

Roger Access Control System

RCC512 Operating Manual

Product version: 1.x

App version: 1.7

Document version: Rev. F

Contents:

1.	Design and application	3
2.	Characteristics	4
3.	Power supply	4
4.	RS485 bus	4
5.	Ethernet interface	5
6.	MD70 panel	5
7.	Identification	5
8.	Other proximity cards and biometrics	5
9.	MCX8 expanders	5
10.	Installation	6
11.	Installation and use guidelines	7
12.	RAACA app	8
13.	Configuration in standalone mode	14
14.	Configuration via web browser	16
15.	Configuration in network mode	16
16.	Management and general issues	16
17.	Troubleshooting	18
18.	Specification	18
19.	Ordering information	19
20.	Product history	19

This document is subject to the Terms of Use in the current version published on the website www.roger.pl. The manufacturer reserves the right to make changes to this product without prior notice. The product communicates only with another network device using a non-Internet-compatible communication protocol.

1. DESIGN AND APPLICATION

RCC512 cabinet controller enables electronic access control to cabinets, lockers, containers etc. Cabinets are connected to the controller through MCX8-BRD I/O expanders. Each expander allows you to connect 8 cabinets. Depending on the number of the RCC512-1C-LIC licenses purchased, the cabinet controller can support up to 512 cabinets. Access to cabinet is controlled by an electric lock. Optionally, the cabinet can be equipped with an opening sensor. The controller can work in the following modes:

- Pool cabinets
- Personal equipment
- Personal cabinets
- Post boxes
- Toolboxes
- Storage box
- Drop box mode

The RCC512 controller can be managed from the touch control panel or remotely from a web browser. Remote management is performed via LAN (Ethernet).

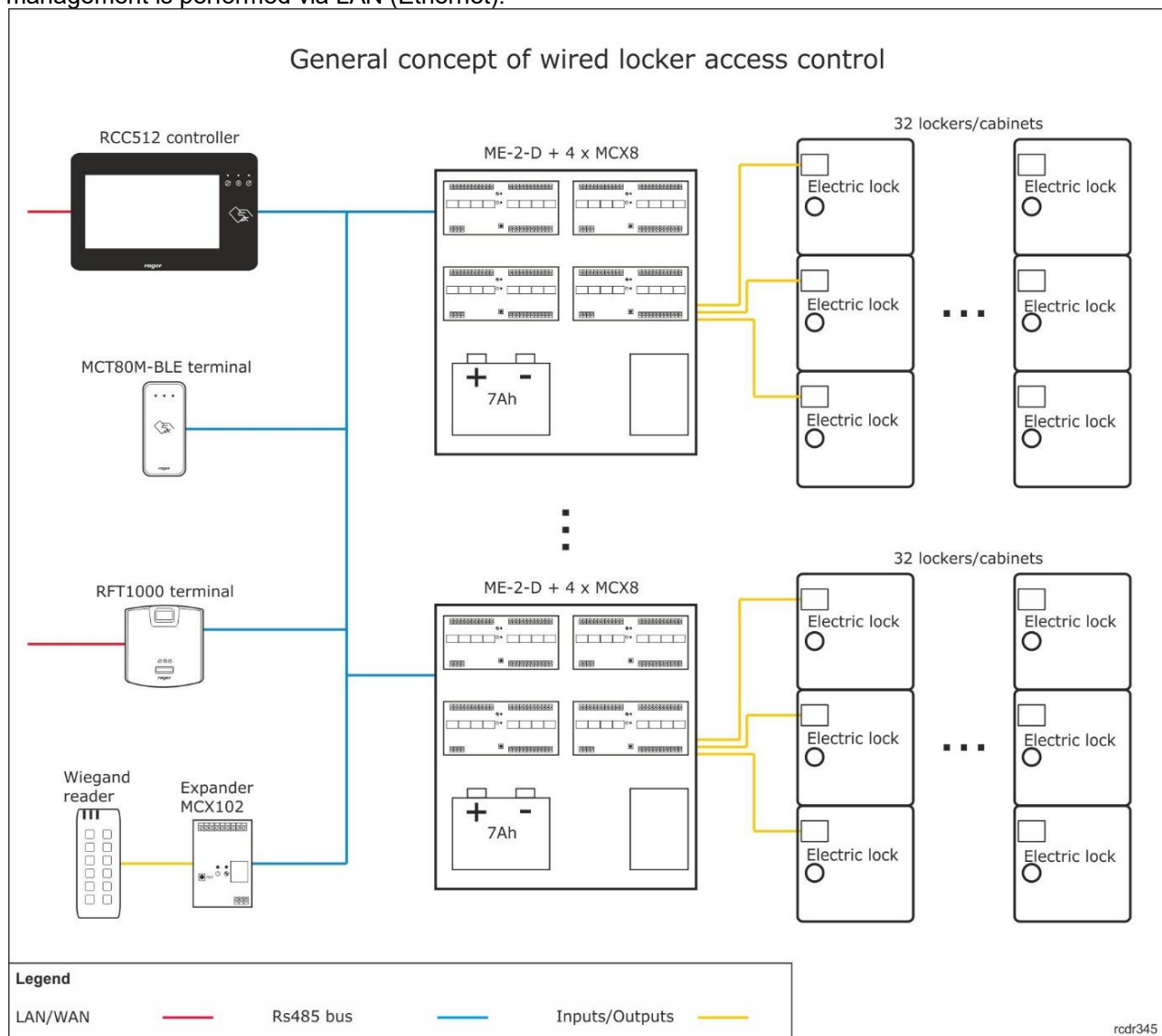


Fig. 1 Typical connection with the RCC512 controller

The user can log in from the RCC512 controller or external MCT series readers (Roger). In the latter case, each reader can control access to a zone of 32 lockers associated with it. System users are identified by means of a proximity card and/or a PIN code. An external identification reader with Wiegand or RS485 (Roger) interface can be connected to the control panel. This reader can be used as a replacement or together with the proximity reader built into the control panel. In particular, the RFT1000 (Roger) fingerprint reader or the MCT80M-BLE reader for identification via a mobile phone can be connected to the control panel.

2. CHARACTERISTICS

- Stand-alone operation
- Local management using controller touch screen
- Remote management using web browser
- Support for up to 512 cabinets, depending on the number of purchased RCC512-1C-LIC licenses
- Groups of cabinets with assigned reader
- Interface for electric lock and door open sensor
- Cabinet assigned to the user (e.g., employee lockers)
- Cabinet assigned on-demand (e.g., pool cabinets)
- Operation in 1:N mode (multiple users assigned to one cabinet, e.g. mailboxes)
- Operation in N:N mode (multiple users with access to multiple cabinets, e.g. toolboxes)
- Operation in the Storage Mode (e.g., deposit lockers in shopping centres)
- Operation in the Parcel Drop Box mode
- 7" touch control panel
- Built-in EM125kHz and ISO/IEC 14443A / MIFARE® Ultralight, Classic, DESFire EV1 Plus card reader
- External reader with Wiegand or RS485 Roger interface
- Event logging and system operation reporting
- LAN communication interface (Ethernet)
- SDK for authorized integrators
- 12V power supply
- Post-warranty service and availability of spare parts for 10 years

3. POWER SUPPLY

The RCC512 controller requires a 12VDC buffer power supply with a current capacity of 1A. The power supply is connected directly to the controller terminals (fig. 4). The controller does not support the battery, so the emergency power supply (battery, UPS) should be provided at the level of the buffer power supply. When selecting the battery capacity or UPS power, the required system operation time after the loss of the main power supply as well as the number of powered devices should be considered.

