Roger Access Control System 5v2

Application note no. 025

Document version: Rev. A

Authorisation Modes

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

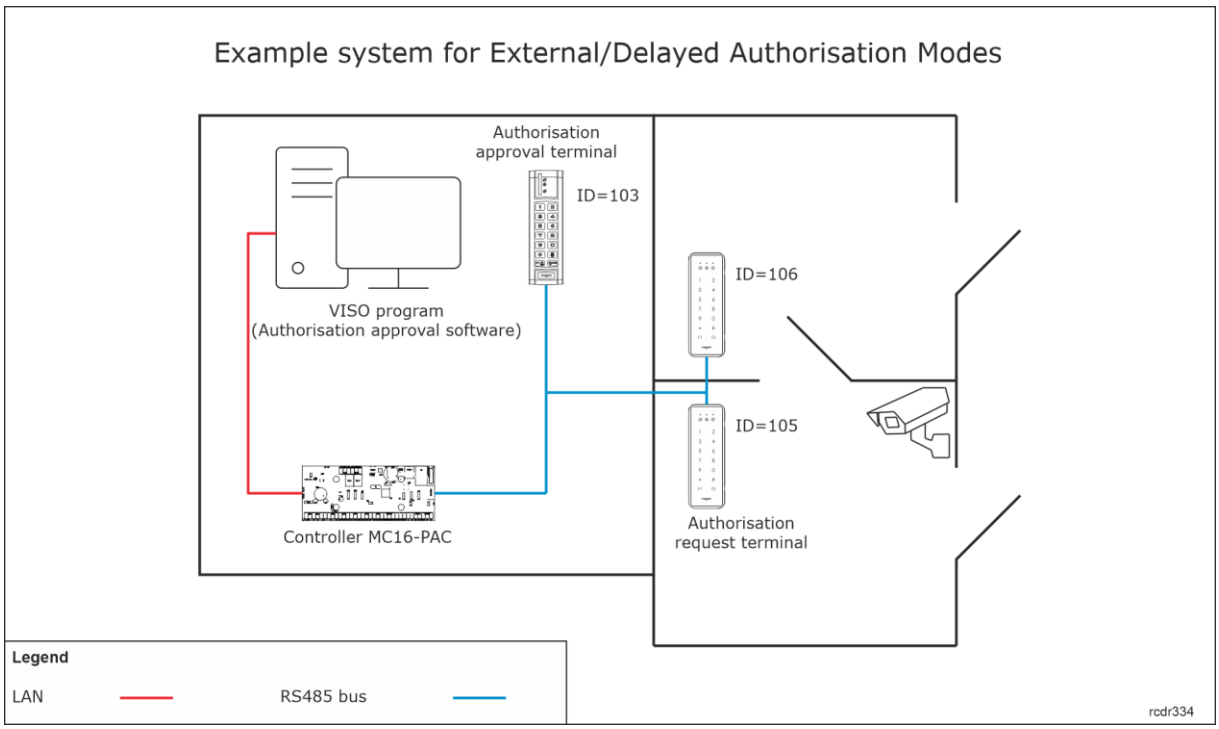
Introduction

Authorisation Modes can be configured and applied on the level of Access Points (readers) in RACS 5 system. The mode defines how the access request from user is processed in the system.

Available Authorisation Modes:

- Normal Authorisation – access is granted after verification of user Authorisation (access right).
- Positive Authorisation – access granting does not require user Authorisation (access right) so any user defined in the system can be granted access.
- Negative Authorisation – access is denied regardless of user Authorisation (access right) excluding Access Credentials with Master exemption.
- External Authorisation – access requires user Authorisation (access right) and additionally it must be approved with input function *[185]* or on the level of VISO software.
- Delayed Authorisation – access resulting from user Authorisation (access right) is delayed and then it can be denied with input function *[186]* or on the level of VISO software.
- Disabled Authorisation – access is denied regardless of user Authorisation (access right) including Access Credentials with Master exemption.

This note is focused on External Authorisation and Delayed Authorisation. Both modes can be applied in military facilities, prisons, detentions, closed hospitals and other objects where some doors in access control system require additional supervision by guard. In such scenario, a guard can approve or deny access requests using terminal, computer with VISO software or even by means of third party software if it is integrated with RACS 5 system based on Integration Server from RogerSVC program.

