Roger Access Control System 5

Application note no. 006

Document version: Rev. G

RACS 5 Quick start guide

Note: This document refers to RACS 5 v1.6.6 or newer

Introduction

The document presents quick start guide for RACS 5 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

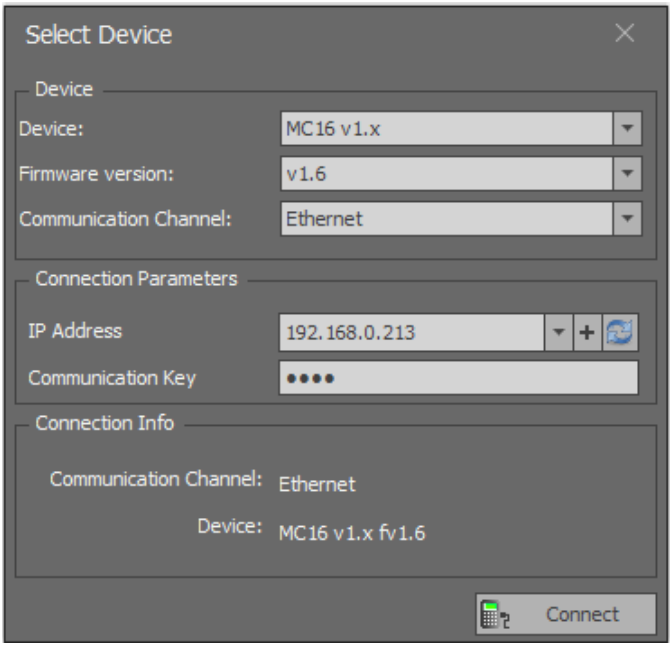
MC16 controller

The purpose of controller's low level configuration is to define controller 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.

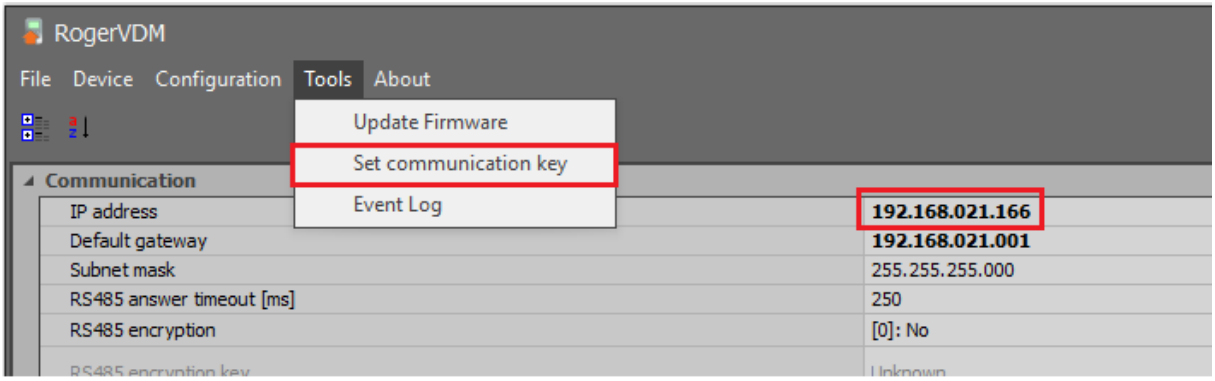
Factory new MC16 controller has IP address set to 192.168.0.213 and the communication key is 1234. Both can be changed with RogerVDM software.

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. Select 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 RS485 bus address. 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.

In the example covered by this note two MCT84M and single MCT12M readers are connected to controller. Each device connected to RS485 bus of MC16 controller must have unique address in range of 100..115. In the example, ID=105, ID=106 and ID=107 addresses will be applied for readers.

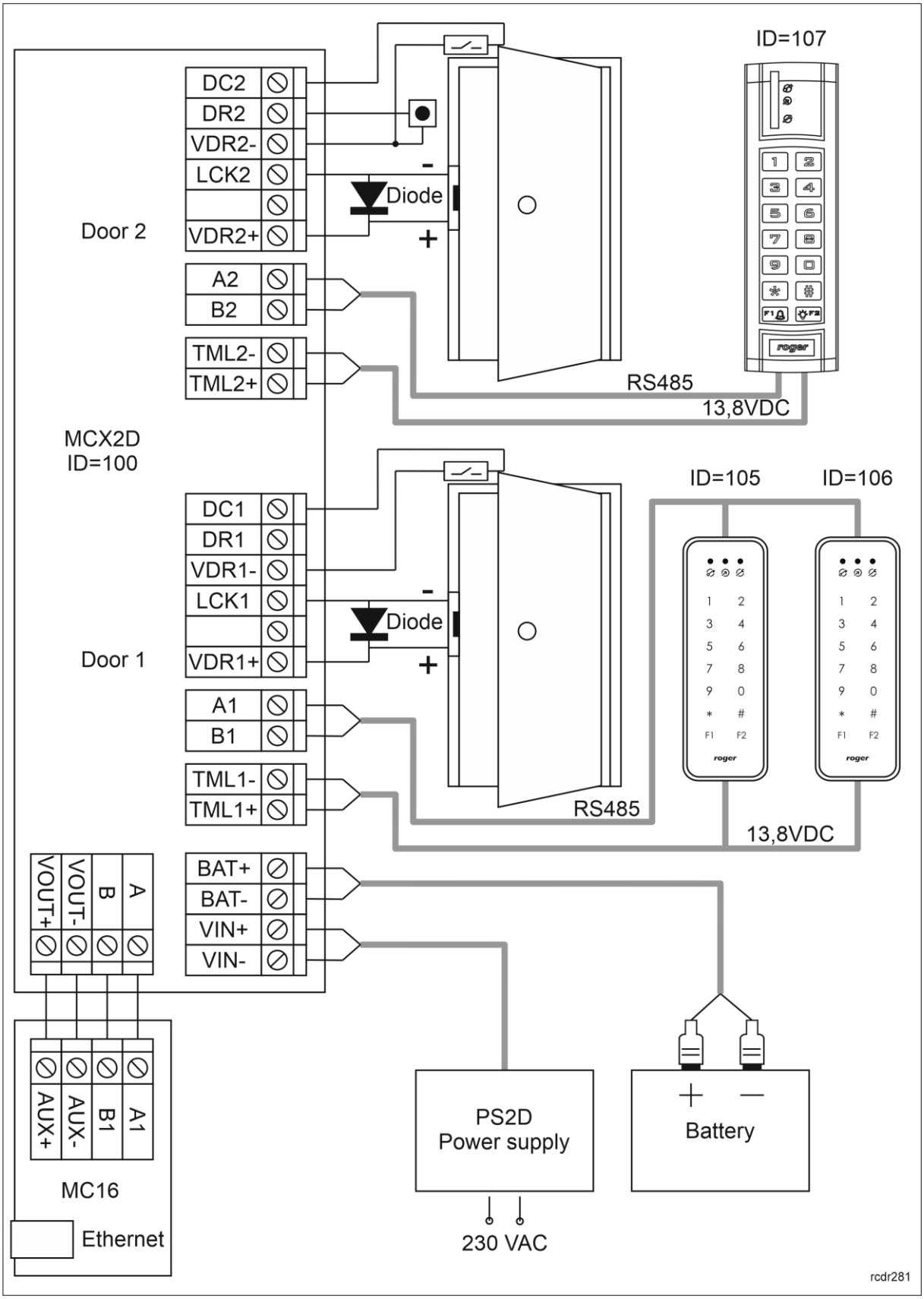
MCX2D expander

MC16-PAC-2-KIT includes MCX2D expander which offers power supply, communication as well as input and outputs for each door. In typical installation scenario the expander does not require low level configuration and it can be operated with default ID=100 address on RS485 bus if addresses of all connected readers differ from default ID=100 address. In RACS 5 system each device on RS485 bus of MC16 controller must have unique address in range of 100..115.

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).

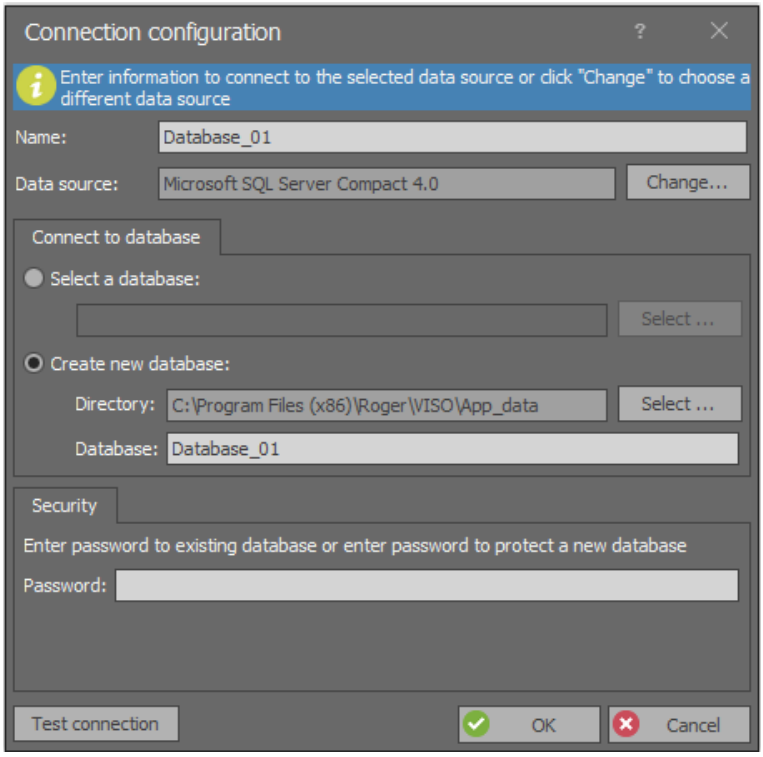
According to AN002 application note other communication and power supply scenarios are available based on other I/O expanders and MCT readers with built-in inputs and outputs.


ID=107
DC2
DR2
VDR2-
LCK2
VDR2+
Door 2
Diode
-
+
A2
B2
TML2-
TML2+
RS485
13,8VDC
MCX2D
ID=100
ID=105
ID=106
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

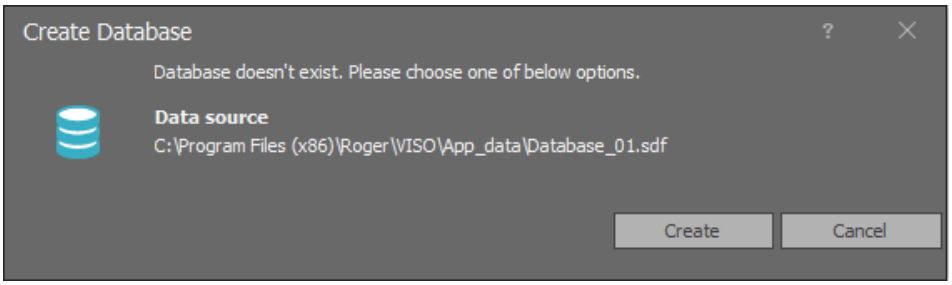
Database

High level configuration of RACS 5 system is stored in VISO software database. The system can work with local type Microsoft SQL Server Compact 4.0 database or centralized type Microsoft SQL Server 2005 (or higher) database. In this note a local type database will be used. Such database type is dedicated to small systems with up to dozen doors. The configuration of centralized database is explained in AN017 Application note.

- Install and start VISO software.
- In the window shown below enter connection name and create new database selecting its target location and name. Optionally define database password. Click *OK* button.



