Face Recognition Terminal

Quick Start Guide

V1.0.0

Foreword

General

This manual introduces the installation and basic operation of the Face Recognition Terminal (hereinafter referred to as "terminal").

Safety Instructions

The following categorized signal words with defined meaning might appear in the manual.

Signal Words	Meaning
⚠CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
🕮 NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

Version	Revision Content	Release Date
V1.0.0	First release	August 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 terminal, hazard prevention, and prevention of property damage. Read these contents carefully before using the terminal, comply with them when using, and keep it well for future reference.

Operation Requirement

- Do not place or install the terminal in a place exposed to sunlight or near the heat source.
- Keep the terminal away from dampness, dust or soot.
- Keep the terminal installed horizontally on the stable place to prevent it from falling.
- Do not drop or splash liquid onto the terminal, and make sure there is no object filled with liquid on the terminal to prevent liquid from flowing into the terminal.
- Install the terminal in a well-ventilated place, and do not block the ventilation of the terminal.
- Operate the terminal within the rated range of power input and output.
- Do not dissemble the terminal.
- Transport, use and store the terminal 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 terminal; 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

1 Dimensions and Components

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

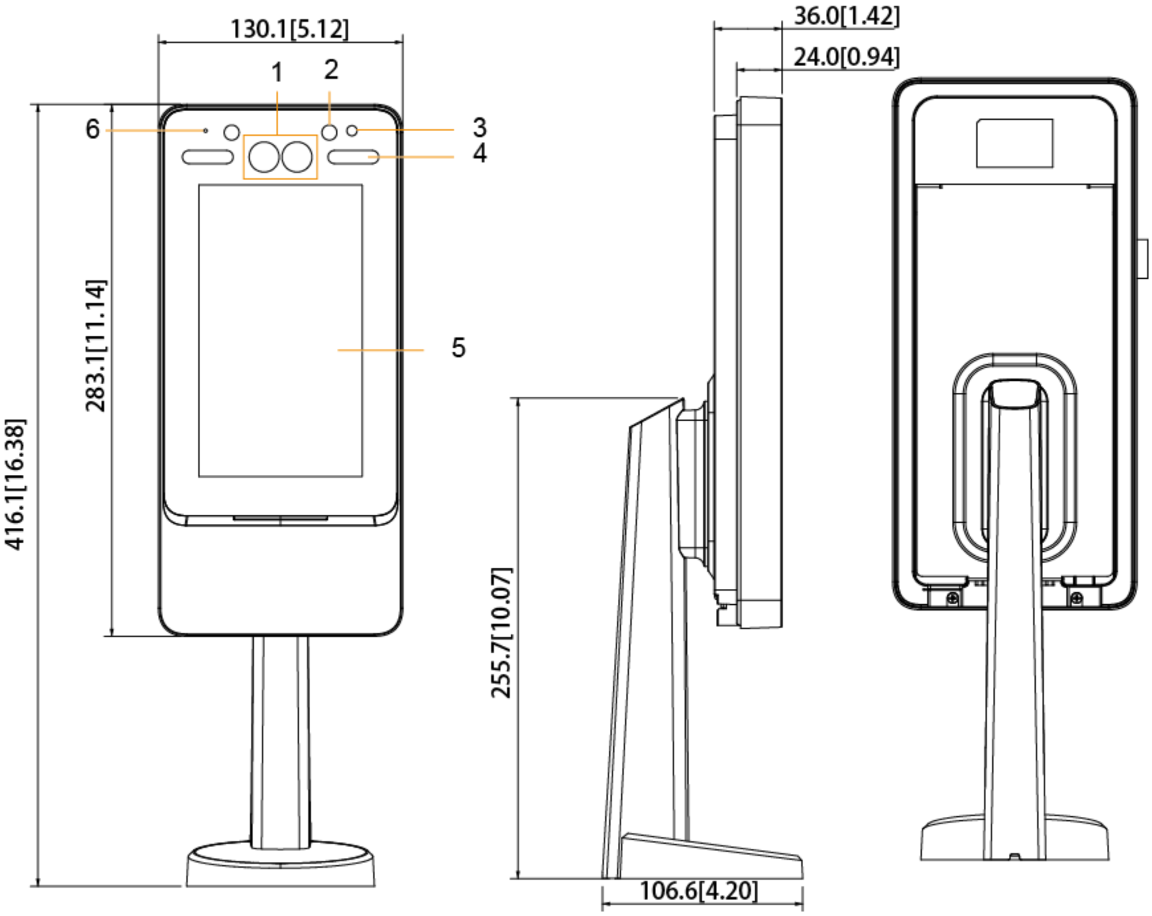


Table 1-1 Component description

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

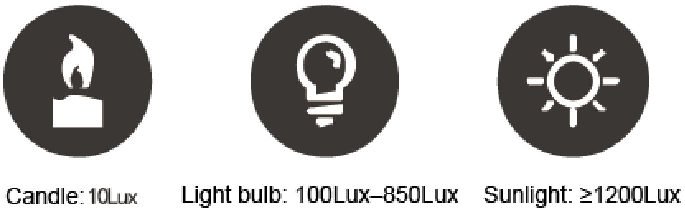
2 Installation

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.

