Face Recognition Access and Time Attendance Terminal

Quick Start Guide

V1.0.1

Mandatory actions to be taken towards cybersecurity

1. Change Passwords and Use Strong Passwords:
The number one reason systems get "hacked" is due to having weak or default passwords. It is recommended to change default passwords immediately and choose a strong password whenever possible. A strong password should be made up of at least 8 characters and a combination of special characters, numbers, and upper and lower case letters.

2. Update Firmware
As is standard procedure in the tech-industry, we recommend keeping NVR, DVR, and IP camera firmware up-to-date to ensure the system is current with the latest security patches and fixes.

"Nice to have" recommendations to improve your network security

1. Change Passwords Regularly
Regularly change the credentials to your devices to help ensure that only authorized users are able to access the system.

2. Change Default HTTP and TCP Ports:
● Change default HTTP and TCP ports for systems. These are the two ports used to communicate and to view video feeds remotely.
● These ports can be changed to any set of numbers between 1025-65535. Avoiding the default ports reduces the risk of outsiders being able to guess which ports you are using.

3. Enable HTTPS/SSL:
Set up an SSL Certificate to enable HTTPS. This will encrypt all communication between your devices and recorder.

4. Enable IP Filter:
Enabling your IP filter will prevent everyone, except those with specified IP addresses, from accessing the system.

5. Change ONVIF Password:
On older IP Camera firmware, the ONVIF password does not change when you change the system's credentials. You will need to either update the camera's firmware to the latest revision or manually change the ONVIF password.

6. Forward Only Ports You Need:

● Only forward the HTTP and TCP ports that you need to use. Do not forward a huge range of numbers to the device. Do not DMZ the device's IP address.

● You do not need to forward any ports for individual cameras if they are all connected to a recorder on site; just the NVR is needed.

7. Disable Auto-Login on SmartPSS:

Those using SmartPSS to view their system and on a computer that is used by multiple people should disable auto-login. This adds a layer of security to prevent users without the appropriate credentials from accessing the system.

8. Use a Different Username and Password for SmartPSS:

In the event that your social media, bank, email, etc. account is compromised, you would not want someone collecting those passwords and trying them out on your video surveillance system. Using a different username and password for your security system will make it more difficult for someone to guess their way into your system.

9. Limit Features of Guest Accounts:

If your system is set up for multiple users, ensure that each user only has rights to features and functions they need to use to perform their job.

10. UPnP:

● UPnP will automatically try to forward ports in your router or modem. Normally this would be a good thing. However, if your system automatically forwards the ports and you leave the credentials defaulted, you may end up with unwanted visitors.

● If you manually forwarded the HTTP and TCP ports in your router/modem, this feature should be turned off regardless. Disabling UPnP is recommended when the function is not used in real applications.

11. SNMP:

Disable SNMP if you are not using it. If you are using SNMP, you should do so only temporarily, for tracing and testing purposes only.

12. Multicast:

Multicast is used to share video streams between two recorders. Currently there are no known issues involving Multicast, but if you are not using this feature, deactivation can enhance your network security.

13. Check the Log:

If you suspect that someone has gained unauthorized access to your system, you can check the system log. The system log will show you which IP addresses were used to login to your system and what was accessed.

14. Physically Lock Down the Device:

Ideally, you want to prevent any unauthorized physical access to your system. The best way to achieve this is to install the recorder in a lockbox, locking server rack, or in a room that is behind a lock and key.

15. Connect IP Cameras to the PoE Ports on the Back of an NVR:
Cameras connected to the PoE ports on the back of an NVR are isolated from the outside world and cannot be accessed directly.

16. Isolate NVR and IP Camera Network
The network your NVR and IP camera resides on should not be the same network as your public computer network. This will prevent any visitors or unwanted guests from getting access to the same network the security system needs in order to function properly.

General

This document elaborates on structure, installation and system function of face recognition access and time attendance terminal.

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.

Privacy Protection Notice

As the device user or data controller, you might collect personal data of others' such as face, fingerprints, car plate number, Email address, phone number, GPS and so on. You need to be in compliance with the local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures include but not limited to: providing clear and visible identification to inform data subject the existence of surveillance area and providing related contact.

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 User's Manual, CD-ROM, QR code or our official website. If there is inconsistency between paper User's 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 Guide (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.

The following description is the correct application method of the device. Please read the manual carefully before use, in order to prevent danger and property loss. Strictly conform to the manual during application and keep it properly after reading.

Operating Requirement

- Please don't place and install the device in an area exposed to direct sunlight or near heat generating device.
- Please don't install the device in a humid, dusty or fuliginous area.
- Please keep its horizontal installation, or install it at stable places, and prevent it from falling.
- Please don't drip or splash liquids onto the device; don't put on the device anything filled with liquids, in order to prevent liquids from flowing into the device.
- Please install the device at well-ventilated places; don't block its ventilation opening.
- Use the device only within rated input and output range.
- Please don't dismantle the device arbitrarily.
- Please transport, use and store the device within allowed humidity and temperature range.

Power Requirement

- Please make sure to use batteries according to requirements; otherwise, it may result in fire, explosion or burning risks of batteries!
- To replace batteries, only the same type of batteries can be used!
- The product shall use electric wires (power wires) recommended by this area, which shall be used within its rated specification!
- Please make sure to use standard power adapter matched with this device. Otherwise, the user shall undertake resulting personnel injuries or device damages.
- Please use power supply that meets SELV (safety extra low voltage) requirements, and supply power with rated voltage that conforms to Limited Power Source in IEC60950-1. For specific power supply requirements, please refer to device labels.
- Products with category I structure shall be connected to grid power output socket, which is equipped with protective grounding.
- Appliance coupler is a disconnecting device. During normal use, please keep an angle that facilitates operation.

Table of Contents

1 Product Overview

Face recognition access and time attendance terminal is a generation of more powerful face recognition device that supports access control and attendance management. By integrating face, fingerprint, card and password identifications, this device is suitable for offices, factories, retail stores, schools and hospitals.

1.1 Functional Features

- 4.3-inch touch screen with 480×272 resolution rate displays software interface and operation prompt, displays face frame and monitors maximum face in a real-time way, so as to facilitate users to calibrate.
- Adopt high-definition binocular camera, 2MP for visible light and 1.3MP for infrared light; facial recognition distance is 0.3m～0.5m.
- Support to recognize fake face picture and mobile phone face picture; support self-adaptation to strong light environment.
- Support 1:N face recognition, advanced face recognition algorithm, max. 1,000 or 3,000 face library depending on model, quick recognition speed and high accuracy rate.
- Face comparison time is ≤1s; face verification accuracy is ≥98%.
- Support face, fingerprint, card and password identification.
- Support voice prompt.
- Support max. 1,000 person's local attendance statistics and max. 6 kinds of customizable attendance events.
- Support max. 30,000 users, 30,000 passwords, 30,000 cards, max. 1,000 or 3,000 faces depending on model, and 3,000 fingerprints.
- Store max. 150,000 records, for future query.
- Support local login management, record query, device and face parameter setting, recorded event import/export.
- Built-in RTC, DST—daylight saving time, online update, NTP—network time protocol, active registration, Wi-Fi and P2P.
- IP55 protection. Avoid direct exposure to sunlight.
- Operating temperature: -5℃～+55℃, operating humidity: ≤95%.

⚠️ Caution

To connect external power source, please use DC12V 2A power adapter and ensure that operating temperature is within -5℃～+55℃.

