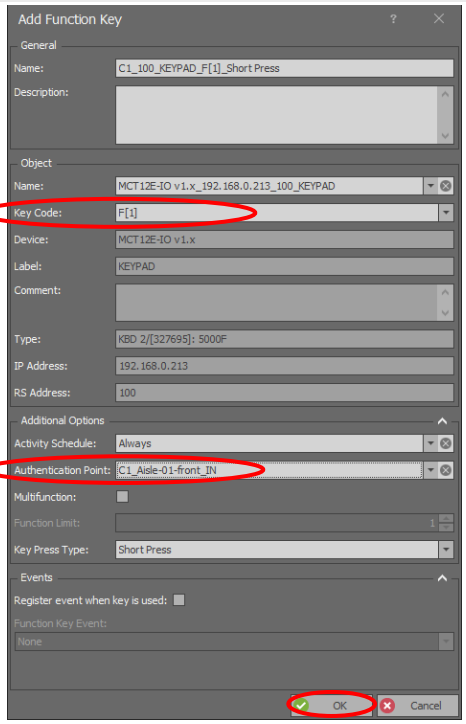


The program will propose a name for the selected object

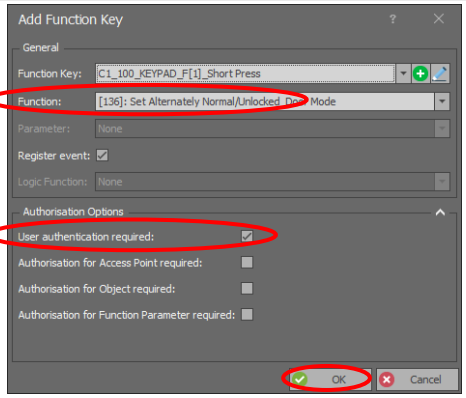
- Confirm the suggestion by clicking *Yes*



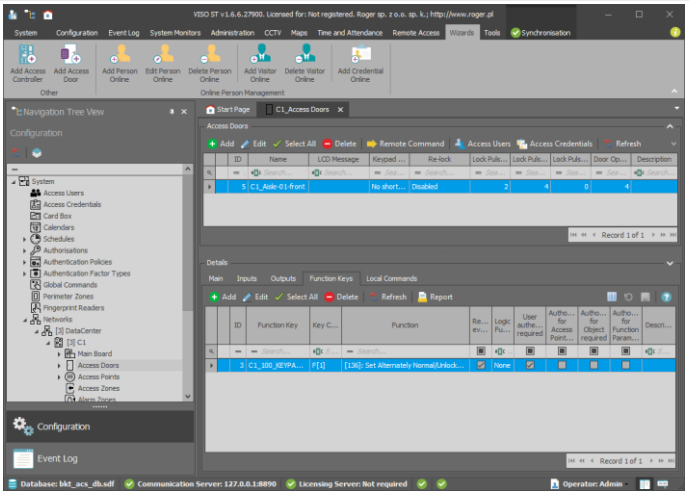
- Select *F1* key.
- Select *Authentication Point* (reader) of the cold/hot aisle containment door.
- Click *OK*



- Select Function *[136]:Set Alternately Normal/Unlock Door Mode*
- Tick *User Authentication required* option
- Click *OK*



The use of the F1 button has been. The above configuration should be sent to the controller. See chapter *9.3 Data synchronising*. After synchronization the controller will restart and it will be possible to use this functionality.



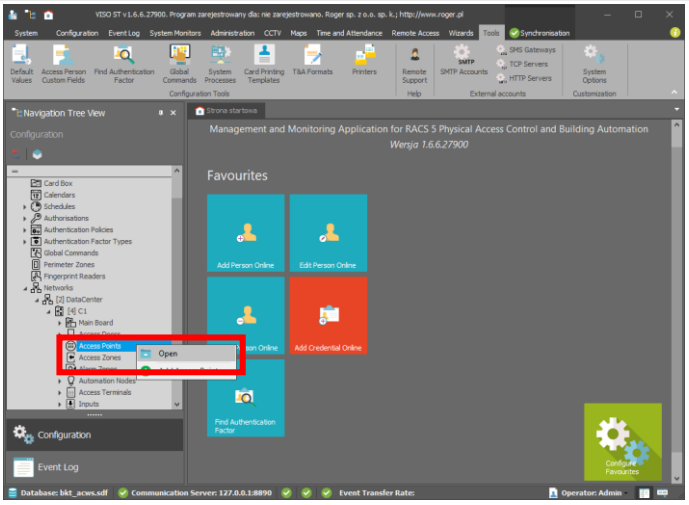
9.7 User identification by card and PIN code

By default, each door can be opened with a card or a PIN code. The system may require the user to hold the card and enter the PIN code at the same time to open the door.

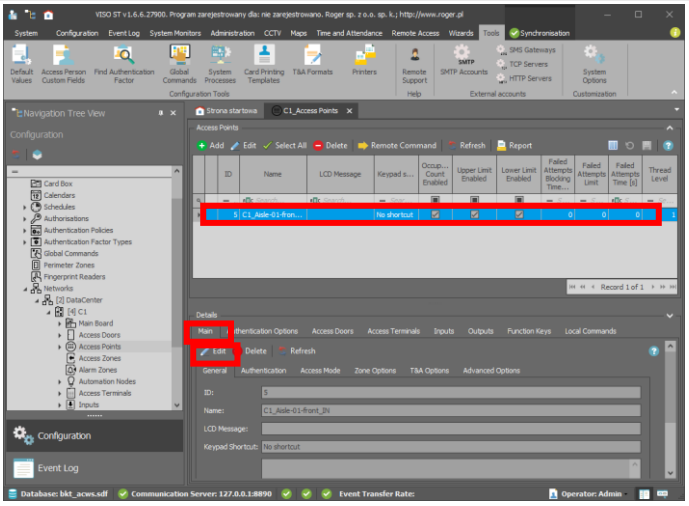
This function is assigned to the access point (reader), which means that the door configured in this way can only be opened by holding the card and entering the PIN code at the same time.

To start configuration:

- In the system tree right click *System->Networks->DataCenter->C1->Access Points* and select *Open*



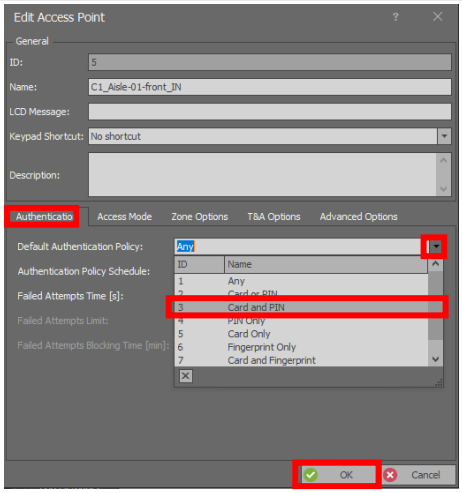
- Select the identification point (reader) to be configured as an input with two-factor identification
- Choose *Main* tab
- Select *Edit*



In the popup window:

- Choose *Authentication* tab
- Select *Card and PIN* from the *Default Authentication Policy* drop-down list.
- Click *OK*

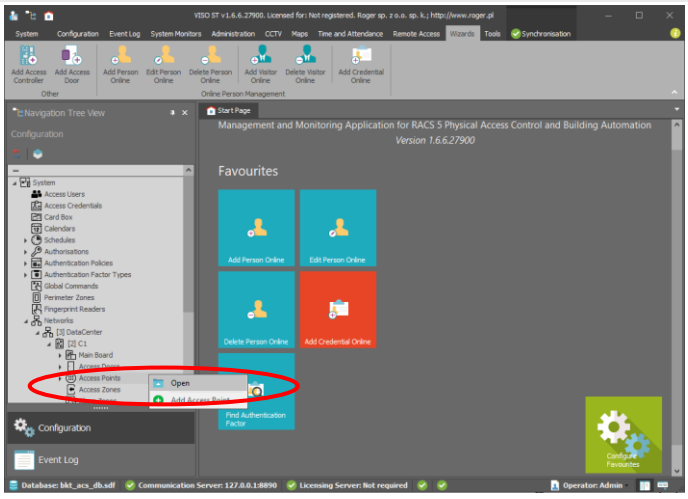
The door with the C1_Aisle-01-front_IN access point (reader) has been configured to be opened with a two-factor mode (card + PIN code).
The configuration made above should be sent to the controller.
See chapter *9.3 Data synchronising*.



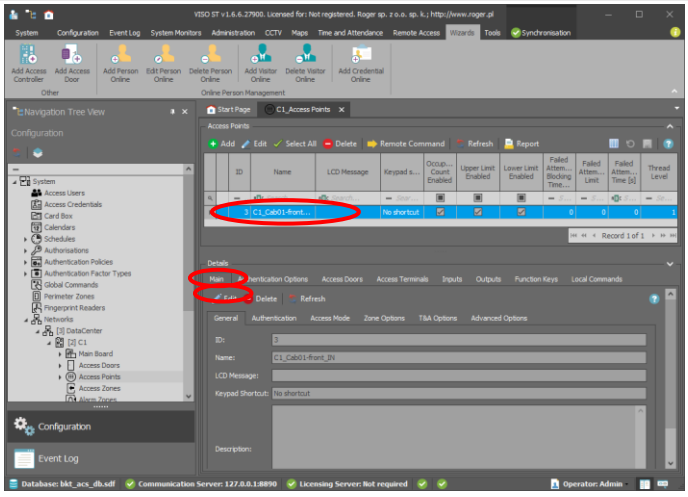
9.8 Two user entry

Two user entry means that two users have to apply the card to the reader in a short time to open the door. Both users must have permission to open this door. If more than two users have permission to open that door, then any two of them can do this.

To start configuration:
In the tree view click right on *System->Networks->DataCenter->C1->Access Points* and select *Open*

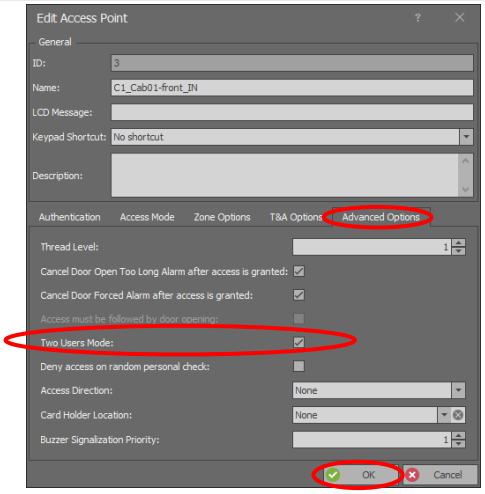


- Select required access point (card reader), which is to be configured as a two user entry.
- Select *Main* tab
- Select *Edit*

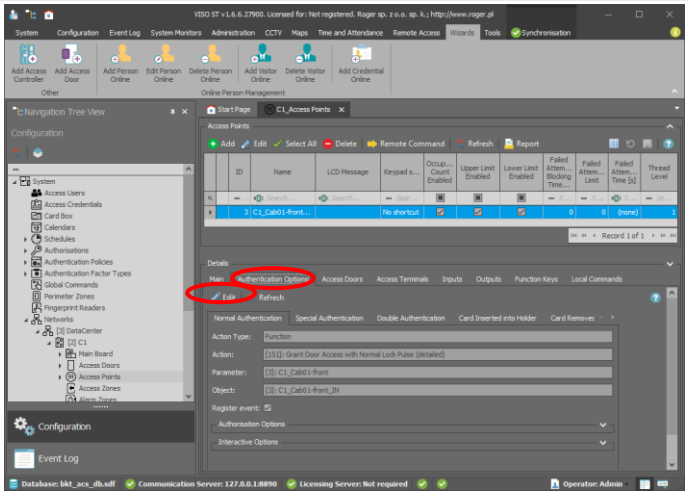


In the newly opened window:

- Select *Advanced Options* tab
- Tick *Two Users* box
- Click *OK*

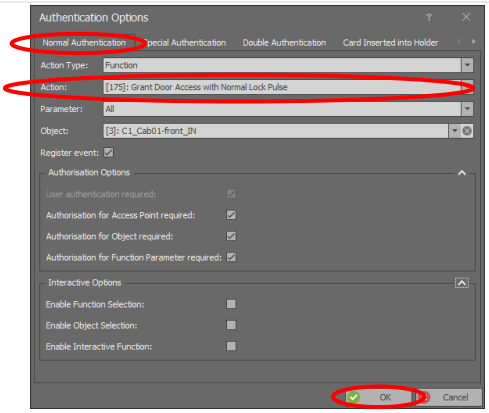


- Select *Authentication Options* tab
- Select *Edit*



In the newly opened window, in the *Normal Authentication* tab:

- In the *Action* field select the function [175]-Grant Door Access with Normal Lock Pulse
- Click *OK*



The door with the access point (reader) C1_Cab-01-front has been configured as a two user entry.
The above configuration should be sent to the controller. See chapter *9.3 Data synchronising*.

