Face Recognition Access Controller

Quick Start Guide

V1.0.4

Foreword

General

This manual introduces the functions, networking and FAQ of the Access Control Extension Module (hereinafter referred to as "the Extension Module"). 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
V1.0.4	Updated the wiring diagram.	March 2024
V1.0.3	Revised network diagram.	February 2023
V1.0.2	Revised "Important Safeguards and Warnings".	December 2022
V1.0.1	Revised the manual name.	November 2022
V1.0.0	First Release.	March 2022

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

Transportation Requirement

⚠

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

Storage Requirement

⚠

Store the Device under allowed humidity and temperature conditions.

Installation Requirements

⚠ WARNING

- Do not connect the power adapter to the Device 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 Device.
- Do not connect the Device to two or more kinds of power supplies, to avoid damage to the Device.
- Improper use of the battery might result in a fire or explosion.
- Please follow the electrical requirements to power the Device.
  - Following are the requirements for selecting a power adapter.
    - The power supply must conform to the requirements of IEC 60950-1 and IEC 62368-1 standards.
    - The voltage must meet the SELV (Safety Extra Low Voltage) requirements and not exceed ES-1 standards.
    - When the power of the device does not exceed 100 W, the power supply must meet LPS requirements and be no higher than PS2.
  - We recommend using the power adapter provided with the Device.
  - When selecting the power adapter, the power supply requirements (such as rated voltage) are subject to the Device label.

⚠

- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not place the Device in a place exposed to sunlight or near heat sources.
- Keep the Device away from dampness, dust, and soot.
- Install the Device on a stable surface to prevent it from falling.
- Install the Device 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 Device is a class I electrical appliance. Make sure that the power supply of the Device is connected to a power socket with protective earthing.

Operation Requirements

⚠

- Check whether the power supply is correct before use.
- Ground the device to protective ground before you power it on.
- Do not unplug the power cord on the side of the Device while the adapter is powered on.
- Operate the Device within the rated range of power input and output.
- Use the Device under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the Device, and make sure that there is no object filled with liquid on the Device to prevent liquid from flowing into it.
- Do not disassemble the Device without professional instruction.
- This product is professional equipment.
- The Device is not suitable for use in locations where children are likely to be present.

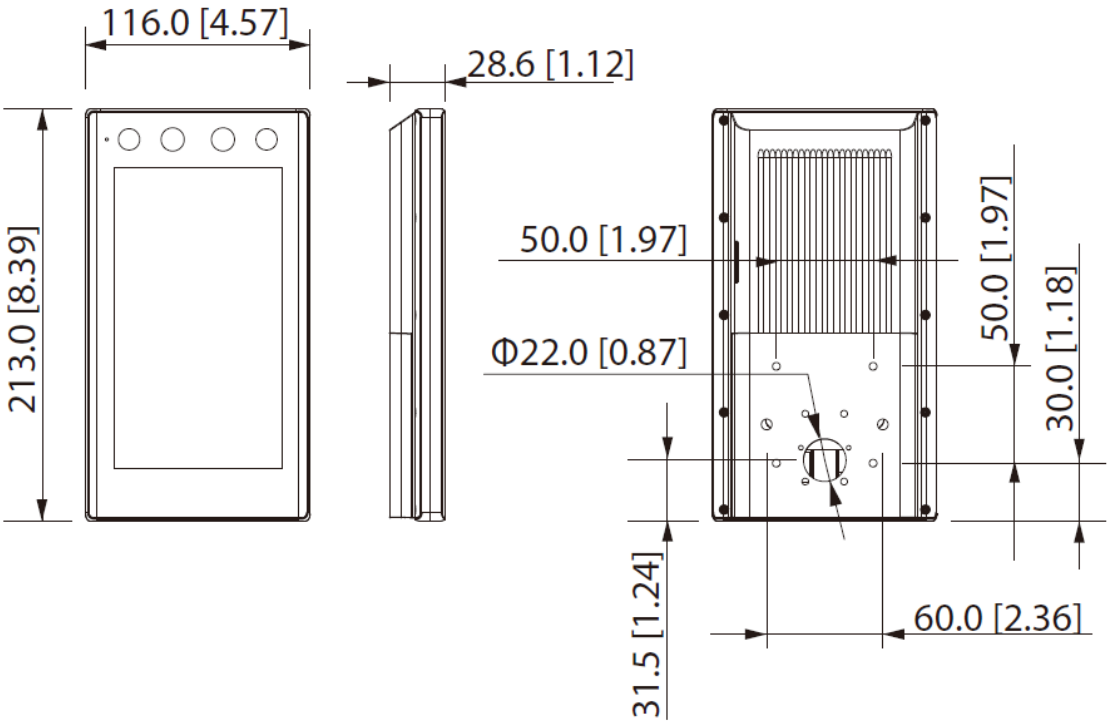
Table of Contents

1 Structure

The front appearance might differ depending on different models of the Access Controller. Here we take the Wi-Fi model as an example.

Face recognition access controller

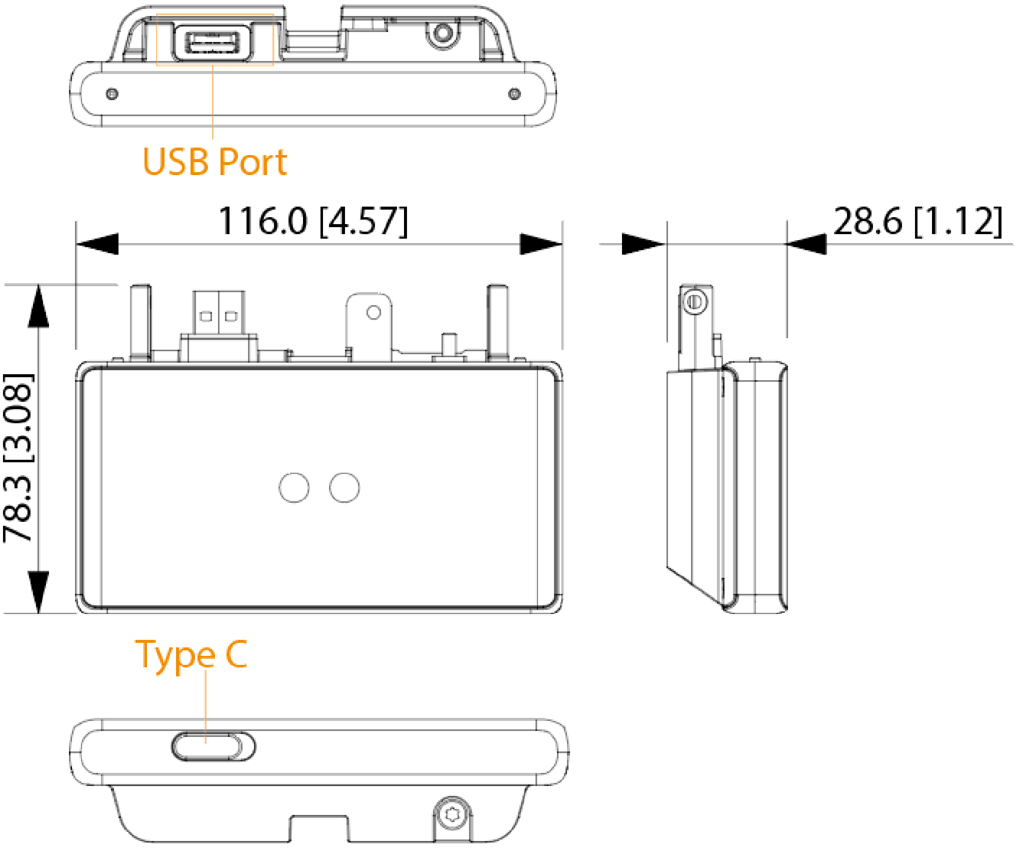
Figure 1-1 Structure (unit: mm[inch])



Extension module

You can mount the extension module to the Access Controller based on your actual needs. The extension modules include 3 types: QR code module, fingerprint module, fingerprint + QR code module. The extension modules have the same dimensions. This section takes QR code module as example.

