Access Reader

User's Manual

V1.0.0

Foreword

General

This manual introduces the functions and operations of the Access Reader (herein referred as to 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.

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.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	March 2023

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 be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: 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 of 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, 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 of 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

 WARNING

- 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.

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, pursuant to 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 in accordance with 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 receiver.
- - Connect the equipment into 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 minimum distance 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 minimum distance 20cm between the radiator& your body.

Cet appareil est
Conforme aux limitesd'exposition de rayonnement RF ISEDC établiespour un environnement non contrôlé.
Cetémetteur ne doit pas être co-implanté oufonctionner en onjunction avec toute autreantenne ou transmetteur.
Cet équipement doit être installé et utilisé avec une distance minimale de 20cm entre le radiateur et votre corps.

IC Warning:
This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-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.

Cet appareil contient des émetteurs/récepteurs sans licence qui sont conformes aux RSS sans licence d'Innovation, Sciences et Développement économique Canada. L'exploitation est soumise aux deux conditions suivantes:
(1) Cet appareil ne doit pas causer d'interférences.
(2) Cet appareil doit accepter toute interférence, y compris les interférences qui pourraient causer un fonctionnement indésirable de l'appareil.

Table of Contents

1 Introduction

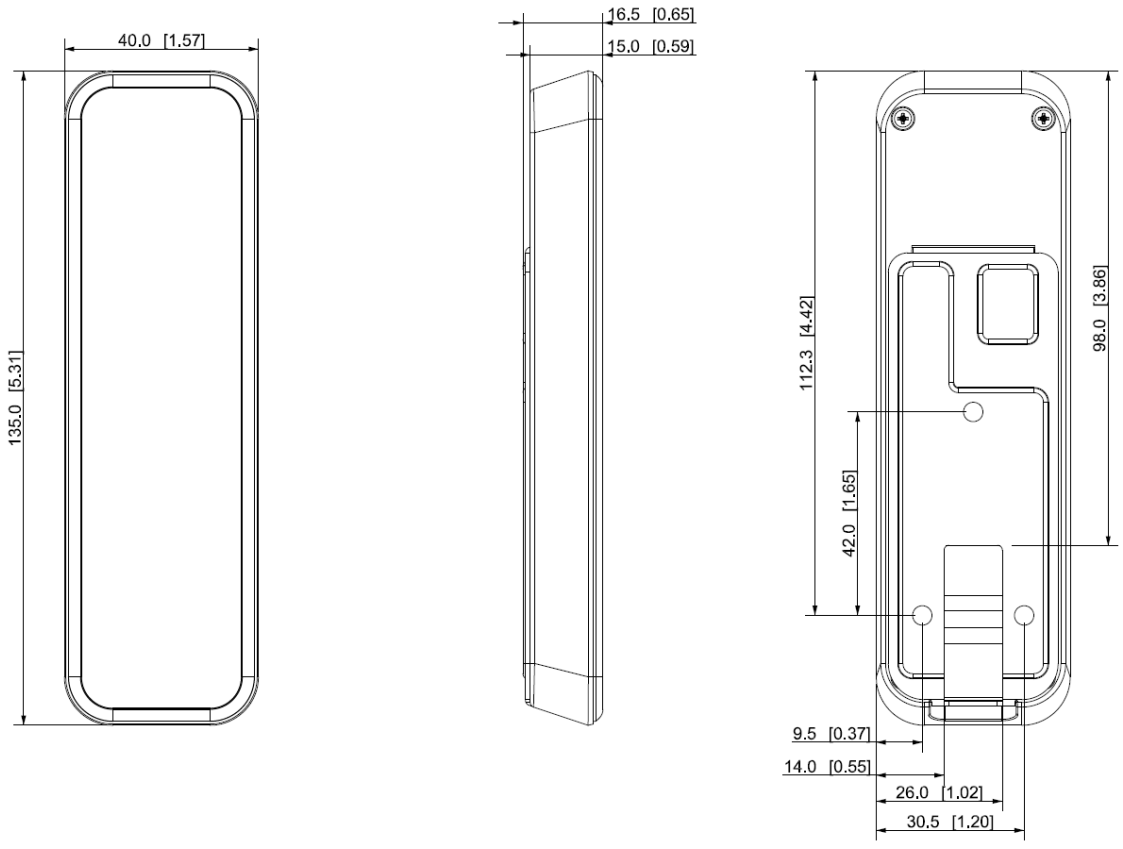
1.1 Features

- PC material, tempered glass panel and IP66, suitable for indoor and outdoor use.
- Contactless card reading for IC cards (Mifare cards).
- Unlock through card swiping and Bluebooth.
- Communicates through the RS-485 port, wiegand port, and Bluetooth.
- Prompts using the buzzer and indicator light.
- Supports the anti-tampering alarm.
- The built-in watchdog program can detect and control the abnormal operation status of the equipment and perform recovery processing to ensure the long-term operation of the equipment.
- All the connection ports have overcurrent and overvoltage protection.
- Works with the mobile client and select models of Access Controller .

Functions may vary according to different models.

1.2 Appearance

Figure 1-1 Dimensions of the LXK101-BD (mm [inch])



2 Ports Overview

Use RS–485 or Wiegand to connect the Device.

Table 2-1 Cable connection description

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	

Table 2-2 Cable specification and length

Device Type	Connection Method	Length
RS485 card reader	Each wire must be within 10 Ω.	100 m (328.08 ft)
Wiegand card reader	Each wire must be within 2 Ω.	80 m (262.47 ft)

3 Installation

Procedure

Step 1 Drill 4 holes and one cable outlet on the wall.

For surface-mounted wiring, cable outlet is not required.

Step 2 Put 3 expansion tubes into the holes.

Step 3 Wire the card reader, and pass the wires through the slot of the bracket.

Step 4 Use three M3 screws to mount the bracket on the wall.

