

User Manual

Horus E2 Series

Mobile Biometric Terminal for T&A and Access Control

Date: December 2024

Doc Version: 1.0

English

Thank you for choosing our product. Please read the instructions carefully before operation. Follow these instructions to ensure that the product is functioning properly. The images shown in this manual are for illustrative purposes only.



For further details, please visit our Company's website
www.zkteco.com.

Copyright © 2024 ZKTECO CO., LTD. All rights reserved.

Without the prior written consent of ZKTeco, no portion of this manual can be copied or forwarded in any way or form. All parts of this manual belong to ZKTeco and its subsidiaries (hereinafter the "Company" or "ZKTeco").

Trademark

ZKTeco is a registered trademark of ZKTeco. Other trademarks involved in this manual are owned by their respective owners.

Disclaimer

This manual contains information on the operation and maintenance of the ZKTeco equipment. The copyright in all the documents, drawings, etc. in relation to the ZKTeco supplied equipment vests in and is the property of ZKTeco. The contents hereof should not be used or shared by the receiver with any third party without express written permission of ZKTeco.

The contents of this manual must be read as a whole before starting the operation and maintenance of the supplied equipment. If any of the content(s) of the manual seems unclear or incomplete, please contact ZKTeco before starting the operation and maintenance of the said equipment.

It is an essential pre-requisite for the satisfactory operation and maintenance that the operating and maintenance personnel are fully familiar with the design and that the said personnel have received thorough training in operating and maintaining the machine/unit/equipment. It is further essential for the safe operation of the machine/unit/equipment that personnel has read, understood and followed the safety instructions contained in the manual.

In case of any conflict between terms and conditions of this manual and the contract specifications, drawings, instruction sheets or any other contract-related documents, the contract conditions/documents shall prevail. The contract specific conditions/documents shall apply in priority.

ZKTeco offers no warranty, guarantee or representation regarding the completeness of any information contained in this manual or any of the amendments made thereto. ZKTeco does not extend the warranty of any kind, including, without limitation, any warranty of design, merchantability or fitness for a particular purpose.

ZKTeco does not assume responsibility for any errors or omissions in the information or documents which are referenced by or linked to this manual. The entire risk as to the results and performance obtained from using the information is assumed by the user.

ZKTeco in no event shall be liable to the user or any third party for any incidental, consequential, indirect, special, or exemplary damages, including, without limitation, loss of business, loss of profits, business interruption, loss of business information or any pecuniary loss, arising out of, in connection with, or

relating to the use of the information contained in or referenced by this manual, even if ZKTeco has been advised of the possibility of such damages.

This manual and the information contained therein may include technical, other inaccuracies or typographical errors. ZKTeco periodically changes the information herein which will be incorporated into new additions/amendments to the manual. ZKTeco reserves the right to add, delete, amend or modify the information contained in the manual from time to time in the form of circulars, letters, notes, etc. for better operation and safety of the machine/unit/equipment. The said additions or amendments are meant for improvement /better operations of the machine/unit/equipment and such amendments shall not give any right to claim any compensation or damages under any circumstances.

ZKTeco shall in no way be responsible (i) in case the machine/unit/equipment malfunctions due to any non-compliance of the instructions contained in this manual (ii) in case of operation of the machine/unit/equipment beyond the rate limits (iii) in case of operation of the machine and equipment in conditions different from the prescribed conditions of the manual.

The product will be updated from time to time without prior notice. The latest operation procedures and relevant documents are available on <http://www.zkteco.com>

If there is any issue related to the product, please contact us.

ZKTeco Headquarters

Address ZKTeco Industrial Park, No. 32, Industrial Road,
Tangxia Town, Dongguan, China.

Phone +86 769 - 82109991

Fax +86 755 - 89602394

For business related queries, please write to us at: sales@zkteco.com.

To know more about our global branches, visit www.zkteco.com.

About the Company

ZKTeco is one of the world's largest manufacturer of RFID and Biometric (Fingerprint, Facial, Finger-vein) readers. Product offerings include Access Control readers and panels, Near & Far-range Facial Recognition Cameras, Elevator/floor access controllers, Turnstiles, License Plate Recognition (LPR) gate controllers and Consumer products including battery-operated fingerprint and face-reader Door Locks. Our security solutions are multi-lingual and localized in over 18 different languages. At the ZKTeco state-of-the-art 700,000 square foot ISO9001-certified manufacturing facility, we control manufacturing, product design, component assembly, and logistics/shipping, all under one roof.

The founders of ZKTeco have been determined for independent research and development of biometric verification procedures and the productization of biometric verification SDK, which was initially widely applied in PC security and identity authentication fields. With the continuous enhancement of the development and plenty of market applications, the team has gradually constructed an identity authentication ecosystem and smart security ecosystem, which are based on biometric verification techniques. With years of experience in the industrialization of biometric verifications, ZKTeco was officially established in 2007 and now has been one of the globally leading enterprises in the biometric verification industry owning various patents and being selected as the National High-tech Enterprise for 6 consecutive years. Its products are protected by intellectual property rights.

About the Manual

This manual introduces the operations of **Horus E2 Series attendance** device.

All figures displayed are for illustration purposes only. Figures in this manual may not be exactly consistent with the actual products.

Features and parameters with ★ are not available in all devices.






Document Conventions

Conventions used in this manual are listed below:

GUI Conventions

For Device	
Convention	Description
< >	Button or key names for devices. For example, press <OK>.
[]	Window names, menu items, data table, and field names are inside square brackets. For example, pop up the [New User] window.
/	Multi-level menus are separated by forwarding slashes. For example, [File/Create/ Folder].

Symbols

Convention	Description
	This represents a note that needs to pay more attention to.
	The general information which helps in performing the operations faster.
	The information which is significant.
	Care taken to avoid danger or mistakes.
	The statement or event that warns of something or that serves as a cautionary example.

Catalogue

1	OVERVIEW	8
2	INSTRUCTIONS FOR USE	8
2.1	STANDING POSITION, FACIAL EXPRESSION AND STANDING POSTURE	8
2.2	FINGER PLACEMENT ★	10
2.3	FACE ENROLLMENT	10
2.4	STANDBY INTERFACE	11
2.5	VIRTUAL KEYBOARD	12
2.6	VERIFICATION MODE	12
2.6.1	PASSWORD VERIFICATION	12
2.6.2	FACIAL VERIFICATION	14
2.6.3	FINGERPRINT VERIFICATION ★	16
2.6.4	CARD VERIFICATION	17
3	MAIN MENU	19
4	USER MANAGEMENT	20
4.1	ADD USER	20
4.2	QUERY USERS	32
4.3	EDIT USERS	34
4.4	DELETE USER	36
5	ACCESS CONTROL SETTINGS	38
5.1	ACCESS CONTROL OPTIONS	39
5.2	TIME RULES SETTING	40
5.3	HOLIDAY SETTINGS	41
5.4	VERIFICATION COMBINATION SETTING	44
5.5	ANTI-PASSBACK SETTINGS	46
5.6	DURESS ALARM SETTING	48
6	ATTENDANCE RECORD QUERY	49
7	DATA MANAGEMENT	52
8	ALARM MANAGER	53
8.1	ADD AN ALARM CLOCK	53
8.2	EDIT ALARM CLOCK	59
8.3	DELETE ALARM CLOCK	61
9	SYSTEM SETTINGS	65

9.1	NETWORK SETTINGS	65
9.1.1	WI-FI SETTINGS	66
9.1.2	MOBILE DATA	66
9.1.3	COMMUNICATION CONNECTION SETTINGS	67
9.2	DATE AND TIME	68
9.2.1	DATE AND TIME SETTINGS	69
9.2.2	DATE AND TIME FORMAT SETTINGS	71
9.3	ATTENDANCE PARAMETER SETTING	72
9.3.1	ATTENDANCE EVENTS	73
9.3.2	STATE MODE	83
9.3.3	PHOTOGRAPHY MODE	91
9.3.4	VERIFICATION SETTINGS	92
9.3.5	VALIDITY PERIOD OF USER INFORMATION	93
9.4	CLOUD SERVICE SETTINGS	94
9.5	WIEGAND SETTINGS	95
9.5.1	WIEGAND IN	95
9.5.2	WIEGAND OUT	97
9.6	DISPLAY SETTINGS	98
9.7	SERIAL PORT SETTINGS	99
9.8	SOUND SETTINGS	100
9.9	BIOMETRIC PARAMETERS	100
9.10	AUTOMATIC TESTING	103
9.11	ADVANCED SETTING	104
9.12	ABOUT DEVICE	105
10	CONNECT TO ZKBIOTIME SOFTWARE	106
10.1	SET THE COMMUNICATION ADDRESS	106
10.2	ADD DEVICE ON THE SOFTWARE	107
10.3	ADD PERSONNEL ON THE SOFTWARE	107
	PRIVACY POLICY	108
	ECO-FRIENDLY OPERATION	110

1 Overview

The Horus E2 from ZKTeco is an Android-based multi-biometrics terminal designed to streamline both time attendance and access control. Leveraging ZKTeco's cutting-edge technology, the Horus E2 supports a variety of authentication methods, including facial recognition, fingerprint scanning, multi-tech card verification, and QR code scanning. These features meet the diverse needs of users across various environments. The device ensures reliable connectivity through dual-frequency Wi-Fi and LTE, facilitating seamless network integration. The Horus E2 is compatible with Android 10 operating system, which simplifies the integration with third-party applications. Additionally, it includes an optional removable backup battery, enhancing its reliability and making it an ideal solution for mobile time attendance and temporary site management.

The Horus E2 comes standard with a B133 card module that supports identification ID and IC cards. The Horus E2 also perfectly supports Elatec card modules and can support 125 kHz/134.2 kHz/13.56 MHz RFID cards without replacing the card module.

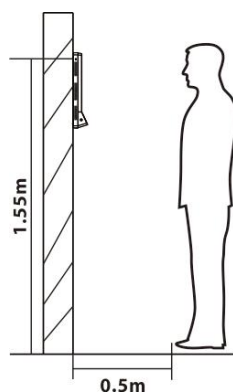
If the above-mentioned function cannot meet customers' needs, we can provide an EDK embedded development kit and adjustment tools. Based on our robust and stable platform, the client's R&D team can quickly develop, integrate, and debug the entire embedded system for better scalability.

2 Instructions for Use

2.1 Standing Position, Facial Expression and Standing

Posture

Recommended Distance

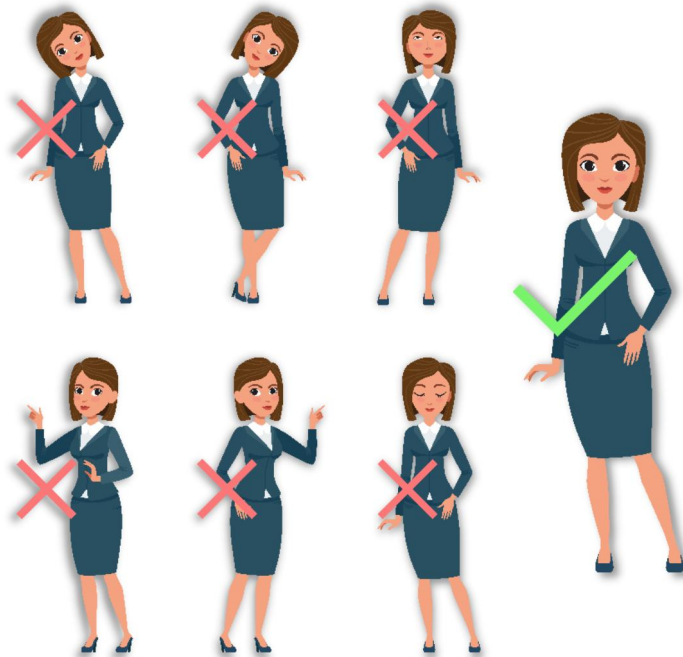


The distance between the device and the user (whose height is within 1.55m to 1.85m) is recommended to be 1.5m. Users may slightly move forward and backward to improve the quality of the captured facial images.

Recommended Facial Expressions



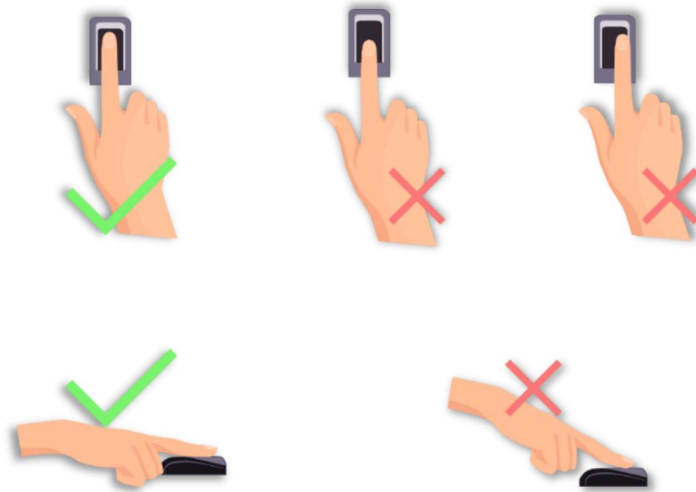
Recommended Standing Postures



Note: During enrolment and verification, please remain natural facial expression and standing posture.

2.2 Finger Placement ★

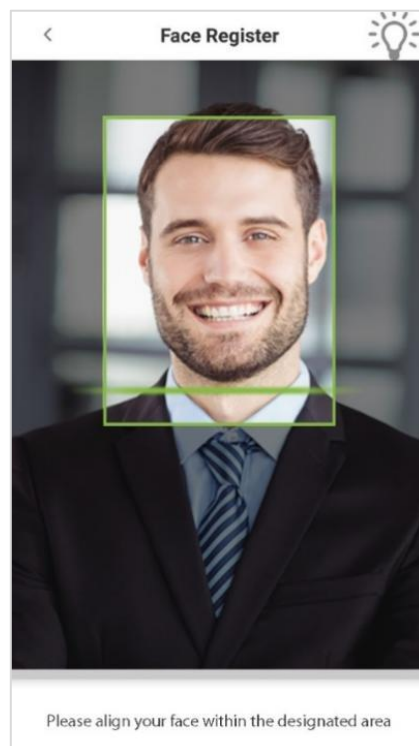
- **Recommended fingers:** Index, middle, or ring fingers.
- Avoid using the thumb or pinky, as they are difficult to accurately tap onto the fingerprint reader.



Note: Please use the correct method when pressing your fingers onto the fingerprint reader for registration and identification.

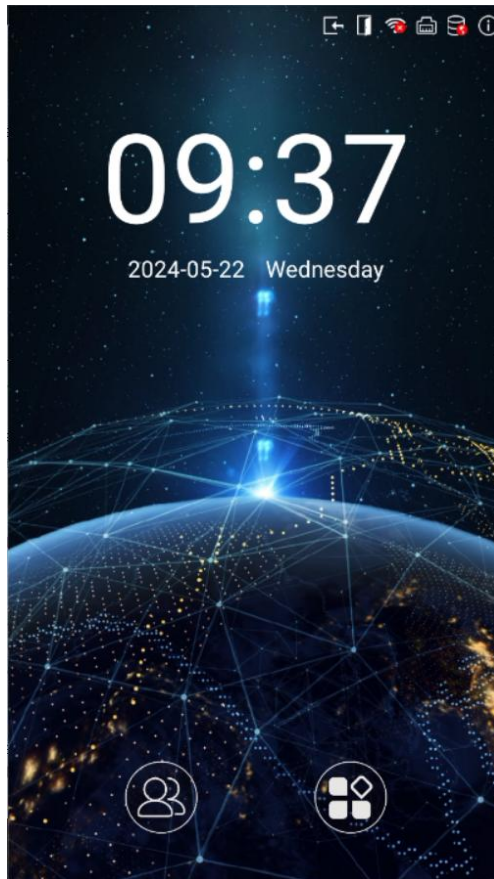
2.3 Face Enrollment

During enrollment, try to adjust your face in the center of the device screen. Please face the camera and stay still. The device screen is shown below:





2.4 Standby Interface

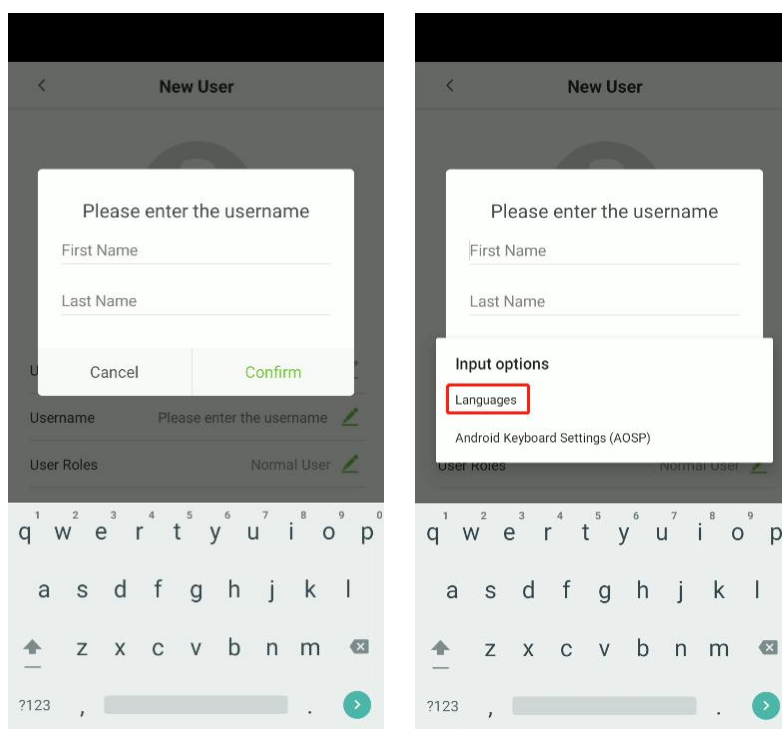
After connecting the power supply, the Device displays the following standby interface.



Notes:

1. Tap on  the button to enter the personnel ID Input screen.
2. Tap on  the button to enter the main menu.
3. If a super administrator has already been registered for this device, you will need the permission of the super administrator to enter the main menu.

2.5 Virtual Keyboard



Note: The kinds of keyboards of device will accord to the system language.

- Long press the “,” button, to set the language of keyboards.

2.6 Verification Mode

The Biometric matching process can be categorized as, One-to-many or “Identification” (1: N), and one-to-one or “Verification” (1:1). Below is a description of each matching type and how its features are described.

1: N Identification Process

A one-to-many (1: N) biometric identification process instantly compares the person’s captured biometric template against all stored biometric templates in the system.

1:1 Verification Process

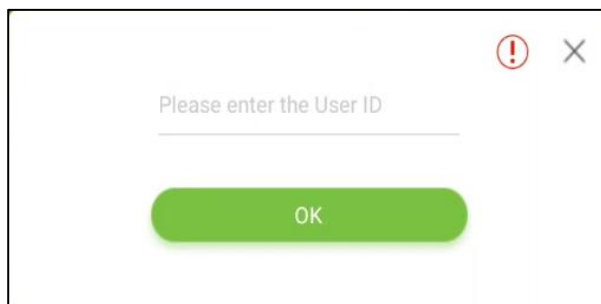
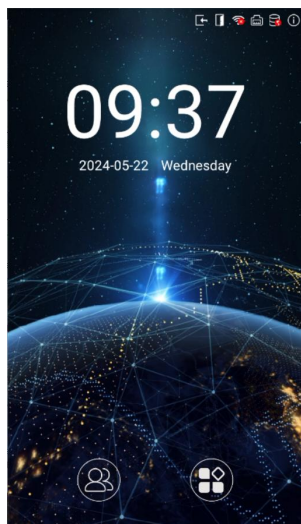
1:1 biometric verification process authenticates a person’s identity by comparing the captured biometric template with a biometric template of that person pre-stored in the database.

2.6.1 Password Verification

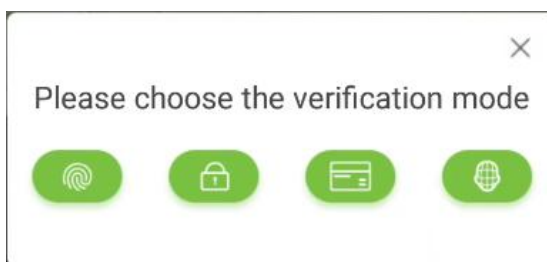
When a user inputs his/her user ID and password into the device, the data will be compared to the user ID and password of that user pre-stored in the system. This process is recommended for administrator users.


- On the **Main** screen, tap on  the button to enter the 1:1 password verification mode.

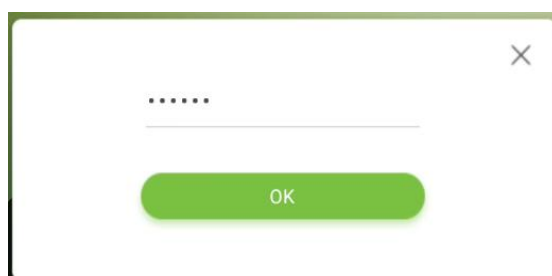
- On the **Input** screen, enter the User ID and tap **[OK]**.



- If a user has registered a face, a fingerprint and card in addition to his/her password and the verification method is set to fingerprint/ password/ card/ face verification, the below screen will appear.



- Tap on  the password button to enter password verification mode. Enter password and tap **[OK]**.



- Below are the sample for successful and unsuccessful verification



Successful Verification

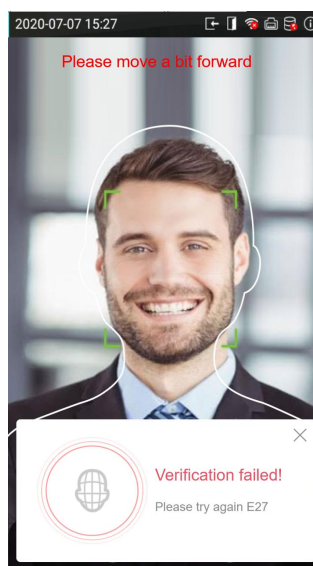
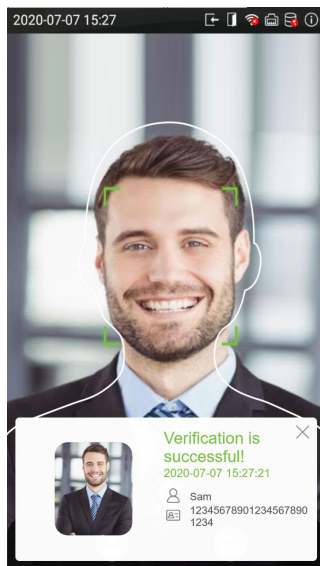


Failed Verification


2.6.2 Facial Verification

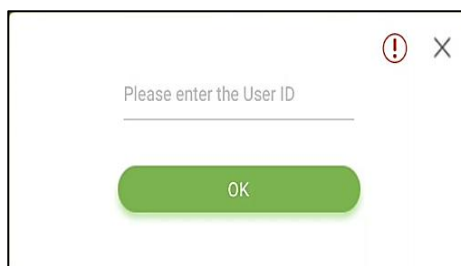
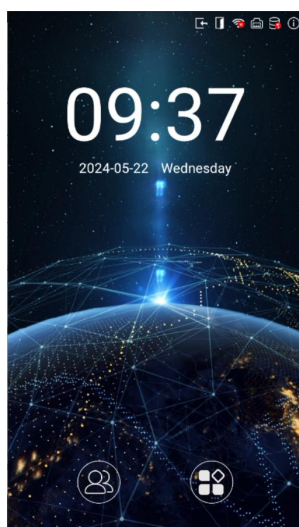
1: N Face Identification

- This method identifies the acquired facial image of the user with all the facial templates that are stored in the device.
- Below are the sample for successful and unsuccessful identification.




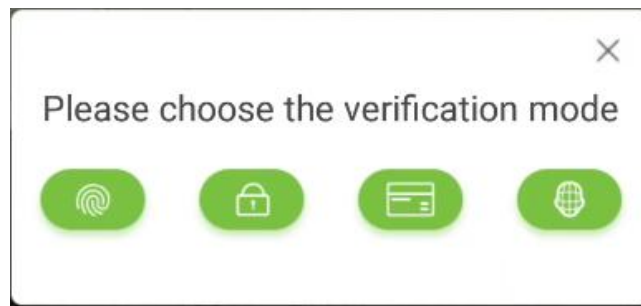
1:1 Face Verification

- This method verifies the face of the user captured by the camera with the facial template related to that User ID provided by the user.
- Tap  on the **Main** interface to enter the 1:1 facial verification mode. Input the User ID, tap [OK].

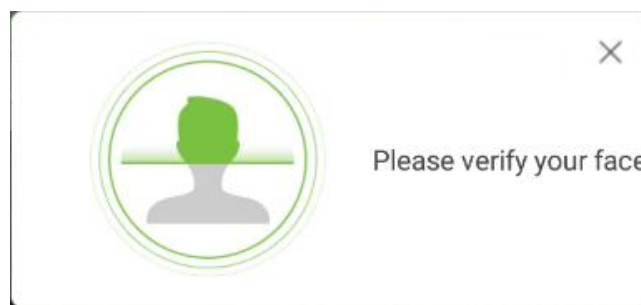


- If a user has registered a fingerprint, a password and card in addition to his/her face and the verification method is set to fingerprint/ password/ card/ face verification, the following screen will appear.

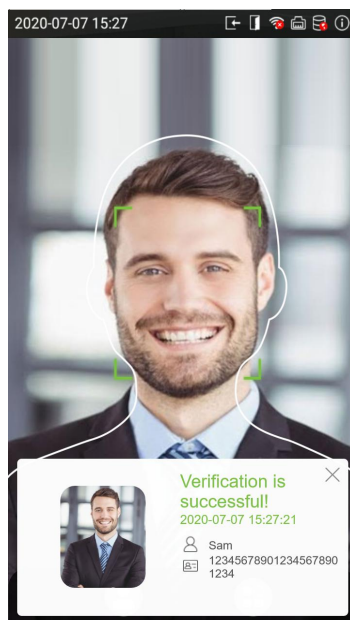
- Tap on the face button  to enter the facial verification mode.



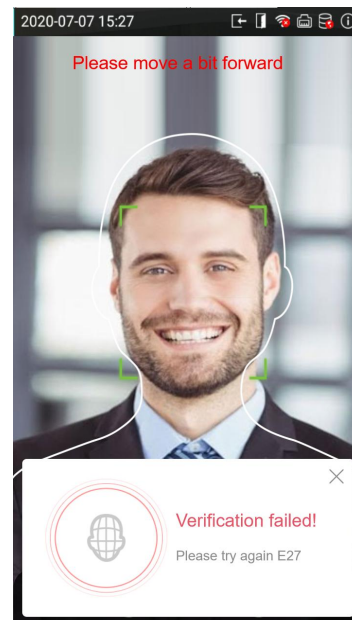
- After the prompt "Please verify your face ", adjust your face in the center of the device screen for face verification.



- Below are the sample for successful and unsuccessful verification.