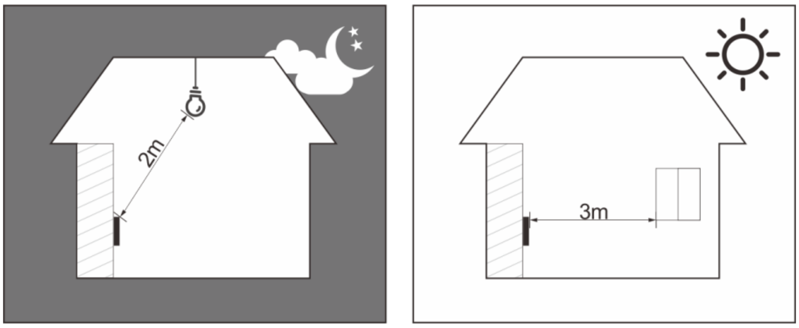
Ambient Illumination Requirement

Figure 2-1 Ambient illumination requirement



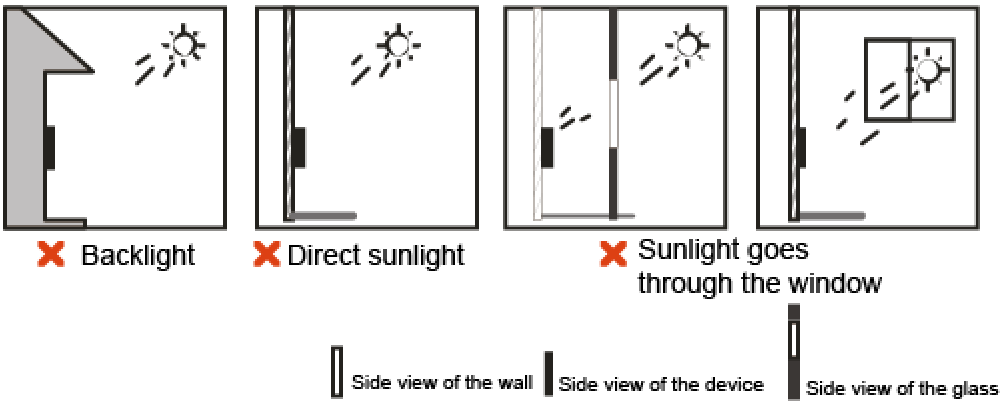
Places Recommended

Figure 2-2 Places recommended



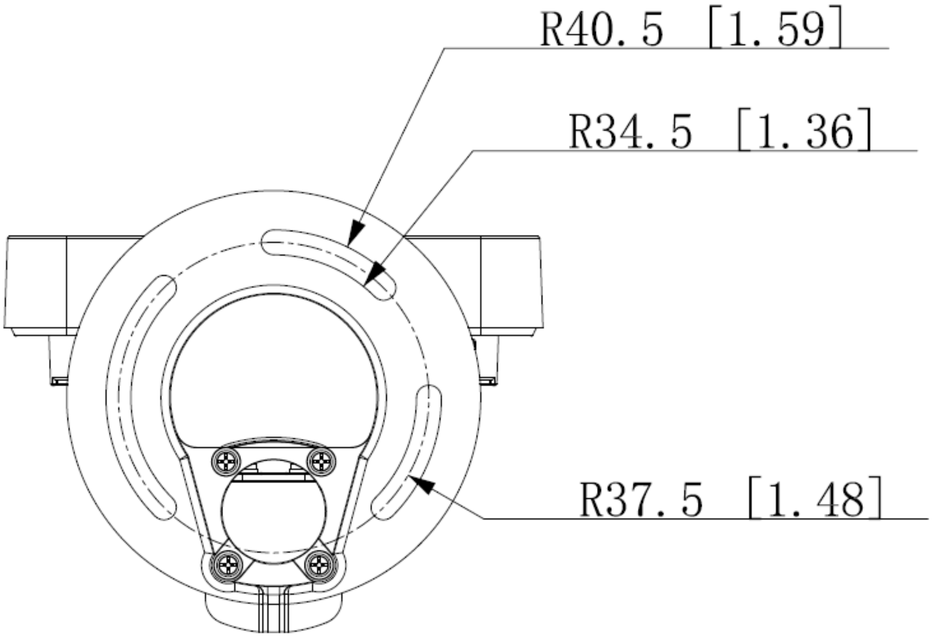
Places Not Recommended

Figure 2-3 Places not recommended



2.2 Installation Drawings

Figure 2-4 Installation drawings (mm[inch])



2.3 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, turnstile control, and firefighting linkage will be invalid.