1.2 External Dimension

External dimension of the device is shown in Figure 1-1. The unit is mm.
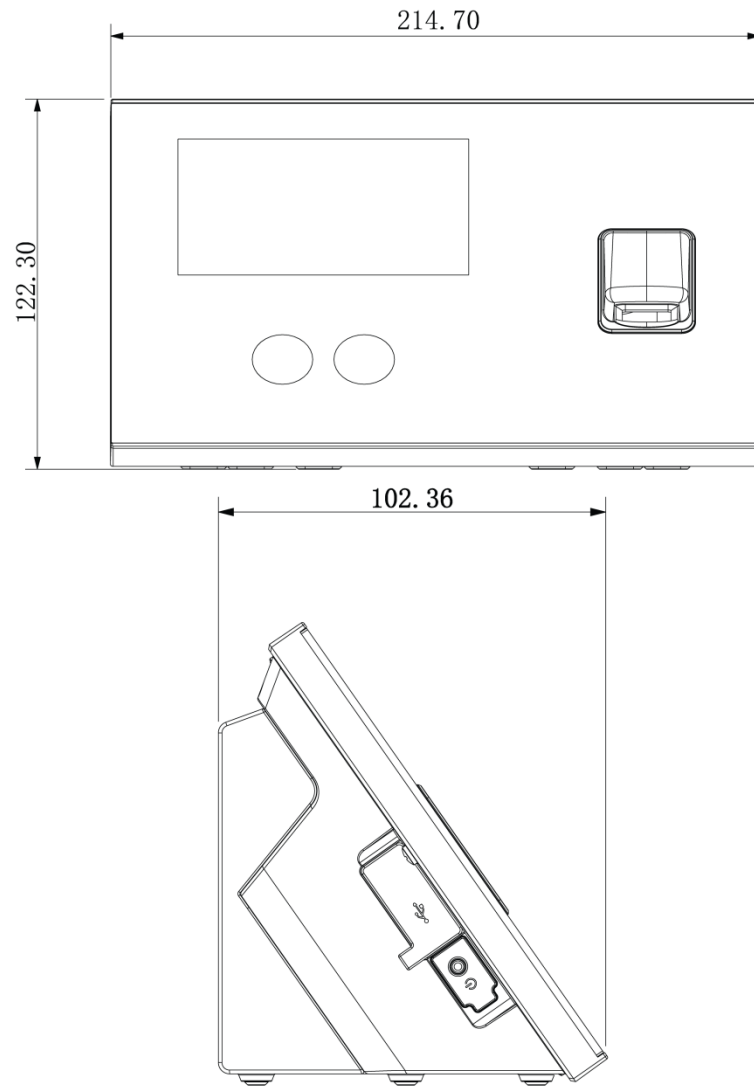

Figure 1-1

2 Installation Guide

2.1 Packing List

Before installation, please check the package according to Table 2-1.

No.	Name	Quantity	Note
1	Device	1	-
2	Power adapter	1	DC12V 2A
3	Cable	4	-
4	M4×30 cross recessed pan head flat-end screw	2	Fix the bracket to concealed mount
5	Screw bag	1 bag ● ST3×18 self-tapping screw, 4 ● Expansion pipe, 4	Without concealed mount, fix the bracket to the mounting surface
6	Quick start guide	1	-

Table 2-1

2.2 System Architecture

Its system architecture is shown in Figure 2-1.
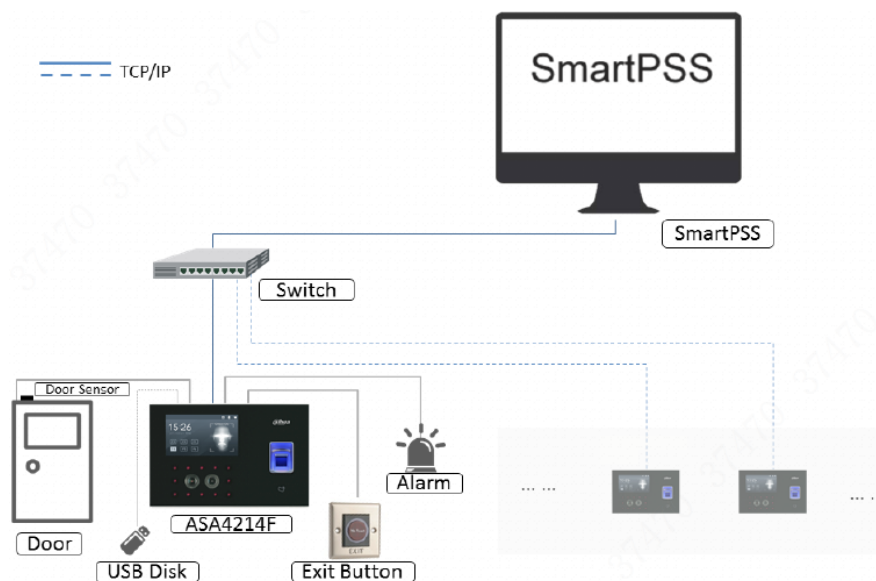
Figure 2-1

2.3 Installation

Installation of the device is shown in Figure 2-2 and Figure 2-4.

Figure 2-2

Figure 2-3

M4×30 cross recessed pan-head flat-end screw

M3×6 exalobular socket counter-sunk head flat-end screws

ST3×18 self-tapping screw
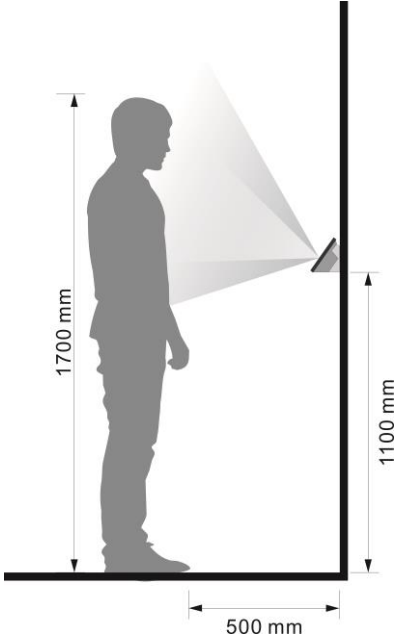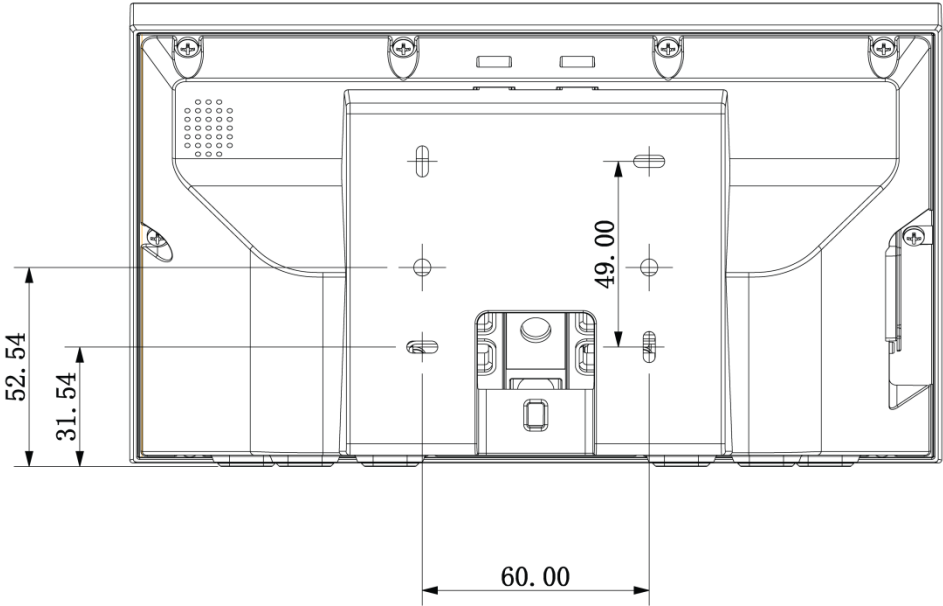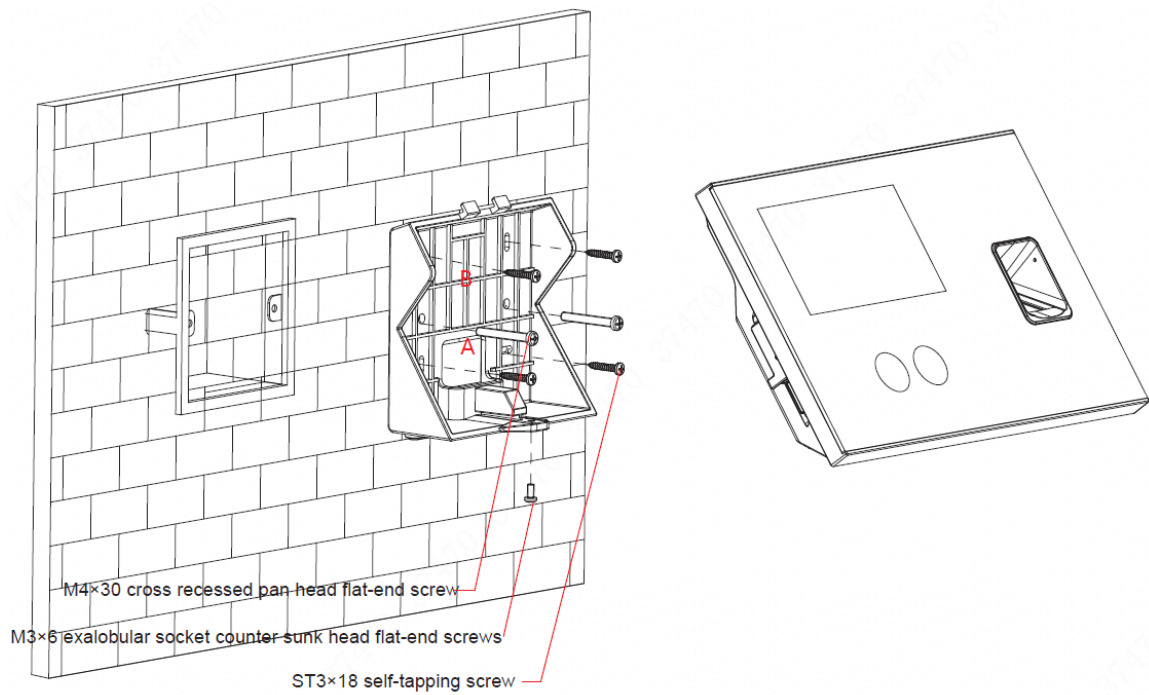
Figure 2-4

