

Face Recognition Access Controller

Quick Start Guide








Foreword

General

This manual introduces the functions and operations of the Face Recognition Access Controller (hereinafter referred to as the "Device"). 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.	April 2022

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, audio, 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 to: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.

- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right 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



- 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.

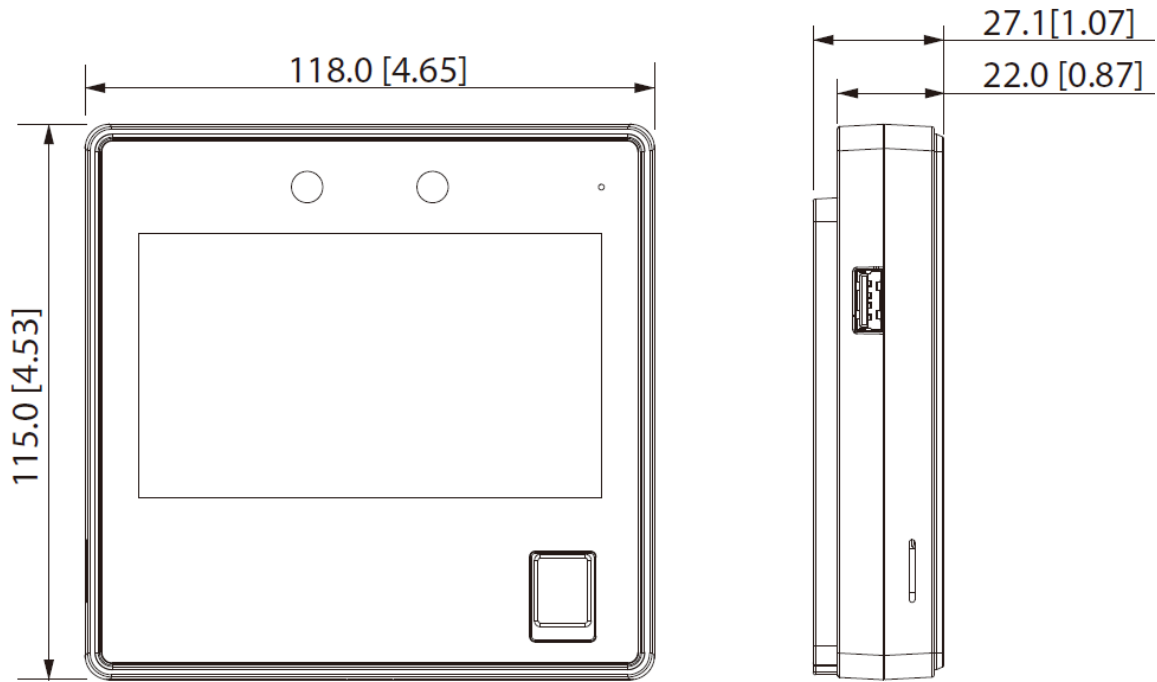
Table of Contents

Foreword	I
Important Safeguards and Warnings	III
1 Structure	1
2 Connection and Installation	2
2.1 Installation Requirements	2
2.2 Wiring	4
2.3 Installation Process	5
2.3.1 Wall mount	5
2.3.2 86 Box Mount	6
3 Local Configurations	8
3.1 Initialization	8
3.2 Adding New Users	9
4 Logging in to the Webpage	12
Appendix 1 Important Points of Fingerprint Registration Instructions	13
Appendix 2 Important Points of Face Registration	15
Appendix 3 Important Points of QR Code Scanning	18
Appendix 4 Security Recommendation	19

1 Structure

The front appearance might differ depending on different models of the Device. Here we take the fingerprint model as an example.