Successful Verification



Failed Verification

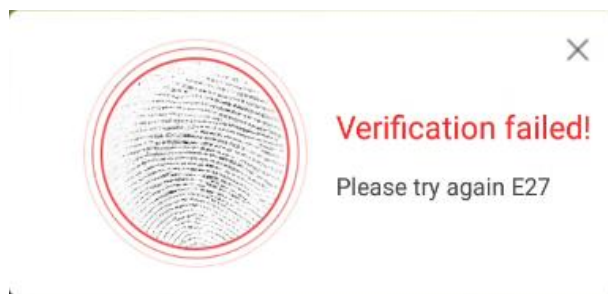
2.6.3 Fingerprint Verification ★

1: N Fingerprint Identification

- This method compares the fingerprint of the user that is being pressed onto the fingerprint reader with all the fingerprint data that is pre-stored in the device.
- To enter fingerprint identification mode, simply tap your finger on the fingerprint reader.
- Below are the sample for successful and unsuccessful identification.




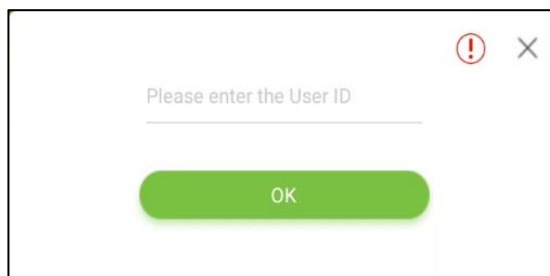
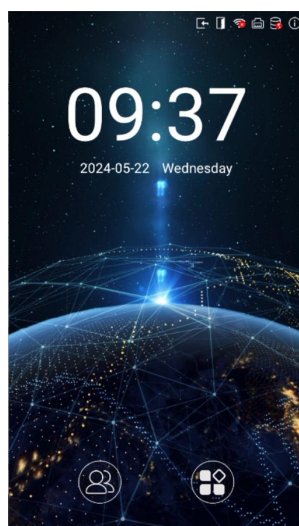
Successful Verification




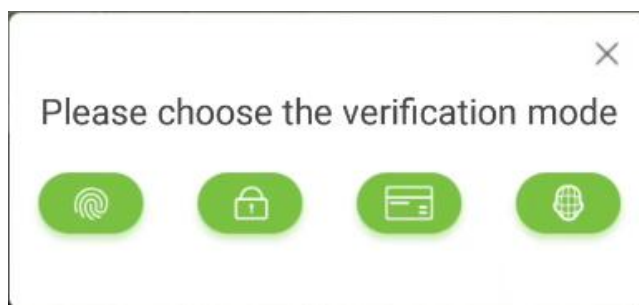
Failed Verification

1:1 Fingerprint Verification

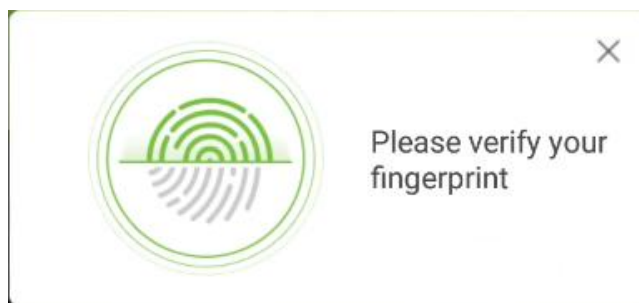
- This method compares the fingerprint of the user that is being pressed onto the fingerprint reader with the fingerprint templates that are linked to that User ID which has been entered via the virtual keyboard.
- Tap the  button on the main screen to enter 1:1 fingerprint verification mode:
- Enter the User ID and Tap [OK].



- If a user has registered a face, a password and card in addition to his/her fingerprint and the verification method is set to fingerprint/ password/ card/ face, the following screen will appear.
- Select the fingerprint button  to enter fingerprint verification mode.



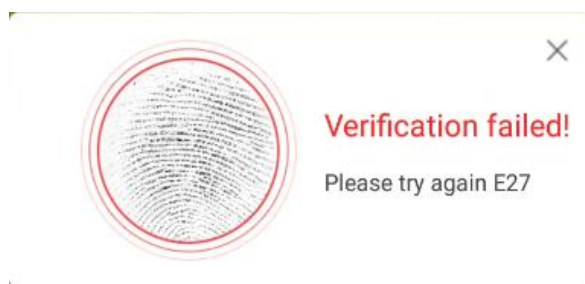
- Tap the finger on the fingerprint reader to proceed with verification.



- Below are the sample for successful and unsuccessful verification.



Successful Verification



Failed Verification

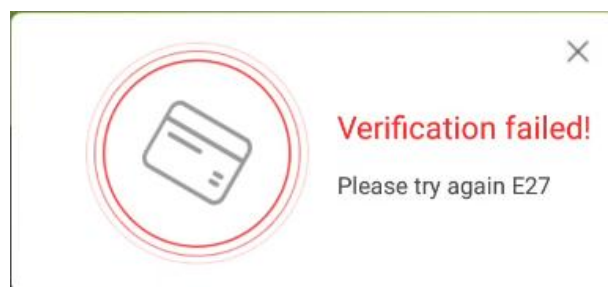
2.6.4 Card Verification

1: N Card Identification

- To enter 1: N card identification mode, please place the registered card on the card reader.
- Below are the sample for successful and unsuccessful identification.




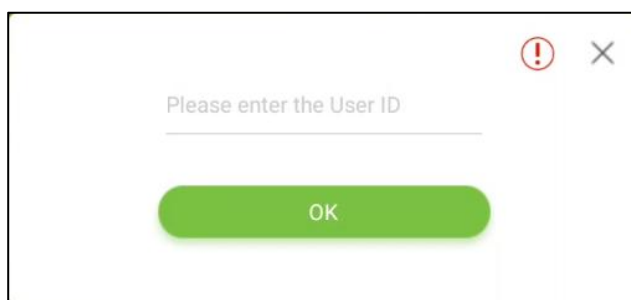
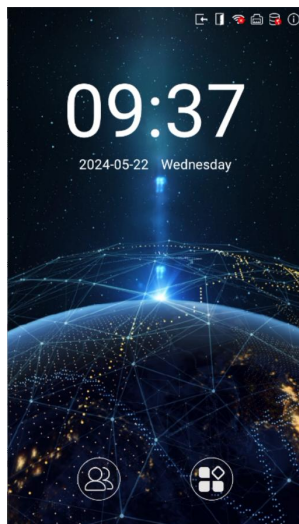
Successful Verification




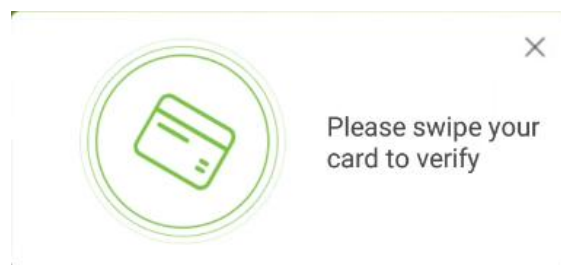
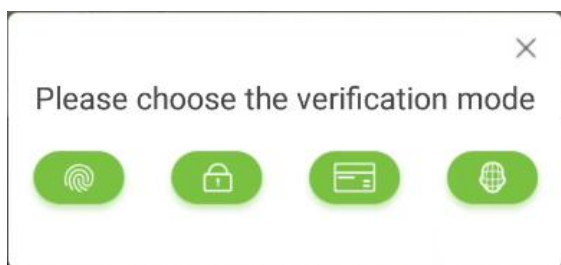
Failed Verification

1:1 Card Verification

- To enter 1:1 card verification mode, tap the  button on the main screen to enter 1:1 card verification mode.
- After that, enter the User ID and tap **[OK]**.



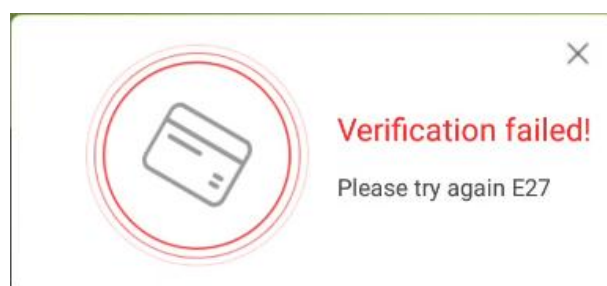
- If a user has registered a face, a password and fingerprint in addition to his/her card and the verification method is set to fingerprint/ password/ card/ face verification, the below screen will appear.
- Tap on the card button  to enter card verification mode. After that, swipe the card to verify.



- Below are the sample for successful and unsuccessful identification.




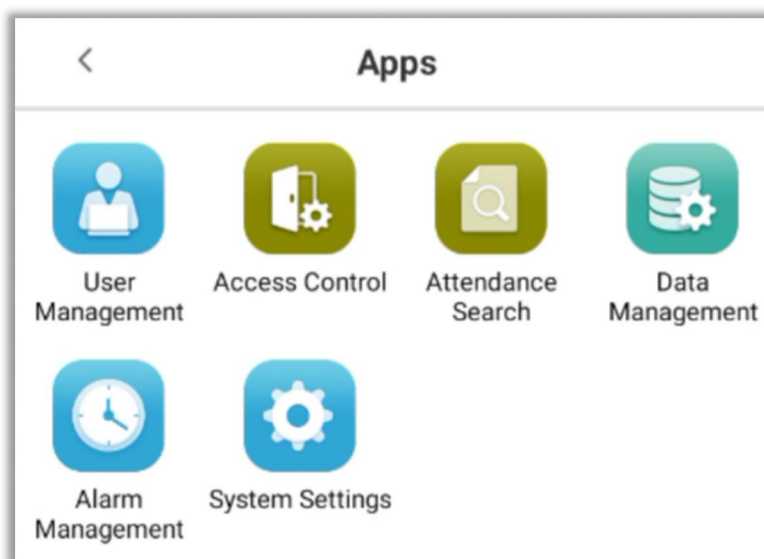
Successful Verification



Failed Verification

3 Main Menu

Click  to open the main menu



Menu	Function Description
User Management	Add, edit, and view user information.
Access Control	Set the access control parameters, time rules, holidays, unlocking combinations, access control groups, and other functions.
Attendance Search	Display detailed attendance records of all users.
Data Management	Manage data on your device.
Alarm Management	After setting the alarm, when the designated time arrives, the device will automatically play the pre-selected ringtone. If it is manually turned off or the duration is over, the ringtone will stop.
System Settings	It mainly includes network settings, date and time, attendance parameters/access control record settings, cloud server settings, Wiegand settings, display settings, sound settings, biometric parameters, automatic testing, advanced settings, serial port, about the device, security settings, and restarting the device.



Note: If the device does not have a super administrator, any user can open the menu by pressing this




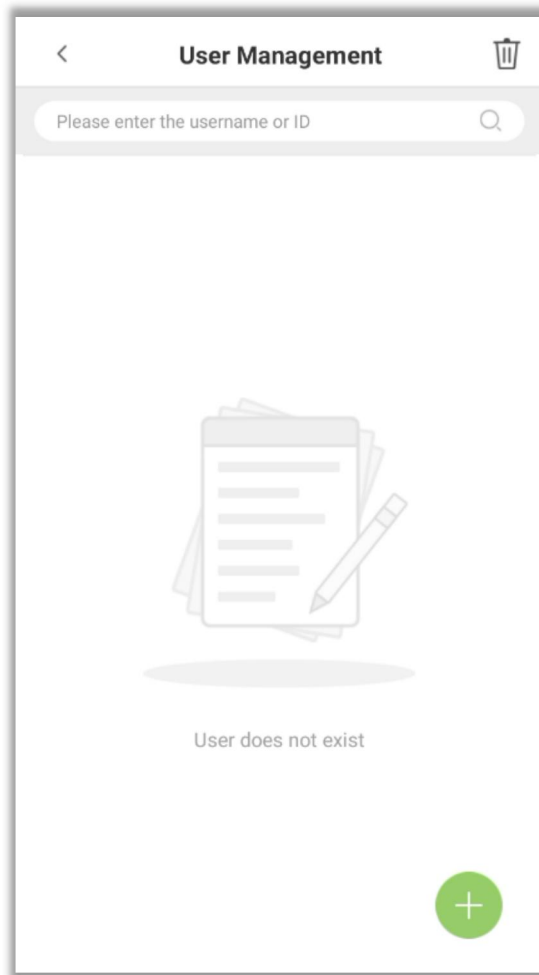
key. After setting a super administrator on the device, opening the menu requires authentication.

After successfully authenticating the password, the user can enter the menu. To ensure the security of the device, it is recommended to register an administrator when using the device for the first time. For specific instructions, see the "Adding Users" section.

4 User Management

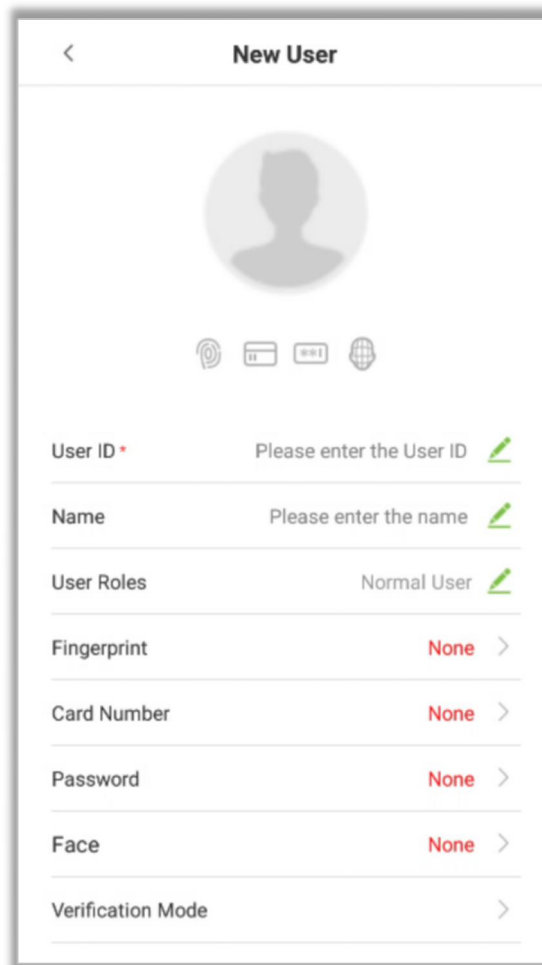
4.1 Add User

Click "User Management"  to open the interface for adding users.



Add user information



Enter the user ID in the [User ID] field and the user name in the [Name] file.

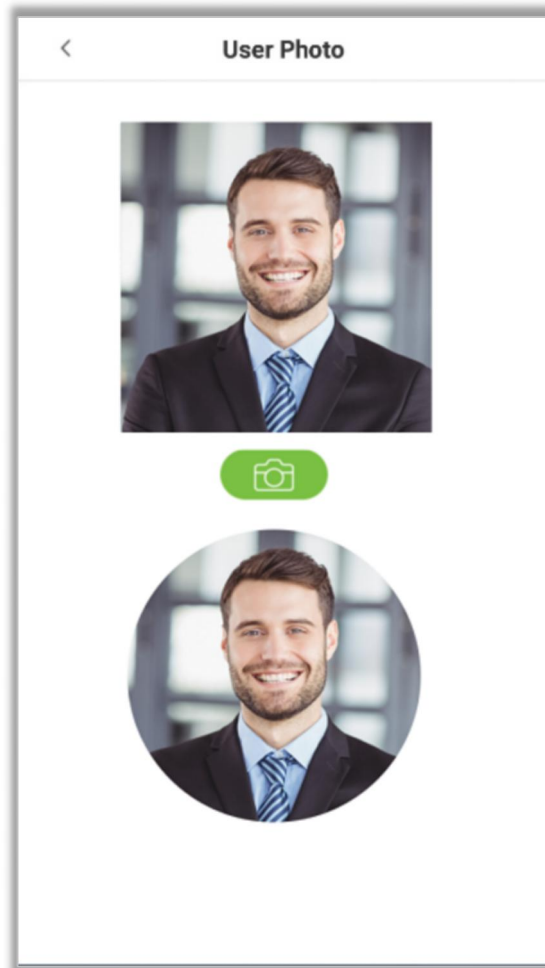


Attention:

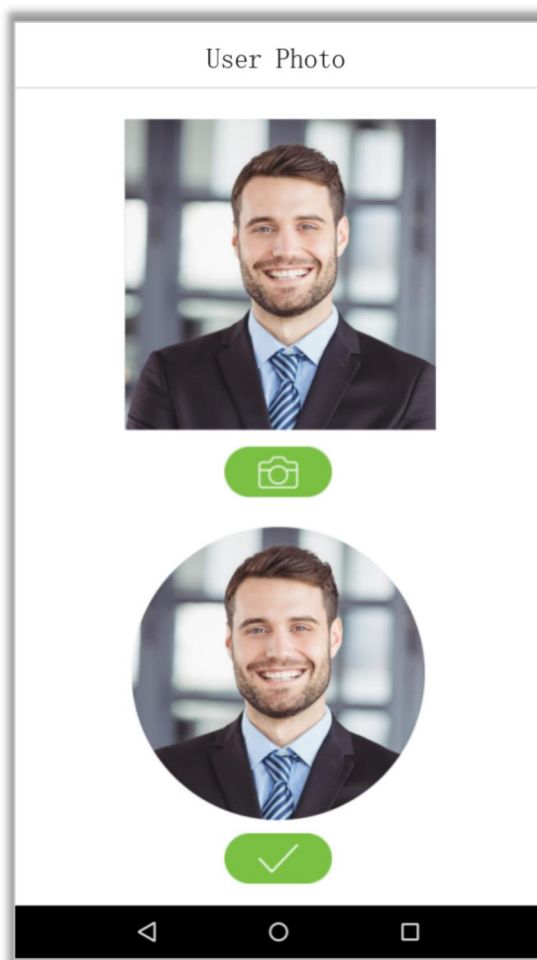
1. This name refers to the user name. The maximum length is 64 characters, including 32 characters for the last name and 32 characters for the first name.
2. By default, the device supports a maximum of 9-digit user IDs.
3. The user ID can be modified during the first registration. After the first registration, the "user ID" cannot be modified.
4. The message "duplicate job number, please re-enter" indicates that the ID number you entered has already been used. Please enter a different ID number.

User photo registration

1. Click the  icon to open the camera interface. The user should face the camera and adjust the position. Click the  icon to take a picture.



2. Click  at the bottom of the interface to complete the addition of photos.



Register verification mode

Authentication methods are the ways to verify login. This includes registering faces, passwords, fingerprints★, or card numbers. Choose the authentication mode that best suits your needs.

After setting the user ID, the user can set the fingerprint ★, card, face and password as follows:

Fingerprint	None	>
Card Number	None	>
Password	None	>
Face	None	>

Register fingerprints ★

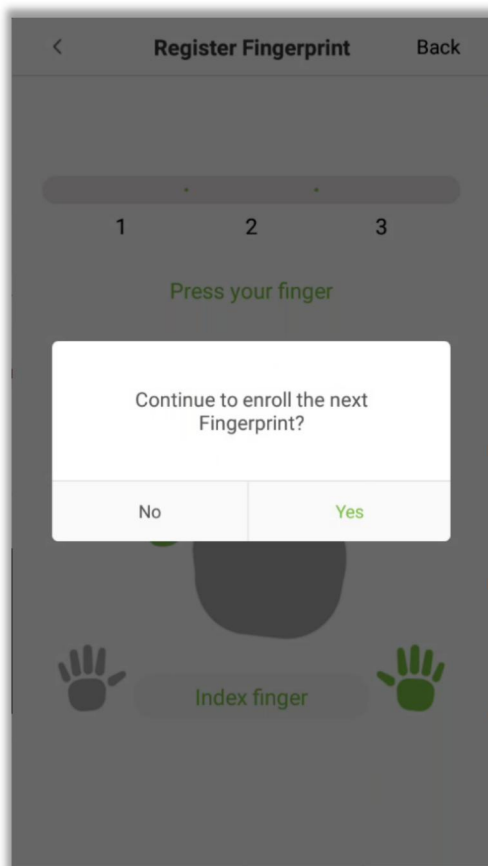
1. In the user registration interface, tap [Fingerprint] to enter the fingerprint registration interface. Select the icon on the left or right side of the screen, then tap the finger you want to register.



2. Press the same finger on the fingerprint reader three times. A green bar indicates successful fingerprint registration
3. If you press a different finger on the fingerprint scanner for the second and third times, the system will prompt you to "Please use the same finger".

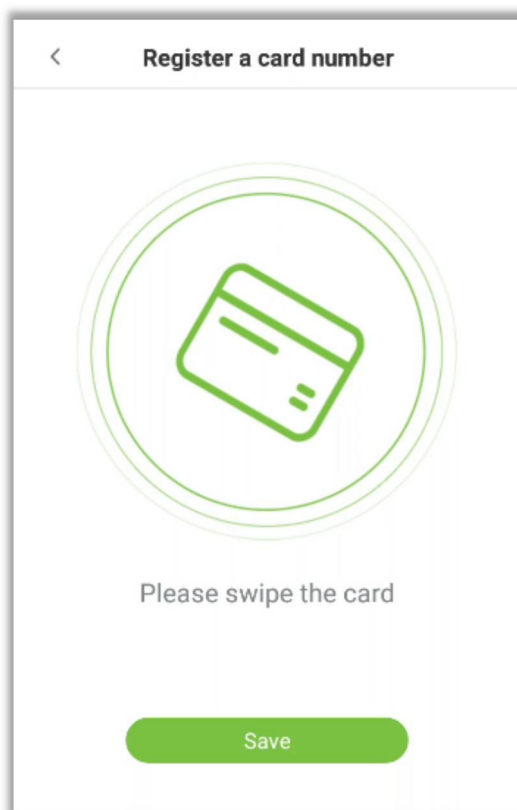


4. If the fingerprint registration is successful, the system will pop up a dialog box asking "Do you want to continue registering the next fingerprint?" Press [Yes] to register the next fingerprint, or press [No] to return to the fingerprint registration interface.






Register card number

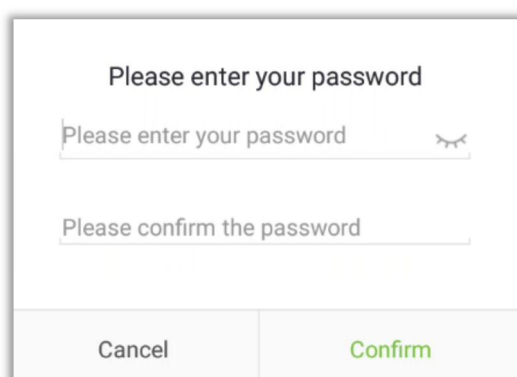
In the user registration interface, click [Card No.] to enter the card number registration page. After the prompt is successful, click Save.



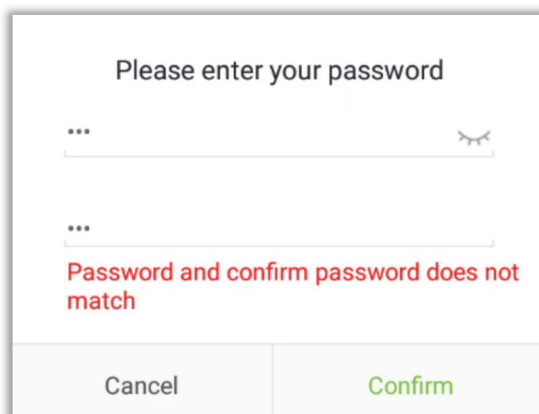
Register password

1. In the user registration interface, click [Password] to enter the registration password interface. Enter the password in the [Enter Password] column, and then enter the password again in the [Enter Password] column. Then, click [Save].

 Note: The user password must be greater than 6 digits and up to 8 digits. Click  to hide the password; click  to make the password visible, as shown in the following figure:



2. If the passwords in the two fields do not match, you must re-enter the password.



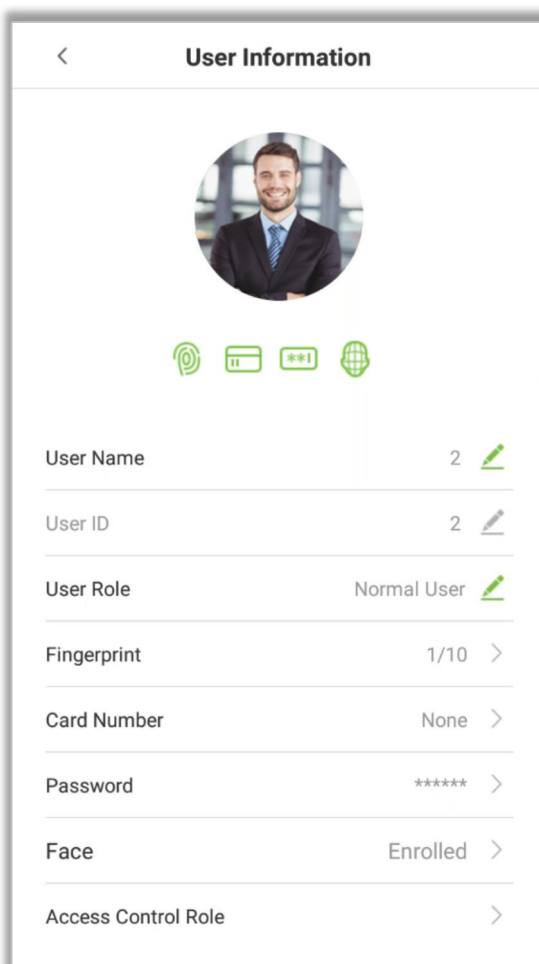
Please enter your password

Password and confirm password does not match


Cancel Confirm





Delete/Update Password


1. In the "User Management" interface, tap the user in the user list to enter the user information interface, and tap "Password"





< User Information



User Name 2 

User ID 2 

User Role Normal User 

Fingerprint 1/10 >

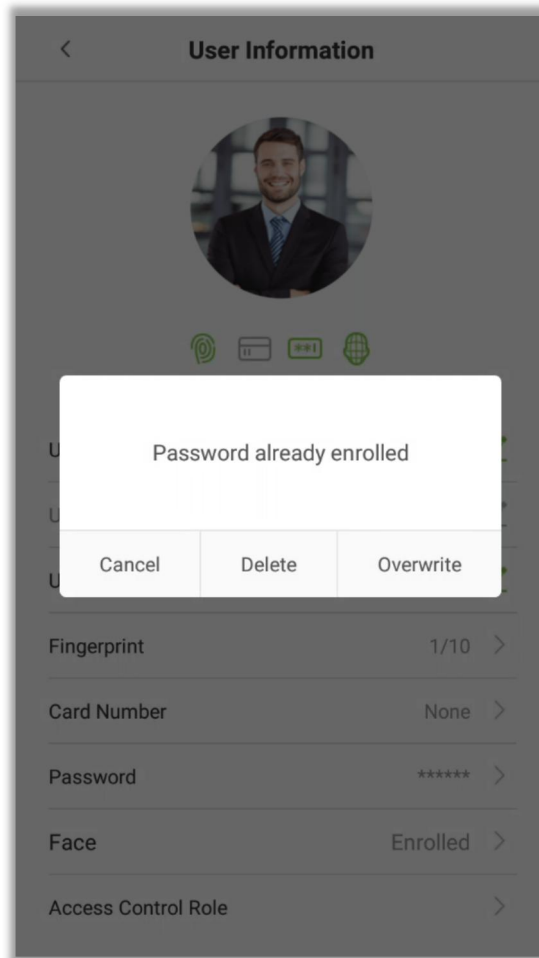
Card Number None >

Password ***** >

Face Enrolled >

Access Control Role >

2. Press the [Delete]/[Overwrite] button in the pop-up dialog box.



Register Face

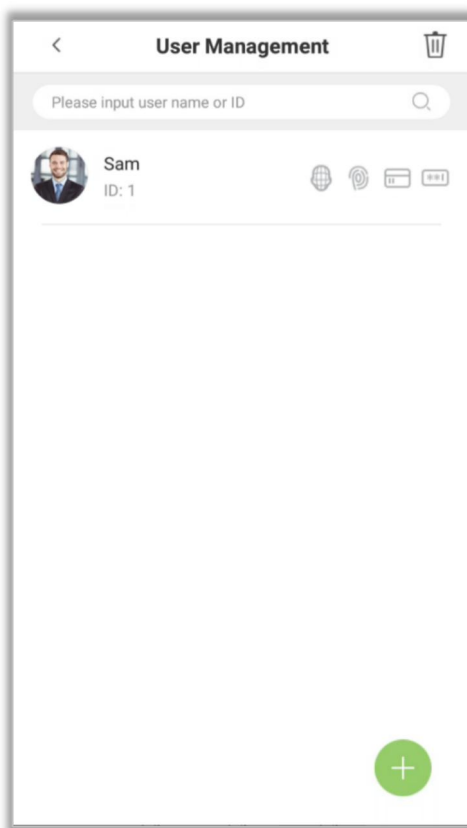
In the user registration interface, tap [Face] to enter the face registration interface. Move and adjust your face on the registration area.