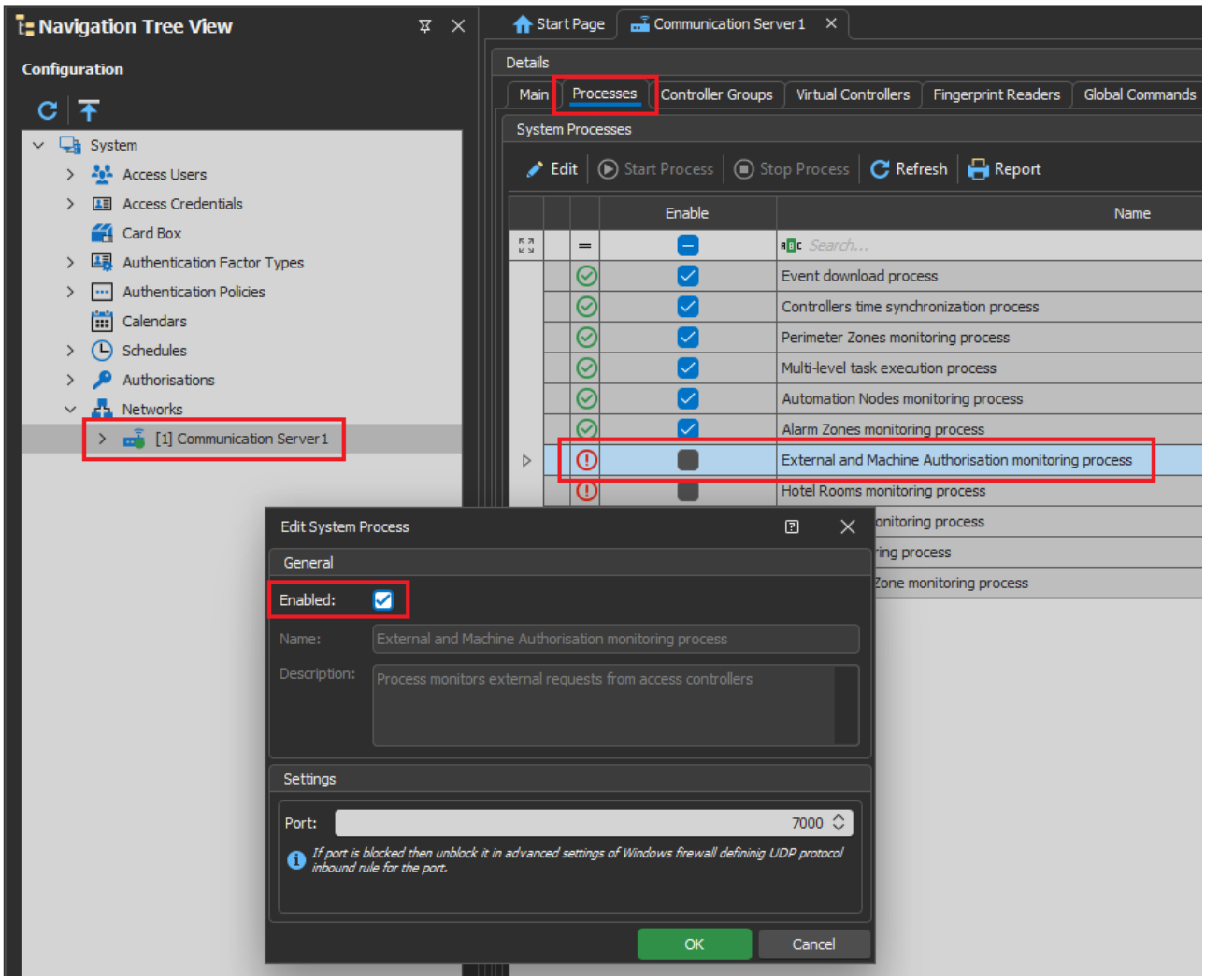


Notes:

- Power supply in the example can be provided by installation of MC16-PAC-2-KIT.
- The total number of MCT/MCX devices on RS485 bus of particular access controller cannot exceed 16 available addresses in ID=100-115 range. The RS485 addresses of readers in the drawing are exemplary.
- Maximal distance for RS485 bus equals to 1200m and all devices on the bus should have common GND.

Preliminary configuration

- Configure RACS 5 system according to AN006 application note in regard of low level configuration, database and servers.
- If remote access approving/denying from VISO software which will be further explained is going to be used then double click particular Communication Server in VISO software and then select *Processes* tab.
- In the opened window right click *External and Machine Authorisation monitoring process* and then *Edit*.
- Enable the process and optionally define communication port (7000 by default).



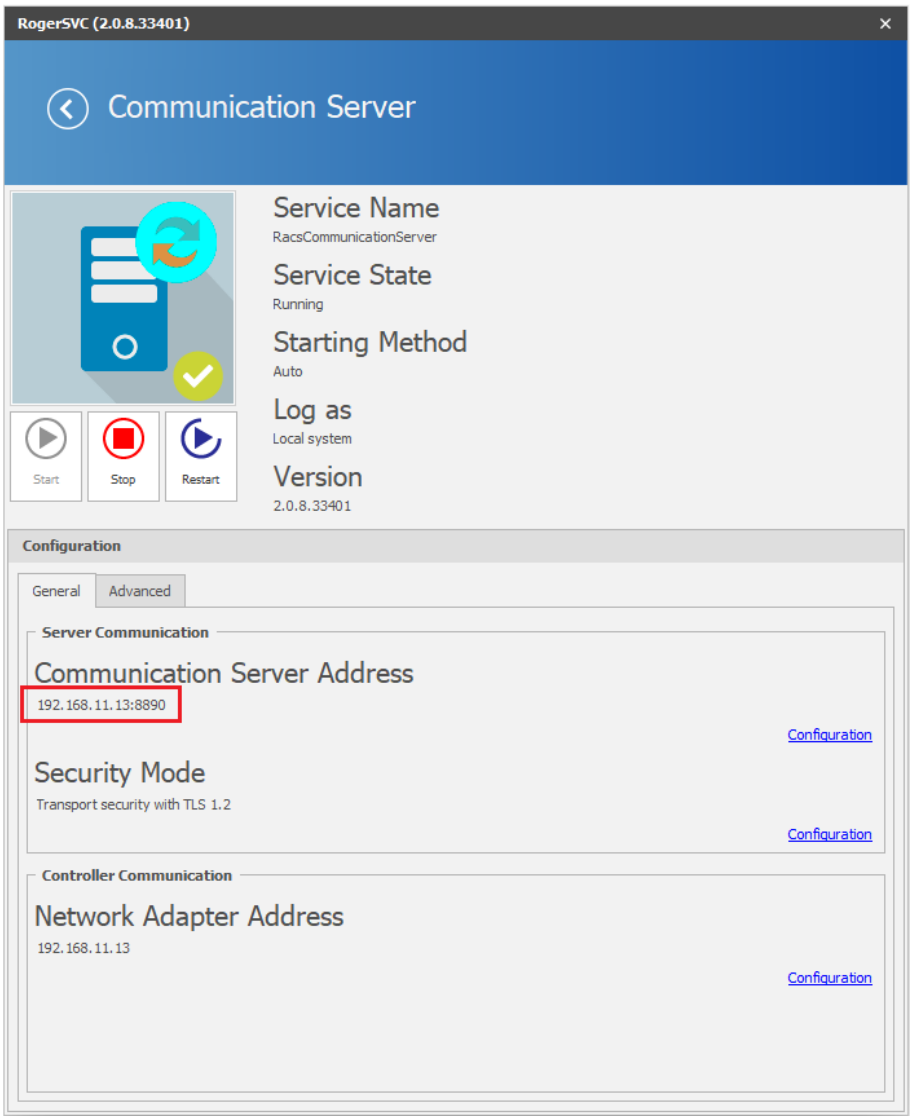
Additional low level configuration

In case of authorisation approving/denying from VISO software, MC16 controller requires not only typical low level configuration with RogerVDM or VISO v2 software but also additional configuration on its memory card.