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

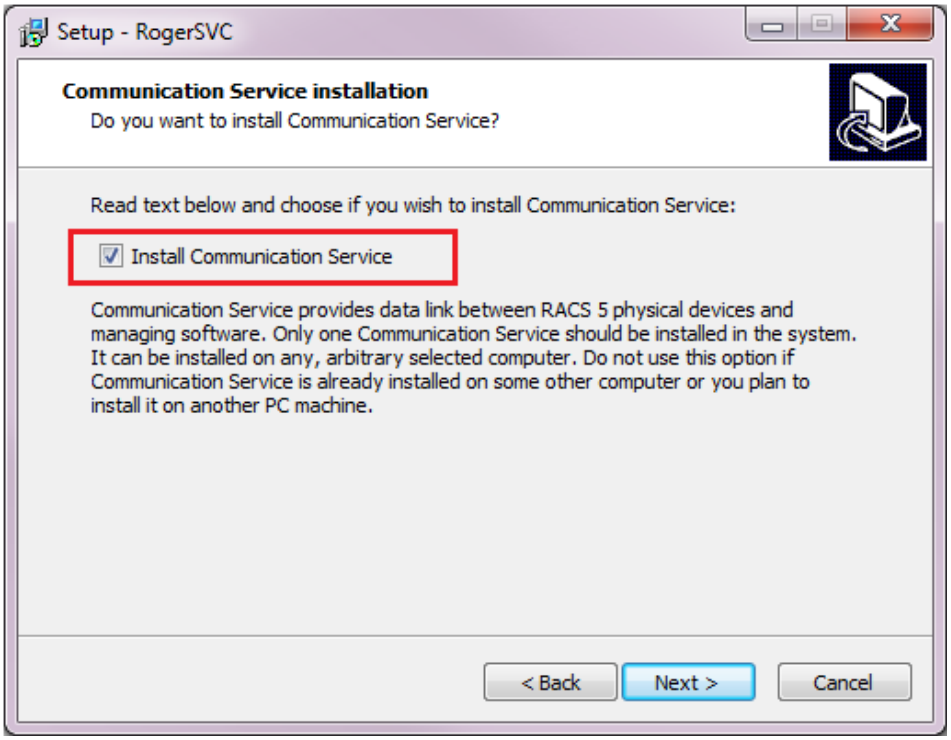


- When new database is created then VISO software login window is displayed.
- When the software is started for the first time then it is necessary to define own password for Admin operator. In case of VISO 1.6.6 or older there is no such requirement so it is enough to click *OK* in order to start the VISO ST software. The password can be later changed/defined by selection of *Administration* in the top menu of VISO software and then *Operators*.

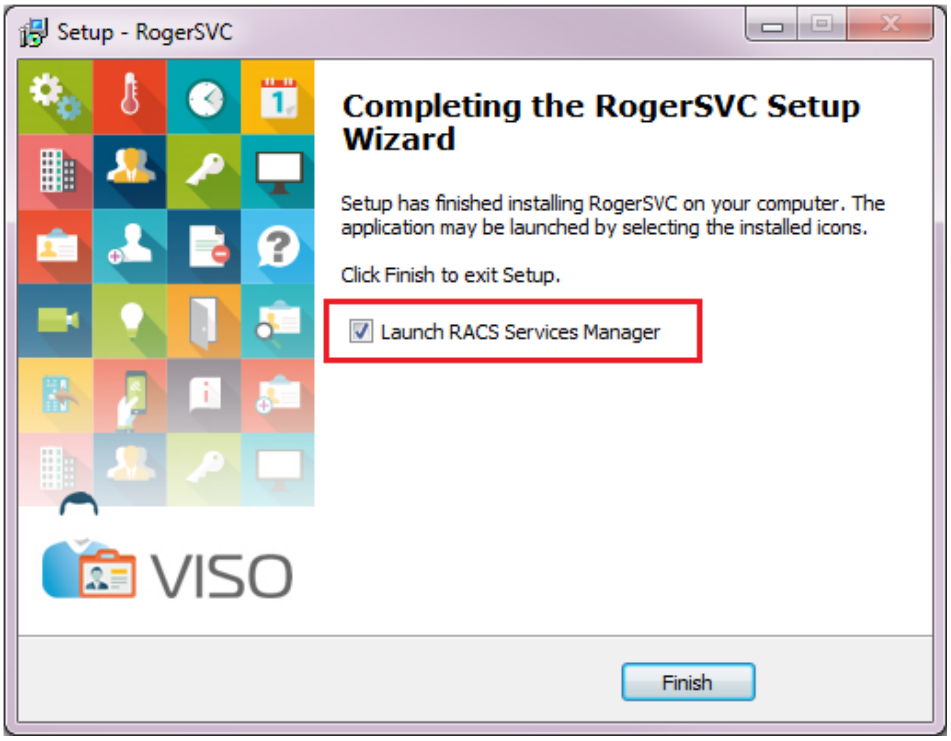
RACS 5 Services

It is necessary to configure 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 selecting Communication service. Other services are optional. They can be installed but they will not be used in this guide.

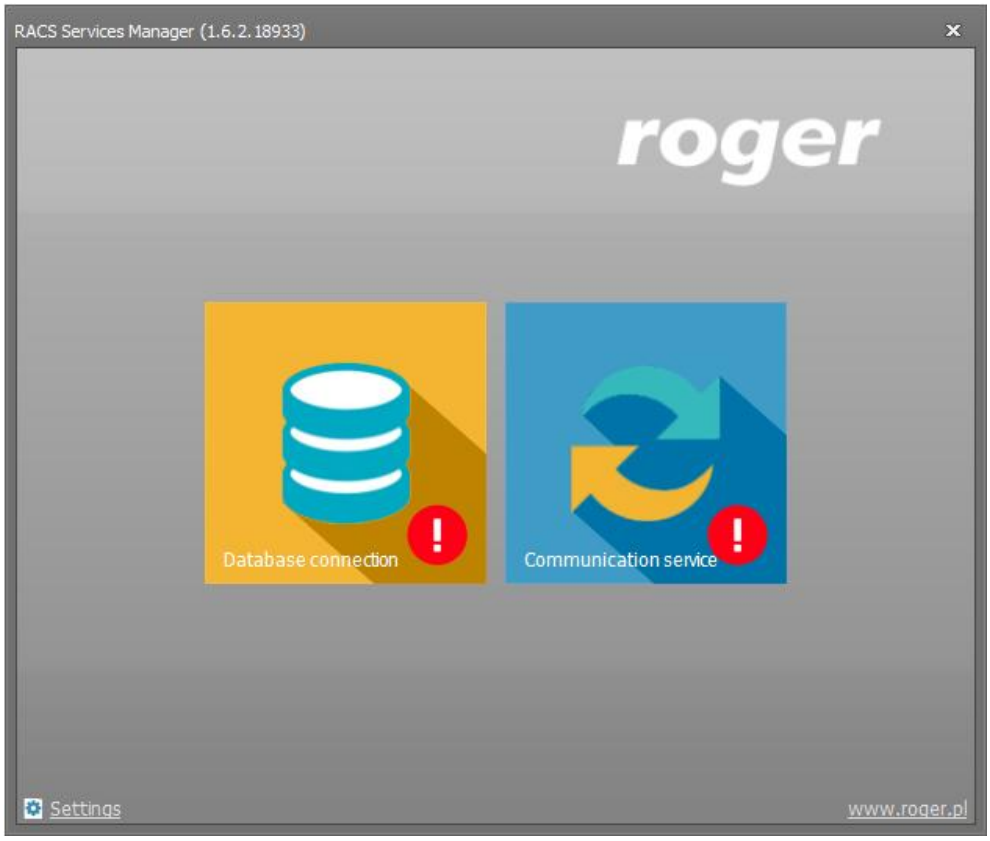


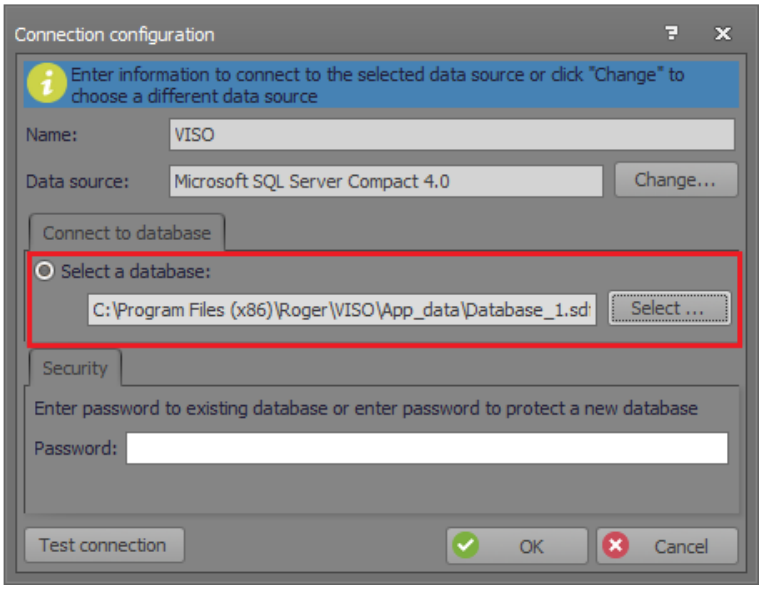
- In the final step of the installation launch RACS Services Manager.



- When RACS Services Manager is started then its icon is displayed in Windows tray. Click it to open the manager. The manager in tray can also be launched from Windows menu *Start->Roger-> RogerSVC.*

- In the RACS Services Manager select the tile *Database connection*, click the command *Configure connection* and then indicate the location of your database created previously with VISO software.
- In case of first installation of RogerSVC it is also necessary to start Communication service by clicking its tile and then selecting *Start*.



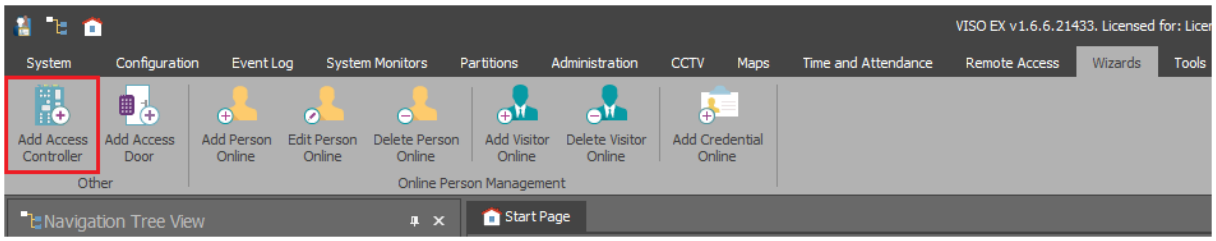


High level configuration

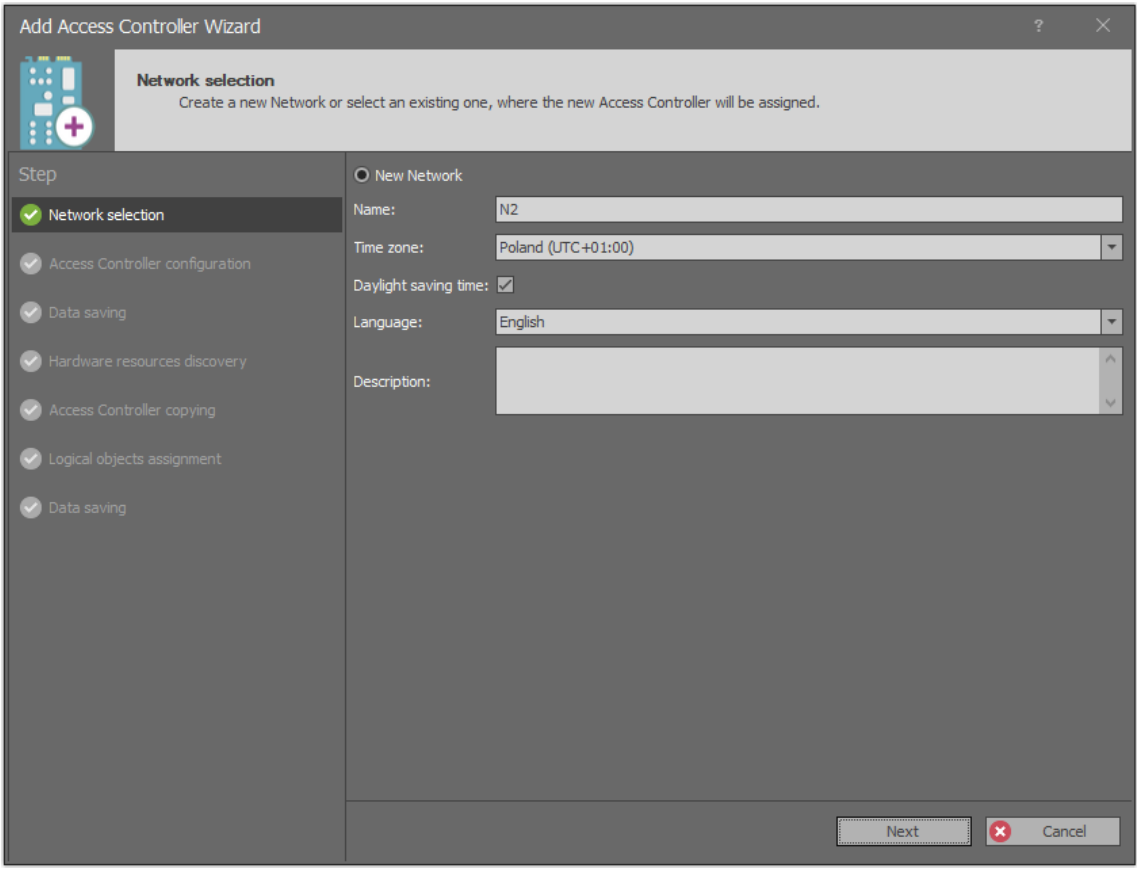
MC16 controller

Add Access Controller Wizard can be used to configure the controller in regard of hardware resources detection.