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

Step 6 Screw in one M2 screw on the bottom of the card reader.

Figure 3-1 In-wall wiring

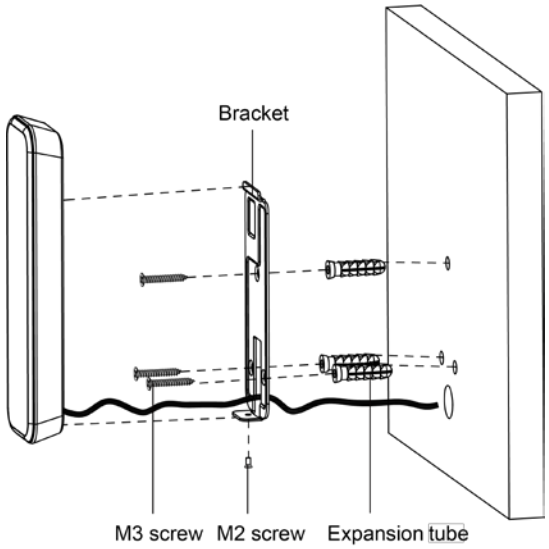
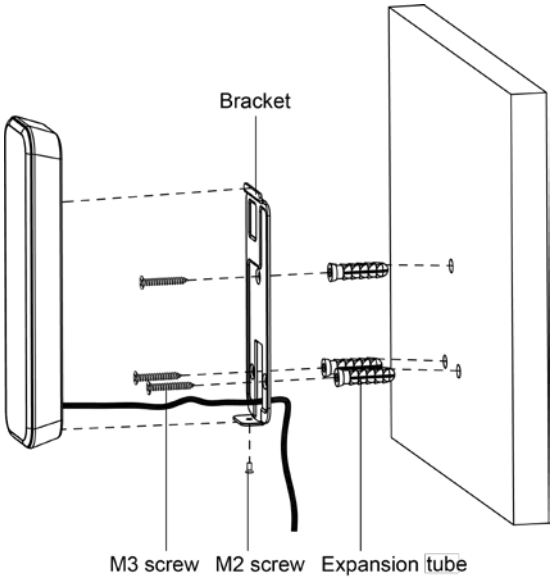


Figure 3-2 Surface mounted wiring



4 Sound and Light Prompt

Table 4-1 Sound and light prompt description

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

5 Unlocking the Door

Unlock the door through IC card or Bluetooth card.

5.1 Unlocking through IC Card

Unlock the door by swiping the IC card.

5.2 Unlocking through Bluetooth

Unlock the door through Bluetooth cards. The card reader must work with the Access controller to realize Bluetooth unlock. For details, see the user's manual of Access Controller.

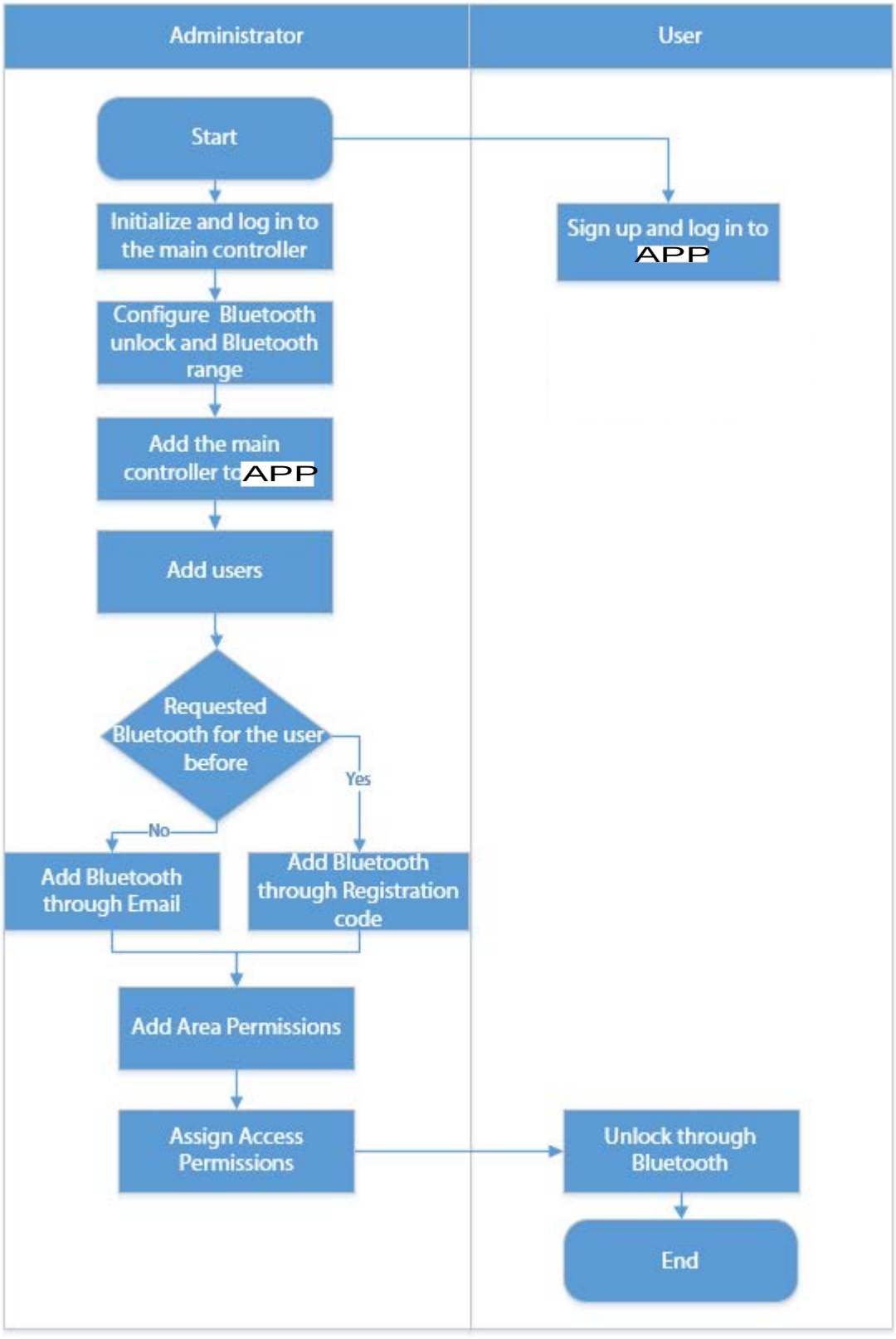
Prerequisites

General users like company employees have signed up to APP with their Email.