Step 1 Drill holes according to the positions in Figure 2-3, and install expansion pipes into holes.

Step 2 Install the bracket.
- If there is a concealed mount, fix the bracket onto concealed mount with screw A.
- Without the concealed mount or good fixation, fix the bracket onto the wall directly with screw B. Before fixing, embed expansion pipes at corresponding positions of the wall.

Step 3 Hang the device onto the hook of the bracket.

Step 4 Insert screws from the device bottom, fasten the bracket and complete installation.

2.4 Panel and Port

The device is shown in Figure 2-5, Figure 2-6 and Figure 2-7. Ports of rear panel are described in Table 2-2.

Screen

Fingerprint

Camera

Card

Figure 2-5

USB Port

Switch Button

Figure 2-6

CON1

RD-
RD+
CASE
DI
DO
LED
485A
485B

1   8

CON2

COM
NC
NO
SR
PUSH
GND
RX
TX

CON3

12V
12V
ERX+
GND
ERX-

ETX+
ETX-
GND

CON4

ALMI
ALM2
GND
COMI
NO1
NO2
COM2
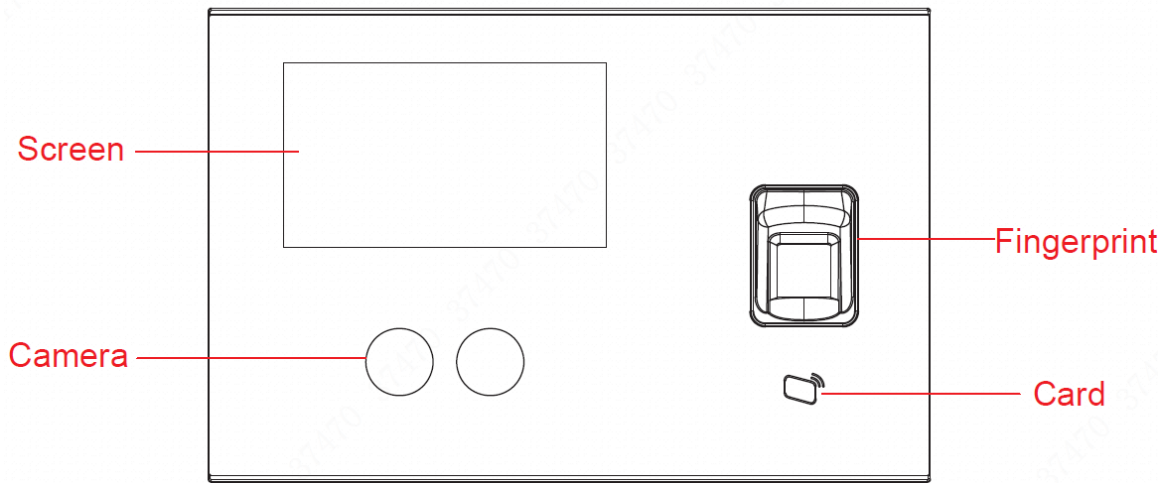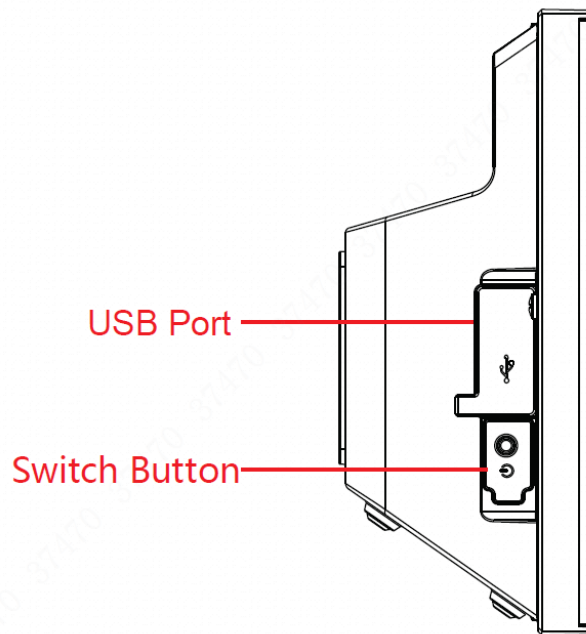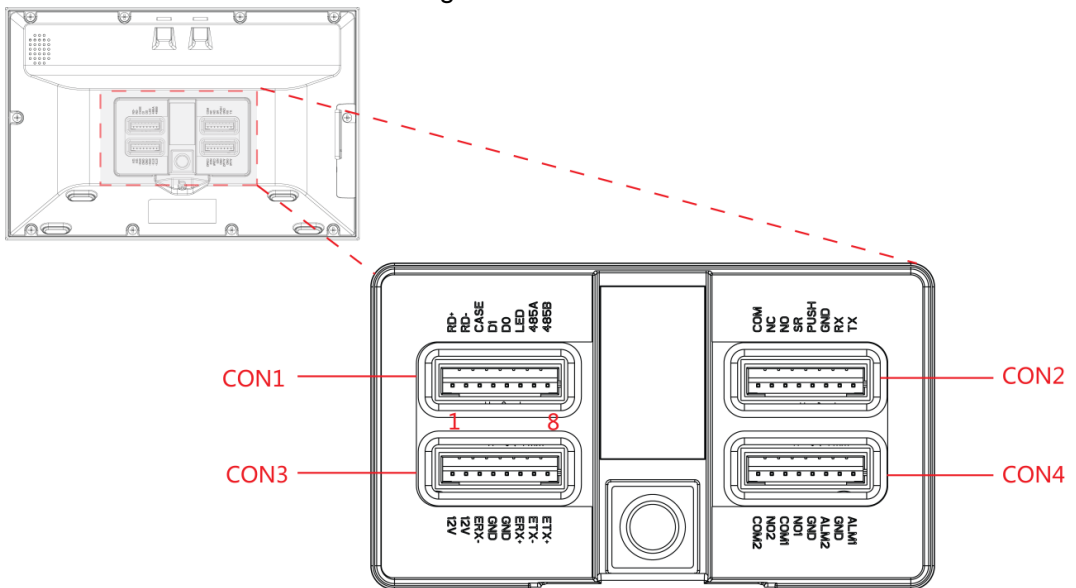
Figure 2-7

