Roger Access Control System 5v2

Application note no. 003

Document version: Rev. A

Authorisations

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

Introduction

In RACS 5 system the execution of any function by user may depend on assignment of adequate Authorisation which is defined for particular function (e.g. access granting request). It is possible to define Basic Authorisations which concerns groups of functions in range of access, automation, arming/disarming, etc. as well as to define Advanced Authorisations which are configured for particular function and include positive and negative rules. Additionally, Authorisation can be joined into groups to facilitate assignment of typical Authorisations to users (e.g. access at main doors in a building).

Authorisation can be assigned to:

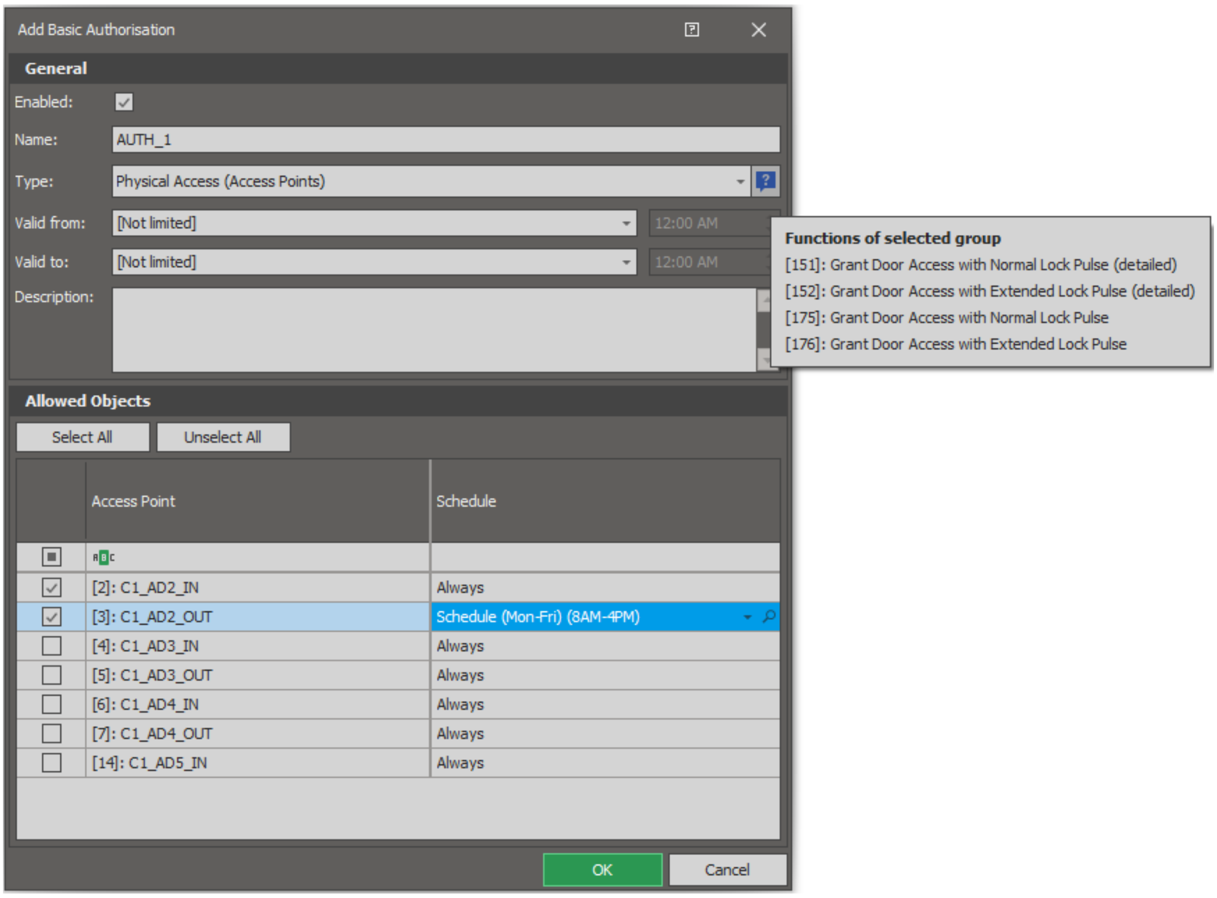
- Users (Persons, Visitors and Assets)
- Access Credentials belonging to Users
- User Groups

Authorisations of certain user are sum of Authorisation assigned on different levels (User, Access Credential and User Group).

Basic Authorisations

RACS 5 system enables to define Basic Authorisations which concern groups of functions in regard of access, automation, arming/disarming, etc. The purpose of the Basic Authorisations is to enable definition and application of the most popular and typical Authorisations in the system. In order to define Basic Authorisation:

- In the navigation tree of VISO software expand *Authorisations* and then double click *Basic Authorisations*.
- In the opened window select *Add*.
- In the newly opened window select *Type*. When question mark icon is selected then list of included functions is displayed.
- In the bottom select elements for the Authorisations e.g. Identification Points in case of *Physical Access (Identification Points)* type. Optionally assign Schedule(s) which are defined by selection of *Schedules* in the navigation tree of VISO software. They are used to limit Authorisation in time.



Add Basic Authorisation

General

Enabled: ☑

Name: AUTH_1

Type: Physical Access (Access Points)

Valid from: [Not limited] 12:00 AM

Valid to: [Not limited] 12:00 AM

Description:

Functions of selected group
[151]: Grant Door Access with Normal Lock Pulse (detailed)
[152]: Grant Door Access with Extended Lock Pulse (detailed)
[175]: Grant Door Access with Normal Lock Pulse
[176]: Grant Door Access with Extended Lock Pulse

Allowed Objects

	Access Point	Schedule
■		
☑	[2]: C1_AD2_IN	Always
☑	[3]: C1_AD2_OUT	Schedule (Mon-Fri) (8AM-4PM)
□	[4]: C1_AD3_IN	Always
□	[5]: C1_AD3_OUT	Always
□	[6]: C1_AD4_IN	Always
□	[7]: C1_AD4_OUT	Always
□	[14]: C1_AD5_IN	Always

Basic Authorisations of *Physical Access (Access Points)* type are also created by default when Access Door is defined by means of *Add Access Door Wizard* as explained in AN006 application note.

