

Face Recognition Time & Attendance

Quick Start Guide



Foreword

General

This manual introduces the installation and basic operations of the Face Recognition Time & Attendance (hereinafter referred to as "attendance").

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
V1.0.1	<ul style="list-style-type: none">Update the distance requirement between the face and camera.Add a warning statement.	August 2020
V1.0.0	First release.	June 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 attendance, hazard prevention, and prevention of property damage. Read these contents carefully before using the attendance, comply with them when using, and keep the manual well for future reference.

Operation Requirements

- Do not place or install the attendance in a place exposed to sunlight or near the heat source.
- Keep the attendance away from dampness, dust or soot.
- Keep the attendance installed horizontally on the stable place to prevent it from falling.
- Do not drop or splash liquid onto the attendance, and make sure that there is no object filled with liquid on the attendance to prevent liquid from flowing into the attendance.
- Install the attendance in a well-ventilated place, and do not block the ventilation of the attendance.
- Operate the attendance within the rated range of power input and output.
- Do not disassemble the attendance randomly.
- When used in outdoors with high temperature, do not directly touch the surface of the attendance, such as the screen, metal back shell, and fingerprint sensor.

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 attendance; 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	2
2.1 Cable Connection	2
2.2 Installation Notes.....	3
2.3 Installation	4
3 System Operations	7
3.1 Initialization	7
3.2 Adding New Users	7
4 Web Operations	9
Appendix 1 Notes of Face Recording/Comparison	10
Appendix 2 Cybersecurity Recommendations	13