Port	Note
CON1	Wiegand /RS485 input/output.
CON2	Electric lock output, door sensor and exit button.
CON3	Power port and network port.
CON4	Alarm input/output port.

Table 2-2

2.5 Wiring Description

From left to right, terminal number is 1～8, as shown in Figure 2-7.

2.5.1 Wiring Description of Wiegand /RS485 Input/output

📖 Note

● This device works as a card reader, and can connect a card reader.
● It is an output device when it works as a card reader.
● It is an input device when connecting a card reader.
● Set input/output in "Main Menu > Connection > Wiegand". Please refer to the user's manual for details.
● 1 door only supports to connect one type of card reader, 485 or Wiegand.

In CON1, corresponding terminals are described in Table 2-3.

Port	No.	Mark	Cable Color	Note	
CON1(Wiega nd /RS45 8 input/o utput)	1	RD+	Red	Positive pole of power	Power output
	2	RD-	Black	Negative pole of power	
	3	CASE	Blue	Tamperproof	Wiegand input/output
	4	D1	White	Wiegand D1	
	5	D0	Green	Wiegand D0	
	6	LED	brown	Wiegand LED	
	7	B1	Yellow	RS485-	RS485 input/output
	8	A1	Purple	RS485+	

Table 2-3

Type	Connection	Length
RS485 input/output	CAT5E network cable, 485 connection	100m
Wiegand input/output	CAT5E network cable, Wiegand connection	40m

Table 2-4

2.5.2 Wiring Description of Lock, Door Sensor and Exit Button

In CON2, corresponding terminals are described in Table 2-5. Please select a proper connection depending on lock type, as shown in Figure 2-8, Figure 2-9 and Figure 2-10. Door contact and exit button connection is shown in Figure 2-11.

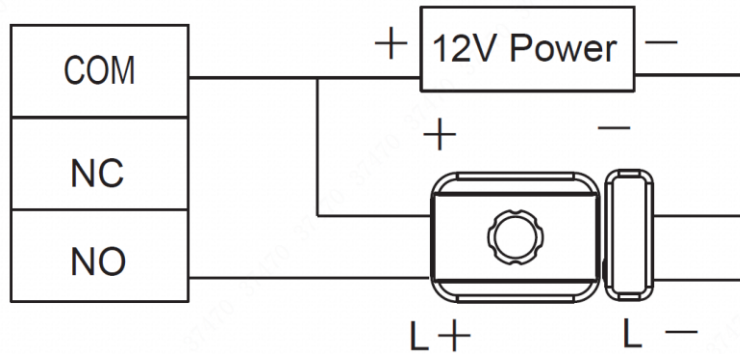| Port	No.	Mark	Note
CON2 (lock, door contact and exit button)	1	COM	Lock control output
	2	NC	
	3	NO	
	4	SR	Door sensor
	5	PUSH	Exit button
	6	GND	GND shared by door sensor and exit button
	7	RX	Reserved
	8	TX	

Table 2-5

Figure 2-8
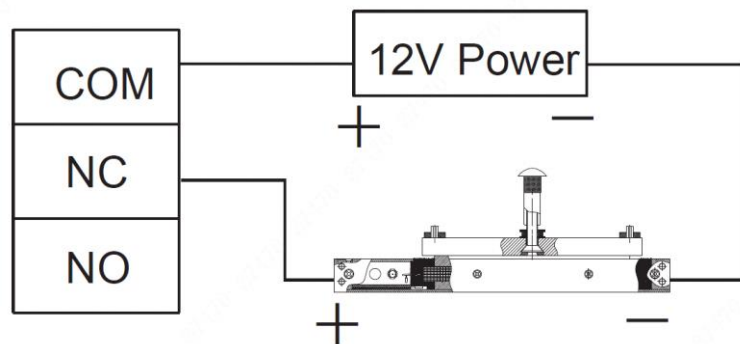
Figure 2-9
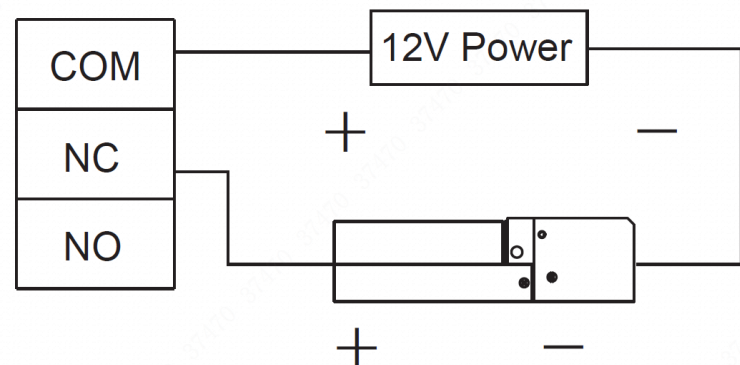
Figure 2-10
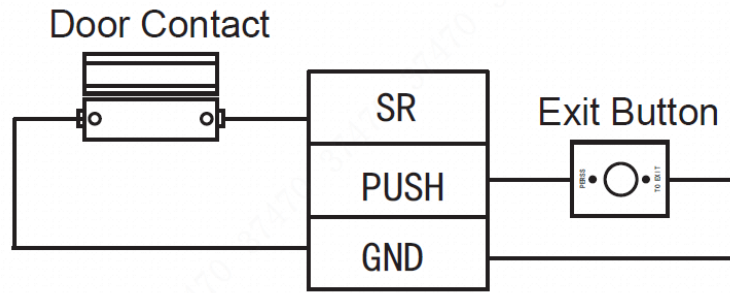
Figure 2-11

2.5.3 Wiring Description of Power and Network Port

In CON3, corresponding terminals are described in Table 2-6.

Port	No.	Mark	Note
CON3 (power and network port)	1	12V	Positive pole of power
	2	12V	
	3	ERX-	100M network port
	4	GND	Negative pole of power
	5	GND	
	6	ERX+	100M network port
	7	ETX-	
	8	ETX+	

Table 2-6

2.5.4 Wiring Description of External Alarm Input/Output

In CON4, corresponding terminals are described in Table 2-7.