Figure 2-5 Cable connection

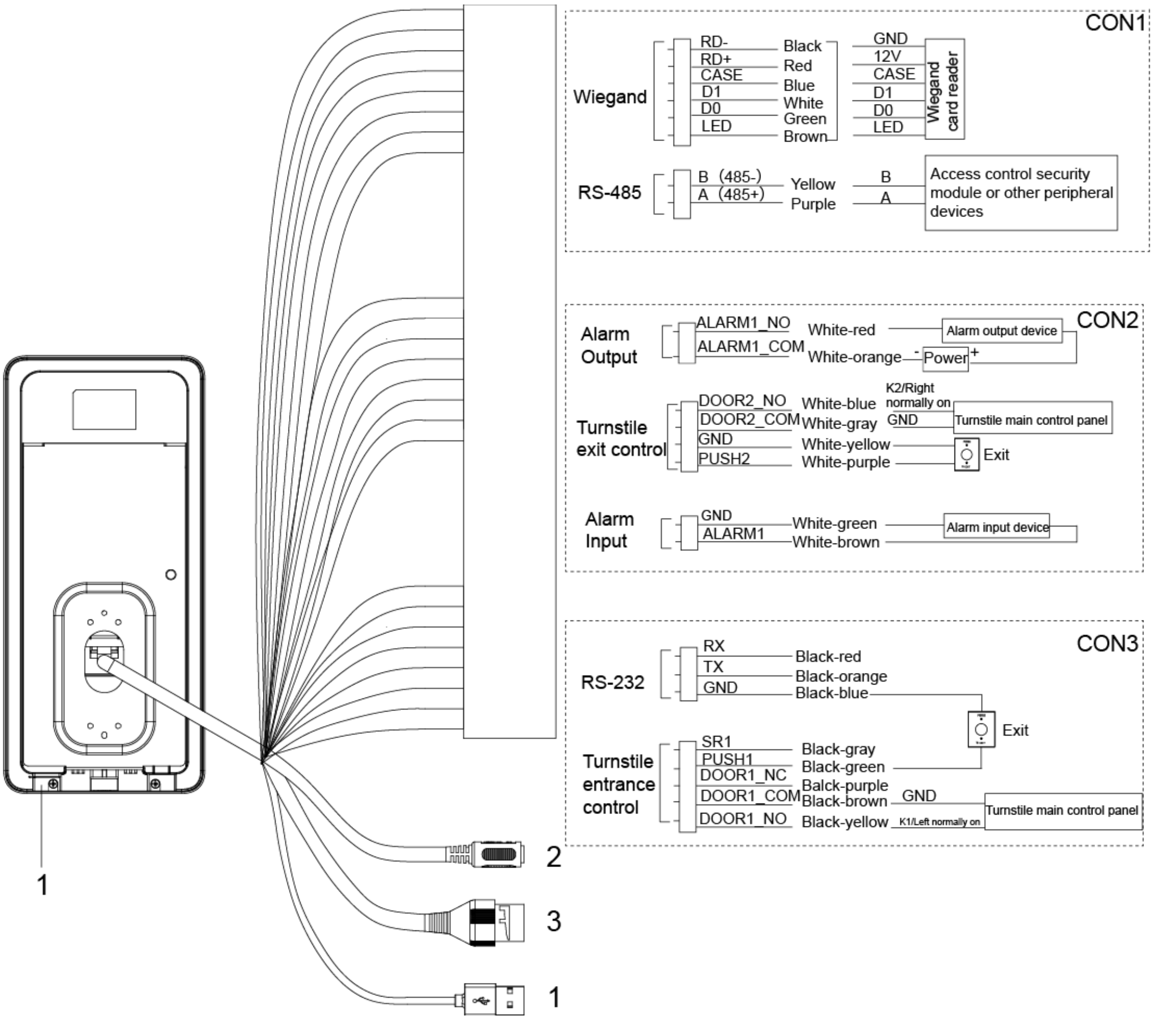


Table 2-1 Component description

No.	Name
1	USB port
2	Power port
3	Ethernet port

2.4 Installation

Figure 2-6 Installed on the gate machine

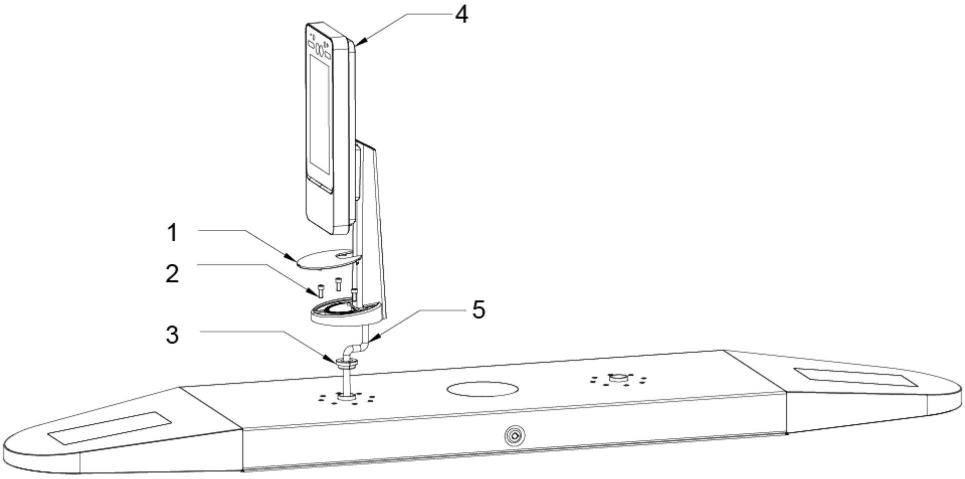


Table 2-2 Component description

No.	Name
1	Ornamental cover
2	M5 screw
3	Waterproof silica gel plug
4	Terminal
5	Cable

Installation Procedure