Background Information

Refer to the flowchart of configuring Bluetooth unlock. Administrator and general users needs to do different operations as below. General users like company employees only need to sign up and log in the APP with their Email, and then they can unlock through Bluetooth cards that are issued to them.

Figure 5-1 Flowchart of configuring Bluetooth unlock



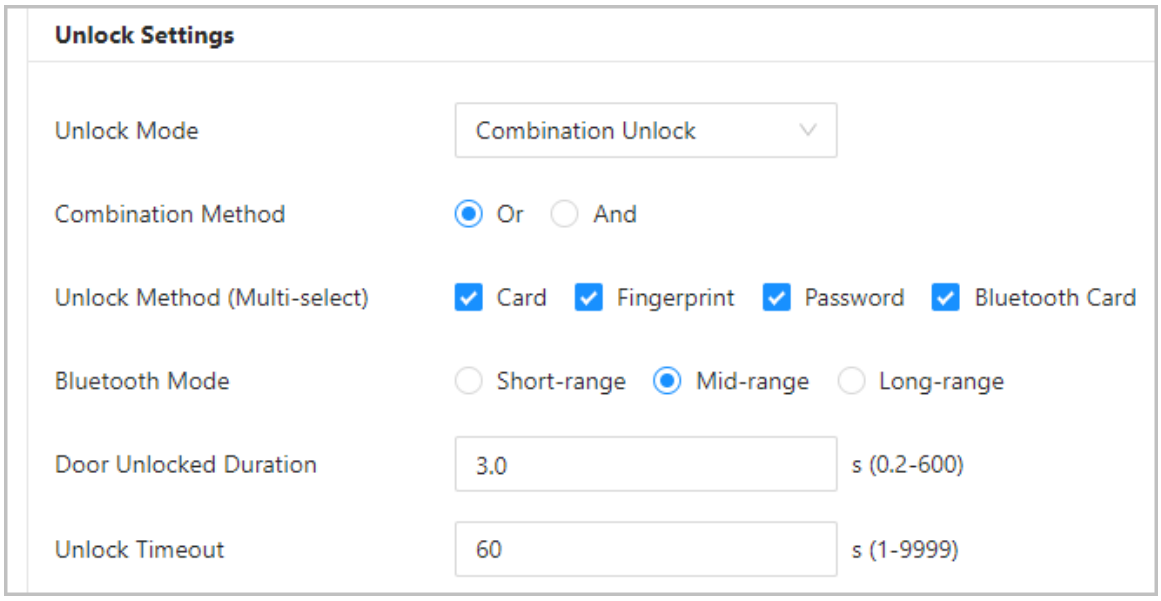
Administrator needs to perform Step1 to Step7, and general users need to perform Step8.

Procedure

Step 1 Initialize and log in to the main access controller.

Step 2 Turn on the Bluetooth card function and configure the Bluetooth range.

Figure 5-2 Unlock settings



The Bluetooth card must be a certain distance away from the access control device to exchange data and unlock the door. Following are the ranges that are most suitable for it.

- Short-range: The Bluetooth unlock range is less than 0.2 m.
- Mid-range: The Bluetooth unlock range is less than 2 m.
- Long-range: The Bluetooth unlock range is less than 10 m.

