

Face Recognition Access and Time Attendance Terminal

User's Manual

V1.0.0

Cybersecurity Recommendations

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.






Foreword

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.

Important Safeguards and Warnings

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

Cybersecurity Recommendations	II
Foreword	V
Important Safeguards and Warnings	VII
1 Product Overview	1
1.1 Functional Features.....	1
1.2 External Dimension.....	2
2 Installation Guide	3
2.1 Packing List.....	3
2.2 System Architecture.....	3
2.3 Installation	4
2.4 Panel and Port.....	5
2.5 Wiring Description.....	7
2.5.1 Wiring Description of Wiegand /RS485 Input/output	7
2.5.2 Wiring Description of Lock, Door Sensor and Exit Button	7
2.5.3 Wiring Description of Power and Network Port	9
2.5.4 Wiring Description of External Alarm Input/Output.....	9
3 System Operation	11
3.1 Boot up	11
3.2 Device Initialization	11
3.3 Standby Interface.....	12
3.4 Main Menu	13
3.5 User.....	13
3.5.1 New User.....	13
3.5.2 User List.....	16
3.5.3 Department List.....	17
3.5.4 Super Password.....	18
3.6 Access	20
3.6.1 Period Management	20
3.6.2 Unlock Mode	24
3.6.3 Alarm.....	26
3.6.4 Door Status	27
3.7 Attendance	28
3.7.1 Shift	28
3.7.2 Schedule.....	31
3.7.3 Verification Interval Time.....	33
3.8 System.....	34
3.8.1 Time.....	34
3.8.2 Face Parameter.....	35
3.8.3 Infrared LED Set.....	36
3.8.4 Volume.....	36
3.8.5 Face Detection Trigger Mode.....	37

3.8.6 Restore Factory	37
3.8.7 Reboot	38
3.9 Connection	38
3.9.1 Network Configuration	38
3.9.2 Serial Port	39
3.9.3 Wiegand	39
3.9.4 Wi-Fi	40
3.10 Features	40
3.10.1 User Photo	41
3.10.2 FP Image	41
3.10.3 Attendance Events	41
3.10.4 Fn Key Definition	42
3.10.5 Bell	43
3.10.6 Lock Holding Time	44
3.10.7 Face Recognition Period	45
3.11 Record	45
3.11.1 Search Card Punch	45
3.11.2 Search Alarm Record	46
3.11.3 Search Admin Record	46
3.11.4 Export 1 Month Attendance Report	47
3.11.5 Export 1 Month Exception Report	48
3.12 USB	49
3.12.1 USB Export	49
3.12.2 USB Import	49
3.12.3 USB Update	50
3.13 Auto Test	51
3.13.1 Screen	51
3.13.2 Voice	51
3.13.3 Button	52
3.13.4 FP	52
3.13.5 Face	53
3.13.6 Clock	53
3.13.7 Auto Test	53
3.14 System Info	53
3.14.1 View Data Capacity	54
3.14.2 View Device Version	55
3.14.3 View Firmware Info	55
4 Technical Parameters	56
5 FAQ	57
1 The device fails to boot up after power-on	57
2 The device fails to recognize face after boot-up.	57
3 The device and third-party controller connect Wiegand port, but no signal is output.....	57
4 Forget admin and fail to set.	57
5 User info, fingerprint and face import error.	57
6 The user's face is recognized to be another user.	57
Appendix 1 Fingerprint Operation	58
Appendix 2 Face Registration Instruction	60

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 ≤ 1 s.
- 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: $-5^{\circ}\text{C} \sim +55^{\circ}\text{C}$, operating humidity: $\leq 95\%$.



Caution

To connect external power source, please use DC12V 2A power adapter and ensure that operating temperature is within $-5^{\circ}\text{C} \sim +55^{\circ}\text{C}$.

1.2 External Dimension

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

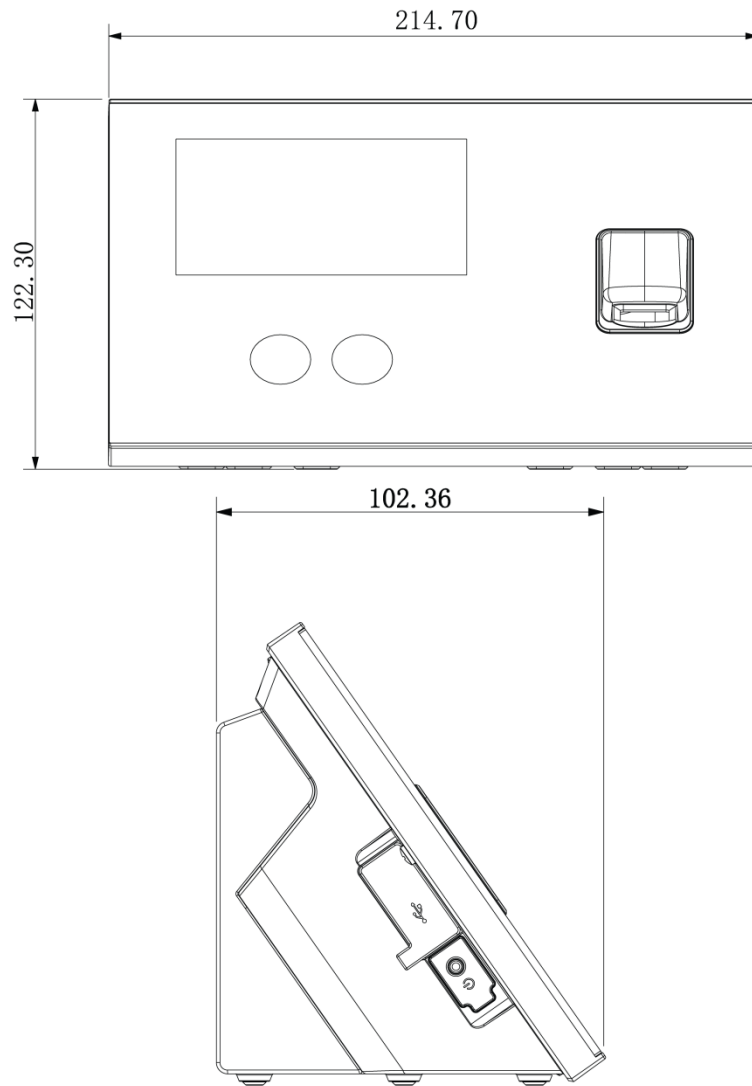


Figure 1-1

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 <ul style="list-style-type: none"> ● 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.

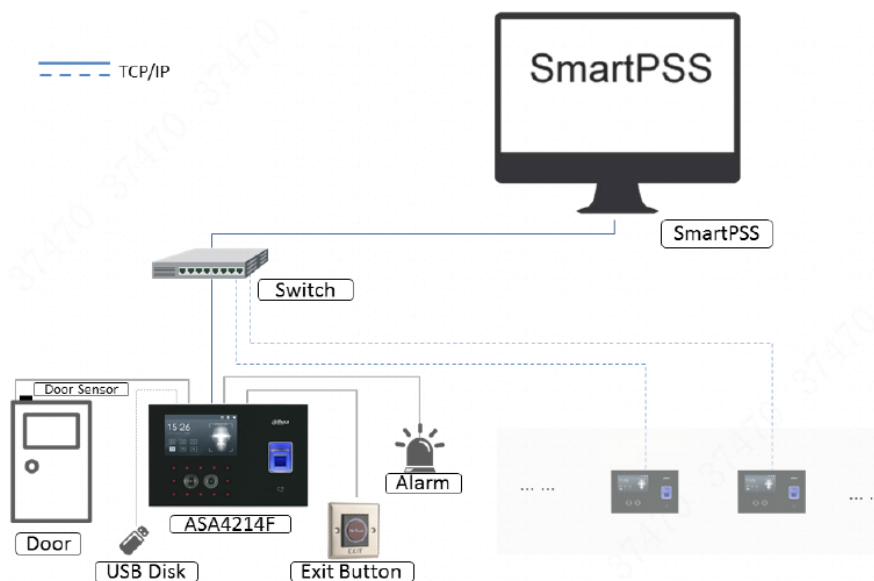


Figure 2-1

2.3 Installation

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

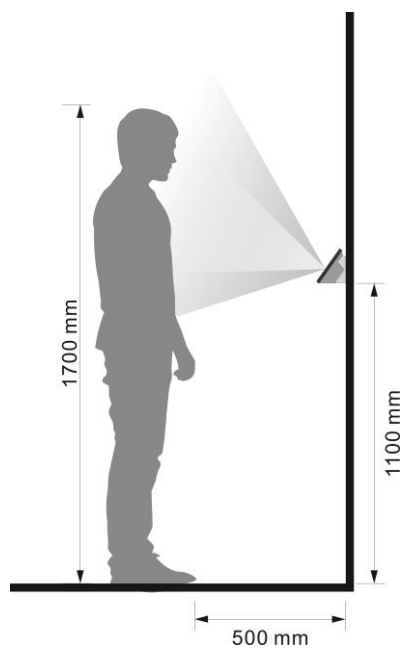


Figure 2-2

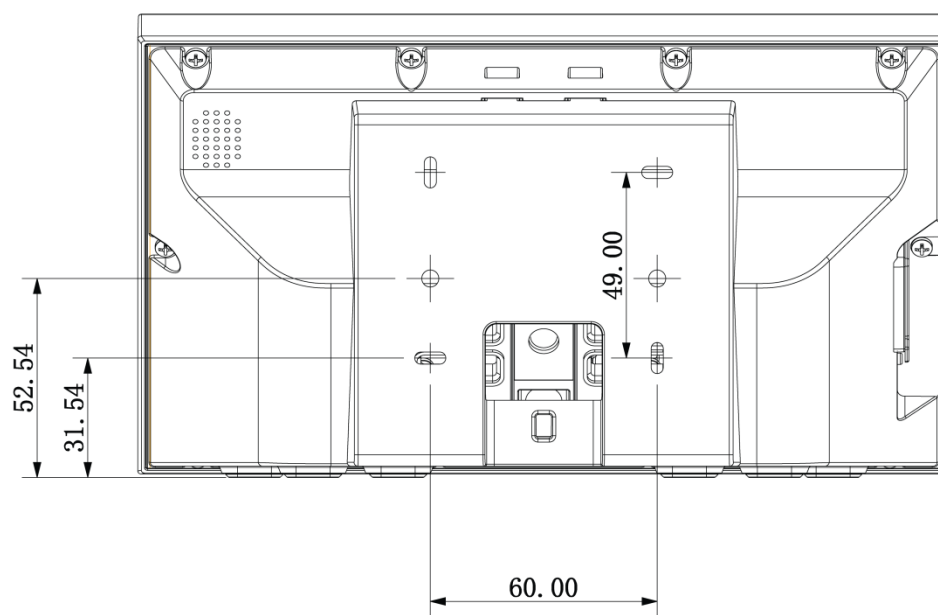


Figure 2-3

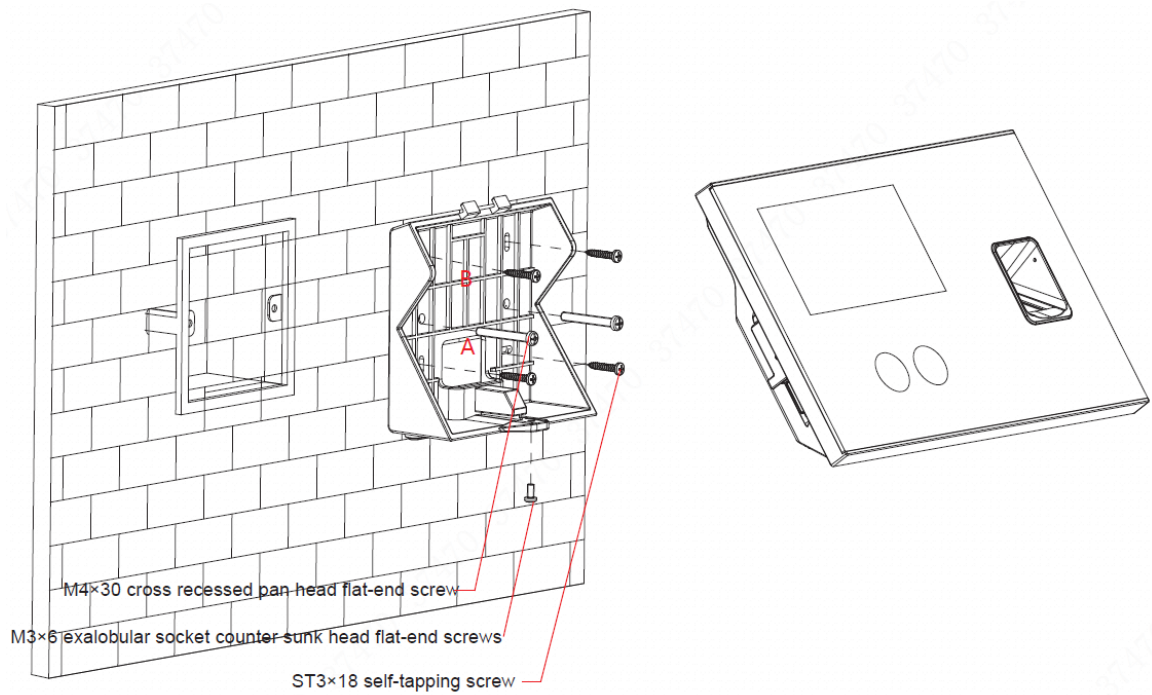


Figure 2-4

- 步骤1 Drill holes according to the positions in Figure 2-3, and install expansion pipes into holes.
- 步骤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.
- 步骤3 Hang the device onto the hook of the bracket.
- 步骤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.

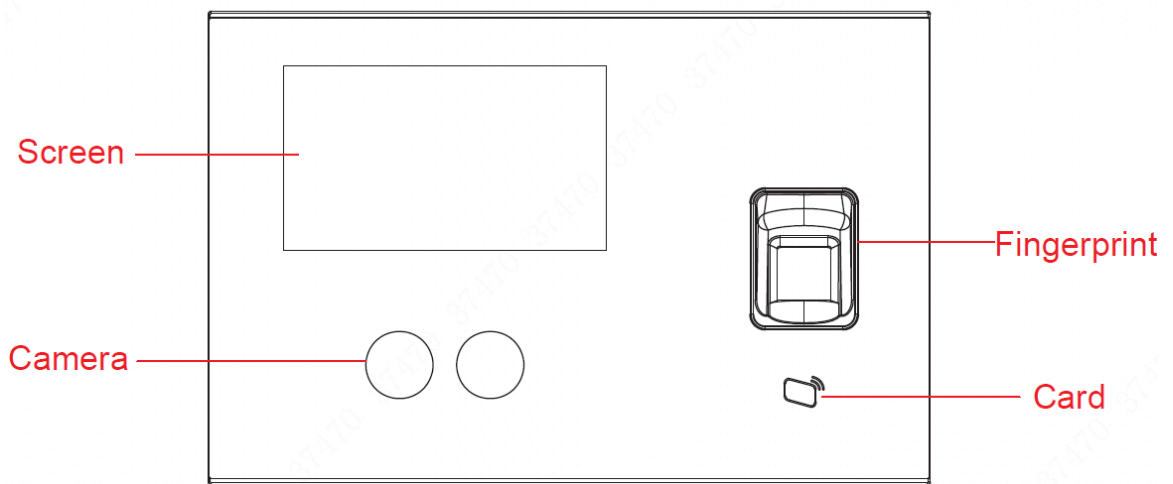


Figure 2-5

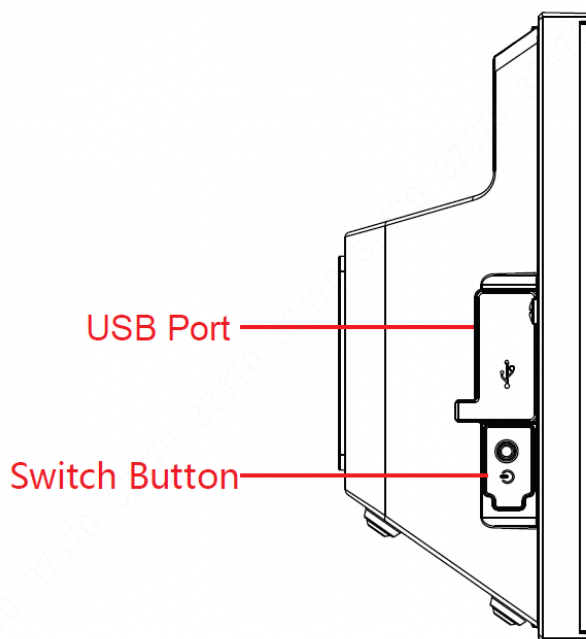


Figure 2-6

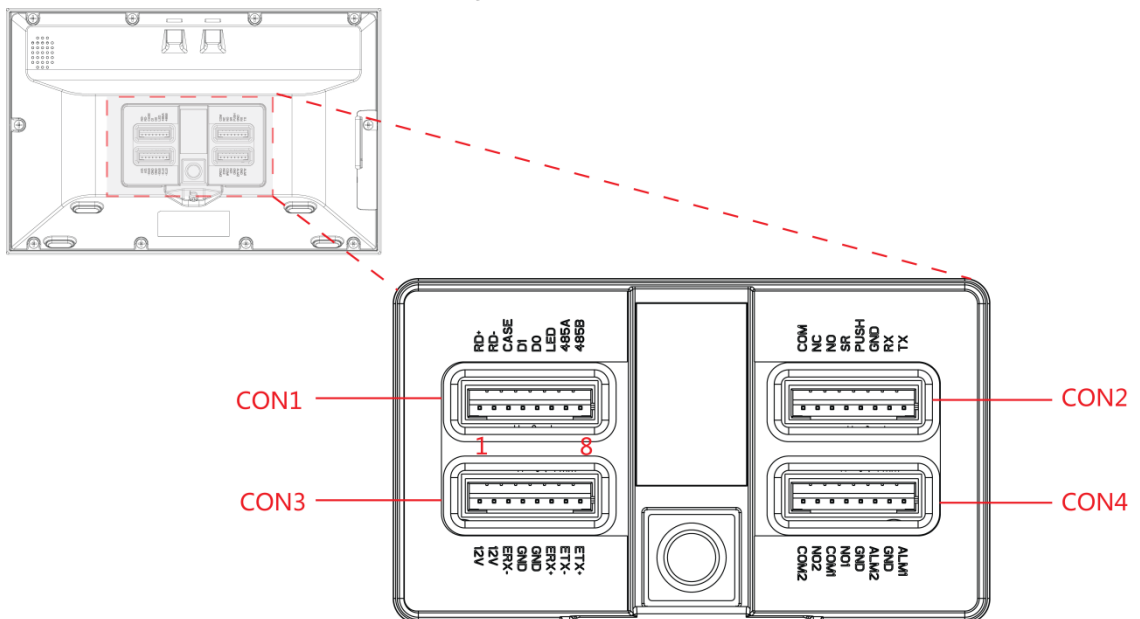


Figure 2-7

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 “3.9.3 Wiegand” 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 (Wieg and /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

