Access Control Card Reader

User's Manual

V1.0.1

# Foreword

General

This manual introduces the functions and operations of the Access Control Card Reader (hereinafter referred to as "the Device").

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
V1.0.1	Updated device models and added bluetooth card reader.	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 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

The following contents are about the proper ways of using the Device, preventing dangers and property damage when it is in use. Read the manual carefully before using the Device, strictly abide by the manual and properly keep it for future reference.

Transportation requirement

⚠

Transport the Device under allowed humidity and temperature conditions.

Storage requirement

⚠

Store the Device under allowed humidity and temperature conditions.

Installation requirements

⚠

- A non-switching mode linear DC power supply is recommended for the better reading distance.
- Power supply distance should not exceed 100 m; otherwise, it is recommended to use a dedicated power supply.
- The input voltage must be within 12 V ± 10% to make sure the Device works properly.
- Connect the device and access controller with the shielded RVVP0.5 cable or above.
- When the Device is installed outdoors or at places with high humidity or water infiltration, we recommend you protect the Device with a waterproof cover.
- To reduce the noise caused by long distance transmission, the shielding layer of the transmission cable should be the connected together with the ground wire of the Device and the ground wire of the access controller.

Operation Requirement

⚠

Use the Device under allowed humidity and temperature conditions.

Table of Contents

1 Introduction

The Device can read fingerprints and various kinds of cards. It sends signals to the access controller for identity verification. It is applicable to industrial zones, office buildings, schools, factories, stadiums, CBD, residential area, government properties, and more.

1.1 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 Device with ID card reading function), identity card reading (only for the Device with IC and CPU card reading function); QR code reading (only for the Device with QR code reading function); Bluetooth card reader (only for the Device with Bluetooth function).
- Features the built-in PSAM card slot and PSAM card, and supports CPU card identification with improved security based on the SM1 cryptographic algorithm (applicable to the Device with CPU card 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 device stability.
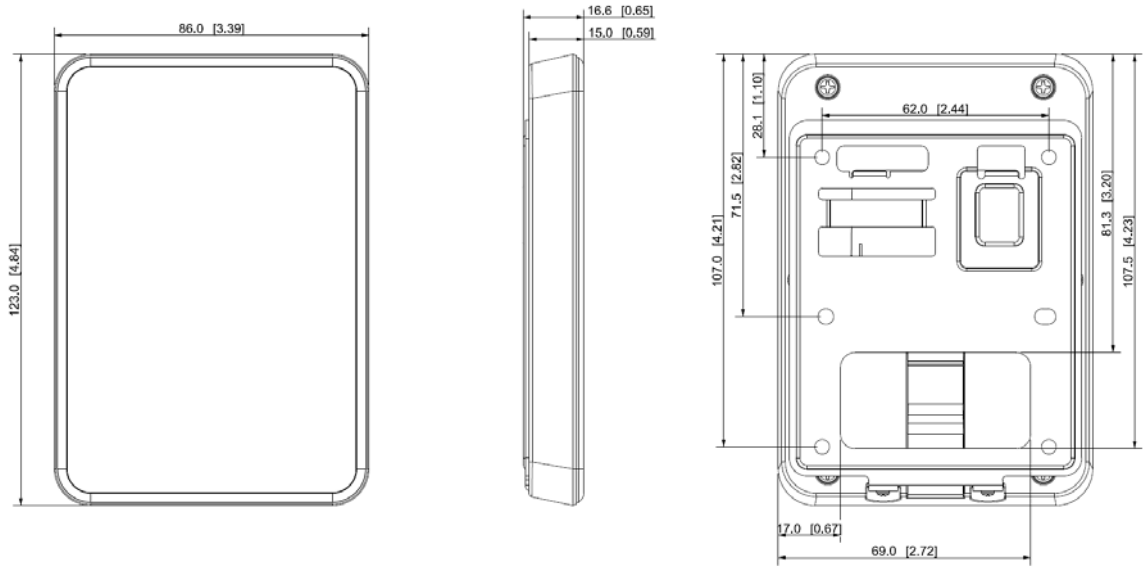- Safe and stable with overcurrent and overvoltage protection.

Functions may vary according to different models.

1.2 Device Appearance

The Device can be divided into 86 box model, slim model, and fingerprint mode according to their appearances.
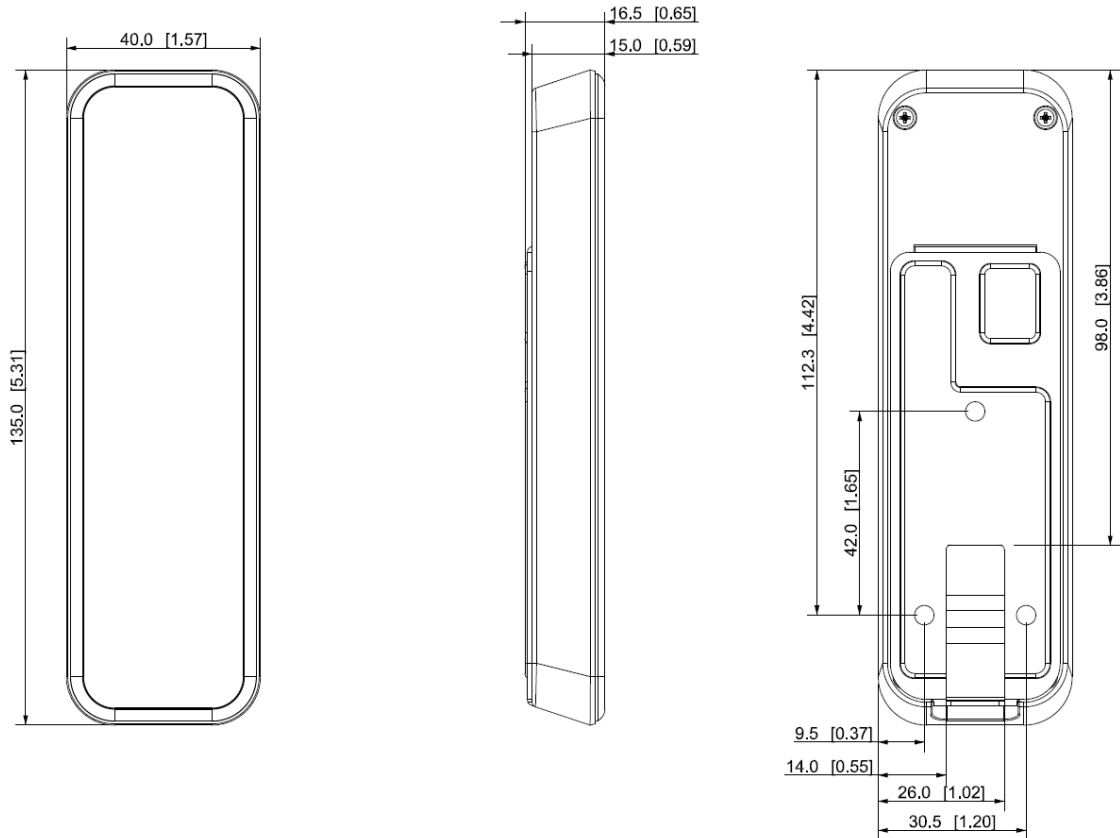
1.2.1 86 Box Model