9.9 Open door signalling with LED

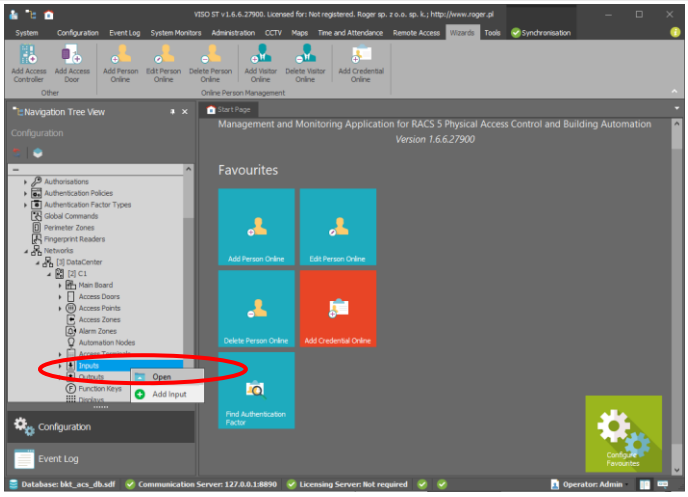
The system enables configuration of signalling LEDs located on the AC100 controller and the AB101 secondary set enclosures. These LEDs are connected to reader outputs

- LED1 – output OUT1 (IO1) of front door card reader
- LED2 – output OUT1 (IO1) of rear door card reader

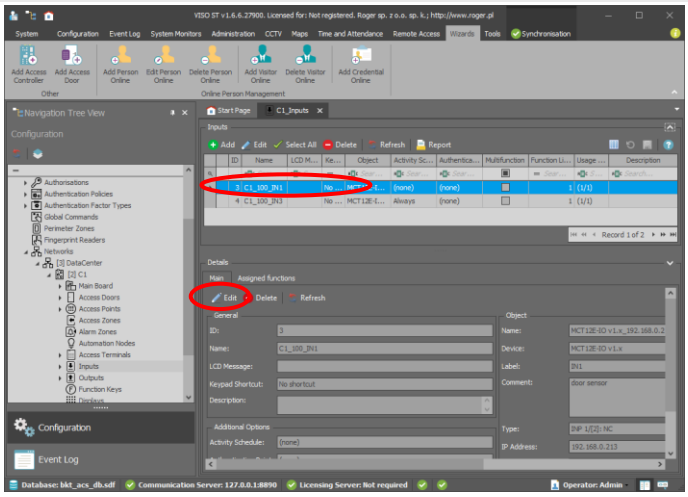
Please see *5.8 Diagram of functional circuits for operating the cabinet door*.

The LED1 will be configured as an indication that the front door of the cabinet is not closed. Similarly, LED2 may be configured to indicate that the rear door of the cabinet is not closed.
The input lines of the reader will be used to check the door status: IN1 - door sensor, IN3 - door handle sensor. Since these lines have already been assigned in the configuration of the door, in order to be able to use them again, you need to change their properties to the multifunctional lines.
For this purpose:

- In the system tree, right-click on *System->Networks-> ->DataCenter (configurable name)->C1 (configurable controller name)->Inputs* and select *Open.*

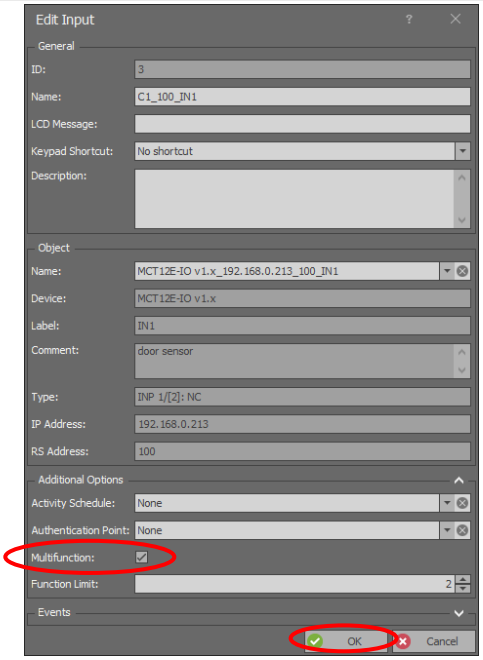


- Select input C1_100_IN1
- Click *Edit*



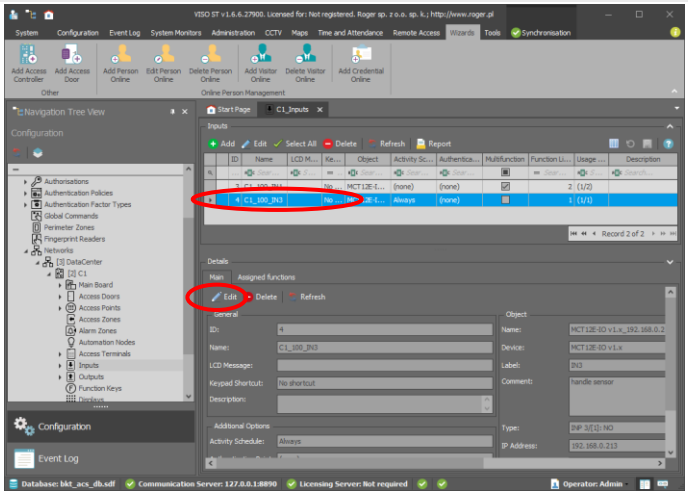
- Tick *Multifunction* option
- Click *OK*

Now you can use again the IN1-door sensor input for configuration.



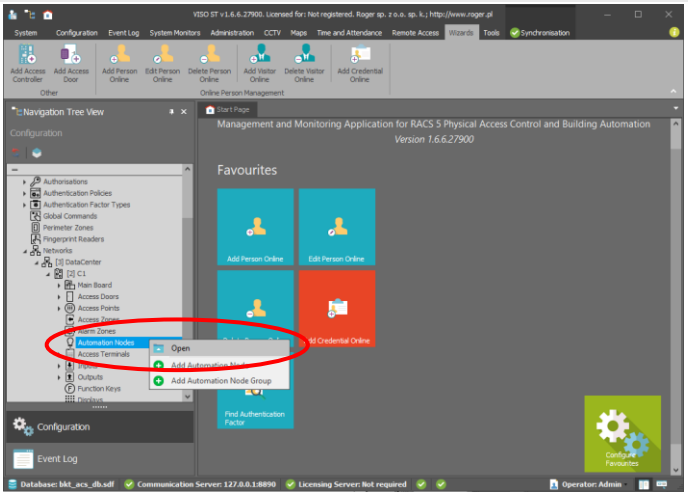
Similar actions should be performed for the line IN3-door handle sensor:

- Select input C1_100_IN3
- Click *Edit*
- Tick *Multifunction* option
- Click *OK*
- Now you can use again the IN3-door handle sensor input for configuration.



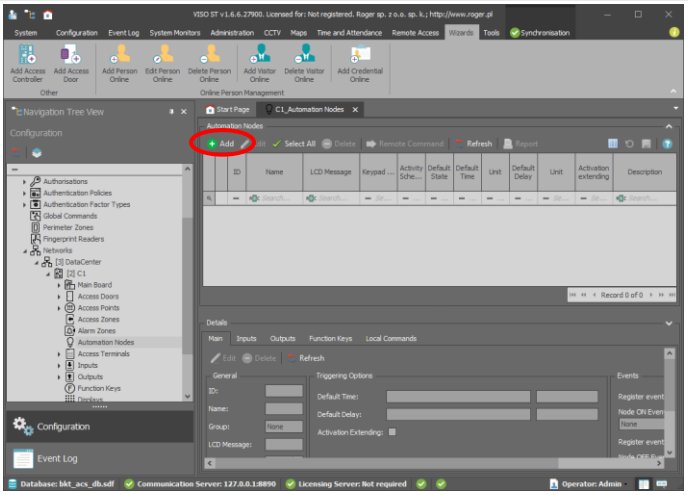
The configuration process of the automation node that will be responsible for the LED1 control:

- In the system tree, right-click on *System->Networks-> ->DataCenter (configurable name)> C1 (configurable controller name)> Automation Nodes* and select *Open*



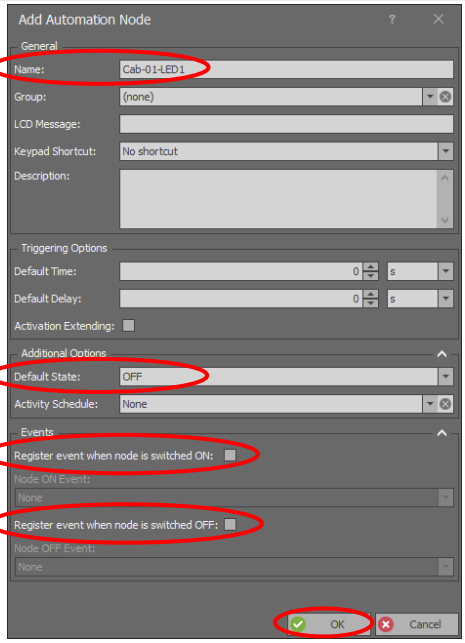
A new automation node should be created that will be responsible for controlling the LED:

- Click *Add*



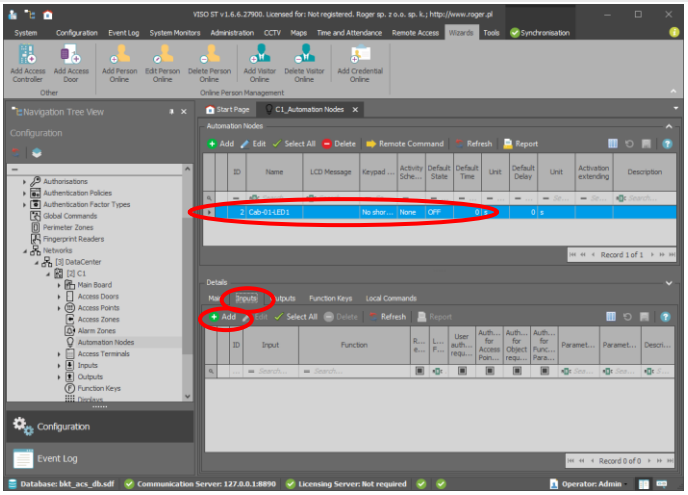
In the pop up window:

- Enter the node name eg. Cab-01-LED1
- Click *OK*
- Set *Default State* to *OFF*
- Untick *Register events*. It is not necessary to log LED events.
- Click *OK*



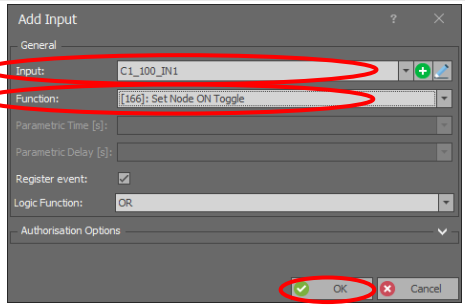
It is now necessary to add input lines that will affect the state of the LED1:

- Select just created automation node *Cab-01-LED12.*
- Click on *Inputs* tab.
- Click *Add.*

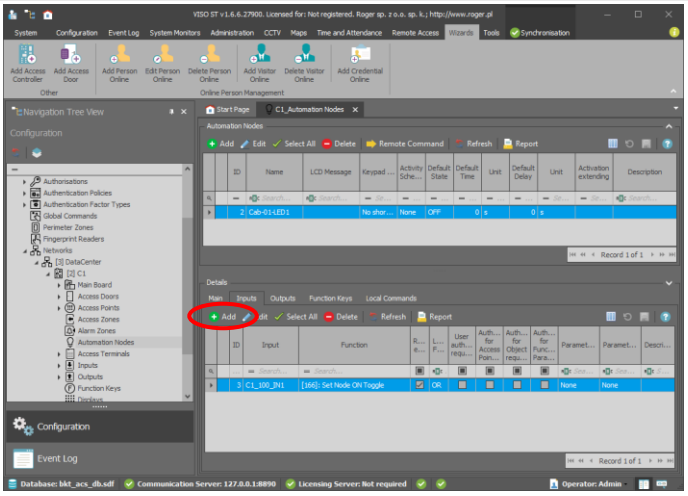


In the pop up window:

- Drop down the *Input* list and select available *IN1* line (door sensor)
- Drop down the *Function* list and select *[166]: Set Node ON Toggle*
- Click *OK*

