Roger Access Control System 5v2

Application note no. 006

Document version: Rev. A

RACS 5 Quick start guide

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

Introduction

The document presents quick start guide for RACS 5 v2 system with MC16-PAC-2-KIT and three MCT series readers. In the system two doors are planned, the first one is read-in/out type while the second one is read-in type.

RACS 5 system can include multiple MC16-PAC-x-KITs to control doors. The configuration of MC16-PAC-3-KIT (3 doors) and MC16-PAC-4-KIT (4 doors) is very similar to configuration of MC16-PAC-2-KIT (2 doors). Other scenarios of operation are presented in AN002 application note.

Low level configuration

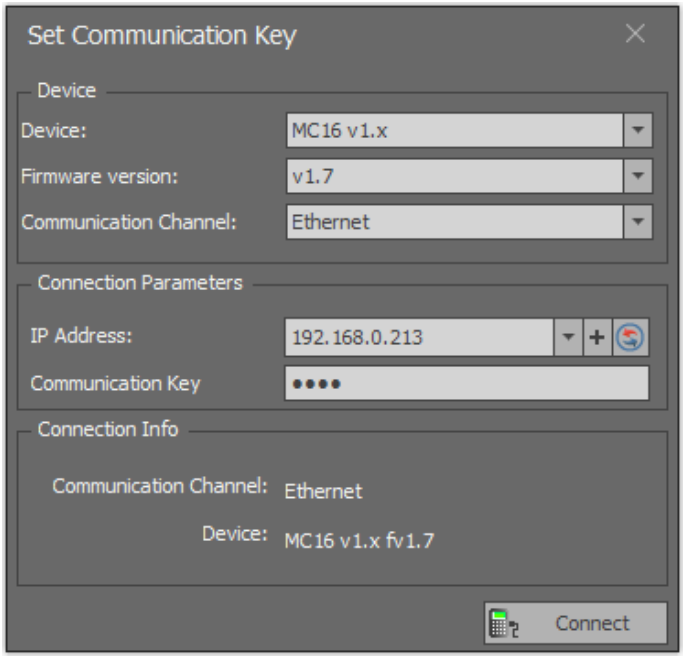
MC16 controller

The purpose of controller's low level configuration is to define its properties. There are a few dozens of low level settings but the most essential are IP address and communication key which is used to encrypt the communication with controller in Ethernet network.

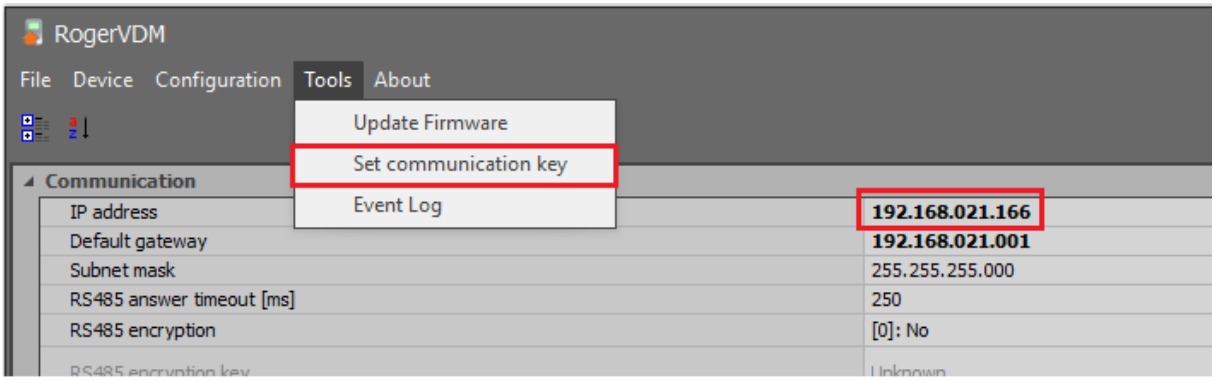
Factory new MC16 controller has IP address set to 192.168.0.213 and the communication key is 1234. Both can be changed with RogerVDM software.

In order to make typical low level configuration of the controller in MC16-PAC-2-KIT:

- Connect power supply to the controller.
- Connect the controller to your computer with Ethernet RJ45 cable, configure the IP address of computer's network adapter in the same range as controller address e.g. 192.168.0.1.
- Install and run RogerVDM software. Apply settings as in figure below. The controller should be detected and displayed on the list of available devices if it is not blocked by firewall or antivirus software. Factory set communication key is 1234.



- When the button *Connect* is selected then the software will connect with controller and the window with low level configuration settings will be displayed.
- In top menu select *Tools->Set communication key* and define your own key using HEX characters (0-9, A-F).



- Enter target IP address for the controller. The address 192.168.21.166 will be used in the guide so the controller could be operated in existing computer network with other devices.
- Upload the settings to controller with *Send to Device* button.
- Disconnect the controller selecting *Device->Disconnect* in the top menu and close RogerVDM program. The controller will restart with LED1 on and LED8 flashing.

MCT readers

The purpose of low level configuration of a reader is to define its properties. There are a few dozens of low level settings but the most essential is address as each device on RS485 bus of MC16 controller must be assigned with unique address in range of 100-115.

According to MCT installation manuals the address can be configured with RogerVDM software after connection via RUD-1 interface or manually. The manual configuration of address can be done with reader's keypad or by reading of any proximity card in a technology supported by the reader.

However, in RACS 5 v2 system, for majority of MCT readers, it is not necessary to configure the address and make low level configuration prior to connection to MC16 controller. According to MCT installation manuals all settings including RS485 bus addresses can be configured later in VISO

software when readers with their default settings are connected to MC16 controller. Such configuration method is more convenient and it is recommended.

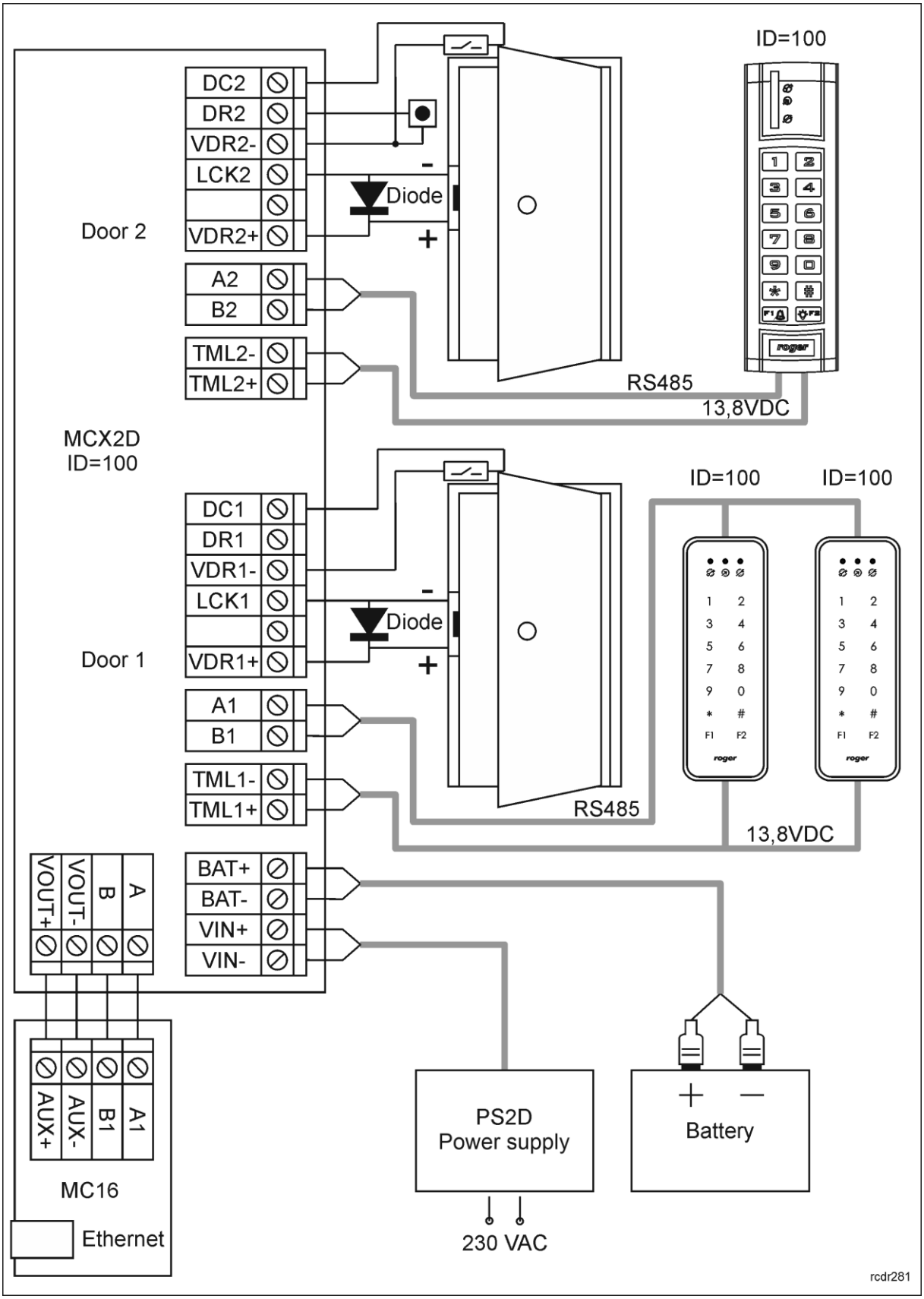
MCX2D expander

MC16-PAC-2-KIT includes MCX2D expander which offers power supply, communication as well as input and outputs for each door. In case of RACS 5 v2 system, it is not necessary to make low level configuration of MCX2D (or MCX4D) expander prior to connection to MC16 controller. According to MCX installation manuals all settings including RS485 bus addresses can be configured later in VISO software when expander with its default settings is connected to MC16 controller. Such configuration method is more convenient and it is recommended.

Installation

The following electrical diagram represents example of access control system which is used in this guide. It is two doors system with read-in/out door (two MCT84M readers) and read-in door (MCT12M reader).

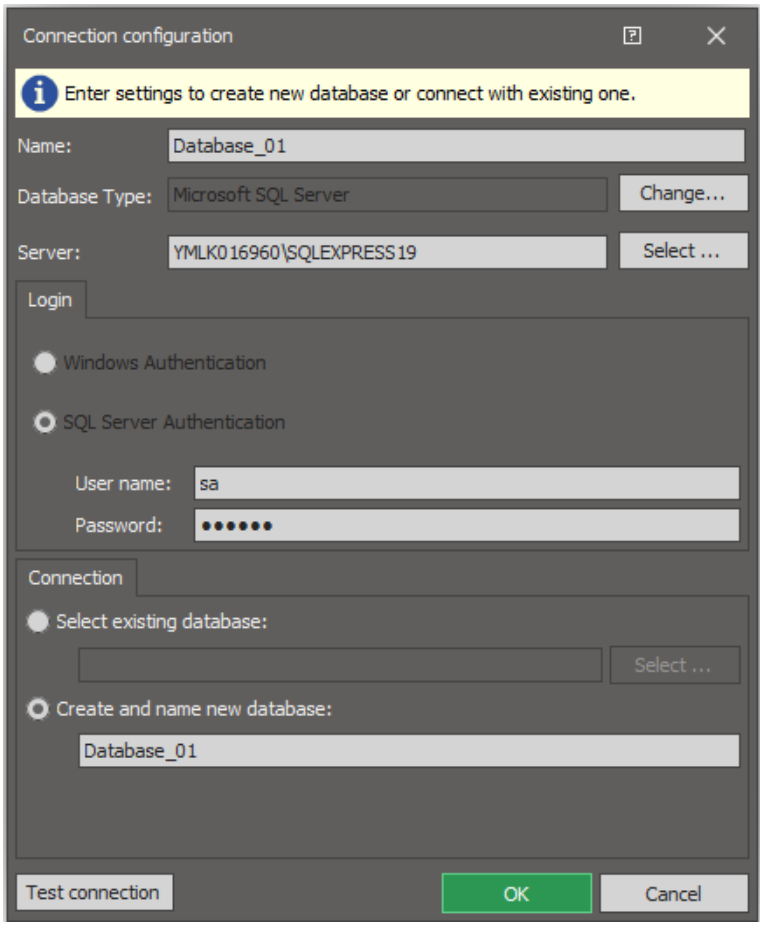
According to AN002 application note other communication and power supply scenarios are available based on other I/O expanders and MCT readers with built-in inputs and outputs.


