Roger Access Control System 5

Application note no. 003

Document version: Rev. C

Authorisations

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

Introduction

In RACS 5 system the execution of any function by user may depend on assignment of adequate Authorisation(s) to such a user. The Authorisation is defined for particular function (e.g. access request) and it specifies conditions for which the function can be or cannot be executed. The Authorisation can be also defined for a Group of functions and in such case, it concerns all function belonging to the group.

Except for functions which are intended to gain access and for arming/ disarming of the alarm system, many functions by default (e.g. input line functions), do not require Authorisation. If necessary, system administrator can activate the need for Authorisation for any function. The need for Authorisation is not set globally but individually for each specific situation. Therefore if request for Authorisation is set for specific function in the specific situation, it is necessary to define such a Authorisation in the system and assign it to the user(s).

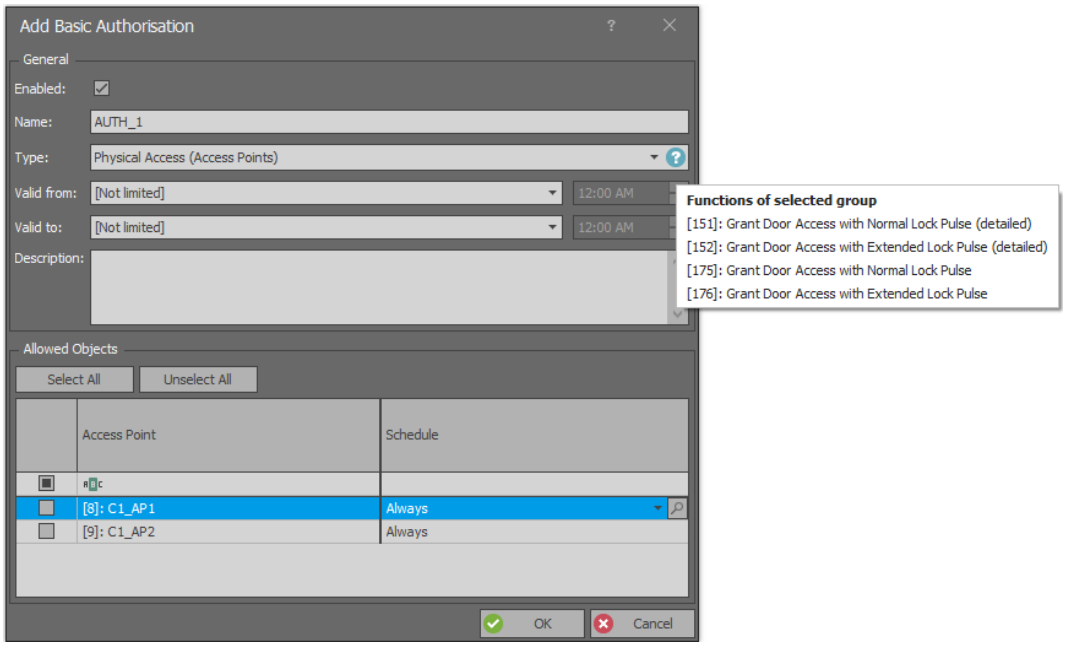
Authorisation can be assigned to:

- 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). Additionally, Authorisation can be joined into groups to facilitate assignment of typical Authorisations to Users (e.g. access at main doors in a buidling).

Standard Authorisations

RACS 5 system enables to define Standard Authorisations which concern groups of functions in regard of Physical Access, Arming/Disarming, Automation, etc. When icon is selected then list of included functions is displayed. Schedules can be applied for Authorisations to limit them in time. The purpose of the Standard Authorisations is to enable definition and application of the most popular and typical Authorisations in RACS 5 access control system.