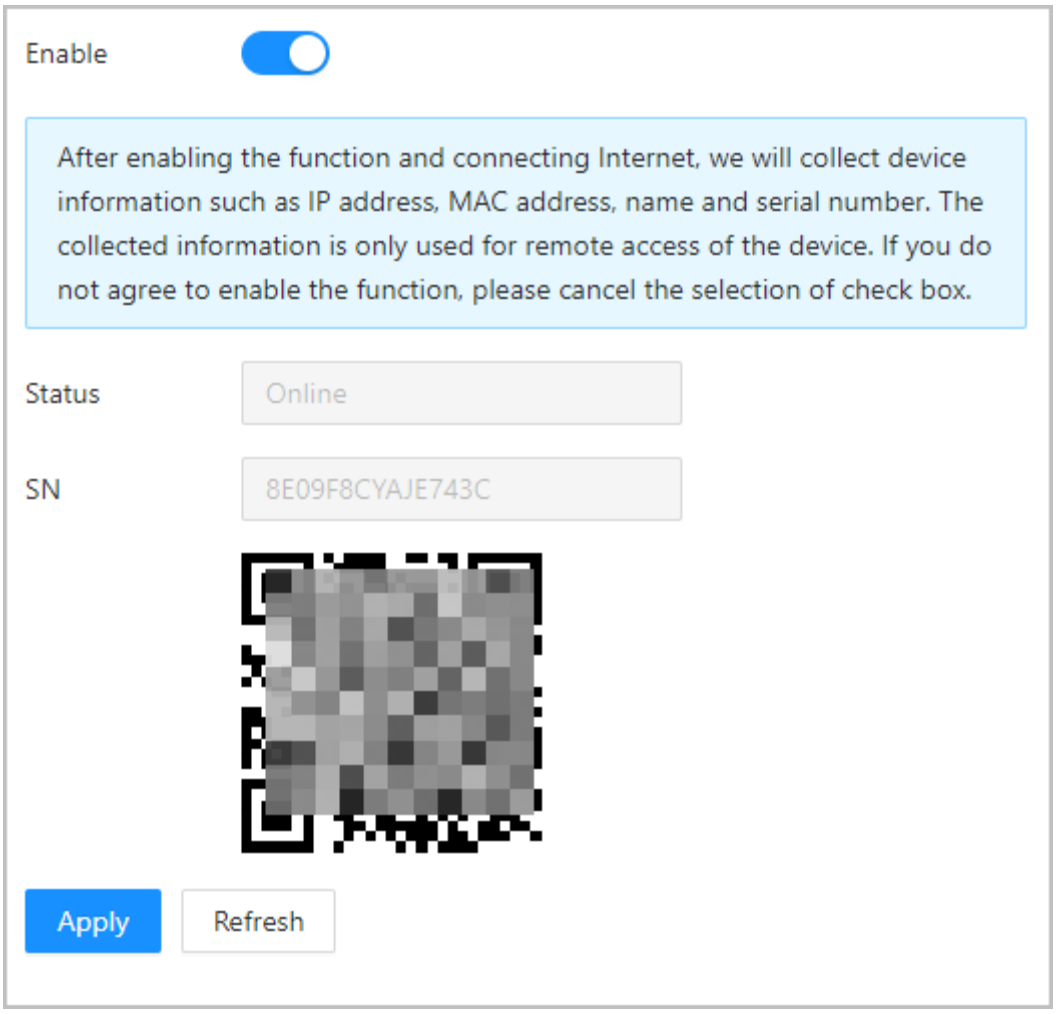
⚠

The Bluetooth unlock range might differ depending on models of your phone and the environment.

Step 3 Download APP and sign up with Email account, and then scan the QR code with APP to add the Access Controller to it.

Make sure the cloud service is turned on.

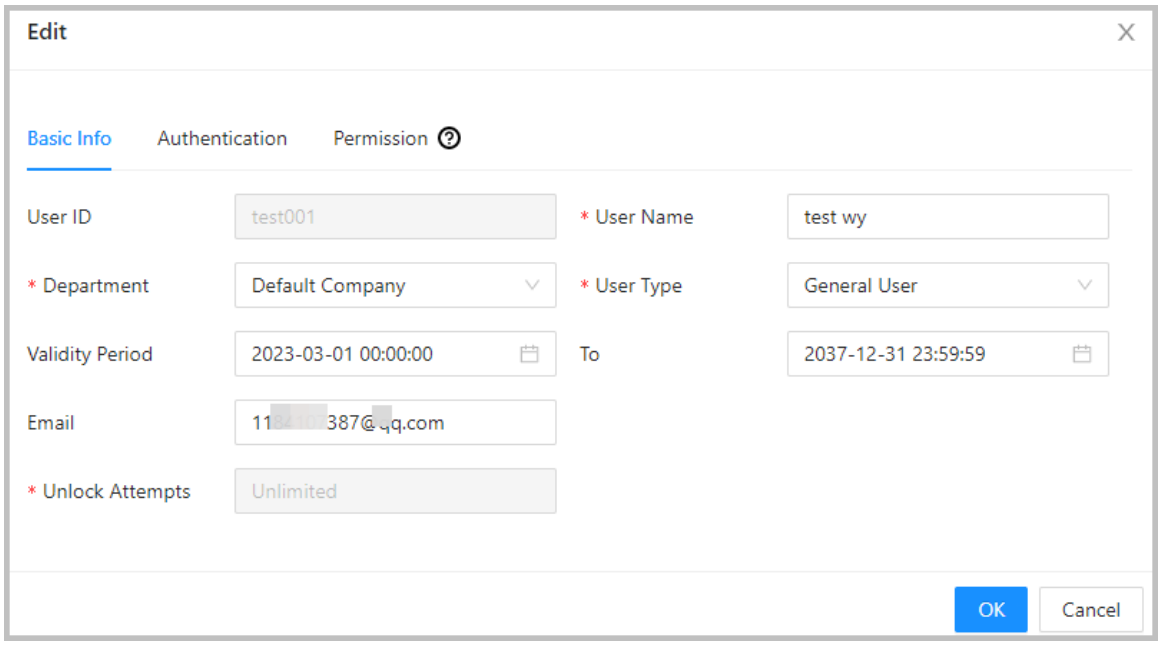
Figure 5-3 Cloud service



Step 4 Add uses to the main controller.

The email address you entered when adding users to the main controller must be same to the email account that users use to sign up to APP.