1 Dimensions and Components

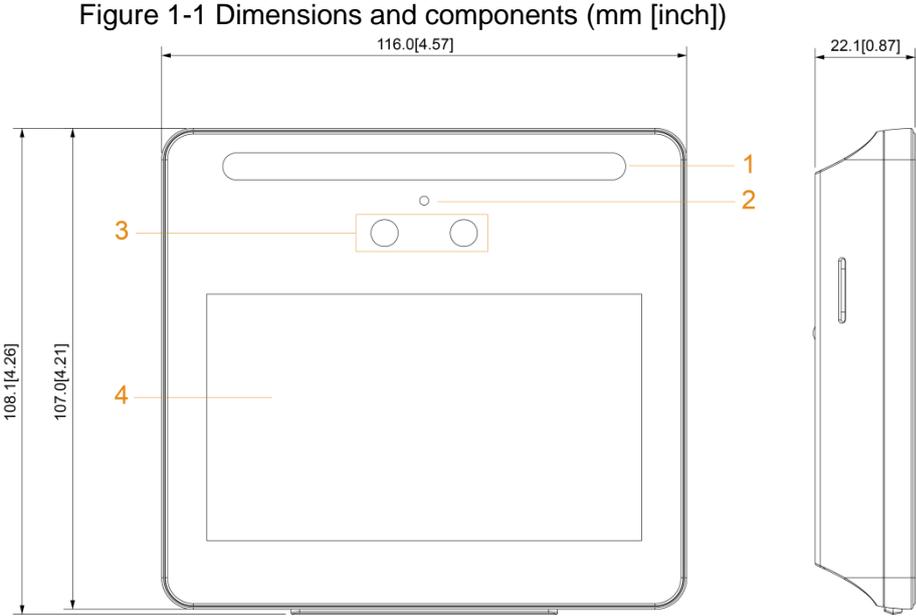


Table 1-1 Component description

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

2 Connection and Installation

2.1 Cable Connection

Figure 2-1 Cable connection

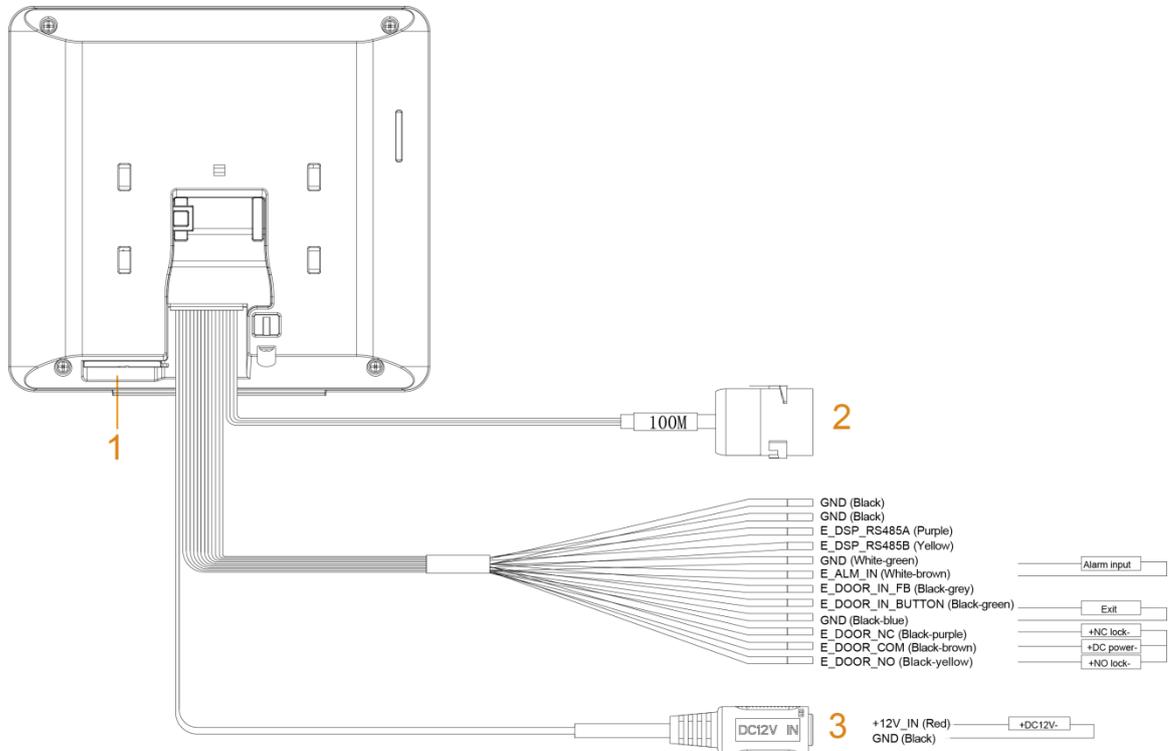
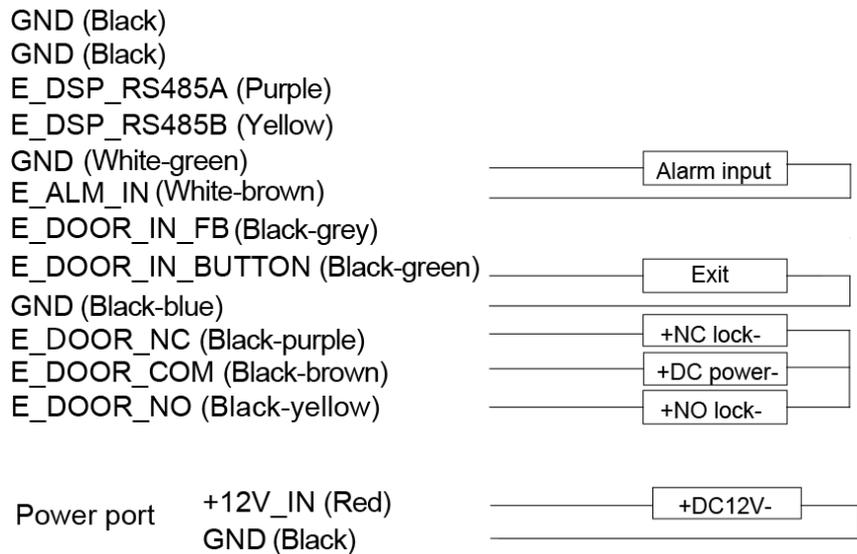


Figure 2-2 Ports



The RS485 port and door contact feedback (FB) port are reserved. Currently the corresponding functions are not supported.