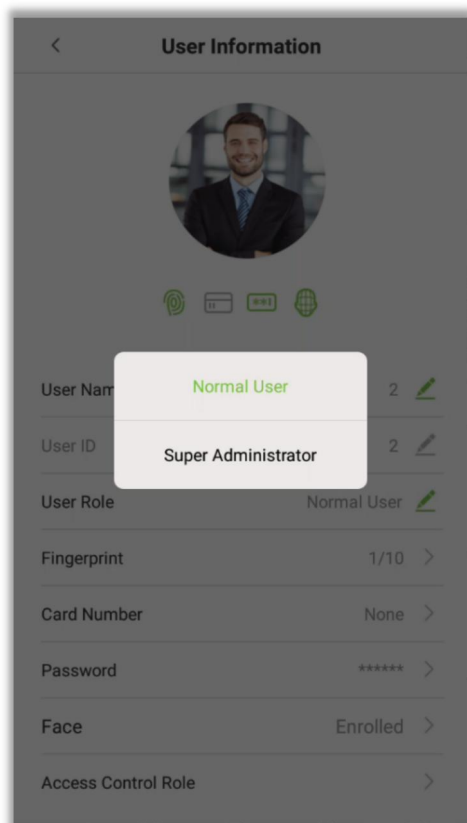
User Role

Users using this device have two types of permissions: "regular users" and "super administrators". After registering a super administrator on the device, regular users can only use the registered authentication methods for authentication. Super administrators have the same permissions as regular users and can open the main menu.

1. In the "User Management" interface, tap on a user in the user list to view that user's information.



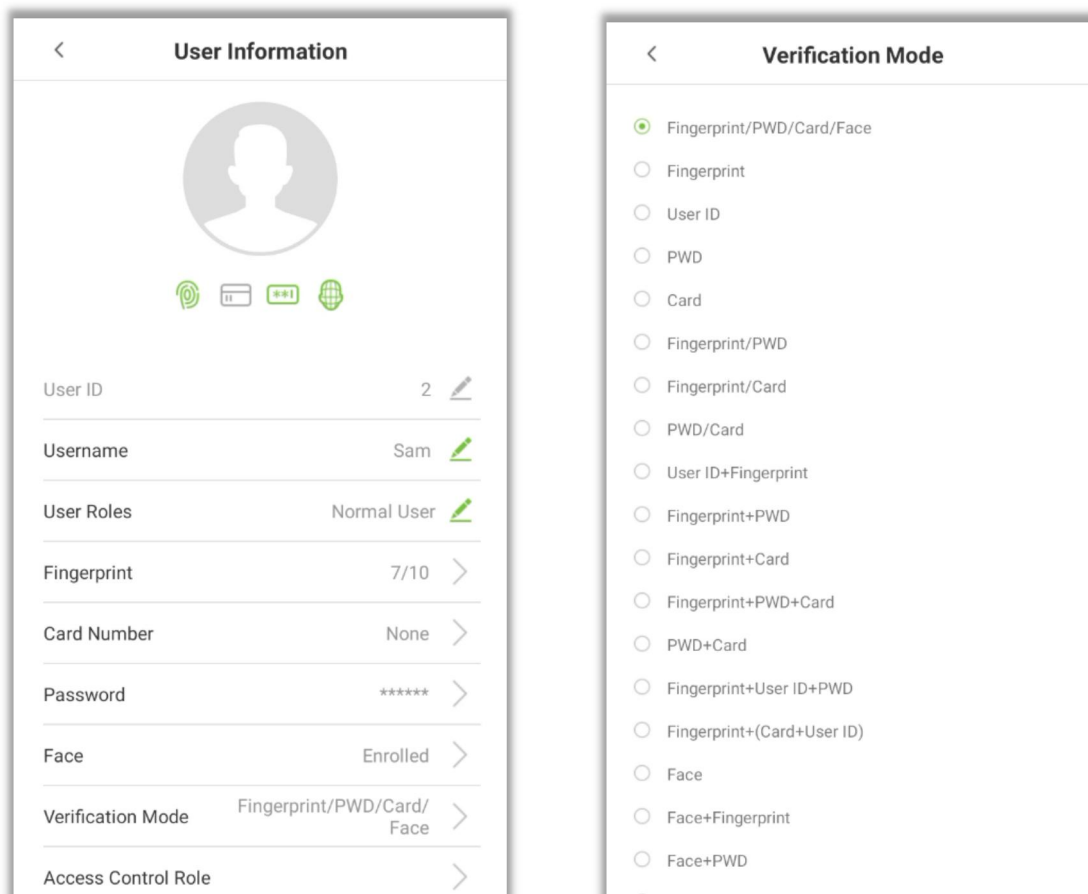
2. After entering the "User Information" interface, click on [User Role] and select [Normal User] or [Super Administrator] in the pop-up window.



Note: When a user is granted super administrator permissions, they must verify before accessing the main menu. The verification process depends on the authentication method used during user registration. Please refer to Authentication Methods for more information. Only users who have registered an authentication method can be set as administrators.

Verification mode

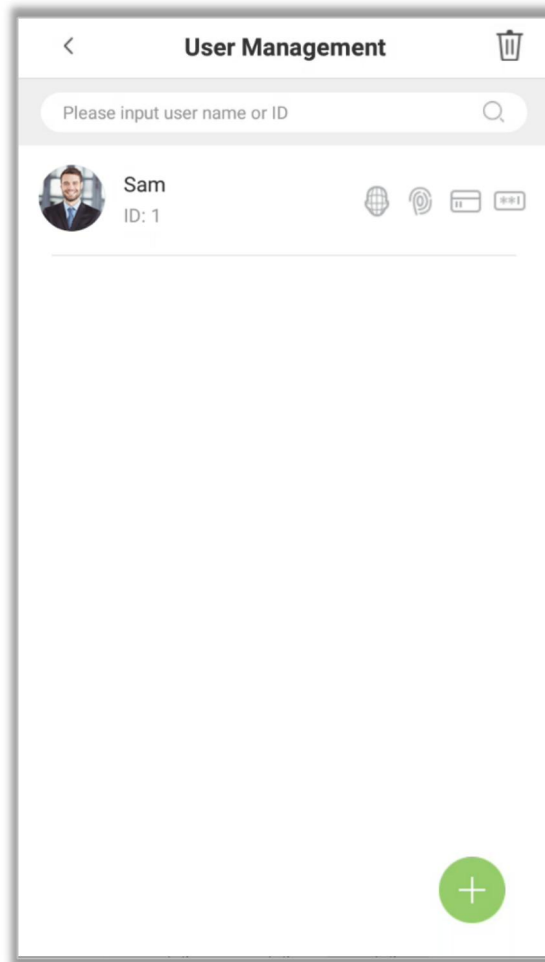
1. In the user information interface, click the **[Verification Mode]** field.
2. Select **[Verification Mode]** and click it to automatically return to the "User Management" interface.



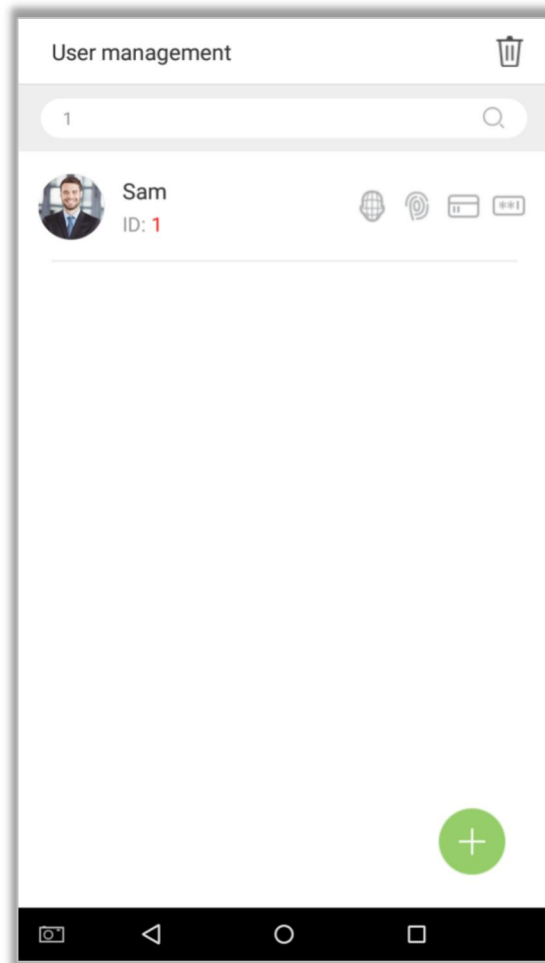
Note: Fingerprint authentication is optional function

4.2 Query Users

1. In the search bar of the [User Management] interface, tap and enter a keyword (Note: you can search based on user ID or name).

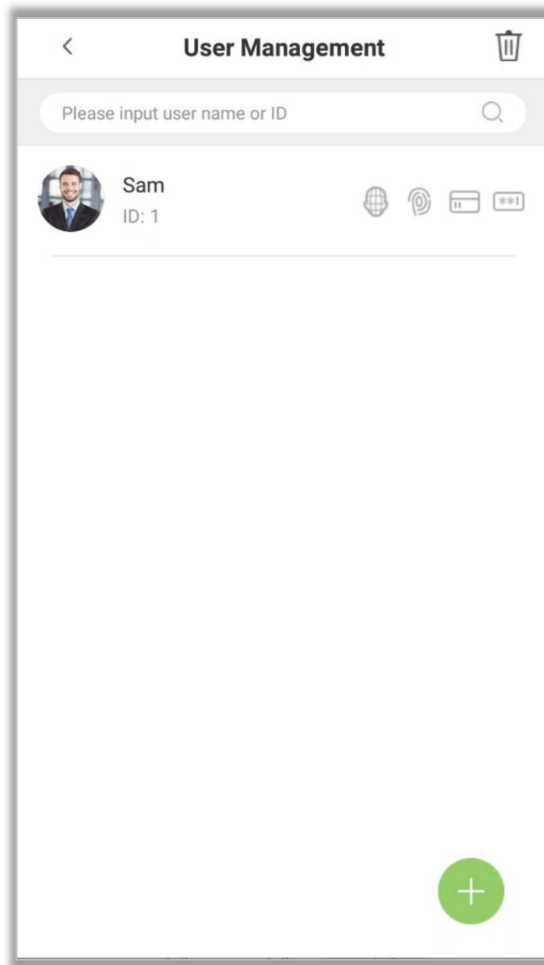


2. The system will automatically display the query results based on the query criteria.



4.3 Edit Users


1. Select a user from the user list.







2. Edit the required user details.

<


User Information






User Name

2




User ID

2



User Role

Normal User



Fingerprint

1/10

>

Card Number

None

>

Password

>


Face

Enrolled


>

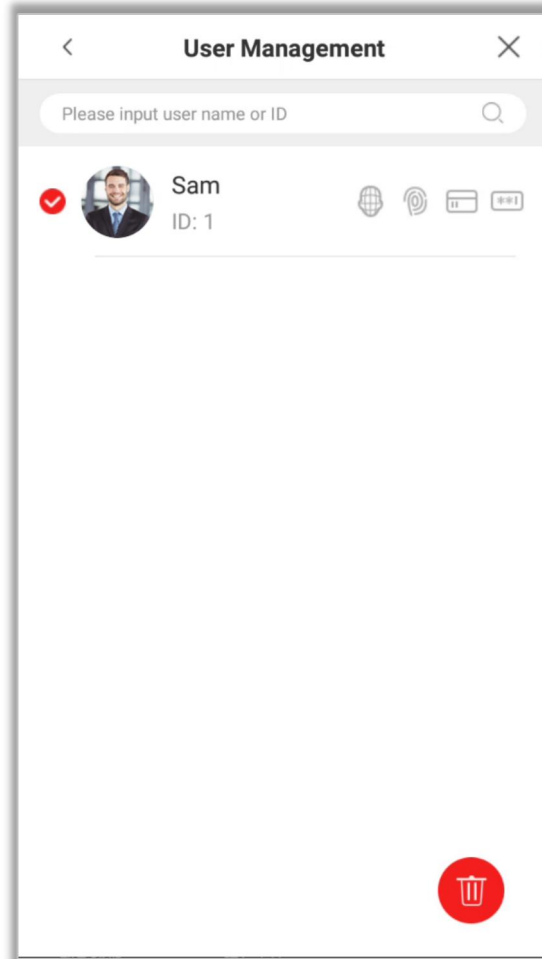
Access Control Role


>

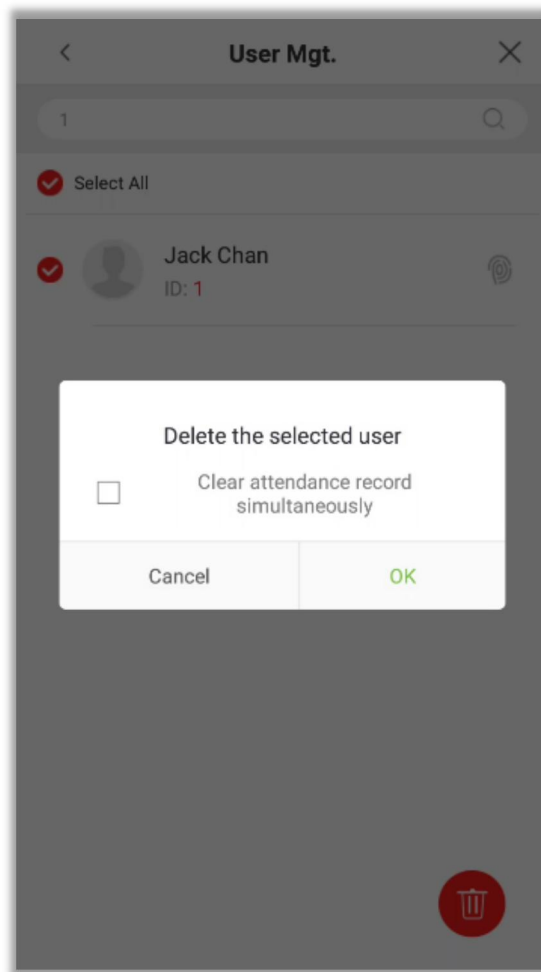
 Note: The User ID field cannot be modified. For additional details on adding user details, see Adding Users

4.4 Delete User

1. In the "User Management" interface, tap the  button in the upper right corner of the interface.



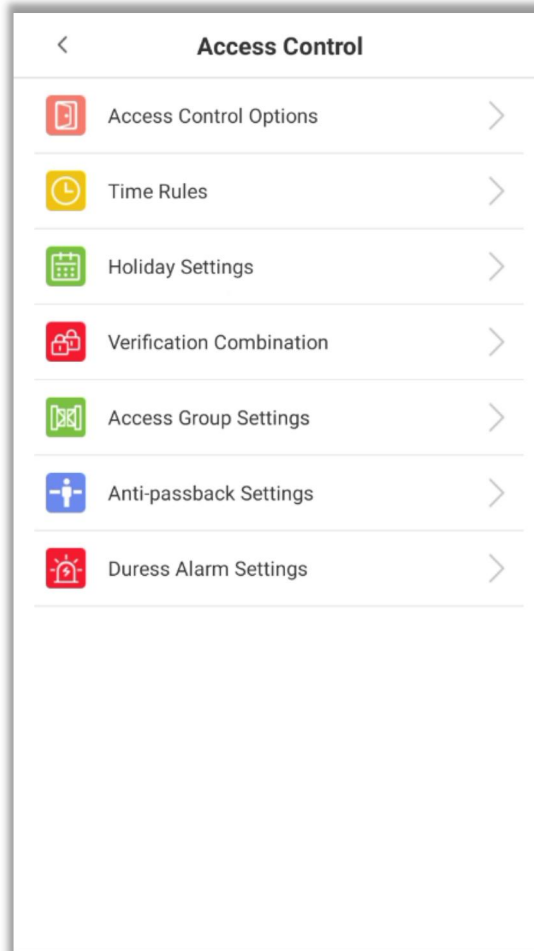
2. Select the user to delete and click the  icon in the lower right corner to bring up a window. If the user wishes to delete attendance records at the same time, please select the check box. Click [OK] (this option can be selected or not selected according to your needs).



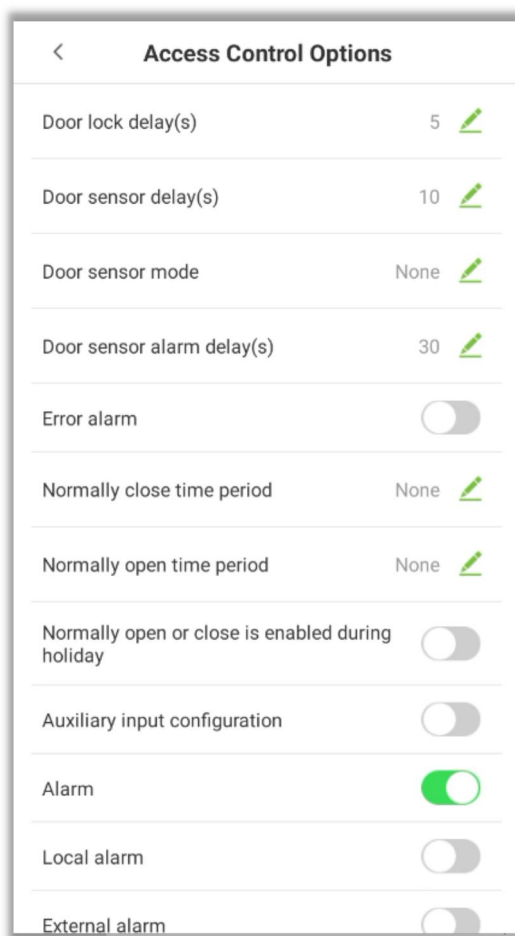
Note: If you select "Clear attendance records at the same time", all the relevant information of the user will be cleared.

5 Access Control Settings

The access control setting function can perform simple access control settings.



5.1 Access Control Options



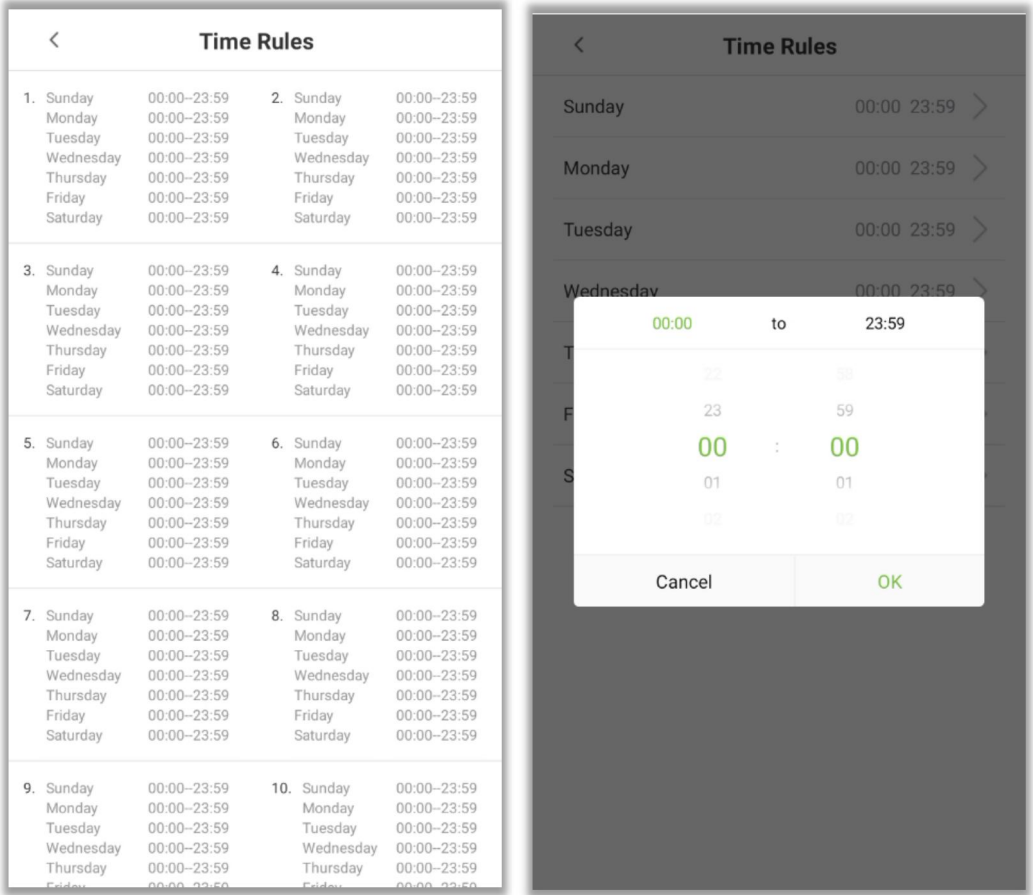
Menu	Function Description
Door lock delay (s)	Set parameter N. After the access control is opened, it will automatically close after N seconds, with a range of 1-254 seconds.
Door sensor delay (s)	Delay the time of checking the door sensor after the door is opened, ranging from 1 to 255 seconds.
Door sensor mode	It is divided into closed (the device does not detect the door magnetic status), normally open (if the door is closed, an alarm will occur), and normally closed (if the door is open, an alarm will occur).
Door sensor alarm delay(s)	After the door is opened, when the time set for the door magnetic delay is reached, the door magnetic sensor begins to detect the door magnetic state. If the door magnetic state is inconsistent with the mode set for the door magnetic mode, an alarm will occur within the range of 0-999 seconds.
Error alarm	After opening, you can set the number of times of wrong alarm and the time interval of wrong alarm.
Normally close time period	A normally closed time period can be set, during which the lock is in a normally closed state.

Normally open time period	A normally open time period can be set, during which the lock is in a normally open state.
Normally open or close is enabled during holiday	Support the implementation of normally open and normally closed time periods during holidays.
Auxiliary input configuration	The types are divided into triggering door opening, triggering alarm, triggering door opening and alarm.
Alarm	It is divided into local alarm and external alarm.
Restore access control settings	Reset the access control settings.

5.2 Time Rules Setting

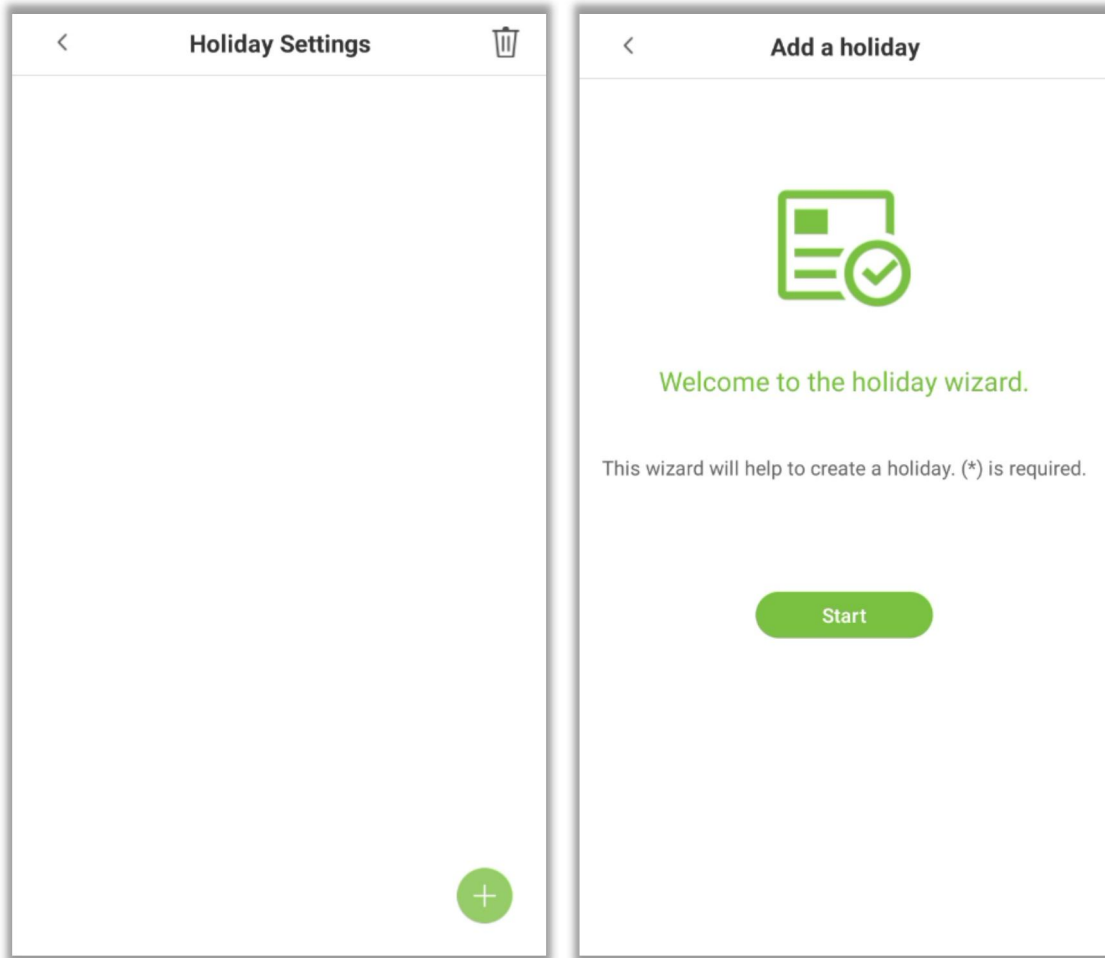
Up to 50 time rules can be defined (default is Rule1), each of which includes seven days of the week and a standard 24-hour time period for each day. Users can only validate within valid time periods. Each user can set up to three time rules, and the relationship between these time periods is "or".

