

Face Recognition Access Controller

Quick Start Guide








Foreword

General

This manual introduces the installation and basic operations of the Face Recognition Access Controller (hereinafter referred to as "access controller").

Safety Instructions

The following categorized signal words with defined meaning 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, lower performance, or unpredictable result.
 TIPS	Provides methods to help you solve a problem or save you time.
 NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	May 2020

About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our 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 the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Important Safeguards and Warnings

This chapter describes the contents covering proper handling of the access controller, hazard prevention, and prevention of property damage. Read these contents carefully before using the access controller, comply with them when using, and keep the manual well for future reference.

Operation Requirements

- Do not place or install the access controller in a place exposed to sunlight or near the heat source.
- Keep the access controller away from dampness, dust or soot.
- Keep the access controller installed horizontally on the stable place to prevent it from falling.
- 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 the access controller.
- Install the access controller in a well-ventilated place, and do not block the ventilation of the access controller.
- Operate the access controller within the rated range of power input and output.
- Do not disassemble the access controller randomly.

Electrical Safety

- Improper battery use might result in fire, explosion, or inflammation.
- When replacing battery, make sure the same model is used.
- Use the recommended power cables in the region and conform to the rated power specification.
- Use the power adapter provided with the access controller; otherwise, it might result in people injury and device damage.
- The power source shall conform to the requirement of the Safety Extra Low Voltage (SELV) standard, and supply power with rated voltage which conforms to Limited power Source requirement according to IEC60950-1. Please note that the power supply requirement is subject to the device label.
- Connect the device (I-type structure) to the power socket with protective earthing.
- The appliance coupler is a disconnection device. When using the coupler, keep the angle for easy operation.

Table of Contents

Foreword	I
Important Safeguards and Warnings	III
1 Dimensions and Components	1
2 Connection and Installation	3
2.1 Cable Connection	3
2.2 Installation Notes.....	6
2.3 Installation	7
2.3.1 Installation of Model G.....	7
2.3.2 Installation of Model J.....	9
3 System Operations	12
3.1 Initialization	12
3.2 Adding New Users	12
4 Web Operations	15
Appendix 1 Notes of Face Recording/Comparison	16
Appendix 2 Fingerprint Record Instruction	19
Appendix 3 Cybersecurity Recommendations	21

1 Dimensions and Components

Figure 1-1 Dimensions and components of model G (mm [inch])

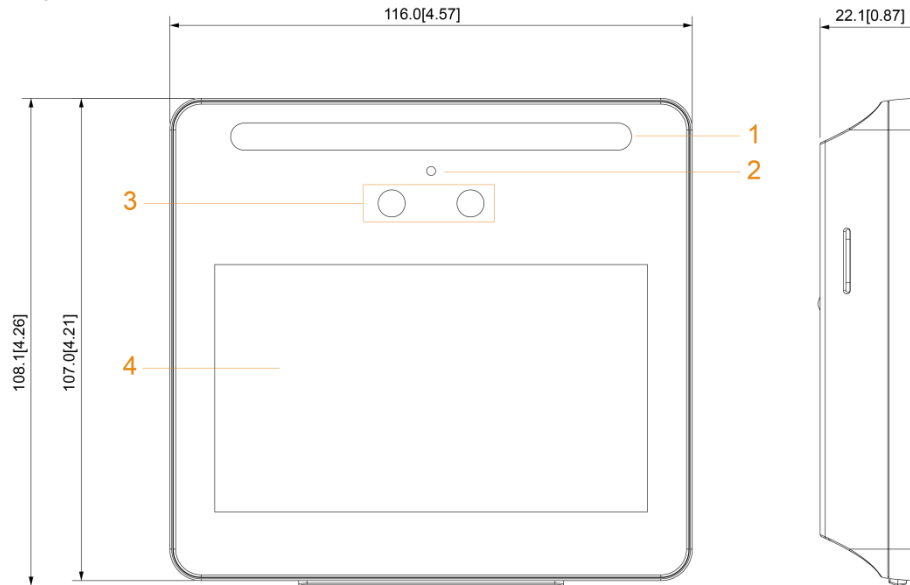


Table 1-1 Component description

No.	Name	No.	Name
1	White LED illuminator	3	Dual cameras
2	Mic	4	Display

Figure 1-2 Dimensions and components of model J with fingerprint sensor (mm [inch])

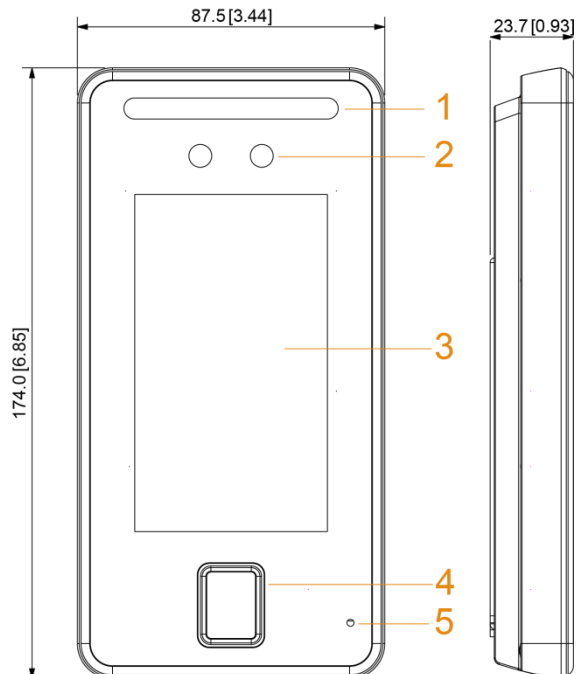


Table 1-2 Component description

No.	Name	No.	Name
1	White LED illuminator	3	Display
2	Dual cameras	4	Fingerprint sensor

5	Mic	—	—
---	-----	---	---

Figure 1-3 Dimensions and components of model J without fingerprint sensor (mm [inch])

