

# Roger Access Control System 5

Application note no. 004

Document version: Rev. D

## Access and Perimeter Zones

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

### *Introduction*

Access Zone in RACS 5 system is an area entered by users through Access Points (readers) called Entry Points and exited through Access Points called Exit Points. Additionally, Internal Points can be configured in order to control doors inside the Access Zone. Particular Access Point can be at the same time Entry Point of an Access Zone and Exit Point of another Access Zone and vice versa.

In general, Access Zones can cover large area with multiple Entry and Exit Points belonging to the same access controller. In opposite case the Access Zone can include single room with single door. Authorizations in RACS 5 can be assigned not only on the level of particular Access Points but also on the level of Access Zones and in such case the Authorizations enables access through any Entry Point of the zone.

Access Zones offer:

- Zone occupancy control and verification (occupancy upper and lower limits)
- Anti-Passback function
- Restriction and control of user movement between zones (neighboring zones)
- Additional access control at internal doors (Internal Points) which prevents tailgating.

Similarly to Access Zone, Perimeter Zone is an area with Entry Points, Exit Points and Internal Points which can be used for additional access control at internal doors of the zone. The functioning of Perimeter zones is ensured by RACS 5 communication service thus Perimeter Zones can include Access Points belonging to multiple access controllers.

---

Note: Functionalities on the level of Access Zone concern identification and counting of Access Credentials. If each user has not more than single Access Credential assigned then the functionalities in fact concern users.

Note: More information on additional quantitative access control with MC16-AZC access controller is given in AN031 application note.

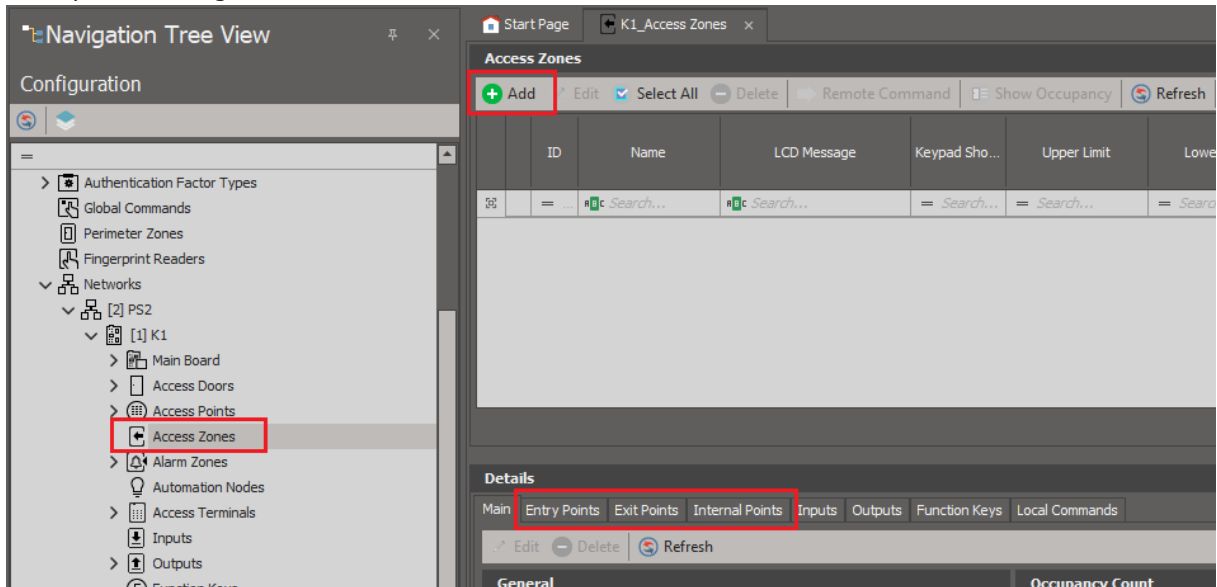
---

### *Access Zone configuration*

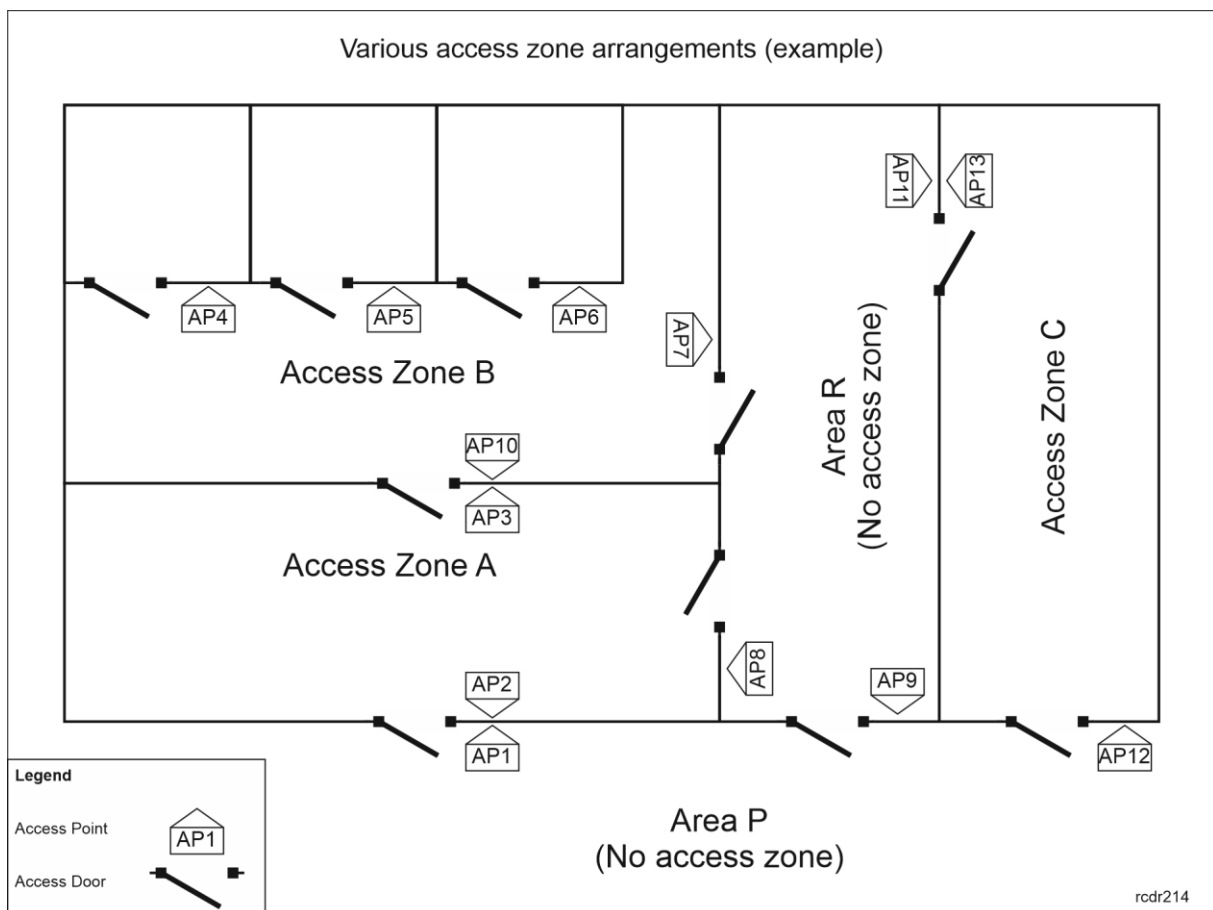
Access Zone is configured within particular access controller in following steps:

- In the navigation tree of VISO software double click *Access Zones* command.
- In the newly opened window click *Add*, enter zone name and then confirm with *OK* button.
- In the bottom, define Entry Points, Exit Points and optionally Internal Points assigning previously created Access Points. Access Points which include Access Terminals are usually defined when Access Doors are created using for example wizard from *VISO-> Wizards->Add Access Controller Wizard*.

- Upload settings to the controller.



The example of Access Zone arrangement is shown in figure below.



where:

- AP1 Access Point is Entry Point to Access Zone A.
- AP2 Access Point is Exit Point from Access Zone A.
- AP3 Access Point is Entry Point to Access Zone B.
- AP4, AP5, AP6 are Internal Points in Access Zone B.

- AP7 Access Point is Exit Point from Access Zone B.
- AP8 Access Point is Entry Point to Access Zone A.
- AP9 Access Point does not belong to any Access Zone.
- AP10 Access Point is Entry Point to Access Zone A and at the same time Exit Point from Access Zone B.
- AP11 Access Point is Entry Point to Access Zone C.
- AP13 Access Point is Exit Point from Access Zone C.
- AP12 Access Point is Entry Point to Access Zone C.
- Access Zone A and B are neighboring zones.
- Access Zone C is not neighboring for any other Access Zone.
- Areas R and P are not assigned to any Access Zone.

## Zone occupancy control and verification

The user who was granted access at Entry Point of Access Zone gains the status of user located inside the Access Zone. The user who was granted access at Exit Point of Access Zone gains the status of user outside the Access Zone. Such user could possibly enter another Access Zone if particular Exit Point is at the same time an Entry Point to another Access Zone.

The total number of users in Access Zone can be controlled. Occupancy limit can be enabled when Access Zone is created/edited. It is possible to define Upper limit and Lower limit, to define prealarms for both limits as well as to assign Occupancy Reset Schedule.

The screenshot shows the 'Add Access Zone' dialog box with the following fields:

- General**
  - Name: C1\_ACZ1
  - LCD Message:
  - Keypad Shortcut: No shortcut
  - Description:
- Occupancy Count** (highlighted with a red border)
  - Upper Limit: 65534
  - Lower Limit: 0
  - Upper Limit (Prealarm): None
  - Lower Limit (Prealarm): None
  - Occupancy Reset Schedule: None
- Anti-passback**
- Neighboring Options**

At the bottom, there are 'OK' and 'Cancel' buttons.

## Occupancy Upper and Lower limits

The parameter *Upper Limit* blocks the access for the next entering user when the total number of users inside the zone achieves the upper limit. The parameter *Lower Limit* blocks the access for the next exiting user when the total number of users inside the zone achieves the lower limit.

The upper limit is usually used on car park where the system is supposed to deny access for drivers when all places are occupied. The lower limit is usually used in locations where the presence of one or more persons is necessary all the time e.g. control room.

### Occupancy limit prealarms


Parameter *Upper Limit (Prealarm)* and parameter *Lower Limit (Prealarm)* are used to define warnings when the number of users inside the zone is getting close to respectively Upper Limit and Lower Limit. When prealarm limits are reached then outputs with functions [247]..[250] are activated and respective prealarm can be signalled acoustically or visually.

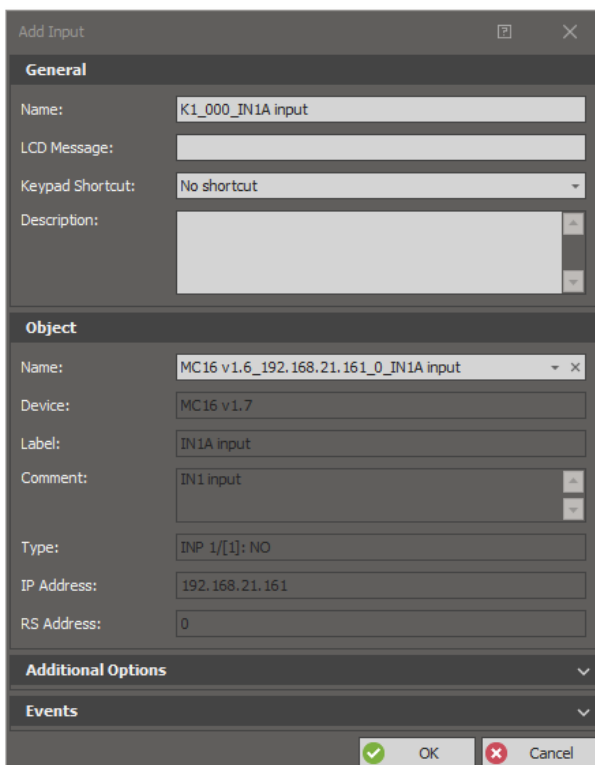
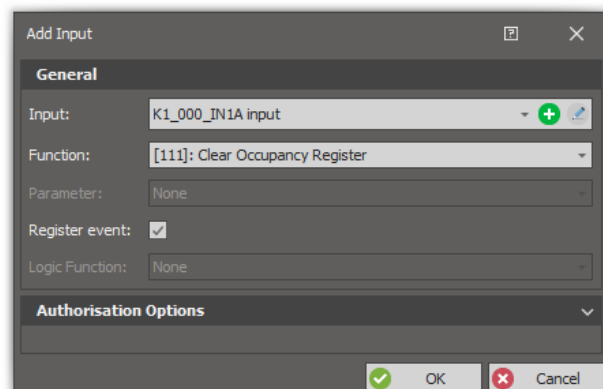
### Occupancy Count Reset Schedule

This schedule defines when Occupancy Register will be cleared for all Access Credentials inside the Access Zone. After reset, the controller counts occupancy in the zone from zero. Any *General Purpose Momentary* type schedule can be applied as reset schedule as it defines time stamps within a week when certain actions are to be executed by system. In this case the action would be Occupancy Register reset. All kinds of Schedules can be defined using the command *Schedules* in VISO software navigation tree.

