Face Recognition Access Controller

User's Manual

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 Time
V1.0.1	Updated the wiring.	June 2022
V1.0.0	First Release.	May 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 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.

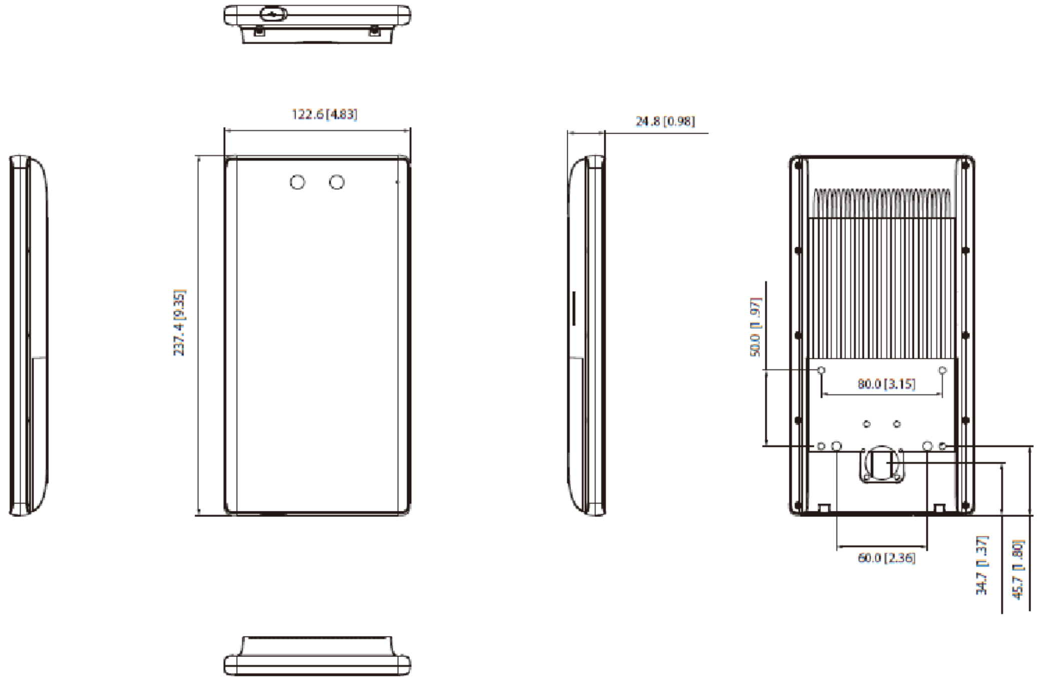
- Operate the Access Controller within the rated range of power input and output.
- Use the Access Controller under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the Access Controller, and make sure that there is no object filled with liquid on the Access Controller to prevent liquid from flowing into it.
- Do not disassemble the Access Controller without professional instruction.

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.

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

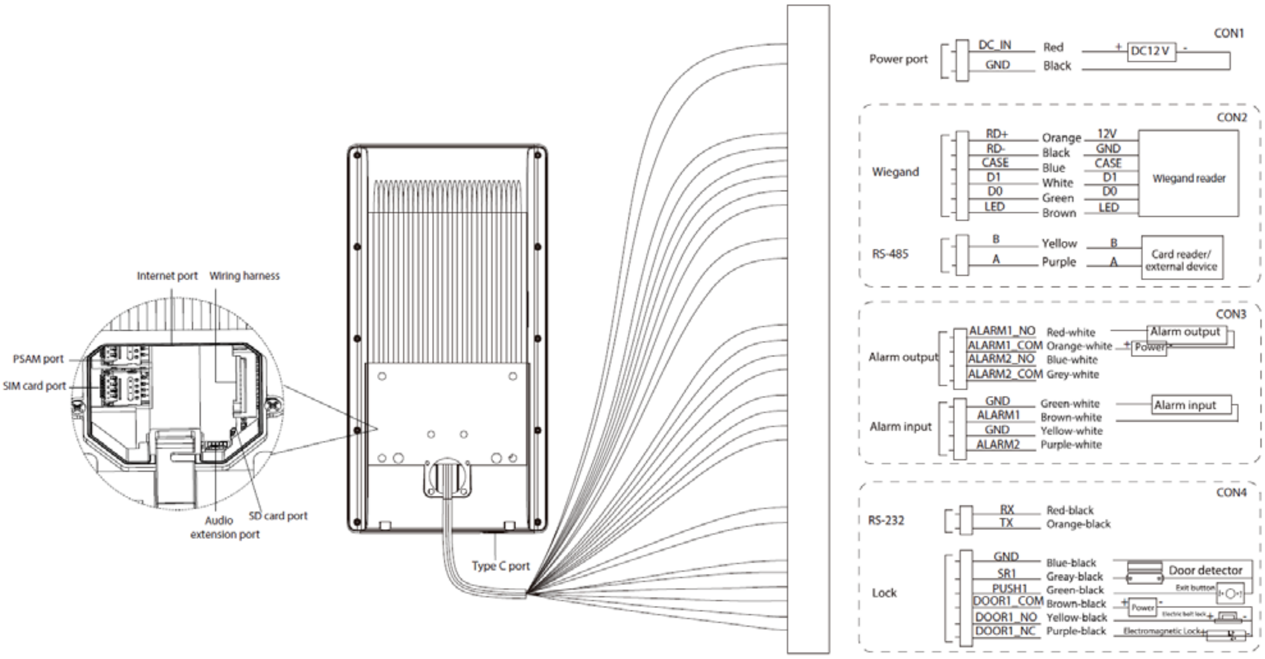


2 Connection and Installation

2.1 Wiring

The access controller needs to be connected to devices like sirens, readers, and door contacts.