Advanced Authorisations

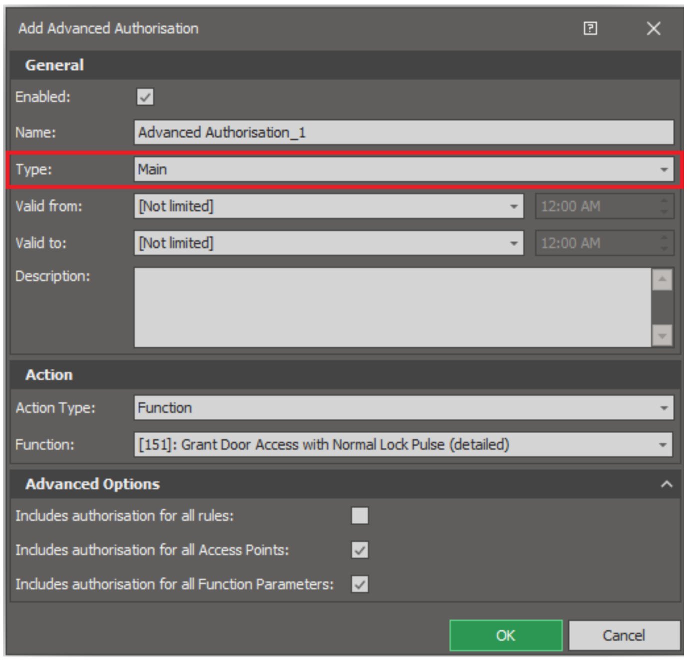
The scope of possible options and settings for the Advanced Authorisations is much greater than in case of the Basic Authorisations and it includes all available functions, authentication and authorisations options, positive/negative rules and related detailed rules. The purpose of Advanced Authorisations is to enable detailed configuration of rights depending on the specific requirements of the particular installation. Both types of Authorisations i.e. Basic and Advanced can be defined and used interchangeably.

Type

Two types of Advanced Authorisations are available:

- Main Authorisation consists of all types of Detailed Rules for a function and it is enough to decide if particular function can or cannot be executed.
- Complementary Authorisation consists of Detailed Rules concerning place of user authentication and action parameter but it is not enough to decide if particular function can or cannot be executed.

In case of Complementary Authorisation only Positive rules can be defined and they sum up with Positive rules included in associated Main Authorisation. If Main Authorisation rule for the execution of function is missing then Positive rule from Complementary Authorisation can be used. Main type Authorisations are commonly used while Complementary type Authorisations are applied only in special scenarios involving elevator and locker access control.



Add Advanced Authorisation

General

Enabled: ☑

Name: Advanced Authorisation_1

Type: Main

Valid from: [Not limited] 12:00 AM

Valid to: [Not limited] 12:00 AM

Description:

Action

Action Type: Function

Function: [151]: Grant Door Access with Normal Lock Pulse (detailed)

Advanced Options

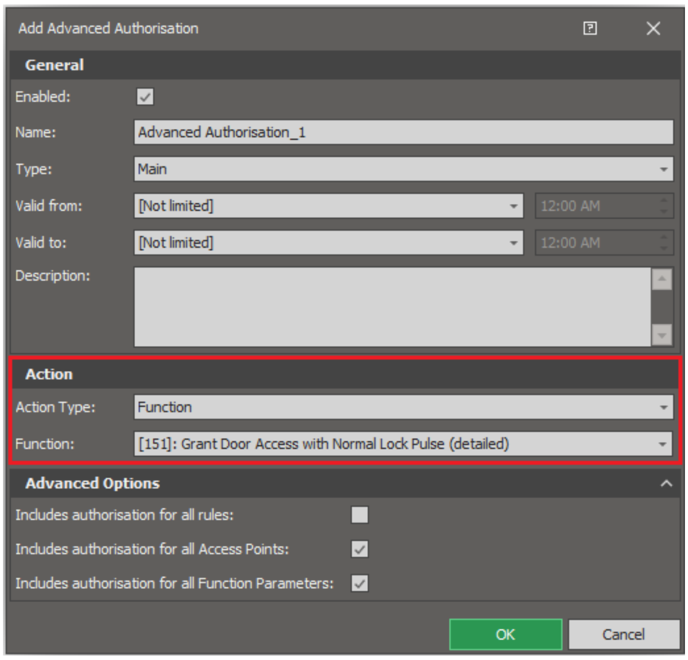
Includes authorisation for all rules: □

Includes authorisation for all Access Points: ☑

Includes authorisation for all Function Parameters: ☑

Action

Advanced Authorisation concerns selected function or group of functions (as in Basic Authorisations). Therefore in RACS 5 system various Authorisations can be defined for such functions as access granting, door unlocking, Alarm Zone arming/disarming, T&A mode selection, activation/deactivation of automation nodes, events registering, etc.



Add Advanced Authorisation

General

Enabled: ☑

Name: Advanced Authorisation_1

Type: Main

Valid from: [Not limited] 12:00 AM

Valid to: [Not limited] 12:00 AM

Description:

Action

Action Type: Function

Function: [151]: Grant Door Access with Normal Lock Pulse (detailed)

Advanced Options

Includes authorisation for all rules: □

Includes authorisation for all Access Points: ☑

Includes authorisation for all Function Parameters: ☑

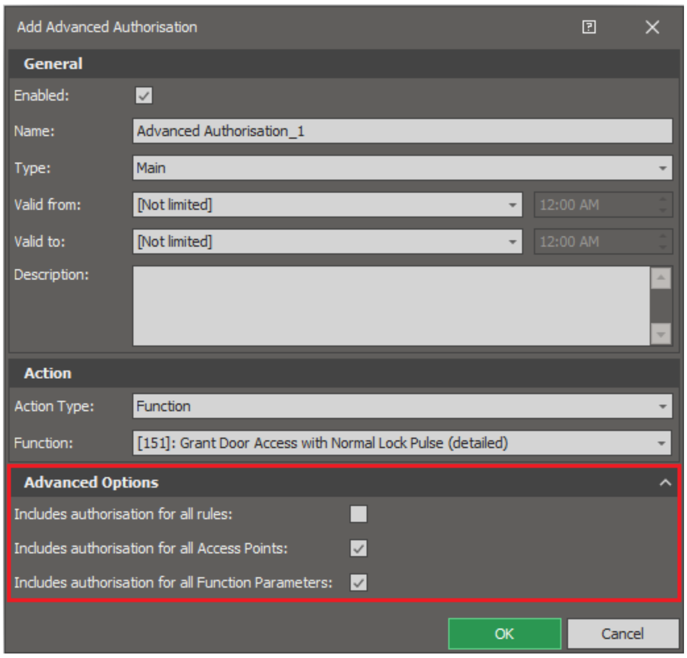
Advanced Options

Options of Advanced Authorisation allow for simplifying the definition of Authorisation when more detailed configuration is not necessary.