MCX8 expanders and optional partition readers, e.g., MCT80M-BLE, require 12VDC power supply. For more information on powering these devices, see their manuals. It is recommended to install the MCX8 expanders in the ME-2-D enclosures, which are equipped with a suitable power supply and allow the installation of the battery.

4. RS485 BUS

Communication between the controller and peripheral devices is provided by the RS485 bus, to which a total of 64 MCX8 expanders and additional 16 identification terminals, e.g., MCT80M-BLE, can be connected. Expanders must have addresses in the ranges 100 - 115, 200 - 215, 300 - 315 and/or 400 - 415. Terminals must have individual addresses in the range 800 - 815. The RS485 bus can be freely shaped using star and tree topologies as well as their combinations. However, loop topology is not allowed. It is not required to use terminating resistors at the ends of transmission lines of the RS485 communication bus. In most cases, communication works without problems with all types of cable (ordinary telephone cable, shielded or unshielded twisted pair), but unshielded twisted pair cable (U/UTP cat. 5) is preferred. The use of shielded cables should be limited to installations exposed to strong electromagnetic interference. The RS485 transmission standard used in the RCC512 system guarantees correct communication over up to 1200 meters (calculated along the cable) and is characterized by high resistance to interference.

Note: Do not use more than one pair of wires in a UTP cable for RS485 communication.

5. ETHERNET INTERFACE

The Ethernet interface of the RCC512 controller is used for configuration via a web browser.

6. MD70 PANEL

Management of RCC512 is performed by means of MD70 panel with graphic touch screen, sounder, and Mifare/EM 125kHz card reader. More information on the panel is given in its Operating Manual which is available at www.roger.pl.

7. IDENTIFICATION

Following user identification methods are offered by the panel:

- MIFARE Ultralight/Classic/Plus/DESFire and EM125kHz proximity cards
- PINs
- RFID fobs

MIFARE cards

By default, the panel reads serial numbers (CSN) of MIFARE cards, but it is possible to program cards with own numbers (PCN) in selected and encrypted sectors of card memory. The use of PCN prevents card cloning and consequently it significantly increases security in the system. More information on MIFARE cards with PCN is given in section 7 and in AN024 application note which is available at www.roger.pl.

EM 125kHz cards

By default, the panel also reads the serial number of EM 125kHz cards. The EM 125kHz card reader works in parallel with the reading of Mifare cards. In the MD70 device settings it is possible to limit card reading to one of two standards.

PINs

The panel accepts variable length PINs (by default 4-16 digits). PIN entered with keypad must be concluded with # or OK key.

8. OTHER PROXIMITY CARDS AND BIOMETRICS

Identification on the cabinet controller can be carried out using other methods than those mentioned above if an additional external terminal is connected to it. For this purpose, you can use the MCT series card reader or the RFT1000 fingerprint reader. The devices should be given individual addresses in the range of 800 - 815 and connected to the A and B terminals of the controller.

If there is a need to identify using methods other than those offered by Roger, an external reader with Wiegand interface can also be connected to the controller and thus support other standards of cards and biometric data. In such a scenario, it is additionally necessary to connect the MCX102 intermediate expander to the RS485 bus with an address in the range of 800 - 815. The reader with Wiegand interface is connected to the IN1 (D0 line) and IN2 (D1 line) terminals of the expander, and the MCX102 expander itself is connected to the A terminals and B controller.

9. MCX8 EXPANDERS

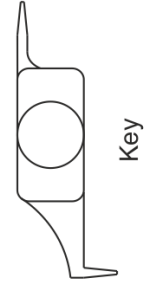
Detailed information on the installation and configuration of the MCX is available in the dedicated user manual. The addresses and polarization of the output lines for connecting the lock are defined in the low-level configuration by means of the RUD-1 interface and the RogerVDM program. The types of NO and NC input lines that can be used to connect the cabinet opening sensors are also defined in the low-level configuration. More information on the expander itself is provided in the MCX8 manual available at www.roger.pl.

10. INSTALLATION

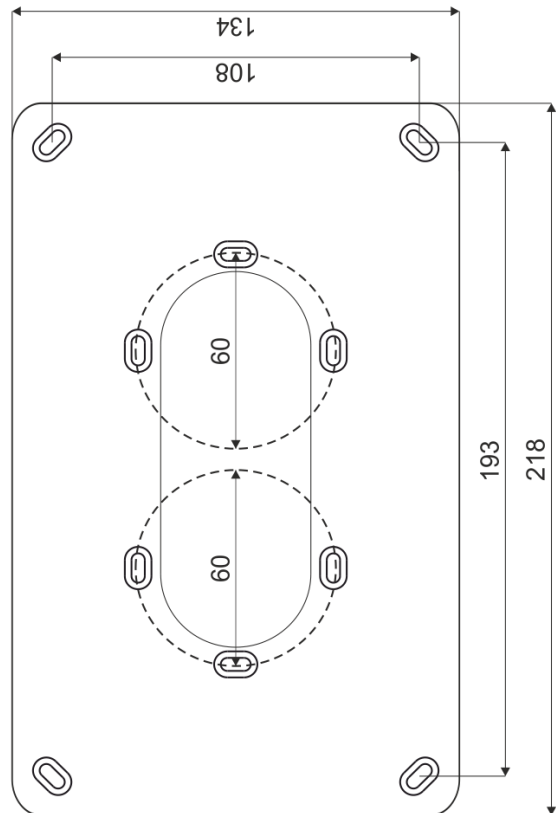
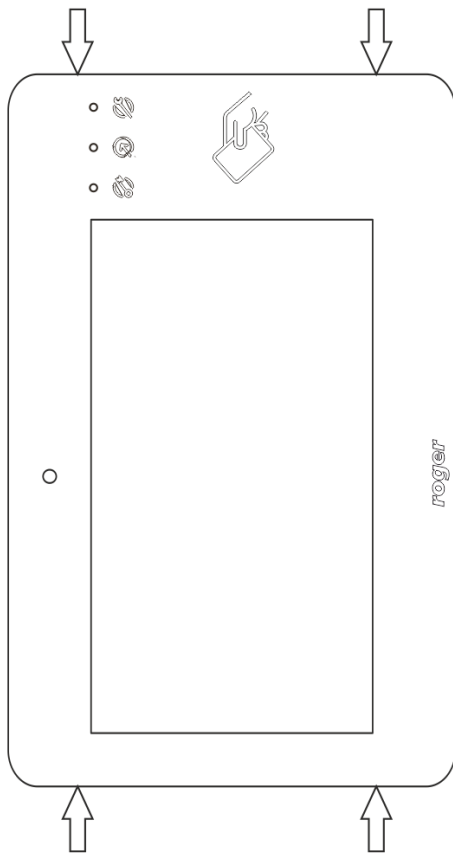


To open the housing, use the included plastic key. Insert one end into each slot until the latches release.