Figure 2-1 Cable connections



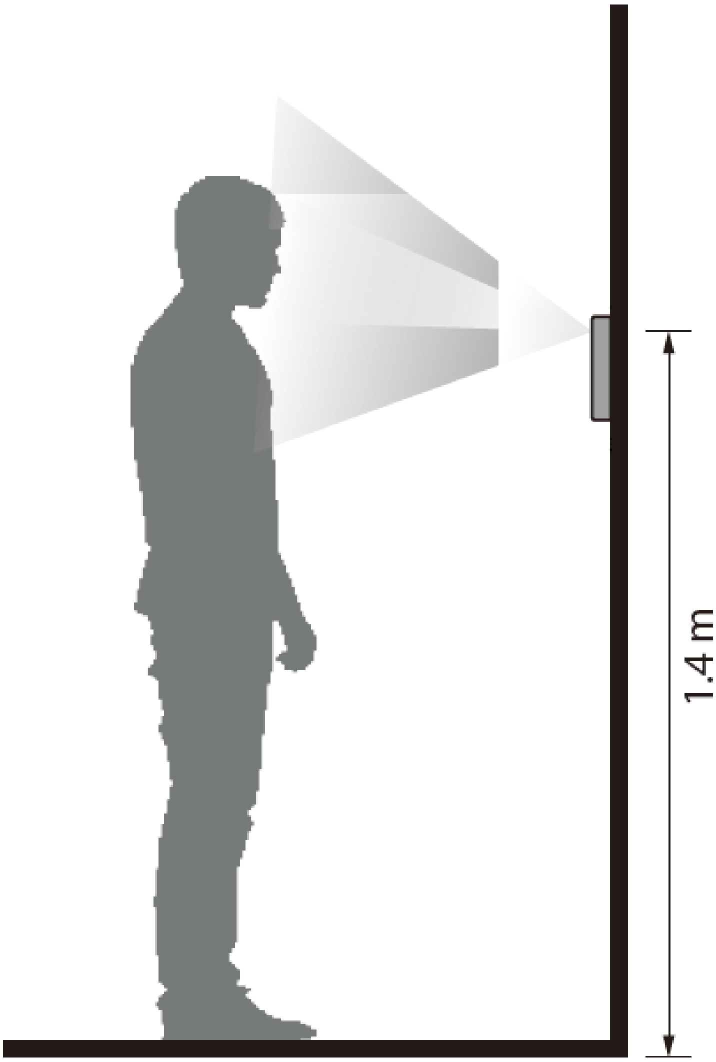
- The back panel of the Access Controller has SIM card port, Internet port, audio extension port, SD card port and wiring harness. Ports might differ depending on different models of Access Controller.
- If you want to connect an external speaker, an audio adapter cable is required.
- The load capacity of type C port is 5 V 500 mA.

2.2 Installation Requirements

- The light at the 0.5 meters away from the access controller should be no less than 100 Lux.
- We recommend 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.