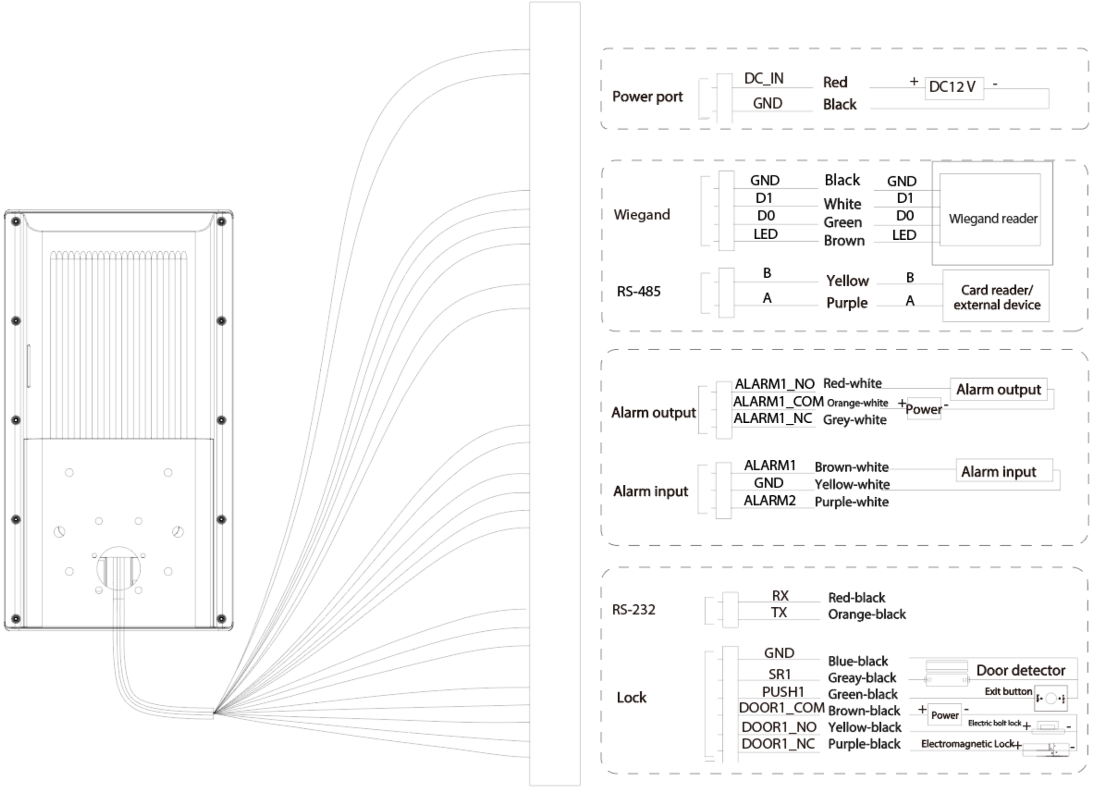
Figure 1-2 QR code model (unit: mm[inch])



2 Connection and Installation

2.1 Wiring

Figure 2-1 Wiring



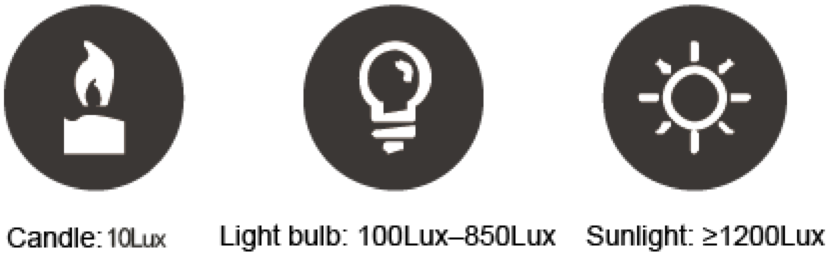
- The back panel of the Access Controller has an internet port, audio extension port, SD card port and wiring harness. Ports might differ depending on different models of Access Controller.
- If you want to connect an external speaker, an audio adapter cable is required.
- If you want to connect a security module, a security module needs to be purchased separately by customers. On the **Main Menu** screen of the Access Controller, select **Connection** > **Serial Port** > **Security Module**. The security module needs a separate power supply.
- When the security module is turned on, the exit button, lock and alarm linkage door opening are not effective.

2.2 Installation Requirements

- The light at the 0.5 meters away from the access controller should be no less than 100 Lux.
- It is recommended that you install the access controller indoors, at least 3 meters away from windows and doors, and 2 meters away from the light source.
- Avoid backlight, direct sunlight, close light, and oblique light.

Ambient Illumination Requirements

Figure 2-2 Ambient illumination requirements

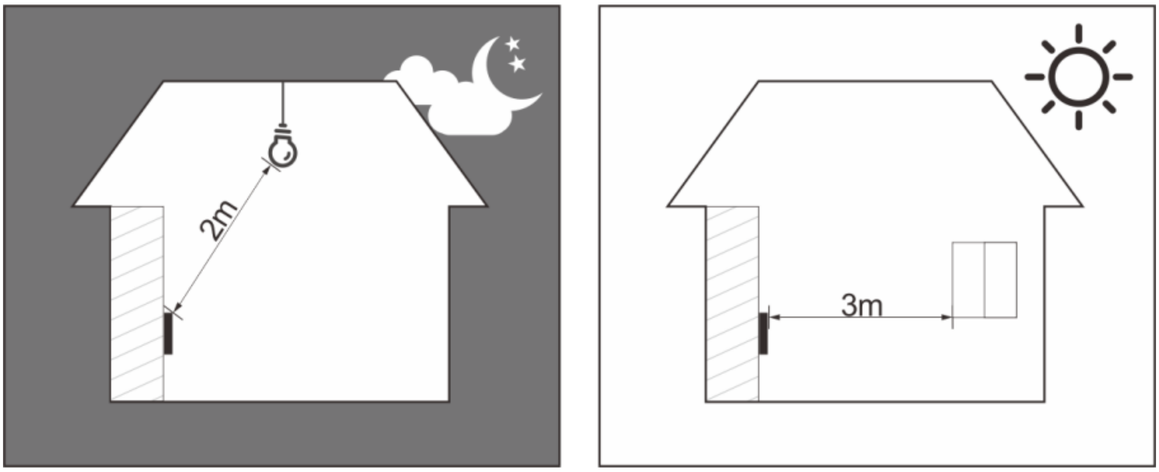


Temperature Monitoring Requirements

- It is recommended to install the access controller in a windless indoor environment (a relatively enclosed area), and the ambient temperature remains at 15 °C to 32 °C.
- Warm up the access controller for more than 20 minutes after power-on to enable the temperature monitoring unit to reach thermal equilibrium.
- If there is no suitable indoor environment, including areas directly facing indoor and outdoor areas, and outdoor doorways, set up a temporary location with stable ambient temperature for temperature monitoring.
- Sunlight, wind, cold air, and air from air conditioning can easily affect the human temperature and the performance of the access controller, which will cause deviation between the monitored temperature and the actual temperature.
- Factors that affect temperature monitoring:
  - ◇ Wind: Wind will take away the heat from the forehead, which will affect the accuracy of temperature monitoring.
  - ◇ Sweating: Sweating is a way for the body to automatically cool down and dissipate heat. When the body sweats, the temperature will also decrease.
  - ◇ Room temperature: If the room temperature is too low, the human temperature will decrease. If the room temperature is too high, the human body will sweat and affect the accuracy of temperature monitoring.
  - ◇ The temperature monitoring unit is sensitive to light waves with a wavelength of 10 um to 15 um. Avoid installing the access controller in locations that have contact with direct sunlight, fluorescent light, air conditioning outlets, heating, cold air outlets, and glass surfaces.

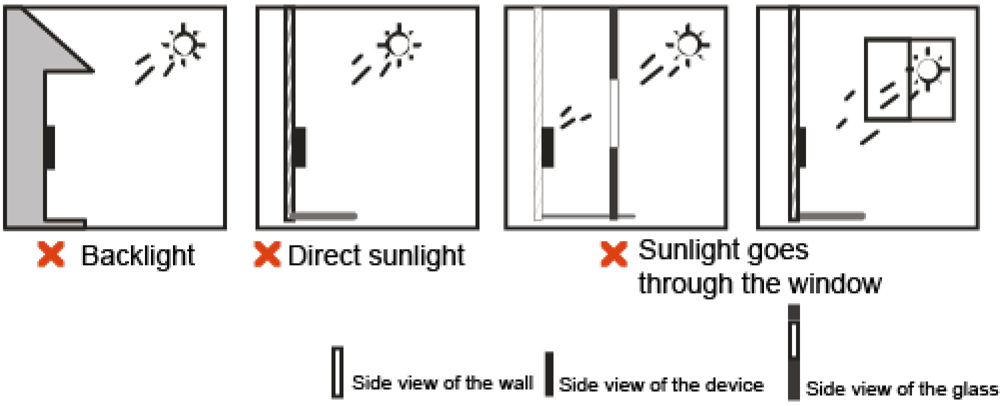
Location Recommended

Figure 2-3 Location recommended



Location Not Recommended

Figure 2-4 Location not recommended



2.3 Installation Process

2.3.1 Installing Access Controller

The Access Controller has four installation methods: wall mount, floor bracket mount, turnstile mount and 86 box mount. This section only introduces wall mount and 86 box mount. For details of floor bracket mount and turnstile mount, please refer to user's manual of corresponding devices.

2.3.1.1 Wall Mount

Procedure

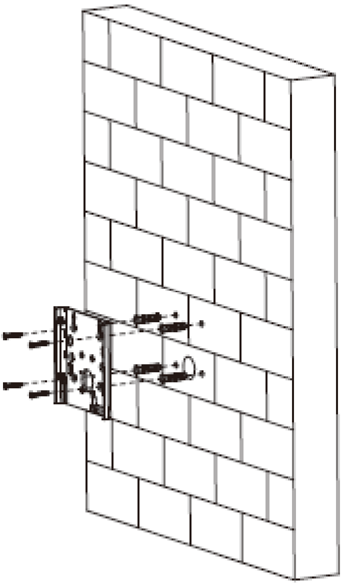
Step 1 According the holes' positions of the installation bracket, drill four holes and one cable outlet in the wall. Put expansion bolts in the holes.