- When the option *Includes authorisation for all rules* is enabled then the owner of such Authorisation has all Detailed Rules required for execution of particular function in any place and any time.

- When the option *Includes authorisation for all Access Points* is enabled then the owner of such Authorisation can authenticate at any Access Point and it omits the rules concerning place of user authentication.
- When the option *Includes authorisation for all Function Parameters* is enabled then the owner of such Authorisation can execute the function with any parameter as it omits rules concerning function parameter.

By default the first option is disabled while two remaining options are enabled which means that in the next steps of configuration of typical Advanced Authorisation it is enough to define Detailed Rule(s) concerning Object. In case of the function *[151]: Grant Door Access with Normal Lock Pulse (each door logged separately)* the Object is Access Point or Access Zone where the access can be granted.



Add Advanced Authorisation

General

Enabled: ☑

Name: Advanced Authorisation_1

Type: Main

Valid from: [Not limited] 12:00 AM

Valid to: [Not limited] 12:00 AM

Description:

Action

Action Type: Function

Function: [151]: Grant Door Access with Normal Lock Pulse (detailed)

Advanced Options

Includes authorisation for all rules: □

Includes authorisation for all Access Points: ☑

Includes authorisation for all Function Parameters: ☑

Positive/Negative Rules

The Authorisation includes Positive Rules and Negative Rules which define respectively when the function can be executed and cannot be executed. Negative Rules have higher priority than Positive Rules. If at least one Authorisation assigned to user includes single Negative Rule concerning particular function then such function cannot be executed at all. If no Negative Rule is found then single Positive Rule is enough to execute the function.

Detailed Rules

Both Positive and Negative Rules consists of Detailed Rules concerning:

- Object
- Access Point
- Function Parameter

Multiple Detailed Rules of the same type can be defined within Positive/Negative Rule. Such Detailed Rules are summed up.

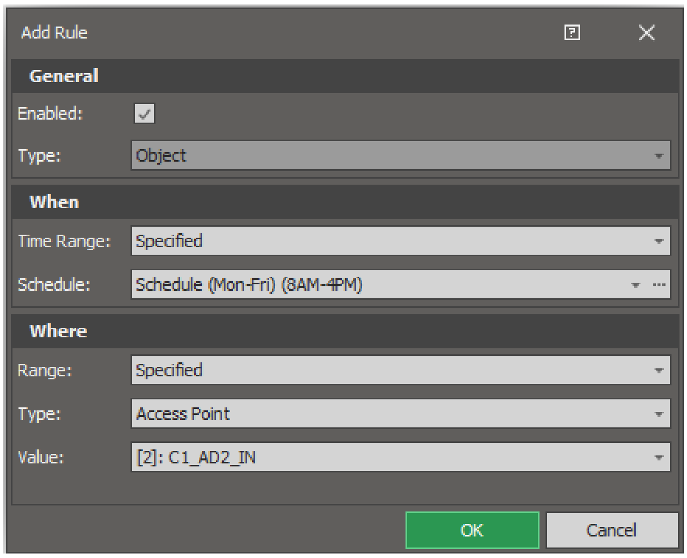
Positive/Negative Rule is completed if it includes at least one of each required Detailed Rules. Positive/Negative Rules are verified in following order in regard of:

- user right to authenticate at certain Access Point
- user right to execute the function at certain Object
- user right to execute the function with certain Function Parameter

The authentication requirement is skipped when the option *Includes authorisation for all Access Points is enabled*.

The verification of right to execute Function Parameter is skipped when the option *Includes authorisation for all Function Parameters* is enabled.

Each Detailed Rule can be additionally assigned with schedule which defines when the rule is valid. Schedules are defined with *Schedules* command in navigation tree of VISO software.



General

Enabled: ☑

Type: Object

When

Time Range: Specified

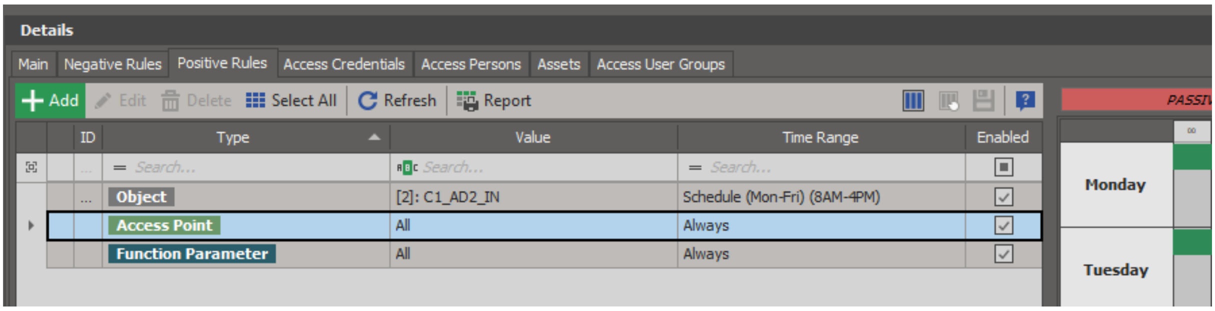
Schedule: Schedule (Mon-Fri) (8AM-4PM)