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

86 box model can be further divided into Bluetooth card reader, QR code card reader, and general card reader according to their functions.
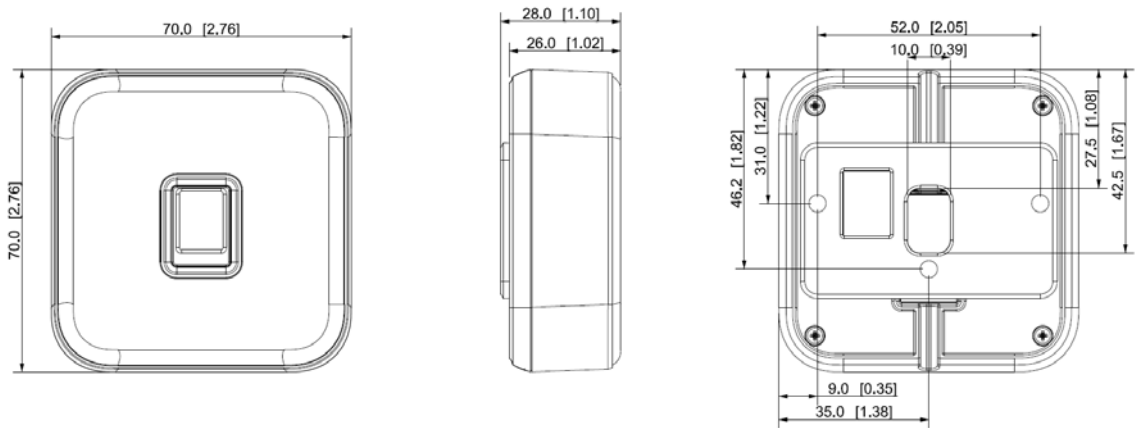
1.2.2 Slim Model

Figure 1-2 Dimensions of the slim model (mm [inch])

Slim model can be further divided into Bluetooth card reader and general card reader according to their functions.

1.2.3 Fingerprint Model

Figure 1-3 Dimensions of the fingerprint model (mm [inch])

2 Cable Connection

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

8-core Cables for the 86 Box and Slim Models

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	Wiegand transmission signal (effective only when using Wiegand protocol)
Brown	LED	Wiegand responsive signal (effective only when using Wiegand protocol)
Yellow	RS–485_B	RS–485_B
Purple	RS–485_A	RS–485_A

5-core Cables for the Fingerprint Model

Table 2-2 Cable connection description (2)

Color	Port	Description
Red	RD+	PWR (12 VDC)
Black	RD–	GND
Blue	CASE	Tamper alarm signal
Yellow	RS–485_B	RS–485_B
Purple	RS–485_A	RS–485_A

Table 2-3 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

The recommended installation height (from the center of the Device to the ground) is 130 cm–150 cm (51.18"–59.06"), and should not be over 200 cm (78.74").

3.1 Installing the 86 Box Model

With an 86 Box

Figure 3-1 Install with an 86 box
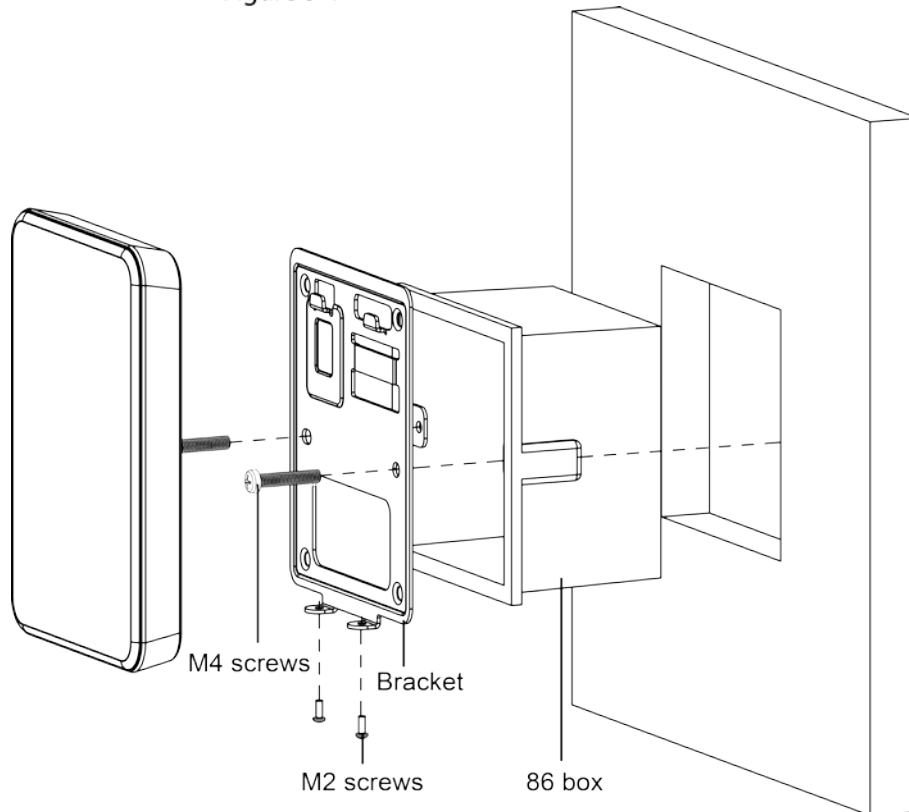
Step 1 Fit the 86 box into the wall.
Step 2 Connect the wires of the Device and put them inside the 86 box.
Step 3 Use two M4 screws to fix the bracket to the 86 box.
Step 4 Attach the Device onto the bracket from top down.
Step 5 Use two M2 screws to secure the Device onto the bracket.

