Manuals+ — User Manuals Simplified.

Luminys RWCA Access Reader User Manual

Contents

Luminys RWCA Access Reader

Product Usage Instructions

1. **Power On:** Connect the power adapter to the Card Reader after ensuring it is powered off. Follow local electric safety standards.
2. **Authentication:** Use authorized cards or biometric data to authenticate access through the reader.
3. **Operation:** Follow the device's interface prompts for further actions or access control operations.
4. **Maintenance:** Regularly clean and inspect the Card Reader to ensure proper functionality.

FAQs

- **Q: What should I do if the Card Reader is not recognizing my access card?**
  - A: Ensure that the card is authorized and properly aligned with the reader. Try cleaning the card surface and contacts for better recognition.
- **Q: Can I use multiple types of authentication methods with the Access Reader?**
  - A: Yes, the Access Reader supports various authentication methods such as cards, fingerprints, and other biometric data.
- **Q: How often should I perform maintenance on the Card Reader?**
  - A: Regular maintenance should be performed at least once every few months to ensure optimal performance.

PRODUCT INFORMATION

Foreword

General

This manual introduces the functions and operations of the Access Reader (hereinafter referred to as the card reader). Read carefully before using the device, and keep the manual safe for future reference.

Safety Instructions

The following signal words might appear in the manual.

Revision History

Signal Words	Meaning
⚠ **DANGER**	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
⚠ **WARNING**	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
⚠ **CAUTION**	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
⚏ **TIPS**	Provides methods to help you solve a problem or save time.
📖 **NOTE**	Provides additional information as a supplement to the text.

Privacy Protection Notice

Version	Revision Content	Release Time
V1.0.3	Updated the unlock method.	March 2023
V1.0.2	Added unlock methods and system updating.	December 2022
V1.0.1	Updated device models.	December 2021
V1.0.0	First release.	October 2020

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, and license plate number. You need to comply with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures that include but are not limited to providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions.
    - For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code, or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in

some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.

- There might be errors in the print or deviations in the description of the functions, operations, and technical data. If there is any doubt or dispute, we reserve the right to a final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks, and company names in the manual are properties of their respective owners.
- Please visit our website, and contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right to a final explanation.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the Card Reader, hazard prevention, and prevention of property damage. Read carefully before using the Card Reader, and comply with the guidelines when using it.

Transportation Requirement

Transport, use, and store the Card Reader under allowed humidity and temperature conditions.

Storage Requirement

Store the Card Reader under allowed humidity and temperature conditions.

Installation Requirements

- Do not connect the power adapter to the Card Reader while the adapter is powered on.
- Strictly comply with the local electric safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the Access Controller.
- Do not connect the Card Reader to two or more kinds of power supplies, to avoid damage to the Card Reader.
- Improper use of the battery might result in a fire or explosion.
- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not place the Card Reader in a place exposed to sunlight or near heat sources.
- Keep the Card Reader away from dampness, dust, and soot.
- Install the Card Reader on a stable surface to prevent it from falling.
- Install the Card Reader in a well-ventilated place, and do not block its ventilation.
- Use an adapter or cabinet power supply provided by the manufacturer.
- Use the power cords that are recommended for the region and conform to the rated power specifications.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Please note that the power supply requirements are subject to the Card Reader label.
- The Card Reader is a class I electrical appliance. Make sure that the power supply of the Card Reader is connected to a power socket with protective earthing.

Operation Requirements

- Check whether the power supply is correct before use.
- Do not unplug the power cord on the side of the Card Reader while the adapter is powered on.
- Operate the Card Reader within the rated range of power input and output.
- Use the Card Reader under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the Card Reader, and make sure that there is no object filled with liquid on the Card Reader to prevent liquid from flowing into it.
- Do not disassemble the Card Reader without professional instruction.

FCC

1. This device complies with Part 15 of the FCC Rules.
    - **Operation is subject to the following two conditions:**
        1. This device may not cause harmful interference.
        2. This device must accept any interference received, including interference that may cause undesired operation.
2. Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, under Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used by the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement:

- This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.
- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- This equipment should be installed and operated with a minimum distance of 20cm between the radiator& your body.