### Occupancy Register reset with Input, Function Key or Local Command

Occupancy Register can be reset on demand using any input of controller and its peripheral devices or any function key at any reader equipped with keypad and connected to the controller. In order to define such input on the level of Access Zone:

- In the navigation tree of VISO software double click *Access Zones* command.
- In the opened window select one of previously created Access Zone.
- In the bottom select *Inputs* tab and then *Add*.
- In the opened window select  and then indicate the location of the input (e.g. IN1 on MC16 board). Close the window with OK button.
- Select the function *[111]: Clear Occupancy Register* and then close the window with OK button.
- Upload settings to the controller.

The configuration of function key for the same purpose is performed in similar way as configuration of the input but in the *Function Keys* tab of particular Access Zone.

Within particular Access Zone it is also possible to define Local Command with *[111]* function for the purpose of Occupancy Register reset. Local Command can be used as Authentication Option at Access Point and it can be activated with Access Credential (e.g. short, long or double card reading at selected reader). In order to use particular Local Command it is necessary to define and assign proper Advanced Authorization with *[111]* function to user(s).

---

Note: Occupancy Register reset additionally clears the APB Register.


---

### Occupancy Register reset with Remote Command

VISO software enables Occupancy Register reset with remote command. Such command can be called by right clicking any Access Zone in navigation tree or on map. Remote command can be used only by Operator with proper rights. Such rights are defined by assignment of Operator to Access User with Authorization(s) to function *[111]* at particular Access Zone(s). Such association of user and operator is done in the properties of user in the tab *Remote Management* in the field *Operator*. The most simple method to grant all Authorizations to operator is to assign such operator to user with Access Credential with enabled *Master exemption* option. More information on this subject is given in AN040 application note.

### Occupancy status signalling with Outputs

Occupancy Register state can be signalled using any output of controller and its peripheral devices. Outputs can be assigned with function *[52]..[57]* and *[247]..[252]* which are described in MC16 Operating Manual. In order to define output on the level of Access Zone:

- In the navigation tree of VISO software double click *Access Zones* command.
- In the opened window select one of previously created Access Zone.
- In the bottom select *Outputs* tab and then *Add*.
- In the opened window select  and then indicate the location of the output (e.g. OUT1 on MC16 board). Close the window with OK button.
- Select the required function and then close the window with OK button.
- Upload settings to the controller.

### Exemption of Access Credential from occupancy rules

Access Credential belonging to a user can be exempted from occupancy counting rules by selection of exemptions in its properties. In case of *Occupancy Count Exemption* option, user with such Access Credential is not included in Occupancy register when accessing the zone. In case *Occupancy Count Limit Exemption* option, user with such Access Credential is included in Occupancy register but Upper Limit and Lower limit do not affect such user. *Master Exemption* option includes all remaining exemptions and additionally gives all Authorisations in the system.

### Zones occupancy

In order to check current number of users in all Access Zones:

- In the navigation tree of VISO software double click *Access Zones* command.
- In the top select the button *Show Occupancy*.

ID	Name	Available	Occupied
4	C1_ACZ1	10	2
5	C1_ACZ2	20	0

The value in column *Available* depends on the parameter *Upper Limit*. The value in column *Occupied* depends on the current number of users inside the zone.

### Anti-passback function

Anti-passback (APB) prevents users from entering particular Access Zone again until they exit such zone. In other words APB prevents double access with the same Access Credential (e.g. card) at Entry Points of Access Zone and forces alternate use of particular Access Credential at Entry and Exit Points. Anti-passback functionality prevent unauthorized passing/exchanging of cards by users in order to access a zone multiple times with the same Access Credential. In practical applications, the APB can be used for example at chargeable car park.

APB functionality can be enabled when Access Zone is created/edited. It is possible to select APB Mode, APB Timeout and assign Activity Schedule as well as APB Reset Schedule.

**Add Access Zone**

**General**

Name: C1\_ACZ1

LCD Message:

Keypad Shortcut: No shortcut

Description:

**Occupancy Count**

**Anti-passback**

APB Mode: None

APB Timeout [min]: 0

APB Activity Schedule: None

APB Reset Schedule: None

**Neighboring Options**

OK Cancel

### APB Modes

Hard Anti-passback results in access denying when APB rules are violated and event is created when such violation occurs. Soft Anti-passback does not deny access when APB rules are violated and only event is created when such violation occurs.

### APB Timeout

APB Timeout is an option defining time for APB rules validity. When the timeout elapses then APB obligation expires and user can enter particular Access Zone again with the same Access Credential (e.g. card). Therefore, when the timeout is defined then APB obligation is cleared automatically after certain time for each user without operator intervention. This functionality enables APB using also at read-in doors.

### APB Activity Schedule

APB Schedule defines when APB rules are effective and enforced on users. Any *General Purpose Maintained* type Schedule can be defined with *Schedules* command in the navigation tree of VISO software and then applied for APB rules.

### APB Reset Schedule

This schedule defines when APB Register shall be cleared for all Access Credentials inside the Access Zone. After reset, the controller allows all users to enter Access Zone again despite of not using their Access Credentials at the exit. In practical applications such reset can be done at night in order to have APB rules restarted in the morning, especially for users who did not use their Access Credentials correctly on the exit the day before. Any *General Purpose Momentary* type Schedule can be applied as reset schedule as it defines time stamps within a week when certain actions are to be executed by system. In this case the action would be APB Register reset. All kinds of Schedules can be defined using the command *Schedules* in VISO software navigation tree.

### APB Register reset with Input, Function Key or Local Command

Input, function key and Local Command for APB Register reset are defined in the same way as in case of previously explained Occupancy Register reset. The only difference consists in the applied

function as [112]: *Clear Anti-passback Register* must be used instead of [111]: *Clear Occupancy Register*.

### APB Register reset with Remote command

APB Register reset with remote command is defined and used in the same way as in case of previously explained Occupancy Register reset. The only difference consists in the applied function as [112]: *Clear Anti-passback Register* must be used instead of [111]: *Clear Occupancy Register*.

### APB status signalling with Output

Output for signalling APB violation is defined in the same way as in case of previously explained outputs for occupancy. In such case the function [51] is applied.

### Exemption of Access Credential from APB rules

Access Credential belonging to a user can be exempted from APB rules by selection of *Anti-passback Exemption* option within its properties. *Master Exemption* option includes all remaining exemptions and additionally gives all Authorisations in the system.