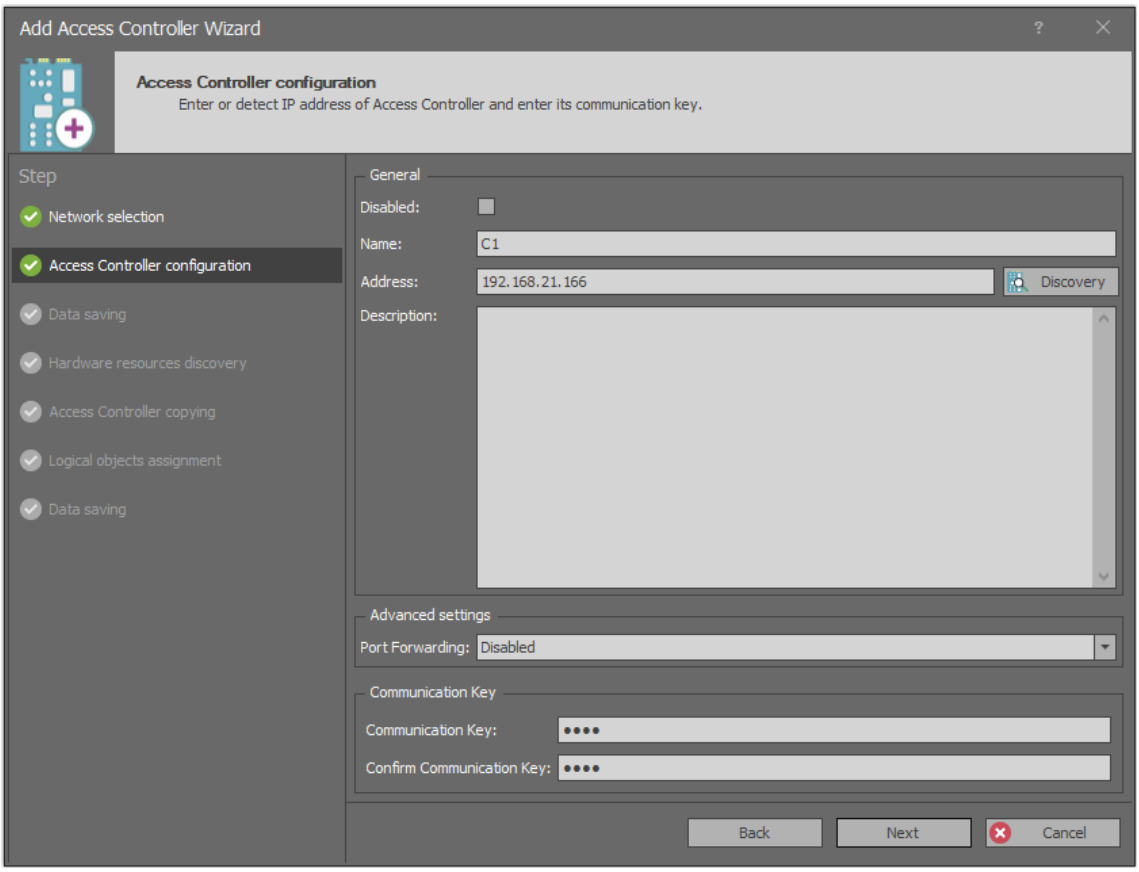
- Select *Wizards* command in the top menu of VISO software and then *Add Access Controller Wizard*.



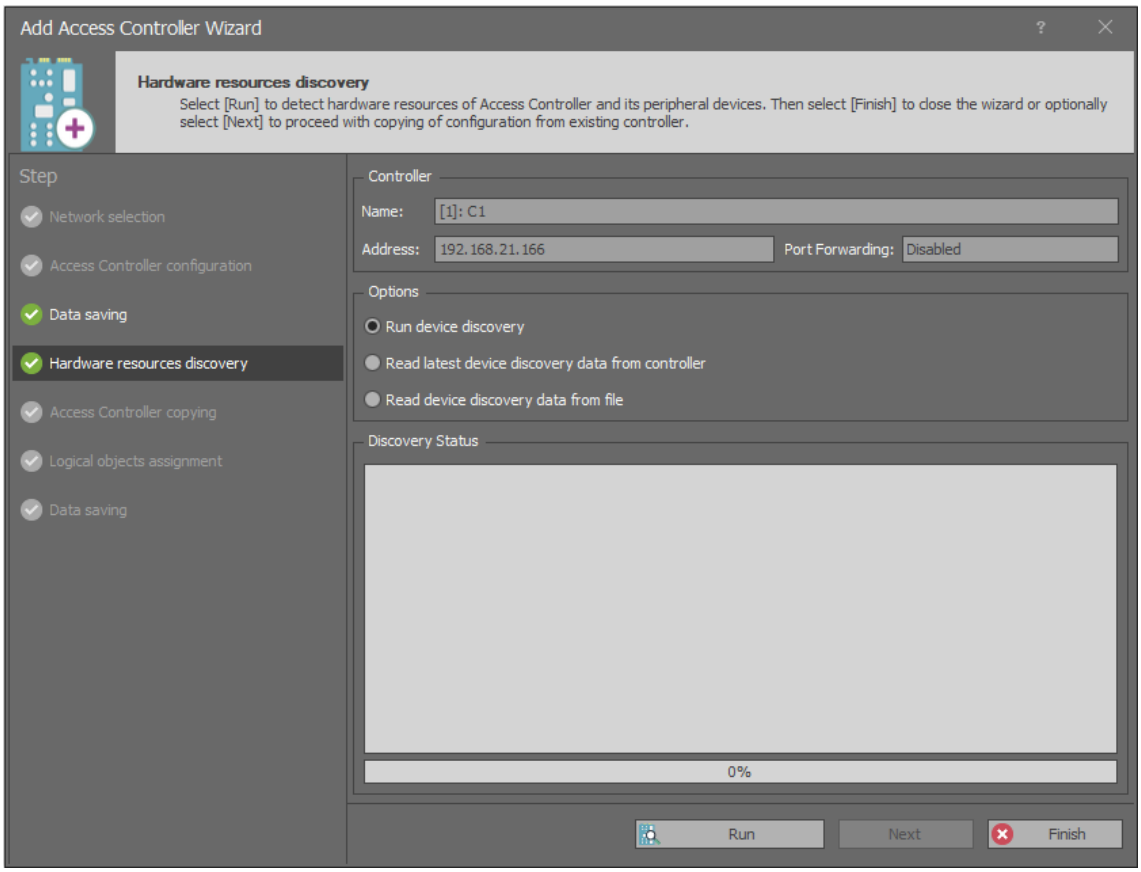
- In the new window enter network name and optionally select time zone and language for the network. Both settings are useful in case of distributed multinational system which is managed by various operators. System can be divided into network for organizational purposes only as it does not affect functionalities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



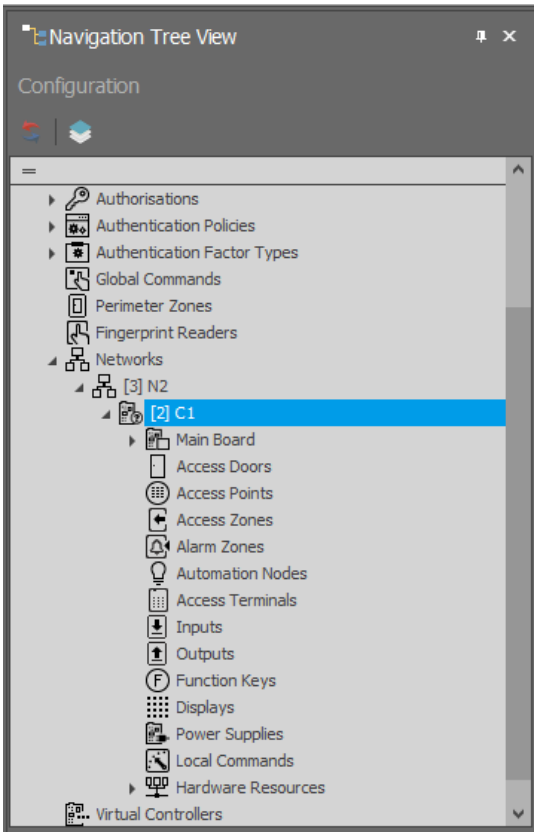
- In the next window enter or detect controller's IP address and enter communication key which was previously configured with RogerVDM software. Port forwarding is obsolete if the connection between computer and controller is in LAN without intermediary router. Click *Next*.



- 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.
- Click *Finish* to close the wizard. The wizard in the next steps enables configuration copying from another existing controller which will not be used in this guide.
- After navigation tree refreshing with button, the newly created network with controller, its objects and resources is displayed.



All the steps covered by wizard can be also executed manually in VISO navigation tree by right clicking *Networks* and then creating network and controller with IP address and communication key and finally detecting hardware resources.

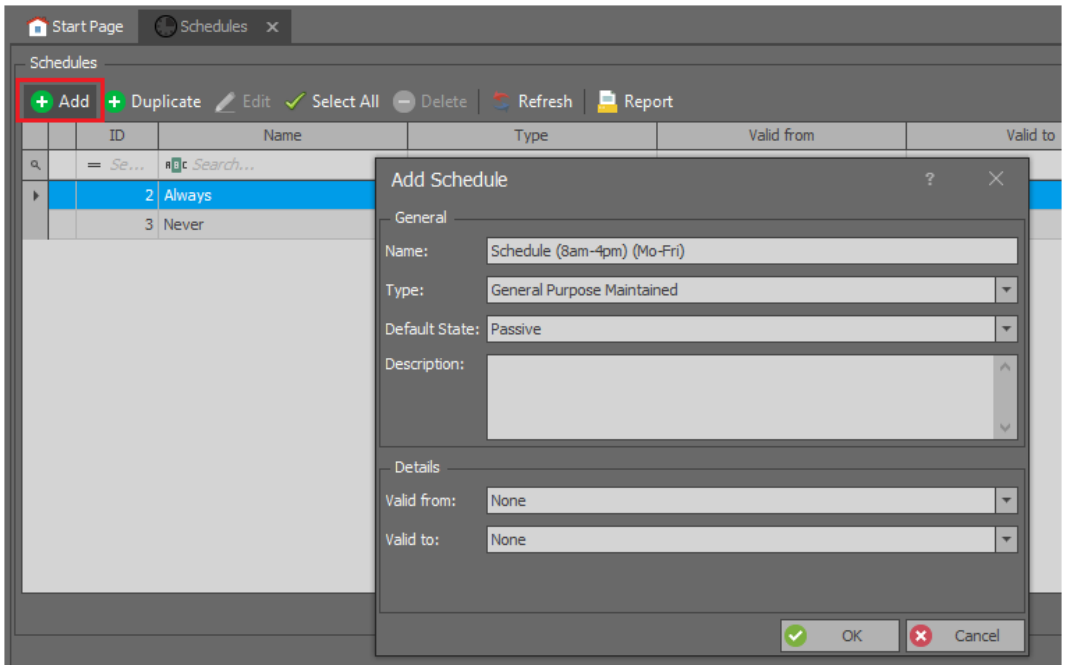
Access doors

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.

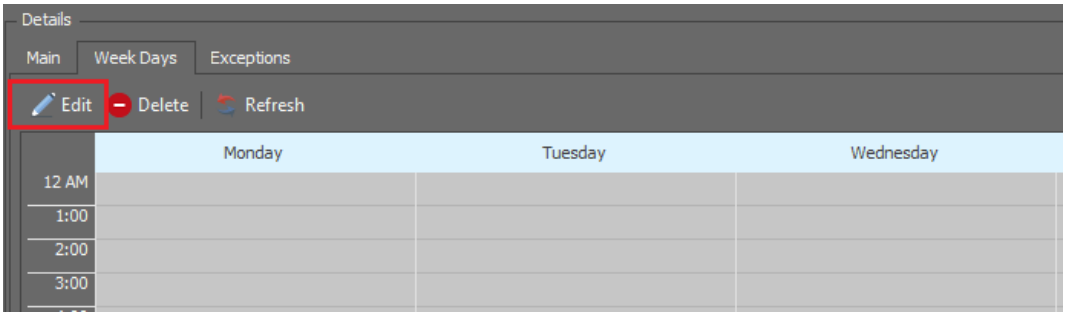
If it is required to limit Authorizations created by wizard in time then General Purpose Maintained Schedule(s) should be defined in advance.