In the Time Rule interface, tap to set the "Time Period", and in the "Time Period 1" interface, set the start and end times, then tap "OK".



5.3 Holiday Settings

1. Tap  to enter the new holiday interface, and tap "Start" to create a new holiday.



2. In the [Add Holiday] interface, select the holiday number, start time, end time, and time period, and then click [Next].

In this interface, tap "Done" to successfully add the newly created holiday, or tap "Continue to add" to create another holiday.

<

Add a holiday

Holiday number *

2 >

Start Time *

06-06 >

End Time *

06-06 >

Period *

1 >


Back

Next

<

Add a holiday

The holiday is created successfully!



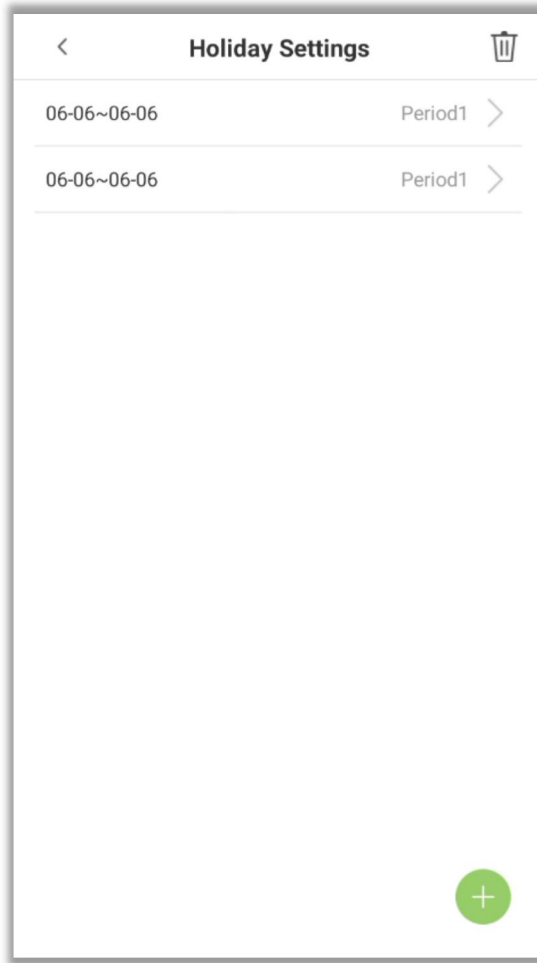
The holiday is successfully added. Tap continue to add new holidays or tap Exit.


Continue

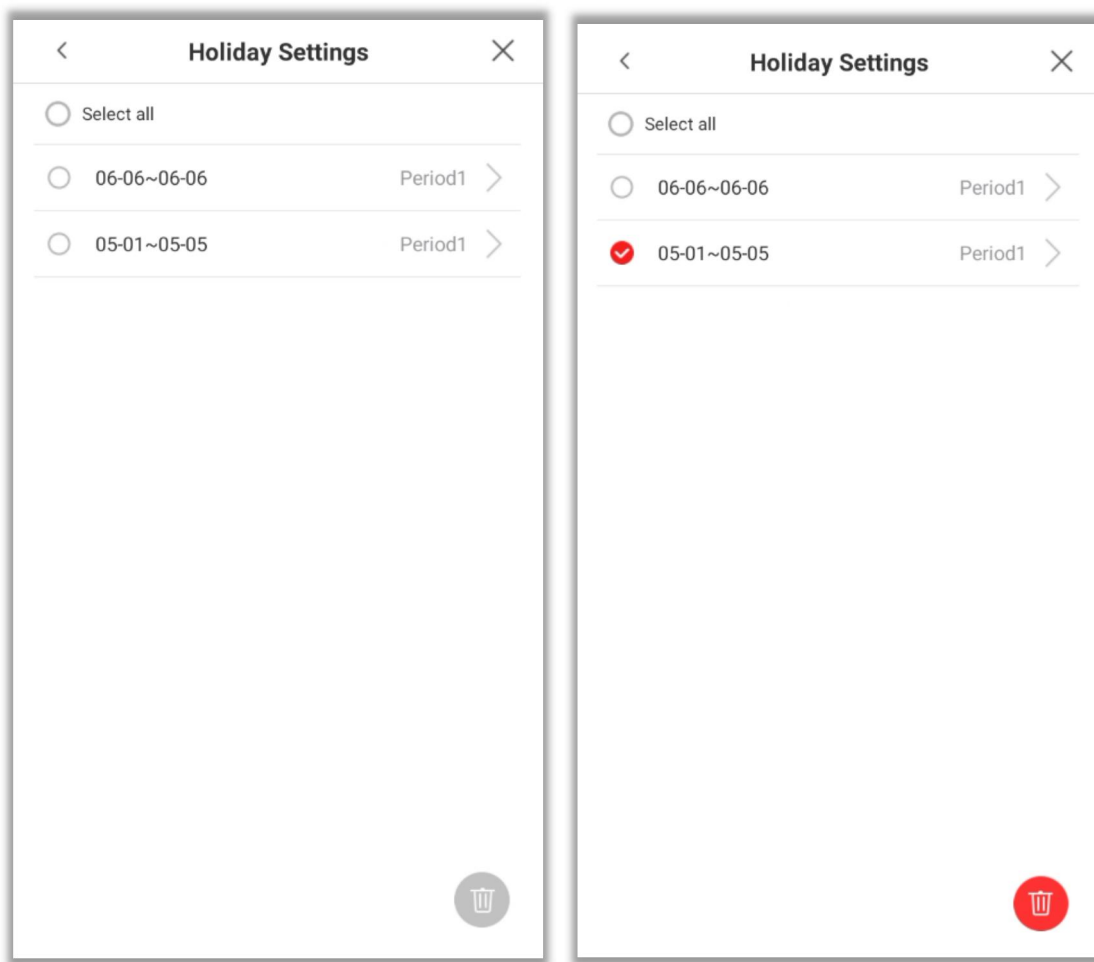
Finish

Page | 42

Copyright©2024 TECO CO., LTD. All rights reserved.



3. In the [Holiday Settings] interface, select the holiday you want to delete. Select the holiday you want to delete, and click the  button in the lower right corner. In the pop-up window, click "OK" to confirm the deletion.



5.4 Verification Combination Setting

You can define 10 unlocking combinations, each of which supports 5 access control groups. Users in the same unlocking combination need to be verified together when opening the door.

In the [Verification Combination] interface, tap one of the groups to set the required access control group.

<

Verification Combination

1	01 00 00 00 00	>
2	00 00 00 00 00	>
3	00 00 00 00 00	>
4	00 00 00 00 00	>
5	00 00 00 00 00	>
6	00 00 00 00 00	>
7	00 00 00 00 00	>
8	00 00 00 00 00	>
9	00 00 00 00 00	>
10	00 00 00 00 00	>


<

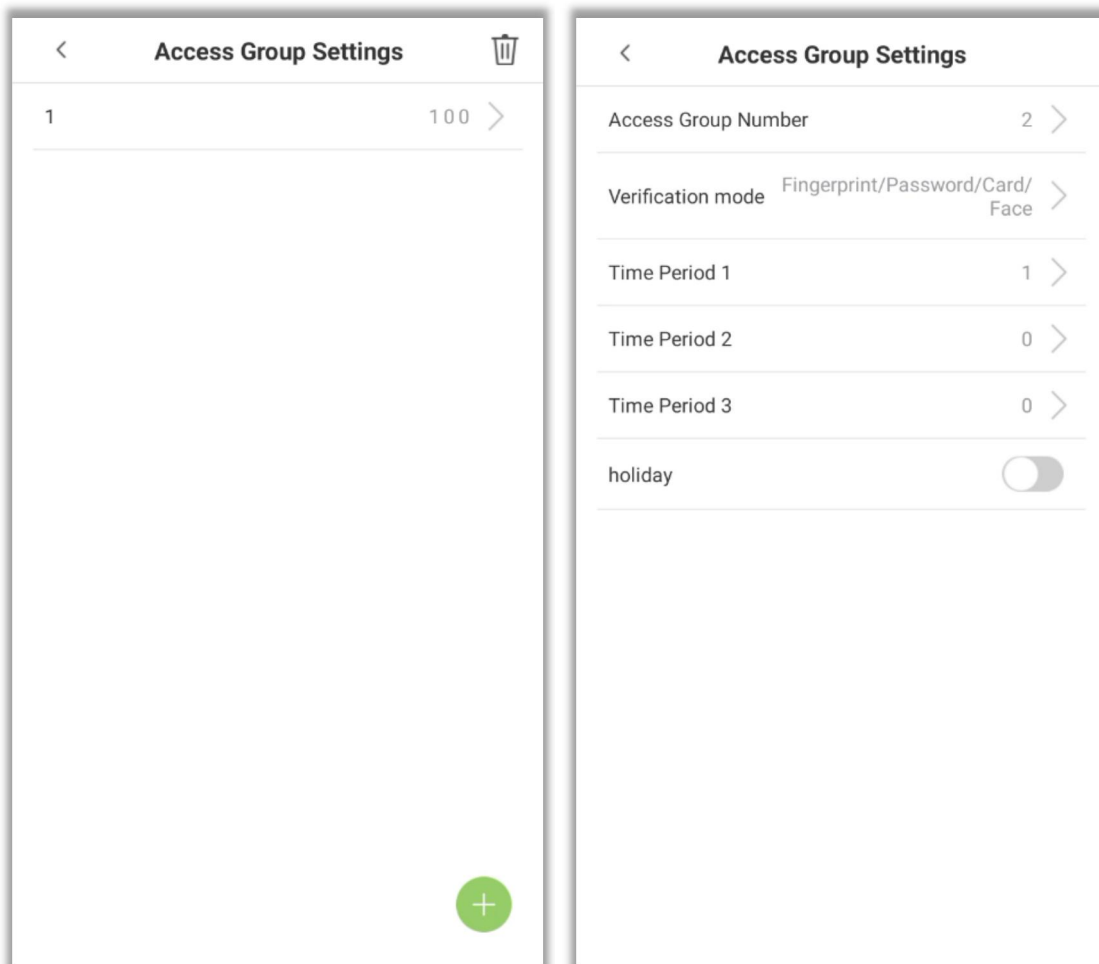
Verification Combination

Save

98	97	97	97	97
99	98	98	98	98
00	99	99	99	99
01	00	00	00	00
02	01	01	01	01
03	02	02	02	02
04	03	03	03	03
1	2	3	4	5

Access control group setting

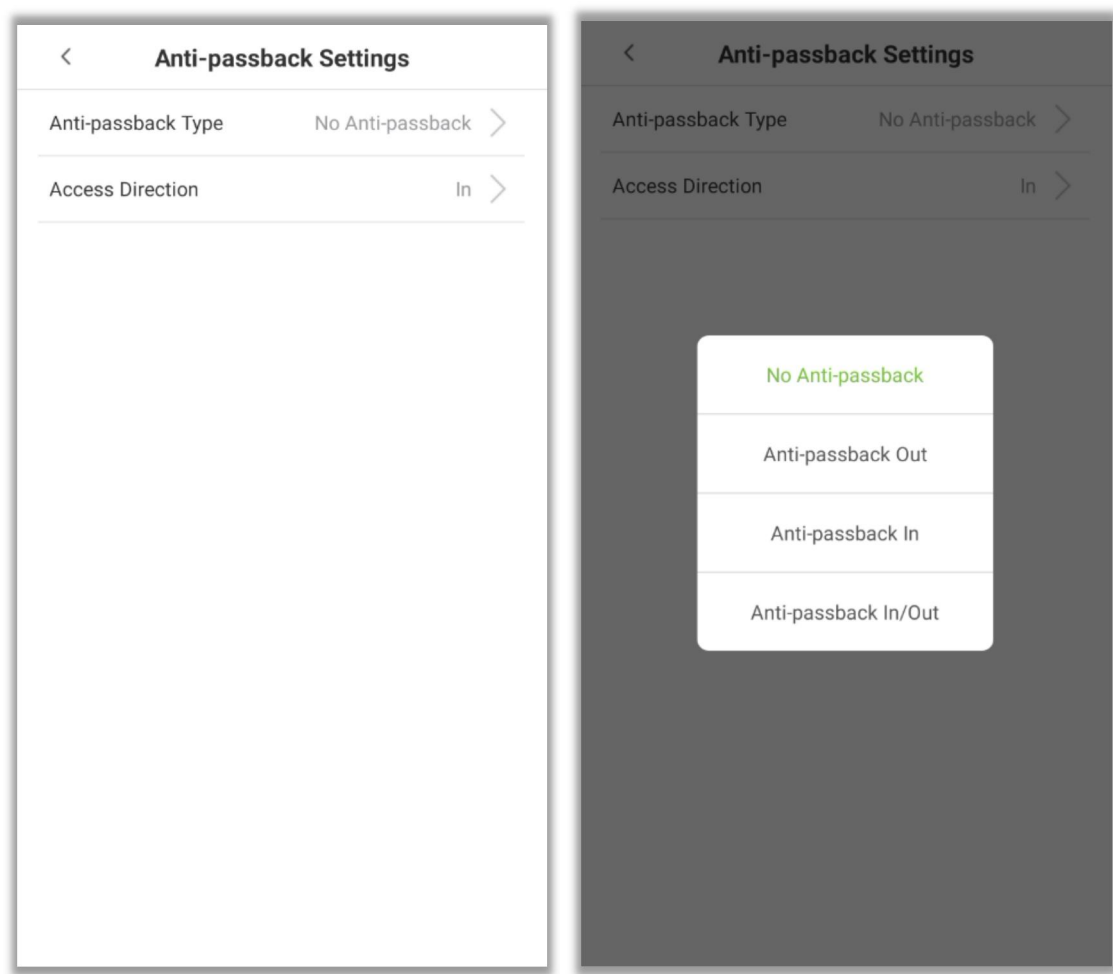
1. Tap  to enter the [Add Access Control Group] interface to make relevant settings for the new access control group.



Menu	Function Description
Access Group Number	The number of the access control group, supporting 1-99, default is 1.
Verification mode	Support 21 different authentication combinations (group authentication is not supported for the time being).
Time Period 1	Support 0-50 groups of time rules, default is 1, 0 is disabled.
Time Period 2	Support 0-50 sets of time rules, default to 0, 0 is disabled.
Time Period 3	Support 0-50 groups of time rules, default is 1, 0 is disabled.
holiday	After being activated, the holiday period will be effective for that access control group.

5.5 Anti-passback Settings

Anti-submarine is a direction control method used to control access to restricted areas. This function involves a specific sequence. If any person follows another person into the restricted area without authentication by a biometric device, the door will not open when that person attempts to leave the area. This function detects whether the user's access is legitimate by determining the user's last access record and local control direction, effectively preventing tailgating.



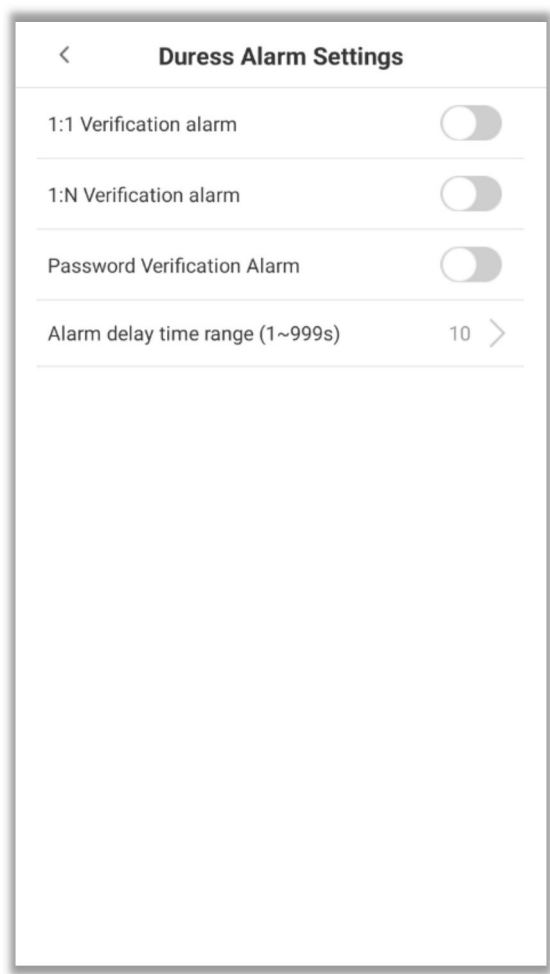
1. Anti submarine type

Menu	Function Description
No anti-passback	There are no anti-submarine settings.
Anti-passback Out	After the user signs out, only the last record is the sign-in record, and the user can sign out again; otherwise, an alarm will be triggered. However, the user can sign in freely.
Anti-passback In	After the user signs in, only the last record is the sign-out record, and the user can sign in again; otherwise, an alarm will be triggered. However, the user can freely sign out.
Anti-passback In/Out	After the user signs in/out, only the last record is the sign-out record, and the user can sign in again; or if it is a sign-in record, the user can sign out again; otherwise, an alarm will be triggered.

2. Direction of entry and exit

The direction of access depends on the selection of the control direction of the device, which corresponds to the state of the device.


5.6 Duress Alarm Setting

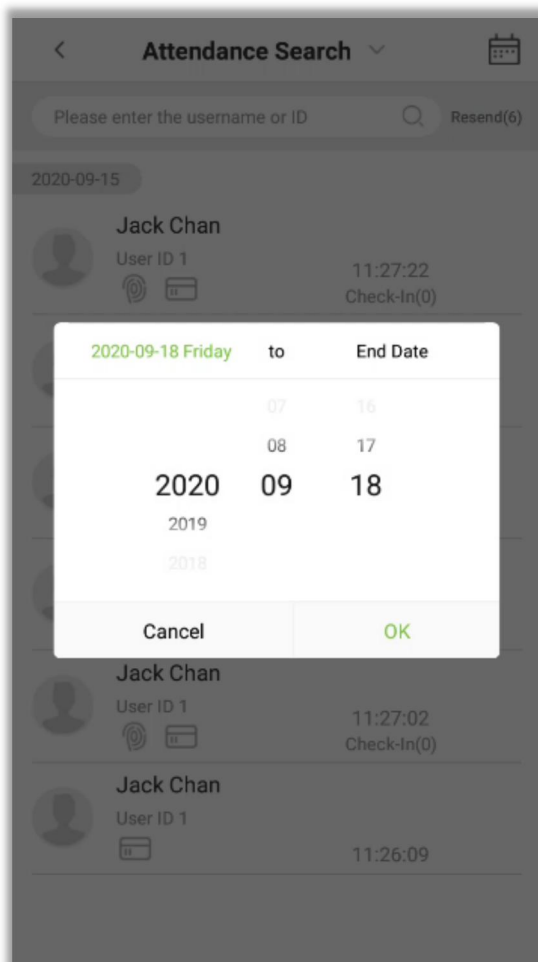


Menu	Function Description
1:1 Verification alarm	After the system is activated, when the user authenticates their fingerprint using their work ID, a coercive fingerprint alarm is triggered.
1: N Verification alarm	After the fingerprint lock is enabled, the user can directly verify the fingerprint and the coercive fingerprint alarm is enabled.
Password Verification Alarm	After opening, users who have set a password can use the password to trigger an alarm.
Alarm delay time range (1~999s)	Set the delay alarm time, default 10 seconds.

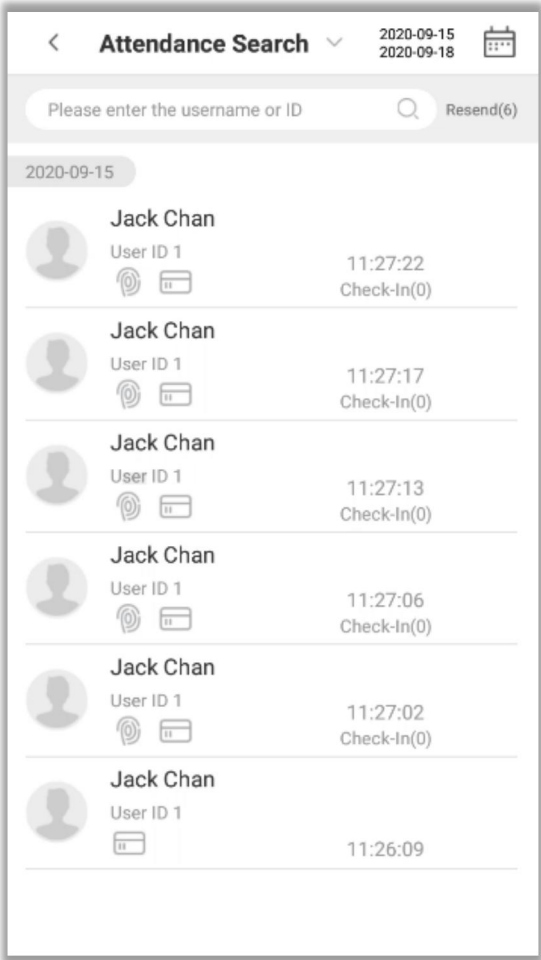
6 Attendance Record Query


The user's attendance records will be saved in the device, making it easy to find the user's attendance records. Users can search for attendance logs and visitor photos by time.

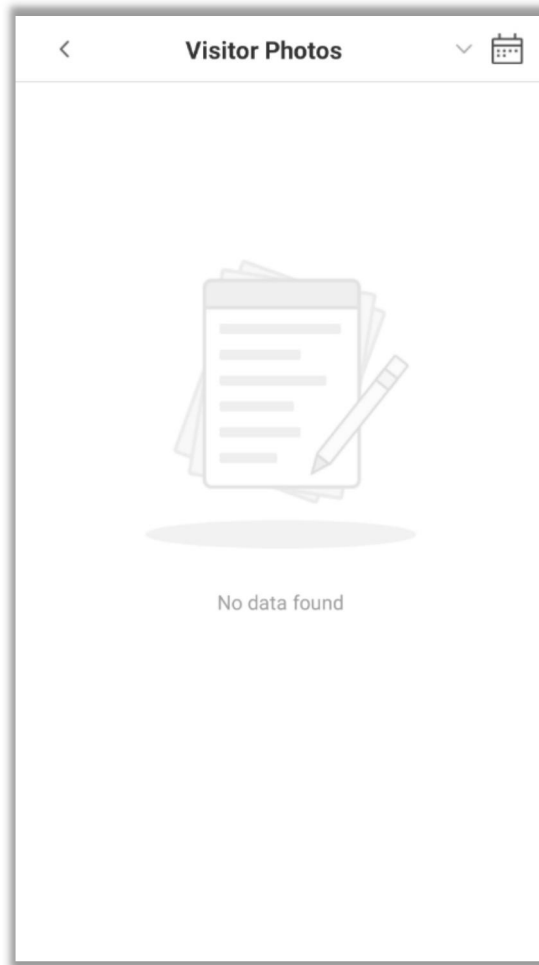
1. Tap the  icon to enter the following window, where you can select [Start Date] and [End Date] to search for records.
2. After setting the start and end dates, click [OK].



3. The search results are displayed as follows:



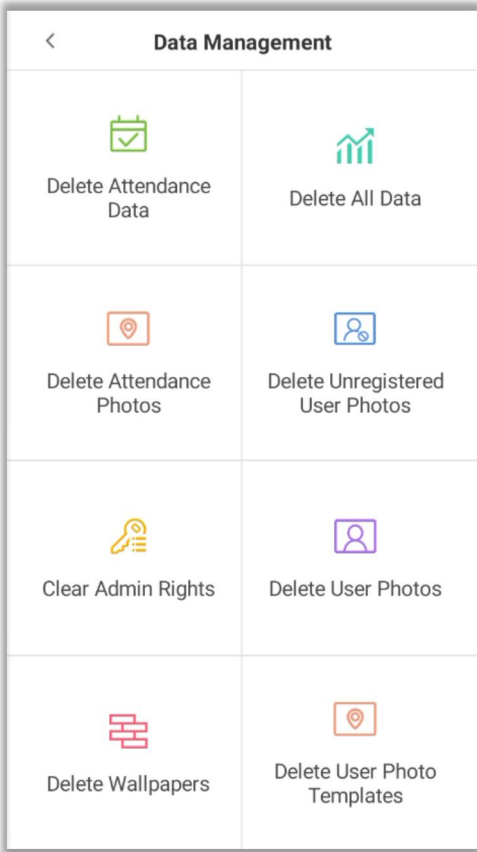
4. Tap the top **Attendance Search**  to switch between the attendance record query and the stranger photo interface.



7 Data Management

The "Data Management" menu is used to manage the data of the device, including: deleting attendance data, deleting all data, deleting attendance photos, deleting unregistered user photos, clearing Admin permissions, deleting user photos, deleting wallpaper, and deleting user template photos.

Click on [Data Management] in the main menu.



Menu	Function Description
Delete Attendance Data	<div><div>1.</div><div>2.</div><div>3.</div></div> <div>Delete all attendance data</div> <div>Delete invalid user attendance records</div> <div>Delete the attendance logs within the specified time period.</div>
Delete All Data	<div><div></div></div> <div>Delete all data on the device, including attendance logs, attendance pictures, blacklist pictures, fingerprint/facial biometric data, super administrator permissions, user photos, user data, access control data, etc.</div>
Delete Attendance Photos	<div><div>1.</div><div>2.</div><div>3.</div></div> <div>Delete all attendance photos</div> <div>Delete invalid user accounts</div> <div>Delete the attendance photos within the specified time period.</div>

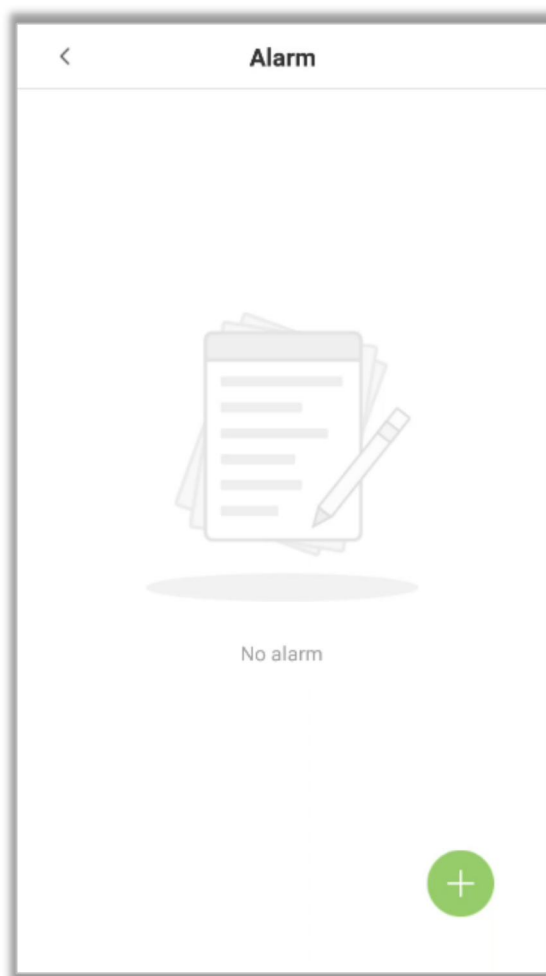
Delete Unregistered User Photos	<ol style="list-style-type: none"> 1. Delete all unregistered user photos 2. Delete unregistered user photos within the specified time range.
Clear Admin Rights	Remove all Admin permissions.
Delete User Photos	Delete all user photos.
Delete Wallpapers	Delete all wallpapers stored in the device.
Delete User Photo Templates	Delete all users' template photos.

