Face Recognition Access Controller

Quick Start Guide

V1.0.1

Foreword

General

This manual introduces the functions and operations of the Face Recognition Access Controller (hereinafter referred to as the "Access Controller"). 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 Date
V1.0.1	Updated the wiring.	June 2022
V1.0.0	First release	August 2019

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 Access Controller, hazard prevention, and prevention of property damage. Read carefully before using the Access Controller, and comply with the guidelines when using it.

Transportation Requirement

⚠

Transport, use and store the Access Controller under allowed humidity and temperature conditions.

Storage Requirement

⚠

Store the Access Controller under allowed humidity and temperature conditions.

Installation Requirements

⚠ WARNING

- Do not connect the power adapter to the Access Controller 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 Access Controller to two or more kinds of power supplies, to avoid damage to the Access Controller.
- 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 Access Controller in a place exposed to sunlight or near heat sources.
- Keep the Access Controller away from dampness, dust, and soot.
- Install the Access Controller on a stable surface to prevent it from falling.
- Install the Access Controller 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 Access Controller label.
- The Access Controller is a class I electrical appliance. Make sure that the power supply of the Access Controller 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 Access Controller while the adapter is powered on.
- Operate the Access Controller within the rated range of power input and output.
- Use the Access Controller under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the Access Controller, and make sure that there is no object filled with liquid on the Access Controller to prevent liquid from flowing into it.
- Do not disassemble the Access Controller without professional instruction.
- This product is professional equipment.

Table of Contents

Foreword .... **II**

Important Safeguards and Warnings .... **IV**

1 Overview **1**

1.1 Features 1

1.2 Dimensions 1

2 Installation **2**

2.1 Application Diagram 2

2.2 Component 2

2.3 Installation 3

3 Cable Connection **5**

3.1.1 Wiegand/RS-485 5

3.1.2 Lock/Door Contact/Exit Button 6

3.1.3 Alarm Input/Output 7

3.1.4 Other Cables 8

4 Operations **9**

4.1 Standby Verification 9

4.2 User Management 9

4.2.1 Adding User 9

4.2.2 Deleting Users 10

4.2.3 Clearing Users 10

4.2.4 Switching Work Mode 10

4.3 USB Flash Drive Management 10

4.3.1 Exporting Data 11

4.3.2 Importing Data 11

4.3.3 Updating Access Controller 11

Appendix 1 Fingerprint Record Instruction **12**

Appendix 2 Packing List **14**

Appendix 3 Cybersecurity Recommendations **15**

1 Overview

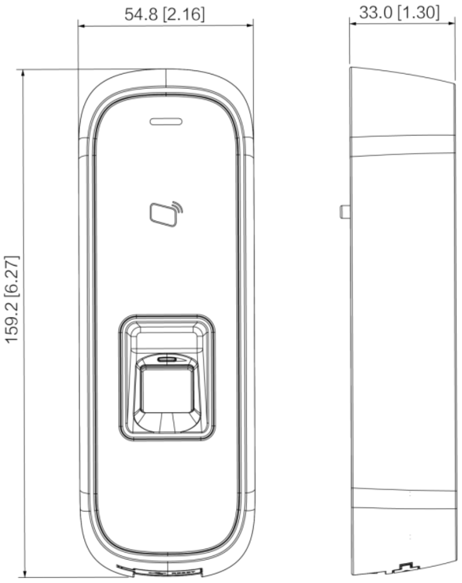
The metal fingerprint access controller is an access control device that supports card unlock and fingerprint unlock.

1.1 Features

- Zinc alloy front panel.
- 32-bit CPU.
- Support W26\W34 (be compatible with the third party products).
- Support RS-485 and Wiegand protocol.
- Card reading frequency: 13.56MHZ; card reading distance: 1 cm–3 cm; response time is less than 0.1 s.
- Contactless card reading, can read Mifare card, read card number of public transportation IC card, bank IC card, and Mifare card.
- Support "watchdog" (a device that protects a system from software or hardware failures).
- Support online upgrade; if online upgrade failed, you can upgrade again.
- Support card unlock, fingerprint unlock, and card & fingerprint unlock.
- Buzzer and indicator lights.
- Support tamper alarm.
- Anti-thunder, anti-static, and short-circuit protection function.
- All ports with overcurrent protection and overvoltage protection function.
- Protection Grade: IP65 and IK10.
- Working temperature: -30°C to +50°C.
- Working humidity: ≤95%.