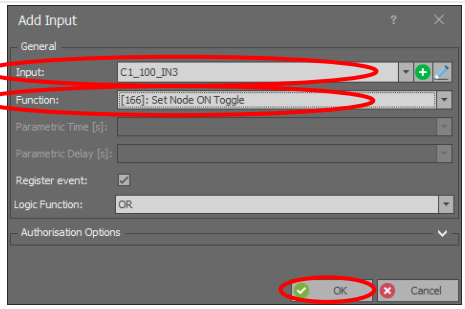


- Click *Add* again to choose IN3 input of door handle sensor



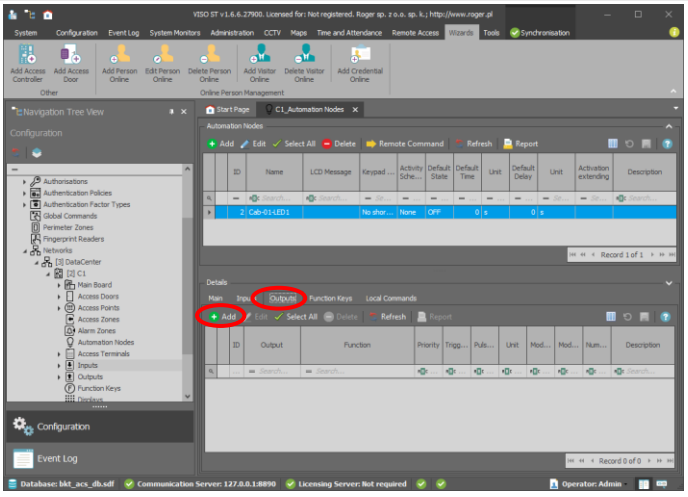
In the pop up window:

- Drop down the *Input* list and select available *IN3* line (door handle sensor)
- Drop down the *Function* list and select *[166]: Set Node ON Toggle*
- Click *OK*



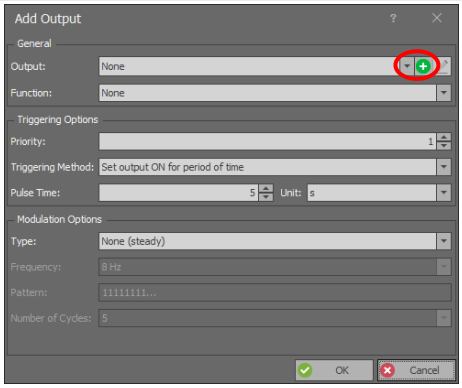
It is now necessary to add the output line to which the LED1 is connected

- Click on *Outputs* tab.
- Click *Add.*



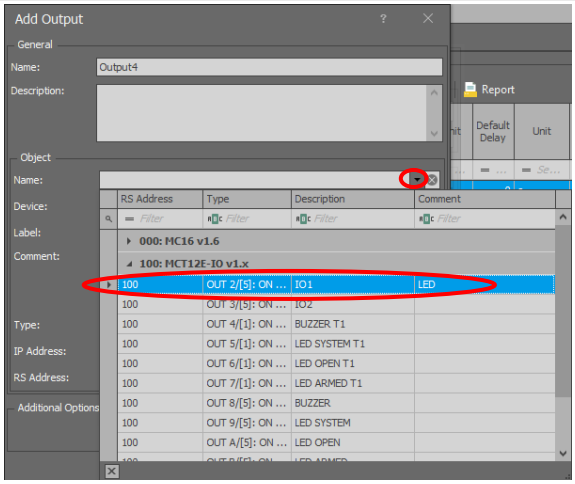
In the pop up window:

- Click on + in *Output* field



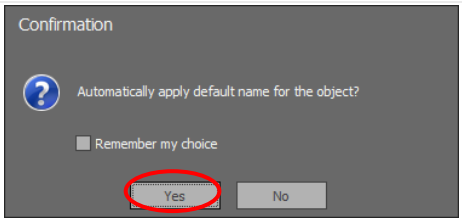
In the next opened window, select the line to which the LED1 is connected – it is OUT1 (IO1) of the front door reader (see *5.8 Diagram of functional circuits for operating the cabinet door*)

- Drop down *Object->Name* list
- Select OUT1 (IO1) of the front door reader

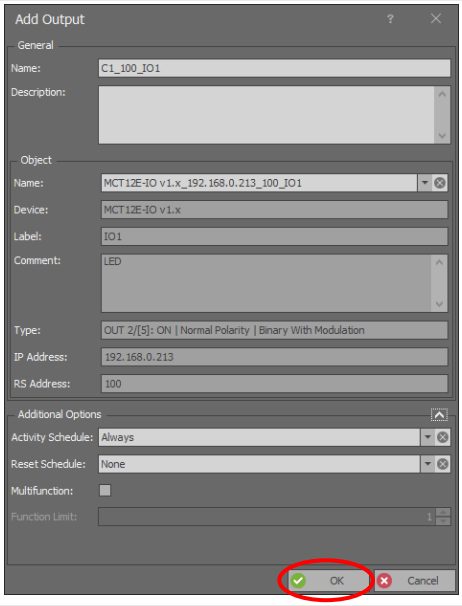


The program will propose a name for the selected object

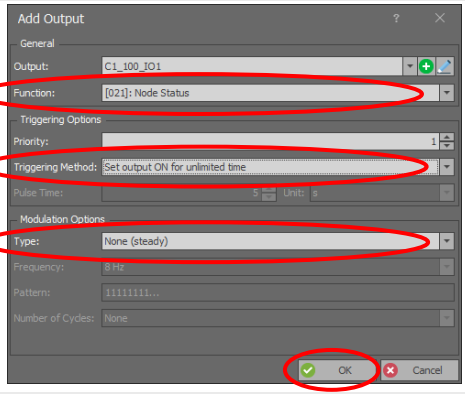
- Confirm the suggestion by clicking *Yes.*



- Confirm the input line by clicking *OK.*

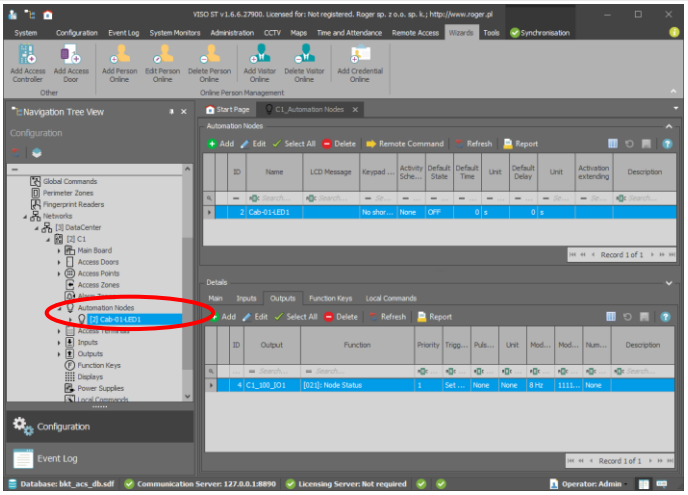


- In the field *Function* select *[021]: Node Status*
- Select *Triggering Method: Set output ON for unlimited time*
- Select *Modulation Type: None (steady)*
- Click *OK*



The LED1 of the controller has been configured. The created automation node that supports the diode should appear in the system tree.
The above configuration should be sent to the controller. See chapter *9.3 Data synchronising*. After synchronization, the controller will restart and the LED1 should light up when the door or handle is open.

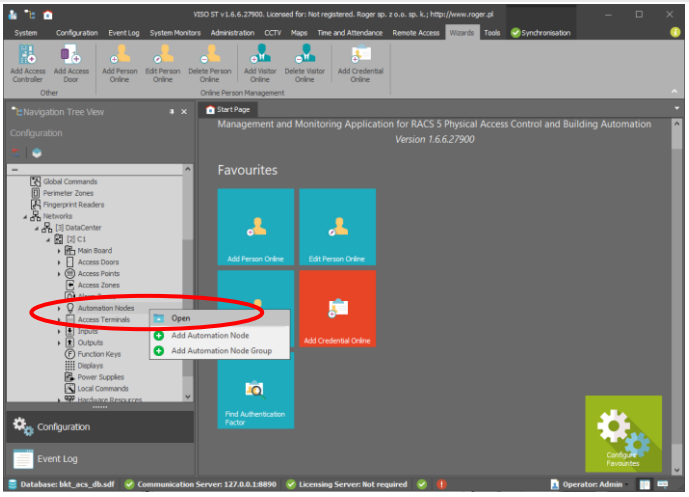
Similarly, configure the LED2, which will signal the opening of the rear door of the cabinet.



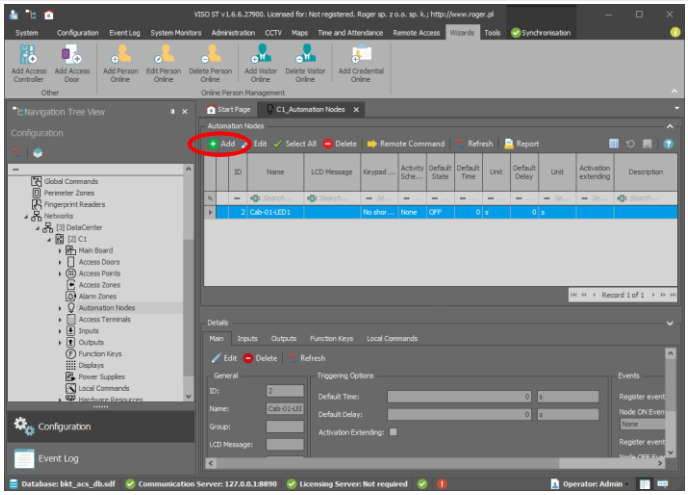
9.10 Tamper signalling

Opening the controller box, the slave set box or the reader casing can be monitored in the system as a sabotage. In order for the sabotage condition to be saved to the database and at the same time to be signalled by sound and led on the reader, the so-called automation nodes must be used:

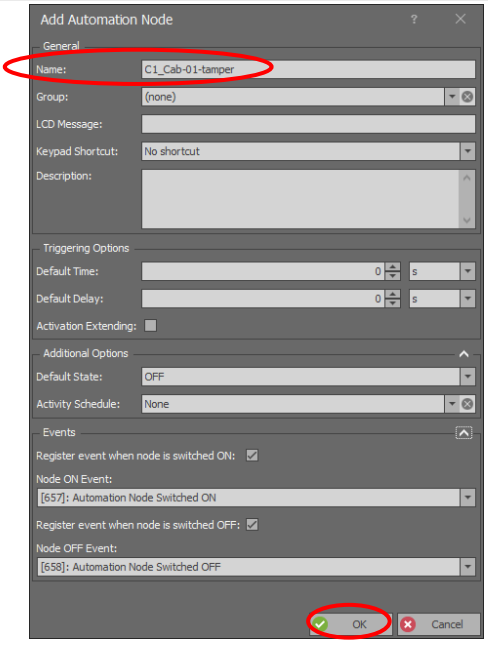
- In the system tree, right-click on *System->Networks-> ->DataCenter (configurable name)->C1 (configurable controller name)-> Automation Nodes* and select *Open.*



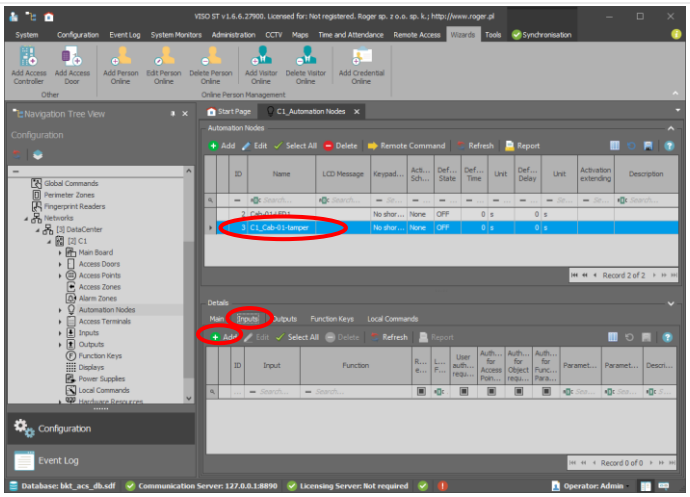
- Click *Add*



- Enter the automation node name eg. *C1_Cab-01-tamper*
- Click *OK*

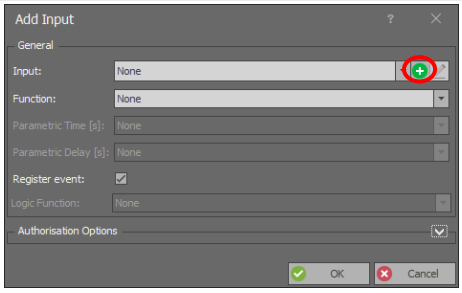


- Make sure the proper automation node is selected.
- Click on *Inputs* tab.
- Click *Add.*