Port	No.	Mark	Note	
CON4 (external alarm input/ output)	1	COM2	External alarm output 2	External alarm output port is able to connect siren etc.
	2	NO2		
	3	COM1	External alarm output 1	
	4	NO1		
	5	GND	External alarm input 2	External alarm input port is able to connect smoke detector and IR detector etc.
	6	ALM2		
	7	GND	External alarm input 1	
	8	ALM1		

Table 2-7

There are two types of external alarm output depending on alarm device. For example, IPC adopts type 1, whereas siren adopts type 2, as shown in Figure 2-12 and Figure 2-13.
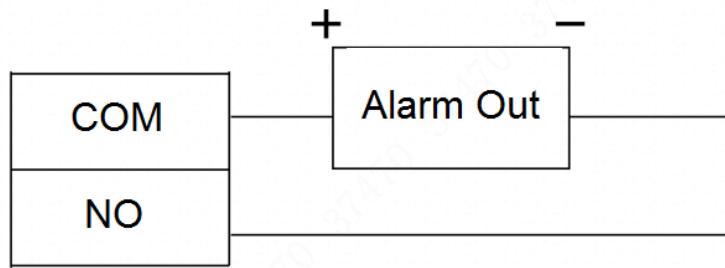
Figure 2-12
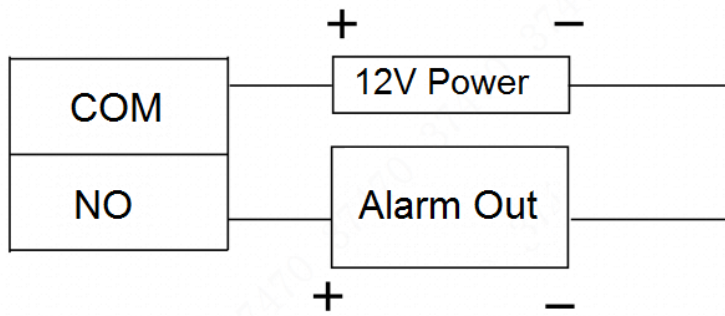
Figure 2-13

External alarm input is shown in Figure 2-14.

Figure 2-14

3 System Operation
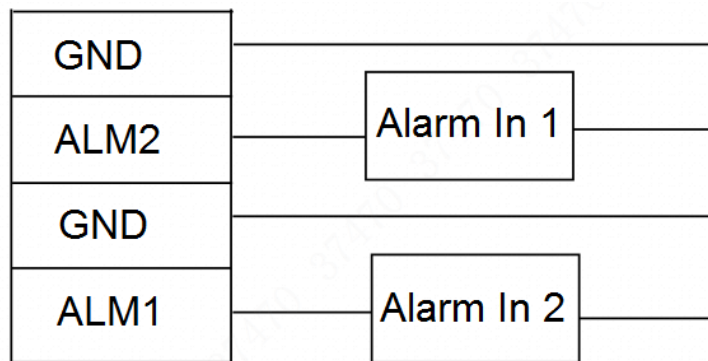
3.1 Boot up

Plug in power, and press switch button on the left to boot up the device. The device displays a white screen, and enters standby interface after 15s, as shown in Figure 3-2.

3.2 Device Initialization

Device initialization means to set admin, password and email during the first login. If the password is not set, the platform will fail to add the device.

📖 Note

- "Admin" and "Password" are only used to add the device, without admin authority in personnel management.
- If the admin password is forgotten, the password can be reset at the platform or ConfigTool through Email.
- Password can be 8 to 32 non-null characters; it consists of capital letters, small letters, numbers and symbols (except """, """, ";", ":" and "&"). The password shall consist of 2 types or over 2 types; "Input Password" and "Password Confirm" shall be the same. Please set a high-security password according to password strength prompt.

Figure 3-1

3.3 Standby Interface

Unlock the door and check attendance with face, card and password.

📖 Note

If you don't operate in one interface for over 30s, it will return to standby interface.

Date and Time   Attendance   USB   Network

Function Key   Main Menu   Password   Super Password
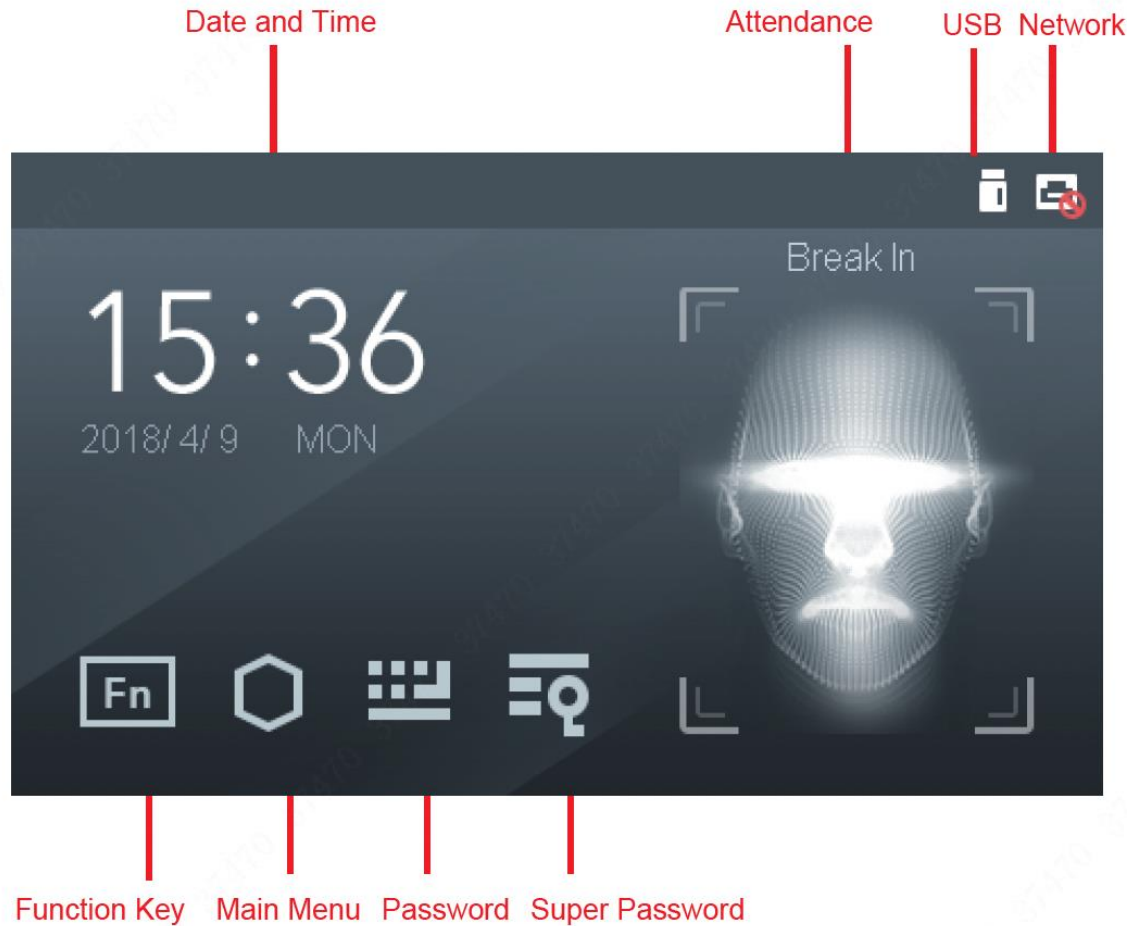
Figure 3-2

📖 Note

Customize the attendance event in "Features > Fn Key". Please refer to the user's manual for details.