8 Alarm Manager

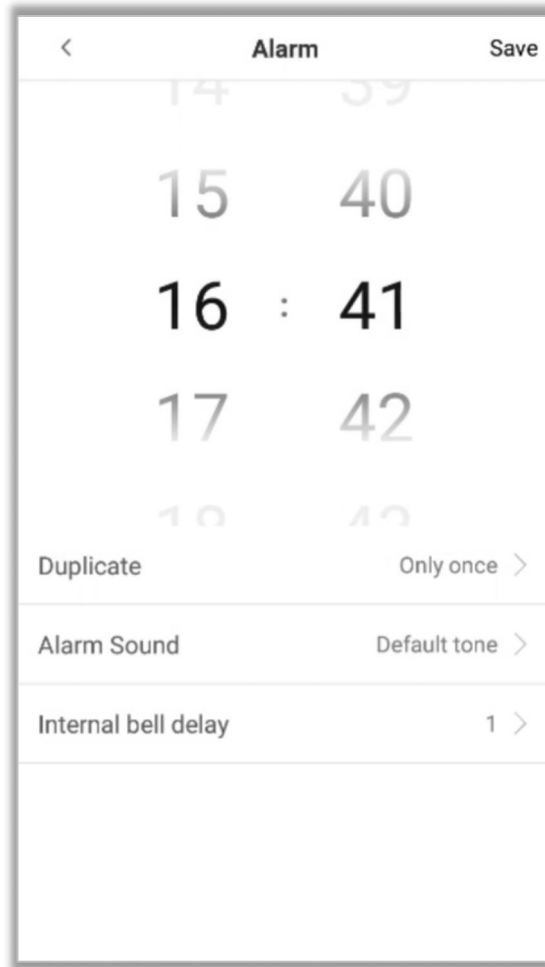
Set an alarm clock, and when the set time arrives, the device will automatically play a pre-selected ringtone. It will stop ringing after the alarm time has elapsed.

8.1 Add an Alarm Clock

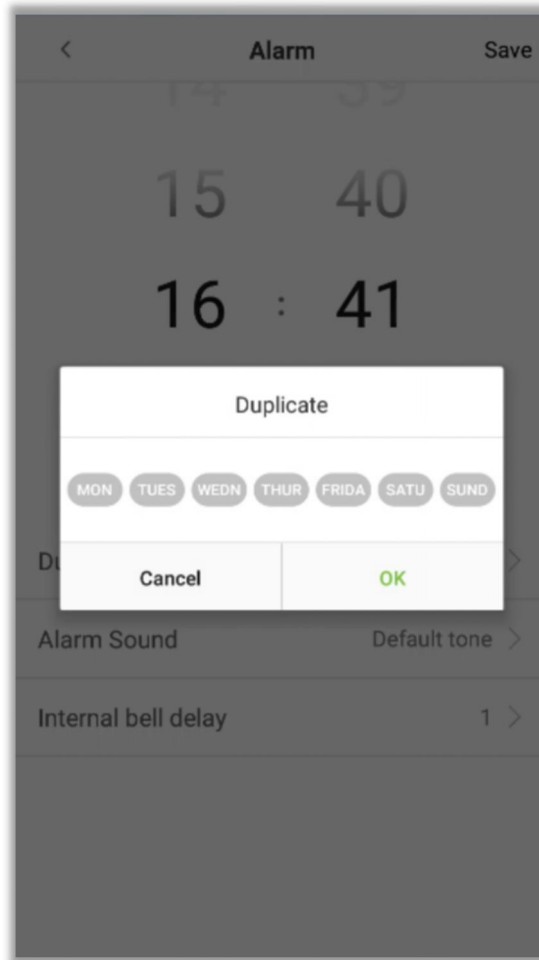
1. In the alarm clock management interface, click  to enter the "Add" page.



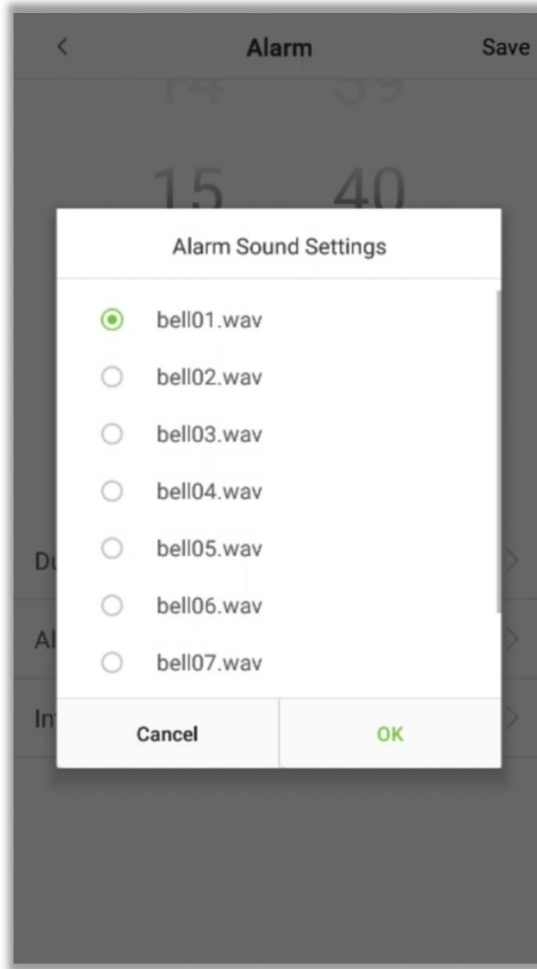
2. Set the time to trigger the alarm clock. Select [Hour] and [Minute].



3. Repeat - the default setting is "Only once". To copy the settings to other days, click the [Copy] button, and a window will pop up. Select the date and click [OK].



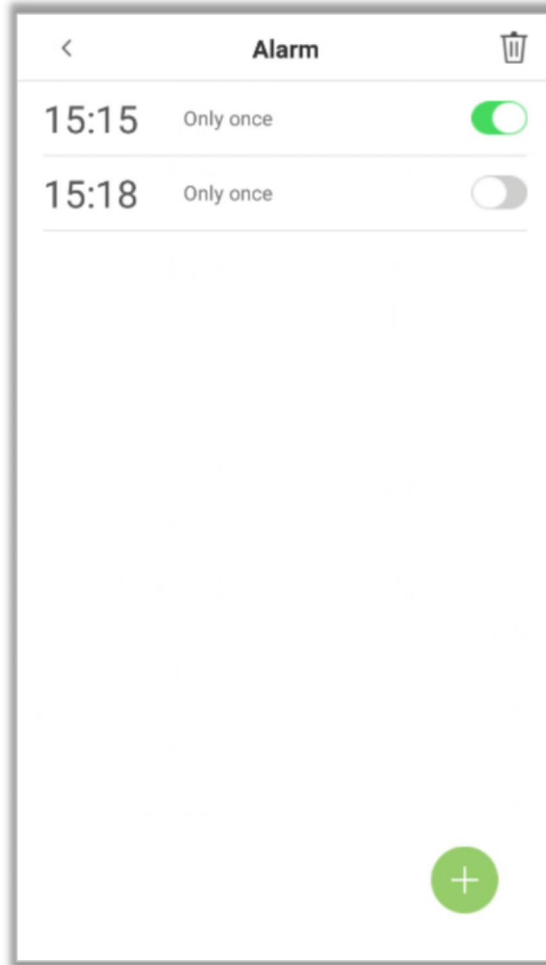
4. Click on [Alarm Sound] and a window will pop up. Select the ringtone and tap [OK].



5. Click [Save] to add the alarm clock successfully. By default, the alarm clock will be turned on at the specified time point.

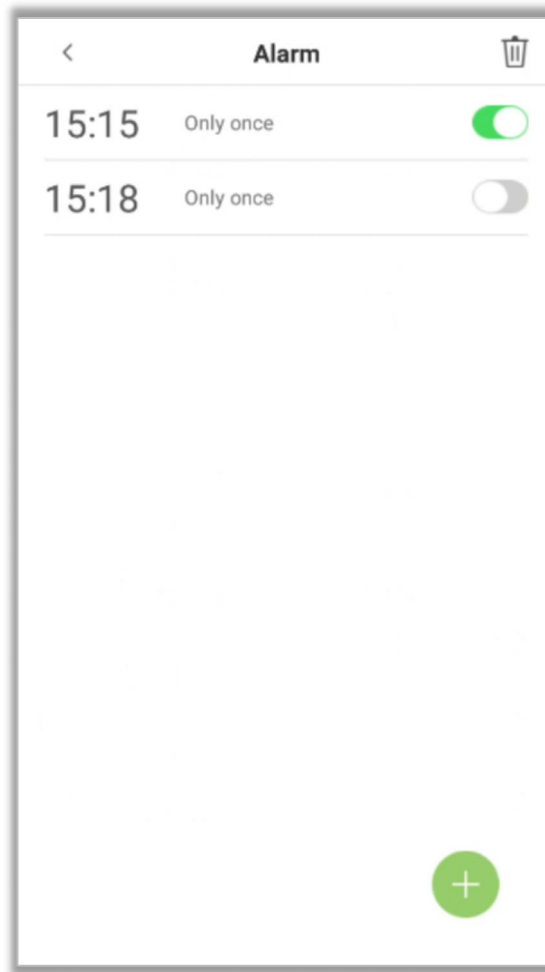


6. Toggle the "Alarm" button to change the alarm status.

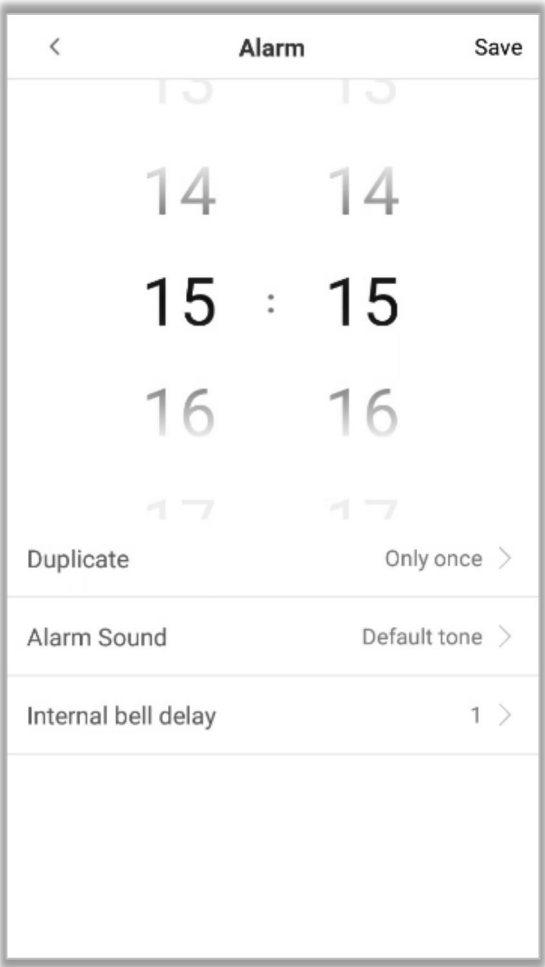


8.2 Edit Alarm Clock

1. Select an alarm from the alarm list.




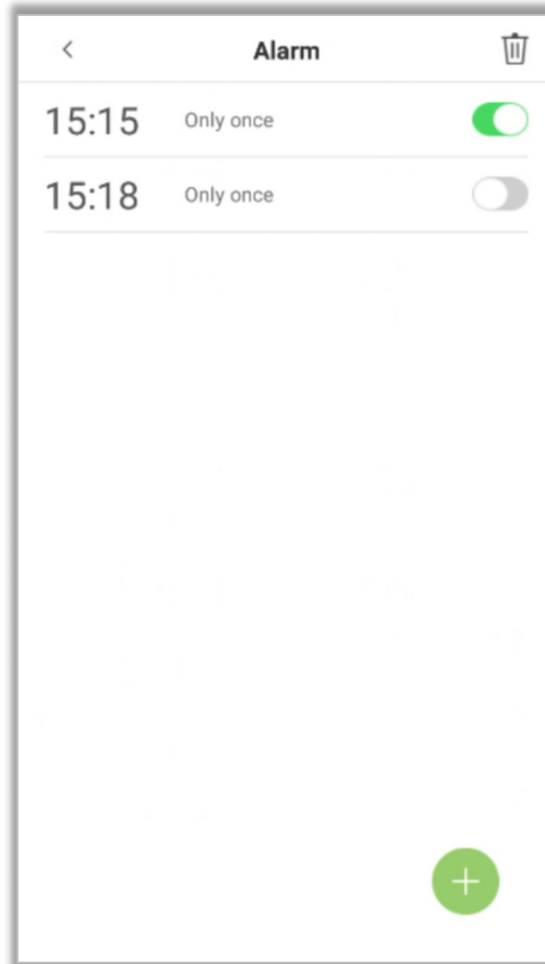
- 2. Edit the alarm time and other settings as needed.



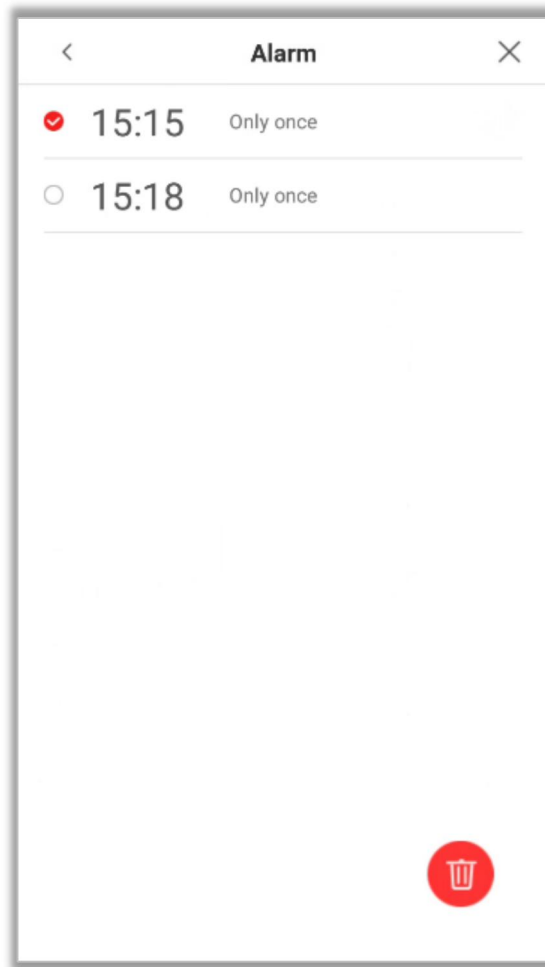
For more information, see Add an alarm.

8.3 Delete Alarm Clock

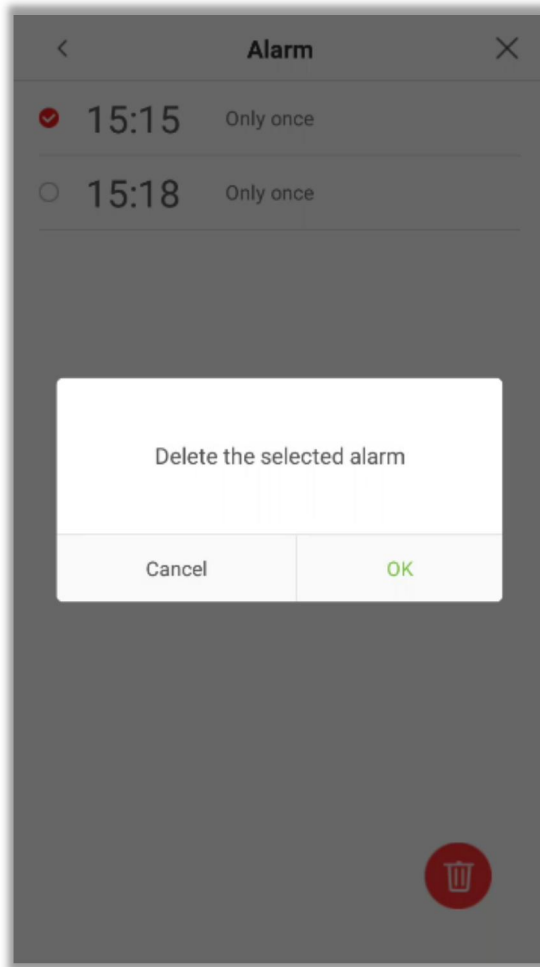
1. In the "Alarm Management" interface, tap the  button in the upper right corner of the interface.



2. Select the alarm to be deleted, and click the  button at the bottom right corner of the interface.



3. Click [OK] to delete the alarm clock.



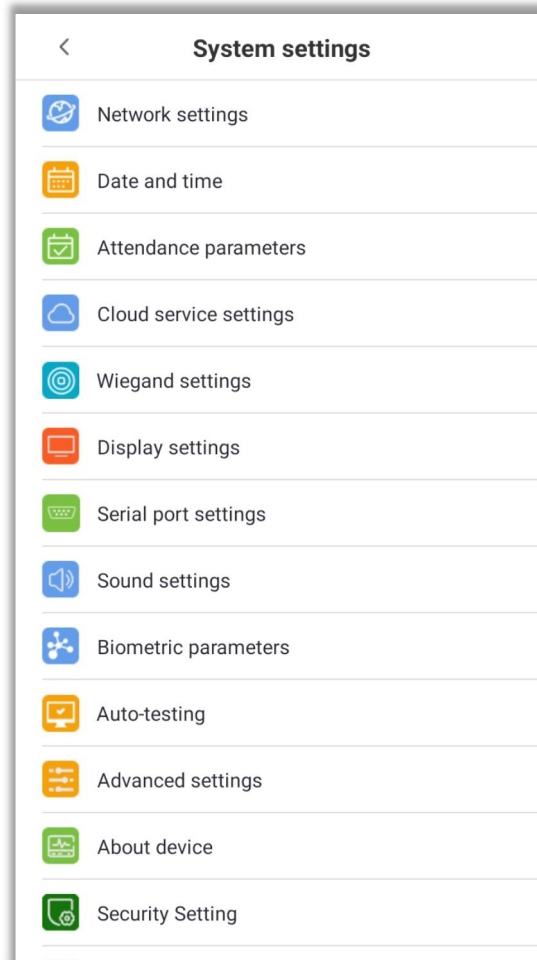
4. The alarm clock has now been deleted and will not appear in the list.



9 System Settings

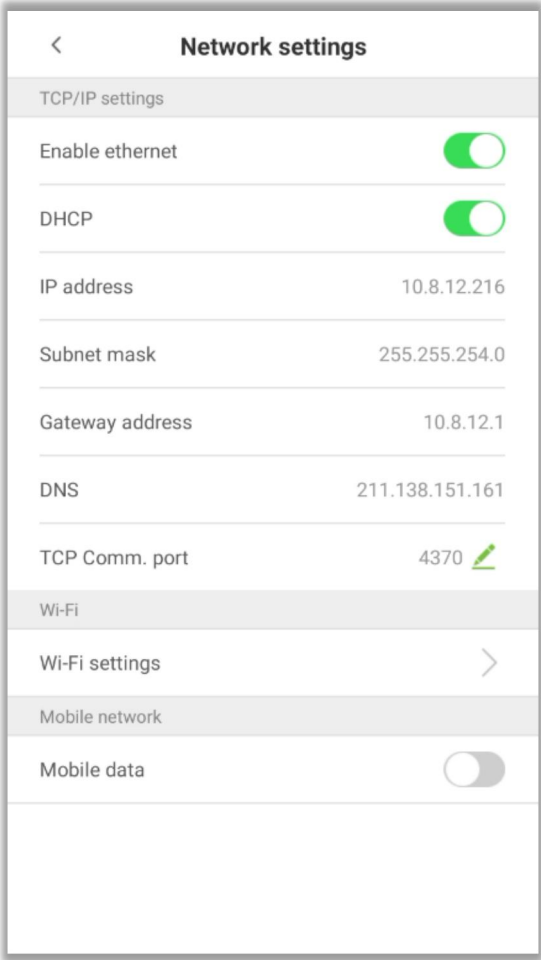
"System configuration" optimizes the performance of the device to maximize its ability to meet user needs.

In the main menu, click [System Settings].



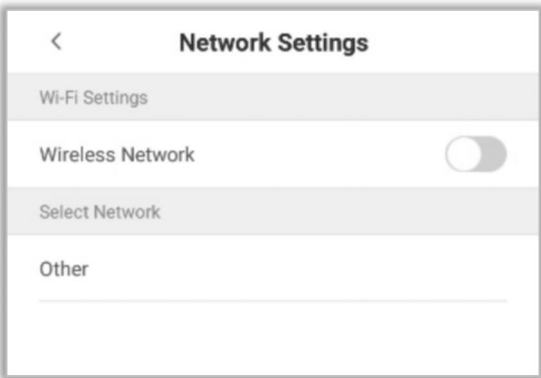
9.1 Network Settings

In the system settings list, click [Network Settings] to enter the network settings interface:



9.1.1 Wi-Fi Settings

Click on "Wi-Fi Settings" to open the network settings interface.



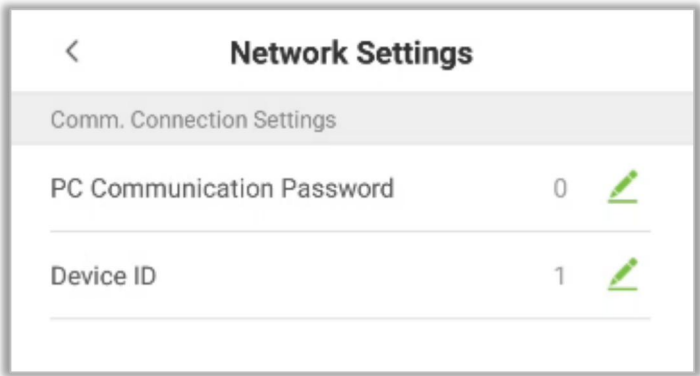
9.1.2 Mobile Data

Click the switch button to enable mobile data. To use mobile data, you need to turn off the Wi-Fi function.

9.1.3 Communication Connection Settings

To improve the security and confidentiality of accessing data, users need to set a connection password. Before successfully connecting the PC software and device, the correct connection password must be entered.

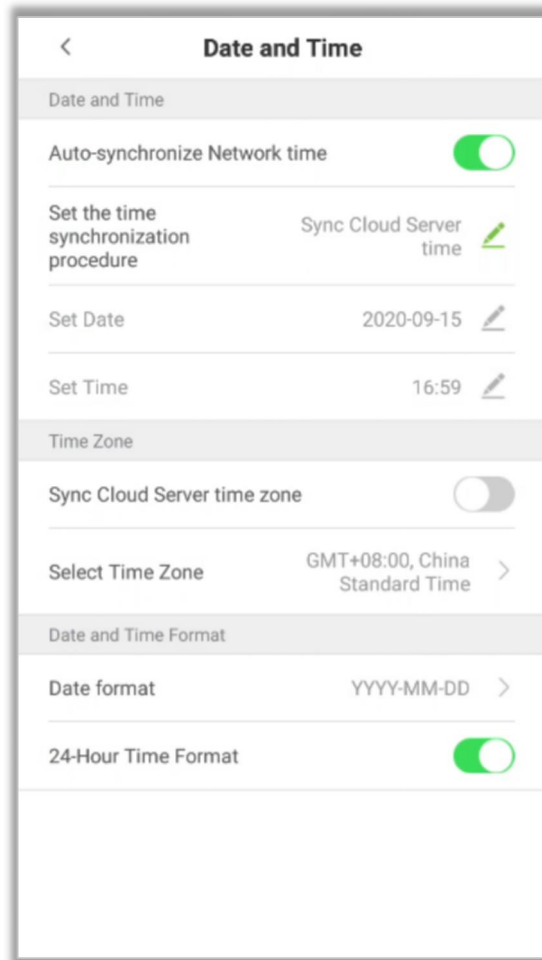
In the "Network Settings" interface, click "Communication Connection Settings".



Menu	Function Description
PC Communication Password	Used to obtain connection permissions when connecting using an offline SDK or PULL SDK. If the password is incorrect, communication cannot be established. The value range is 0 to 999999. When the value is 0, it indicates a no-code state
Device ID	The value range is 1 to 255. If the system uses RS232/RS485 communication, please enter the device ID during software communication.