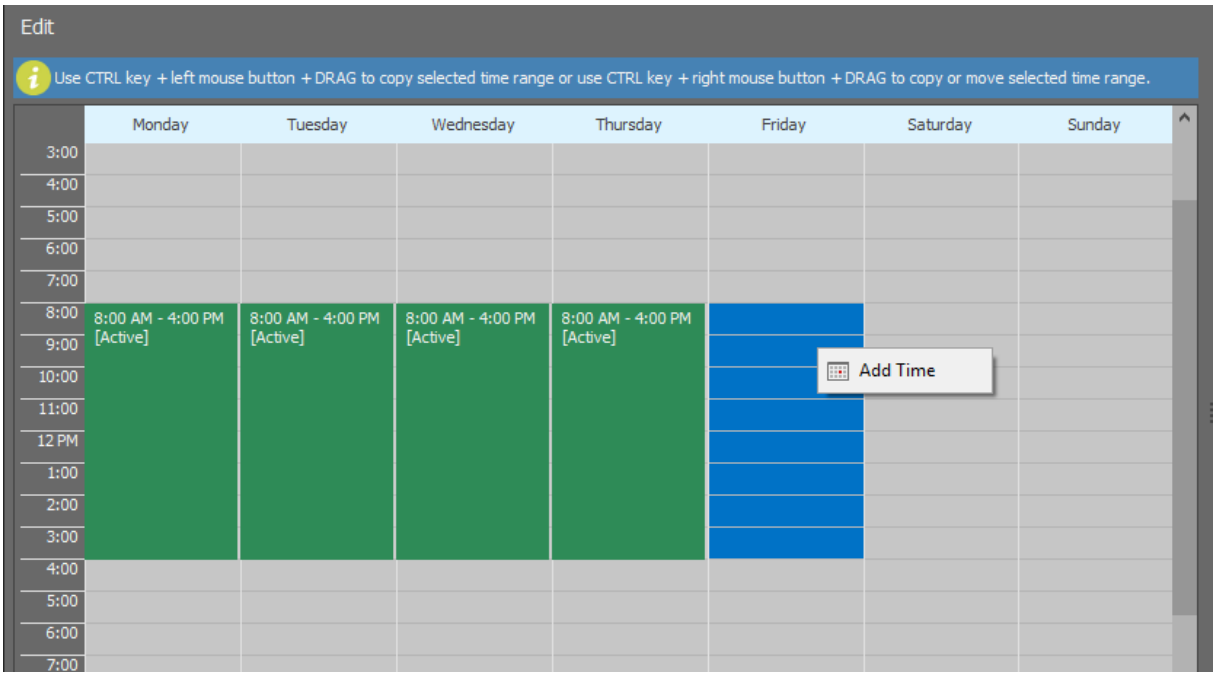
In order to define a Schedule:

- 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*.



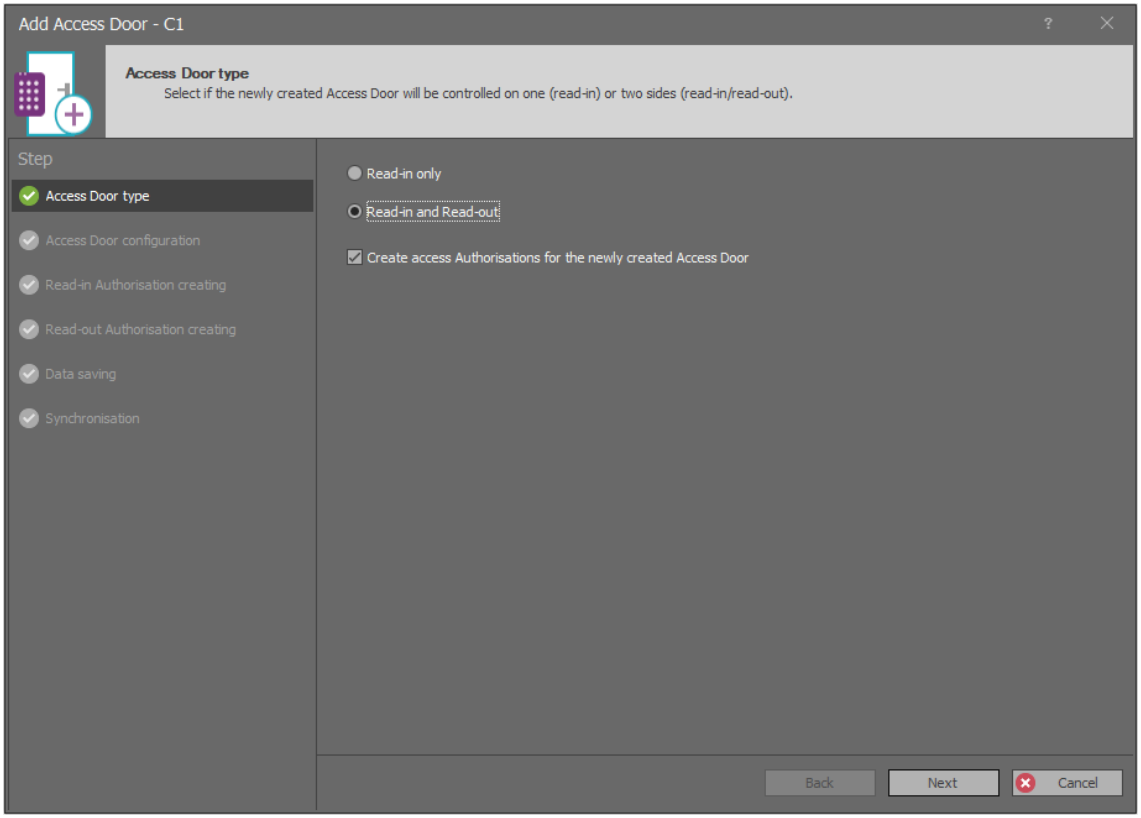


- In the newly opened window select period from 8 AM to 4 PM with left mouse button pressed and then right click to select the command *Add time*.

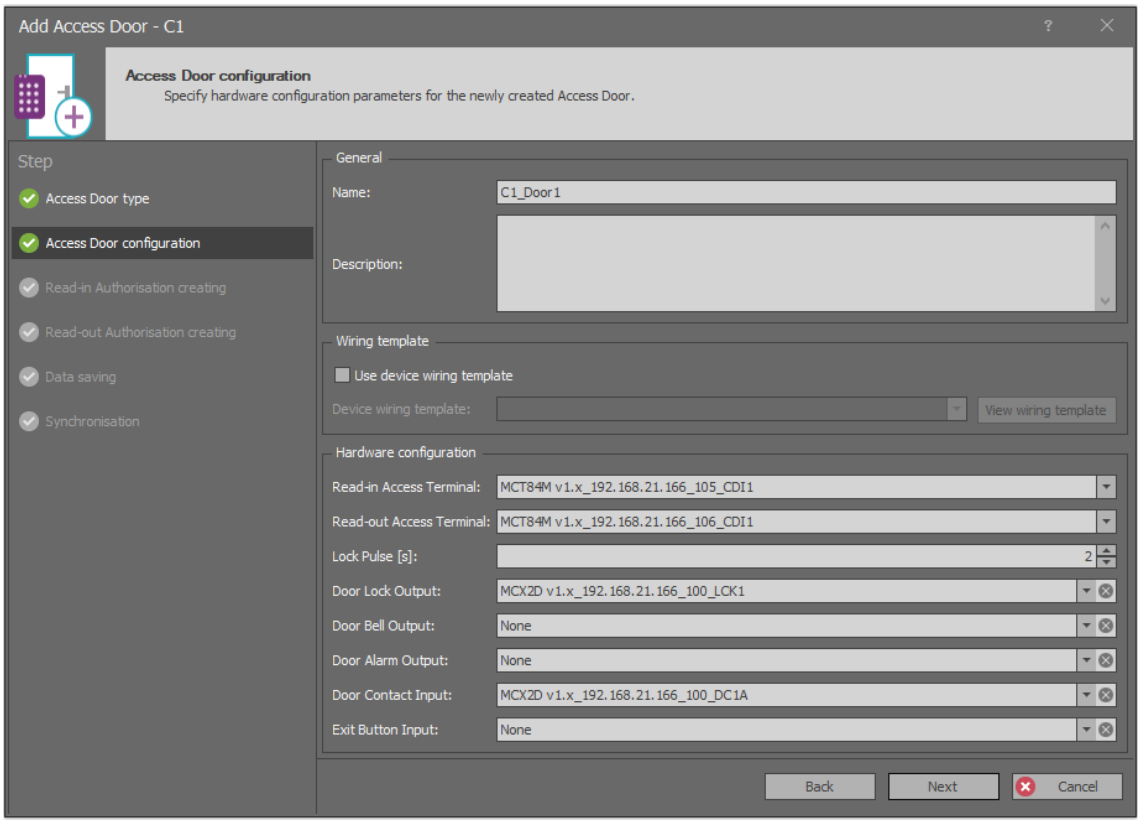
- In the next window confirm or correct the period.
- Define the same periods for remaining days i.e. for Tuesday, Wednesday, Thursday and Friday.

In order to define Access Doors with wizard:

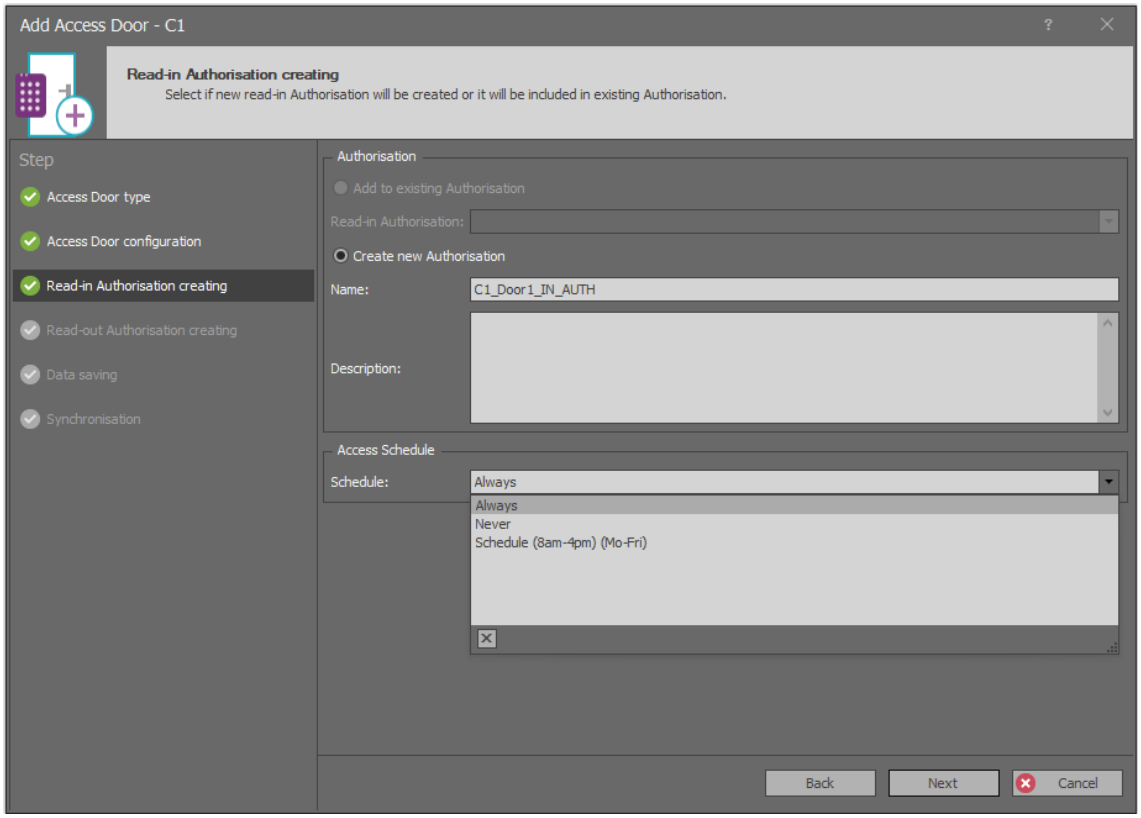
- Select *Wizards* command in the top menu of VISO software and then *Add Access Door Wizard*.
- In the newly opened window select type of a door and then click *Next*. According to installation diagram, Door 1 is read-in/out door with MCT84M readers on both sides.