ID=100
DC2
DR2
VDR2-
LCK2
VDR2+
Door 2
Diode
A2
B2
TML2-
TML2+
RS485
13,8VDC
MCX2D
ID=100
ID=100
ID=100
DC1
DR1
VDR1-
LCK1
VDR1+
Door 1
Diode
A1
B1
TML1-
TML1+
RS485
13,8VDC
BAT+
BAT-
VIN+
VIN-
VOUT+
VOUT-
B
A
AUX+
AUX-
B1
A1
MC16
Ethernet
PS2D
Power supply
230 VAC
Battery
rcdr281

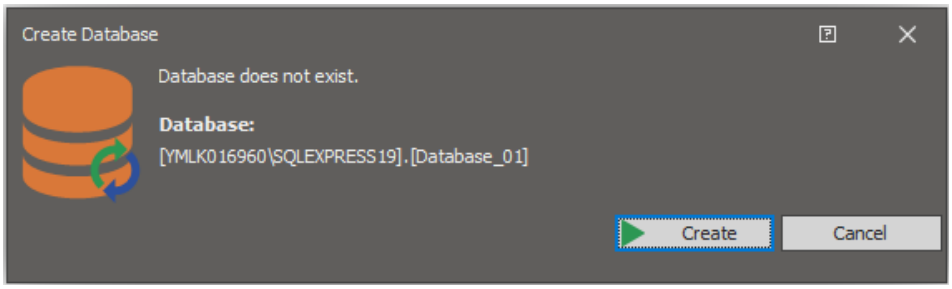
Database

High level configuration of RACS 5 system is stored in VISO software database. The RACS 5 v1 system could work with local type Microsoft SQL Server Compact 4.0 database or centralized type Microsoft SQL Server 2005 (or higher) database. Due to discontinued support of Microsoft company for local type databases, in RACS 5 v2 system only centralized type Microsoft SQL Server 2005 (or higher) database can be applied.

- Install MS SQL Server system according to AN017 application note.
- Install and start VISO software.
- In the window shown below enter connection name, indicate previously installed MS SQL Server, select authentication method and define database name. Click *OK* button.



- Click *Create* button when *Create database* window is displayed.

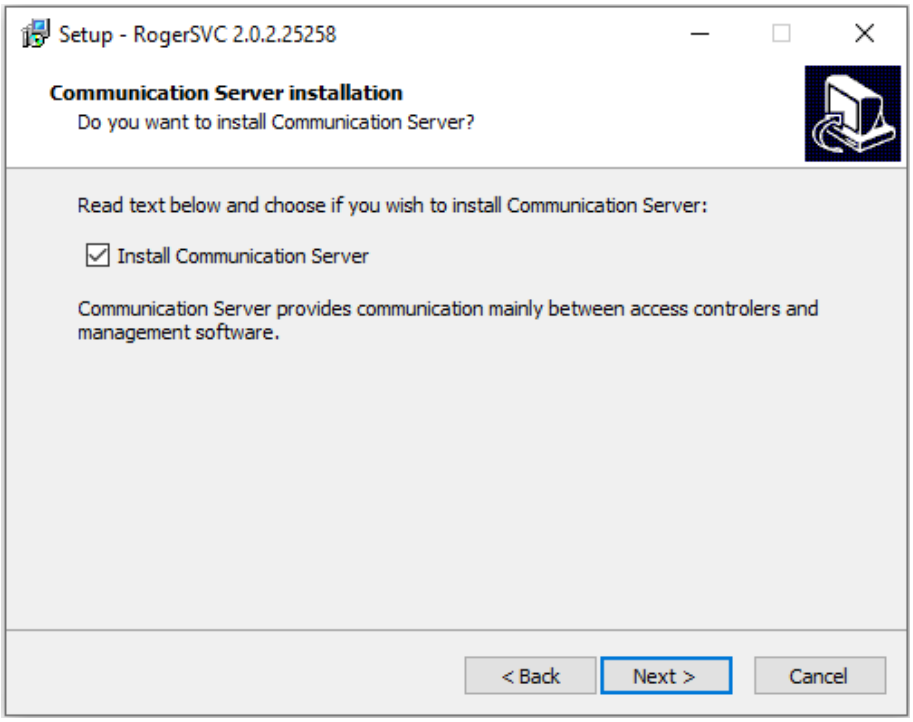


- When new database is created then VISO login window is displayed. Click *OK* and in the next window define own password. The password can be later changed by selection of *Administration* in the top menu of VISO software and then *Operators*.

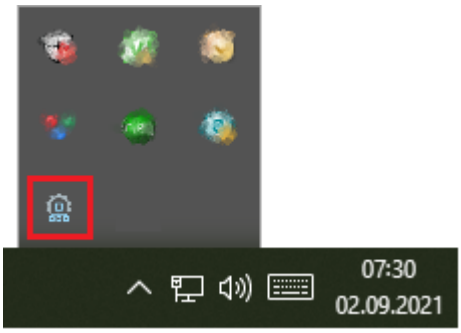
RACS 5 Servers

It is necessary to configure servers (Windows services) to ensure proper operation of RACS 5 system. They are used among others for VISO software communication with controllers and for connection with database.

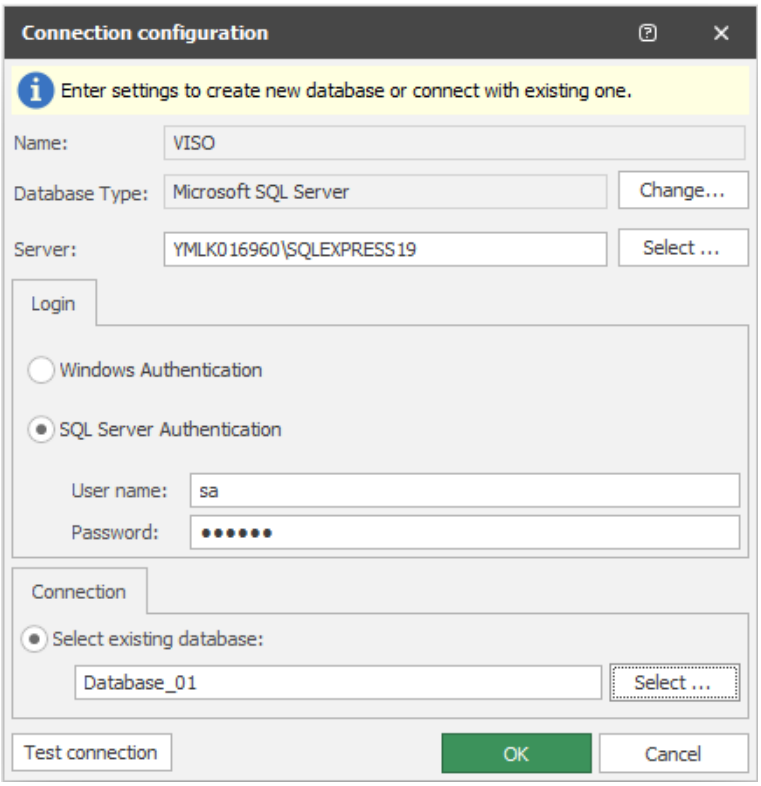
- Install Roger SVC software and select Communication Server. Optionally if additional licensed features are purchased for VISO software then also select License Server. Other servers are not necessary and they will not be used in this guide.



- In the final step of the installation enable the option *Launch RogerSVC*.
- When RogerSVC is launched then its icon is displayed in Windows tray. Click the icon . The RogerSVC icon in tray can also be launched from Windows menu *Start ->Roger-> RogerSVC.*



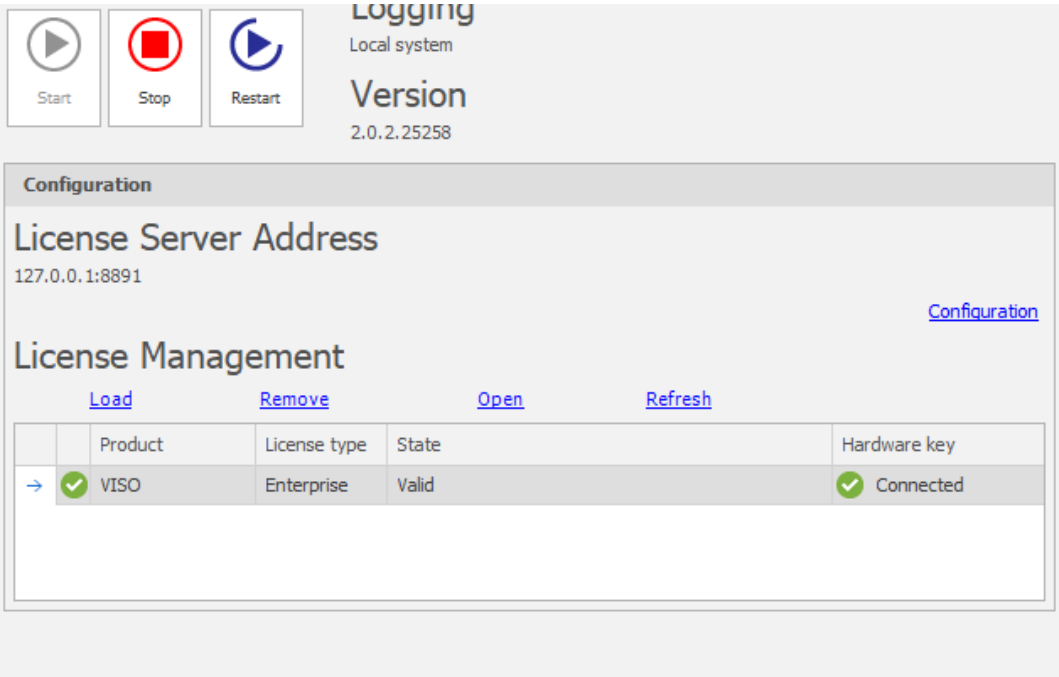
- In the RogerSVC window select *Database Connection* tile and then *Configuration* to indicate previously created RACS 5 database. Return to the main window



- In the RogerSVC window select *Communication Server*, click *Start* and return to the main window. More information on the server is given in AN008 application note.

Note: It is recommended to enable Security Mode with TLS 1.2 encryption.

- If Licenser Server is installed then click it, connect purchased RUD-6-LKY hardware key to computer's USB port, load purchased license file and click *Start*.



- Install and run VISO software. In the top menu select *System* and then *Select License Server*.
- In the opened window select previously define Licence Server from RogerSVC software.

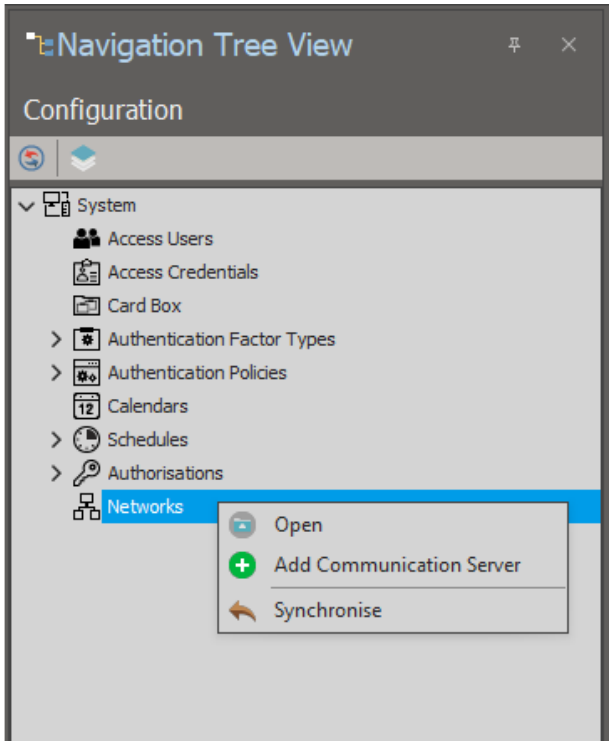
System configuration

Communication Server

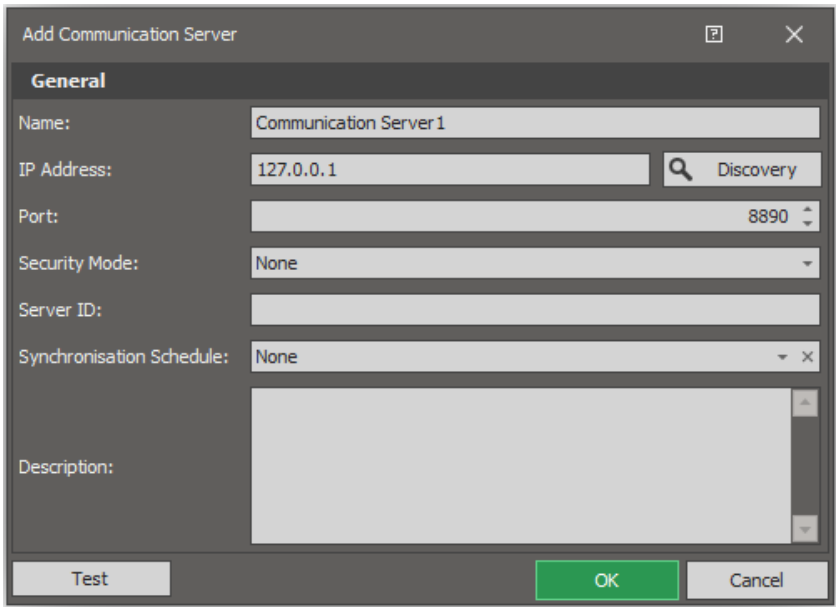
In RACS 5 v2 a new concept of multiple Communication Servers with their MC16 controller groups was implemented. This is intended to be used in distributed system where RACS 5 system is installed in multiple buildings in geographically varied locations. In such case Communication Server from RogerSVC software can be installed on computer in each location and then all servers can be added in VISO software. Communication Servers can be installed behind routers and they can be distinguished by means of their configurable *Server ID* parameter. More information on Communication Servers is given in AN008 application note.

For the purpose of this application note only single Communication Server will be used. In order to add the server in VISO software:

- Start VISO software and in the navigation tree right click *Networks* and then select *Add Communication Server*.



- In the opened window enter details of previously installed Communication Server from RogerSVC software.