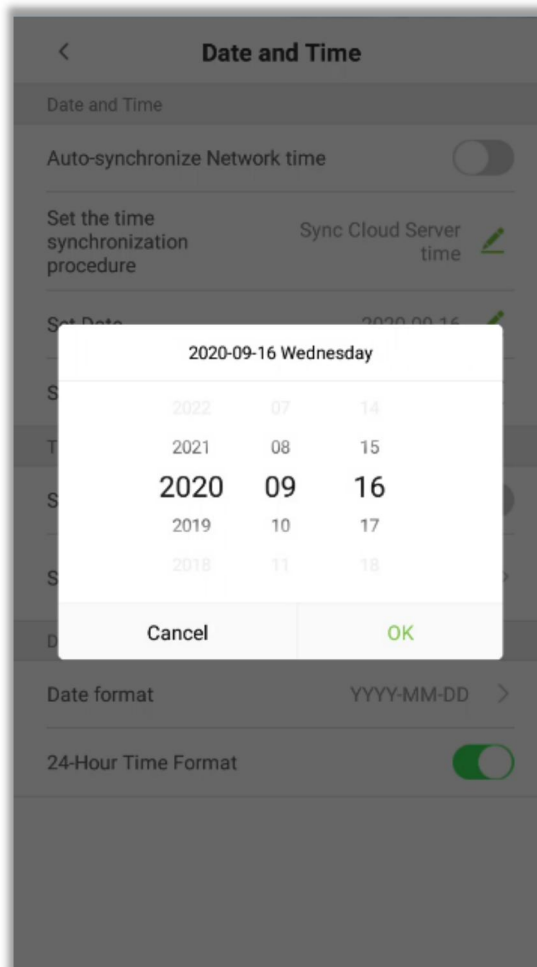
9.2 Date and Time

In the system settings, tap [Date and Time] to enter the date and time settings interface:

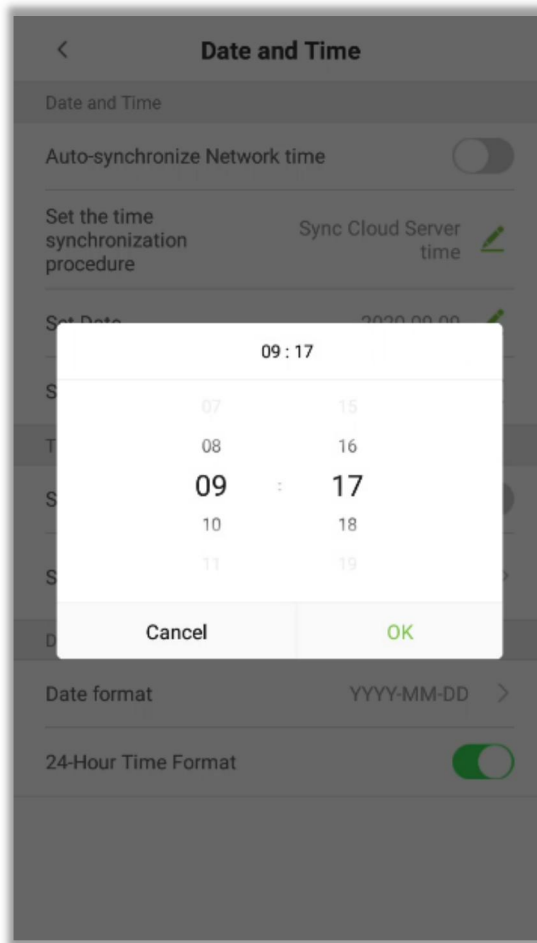


9.2.1 Date and Time Settings

1. Tap [Set Date], slide up and down to set the year, month, and day, and click [Confirm].

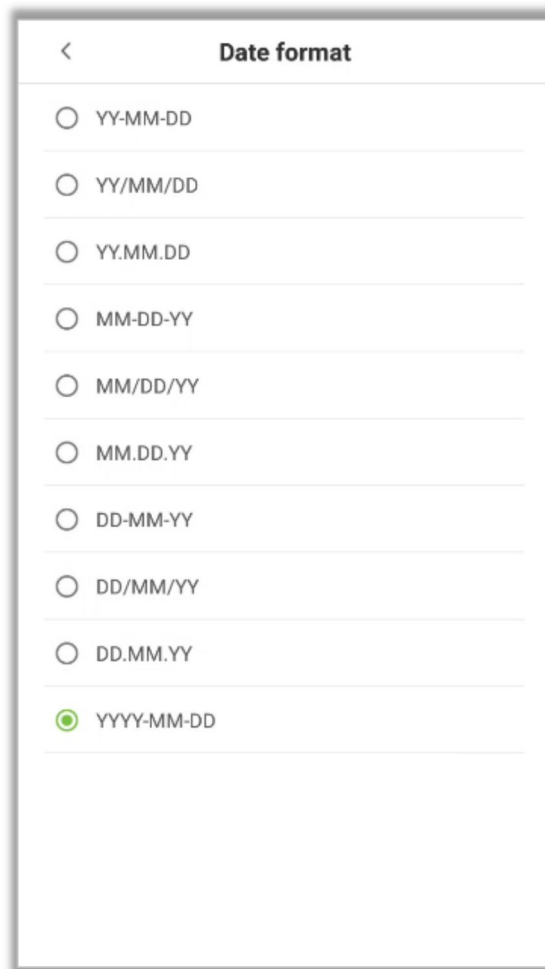


2. Click [Set Time], slide up and down to set the hour and minute, and click [Confirm].

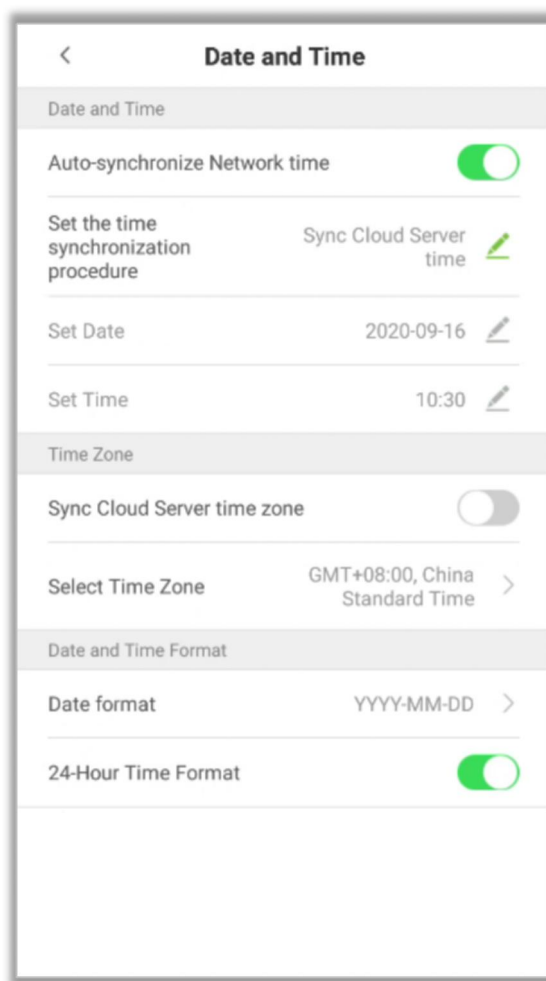


9.2.2 Date and Time Format Settings

1. Click on [Date Format] and select the desired date format.



2. Click [24-hour clock] to set the time format to 24-hour clock.



Auto-synchronize Network time: It is enabled by default, and the device automatically synchronizes the current network time. If disabled, users can set the date and time.

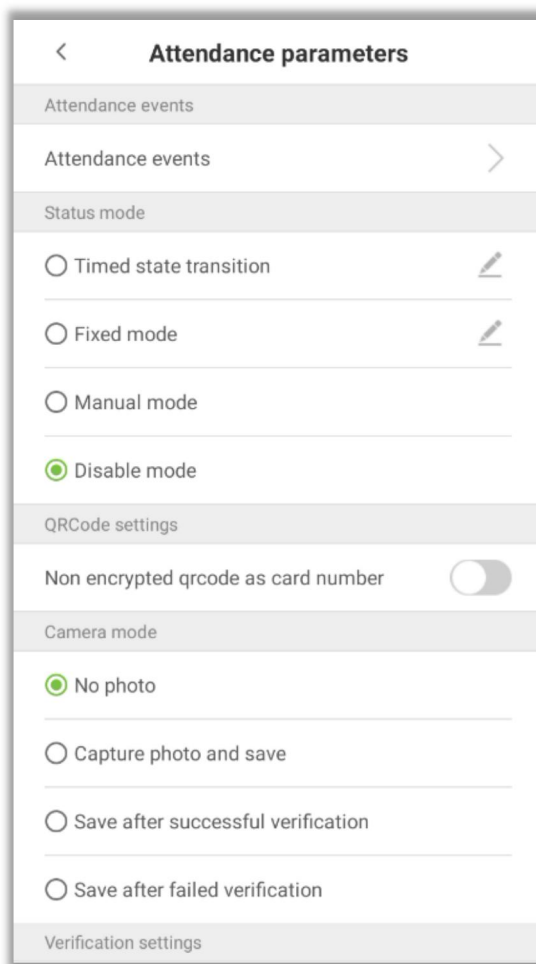
Sync Cloud Server time: Synchronize the time of the cloud server where the software connected to the device is located.

Synchronize network time: Synchronize the actual time of the Internet.

Select the time zone. The default time zone is GMT + 8:00. Users can modify it according to their actual situation.

9.3 Attendance Parameter Setting

In the "System Settings" section, click on "Attendance Parameters" to access the attendance parameter settings interface.



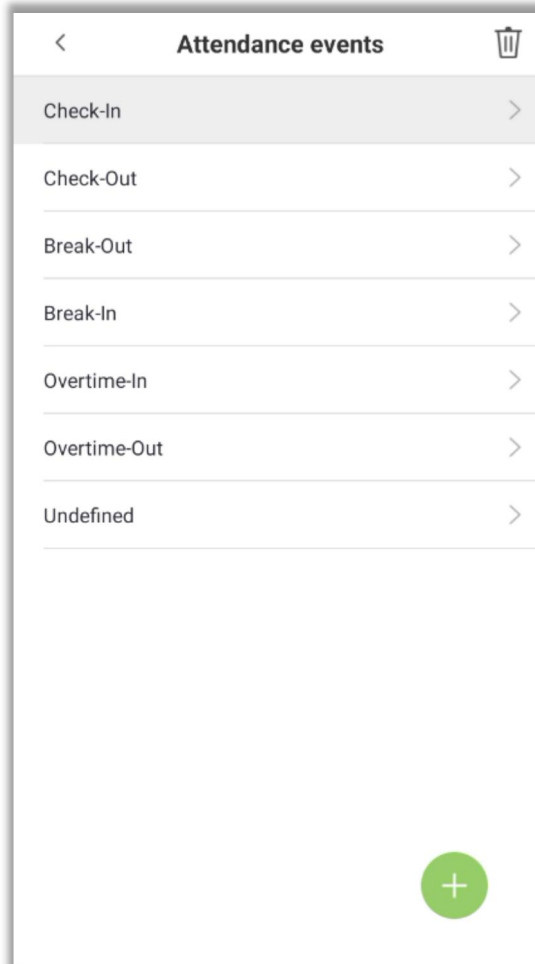
9.3.1 Attendance Events

Attendance events are used to record attendance status. There are 7 default attendance statuses, including check-in for work, check-out for work, out, return from out, overtime check-in, overtime check-out, and undefined. The 7 default statuses cannot be deleted or modified.

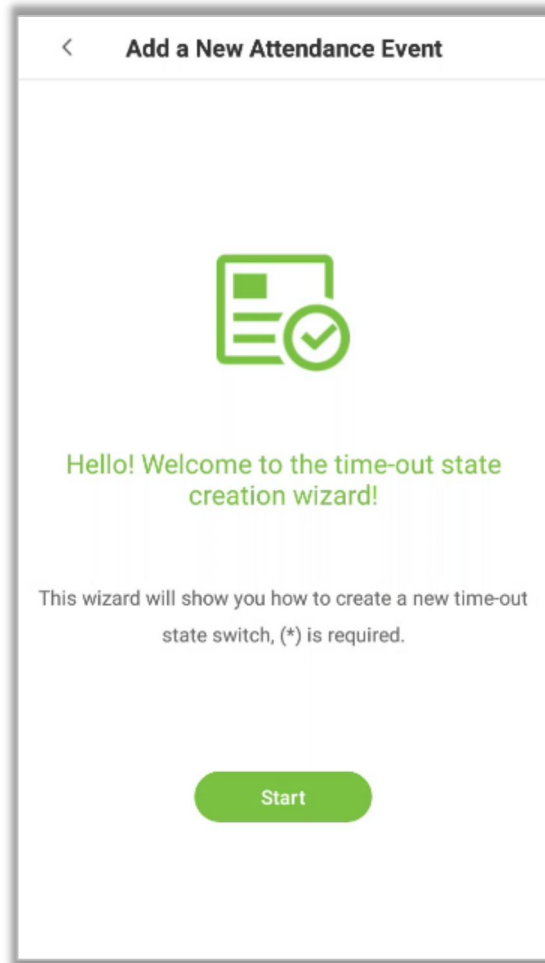
Add Attendance Event

Click on [Attendance Event].

1. In the "Attendance Event" interface, click  to open the "Attendance Event" interface.



2. In the attendance event creation wizard, click [Start].



3. Enter the Name and Status Value of the newly created attendance event.



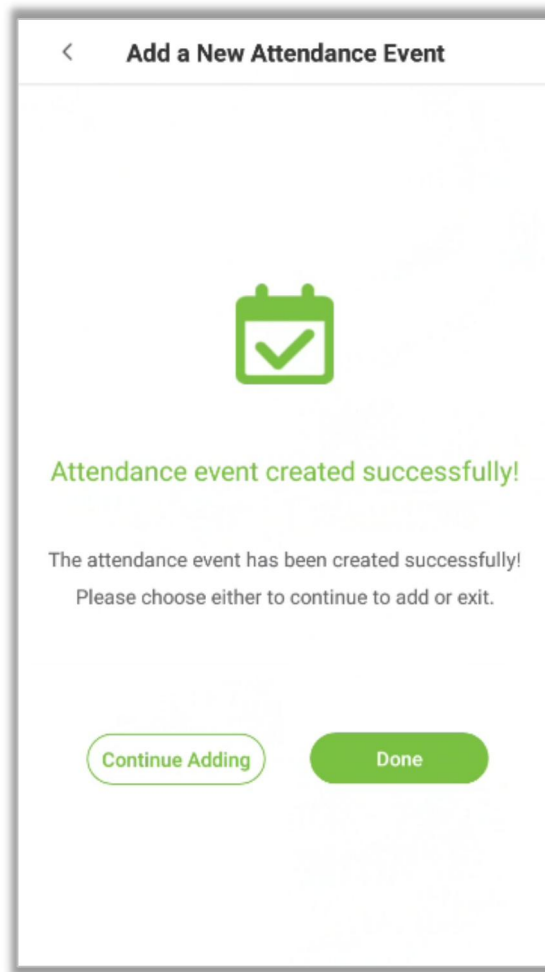
Note: The maximum length of the name is 24 characters. The status value must be unique and cannot be repeated. The value range is 6 to 250.

A screenshot of a mobile application screen titled "Add a New Attendance Event". The screen has a white background with a light gray border. At the top, there is a back arrow icon and the title "Add a New Attendance Event". Below the title, there are two input fields. The first field is labeled "Please enter the name" and has a red asterisk to its right. The second field is labeled "Please enter the status value (6-250)" and also has a red asterisk to its right. At the bottom of the screen, there are two green buttons: "Back" on the left and "Next" on the right. The "Back" button is outlined in green, while the "Next" button is solid green.

4. If the input status value is repeated or exceeds the limit, the following message will appear.

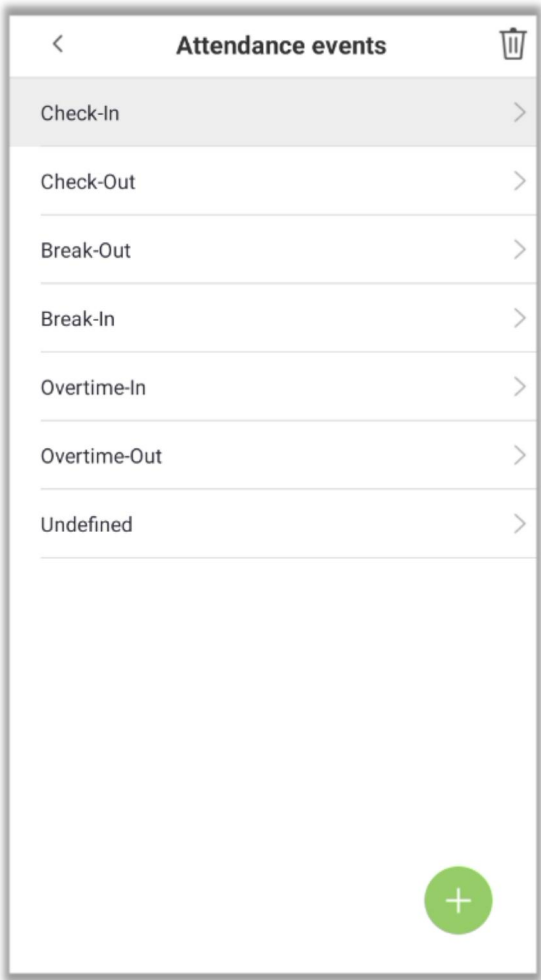
The screenshot shows a mobile application interface for adding a new attendance event. The title bar at the top is white with a back arrow and the text "Add a New Attendance Event". Below the title bar, there are two input fields. The first field is labeled "Checkvalue" and has a red asterisk to its right. The second field contains the number "3" and also has a red asterisk to its right. Below the second input field, a red error message reads: "(Incorrect status value range, please try again)". At the bottom of the form, there are two buttons: "Back" (outlined in green) and "Next" (solid green). Below the buttons is a standard QWERTY keyboard with a numeric keypad at the top.

5. If the attendance event is successfully created, a success message will be displayed as shown below:




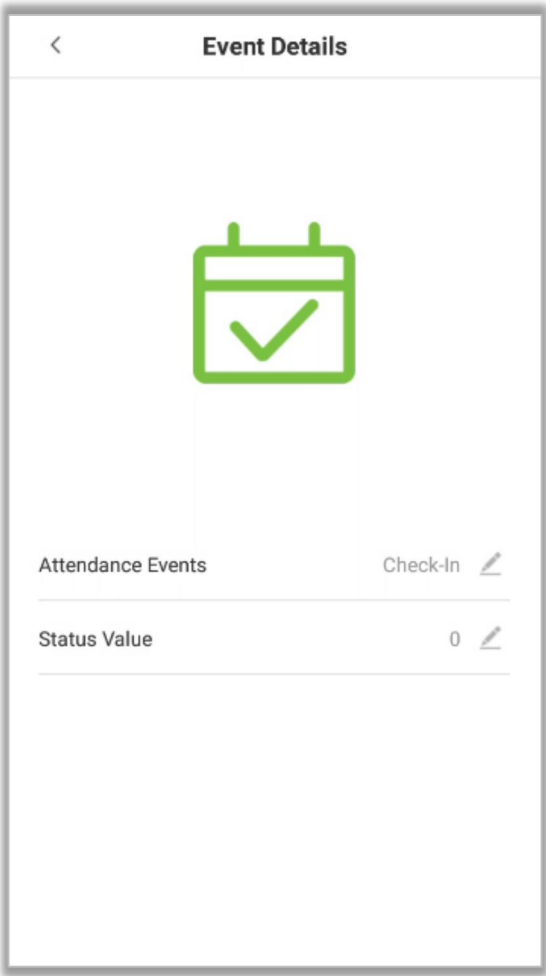
Edit attendance events

- 1. Select an attendance event.




2. Click on [Name] or [Status Value] to edit.

 **Note:** The first 7 attendance events cannot be edited. The status value must be unique and cannot be repeated.



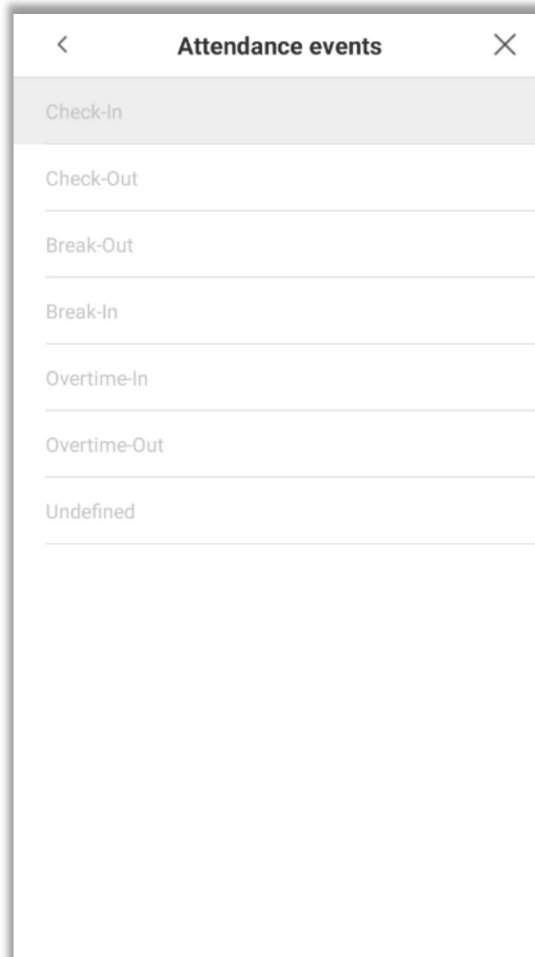
For more information, see Adding Attendance Events.

Delete attendance event

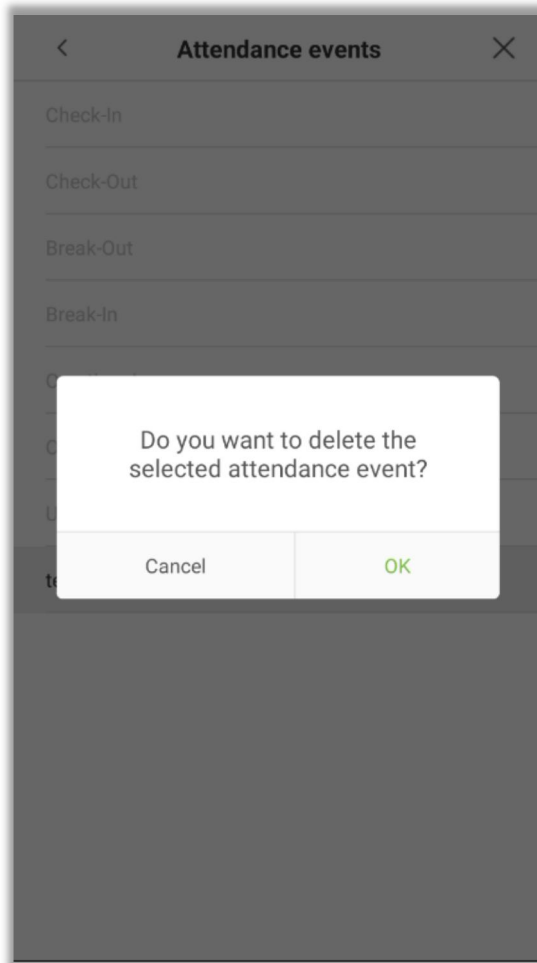
1. Tap the  icon in the upper right corner.



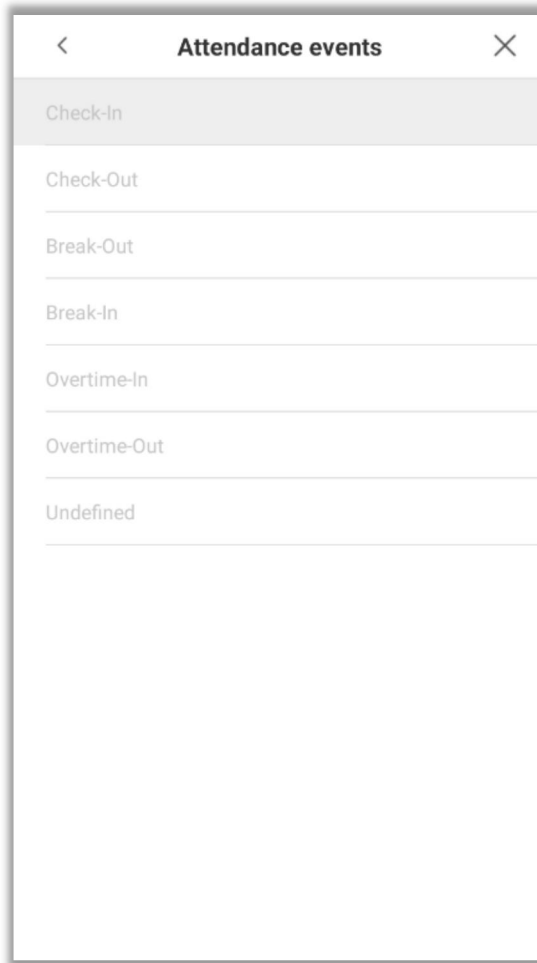
Note: The first 7 events cannot be deleted, so the options are grayed out.



2. Click [OK] in the window that appears to delete the attendance event.



3. The event is deleted and will not appear in the list.



9.3.2 State Mode

There are four modes of attendance status.


Timed status transition: Display different attendance statuses at different times.

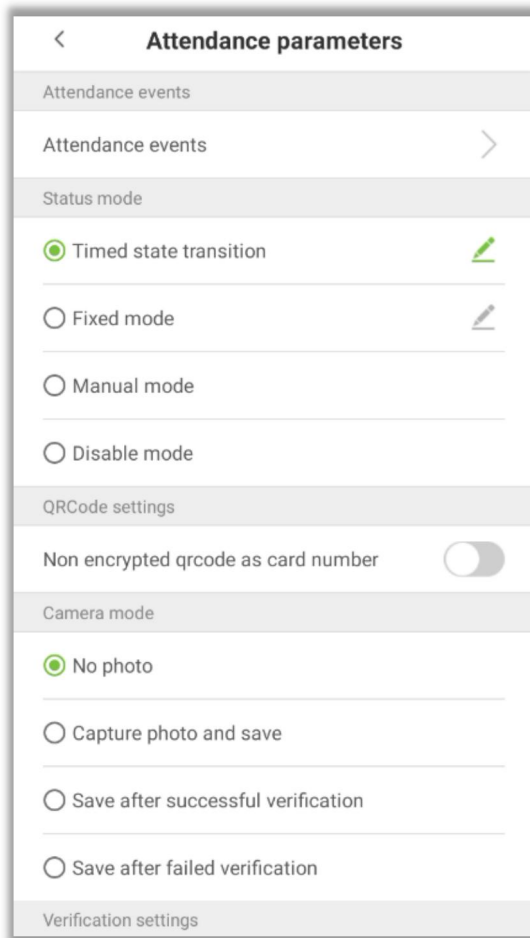
Fixed attendance mode: There is only one fixed attendance mode.

Manual mode: After successful verification, manually select the attendance status.

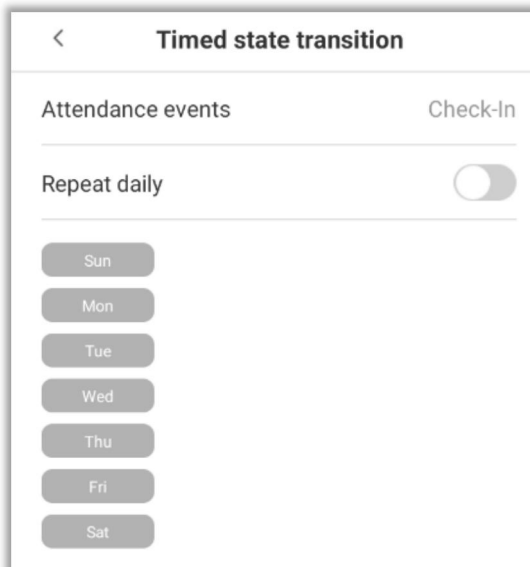
Disabled mode: Do not use the "status" mode.

Timed state transition

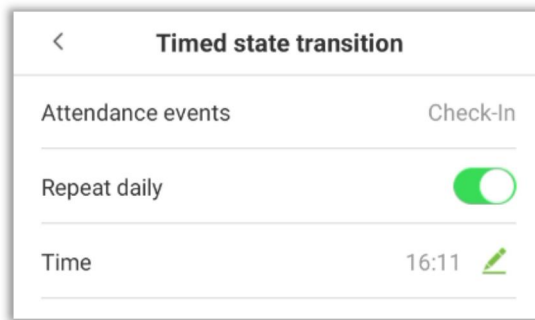
1. After selecting the "Timed State Transition" button, click the  button to set the relevant parameters.