Wall Mount

Figure 3-2 Wall mount

Bracket

M3 Screw   M2 screw   Expansion tube
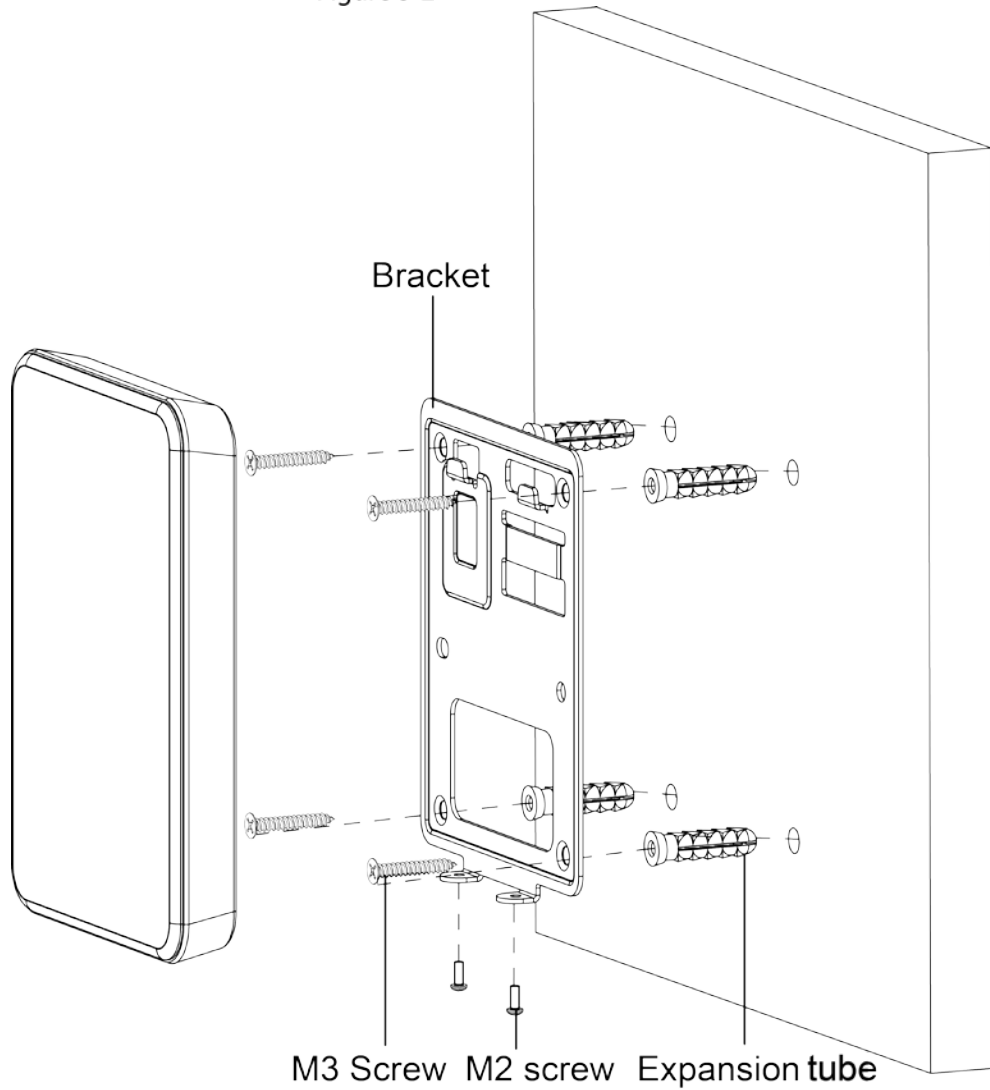
Step 1   Drill holes on the wall.
Step 2   Put four expansion bolts into the holes.
Step 3   Connect the wires of the Device and put them inside the wall.
Step 4   Use two M3 screws to fix the bracket on the wall.
Step 5   Attach the Device onto the bracket from top down.
Step 6   Use two M2 screws to secure the Device onto the bracket.

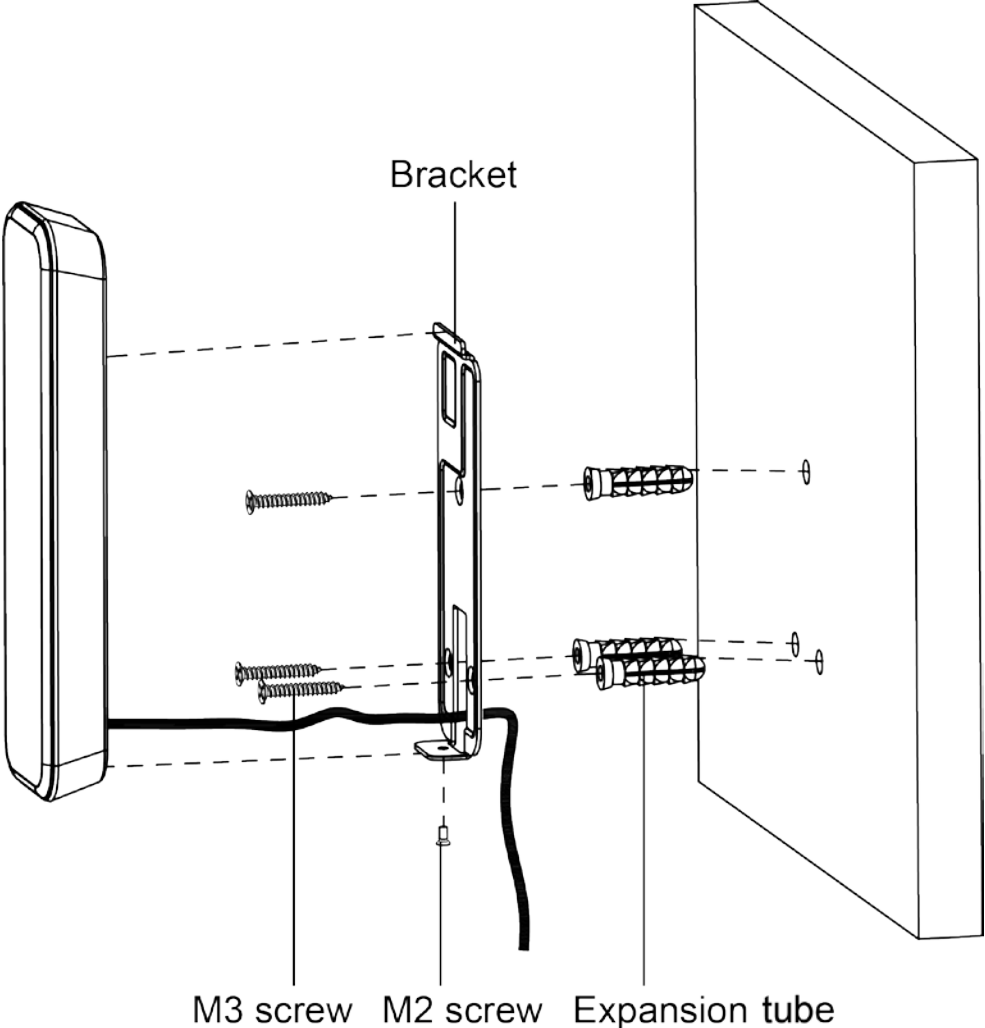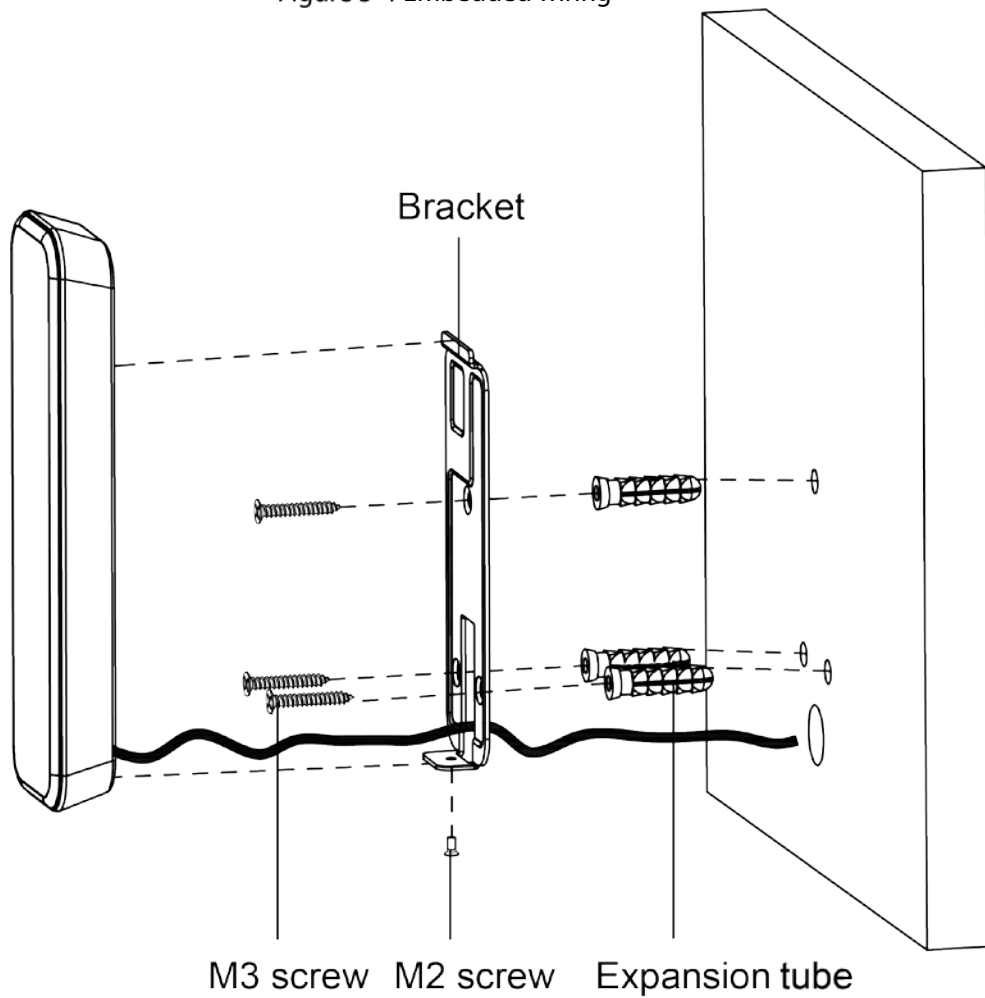## 3.2 Installing the Slim Model