The screenshot shows the 'Add Access Credential' dialog box. The 'General' tab is selected, displaying fields for Name (Access\_Credential5), Type (None), Belongs to (None), Valid from (None), and Valid to (None). Below these are three tabs: 'Additional Options', 'Exemptions', and 'Description'. The 'Exemptions' tab is active, showing a list of checkboxes: 'Master Exemption', 'Anti-passback Exemption', 'Occupancy Count Exemption', 'Occupancy Count Limit Exemption', and 'Perimeter Zone Exemption'. The 'Anti-passback Exemption' checkbox is highlighted with a red rectangle. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

### Restriction and control of user movements between zones

In RACS 5 system it is possible to limit user movements between neighboring Access Zones. Two Access Zones are considered neighboring when at least single Access Points (reader) is defined as Entry Point of the first zone and at the same time as Exit Point of the second zone or vice versa. Such neighboring zone control is enabled when Access Zone is created/edited by selection of one of blocking options.



**Add Access Zone**

**General**

Name:

LCD Message:

Keypad Shortcut:

Description:

**Occupancy Count**

**Anti-passback**

**Neighboring Options**

Do not allow to enter this zone from not neighboring zone: ☐

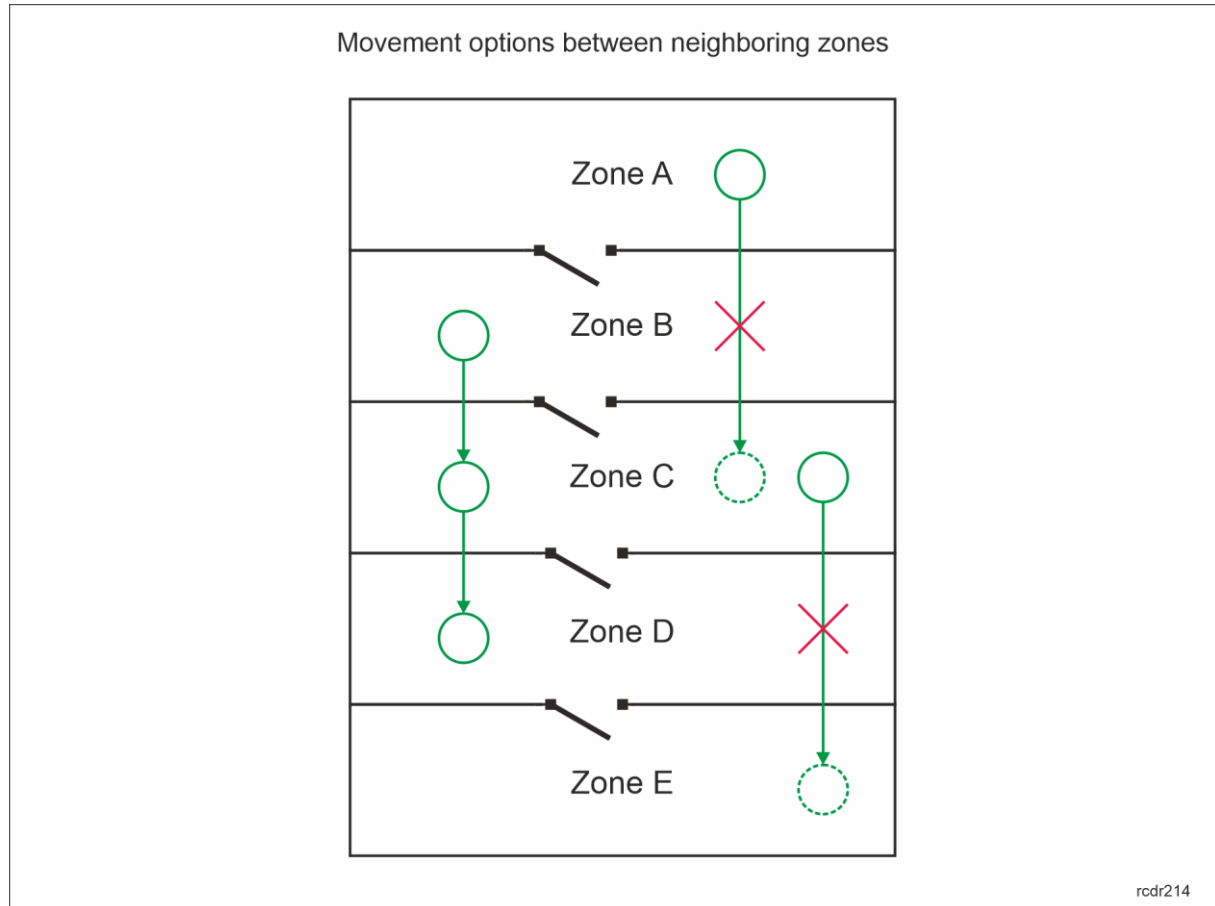
Do not allow to exit this zone to not neighboring zone: ☐

### Access Zone neighboring options

When the option *Do not allow to enter this zone from not neighboring zone* is enabled then the controller does not allow user to enter this zone if the zone left by such user is not the neighboring one.

When the option *Do not allow to exit this zone to not neighboring zone* is enabled then the controller does not allow user to exit this zone if the zone entered by such user is not the neighboring one.

## The concept of neighboring Access Zones



In the figure above when the option *Do not allow to enter this zone from not neighboring zone* is enabled for Zone C then it is not possible for user to move from Zone A to C but it is possible to move from Zone B to C.