Do not rotate the key in the slot and do not lift the latches!



RCC512 controller



rod345

Fig. 2 RCC512 installation

Table 1. Terminals and ports	
Terminal/ port	Description
12V	12VDC power supply
GND	Ground and RS485 bus reference potential
A	RS485 communication bus, line A
B	RS485 communication bus, line B
ETHERNET	Ethernet port
USB	USB host port

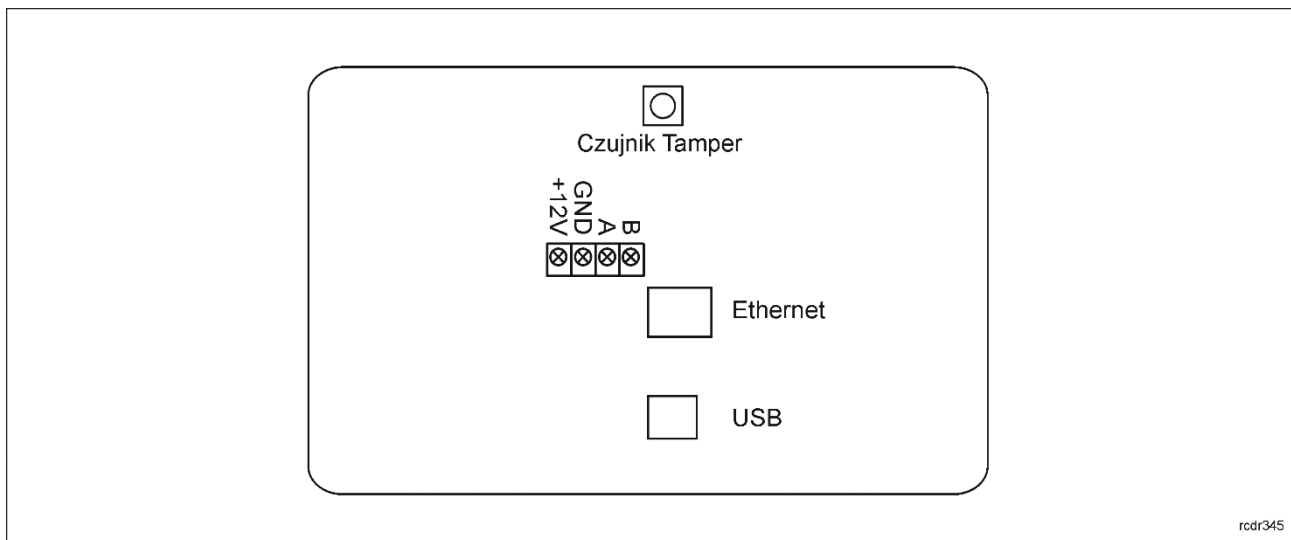


Fig. 3 The inside of the RCC512 panel

11. INSTALLATION AND USE GUIDELINES

- The RCC512 controller should be mounted on a vertical part of the structure (wall) away from sources of heat and moisture.
- In particular, it is not allowed to install the reader in places with high humidity such as saunas, swimming pools, car washes, etc.
- The front panel of the device should be mounted so that the tamper sensor is pressed against the base of the terminal (fig. 3).
- All electrical connections must be made without voltage.
- If the peripheral device and the controller are powered from separate sources, it is necessary to connect the minus of the power supply of such a device with the minus of the controller's power supply.
- Clean the front panel periodically with a slightly damp cloth and mild detergents. Never use abrasive materials or strong cleaning agents such as alcohols, thinners, gasoline, etc. Damage resulting from improper maintenance or improper use is not covered by the warranty.
- The electronic module inside the housing is sensitive to electrostatic discharge. Before performing any work on the module, any electrical charge accumulated on the person performing work inside the device must be removed. This can be accomplished, for example, by touching a grounded metal object with a bare hand.
- The product communicates only with another network device using a non-Internet-compatible communication protocol.