ISEDC Radiation Exposure Statement:

- This equipment complies with ISEDC RF radiation exposure limits set forth for an uncontrolled environment.
- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- This equipment should be installed and operated with a minimum distance of 20cm between the radiator& your body.

IC Warning

This device contains license-exempt transmitter(s)/receiver(s) that comply with Innovation, Science, and Economic Development Canada's license-exempt RSS(s). Operation is subject to the following two conditions:

1. This device may not cause interference.
2. This device must accept any interference, including interference that may cause undesired operation of the device.

Introduction

Features

- PC material and acrylic panel with a slim and waterproof design.
- Supports non-contact card reading.
- Supports IC card (Mifare) reading, ID card reading (only for the card reader with ID card reading function), and QR code reading (only for the card reader with QR code reading function).
- Supports communication through RS–485 and Wiegand (fingerprint card reader and QR code reader only support RS–485).
- Supports online update.
- Supports tamper alarm.
- Built-in buzzer and indicator light.
- Built-in watchdog to ensure card reader stability.
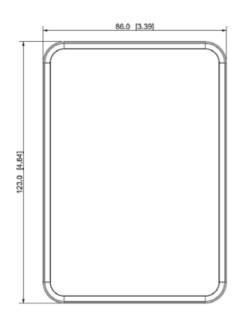- Safe and stable with overcurrent and overvoltage protection.

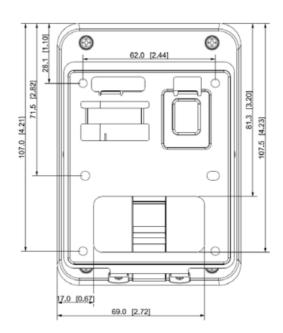Functions may vary according to different models.

Appearance

The card reader can be divided into R-WCA model

R-WCA Model

Figure 1-1 Dimensions of the 86 box model (mm [inch])

Ports Overview

Use RS–485 or Wiegand to connect the card reader. Fingerprint model and QR code model only support RS–485.

8-core Cables for the R-WCA Model

Table 2-1 Cable connection description (1)

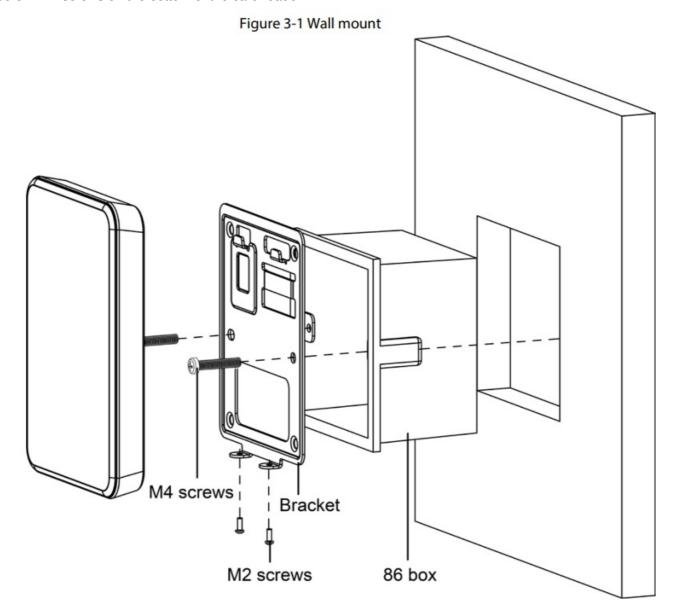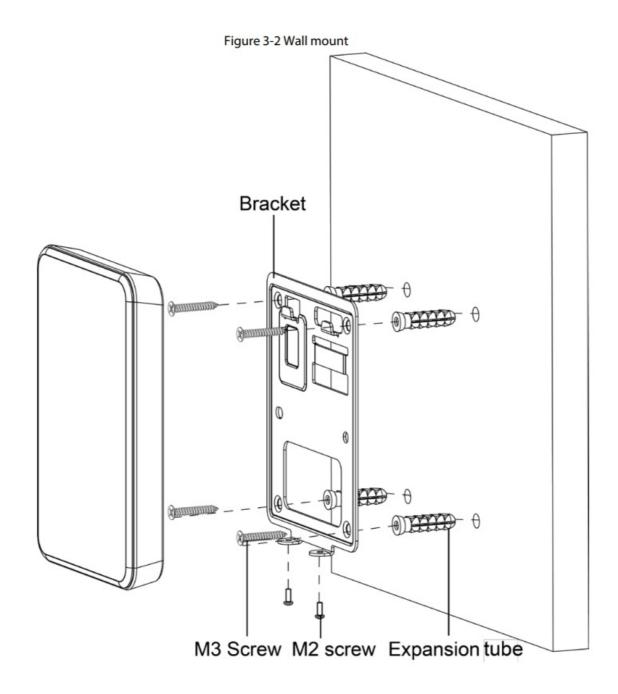| Color	Port	Description
Red	RD+	PWR (12 VDC)
Black	RD–	GND
Blue	CASE	Tamper alarm signal
White	D1	Wiegand transmission signal (effective only when using Wiegand protocol)
Green	D0	
Brown	LED	Wiegand responsive signal (effective only when using Wiegand protocol)
Yellow	RS–485_B	
Purple	RS–485_A	