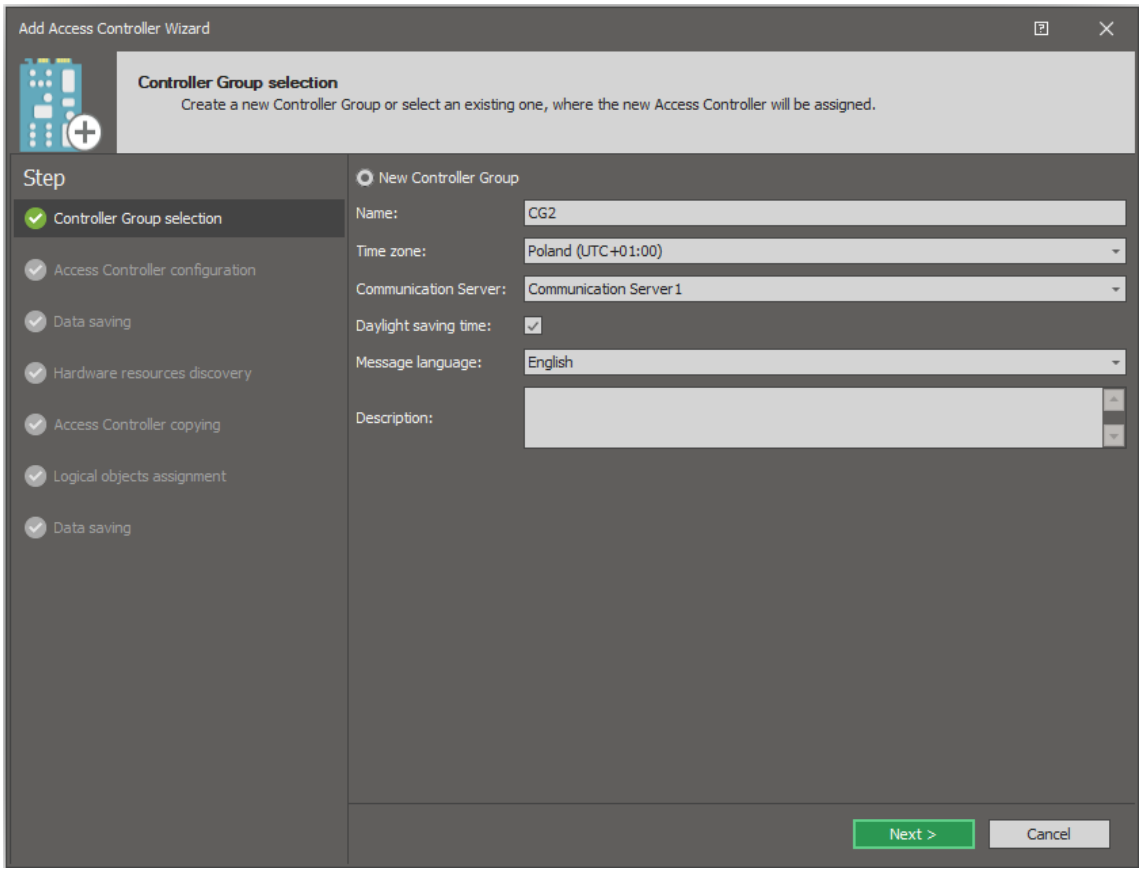
Note: In this application note it is assumed that RogerSVC and VISO are operated on the same computer. Therefore default 127.0.0.1 IP address is used for Communication Server in RogerSVC and VISO. If Communication Server is installed on a different computer than VISO then use IP address of computer's network adapter both in RogerSVC and VISO.

MC16 controller

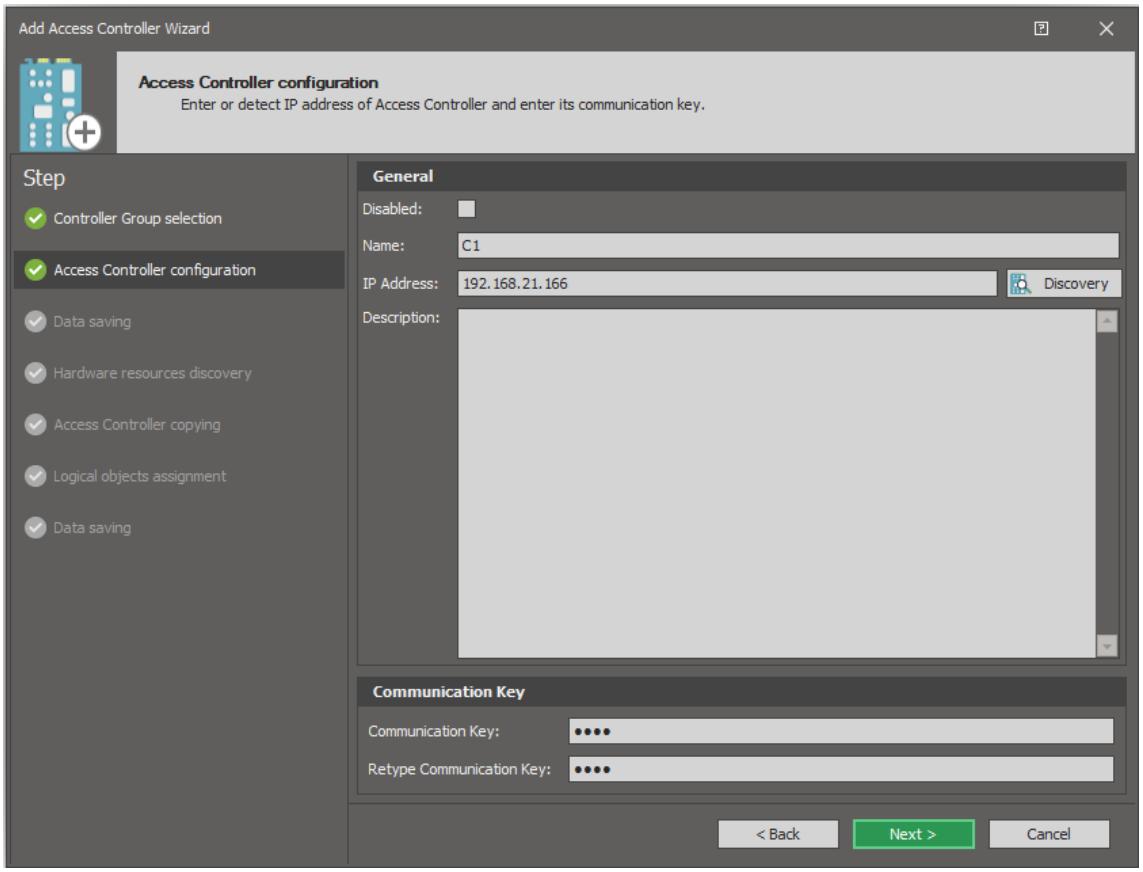
Add Access Controller Wizard can be used to configure the MC16 controller and detect its hardware resources.

- Select *Wizards* in the top menu of VISO software and then *Add Access Controller*.

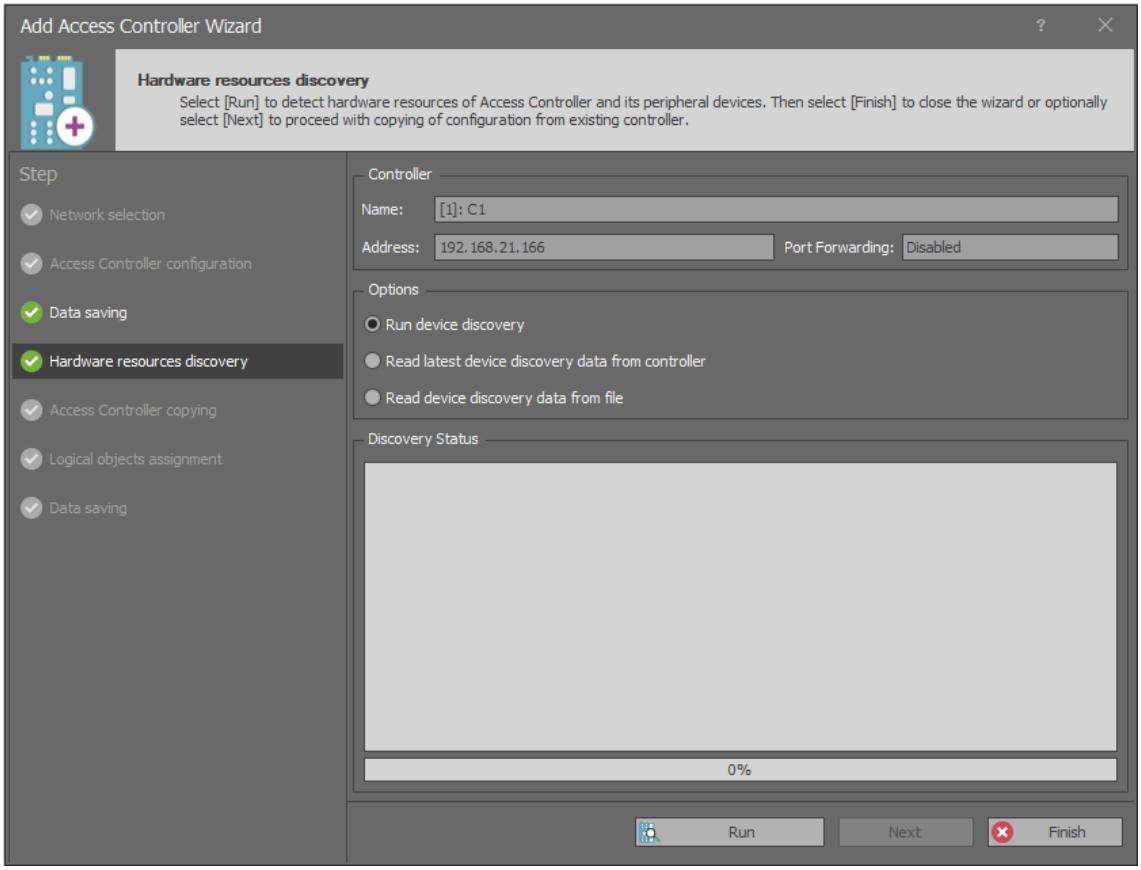
- In the opened window enter Controller Group name, indicate Communication Server and optionally select time zone and language for the group. Both final settings are useful in case of distributed multinational system which is managed by various operators. System can be divided into Controller Groups for organizational purposes only as it does not affect functionalities of access controllers. Click *Next*.



- In the next window enter or detect controller's IP address and enter communication key which was previously configured with RogerVDM software. Click *Next*.

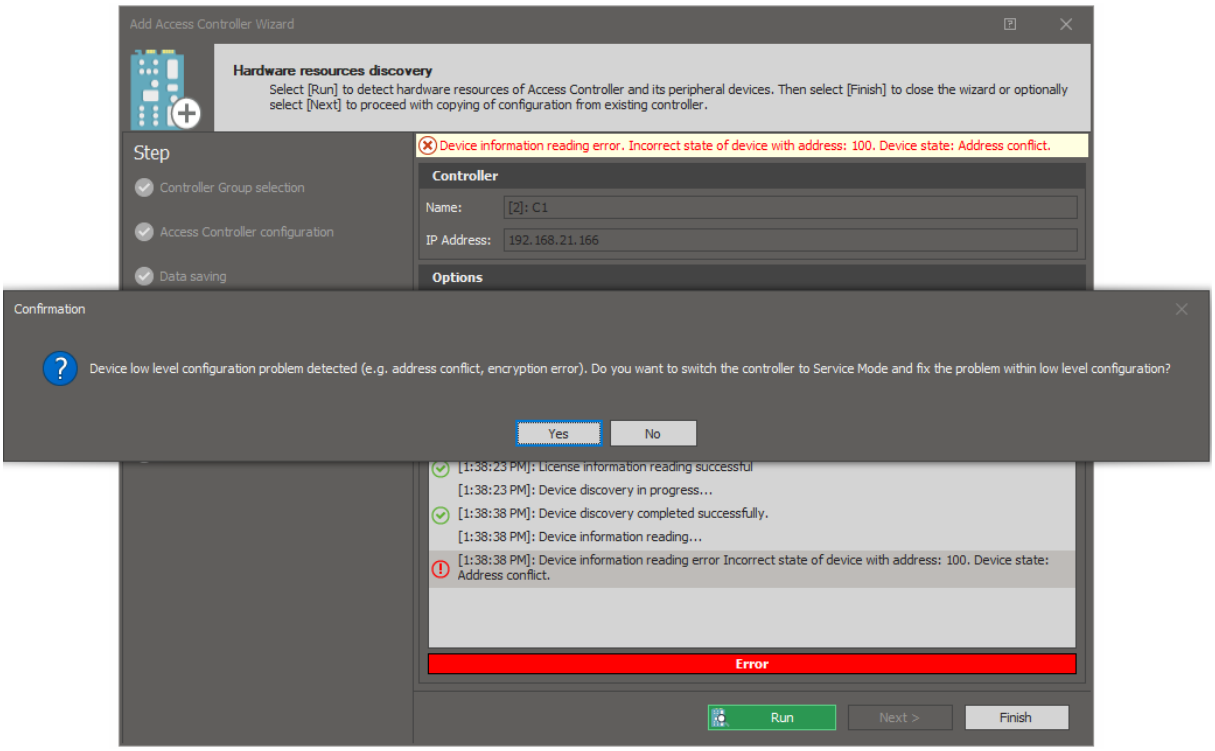


- In the next window select *Next* in order to save settings into VISO database.