Advanced Authorisations

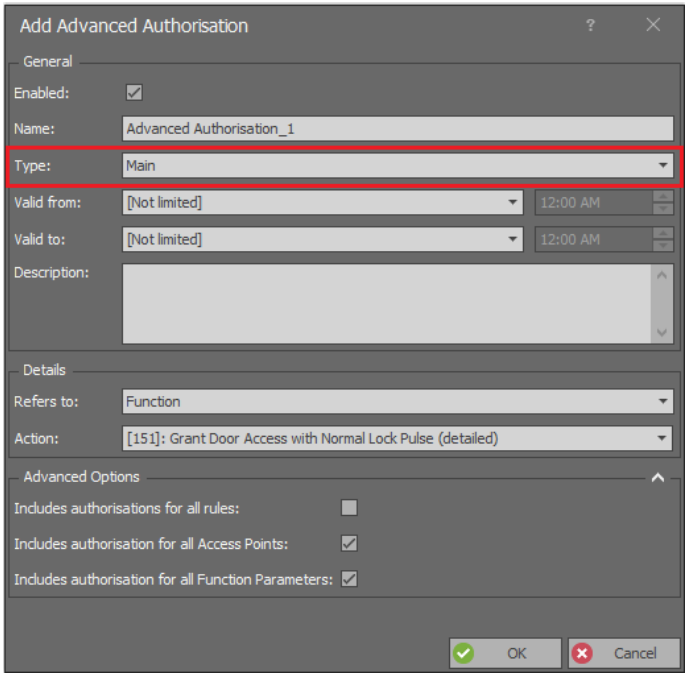
The scope of possible options and settings for the Advanced Authorisations is much greater than in case of the Standard Authorisations and it includes all available functions, authentication and authorisations options, positive/negative rules and related detailed rules. The purpose of Advanced Authorisations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

Types of Advanced Authorisations

Two types of Advanced Authorisations are available:

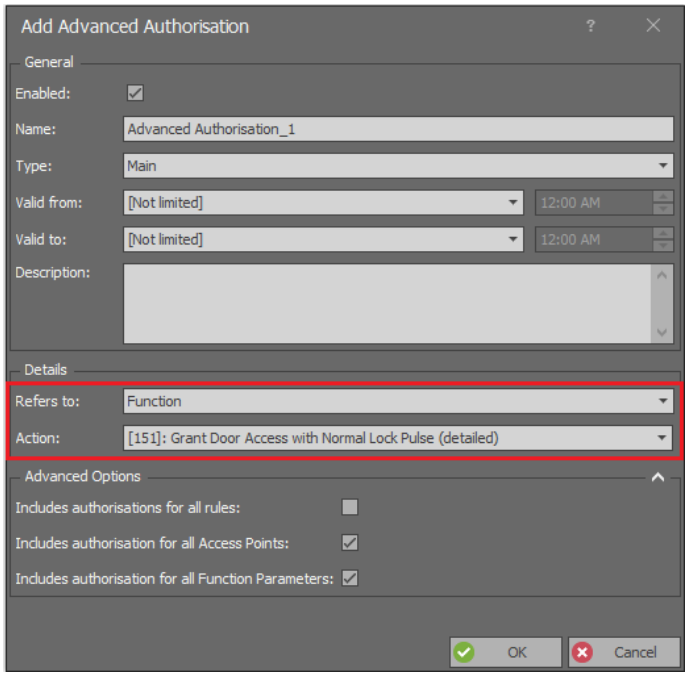
- Main Authorisation consists of all types of Detailed Rules for a function and it is enough to decide if particular function can or cannot be executed.
- Complementary Authorisation consists of Detailed Rules concerning place of user authentication and action parameter but it is not enough to decide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

In case 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. Complementary Authorisations are mainly used in case of elevator and locker access control.



Action of Advanced Authorisation

Advanced Authorisation concerns selected function or group of functions (as in Basic Authorisations). Therefore in RACS 5 system multiple 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.

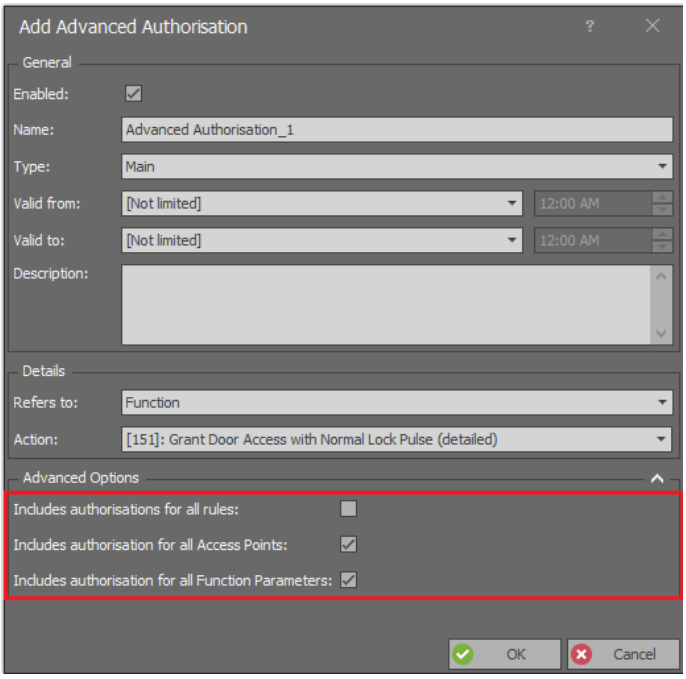


Options of Advanced Authorisation

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 is granted.