Where

Range: Specified

Type: Access Point

Value: [2]: C1_AD2_IN

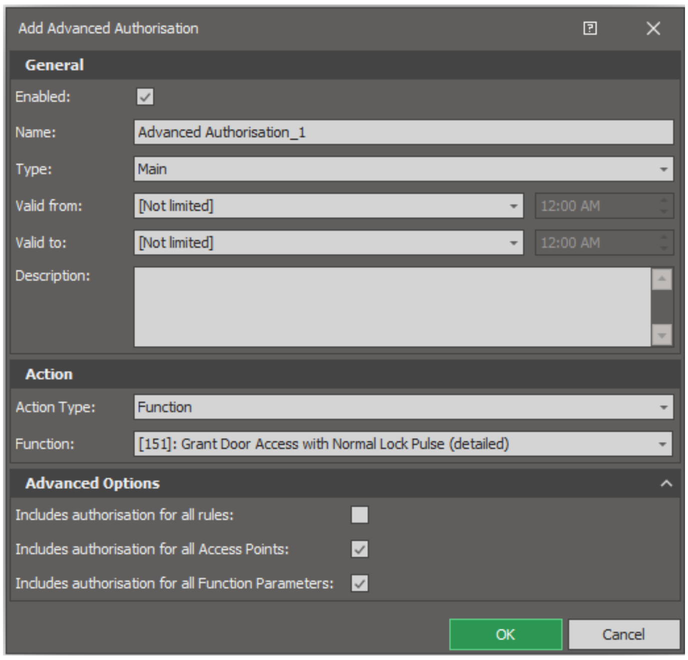


ID	Type	Value	Time Range	Enabled
	Object	[2]: C1_AD2_IN	Schedule (Mon-Fri) (8AM-4PM)	☑
	Access Point	All	Always	☑
	Function Parameter	All	Always	☑

Typical configuration

In order to configure Advanced Authorisation for access control using typical function *[151]*:

- In the navigation tree of VISO software expand *Authorisations* and then double click *Advanced Authorisations*.
- In the opened window select *Add*.
- Select the function *[151]: Grant Door Access with Normal Lock Pulse (detailed)* from the list and close the window with *OK* button.



Add Advanced Authorisation

General

Enabled:	☑
Name:	Advanced Authorisation_1
Type:	Main
Valid from:	[Not limited] 12:00 AM
Valid to:	[Not limited] 12:00 AM
Description:	

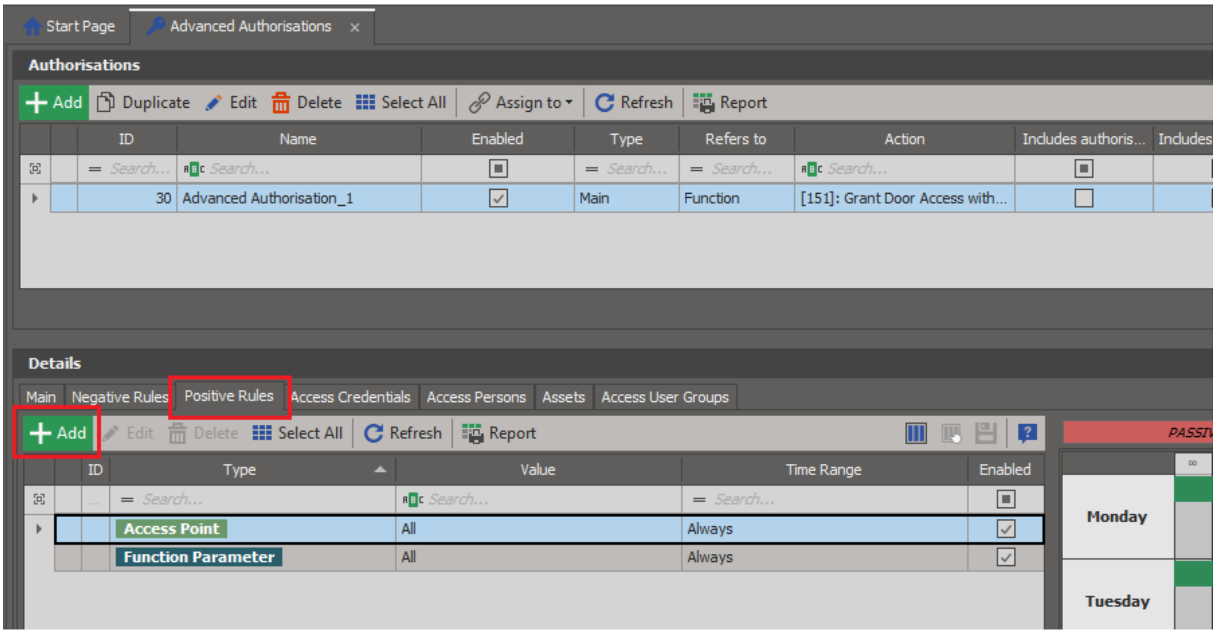
Action

Action Type:	Function
Function:	[151]: Grant Door Access with Normal Lock Pulse (detailed)

Advanced Options

Includes authorisation for all rules:	□
Includes authorisation for all Access Points:	☑
Includes authorisation for all Function Parameters:	☑

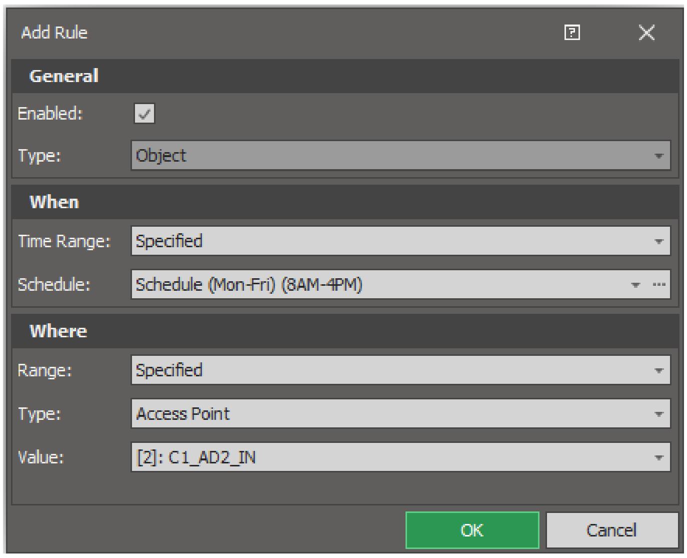
- For created Authorisation in the bottom select *Positive Rules* tab and then *Add*.



ID	Name	Enabled	Type	Refers to	Action	Includes authoris...	Includes
30	Advanced Authorisation_1	☑	Main	Function	[151]: Grant Door Access with...	□	

ID	Type	Value	Time Range	Enabled
	Access Point	All	Always	☑
	Function Parameter	All	Always	☑

- In the newly opened window select *Object* type, optionally assign Schedule to limit the rule in time and select Access Point where the access can be granted based on this Authorisation. Schedule must be earlier defined by selection of *Schedules* in the navigation tree of VISO software.