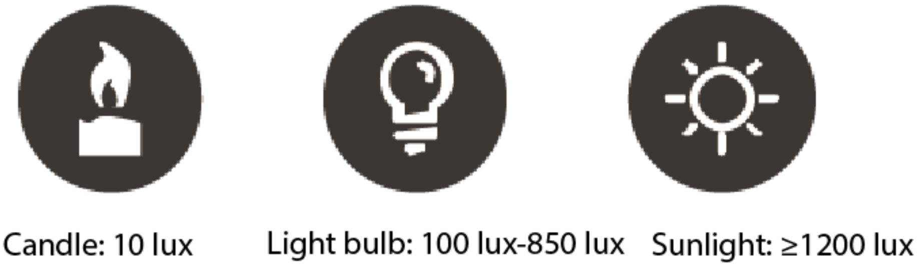
Installation Height

Figure 2-2 Installation height requirement



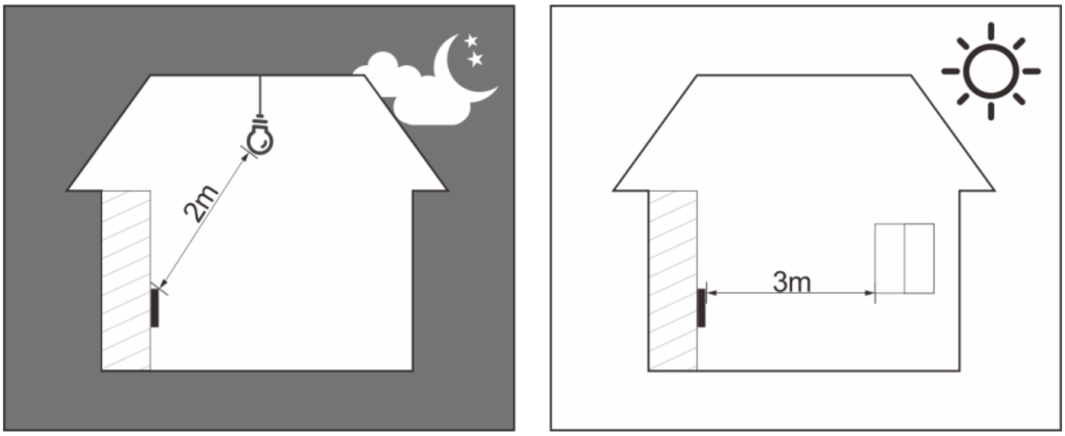
Ambient Illumination Requirements

Figure 2-3 Ambient illumination requirements



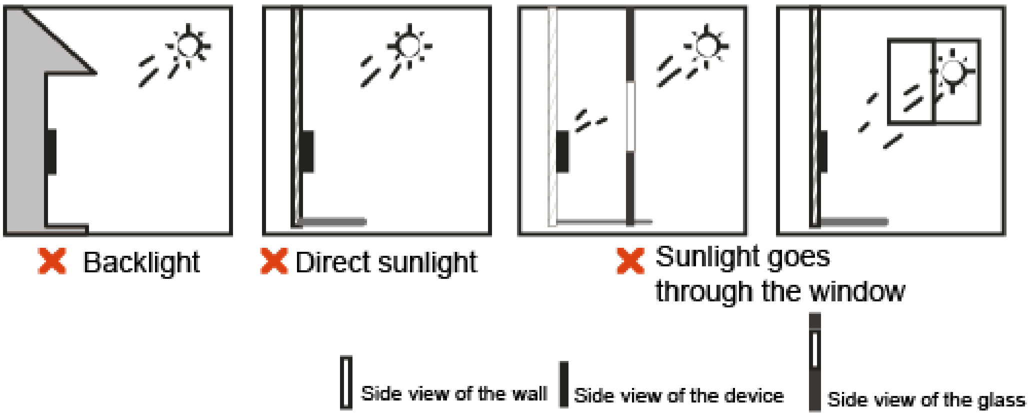
Recommended Installation Location

Figure 2-4 Recommended installation location



Installation Location Not Recommended

Figure 2-5 Installation location not recommended



2.3 Installation Process

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

2.3.1 Wall mount

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

Step 2 Remove the sheet metal at the bottom of the bracket.

Step 3 Use the four screws to fix the bracket to the wall.

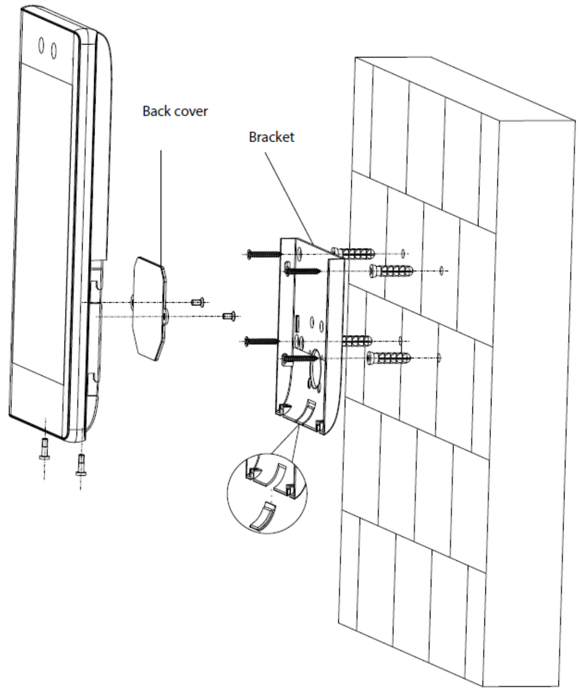
Step 4 Wire the Access Controller. For details, see "2.1 Wiring".

Step 5 Use two screws to fix the back cover to the Access Controller.

Step 6 Fix the Access Controller on the bracket.

Step 7 Screw in two screws securely at the bottom of the Access Controller.

Figure 2-6 Wall mount



2.3.2 86 Case Mount

Step 1 Put an 86 case in the wall at an appropriate height.

Step 2 Fasten the bracket to the 86 case with two screws.

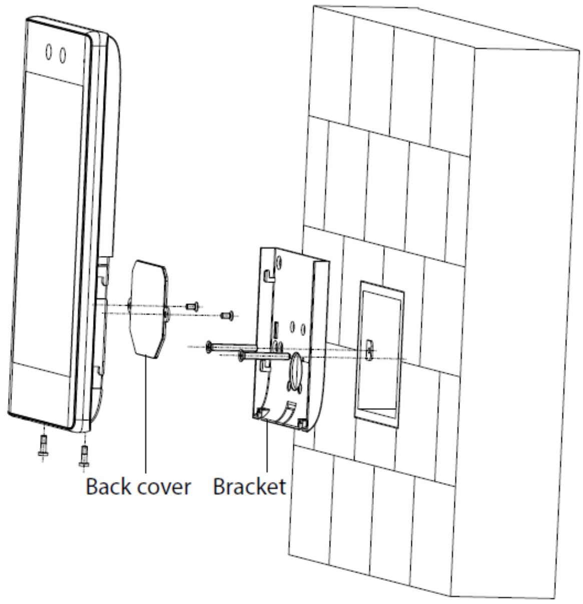
Step 3 Wire the Access Controller. For details, see "2.1 Wiring"

Step 4 Use two screws to fix the back cover to the Access Controller.