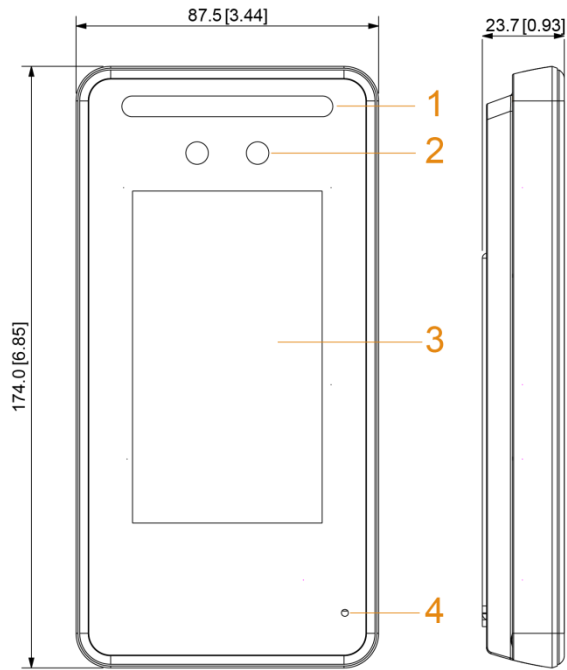


Table 1-3 Component description

No.	Name	No.	Name
1	White LED illuminator	3	Display
2	Dual cameras	4	Mic

2 Connection and Installation

2.1 Cable Connection



- Check whether the access control security module is enabled in **Function > Security Module**. If enabled, you need to purchase access control security module separately. The security module needs separate power supply.
- Once the security module is enabled, the exit button, turnstile control, and firefighting linkage will be invalid.