Figure 3-3 Surface wiring

Bracket

M3 screw   M2 screw   Expansion tube

Figure 3-4 Embedded wiring

Bracket

M3 screw   M2 screw   Expansion tube

Step 1   Drill holes on the wall.
Step 2   Put three expansion bolts into the holes.
Step 3   Connect the wires of the Device and thread them through the slot of the bracket.
Step 4   (Optional) Put the wires inside wall.
Step 5   Use three M3 screws to fix the bracket on the wall.
Step 6   Attach the Device onto the bracket from top down.
Step 7   Use one M2 screw to secure the Device onto the bracket.

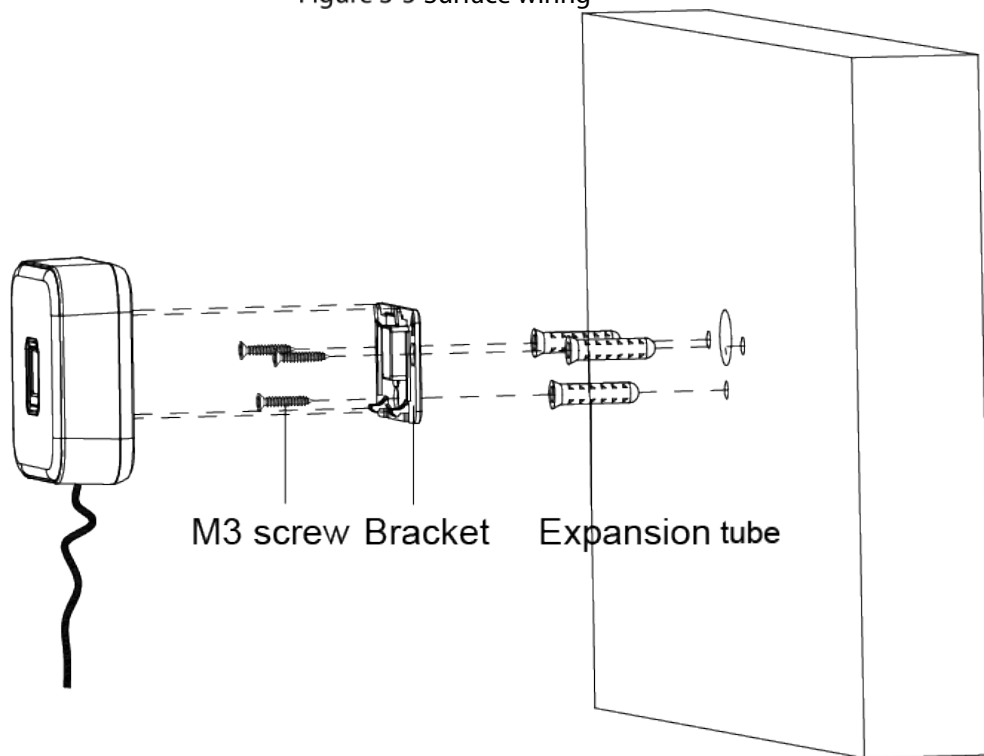# 3.3 Installing the Fingerprint Model
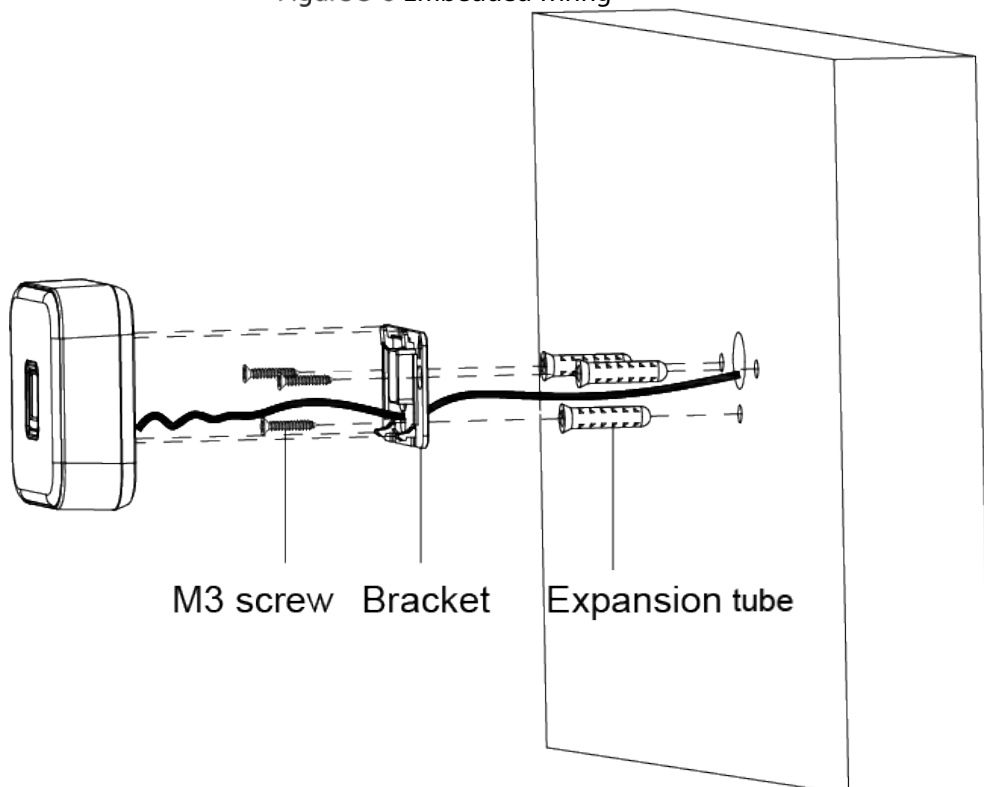
Figure 3-5 Surface wiring