Figure 5-4 Basic information on the user

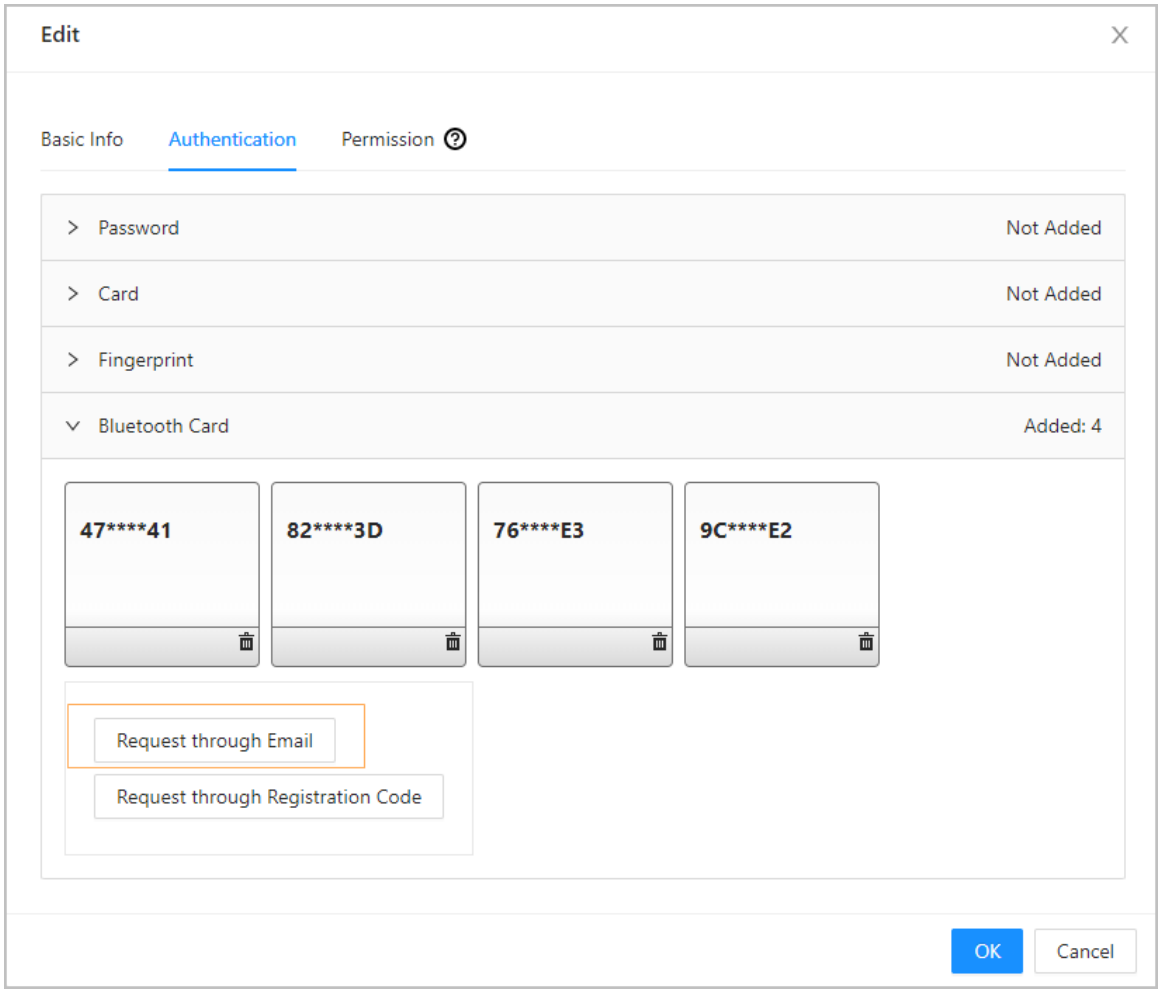


Step 5 On the tab, click **Bluetooth Card**.

3 methods are available to add Bluetooth cards.

- Request through Email one by one: Click **Request through Email**.
  A Bluetooth card is generated automatically. You can generate up to 5 cards for each user.

Figure 5-5 Request through Email

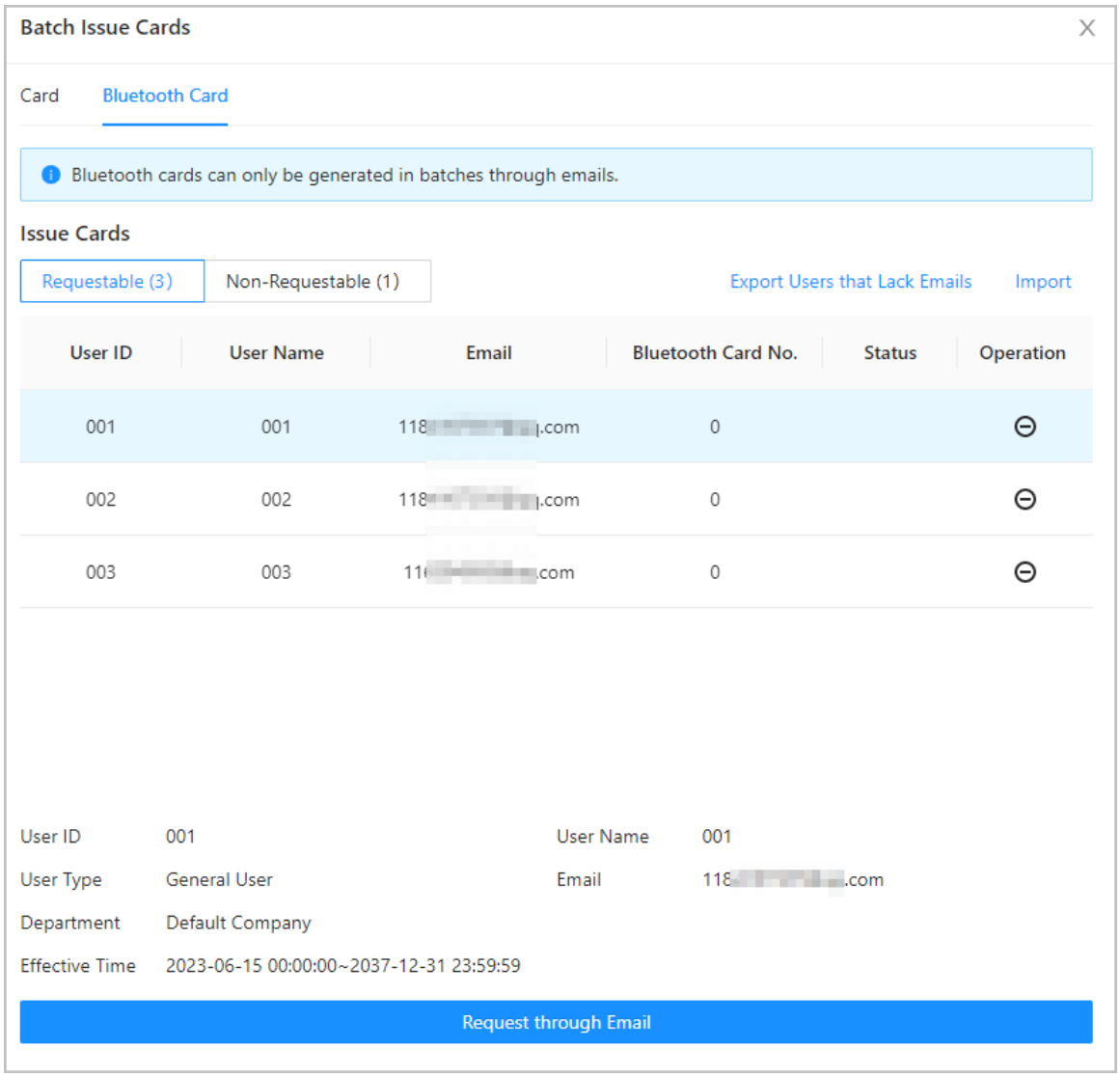


- Request through Email in batches.
  1. On the **Person Management** page, click **Batch Issue Cards**.