Cable Connection of Model G

Figure 2-1 Cable connection of model G

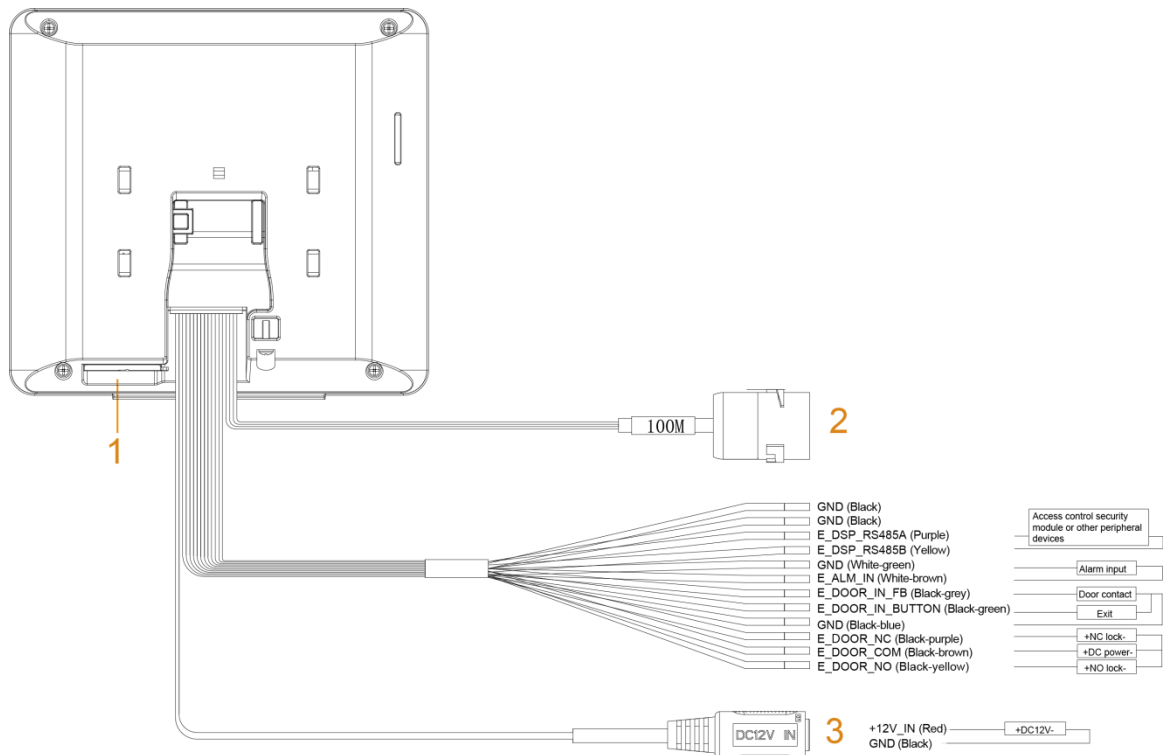


Figure 2-2 Ports of model G

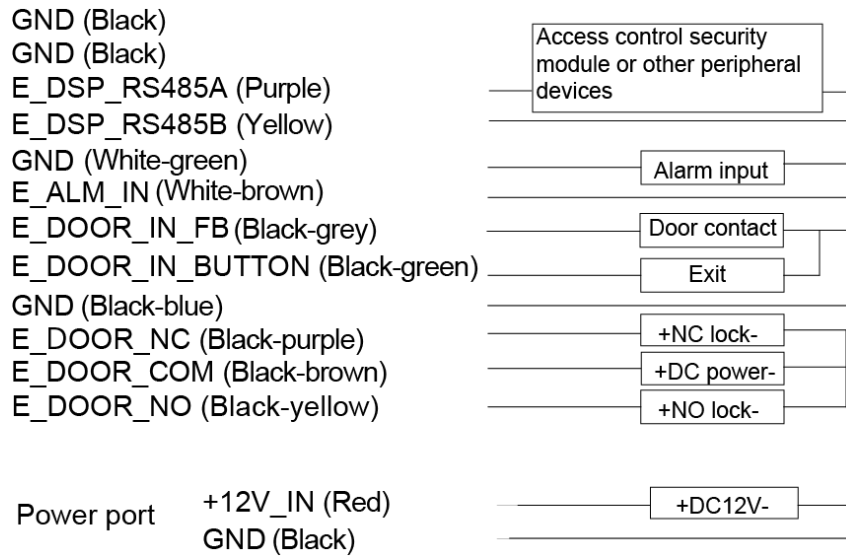


Table 2-1 Component description

No.	Name
1	USB port
2	100M network port
3	Power port

Cable Connection of Model J

Figure 2-3 Cable connection of model J

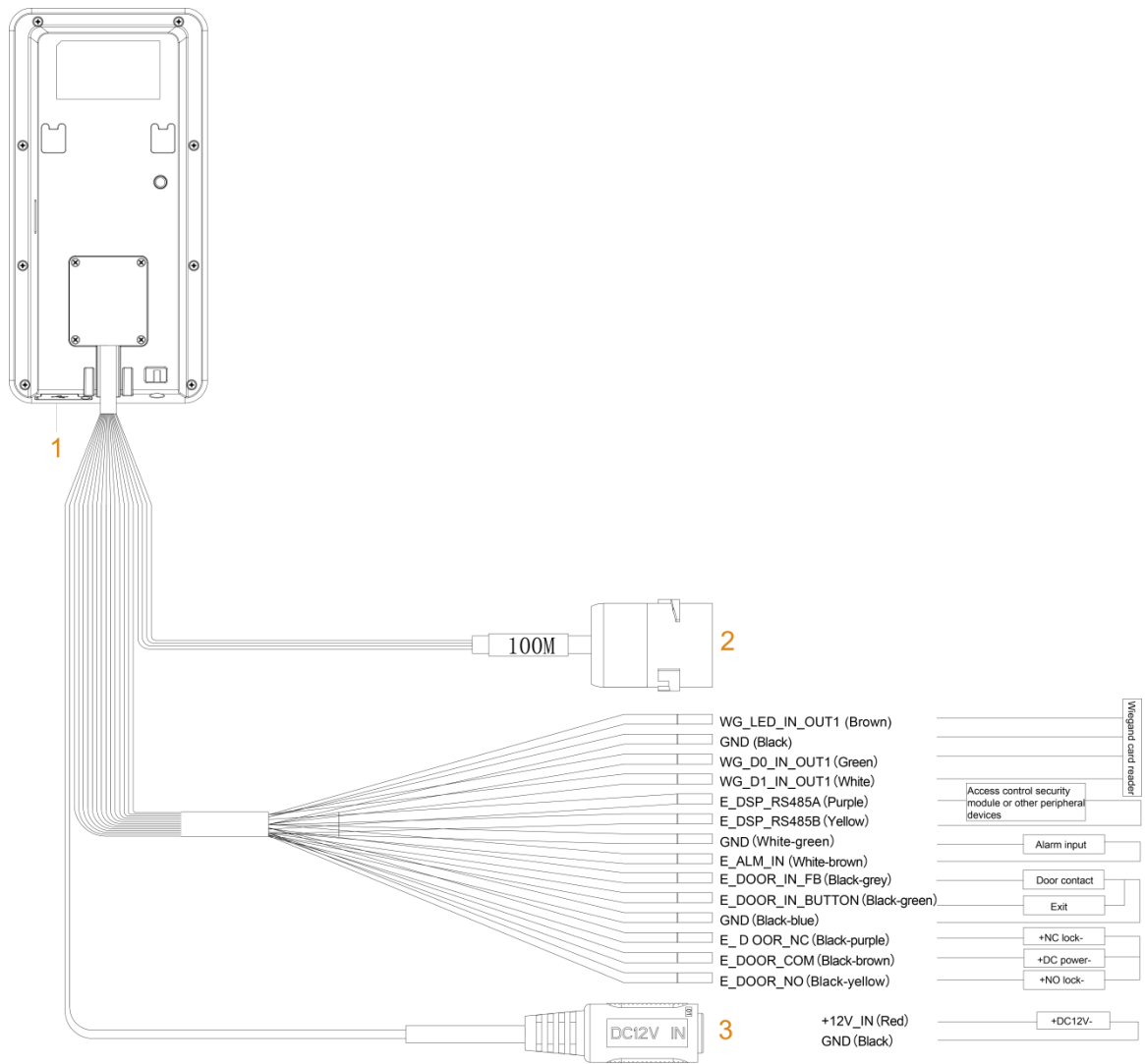


Figure 2-4 Ports of model J

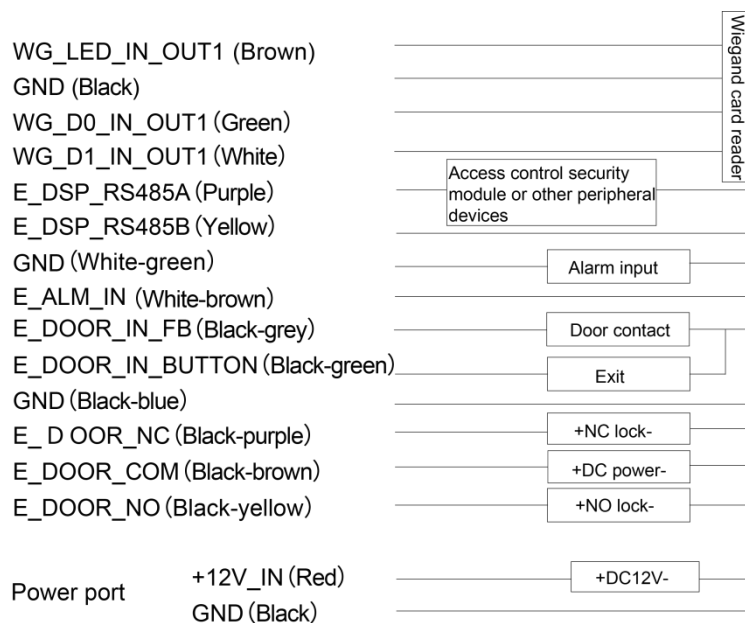


Table 2-2 Component description

No.	Name
1	USB port
2	100M network port
3	Power port

2.2 Installation Notes



- If there is light source 0.5 meters away from the access controller, the minimum illumination should be no less than 100 Lux.
- It is recommended that the access controller is installed indoors, at least 3 meters away from windows and doors and 2 meters away from lights.
- Avoid backlight and direct sunlight.

