

Face Recognition Access Controller

Quick Start Guide

V1.0.0

General

This manual introduces the installation and basic operation 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
 NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

Version	Revision Content	Release Date
V1.0.0	First release	November 2019

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 it well for future reference.

Operation Requirement

- 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 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.
- Transport, use and store the access controller under the allowed humidity and temperature conditions.

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	II
1 Dimensions and Components	1
2 Installation	6
2.1 Installation Notes.....	6
2.2 Cable Connections.....	7
2.3 Installation	8
3 System Operation	12
3.1 Initialization	12
3.2 Adding New Users	12
4 Web Operation	15
Appendix 1 Notes of Face Recording/Comparison	16
Appendix 2 Cybersecurity Recommendations	21

1 Dimensions and Components

The access controller has two types: 7-inch and 10-inch access controllers. See Figure 1-1 to Figure 1-6.

The 7-inch access controller has two models: model A and model B. See Figure 1-1 to Figure 1-4.

7-Inch Access Controller

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

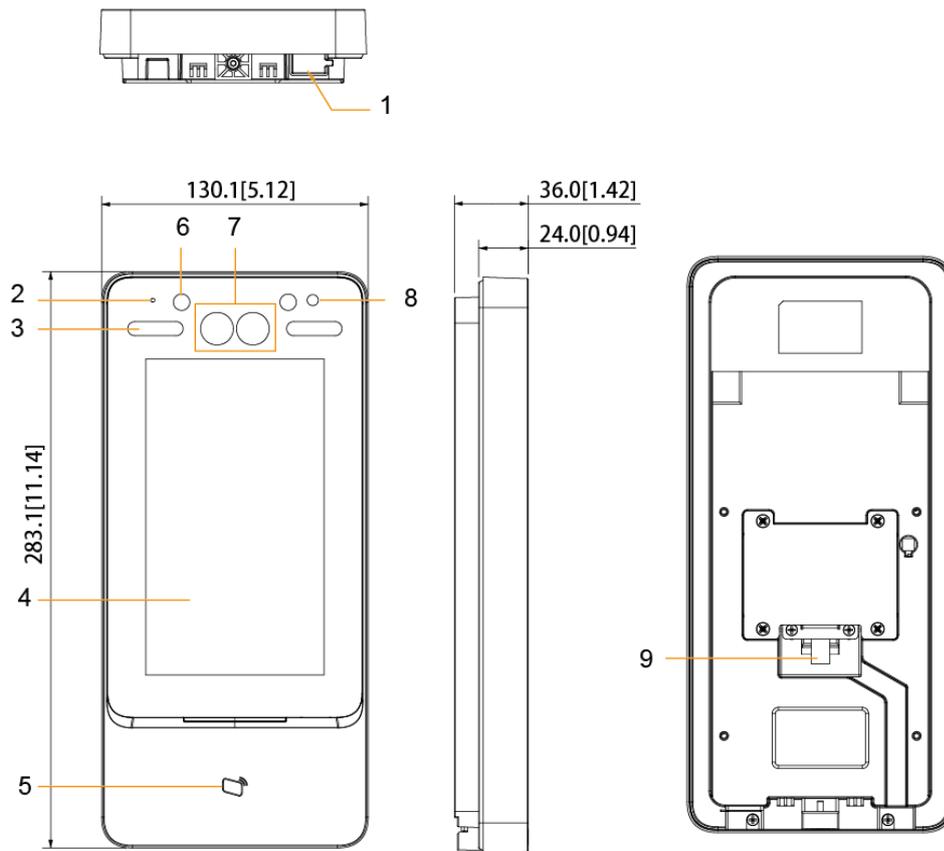


Table 1-1 Component description (1)

No.	Name	No.	Name
1	USB port	6	IR light
2	MIC	7	Dual camera
3	White fill light	8	Phototransistor
4	Display	9	Cable entry
5	Card swiping area	—	—

Figure 1-2 Dimensions and components of model A (2) (mm [inch])