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

STP=7001
VRI=192.168.11.13
VRP=7000

where:
STP – any unoccupied UDP port for communication with controller.
VRI – IP address of computer with Communication Server from RogerSVC software.
VRP – UDP port which is configured when previously mentioned *External and Machine Authorisation monitoring process* is configured in VISO software.



Note: DEBUG.CFG file must include empty line in the end. Press Enter key at the end of VRP line and then save the file on memory card.

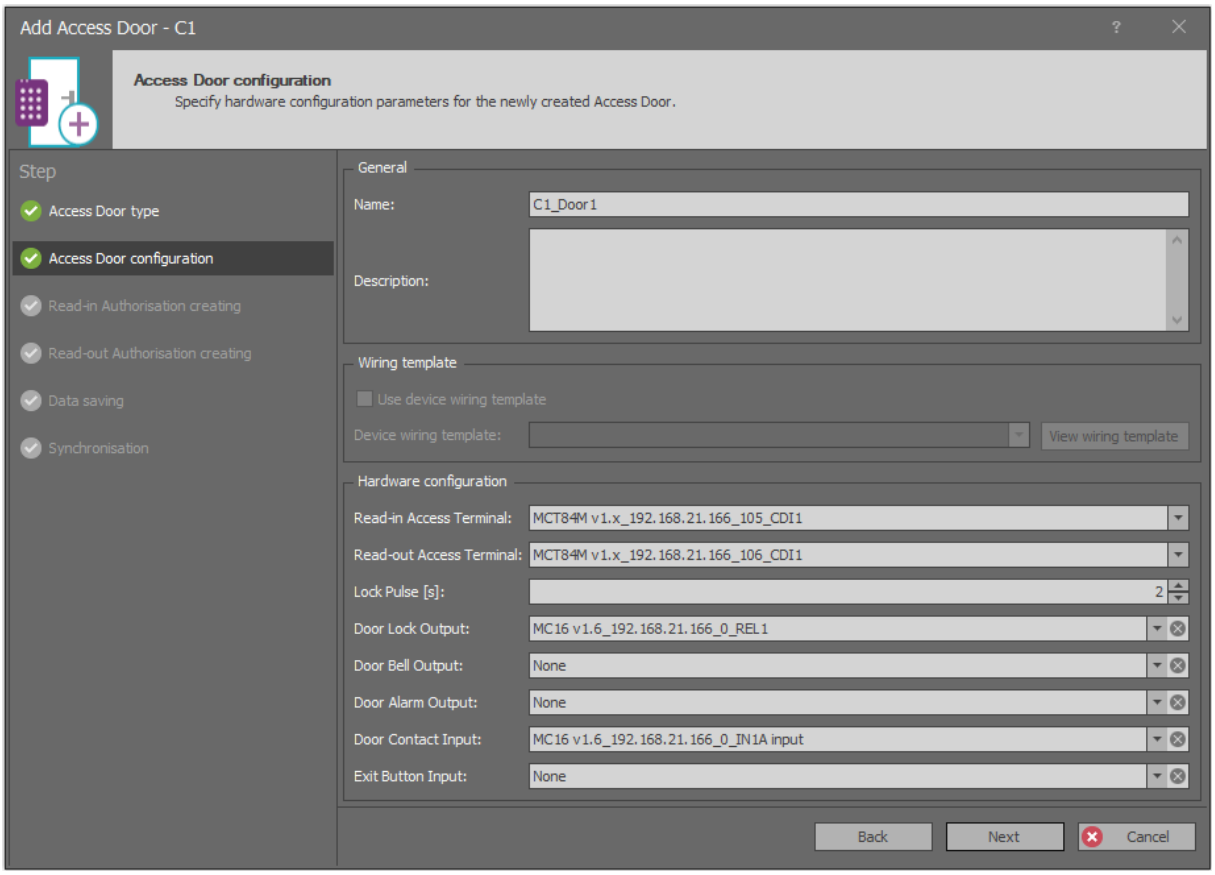
Note: It might be necessary to unblock STP and VRP communication ports in Windows firewall of the computer with Communication Server.

- Insert the card into controller socket.
- Switch on the power supply of MC16 controller.

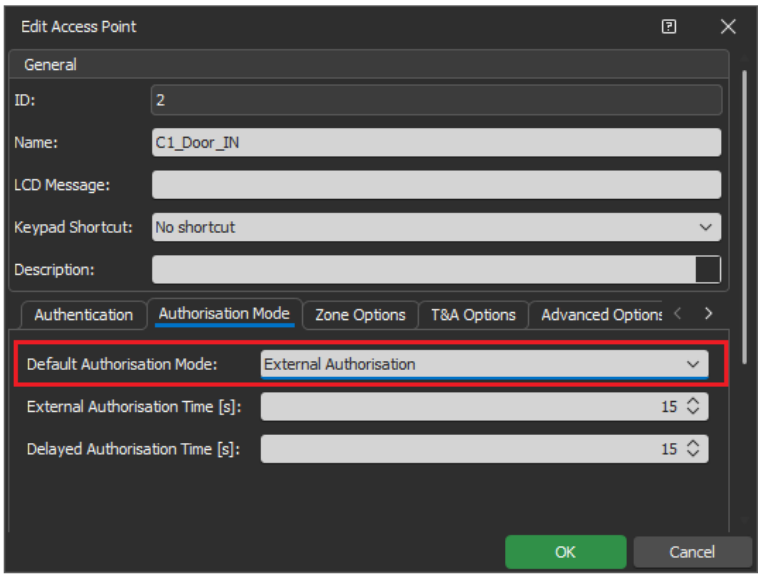
Access Door and Access Points

In order to configure Access Door according to previous example figure:

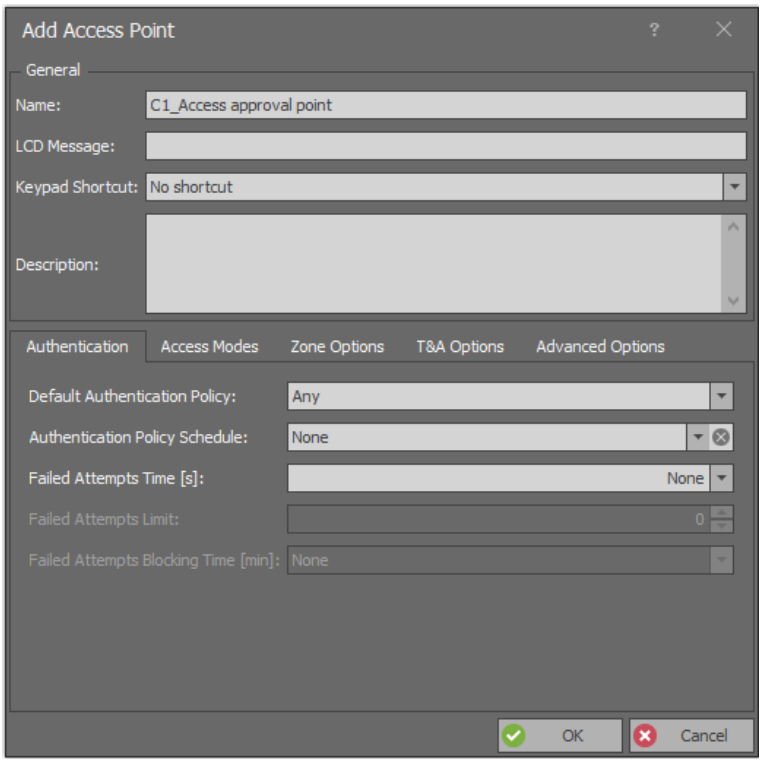
- In the top menu of VISO software select *Wizards* and then *Add Access Door*.
- Define *Read-in and Read-out* type Access Door with ID=105 and ID=106 readers.
- Add user selecting *Add Person Online.* Assign previously created Authorisations and define Authentication Factor (card, PIN).



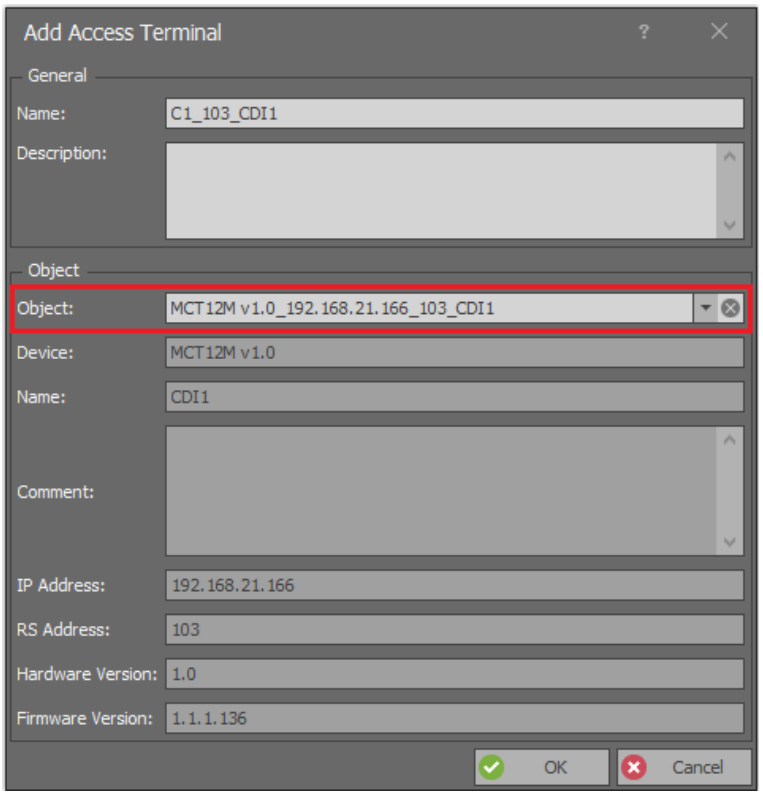
- When configuration with wizard is finished then expand controller in VISO navigation tree and double click *Access Points*.
- In the opened window select previously created Access Point *C1_Door1_IN* with ID=105 reader and then *Edit*.
- In the opened window in *Authorisation Modes* tab select *External Authorisation* or *Delayed Authorisation*. Optionally waiting time for both modes can be configured. Close the window with *OK* button.



- In the same window with Access Points select *Add* to create Access Point to be operated as authorisation approval terminal. Name the point and close the window with *OK* button.



- In the bottom select *Access Terminals* tab, then *Add* and in the opened window select ID=103 reader according to previous example figure.



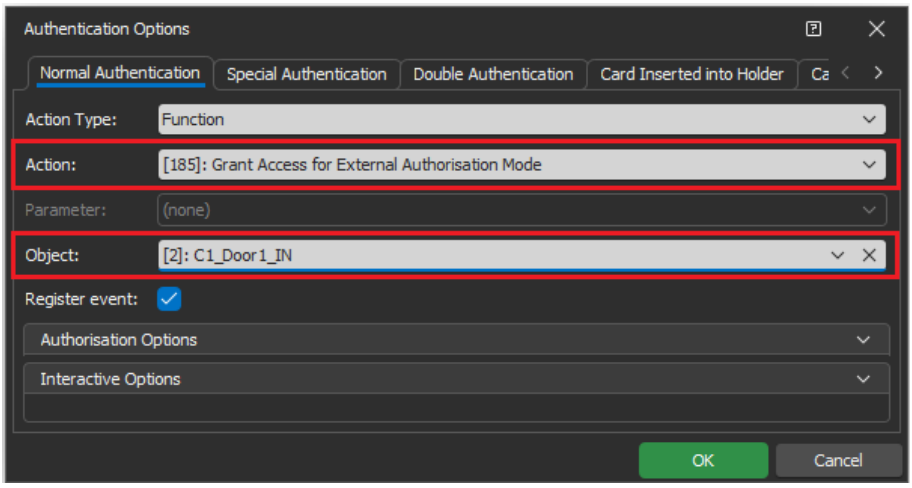
Access approving/denying from device

There a few methods to accept or deny access request from user who identifies at Access Point. It can be done with proximity card reading, PIN entered with reader's keypad, button connected to input of controller/reader/expander and with function key on reader's keypad. Optionally in case of input and

function key, it can be configured that their use requires user identification (card, PIN) and verification of user Authorisations for access request approving.