3.4 Main Menu

At standby interface, press and the screen will display main menu interface, as shown in Figure 3-3.
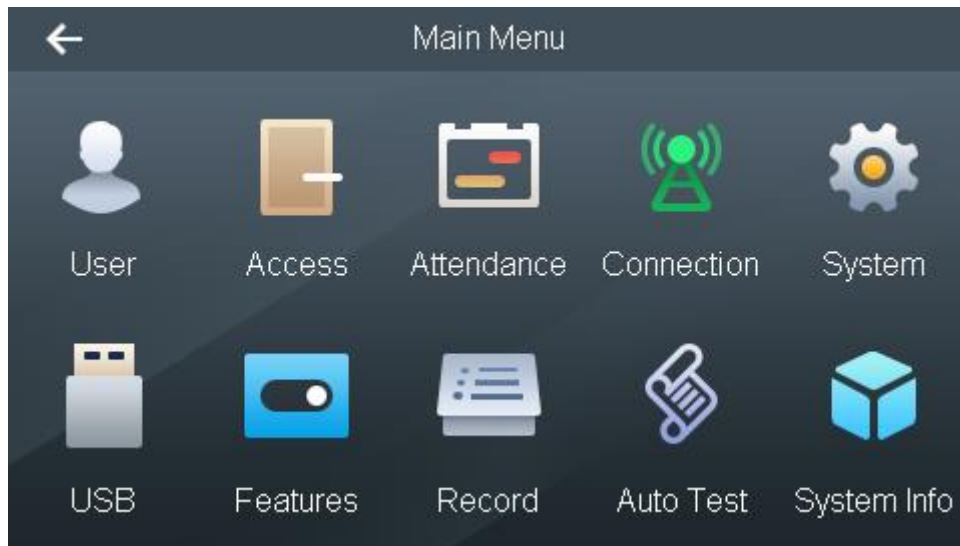
Figure 3-3

3.5 User

Add access and attendance users, customize department name and set super password.

3.5.1 New User

Add a new user, including user ID, name, fingerprint, card number, password and face, so the user can unlock or check attendance with fingerprint, card or password. The system supports max. 30,000 users.

Step 1 Select "User > New User", and the screen displays Figure 3-4.
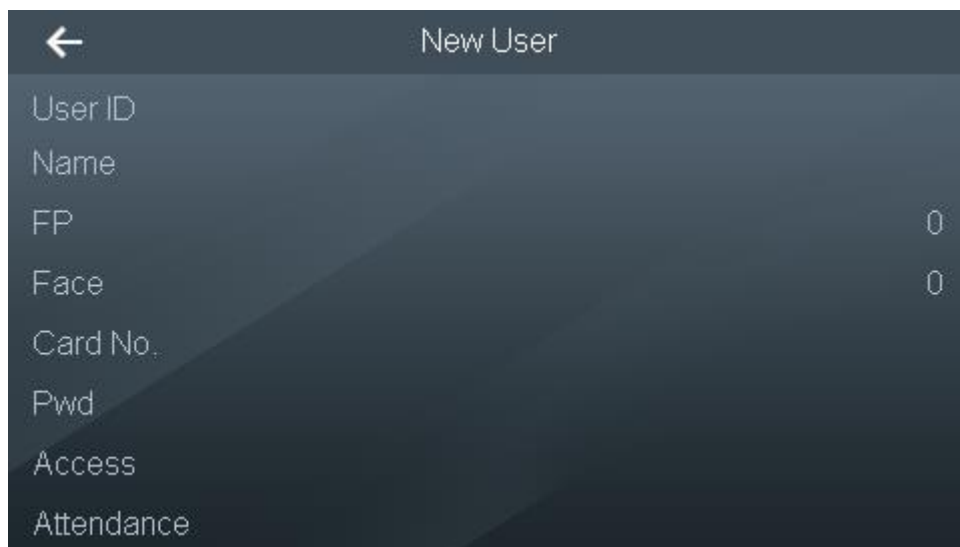
Figure 3-4

Step 2 Press corresponding parameters to enter the info, and press 🖫 to save the setting. Please refer to Table 3-1 for details.

Parameter	Note
User ID	Enter user ID, max. 8-digit number.
Name	Enter username, max. 32 characters.
FP	Collect fingerprints. One user can collect max. 3 fingerprints and every fingerprint shall be verified for 3 times. Please operate according to voice prompt. It will prompt "Registration Success" on completion. After success, pop up "Save it as Duress FP?" dialog box. After setting it to be duress fingerprint, duress alarm will be triggered if this fingerprint is used to unlock. 　　Note It is suggested that the first fingerprint should not be set to be duress fingerprint.
Face	Collect face. According to voice prompt, put your face in the frame and start registration. During registration, please move your head slowly back and forth, turn left and right within a small range. The registration process takes about 15s. Please refer to "错误!未找到引用源。 错误!未找到引用源。" for details.
Card No.	Enter card no. or put the card in card-swiping area, the system will recognize the card no. automatically.
Pwd	Enter password, supporting 1 ～8 digits of number.
Access	● Period: select preset access period. Please refer to "错误!未找到引用源。错误!未找到引用源。" for details. ● Card type: select card type. 　◇ Ordinary card 　　There is no limitation on number of times. 　◇ VIP card 　　There is no limitation on number of times. When the VIP cardholder comes in, the software platform prompts service personnel. 　◇ Guest card 　　There is limitation on number of times. This card will lose efficacy beyond the number of times. 　◇ Patrol card 　　Swipe the patrol card anytime and record card-swiping info. It cannot unlock the door successfully. 　◇ Blacklist card 　　There is no limitation on number of times. When the cardholder comes in, the background prompts service personnel. 　◇ Duress card 　　There is no limitation on number of times. It can unlock normally, but the system produces and uploads alarm info to management center. ● Number of times is only valid to guest card. ● Valid period: set the valid period of access control.

Parameter	Note

Attendance	● Photo
	Take a photo. When swiping a card, the screen displays the user's photo.
	● Department
	Users check attendance according to department shift.
	● Shift
	  ◇ Department shift: check attendance according to the shift of department where the user belongs to.
	  ◇ Personal schedule: check attendance according to personal schedule. Please refer to "错误!未找到引用源。错误!未找到引用源。" for details.
	● User Level
	📖 Note
	This authority is valid globally, not just valid to attendance management.
	  ◇ User: only have use authority.
	  ◇ Admin: login the system to configure.

Table 3-1

Step 3   After parameter configuration is completed, press ⬅.

The screen prompts "Do you want to save settings?"

Step 4   Press [Yes] to save and complete configuration.

3.5.2 User List

Search users in the system; modify and delete user info.

Select "User > User List". User info, if any, will be displayed as shown in Figure 3-5.
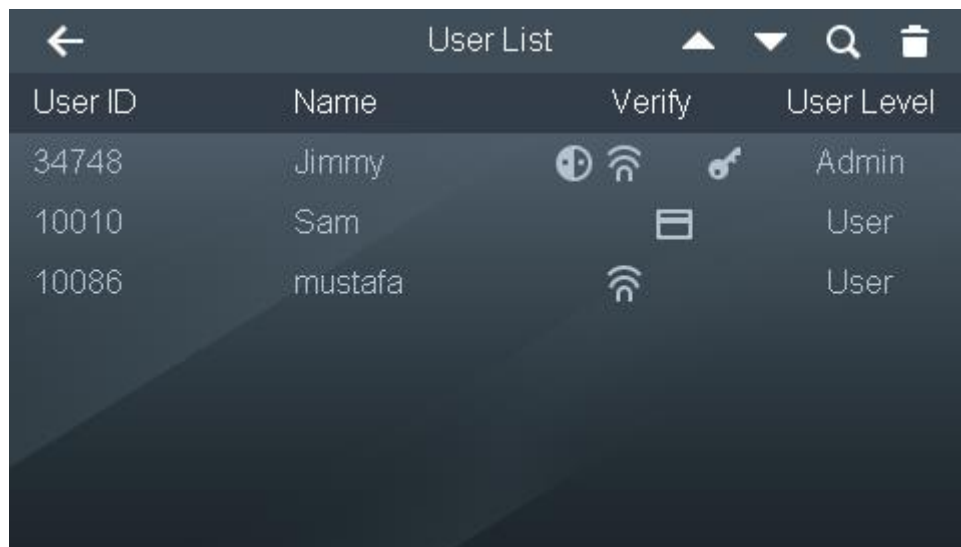
Figure 3-5

● "Icons under "Verify" represent the user's available verification mode.