Ambient Illumination Requirement

Figure 2-5 Ambient illumination requirement



Candle: 10Lux



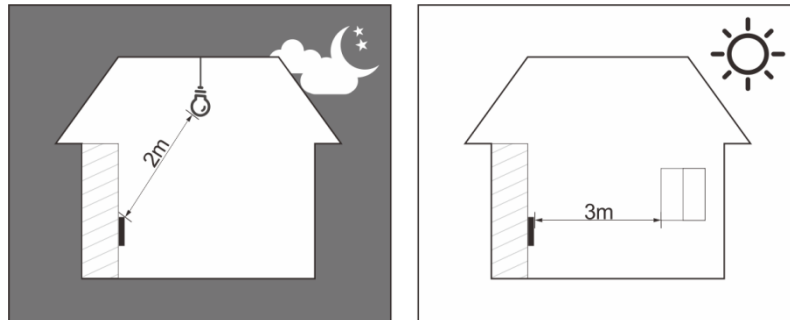
Light bulb: 100Lux–850Lux



Sunlight: ≥ 1200 Lux

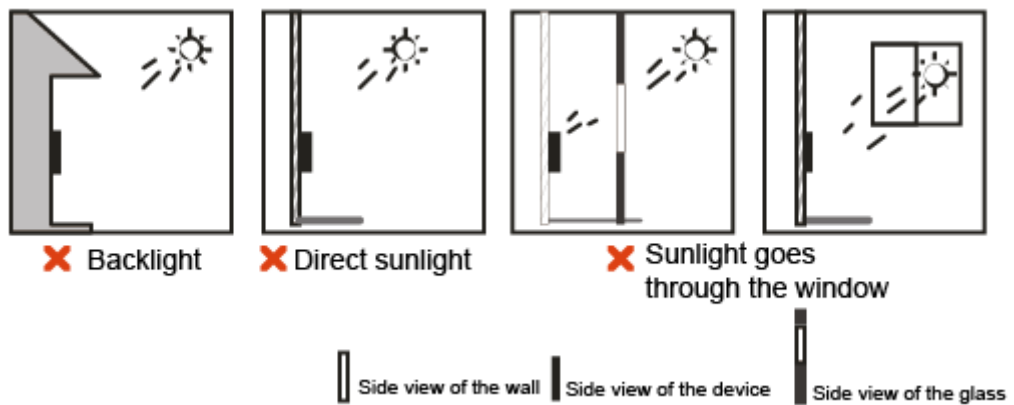
Places Recommended

Figure 2-6 Places recommended



Places Not Recommended

Figure 2-7 Places not recommended



2.3 Installation

2.3.1 Installation of Model G

Desktop Installation

Insert the buckle of the desktop bracket into the rear slot of the access controller, and then slide it down to the end.

Figure 2-8 Desktop installation (1)

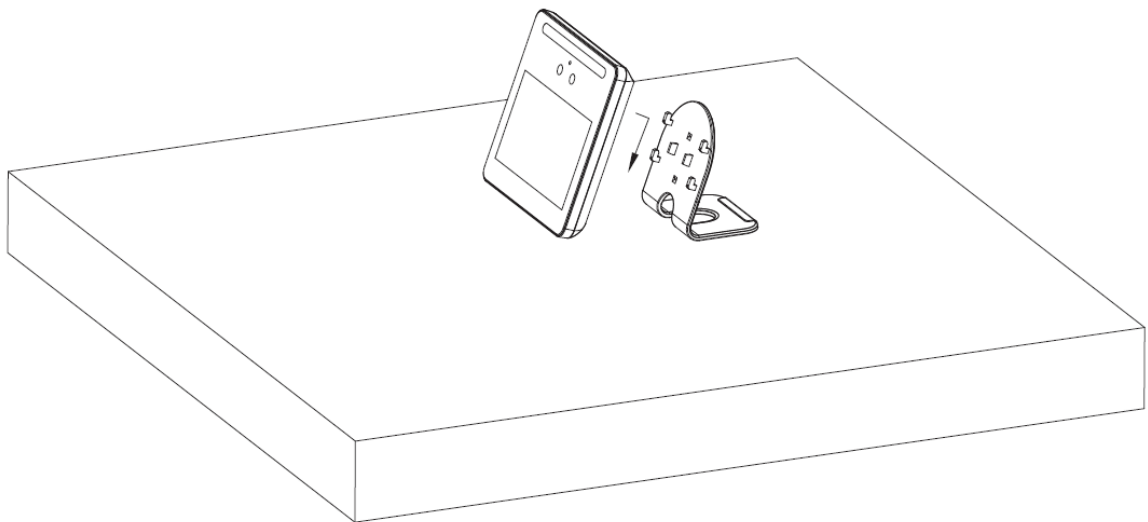
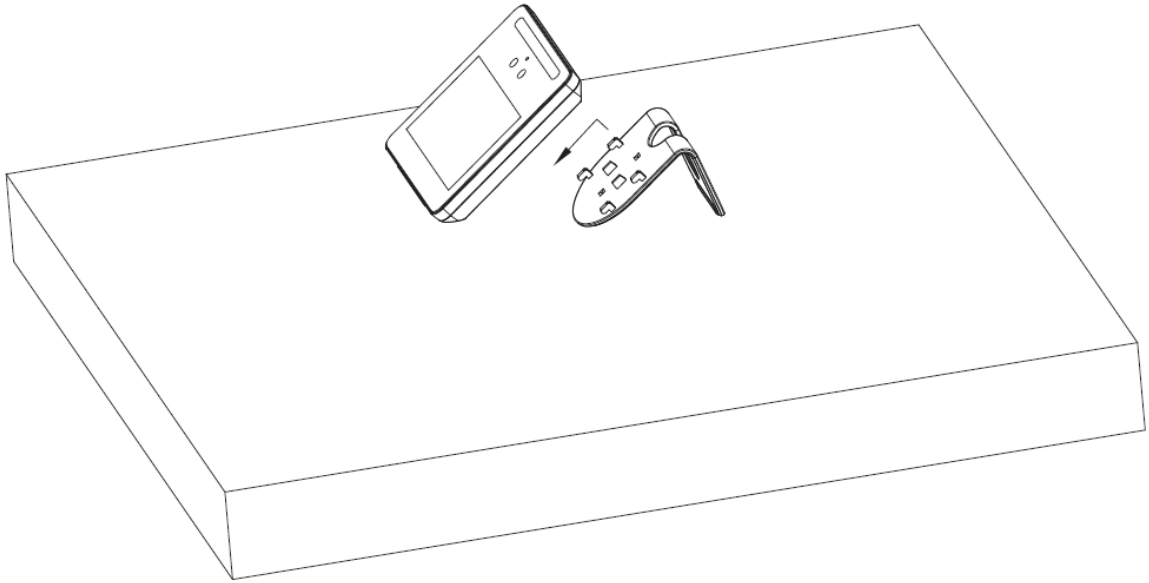


Figure 2-9 Desktop installation (2)



Wall Installation

The recommended distance between the lens and ground is 1.4–1.6 meters.