Step 1 Thread cable through the turnstile.

Step 2 Put the waterproof silica gel plug on the cable.

Step 3 Fix the terminal onto the turnstile with M5 screw.

Connect cables for terminal. See "2.3 Cable Connections."

Step 4 Apply sealant to gaps between the waterproof silica gel plug and turnstile.

Step 5 Install the ornamental cover on the base of the terminal.

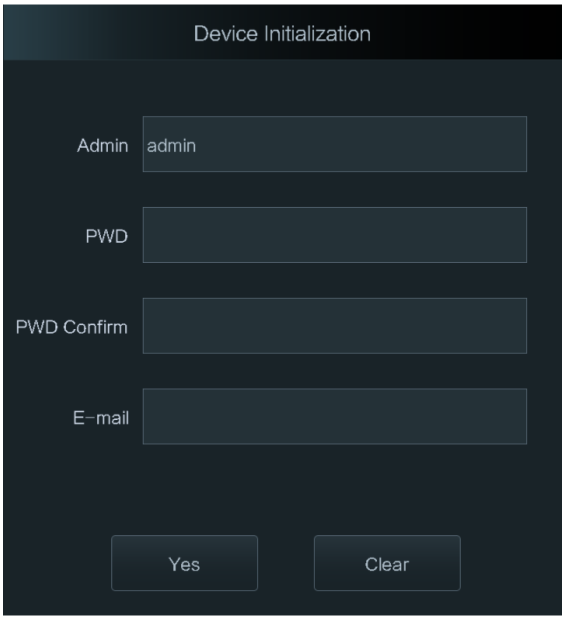
The installation is competed.