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



2 Connection and Installation

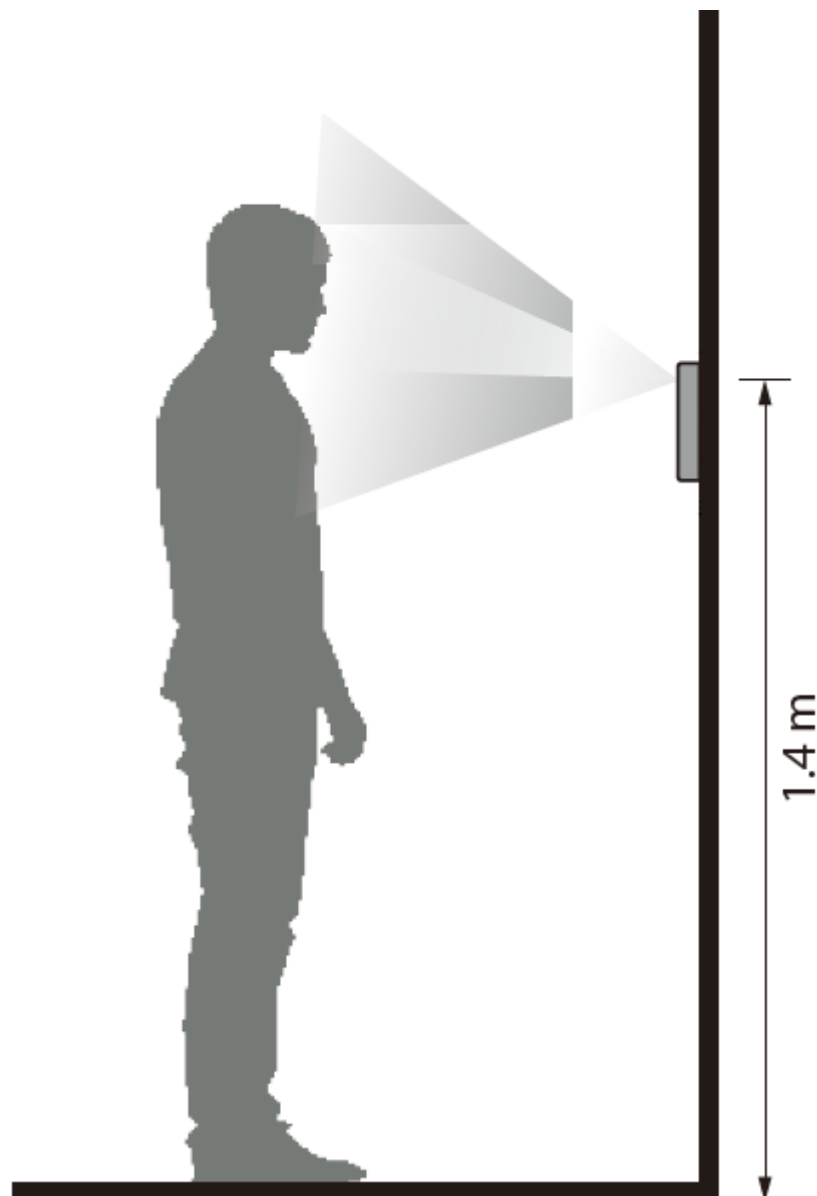
2.1 Installation Requirements



- The installation height is 1.4 m (from the lens to the ground).
- The light at the 0.5 meters away from the Device should be no less than 100 lux.
- We recommend you install the 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.