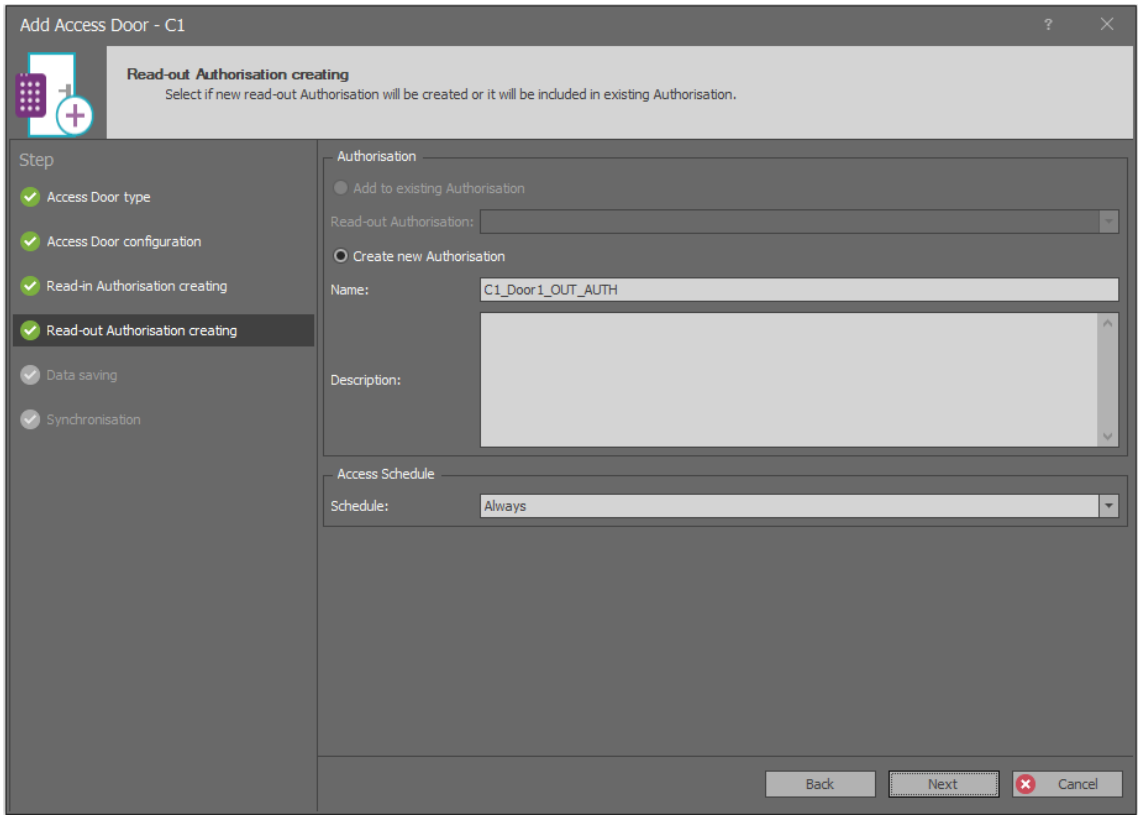
- In the next window select readers, input and output lines in accordance with the diagram and then select *Next*. Alternatively and optionally select *Use device wiring template* to automatically assign terminals, input and outputs in typical way.



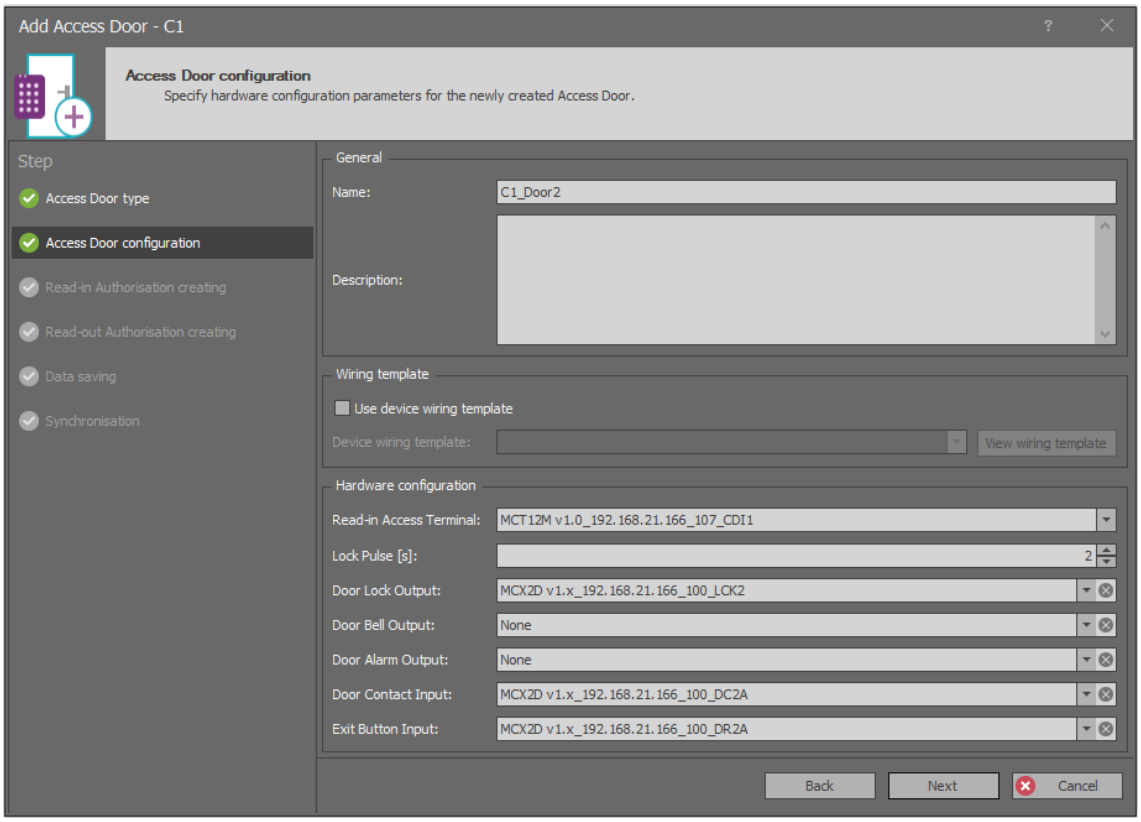
- In the next window a read-in Authorization is created. It enables access granting at read-in terminal MCT84M (ID=105). The Authorization can be later assigned to users. If it is required to limit the Authorization in time then previously created *Schedule (8am-4pm) (Mo-Fri)* can be selected. Click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



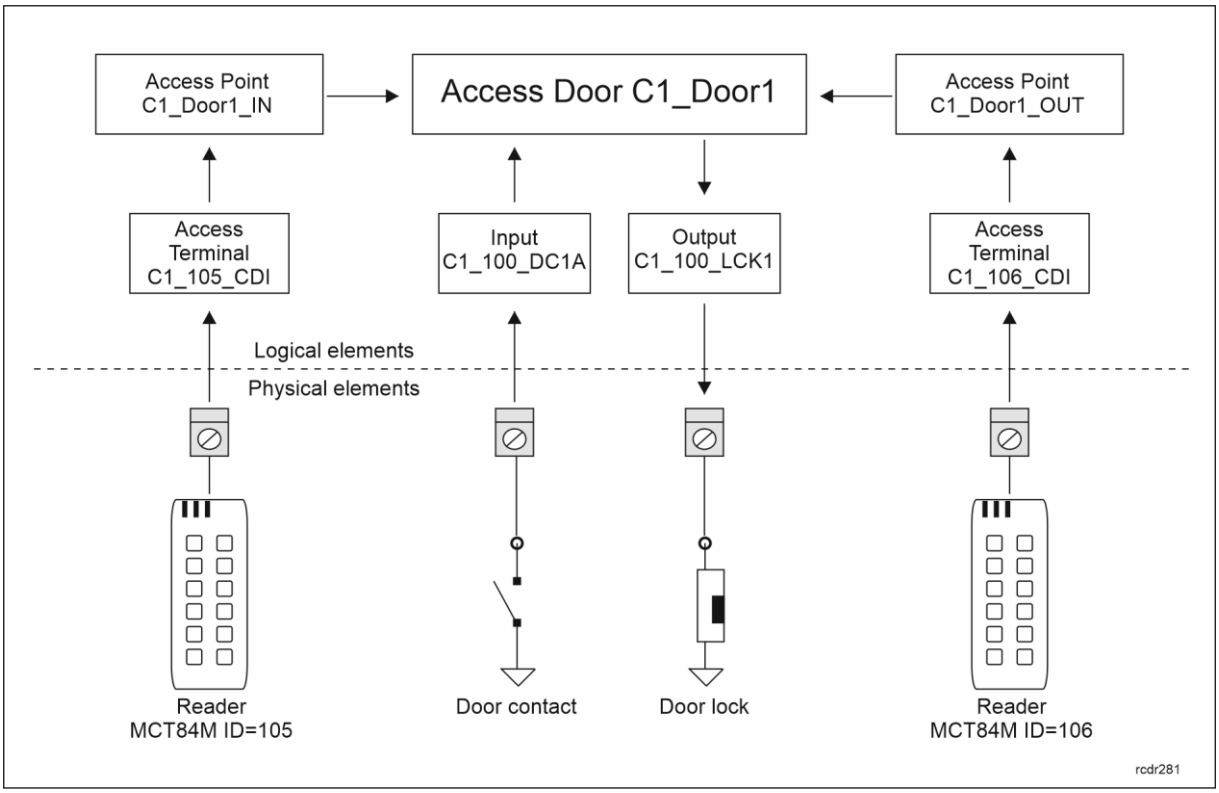
- In the next window similarly a read-out Authorization is created for read-out terminal MCT84M (ID=106). Click *Next*.

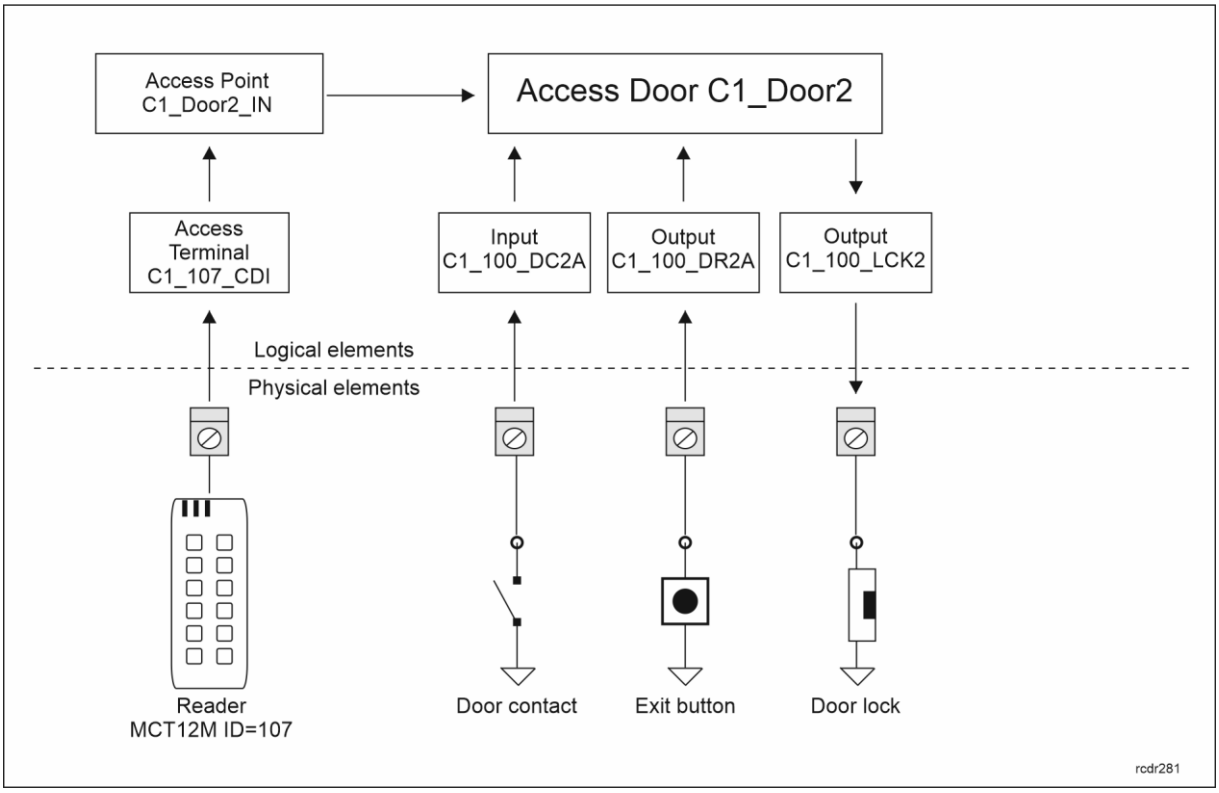


- In the next window select *Next* in order to save settings into VISO database and to create logic objects resulting from settings entered with the wizard.
- In the last window select *Start* button to synchronize settings with controller.
- Define Door 2 in similar way using the wizard and keeping in mind that according to the diagram this is read-in door with single reader and consequently 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.