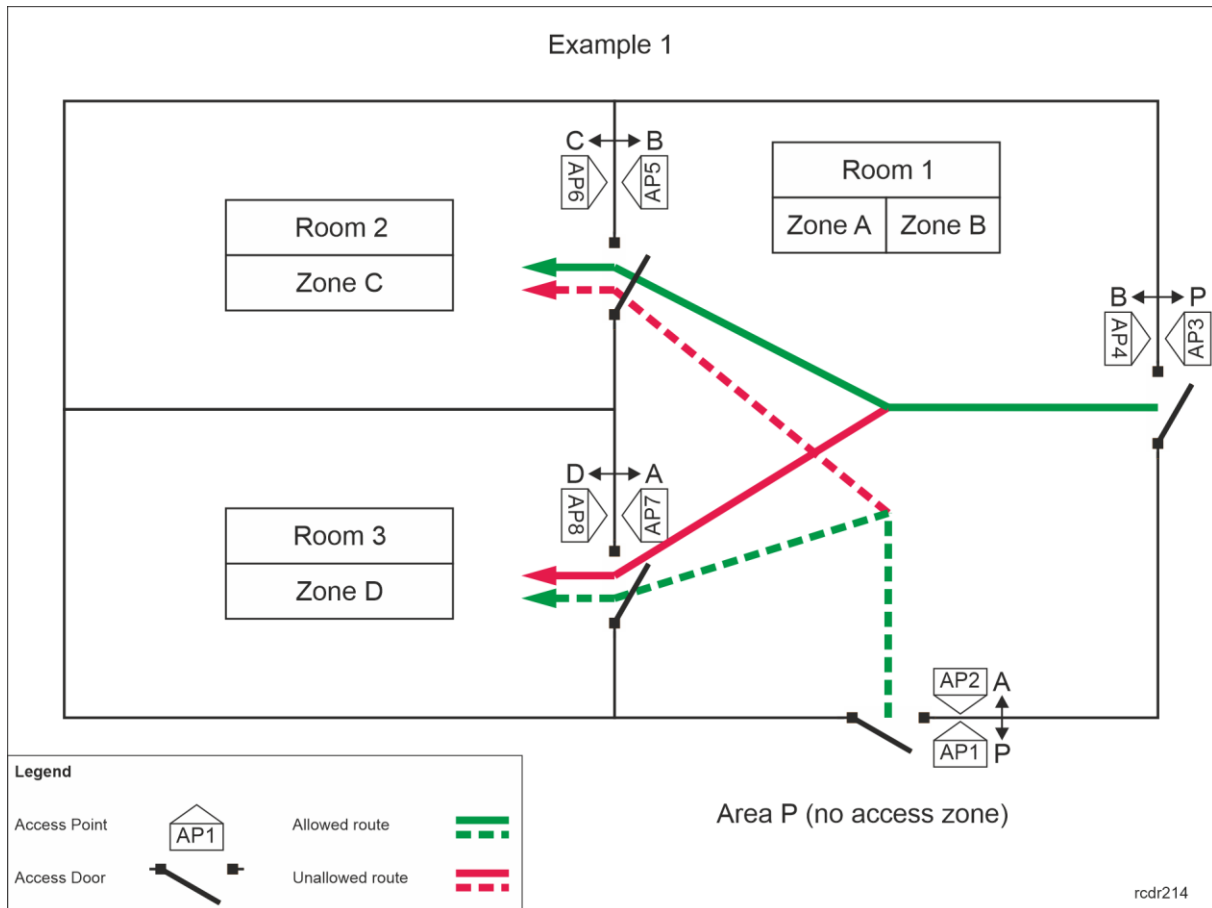
In the example above when the option *Do not allow to exit this zone to not neighboring zone* is enabled for Zone C then it is not possible for user to move from Zone C to E but it is possible to move from Zone C to D.

Neighboring options affect users only if they move between Access Zones. If user is moving from or to area not associated with any Access Zones then neighboring options are not effective. When the option *Occupancy Count Exemption* is enabled for particular Access Credential belonging to user then such user does not have to follow rules of neighboring zones.

In practical applications, neighboring zones enable restriction and enforcement of user movement apart from their Authorizations and according to operator defined routes and they can prevent users to avoid particular Access points of the system.

### Example 1

In the figure below, user with access Authorizations at all four doors who enters Room 1 using Access Point AP3 can enter Room 2 but cannot enter Room 3. If the same user enters Room 1 using Access Point AP1 then he can enter Room 3 but cannot enter Room 2. In this example, physical Room 1 is logically represented by Access Zone A and B with respectively AP1 and AP3 Entry Points.

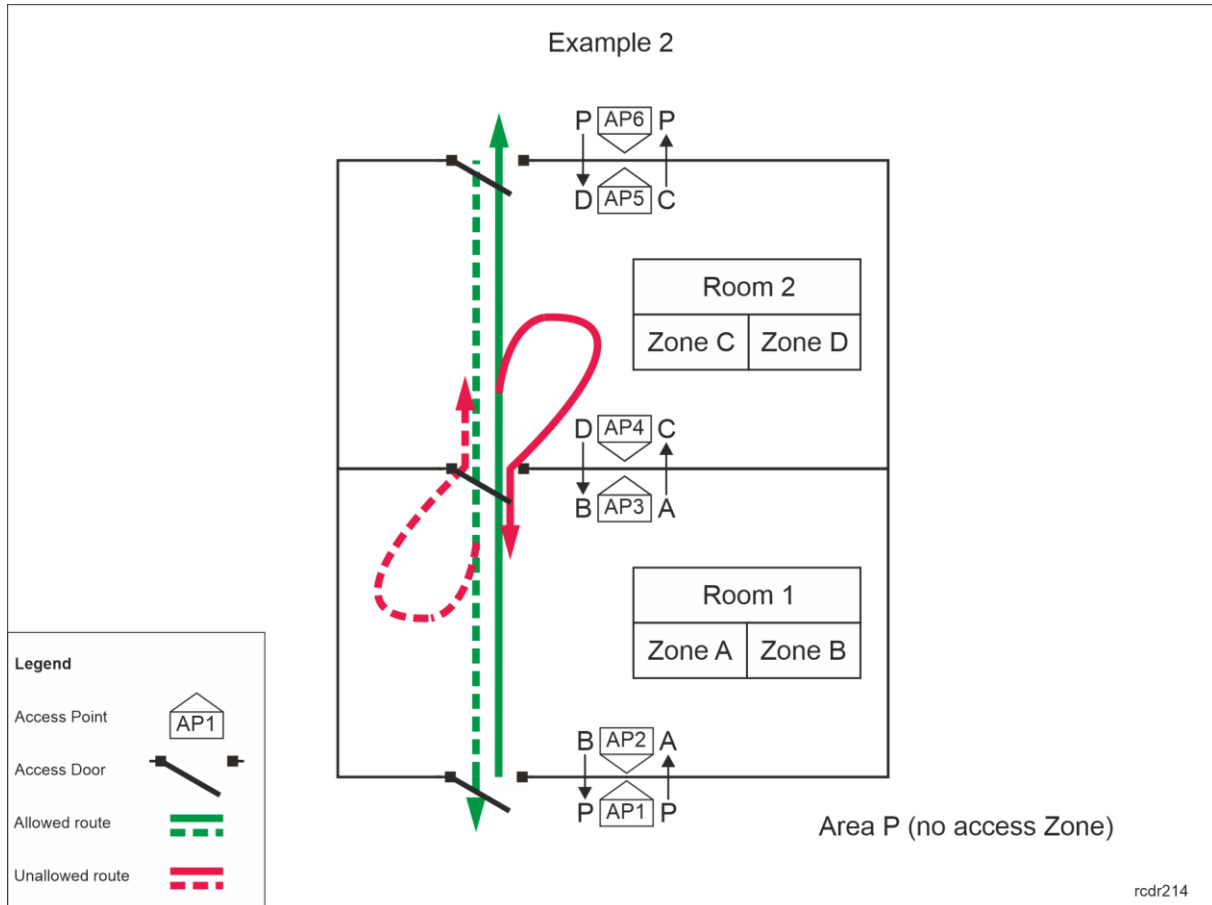


In order to configure movement restrictions in accordance with example 1:

- Create all four Access Doors with *Add Access Door Wizard* including all access Authorizations.
  - Enrol user with *Add Person Online* wizard assigning Authentication Factor(s) and all access Authorizations.
  - Create four Access Zones assigning:
    - AP1 and AP8 as Entry Points to Zone A.
    - AP2 and AP7 as Exit Points from Zone A .
    - AP3 and AP6 as Entry Point to Zone B.
    - AP4 and AP5 as Exit Points from Zone B.
    - AP5 as Entry Point to Zone C.
    - AP6 as Exit Point from Zone C.
    - AP7 as Entry Point to Zone D.
    - AP8 as Exit Point from Zone D.
- AP5 Access Point (as well as AP6) make Zones B and C the neighboring zones.  
 AP7 Access Point (as well as AP8) make Zones A and D the neighboring zones.  
 Zones A and C are not the neighboring zones.  
 Zones B and D are not the neighboring zones.  
 Zones A and B are not the neighboring zones.  
 Zones C and D are not the neighboring zones.
- Enable the option *Do not allow to enter this zone from not neighboring zone* for Zones C and D or enable the option *Do not allow to exit this zone to not neighboring zone* for Zones A and B. In the first case it is possible to leave the building through any door while in the second case the same door must be used for building entry and exit.
  - Upload settings to the controller.

## Example 2

In the figure below, user with access Authorizations at all three doors can only move forward regardless of starting point. When user enters Room 2 from Room 1 then he cannot return to Room 1 but he can proceed to Area P. When user enters Room 1 from Room 2 then he cannot return to Room 2 but he can proceed to Area P. In this example, physical Room 1 is logically represented by Access Zone A and B with respectively AP1 and AP4 Entry Points while physical Room 2 is logically represented by Access Zone C and D with respectively AP3 and AP6 Entry Points



In order to configure movement restrictions in accordance with example 2:

- Create all three Access Doors with *Add Access Door Wizard* including all access Authorizations.
- Enrol user with *Add Person Online* wizard assigning Authentication Factor(s) and all access Authorizations.
- Create four Access Zones assigning:
  - AP1 as Entry Point to Zone A.
  - AP3 as Exit Point from Zone A.
  - AP4 as Entry Point to Zone B.
  - AP2 as Exit Point from Zone B.
  - AP3 as Entry Point to Zone C.
  - AP5 as Exit Point from Zone C.
  - AP6 as Entry Point to Zone D.
  - AP4 as Exit Point from Zone D.

AP3 Access Point makes Zones A and C the neighboring zones.

AP4 Access Point makes Zones B and D the neighboring zones.

Zones A and D are not the neighboring zones.

Zones B and C are not the neighboring zones.

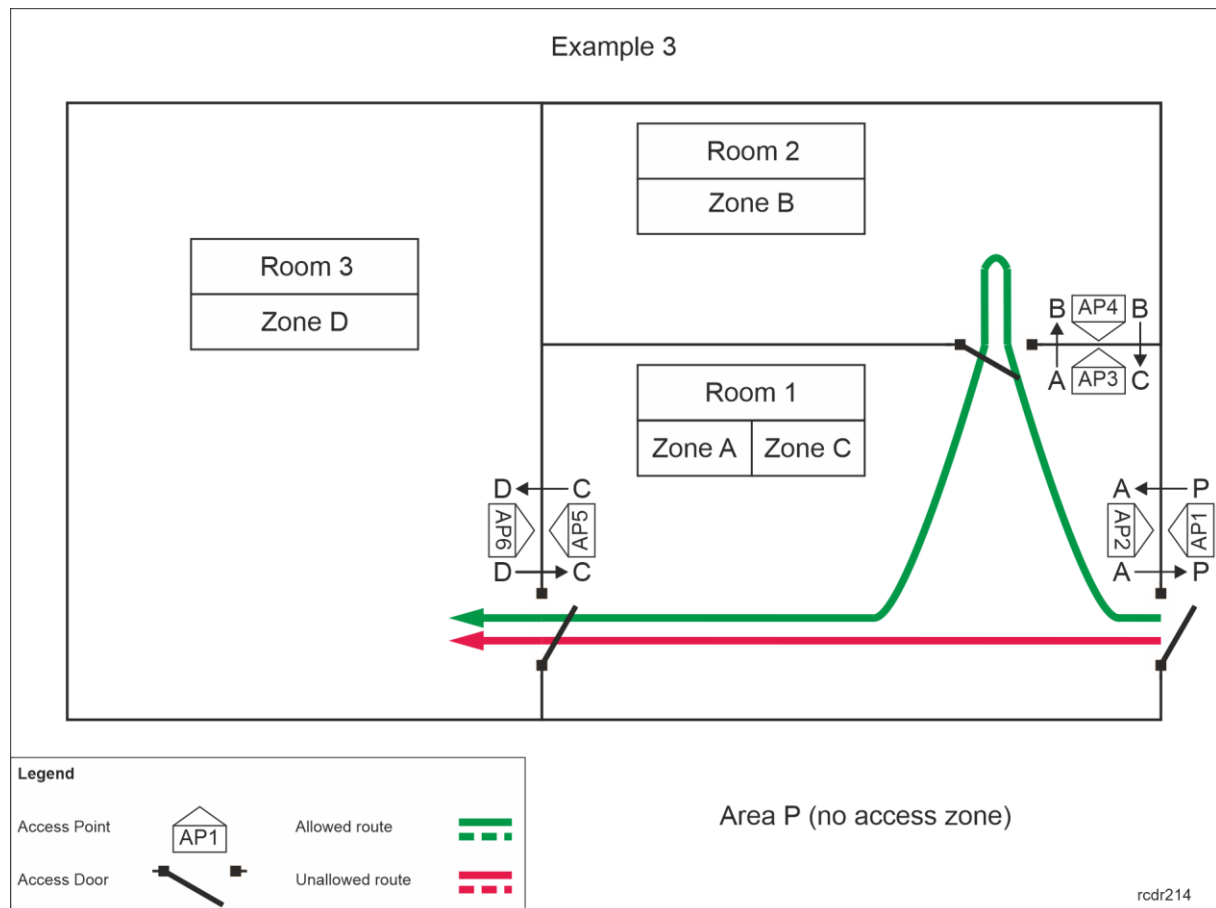
Zones A and B are not the neighboring zones.