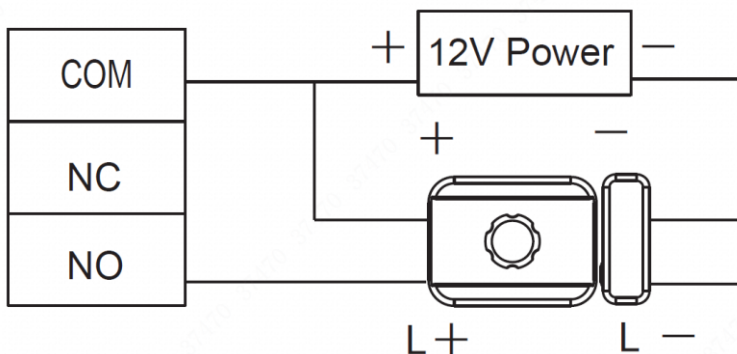


Figure 2-8

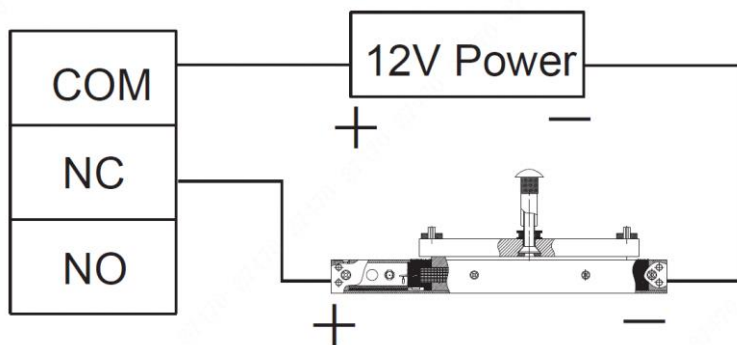


Figure 2-9

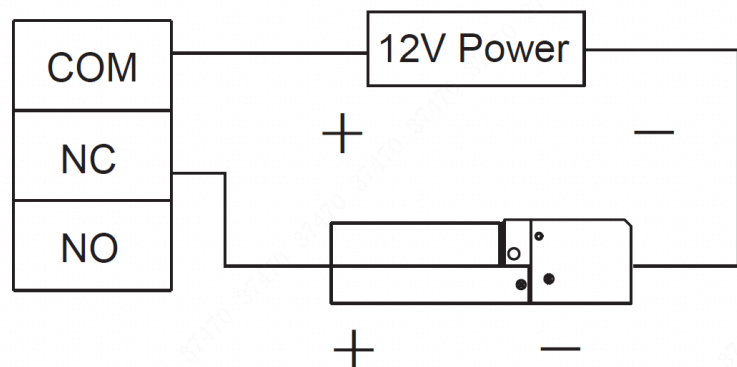


Figure 2-10

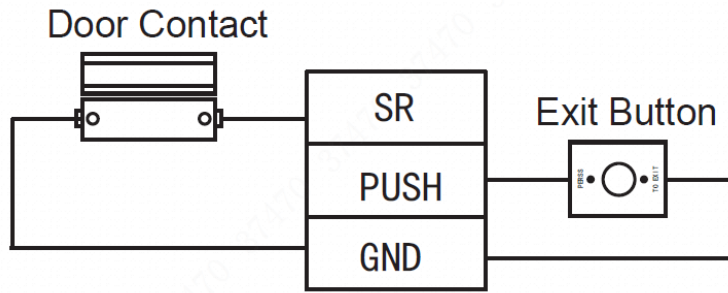


Figure 2-11

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
	2	NO2	
	3	COM1	External alarm output 1
	4	NO1	
	5	GND	External alarm input 2
	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.

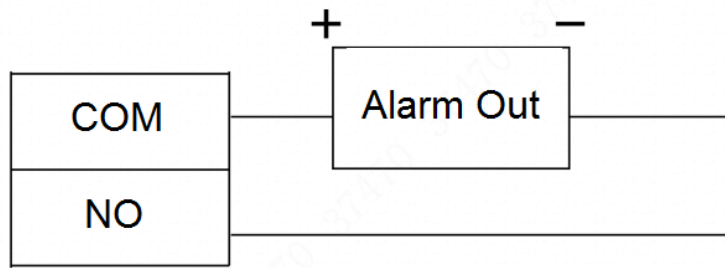


Figure 2-12

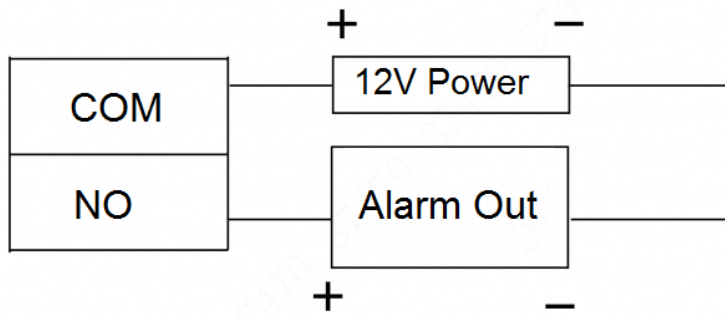


Figure 2-13

External alarm input is shown in Figure 2-14.

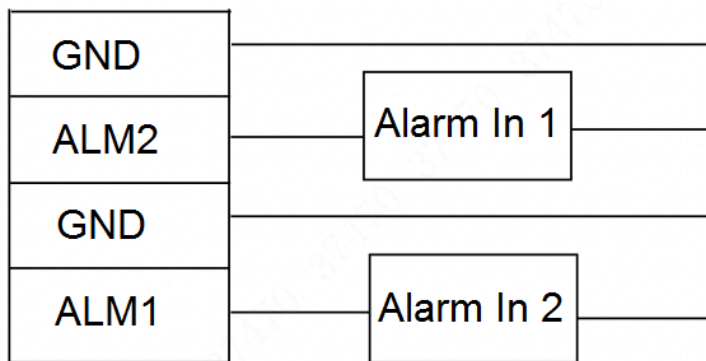


Figure 2-14

3 System Operation

Note

- The operation involves fingerprint registration. For specific pressing method, please refer to “附录 1 Fingerprint ”.
- The operation involves input method. For specific input method, please refer to “附录 2 Face Registration Instruction”.

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.

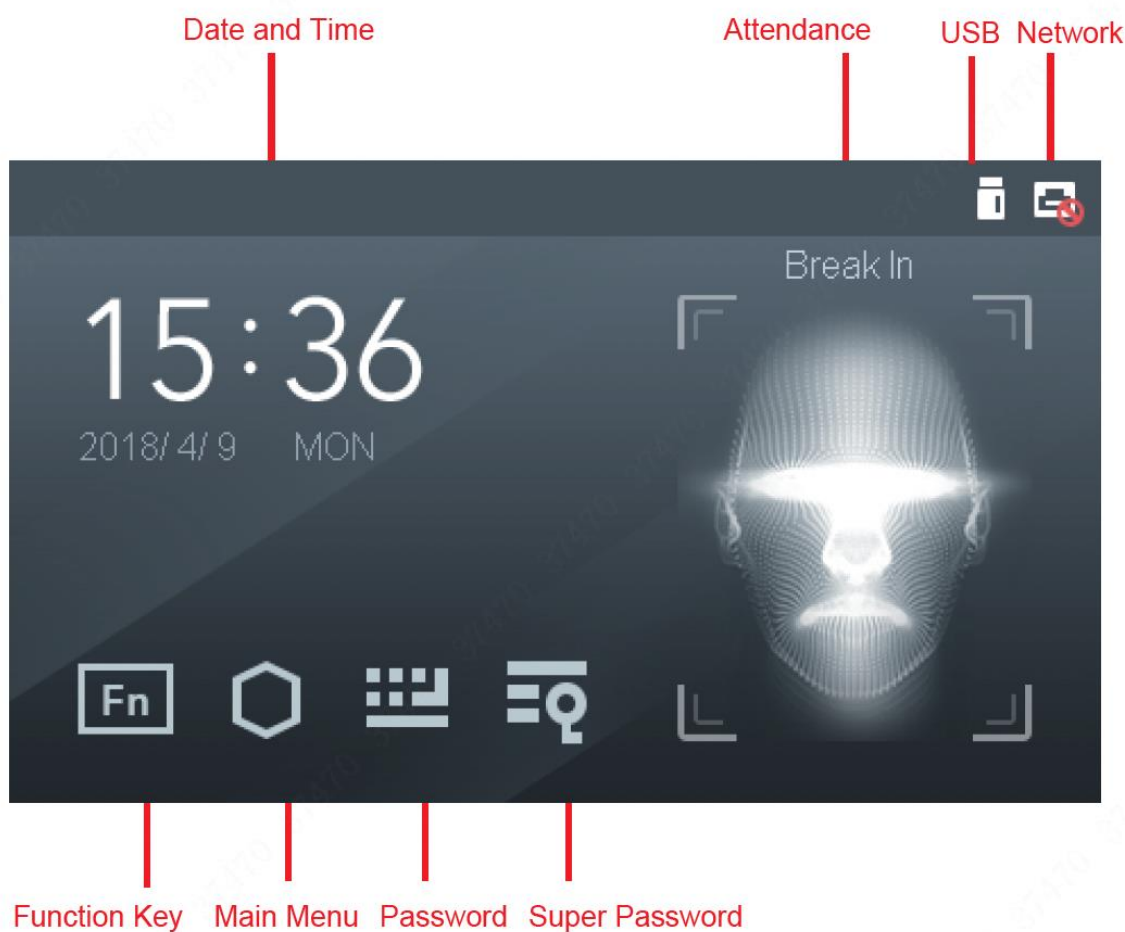



Figure 3-2



Customize the attendance event in “Features > Fn Key”. Please refer to “3.10 Features” for details.

3.4 Main Menu

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

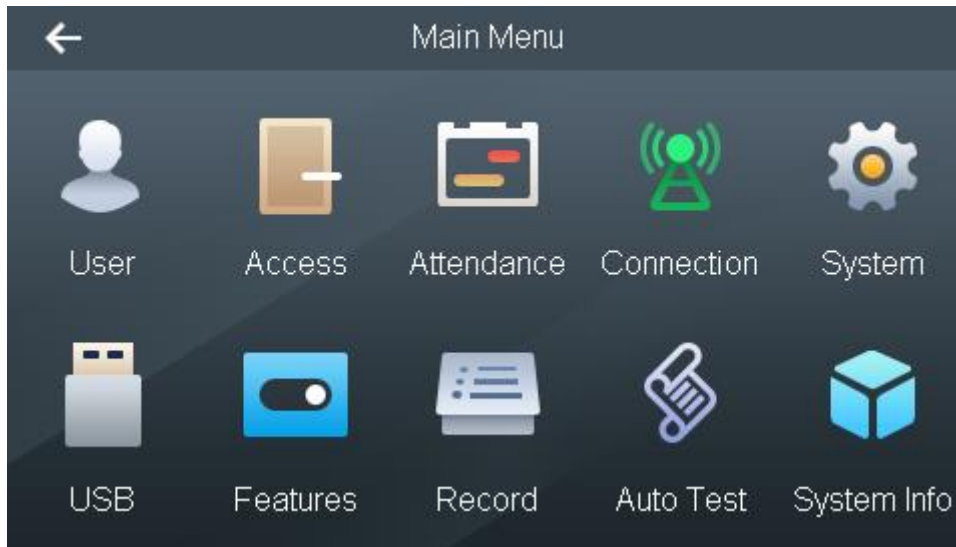


Figure 3-3

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.

步骤1 Select “User > New User”, and the screen displays Figure 3-4.

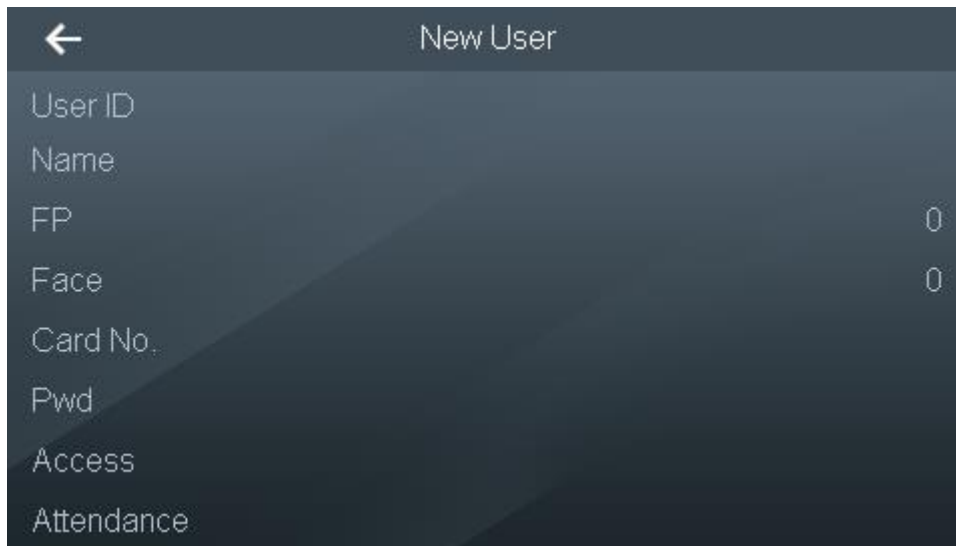




Figure 3-4

步骤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	<p>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 “Added Successfully” on completion.</p> <p>After success, pop up “Set to be duress fingerprint?” dialog box. After setting it to be duress fingerprint, duress alarm will be triggered if this fingerprint is used to unlock.</p> <p> Note</p> <p>It is suggested that the first fingerprint should not be set to be duress fingerprint.</p>
Face	<p>Collect face. According to voice prompt, put your face in the frame and start registration.</p> <p>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 “附录 2 Face Registration Instruction” for details.</p>
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.


Parameter	Note
Access	<ul style="list-style-type: none"> ● Period: select preset access period. Please refer to “3.6.1 Period” for details. ● Card type: select card type. <ul style="list-style-type: none"> ◇ 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.
Attendance	<ul style="list-style-type: none"> ● Photo Take a photo. When swiping a card, the screen displays the user’s photo. ● Department Users check attendance according to department shift. ● Shift <ul style="list-style-type: none"> ◇ 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 “3.7.2.1 Personal Schedule” for details. ● User Level <ul style="list-style-type: none"> ◇ User: only have use authority. ◇ Admin: login the system to configure. <p> Note</p> <p>This authority is valid globally, not just valid to attendance management.</p>

Table 3-1

步骤3 After parameter configuration is completed, press .

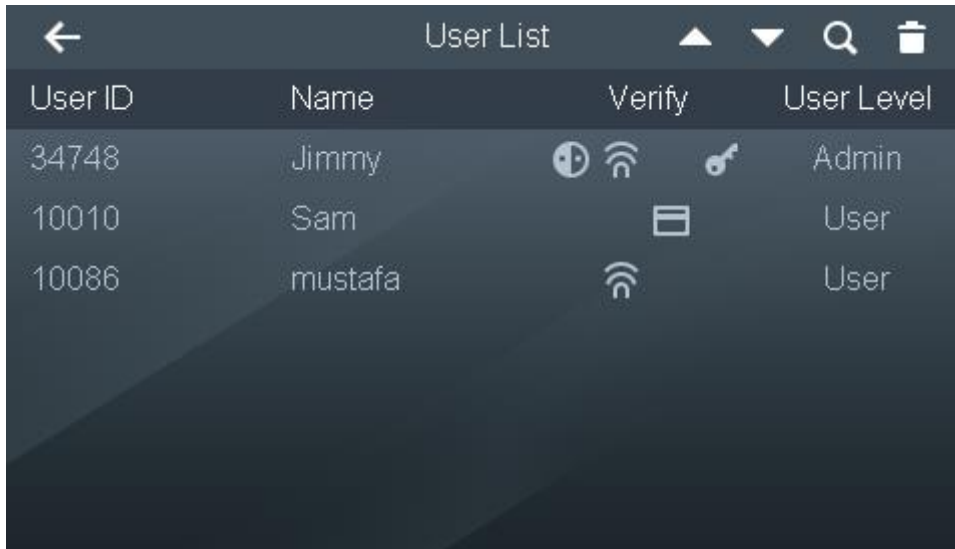
The screen prompts “Do you want to save settings?”

步骤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.