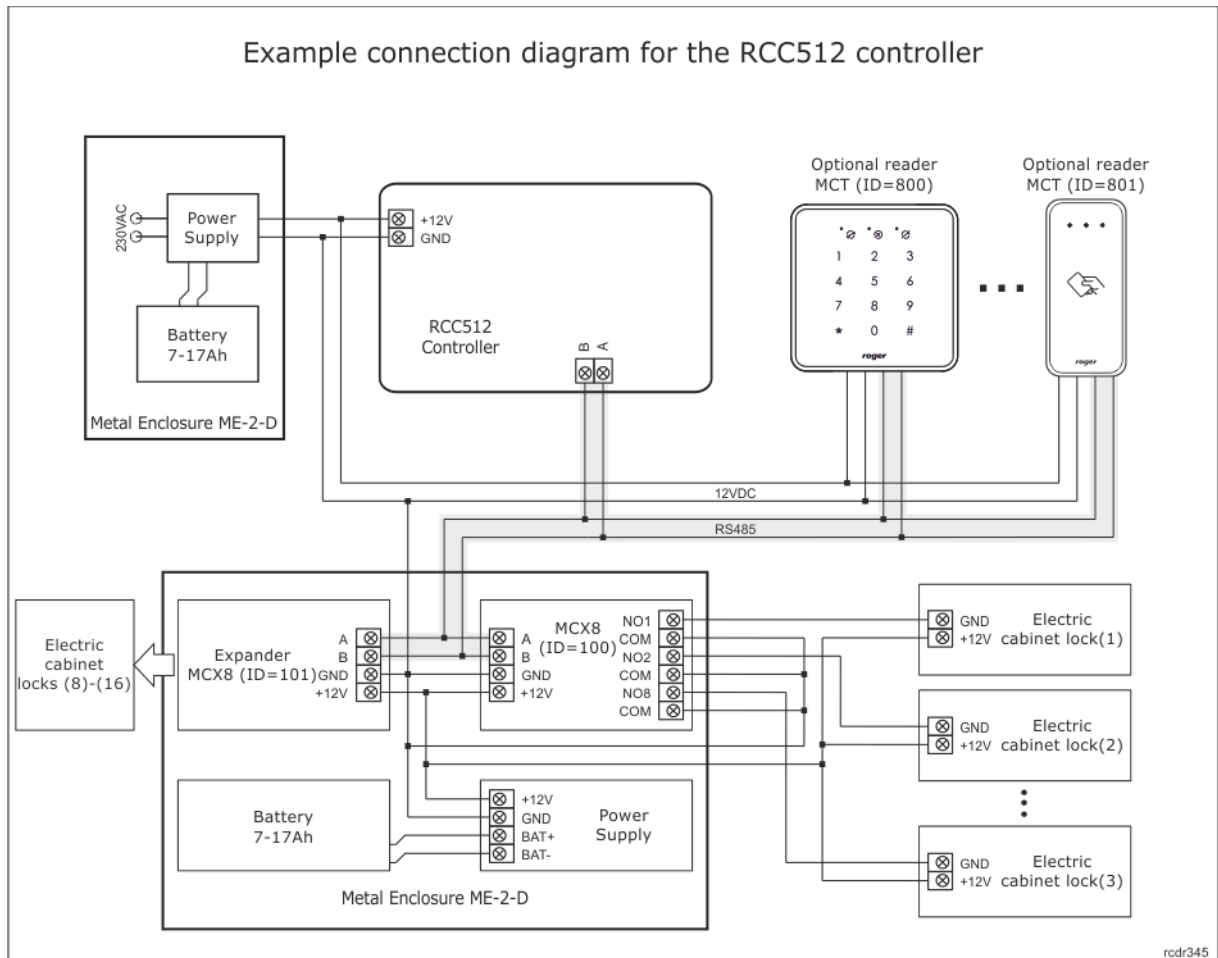


Fig. 4 Example connection diagram

Schematic notes:

- Cabinet electric locks are controlled by MCX8 expander relays. The set shown in the diagram with two MCX8 expanders enables control of 16 electric locks, which can be operated from the RCC512 controller or optional external terminals.
- Further expansion of the system can be achieved by connecting additional expanders to the RCC512 controller.
- The maximum length of the RS485 bus is 1200m and all devices on this bus should have a common negative power supply.
- Optionally, door opening sensors can be connected to the expander inputs if they are installed to monitor the status of opening the cabinets.
- Select the buffer power supply depending on the required current consumption by the electric locks. The example assumes a 12VDC/3.5A power supply, which is normally mounted in the ME-2-D metal enclosure.

12. RAACA APP

After connecting the power, the RCC512 controller will launch the RAACA application. At the first start, it will be proposed to create a default Master user with the password 9999. You can log in to the application with the password 9999# (if it has been created) or possibly with the administrator password 12345*. The administrator account is intended for the installer or the person managing the system, i.e., for maintenance and service purposes. Normal operation and configuration change of the controller should be done using a user account with appropriate permissions.

Note: Both default passwords must be changed to your own passwords as described in section 16.

In the next step, it is possible to select the controller operating mode, which affects its functionality. The RCC512 controller can operate in the following modes:

- Pool cabinets - the user, after identification, is assigned the first free locker.
- Personal equipment - inverted pool cabinet mode.
- Personal cabinets - the user is assigned one locker.
- Postboxes - the user is assigned a locker but, unlike in the Personal equipment mode, multiple users can be assigned to one locker.
- Toolboxes - a user can have multiple lockers assigned.
- Storage box – after entering the code *0#, the user defines his own PIN code to open the locker and then the first free locker is assigned to him.
- Drop box mode – allows you to assign a deposit by the "postman" and collect parcels using one-time codes.

After selecting a mode, the home screen is displayed.



Fig. 5 Home screen

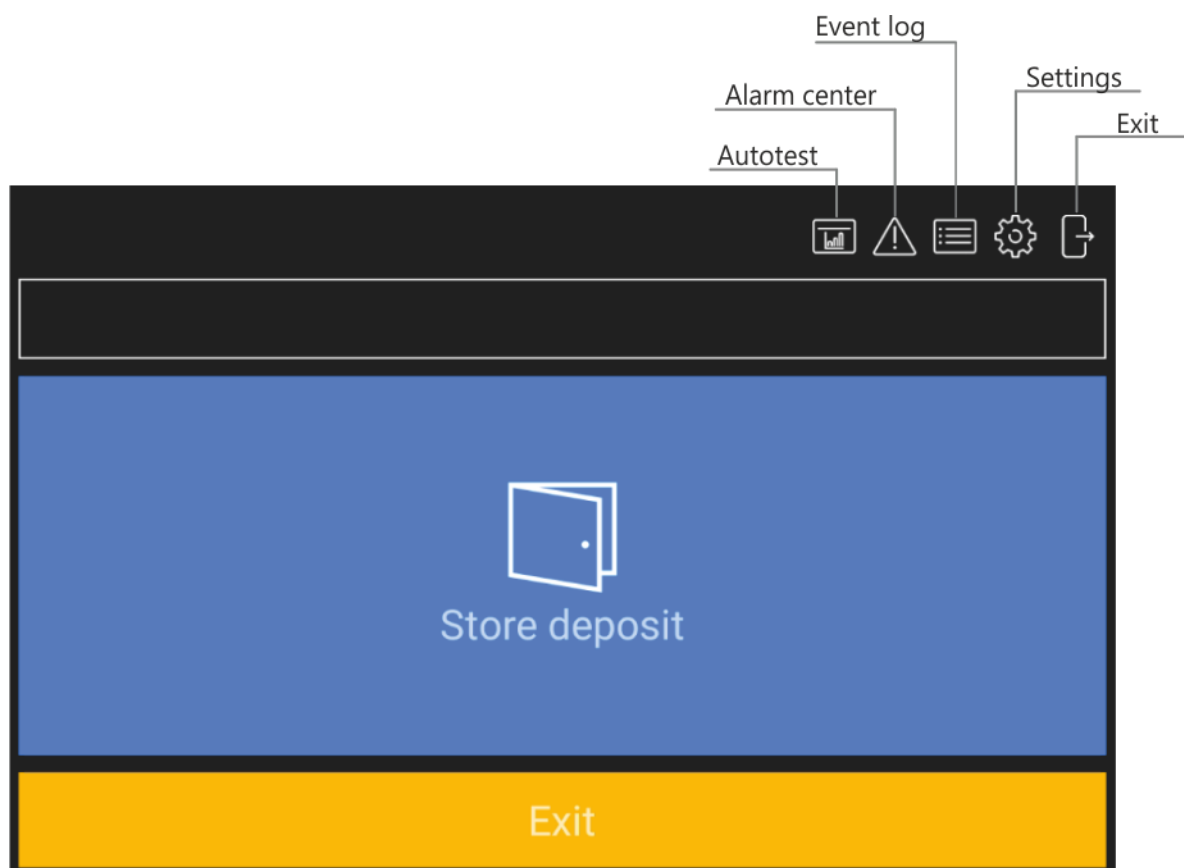


Fig. 6 Main menu

Note: Depending on the operating mode, the descriptions in the window in Fig. 6 may be slightly different.