1.2 Dimensions

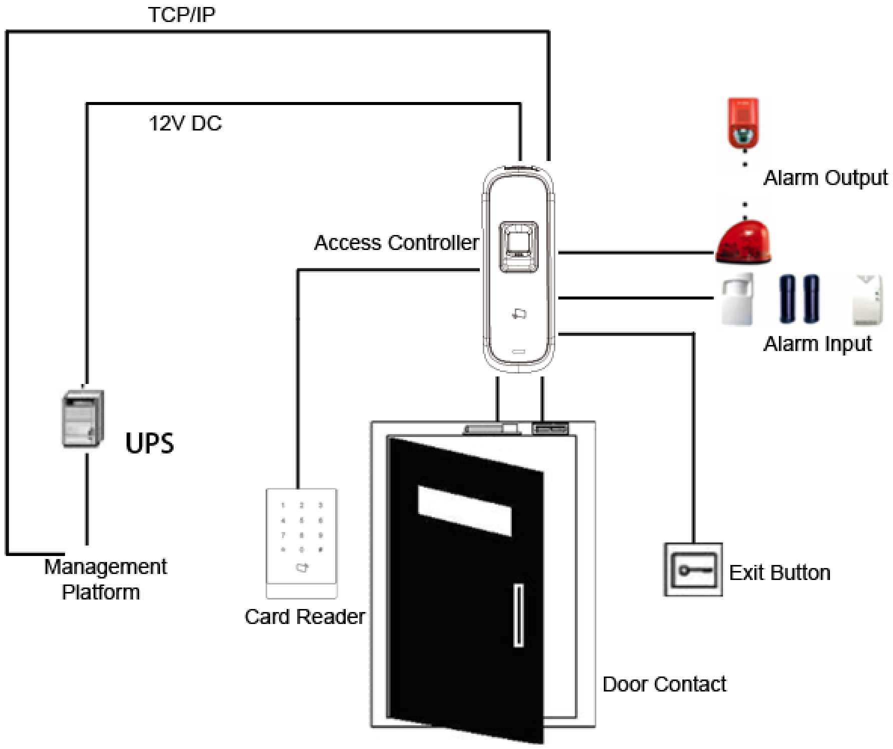
Figure 1-1 Dimensions (mm [inch])



2 Installation

2.1 Application Diagram

Figure 2-1 Application diagram



2.2 Component

Figure 2-2 Front panel

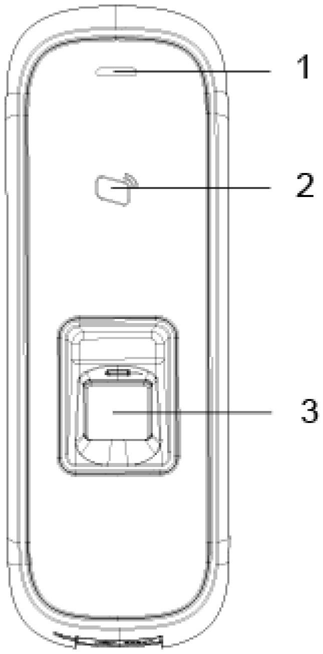


Figure 2-3 Ports at the bottom

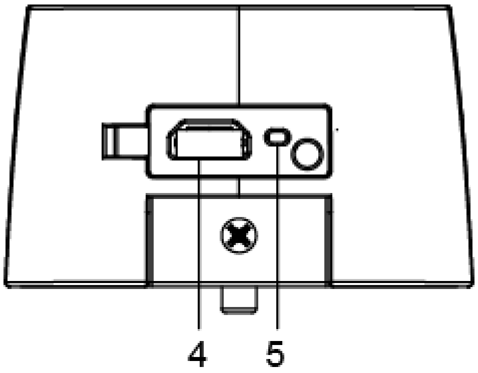


Table 2-1 Component description (1)