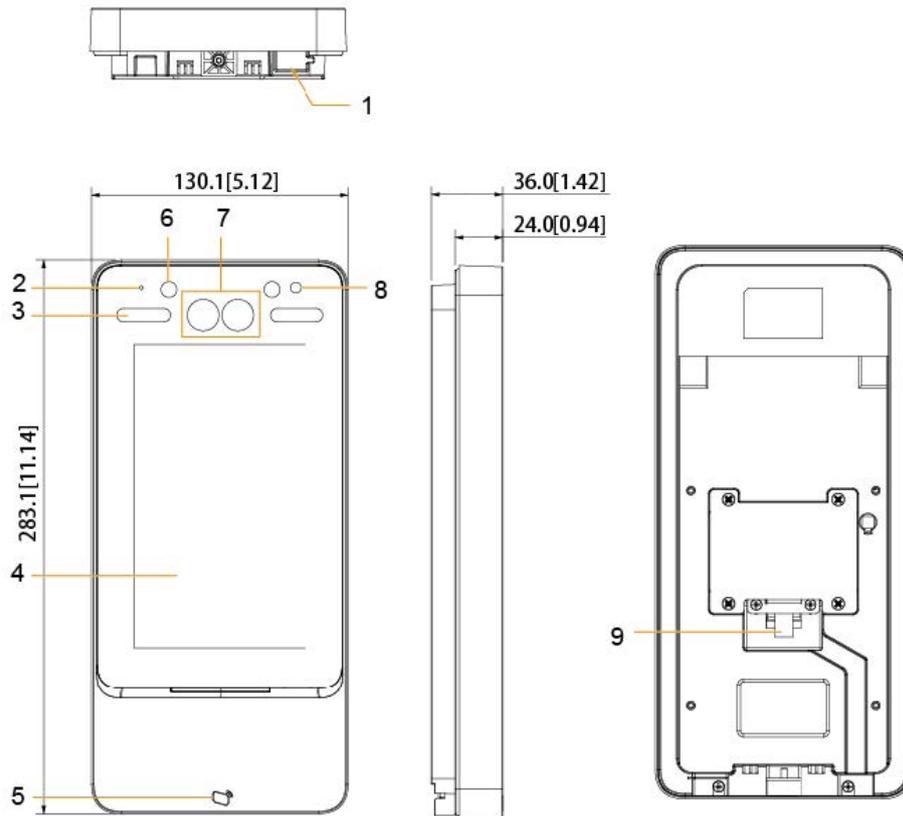


Table 1-2 Component description (2)

No.	Name	No.	Name
1	USB port	6	IR light
2	MIC	7	Dual camera
3	White fill light	8	Phototransistor
4	Display	9	Cable entry
5	Card swiping area	—	—

Figure 1-3 Dimensions and components of model B (1) (mm [inch])

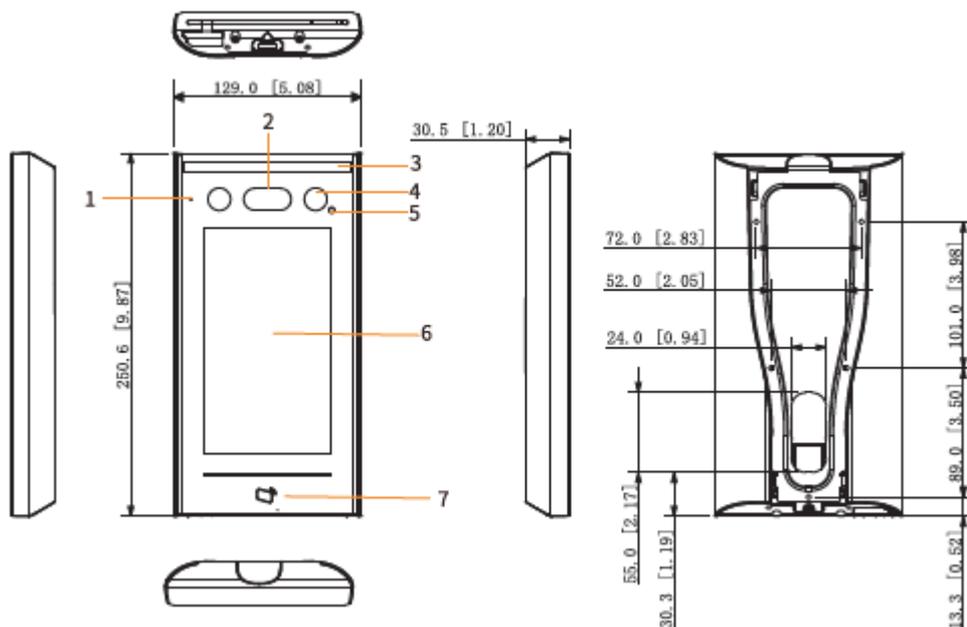


Table 1-3 Component description (3)

No.	Name	No.	Name
1	MIC	5	Phototransistor
2	Dual camera	6	Display
3	White fill light	7	Card swiping area
4	IR light	—	—

Figure 1-4 Dimensions and components of model B (2)(mm [inch])