Positive/Negative Rules of Advanced Authorisation

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 of Advanced Authorisation

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.

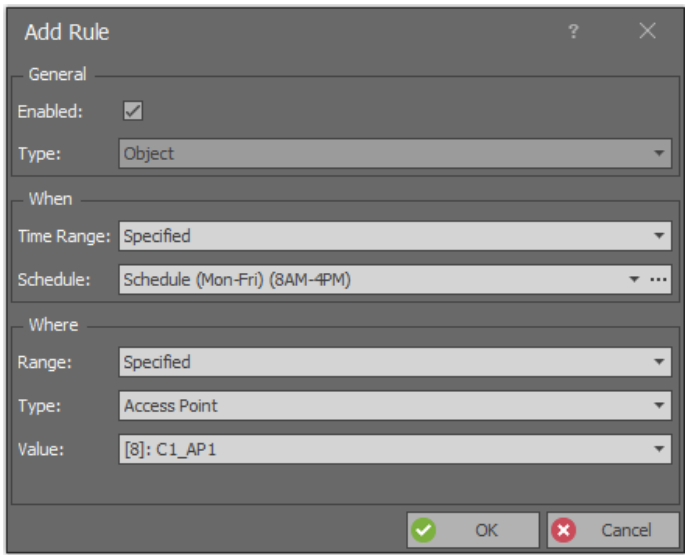
Positive/Negative Rule is completed if it includes at least one of each required Detailed Rules. Positive/Negative Rules are verified in following order in regard of:

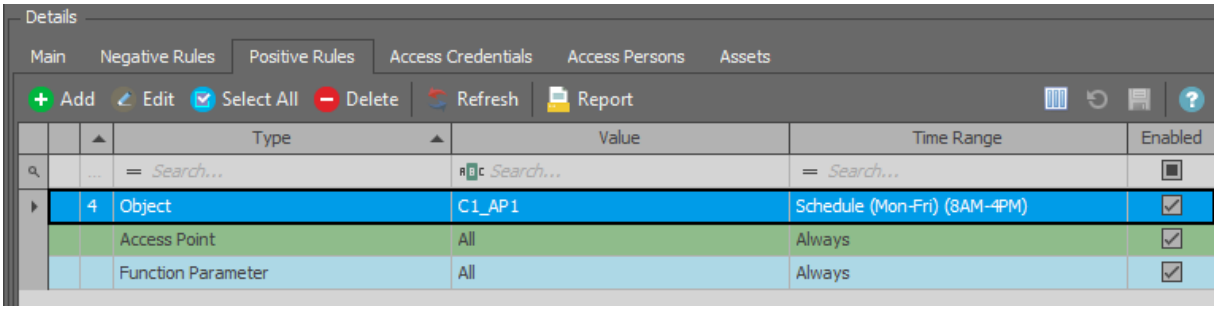
- user right to authenticate at certain Access Point
- user right to execute the function at certain Object
- user right to execute the function with certain Function Parameter

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.