User ID	Name	Verify	User Level
34748	Jimmy	Face verification, Fingerprint verification, Password verification	Admin
10010	Sam	Card verification	User
10086	mustafa	Fingerprint verification	User

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

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

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

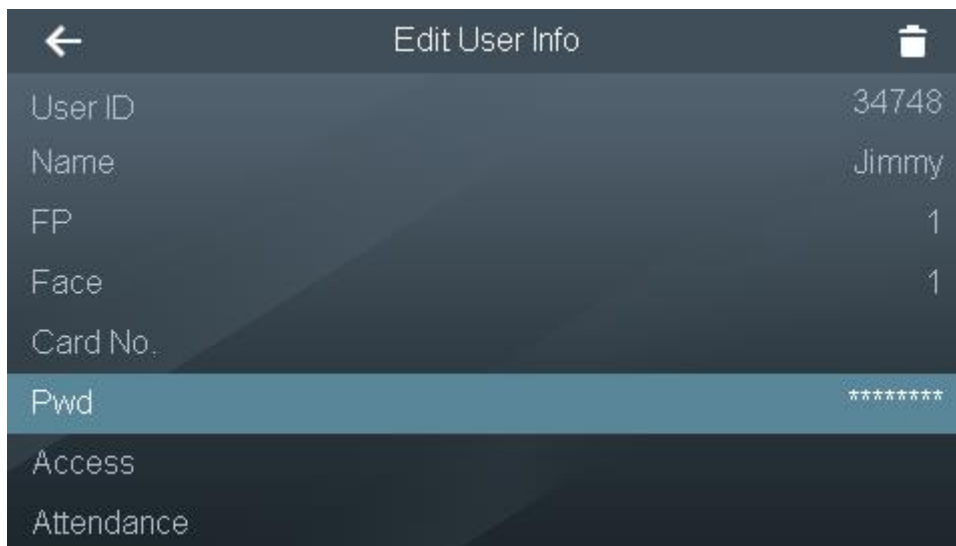



Figure 3-6

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

The screen prompts “Do you want to save settings?”

步骤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.

3.5.3 Department List

The system supports max. 20 departments. Modify department name according to needs.

步骤1 Select “User > Dept. List”, and the screen displays Figure 3-7.

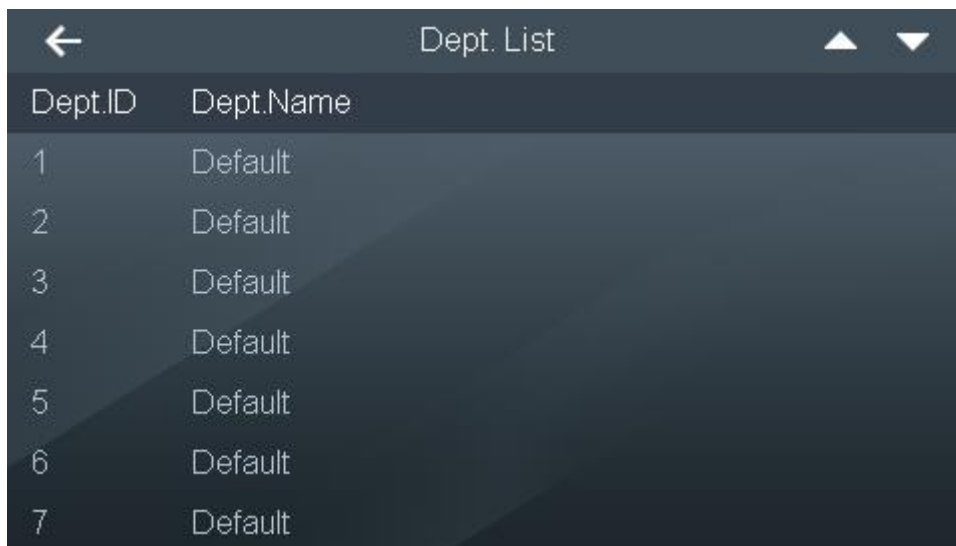




Figure 3-7

步骤2 Select a corresponding department, modify department name and press  to save.

步骤3 Click  to return to user interface and complete modification.

3.5.4 Super Password

When super password is used, it is unnecessary to enter user ID; it won't be limited by the user or any access authority. It is suggested that only one super password should be set for one device.

步骤1 Select "User > Super Pwd", and the screen displays Figure 3-8.

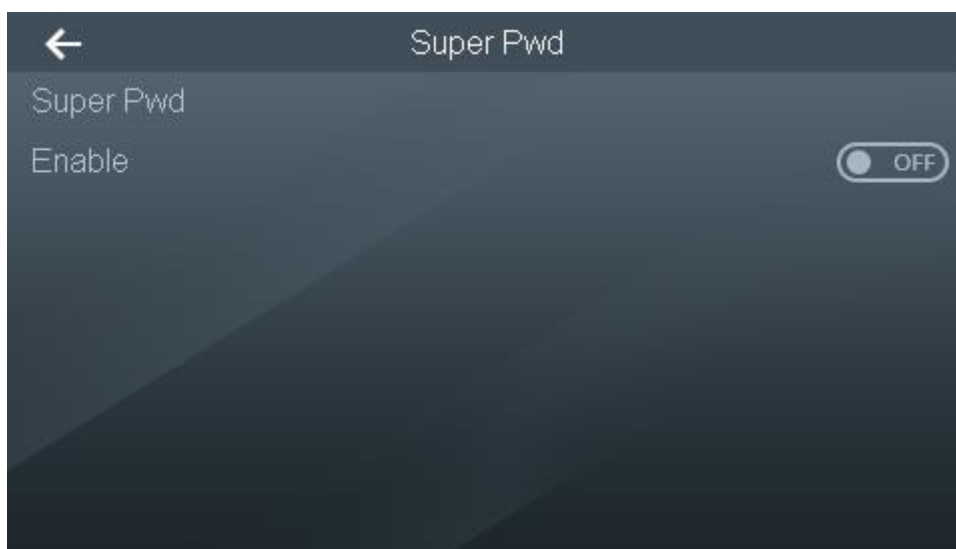


Figure 3-8

步骤2 Press "Super Pwd", and the screen displays Figure 3-9.

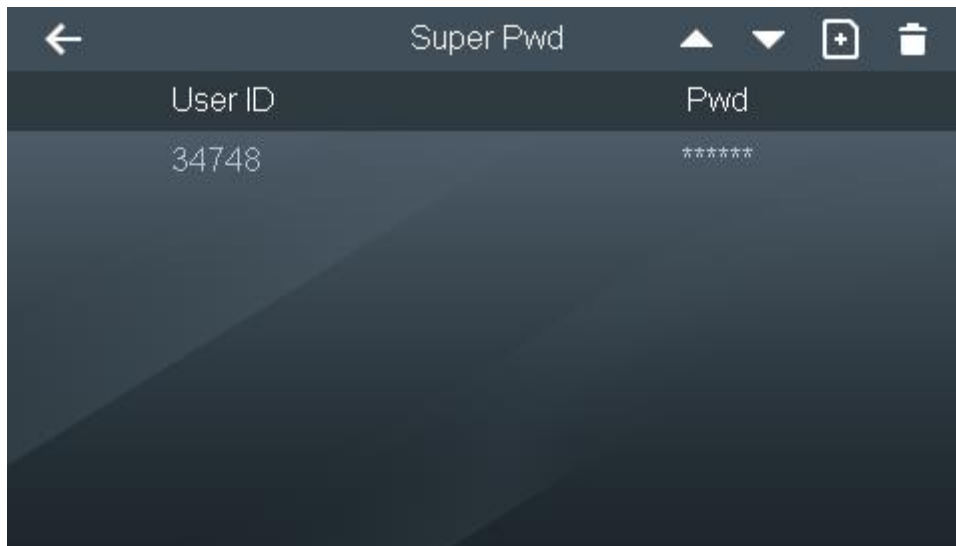



Figure 3-9

步驟3 Click , and the screen displays Figure 3-10.

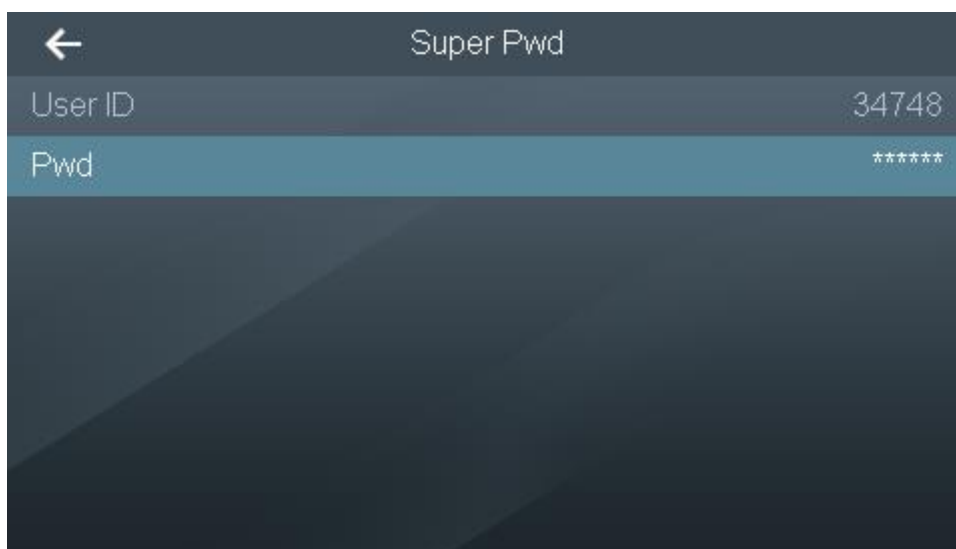




Figure 3-10

步驟4 Press [User ID] to enter the added user ID with 1 ~ 8 digits, and press  to save user ID.

步驟5 Press [Pwd] to enter super password, and press  to save password.

步驟6 Press . The screen prompts “Do you want to save settings?”

步驟7 Press [Yes] to complete setting the super password. Return to Figure 3-8.

步驟8 Press the switch after “Enable”, and enable super password.

- : enable.
- : disable.

3.6 Access

Manage the door by period, set unlock mode, alarm and status.

3.6.1 Period Management

Set unlock period, including card period, holiday period, mode period and normally open (NO) period.

3.6.1.1 Period Config

The system supports a total of 128 periods ranging from 0 to 127. In every period, set daily timetable from Sunday to Saturday; support to configure 4 periods every day.

During unlocking, the access judges whether the present time is within a period value. The system only supports to enable access control within the set period; it is invalid in other time.

步骤1 Select “Access > Period Management> Period Config”, and the screen displays Figure 3-11.

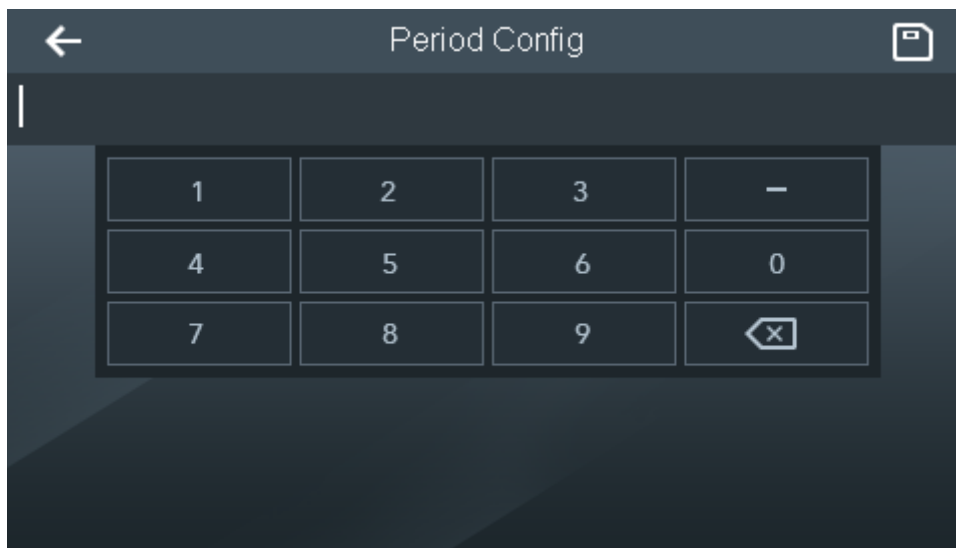



Figure 3-11

步骤2 Enter any number from 0 to 127 as period number and click . The screen displays Figure 3-12.

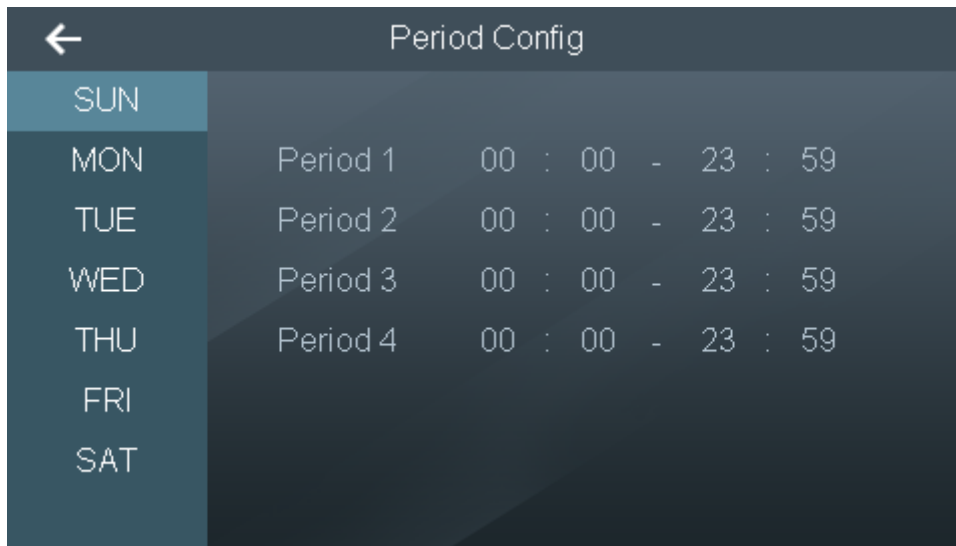




Figure 3-12

- 步骤3 Select the week, press period, enter start time and end time, and press  to save.
- 步骤4 Configure other periods and press . The screen prompts “Do you want to save settings?”
- 步骤5 Press [Yes] to complete period configuration.

3.6.1.2 Holiday Config

The system supports a total of 128 holidays ranging from 0 to 127. All holidays can be managed together. Enable access control within the set period of holiday; it is invalid in other time.

- 步骤1 Select “Access > Period Management> Holiday Config”, and the screen displays Figure 3-13.

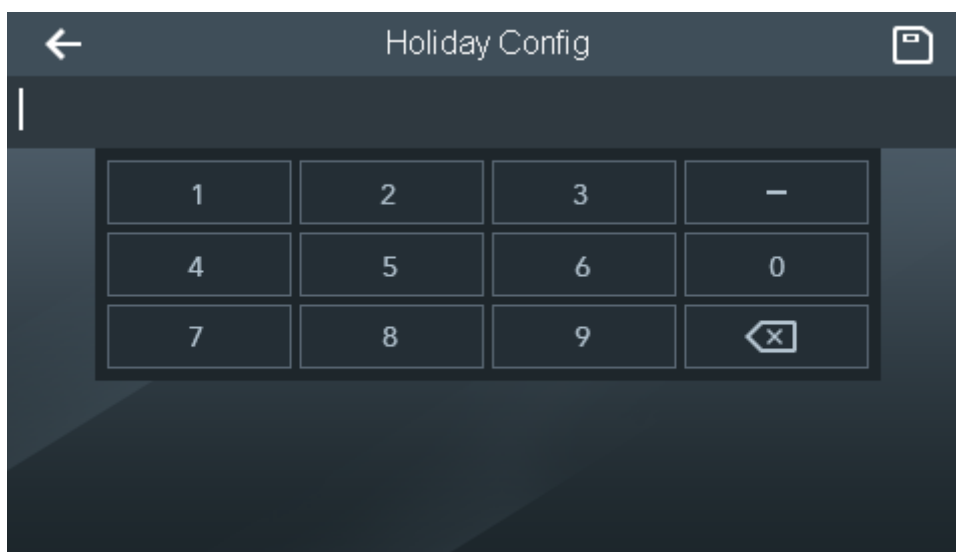


Figure 3-13

- 步骤2 Enter holiday number and click , and the screen displays Figure 3-14.

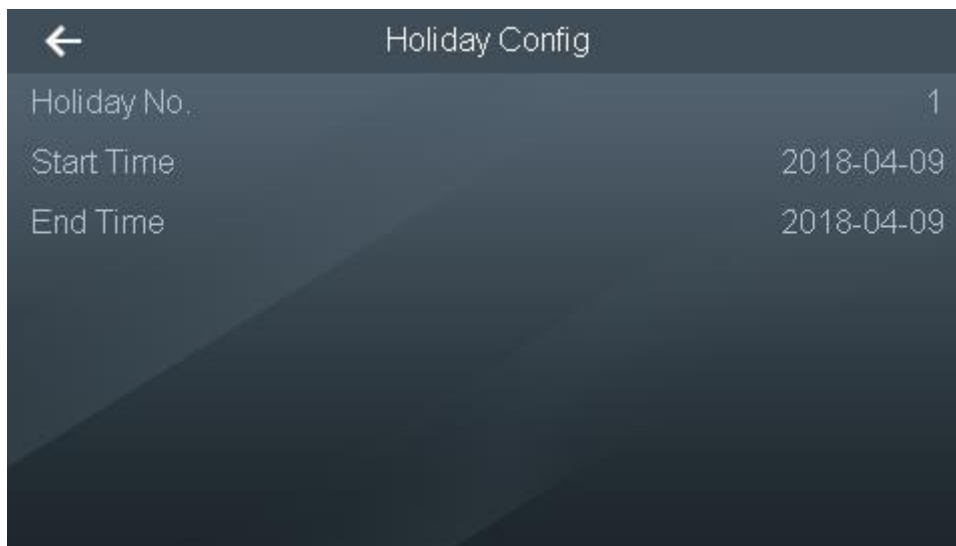



Figure 3-14

步骤3 Enter “Start Time” and “End Time”, and press . The screen prompts “Do you want to save settings?”