No.	Name	No.	Name
1	Indicator light	4	USB port
2	Card swiping area	5	RESET
3	Fingerprint sensor	–	–

2.3 Installation

Figure 2-4 Installation

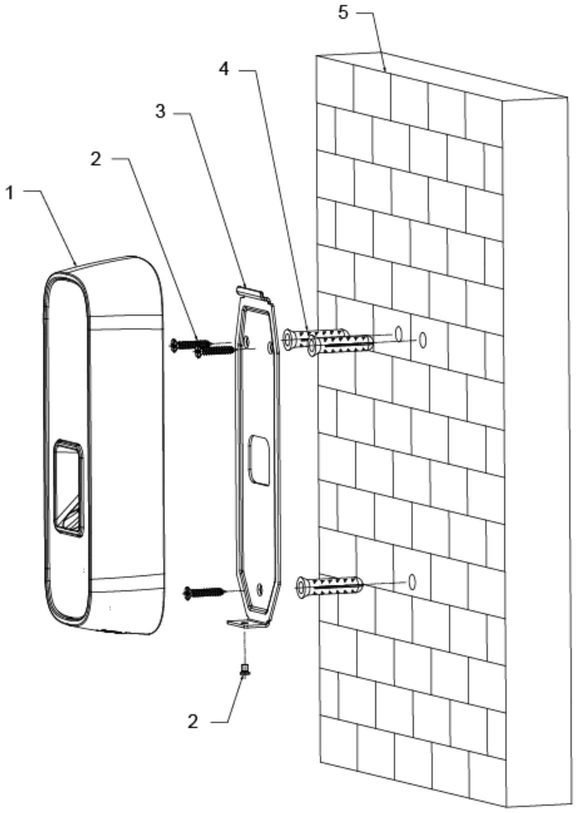


Table 2-2 Component description (2)

No.	Name	No.	Name
1	Access controller	4	Anchor bolt
2	ST3×18 screw	5	Wall
3	Bracket	–	–

Procedure

Step 1 Drill three holes at appropriate height on the wall according to hole positions on the bracket.

Step 2 Hammer the anchor bolts in the wall.

Step 3 Fix the bracket on the wall through the three ST3×18 screws.

Step 4 Install the access controller on the bracket through the bracket fastener.

Step 5 Check whether the access controller is firmly fixed on the wall.

3 Cable Connection

Figure 3-1 Cable connection

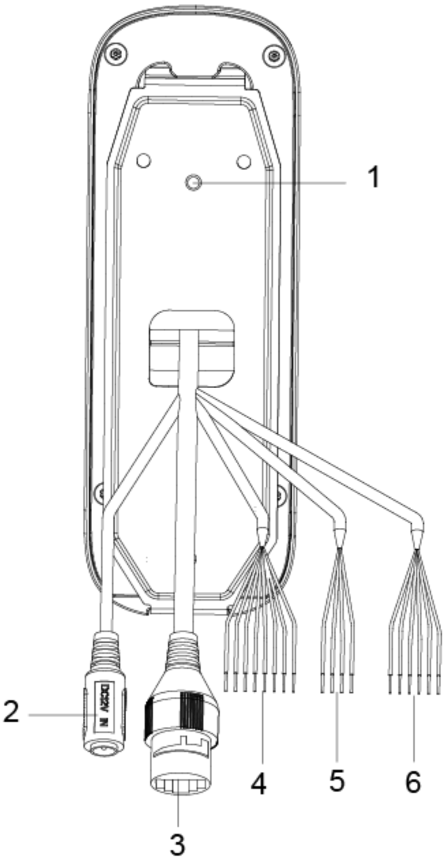


Table 3-1 Component description (3)

No.	Name	No.	Name
1	Tamper switch	4	CON4
2	Power port	5	CON5
3	Ethernet port	6	CON6

3.1.1 Wiegand/RS-485

Table 3-2 Wiegand/RS-485 cable connection

Parameter	Cable Color	Cable Name	Description
CON4 (Wiegand/RS-485)	Blue	CASE	Connected to CASE signal cable of peripheral devices; used to detect tamper.
	White	D1	Wiegand D1 input (connected to peripheral card readers)/output (connected to access controllers).
	Green	D0	Wiegand D0 input (connected to peripheral card readers)/out (connected to access controllers).