Installation Height

Figure 2-1 Installation height requirement



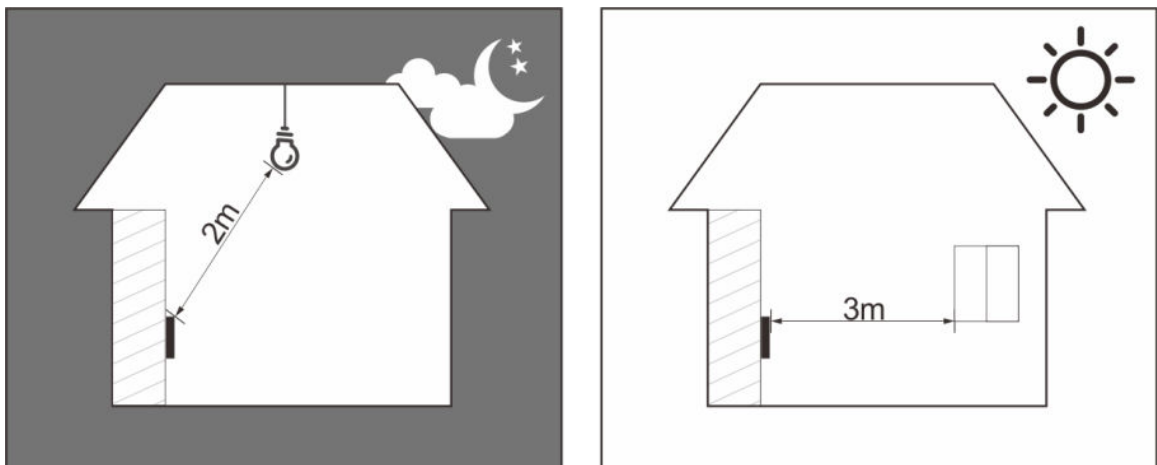
Ambient Illumination Requirements

Figure 2-2 Ambient illumination requirements



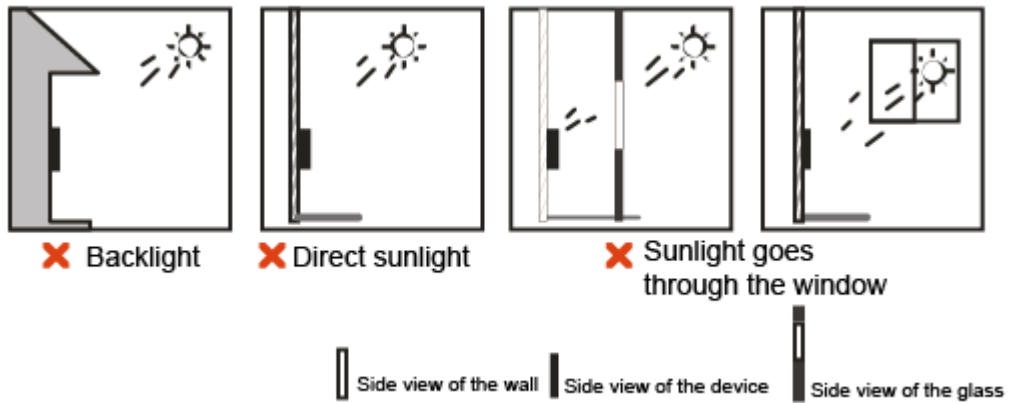
Recommended Installation Location

Figure 2-3 Recommended installation location



Installation Location Not Recommended

Figure 2-4 Installation location not recommended



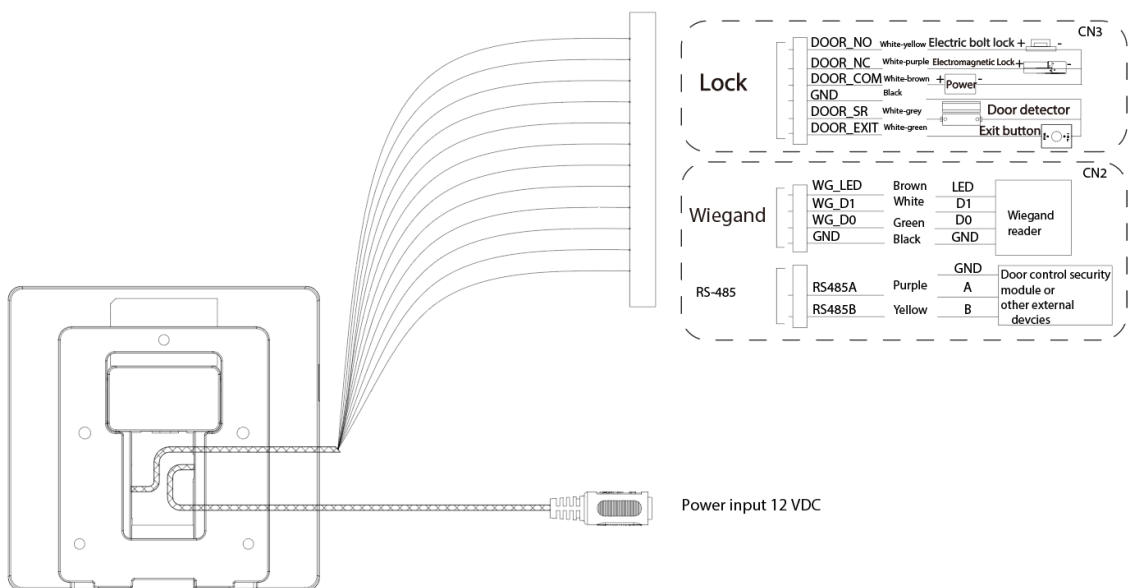
2.2 Wiring

Background Information



- If you want to connect an external security module, select **Connection > Serial Port > RS-485 Settings > Security Module**. The security module needs to be purchased separately by customers.
- When the security module is turned on, the exit button and the lock control will not be effective.