Figure 2-1 Installation height

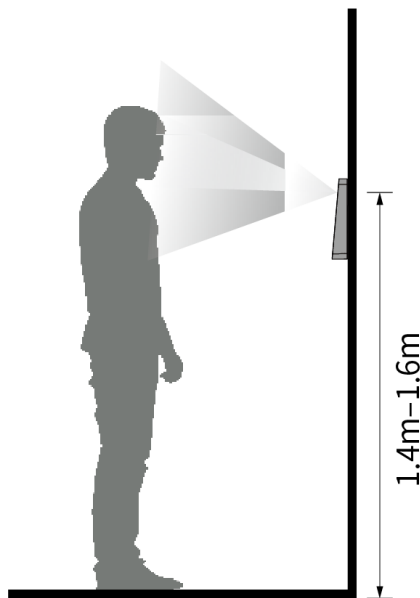
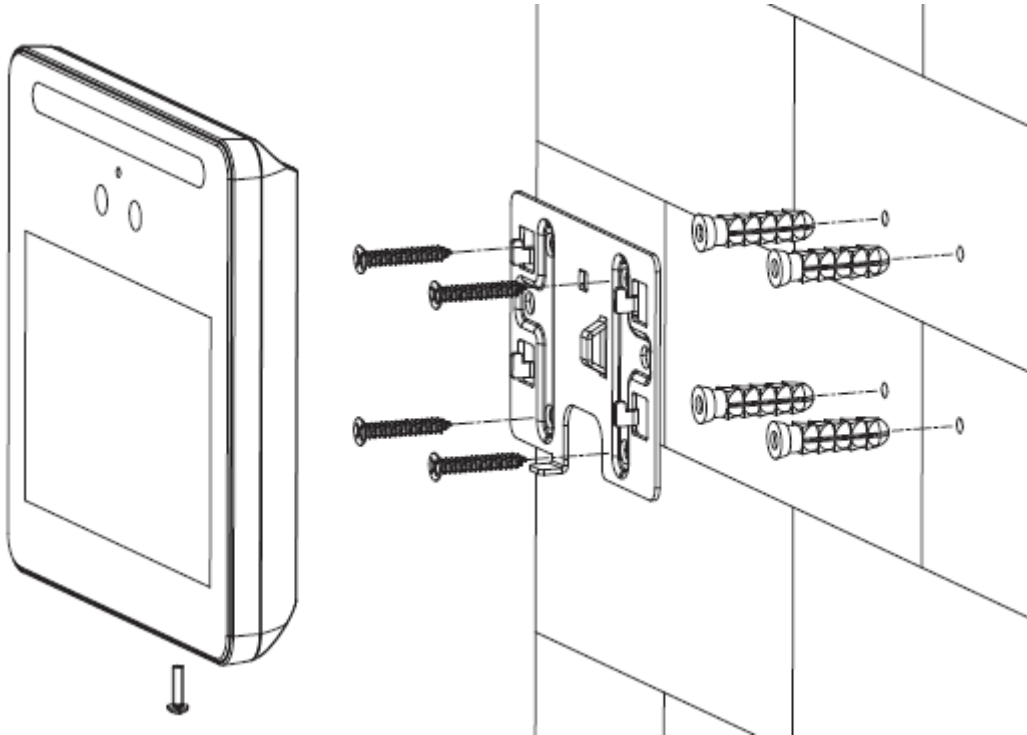


Figure 2-2 Wall installation



- Step 1 Drill four holes in the wall according to holes in the bracket.
- Step 2 Fix the bracket on the wall by installing the expansion screws into the four bracket installation holes.
- Step 3 Connect cables for access controller. See "2.1 Cable Connection".
- Step 4 Hang the access controller on the bracket hook.
- Step 5 Tighten the screws at the bottom of the access controller.

2.3.2 Installation of Model J

The recommended distance between the lens and ground is 1.4 meters.

Figure 2-3 Installation height

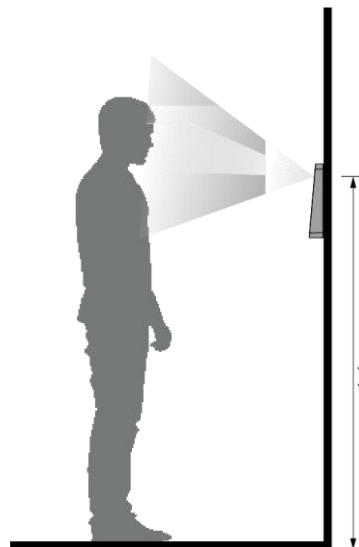


Figure 2-4 Wall installation

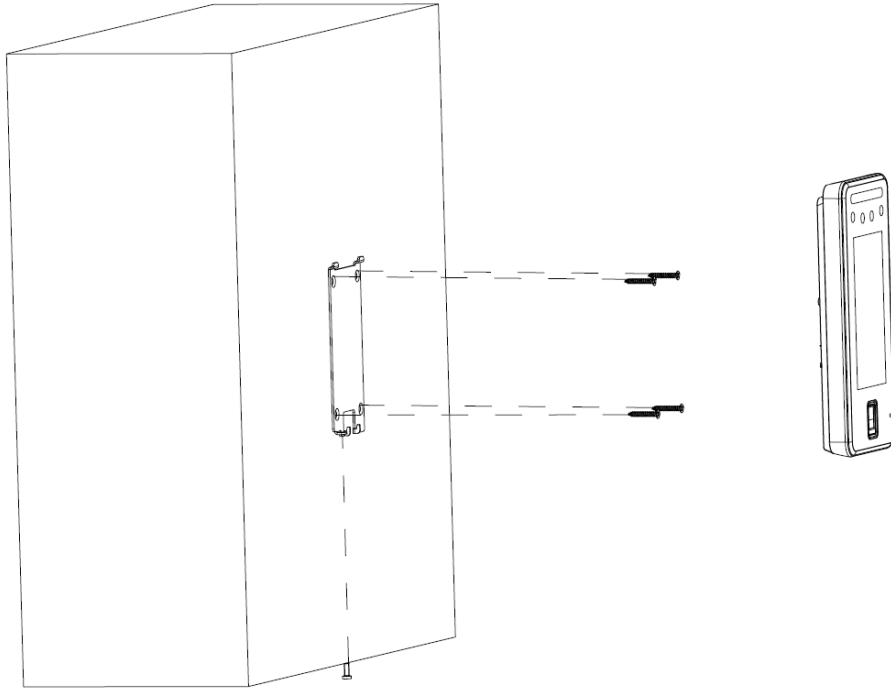
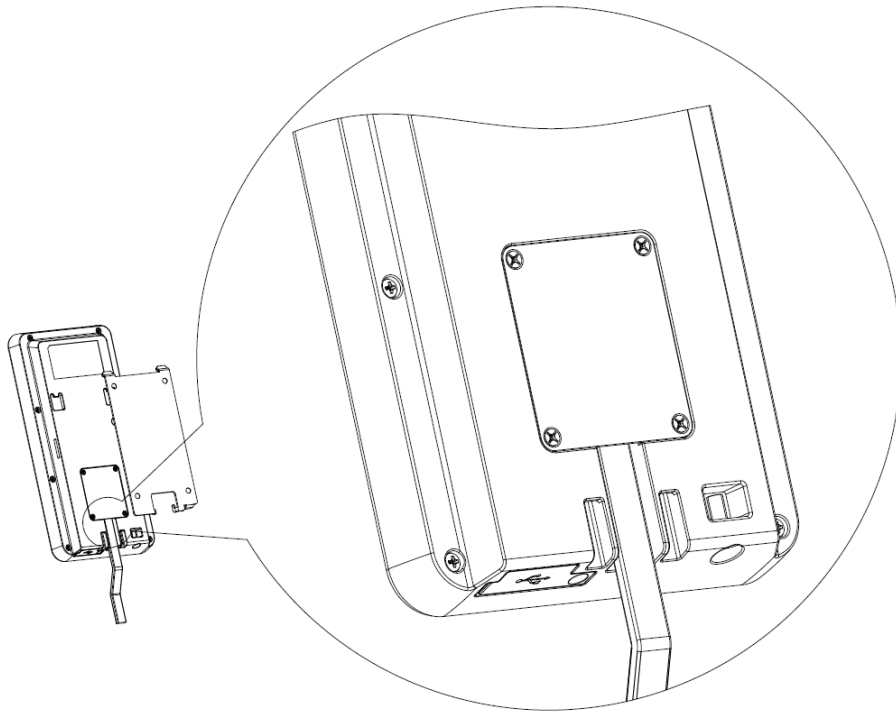