     Batch issue cards only supports requesting through Email.
     - Issue Bluetooth cards to all the users on the list: Click **Issue Cards to All Users**.
     - Issue Bluetooth cards to selected users: Select users, and then click **Issue Cards to Selected Users**.
  2. Click **Bluetooth Card**.
  3. Click **Request through Email**.

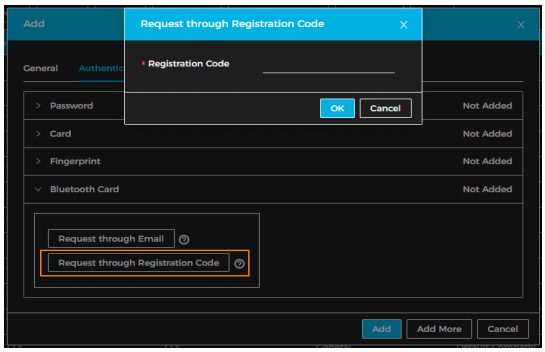
     - Users who do not have an email or already have 5 Bluetooth cards will be displayed on the non-requestable list.
     - Export users that lack emails: Click **Export**, enter the emails in the correct format, and then click **Import**. They will be moved to the requestable list.

Figure 5-6 Batch issue cards



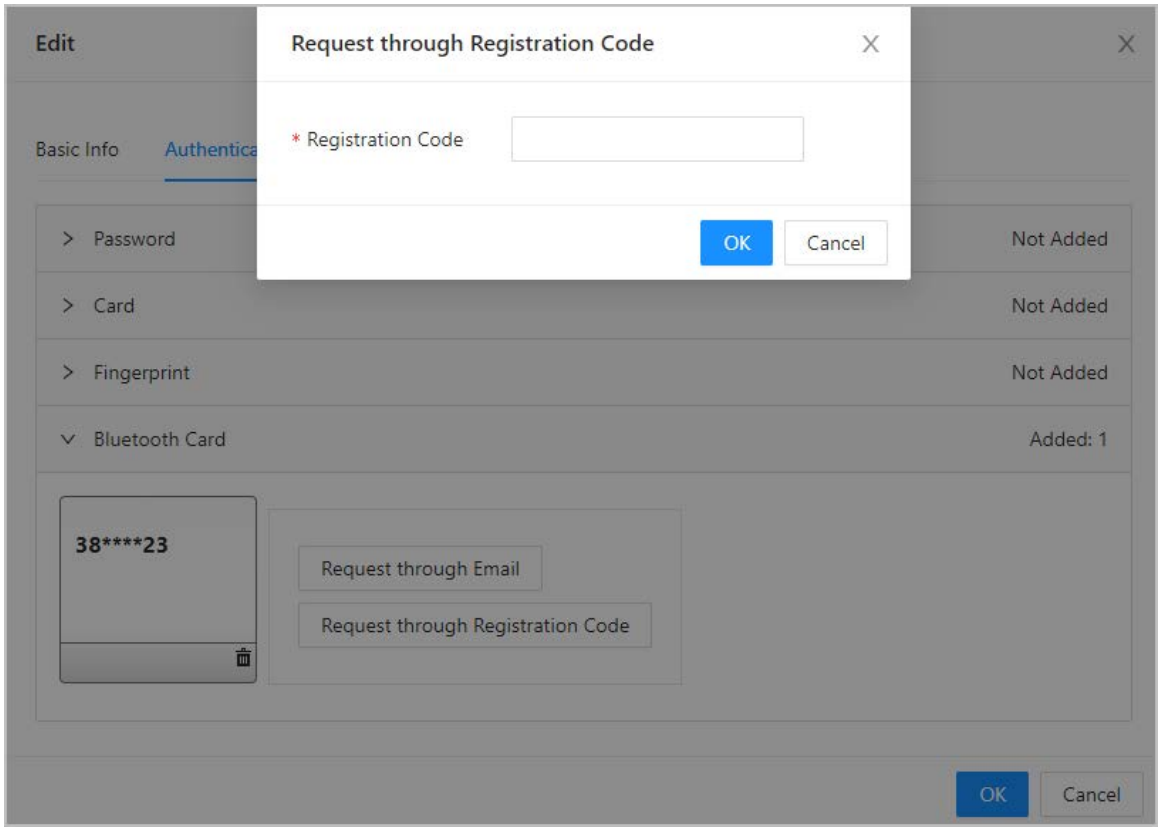
- If you have requested Bluetooth cards for the user before, you can add the Bluetooth cards through registration code. using registration codes.

Figure 5-7 The flowchart for requesting through registration code



1. On APP, tap **Registration Code** of a Bluetooth card.
   The registration code is automatically generated by APP.
2. Copy the registration code.
3. On the **Bluetooth Card** tab, click **Request through Registration Code**, paste the registration code, and then click **OK**.