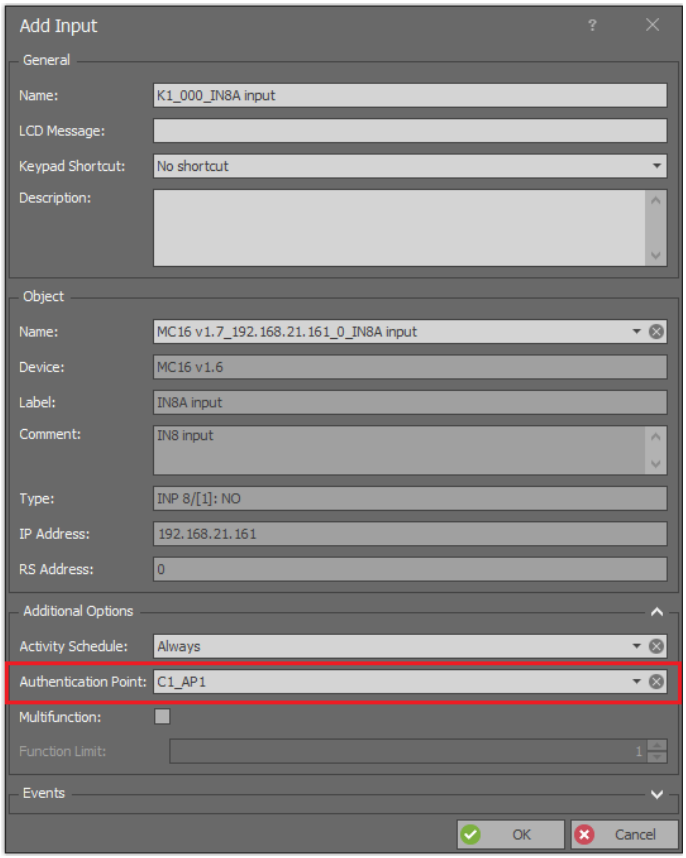


Assignment of Authorisations

Authorisations in RACS 5 system can be assigned to Access Credentials, Access Users and Access User Groups. 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.

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*.



Authentication options

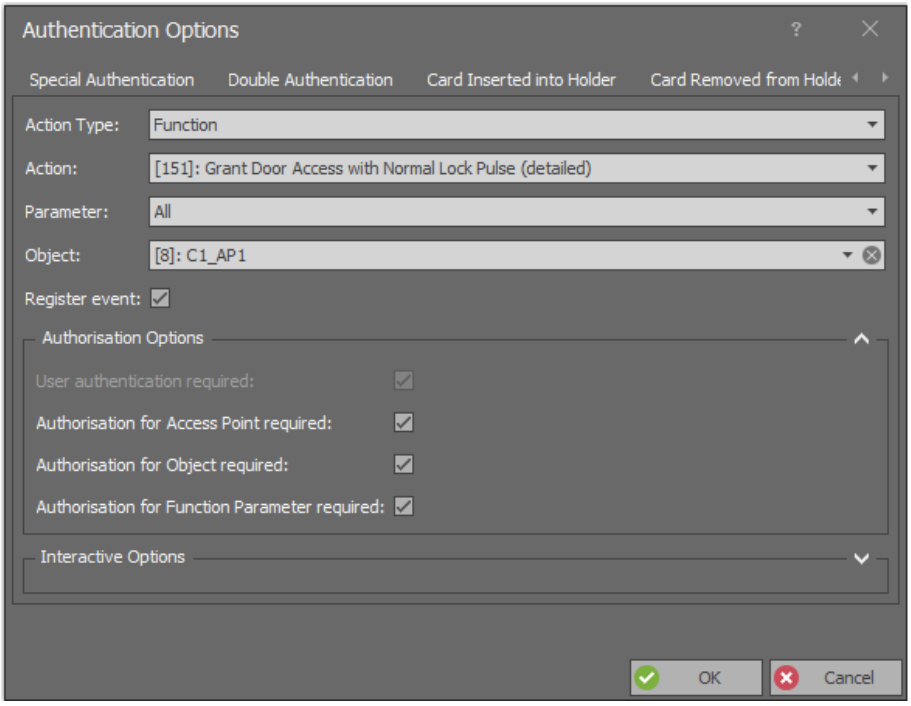
In RACS 5 system the authentication is a sequence of actions performed by user for the purpose of identification. Depending on current Authentication Policy at certain Access Point, a user is obliged to apply at least single Authentication Factor (card, PIN, fingerprint, etc.)

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.