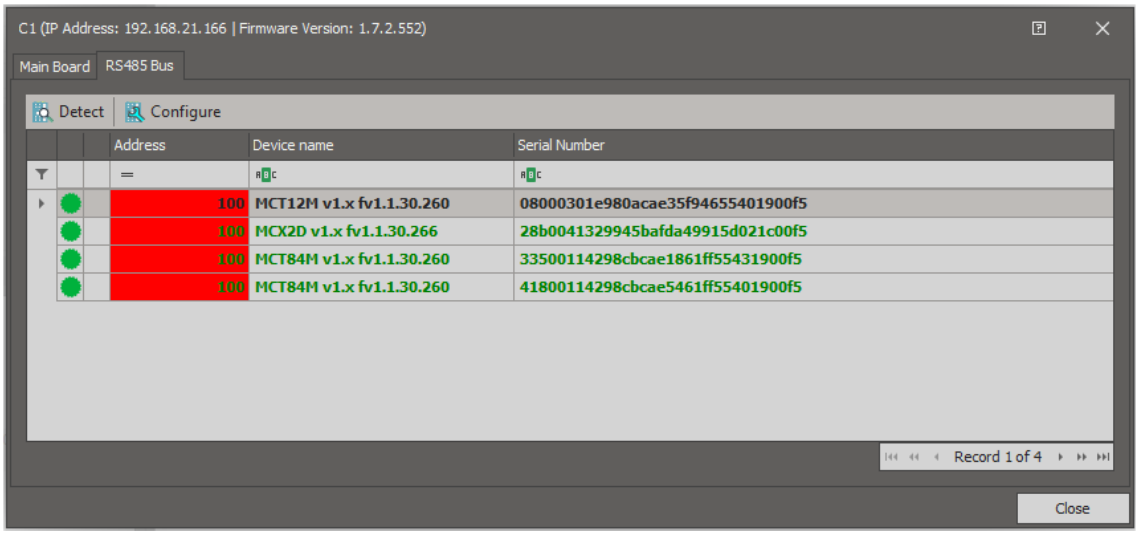
- In the next window select *Run* in order to detect hardware resources including controller and connected peripheral devices. If MCT/MCX devices were not previously addressed on controller's RS485 bus then conflict will be detected because according to their default settings all MCT/MCX devices are configured with ID=100 address. In such case select *Yes* to proceed with low level configuration.

Note: Due to security reasons the low configuration is possible only from the computer which is located in the same local area network (LAN) or virtual private network (VPN) as the MC16 controller.

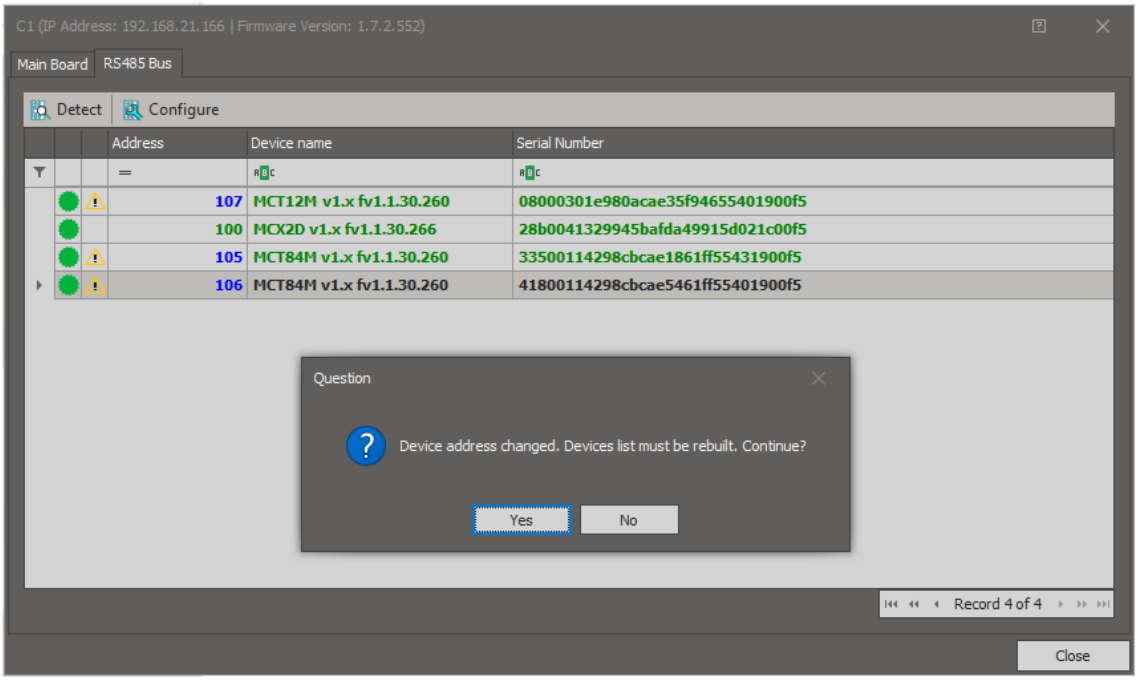


- In the opened window select *RS485 Bus* and after detection of devices select *Configure* for each device to start low level configuration of particular device. During the configuration, selected device blinks and makes sound so it could be easily distinguished from other devices in the place of its installation.

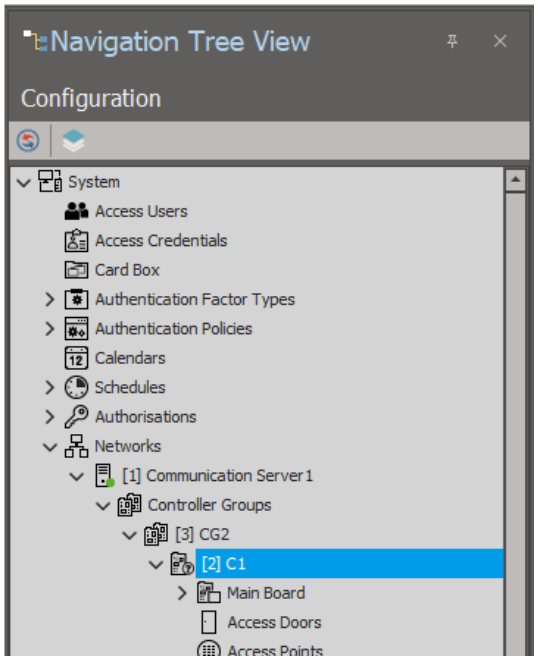
Note: MCT/MCX devices can be configured from VISO v2 software if jumper is placed properly on their contacts, usually MEM contacts. More information on this subject is given in their installation manuals.



- In the next windows configure RS485 addresses and optionally some other settings of peripheral devices. In this application note following address are applied: MCX2D address ID=100, MCT84M address ID=105, MCT84M address ID=106, MCT12M address ID=107. The range of possible addresses is 100-115 and each device on RS485 bus of MC16 controller must have unique address. At the final step confirm rebuilding of the list with devices, then select *Close* and return to wizard.



- Select *Run* to start detection of MCT/MCX devices again. After successful detection select *Finish* to close the wizard. The wizard in the next steps enables copying of configuration from another existing controller which will not be used in this guide.
- Refresh the navigation tree with button and the newly created Controller group with controller, its objects and resources will be displayed.



All the steps covered by wizard can be also executed manually in VISO navigation tree by right clicking *Networks* and then adding Communication Server, creating Controller Group, adding controller with its IP address and communication key and finally detecting hardware resources. Low level configuration can be started any time by right clicking the controller in the navigation tree of VISO software and then selecting *Low Level Configuration*.

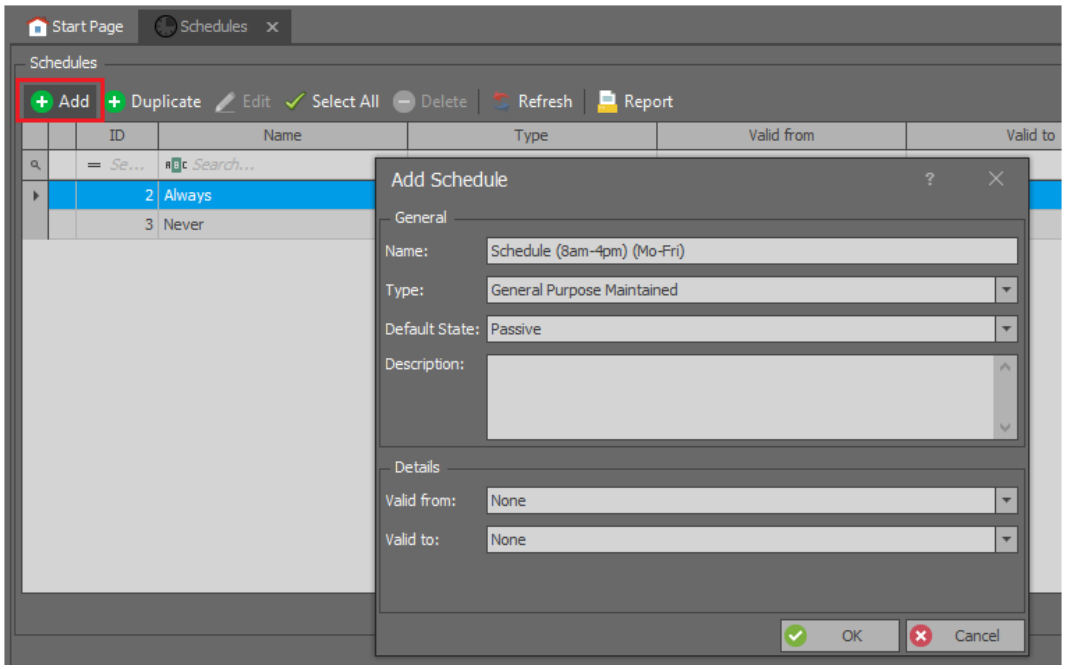
Access doors

Add Access Door Wizard can be used to configure doors and indicate input lines, output lines and Access Points (readers) as well define Basic Authorizations which can be further assigned to users in order to define their access rights at a door.

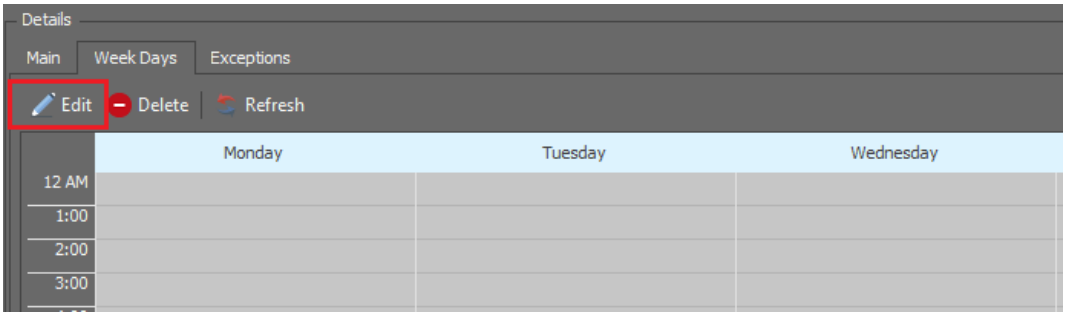
If it is required to limit Authorizations created by wizard in time then General Purpose Maintained Schedule(s) should be defined in advance.

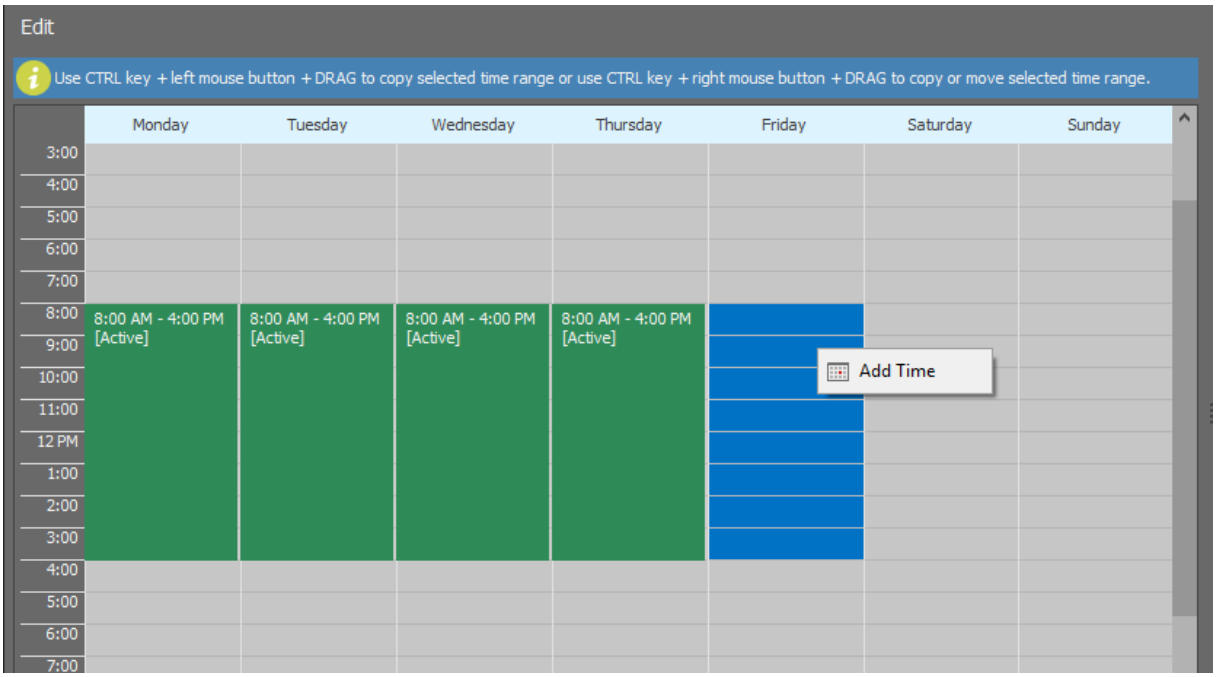
In order to define a Schedule:

- Double click *Schedules* in the navigation tree.
- In the newly opened window two predefined *Always* and *Never* Schedule are listed. Select *Add* button.
- In order to create exemplary Schedule for 8 AM to 4 PM periods from Monday to Friday enter the name of a Schedule and confirm with *OK* button.



