Roger Access Control System 5

Application note no. 052

Document version: Rev. A

PIN numbers

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

Introduction

Various types of Authentication Factors can be applied in RACS 5 system to identify users. The most commonly used are proximity cards and PINs which are numbers entered on the keypad of terminal/reader in access control system.

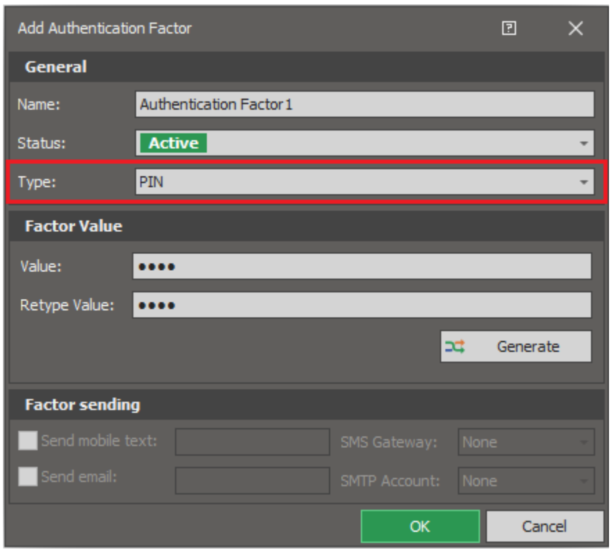
Low level configuration

Some of PIN settings are available on the level of keypad terminals/readers. According to their installation manuals, low level configuration can be conducted with RogerVDM software or VISO v2 software. Following parameters can be configured:

Parameter	Default value	Description
Time between keys in PIN [s]	10	Parameter defines max. time between two consecutive key pressings.
Single key press	Yes	Parameter enables separate transmission of each pressed key to controller.
PIN followed by [#] key	Yes	Parameter enable use of PINs with variable length. In such scenario PIN is concluded with [#] key.
Min. length of PIN	4	Parameter defines the minimal number of digits for PIN entered with keypad. If the number of entered digits is lower that this parameter then it cannot be sent to controller when concluded with [#] key. When set to 0 then PINs are disabled.
Max. length of PIN	8	Parameter defines the maximal number of digits for PIN entered with keypad. If the number of entered digits reaches this parameter then PIN is automatically sent to controller and [#] key pressing is not necessary. When set to 0 then automatic PIN transmission is disabled.

PIN defining

PINs and other types of Authentication Factors are usually defined when user is added using one of available methods. More information on user management is given in AN051 application note.



Add Authentication Factor

General

Name: Authentication Factor 1

Status: Active

Type: PIN

Factor Value

Value: ••••

Retype Value: ••••

Random PIN generating

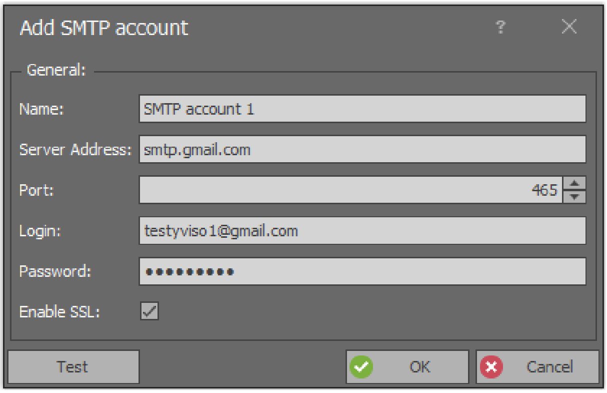
VISO management software enables to generate random PIN using *Generate* button when PIN is defined. According to default settings in VISO software, the random PIN consists of 4 digits. This can be changed after selection of *Tools* in the top menu of VISO and then *System Options* where following parameters are available:

Parameter	Default value	Description
PIN fixed length	Yes	When option is enabled then fixed length for random PIN can be defined.
PIN digits	4	The parameter specifies fixed number of digits for randomly generated PINs.

PIN sending

PIN which was defined for a user can be immediately sent to such user via email or mobile text (SMS). In such case it is necessary to define SMTP Account and/or SMS Gateway. In order to define PIN sending by email:

- In the top menu of VISO software select *Tools* and then *SMTP Accounts*.
- In the opened window enter parameters of your SMTP account and server as in example below.