Step 5 Fix the Access Controller on the bracket.

Step 6 Screw in two screws securely at the bottom of the Access Controller.

Figure 2-7 86 case mount



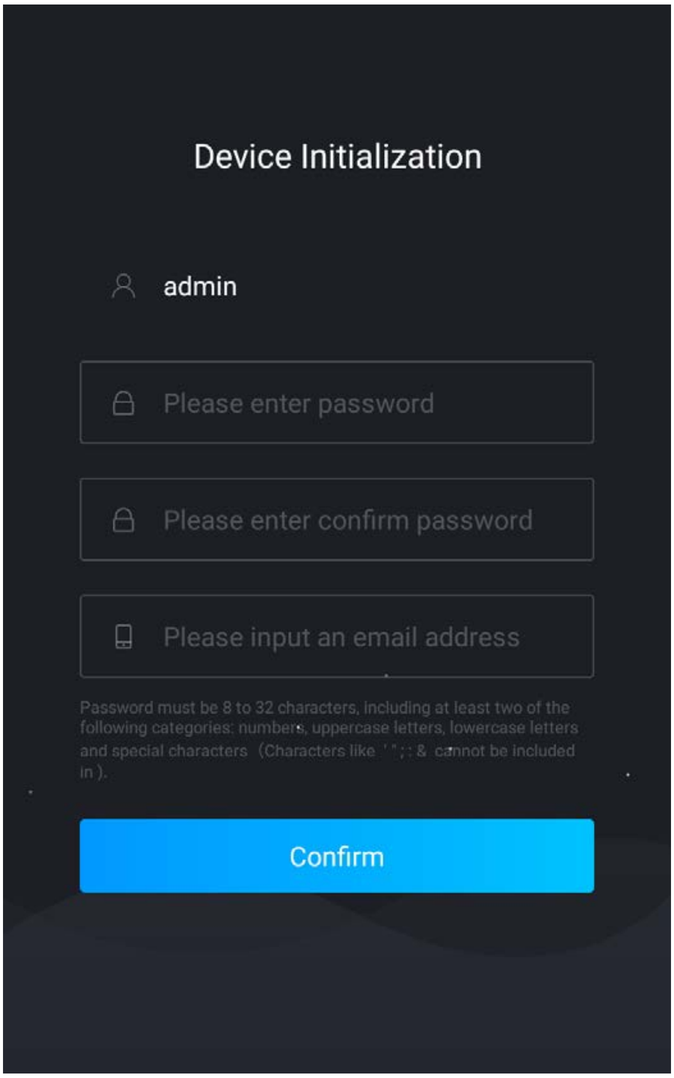
3 Local Configurations

Local operations might differ depending on different models of Access Controller.

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 screen of the Access Controller and the web interface.

Figure 3-1 Initialization



Device Initialization

admin

Please enter password

Please enter confirm password

Please input an email address

Password must be 8 to 32 characters, including at least two of the following categories: numbers, uppercase letters, lowercase letters and special characters（Characters like ' " ; : & cannot be included in).