  ◇ 🔵: face verification.

  ◇ 📶: fingerprint verification.

◇ ▭ : card verification.

◇ 🔑 : password verification.

● User level displays the user's level, including user and admin.

Edit User Info

Step 1 Select the line of the user to be edited.

The screen displays "Edit User Info" interface, as shown in Figure 3-6.
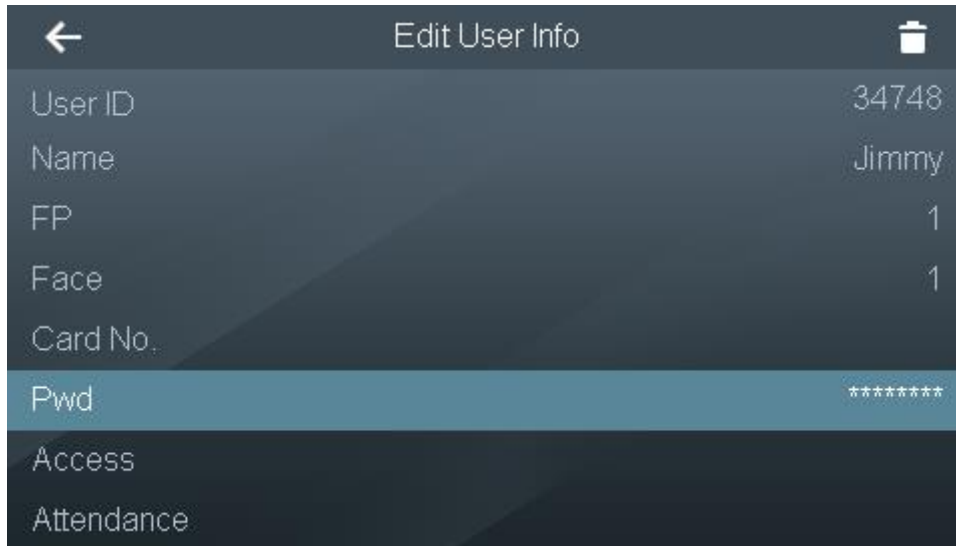
Figure 3-6

Step 2 Select a corresponding parameter to edit and modify it, and press ←.

The screen prompts "Do you want to save settings?"

Step 3 Press [Yes] to save and complete configuration.

Search User

Click 🔍, and the screen displays "Search User" interface, so as to search user info according to user ID. Select a corresponding parameter to edit and modify it.

Delete User

Select a user and click 🗑 to delete it.

📖 Note

Press ▲ and ▼ to page up and down.

3.6 Unlock Mode

Unlock mode includes any combination unlock, unlock config by period and group combination config.

3.6.1 Unlock Mode

Unlock with any one or multiple combination of card, fingerprint, face and password.

Step 1 Select "Access > Unlock Mode > Unlock Mode".

Step 2 Press up and down button to select the combination mode.

- / represents "or". For example, card/fingerprint means that the door can be unlocked with card or fingerprint.
- + represents "and". For example, card + fingerprint means that the door can be unlocked by swiping card first and then pressing the fingerprint.

Step 3 Press ![back]. The screen prompts "Do you want to save settings?"

Step 4 Press [Yes]. The system returns to "Unlock Mode" interface.

Step 5 Press the switch after "Unlock Mode" to enable.
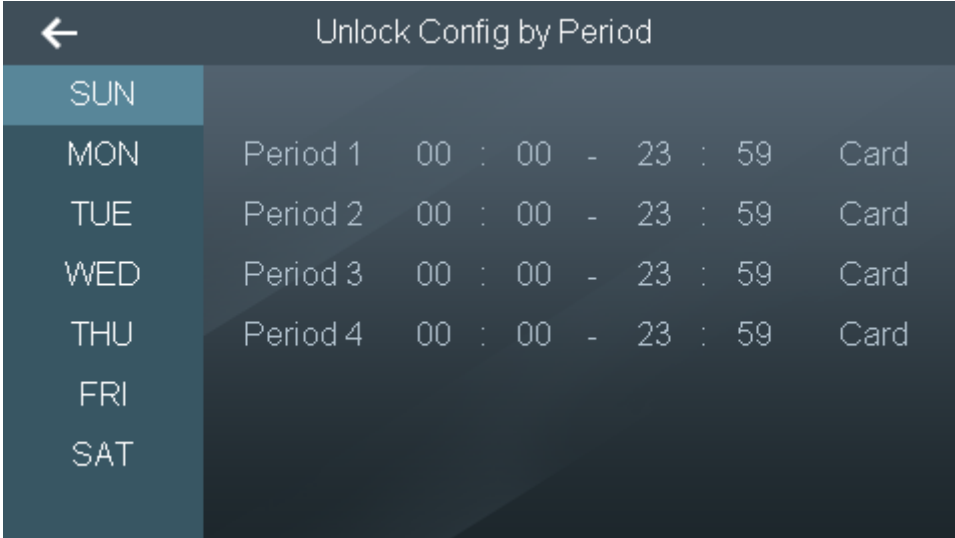
- ![ON]: enable.
- ![OFF]: disable.

3.6.2 Unlock by Period

Set different unlock modes for different periods. For example, period 1 selects unlocking by card, whereas period 2 selects unlocking by fingerprint.

Step 1 Select "Access > Unlock Mode > Unlock by Period".

The screen displays Figure 3-7。

Figure 3-7

Step 2 Press a period, set the time, and press the unlock mode to select it.

Step 3 Press ![back]. The screen prompts "Do you want to save settings?"

Step 4 Press [Yes]. The system returns to "Unlock Mode" interface.
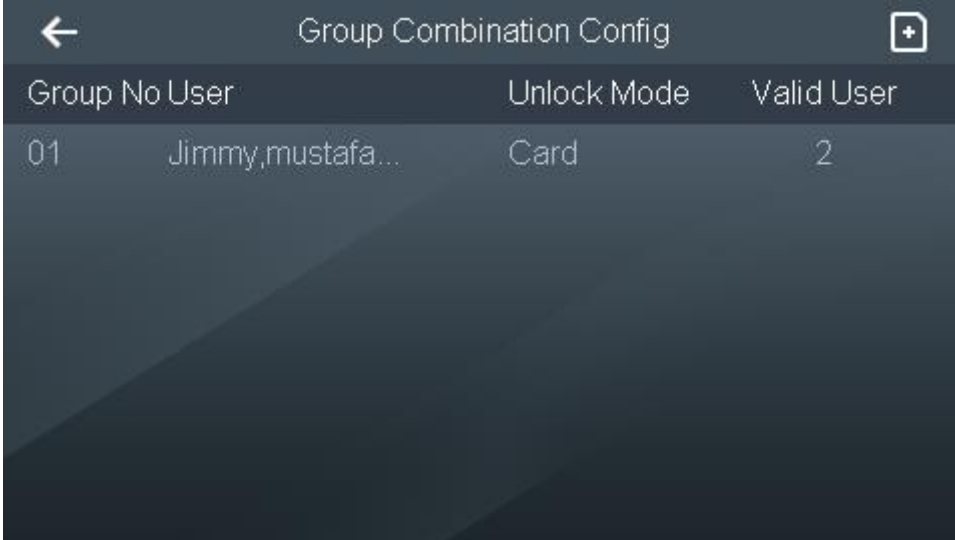Step 5 Press the switch after "Unlock by Period" to enable.

- ON ⬤ : enable.
- ⬤ OFF : disable.