Add Rule

General

Enabled: ☑

Type: Object

When

Time Range: Specified

Schedule: Schedule (Mon-Fri) (8AM-4PM)

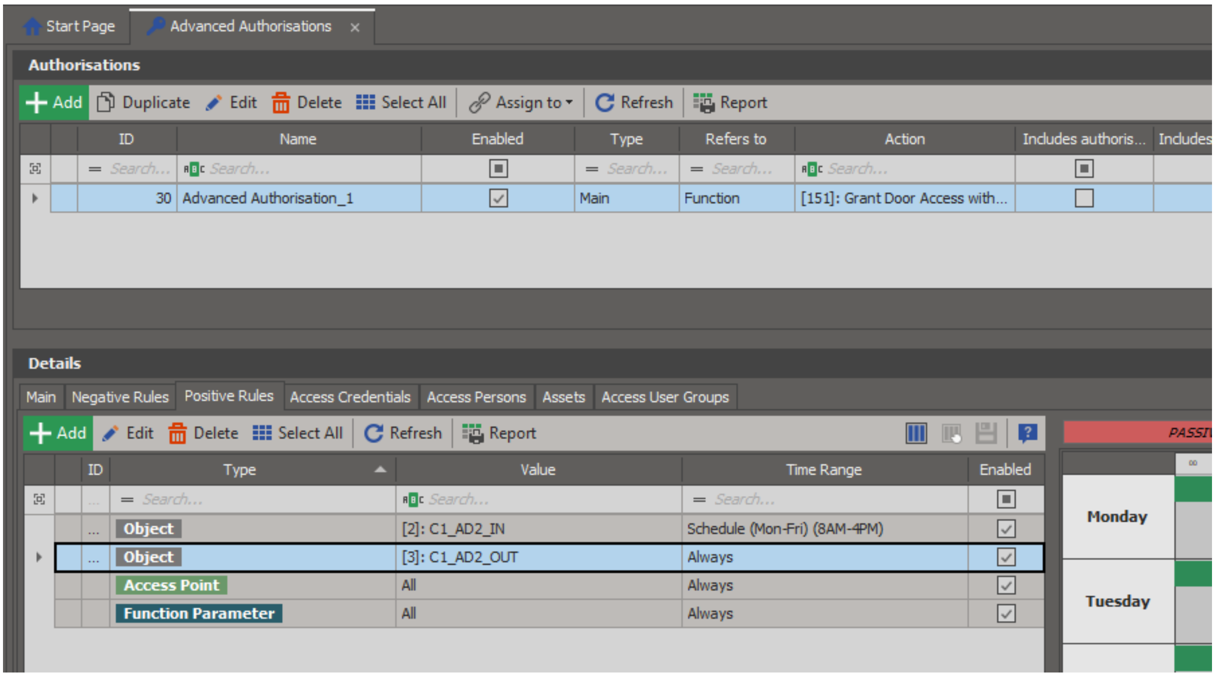
Where

Range: Specified

Type: Access Point

Value: [2]: C1_AD2_IN

- If needed, define more positive rules for the Authorisation so it could cover more Access Points.



Authorisations

ID	Name	Enabled	Type	Refers to	Action	Includes authoris...	Includes
30	Advanced Authorisation_1	☑	Main	Function	[151]: Grant Door Access with...	☐	

Details

ID	Type	Value	Time Range	Enabled
...	Object	[2]: C1_AD2_IN	Schedule (Mon-Fri) (8AM-4PM)	☑
...	Object	[3]: C1_AD2_OUT	Always	☑
	Access Point	All	Always	☑
	Function Parameter	All	Always	☑

- Similarly define more Authorisations so they could be further assigned to users directly or via *Add Person online* or *Edit Person Online* wizards.

Authorisation Groups

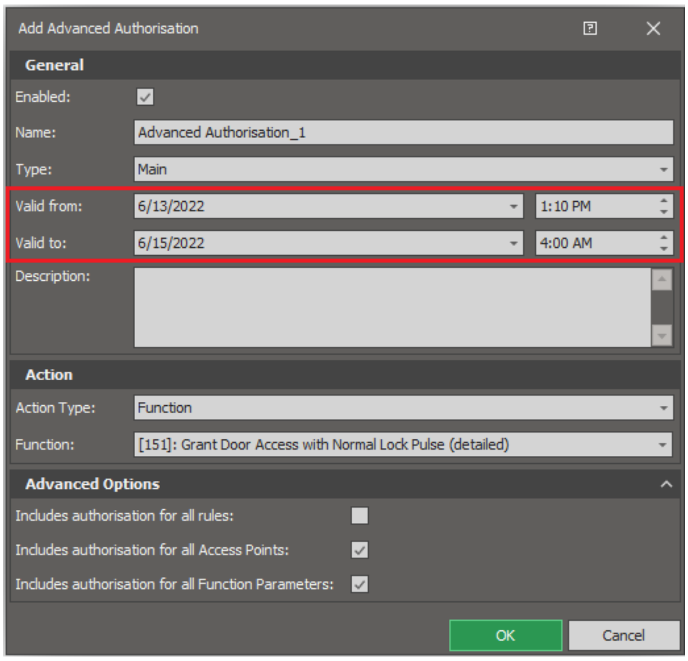
VISO software enables to group Authorisations in order to facilitate management of user rights. This is usually useful when there are main doors and corridor doors which are entered by many users and consequently all of them must be assigned with rights at such doors. In such scenario these Authorisations can be grouped and then entire Authorisation Groups can be assigned to users instead of individual rights. Authorisation Groups are defined by expanding *Authorisation* in the navigation tree of VISO software and then double clicking *Authorisation Groups*.

Assignment of Authorisations

Authorisations in RACS 5 system can be assigned to Access Credentials, Access Users and Access User Groups. The recommended method is to use *Add Person Online* wizard or *Edit Person Online* wizard which are available after selection of *Wizards* in the top menu of VISO software. When the particular function is to be executed then not only Authorisations assigned to particular Access Credential are verified but also Authorisation assigned to the owner (user) of such credential as well as Authorisations assigned to User Group of the owner. Consequently all these Authorisations assigned at various levels are summed up. Such adding concerns both Positive and Negative Rules.

Time limits for Authorisations

As explained in previous sections, Detailed Rules can limit Authorisation in time, based on weekly Schedules. Additionally when Basic or Advanced Authorisation is defined then it is possible to define time range when the Authorisation is enabled. Beyond that time the Authorisation is inactive and cannot be used to start its function. However such limitation will affect all users who are assigned with such Authorisation.