3 System Operation

3.1 Initialization

Administrator password and an email should be set the first time the terminal is turned on; otherwise the terminal cannot be used. See Figure 3-1.

Figure 3-1 Initialization



Device Initialization

Admin: admin

PWD:

PWD Confirm:

E-mail:

- The administrator password can be reset through the email address you entered if the administrator forgets the administrator password.
- 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 terminal without touch screen, initialization can be completed through the web. See the user manual for details.

3.2 Adding New Users

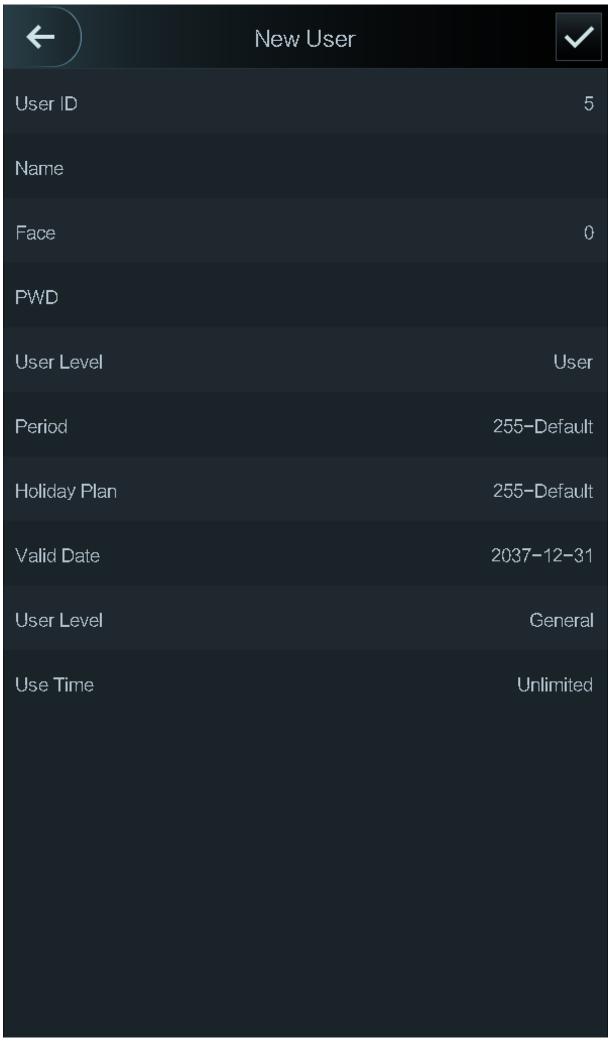
You can add new users by entering their user IDs, names, importing face images, passwords, selecting their user levels, and more.

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

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

The following figure is for reference only and the actual interface shall prevail.

Figure 3-2 New user



New User

User ID	5
Name	
Face	0
PWD	
User Level	User
Period	255-Default
Holiday Plan	255-Default
Valid Date	2037-12-31
User Level	General
Use Time	Unlimited

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).
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."
Password	The door unlocking password. The maximum length of the ID digits is 8. 📖 If the terminal is without touch screen, you need to connect the terminal to a peripheral card reader. There are buttons on the card reader.

Parameter	Description
Level	You can select a user level for new users. There are two options. ● User: Users only have door unlock authority. ● Admin: Administrators can not only unlock the door but also have parameter configuration authority. In case that you forget the administrator password, you had better create more than one administrator.
Period	You can set a period in which the user can unlock the door. For detailed period settings, see the configuration 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	There are six levels: ● 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. ● Disable: When disabled 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 number of times that the guest can unlock the door.

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

For terminal without touch screen, adding new users can be completed through the web. See the user manual for details.

4 Web Operation

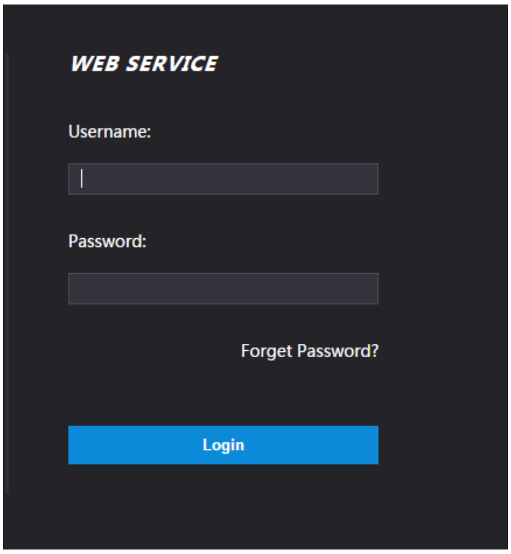
The terminal can be configured and operated on the web. Through the web you can set parameters including network parameters, video parameters, and terminal parameters; and you can also maintain and update the system.