Table 2-1 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 attendance, the minimum illumination should be no less than 100 Lux.
- It is recommended that the attendance 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 2-3 Ambient illumination requirement



Candle: 10Lux



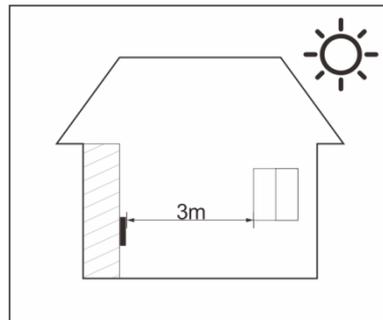
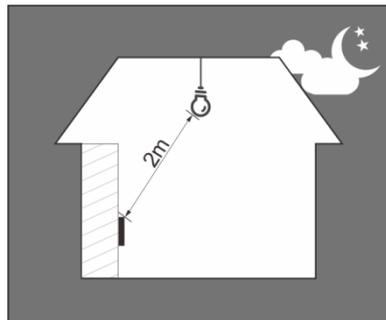
Light bulb: 100Lux–850Lux



Sunlight: $\geq 1200\text{Lux}$

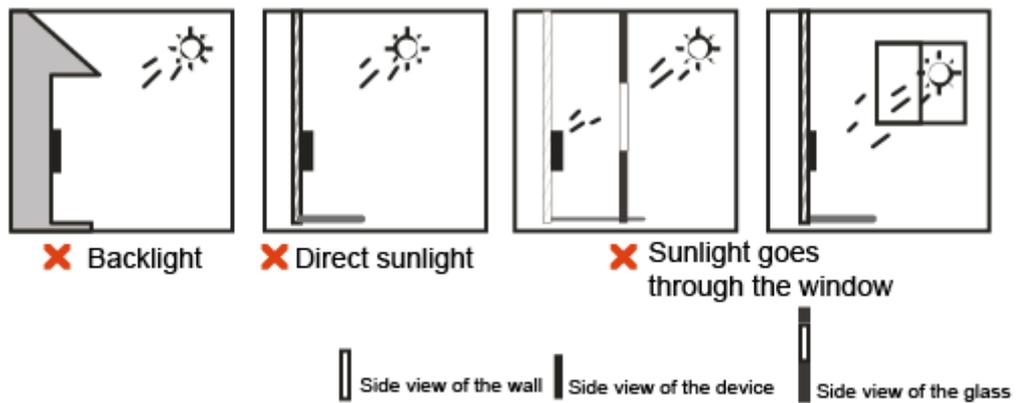
Places Recommended

Figure 2-4 Places recommended



Places Not Recommended

Figure 2-5 Places not recommended



2.3 Installation

Desktop Installation

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

Figure 2-6 Desktop installation (1)