Figure 2-5 Wiring



2.3 Installation Process

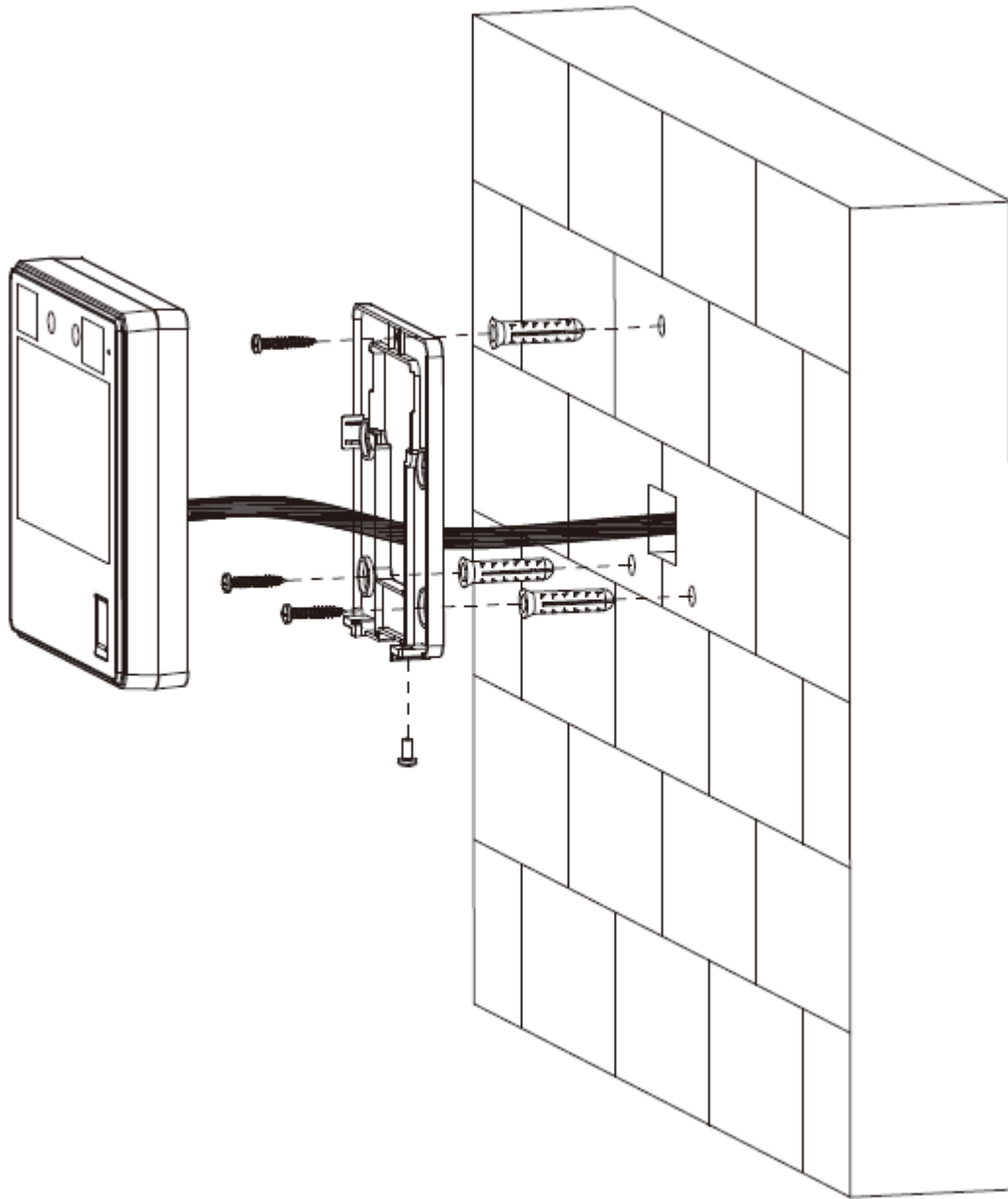
This section uses the fingerprint model of the Device as an example.

2.3.1 Wall mount

Procedure

- Step 1 According the position of the holes in the installation bracket, drill 3 holes in the wall. Put expansion bolts in the holes.
- Step 2 Use the 3 screws to fix the installation bracket to the wall.
- Step 3 Wire the Device.
- Step 4 Attach the Device to the bracket.
- Step 5 Screw in 1 screw securely at the bottom of the Device.