📖

Cable outlet is not required in surface-mounted wiring.

Step 2 Use the four screws to fix the installation bracket to the wall.

Figure 2-5 Fix the installation bracket to the wall



Step 3 Wire the Access Controller. For details, see "2.1 Wiring".

📖

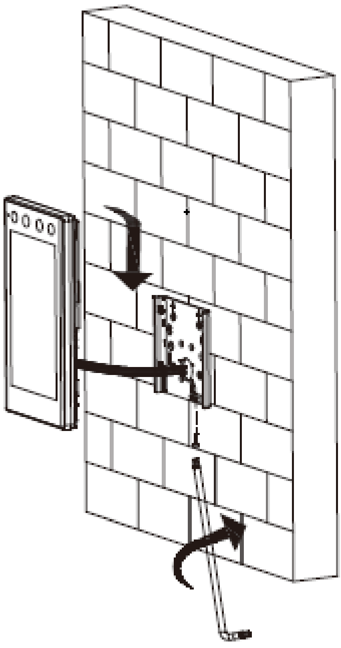
Choose in-wall wiring or surface-mounted wiring based on your actual needs.

Step 4 Fix the Access Controller on the bracket.

Step 5 Screw in one socket head cap screw securely at the bottom of the Access Controller.

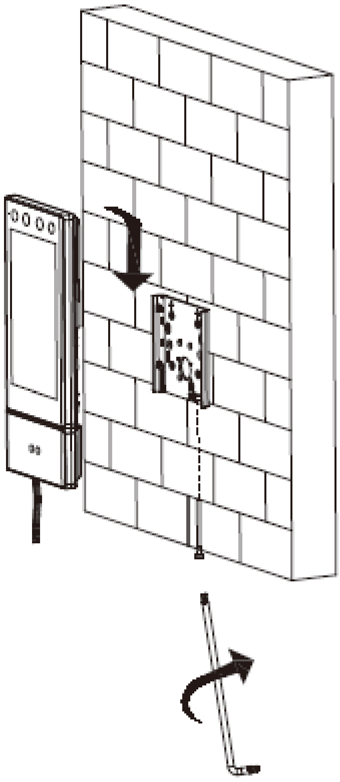
The figure below takes in-wall wiring of Access Controller for example.

Figure 2-6 In-wall wiring of Access Controller



If an expansion module is mounted to the Access Controller, select a proper socket head cap screw based on the size of the expansion module. The figure below takes surface-mounted wiring of extension module for example.

Figure 2-7 Surface-mounted wiring of Access Controller (with QR code extension module)



2.3.1.2 (Optional) Sunshield Mount

Mount a sunshield to the Access Controller based on your own needs. The sunshield needs to be purchased separately by customers.

Procedure

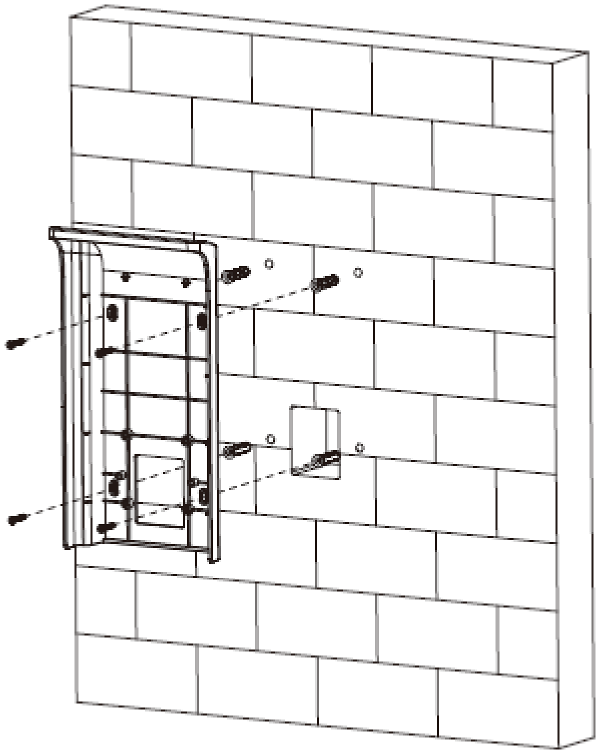
Step 1 Tap the knock outs gently with a screwdriver to push the knock outs away from the sunshield.

A knock out is a partially stamped opening that allows quick entry of a wire or screws.

Step 2 According the position of the holes in the sunshield, drill four holes, and then put expansion bolts in the holes.

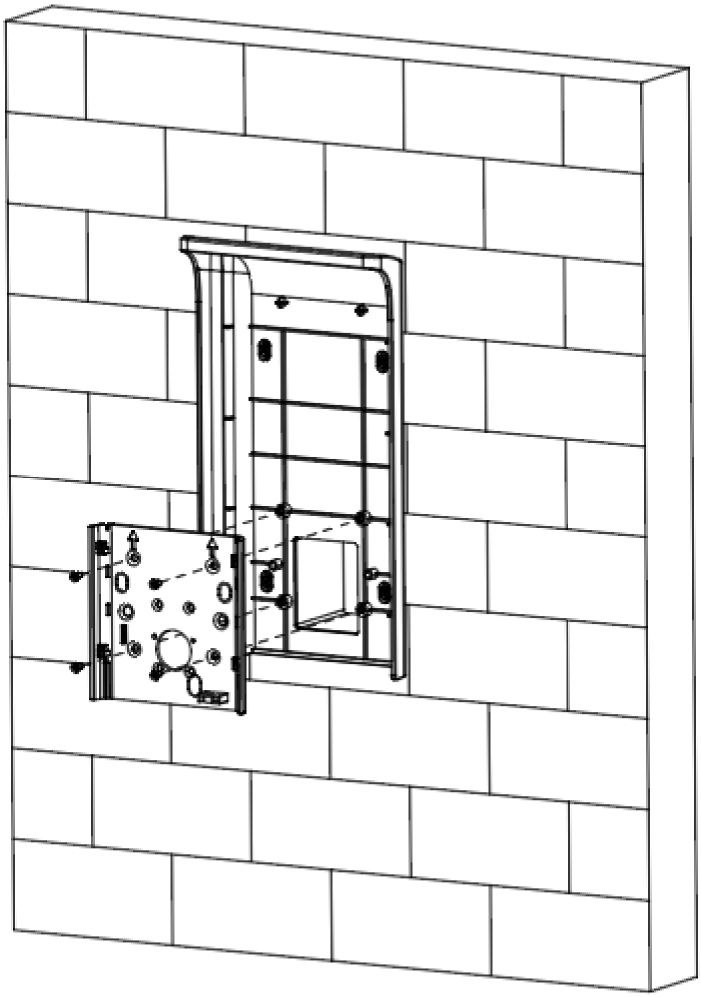
Step 3 Fix the sunshield to the wall with four screws.

Figure 2-8 Fix the sunshield to the wall



Step 4 Fix the installation bracket to the sunshield with four screws.

Figure 2-9 Fix the installation bracket to the sunshield



Step 5 Wire the Access Controller. For details, see "2.1 Wiring"

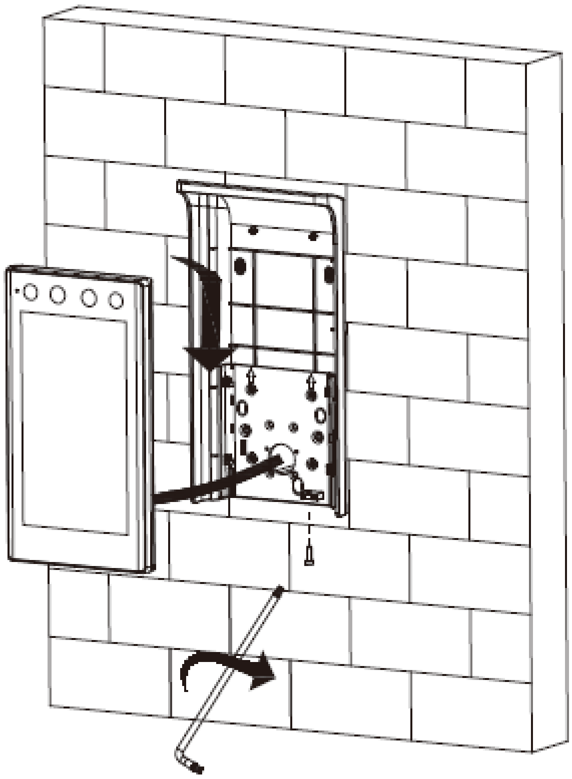
Choose in-wall wiring or surface-mounted wiring based on your needs.

Step 6 Fix the Access Controller on the installation bracket.

Step 7 Screw in one socket head cap screw securely at the bottom of the Access Controller.