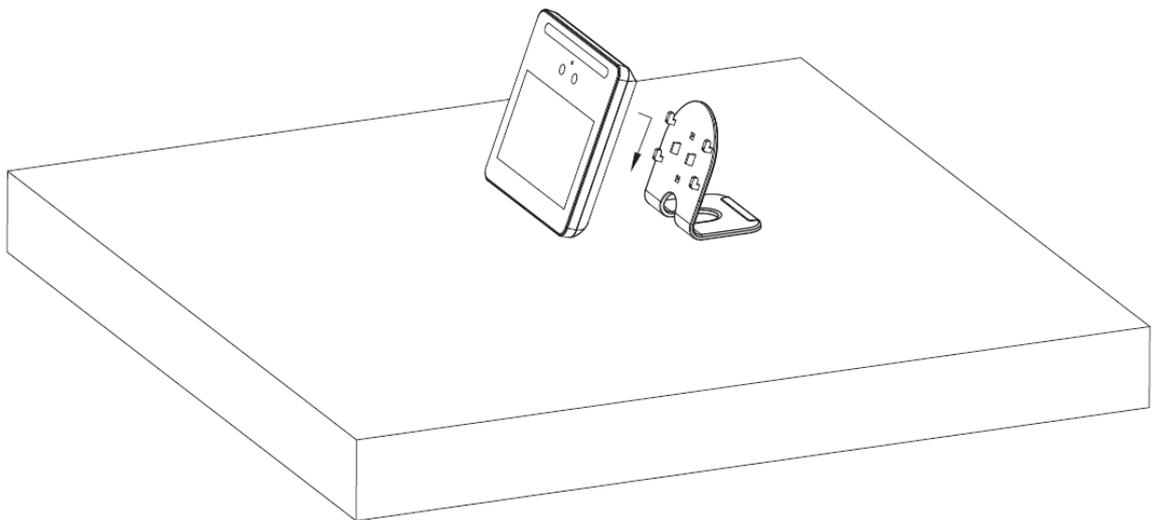
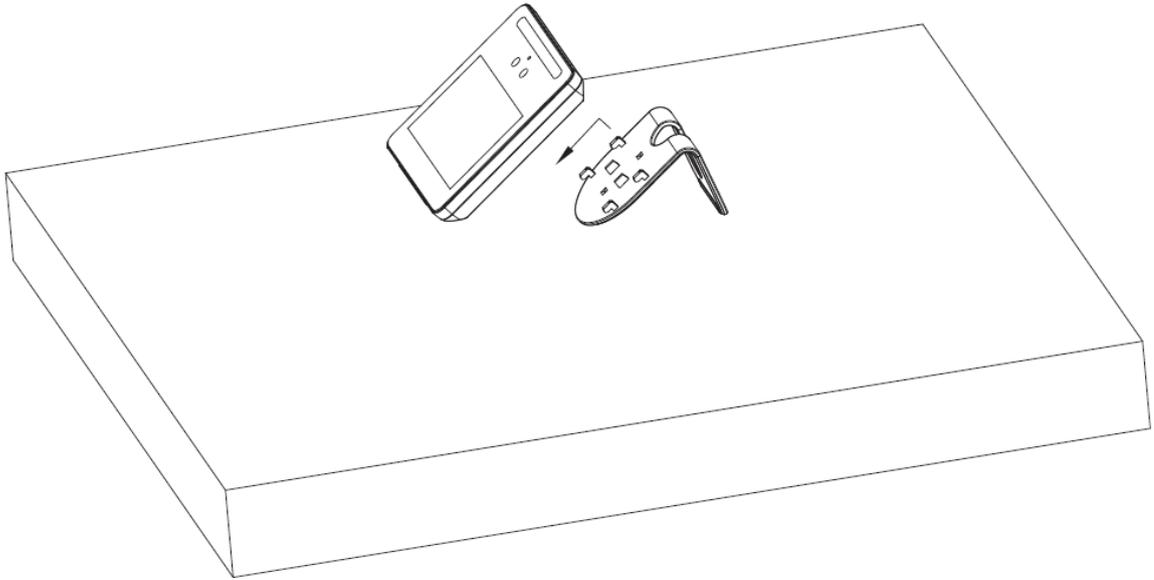


Figure 2-7 Desktop installation (2)



Wall Installation

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

Figure 2-1 Installation height

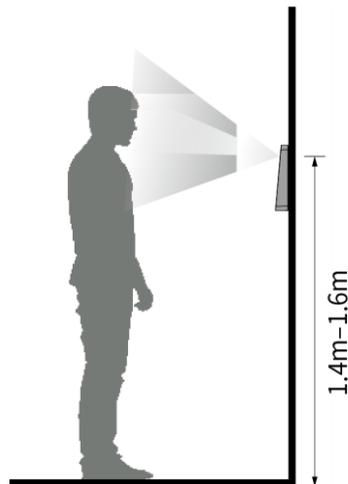
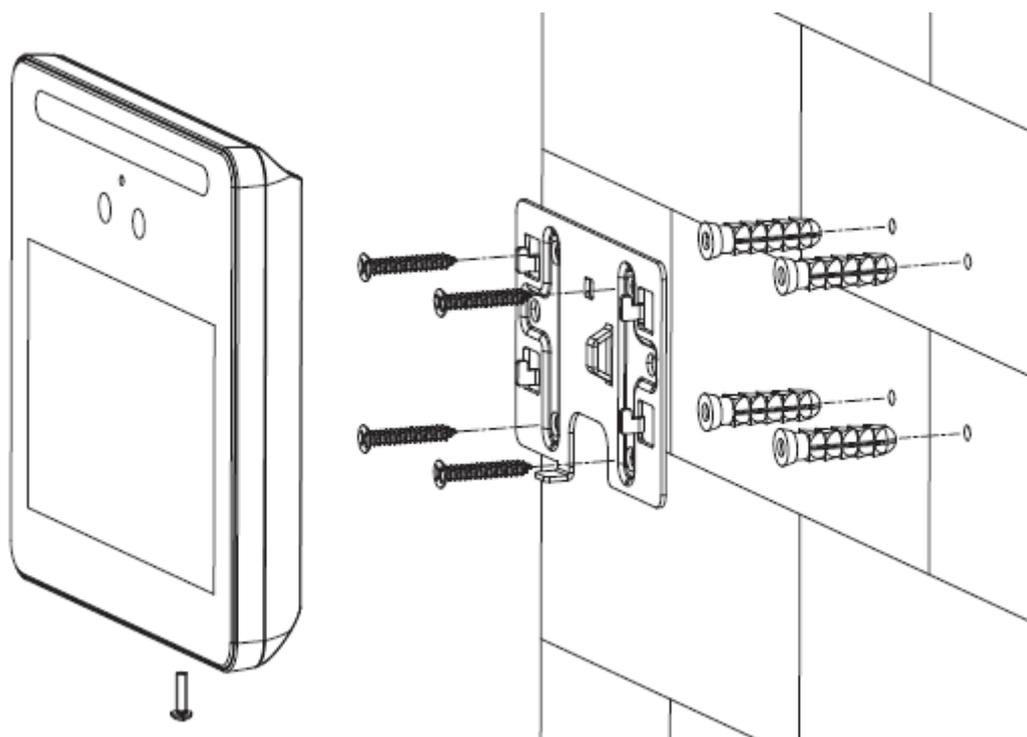