Add SMTP account

General:

Name: SMTP account 1

Server Address: smtp.gmail.com

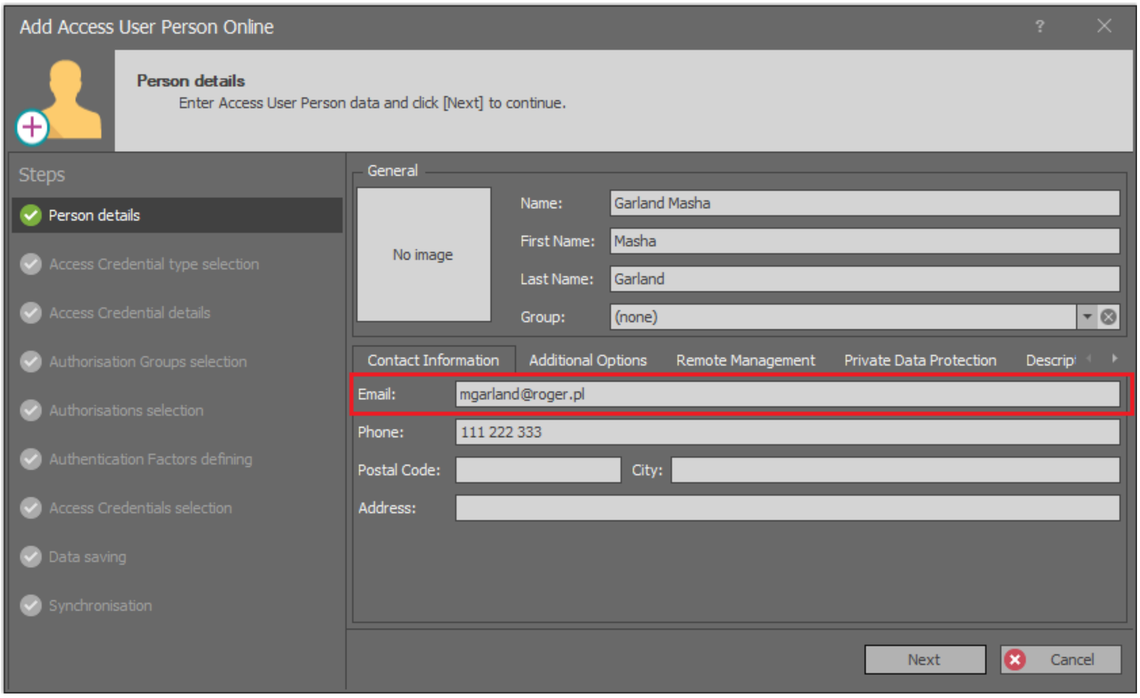
Port: 465

Login: testyviso1@gmail.com

Password: •••••••••

Enable SSL: ☑

- When Person is defined by means of *Add Person Online* wizard then define email address where later PIN will be sent.

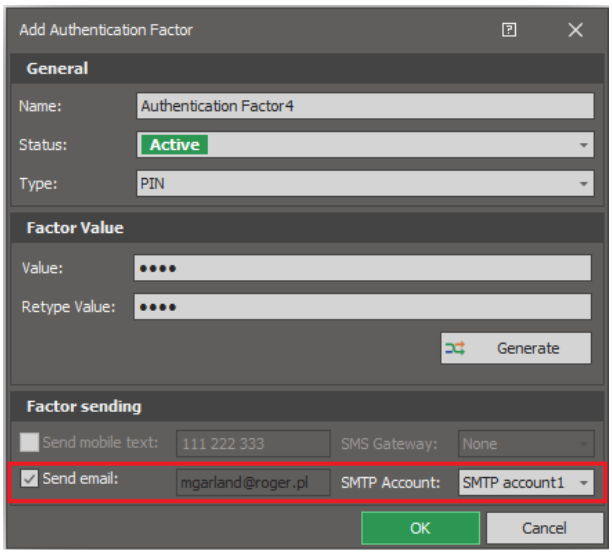


Add Access User Person Online

Person details
Enter Access User Person data and click [Next] to continue.

Name: Garland Masha
First Name: Masha
Last Name: Garland
Group: (none)
Email: mgarland@roger.pl
Phone: 111 222 333
Postal Code:
City:
Address:

- When PIN type Authentication Factor is defined then select *Send* in order to send the PIN by email.