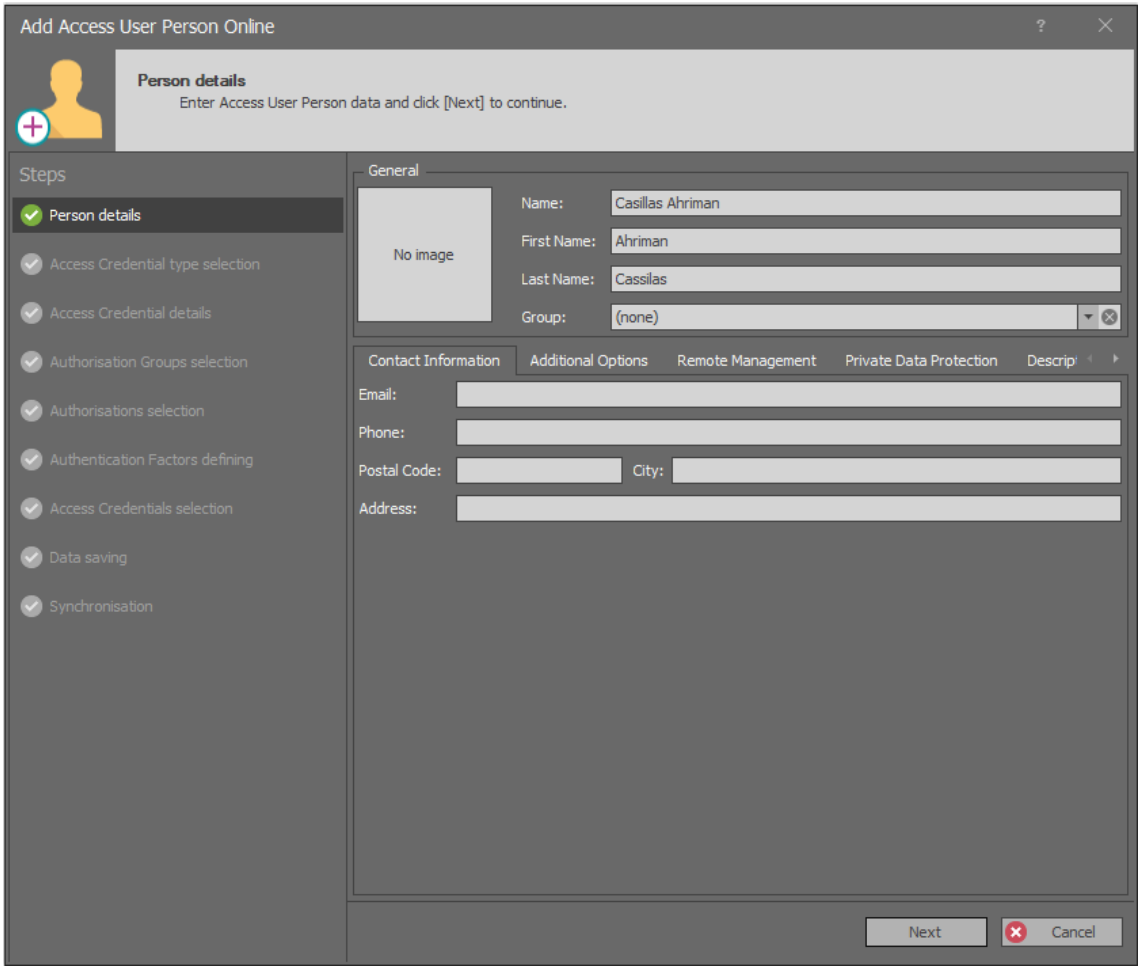


Users

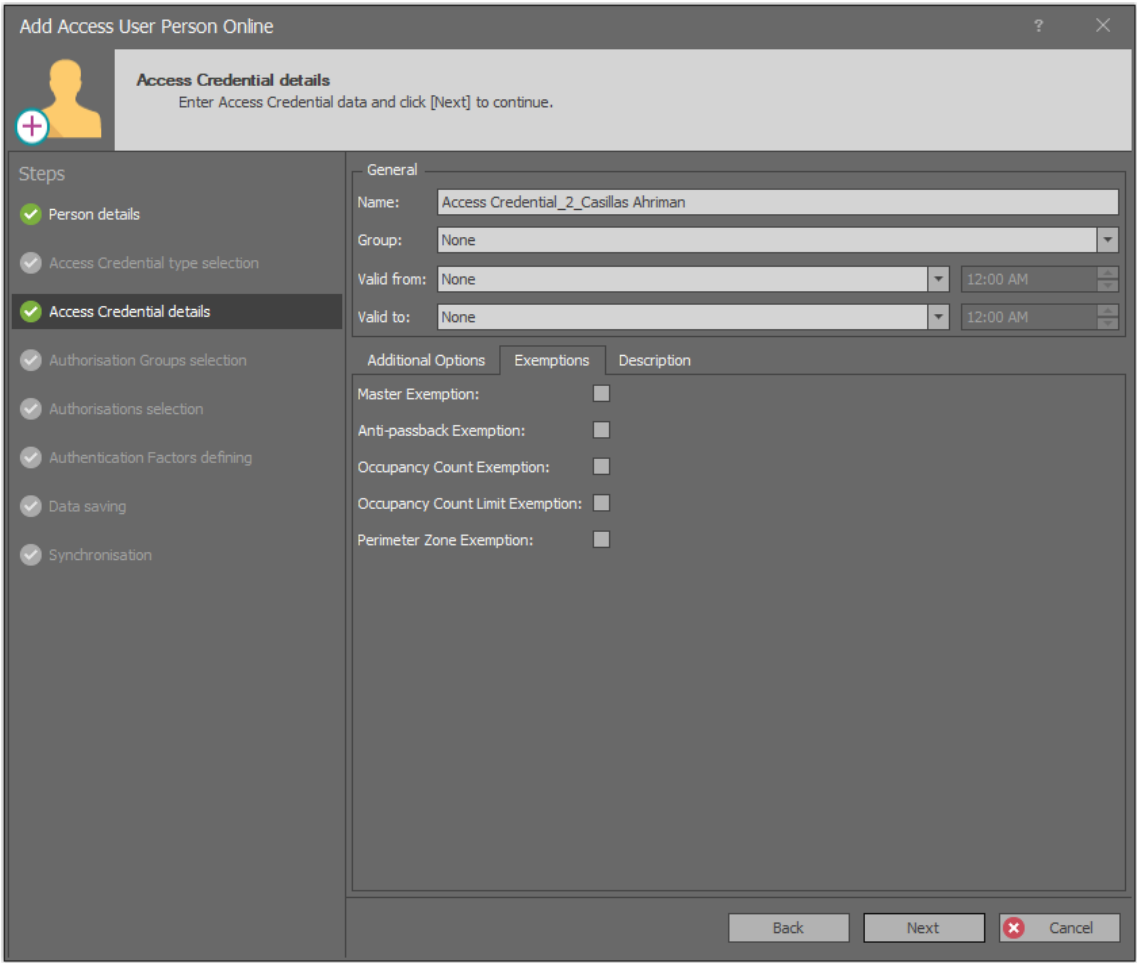
User defining, editing and deleting can be done with wizards in VISO software.

In order to define a user with wizard:

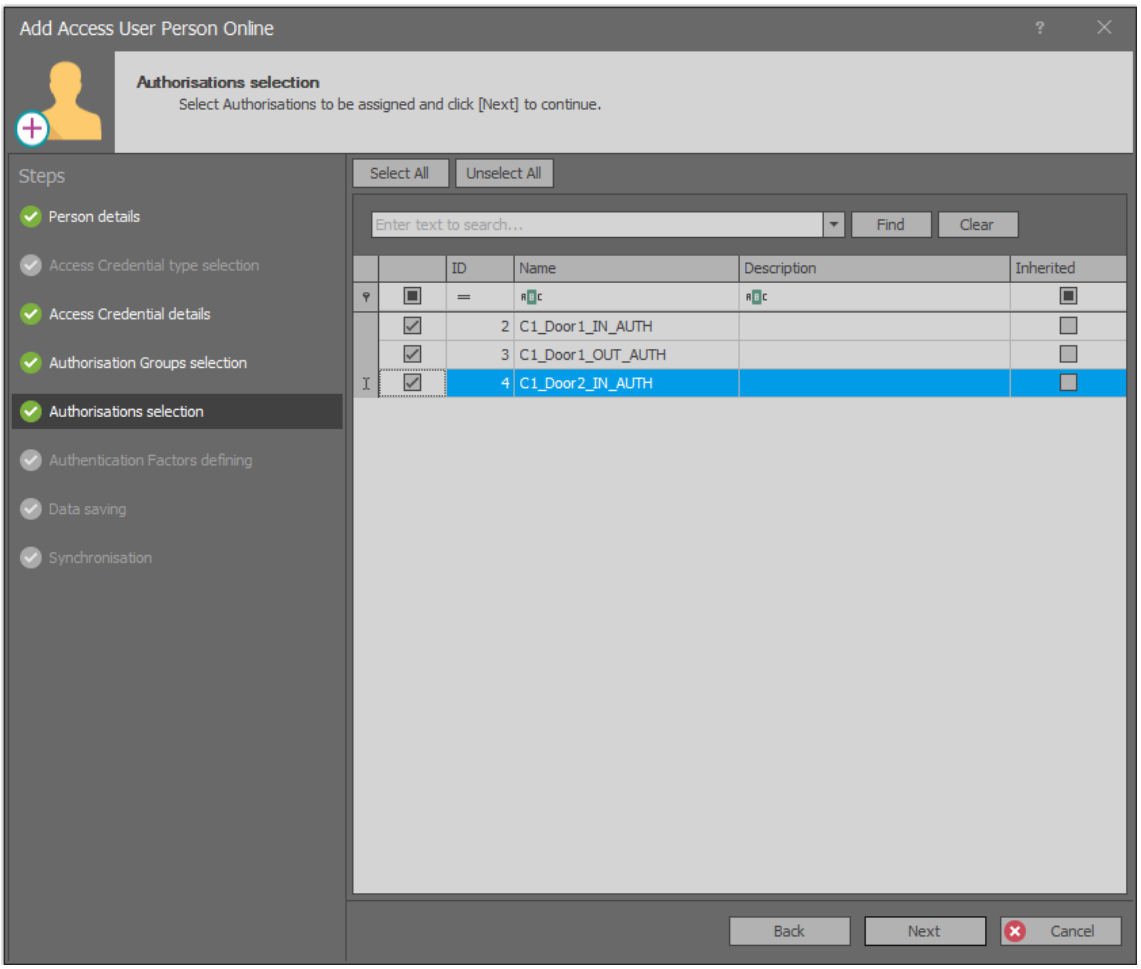
- Select *Wizards* command in the top menu of VISO software and then *Add Person Online*.
- In the newly opened window enter user names and click *Next*. Optionally photo can be assigned by right clicking *No image* area and selecting respective command.