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

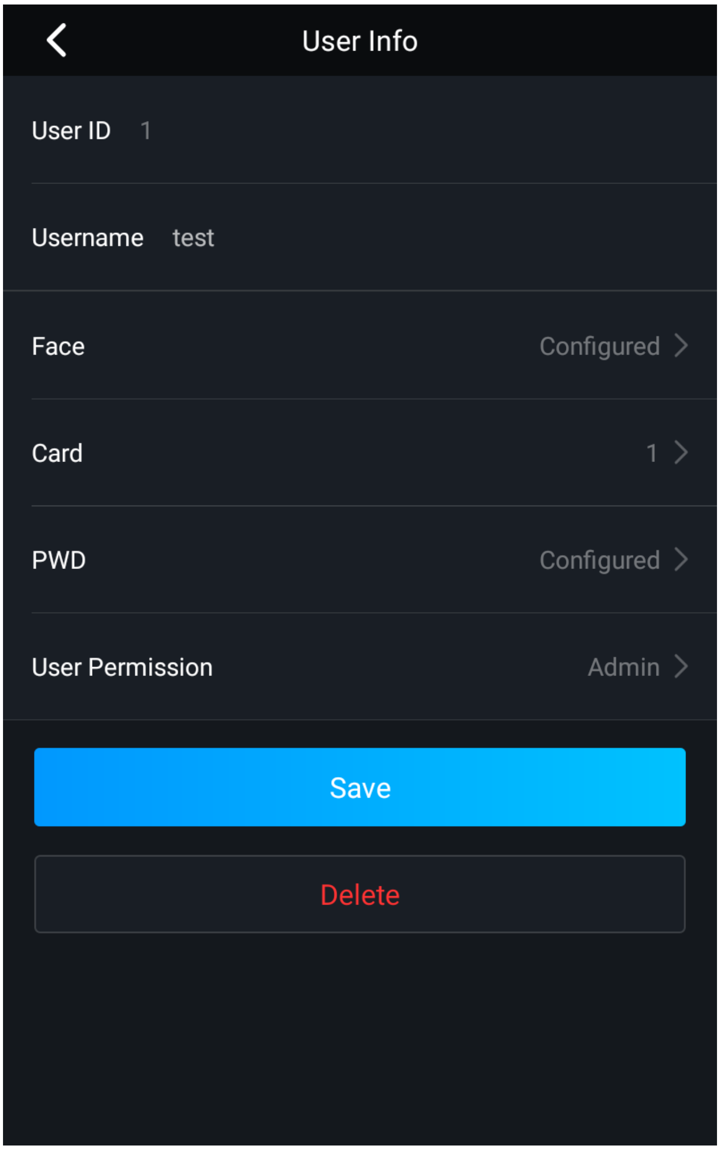
3.2 Adding New Users

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

Step 1 On the **Main Menu** screen, select **User**, and then tap ➕.

Step 2 Configure user parameters.

Figure 3-2 New user



User Info

User ID 1

Username test

Face Configured

Card 1

PWD Configured

User Permission Admin

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.
Username	Enter the username and the maximum length is 32 characters, including numbers, symbols, and letters.

Parameter	Description
Fingerprint	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. ● We do not recommend you set the first fingerprint as the duress fingerprint. ● Fingerprint function is only available for the fingerprint model of the Access Controller.
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	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 Access Controller. 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.
PWD	Enter the user password to unlock the door. The maximum length of the password is 8 digits.
User Permission	Set user permissions for new users. ● **General**: Users only have door access permission. ● **Admin**: Administrators can unlock the door and configure the Access Controller.

Step 3 Tap **Save**.

Related Operations

On the **User** screen, you can manage the added users.

- Search for users: Tap the search bar and then enter the username.
- Edit users: Select the user, edit the user, and then tap **Save** to save the changes.
- Delete users
  - Delete individually: Select a user, and then tap **Delete**.
  - Delete in batches:
    1. On the **User** screen, tap •••, and then tap **Batch Delete**.
    2. Select users and then tap **Delete**.
  - Clear all users: On the **Batch Delete** screen, tap **Clear**.

4 Web Configurations

On the web interface, you can also configure and update the Access Controller.

Web configurations differ depending on models of the Access Controller.

4.1 Initialization

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

Prerequisites

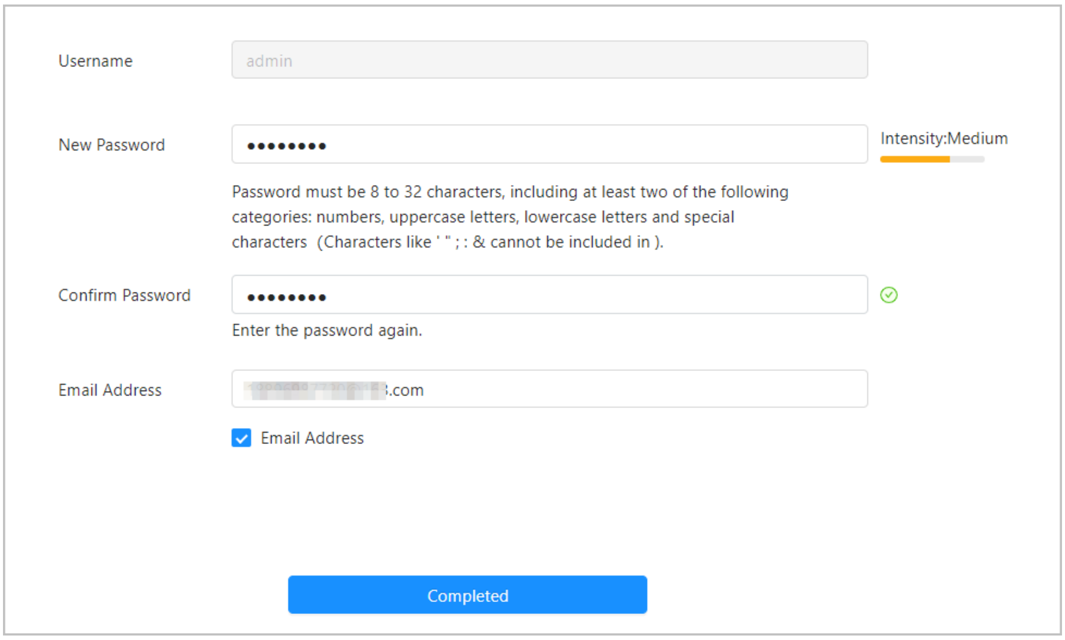
Make sure that the computer used to log in to the web interface is on the same LAN as the Access Controller.

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

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

You can log in to the web with Chrome or Firefox.

Figure 4-1 Initialization



Username: admin

New Password: •••••••• Intensity:Medium

Password must be 8 to 32 characters, including at least two of the following categories: numbers, uppercase letters, lowercase letters and special characters (Characters like ' " ; : & cannot be included in).