General

Enabled: ☑

Name: Advanced Authorisation_1

Type: Main

Valid from: 6/13/2022 1:10 PM

Valid to: 6/15/2022 4:00 AM

Description:

Action

Action Type: Function

Function: [151]: Grant Door Access with Normal Lock Pulse (detailed)

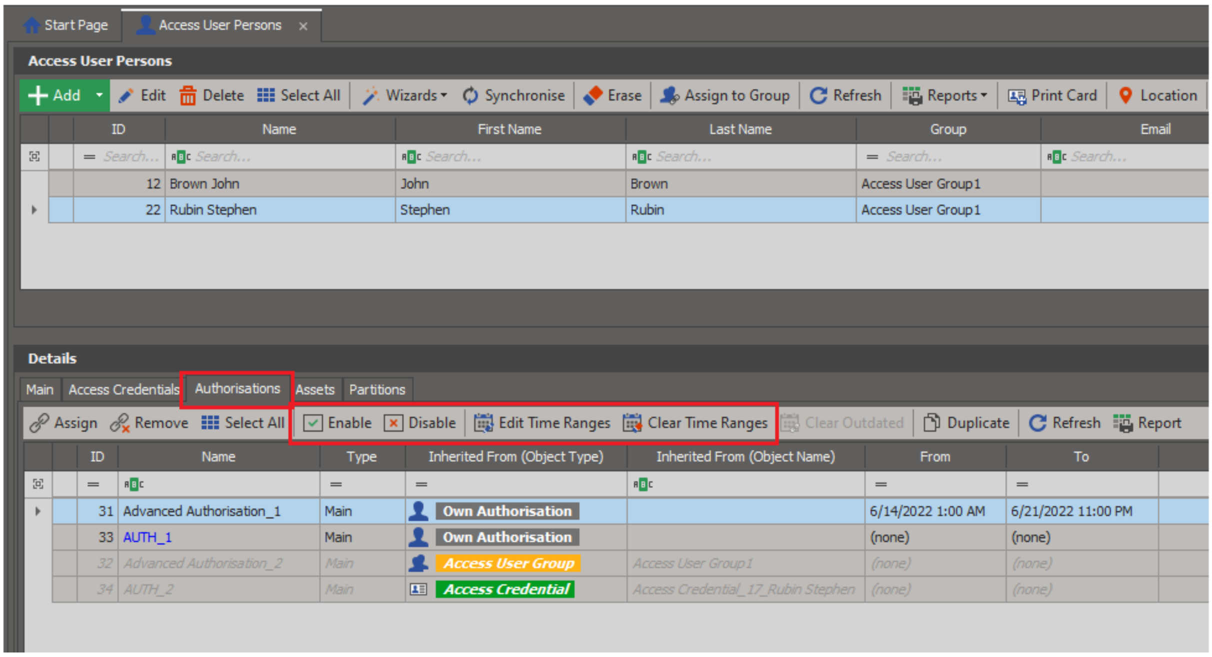
Advanced Options

Includes authorisation for all rules: □

Includes authorisation for all Access Points: ☑

Includes authorisation for all Function Parameters: ☑

It is also possible to manage Authorisations of particular Person in time. In such case the modification of assigned Authorisation does not affect other Persons with the same Authorisation. Such management is possible only in case of Authorisations which are directly assigned on the level of Person and not on the level of Access Credential or User Group. In the same window Authorisations can also be activated and deactivated for particular Person. The window for management of Person's Authorisations in time can be accessed by selection of *Configuration* in the top menu of VISO software, then *Persons* and *Authorisations* tabs in the bottom.



ID	Name	First Name	Last Name	Group	Email
12	Brown John	John	Brown	Access User Group1	
22	Rubin Stephen	Stephen	Rubin	Access User Group1	

ID	Name	Type	Inherited From (Object Type)	Inherited From (Object Name)	From	To
31	Advanced Authorisation_1	Main	Own Authorisation		6/14/2022 1:00 AM	6/21/2022 11:00 PM
33	AUTH_1	Main	Own Authorisation		(none)	(none)
32	Advanced Authorisation_2	Main	Access User Group	Access User Group1	(none)	(none)
34	AUTH_2	Main	Access Credential	Access Credential_17_Rubin Stephen	(none)	(none)