Figure 2-6 Wall mount

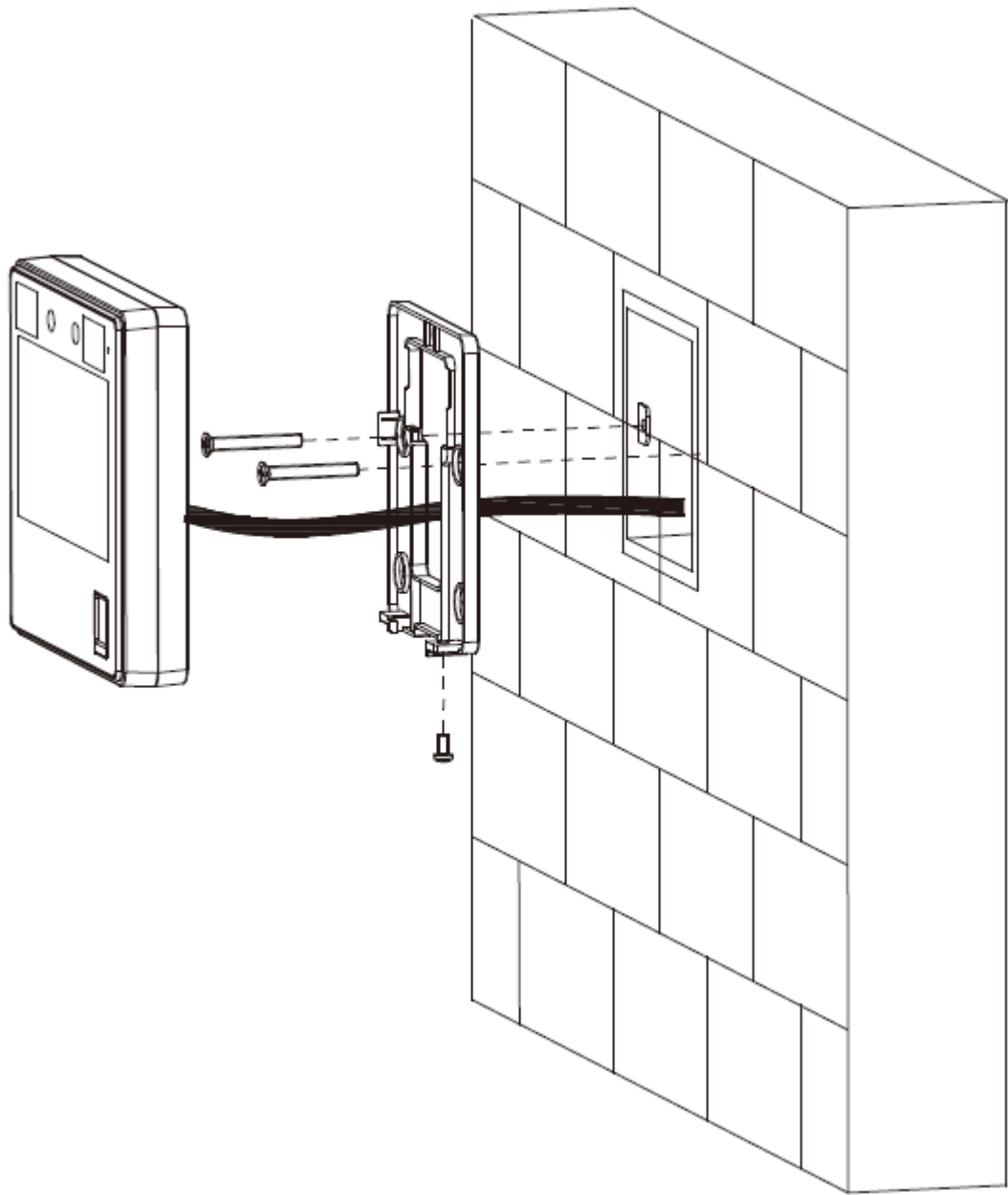


2.3.2 86 Box Mount

Procedure

- Step 1 Put an 86 box in the wall at an appropriate height.
- Step 2 Fasten the installation bracket to the 86 box with 2 screws.
- Step 3 Wire the Device.
- Step 4 Attach the Device to the bracket.
- Step 5 Screw in 1 screw securely at the bottom of the Device.

Figure 2-7 86 box mount



3 Local Configurations

Local operations might differ depending on different models.

3.1 Initialization

For the first-time use or after you restored factory defaults, you need to select a language, and then set a password and email address for the admin account. After that, you can use the admin account to log in to the main menu screen of the Device and its webpage.

Figure 3-1 Initialization

The screenshot shows a dark-themed 'Device Initialization' screen. It features four input fields stacked vertically: 'Admin' (containing 'admin'), 'PWD', 'PWD Confirm', and 'E-mail'. At the bottom, there are two buttons labeled 'Yes' and 'Clear'.



- If you forget the administrator password, send a reset request to your linked e-mail address.
- 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.

3.2 Adding New Users

Add new users by entering user information such as name, card number, face, and fingerprint, and then set user permissions.

Procedure

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

Step 2 Configure user parameters.



Figure 3-2 New user (1)

User Level	User
Period	255-Default
Holiday Plan	255-Default
Valid Date	2037-12-31
User Type	General

Figure 3-3 New user (2)

User ID	3
Name	
FP	0
Face	0
Card	0
PWD	

Table 3-1 New user description

Parameter	Description
User ID	Enter the user ID. The ID can be numbers, letters, and their combinations, and the maximum length of the user ID is 32 characters. Each ID is unique.
Name	Enter the username and the maximum length is 32 characters, including numbers, symbols, and letters.
FP	<p>Each user can register up to 3 fingerprints. Follow the on-screen prompts to register fingerprints. You can set the registered fingerprint as the duress fingerprint, and an alarm will be triggered if the door is unlocked by the duress fingerprint.</p>  <ul style="list-style-type: none"> • We do not recommend you set the first fingerprint as the duress fingerprint. • Fingerprint function is only available for the fingerprint model of the Device.
Face	Make sure that your face is centered on the image capturing frame, and the face image will be captured automatically. You can register again if you find the captured face image is not satisfying.
Card	<p>A user can register up to five cards. Enter your card number or swipe your card, and then the card information will be read by the Device.</p> <p>You can set the registered card as the duress card, and then an alarm will be triggered when a duress card is used to unlock the door.</p>  <p>Only card swiping model supports this function.</p>
PWD	Enter the user password to unlock the door. The maximum length of the password is 8 digits.
User Level	<p>Set user permissions for new users.</p> <ul style="list-style-type: none"> • General : Users only have door access permission. • Admin : Administrators can unlock the door and configure the Device.
Period	Users are allowed to enter a controlled area within the defined period. The default value is 255, which means no period is configured.
Holiday Plan	Users are allowed to enter a controlled area within the scheduled holidays. The default value is 255, which means no holiday plan is configured.
Valid Date	Define a period during which the user is granted with access to a secured area.