步骤4 Press [Yes] to complete holiday configuration.

3.6.1.3 Holiday Period

Bond holiday with period. Enable access control according to the selected period during holiday; it is invalid in other time.

步骤1 Select “Access > Period Management> Holiday Period”, and the screen displays Figure 3-15.

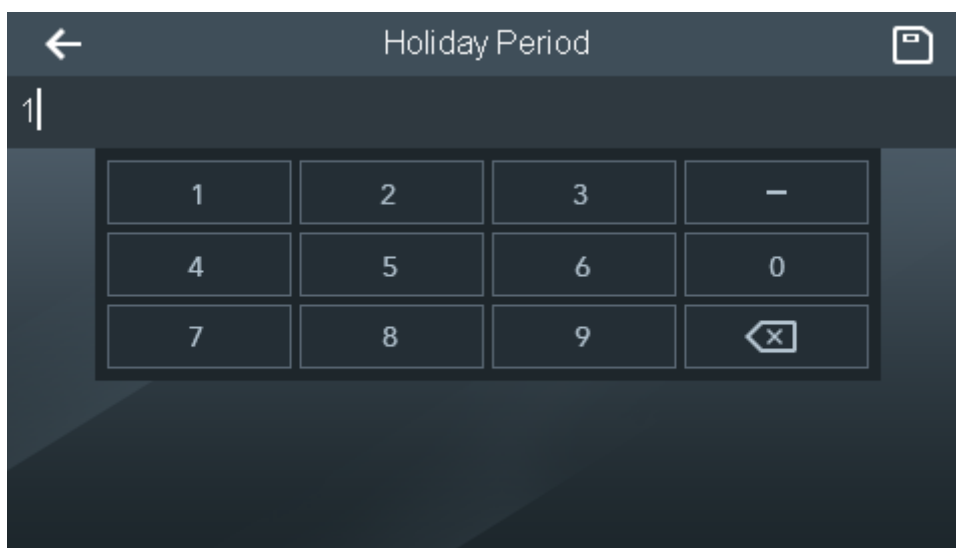



Figure 3-15

步骤2 Enter the period number set in “Period Config” and press .

The screen prompts “Bonded successfully”, so holiday and period are bonded.

3.6.1.4 NO Period

After setting NO period, the door keeps open within the period.

步骤1 Select “Access > Period Management> NO Period”, and the screen displays Figure 3-16.

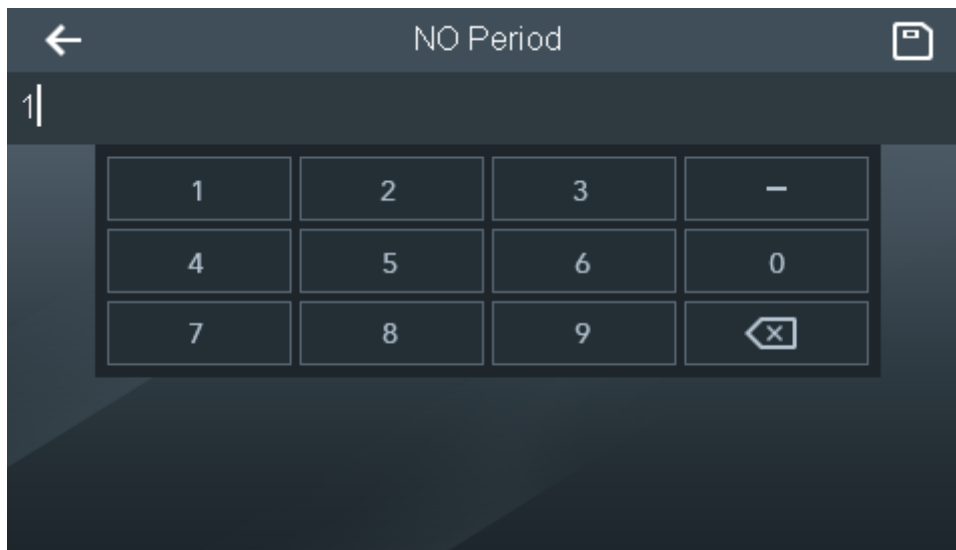



Figure 3-16

步骤2 Enter the period number set in “Period Config” and press .

The screen prompts “Bonded successfully”, so as to complete NO period config.

3.6.1.5 NC Period

After setting NC period, the door keeps closed within the period.

步骤1 Select “Access > Period Management> NC Period”, and the screen displays Figure 3-17.

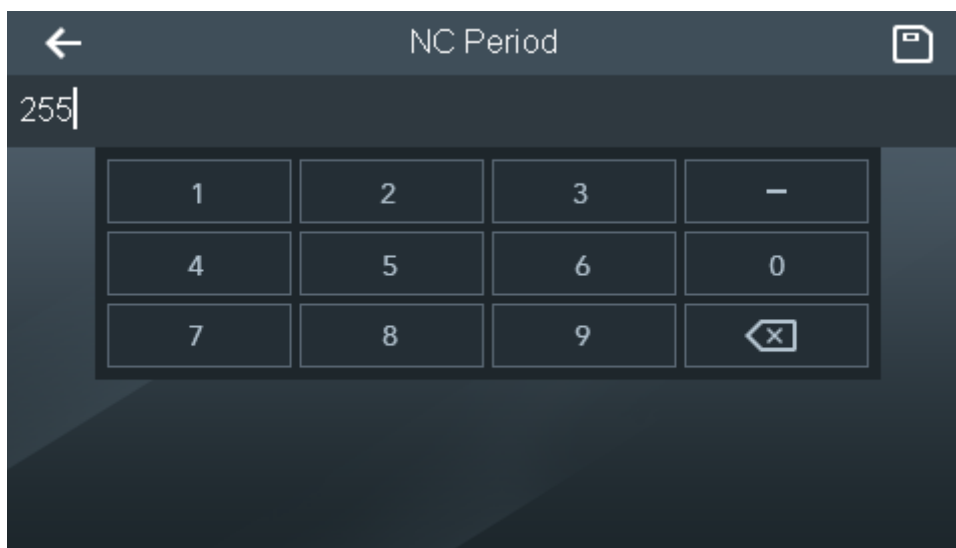



Figure 3-17


步骤2 Enter the period number set in “Period Config” and press .

The screen prompts “Bonded successfully”, so as to complete NC period config.

3.6.1.6 Remote Verification Period

During this period, the door can be opened only after the platform issues a remote unlock order.

步骤1 Select “Access > Period Management> Remote Verification Period”.

步骤2 Enter the period and press .

3.6.2 Unlock Mode

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

3.6.2.1 Unlock Mode

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

步骤1 Select “Access > Unlock Mode > Unlock Mode”.

步骤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.

步骤3 Press . The screen prompts “Do you want to save settings?”

步骤4 Press [Yes]. The system returns to “Unlock Mode” interface.

步骤5 Press the switch after “Unlock Mode” to enable.

- : enable.
- : disable.

3.6.2.2 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.

步骤1 Select “Access > Unlock Mode > Unlock by Period”.

The screen displays Figure 3-18.

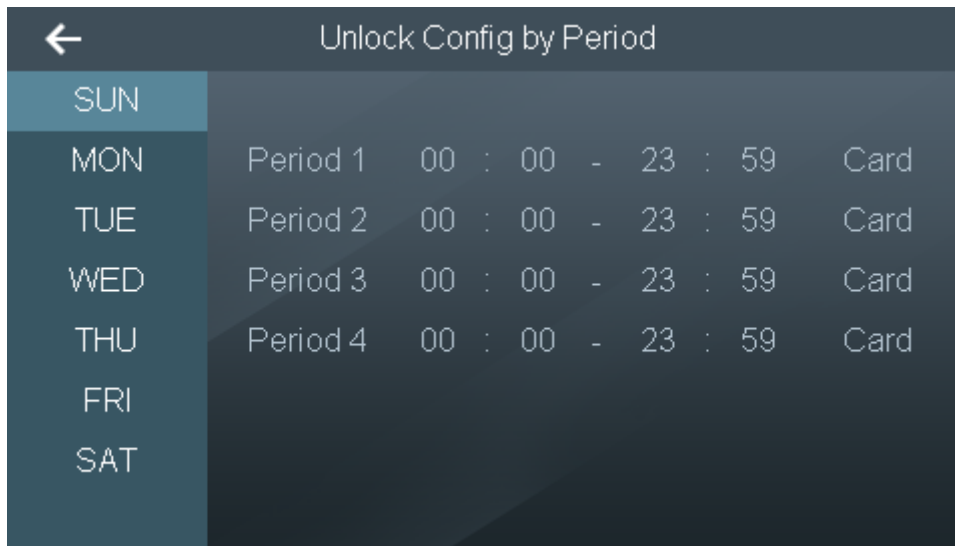


Figure 3-18

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

步骤3 Press . The screen prompts “Do you want to save settings?”

步骤4 Press [Yes]. The system returns to “Unlock Mode” interface.

步骤5 Press the switch after “Unlock by Period” to enable.

- : enable.
- : disable.

3.6.2.3 Group Combination


Set to unlock after authorized by multiple users or user groups.

步骤1 Select “Access > Unlock Mode > Group Combination”.

The screen displays Figure 3-19.

Group No	User	Unlock Mode	Valid User
01	Jimmy,mustafa...	Card	2

Figure 3-19

步骤2 Press  to add a group. Please refer to Table 3-2 for details.

The screen displays Figure 3-20.

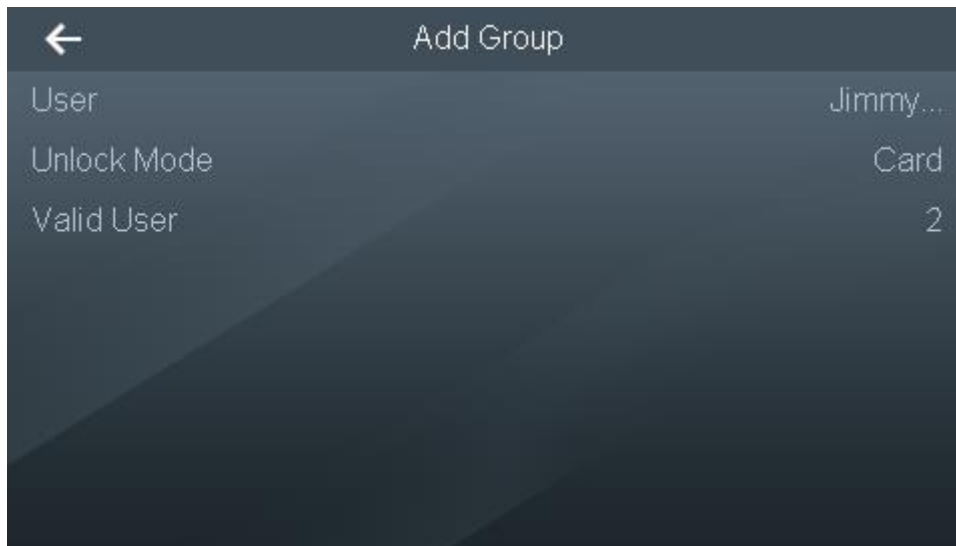


Figure 3-20





Parameter	Note
User	<p>Add users to the new group.</p> <ol style="list-style-type: none"> 1. Press [User]. 2. Press  in the pop-up interface. 3. Press  to enter user ID. Repeat Step 2~ Step 3 and continue to add users. Max. 50 users can be added. 4. Press , and press [Yes] to save according to interface prompt.
Unlock Mode	<p>Select unlock mode, including card, fingerprint, password and face.</p> <ol style="list-style-type: none"> 1. Press [Unlock Mode] to select the mode. 2. Press , and press [Yes] to save according to interface prompt.
Valid User	<p>The door can be unlocked after valid users unlock.</p> <ul style="list-style-type: none"> • 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

步骤3 Press . The screen prompts "Do you want to save settings?"

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

3.6.3 Alarm

Enable or disable alarm, including intrusion, anti-passback, duress, door sensor timeout and door sensor on.

步骤1 Select “Access > Alarm”, and the screen displays Figure 3-21.

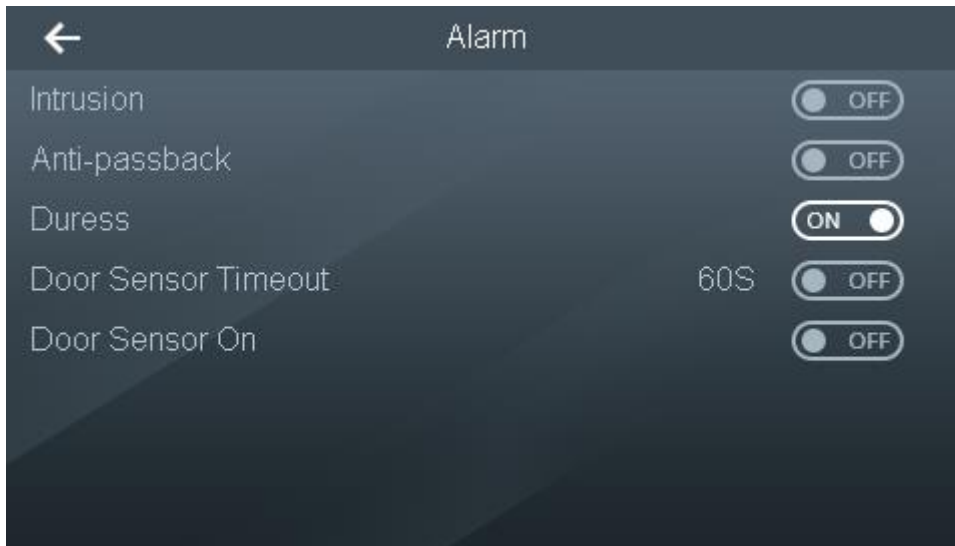




Figure 3-21

步骤2 Set the alarm according to needs. Please refer to Table 3-3 for details.

- : enable.
- : disable.


Parameter	Note
Intrusion	Intrusion alarm will be triggered if the door sensor is opened when the door is not opened normally.
Anti-passback	After enabling anti-passback function, an alarm will be triggered if a person is verified to enter, leaves without verification and then requests entry verification again.
Duress	Duress alarm will be triggered if the user enters with duress card, duress password or duress fingerprint.
Door Sensor Timeout	Timeout alarm will be triggered if opening time exceeds “Door Sensor Timeout”. Press “Door Sensor Timeout”, enter timeout (1s~9999s) and press  to save.
Door Sensor On	Enable door sensor. Intrusion and door sensor timeout alarm will be valid only after door sensor is enabled.

Table 3-3

3.6.4 Door Status

Door can be set to be normal, NO or NC.

步骤1 Select “Access > Door Status”, and the screen displays Figure 3-22.

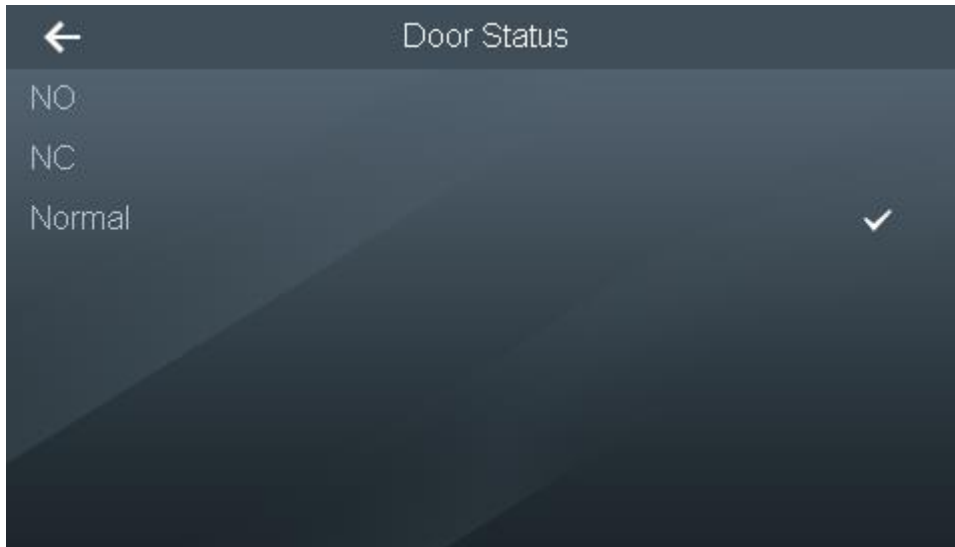


Figure 3-22

步骤2 Press the corresponding status. will be displayed after the status, so as to enable this status.

3.7 Attendance

3.7.1 Shift


3.7.1.1 Add Shift

Add attendance shift, max. 24 shifts.

步骤1 Select "Attendance > Shift Setting > Shift", and the screen displays Figure 3-23.

Index	Parameter	Value
1	Shift Name	day-shift
2	Period 1	08:00-17:00
3	Period 2	00:00-00:00
4	Overtime Period	00:00-00:00
5	Late-in Allowed	5
6	Early-out Allowed	5
7		
8		

Figure 3-23

步骤2 Select shifts, configure parameters and press  to save. Please refer to Table 3-4

for details.