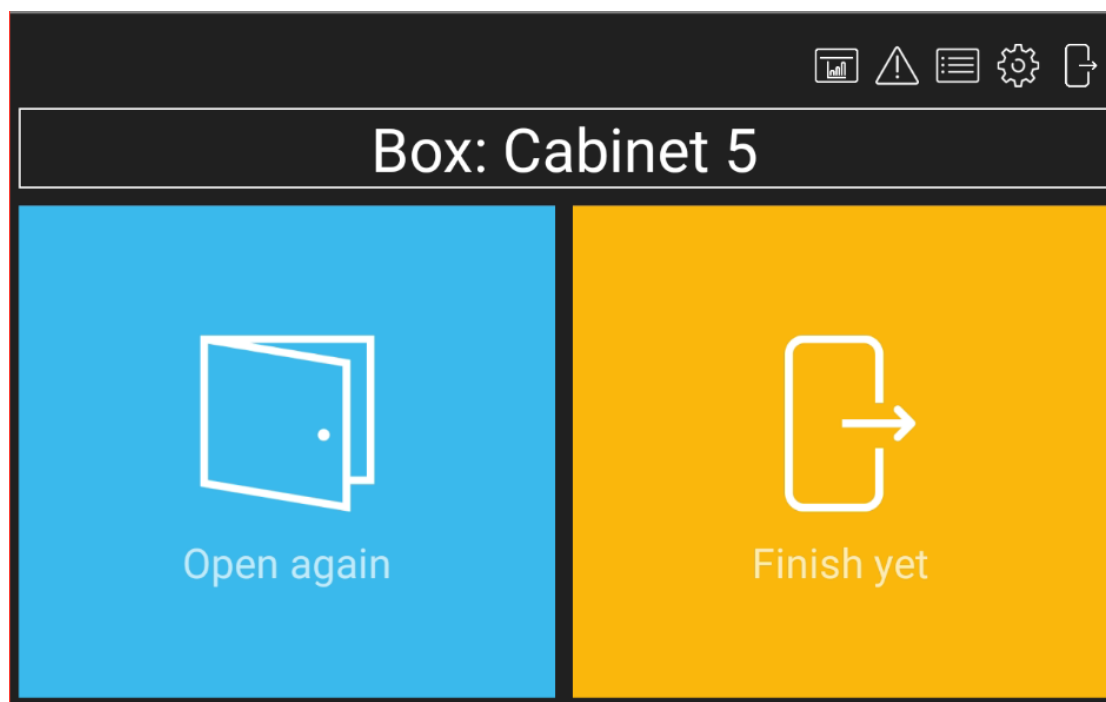





Fig. 7 Menu after opening the cabinet

After selecting  the Alarm Center is displayed in the upper right corner, containing a list of alarm events (e.g., force opening, tamper, etc.) recorded by the cabinet controller in the selected period of time. The colour of the icon indicates the status:

- White: no unacknowledged alarms.
- Orange: Historical alarms are stored in the device's memory.
- Red: One or more unacknowledged alarms still pending.

After selecting  the Report Center is displayed, shown in Fig. 8. After selecting the Events field, it is possible to view events (e.g. user login, key download, etc.) and after selecting  in the same window, also deleting and exporting events recorded by the cabinet controller. User Report allows you to view and export events related to the selected user. Events from the Report Center can be exported to a flash drive connected to the USB port of the controller (Fig. 3), to the internal memory or sent to the e-mail address defined in the Configuration window (Table 2). The available formats for exported data are Excel (XLS) and PDF.

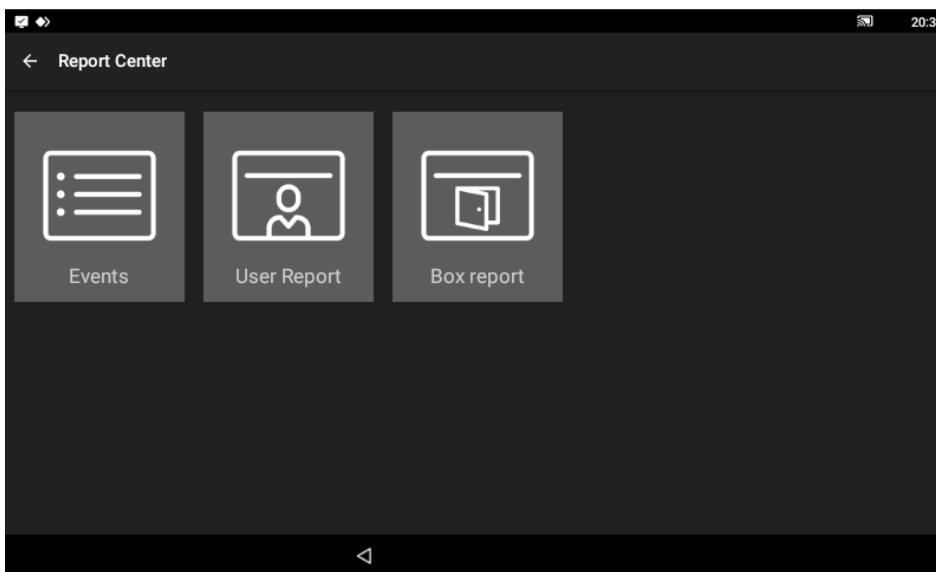




Fig. 8 Report Center

After selecting  the controller settings window is displayed, shown in Fig. 9. And after selecting  you return to the start screen.

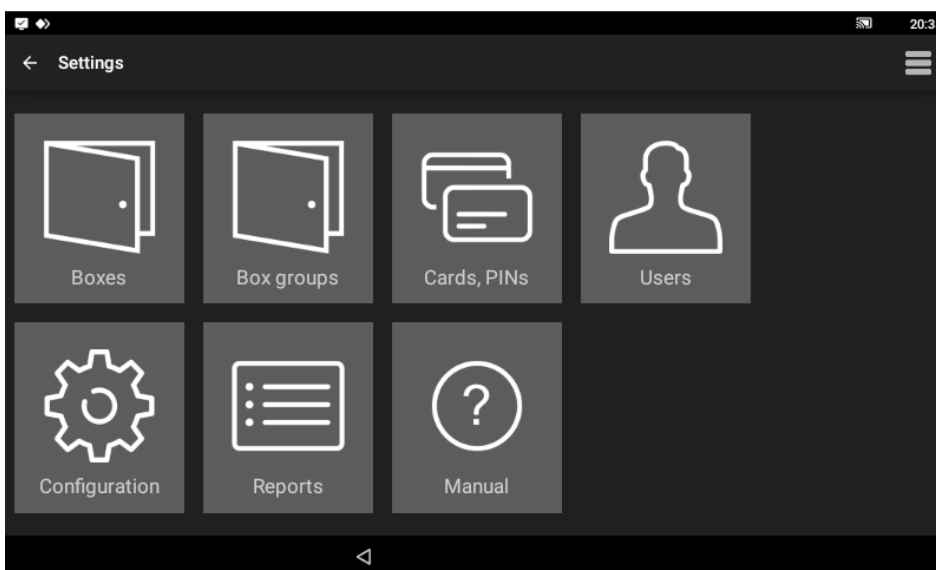



Fig. 9 Settings menu

Boxes

When selected the list of RCC512 boxes/lockers is displayed. Items on the list can be edited and then assigned to groups and individual users. It is also possible to change the names of individual boxes/lockers as well as change all the names after selecting .