Add Authentication Factor

General
Name: Authentication Factor4
Status: Active
Type: PIN

Factor Value
Value: ••••
Retype Value: ••••

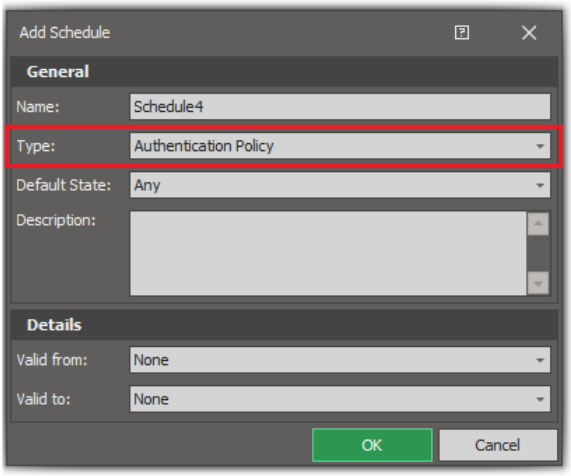
Factor sending
□ Send mobile text: 111 222 333 SMS Gateway: None
☑ Send email: mgarland@roger.pl SMTP Account: SMTP account1

Similarly, PIN can be sent via mobile text (SMS) and in such case SMS Gateway must be defined and phone number must be entered for a Person.

Multistep authentication

RACS 5 system enables multistep authentication of users. The most popular mode of such authentication is Card and PIN. When it is configured at particular Access Point (reader) then it is necessary to use not only card but also PIN to activate a function (e.g. access granting) at a reader. The sequence is irrelevant.

Authentication Mode can be configured permanently at Access Point or it can be changed based on schedule which can be defined by selection of *Schedules* in the navigation tree of VISO software. In such case the schedule must be *Authentication Mode* type. It is also possible to define own Authentication Modes.



Add Schedule

General

Name: Schedule4

Type: Authentication Policy

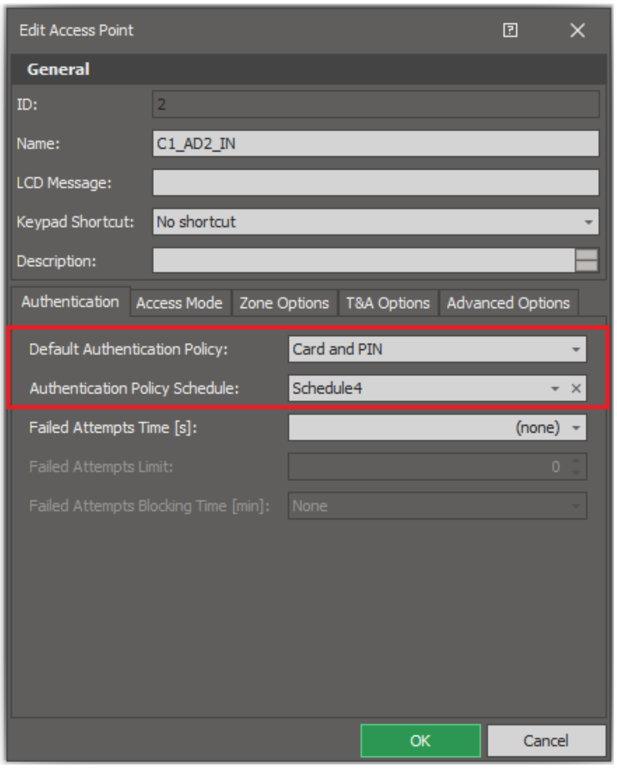
Default State: Any

Description:

Details

Valid from: None

Valid to: None



Edit Access Point

General

ID: 2

Name: C1_AD2_IN

LCD Message:

Keypad Shortcut: No shortcut

Description:

Default Authentication Policy: Card and PIN

Authentication Policy Schedule: Schedule4

Failed Attempts Time [s]: (none)