Parameter	Cable Color	Cable Name	Description
	Brown	LED	Connected to peripheral LED signal cables to confirm validity of Wiegand D0 and D1 data transmission.
	Yellow	RS–485_B	RS-485 negative input (connected to peripheral card readers)/output (connected to access controllers).
	Purple	RS–485_A	RS-485 positive input (connected to peripheral card readers)/output (connected to access controllers).
	Red	12V_OUT	Power positive output.
	Black	GND	GND of power port.

Table 3-3 Cable specification and length

Parameter	Cable Connection Description	Length
RS-485 Input/ Output	CAT5e cable, RS-485 connection	100 m
Wiegand Input/ Output	CAT5e cable, Wiegand connection	50 m

3.1.2 Lock/Door Contact/Exit Button

Table 3-4 Lock/door contact/exit button cable connection

Parameter	Cable Color	Cable Name	Description
CON6	Black and green	DOOR_BUTTON	Exit button
	Black and blue	GND	Lock signal GND
	Black and grey	DOOR_SR	Door contact input
	Black and brown	DOOR_COM	Common port of lock
	Black and yellow	DOOR_NO	Normally open port of lock
	Black and purple	DOOR_NC	normally closed port of lock

Cable connection methods might vary according to lock types. See Figure 3-2, Figure 3-3, Figure 3-4, and Figure 3-5.

Figure 3-2 Motor lock cable connection

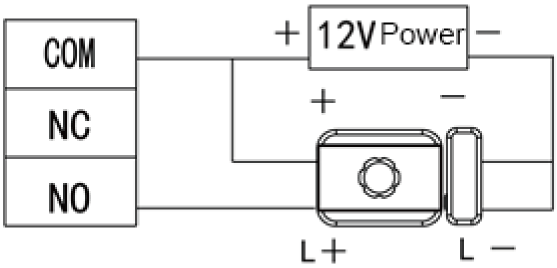


Figure 3-3 Magnetic lock cable connection

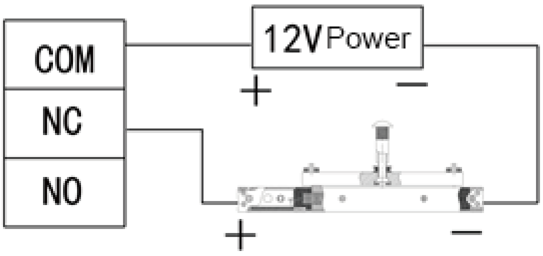


Figure 3-4 Electric lock cable connection

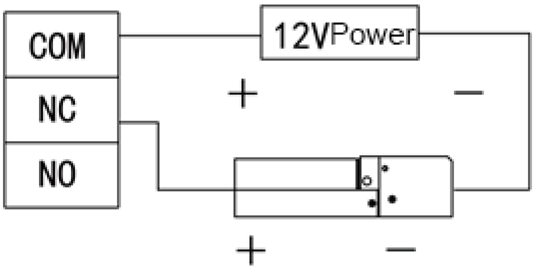
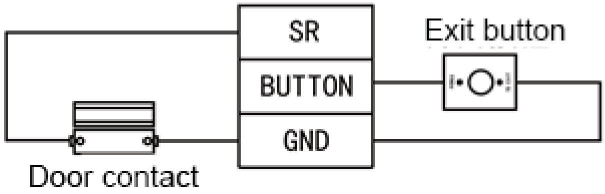