Parameter	Description
User Type	<ul style="list-style-type: none"> ● General : General users can unlock the door normally. ● Blocklist : When users in the blocklist unlock the door, service personnel receive a notification. ● Guest : Guests can unlock the door within a defined period or for a certain number of times. After the defined period expires or the unlocking times runs out, they cannot unlock the door. ● Patrol : Paroling users can have their attendance tracked, but they have no unlocking permissions. ● VIP : When VIP unlock the door, service personnel will receive a notification. ● Others : When they unlock the door, the door will stay unlocked for 5 more seconds. ● Custom User 1/2 : Same as General.

Step 3 Tap .

4 Logging in to the Webpage

On the webpage, you can also configure and update the Device.

Prerequisites

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

Background Information



Webpage configurations differ depending on models of the Device. Only certain models of the Device support network connection.

Procedure

Step 1 Open a web browser, go to the IP address of the Device.



You can use IE11, Firefox or Chrome.

Step 2 Enter the user name and password.

Figure 4-1 Initialization

WEB SERVICE

Username:

Password:

[Forget Password?](#)

Login



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

Step 3 Click **Login**.

Appendix 1 Important Points of Fingerprint Registration Instructions

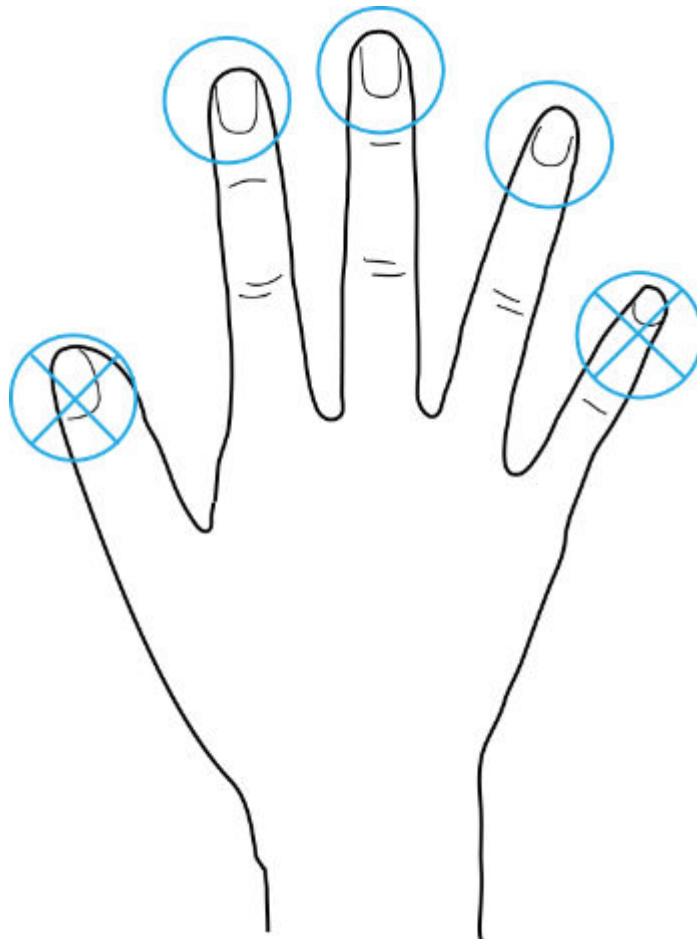
When you register the fingerprint, pay attention to the following points:

- 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

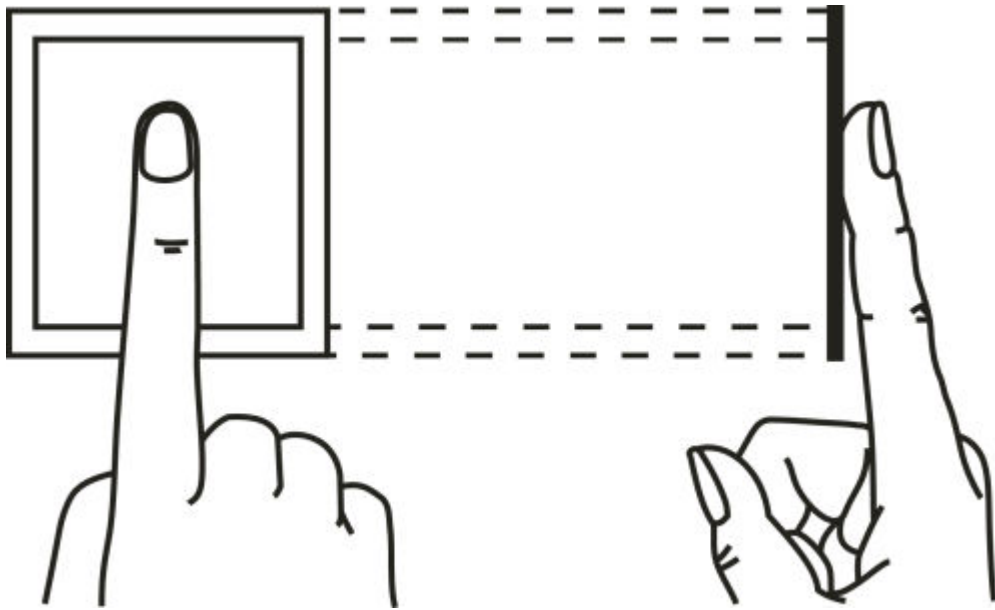
Forefingers, middle fingers, and ring fingers are recommended. Thumbs and little fingers cannot be put at the recording center easily.