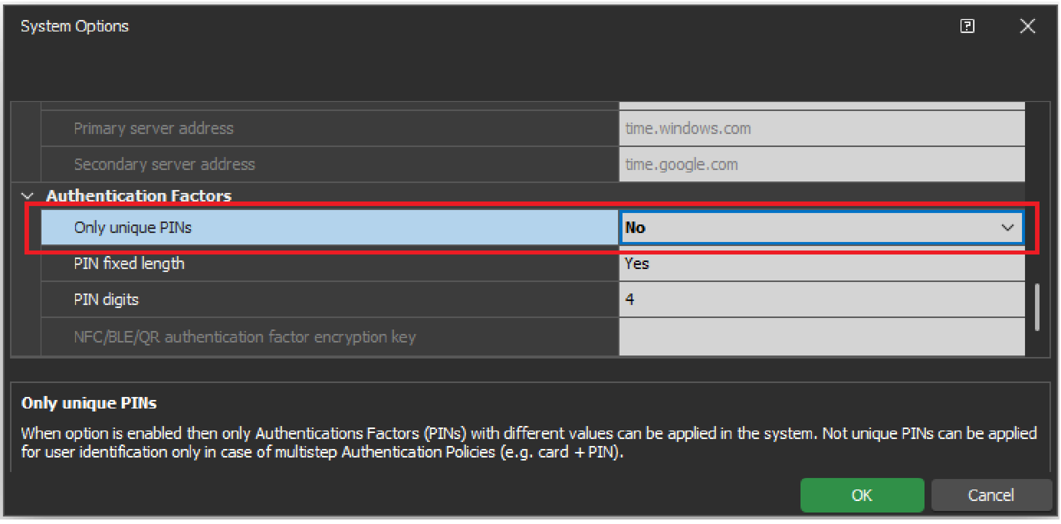
Failed Attempts Limit: 0

Failed Attempts Blocking Time [min]: None

Secret and not unique PINs

In general perspective PINs in RACS 5 system must be unique. When already occupied PIN is assigned to user then warning is generated by VISO and such PIN cannot be added.

However in case of multistep authentication it is possible to use non unique PINs. This functionality can be applied when users are supposed to define their PINs by themselves in such way that even the administrator does not know them. At the same time when user defines own PIN there shouldn't be any warning that particular PIN is already taken. On the other hand in case of multistep authentication such as Card and PIN still the pair of Authentication Factors is still unique and user can be identified by the system. In case of non-unique PINs the sequence is relevant and PIN cannot be entered within the first step. Non-unique PINs can be enabled in the window which is opened after selection of *Tools* in the top menu of VISO software and then *System Options*.



System Options

Primary server address: time.windows.com

Secondary server address: time.google.com

Authentication Factors

Only unique PINs: No

PIN fixed length: Yes

PIN digits: 4

NFC/BLE/QR authentication factor encryption key:

Only unique PINs

When option is enabled then only Authentications Factors (PINs) with different values can be applied in the system. Not unique PINs can be applied for user identification only in case of multistep Authentication Policies (e.g. card + PIN).

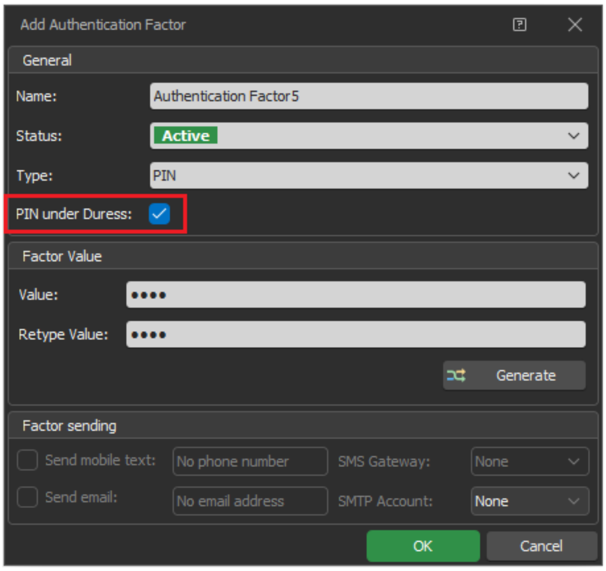
PINs under duress

PIN under duress can be applied when a user is under duress and wants to start silent alarm during access granting. In normal conditions such user enters normal PIN while in alarm situation the user can enter PIN under duress. When PIN under duress is used then not only access is granted (if user is equipped with adequate access rights) but also the event *[9]: PIN under Duress* is registered in the system. Various automatic actions can be defined for such event such as:

- Email or mobile text (SMS) sending to selected recipients (AN041 application note)
- Global Command starting and such command can for example activate siren in security personnel room (AN048 application note)
- Signalling in VISO SMS Security Management System (AN055 application note)

In order to define PIN under duress for existing Person:

- In the top menu of VISO software select *Configuration* and then *Access Credentials*.
- In the opened window select the Access Credential belonging to particular Person and then in the bottom select *Authentication Factors* tab.
- Select *Add* and enable the option *PIN under Duress* when PIN is defined.



Name: Authentication Factor5

Status: Active

Type: PIN

PIN under Duress: ☑

Value: ••••

Retype Value: ••••

□ Send mobile text: No phone number SMS Gateway: None

□ Send email: No email address SMTP Account: None

- Synchronise settings of the system.

PIN under duress can also be defined when new user is created by means of Add Person Online wizard or existing user is edited by means of Edit Person Online wizard.

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