3.6.3 Group Combination

Set to unlock after authorized by multiple users or user groups.
Step 1 Select "Access > Unlock Mode > Group Combination".
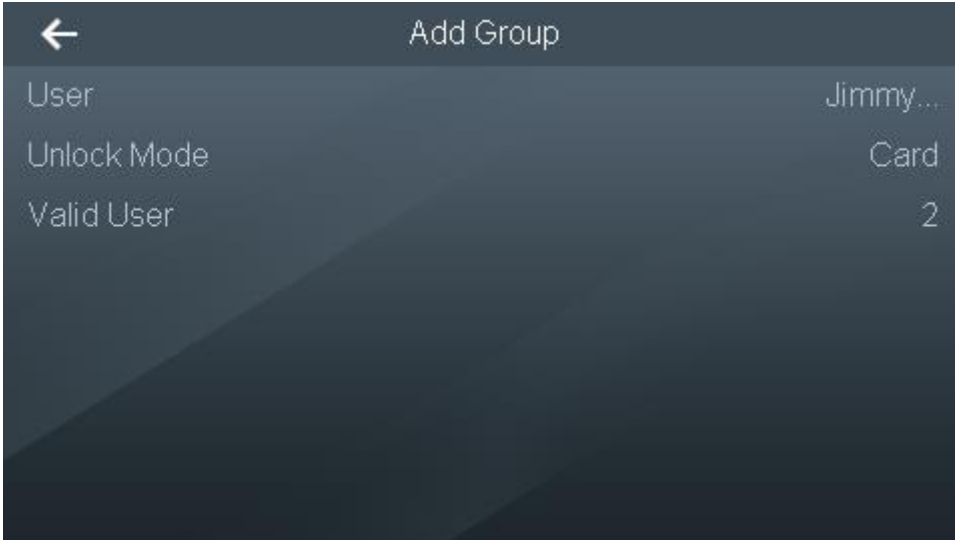
The screen displays Figure 3-8.

Figure 3-8

Step 2 Press [+] to add a group. Please refer to Table 3-2 for details.

The screen displays Figure 3-9.

Figure 3-9

Parameter	Note

Parameter	Note
User	Add users to the new group. 1. Press [User]. 2. Press [icon] in the pop-up interface. 3. Press [icon] to enter user ID. Repeat Step 2~ Step 3 and continue to add users. Max. 50 users can be added. 4. Press [icon], and press [Yes] to save according to interface prompt.
Unlock Mode	Select unlock mode, including card, fingerprint, password and face. 5. Press [Unlock Mode] to select the mode. 6. Press [icon], and press [Yes] to save according to interface prompt.
Valid User	The door can be unlocked after valid users unlock. ● Valid user cannot be greater than total number of user. ● When valid user equals to total number of user, the door can be unlocked after all members of the group unlock. ● When valid user is less than total number of user, the door can be unlocked after any members of the group reach valid user.

Table 3-2

Step 3 Press [icon]. The screen prompts "Do you want to save settings?"

Step 4 Press [Yes] to complete group combination config.

3.7 Lock Holding Time

After a card is swiped, the lock is kept open for some time and is closed automatically after the time. The unit is second.

Step 1 Select "Features > Lock Holding Time", and the screen displays Figure 3-10.
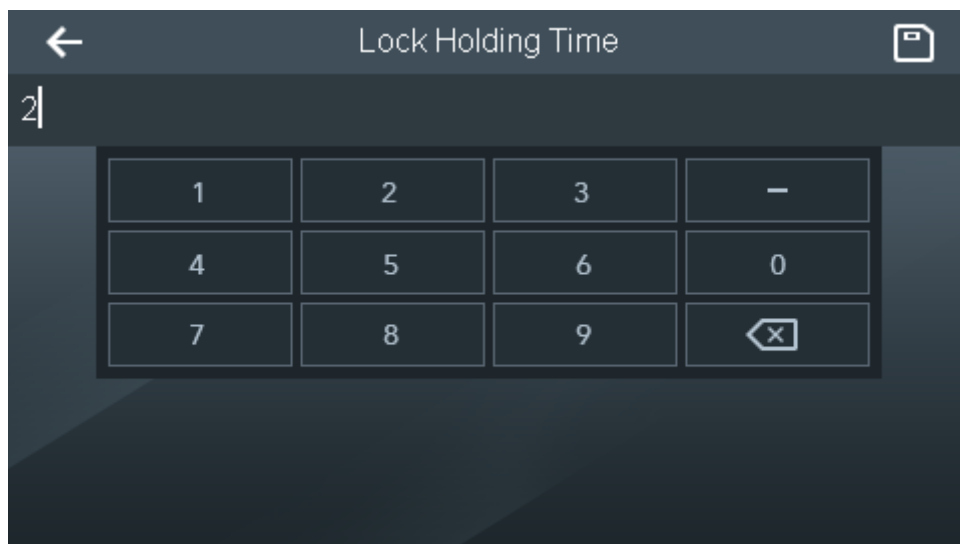
Figure 3-10

Step 2 Enter "Lock Holding Time" and press ⊡ to save the setting.

3.8 Network Configuration

Step 1 Select "Connection > Network Configuration", and the screen displays Figure 3-11.

Figure 3-11

Step 2 Select adding mode according to actual situation.
- IP Address
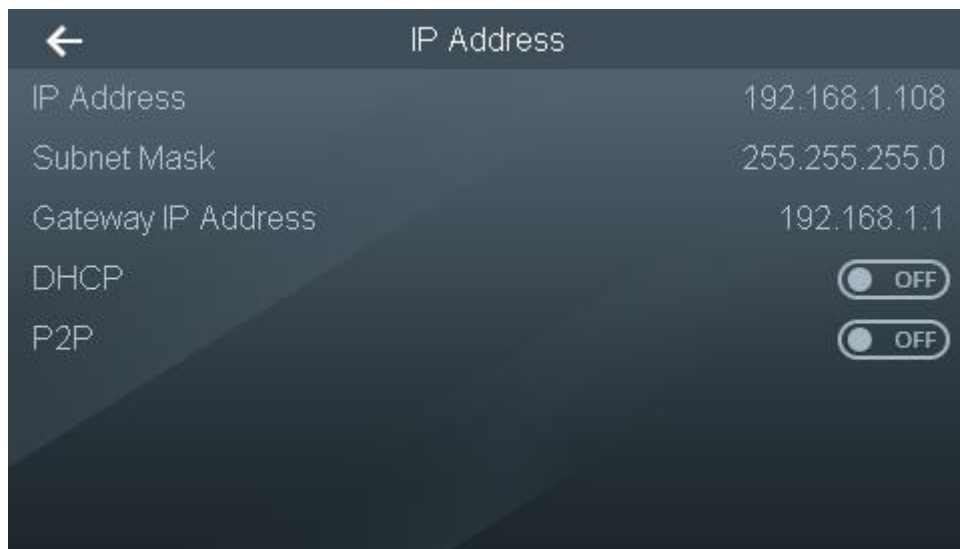1) Select "IP Address", and the screen displays Figure 3-12.

Figure 3-12

2) According to actual situation, configure parameters by reference to Table 3-3.

Parameter	Note

Parameter	Note
IP Address, Subnet Mask and Gateway IP Address	Set device IP address, subnet mask and gateway, ensure that IP address and gateway are in the same network segment, and press to save.
Enable/Disable DHCP	DHCP: Dynamic Host Configuration Protocol. Enable DHCP function and obtain IP address automatically. Then, "IP Address", "Subnet Mask" and "Gateway IP Address" cannot be set.
Enable/Disable P2P	During use, it is unnecessary to apply for dynamic domain name, carry out port mapping or deploy transit server, so as to manage the device easily and conveniently.

Table 3-3

3)   Press to save the setting.

●   Active registration is a reserved function.