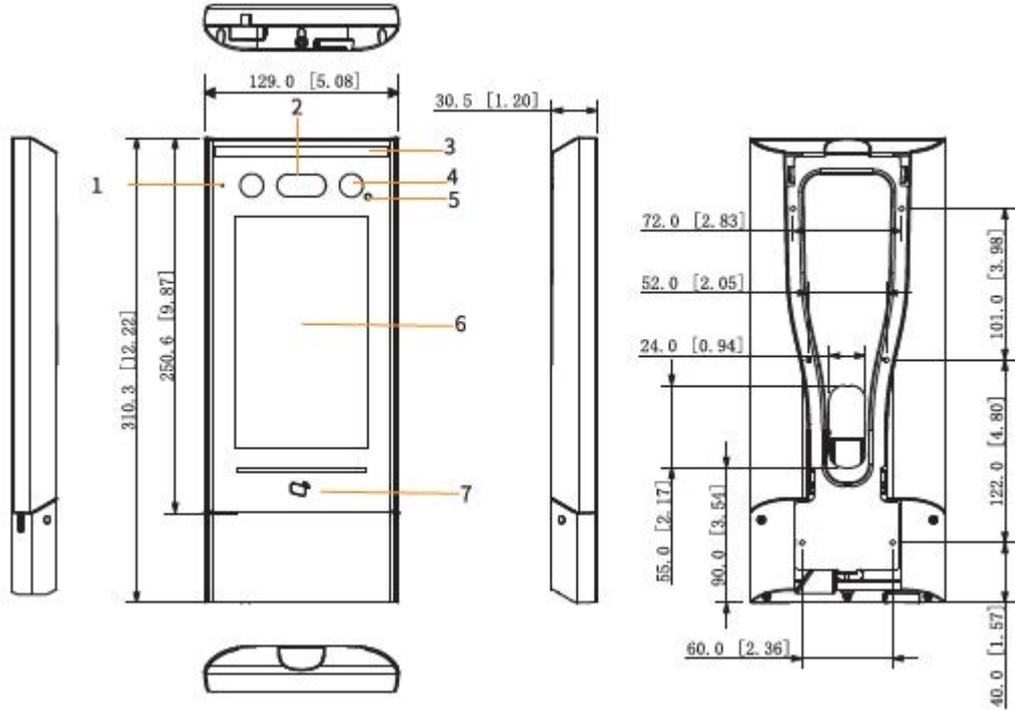


Table 1-4 Component description (4)

No.	Name	No.	Name
1	MIC	5	Phototransistor
2	Dual camera	6	Display
3	White fill light	7	Card swiping area
4	IR light		

10-Inch Access Controller

Figure 1-5 Dimensions and components (1) (mm [inch])

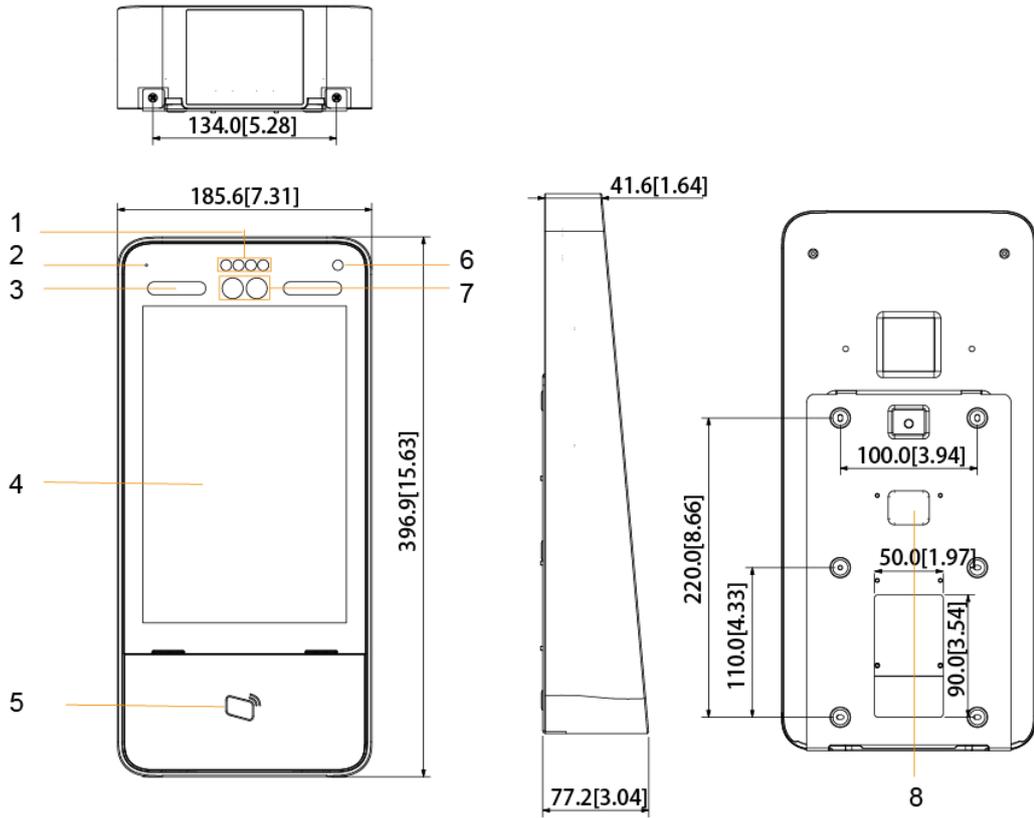


Table 1-5 Component description (1)

No.	Name	No.	Name
1	IR light	6	Phototransistor
2	MIC	7	Dual camera
3	White fill light	8	Cable entry
4	Display	–	–
5	Card swiping area	–	–

Figure 1-6 Dimensions and components (2) (mm [inch])