Authentication Factor (card, PIN)

- In the window with Access Points select *C1_Access approval point* i.e. point with ID=103 reader where access request will be approved/denied.
- In the bottom select *Authentication Options* tab and then *Edit*.
- Depending on previously selected Authorisation Mode, in the opened window select the function *[185]: Grant Access for External Authorisation Mode* or the function *[186]: Deny Access for Delayed Authorisation Mode*.
- In the field *Object* select *C1_Door1_IN* i.e. point with ID=105 reader where access will be requested.



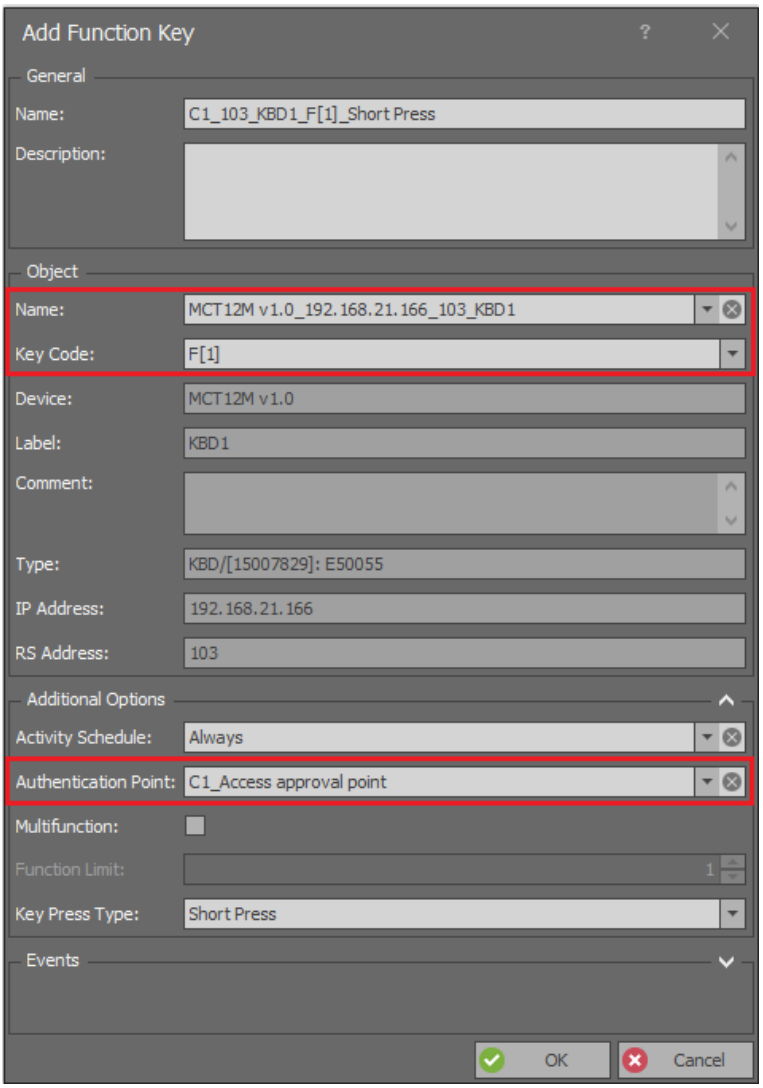
Function key without user verification

- In the window with Access Points select *C1_Door1_IN* i.e. point with ID=105 reader where access will be requested.
- In the bottom select *Function keys* tab and then *Add*.
- In the opened window select the button  to indicate the location of function key.
- In the next window, in the *Name* field of *Object* area select terminal with function key (ID=103), then indicate particular key code e.g. F1 and close the window with *OK* button.
- Depending on previously selected Authorisation Mode, in the opened window select the function *[185]: Grant Access for External Authorisation Mode* or the function *[186]: Deny Access for Delayed Authorisation Mode*.
- Upload settings to controller.

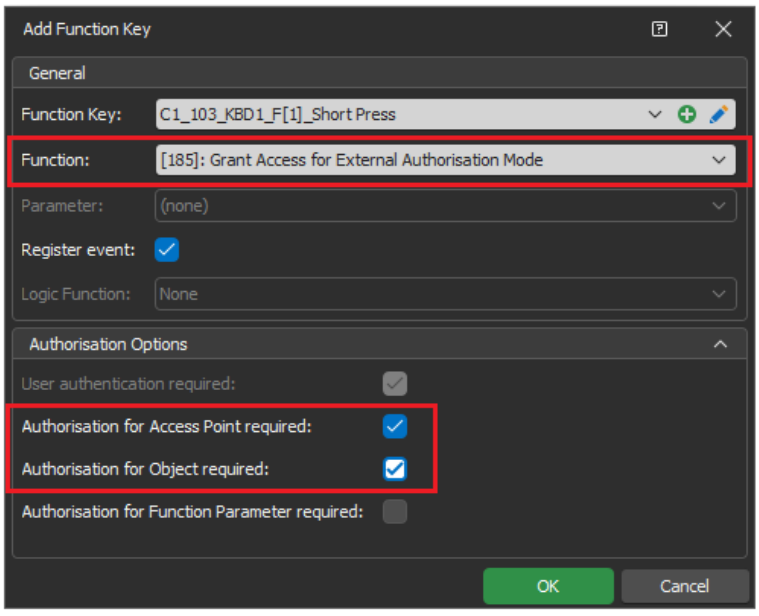
Similarly an input line for access approving/denying can be defined by selection of *Inputs* tab.