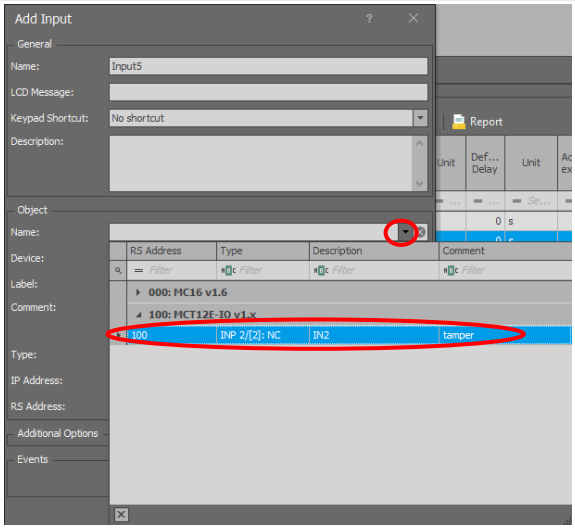
In the pop up window:

- Click on + in *Input* field



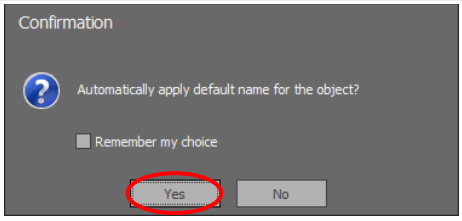
In the next opened window, select the IN2 - tamper line of the card reader, which is installed on the door of the configured cabinet:

- Drop down *Object->Name* list and select input *IN2* of the card reader of the configured door

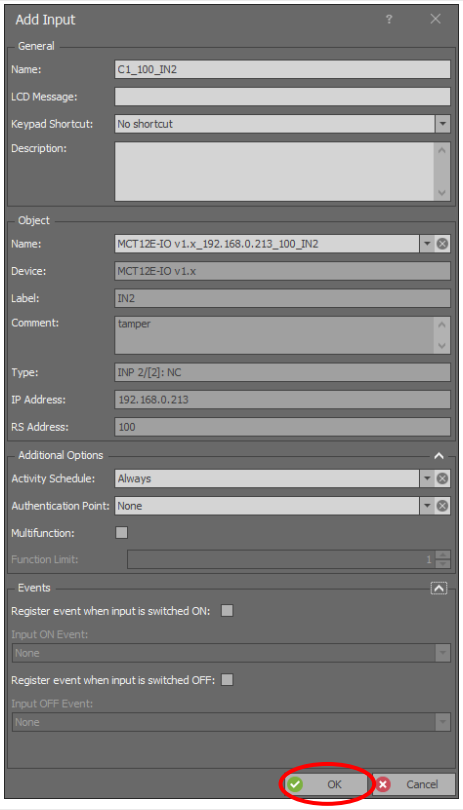


The program will propose a name for the selected object

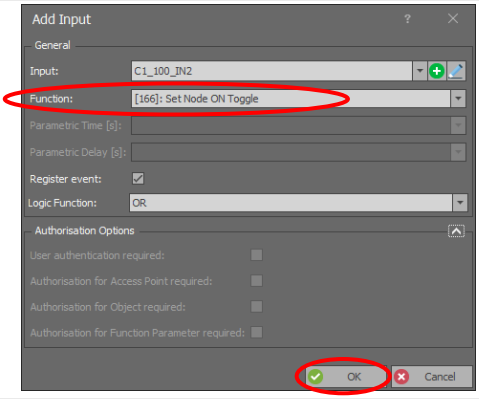
- Confirm the suggestion by clicking *Yes.*



- Confirm the input line by clicking *OK.*



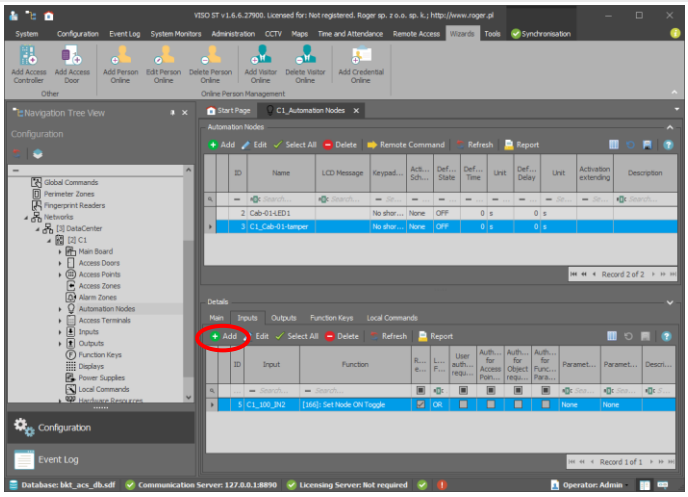
- In the Function field, select the function *[166]: Automation Node On Toggle*
- Click *OK*



In a similar way, add the tamper input IN2 of the cabinet other door reader (if it exists).

- Click *Add* to add all tamper lines of currently configured cabinet

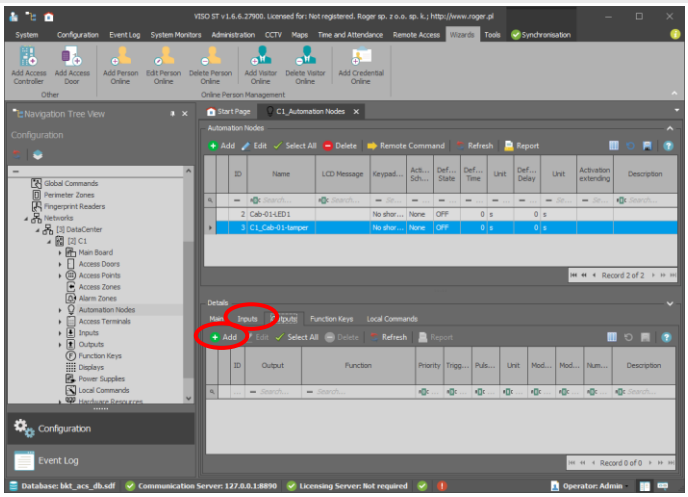
This configuration is sufficient to log readers tampering. in events. You just need to sync data (see chapter *9.3 Data synchronising*).



Additional tamper acoustic signaling

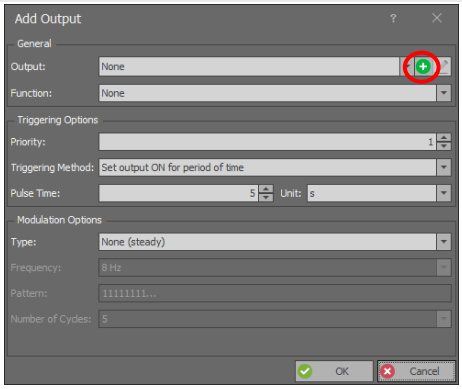
To additionally signal the tamper status audibly appropriate output line should be added:

- Click *Outputs* tab.
- Click *Add.*



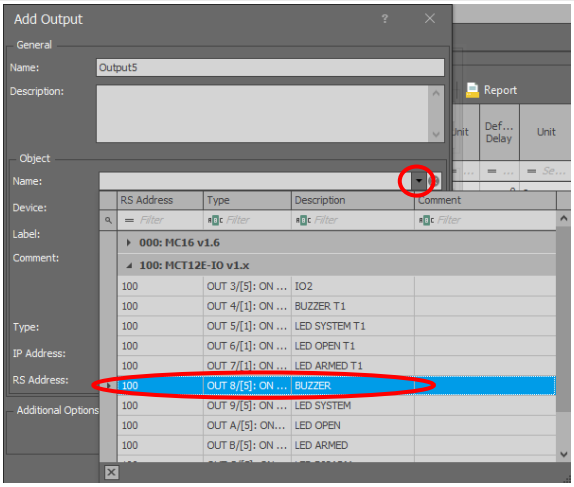
In the pop up window:

- Click on + in *Output* field



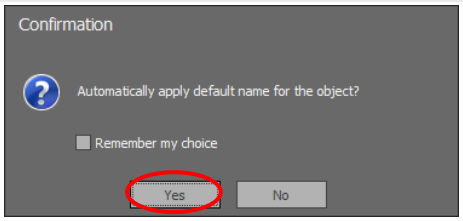
In the next opened window, select the buzzer (BUZZER) of the reader, eg. the front door of the configured cabinet:

- Drop down the *Object->Name* list and select BUZZER output of the cabinet front door reader.

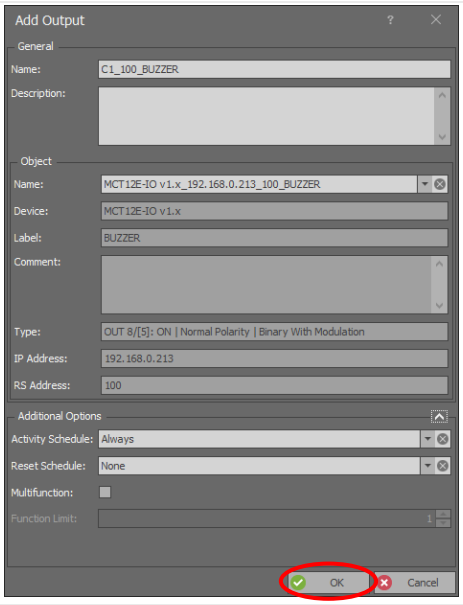


The program will propose a name for the selected object

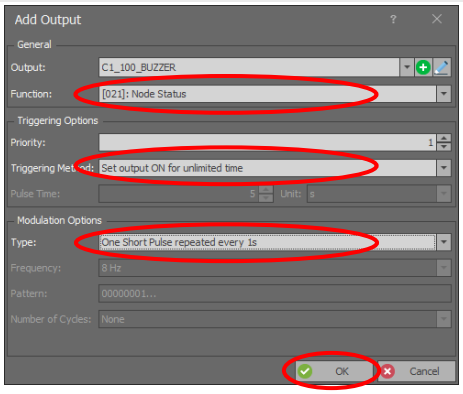
- Confirm the suggestion by clicking *Yes.*



- Confirm the input line by clicking *OK.*



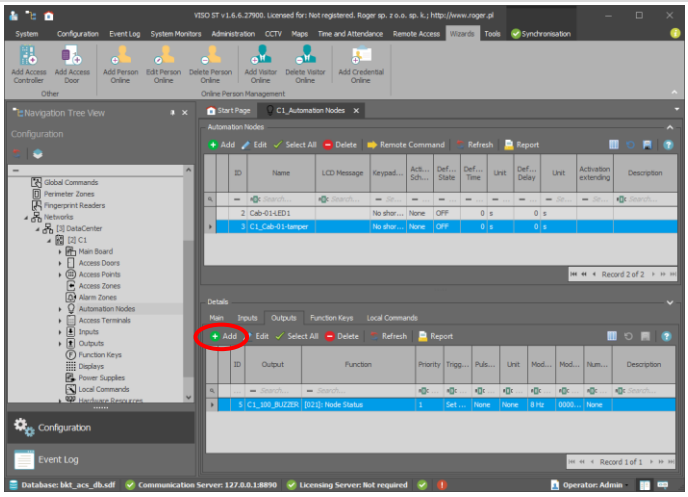
- In the field *Function* select *[021]:Automation Node Status*
- Select *Triggering Method: Set output ON for unlimited time*
- Select *Modulation Type: One Short Pulse repeated every 1s*
- Click *OK*



Additional tamper LED signaling

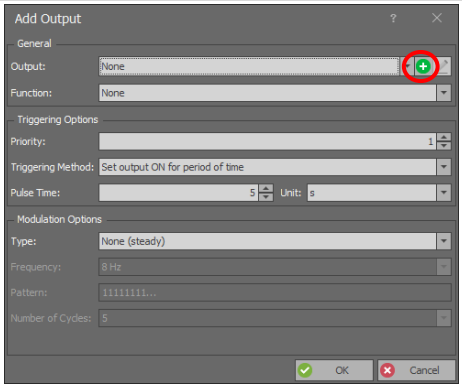
To additionally indicate the tamper state by the LED on the reader, add the appropriate output lines:

- Click *Add.*



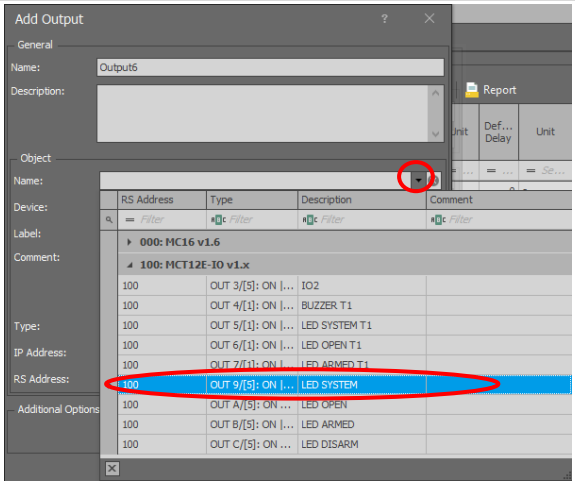
In the pop up window:

- Click on + in *Output* field



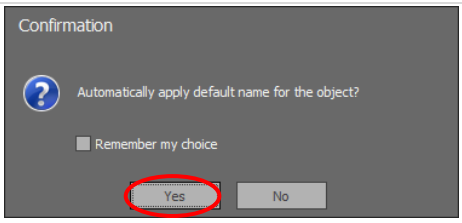
In the next opened window, select the LED of the cabinet door reader:

- Drop down the *Object->Name* list and select *LED_SYSTEM* output of the reader.