Figure 3-5 Door contact and exit button cable connection



3.1.3 Alarm Input/Output

Table 3-5 Alarm Input/output cable connection

Parameter	Cable Color	Cable Name	Description
CON5 (Peripheral alarm input and output)	White and red	ALM_NO	One alarm output port, used to connect the access controller to sound and light alarm devices. 📖 Once alarms like door contact timeout (internal alarm input) and intrusion (external alarm output) occur, alarm output device will give out sound and light alarms for 15 seconds.
	White and orange	ALM_COM	
	White and brown	ALM_IN	One alarm input port, used to connect the access controller to peripheral alarm input devices like infrared detectors and smoke detectors.
	White and green	GND	Alarm input signal GND

- There are two methods to connect peripheral alarm output devices. You need to select as needed.
  - ◇ When you use IP camera, you can select peripheral output device cable connection method in Figure 3-6.
  - ◇ When you use sound and light siren, you can select cable connection method in Figure 3-7.

Figure 3-6 Peripheral alarm output device cable connection (1)

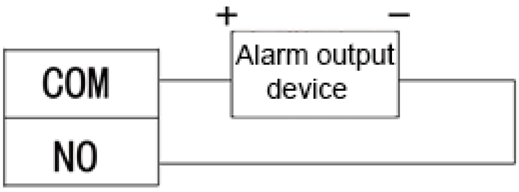
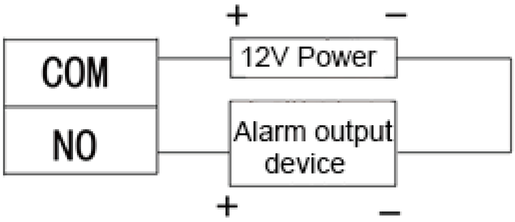
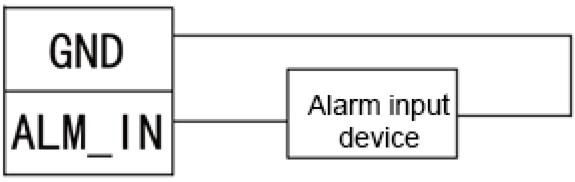


Figure 3-7 Peripheral alarm output device cable connection (2)



- For peripheral alarm input device cable connection, see Figure 3-8.

Figure 3-8 Peripheral alarm input device cable connection



3.1.4 Other Cables

Table 3-6 Other cable connection descriptions

Parameter	Description
Tamper switch	When the access controller is detached from the wall forcibly, the access controller will give out alarms.
Power port	Connected to 12V DC power supply.
Ethernet port	Connected to network cable.

4 Operations

After the access controller is powered on for the first time, the first card that is swiped is the administrator card. Three modes are available for the access controller: Standby verification, local user management, and USB flash drive management. You can add, delete, and clear users; export data to and import data from USB flash drive, and update the access controller with the USB flash drive.

- The access controller can work as an all-in-one or a card reader. This section only introduces the operations of the device as an all-in-one.
- If the administrator card is lost, you can open the back cover of the access controller, and press the reset button on the motherboard for 5 seconds to reset the device to factory settings.

4.1 Standby Verification

Power on the access controller, and then swipe the administrator card, the yellow light glows, which means the device as an all-in-one is in standby verification mode.

If the yellow light does not glow, continuously swipe the administrator card 7 times in 15 seconds to put the device as an all-in-one in standby verification mode.

4.2 User Management

You can add, delete, and clear users on the access controller.

- Make sure that the access controller as an all-in-one is in standby verification mode, and no USB flash drive is inserted.
- The interval of continuously swiping the administrator card cannot be greater than 5 seconds.
- If there is no operation within 15 seconds, the system will exit from user management mode.

4.2.1 Adding User

You can add a user by adding a card or a fingerprint.

Step 1 Swipe the administrator card once.
The yellow light is on.

Step 2 Swipe the administrator card again, and then you can start to add user.
Wait for 5 seconds, the cyan light is on, and the fingerprint module light also flashes.

Step 3 Swipe the card, or press the fingerprint that you want to add.

Step 4 Swipe the administrator card once to save the user.