Function key with user verification

- In the window with Access Points select *C1_Door1_IN* i.e. point with ID=105 reader where access will be requested.
- In the bottom select *Function keys* tab and then *Add*.
- In the opened window select the button  to indicate the location of function key.
- In the next window, in the *Name* field of *Object* area select terminal with function key (ID=103), then indicate particular key code e.g. F1 and close the window with *OK* button.
- In the same window expand *Additional Options* area and select Access Point where the use of function key will have to be verified. This can be Access Point with the same reader where function key is located or any other Access Point with reader connected to the same MC16 access controller. Close the window with *OK* button.



- Depending on previously selected Authorisation Mode, in the opened window select the function *[185]: Grant Access for External Authorisation Mode* or the function *[186]: Deny Access for Delayed Authorisation Mode*. Additionally select options *Authorisation for Access Point required* and *Authorisation for Object required*. Close the window with *OK* button.

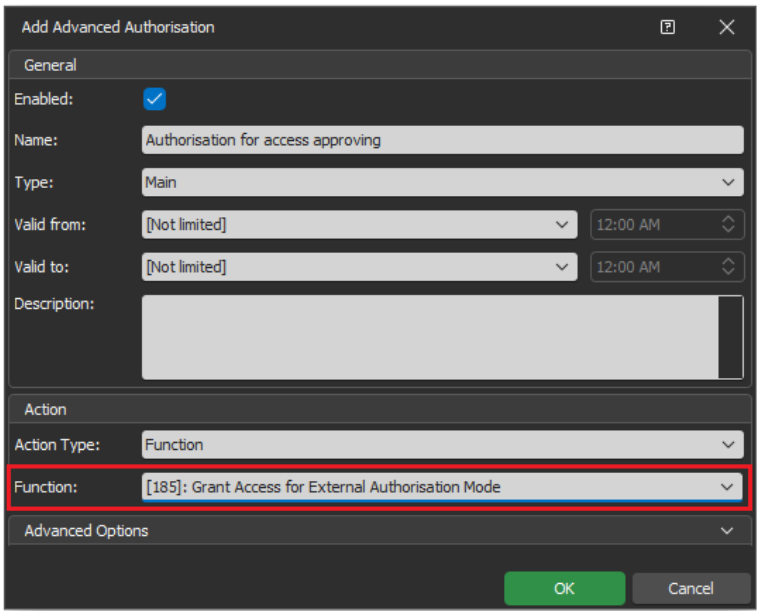


Similarly an input line for access approving/denying can be defined by selection of *Inputs* tab.

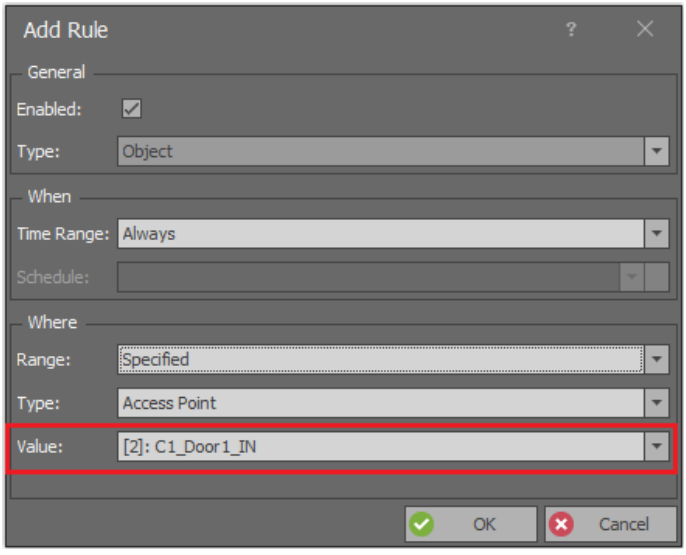
Authorisation

In case of access approving/denying with verification it is necessary to define Authorisation for the user who could approve/deny the access. It must be Advanced Authorisation for function *[185]* or *[186]* depending on previously selected Authorisation Mode. In order to define such Authorisation:

- In the navigation tree of VISO software expand *Authorisations* command, double click *Advanced Authorisations* and in the opened window select *Add* button.
- Depending on previously selected Authorisation Mode, in the opened window select the function *[185]: Grant Access for External Authorisation Mode* or the function *[186]: Deny Access for Delayed Authorisation Mode*. Close the window with *OK* button.



- In the bottom select *Positive Rules* tab and then *Add* button.
- In the opened window optionally select *Specified* as *Time Range* and assign one of available schedule if the Authorisation is supposed to be limited by time. *General Purpose Maintained Type* schedule can be defined with *Schedule* command in VISO navigation tree.
- In the same window select *Specified* as *Range* and then assign Access Point *C1_Door1_IN* Access Point i.e. point with ID=105 reader where access will be requested.



- Upload settings to controller.

- Assign new Authorisations to user(s) using *Add Person Online* or *Edit Person Online* wizard which is available when *Wizard* command is selected in the top menu of VISO software.

More information on Authorisations is given in AN003 application note.