Figure 2-5 Applying silicon sealant to the access controller



Installation Procedure

- Step 1 Drill four holes in the wall according to holes in the bracket.
- Step 2 Fix the bracket on the wall by installing the expansion screws into the four bracket installation holes.
- Step 3 Connect cables for access controller. See "2.1 Cable Connection".
- Step 4 Apply silicon sealant to gaps of the cable entry for waterproof. See Figure 2-5.
- Step 5 Hang the access controller on the bracket hook.
- Step 6 Tighten the screws at the bottom of the access controller.

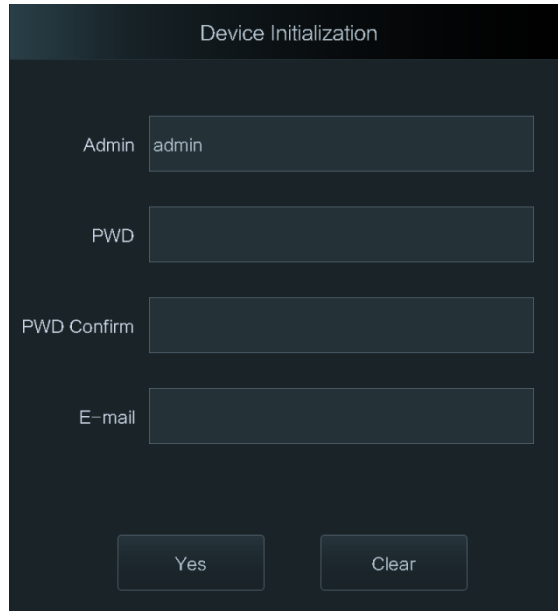
Step 7 Apply silicon sealant to gaps between the wall and the access controller.

3 System Operations

3.1 Initialization

Administrator password and an email should be set the first time the access controller is turned on; otherwise the access controller cannot be used.

Figure 3-1 Initialization



The screenshot shows a 'Device Initialization' screen with the following fields and buttons:

- Admin: admin
- PWD: [Empty]
- PWD Confirm: [Empty]
- E-mail: [Empty]
- Buttons: Yes, Clear



- The administrator password can be reset through the email address that you entered if the administrator forgets the administrator password.
- 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 ' ; : &).
- For access controllers without touch screen, initialization can be completed through the web interface. See the user manual for details.

3.2 Adding New Users

You can add new users by entering user IDs, names, importing fingerprints, face images, passwords, and selecting user levels.



The following figures are for reference only, and the actual interface shall prevail.

Step 1 On the standby interface, long press 3 s to go to the **Administrator Login** interface.

Step 2 Tap **Admin** to log in to the **Main Menu** interface with an admin account.


Step 3 Select **User > New User**.




Figure 3-2 New user


Parameter	Value
User ID	1
User Level	General
Name	
FP	0
Face	0
Card	0
PWD	
User Level	User
Period	255-Default
Holiday Plan	255-Default
Valid Date	2037-12-31

Step 4 Configure parameters on the interface.

Table 3-1 New user parameter description

Parameter	Description
User ID	Enter user IDs. The IDs consist of 32 characters (including numbers and letters), and each ID is unique.
Name	Enter names with at most 32 characters (including numbers, symbols, and letters).
FP	<p>At most three fingerprints of one user can be recorded, and one fingerprints need to be verified three times.</p> <p>You can enable the Duress FP function under each fingerprint, and only one of the three fingerprints can be the duress fingerprint. Alarms will be triggered if a duress fingerprint is used to unlock the door.</p> <p></p> <ul style="list-style-type: none"> It is not recommended that you select the first fingerprint as the duress fingerprint. Fingerprint unlock is only supported by access controllers with fingerprint sensors.
Face	Make sure that your face is centered on the picture capturing frame, and then a picture of your face will be automatically captured. For details about face image recording, see "Appendix 1 Notes of Face Recording/Comparison."

Card	<p>You can register at most five cards for each user. On the card registration interface, enter your card number or swipe your card, and then the card information will be read by the access controller.</p> <p>You can enable the Duress Card function on the card registration interface. Alarms will be triggered if a duress card is used to unlock the door.</p>  <p>If the access controller is without card reading module, you need to connect the device to peripheral card readers.</p>
PWD	<p>The door unlocking password. The maximum length of the password is 8 digits.</p>  <p>If the access controller is without touch screen, you need to connect the access controller to a peripheral card reader. There are buttons on the card reader.</p>
Level	<p>You can select a user level for new users. There are two options.</p> <ul style="list-style-type: none"> • User: Users only have door unlock permission. • Admin: Administrators can unlock the door and also have parameter configuration permission.  <p>In case that you forget the administrator password, you had better create more than one administrator.</p>
Period	The period in which the user can unlock the door. For detailed period settings, see the user manual.
Holiday Plan	You can set a holiday plan in which the user can unlock the door. For detailed holiday plan settings, see the user manual.
Valid Date	You can set a period during which the unlocking information of the user is valid.
User Level	<p>There are eight levels:</p> <ul style="list-style-type: none"> • General: General users can unlock the door normally. • Blacklist: When users in the blacklist unlock the door, service personnel will get a prompt. • Guest: Guests are allowed to unlock the door certain times or in certain periods. Once they exceed the maximum times or periods, they cannot unlock the door. • Patrol: Patrolling users can get their attendance tracked, but they have no unlock permission. • VIP: When VIP unlocks the door, service personnel will get a prompt. • Special: When special people unlock the door, there will be a delay of 5 seconds before the door is closed. • Custom User 1: Reserved for customization. Users can unlock the door normally. • Custom User 2: Reserved for customization. Users can unlock the door normally.
Use Time	When the user level is Guest, you can set the maximum number of times that the guest can unlock the door.