2. In the timing status transition interface, click [Sign in for work] and then click [Repeat daily].

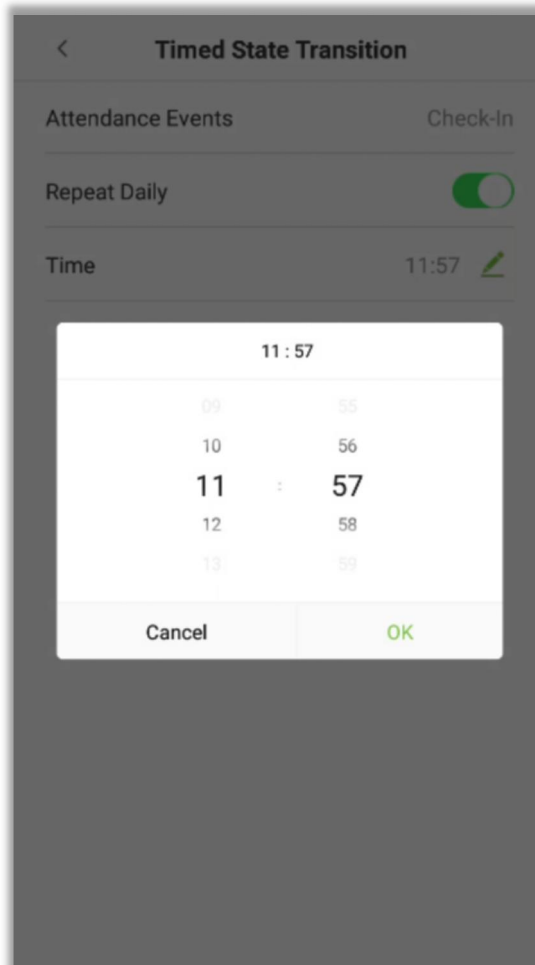


- When the [Repeat daily] option is enabled, the system displays the following interface.



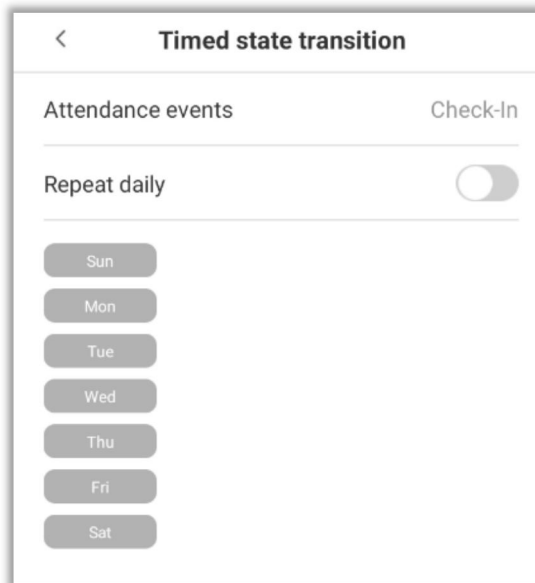
The screenshot shows a mobile application interface titled "Timed state transition". It has a back arrow on the top left. Below the title, there are three rows of settings: "Attendance events" with the value "Check-In", "Repeat daily" with a green toggle switch turned on, and "Time" with the value "16:11" and a green pencil icon for editing.

- Tap the [Time] button and slide up or down to set the time. Click [Finish].

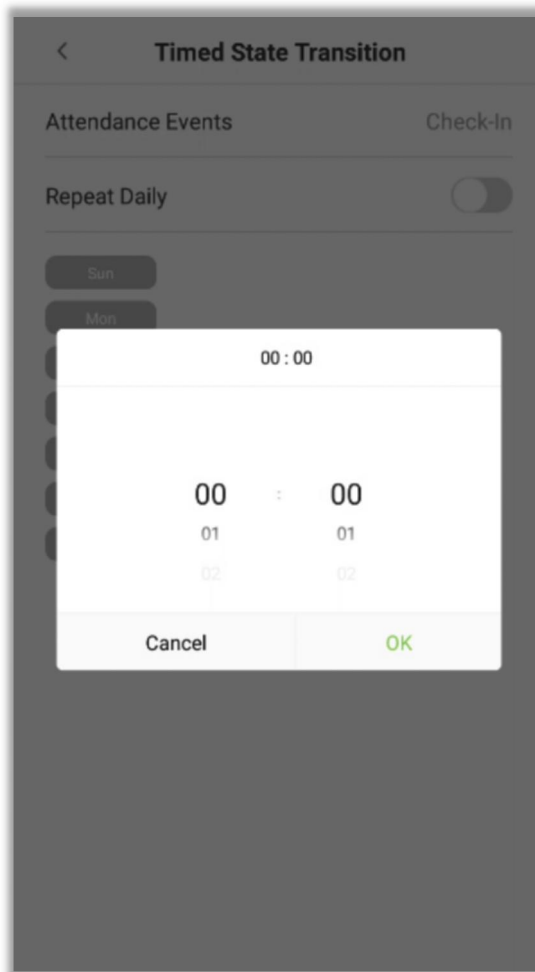


The screenshot shows the same "Timed State Transition" interface, but with a time picker overlay. The overlay is a white box with a dark border. At the top, it displays "11 : 57". Below this, there are two columns of numbers: the left column contains 09, 10, 11, 12, and 13; the right column contains 55, 56, 57, 58, and 59. The number 11 is selected in the left column and 57 is selected in the right column. At the bottom of the overlay, there are two buttons: "Cancel" and "OK".

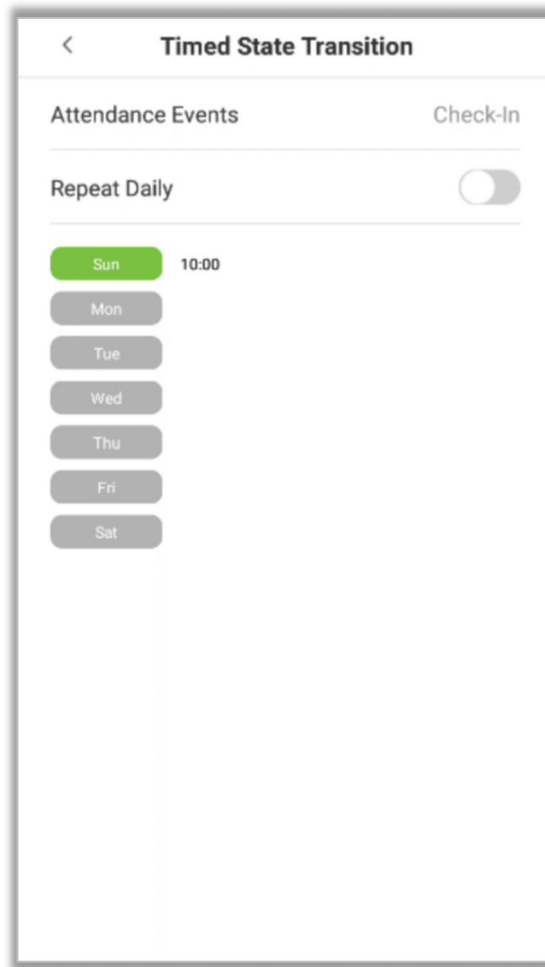
5. When the [Repeat daily] option is disabled, the system displays the following interface.



6. Click the date button you want to set, and then slide up and down to set the corresponding time. Click [OK].




7. After applying the settings, the interface is shown in the following figure.



Note: The setting process for "sign-out after work", "going out", "returning from going out", "signing in for overtime", "signing out for overtime", and "undefined" is the same as that for "signing in for work".

Fixed mode

1. Set the status mode to "Fixed Mode", and click the  button to open the Fixed Mode option menu.

< **Attendance parameters**

Attendance events

Attendance events >

Status mode

☐ Timed state transition

☒ Fixed mode

☐ Manual mode

☐ Disable mode

QRCode settings

Non encrypted qrcode as card number ☐

Camera mode

☒ No photo

☐ Capture photo and save

☐ Save after successful verification

☐ Save after failed verification

Verification settings

2. In the "Fixed Mode" selection menu, select the attendance status that the user wants to set.

< **Attendance parameters**

Fixed mode selection

☒ Check-In

☐ Check-Out

☐ Break-Out

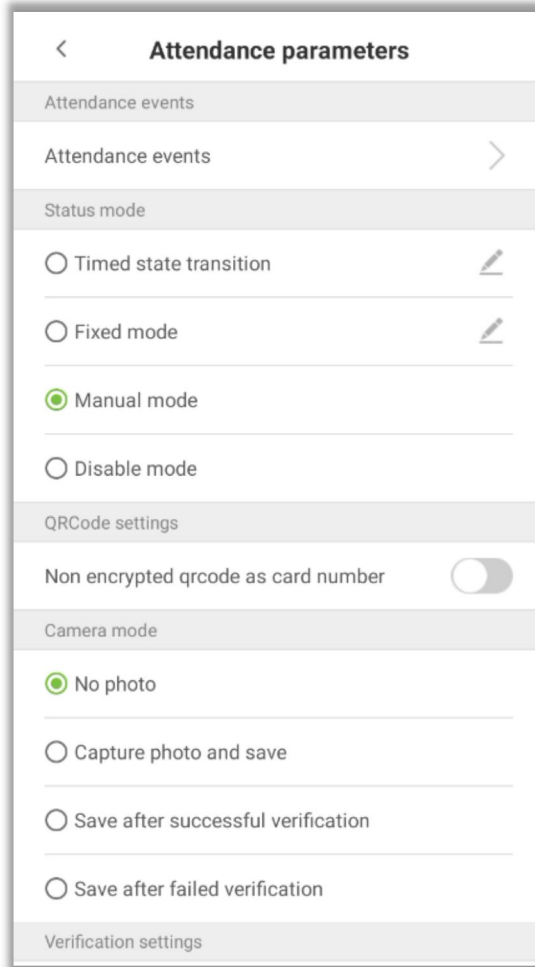
☐ Break-In

☐ Overtime-In

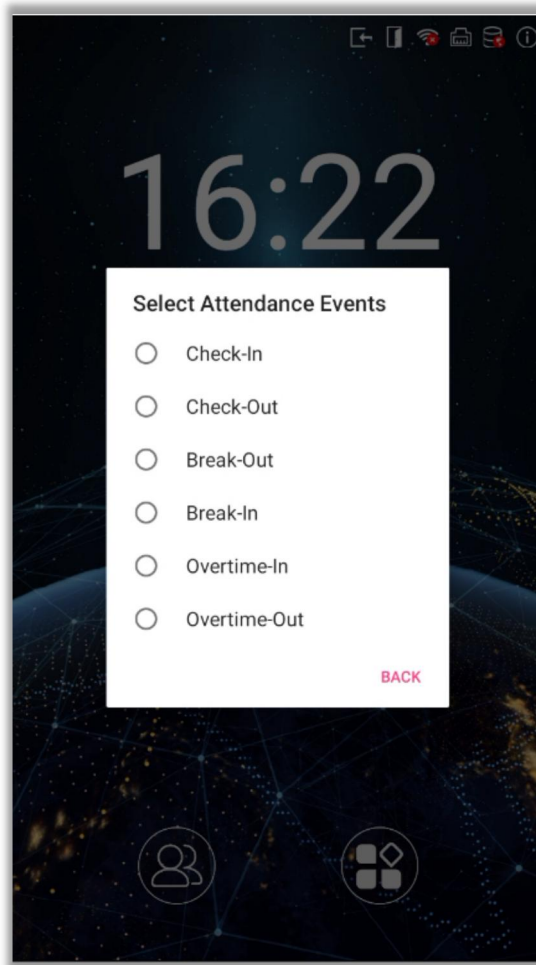
☐ Overtime-Out

Manual mode

1. The status mode is set to "Manual Mode".

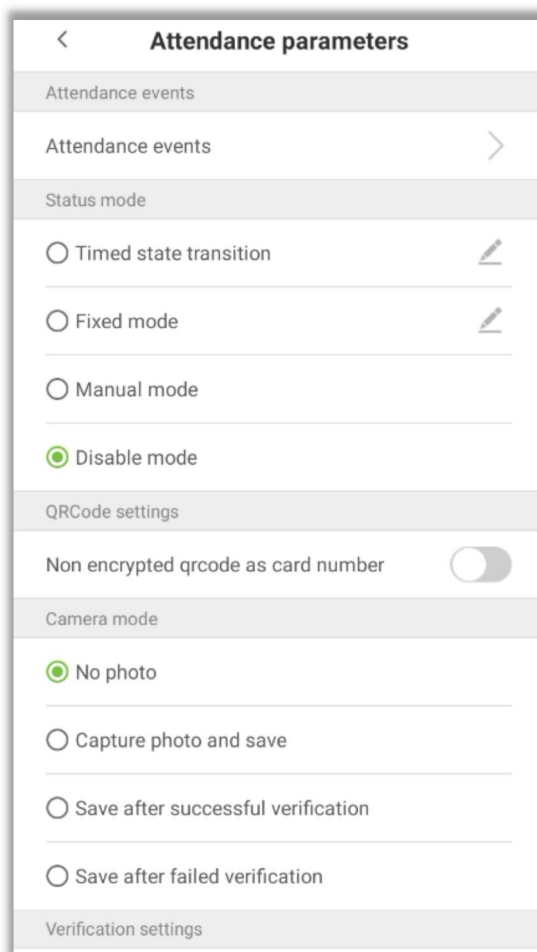


2. When the verification is successful, a pop-up window for selecting attendance events will be displayed.



Disabled mode

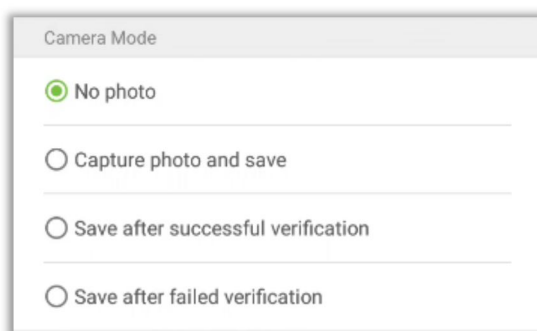
1. Select "Status Mode" as "Disabled Mode".



9.3.3 Photography Mode

Here, users can set the capture and save process of the verified user photo according to their requirements.

Tap on [Shooting Mode] to set the desired parameters.



No photo: No user photo will be saved during verification.

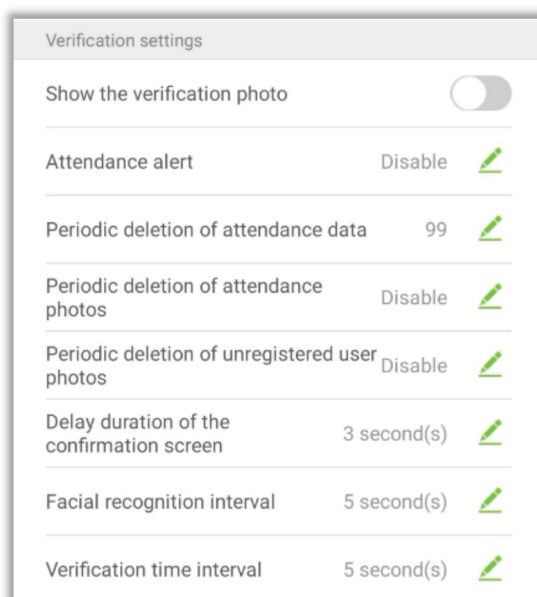
Verify and save photos: photos will be taken and saved for both successful and failed verification.

Successful verification and saving: After the user is successfully verified, take a picture and save it.

Save failed verification: When the user fails to verify, take a picture and save it.

9.3.4 Verification Settings

Here, users can configure parameters for user authentication.



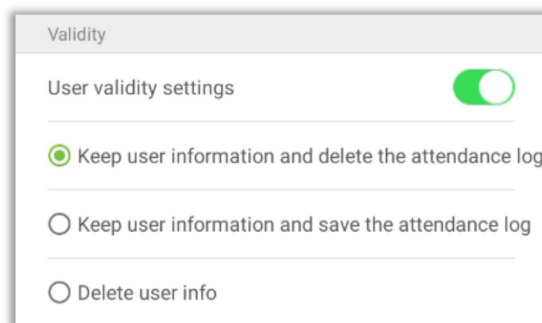
Menu	Function Description
Show the verification photo	If it is enabled, the user's photo will be displayed after verification. Otherwise, the user's photo will not be displayed.
Attendance alert	When the remaining recording memory space reaches the set value, the device will automatically display a warning. When set to 0, this function will be disabled.
Periodic deletion of attendance data	When the attendance record memory reaches its full capacity, the device will automatically delete old attendance records with the set value. When set to 0, this function will be disabled.
Periodic deletion of attendance photos	When the capacity of the attendance photos reaches its maximum, the device will automatically delete the old attendance photos of the set value. When set to 0, this function will be disabled.
Periodic deletion of unregistered user photos	When the blacklist photo capacity reaches full capacity, the device will automatically delete old stranger photos with a set value. When set to 0, this function will be disabled.
Delay duration of the confirmation screen	The duration of the verification information displayed on the system screen after verification. Unit: seconds.

Facial recognition interval	Set the face template matching time interval as needed. The value range is 0 to 9 seconds.
Verification time interval	Set the verification interval as needed. The value range is 0 ~ 999999 seconds.

9.3.5 Validity Period of User Information

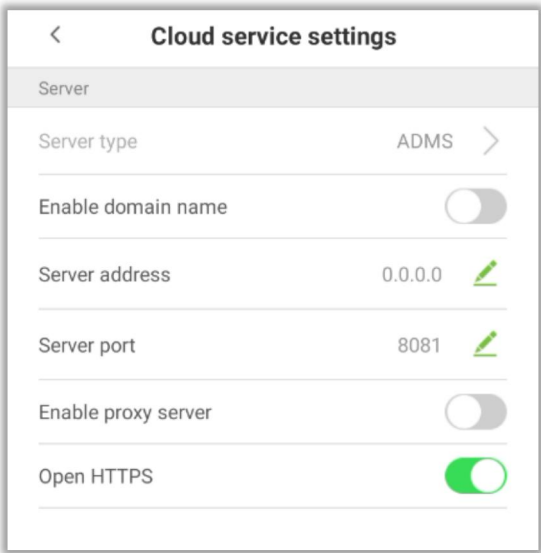
This is used to determine whether to enable or disable user validity period when registering users.

1. Click the [User Validity Period Settings] button.
2. After enabling this feature, the following screen will be displayed. Configure the required parameters.



9.4 Cloud Service Settings

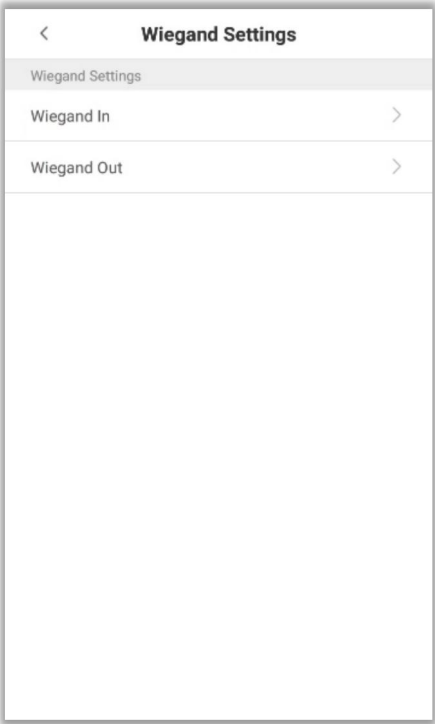
In the system settings list, click [Cloud Service Settings] to open the cloud service settings interface.



Menu		Function Description
Enable domain name	Server Address	After enabling this function, the domain name pattern is "http://... net". For example, http://www.XYZ.com, where "XYZ" represents the domain name when this mode is enabled.
Disable domain name	Server Address	IP address of the ADMS server.
	Server port	Port used by ADMS server.
Enable proxy		When selecting to enable the proxy, you need to set the IP address and port number of the proxy server.
Enable HTTPS		After enabling, you need to restart the device for it to take effect and upload the data to the push device. Change the HTTP address to HTTPS address.

9.5 Wiegand Settings

On **System Settings** interface, tap [**Wiegand Settings**] to access the interface as shown below.



9.5.1 Wiegand In

On **Wiegand Settings** interface, tap [**Wiegand In**] to open the settings.



Function Descriptions

Menu	Function Description
Wiegand Format	The Wiegand value could be 26bits, 34bits, 36bits, 37bits, or 50bits.
Wiegand in bits	It displays the number of bits of Wiegand data. After choosing Wiegand input bits , the device will use the set number of bits to find the suitable Wiegand format in Wiegand Format .
ID Type	The user can input User ID or Card number .

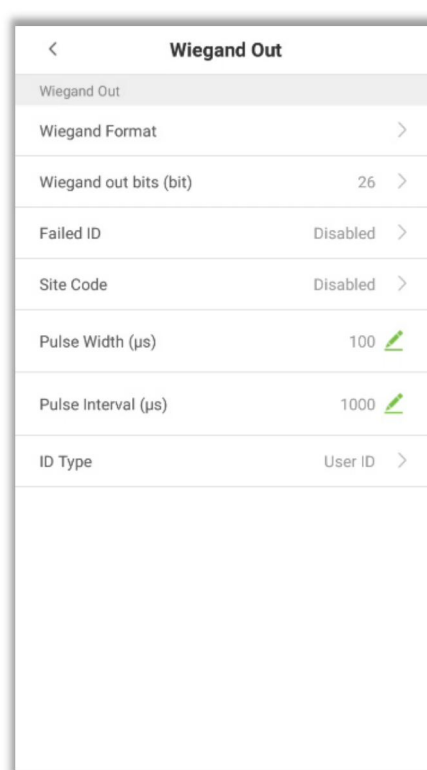
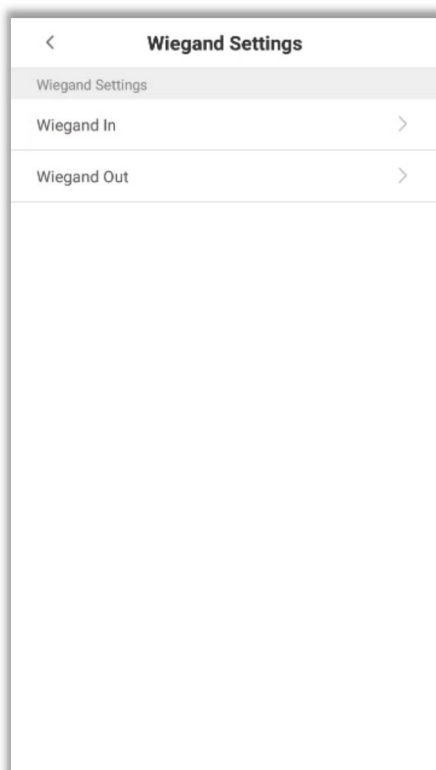
Various common Wiegand format definitions:

Wiegand Format	Description
Wiegand26	<p>EEEEEEEEEEEEEEEEEEEEEEEEEEEEEE</p> <p>Consists of 26 bits binary code. The 1st bit is the even parity bit of the 2nd to 13th bits, while the 26th bit is the odd parity bit of the 14th to 25th bits. 2nd to 25th bits are the card numbers.</p>
Wiegand26a	<p>ESSSSSSSSSSSSSSSSSSSSSSSSSSSS</p> <p>Consists of 26 bits of binary code. The 1st bit is the even parity bit of the 2nd to 13th bits, while the 26th bit is the odd parity bit of the 14th to 25th bits. 2nd to 9th bits are the site codes, while the 10th to 25th bits are the card numbers.</p>
Wiegand34	<p>EEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE</p> <p>Consists of 34 bits of binary code. The 1st bit is the even parity bit of the 2nd to 17th bits, while the 34th bit is the odd parity bit of the 18th to 33rd bits. 2nd to 25th bits are the card numbers.</p>
Wiegand34a	<p>ESSSSSSSSSSSSSSSSSSSSSSSSSSSS</p> <p>Consists of 34 bits of binary code. The 1st bit is the even parity bit of the 2nd to 17th bits, while the 34th bit is the odd parity bit of the 18th to 33rd bits. 2nd to 9th bits are the site codes, while the 10th to 25th bits are the card numbers.</p>
Wiegand36	<p>OFFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCMME</p> <p>Consists of 36 bits of binary code. The 1st bit is the odd parity bit of the 2nd to 18th bits, while the 36th bit is the even parity bit of the 19th to 35th bits. 2nd to 17th bits are the device codes. The 18th to 33rd bits are the card numbers, and the 34th to 35th bits are the manufacturer codes.</p>
Wiegand36a	<p>EEEEEEEEEEEEEEEEFFFFFFFFCCCCCCCCCCCC</p> <p>Consists of 36 bits of binary code. The 1st bit is the even parity bit of the 2nd to 18th bits, while the 36th bit is the odd parity bit of the 19th to 35th bits. 2nd to 19th bits are the device codes, and the 20th to 35th bits are the card numbers.</p>
Wiegand37	<p>OMMMMMSSSSSSSSSSSSSSSSSSSSSSSSSS</p> <p>Consists of 37 bits of binary code. The 1st bit is the odd parity bit of the 2nd to 18th bits, while the 37th bit is the even parity bit of the 19th to 36th bits. 2nd to 4th bits are the manufacturer codes. 5th to 16th bits are the site codes, and the 21st to 36th bits are the card numbers.</p>
Wiegand37a	<p>EMMMFFFFFFFFFFFFSSSSSSSSSSSSSSSSSSSS</p> <p>Consists of 37 bits of binary code. The 1st bit is the even parity bit of the 2nd to 18th bits, while the 37th bit is the odd parity bit of the 19th to 36th bits. 2nd to 4th bits are the manufacturer codes. 5th to 14th bits are the device codes, and 15th to 20th bits are the site codes, and the 21st to 36th bits are the card numbers.</p>
Wiegand50	<p>ESSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSS</p> <p>Consists of 50 bits of binary code. The 1st bit is the even parity bit of the 2nd to 25th bits, while the 50th bit is the odd parity bit of the 26th to 49th bits. 2nd to 17th bits are the site codes, and the 18th to 49th bits are the card numbers.</p>

“C” denotes the card number; “E” denotes the even parity bit; “O” denotes the odd parity bit; “F” denotes the facility code; “M” denotes the manufacturer code; “P” denotes the parity bit; and “S” denotes the site code.

9.5.2 Wiegand Out

On **Wiegand Settings** interface, tap [**Wiegand Out**] to open the Wiegand Out interface.