Access approving/denying from VISO software

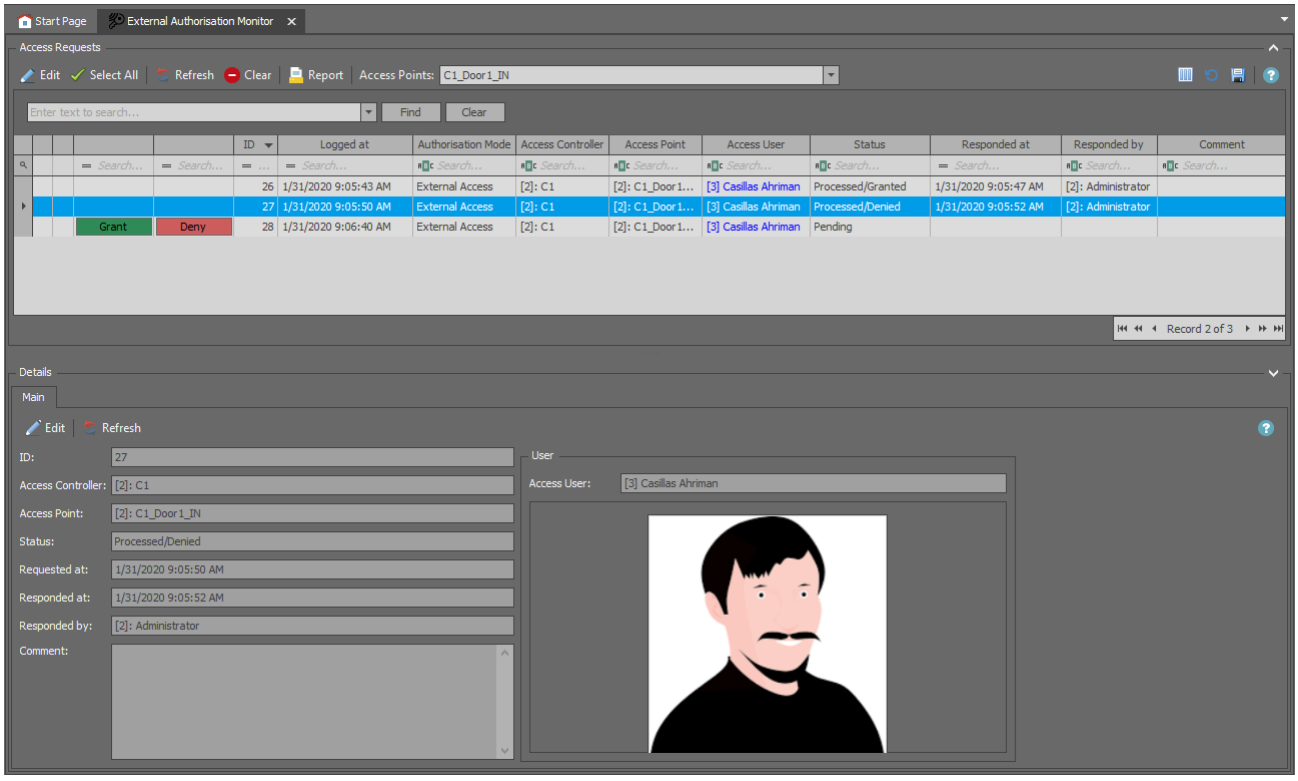
VISO software operator can remotely approve or deny access request from users. Additionally, CCTV cameras can be applied in one of the monitors if they are integrated with RACS 5 system. More information on CCTV integration in RACS 5 system is given in AN007 application note.

External Authorisation Monitor

The monitor can be started by selection of *External Authorisation* in the top menu of VISO software and then *External Authorisation Monitor*.

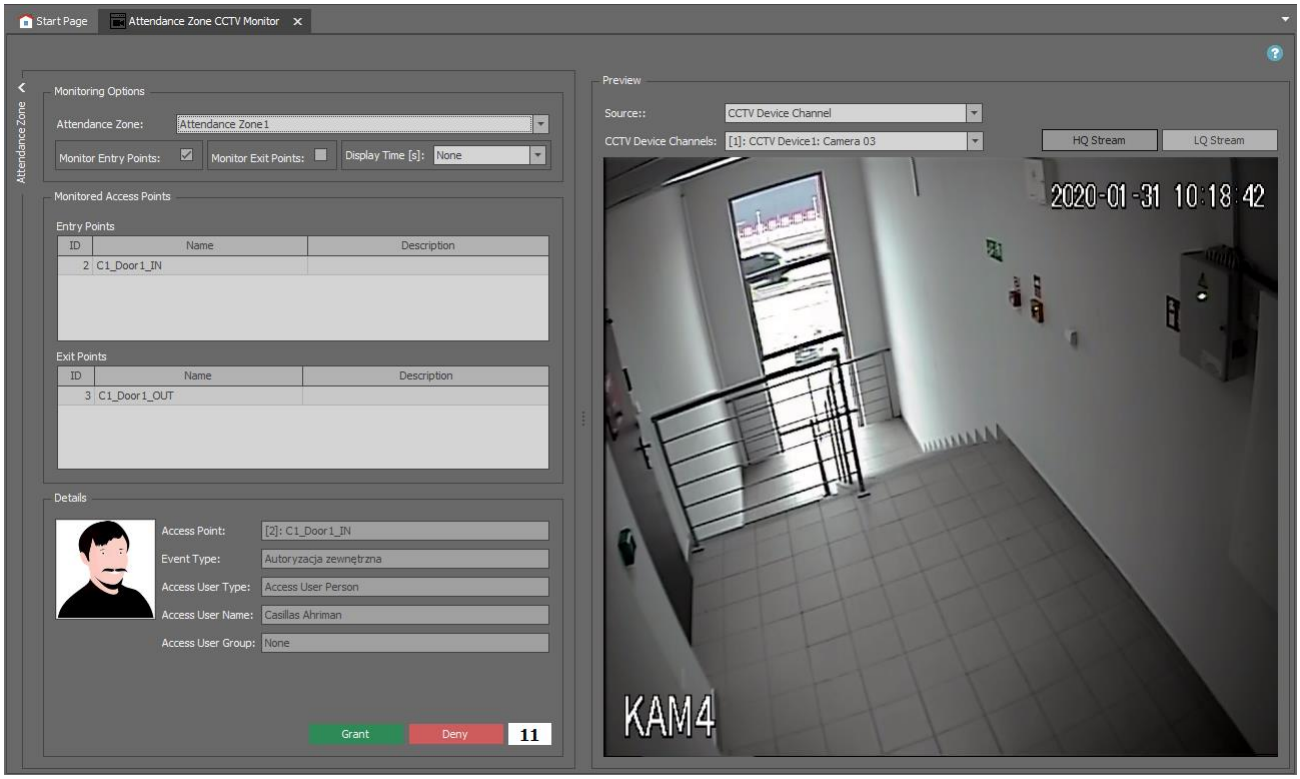
The monitor enables to:

- Indicate which Access Points with External or Delayed Authorisation Modes are monitored.
- Remotely grant or deny access for user at Access Point.
- Display personal details of requesting users including photo if previously assigned to the user.
- Filter, sort and clear the list with access requests.