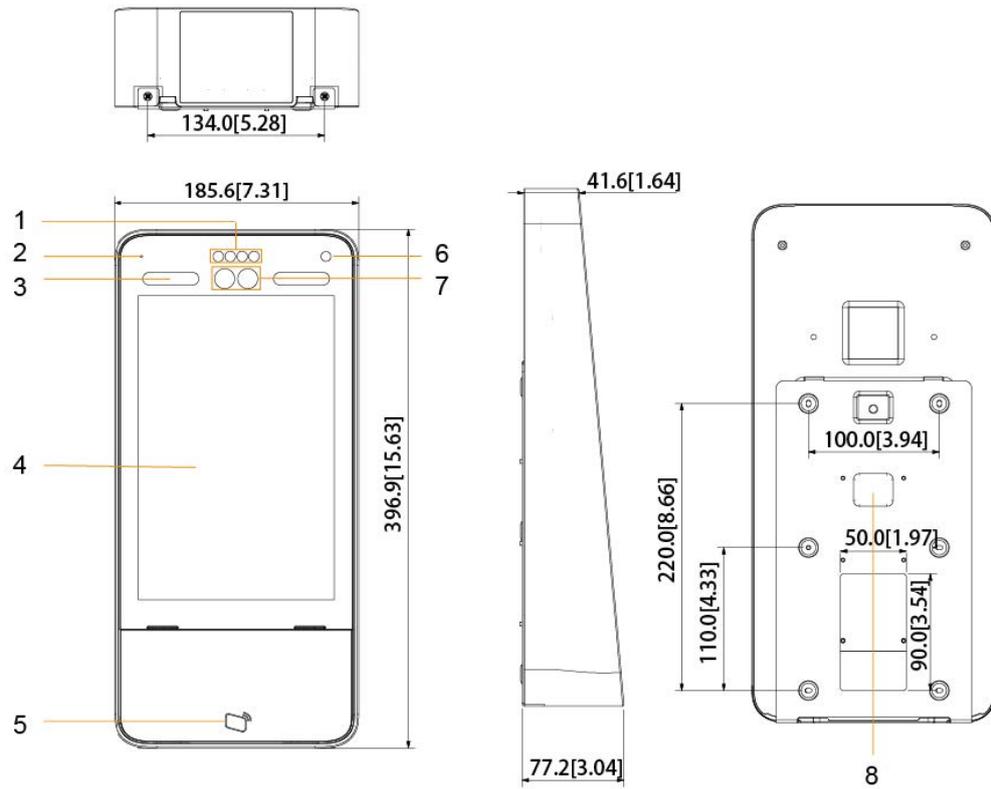


Table 1-6 Component description (2)

No.	Name	No.	Name
1	IR light	6	Phototransistor
2	MIC	7	Dual camera
3	White fill light	8	Cable entry
4	Display	—	—
5	Card swiping area	—	—

2 Installation

2.1 Installation Notes



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

Ambient Illumination Requirement

Figure 2-1 Ambient illumination requirement



Candle: 10Lux



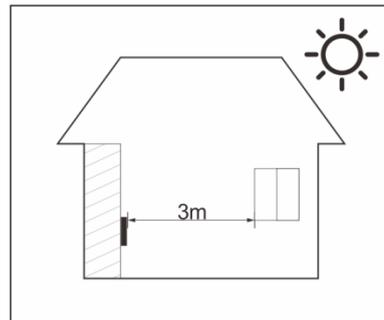
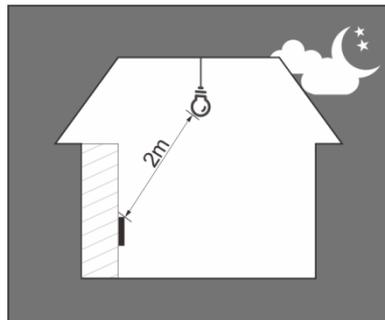
Light bulb: 100Lux–850Lux