- In the bottom of the window select the tab *Week Days* and then the button *Edit*.



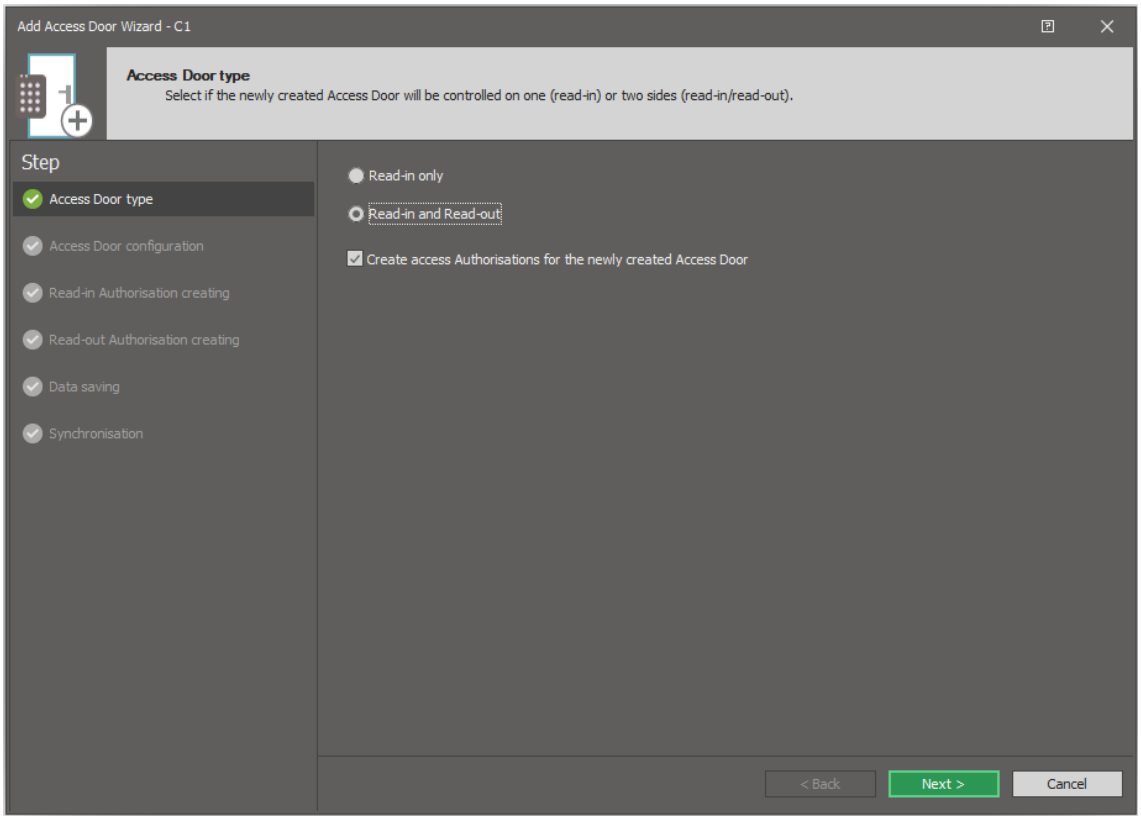


- In the newly opened window select period from 8 AM to 4 PM with left mouse button pressed and then right click to select the command *Add time*.

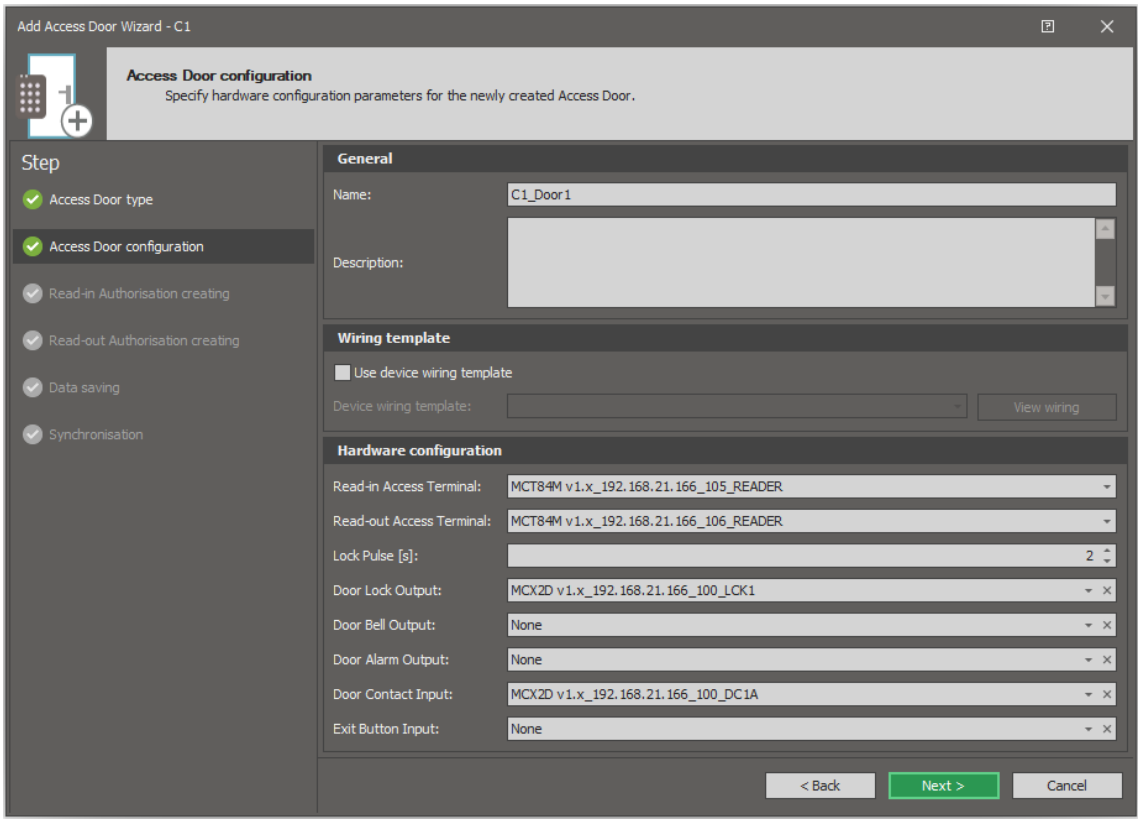
- In the next window confirm or correct the period.
- Define the same periods for remaining days i.e. for Tuesday, Wednesday, Thursday and Friday.

In order to define Access Door with wizard:

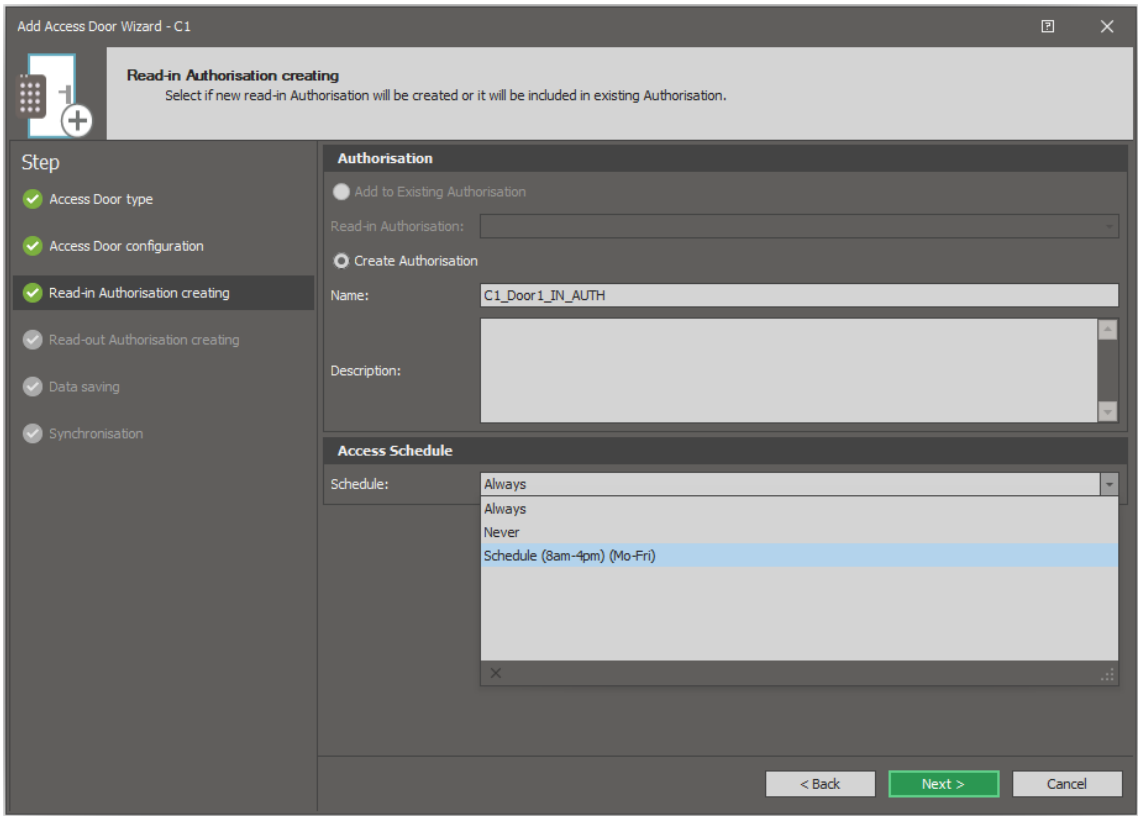
- Select *Wizards* in the top menu of VISO software and then *Add Access Door*.
- In the newly opened window select door type and then click *Next*. According to installation diagram, Door 1 is read-in/out door with MCT84M readers on both sides.



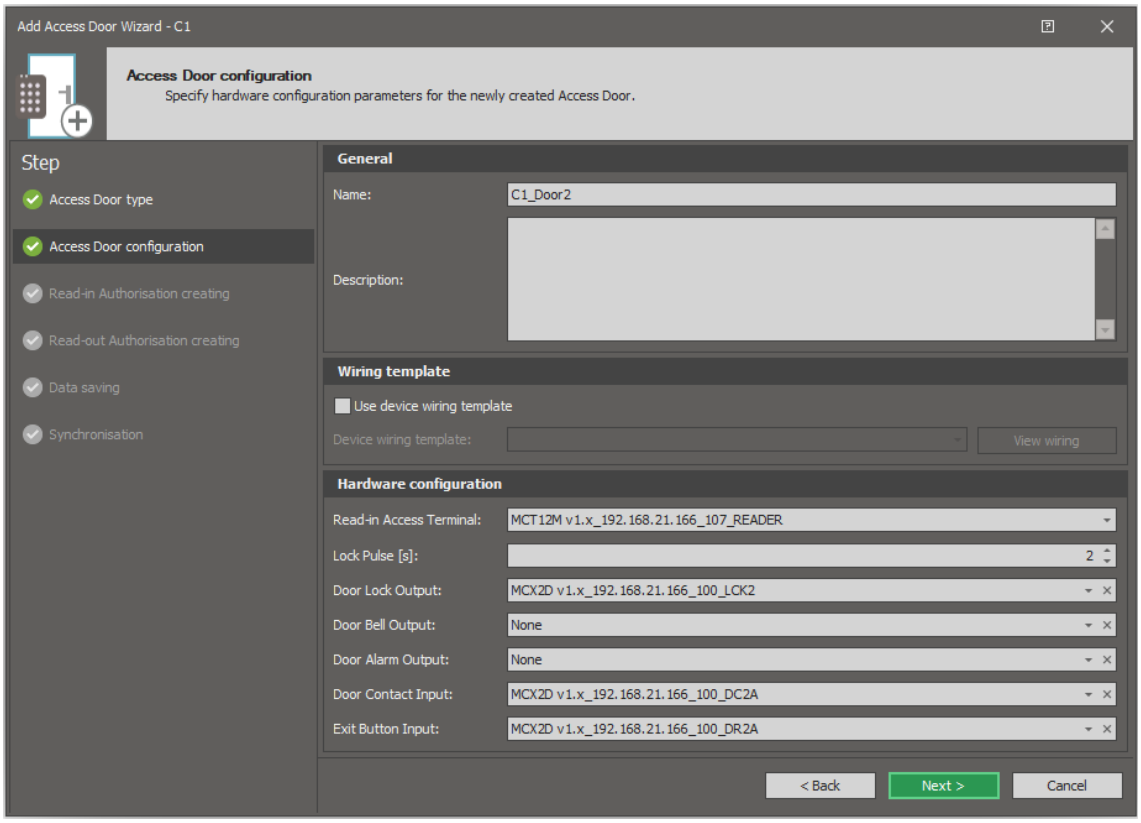
- In the next window select readers, input and output lines in accordance with the diagram and then select *Next*. Alternatively and optionally select *Use device wiring template* to automatically assign terminals, input and outputs in typical way.