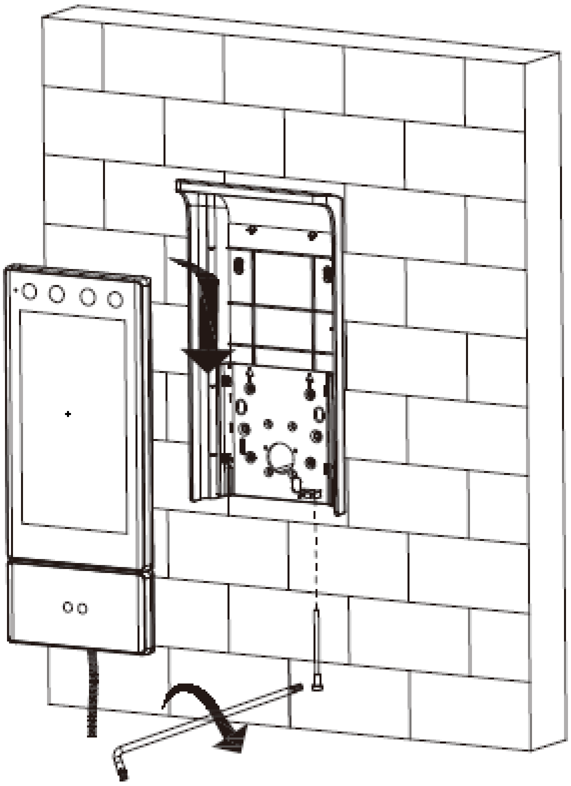
The figure below takes in-wall wiring of Access Controller for example.

Figure 2-10 In-wall wiring of Access Controller



If an expansion module is mounted to the Access Controller, select a proper socket head cap screw based on the size of the expansion module. The figure below takes surface-mounted wiring of QR code extension module for example.

Figure 2-11 In-wall wiring of Access Controller (with QR code extension module)



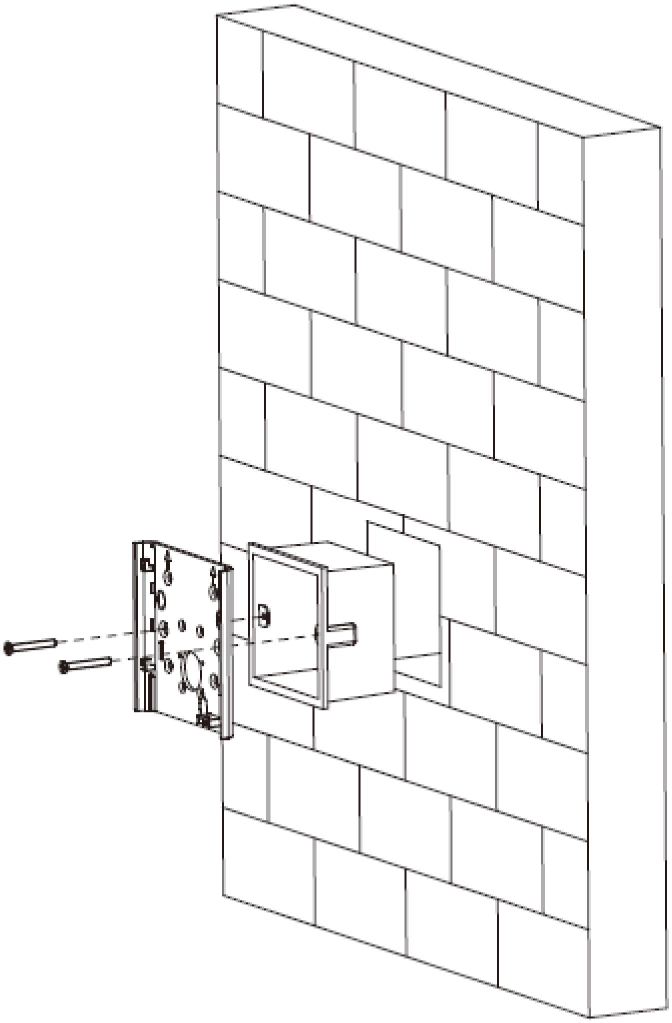
2.3.1.3 86 Box Mount

Procedure

Step 1 Put the 86 box in the wall at a proper height.

Step 2 Fix the installation bracket to the 86 box with two screws.

Figure 2-12 Fix the bracket to the 86 box



Step 3 Wire the Access Controller. For details, see "2.1 Wiring".

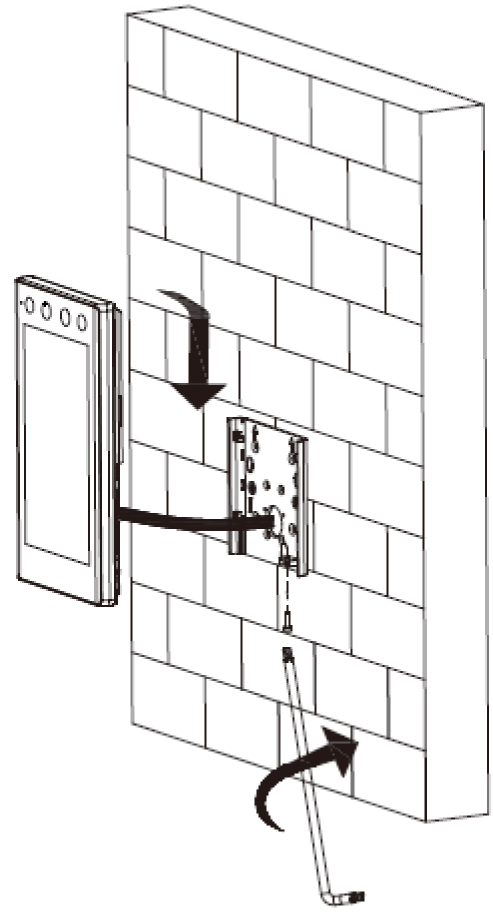
Choose in-wall wiring or surface-mounted wiring based on your needs.

Step 4 Fix the Access Controller to the installation bracket.

Step 5 Screw in one socket head cap screw securely at the bottom of the Access Controller.

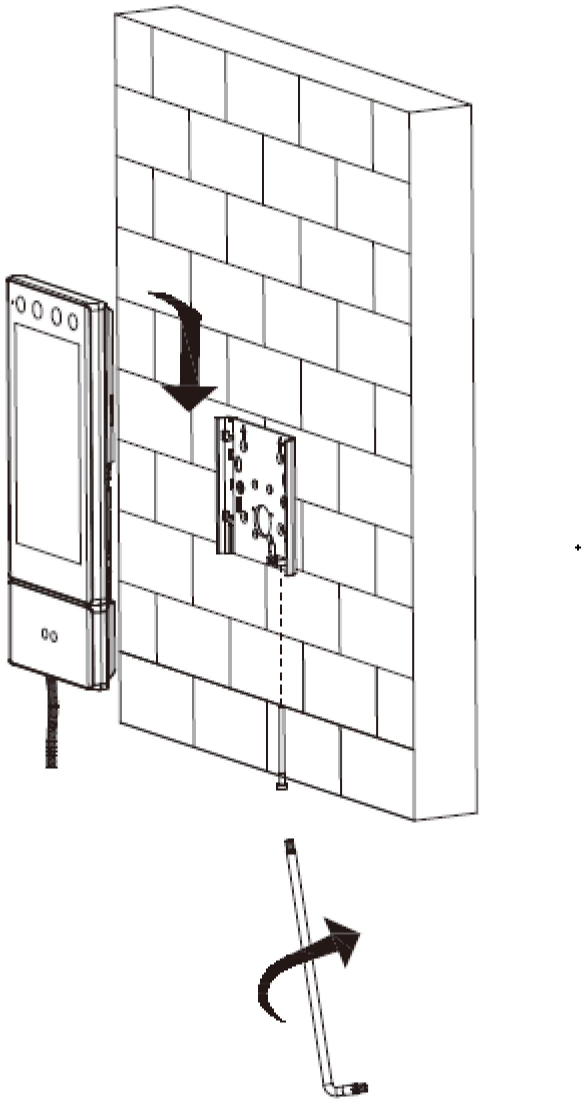
The figure below takes in-wall wiring of Access Controller for example.

Figure 2-13 In-wall wiring of Access Controller



If an expansion module is mounted to the Access Controller, select a proper socket head cap screw based on the size of the expansion module. The figure below takes surface-mounted wiring of QR code extension module for example.