Figure 3-6 Embedded wiring

Procedure

Step 1 On the wall, drill three holes for expansion bolts and one hole for the wires.
Step 2 Put three expansion bolts into the holes.
Step 3 Use three M3 screws to fix the bracket on the wall.
Step 4 Connect the wires of the Device.
Step 5 (Optional) Put the wires inside the wall.

Step 6 Attach the device onto the bracket from top down.
Step 7 Press the Device hard toward the arrow direction until you hear a "click", and the installation completes.
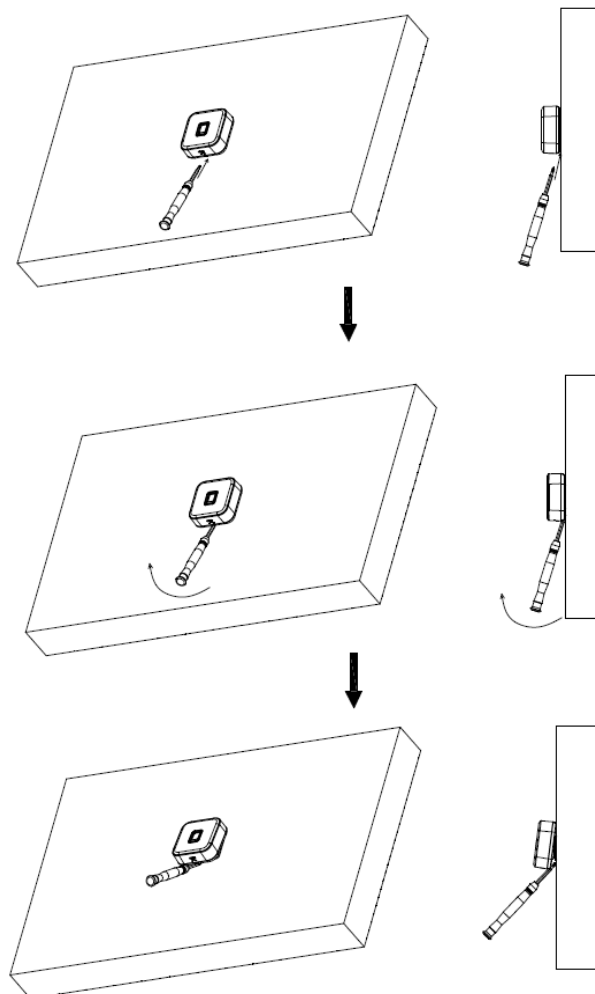
Figure 3-7 Press the Device hard until you hear a "click"
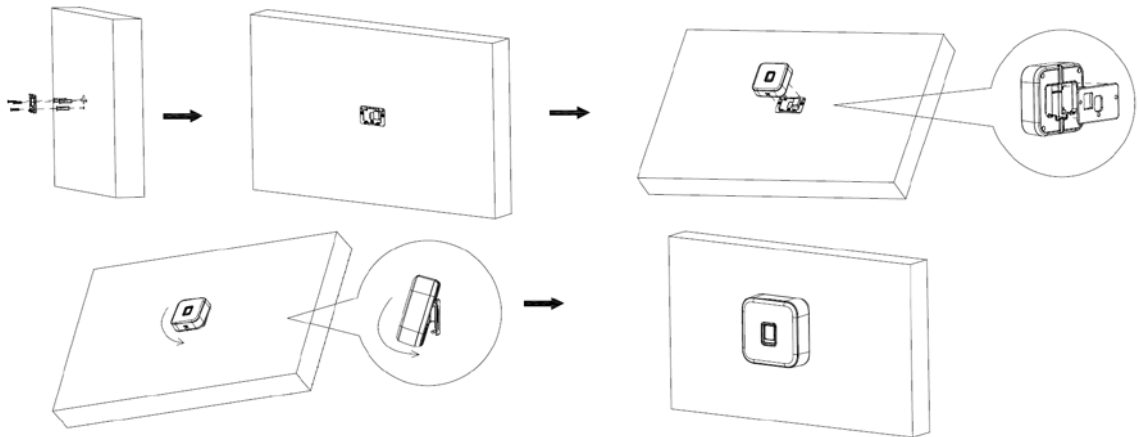
Related Operation

To unbuckle the Device from the wall, insert the provided screwdriver in the slot on the bottom, pry the Device open according to the arrow direction below until you hear a "click".

Figure 3-8 Unbuckle the Device

4 Configuring Bluetooth Card Reader

The Bluetooth card reader is used together with the Easy4Key app to open the door remotely.

Prerequisites

- The latest version of the SmartPSS AC is installed on the computer.
- Card swiping permissions have been successfully assigned to users. For details, see the user manual of the SmartPSS AC.
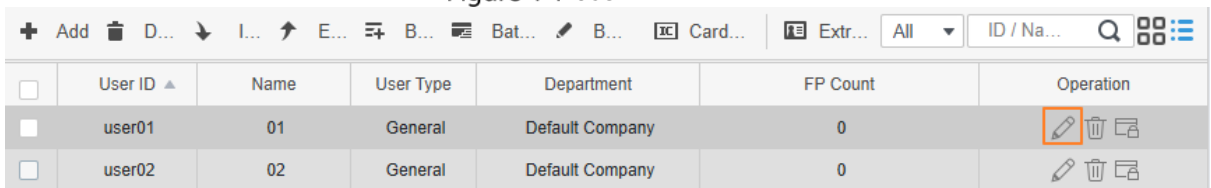- Easy4Key app is installed on the phone.

Procedure

Step 1   Log in to the SmartPSS AC.

Step 2   Select "Access Solution > Personnel Manager".

Step 3   Select the added user and click [pencil icon].