Box groups

This option allows you to create and manage groups of caches. They can be used to divide the boxes into individual sizes or types of stored items.

Card, PINs

When selected, a list of cards and PIN codes used by users for identification on the controller panel is displayed. You can add, edit, and delete items in the list. When adding the card, its number can be read on the reader built into the RCC512 controller.


Users

When selected, a list of system users is displayed. Users can be assigned cards and PINs as well as groups of boxes. In addition, you can attach a Master exception to the user, which assigns the user unlimited rights to operate the cabinet controller (Depending on the previously set mode, some options may not be available).

Configuration

When selected then list of parameters given in table 2 is displayed.


Table 2. Parameter list in Configuration window	
General	
Admin password	Administrator password. In case of login at MD70 panel the admin, password is concluded with * key. Range: 4-10 digits. Default value: 12345.
Logout when door closed	Parameter enables automatic user logout and reverting to starting screen when locker door is closed. Range: ON, OFF. Default value: ON.
Automatic logout time [s]	Parameter defines time after which user is automatically logged out and panel reverts to starting screen if no actions are performed by user in the main menu of the panel. Range: 0-99. Default value: 60.
Automatic logout	Parameter enables automatic user logout and reverting to starting screen when <i>Automatic logout time</i> elapses. Range: ON, OFF. Default value: ON.
Alarm signalling time [min]	Parameter defines time for tamper alarm signaling on speaker. Range: 0-99. Default value: 3.
Door open too long prealert time [s]	Parameter defines time for acoustic warning at MD70 panel when door is opened, and user is logged out. Range: 0-99. Default value: 60.
Automatic daily release of all boxes	Releasing cabinets from assigned users (e.g., Pool cabinets mode). Value range: ON, OFF. Default value: OFF.
Boxes release time	Daily time of releasing lockers.
Pool mode settings	
Temporary reuse lock [h]	The parameter determines the possibility of reusing the cabinet by the user in the Pool cabinets mode.
Personal cabinets mode settings	
Any zone reader	Entering the card, user defined PIN code on any zone reader will open the locker
Fast mode (workers lockers)	The parameter enables faster handling of cabinets in the Personal cabinets mode. When the parameter is enabled, closing the cabinet automatically logs out the user and goes to the start screen. Value range: ON, OFF. Default value: ON.

Storage / drop box mode settings	
Choosing a group of cabinets	The parameter enables the selection of a group of lockers when depositing an item. Default value: OFF.
Automatic opening of the cabinet	Enabling the parameter allows after logging in that the box is automatically opened to retrieve the item. Default value: OFF.
Card authentication	Enabling the parameter activates additional authorization with the user's card to retrieve the item. Default value: OFF.
Cabinet expander's settings	
Cabinet lock time [s]	The parameter defines the duration of the impulse on the expander outputs releasing the electric locks. Value range: 0.25, 0.5, 0.75 and 1. Default value: 0.25s.
Cabinet expander input polarization	The parameter makes it possible to collectively define the types of expander input lines to which door opening sensors can be connected. After changing the parameter, it may be necessary to restart the controller. Range of values: NO, NC. Default value: NO.
Display	
Custom wallpaper	Parameter enables switching between default and custom wallpaper for RCC512 panel. Custom wallpaper is indicated by <i>Select wallpaper</i> command in  menu. Range: ON, OFF. Default value: OFF.
Font colour	Parameter specifies colour of the font used on MD70 starting screen. Range: Light, Dark, Orange. Default value: Light.
RACS 5 settings	
RACS 5 mode	Parameter not used.
Server address	Parameter not used.
Communication port	Parameter not used.
Login	Parameter not used.
Communication password	Parameter not used.
TLS	Parameter not used.
Device name (comment)	Parameter specifies the name of RKD32 which is then used in reports and logs.
MAC	Controller MAC address number.
WWW settings	
Web access enable	Parameter enables RCC512 configuration and management via web browser.
Port	Parameter defines communication port for web browser access. Due to security reasons the port cannot be less than 1024. Default value: 8888.
Login	Parameter defines login for web browser access.
Password	Parameter defines password for web browser access.
Email account	
Address	Email account which is used for sending messages and reports from RCC512.
Login	Email account login for email sending by RCC512.
Password	Email account password for email sending by RCC512.
SMTP port	Email port. Default value: 587.
Host	Email host address.
SSL	Parameter enables SSL encryption for email sending. Range: ON, OFF. Default value: OFF.
Address 1	Recipient email address.

Address 2	Recipient additional email address.
-----------	-------------------------------------

Select wallpaper	Command enables indication of custom wallpaper (800x480px, *.jpg format) for starting screen. Additionally, the parameter <i>Custom wallpaper</i> (table 2) must be enabled.
Detect devices	The command starts the view of the list of expanders/readers connected to the RCC512 controller. After adding more expanders to support cabinets, you should start scanning to detect them.
Check for update	Command enables to check and download updates. In such case the RKD32 must be connected to computer network.
Install update	Command enables installation of downloaded update.
Factory reset	Command enables to restore factory settings as explained in section 16.



Reports

After selecting, you go to the Report Center in the same way as using the previously described icon , which is available in the upper right corner of the main menu (Fig. 6).

Manual

When selected then app manual is displayed on RCC512 screen.

Menu in Settings window

Menu  in window shown in fig. 9 includes additional commands that are not available in the menu  displayed in *Configuration* window.

Show launcher	The command enables to exit RAACA app and start Android environment. Default password is admin.
System settings	The command enables configuration of Android system settings. More information is given in MD70 manual.
MD70 settings	The command enables configuration of MD70 parameters. More information is given in MD70 manual.
Files	Command starts app that enables file navigation at MD70 panel.
About	The command displays change log.
License	The command displays license agreement for Roger software.
License file	The command displays information about the license of the RCC512 cabinet controller in terms of the number of supported cabinets and management via a web browser.
Export database	Command enables to make backup of RKD32 settings on pendrive as explained in section 16.
Import database	Command enables to import RKD32 settings from file on pendrive as explained in section 16.
Remote support	Command enables to establish remote connection with MD70 panel in computer network for the purpose of technical support by specialist as explained in section 16.

13. CONFIGURATION IN STANDALONE MODE


The configuration of the RCC512 controller depends on the selected operating mode.

Note: Editing and deleting are possible with a long click on the selected item (e.g., user).