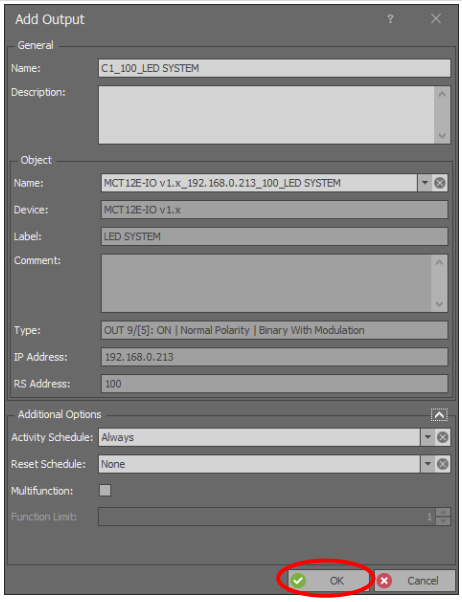


The program will propose a name for the selected object

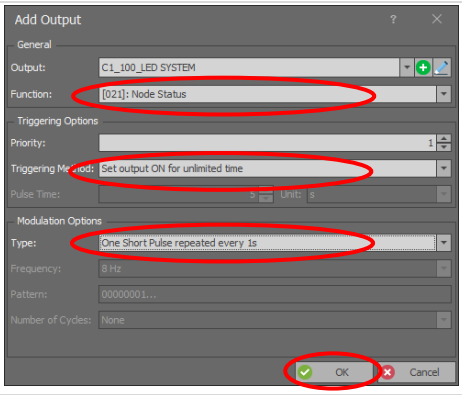
- Confirm the suggestion by clicking *Yes.*



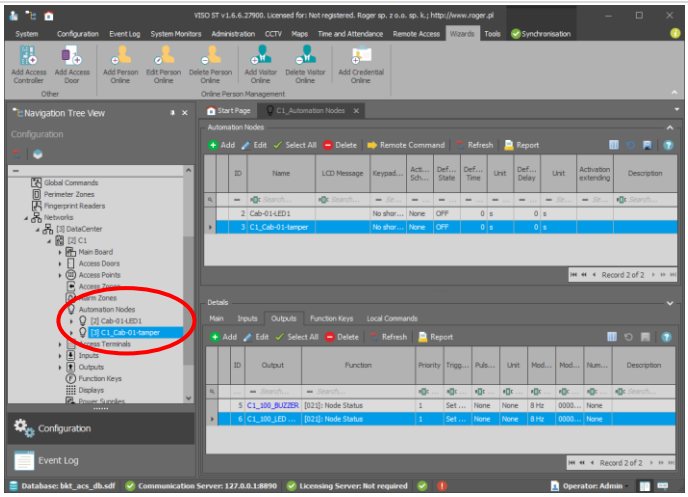
- Confirm the input line by clicking *OK.*



- In the field *Function* select *[021]:Automation Node Status*
- Select *Triggering Method: Set output ON for unlimited time*
- Select *Modulation Type: One Short Pulse repeated every 1s*
- Click *OK*



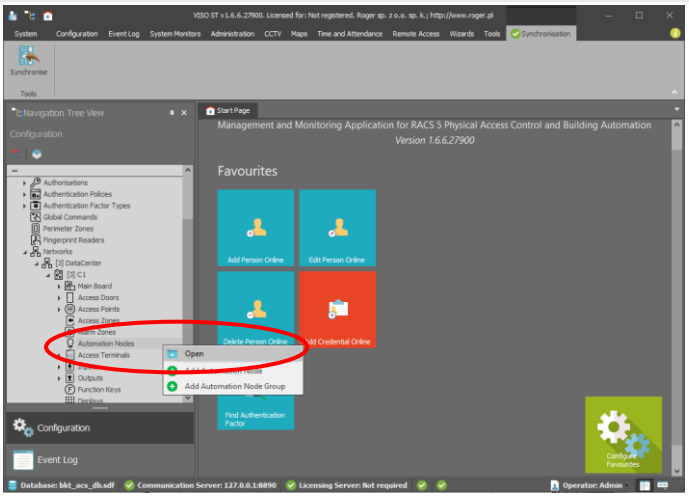
The cabinet tamper signalling has been configured. The created tamper automation node should appear in the system tree.
The above configuration should be sent to the controller. See chapter *9.3 Data synchronising.* After synchronization, if the controller box is opened, the reader on the front door will flash a yellow LED and buzz the buzzer once a second until the tamper condition returns to normal.



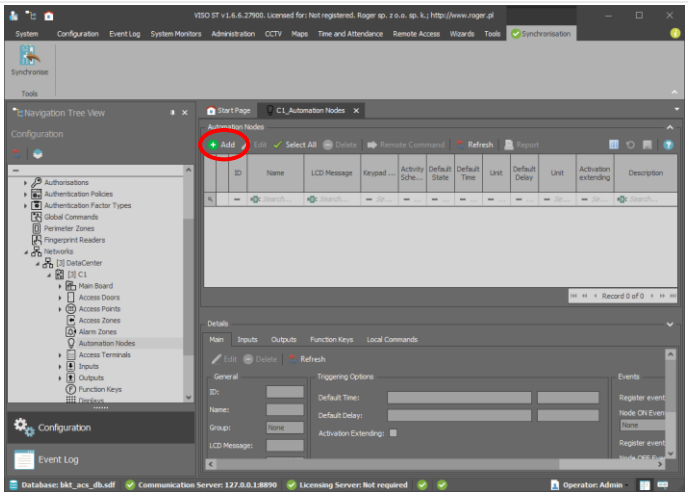
9.11 Emergency button use signalling

The use of the emergency exit button in the cold/hot aisle containment can be monitored in the system. In order to save status of this button into the database and simultaneously indicate the use of it by sound and LED on the reader, the automation node has to be used:

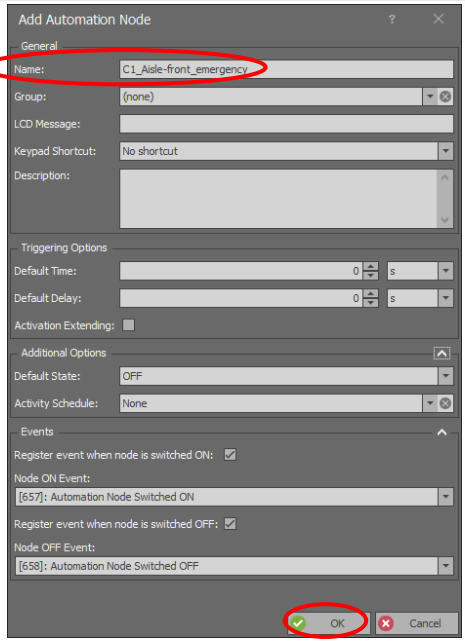
- In the system tree, right-click on *System->Networks-> ->DataCenter (configurable name)> C1 (configurable controller name)> Automation Nodes* and select *Open*



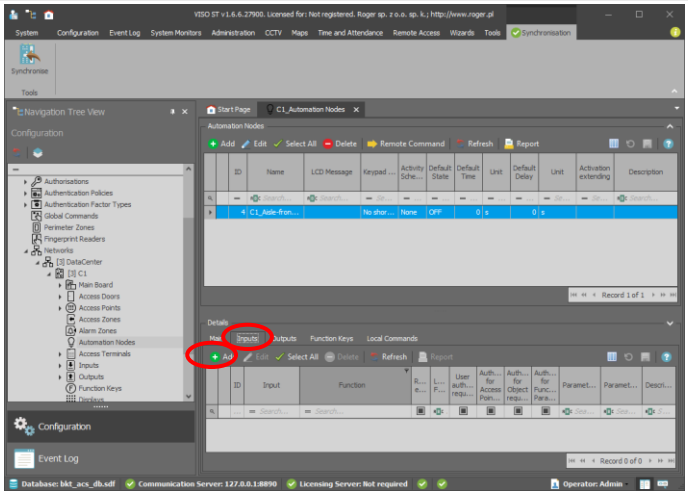
- Click *Add*



- Enter the name of automation node eg. C*1_Aisle-front_emergency*
- Click *OK*

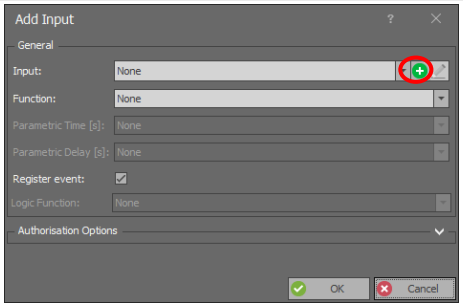


- Click on *Inputs* tab.
- Click *Add.*



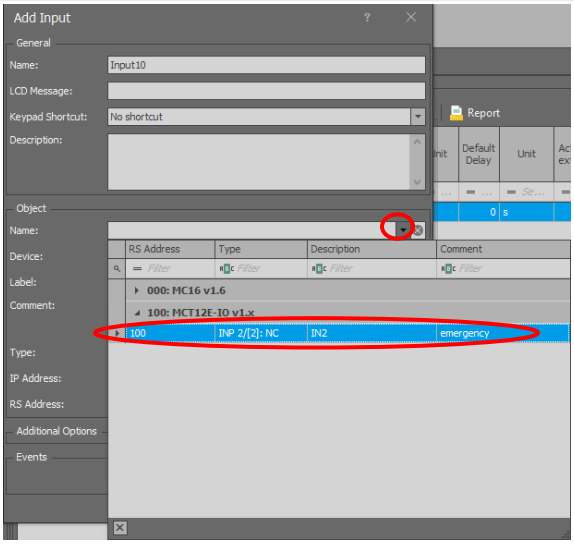
In the pop up window:

- Click on + in *Input* field



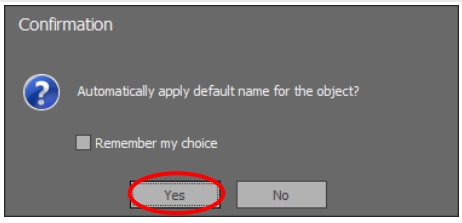
In the next opened window, select the IN2 line of the reader, which is mounted next to the cold/hot aisle containment sliding door. In AR122 readers, this line is also used to control the reader's tamper.
To add IN2 line:

- Drop down *Object->Name* list and select input *IN2* of the reader, which controls aisle door.

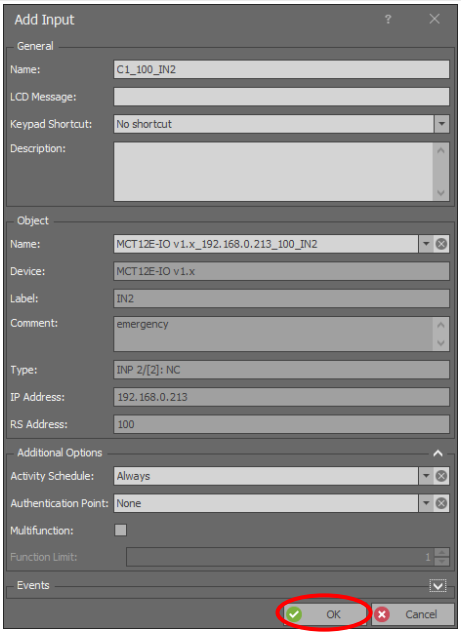


The program will propose a name for the selected object

- Confirm the suggestion by clicking *Yes.*

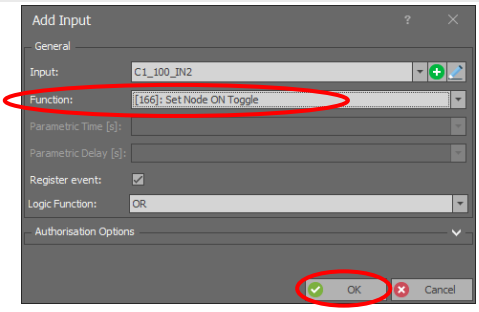


- Confirm the input line by clicking *OK.*



- In the Function field, select the function *[166]: Automation Node On Toggle*
- Click *OK*

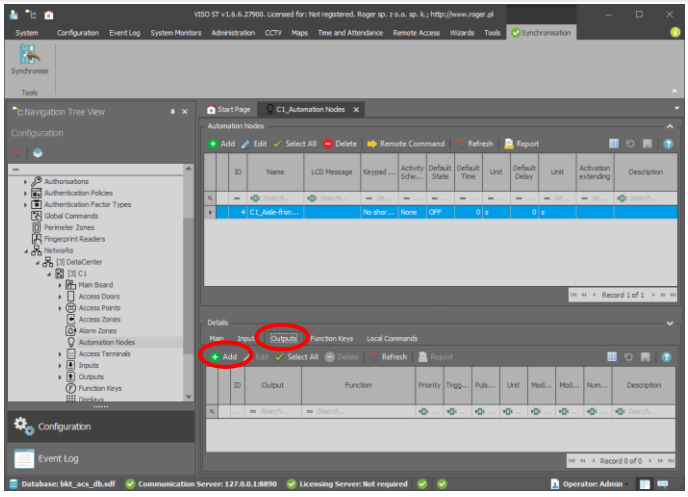
This configuration is sufficient to log the use of the emergency button. The data must be only synchronize (see chapter *9.3 Data synchronising*).