Figure 2-2 Wall installation



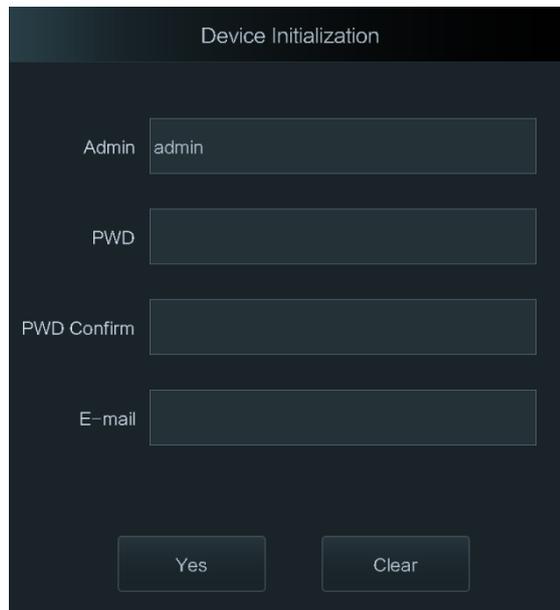
- Step 1 Drill four holes in the wall according to holes in the bracket.
- Step 2 Fix the bracket on the wall by installing the expansion screws into the four bracket installation holes.
- Step 3 Connect cables for attendance. See "2.1 Cable Connection".
- Step 4 Hang the attendance on the bracket hook.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

3 System Operations

3.1 Initialization

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

Figure 3-1 Initialization



- 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 ' " ; : &).

3.2 Adding New Users

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



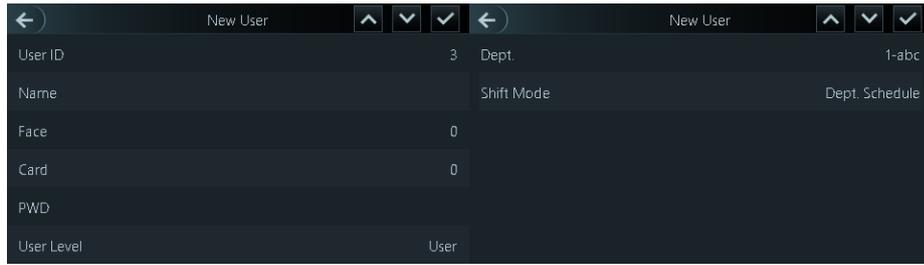
The following figures are for reference only, and the actual interface shall prevail.

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



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).
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	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 attendance.
PWD	The user password. The maximum length of the password is 8 digits.
User Level	You can select a user level for new users. There are two options: User and Admin.  In case that you forget the administrator password, you had better create more than one administrator.
Dept.	Select a department that the user belongs to.
Shift Mode	Select a shift mode for the user. <ul style="list-style-type: none"> Dept. Schedule: Check attendance according to the schedule of department that the user belongs to. Personal Schedule: Check attendance according to personal schedule.

Step 5 Tap  to save the configuration.