Pool cabinets

In this mode, the first free unassigned locker is assigned to the user after identification. Optionally, it is possible to assign a predetermined locker to a given user, as well as define a group of up to 32 lockers, from which a locker can be assigned to the user. Configuration consists primarily in defining users and their PIN codes and/or ID cards/tags.


Boxes

1. After logging in on the panel (default PIN: 9999#), select  and then Boxes.
2. Press and hold the locker and then select Edit. In the opened window, it is possible to assign a locker to a given group. It is also possible to assign a given locker to a specific user (if it has been created). Individual cabinets can also be given their own names to facilitate their recognition in the system. After selecting, it is possible to rename all cabinets.

Card, PINs

1. After logging in on the panel (default PIN: 9999#), select  and then Cards, PINs.
2. In the window that opens, select Add card or Add PIN to define factors for users to be identified on the control panel. Keychain, card can be read on the panel after selecting the Card code parameter and entering it into the reader .


Users

1. After logging in on the panel (default PIN: 9999#), select  and then Users.
2. In the opened window, select Add.
3. In the next window, enter the user a name (e.g. name and surname). In the Cards, PINs field, assign the previously defined factor(s) that will be used by the user for identification on the control panel. Optionally, in the box group field, assign a previously defined box group. A user with an assigned group will be assigned a free locker from the indicated group, not the entire locker system.


Personal cabinets

In this mode, the user is assigned one locker. Configuration consists in defining users and their PIN codes and/or ID cards/tags, as well as assigning lockers to which they will have access.


Boxes

1. After logging in on the panel (default PIN: 9999#), select  and then Boxes.
2. Optionally, give individual cabinets your own names to make them easier to recognize in the system. After selecting, it is possible to rename all cabinets.

Card, PINs

1. Log in at the panel (default PIN: 9999#), select  and then *Cards, PINs*.
2. In the opened window select Add card or Add PIN to specify factor(s) that can be used to identify user at RCC512 panel. Card or fob can be read at built-in reader in the RCC512 panel.

Users

1. Log in at the panel (default PIN: 9999#), select  and then *Users*.
2. In the opened window select *Add*.
3. In the next window, enter the user a name (e.g. name and surname). In the Cards, PINs field, assign the previously defined factor(s) that will be used by the user for identification on the controller panel. In the boxes field, assign a locker/box that the user can open.

Post boxes

In this mode, the user is assigned a locker, but unlike the Personal cabinets mode, many users can be assigned to one locker. Configuration is carried out analogously to "Personal cabinets.

Toolboxes

In this mode, a user can have multiple lockers assigned. The configuration is analogous to the Safety Cabinets

Storage box / Drop box mode

In this mode, the user can define his own PIN code to open the locker, and the first free locker is assigned to him. Your own code is defined after entering *0# on the controller panel.

14. CONFIGURATION VIA WEB BROWSER

RCC512 can be remotely configured and managed via web browser. In such scenario it is necessary to define parameters in section WWW settings (table 2). The communication with control panel can be in Ethernet network. The IP address of the panel in LAN is configured by means of Ethernet app after exiting RAACA app with the command *Show launcher* (table 4). Prior to establishing connection with the RCC512 it is necessary to enter IP address and communication port (8888 by default). The port may require unblocking in firewall and/or antivirus software.

Note: Configuration via web browser requires license purchase. You can verify if your RCC512 has the proper license selecting *License file* command (table 4).

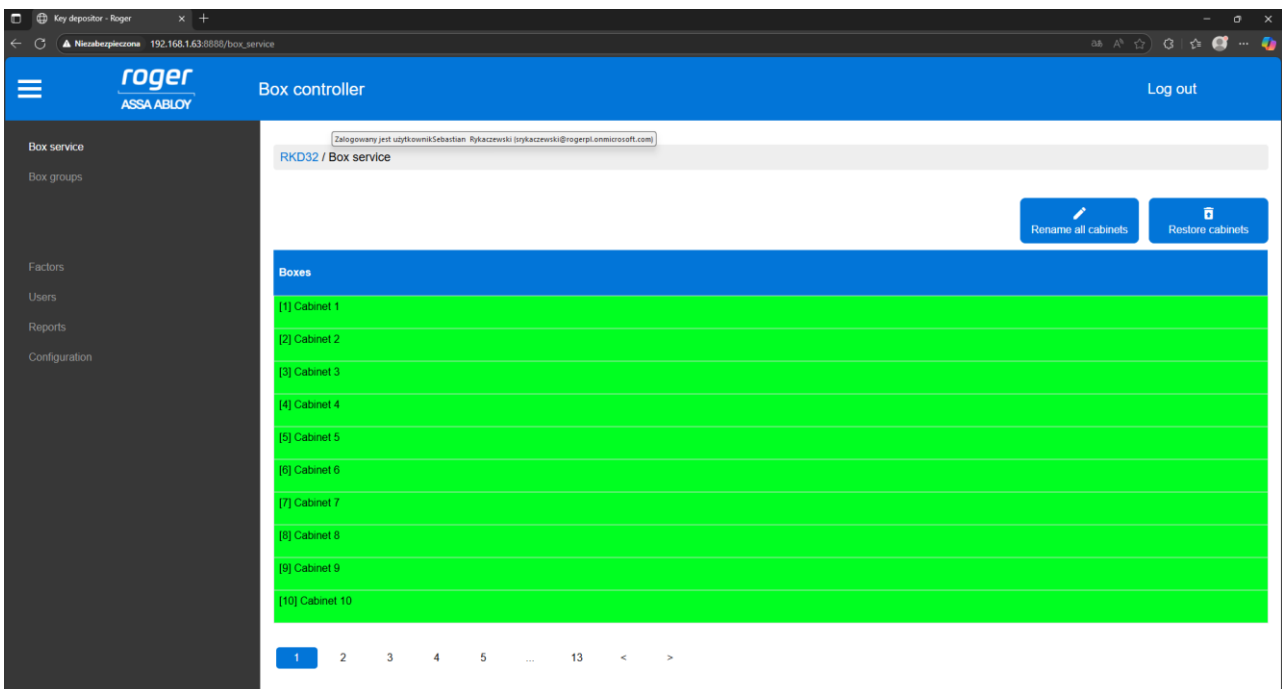



Fig. 10 RCC512 web application screen

15. CONFIGURATION IN NETWORK MODE


Configuration and operation in network mode are not currently available.

16. MANAGEMENT AND GENERAL ISSUES

Admin password change



1. Log in at the panel (default PIN: 9999# or 12345*), select  and then *Configuration*.
2. Click *Admin password* and replace default 12345 password with your own.

Default Master user password change (if available)

1. Log in at the panel (default PIN: 9999# or 12345*), select  and then *Cards, PINs*.
2. Select *Add PIN* in order to define new factor and return to *Settings* window.
3. Select *Users*.
4. Long click *USER_ADMIN* and then select *Edit*.
5. Click *Cards, PINs* deselect default *PIN_ADMIN* (e.g., 9999) and select your previously defined PIN.