Additional acoustic signaling

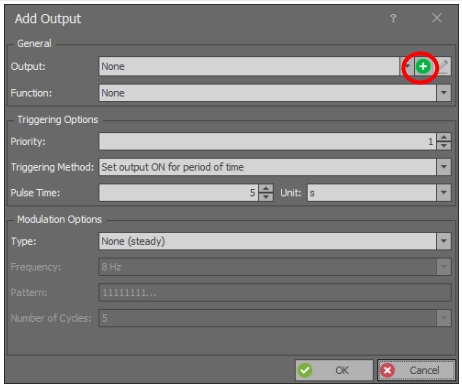
In order to indicate the emergency button use with buzzer and/or LED, the appropriate output lines should be added:

- Click *Outputs* tab.
- Click *Add.*



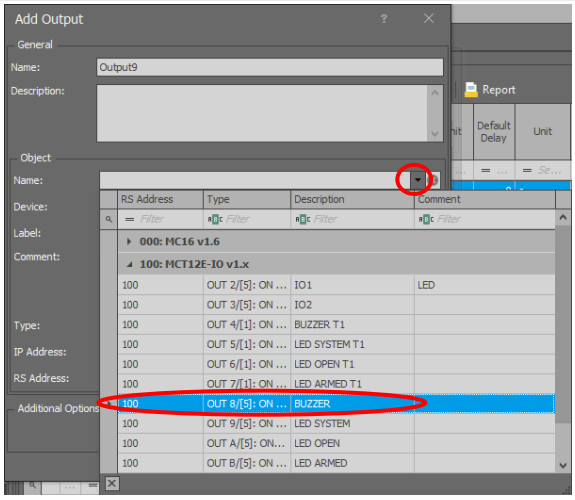
In the pop up window:

- Click on + in *Output* field



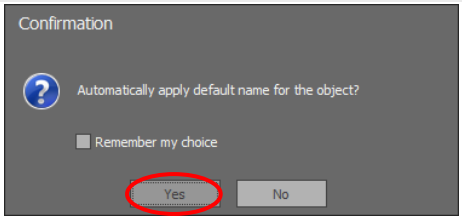
In the next opened window, select the buzzer (BUZZER) of the aisle sliding door reader:

- Drop down the *Object->Name* list and select BUZZER output of the reader, which controls aisle door.

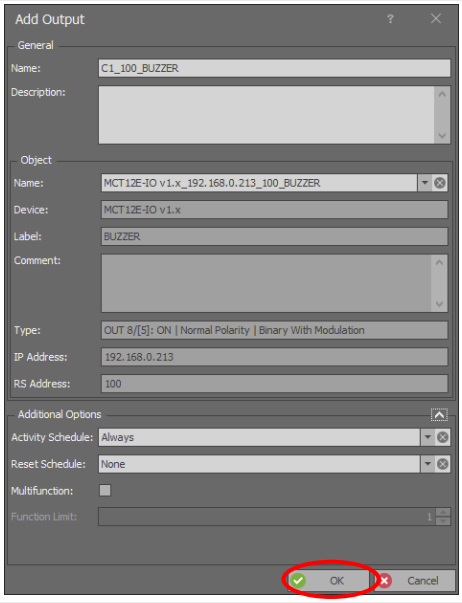


The program will propose a name for the selected object

- Confirm the suggestion by clicking *Yes.*

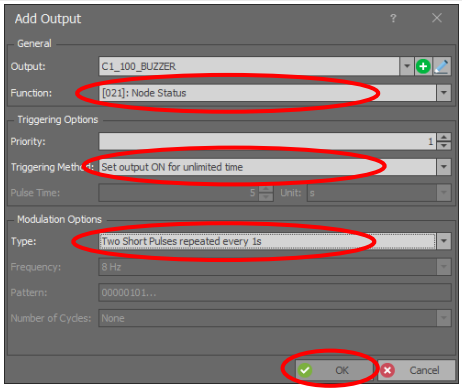


- Confirm the input line by clicking *OK.*



- In the field *Function* select *[021]:Automation Node Status*
- Select *Triggering Method: Set output ON for unlimited time*
- Select *Modulation Type: Two Short Pulses repeated every 1s*
- Click *OK*

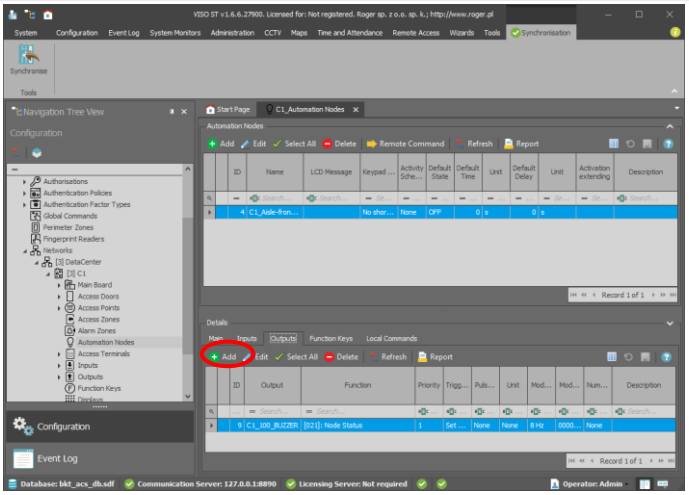
This configuration is sufficient to log the use of the emergency button and to indicate with buzzer. The data must be only synchronize (see chapter *9.3 Data synchronising*).



Additional LED signaling

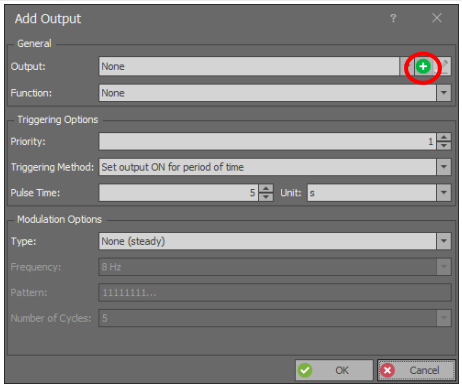
To additionally indicate the evacuation state by the LED on the reader, add the appropriate output lines:

- Click *Add.*



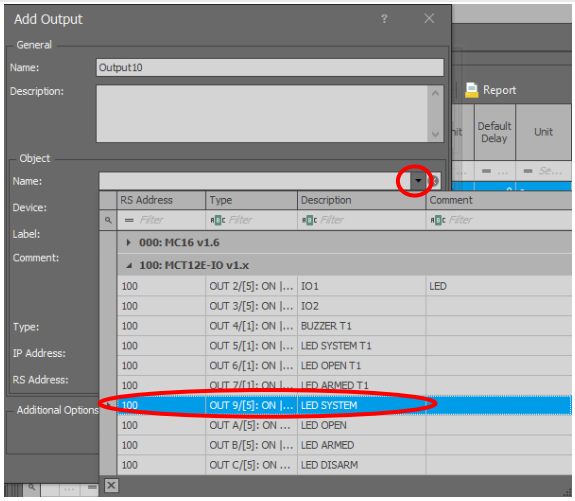
In the pop up window:

- Click on + in *Output* field



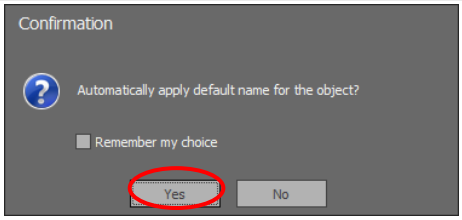
In the next opened window, select the LED of the cold/hot aisle containment sliding door reader:

- Drop down the *Object->Name* list and select *LED_SYSTEM* output of the reader, which controls aisle door.

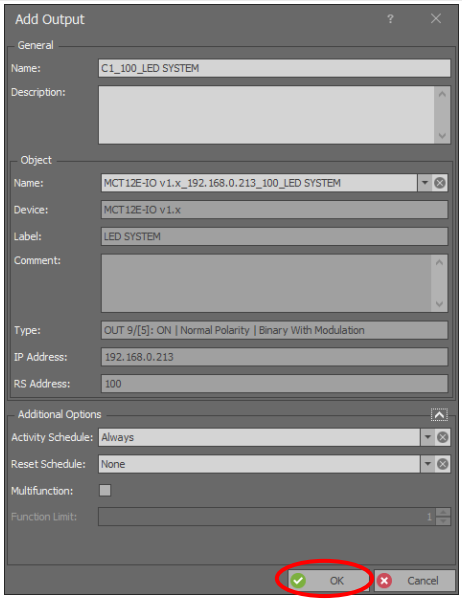


The program will propose a name for the selected object

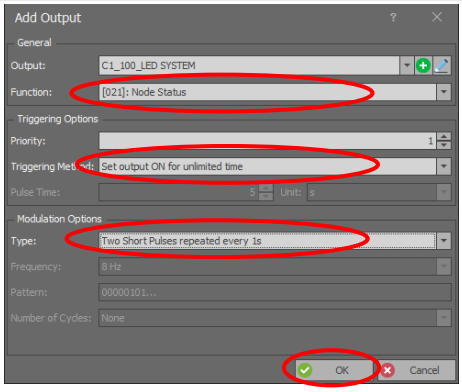
- Confirm the suggestion by clicking *Yes.*



- Confirm the input line by clicking *OK.*

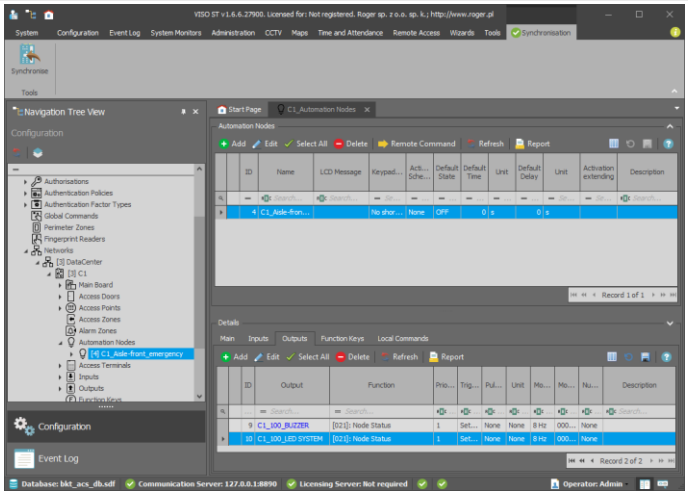


- In the field *Function* select *[021]:Automation Node Status*
- Select *Triggering Method: Set output ON for unlimited time*
- Select *Modulation Type: Two Short Pulse repeated every 1s*
- Click *OK*



The indication of the use of the emergency button has been configured. The created automation node that supports this feature should appear in the system tree.

The above configuration should be sent to the controller. See chapter *9.3 Data synchronising.* After synchronization the controller will restart and if the emergency exit button is used, the reader on the cold/hot aisle containment door will flash the yellow LED and buzz the buzzer twice a second until the emergency exit button is reset.