Figure 2-14 In-wall wiring of Access Controller (with QR code extension module)



2.3.2 (Optional) Installing Extension Module

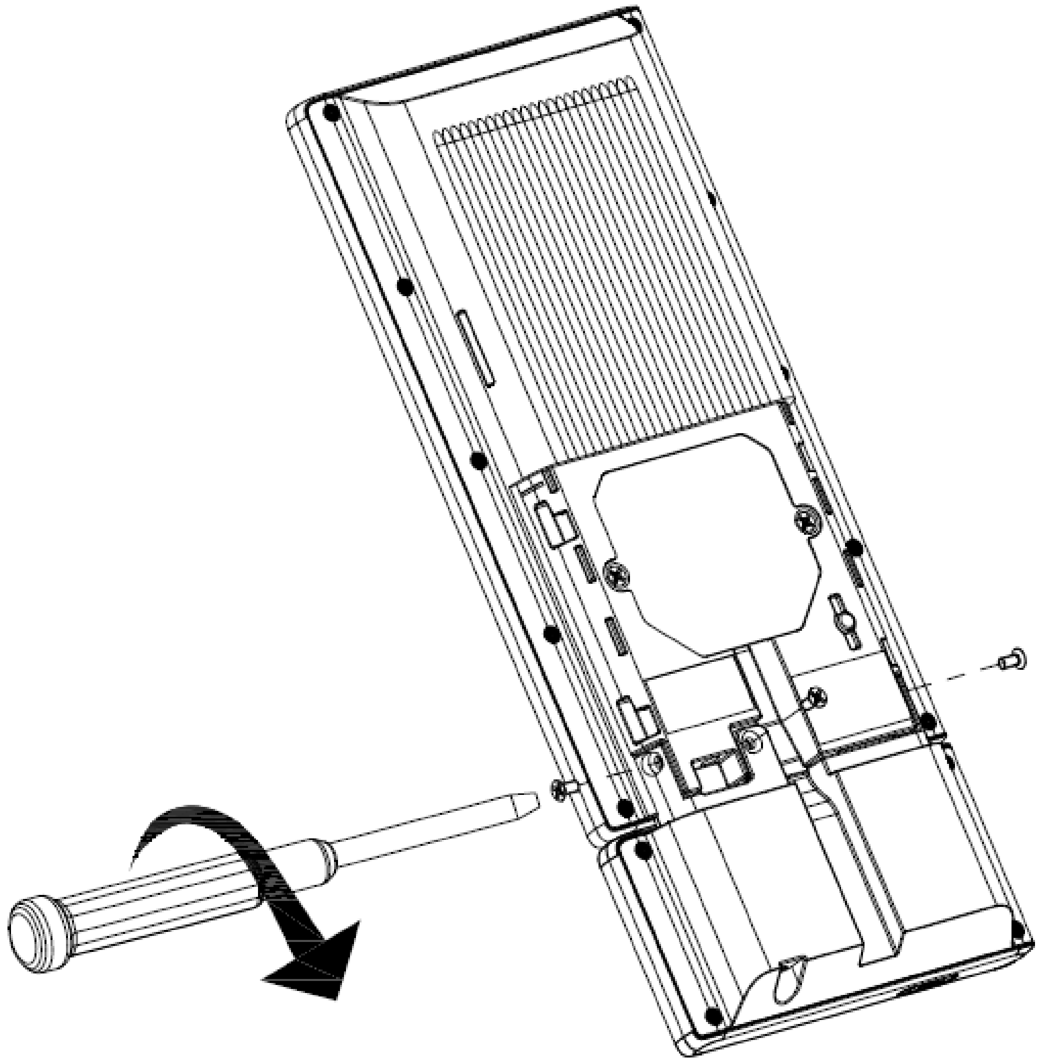
You can mount the extension module to the Access Controller based on your actual needs. The extension module needs to purchased separately by customer.

Procedure

Step 1 Insert a USB to the Access Controller.

Step 2 Screw in three screws to fasten the extension module to the Access Controller securely.

Figure 2-15 Fasten the extension module

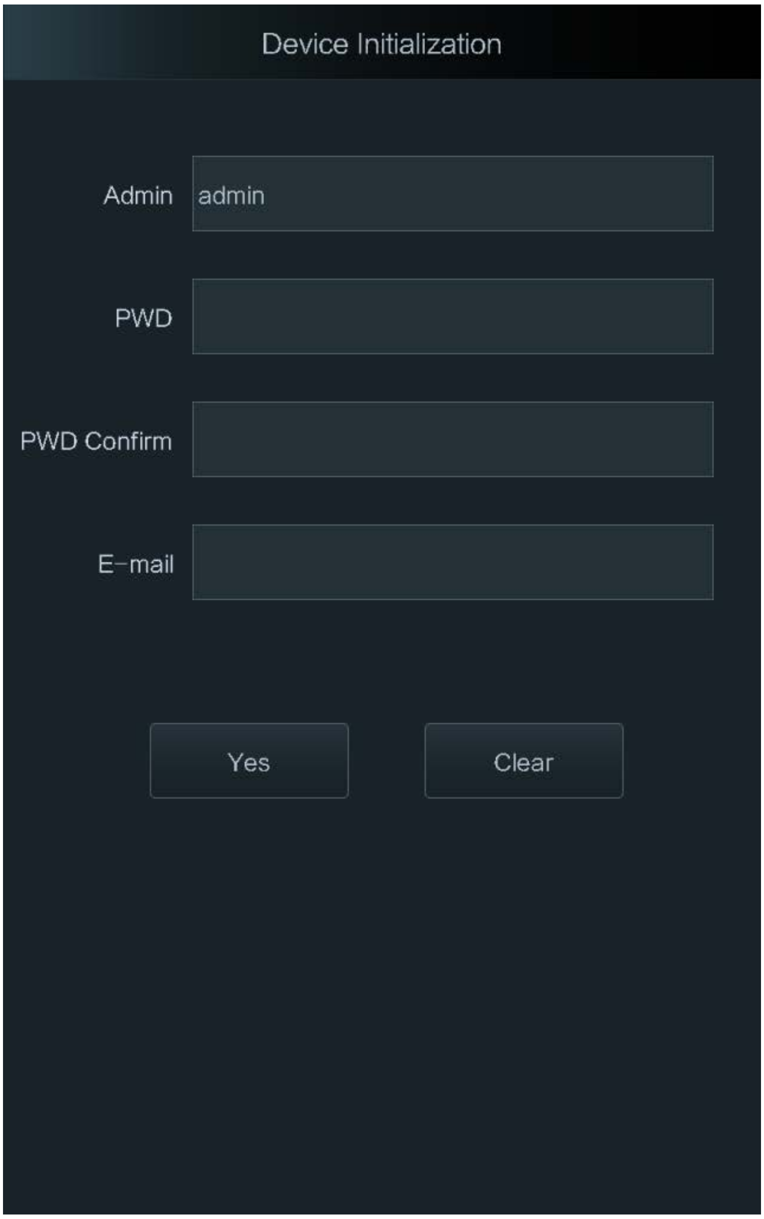


3 Local Operations

3.1 Initialization

For the first-time use or after restoring factory defaults, you need to set a password and email address for the admin account. You can use the admin account to log in to the main menu of the access controller and the web interface.

Figure 3-1 Initialization



Device Initialization

Admin: admin

PWD

PWD Confirm

E-mail

- If you forget the administrator password, send a reset request to your registered e-mail address.
- The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : &).

3.2 Adding New Users

Background Information

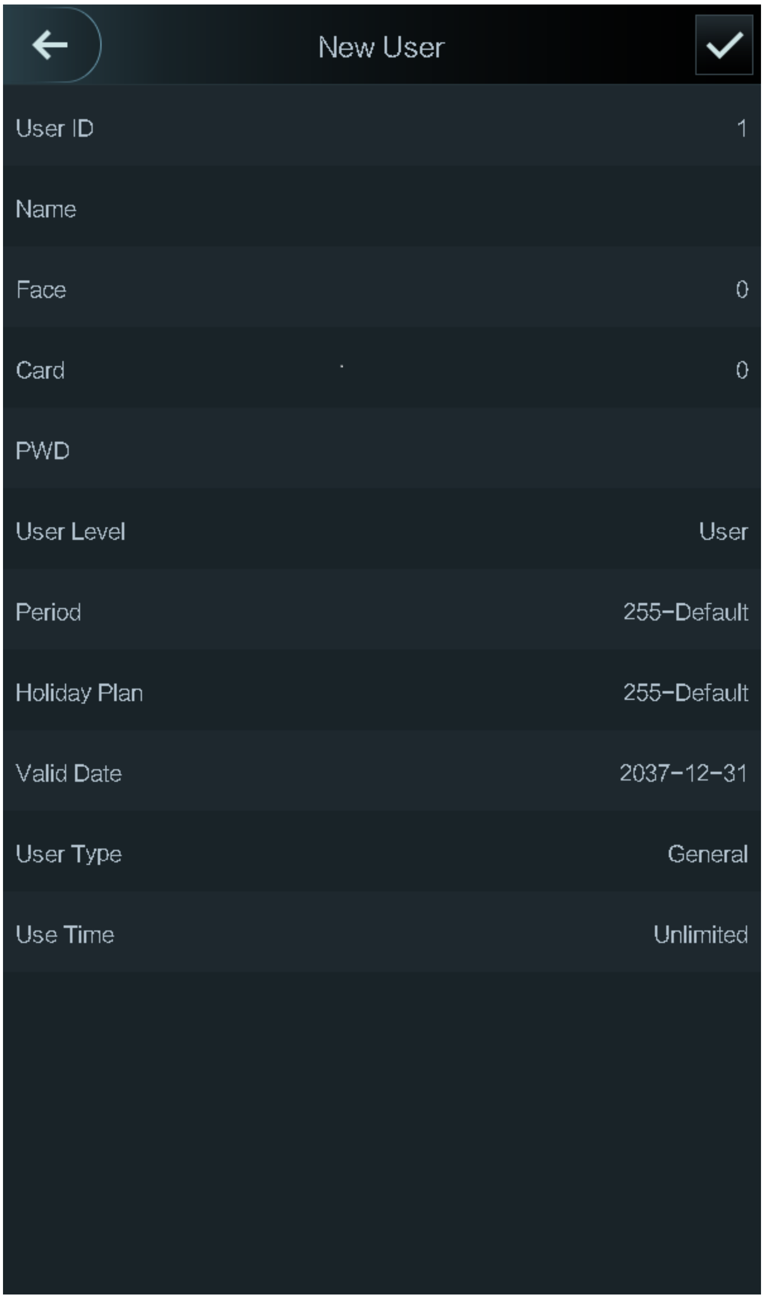
This manual is for reference only. Slight differences might be found between the interfaces in this manual and the actual device.