Confirm Password: •••••••• ✓

Enter the password again.

Email Address: [redacted].com

☑ Email Address

Step 2 Enter and confirm the password, enter an email address, and then click **Completed**.

- 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

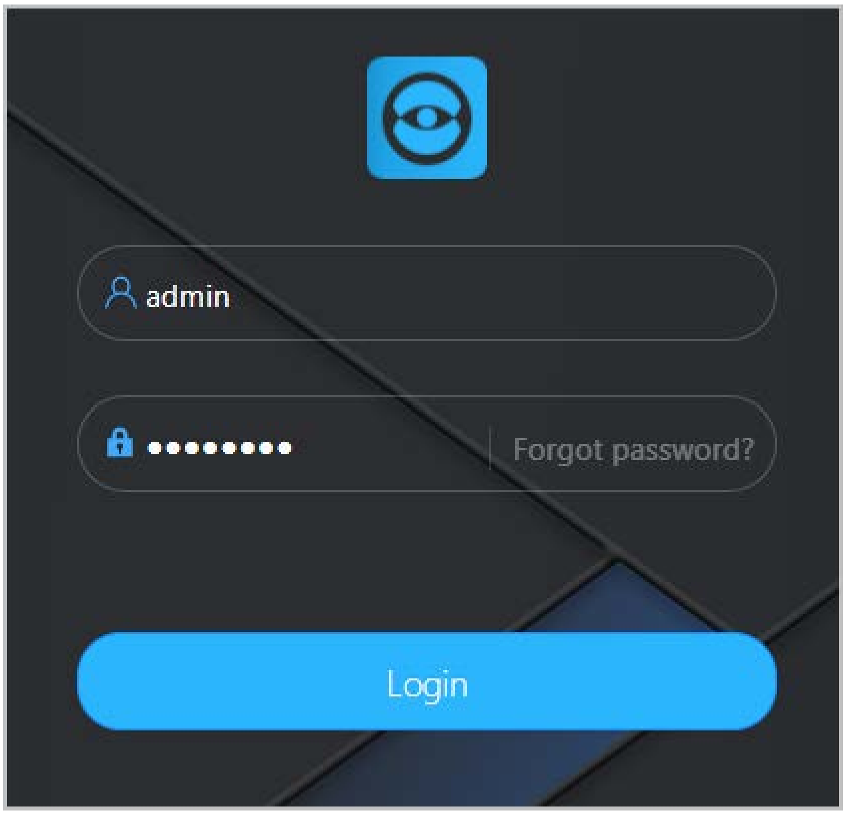
improve security.

- If you want to reset the administrator password by scanning the QR code, you need the linked email address to receive the security code.

4.2 Logging In

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

Figure 4-2 Login



Step 2 Enter the user name and password.

- 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 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 ☎

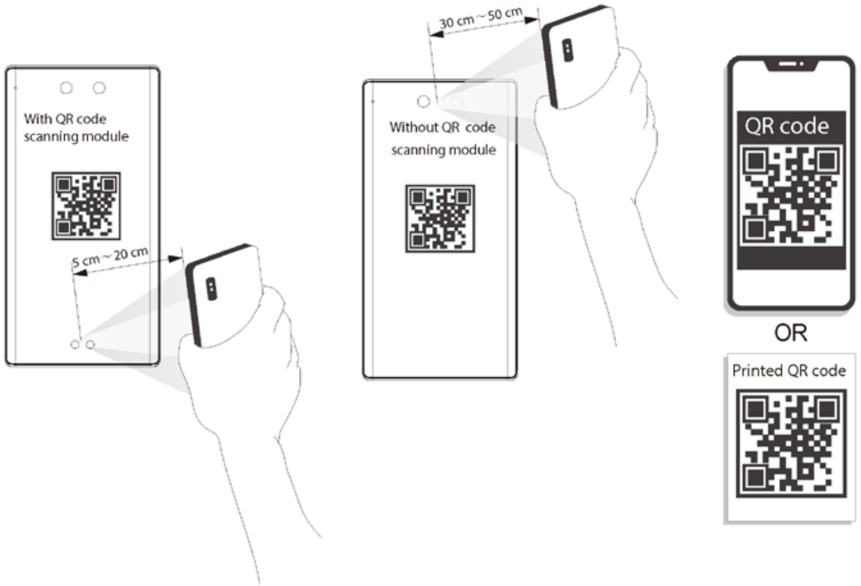
Step 2 Enter the room No, and then tap ☎.