Figure 4-1 User

	User ID ▲	Name	User Type	Department	FP Count	Operation
☐	user01	01	General	Default Company	0	✎ 🗑 🖽
☐	user02	02	General	Default Company	0	✎ 🗑 🖽

Toolbar: ➕ Add 🗑 D... ↓ I... ↑ E... ⊟ B... ▬ Bat... ✎ B... 🆔 Card... 🗒 Extr... All ▾ ID / Na... 🔍 ▦ ☰

Step 4   Click "Certification", and then click [icon]

Figure 4-2 Certification

Edit user

Basic Info | Certification | Permission configuration

Card Add ⚠ The card number must be added if not the 2nd generation access controller is used. ⚙

122334
Card Issuin... 2021-12-03
Card Repla... 2021-12-03

[1] [icons]

Display QR Code ✕

Fingerprint ⚙

➕ Add 🗑 Delete
☐ Fingerprint Name

Finish   Cancel
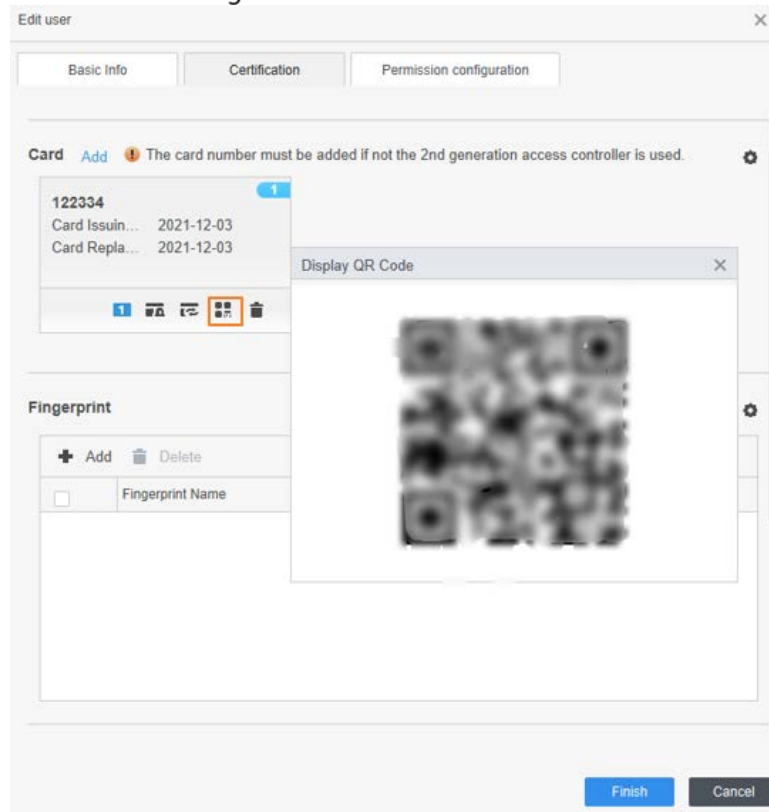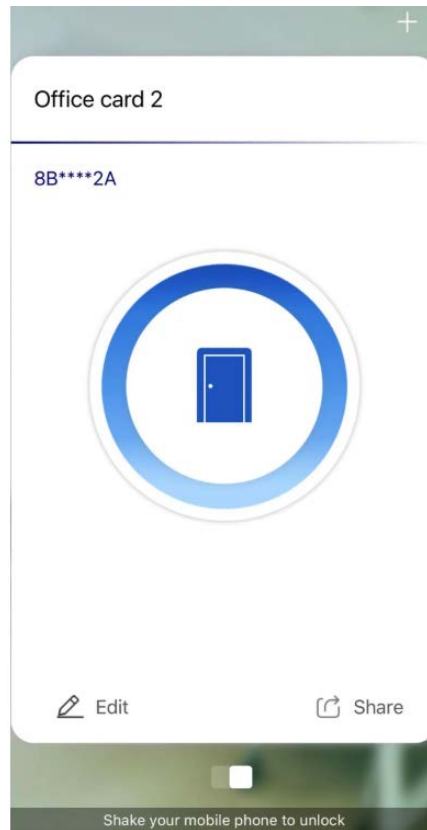
Step 5   Open Easy4Key on the phone and click

Step 6   Scan the QR code on the SmartPSS AC to add the card.

After the card is successfully added, the user can open the door through Easy4Key on the phone.

📖

The distance between the phone and the card reader must be less than 10 m.

Figure 4-3 Easy4Key

5 Sound and Light Prompt

After the Device is powered on, the Device will buzz once and the indicator is solid blue, which means the Device is working properly.

⚠

The Device can only read one card at a time. When multiple cards stack together, it cannot work properly.

5.1 86 Box and Slim Models

The sound and light prompt of the 86 box and slim models are the same.

Figure 5-1 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.

5.2 Fingerprint Model

Figure 5-2 Sound and light prompt description

Situation	Sound and Light Prompt
Device is powered on	Buzz once. The indicator is solid blue.

Situation	Sound and Light Prompt
Removing the Device.	Long buzz for 15 seconds.
Alarm linkage triggered by the controller.	Long buzz for 15 seconds.
485 communication and swiping an authorized card.	Buzz once. The indicator flashes green once, and then turns to solid blue as standby mode.
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 or unauthorized card/ fingerprint.	Buzz three times. The indicator flashes red once, and then turns to solid blue as standby mode.
485 communication and a fingerprint is recognized	Buzz once.
485 communication and swiping an authorized fingerprint	Buzz twice with 1 second interval. The indicator flashes green once, and then turns to solid blue as standby mode.
485 communication and swiping an unauthorized fingerprint	Buzz once, and then four times. The indicator flashes red once, and then turns to solid blue as standby mode.
Fingerprint operations, including adding, deleting and synchronization	The indicator flashes green.
Exiting fingerprint operations, including adding, deleting and synchronization	The indicator is solid blue.
Software updating or waiting for update in BOOT	The indicator flashes blue until update is complete.

6 Device Update

6.1 SmartPSS AC

Use SmartPSS AC to update the Device through the access controller.
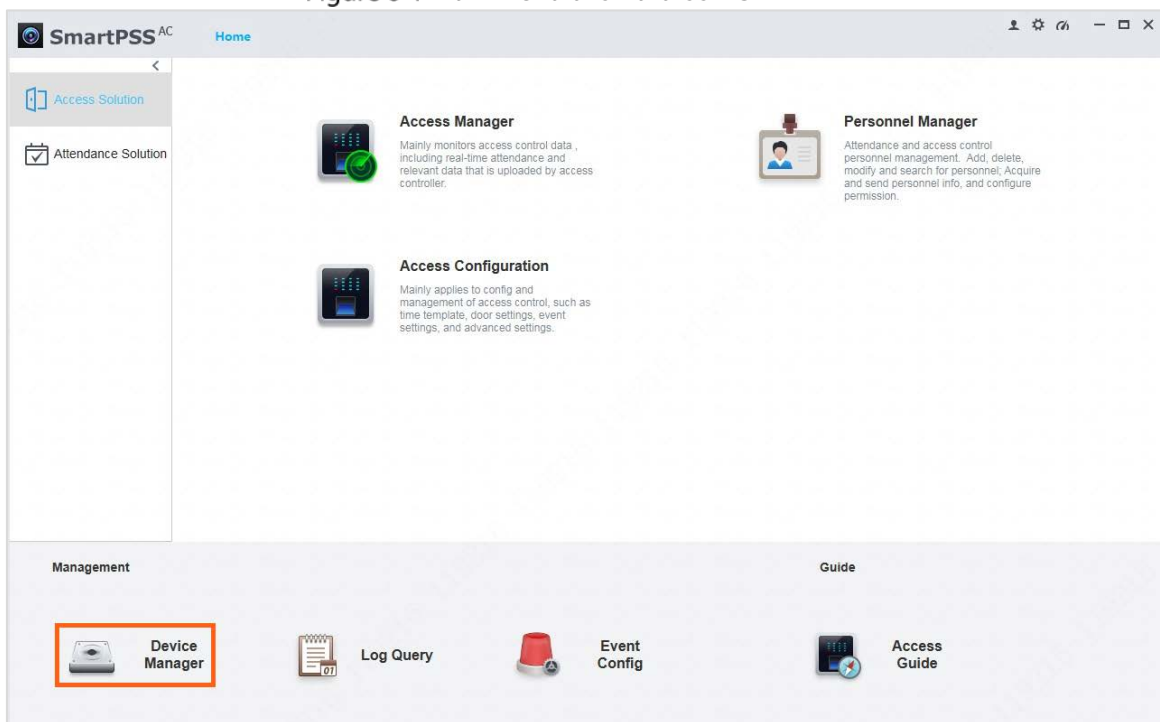
Prerequisites