Parameter	Note
Shift Name	Customize shift name.
Period 1 and Period 2	Set attendance period. When the period between Check In and Check Out meets this period, it is a normal attendance; otherwise, it is an exception attendance. The system supports two periods. If two periods are set, they are regarded to be normal attendance when both period 1 and period 2 carry out normal Check In and Check Out.
Overtime Period	Set overtime period. If period between overtime check-in and check-out meets the set period, it is regarded to be overtime period.  Note Overtime check-in is valid only if the card is swiped between off-duty time and overtime check-in time of "Period 1" or "Period 2".
Late-in Allowed	The range of check-in time later than on-duty time. For example, when on-duty time is 8:00, if "Late-in Allowed" time is set to be "5" minutes, it is regarded to be late if you check in after 8:05.
Early-out Allowed	The range of check-out time earlier than off-duty time. For example, when off-duty time is 17:00, if "Early-out Allowed" time is set to be "5" minutes, it is regarded to be early-out if you check out before 16:55.

Table 3-4

步骤3 Press . The screen prompts "Do you want to save settings?"

步骤4 Press [Yes] to complete shift config.

3.7.1.2 Shift Import



Caution

Before importing shift table, please ensure that USB disk has been inserted. Please don't pull out USB disk or execute other operations during uploading; otherwise, uploading will fail, even the device cannot work normally.

步骤1 Update the corresponding file and store it in USB disk.

步骤2 Select "Attendance > Shift Setting > Shift Import".

The screen prompts "Are you sure to import?"

步骤3 Press [Yes] to import.

It is suggested that files should be exported first and used as import template.

3.7.1.3 Shift Export



Caution

Before downloading shift table, please ensure that USB disk has been inserted. Please don't

pull out USB disk or execute other operations during downloading; otherwise, downloading will fail, even the device cannot work normally.

Download the shift in the system to USB disk.

步骤1 Select “Attendance > Shift Setting > Shift Export”.

The screen prompts “Are you sure to export?”

步骤2 Press [Yes] to export.

3.7.1.4 Holiday

Set holidays; add max. 64 holidays. All shifts don't check attendance during holidays.

步骤1 Select “Attendance > Shift Setting > Holiday”, and the screen displays Figure 3-24.

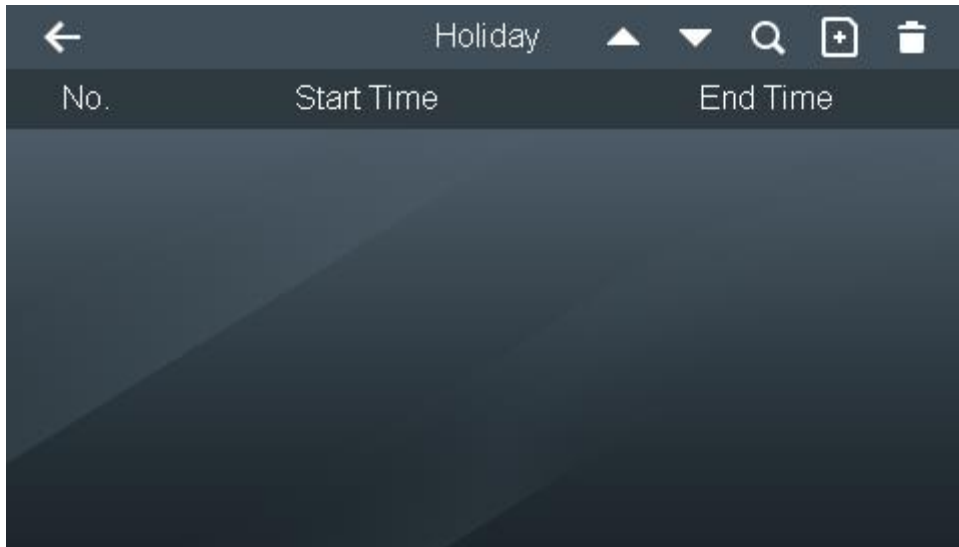



Figure 3-24

步骤2 Press , and the screen displays Figure 3-25.

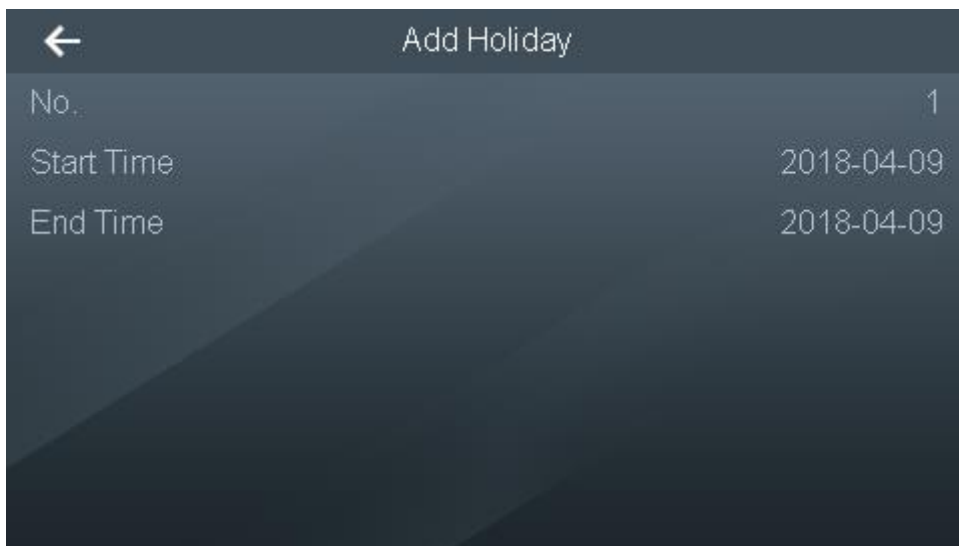



Figure 3-25

步骤3 Enter “Start Time” and “End Time”, and press . The no. is generated automatically according to sequence.

The screen prompts “Do you want to save settings?”

步骤4 Press [Yes] to complete holiday config.

3.7.2 Schedule

3.7.2.1 Personal Schedule

Set a single user's shift of the present month and next month. When the user selects "Personal Schedule", execute attendance according to this shift config.

步骤1 Select "Attendance > Schedule > Personal Schedule".

The screen displays Figure 3-26.

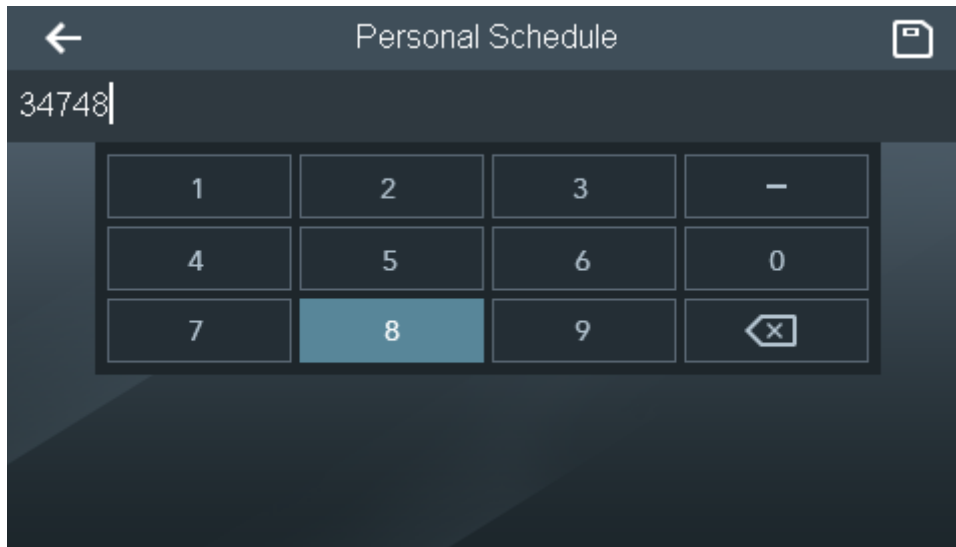



Figure 3-26

步骤2 Enter user ID and press , and the screen displays Figure 3-27.



Figure 3-27

步骤3 Press a date and select shift number.

步骤4 Press  to switch between the present month and next month.

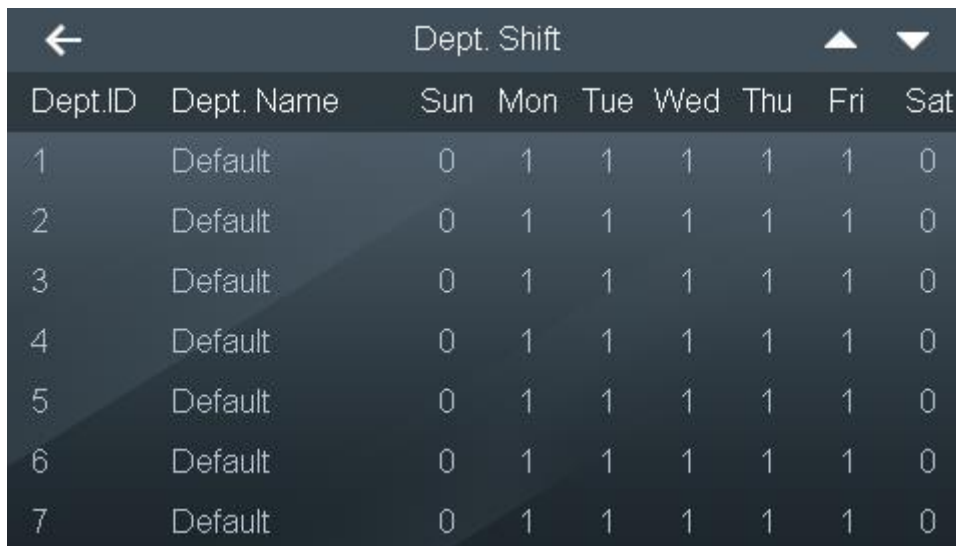
步骤5 Press . The screen prompts “Do you want to save settings?”

步骤6 Press [Yes] to complete personal schedule.

3.7.2.2 Department Schedule

Select a department, and set weekly department shift.

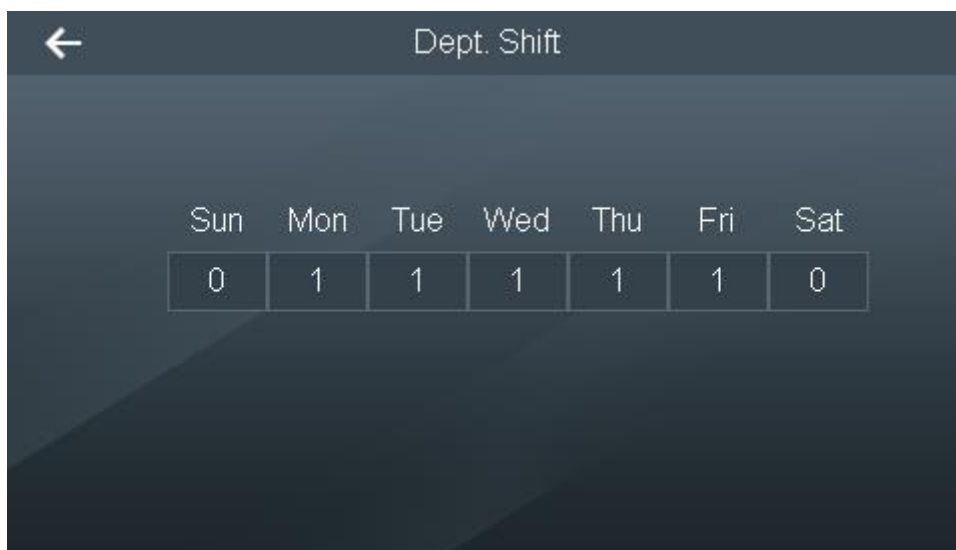
步骤1 Select “Attendance > Schedule > Dept. Schedule”, and the screen displays Figure 3-28.



Dept.ID	Dept. Name	Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	Default	0	1	1	1	1	1	0
2	Default	0	1	1	1	1	1	0
3	Default	0	1	1	1	1	1	0
4	Default	0	1	1	1	1	1	0
5	Default	0	1	1	1	1	1	0
6	Default	0	1	1	1	1	1	0
7	Default	0	1	1	1	1	1	0

Figure 3-28

步骤2 Select department and set weekly shift, as shown in Figure 3-29.



Sun	Mon	Tue	Wed	Thu	Fri	Sat
0	1	1	1	1	1	0

Figure 3-29

步骤3 Press . The screen prompts “Do you want to save settings?”

步骤4 Press [Yes] to complete department shift.

3.7.2.3 Schedule Import



Caution

Before importing shift table, please ensure that USB disk has been inserted. Please don't pull out USB disk or execute other operations during import; otherwise, import will fail, even the device cannot work normally.

步骤1 Update the corresponding file and store it in USB disk.

步骤2 Select "Attendance > Schedule > Schedule Import".

The screen prompts "Are you sure to import?"

步骤3 Press [Yes] to import.

3.7.2.4 Schedule Export



Caution

Before exporting shift table, please ensure that USB disk has been inserted. Please don't pull out USB disk or execute other operations during export; otherwise, export will fail, even the device cannot work normally.

步骤1 Select "Attendance > Schedule > Schedule Export".

The screen prompts "Are you sure to export?"

步骤2 Press [Yes] to export.

3.7.3 Verification Interval Time

Set the verification interval time. In case of continuous card swiping during the set time, record the first card swiping time only. For example, when the card is swiped repeatedly during the set time, record the first card swiping time only.

步骤1 Select "Attendance > Verification Interval Time", and the screen displays Figure 3-30.

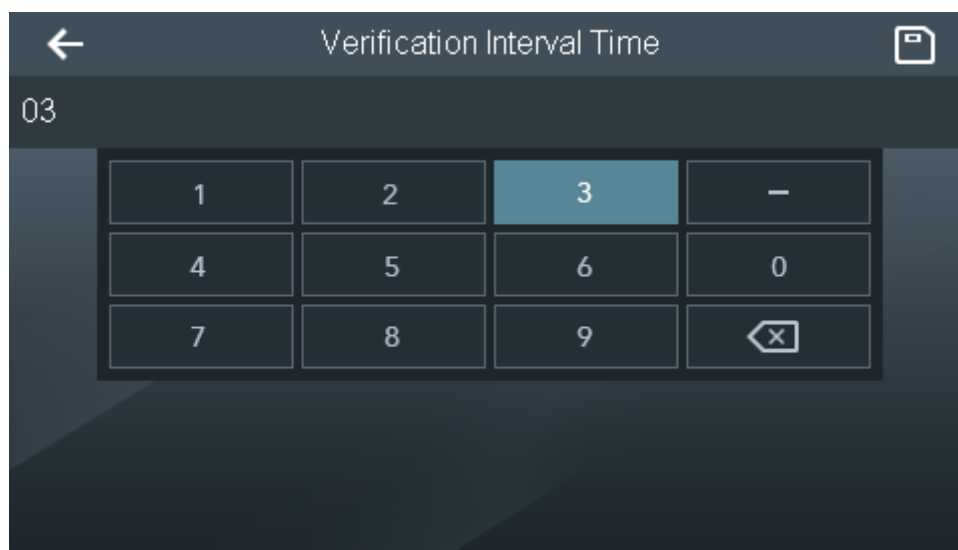


Figure 3-30

步骤2 Enter “Verification Interval Time” (unit: minute). In case of continuous card swiping during the set time, record the first card swiping time only.

步骤3 Press  to complete config.

3.8 System

3.8.1 Time

Set system date, time format, DST (Daylight Saving Time) and NTP check.

步骤1 Select “System > Time”, and the screen displays Figure 3-31.

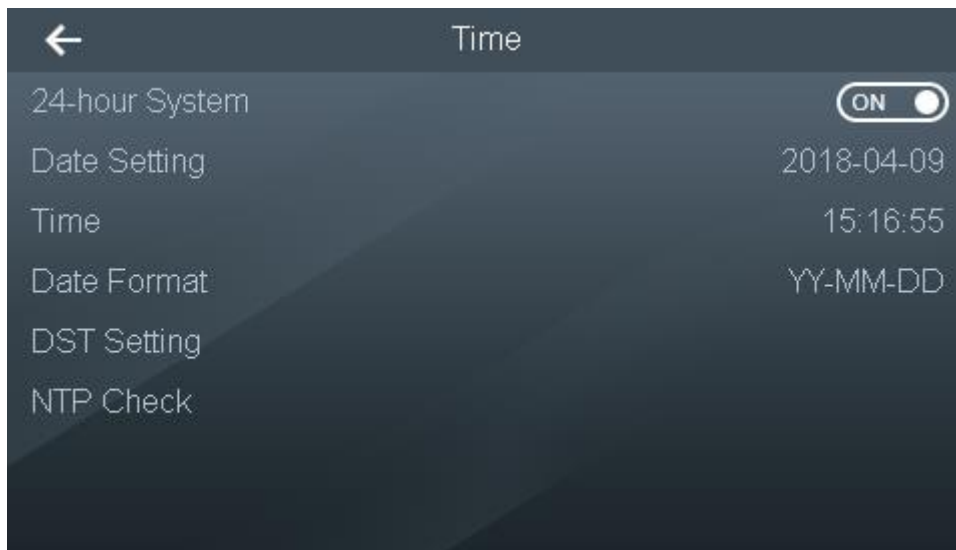






Figure 3-31

步骤2 Configure parameters by reference to Table 3-5. Then, press  to save config.

Parameter	Note
24-hour System	After it is enabled, the time is displayed in 24-hour system. Otherwise, the time is displayed in 12-hour system.
Date Setting	<ol style="list-style-type: none"> 1. Press [Date Setting]. 2. Enter year, month and date. 3. Press  to save.
Time	<ol style="list-style-type: none"> 1. Press [Time]. 2. Enter the time. 3. Press  to save.
Date Format	<ol style="list-style-type: none"> 1. Press [Date Format]. 2. Press textbox in the pop-up interface; select date format, including DD-MM-YY, YY-MM-DD and MM-DD-YY. 3. Press  to save.