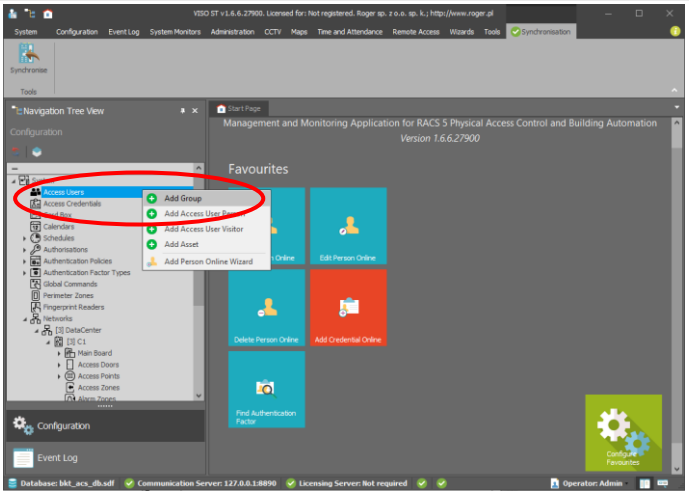


10 SYSTEM MANAGEMENT

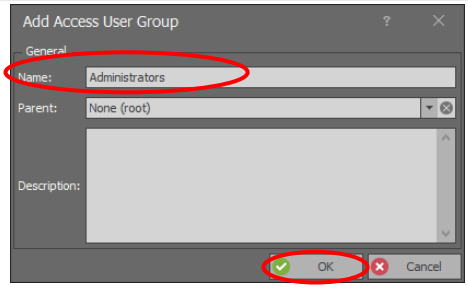
10.1 Adding user group

It is convenient to start adding users from creating a group of users who will have the rights to open a defined group of doors. Any user who belongs to such group will have the rights of this group.

- In the system tree view click with the right button on *Access Users* and select *Add Group*.

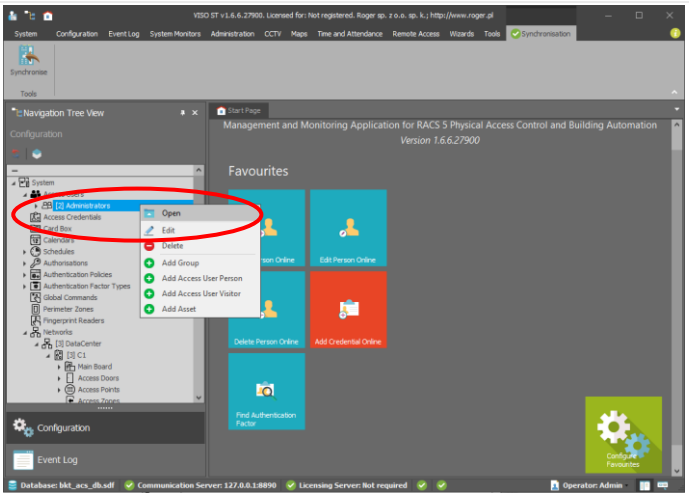


- Enter the name of user group.
- Click *OK*

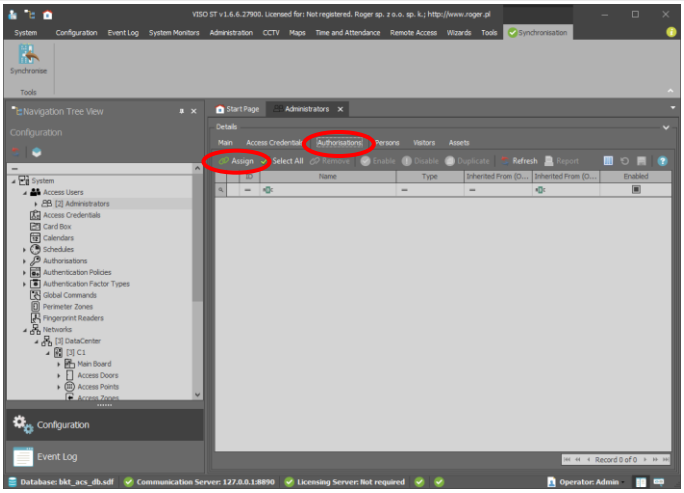


You must assign authorisations that were created during the door configuration to just created group.

- In the system tree view click with the right button on just created user group and select *Open*

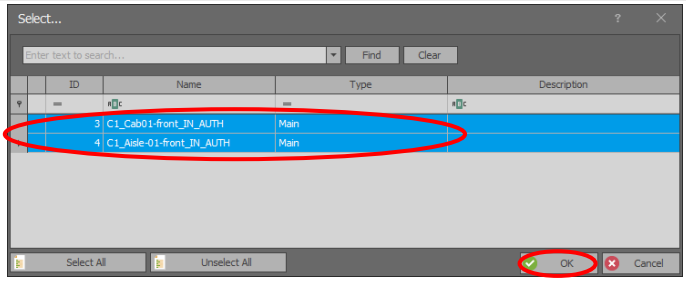


- Click on *Authorisations.*
- Click on *Assign.*

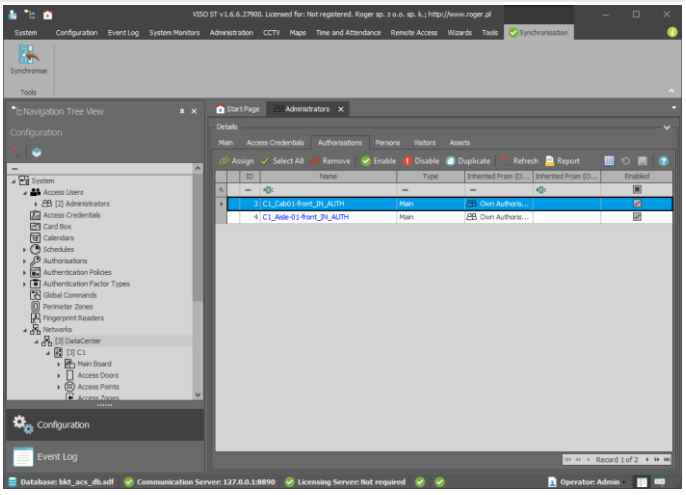


In the pop up window, you should see the authorisations for all doors previously configured in the system.

- Select authorisations, which you want to assign to this group of users. Use CTRL key.
- Click *OK*



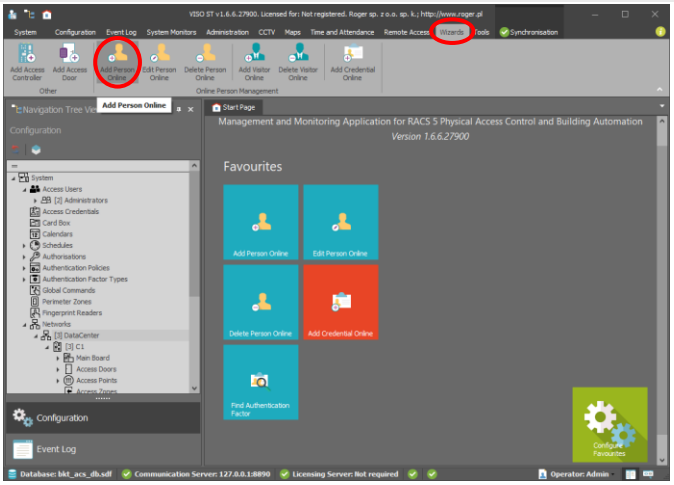
A group of users with permissions to open dedicated doors has been created.
The above configuration should be sent to the controller. See chapter *9.3 Data synchronising*.



10.2 Adding user to group

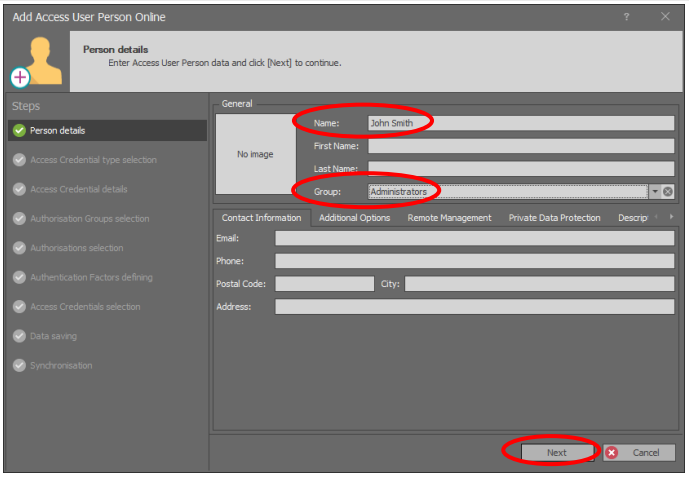
In order to add a new user:

- Choose *Wizards->Add person Online.*



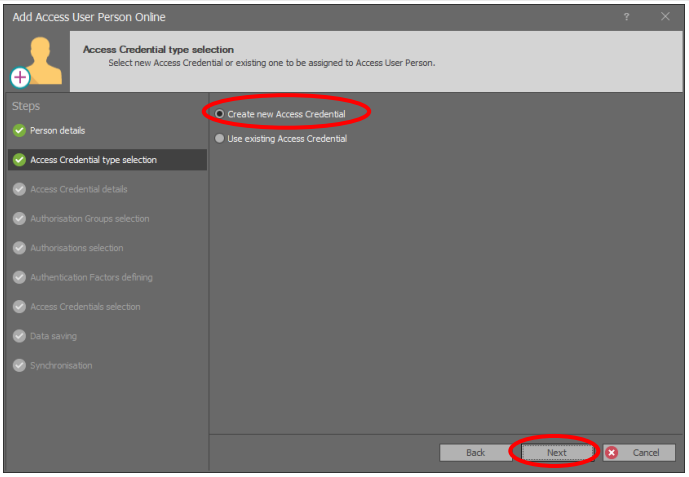
In the opened window:

- Enter user name.
- Select the user group to which user should belong - in this way the user will be given the rights to open the doors that has been assigned to the group. If there is no group, go to the chapter *10 SYSTEM MANAGEMENT*
- *Adding* user group.
- Click *Next.*

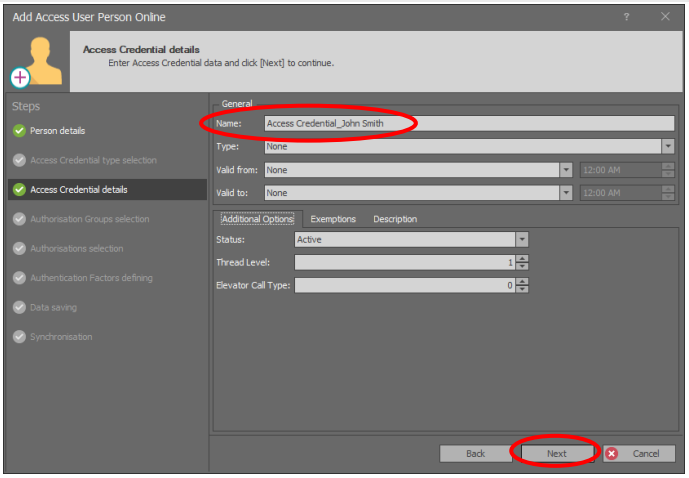


You must assign a credential to the user:

- Select *Create new Access Credential.*
- Click *Next.*

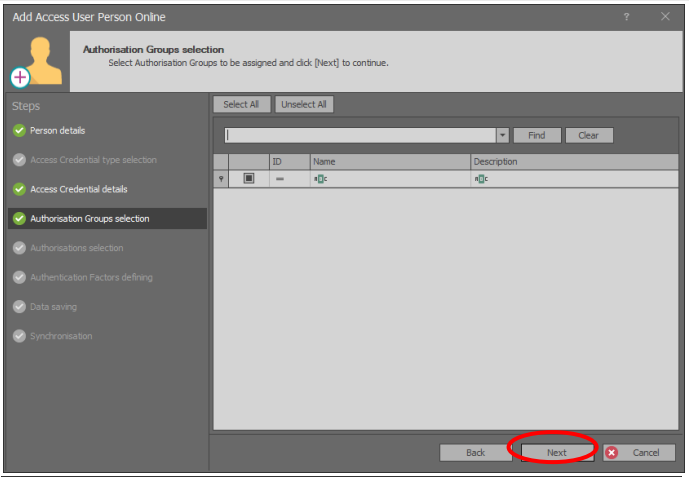


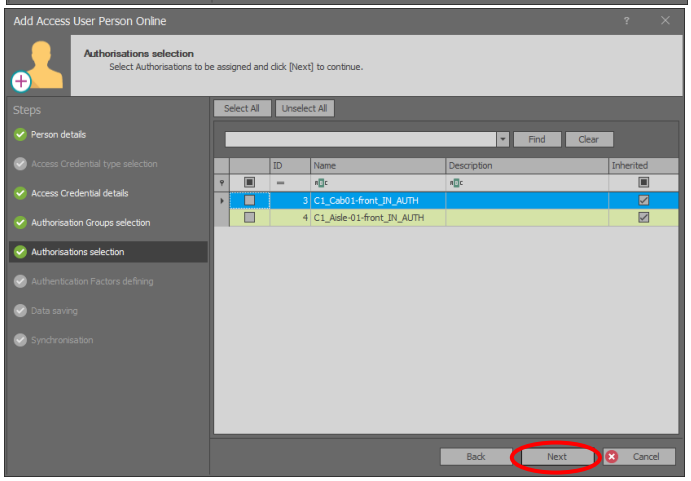
- The credential name can be edited here.
- Click *Next.*



In the next two windows it is possible to assign permissions directly to the user. Since the user being added at this moment has already been granted permissions from the user group to which he belongs, these two configuration windows should be left out without making any changes.