Figure 5-8 Request through registration code

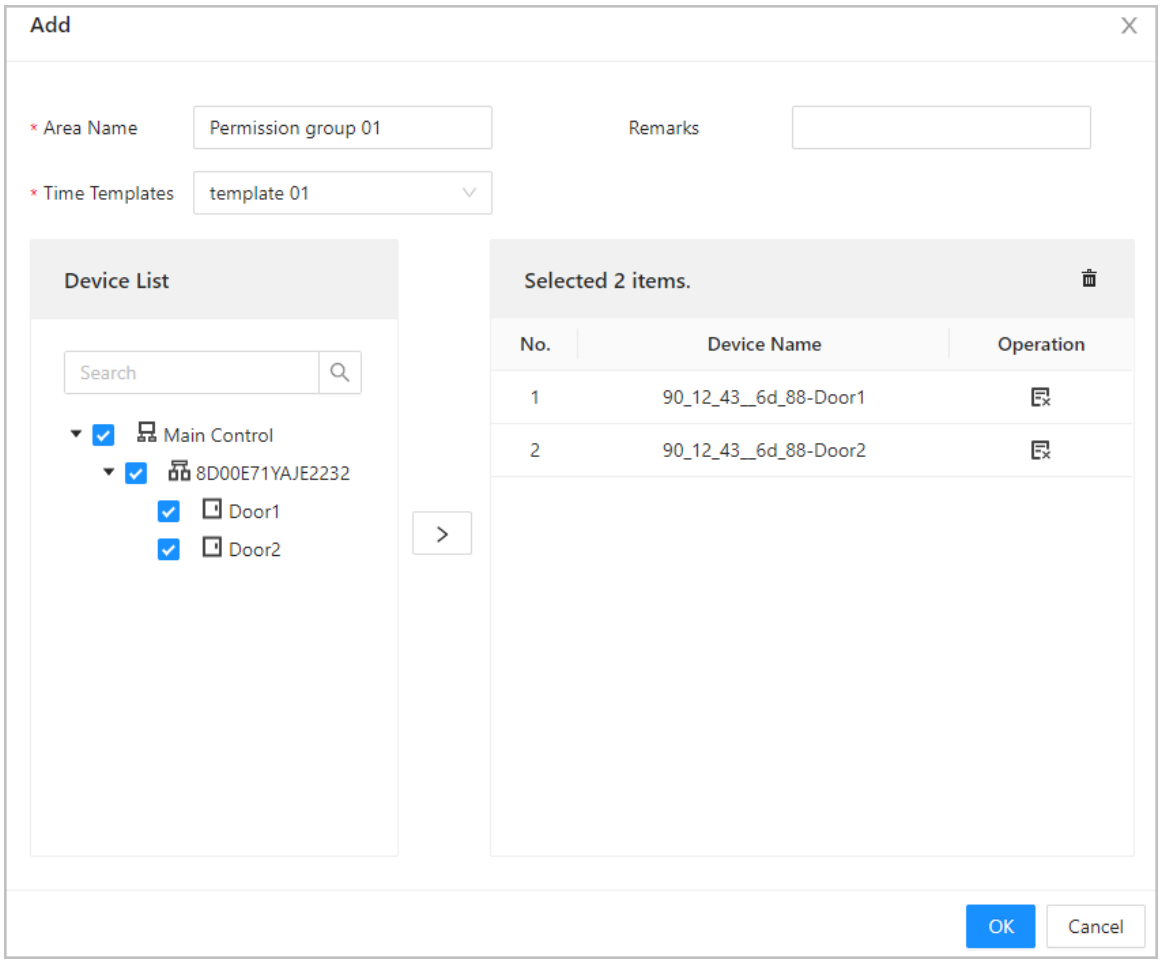


4. Click **OK**.
   The Bluetooth card is added.

Step 6 Add area permissions.

Create a permission group, and then associate users with the group so that users will be assigned with access permissions defined for the group.

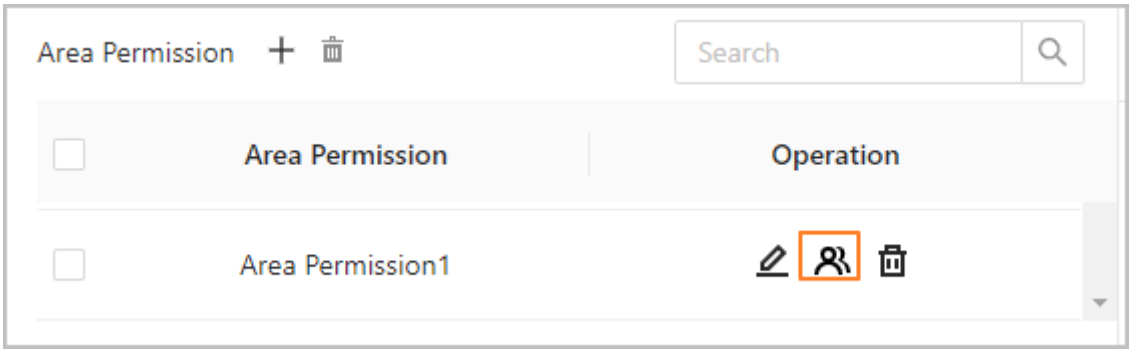
Figure 5-9 Create area permission groups



Step 7 Add access permissions to users.

Assign access permissions to users by linking them to the area permission group. This will allow the users to gain access to secure areas.

Figure 5-10 Select users



Step 8 After users sign up and log in to APP with the email address, they need to open APP to unlock the door through Bluetooth cards. For details, see the user's manual of APP.