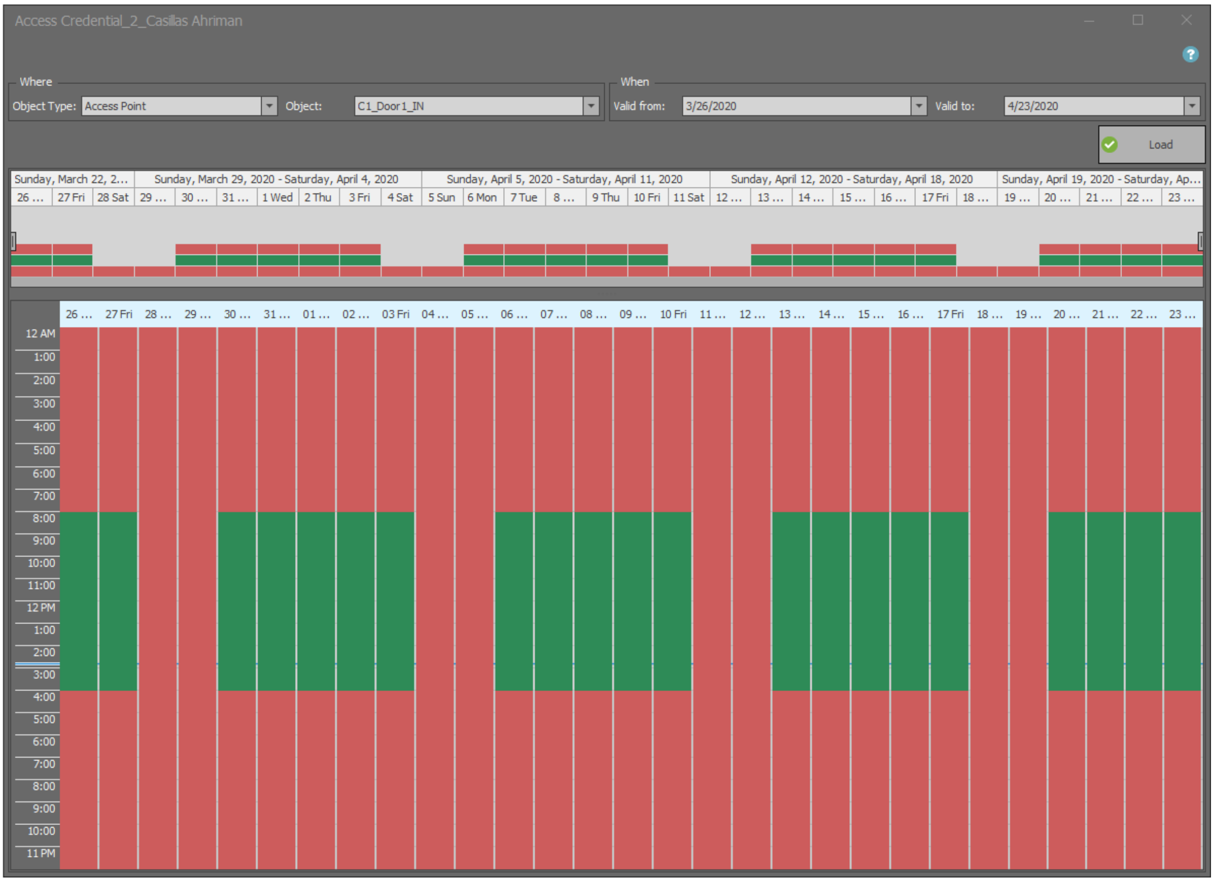
Verification of Authorizations

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 of user at particular Access Door or Access Zone:

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



Access Credential_2_Casillas Ahriman

Where

Object Type: Access Point

Object: C1_Door1_IN

When

Valid from: 3/26/2020

Valid to: 4/23/2020

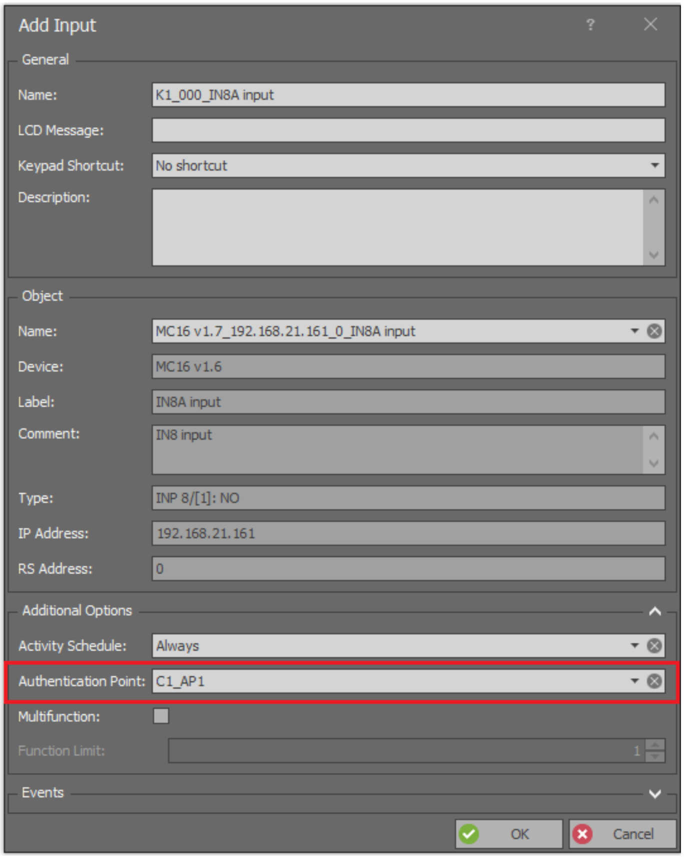
Load
Sunday, March 22, 2...
Sunday, March 29, 2020 - Saturday, April 4, 2020
Sunday, April 5, 2020 - Saturday, April 11, 2020
Sunday, April 12, 2020 - Saturday, April 18, 2020
Sunday, April 19, 2020 - Saturday, Ap...
26 ... 27 Fri 28 Sat 29 ... 30 ... 31 ... 1 Wed 2 Thu 3 Fri 4 Sat 5 Sun 6 Mon 7 Tue 8 ... 9 Thu 10 Fri 11 Sat 12 ... 13 ... 14 ... 15 ... 16 ... 17 Fri 18 ... 19 ... 20 ... 21 ... 22 ... 23 ...
26 ... 27 Fri 28 ... 29 ... 30 ... 31 ... 01 ... 02 ... 03 Fri 04 ... 05 ... 06 ... 07 ... 08 ... 09 ... 10 Fri 11 ... 12 ... 13 ... 14 ... 15 ... 16 ... 17 Fri 18 ... 19 ... 20 ... 21 ... 22 ... 23 ...
12 AM
1:00
2:00
3:00
4:00
5:00
6:00
7:00
8:00
9:00
10:00
11:00
12 PM
1:00
2:00
3:00
4:00
5:00
6:00
7:00
8:00
9:00
10:00
11 PM

In order to obtain information on users with Access Authorisations at particular Access Door:

- In the top menu of VISO software select *Configuration* and then *Access Doors*.
- In the opened window expand particular controller, select Access Door and then click *Access Users* or Access Credentials in the top menu of this window.

Methods of function execution (sources)

Generally functions can be invoked in multiple ways which can be divided into personal and impersonal ones. In case of personal invoking a function is activated by user who is also identified within the process. In case of impersonal invoking a function is not activated by user or is activated by user without identification. Typical personal invoking of a function is identification at Access Point (e.g. with proximity card) or remote command by system operator. Typical impersonal invoking of a function is input activation (without authentication), Function key activation (without authentication) or automatic activation of a function by schedule. Authorisations can be verified only for personal function invoking but in case of impersonal invoking usually it is possible to indicate *Authentication Point* where input or function key activation would require authentication. Consequently such invoking becomes personal one because user identification with adequate Authorisation(s) is required depending on *Authorisation Options*.