- The Device and access controller are connected and powered on.
- SmartPSS AC is installed on your PC.

Procedure

Step 1   Log in to SmartPSS AC, and then select **Device Manager**.
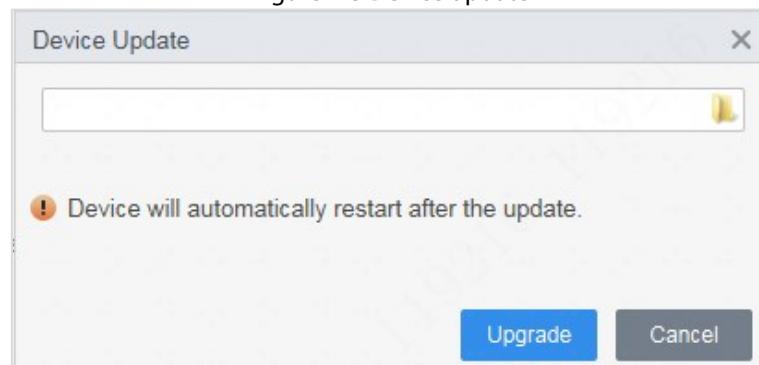
Figure 6-1 Main menu of SmartPSS AC

Step 2   Click

Figure 6-2 Select the access controller

Step 3   Click   and   to select the update file.

Figure 4-3 Device update

Step 4   Click **Upgrade.**
         The indicator of the Device flashes blue until update is completed, and then the Device automatically restarts.

6.2 Configuration Tool

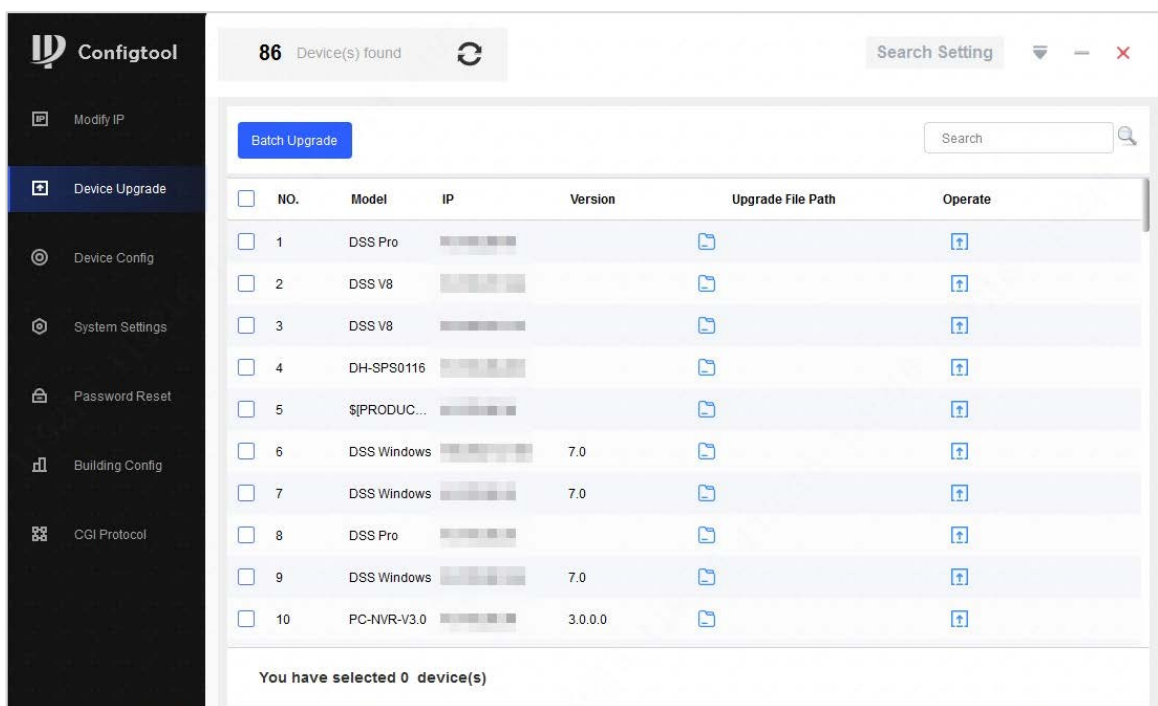Use the Configtool to update the Device through the access controller.

Prerequisites
- The Device and the access controller are connected and powered on.
- The Configtool is installed on your computer.

Procedure
Step 1   Open the Configtool, and then select **Device upgrade**.

Figure 4-4 Main menu of the Configtool

Step 2   Click 📁 and select the update file for each access controller, and then click ⬆.
Step 3   Click **Batch Upgrade.**
         The indicator of the Device flashes blue until update is completed, and then the Device automatically restarts.

Figure 4-5 Batch update

	NO.	Model	IP	Version	Upgrade File Path	Operate
☐	16	VTH5422H		4.500.0000000.0.R 📁		⬆
☐	17	VTS5340B		4.500.0000000.5.R 📁		⬆
☐	18	ASI7214Y-V3		1.000.0000006.3.R 📁		⬆
☐	19	VTH5422H		4.500.0000000.0.R 📁		⬆
☐	20	DH-ASI7223...		1.000.0000002.5.R 📁		⬆
☐	21	VTH2421F		4.500.0000000.5.R 📁		⬆
☐	22	VTH5441G		4.500.0000000.4.R 📁		⬆