Installation

Installing R-WCA Model

Box mount

1. Mount the 86 box to the wall.

2. Wire the card reader, and put the wires inside the 86 box.

3. Use two M4 screws to attach the bracket to the 86 box.

4. Attach the card reader to the bracket from top down.

5. Screw in 2 screws on the bottom of the card reader.

Figure 3-1 Wall mount

M4 screws

Bracket

M2 screws

86 box

Wall mount

1. Drill holes on the wall.

2. Put 4 expansion bolts into the holes.

3. Wire the card reader through the slot of the bracket.

4. Use two M3 screws to mount the bracket on the wall.

5. Attach the card reader to the bracket from the top down.

6. Screw in 2 screws on the bottom of the card reader.

Figure 3-2 Wall mount

Figure 3-2 Wall mount

Sound and Light Prompt

R-WCA Model

Table 4-1 Sound and light prompt description

Situation	Sound and Light Prompt
Power on.	Buzz once. The indicator is solid blue.
Removing the card reader.	Long buzz for 15 seconds.
Pressing buttons.	Short buzz once.
The alarm is triggered by the controller.	Long buzz for 15 seconds.
RS–485 communication and swiping an authorized card.	Buzz once. The indicator flashes green once and then turns to solid blue in standby mode.
RS–485 communication and swiping an unauthorized card.	Buzz four times. The indicator flashes red once and then turns to solid blue in standby mode.
Abnormal 485 communication and swiping an authorized/unauthorized card.	Buzz three times. The indicator flashes red once and then turns to solid blue in standby mode.
Wiegand communication and swiping an authorized card.	Buzz once. The indicator flashes green once and then turns to solid blue in standby mode.
Wiegand communication and swiping an unauthorized card.	Buzz three times. The indicator flashes red once and then turns to solid blue in standby mode.
Software updating or waiting for updates in BOOT.	The indicator flashes blue until the update is completed.

Unlocking the Door

Swipe the card on the card reader to open the door. For a card reader with a keypad, you can also unlock the door by entering the user ID and password.

- Unlock the door through the public password: Enter the public password, and then tap #.
- Unlock the door through the user password: Enter the user ID and tap #, and then enter the user password and tap #.
- Unlock the door through the card + password: Swipe the card, enter the password, and then tap #. If the password is correct, the indicator is green, and the buzzer sounds once. If the password is incorrect, the indicator is red, and the buzzer sounds 4 times (RS-485 communication) or sounds 3 times (Wiegand communication or no signal line is connected).