- When adding a user, swipe the card only once. One fingerprint needs to be collected three times, and up to three fingerprints can be collected.
- You can only add one user at a time. A user must be linked to at least 1 card or 1 fingerprint, or at most 1 card and 3 fingerprints.

4.2.2 Deleting Users

You can delete a user by deleting the user's card or fingerprint.

Step 1 Swipe the administrator card once.

The yellow light is on.

Step 2 Swipe the administrator card 3 times, and then you can start to delete user.

Wait for 5 seconds, the cyan light is on.

Step 3 Swipe the card, or press the fingerprint that has been added to the access controller.

You can delete up to 10 users at a time.

Step 4 Swipe the administrator card once to delete the user.

4.2.3 Clearing Users

You can clear users by swiping the administrator card.

Step 1 Swipe the administrator card once.

The yellow light is on.

Step 2 Swipe the administrator card 5 times.

Wait for 5 seconds, the cyan light is on.

Step 3 Swipe the administrator card once to clear users.

4.2.4 Switching Work Mode

The access controller can work as an all-in-one or a card reader.

Step 1 Swipe the administrator card once.

The yellow light is on.

Step 2 Swipe the administrator card 7 times.

Wait for 5 seconds, the cyan light is on.

Step 3 Swipe the administrator card once, and the access controller switch to a card reader.

When the access controller works as a card reader, continuously swipe the administrator card 7 times in 15 seconds to switch the device to an all-in-one in standby verification mode.

4.3 USB Flash Drive Management

You can export user data to or import such data from USB flash drive, export card swiping records and alarm records to the flash drive, or update the access controller with the flash drive.

- Make sure that the access controller as an all-in-one is in standby verification mode, and USB flash drive is inserted.
- Do not remove the USB flash drive or perform other operations during import, export or update. Otherwise, the import, export, or update might fail.
- The interval of continuously swiping the administrator card cannot be greater than 5 seconds.

4.3.1 Exporting Data

Export data on the access controller to the USB flash drive.

Step 1 Swipe the administrator card once.
The yellow light is on.

Step 2 Swipe the administrator card 2 times.

Step 3 After 5 seconds, swipe the administrator card once, and the data is exported to the USB flash drive.

📖

During exporting, the purple light is on.

4.3.2 Importing Data

After exporting user data from an access controller using USB flash drive, you can import such data to another access controller.

Step 1 Insert the USB flash drive with user data to the target access controller. Swipe the administrator card once.
The yellow light is on.

Step 2 Swipe the administrator card 4 times.

Step 3 After 5 seconds, swipe the administrator card, and the data is imported to the target access controller.

📖

During importing, the purple light is on.

4.3.3 Updating Access Controller

You can update your access controller with USB flash drive.

Step 1 Name the update file on PC as "update.bin", and save the update file in the root directory of the USB flash drive.

Step 2 Swipe the administrator card once.
The yellow light is on.

Step 3 Swipe the administrator card 6 times.

Step 4 After 5 seconds, swipe the administrator card once, and the update starts.
The access controller will restart after the update finishes.

📖

During updating, the purple light is on.

Appendix 1 Fingerprint Record Instruction

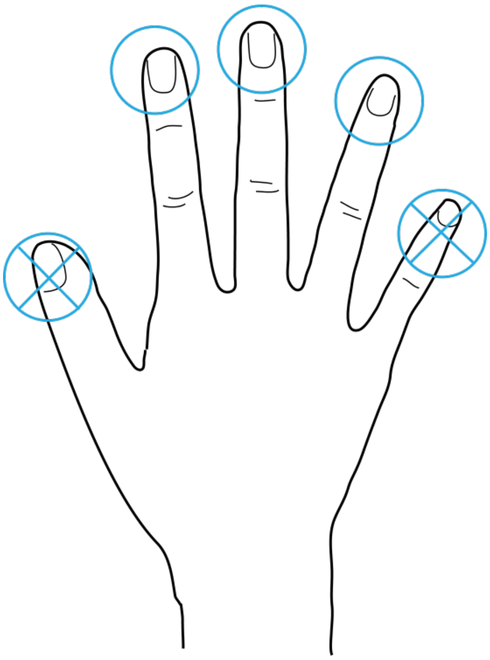
Notice

- Make sure that your fingers are clean and dry before recording your fingerprints.
- Press your finger to the fingerprint recording area, and make your fingerprint is centered on the recording area.
- Do not put the fingerprint sensor at places with intense light, high temperature, and high humidity.
- For the ones whose fingerprints are worn or are unclear, try other unlock methods.