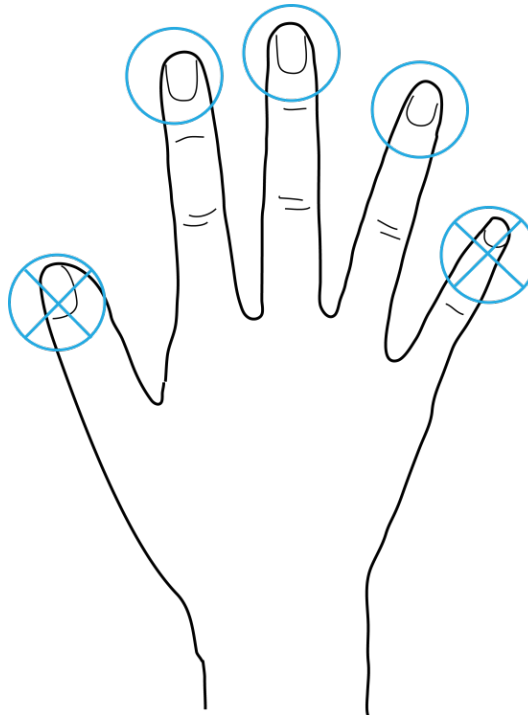# Appendix 1 Fingerprint Collecting Instruction

Precautions

- Make sure that your fingers are clean and dry before collecting your fingerprints.
- Do not expose the fingerprint scanner to high temperature and humidity.
- If your fingerprints are worn or unclear, use other methods including password and card.

Recommended Fingers

Forefingers, middle fingers, and ring fingers are recommended. Thumbs and little fingers cannot be put at the capturing center easily.

Appendix Figure 1-1 Recommended fingers

Correct Way of Pressing Your Finger

Press you finger to the fingerprint collecting area, and align the center of your fingerprint to the center of the collecting area.

Appendix Figure 1-2 Correct way
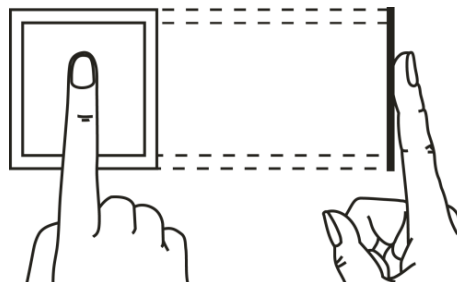
Appendix Figure 1-3 Incorrect ways

Fingerprint not entirely
on the collecting area

Fingerprint not on the
center of the collecting area
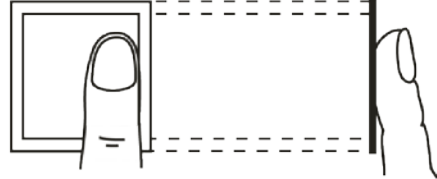
Fingerprint not on the
center of the collecting area
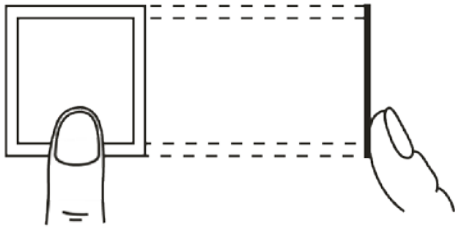
Fingerprint not on the
collecting area
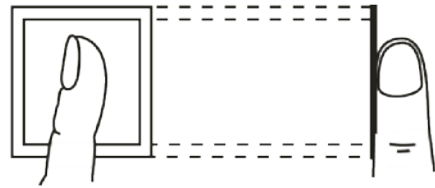
Appendix 2 QR Code Scanning Requirements

📖

- To ensure better QR code scanning performance, good lighting conditions are required, and the illuminator is required to give light at night or on cloudy days.
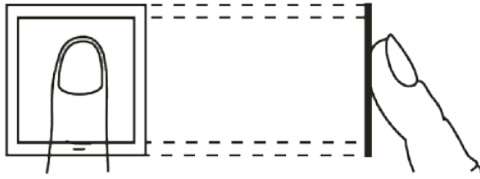- The distance between the QR code and the scanning lens of the reader is 3 cm – 30 cm.
- The size of the QR code should not be less than 30 mm × 30 mm.
- The byte capacity of QR code must be less than 100 bytes, and the two-dimensional code paper needs to be flat.
- The privacy film attached to the phone might affect scanning performance.

Appendix Figure 2-1 Distance requirement
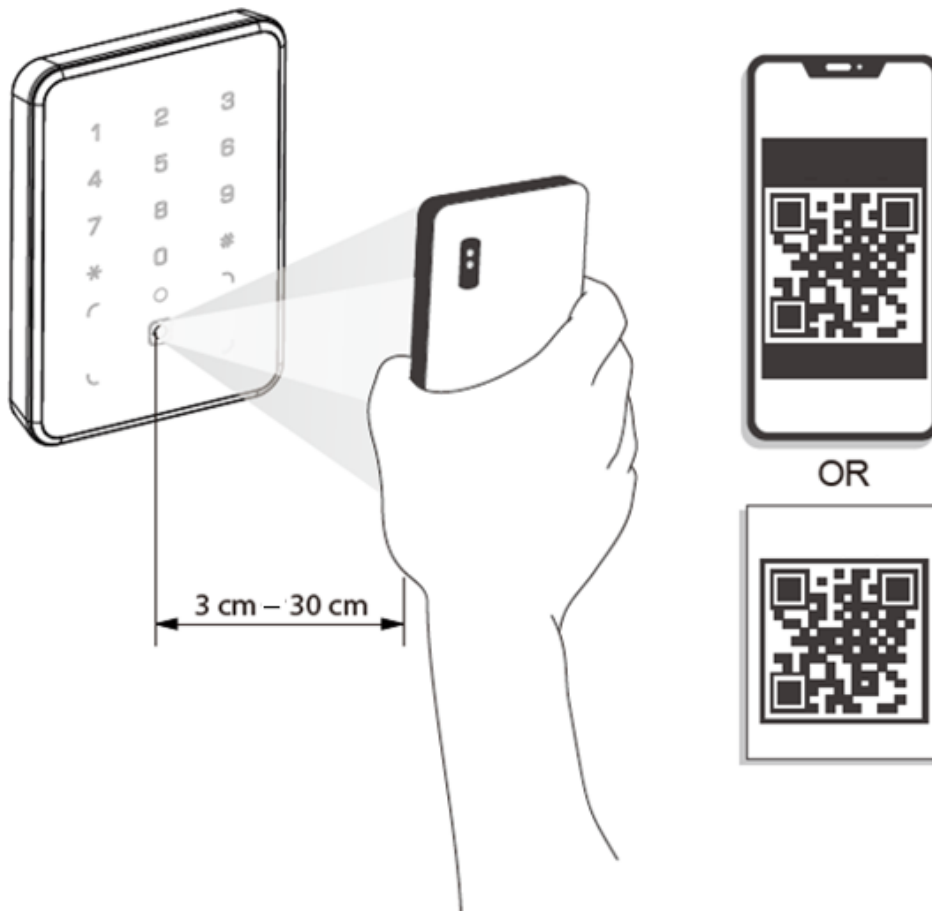
Appendix 3 Cybersecurity Recommendations

Mandatory actions to be taken for basic device 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 device (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 device 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 device network security:
1. **Physical Protection**
   We suggest that you perform physical protection to device, especially storage devices. For example, place the device 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 device (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 device, 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 device 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 device, 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 device 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.