Parameter	Note
DST Setting	<ol style="list-style-type: none"> 1. Press [DST Setting]. 2. Press the switch and it is enabled when it displays . 3. Press [DST Type] to select weekly or monthly. 4. Press [Start Time] and "End Time" to set the time.
NTP Check	<p>Set NTP check function.</p> <ol style="list-style-type: none"> 1. Press [NTP Check]. 2. Set parameters. <ul style="list-style-type: none"> ◇ Server IP address: fill in IP address of NTP check server. The device will check time according to the server. ◇ Port: fill in port number of NTP check server. ◇ Interval (min): time interval of NTP check. 3. Press the switch and it is enabled when it displays . 4. Press  to save.

Table 3-5

3.8.2 Face Parameter

Note

It is suggested that this parameter should be used by professionals during debugging, and should not be adjusted by users.

According to actual situation, adjust camera parameters and ensure picture definition.

Select "System > Face Parameter", and the screen displays Figure 3-32.

Note

For indoor use, it is suggested that exposure should be adjusted to manual mode and exposure time should be 1/4000, in order to obtain better face recognition experience. Specific setting method: Exposure (select the 5th, and press OK) → Exposure Mode (press Left key) → Manual (press OK) → Shutter (press Left key) → 1/4000.

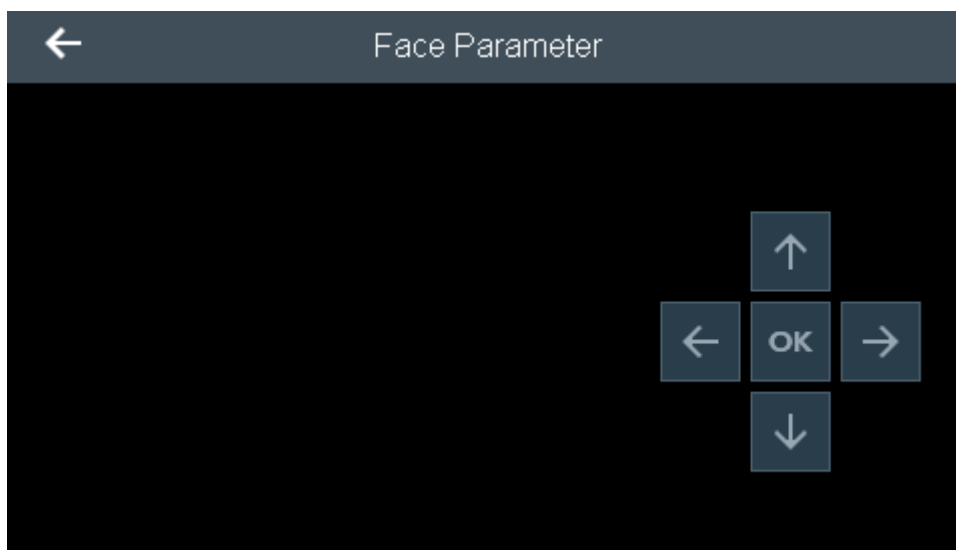


Figure 3-32



3.8.3 Infrared LED Set

Set brightness of infrared LED.

步骤1 Select “System > Infrared LED Set”, and the screen displays Figure 3-33.



Figure 3-33

步骤2 Adjust brightness with  and .

步骤3 Press  to save the setting.



3.8.4 Volume

Adjust volume of the device.

步骤1 Select “System > Volume”, and the screen displays Figure 3-34.



Figure 3-34


步骤2 Adjust volume with  and .

3.8.5 Face Detection Trigger Mode

步骤1 Select “System >Face Detection Trigger Mode”, and the screen displays Figure 3-35.



Figure 3-35

步骤2 Select trigger mode according to actual needs, and press  to save the setting.

- Motion: the screen displays “Face Recognition” interface when a moving object is detected within the camera range and face recognition is triggered.
- Proximity: the screen displays “Face Recognition” interface when infrared sensor within 30cm~50cm range in front of the device is blocked and face recognition is triggered.
- Motion & proximity: it is suggested to be used indoors.
- Only motion: it is suggested to be used outdoors.

3.8.6 Restore Factory



Caution

Data will be lost if restoring factory settings. Please operate cautiously.

Restore factory settings of the device; select to keep user info and log or not according to needs.

- Restore factory: restore all settings, including user settings. Device info and user info will be cleared.
- Restore factory (save user & log): after restoration, shift schedule will be cleared and shall be configured again.

Select “System > Restore Factory”, and the screen displays Figure 3-36. Select the needed mode and press [Yes].

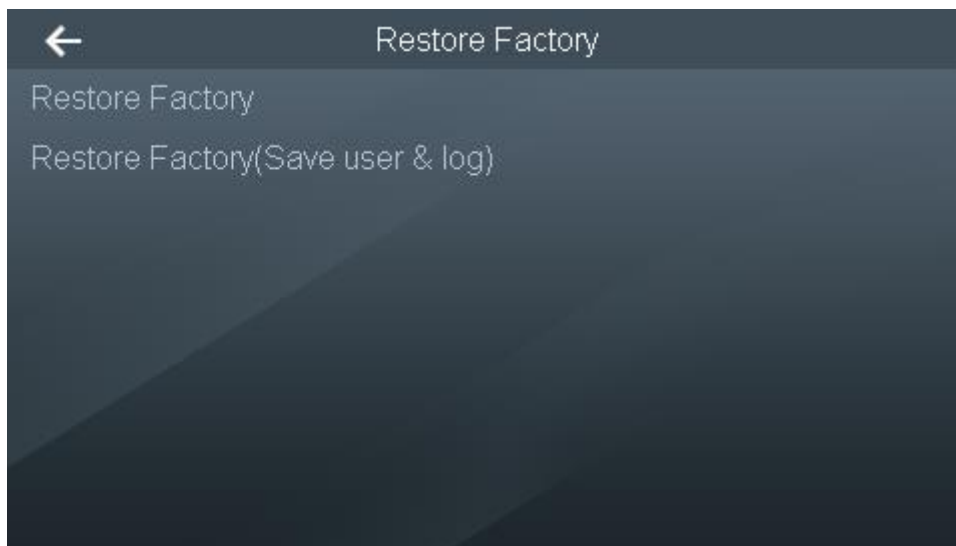


Figure 3-36

3.8.7 Reboot

Select "System > Reboot"; press [Yes] to reboot the device.

3.9 Connection

When attendance host is connected with the platform, configure IP address of the device, so as to add the device to the platform.

3.9.1 Network Configuration

步骤1 Select "Connection > Network Configuration", and the screen displays Figure 3-37.



Figure 3-37

步骤2 Select adding mode according to actual situation.

- IP Address
1. Select “IP Address”, and the screen displays Figure 3-38.

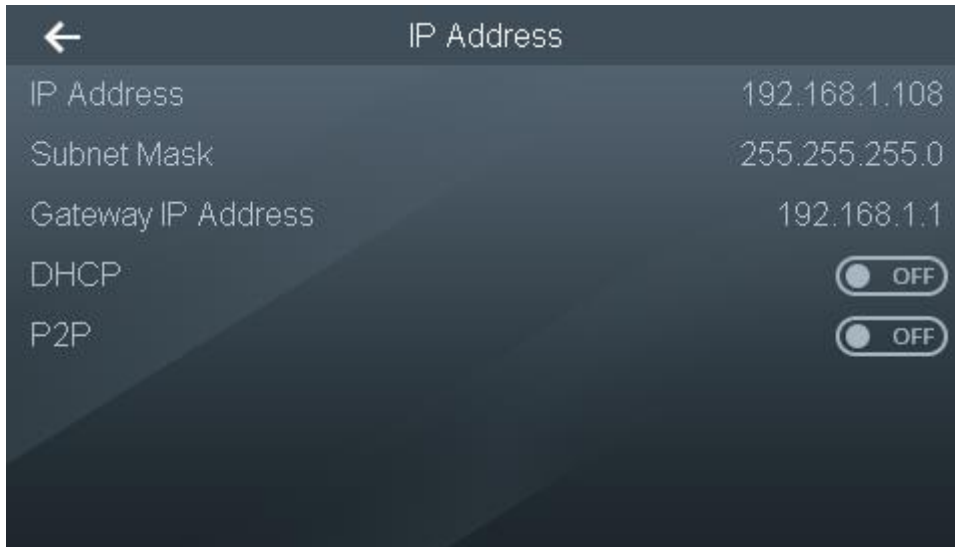


Figure 3-38

2. According to actual situation, configure parameters by reference to Table 3-6.



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 3-6

3. Press  to save the setting.
 - Active registration is a reserved function.

3.9.2 Serial Port

Select input/output mode according to purpose of the connected device.

Select “Connection > Serial Port”.

- Select “Serial Input” when connecting other card readers.
- Select “Serial Output” when connecting a third-party device or custom-made device.

3.9.3 Wiegand

Select input/output mode according to purpose of the connected device.

Select “Connection > Serial Port”.

- Select “Wiegand Input (Connect Reader)” when connecting other readers.

- Select “Wiegand Output Setting” when the device itself works as a card reader; controller can be connected. Please refer to Table 3-7 for details.

Parameter	Note
Wiegand Output Type	Digits of output card no. or ID that can be recognized by the device. <ul style="list-style-type: none"> • Wiegand 26: recognize 3 bytes, 6 digits. • Wiegand 34: recognize 4 bytes, 8 digits. • Wiegand 66: recognize 8 bytes, 16 digits.
Pulse Width	Set pulse width and interval of Wiegand output.
Pulse Interval	
Output Data Type	Obtain data type. <ul style="list-style-type: none"> • User ID: if user ID is selected, output corresponding data according to user ID. • Card no.: if card no. is selected, output corresponding data according to user card number.

Table 3-7

3.9.4 Wi-Fi

Add Wi-Fi, and thus connect the device into network.

步骤1 Select “Connection > Wi-Fi”, and the screen displays Figure 3-39.

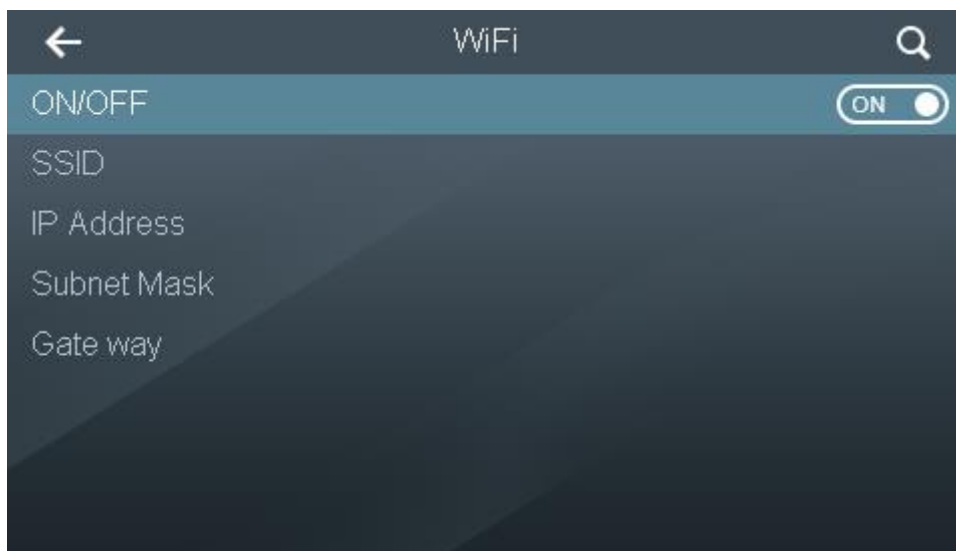




Figure 3-39

步骤2 Select “ON” to enable Wi-Fi function.

步骤3 Press  to select the needed wireless network.

步骤4 Enter the password and press  to save.

3.10 Features

Enter main menu and select “Features”, and the screen displays Figure 3-40.

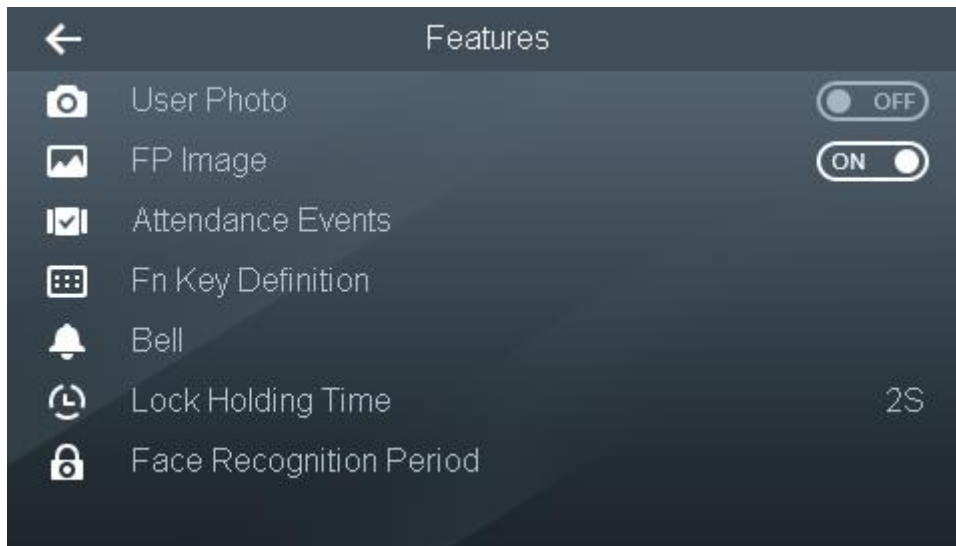




Figure 3-40



3.10.1 User Photo

After this function is turned on, the device will automatically snapshot face when the door is opened, and store the images locally (max. 10,000 images can be stored). If the device is connected with the platform, images will be uploaded to the platform automatically. If this function is turned off, the device won't snapshot or store images.

- : turn on.
- : turn off.

3.10.2 FP Image

After this function is turned on, when the device is collecting fingerprint, real fingerprint image will be displayed in scanning frame. If this function is turned off, real fingerprint image won't be displayed.

- : turn on.
- : turn off.

3.10.3 Attendance Events

Set attendance event and time according to actual situation. The events mainly apply to the platform.

步骤1 Select "Features > Attendance Events", and the screen displays Figure 3-41.

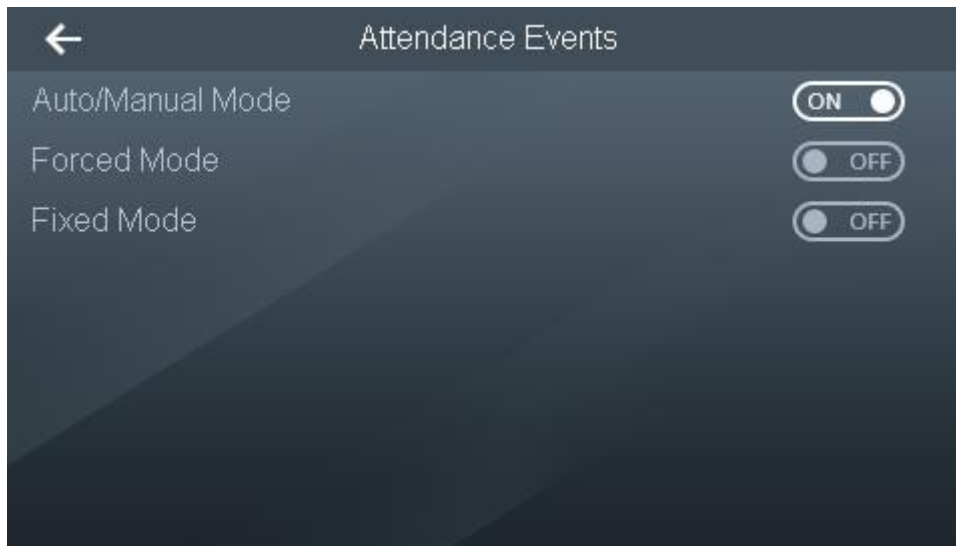




Figure 3-41

步骤2 According to actual situation, configure parameters by reference to Table 3-8.

- : turn off.
- : turn off.


Parameter	Note
Auto/Manual Mode	Press [Auto/Manual Mode], set corresponding period of every event, and press  to save. In standby interface, display corresponding event according to the set time.
Forced Mode	After this function is turned on, standby interface doesn't display default attendance event, but attendance event is forced to be selected manually, in order to complete the verification. Press Fn key to select and verify. Alternatively, verify first, and then select attendance event.
Fixed Mode	After this function is turned on, select the event. Standby interface displays the selected event, which cannot be modified manually.

Table 3-8

3.10.4 Fn Key Definition

Customize event name of Fn key.

步骤1 Select "Features > Fn Key Definition", and the screen displays Figure 3-42.