Sunlight: ≥ 1200 Lux

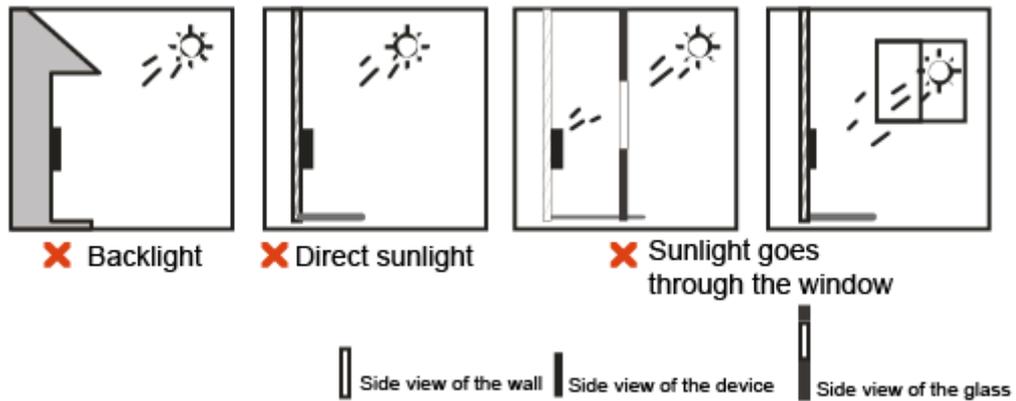
Places Recommended

Figure 2-2 Places recommended



Places Not Recommended

Figure 2-3 Places not recommended



2.2 Cable Connections



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

Figure 2-4 Cable connection

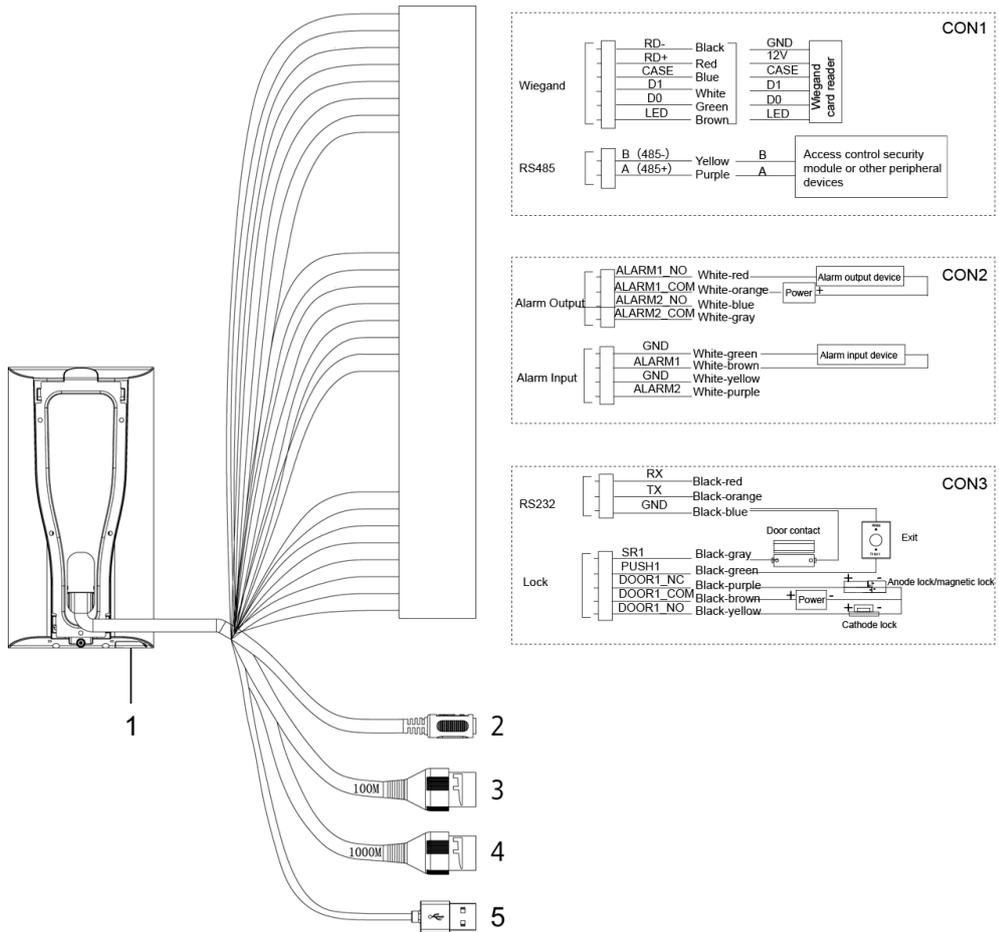


Table 2-1 Component description

No.	Name
1	USB port
2	Power port
3	Ethernet port
4	Ethernet port (only supported by 7-inch model B access controllers)
5	USB port (only supported by 7-inch model B access controllers)

2.3 Installation

Installation method of model A and model B are the same. Make sure that the distance between the lens and ground is 1.4 meters. See Figure 2-5.

Figure 2-5 Installation height

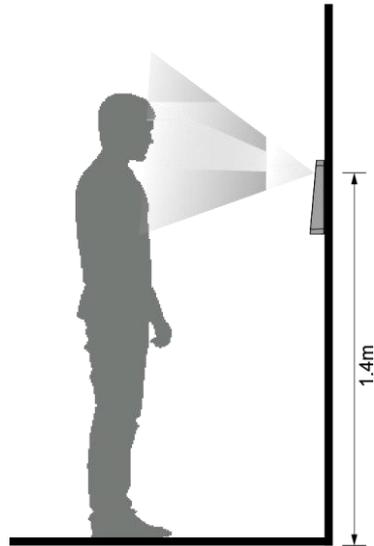


Figure 2-6 Installation diagram (1)

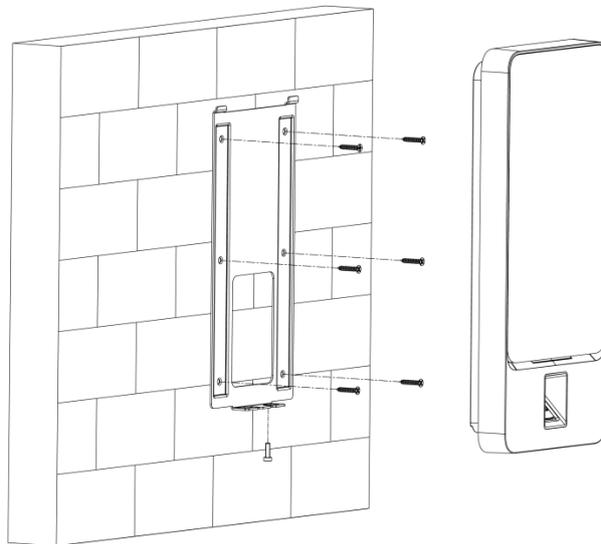
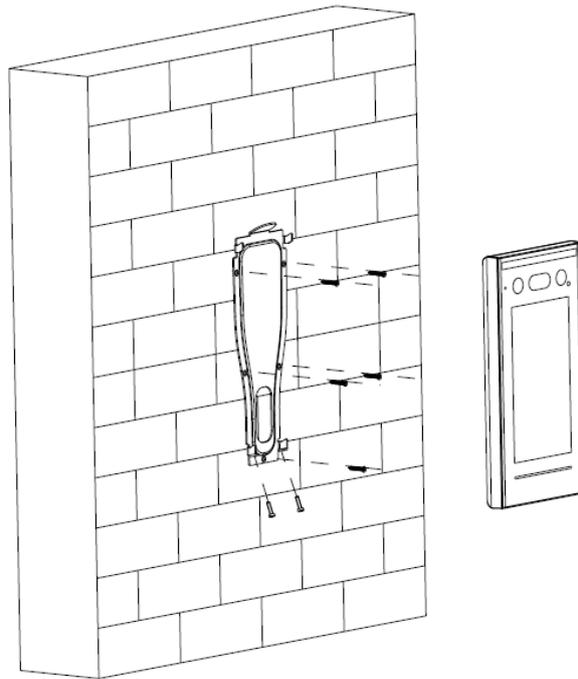


Figure 2-7 Installation diagram (2)



Installation Procedure

This document uses a 7-inch model A access controller as an example.