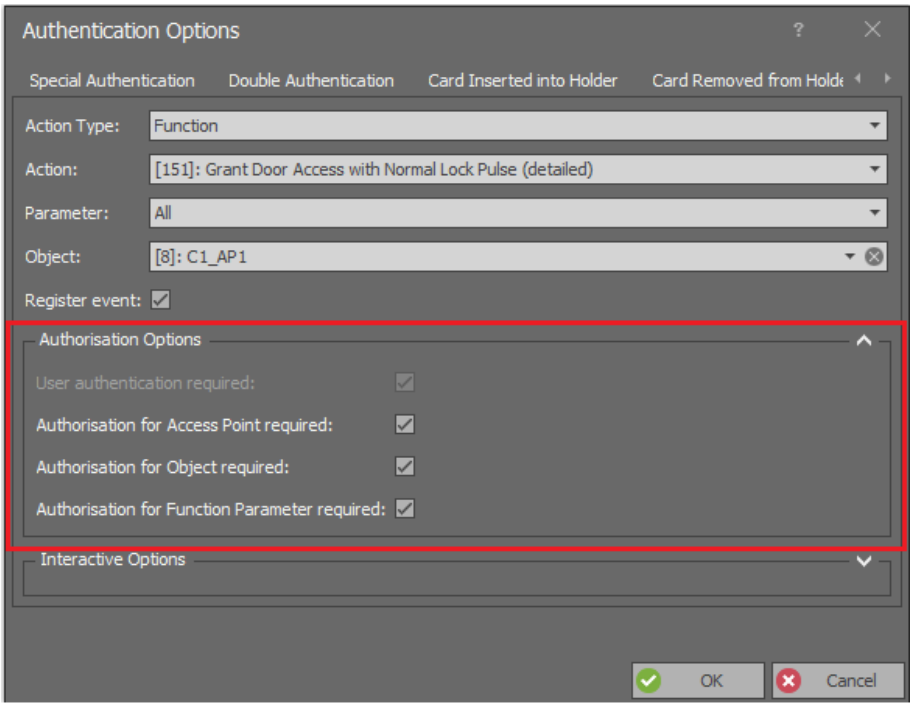
Authorisation Options

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:

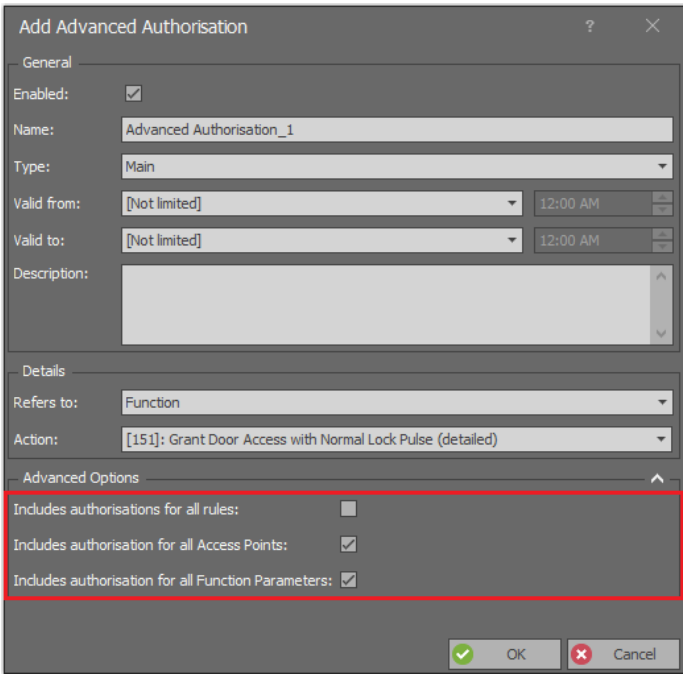
- Access Point (for each Authentication Option)
- Input line
- Function key
- Local Command functions