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 5 cm - 20 cm away from the QR code scanning lens. It supports QR code that is 2 cm×2 cm - 5 cm×5 cm and less than 512 bytes in size.
- Access Controller (without QR code scanning module): Place the printed QR code at a distance of 30 cm-50 cm away from the lens of the Access Controller. It supports QR code that is 2.2 cm×2.2 cm～5 cm×5 cm and less than 64 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 Important Points of Fingerprint Registration Instructions

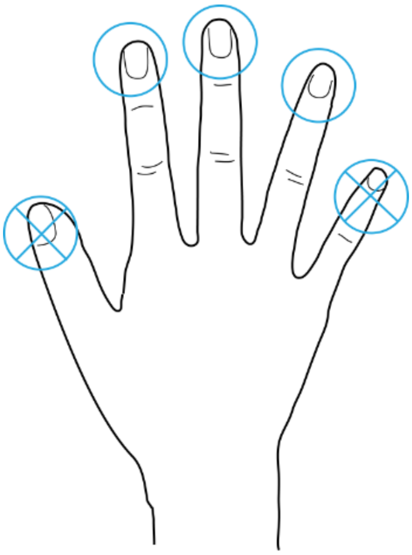
When you register the fingerprint, pay attention to the following points:

- 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

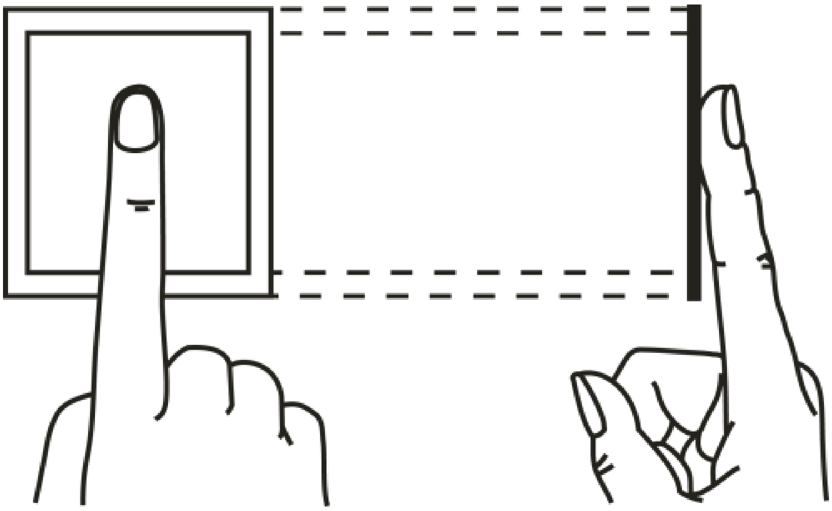
Forefingers, middle fingers, and ring fingers are recommended. Thumbs and little fingers cannot be put at the recording center easily.

Appendix Figure 3-1 Recommended fingers

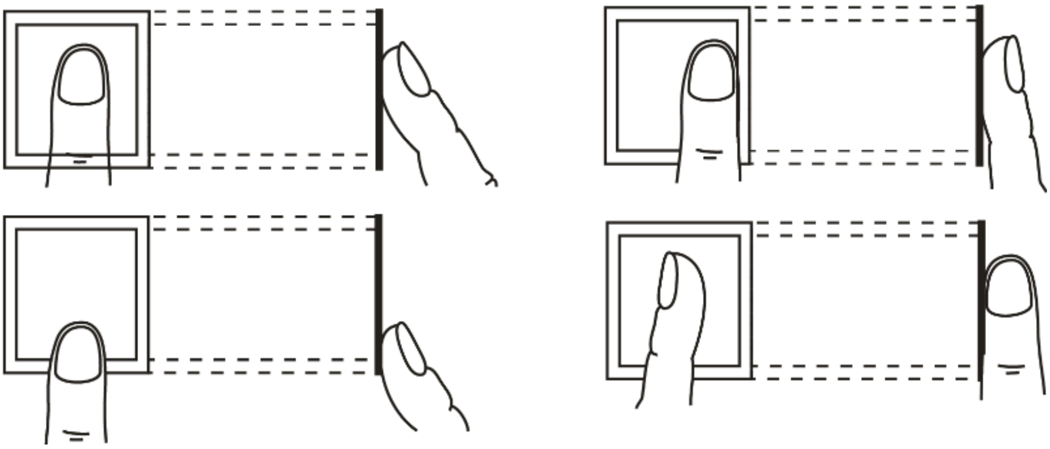


How to Press Your Fingerprint on the Scanner

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 access controller; otherwise face recognition might fail.
- Keep your face clean.
- Keep the access controller at least two meters away from light source and at least three meters away from windows or doors; otherwise backlight and direct sunlight might influence face recognition performance of the access controller.

During Registration

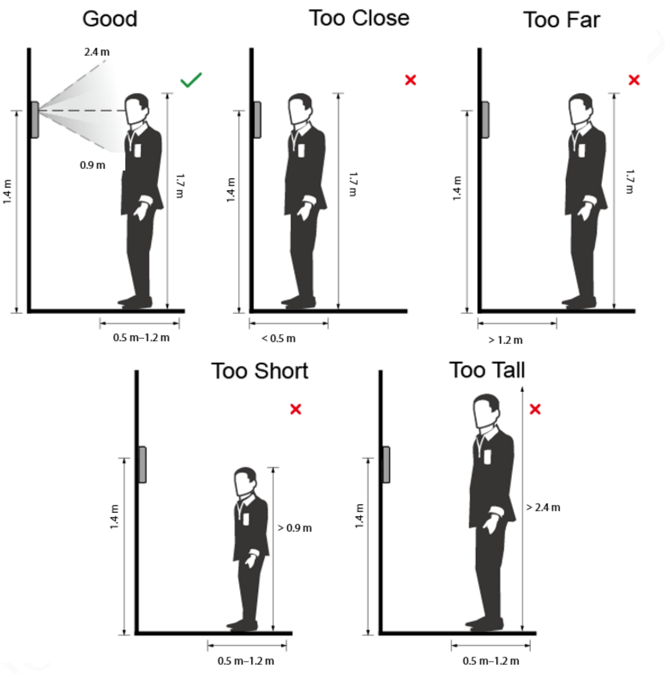
- You can register faces through the Access Controller or through the platform. For registration through the platform, see the platform user manual.
- Make your head center on the photo capture frame. The face image will be captured automatically.