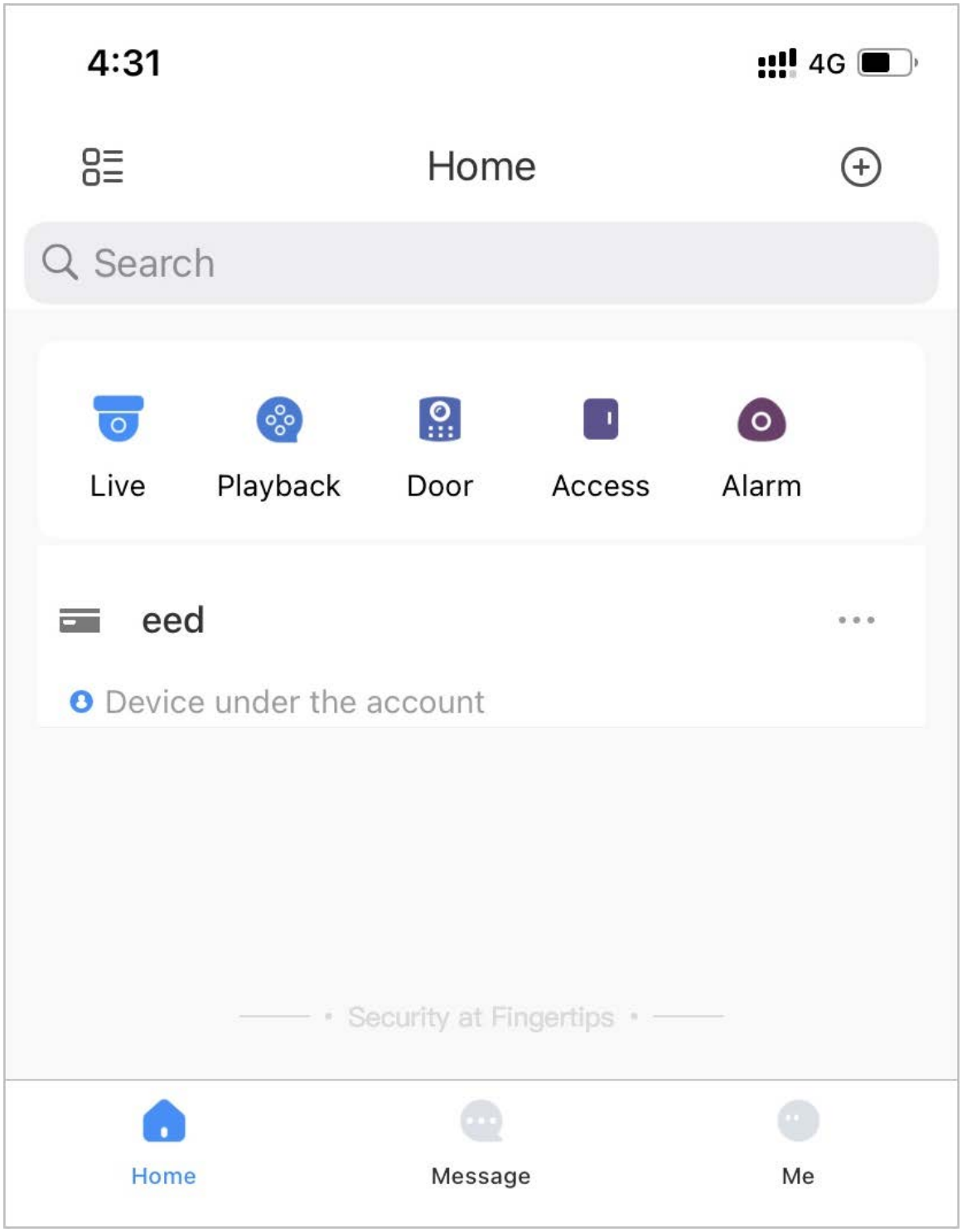
- Auto Unlock: The door automatically unlocks when you are in the defined Bluetooth range, which allow the Bluethooth card transmit signals to the card reader.

  In the auto unlock mode, the Buletooth card will frequently unlock the door if you are still in the Bluetooth range, and finally a failure might occur. Please turn off Bluetooth on the phone and turn it on again.

- Shake to Unlock: The door unlocks when you shake your phone to allow the Bluethooth

card transmits signals to the card reader.

Figure 5-11 Unlock the door through Bluetooth cards



Result

- Successfully unlock: The green indicator flashes and the buzzer sounds once.
- Failed to unlock: The red indicator flashes and the buzzer sounds 4 times.

6 Updating the System

Update the system of the card reader through the Access Controller or X poratl.

6.1 Updating through the Access Controller

Prerequisites

Connect the card reader to the Access Controller through RS-485.

Background Information

- Use the correct update file. Make sure that you get the correct update file from technical support.
- Do not disconnect the power supply or network, and do not restart or shutdown the Access Controller during the update.

Procedure

Step 1 On the home page of the Access Controller, select **Local Device Config** > **System Update**.

Step 2 In **File Update**, click **Browse**, and then upload the update file.

The update file should be a .bin file.

Step 3 Click **Update**.

After the system of the card reader is successfully updated, both the Access Controller and the card reader will restart.

6.2 Updating through X portal

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 X portal, and then select **Device upgrade**.

Step 2 Click of an access controller, and then click .

Step 3 Click **Upgrade**.

The indicator of the Card Reader flashes blue until 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 to set 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 Tech-industry, we recommend to keep 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 of firmware updates released by the manufacturer.
   - We suggest that you download and use the latest version of client software.

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

1. **Physical Protection**

   We suggest that you perform physical protection to 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.

2. **Change Passwords Regularly**

   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. **Set and Update Passwords Reset Information Timely**

   The device supports 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.

4. **Enable Account Lock**

   The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the 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.

5. **Change Default HTTP and Other Service Ports**

   We suggest you to change 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.

6. **Enable HTTPS**

   We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. **MAC Address Binding**

   We recommend you to bind the IP and MAC address of the gateway to the equipment, thus

reducing the risk of ARP spoofing.

8. **Assign Accounts and Privileges Reasonably**

   According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

9. **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 mailbox server.
   - FTP: Choose SFTP, and set up strong passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

10. **Audio and Video Encrypted Transmission**

    If your audio and video data contents are very important or sensitive, we recommend that you use 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.

11. **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.

12. **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.

13. **Construct a Safe Network Environment**

    In order 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 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, so as to achieve the network isolation effect.
    - Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
    - Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.