4 Web Operations

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



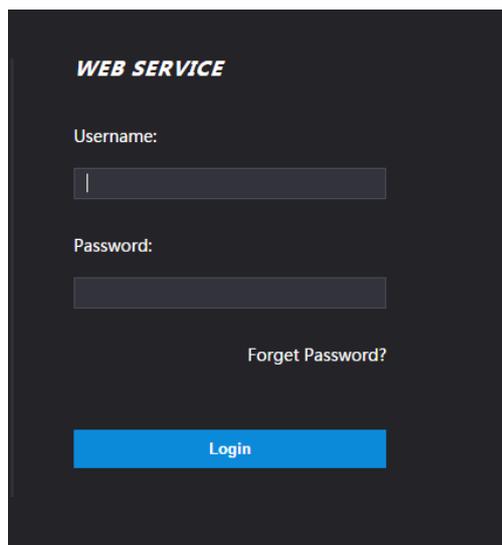
You need to set a password and an email address before logging in to the web interface for the first time. Password you set is used to log in to the web, and the email is used to reset passwords.

Step 1 Open IE web browser, enter the IP address of the attendance 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 attendance.
- The default IP address of the attendance 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 attendance. 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

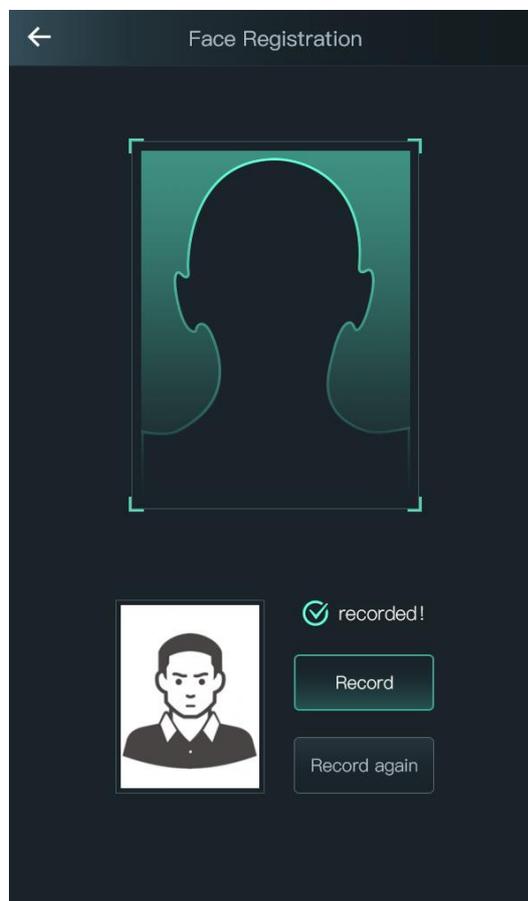
- Glasses, hats, and beards might influence face recognition performance.
- Do not cover your eyebrows when wearing hats.
- Do not change your beard style greatly if you will use the device; otherwise face recognition might fail.
- Keep your face clean.
- Keep the device at least two meters away from 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 attendance 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