Appendix Figure 1-1 Recommended fingers

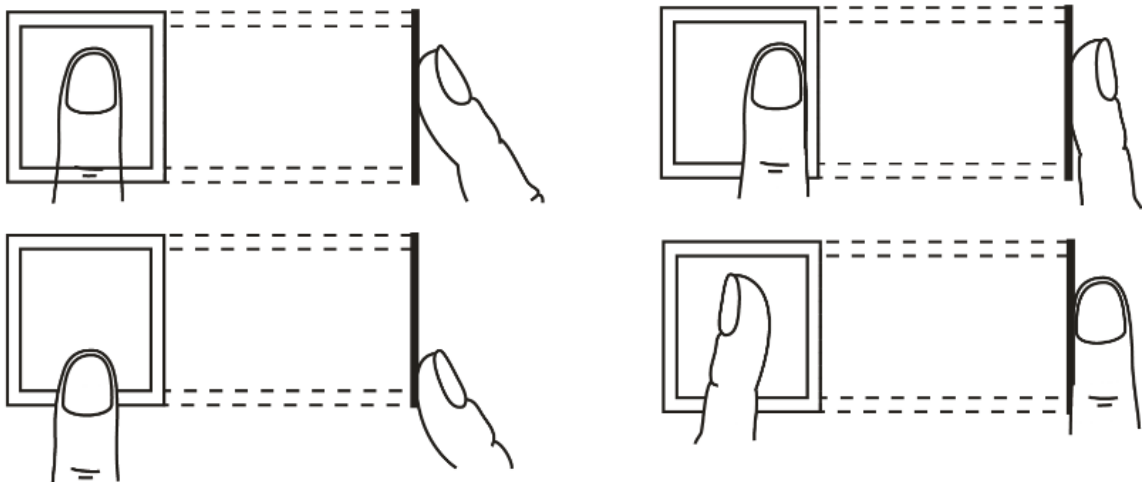


How to Press Your Fingerprint on the Scanner

Appendix Figure 1-2 Correct placement



Appendix Figure 1-3 Wrong placement



Appendix 2 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.