Add Input

General

Name: K1_000_IN8A input

LCD Message:

Keypad Shortcut: No shortcut

Description:

Object

Name: MC16 v1.7_192.168.21.161_0_IN8A input

Device: MC16 v1.6

Label: IN8A input

Comment: IN8 input

Type: INP 8/[1]: NO

IP Address: 192.168.21.161

RS Address: 0

Additional Options

Activity Schedule: Always

Authentication Point: C1_AP1

Multifunction: □

Function Limit: 1

Events

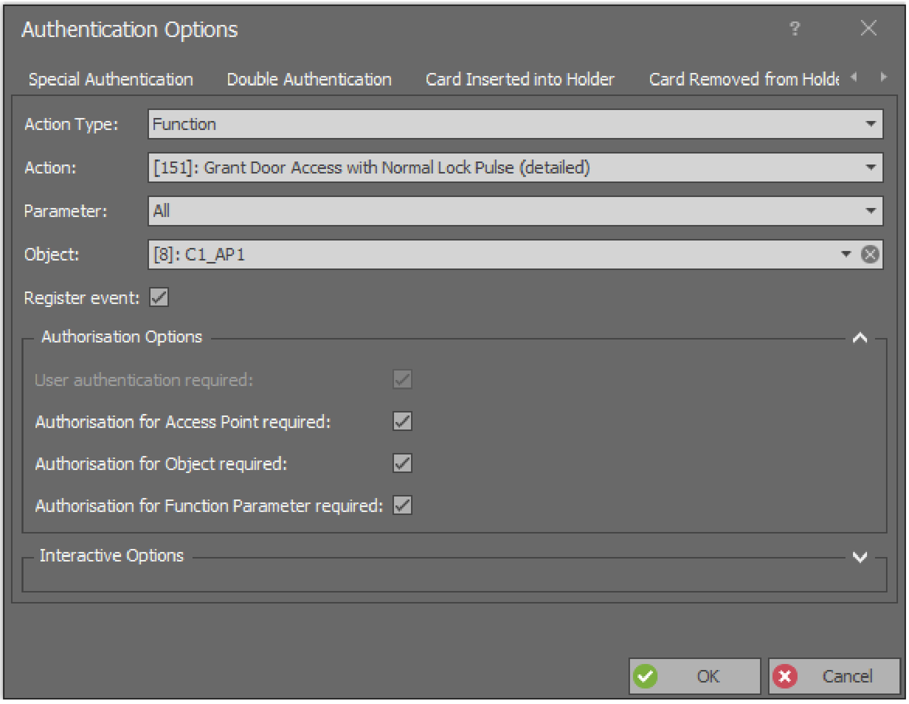
Authentication options

In RACS 5 system the authentication is a sequence of actions performed by user for the purpose of identification. Depending on current Authentication Policy at certain Access Point, a user is obliged to apply at least single Authentication Factor (card, PIN, fingerprint, etc.)

Additionally the controller can recognize five Authentication Options (methods) at Access Point:

- Normal Authentication (e.g. single card reading)
- Special Authentication (e.g. long card reading)
- Double Authentication (e.g. double card reading)
- Card Inserted into Holder (concerns readers with holder e.g. MCT82M-IO-CH)
- Card Removed from Holder (concerns readers with holder e.g. MCT82M-IO-CH)

Each Authentication Option can be assigned with a function thus Authentication Options are methods for function invoking (e.g. access granting) while Authorisations are permissions for such invoking. Authentication Option can be assigned with single function or group of functions defined with Local Command. In case of Local Command the Authorisation for every function is verified individually which means that if a user invokes Local Command but doesn’t have Authorisations for each function of the command then such Local Command shall be executed but it will be limited to functions covered by Authorisations.



Action Type: Function

Action: [151]: Grant Door Access with Normal Lock Pulse (detailed)

Parameter: All

Object: [8]: C1_AP1

Register event: ☑

Authorisation Options

User authentication required: ☑

Authorisation for Access Point required: ☑

Authorisation for Object required: ☑

Authorisation for Function Parameter required: ☑

Interactive Options

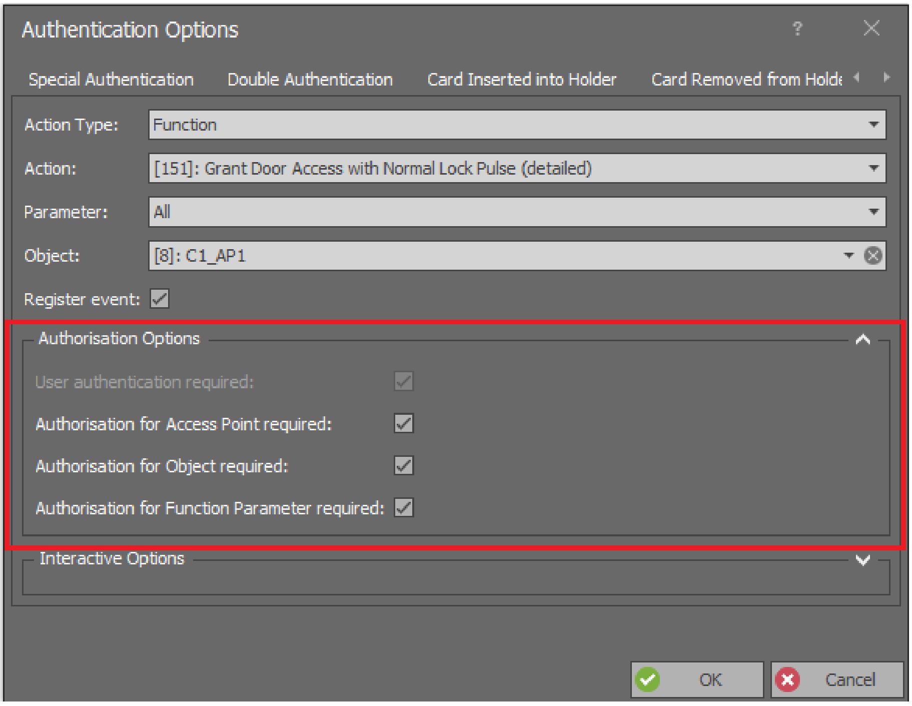
Authorisation Options

Authorisations Options can be defined for various methods of function invoking in order to make user identification necessary and to define scope of required Authorisations. For example if all the options are disabled then no Authorisation is required to invoke particular function and every user can activate it.

Authorisation Options can be defined for a function at the level of:

- Access Point (for each Authentication Option)
- Input line
- Function key
- Local Command functions

In case of inputs and function keys the options are effective only if *Authentication Point* for verification of Authorisation(s) is indicated.



Authentication Options

Action Type: Function

Action: [151]: Grant Door Access with Normal Lock Pulse (detailed)

Parameter: All

Object: [8]: C1_AP1

Register event: ☑

Authorisation Options

User authentication required: ☑

Authorisation for Access Point required: ☑

Authorisation for Object required: ☑

Authorisation for Function Parameter required: ☑

Interactive Options

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