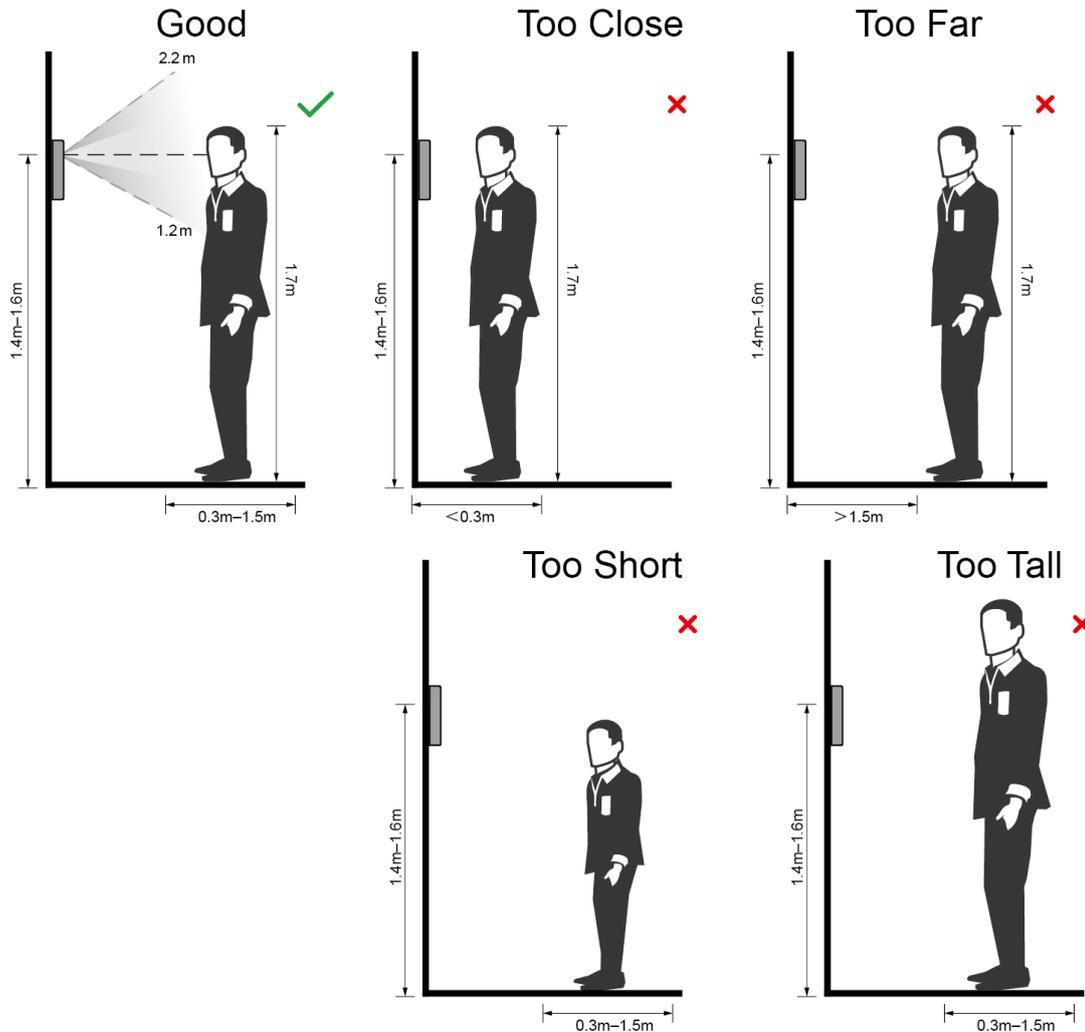


- Do not shake your head or body, otherwise the registration might fail.
- Avoid two faces appear in the capture frame at the same time.

Face Position

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

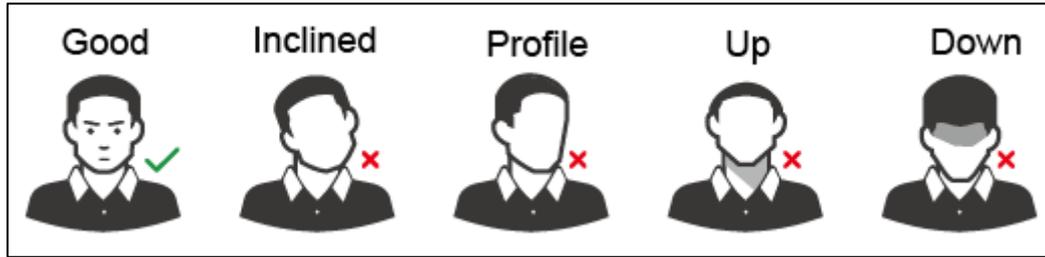
Appendix Figure 1-2 Appropriate face position



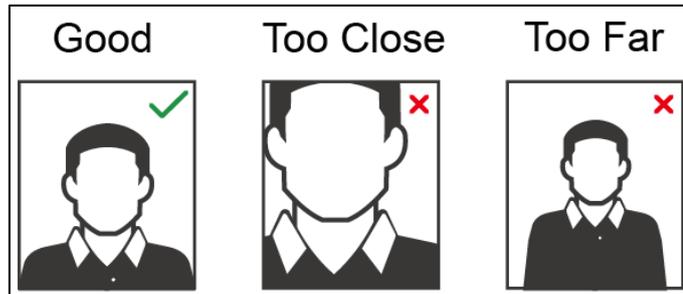
Requirements of Faces

- 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 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.