Step 5 Tap  to save the configuration.

4 Web Operations

The access controller can be configured and operated on the web interface. Through the web interface you can set parameters including network parameters, video parameters, and access controller parameters; and you can also maintain and update the system. For details, see the user manual. Here only describe the login operation.



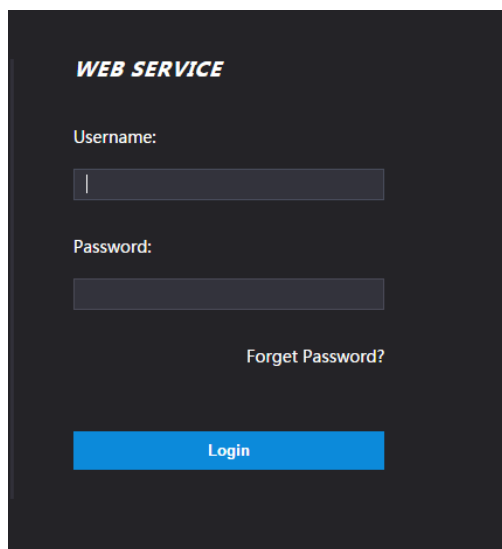
You need to set a password and an email address before logging in to the web interface for the first time. Password you set is used to log in to the web, and the email is used to reset passwords.

Step 1 Open IE web browser, enter the IP address of the access controller in the address bar, and then press Enter key.



- Make sure that the IP address of computer used to log in to the web is in the same LAN with the access controller.
- The default IP address of the access controller is 192.168.1.108.

Figure 4-1 Login



Step 2 Enter the username and password.



- The default username of administrator is admin, and the password is the login password after initializing the access controller. Modify the administrator password regularly and keep it properly for security.
- If you forget the administrator login password, you can click **Forget Password?** to reset it. See the user manual.

Step 3 Click **Login**.

The homepage of the web interface is displayed.

Appendix 1 Notes of Face Recording/Comparison

Before Registration

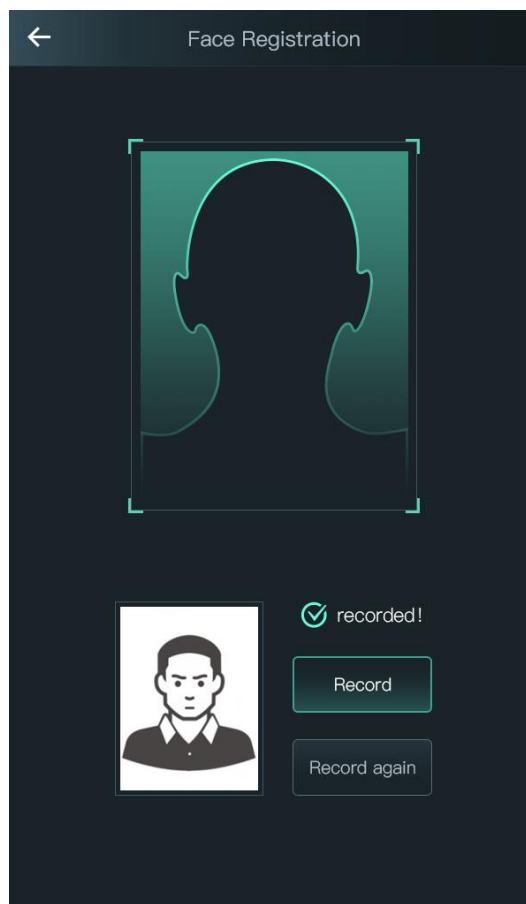
- Glasses, hats, and beards might influence face recognition performance.
- Do not cover your eyebrows when wearing hats.
- Do not change your beard style greatly if you will use the device; otherwise face recognition might fail.
- Keep your face clean.
- Keep the device at least two meters away from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

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. A picture of your face will be captured automatically.

Appendix Figure 1-1 Registration



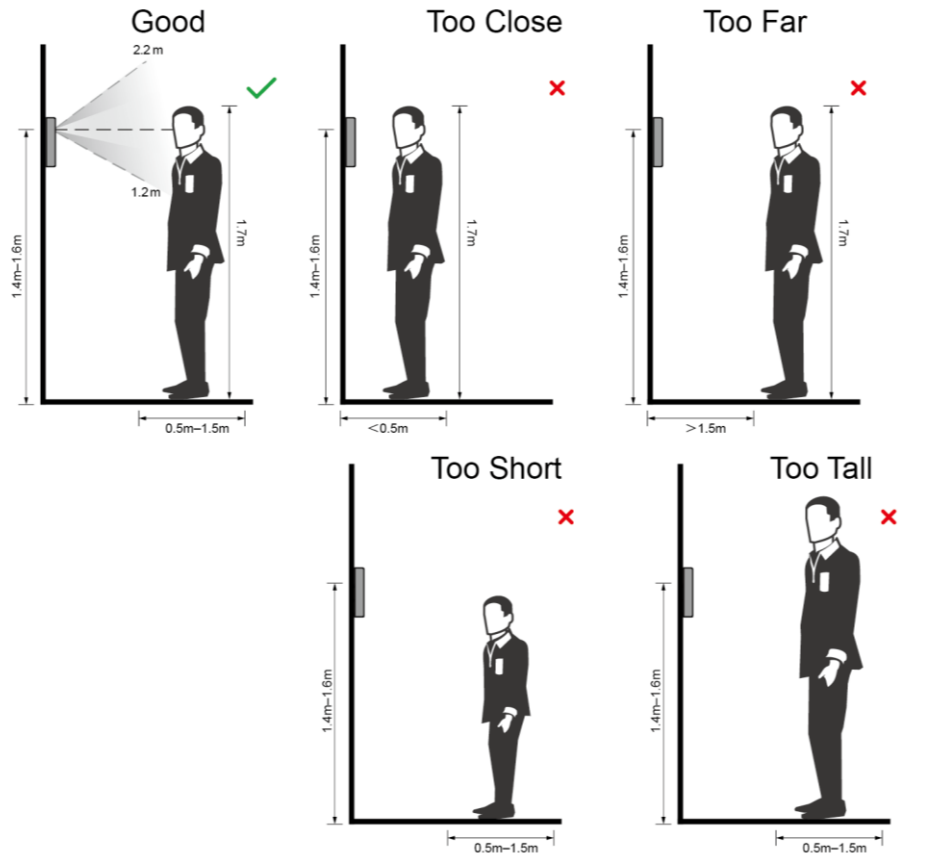


- Do not shake your head or body, otherwise the registration might fail.
- Avoid two faces appear in the capture frame at the same time.