Procedure

Step 1 On the **Main Menu** interface, select **User** > **New User**.

Step 2 Configure the parameters on the interface.

Figure 3-2 New user



New User

User ID	1
Name	
Face	0
Card	0
PWD	
User Level	User
Period	255-Default
Holiday Plan	255-Default
Valid Date	2037-12-31
User Type	General
Use Time	Unlimited

Table 3-1 Description of new user parameters

Parameter	Description
User ID	Enter user IDs. The IDs can be numbers, letters, and their combinations, and the maximum length of the ID is 32 characters. Each ID is unique.
Name	Enter name with at most 32 characters (including numbers, symbols, and letters).
Face	Make sure that your face is centered on the image capturing frame, and an image of the face will be captured and analyzed automatically.

Parameter	Description
Card	A user can register five cards at most. Enter your card number or swipe your card, and then the card information will be read by the access controller. You can enable the **Duress Card** function. An alarm will be triggered if a duress card is used to unlock the door. Only certain models support card unlock.
PWD	Enter the user password. The maximum length of the password is 8 digits.
User Level	You can select a user level for new users. ● **User**: Users only have door access permission. ● **Admin**: Administrators can unlock the door and configure the access controller.
Period	A user can only unlock the door within the defined period. The default value is 255, which means the user can unlock the door at any time.
Holiday Plan	A user can only unlock the door within the defined holiday plan. The default value is 255, which means the user can unlock the door at any time.
Valid Date	Set a period during which the access permission of the user is valid.
User Type	● **General**: General users can unlock the door. ● **Blocklist**: When users in the blocklist unlock the door, service personnel will receive a notice. ● **Guest**: Guests can unlock the door within a defined period or for certain amount of times. After the defined period expires or the unlocking times runs out, they cannot unlock the door. ● **Patrol**: Patrol users will have their attendance tracked, but they have no unlocking permissions. ● **VIP**: When VIP unlock the door, service personnel will receive a notice. ● **Others**: When they unlock the door, the door will stay unlocked for 5 more seconds.
Use Time	When the user level is **Guest**, set the maximum access times.

Step 3 Tap ☑ to save the configuration.

3.3 Configuring Extension Module

If an extension module is mounted to the Access Controller, configure the extension module first.

Procedure

Step 1 Tap the standby screen.

Step 2 Log in to the main menu with administrator account.

Step 3 On the main menu, select **Features** > **External Module Type**.

Step 4 Select the type of the extension module.

Step 5 Click **Yes**.

After the device restarts, is displayed on the upper-right corner of the standby screen, which means the extension module is configured successfully.

4 Web Operations

4.1 Initialization

Initialize the Access Controller when you log in to the webpage for the first time or after the Access Controller is restored to the factory defaults.

Prerequisites

Make sure that the computer used to log in to the webpage is on the same LAN as the Access Controller.

Background Information

Set a password and an email address before logging in to the webpage for the first time.

Procedure

Step 1 Open a browser, go to the IP address (the default address is 192.168.1.108) of the Access Controller.

📖

We recommend you use the latest version of Chrome or Firefox.

Step 2 Set the password and email address according to the screen instructions.

📖

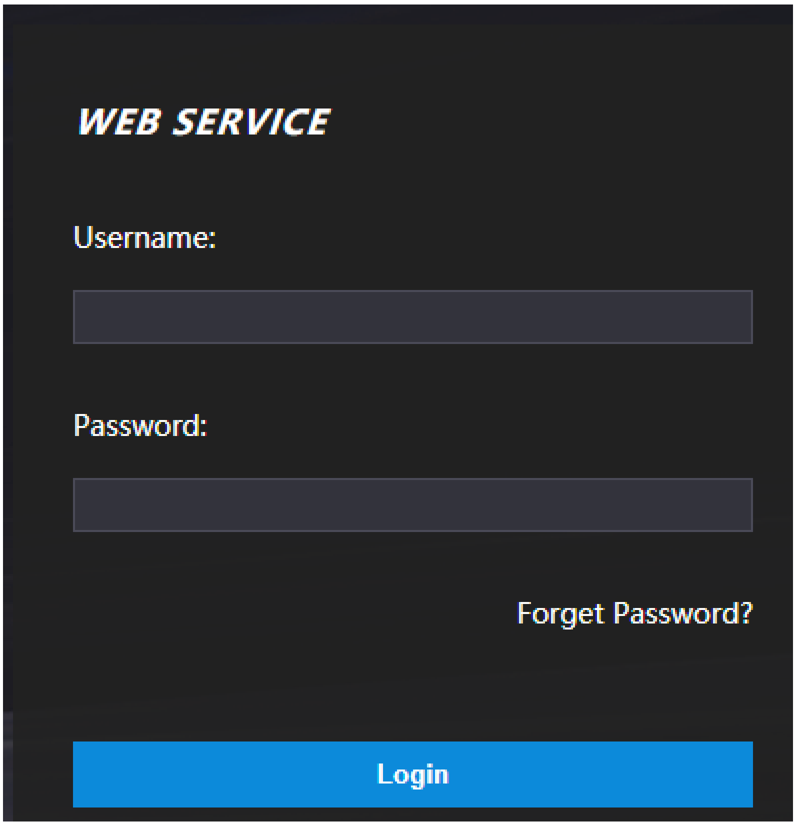
- The password must consist of 8 to 32 non-blank characters and contain at least two types of the following characters: upper case, lower case, numbers, and special characters (excluding ' " ; : &). Set a high-security password by following the password strength prompt.
- Keep the password safe after initialization and change the password regularly to improve security.

4.2 Logging In

Procedure

Step 1 Open a browser, enter the IP address of the Access Controller in the **Address** bar, and press the Enter key.

Figure 4-1 Login



WEB SERVICE

Username:

Password:

Step 2 Enter the user name and password.

- The default administrator name is admin, and the password is the one you set up during initialization. We recommend you change the administrator password regularly to increase security.
- If you forget the administrator login password, you can click **Forget password?**.

Step 3 Click **Login**.

Appendix 1 Important Points of Intercom Operation

The Access Controller can function as VTO to realize intercom function.

Prerequisites

The intercom function is configured on the Access Controller and VTO.

Procedure

Step 1 On the standby screen, tap ☎

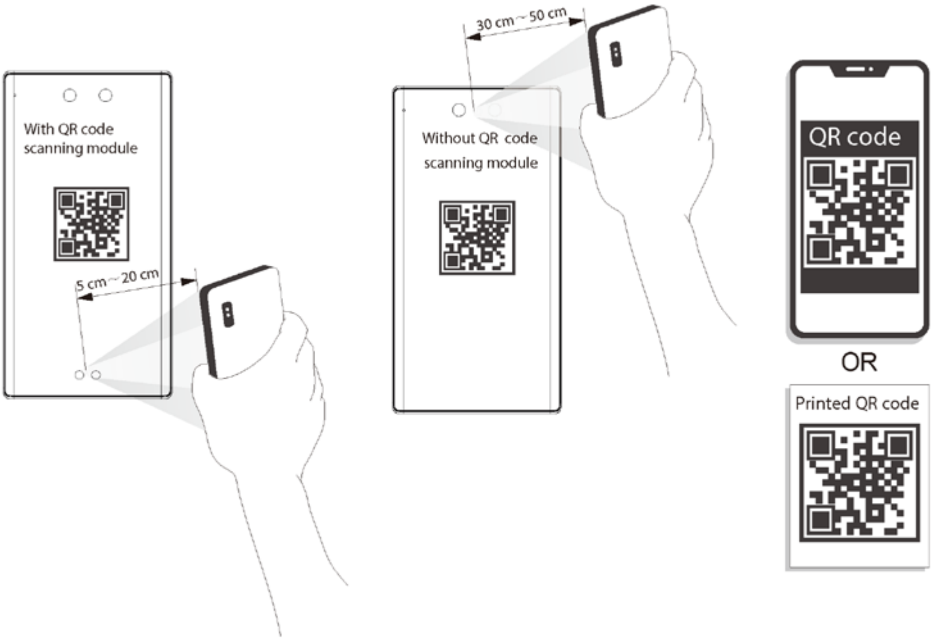
Step 2 Enter the room No, and then tap ☎.