Step 1 Drill seven holes (six bracket installation holes and one cable entry) in the wall according to holes in the bracket.

Step 2 Fix the bracket on the wall by installing the expansion screws into the six bracket installation holes.

Step 3 Connect cables for access controller.
See "2.2 Cable Connections."

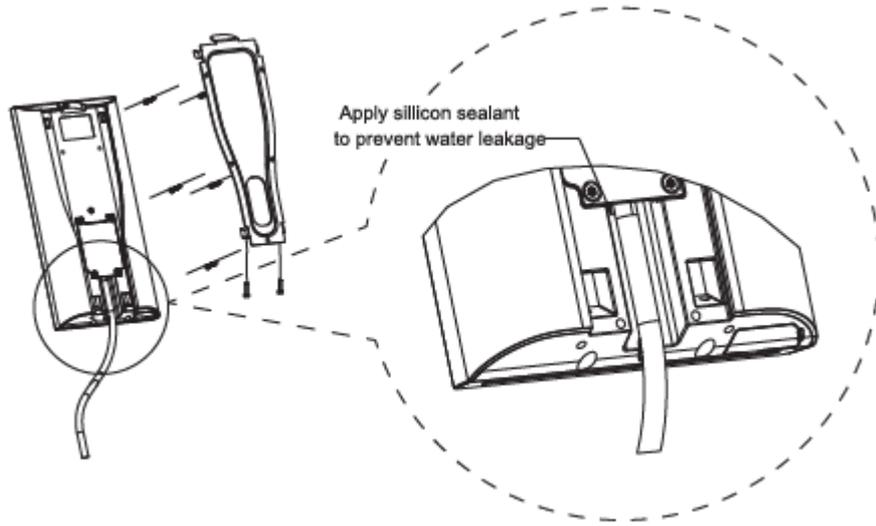
Step 4 Hang the access controller on the bracket hook.

Step 5 Tighten the screws at the bottom of the access controller.
The installation is completed.



You need to apply silicon sealant to the cable outlet of 7-inch model B access controller. See Figure 2-8.

Figure 2-8 Applying silicon sealant

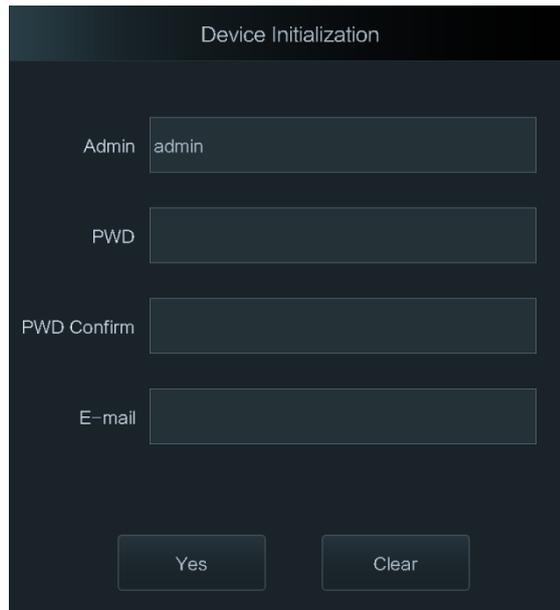


3 System Operation

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. See Figure 3-1.

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 you entered if the password is forgotten.
- The password should 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 controller without touch screen, initialize through the web. See the user manual for details.

3.2 Adding New Users

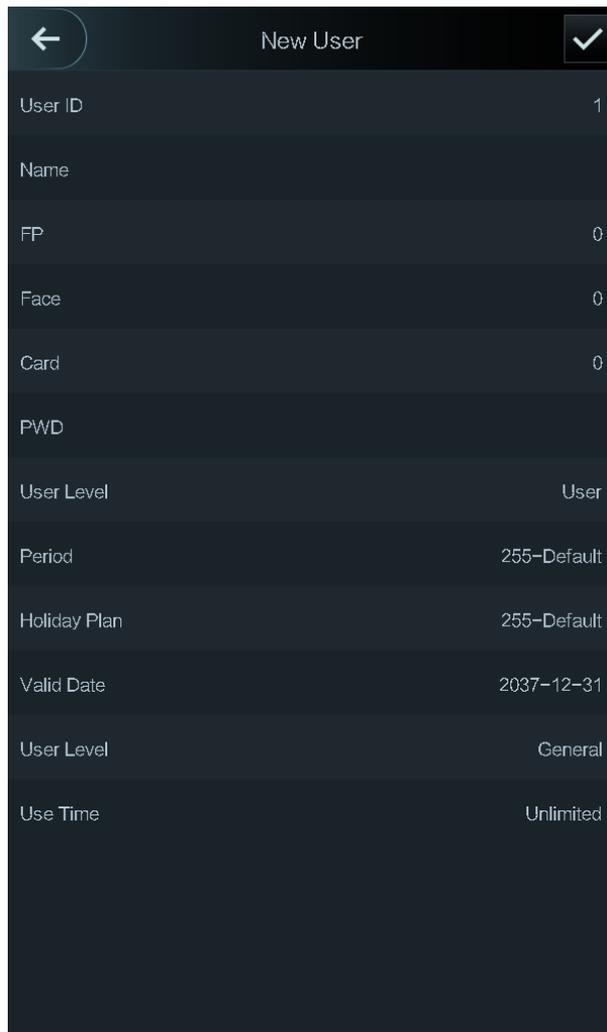
You can add new users by entering their user IDs, names, face images, passwords, and selecting their user levels.