Face Position

If your face is not at the appropriate position, face recognition effect might be influenced.

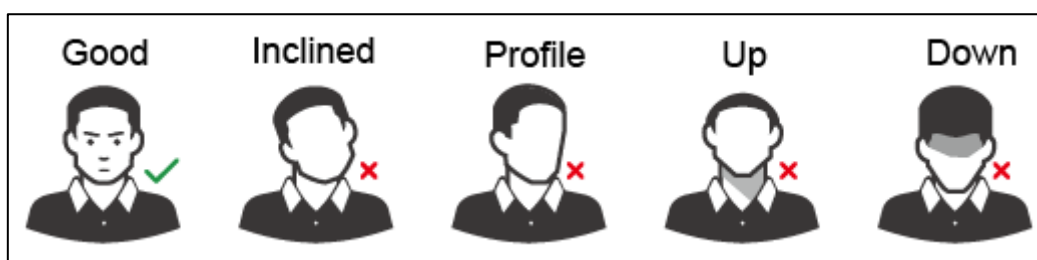
Appendix Figure 1-2 Appropriate face position



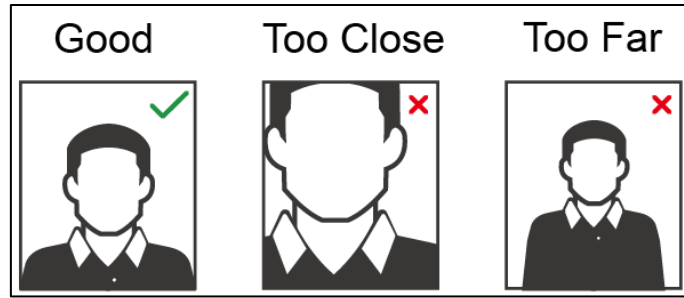
Requirements of Faces

- 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 1-3 Head position



Appendix Figure 1-4 Face distance



- When importing face images through the management platform, make sure that image resolution is within the range 150 × 300–600 × 1200; image pixels are more than 500 × 500; image size is less than 75 KB, and image name and person ID are the same.
- Make sure that face does not take 2/3 of the whole image area, and the aspect ratio does not exceed 1:2.

Appendix 2 Fingerprint Record Instruction

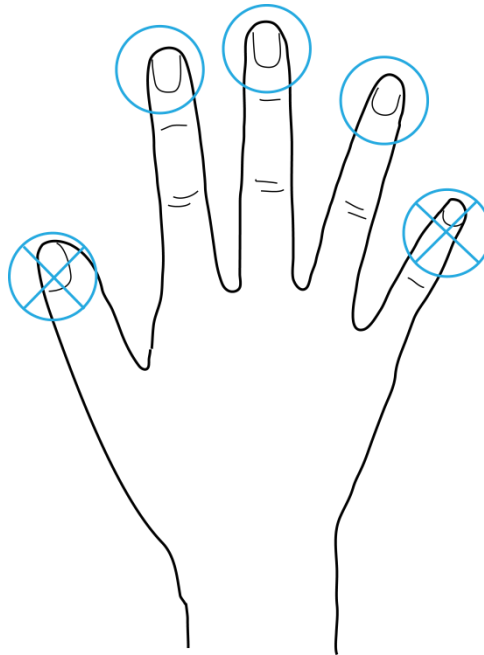
Notice

- 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.
- If your 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.

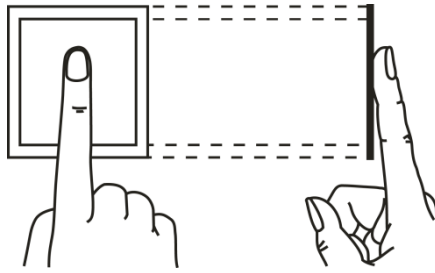
Appendix figure 1-1 Recommended fingers



Finger Pressing Method

- Correct method

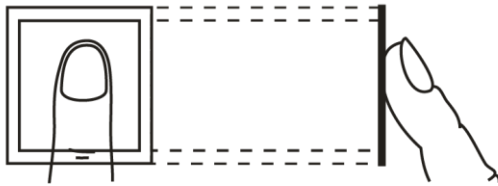
Appendix figure 1-2 Correct finger pressing



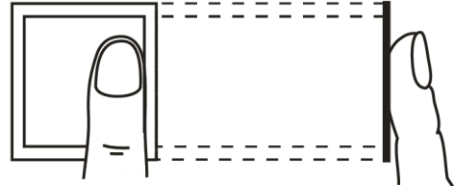
- Incorrect method

Appendix figure 1-3 Wrong finger pressing

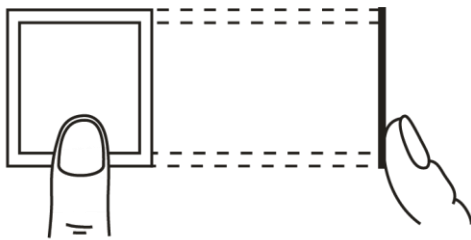
Fingertip perpendicular to the record area



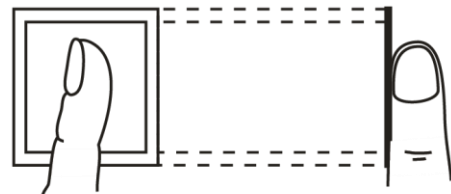
Fingertip not at the center of the record area



Fingertip not at the center of the record area



Fingertip inclination



Appendix 3 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations on how to create a more secured security system.

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 equipment 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. Enable Whitelist

We suggest you to enable whitelist function to prevent everyone, except those with specified IP addresses, from accessing the system. Therefore, please be sure to add your computer's IP address and the accompanying equipment's IP address to the whitelist.

8. 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.

9. Assign Accounts and Privileges Reasonably

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

10. 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.

11. 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.

12. 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.

13. 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.

14. 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.
- It is recommended that you enable your device's firewall or blacklist and whitelist feature to reduce the risk that your device might be attacked.