Updating the System

Updating through application

Prerequisites

- The Card Reader was added to the access controller through RS-485 wires.
- The access controller and Card Reader are powered on.

Procedure

- **Step 1** Install and log in to the application, and then select Device Manager.
- **Step 2** Click ⚙

Figure 6-1 Select the access controller

- **Step 3** Click ☁ and 📁 select the update file.
- **Step 4** Click Upgrade. The indicator of the Card Reader flashes blue until the update is completed, and then the Card Reader automatically restarts

Updating through lumiutility

Prerequisites

- The Card Reader was added to the access controller through RS-485 wires.
- The access controller and Card Reader are powered on.

Procedure

- **Step 1** Install and open the lumiutility, and then select Device upgrade.
- **Step 2** Click 📄 on an access controller, and then click 🔼 .
- **Step 3** Click Upgrade.

The indicator of the Card Reader flashes blue until the update is completed, and then the Card Reader automatically restarts.

Appendix 1 Cybersecurity Recommendations

Mandatory actions to be taken for basic equipment network security:

1. **Use Strong Passwords**
   - Please refer to the following suggestions for setting passwords:
   - The length should not be less than 8 characters.
   - Include at least two types of characters; character types include upper and lower case letters, numbers,

and symbols.

- Do not contain the account name or the account name in reverse order.
- Do not use continuous characters, such as 123, ABC, etc.
- Do not use overlapped characters, such as 111, aaa, etc.

2. **Update Firmware and Client Software in Time**

- According to the standard procedure in the industry, we recommend keeping your equipment (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the equipment is connected to the public network, it is recommended to enable the"auto-check for updates" function to obtain timely information on firmware updates released by the manufacturer.
- We suggest that you download and use the latest version of the client software.

"Nice to have" recommendations to improve your equipment network security:

- **Physical Protection**
  - We suggest that you perform physical protection on equipment, especially storage devices. For example, place the equipment in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable equipment (such as USB flash disk, serial port), etc.
- **Change Passwords Regularly**
  - We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.
- **Set and Update Passwords Reset Information Timely**
  - The device supports a password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.
- **Enable Account Lock**
  - The account lock feature is enabled by default, and we recommend you keep it on to guarantee account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.
- **Change Default HTTP and Other Service Ports**
  - We suggest you change the default HTTP and other service ports into any set of numbers between 1024–65535, reducing the risk of outsiders being able to guess which ports you are using.
- **Enable HTTPS**
  - We suggest you enable HTTPS so that you visit Web service through a secure communication channel.
- **MAC Address Binding**
  - We recommend you find the IP and MAC address of the gateway to the equipment, thus. Reducing the risk of ARP spoofing.
- **Assign Accounts and Privileges Reasonably**
  - According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.
- **Disable Unnecessary Services and Choose Secure Modes**
  - If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce

risks.

- If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:
    - **SNMP**: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
    - **SMTP**: Choose TLS to access the mailbox server.
    - **FTP**: Choose SFTP, and set up strong passwords.
    - **AP hotspot**: Choose WPA2-PSK encryption mode, and set up strong passwords.

- **Audio and Video Encrypted Transmission**
    - If your audio and video data contents are very important or sensitive, we recommend that you use an encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.
    - **Reminder**: encrypted transmission will cause some loss in transmission efficiency.

- **Secure Auditing**
    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check equipment log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

- **Network Log**
    - Due to the limited storage capacity of the equipment, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

- **Construct a Safe Network Environment**
    - To better ensure the safety of equipment and reduce potential cyber risks, we recommend:
        - Disable the port mapping function of the router to avoid direct access to the intranet devices from the external network.
        - The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub-networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, to achieve the network isolation effect.
        - Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
        - Enable the IP/MAC address filtering function to limit the range of hosts allowed to access the device.

Documents / Resources

Access Reader User's Manual	**Luminys RWCA Access Reader** [pdf] User Manual 2BHII-RWCA, 2BHIIRWCA, rwca, RWCA Access Reader, RWCA, Access Reader, Reader

References

- **User Manual**