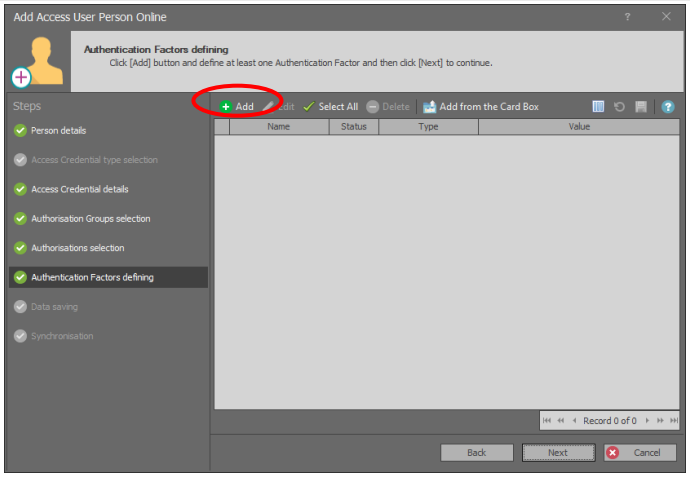
- Click *Next.*
- Once again click *Next.*





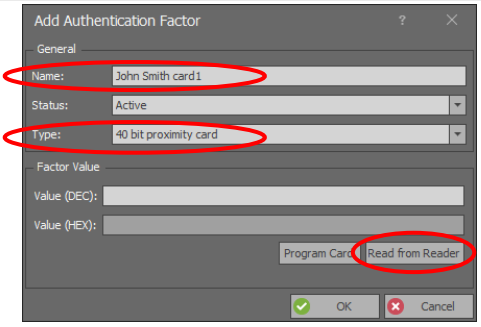
An authentication factor, that is a card or a PIN, should be added to the user credential:

- Click *Add*



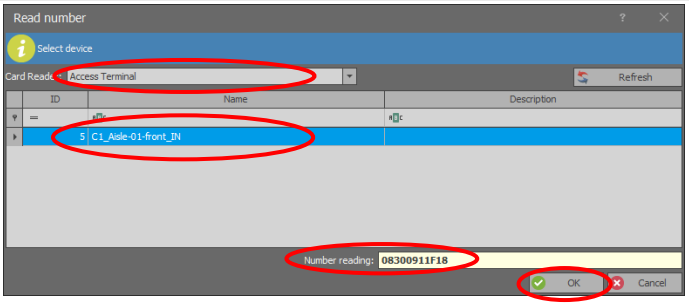
In the opened window:

- Enter the name of user authentication factor (unique to the entire system)
- Select the type, eg. card or PIN
- Enter the PIN or card number or click *Read from Reader*

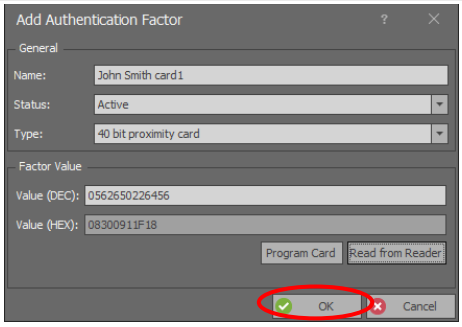


If you have chosen to read from the reader, a new window will appear:

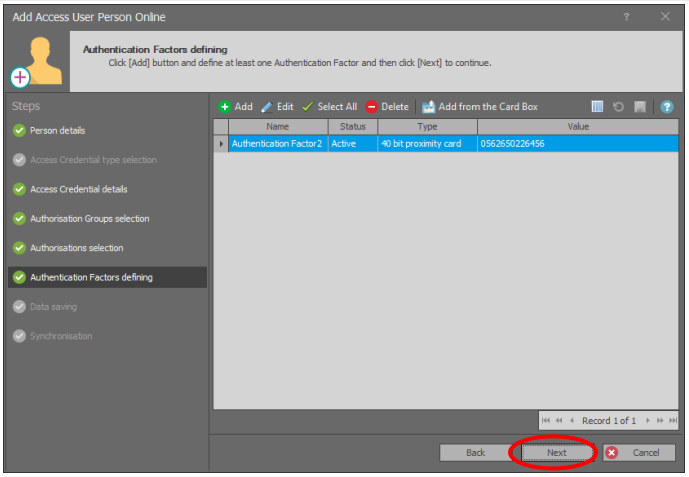
- Choose the type of reader: USB - reader connected to a computer or system reader - any reader so far configured in the system.
- If you have chosen a system reader, click on the reader you want to use to read the card.
- Present the card to the reader.
- The number of the card read will appear in the *Card Number Read* field.
- Click *OK.*



- Click *OK.*

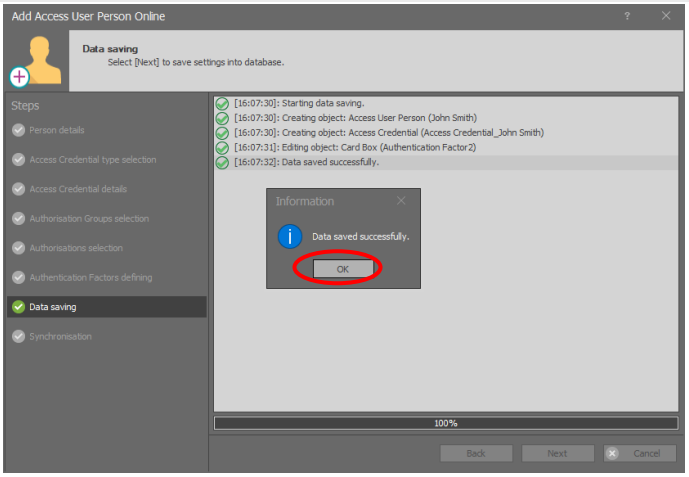


- Click *Next.*



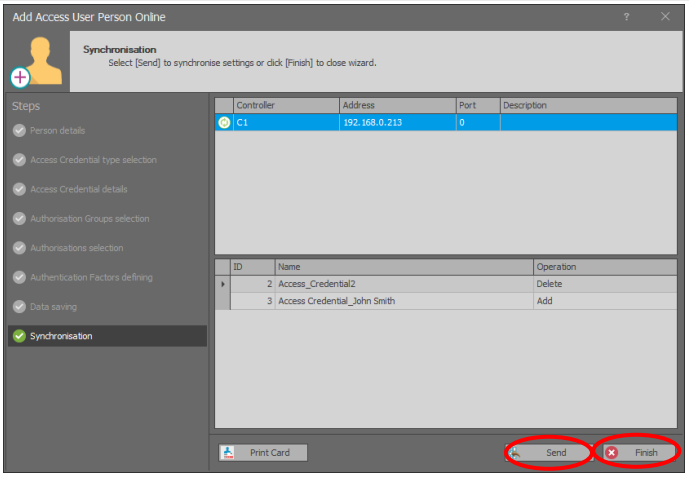
Data have been saved to database.

- Click *OK.*



Upload the configuration to the device, that is, synchronise the controller.

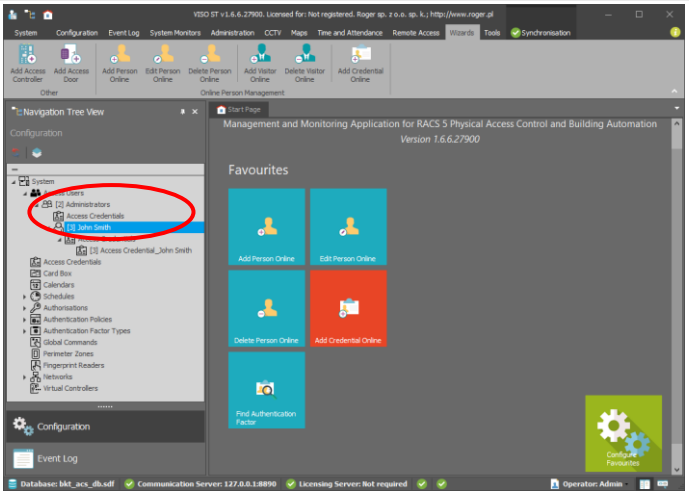
- Click *Send*.
- After synchronisation click *Finish*.



The new user should appear in the system tree

- In the system tree view expand System->
  ->Access Users->"Chosen user group"

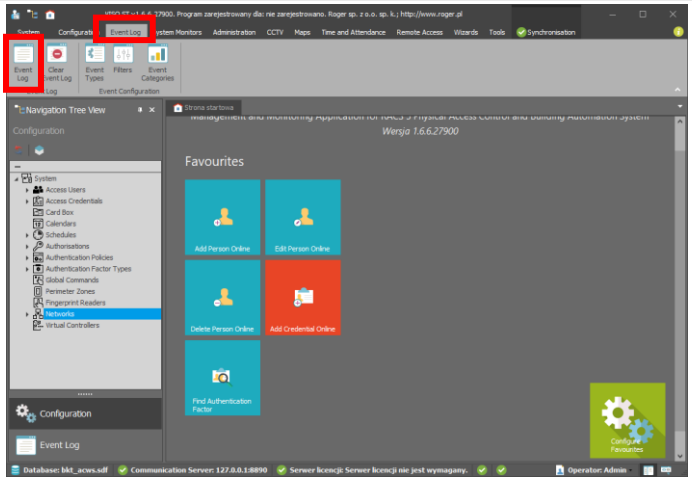
Applying just a configured card to the reader should open the door.



10.3 Event viewer

VISIO allows viewing all events taking place in the system

- From the menu, select *Event Log* and then *Event Log*

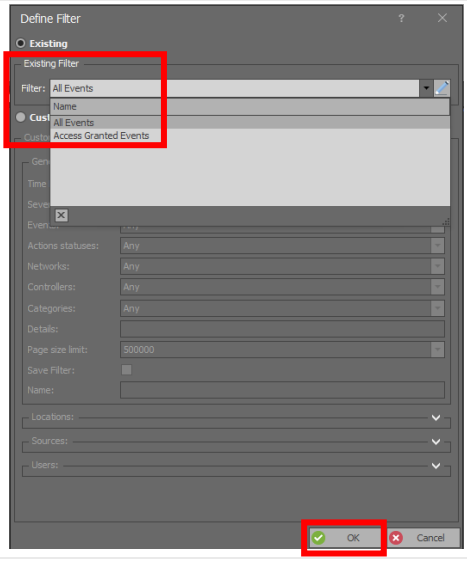


Select the predefined event filters:

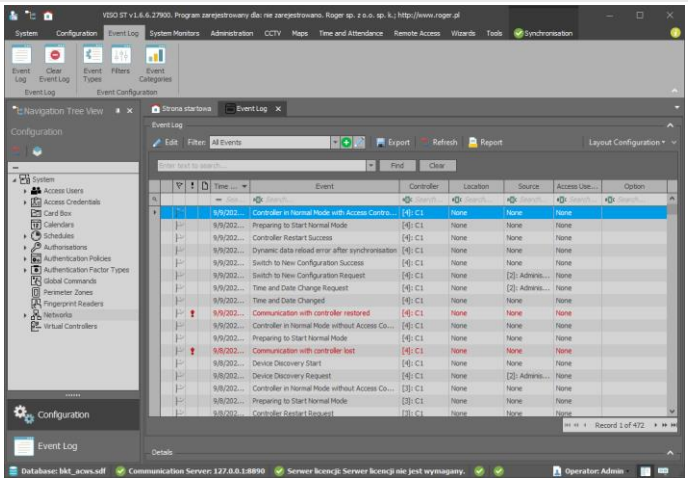
- All Events – all events in the system,
- Access Granted Events – opening doors only

It is also possible to select custom filtering.

Custom filters can be defined in the *Event log -> Filters* menu.



By default, the list of all events in the system is sorted by the date they occurred.



11 DOCUMENT REVISIONS

Version	Changes	Date
1	Initial version	June 2018
2	Added communication key setting in the controller low-level configuration.	July 2018
3	Added comparison to the BKT ACWS system. Small updates have been made.	November 2018
4	Added two user entry configuration	February 2019
5	Updated with new AC100 controller and AB101 secondary set	June 2022
6	Modified 3.7, added 9.2, 9.7, 10.3	September 2022
7	Updated 3.7.1, 8.4 with new Roger RACS v2.0 features (SQL Server only, licenses)	June 2023