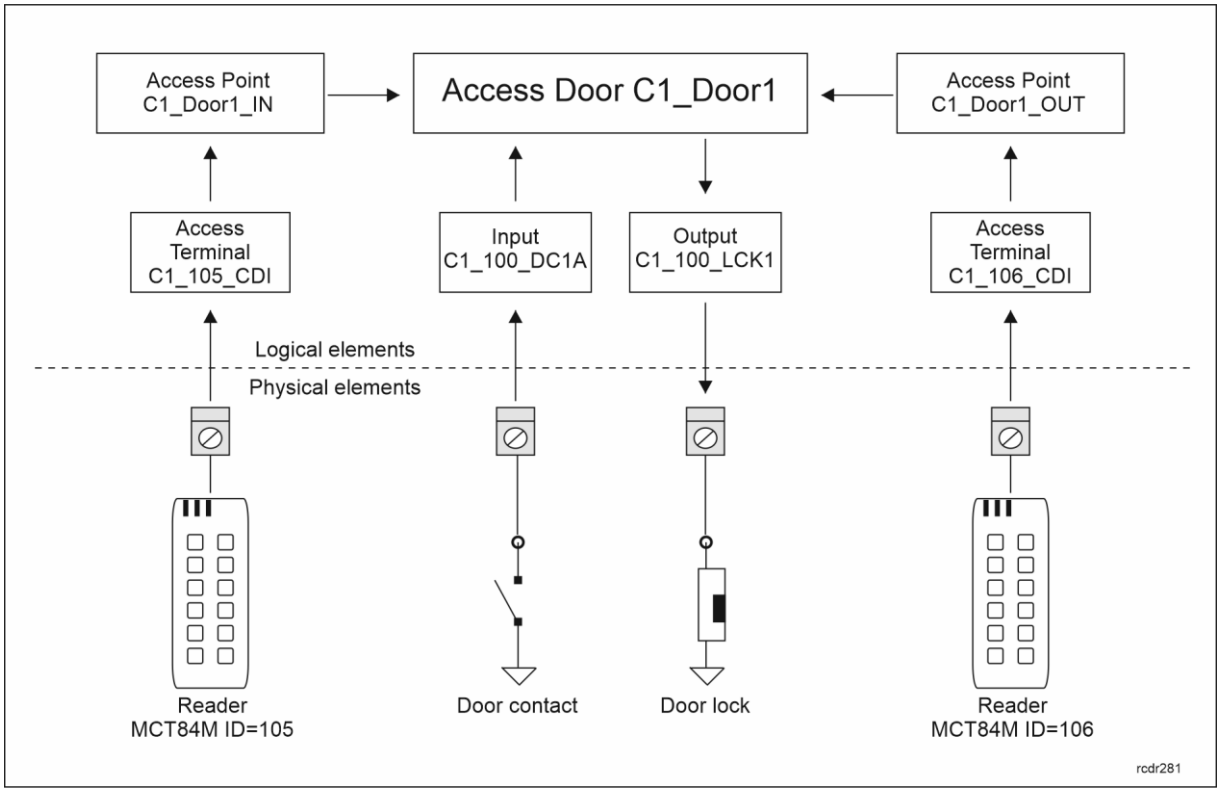
- In the next window a read-in Authorization is created. It enables access granting at read-in terminal MCT84M (ID=105). The Authorization can be later assigned to users. If it is required to limit the Authorization in time then previously created *Schedule (8am-4pm) (Mo-Fri)* can be selected. Click *Next*.

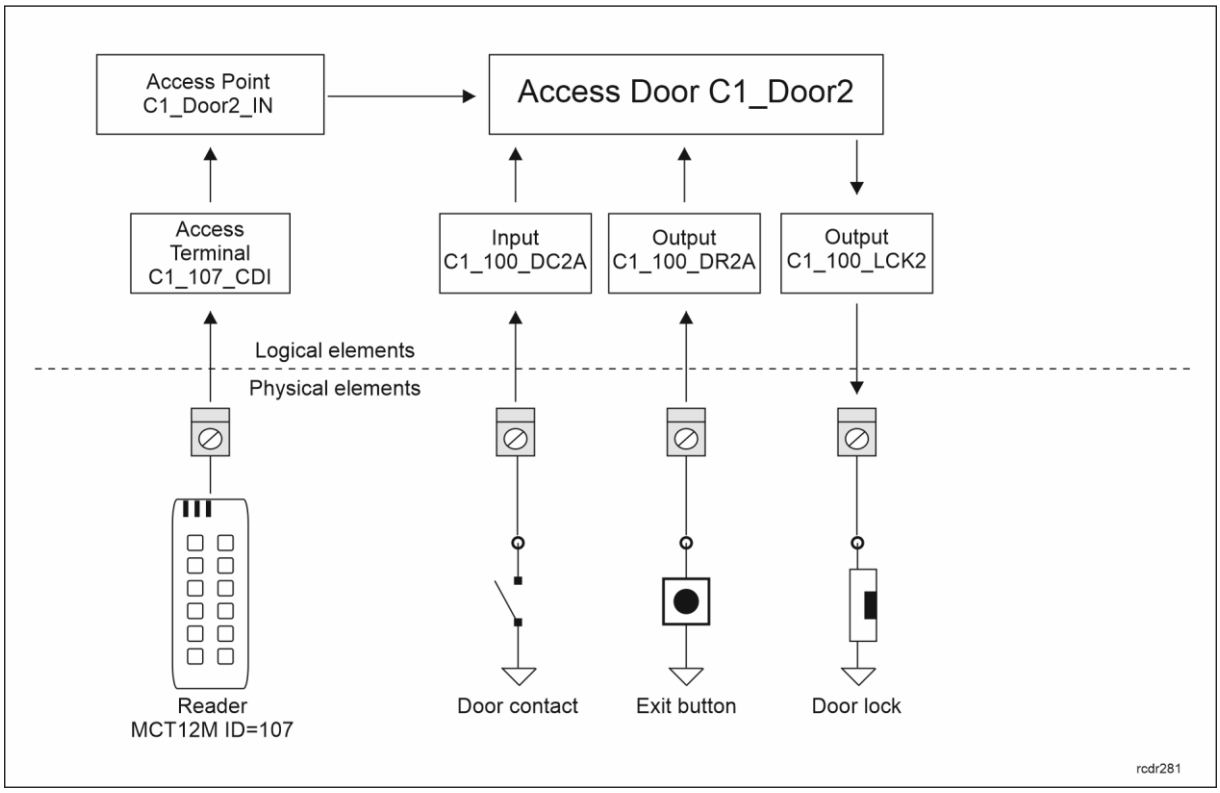


- In the next window similarly a read-out Authorization is created for read-out terminal MCT84M (ID=106). Click *Next*.
- In the next window select *Next* in order to save settings into VISO database and to create logic objects resulting from settings entered with the wizard.
- In the last window select *Start* button to synchronize settings with controller.
- Define Door 2 in similar way using the wizard and keeping in mind that according to the diagram this is read-in door with single reader, output for exit button and single Authorization.



Alternatively, Doors with their input and outputs as well as Access Points with their readers can be configured manually using VISO navigation tree. The structure of relations between objects created by wizard for Door 1 and Door 2 is given in diagrams below.





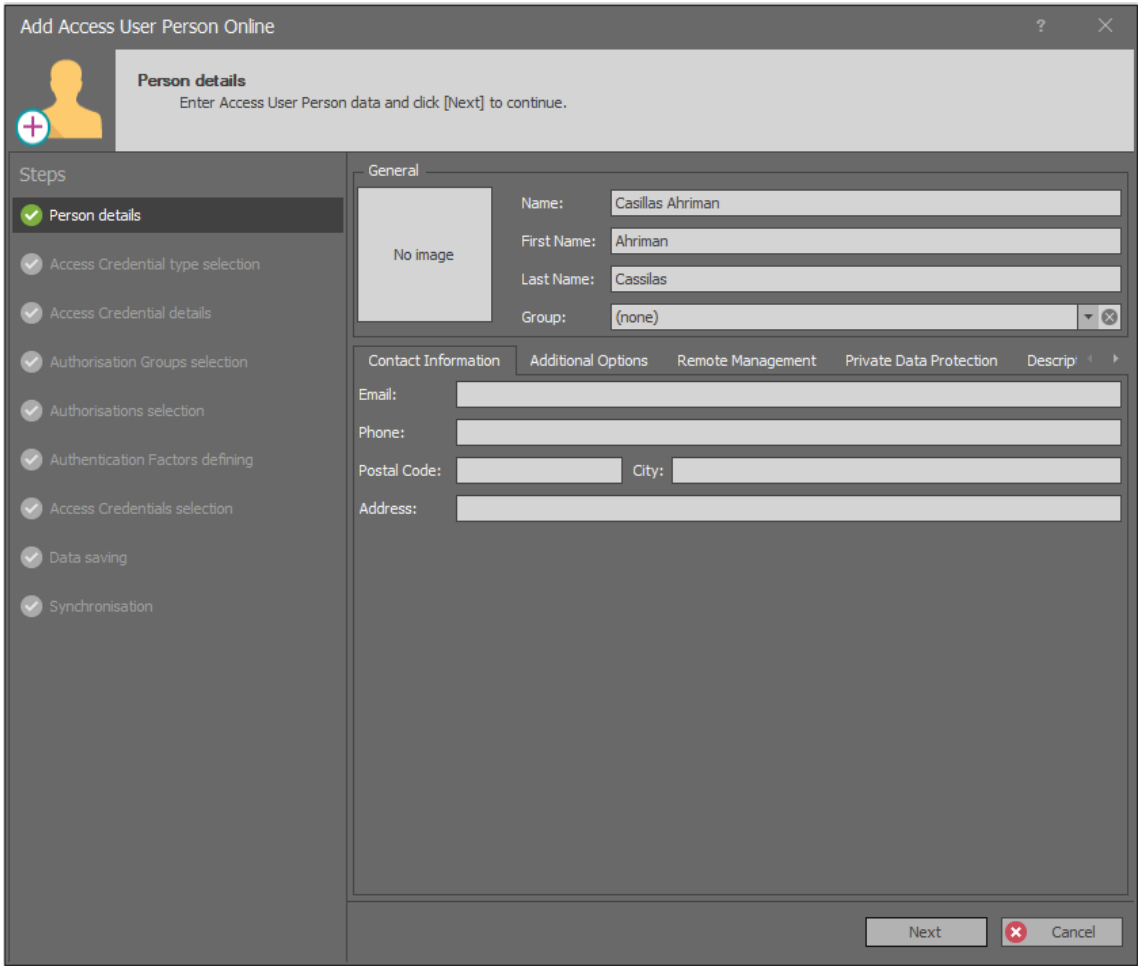
Users

User defining, editing and deleting can be done with wizards in VISO software.

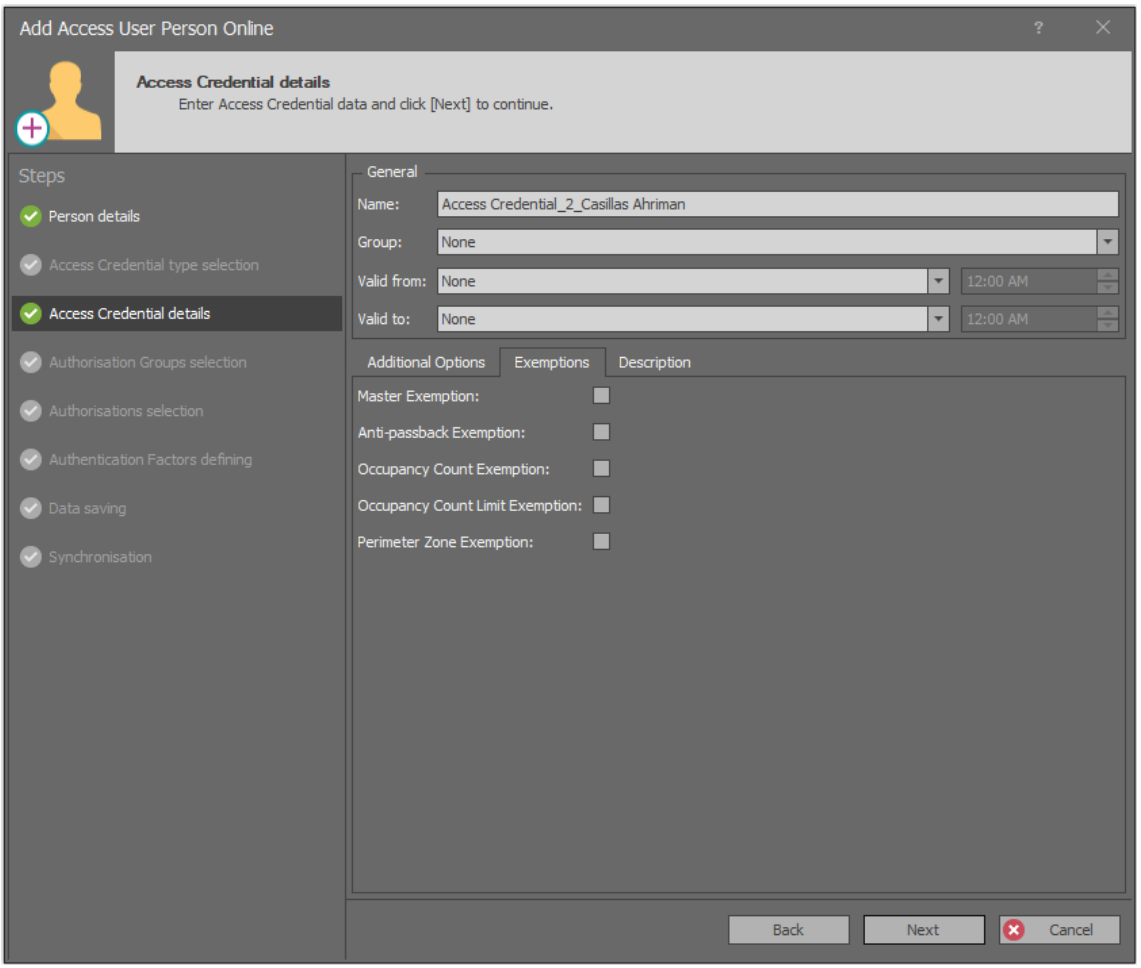
In order to define a user with wizard:

- Select *Wizards* in the top menu of VISO software and then *Add Person Online*.