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

Step 1 Select **User > New User**.

The **New User** interface is displayed. See Figure 3-2.

Figure 3-2 New user



Step 2 Configure parameters on the interface. See Table 3-1.

Table 3-1 New user parameter description

Parameter	Description
User ID	You can enter user IDs. The IDs consist of 32 characters (including numbers and letters), and each ID is unique.
Name	You can 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 fingerprint needs 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 to set the thumb fingerprint as the duress fingerprint. Fingerprint unlock is available only on select models.
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."

Parameter	Description
Card	<p>You can register 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>
Password	<p>The door unlocking password. The maximum length of the password is 8 characters.</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 authority. • Admin: Administrators can not only unlock the door but also have parameter configuration authority.  <p>In case that you forget the administrator password, you had better create more than one administrator.</p>
Period	You can set a 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 configuration manual.
Valid Date	You can set a period during which the unlocking information of the user is valid.
User Level	<p>There are six 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 in certain periods. Once they exceed the maximum times and periods, they cannot unlock the door again. • Patrol: Patrolling users can get their attendance tracked, but they have no unlock authority. • 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.
Use Time	When the user level is Guest , you can set the maximum times that the guest can unlock the door.

Step 3 After you have configured all the parameters, tap  to save the configuration.

A new user is created.



For access controllers without touch screen, you need to create users through management platforms. See details in the user manual.

4 Web Operation

The access controller can be configured and operated on the web. Through the web you can set parameters including network parameters, video parameters, and access controller parameters; and you can also maintain and update the system.

Login



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

Step 1 Open IE web browser, enter the IP address (192.168.1.108 by default) of the access controller in the address bar, and then press Enter.



- Make sure that the computer used to log in to the web is in the same LAN with the device.
- 7-inch model B access controllers of have dual NICs. The default management address for 1000M Ethernet port is 192.168.1.108, and for 100M Ethernet port is 192.168.2.108.

Figure 4-1 Login

WEB SERVICE

Username:

Password:

[Forget Password?](#)

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 is displayed.

Appendix 1 Notes of Face Recording/Comparison

Before Registration

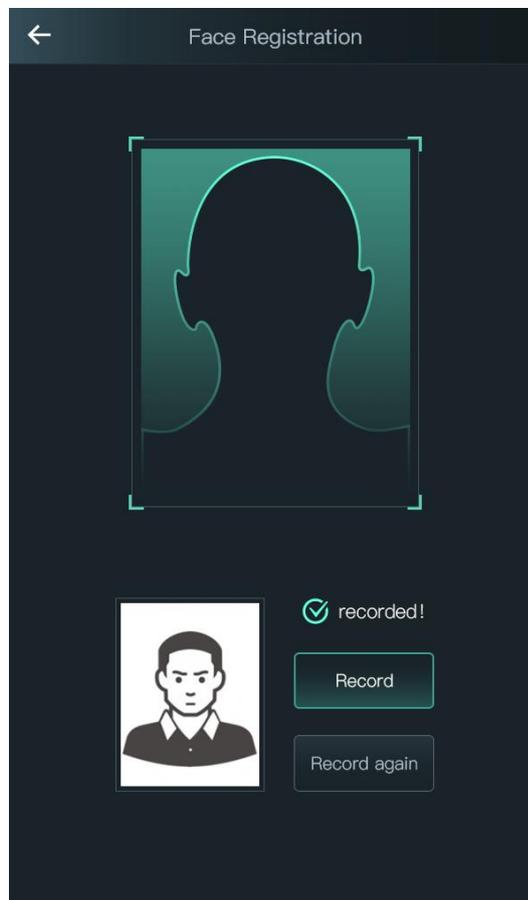
- Glasses, hats, and beards might influence face recognition performance.
- Do not cover your eye brows when wearing hats.
- Do not change your beard style greatly if you will use the device; otherwise face recognition might fail.
- Keep your face clean.
- Keep the device at least two meters away from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