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 terminal in the address bar, and then press Enter.

Figure 4-1 Login



Step 2 Enter the user name and password.

- The default username of administrator is admin, and the password is the login password after initializing the terminal. 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

Before Registration

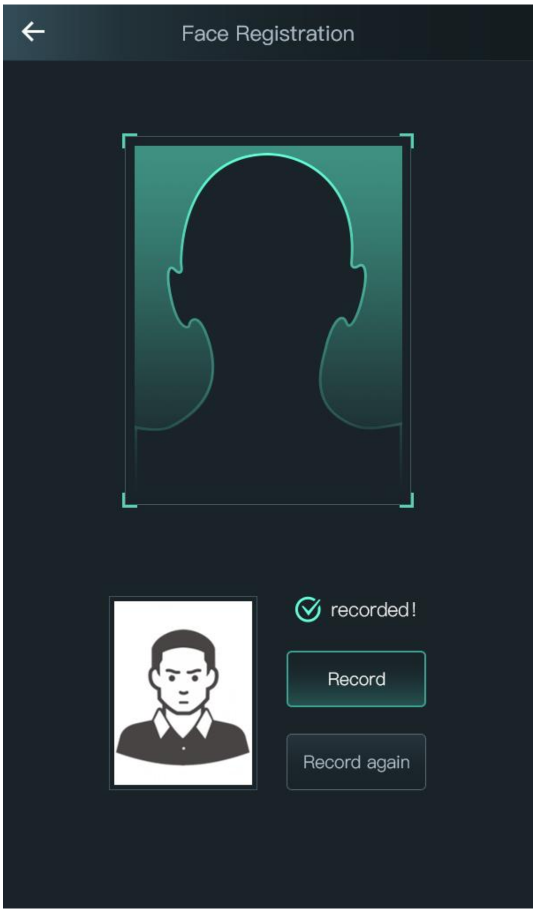
- Glasses, hats, and beards might influence face recognition performance.
- Do not cover your eye brows when wearing hats.
- Do not change your beard style greatly if you will use the device; otherwise face recognition might fail.
- Keep your face clean.
- Keep the device at least two meters away from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