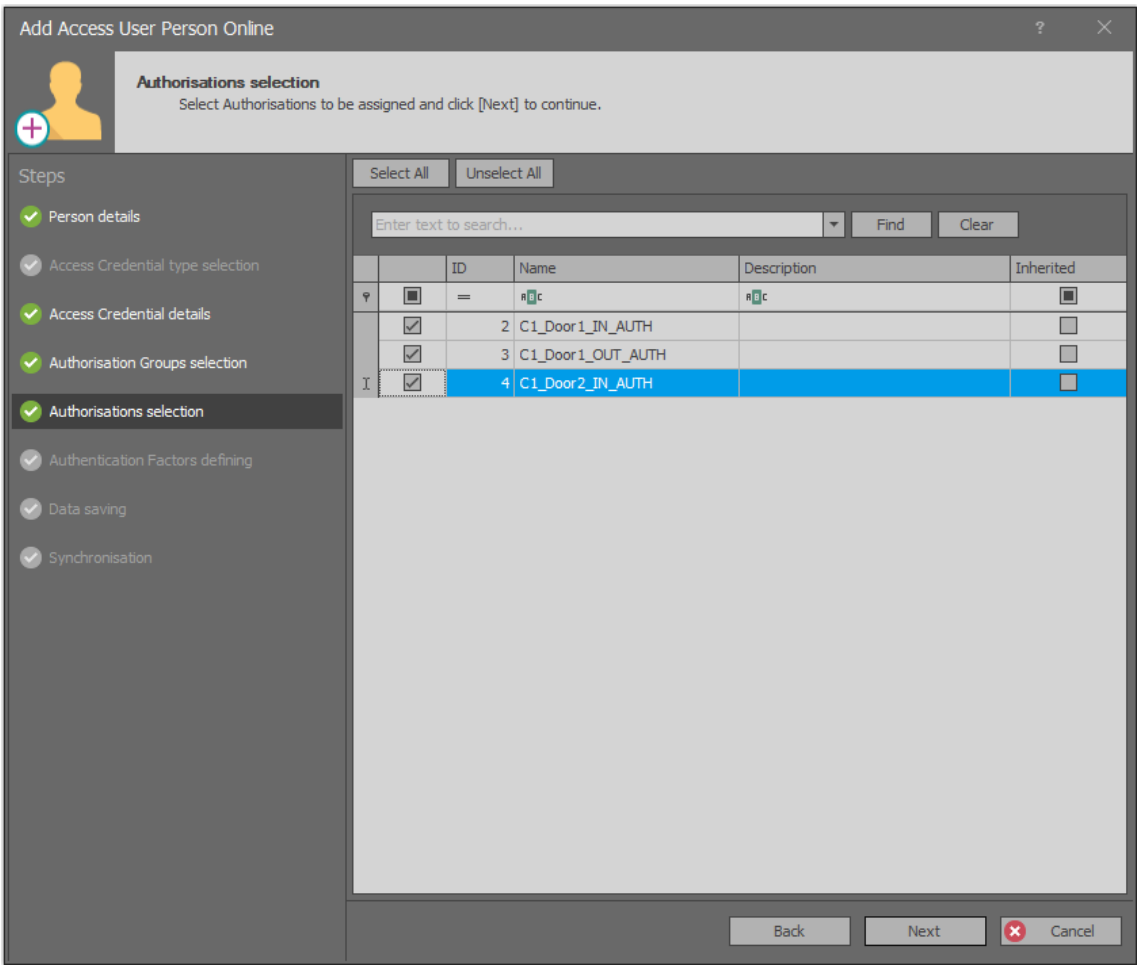
- In the newly opened window enter user names and click *Next*. Optionally photo can be assigned by right clicking *No image* area and selecting respective command.



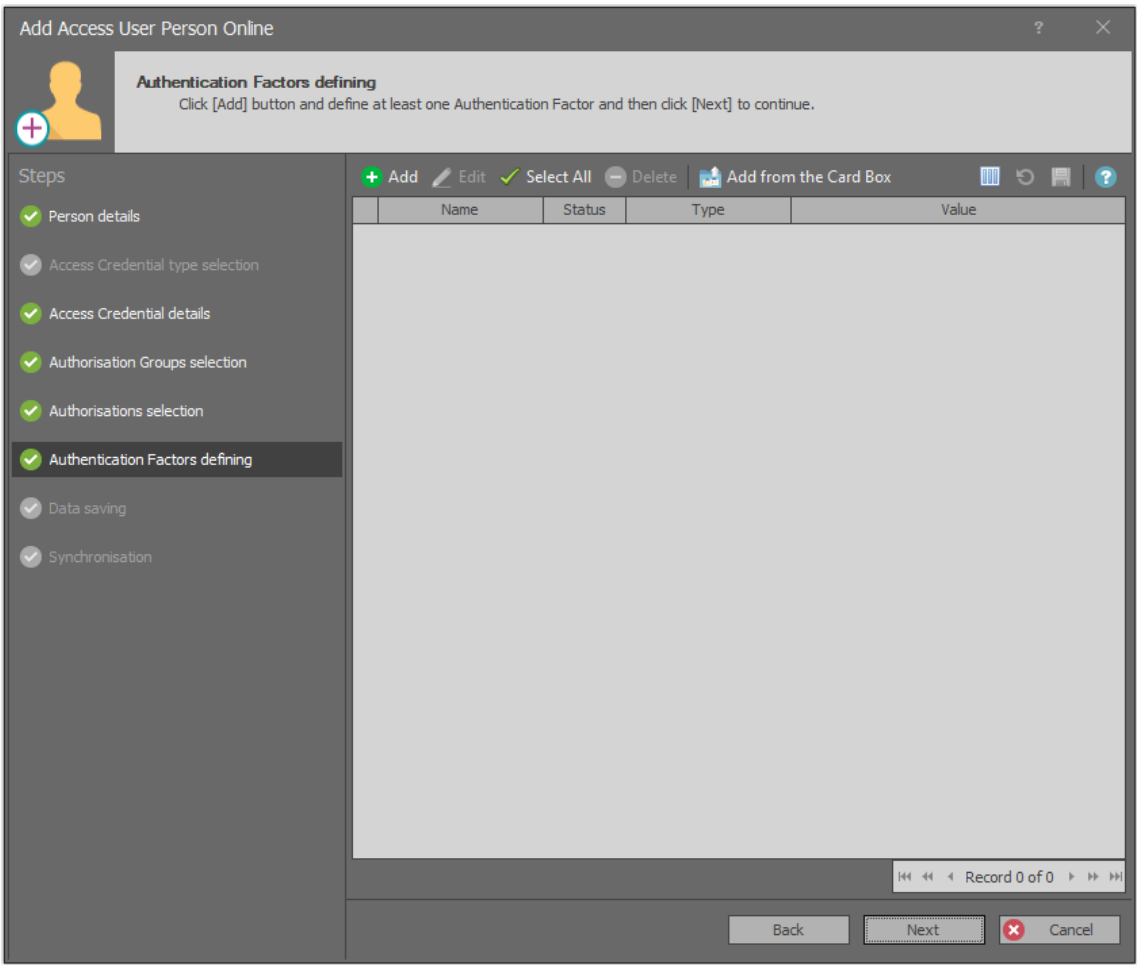
- In the next window select *Create new Access Credential* and then *Next*.



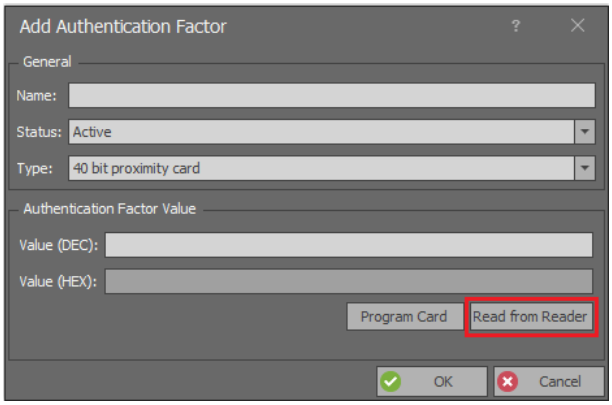
- In the next window it is possible to define credential validity period. Optionally, in the *Exemptions* tab various privileges can be assigned to the credential. If *Master Exemption* is selected then the user will gain all possible Authorizations in the system in regard of access, arming/disarming and other functions. Click *Next*.
- In the next step, Authorization Groups can be assigned to the Access Credential if they were created earlier. Authorizations can be grouped by selection of *Authorizations-> Authorization Groups* in VISO navigation tree. The purpose of Authorisation grouping is to facilitate assignment of typical Authorisations (e.g. main doors) to users by avoiding individual assignment of such Authorisations every time a user is defined in the system. Such grouping is not used in this application note so click *Next*.
- In the next window it is possible to assign individual Authorizations to the Access Credential. Three Authorizations are available in the system. Select all of them so the user could open each door using associated readers. Click *Next*.



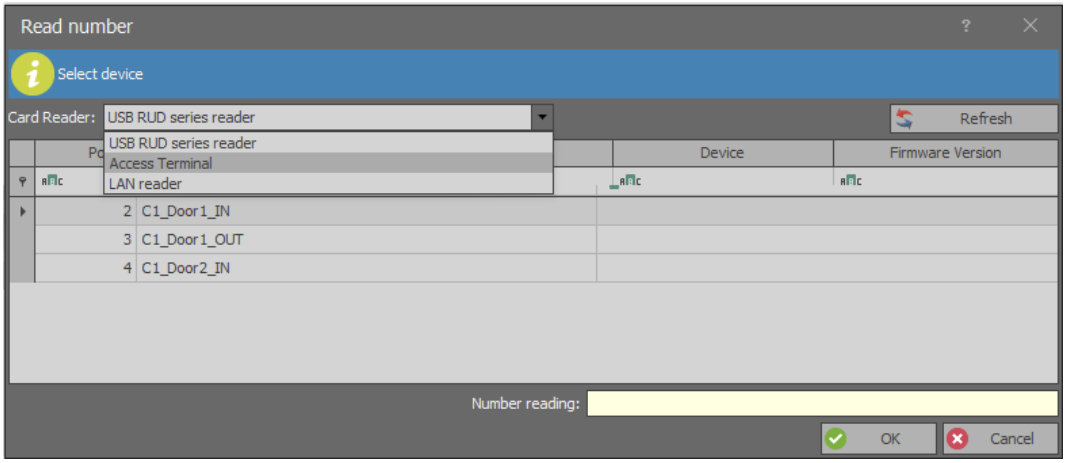
- In the next step start configuration of Authorization Factors selecting *Add* button.



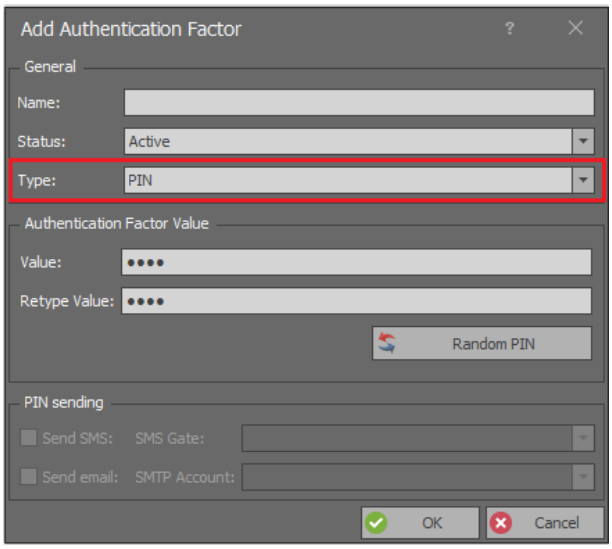
- Select the button *Read from Reader*. Alternatively the card number can be entered manually in the *Value(DEC)* field if card number is known.