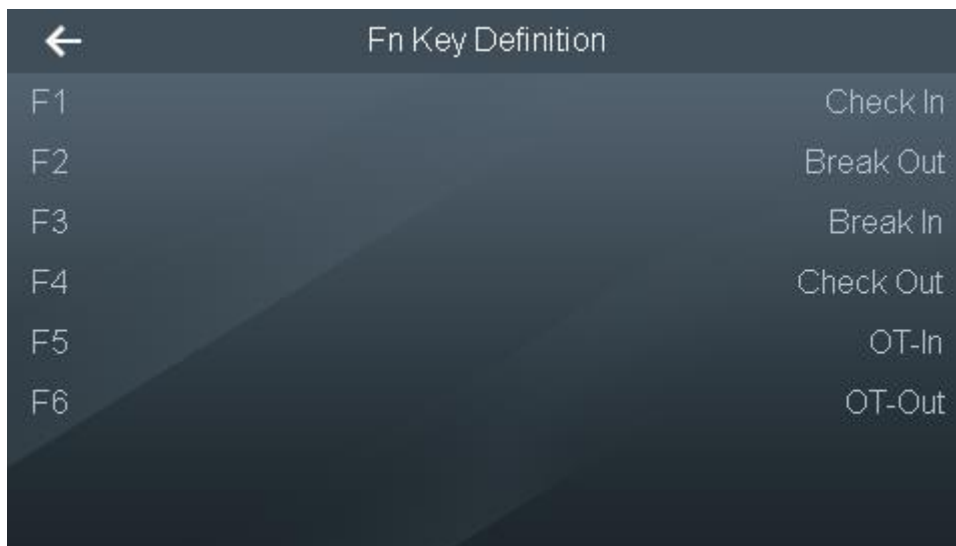


Figure 3-42

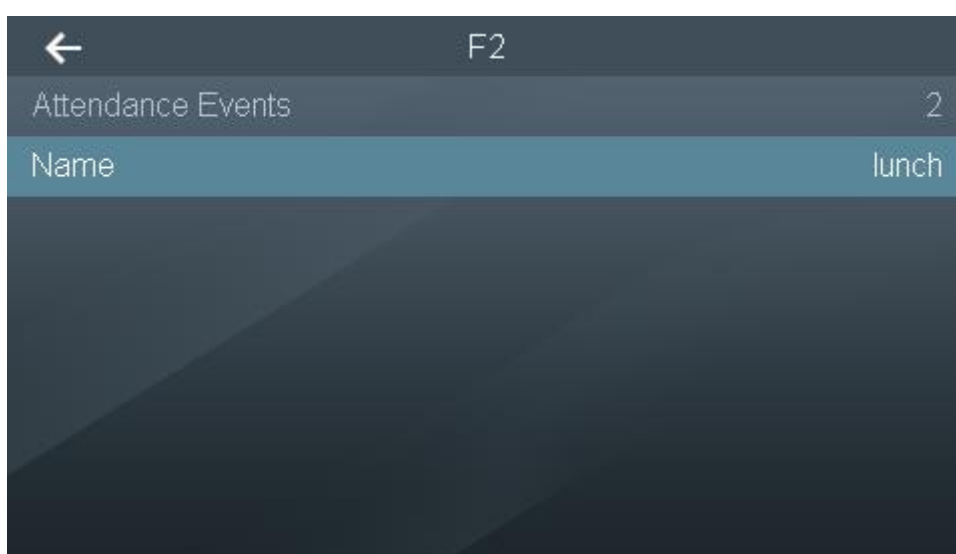


Figure 3-43

步骤2 Select Fn key to modify its name.

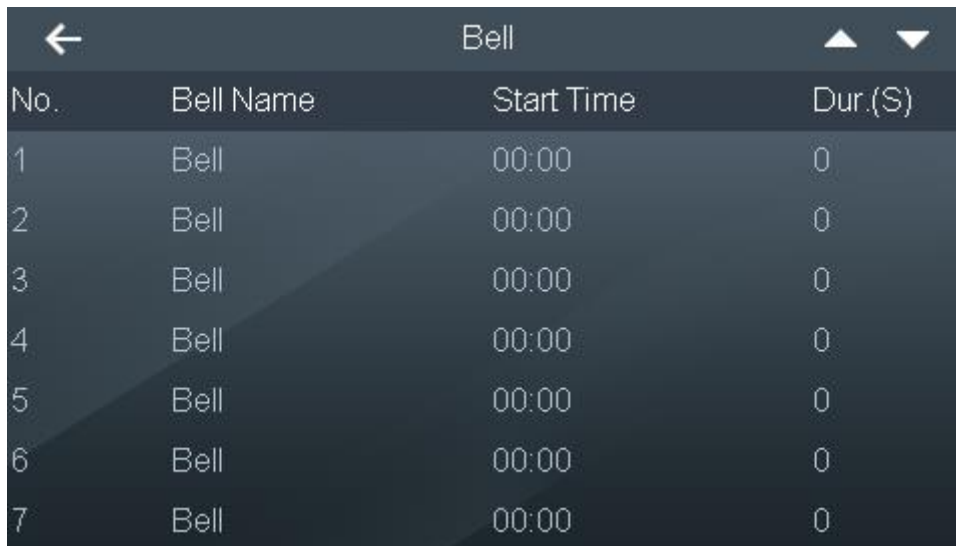
步骤3 Press  to save the setting.

3.10.5 Bell

Bell is mainly linked with device loudspeaker, so as to remind the user at fixed time.

The system supports max. 8 bells.

步骤1 Select “Features > Bell”, and the screen displays Figure 3-44.



No.	Bell Name	Start Time	Dur.(S)
1	Bell	00:00	0
2	Bell	00:00	0
3	Bell	00:00	0
4	Bell	00:00	0
5	Bell	00:00	0
6	Bell	00:00	0
7	Bell	00:00	0

Figure 3-44

步骤2 Select the required bell; press numeric key to enter relevant info. Please refer to Table 3-9 for details.

Parameter	Note
No.	The system generates bell no. automatically.
Bell Name	Customize bell name, max. 10 Chinese characters or 32 characters.
Start Time	Enter start time of the bell.
Dur. (s)	Set duration of the bell.

Table 3-9

步骤3 Press  to save the setting.

3.10.6 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.

步骤1 Select “Features > Lock Holding Time”, and the screen displays Figure 3-45.

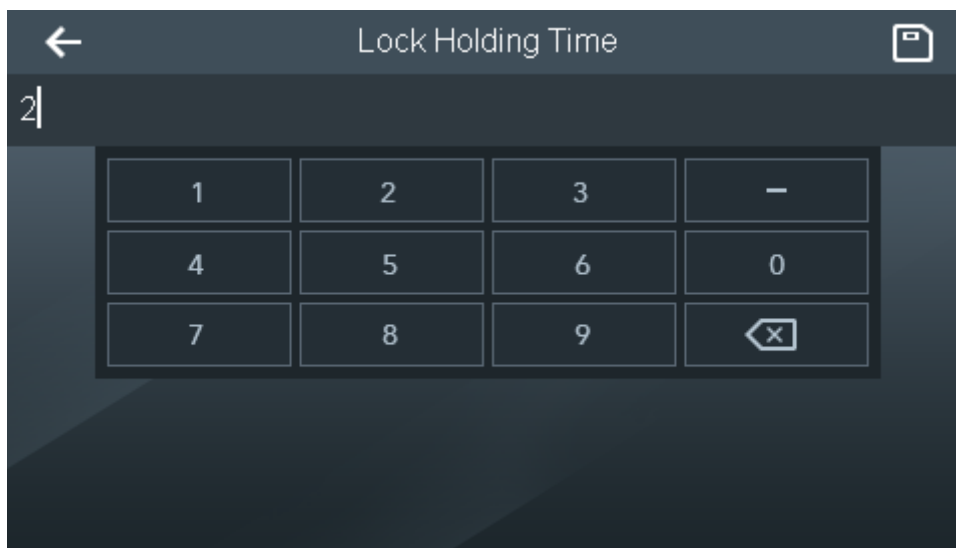




Figure 3-45

步骤2 Delete original data with [] key, enter “Lock Holding Time” and press  to save the setting.

3.10.7 Face Recognition Period

Face recognition function is valid only within the set period.

步骤1 Select “Features > Face Recognition Period”, and the screen displays Figure 3-46.

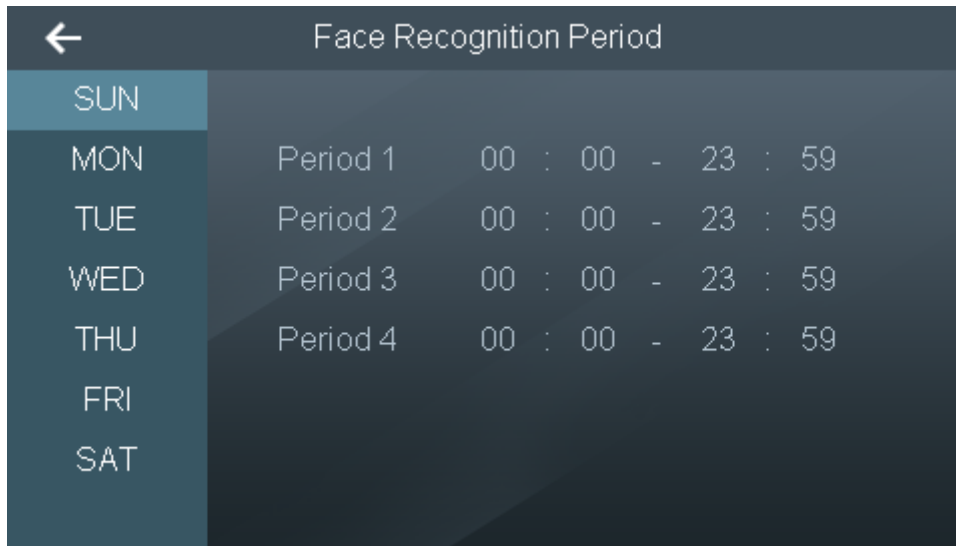



Figure 3-46

步骤2 Set the period according to actual situation.

步骤3 Enter the time with numeric key and press  to save the setting.

步骤4 Press . The screen prompts “Do you want to save settings?”

步骤5 Press [Yes] to complete the setting.

3.11 Record



Before exporting attendance record, please ensure that USB disk has been inserted. Please don't pull out USB disk or execute other operations during export; otherwise, export will fail.

3.11.1 Search Card Punch

Select “Record > Search Card Punch”, and the screen displays Figure 3-47. All records can be viewed, including time, name, status and verify mode.

 Note

Press  and  to page up and down.

User ID.	Name	Time	Status	Verify Mode
		04-09 15:38	Failed	FP
		04-09 15:38	Failed	FP
34748	Jimmy	04-09 15:38	OK	FP
10086	mustafa	04-09 15:38	OK	FP
		04-09 15:37	Failed	FP
34748	Jimmy	04-09 15:37	OK	FP


All 3 P, P.No 2 P

Figure 3-47

3.11.2 Search Alarm Record

Select “Record >Search Alarm Record”, and the screen displays Figure 3-48. All alarm records can be viewed, including alarm type and time.

 Note

Press  and  to page up and down.

Alarm Type	Alarm Time
------------	------------

All 1 P, P.No 1 P

Figure 3-48

3.11.3 Search Admin Record

步骤1 Select “Record > Search Admin Record”, and the screen displays Figure 3-49.

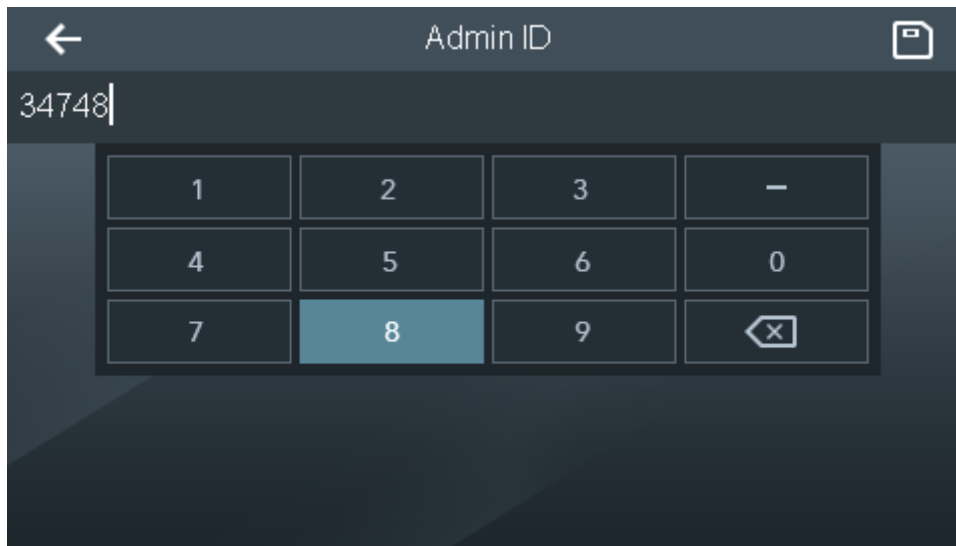



Figure 3-49

步骤2 Enter admin ID and press  to save the setting.

The screen displays searched info, as shown in Figure 3-50.

Operate Type	Operate Time	User ID.
Add super user	2018-04-09 14:59:33	

All 3 P, P.No 3 P

Figure 3-50

3.11.4 Export 1 Month Attendance Report


Export all attendance report of the present month or previous month to USB disk.

步骤1 Select “Record > Export 1 Month Attendance Report”, and the screen displays Figure 3-51.



Figure 3-51

步骤2 Press  or  to select month.

步骤3 Press  to export the report and press [Yes].
Generate Excel file and save it in USB disk.

3.11.5 Export 1 Month Exception Report


Export all exception attendance report of the present month or previous month to USB disk.

步骤1 Select "Record > Export 1 Month Exception Report", and the screen displays Figure 3-52.



Figure 3-52

步骤2 Press  or  to select month.

步骤3 Press  to export the report and press [Yes].
Generate Excel file and save it in USB disk.

3.12 USB



Caution

Before exporting user info and updating, please ensure that USB disk has been inserted. Please don't pull out USB disk or execute other operations during export or update; otherwise, export or update will fail.

Export user info from USB or import user info into USB disk; also, update the system with USB disk.


3.12.1 USB Export

步骤1 Select "USB > USB Export", and the screen displays Figure 3-53.



Figure 3-53

步骤2 According to actual situation, select the required info.

步骤3 Press  to import records, and press [Yes] to import USB info into the device.

3.12.2 USB Import

步骤1 Select "USB > USB Import", and the screen displays Figure 3-54.

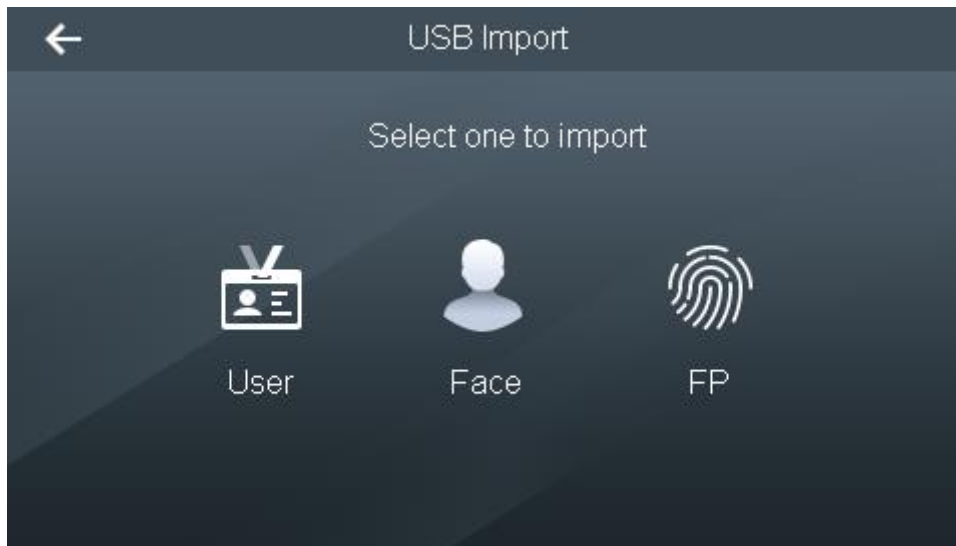



Figure 3-54

步驟2 According to actual situation, select the required info.

步驟3 Press  to import records, and press [Yes].
Generate Excel file and save it in USB disk.

3.12.3 USB Update

Update the system with USB disk.

步驟1 Rename the update file to be “update.bin”, put it under root directory of USB disk, and insert the USB disk into the device.

步驟2 Select “USB > USB Update”.

The system pops up “Are you sure to update?” dialog box, as shown in Figure 3-55.

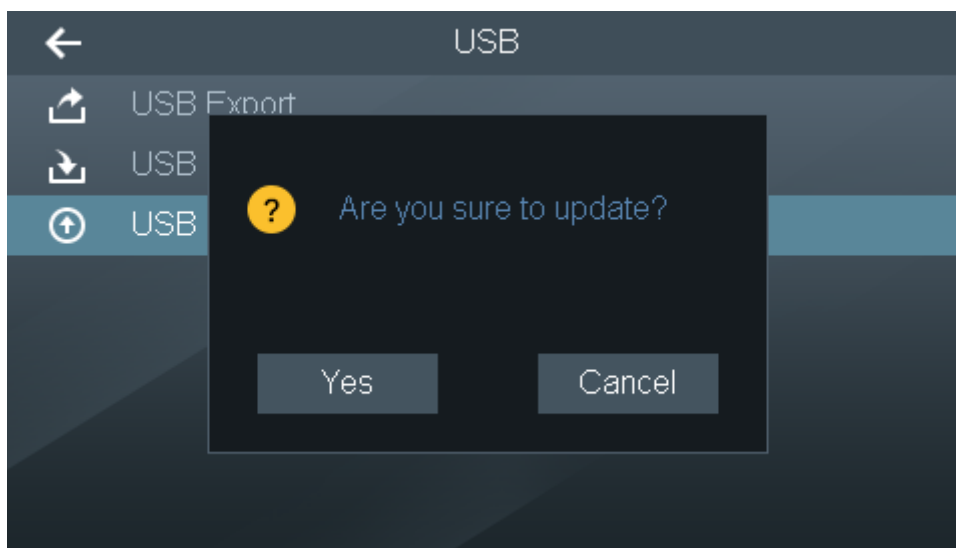


Figure 3-55

步驟3 Press [Yes].

The system starts to update, and the device is rebooted automatically after update is completed.

3.13 Auto Test

Test or auto test the device screen, button and fingerprint collection.

3.13.1 Screen

步骤1 Select “Auto Test > Screen”, and the screen displays Figure 3-56.