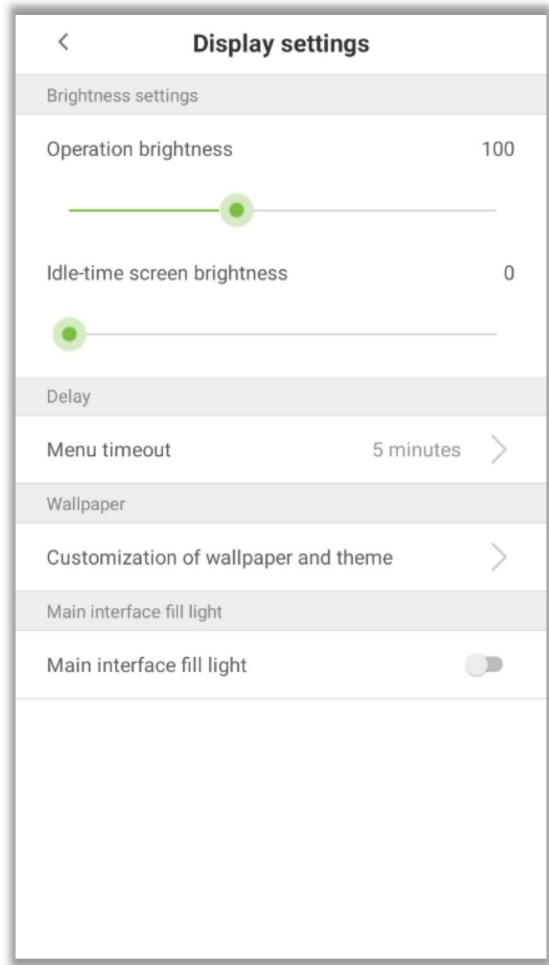


Function Description

Menu	Function Description
Wiegand Format	The Wiegand format value could be 26bits, 34bits, 36bits, 37bits, 50bits.
Wiegand out bits	After choosing the Wiegand format, you can select one of the corresponding output digits in the Wiegand format.
Failed ID	If the verification is failed, the system will send the failed ID to the device and replace the card number or personnel ID with the new ones.
Site Code	It is similar to device ID except that it can be set manually and repeatable with different devices. The default value ranges from 0 to 256.
Pulse Width(us)	The time width represents the changes of the quantity of electric charge with high-frequency capacitance regularly within a specified time.
Pulse Interval(us)	The time interval between pulses.
ID Type	Select the ID type as User ID or Card number.

9.6 Display Settings

In the system settings list, click Display Settings to open the display settings page:

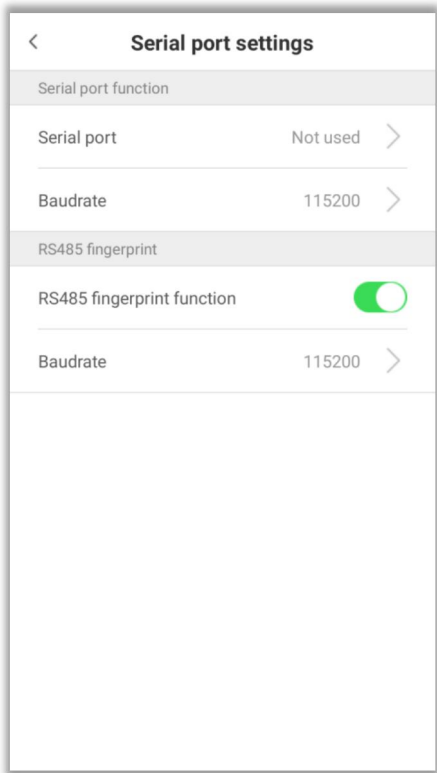


Menu		Function Description
Brightness settings	Operation brightness	Set the device brightness during operation, such as face recognition.
	Idle-time screen brightness	Screen brightness in standby mode.
Delay	Menu timeout	<p>When the user enters the menu and does not perform any operation within a certain period of time, a menu timeout occurs and the device enters standby mode.</p> <p>The options are: 30 seconds, 1 minute, 2 minutes, 5 minutes, 10 minutes, or disabled. When this feature is disabled, the menu (including submenus) will not automatically close. Users must press the "Exit" button to exit the menu.</p>

Wallpaper	Customization of wallpaper and theme	Users can choose their favorite wallpaper from the theme wallpaper interface to improve the user experience
Main interface fill light	Main interface fill light	After activation, the light-compensation function will be activated on the standby screen when the environment is dark

9.7 Serial port settings

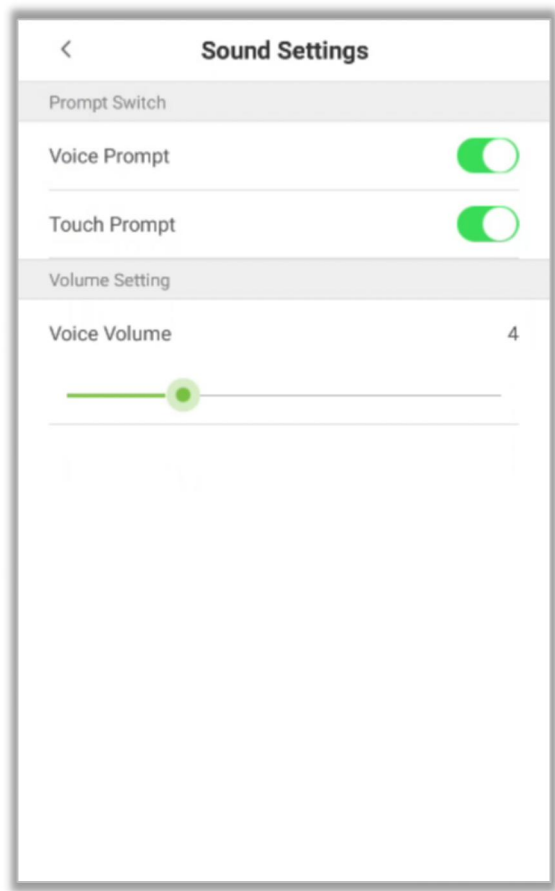
- On the System Settings interface, tap [Serial port settings] to enter sound settings interface.



Menu	Function Description
Serial Port	Not used: Do not communicate with the device through the serial port.
Baudrate	The rate at which the data is communicated with PC, there are 4 options of baud rate: 115200 (default), 57600, 38400, and 19200. The higher is the baud rate, the faster is the communication speed, but also the less reliable. Hence, a higher baud rate can be used when the communication distance is short; when the communication distance is long, choosing a lower baud rate would be more reliable.
RS485 fingerprint function	Communicates with the RS485 fingerprint through RS485 serial port.

9.8 Sound Settings

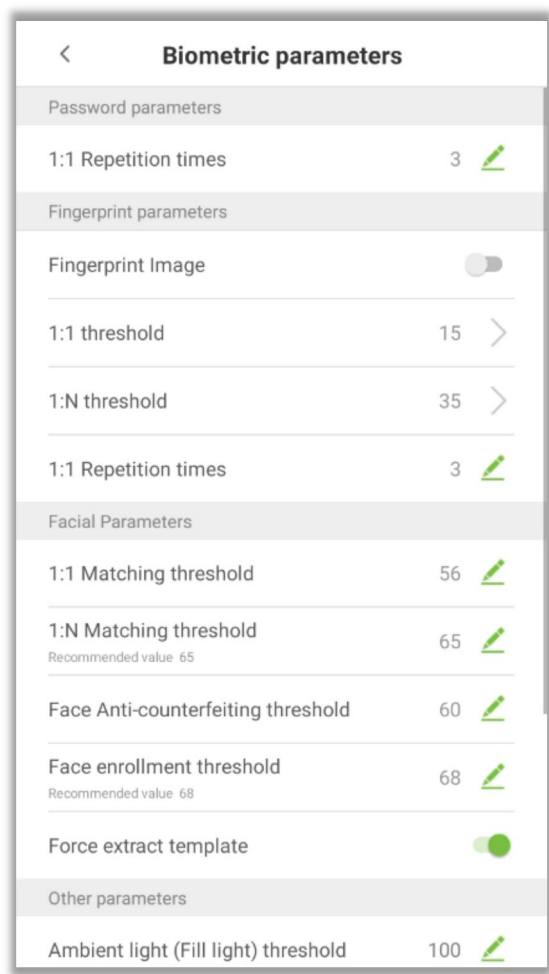
In the system settings list, tap on "Sound Settings" to access the sound settings interface.



Menu	Function Description
Voice Prompt	When voice prompts are enabled, users will receive voice prompts. When this setting is disabled, users will not receive voice prompts.
Touch Prompt	This option enables/disables touchscreen prompts. When enabled, users will receive touchscreen prompts. When disabled, they will not receive touchscreen prompts
Voice Volume	This option is used to adjust the volume. This can only be used when audio prompts are enabled. The value range is 0 ~ 15.

9.9 Biometric Parameters

In the system settings list, click on "Biometric Parameters" to open the "Biometric Parameters" interface

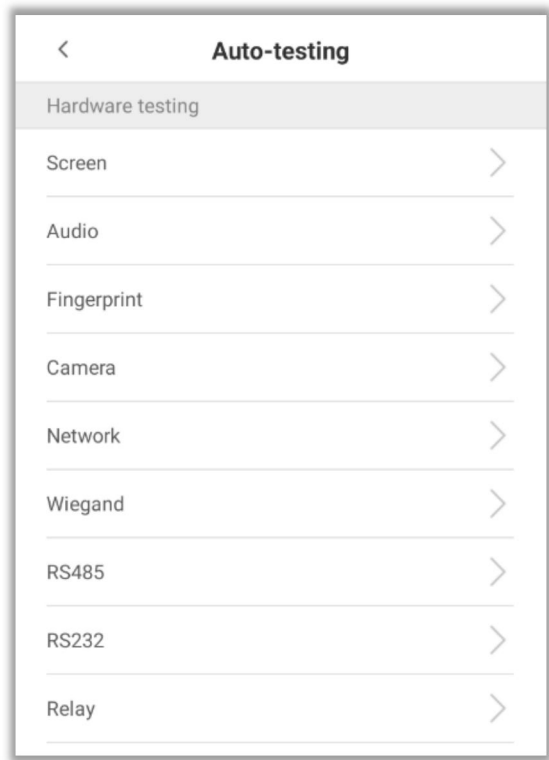


Menu		Function Description
Password parameters	1:1 Repetition times	The upper limit of the number of verification failures for 1:1. When the number of verification failures reaches the set value, the system will return to the backup interface.
Fingerprint parameters ★	Fingerprint image	The verification result pop-up will display the fingerprint image.
	1:1 threshold	<p>When performing 1:1 fingerprint verification, fingerprint data is collected and instantly compared with the fingerprint data using a 1:1 algorithm. This is converted into a value, which is then compared with a set value. If the scanned fingerprint value exceeds the set value, the verification passes. If not, the verification fails.</p> <p>The higher the threshold, the more accurate the matching; the lower the threshold, the higher the matching success rate.</p>
	1:N threshold	During 1: N verification, fingerprint data is collected and compared with all fingerprint templates in the system using the 1: N algorithm. It is converted into a value and compared with a set value. If the scanned fingerprint value exceeds the set value, the verification passes. If not, the verification fails.

Facial parameters		The higher the threshold, the more accurate the matching; the lower the threshold, the higher the matching success rate.
	1:1 Repetition times	The upper limit of the number of failed 1:1 verification attempts. When the number of failed verification attempts reaches the set value, the system will return to the alternate interface.
	1:1 Matching threshold	<p>When performing 1:1 face verification, face data is collected and instantly compared with the face data using a 1:1 algorithm. This is converted into a value and then compared with a set value. If the scanned face value exceeds the set value, the verification passes. If not, the verification fails.</p> <p>The higher the threshold, the more accurate the matching; the lower the threshold, the higher the matching success rate.</p>
	1:N Matching threshold	<p>During 1:N verification, face data is collected and instantly compared with all face templates on the system using a 1:N algorithm. It is converted into a value and compared with a set value. If the scanned face value exceeds the set value, the verification passes. If not, the verification fails.</p> <p>The higher the threshold, the more accurate the matching; the lower the threshold, the higher the matching success rate.</p>
	Face anti-counterfeiting threshold	Set parameter N. Only when the recognition accuracy rate reaches N or above, can it be considered as a successful recognition.
	Face enrollment threshold	In facial recognition, the higher the threshold is set, the higher the accuracy of face recognition will be, which may lead to failure to recognize. On the contrary, if the threshold is too low, the accuracy of face recognition will be low, which may lead to misjudgment and other phenomena. The default value is 68.
	Force extract template	Forced extraction of faces from some photos with poor quality.

9.10Automatic Testing

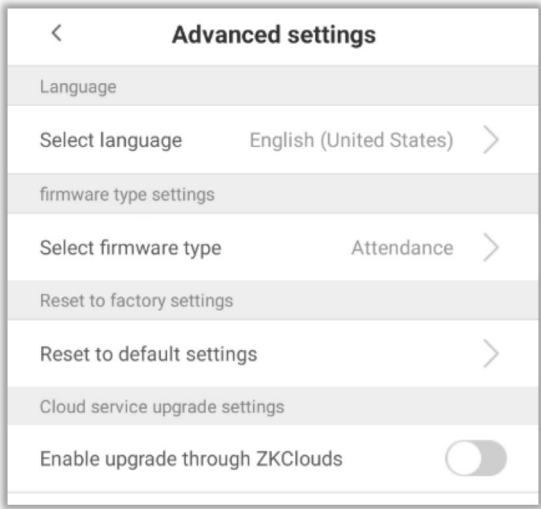
In the system settings list, tap [Auto Test] to enter the auto test interface.



Menu	Function Description
Screen testing	Test the screen display. The screen will be tested to display red, green, blue, white, and black. It also checks whether the screen colors are consistent and correct in each area of the screen. During the test, click anywhere on the screen to continue the test. Tap the back button to exit the test
Audio testing	The device automatically tests the audio prompt by playing the audio file stored in the device to test whether the audio file of the device is complete and whether the audio effect works normally. Tap the back button to exit the test.
Camera test	Test whether the camera works normally. It also checks whether the image quality is clear and obvious.
Network testing	Enter the corresponding IP address to test whether the network is normal.
Wiegand test	Test whether Wiegand works normally.
RS485	Test whether RS485 works normally.
RS232	Test whether RS232 works normally.
Relay	Test whether the lock can be opened/closed and the alarm lamp can be turned on/off normally.

9.11 Advanced Setting

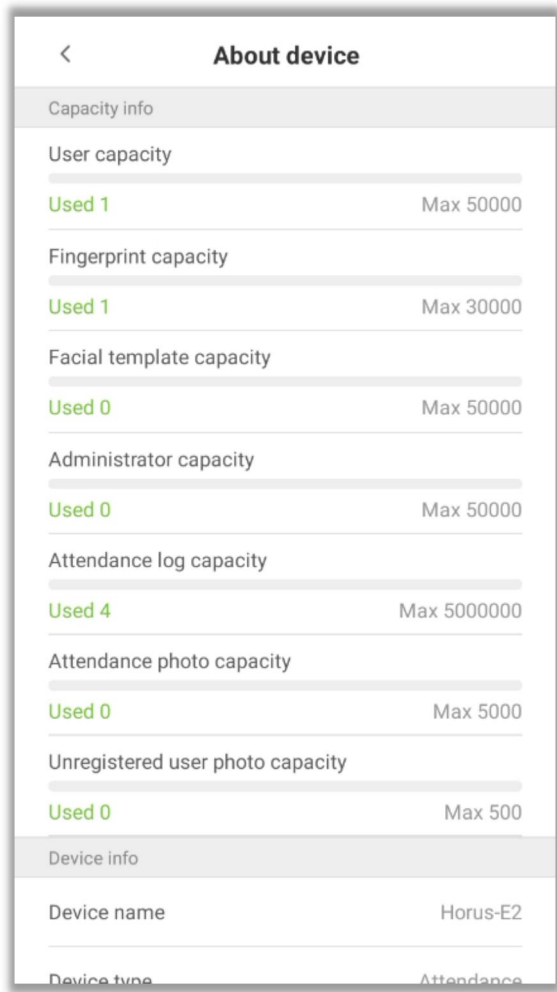
In the system settings list, tap on "Advanced Settings" to enter the "Advanced Settings" interface.



Menu	Function Description
Select language	Multi-language optional
Ret to default settings	Restore the device settings, including communication settings, system settings, etc., to the factory default settings
ADB network debugging	ADB tool refers to the Android Debug Bridge tool. It is a command line window used to interact with the emulator or real device through the system.
Enable upgrade through ZKClouds	Online upgrade can be performed through software.

9.12 About Device

In the system settings list, tap "About Device" to open the "About Device" interface.



Menu	Function Description
Capacity information	Display the user capacity, fingerprint ★, face template, administrator, attendance record, attendance photo, stranger photo, and user photo of the current device.
Device information	Display the name, type, serial number, MAC address, platform information, platform version, and manufacturer details of the device.
Version	Display all versions of all apps in the system, such as system settings, data management, and other installed apps.

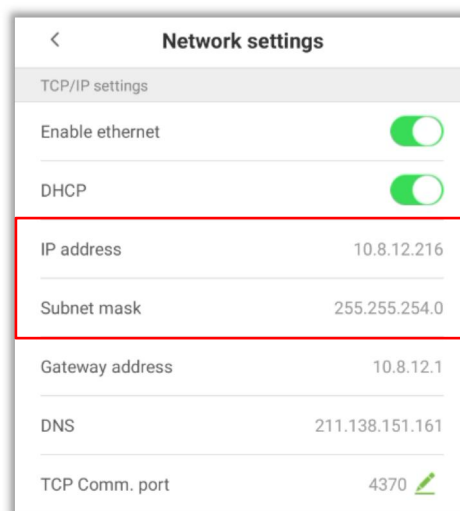
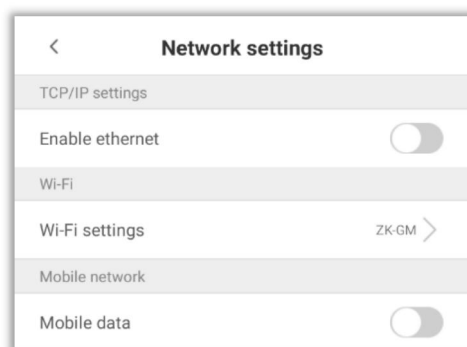
10 Connect to ZKBioTime Software

10.1 Set the Communication Address

Device Side

1. Tap **[Enable ethernet]** on the **"Network Settings"** interface to set the IP address and gateway of the device.

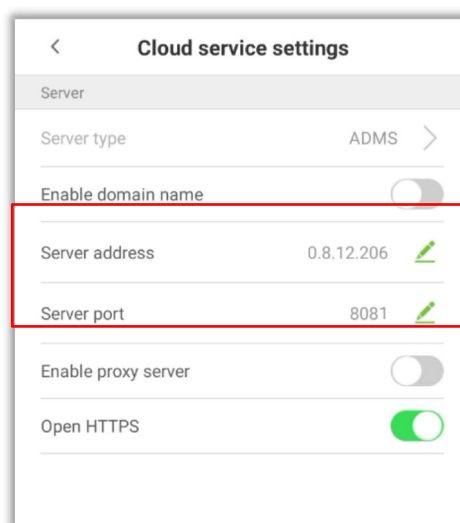
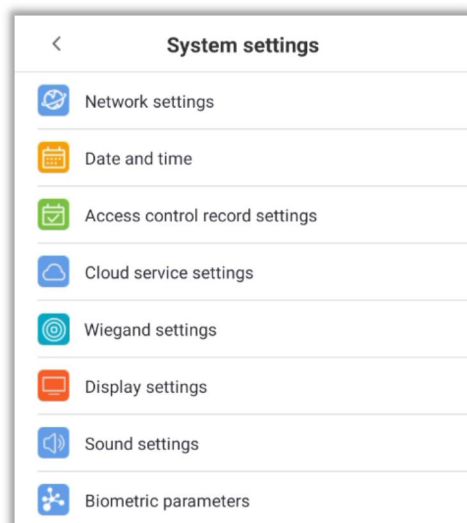
Note: Please ensure that the IP address is in the same network segment as the server address and can communicate with the ZKBioTime server.



2. On System Settings interface, tap **[Cloud Service Settings]** to enter the Cloud Service Settings interface. To set the server address and server port.

Server address: Set the IP address as of ZKBioTime server.

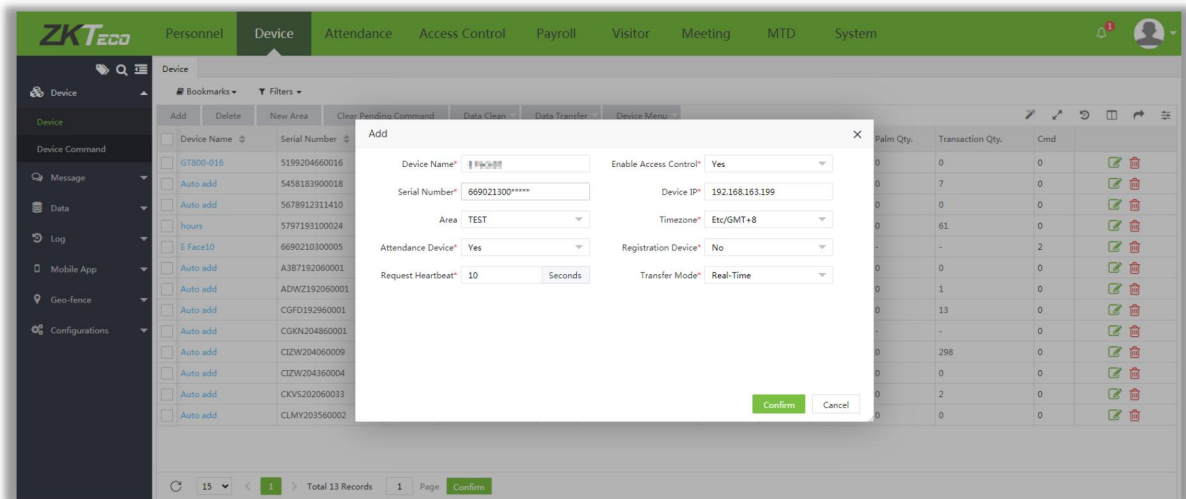
Server port: Set the server port as of ZKBioTime (The default is 8081).



10.2 Add Device on the Software

Add the device by searching. The process is as follows:

1. Click **Device > Device > Add**, to add the device on the software.
2. A new window pops-up on clicking **Add**. Enter the required information about the device and click **Confirm**, then the added devices are displayed automatically.



10.3 Add Personnel on the Software

1. Click **Personnel > Employee > Add**:

2. Fill in all the required fields and click **Confirm** to register a new user.

Click **Device > Device > Data Transfer > Sync Data to Device** to synchronize all the data to the device including the new users.

Privacy Policy

Notice:

To help you better use the products and services of ZKTeco and its affiliates, hereinafter referred as "we", "our", or "us", the smart service provider, we consistently collect your personal information. Since we understand the importance of your personal information, we took your privacy sincerely and we have formulated this privacy policy to protect your personal information. We have listed the privacy policies below to precisely understand the data and privacy protection measures related to our smart products and services.

Before using our products and services, please read carefully and understand all the rules and provisions of this Privacy Policy. If you do not agree to the relevant agreement or any of its terms, you must stop using our products and services.

I. Collected Information

To ensure the normal product operation and help the service improvement, we will collect the information voluntarily provided by you or provided as authorized by you during registration and use or generated as a result of your use of services.

- 1. User Registration Information:** At your first registration, the feature template (Fingerprint template/Face template/Palm template) will be saved on the device according to the device type you have selected to verify the unique similarity between you and the User ID you have registered. You can optionally enter your Name and Code. The above information is necessary for you to use our products. If you do not provide such information, you cannot use some features of the product regularly.
- 2. Product information:** According to the product model and your granted permission when you install and use our services, the related information of the product on which our services are used will be collected when the product is connected to the software, including the Product Model, Firmware Version Number, Product Serial Number, and Product Capacity Information. **When you connect your product to the software, please carefully read the privacy policy for the specific software.**

II. Product Security and Management

1. When you use our products for the first time, you shall set the Administrator privilege before performing specific operations. Otherwise, you will be frequently reminded to set the Administrator privilege when you enter the main menu interface. **If you still do not set the Administrator privilege after receiving the system prompt, you should be aware of the possible security risk (for example, the data may be manually modified).**
2. All the functions of displaying the biometric information are disabled in our products by default. You can choose Menu > System Settings to set whether to display the biometric information. If you enable these functions, we assume that you are aware of the personal privacy security risks specified in the privacy policy.

3. Only your user ID is displayed by default. You can set whether to display other user verification information (such as Name, Department, Photo, etc.) under the Administrator privilege. **If you choose to display such information, we assume that you are aware of the potential security risks (for example, your photo will be displayed on the device interface).**
4. The camera function is disabled in our products by default. If you want to enable this function to take pictures of yourself for attendance recording or take pictures of strangers for access control, the product will enable the prompt tone of the camera. **Once you enable this function, we assume that you are aware of the potential security risks.**
5. All the data collected by our products is encrypted using the AES 256 algorithm. All the data uploaded by the Administrator to our products are automatically encrypted using the AES 256 algorithm and stored securely. If the Administrator downloads data from our products, we assume that you need to process the data and you have known the potential security risk. In such a case, you shall take the responsibility for storing the data. You shall know that some data cannot be downloaded for sake of data security.
6. All the personal information in our products can be queried, modified, or deleted. If you no longer use our products, please clear your personal data.

III. How we handle personal information of minors

Our products, website and services are mainly designed for adults. Without consent of parents or guardians, minors shall not create their own account. If you are a minor, it is recommended that you ask your parents or guardian to read this Policy carefully, and only use our services or information provided by us with consent of your parents or guardian.

We will only use or disclose personal information of minors collected with their parents' or guardians' consent if and to the extent that such use or disclosure is permitted by law or we have obtained their parents' or guardians' explicit consent, and such use or disclosure is for the purpose of protecting minors.

Upon noticing that we have collected personal information of minors without the prior consent from verifiable parents, we will delete such information as soon as possible.

IV. Others

You can visit https://www.zkteco.com/cn/index/Index/privacy_protection.html to learn more about how we collect, use, and securely store your personal information. To keep pace with the rapid development of technology, adjustment of business operations, and to cope with customer needs, we will constantly deliberate and optimize our privacy protection measures and policies. Welcome to visit our official website at any time to learn our latest privacy policy.

Eco-friendly Operation



The product's "eco-friendly operational period" refers to the time during which this product will not discharge any toxic or hazardous substances when used in accordance with the prerequisites in this manual.

The eco-friendly operational period specified for this product does not include batteries or other components that are easily worn down and must be periodically replaced. The battery's eco-friendly operational period is 5 years.

Hazardous or Toxic substances and their quantities

Component Name	Hazardous/Toxic Substance/Element					
	Lead (Pb)	Mercury (Hg)	Cadmium (Cd)	Hexavalent Chromium (Cr6+)	Polybrominated Biphenyls (PBB)	Polybrominated Diphenyl Ethers (PBDE)
Chip Resistor	×	○	○	○	○	○
Chip Capacitor	×	○	○	○	○	○
Chip Inductor	×	○	○	○	○	○
Diode	×	○	○	○	○	○
ESD component	×	○	○	○	○	○
Buzzer	×	○	○	○	○	○
Adapter	×	○	○	○	○	○
Screws	○	○	○	×	○	○

This table is prepared in accordance with the provisions of SJ/T 11364.

○ indicates that the total amount of toxic content in all the homogeneous materials is below the limit as specified in GB/T 26572.

× indicates that the total amount of toxic content in all the homogeneous materials exceeds the limit as specified in GB/T 26572.

Note: 80% of this product's components are manufactured using non-toxic and eco-friendly materials. The components which contain toxins or harmful elements are included due to the current economic or technical limitations which prevent their replacement with non-toxic materials or elements.

ZKTeco Industrial Park, No. 32, Industrial Road,
Tangxia Town, Dongguan, China.
Phone : +86 769 - 82109991
Fax : +86 755 - 89602394
www.zkteco.com