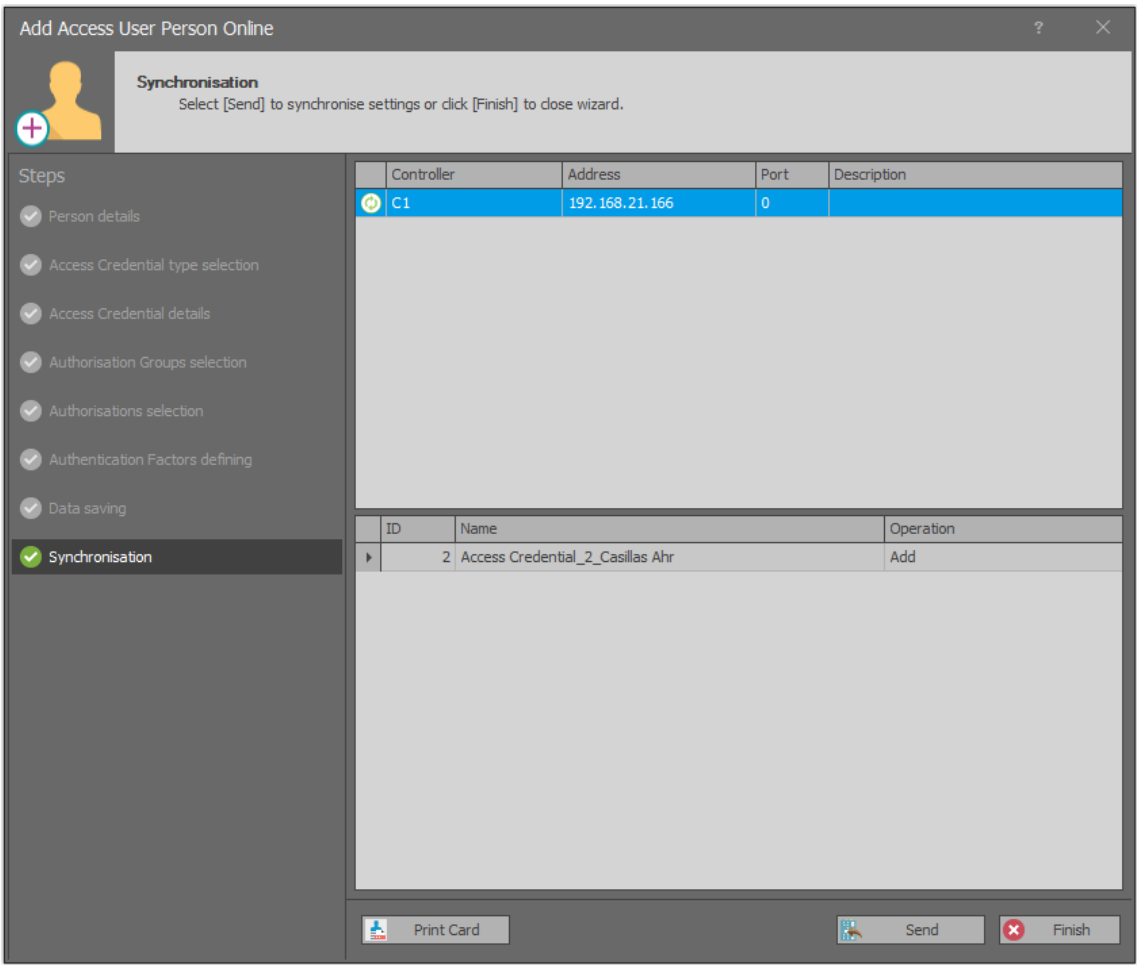
- In the newly opened window select card reader type. The list of devices for the option *USB RUD series reader* is empty if no RUD type (e.g. RUD-3) administrator reader is connected to computer. Access Terminals are MCT readers connected to the controller. Select *C1_Door1_IN* reader and then read your card at MCT84M (ID=105) reader so the card number would be displayed in *Number Reading* field.



- Click *OK* and then once again *OK* to confirm proximity card and return to Authentication Factors window. Select *Add* button to configure one more Factor. Select *PIN code* type instead of *40 bit proximity card*.



- Enter PIN (e.g. 1234) in the field *Value* and again in the field *Retype Value*. Click *OK* to confirm PIN and return to Authentication Factors window.
- In the next window select *Next* in order to save settings into VISO database and to create logic objects resulting from the wizard.
- In the last window select *Send* button to synchronize settings with controller using special method which does not interrupt controller operation. If the *Send* button is gray and not available for use then select *Finish* button and upload full configuration to the controller, for example by right clicking *Networks* in VISO navigation tree and then *Synchronise* and *Start*.

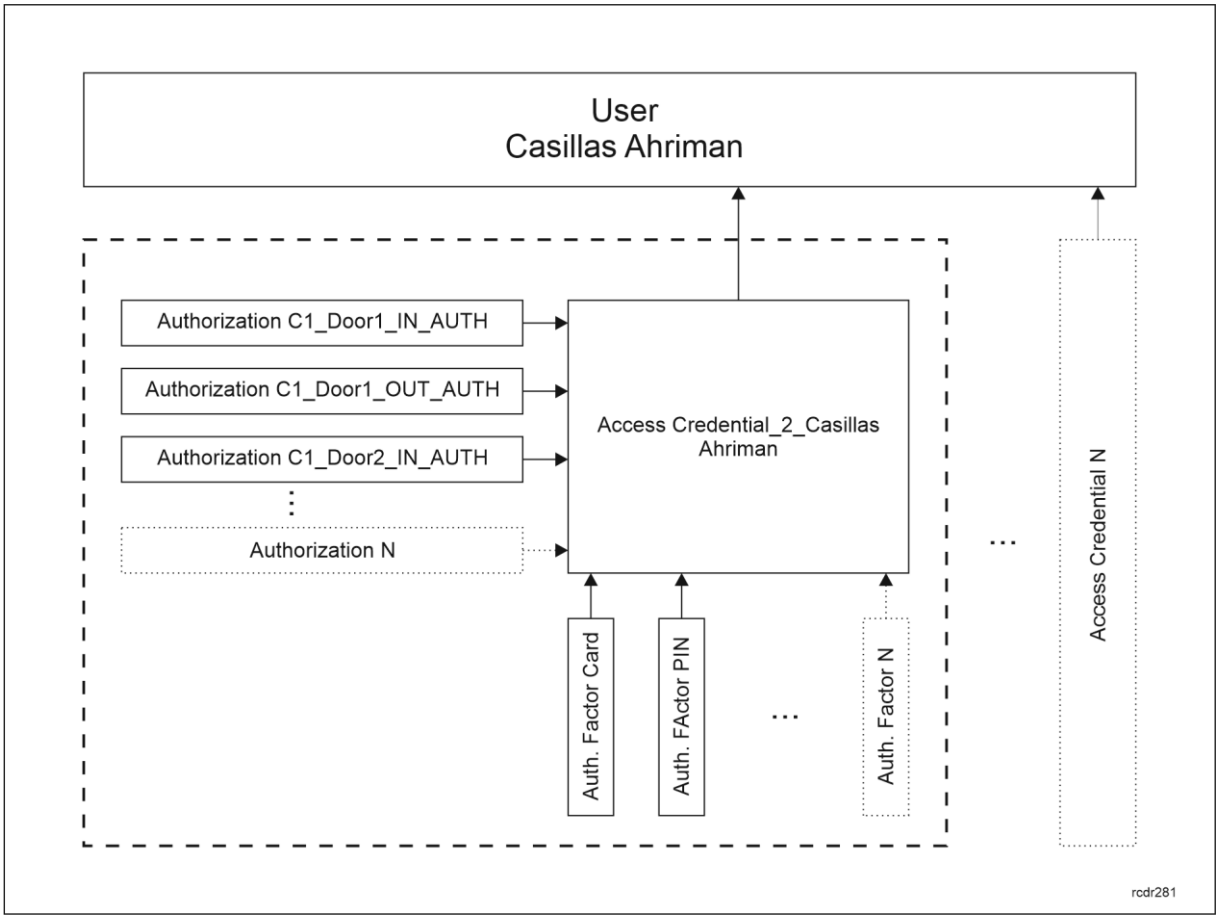


- Verify if proximity card and PIN used on any reader enable activation of LCK1 and LCK2 outputs of MCXD2D expander. These outputs will be used to control door locks. PIN must be concluded with # key on reader's keypad.

Users can be edited and deleted with two remaining wizards i.e. *Edit Person Online* and *Delete Person Online*.

Alternatively, Users, Access Credentials, Authorizations and Authentication Factors can be configured manually using VISO navigation tree. The structure of relations between objects created by wizard for Casillas Ahriman user is shown in diagram below.

In RACS 5 v2 system new method for quick user defining in single window is available. *Add Person Quickly* wizard can be accessed via *Favourites* section in VISO start page and via *Add* button on the list of Access User Persons. More information on users is given in AN051 application note.



Technical diagnostics

Hardware

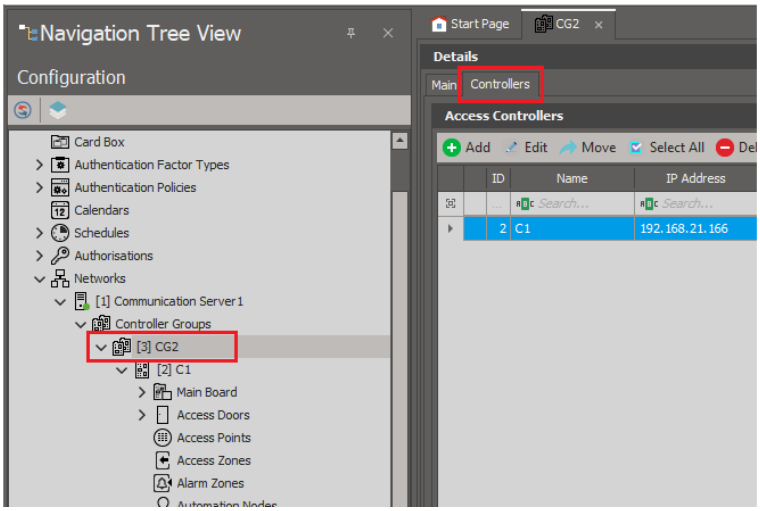
In the system with detected access controllers and peripheral devices (MCT, MCX) it is possible to:

- Verify connection with devices
- Check status of input lines
- Trigger output lines
- Make low level configuration of devices

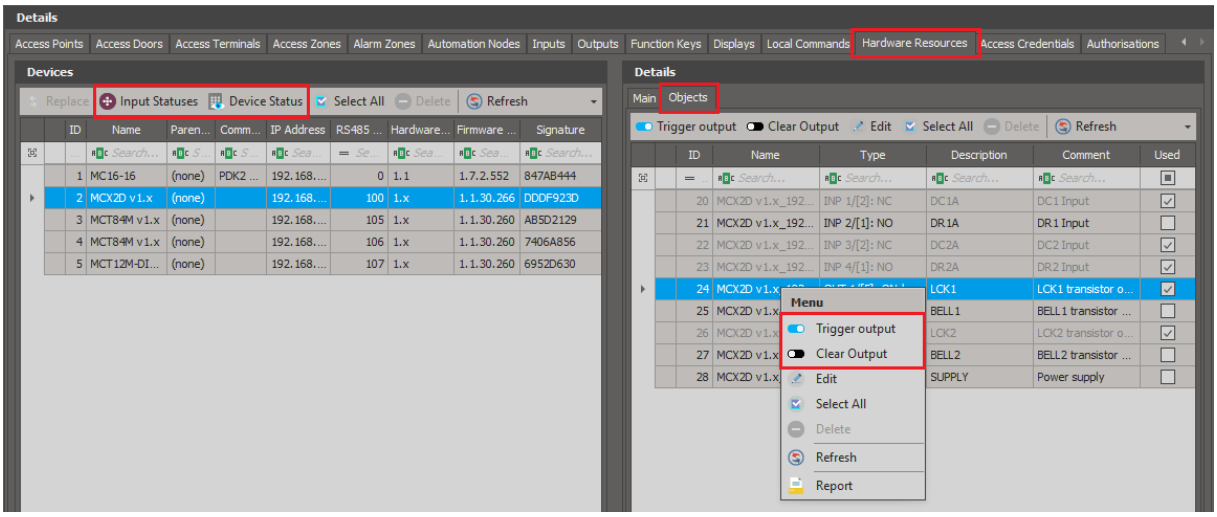
These tools are used for diagnosis of the system during installation and verification of cable connections. They can also be used for troubleshooting in case of system failure.

In order to access diagnostic tools:

- In the navigation tree of VISO software expand *Networks,* particular Communication Server, then *Controller Groups* and double click one of Controller Groups.
- In the opened window select *Controllers* tab.



- Select controller and in the window on the right select *Hardware Resources* tab.



- Use such commands as *Input Statuses* and *Device Status*.
- On the right, select *Objects* tab to display window where outputs can be triggered.

The same functionalities are also available when *Hardware Resources* within particular access controller are double clicked in the navigation tree of VISO software.

Contact:
Roger sp. z o.o. sp.k.
82-400 Sztum
Gościszewo 59
Tel.: +48 55 272 0132
Fax: +48 55 272 0133
Tech. support: +48 55 267 0126
E-mail: support@roger.pl
Web: www.roger.pl