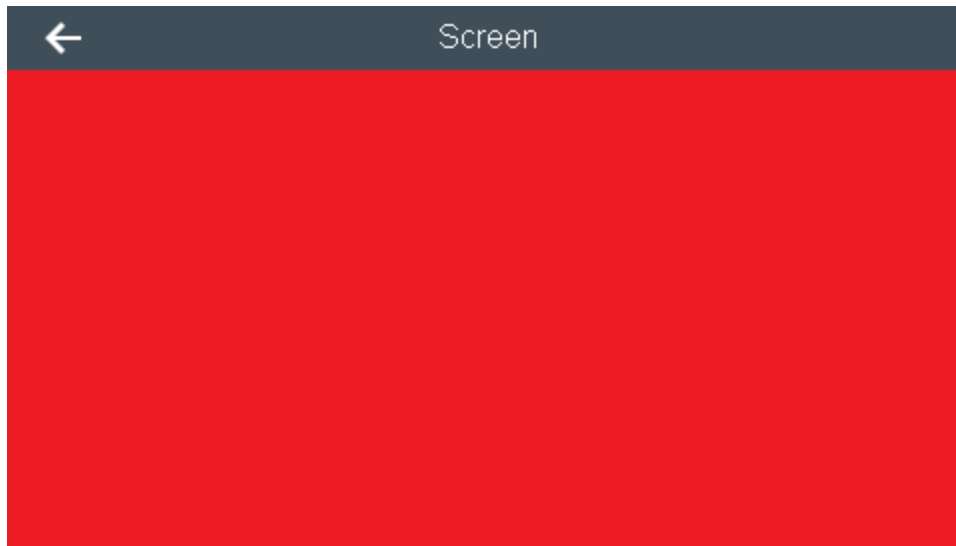


Figure 3-56

步骤2 Press the touch screen, and the screen displays red, green, blue, black and white in turn. Check whether it is abnormal.

步骤3 Press  to exit screen test.

3.13.2 Voice

步骤1 Select “Auto Test > Voice”, and the screen displays Figure 3-57.

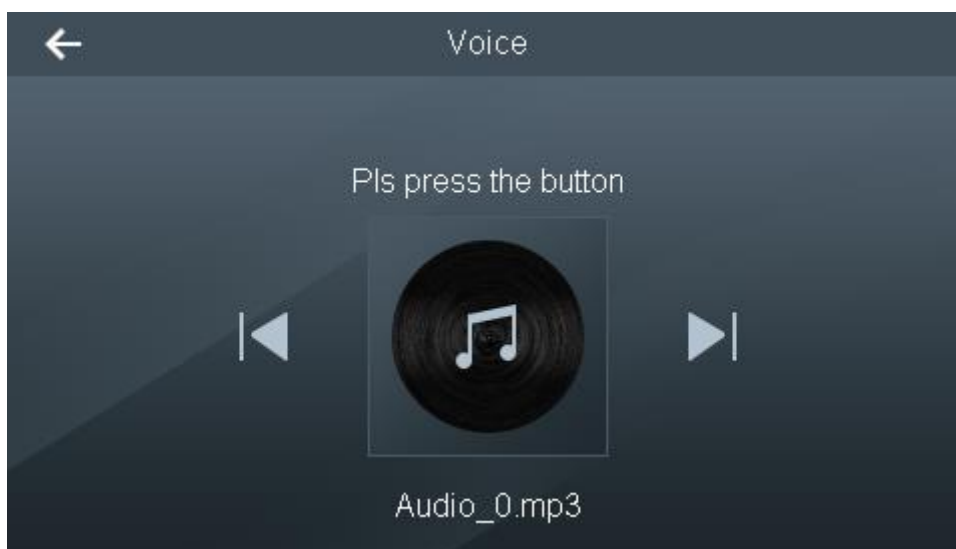




Figure 3-57

步骤2 Press the touch screen to play and press  or  to switch. Listen to prompt tone and check whether it is abnormal.

步骤3 Press  to exit voice test.

3.13.3 Button

步骤1 Select “Auto Test > Button”, and the screen displays Figure 3-58.

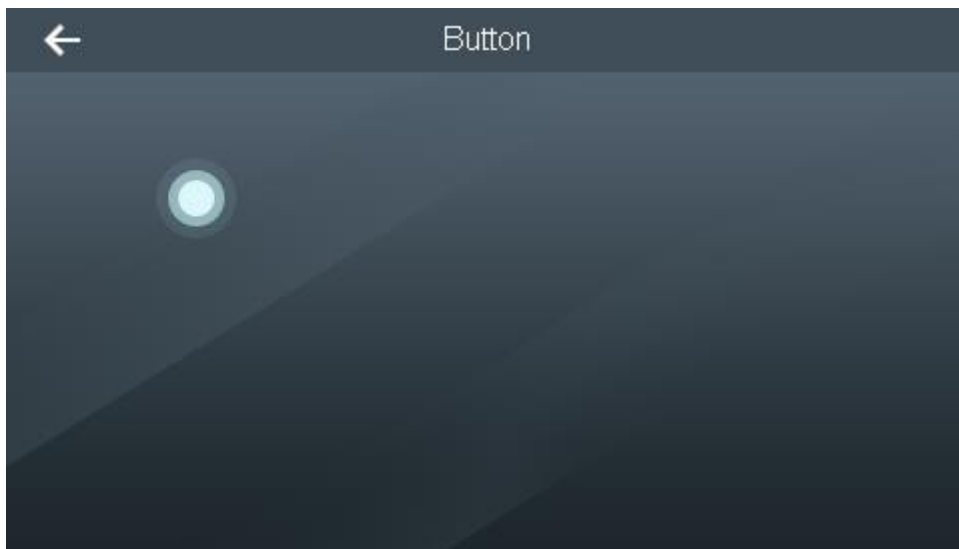


Figure 3-58

步骤2 Touch control button is displayed in the screen. Touch the screen at corresponding position to test it.

步骤3 Press  to exit button test.

3.13.4 FP

步骤1 Select “Auto Test > FP”, and the screen displays Figure 3-59.

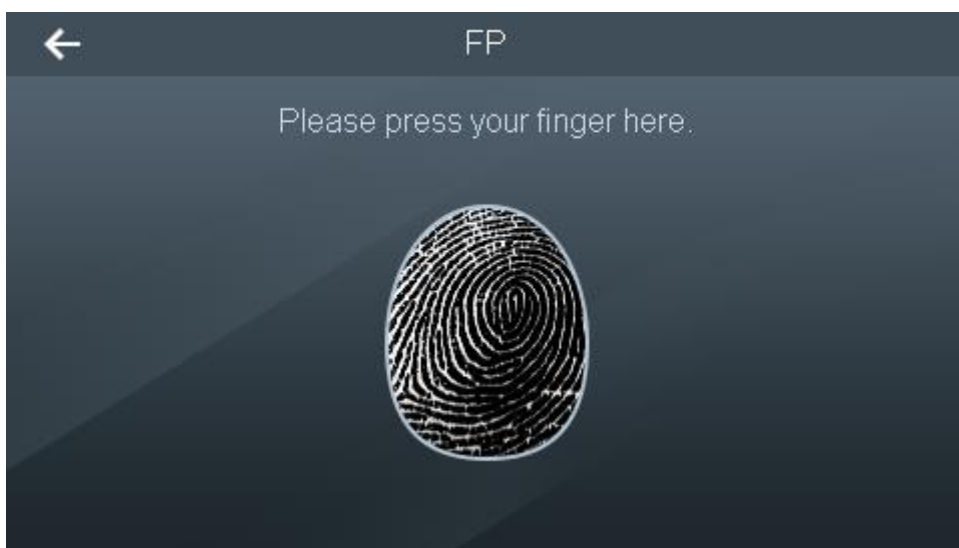


Figure 3-59

步骤2 According to system prompt, press your finger in fingerprint collection zone, and check whether fingerprint is displayed normally.

步骤3 Press  to exit FP test.

3.13.5 Face

Select “Auto Test > Face”, and check whether face is detected.

3.13.6 Clock

步骤1 Select “Auto Test > Clock”, and the screen displays Figure 3-60.

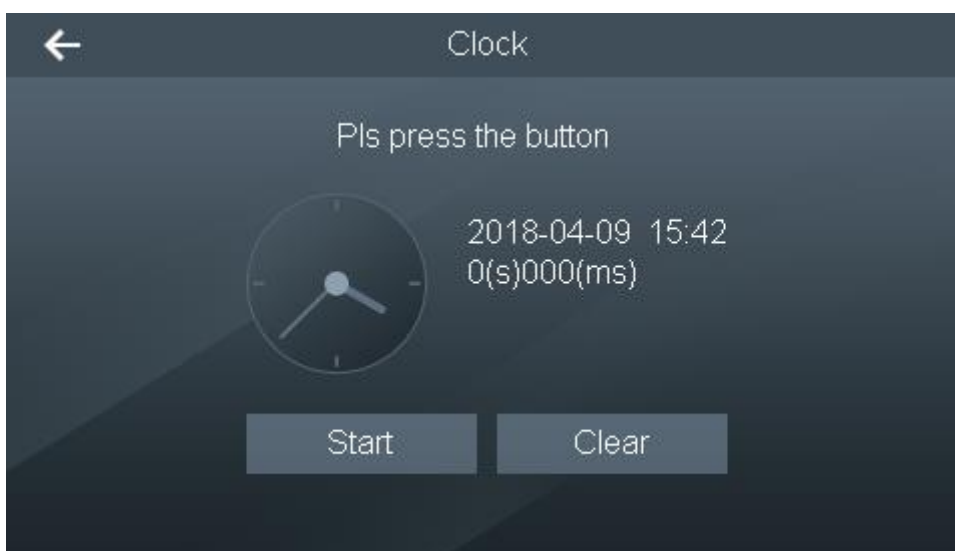


Figure 3-60

步骤2 Press “Start” or “Clear” to test whether the time is normal.

步骤3 Press  to exit clock test.

3.13.7 Auto Test

Select “Auto Test > Auto Test”, and the system starts auto test.

3.14 System Info

View data capacity, device version and firmware info.

At main interface, select “System Info” and the screen displays Figure 3-61.



Figure 3-61

3.14.1 View Data Capacity

Select "System Info > Data Capacity" and the screen displays present usage and max. capacity

of user, fingerprint, face, alarm record, punch record, admin record, admin quantity and super password.

3.14.2 View Device Version

Select “System Info > Device Version” and the screen displays serial no., MAC address, IP address, software version and MCU version.

3.14.3 View Firmware Info

Select “System Info > Firmware Info” and the screen displays firmware version number.

4

Technical Parameters

Type	Name	Value
System	Main processor	A11-core processor
	Storage capacity	512M
Door Control	Lock control	1-ch
	Door contact	1-ch
	Exit button	1-ch
	External reader	1-ch (Wiegand)
Alarm	Alarm input	2-ch
	Alarm output	2-ch
Access	Door overtime alarm	When opening time exceeds "Door Overtime", overtime alarm will be triggered, which shall be set.
	Intrusion alarm	Intrusion alarm will be triggered if someone breaks in without swiping card or entering password.
	Duress alarm	Duress alarm will be triggered if someone enters with duress card.
	Tamper alarm	Tamper alarm will be triggered if the device is dismantled.
	Opening mode	Card, password, fingerprint and face combination
	Remote verification	Support period bonding
	Period	128 groups
	Holiday period	128 groups
	Network update	Update the device through network
	Patrol card	Patrol card can only be swiped at patrol site, but the door cannot be opened.
	Guest card	Set use number of the guest card. The card loses efficacy in case of exceeding the use number.
Attendance	Attendance period	24
	Shift mode	Personal schedule (monthly), department shift (weekly)
	Attendance record	150000
	Attendance report	Standalone USB exports EXCEL
Port	Network port	1
	RS232 port	1
	RS485 port	1
General	Power supply	DC 12V
	Power consumption	≤10W (excluding card reader)
	Operating temperature	-5℃~+55℃
	Operating humidity	5%~95%
	Barometric pressure	86kPa~106kPa
	Dimension (mm)	215mm×122m×102mm
	Weight	1.0kg
	Mounting	Desktop/wall-mounting
Operating environment	Indoor, semi-outdoor, avoid direct exposure to sunlight	

1 The device fails to boot up after power-on.

Answer: please check whether 12V power is connected correctly; whether switch button on the left is pressed.

2 The device fails to recognize face after boot-up.

Answer:

- Please refer to “Features > Face Recognition Period” and check whether it is within face recognition period. Please refer to “3.10.7 Face Recognition Period” for details.
- Please refer to “Access > Unlock Mode > Any Combination Unlock” and check whether face mode is configured. Please refer to “3.6.2.1 Unlock” for details.

3 The device and third-party controller connect Wiegand port, but no signal is output.

Answer: please check whether GND wire of the device is connected with GND wire of third-party controller. Please check whether device Wiegand format is consistent with controller format.

4 Forget admin and fail to set.

Answer: Please use matched PSS software to delete admin, or contact technical support personnel to carry out remote unlock with professional software tool.

5 User info, fingerprint and face import error.

Answer: please check whether XML file name and header name have been changed. The system judges files automatically according to name.

6 The user’s face is recognized to be another user.

Answer: Please confirm no one else appears around when you are scanning face. In case of this problem, please delete original face and scan again.

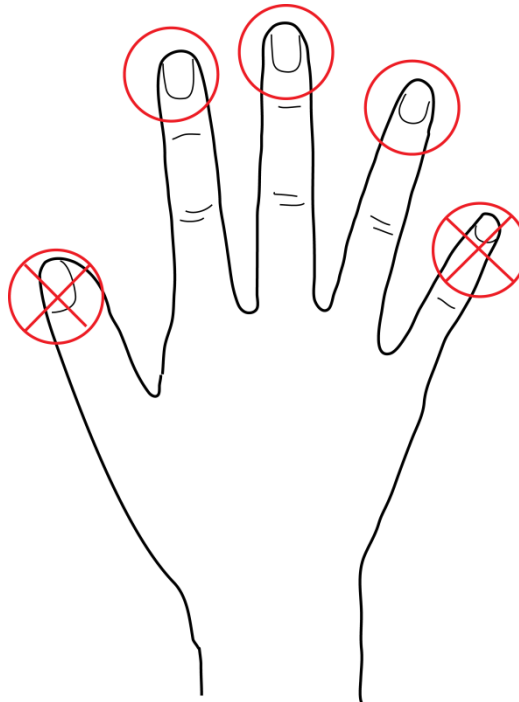
附录1 Fingerprint Operation

Points for Attention

- Before pressing your finger, please keep your fingers clean, without stain or water.
- During pressing or scanning, place your finger onto collector window flatly; try to align the center of your fingerprint with window center.

Recommended Finger

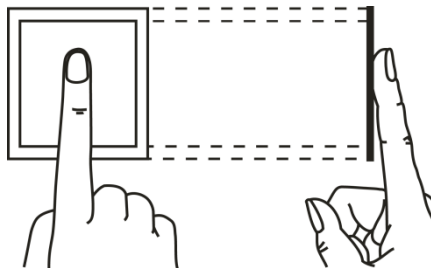
Index finger, middle finger and ring finger are recommended for fingerprint collection. Thumb and little finger cannot be placed onto collector window easily.



Appendix Figure 1-1

Press

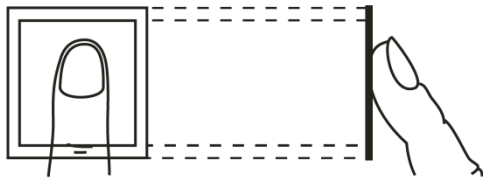
- Correct



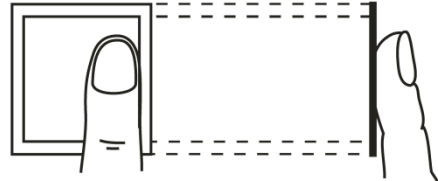
Appendix Figure 1-2

- False

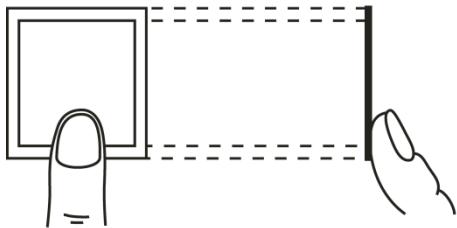
Vertical



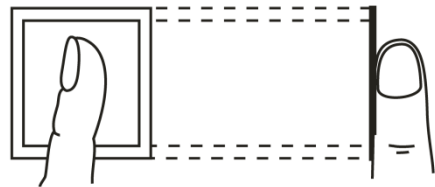
Far away from center



Too low



Oblique



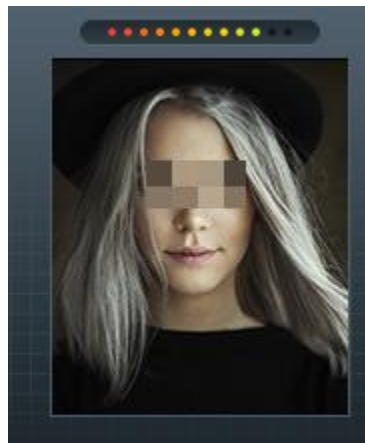
Appendix Figure 1-3

附录2 Face Registration Instruction

Points for Attention

- During registration, glasses, hats and mustache may affect registration effect.
- Please don't hide your eyebrows if you put on a hat.
- Too long or too large mustache affects registration effect. It is suggested that mustache should not change greatly during use from the registration. Otherwise, it may affect recognition.
- Please keep the face clean during registration and verification.

Registration



Appendix Figure 2-1

- During registration, please put your face in the frame and move your head according to prompt. Pay attention to move your head slowly back and forth; turn left and right within a small range.
- Every dot on the frame represents an image. After all dots are marked, the registration has been completed, which takes about 15s.

Note:

- This manual is for reference only. Slight difference may be found in user interface.
- All the designs and software here are subject to change without prior written notice.
- All trademarks and registered trademarks are the properties of their respective owners.
- If there is any uncertainty or controversy, please refer to the final explanation of us.
- Please visit our website or contact a user local service engineer for more information.