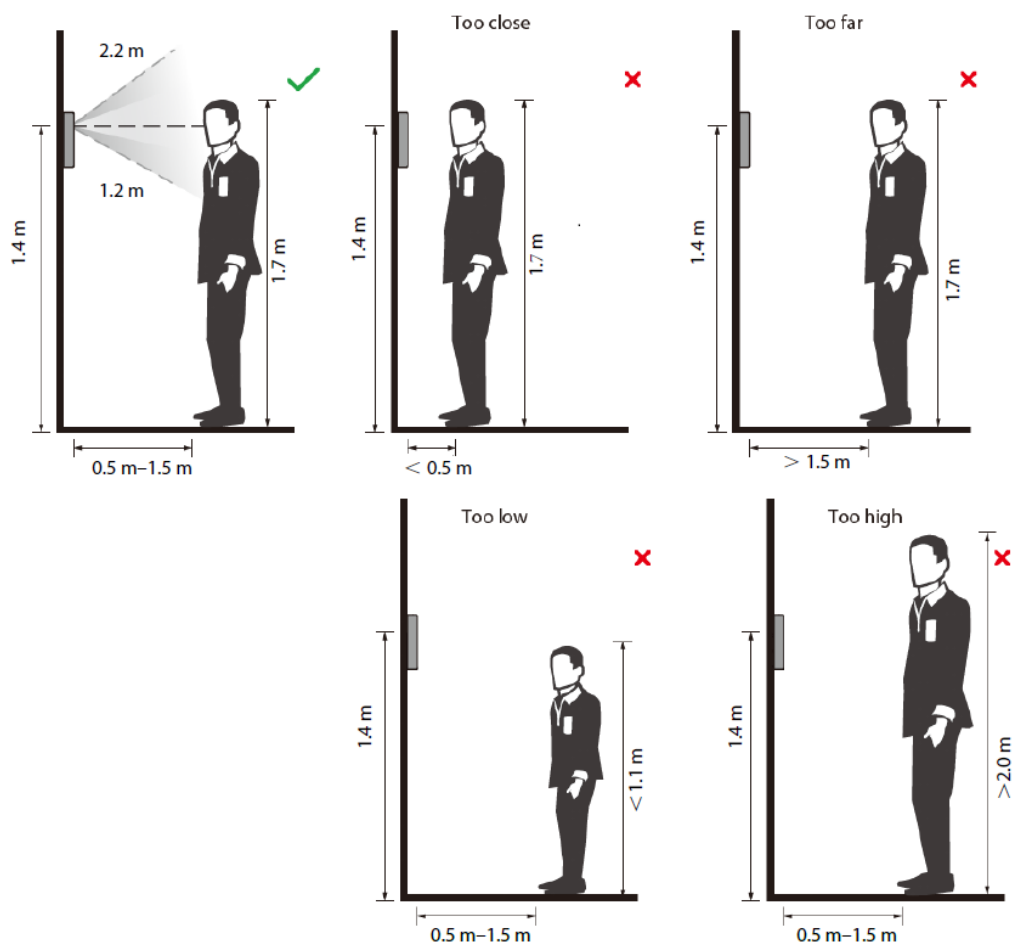
Face Position

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 2-1 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 2-2 Head position



Appendix Figure 2-3 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.

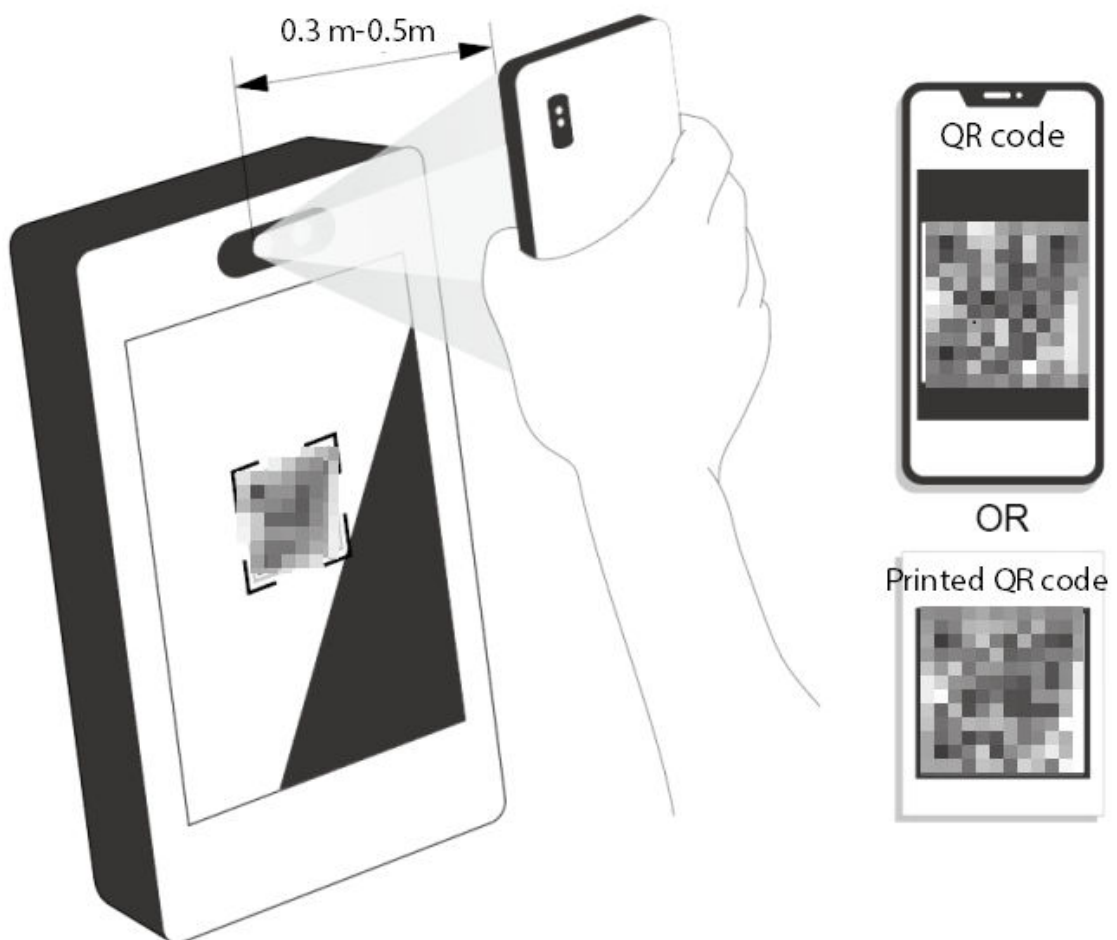
Appendix 3 Important Points of QR Code Scanning

Place the QR code at a distance of 30 cm-50 cm away from the lens of the Access Controller or the lens of the QR code extension module. It supports QR code that is larger than 30 cm×30 cm and less than 100 bytes in size.



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

Appendix Figure 3-1 QR code scanning



Appendix 4 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;
- Establish 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).