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

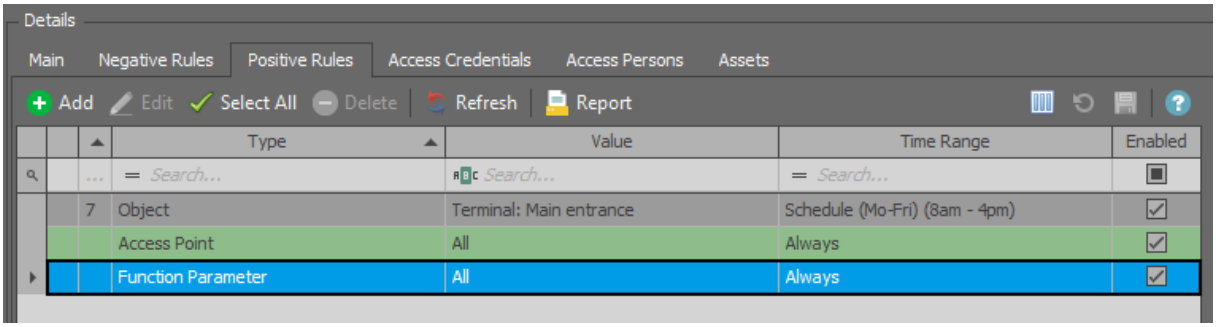


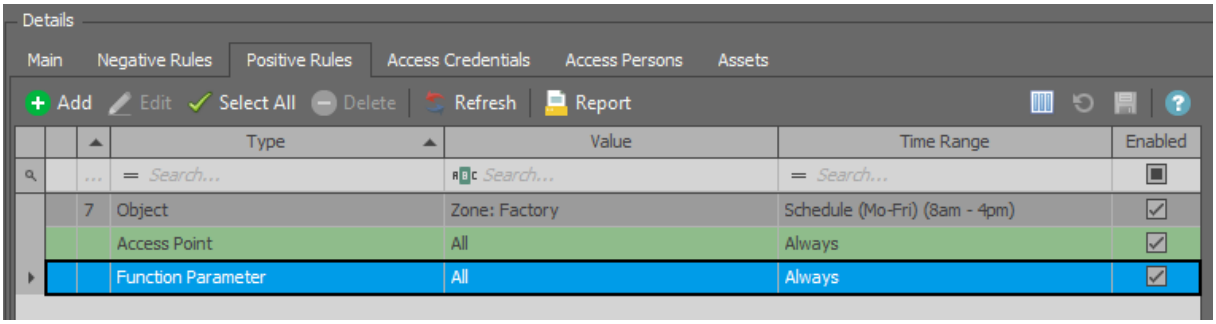
Advanced Authorisation for access

Access granting rights in RACS 5 system are usually defined by means of Authorisation to the function *[151]: Grant Door Access with Normal Lock Pulse (detailed)*. In typical case when the access is requested with Access Credential (e.g. card) at Access Points the option *Includes authorisation for all Access Points* can be enabled so it is not necessary to configure Detailed Rules concerning authentication at Access Points. Moreover if each Access Point is associated with single Access Door then the option *Includes authorisations for all Functions Parameters* can also be enabled so it will not be necessary to configure Detailed Rules in order to decide which Access Door can be opened at certain Access Point. Therefore when new Advanced Authorisation is created then both mentioned options by default are enabled and further configuration of Positive and Negative Rules concerns only Object i.e. Access Point or Access Zone where access can be granted.

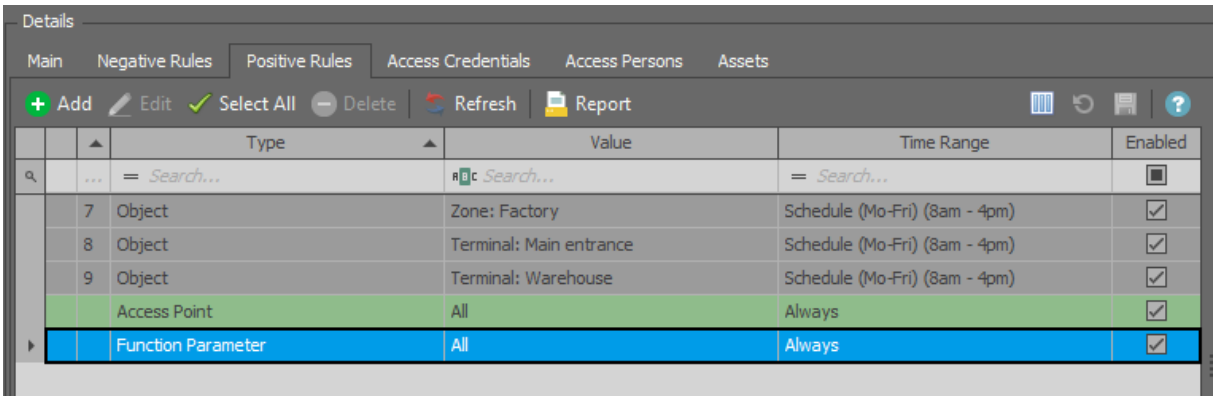


Usually in smaller systems individual Authorisations for each Access Point and/or Access Zone are created. In such case user access rights are defined by assignment of such Authorisations to Access Point and/or Access Zone where particular user is allowed to pass. Examples of such approach to access rights configuration are shown in figures below.





It is also possible to create complex Authorisations which enable access at various Access Points and/or Access Zones. In such case assignment of single Authorisation to a user may define all his access rights at once. The example of such approach is shown in figure below.



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