Fingers Recommended

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

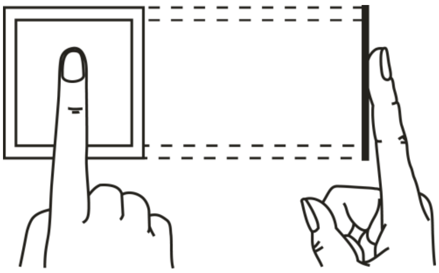
Appendix Figure 1-1 Recommended fingers



Finger Pressing Method

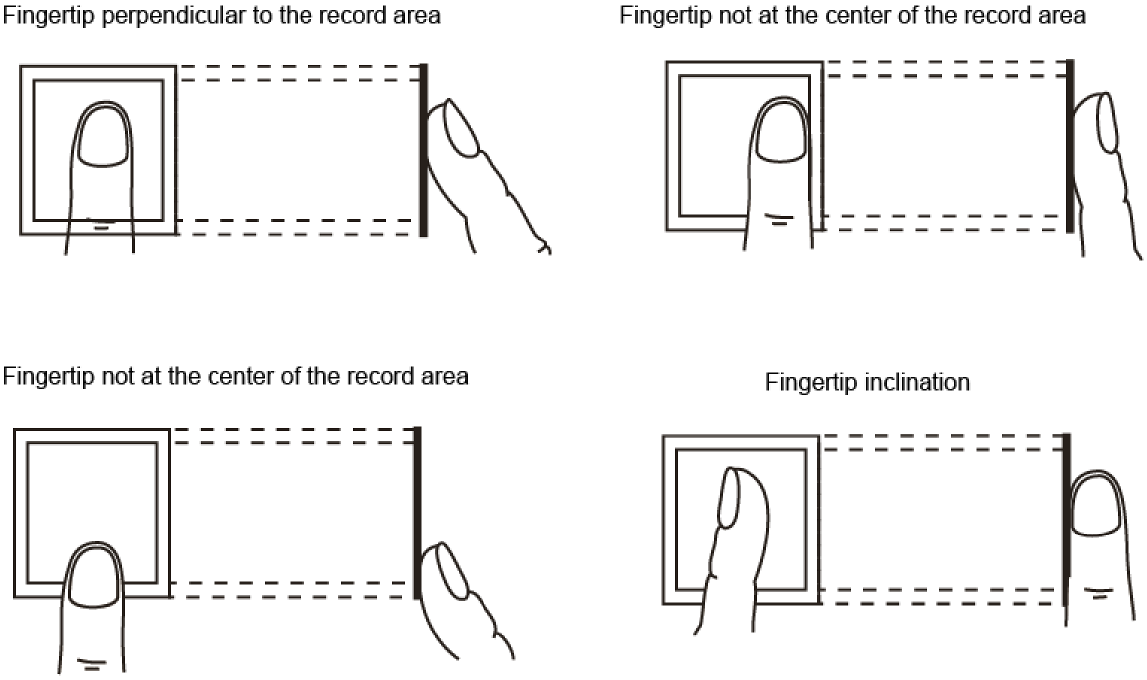
- Correct method

Appendix Figure 1-2 Correct finger pressing



- Incorrect method

Appendix Figure 1-3 Wrong finger pressing



Fingertip perpendicular to the record area

Fingertip not at the center of the record area

Fingertip not at the center of the record area

Fingertip inclination

Appendix 2 Packing List

📖

After unpacking the package, check whether the items are complete against the packing list and keep this guide properly for future reference.

Appendix Table 2-1 Packing list

Name	Quantity
Access controller	1
Quick start guide	1
Screw bag	1
USB patch cable	1

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.