Expansion and division of the system



In the case of expanding the system with additional cabinets connected to expanders, as well as in the case of connecting additional identification terminals, it is necessary to detect new devices on the RS485 bus of the controller. To run a scan:

1. After logging in on the panel (default PIN: 9999# or 12345*), select  and then Configuration.
2. In the opened window, select the menu  and then Detect Devices.

In the case of the Personal cabinets and Post boxes modes, it is possible to use zone readers. Each such additional reader on the RS485 bus can be assigned to a group of 32 cabinets. The use of zone readers facilitates the operation of larger cabinet systems.

Programmable cards

By default, the panel reads serial numbers (CSN) of MIFARE cards, but it is possible to program cards with own numbers (PCN) in selected and encrypted sectors of card memory. The use of PCN prevents card cloning and consequently it significantly increases security in the system. To configure how the panel will read card numbers:

1. Log in at the panel (default PIN: 9999#) and select .
2. In the opened window select  menu and then *MD70 settings* command.
3. In the next window click *Credentials settings*.



Note: If other than default card reading method is defined for MD70 panel then its reader cannot be used for fob enrolment and for quick fob return mode.

Mifare cards are programmed with RogerVDM software and RUD series reader (e.g., RUD-3-DES). Card programming is explained in AN024 application note which is available at www.roger.pl.



Settings backup

RCC512 settings (including users) can be exported to file for the purpose of backup. Exporting and importing is also recommended in case of RAACA app update.

Database export



1. Connect your pendrive to USB port on RCC512 (Fig. 3).
2. Log in at the panel (default PIN: 9999# or 12345*), select  and then .
3. Select the command *Export database*.

Database import

1. Rename previously exported database file into RKDdb.db and copy into pendrive.
2. Connect your pendrive to USB port on RCC512 (Fig. 3).
3. Log in at the panel (default PIN: 9999# or 12345*), select  and then .
4. Select the command *Import database*.

Factory settings reset

To restore factory default settings:

1. Log in at the panel (default PIN: 9999# or 12345*), select  and then *Configuration*.
2. In the opened window select  menu and then *Factory reset*.

License upload

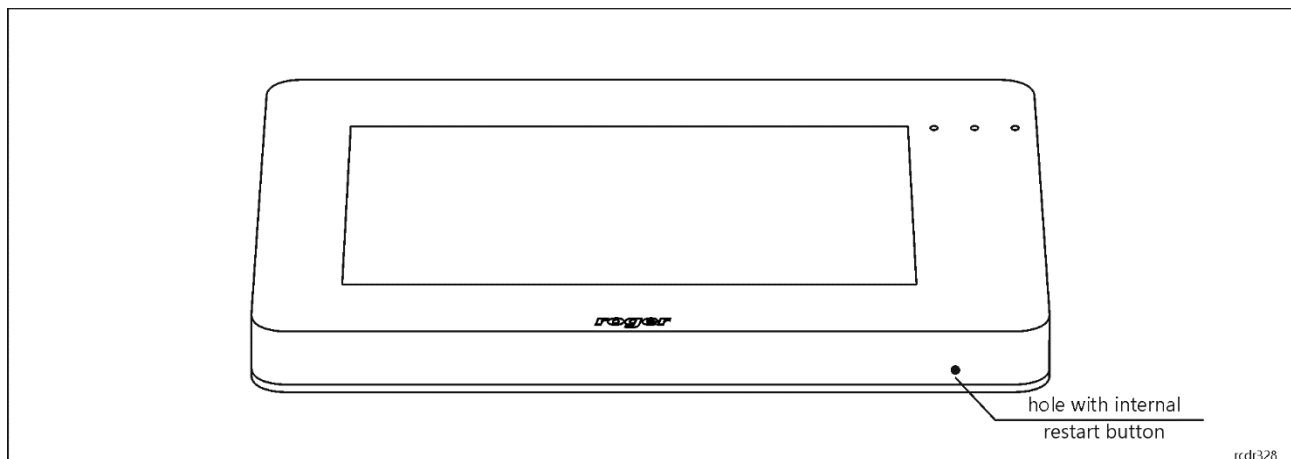
In case of RCC512 depending on the number of supported cabinets, management via web browser it is necessary to activate license. You can verify your license selecting *License file* command (table 4). To upload purchased license place license file on USB disk or internal storage of device. Run "RKD receiver" app and import license.

Remote technical support

Remote technical support by Roger specialist is available. In such scenario, RCC512 must be connected to Ethernet network, and it must be connected to Internet. After selection of *Remote support* command (table 4) AnyDesk app is started. Reveal the number from the app to Roger technician so he could connect remotely. Then, accept the connection request from Roger technician on the RCC512 panel.

17. TROUBLESHOOTING

Table 5. Troubleshooting	
Issue	Solution
Starting screen is not displayed on RCC512 panel.	Restart RCC512 panel by switching power supply off and on or press the button as in fig. 11. Start RAACA app manually.
RCC512 panel is not reacting for touching.	Verify power supply. Restart MD70 panel by switching power supply off and on or press the button as in fig. 11.



Rys. 11 RCC512 restart button

18. SPECIFICATION

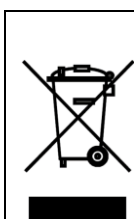
Table 6. Specification	
Nominal supply voltage	12VDC
Current consumption	RCC512 control panel: avg. 500 mA, max. 800mA MCX8 expander: avg. 30 mA
Identification methods	ISO/IEC14443A MIFARE Ultralight, Classic, Desfire EV1 and Plus proximity cards and PINs (4-16 digits)
Reading range	Up to 5 cm
Environment	Indoor general conditions, temperature: +5°C to +40°C, relative humidity: 10 to 75% (no condensation)
Dimensions H x W x D	134 x 218 x 25mm
Weight	500 g
Compliance	CE, RoHS

19. ORDERING INFORMATION

Table 7. Ordering information	
RCC512	Cabinet access controller for 512 cabinets; 7" touch control panel; stand-alone operation only; purchase of RCC512-1C-LIC licenses required
MCX8-BRD	I/O expander; 8 inputs, 8 relay outputs 1.5 A/30 V; 13.8 VDC supply input
RCC512-1C-LIC	Single cabinet license
RUD-1	Communication interface

20. PRODUCT HISTORY

Table 8. Product history		
Version	Date	Description
RCC512	II 2020	The first commercial version of product
RCC512	III 2023	The second commercial version of the product



This symbol placed on a product or packaging indicates that the product should not be disposed of with other wastes as this may have a negative impact on the environment and health. The user is obliged to deliver equipment to the designated collection points of electric and electronic waste. For detailed information on recycling, contact your local authorities, waste disposal company, or point of purchase. Separate collection and recycling of this type of waste contribute to the protection of the natural resources and is safe to health and the environment. Weight of the equipment is specified in the document.

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