- Do not shake your head or body, otherwise the registration might fail.
- Avoid two 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.

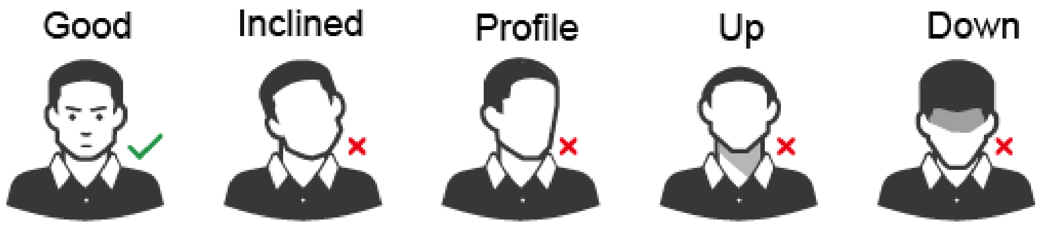
Appendix Figure 4-1 Appropriate face position



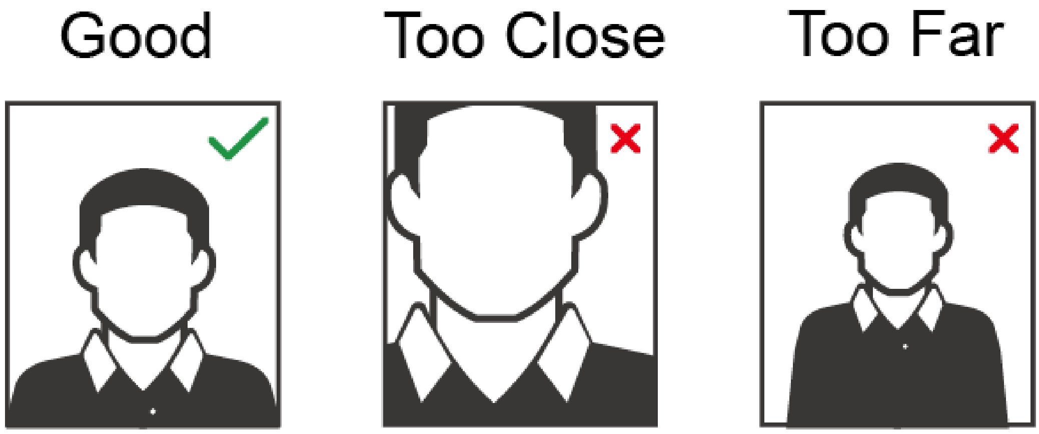
Requirements of Faces

- 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 150 × 300 pixels–600 × 1200 pixels; image pixels are more than 500 × 500 pixels; image size is less than 100 KB, and image name and person ID are 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 Cybersecurity Recommendations

Mandatory actions to be taken for basic equipment network security:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords:

   - The length should not be less than 8 characters.
   - Include at least two types of characters; character types include upper and lower case letters, numbers and symbols.
   - Do not contain the account name or the account name in reverse order.
   - Do not use continuous characters, such as 123, abc, etc.
   - Do not use overlapped characters, such as 111, aaa, etc.

2. **Update Firmware and Client Software in Time**

   - According to the standard procedure in Tech-industry, we recommend to keep your equipment (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the equipment is connected to the public network, it is recommended to enable the“auto-check for updates” function to obtain timely information of firmware updates released by the manufacturer.
   - We suggest that you download and use the latest version of client software.

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

1. **Physical Protection**

   We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable equipment (such as USB flash disk, serial port), etc.

2. **Change Passwords Regularly**

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

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

   The device supports password reset function. Please set up related information for password reset in time, including the end user’s mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. **Enable Account Lock**

   The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

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

   We suggest you to change default HTTP and other service ports into any set of numbers between 1024–65535, reducing the risk of outsiders being able to guess which ports you are using.

6. **Enable HTTPS**

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

7. **MAC Address Binding**

   We recommend you to bind the IP and MAC address of the gateway to the equipment, thus reducing the risk of ARP spoofing.

8. **Assign Accounts and Privileges Reasonably**

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

9. **Disable Unnecessary Services and Choose Secure Modes**

   If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

   If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

   - SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up strong passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

10. **Audio and Video Encrypted Transmission**

    If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

    Reminder: encrypted transmission will cause some loss in transmission efficiency.

11. **Secure Auditing**

    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check equipment log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. **Network Log**

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

13. **Construct a Safe Network Environment**

    In order to better ensure the safety of equipment and reduce potential cyber risks, we recommend:

    - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
    - The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
    - Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
    - Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.