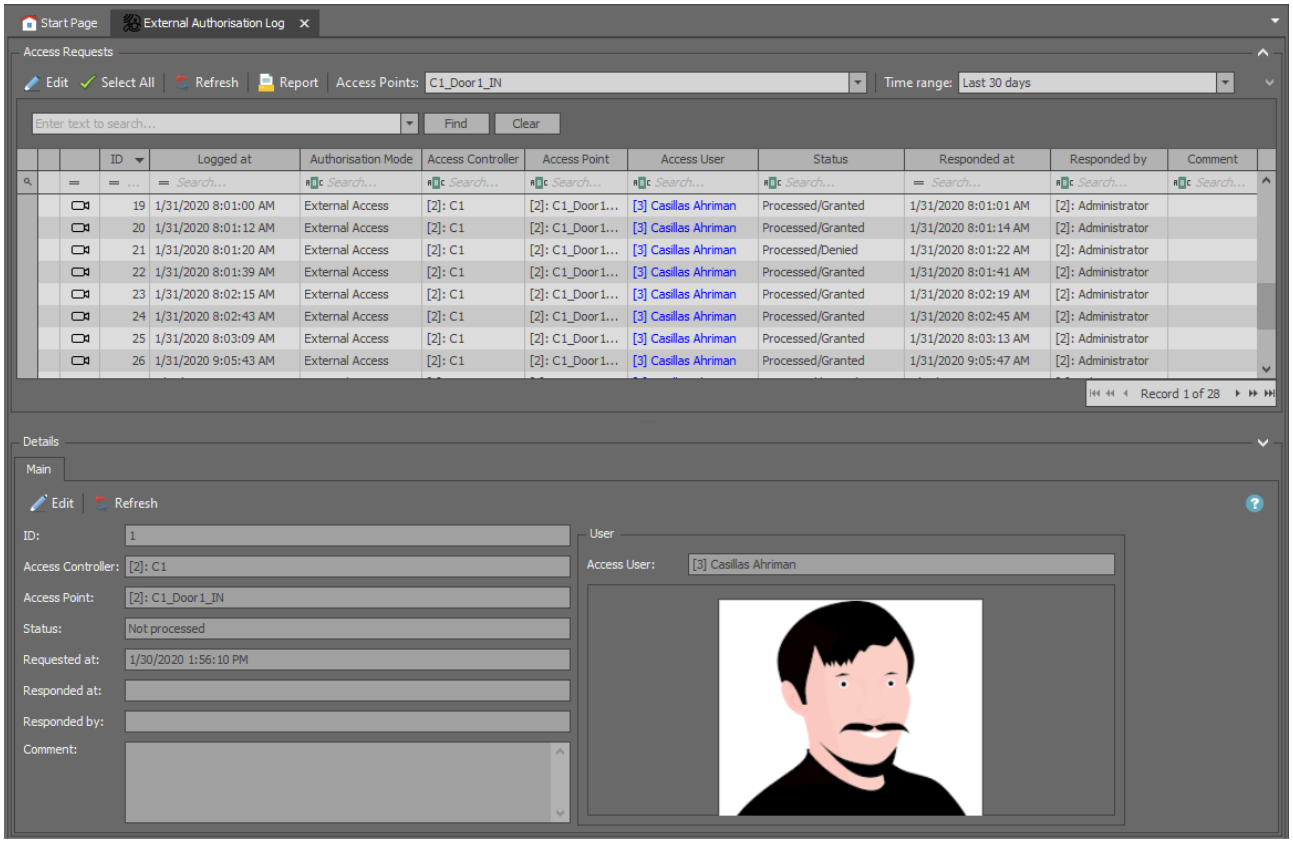
Attendance Zone CCTV Monitor

The monitor which is described in AN007 application note enables to monitor users who identify at selected Access Points. The monitor can not only display user personal data including photo but it can also automatically display video from a camera which is associated with the Access Point. If the External Authorisation Mode or Delayed Authorisation Mode is configured for such Access Point then buttons for remote access granting and denying are available.



External Authorisation Log

The log can be started by selection of *External Authorisation* in the top menu of VISO software and then *External Authorisation Log*. The log displays access request including information on users and operators.



External Authorisation Operators

RACS 5 system can be managed from multiple workstation by operators with access to various parts of VISO software. It is possible to define Role for Operator that would allow only manage monitors with external authorisation. More information on Operators and Roles is given in AN040 application note.

Authorisation Mode switching and signalling

Default Authorisation Mode is defined on the level of Access Point. It is also possible to switch current Authorisation Mode to another one using input functions *[177]* – *[184]*, and these functions can be started with card, PIN, input or function key. Additionally, current Authorisation Mode can be signalled with output functions *[80]* – *[85]* and waiting status for External and Delayed Authorisation Modes can be signalled with output function *[86]*. This function can be assigned to LED or buzzer at a reader or to any external signalling device using relay or transistor output of RACS 5 device.

Kontakt:
Roger sp. z o.o. sp.k.
82-400 Sztum
Gościszewo 59
Tel.: +48 55 272 0132
Faks: +48 55 272 0133
Pomoc tech.: +48 55 267 0126
Pomoc tech. (GSM): +48 664 294 087
E-mail: pomoc.techniczna@roger.pl
Web: www.roger.pl