Zones C and D are not the neighboring zones.

- Enable the option *Do not allow to enter this zone from not neighboring zone* for Zones B and C or enable the option *Do not allow to exit this zone to not neighboring zone* for Zones B and C. In both cases the result will be the same.
- Upload settings to the controller.

### Example 3

In the figure below, user with access Authorizations at all three doors can move to Room 3 only if Room 2 and specifically Access Point AP4 was visited previously. In this example, physical Room 1 is logically represented by Access Zone A and C with respectively AP1 and AP4 Entry Points.



In order to configure movement restrictions in accordance with example 3:

- Create all three Access Doors with *Add Access Door Wizard* including all access Authorizations.
- Enrol user with *Add Person Online* wizard assigning Authentication Factor(s) and all access Authorizations.
- Create four Access Zones assigning:
  - AP1 as Entry Point to Zone A.
  - AP2 and AP3 as Exit Points from Zone A.
  - AP3 as Entry Point to Zone B.
  - AP4 as Exit Point from Zone B.
  - AP4 and AP6 as Entry Points to Zone C.
  - AP5 as Exit Point from Zone C.
  - AP5 as Entry Point to Zone D.
  - AP6 as Exit Point from Zone D.

AP3 Access Point makes Zones A and B the neighboring zones.

AP4 Access Point makes Zones B and C the neighboring zones.

AP5 Access Point (as well as AP6) make Zones C and D the neighboring zones.

Zones A and D are not the neighboring zones.

Zones B and D are not the neighboring zones.

Zones A and C are not the neighboring zones.

- Enable the option *Do not allow to enter this zone from not neighboring zone* for Zone D.
- Upload settings to the controller.

### ***Additional access control at internal doors***

Access Zone definition requires configuration of Entry Points and Exit Points. Additionally, Internal Points can be specified in order provide additional access control at internal door. Regardless of their Authorizations users cannot be granted access at Internal Points of particular Access Zone if they are not inside such zone i.e. they were not granted access at any Entry Point of such zone. In practical applications Internal Points can be used to prevent users with Authorizations to avoid identification at Entry Points (e.g. tailgating) as such Entry Points can be used for additional functionalities e.g. Time&Attendance.

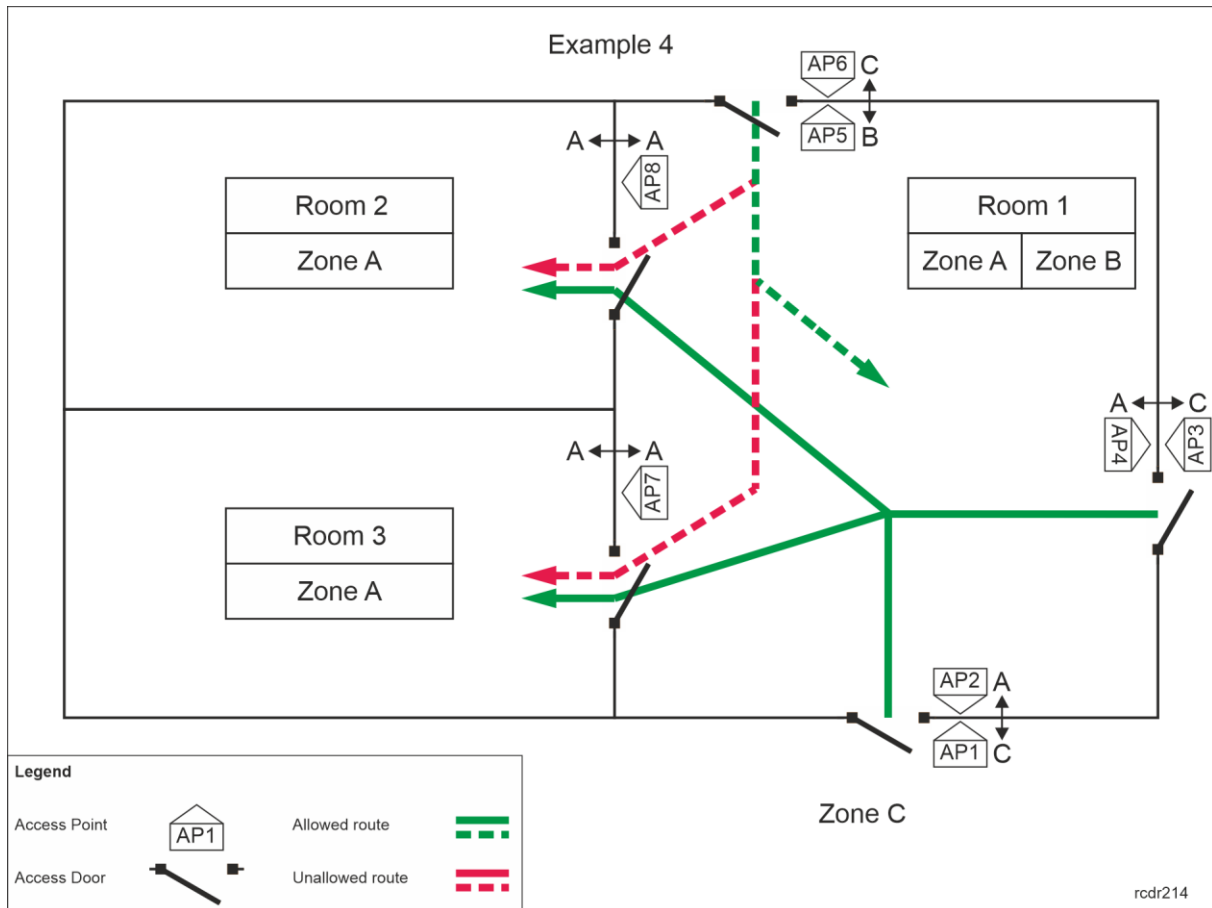
Internal Points are defines in the same way as Entry Points and Exit Points of Access Zone i.e. by selection and assignment of already created Access Points in the system. Internal Points affect users only if they move between Access Zones. If user is moving from or to area not associated with any Access Zones then Internal Point requirement is not effective. When the option *Occupancy Count Exemption* is enabled for particular Access Credential belonging to user then such user does not have to follow rules of Internal Points.