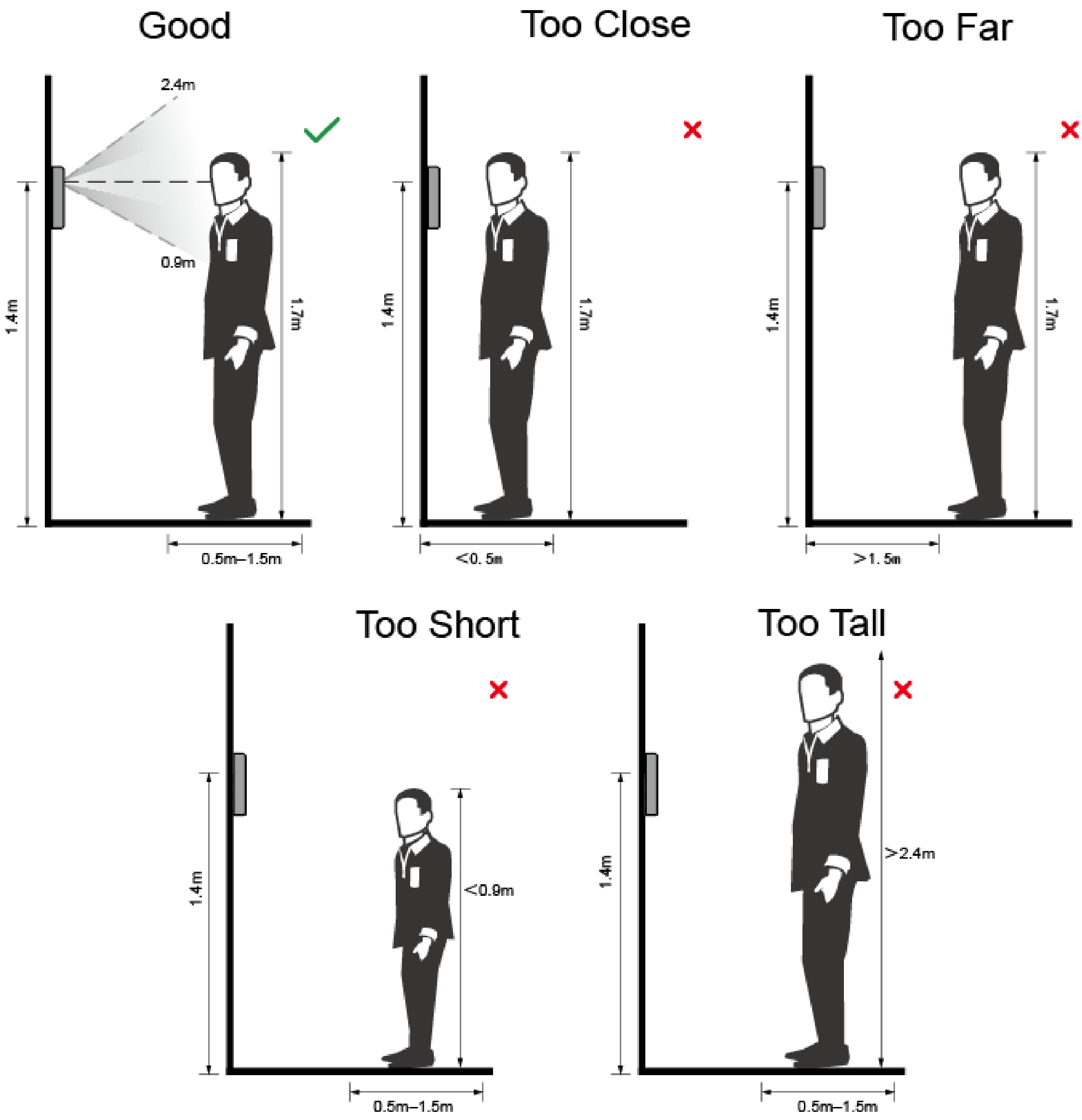


- Do not shake your head or body, or the registration might fail.
- Avoid two faces appear in the box at the same time.

Face Position

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

Appendix figure 1-2 Appropriate face position

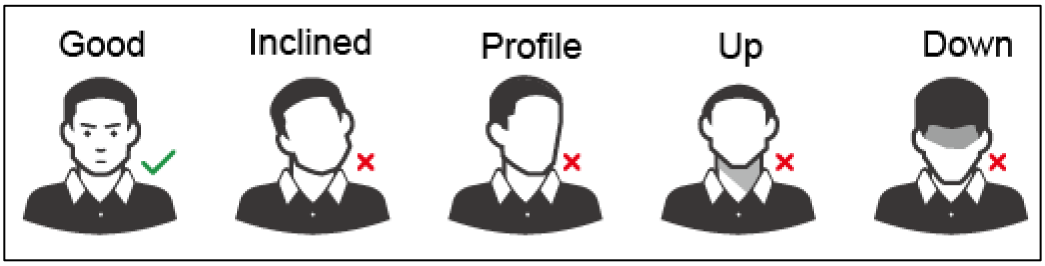


Requirements of Faces

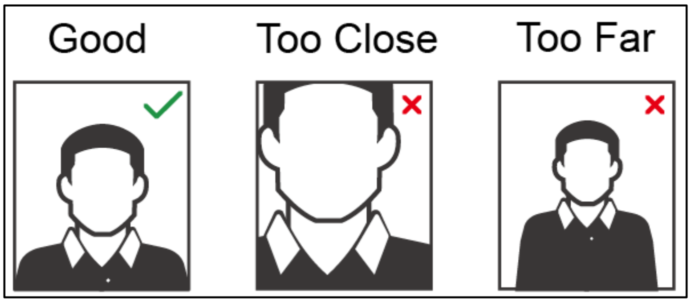
- Make sure that the face is clean and forehead is not covered by hair.
- Do not wear glasses, hats, heavy beards, or other face ornaments that influence face image recording.
- With eyes open, without facial expressions, and make your face is toward the center of camera.
- When recording your face or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