Appendix 2 Important Points of QR Code Scanning

- Access Controller (with QR code scanning module): Place the QR code on your phone at a distance of 3 cm - 5 cm away from the QR code scanning lens. It supports QR code that is larger than 30 mm ×30 mm - 5 cm × 5 cm and less than 100 bytes in size.

  QR code detection distance differs depending on the bytes and size of QR code.

Appendix Figure 2-1 QR code scanning



Appendix 3 Fingerprint Registration Instructions

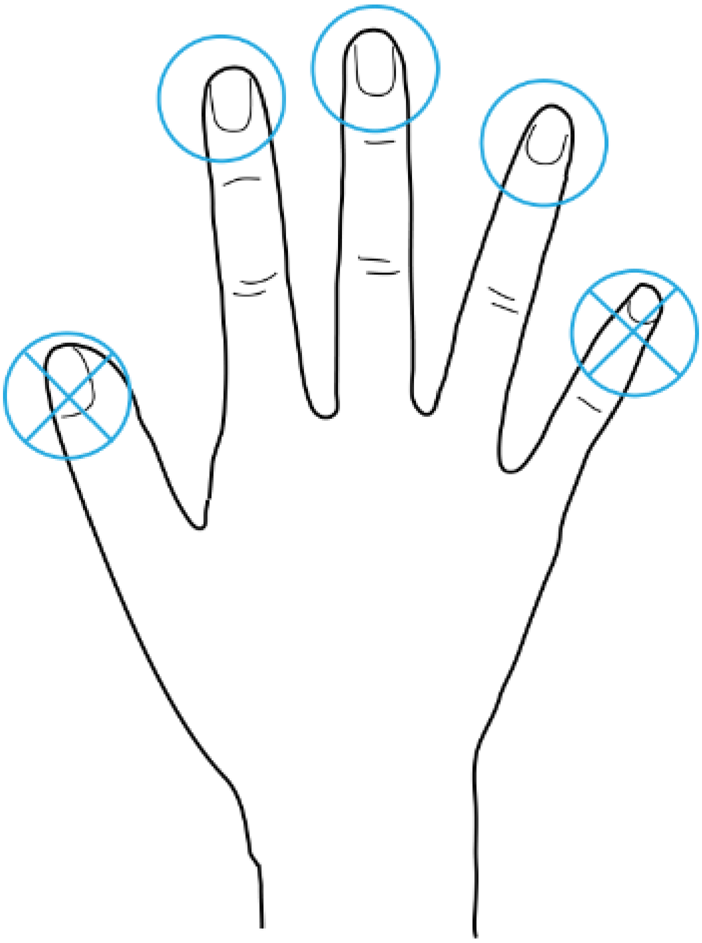
When you register the fingerprint, pay attention to the following points:

- Make sure that your fingers and the scanner surface are clean and dry.
- Press your finger on the center of the fingerprint scanner.
- Do not put the fingerprint sensor in a place with intense light, high temperature, and high humidity.
- If your fingerprints are unclear, use other unlocking methods.

Fingers Recommended

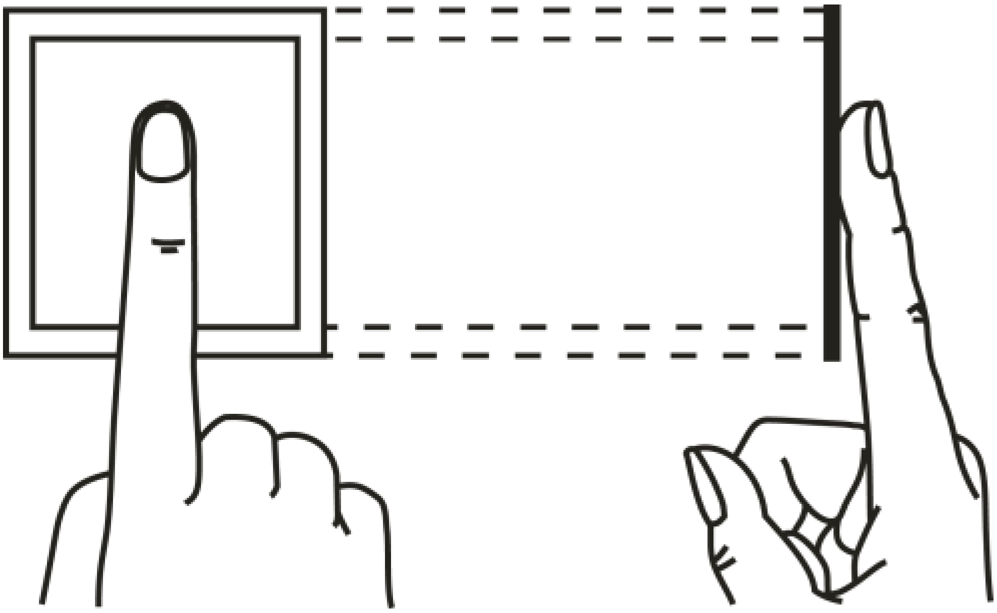
Forefingers, middle fingers, and ring fingers are recommended. Thumbs and little fingers cannot be put at the recording center easily.

Appendix Figure 3-1 Recommended fingers

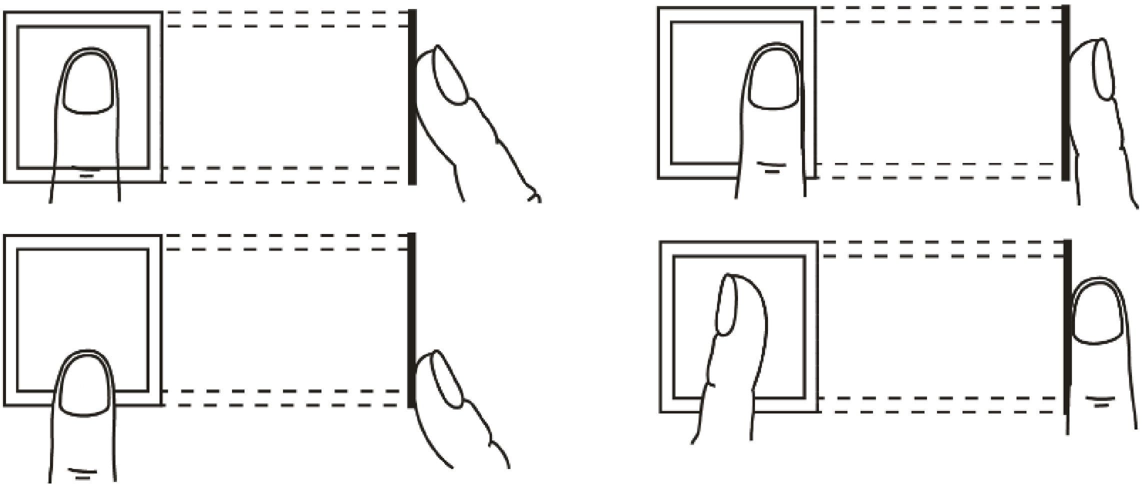


How to Press Your Fingerprint on the Scanner

Appendix Figure 3-2 Correct placement



Appendix Figure 3-3 Wrong placement



Appendix 4 Important Points of Face Registration

Before Registration

- Glasses, hats, and beards might influence face recognition performance.
- Do not cover your eyebrows when wearing hats.
- Do not change your beard style greatly if you use the Device; otherwise face recognition might fail.
- Keep your face clean.
- Keep the Device at least 2 meters away from light source and at least 3 meters away from windows or doors; otherwise backlight and direct sunlight might influence face recognition performance of the access controller.

During Registration

- You can register faces through the Device or through the platform. For registration through the platform, see the platform user manual.
- Make your head center on the photo capture frame. The face image will be captured automatically.