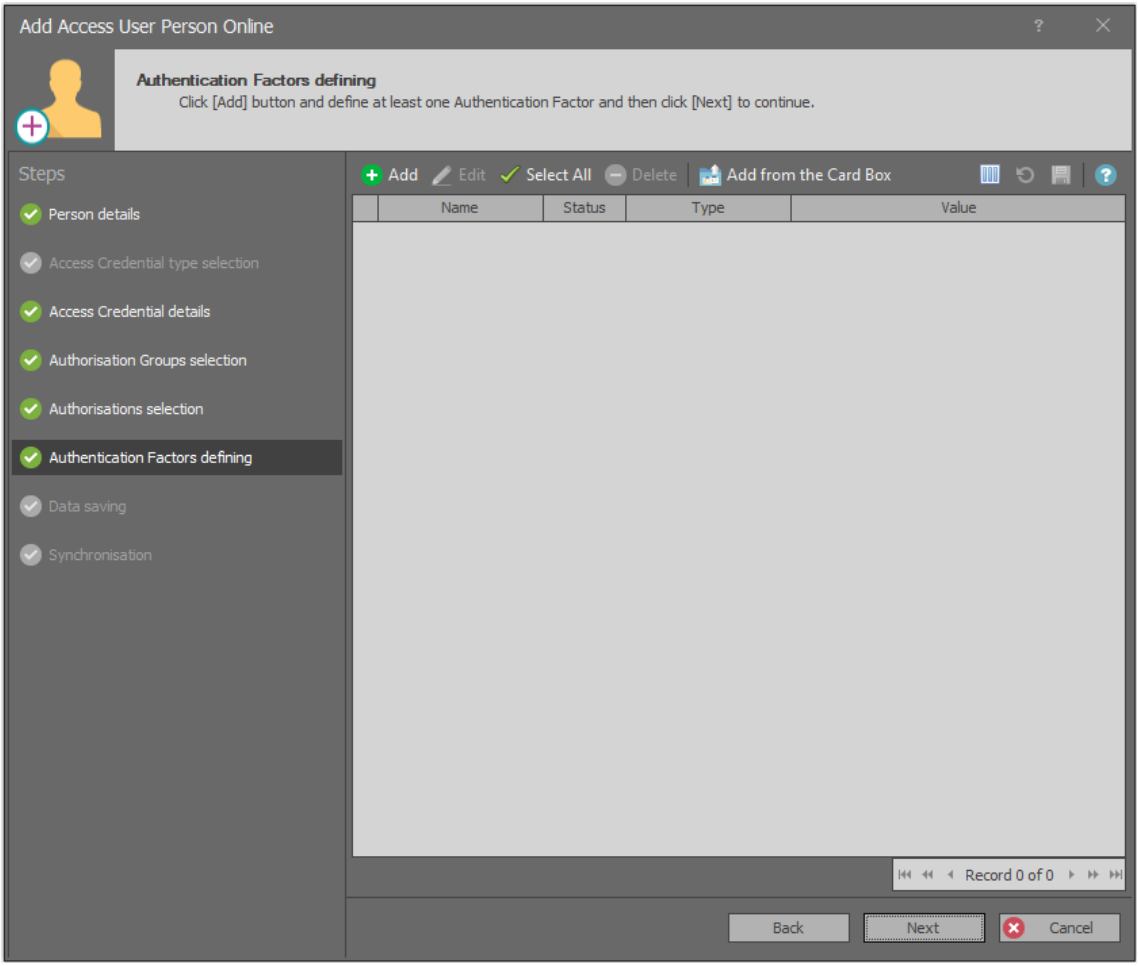
- In the next window select *Create new Access Credential* and then *Next*.



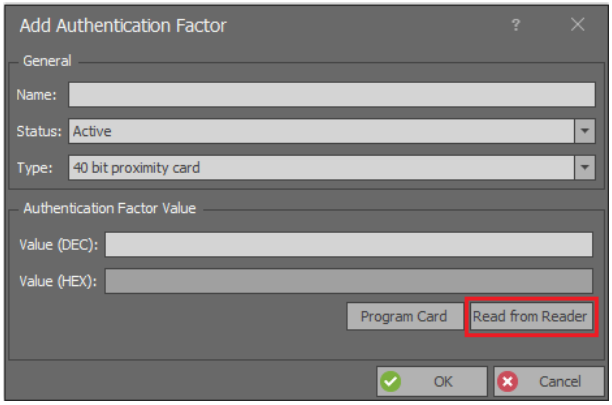
- In the next window it is possible to define credential validity period. Optionally, in the *Exemptions* tab various privileges can be assigned to the credential. If *Master Exemption* is selected then the user will gain all possible Authorizations in the system in regard of access, arming/disarming 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*.



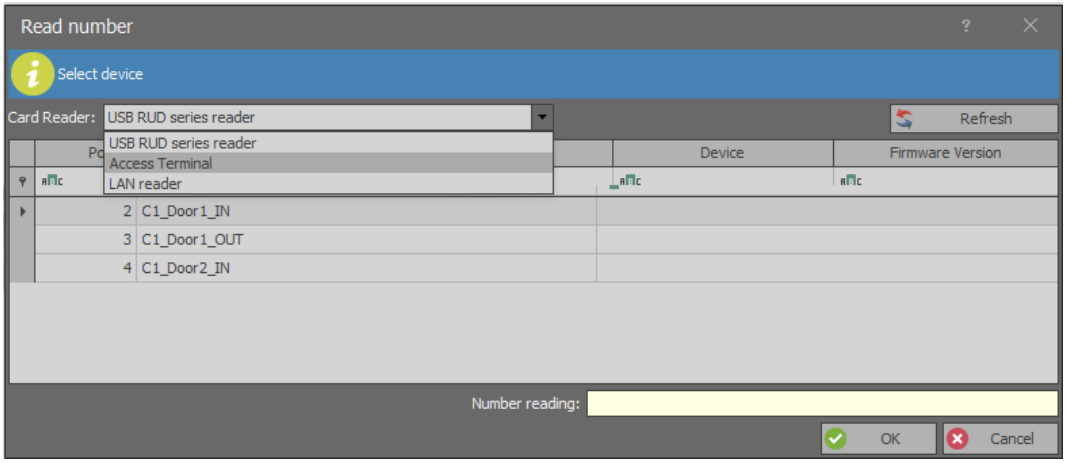
- In the next step start configuration of Authorization Factors selecting *Add* button.



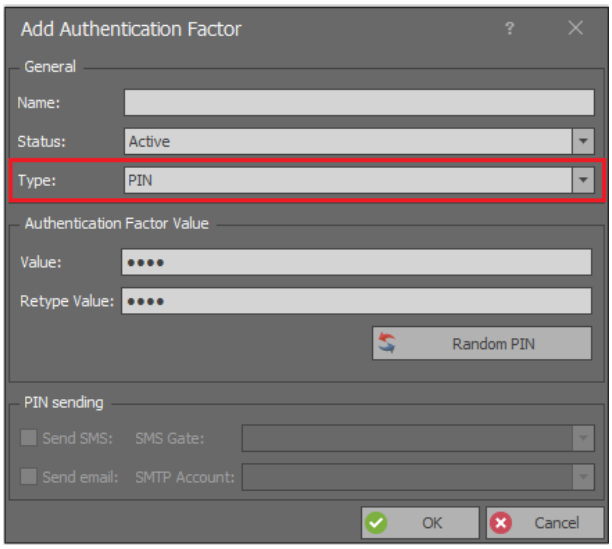
- Select the button *Read from Reader*. Alternatively the card number can be entered manually in the *Value(DEC)* field if card number is known.



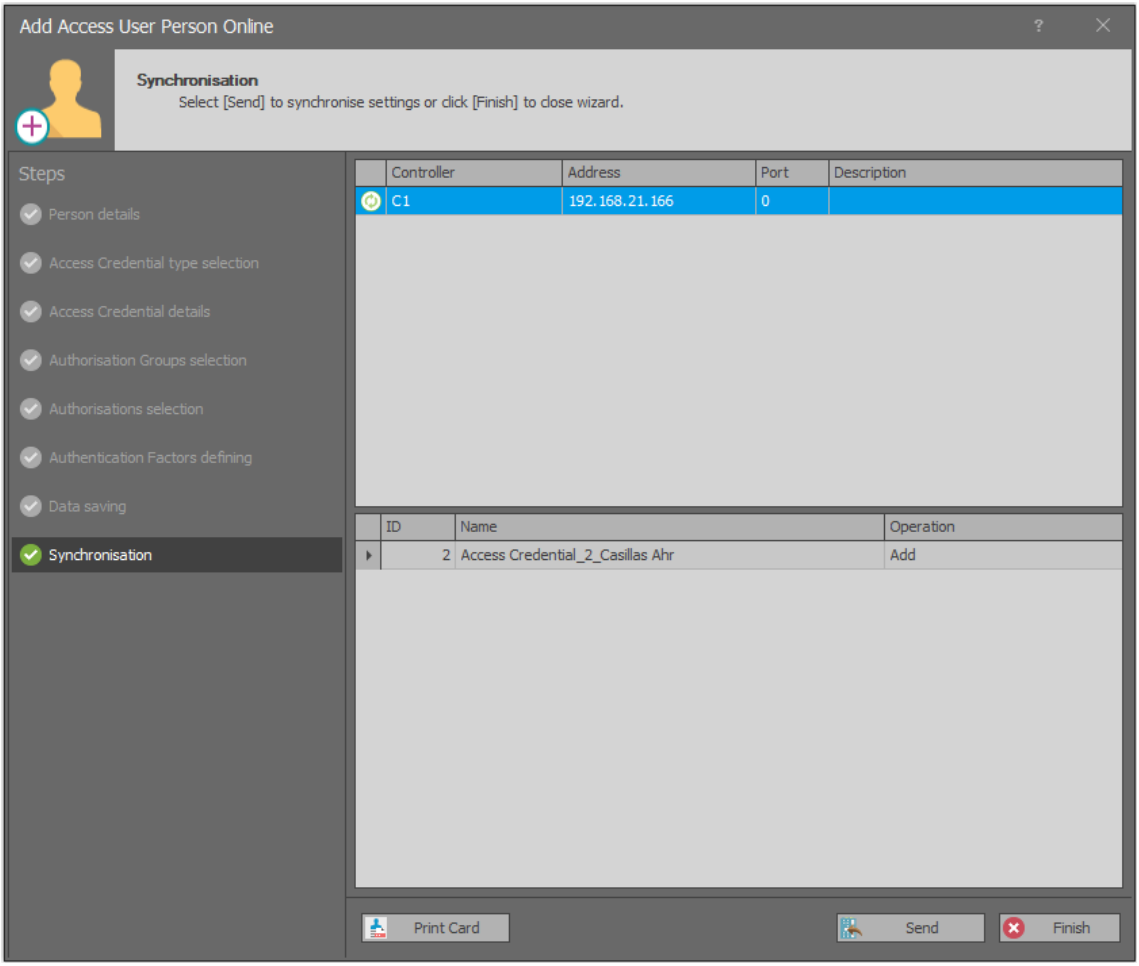
- In the newly opened window select card reader type. The list of devices for the option *USB RUD series reader* is empty if no RUD type (e.g. RUD-3) administrator reader is connected to computer. Access Terminals are MCT readers connected to the controller. Select *C1_Door1_IN* reader and then read 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*.



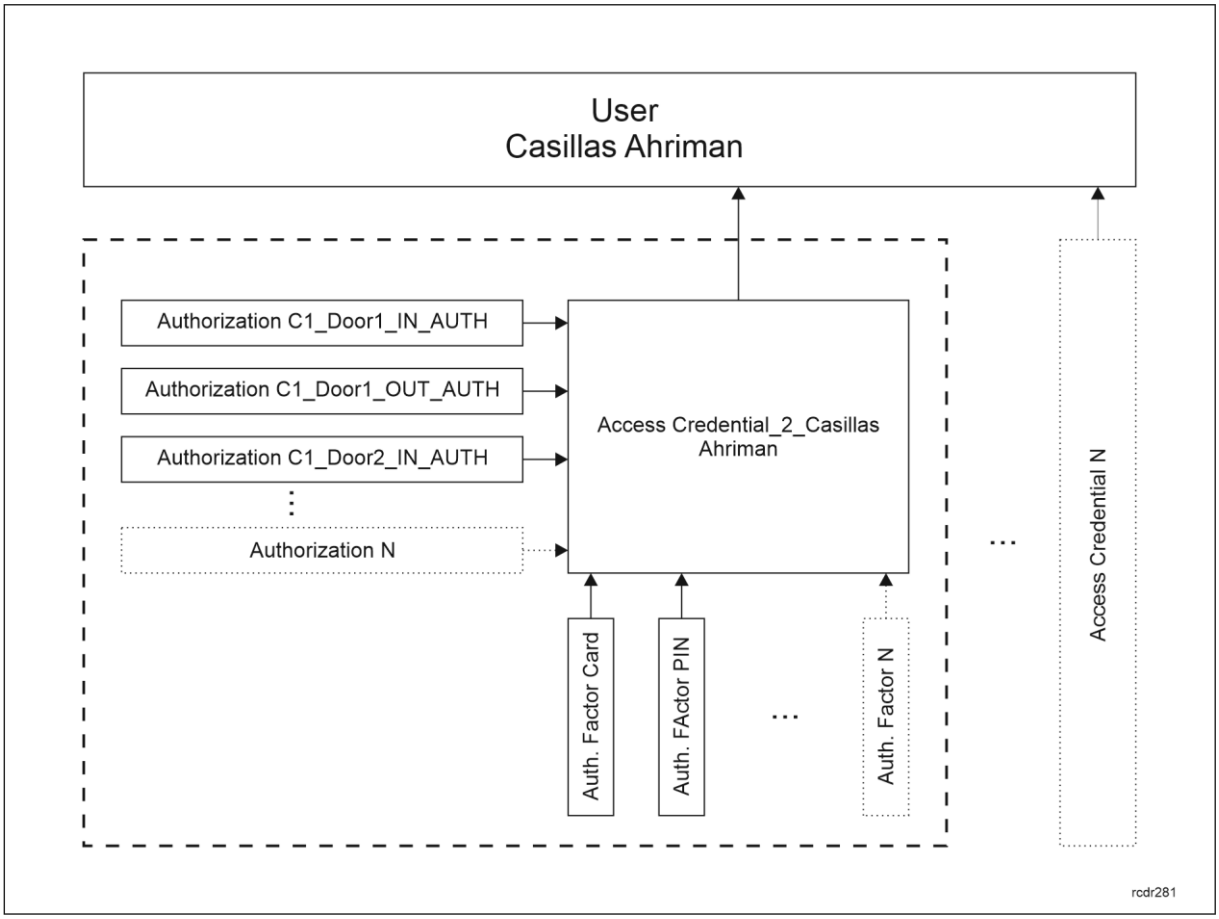
- Enter PIN (e.g. 1234) in the field *Value* and again in the field *Retype Value*. Click *OK* to confirm PIN and return to Authentication Factors window.
- In the next window select *Next* in order to save settings into VISO database and to create logic objects resulting from the wizard.
- In the last window select *Send* button to synchronize settings with controller using special method which does not interrupt controller operation at all. 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. By default, PIN must be concluded with # key on reader's keypad.