#### **Example 4**

In the figure below, user with access Authorizations at all four doors can move to Room 2 and Room 3 only if Room 1 was entered with Access Points AP1 or AP3. In this example Access Points AP7 and AP8 are Internal Points of Access Zone A. Therefore they can be accessed only if user properly entered Access Zone A (no tailgating). Additionally, when user identifies at Access Point AP6 then Access Zone B is entered so access at AP7 and AP8 is denied as well.

In order to configure movement restrictions in accordance with example 4:

- Create all five Access Doors with *Add Access Door Wizard* including all access Authorizations.
- Enrol user with *Add Person Online* wizard assigning Authentication Factor(s) and all access Authorizations.
- Create three Access Zones assigning:
  - AP1 and AP3 as Entry Points to Zone A.
  - AP2 and AP4 as Exit Points from Zone A.
  - AP7 and AP8 as Internal Points in Access Zone A.
  - AP6 as Entry Point to Zone B.
  - AP5 as Exit Point from Zone B.
  - AP2, AP4 and AP5 as Entry Points to Zone C.
  - AP1, AP3 and AP6 as Exit Points from Zone C.
- Upload settings to the controller.

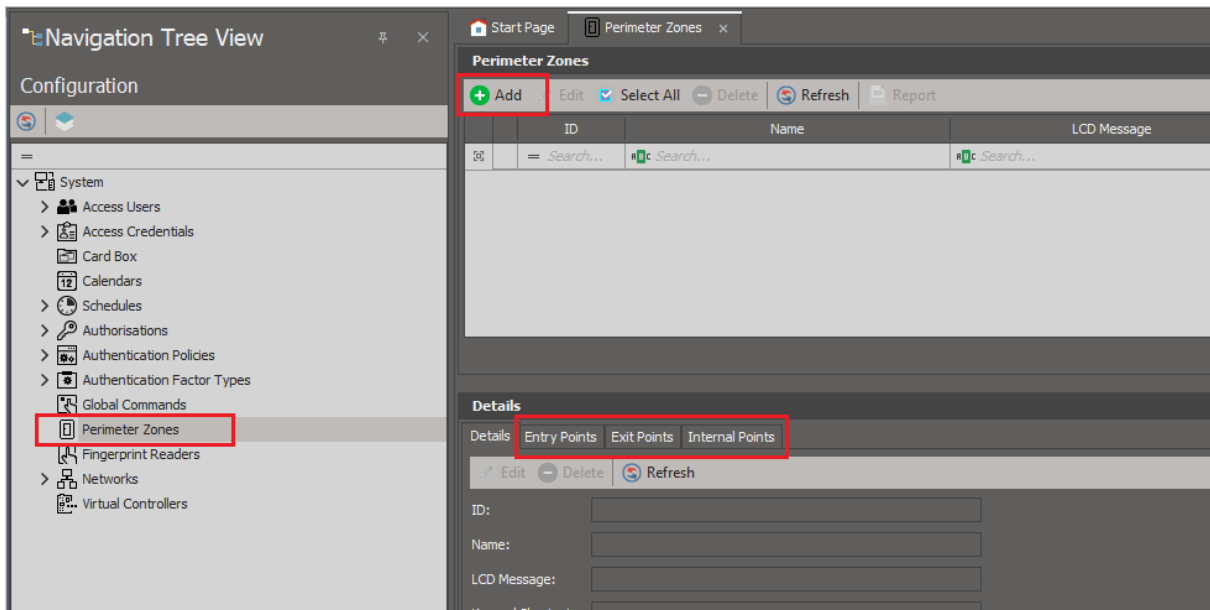


## Perimeter Zones

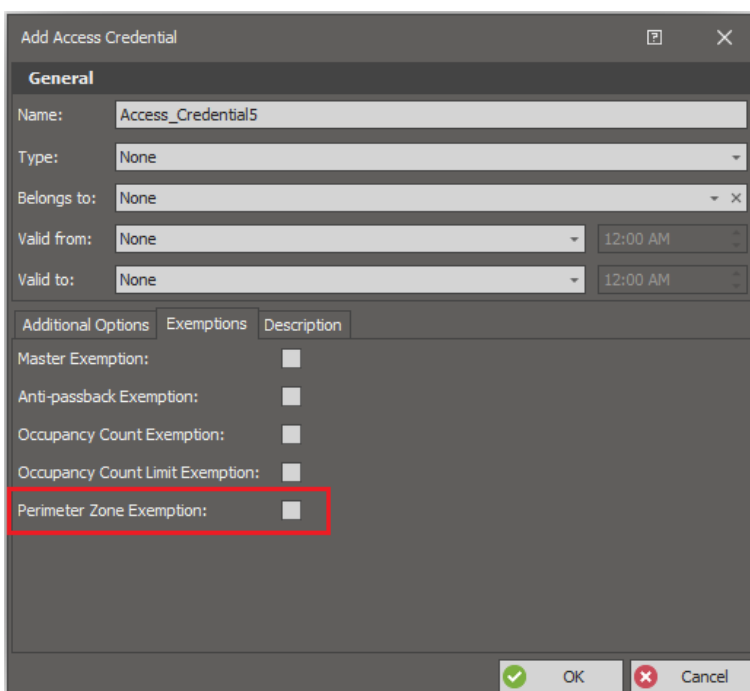
Perimeter Zones similarly to Access Zones include Entry Points, Exit Points and Internal Points and they offer the same functionality of additional access control at internal door as Access Zone which means that regardless of their Authorizations users cannot be granted access at Internal Points of particular Perimeter Zone if they are not inside such zone i.e. they were not granted access at any Entry Point of such zone. As opposed to Access Zones, Perimeter Zones functionality is provided by RACS 5 Communication Service of RogerSVC software. Perimeter Zone can cover area with Access Points from multiple access controllers connected to Ethernet network and communicating with the service.

In order to configure Perimeter Zone:

- Create all necessary Access Doors with *Add Access Door Wizard* including all necessary Access Authorizations.
- Enrol user(s) with *Add Person Online* wizard assigning Authentication Factor(s) and all Authorizations.
- In the navigation tree of VISO software double click *Perimeter Zones* command with left mouse button.
- In the newly opened window select *Add* button, name the zone and confirm with *OK* button.
- In the bottom part of window define, Entry Points, Exit Points and Internal Points assigning previously created Access Points.



Access Credential belonging to a user can be assigned exemption for rules governing the Perimeter Zone. This is enabled by means of the option *Perimeter Zone Exemption* in the properties of particular Access Credential. *Master Exemption* option includes all remaining exemptions and additionally gives all Authorisations in the system.





**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](mailto:support@roger.pl)**  
**Web: [www.roger.pl](http://www.roger.pl)**