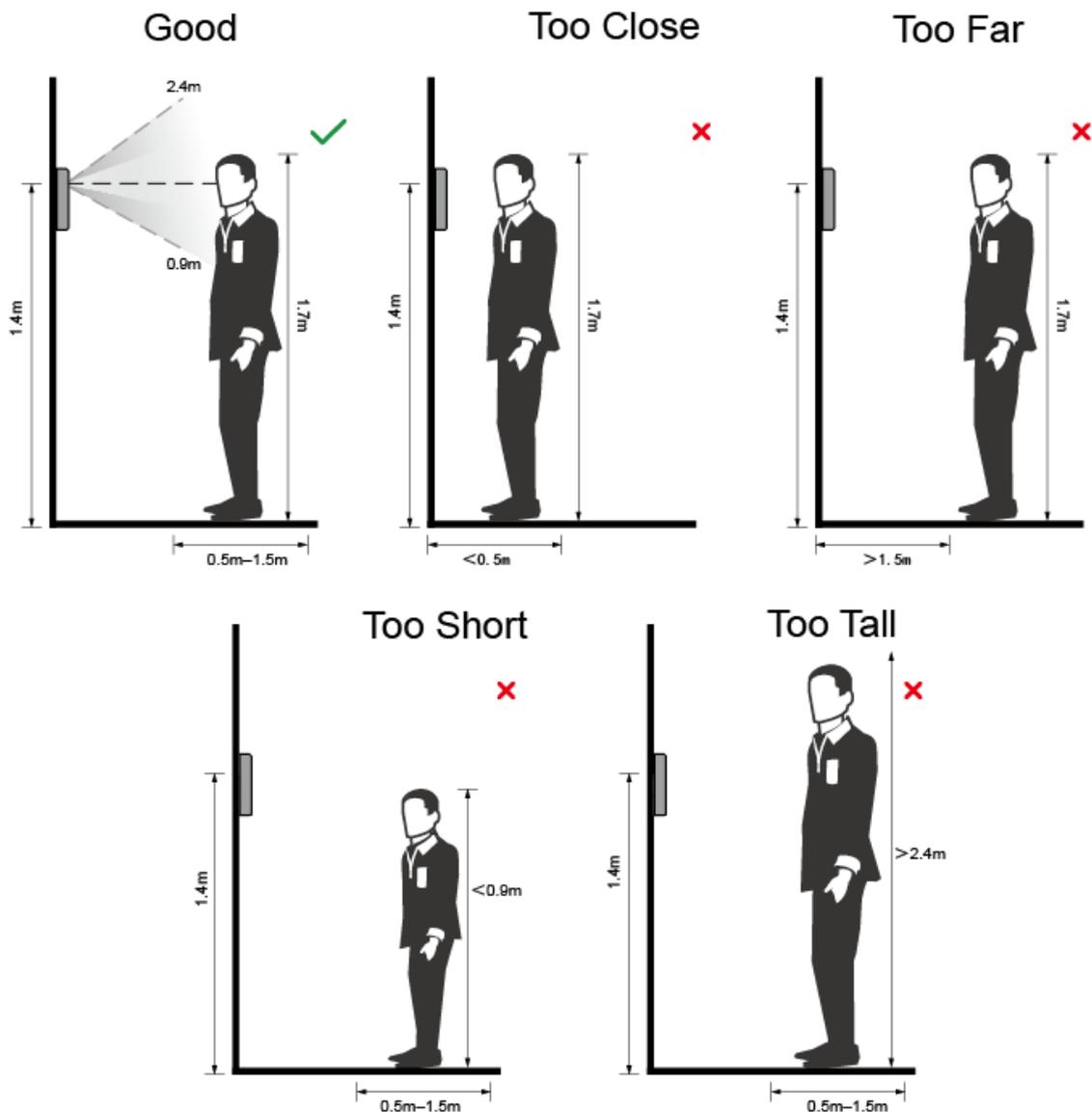


- Do not shake your head or body, or the registration might fail.
- Avoid two faces appear in the box at the same time.

Face Position

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

Appendix figure 1-2 Appropriate face position

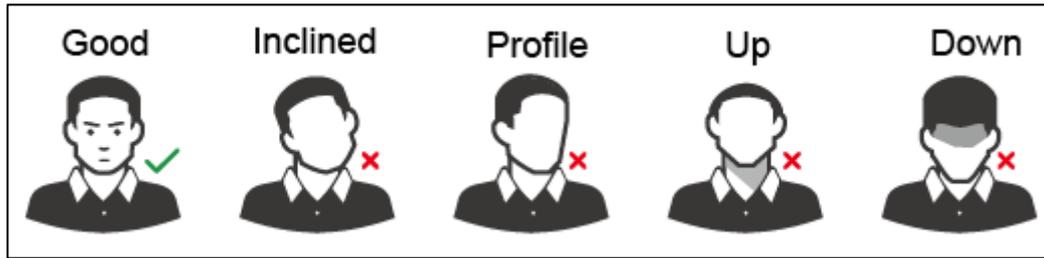


Requirements of Faces

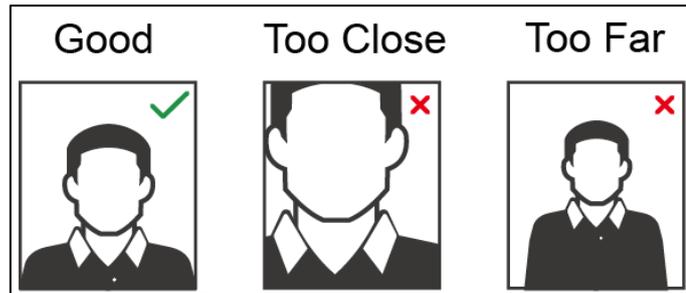
- Make sure that the face is clean and forehead is not covered by hair.
- Do not wear glasses, hats, heavy beards, or other face ornaments that influence face image recording.
- With eyes open, without facial expressions, and make your face is toward the center of camera.
- When recording your face or 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 75KB, 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 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.