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.

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



Technical diagnostics

Hardware

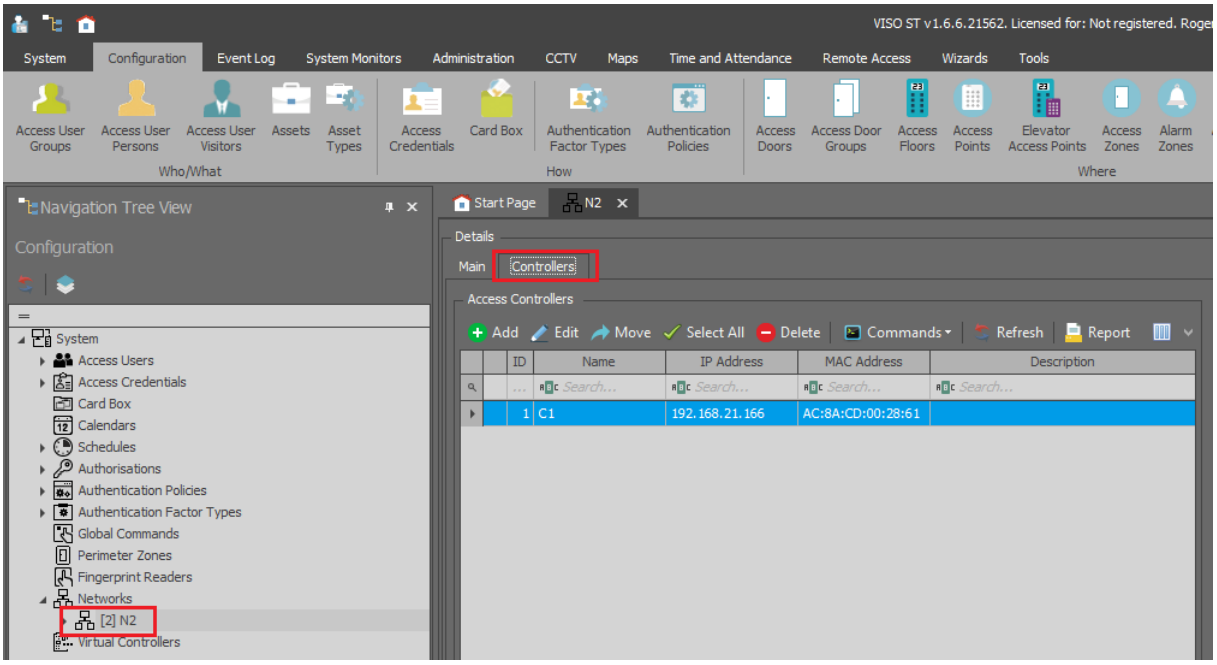
In the system with detected access controllers and peripheral devices (MCT, MCX) it is possible to:

- Verify connection with devices
- Check status of input lines
- Trigger output lines

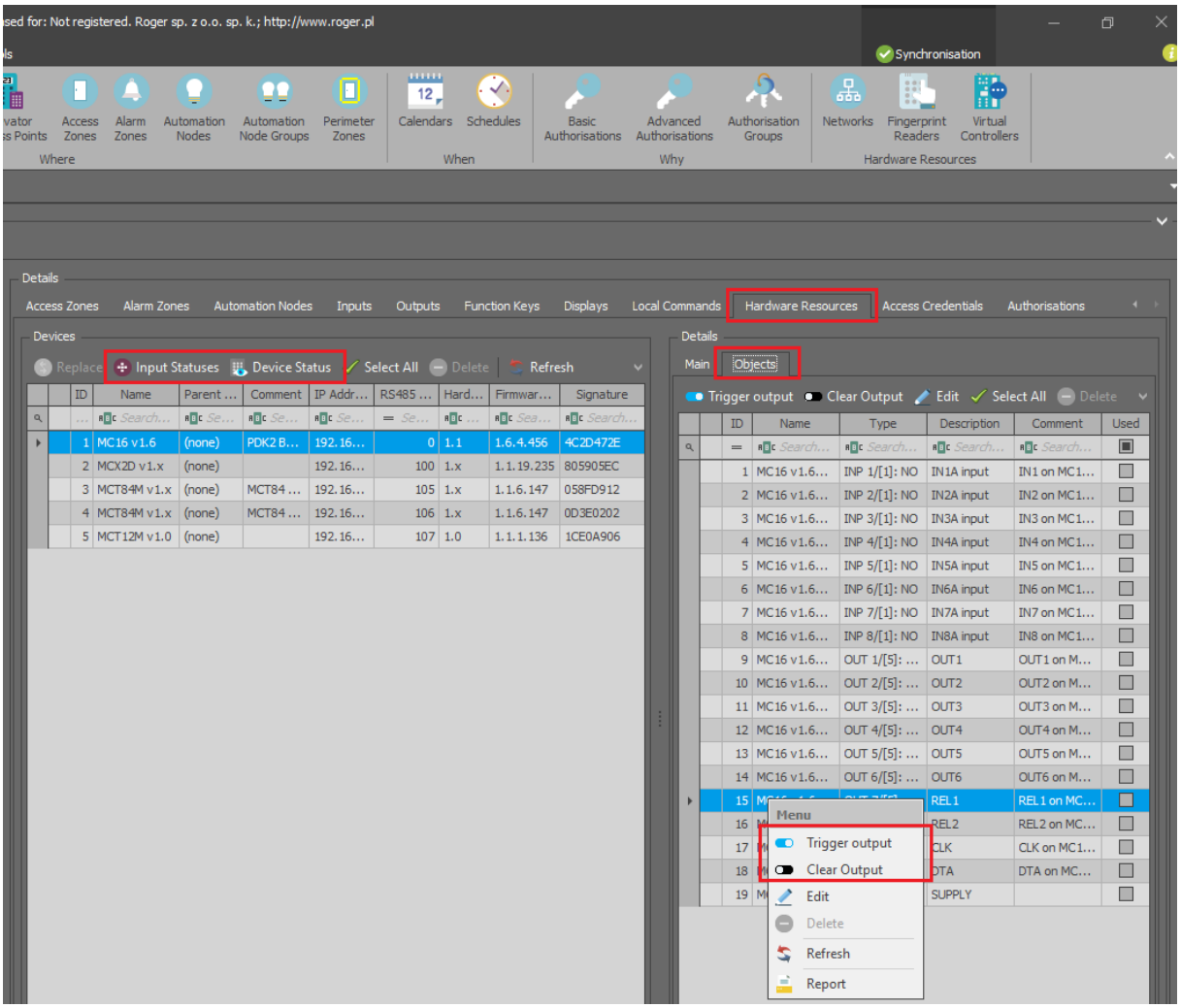
These tools are used for diagnosis of the system during installation and verification of cable connections. They can also be used for troubleshooting in case of system failure.

In order to access diagnostic tools:

- In the navigation tree of VISO software expand *Networks* command and double click one of Networks.
- 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.

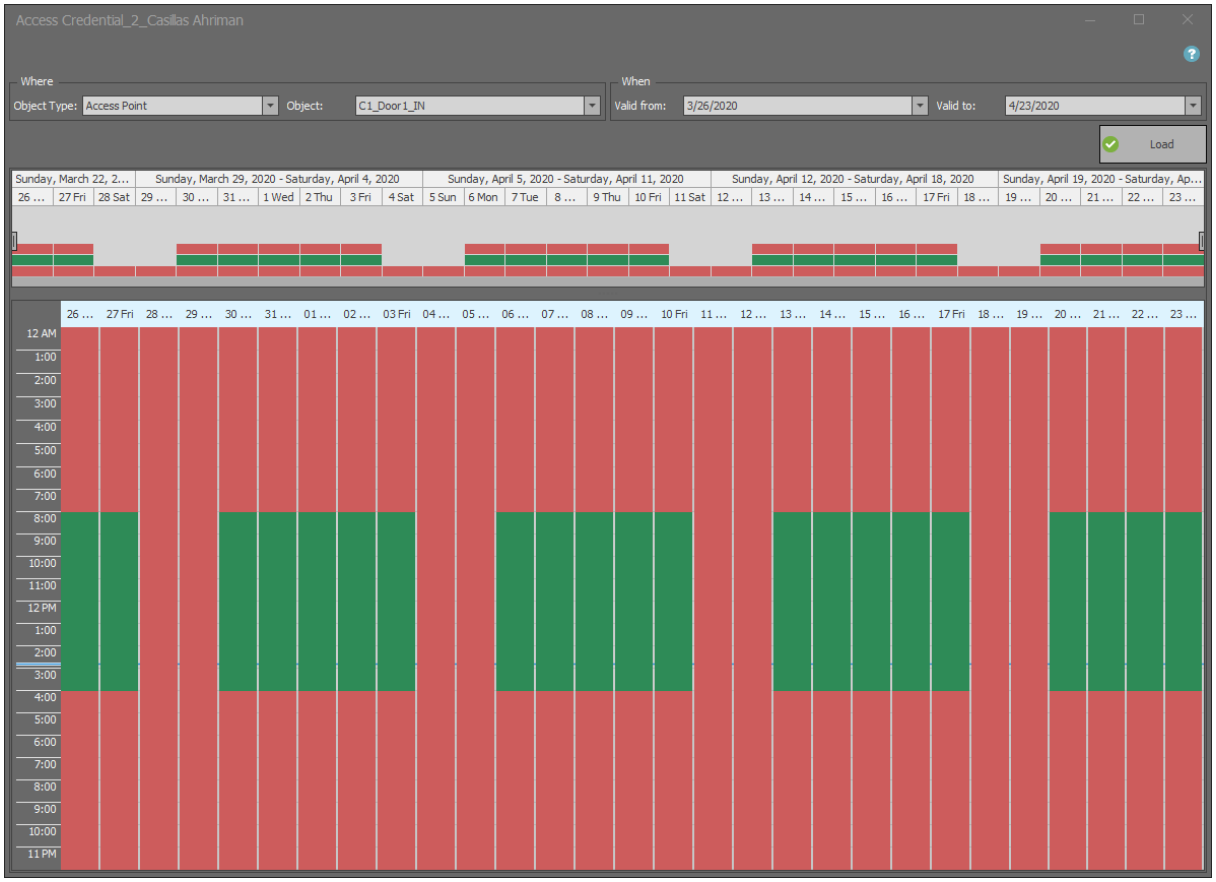
User Authorisations

User Authorisations can be defined and assigned on various levels. Therefore, sometimes it may not be obvious what are the resultant Authorisations of particular user as they may result from:

- Assignment of user to Access User Group which has Authorisations.
- Assignment of individual Authorisations to user's Access Credential.
- Assignment of Authorisation Groups to user's Access Credential.
- Assignment of individual Authorisation to user.

In order to obtain information on resultant Access Authorisations:

- In the top menu of VISO software select *Configuration* and then *Access Credentials*.
- In the opened window for Access Credential of particular user and then select *Access Preview*.
- In the next window select Access Point and then click *Load* to view the data.



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