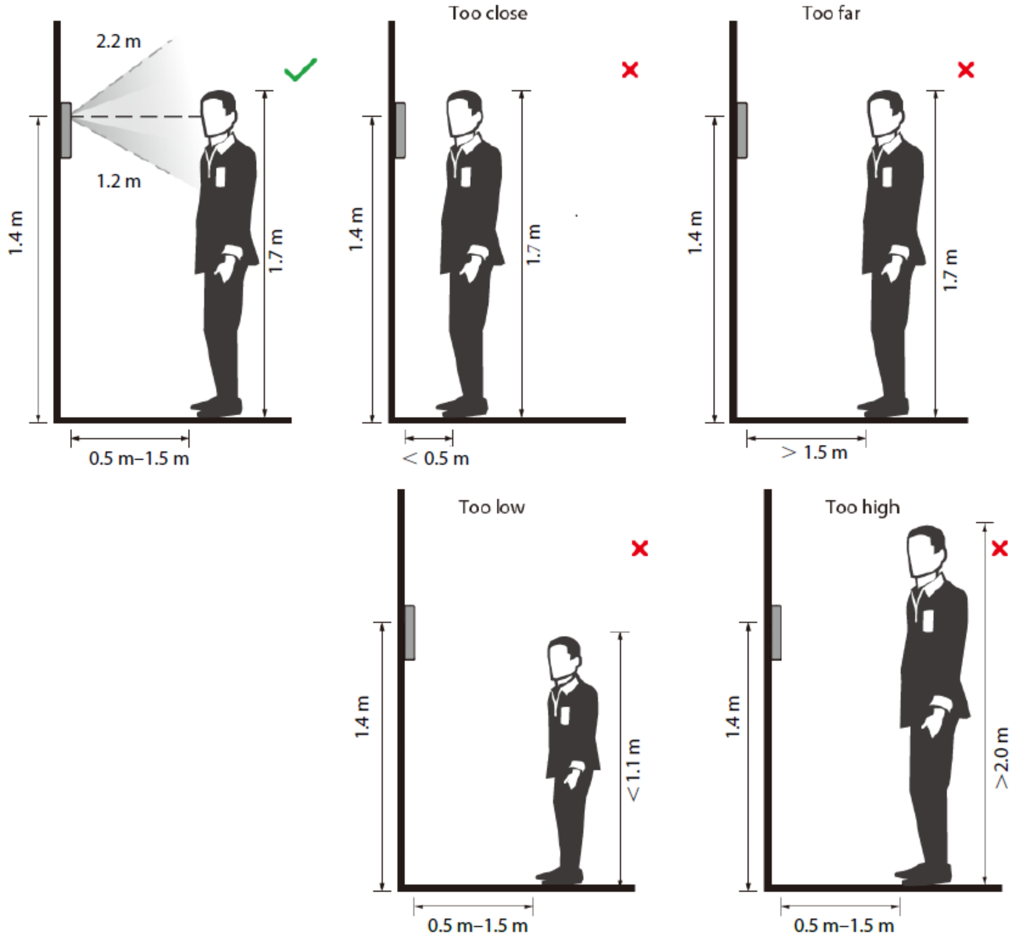
- Do not shake your head or body, otherwise the registration might fail.
- Avoid 2 faces appear in the capture frame at the same time.

Face Position

If your face is not at the appropriate position, face recognition accuracy might be affected.

The face position below is for reference only, and might differ from the actual situation.

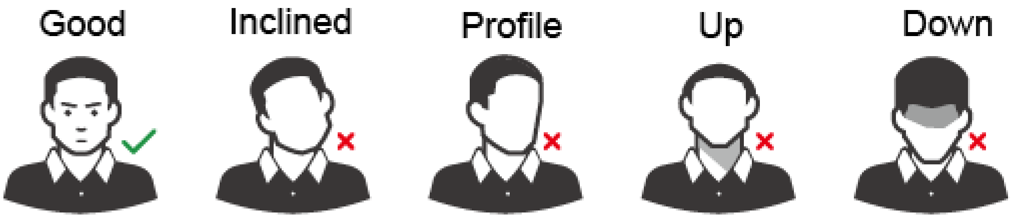
Appendix Figure 4-1 Appropriate face position



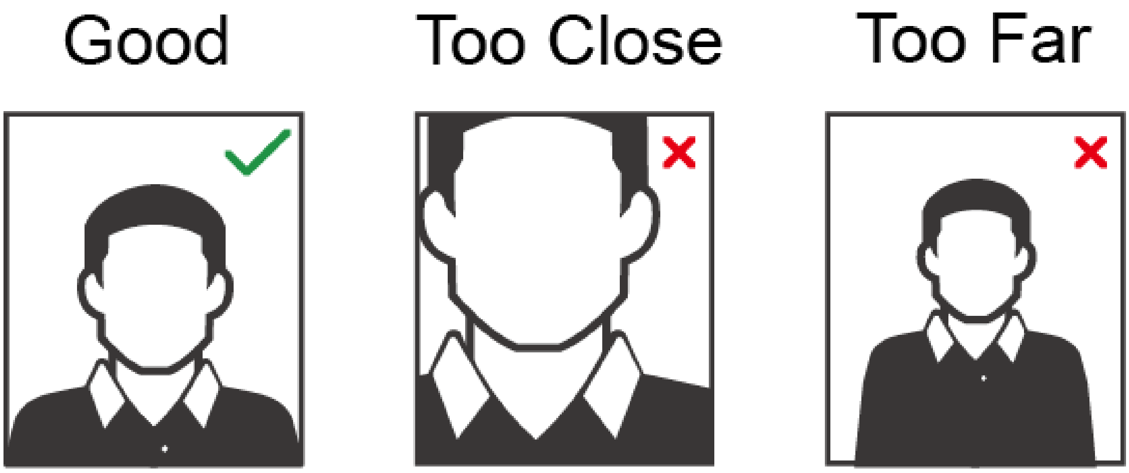
Requirements of Faces

- Make sure that the face is clean and forehead is not covered by hair.
- Do not wear glasses, hats, heavy beards, or other face ornaments that influence face image recording.
- With eyes open, without facial expressions, and make your face toward the center of camera.
- When recording your face or during face recognition, do not keep your face too close to or too far from the camera.

Appendix Figure 4-2 Head position



Appendix Figure 4-3 Face distance



- When importing face images through the management platform, make sure that image resolution is within the range from 150 × 300 pixels to 600 × 1200 pixels. It is recommended that the resolution be greater than 500 × 500 pixels, the image size be less than 100 KB, and the image name and person ID be the same.
- Make sure that the face takes up more than 1/3 but no more than 2/3 of the whole image area, and the aspect ratio does not exceed 1:2.

Appendix 5 Security Recommendation

Account Management

1. **Use complex 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: 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 repeating characters, such as 111, aaa, etc.
2. **Change passwords periodically**
   It is recommended to periodically change the device password to reduce the risk of being guessed or cracked.
3. **Allocate accounts and permissions appropriately**
   Appropriately add users based on service and management requirements and assign minimum permission sets to users.
4. **Enable account lockout function**
   The account lockout function is enabled by default. You are advised to keep it enabled to protect account security. After multiple failed password attempts, the corresponding account and source IP address will be locked.
5. **Set and update password reset information in a timely manner**
   The device supports password reset function. To reduce the risk of this function being used by threat actors, if there is any change in the information, please modify it in time. When setting security questions, it is recommended not to use easily guessed answers.

Service Configuration

1. **Enable HTTPS**
   It is recommended that you enable HTTPS to access web services through secure channels.
2. **Encrypted transmission of audio and video**
   If your audio and video data contents are very important or sensitive, it is recommended to use encrypted transmission function in order to reduce the risk of your audio and video data being eavesdropped during transmission.
3. **Turn off non-essential services and use safe mode**
   If not needed, it is recommended to turn off some services such as SSH, SNMP, SMTP, UPnP, AP hotspot etc., to reduce the attack surfaces.
   If necessary, it is highly recommended to choose safe modes, including but not limited to the following services:
   - SNMP: Choose SNMP v3, and set up strong encryption and authentication passwords.
   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up complex passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up complex passwords.
4. **Change HTTP and other default service ports**
   It is recommended that you change the default port of HTTP and other services to any port between 1024 and 65535 to reduce the risk of being guessed by threat actors.

Network Configuration

1. **Enable Allow list**

   It is recommended that you turn on the allow list function, and only allow IP in the allow list to access the device. Therefore, please be sure to add your computer IP address and supporting device IP address to the allow list.
2. **MAC address binding**

   It is recommended that you bind the IP address of the gateway to the MAC address on the device to reduce the risk of ARP spoofing.
3. **Build a secure network environment**

   In order to better ensure the security of devices and reduce potential cyber risks, the following are recommended:
   - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network;
   - According to the actual network needs, partition the network: if there is no communication demand between the two subnets, it is recommended to use VLAN, gateway and other methods to partition the network to achieve network isolation;
   - Stablish 802.1x access authentication system to reduce the risk of illegal terminal access to the private network.

Security Auditing

1. **Check online users**

   It is recommended to check online users regularly to identify illegal users.
2. **Check device log**

   By viewing logs, you can learn about the IP addresses that attempt to log in to the device and key operations of the logged users.
3. **Configure network log**

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

Software Security

1. **Update firmware in time**

   According to the industry standard operating specifications, the firmware of devices needs to be updated to the latest version in time in order to ensure that the device has the latest functions and security. If the device is connected to the public network, it is recommended to enable the online upgrade automatic detection function, so as to obtain the firmware update information released by the manufacturer in a timely manner.
2. **Update client software in time**

   It is recommended to download and use the latest client software.

Physical Protection

It is recommended that you carry out physical protection for devices (especially storage devices), such as placing the device in a dedicated machine room and cabinet, and having access control and key management in place to prevent unauthorized personnel from damaging hardware and other peripheral equipment (e.g. USB flash disk, serial port).