

User Manual

G4

Version: 1.0

Date: November 2018

Important Notice

Thank you for choosing our product. Before using this product, please carefully read this instruction manual. This will help prevent unnecessary damage to the product. Follow these instructions to ensure that your product functions properly and completes verifications in a timely manner.

Unless authorized by our company, no group or individual shall take excerpts of or copy all or part of these instructions nor transmit the contents of these instructions in any way.

The products described in this manual may include software that is copyrighted by our company and its possible licensors. No one may copy, publish, edit, take excerpts of, decompile, decode, reverse-engineer, rent, transfer, sublicense, or otherwise infringe upon the software's copyright unless authorized by the copyright holder. This is subject to relevant laws prohibiting such restrictions.



As this product is regularly updated, we cannot guarantee exact consistency between this product and the information provided in these instructions. We will hear no disputes that arise due to differences between the actual product and the contents of these instructions, and you may not be informed of changes in advance.

Contents

1. Instruction for Use.....	1
1.1 Using Your Fingerprints.....	1
1.2 Startup Screen.....	2
1.3 Virtual Keyboard.....	3
1.4 Change the Theme and Wallpaper.....	4
1.5 Verification Methods.....	9
1.5.1 Fingerprint Verification.....	9
1.5.2 Password Verification.....	16
1.5.3 Facial Verification.....	21
1.5.4 Combined Verification.....	25
2. Main Menu.....	29
3. Employee Management.....	31
3.1 Add an Employee.....	31
3.1.1 Register Basic Employee Information.....	33
3.1.2 Register Employee Photo.....	34
3.1.3 Registration Comparison Methods.....	38
3.1.4 Permission Settings.....	49
3.1.5 Period of Validity Settings.....	51
3.1.6 Verification Method Setup.....	53
3.2 Searching for an Employee.....	56
3.3 Edit an Employee.....	58
3.4 Delete Employee.....	60
4. Attendance Events.....	63
4.1 Add Attendance Events.....	63
4.2 Edit Attendance Events.....	68
4.3 Delete Attendance Events.....	70
5. Access Control Settings.....	73
6. Record Search.....	75
6.1 Search for Attendance Records.....	75
6.2 Search for Attendance Photos.....	80
6.3 Search for Blacklist Photos.....	85
7. Data Management.....	86
8. USB Disk Management.....	88
8.1 Upload to USB Drive.....	89
8.2 Download to a USB Drive.....	90
8.3 USB Disk Settings.....	91
9. Alarm Management.....	92

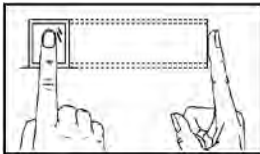
9.1 Add Alarms	92
9.2 Edit Alarms.....	98
9.3 Delete Alarms	100
10. System Settings	104
10.1 Network Settings.....	105
10.1.1 Ethernet Settings	106
10.1.2 Comm Connection Settings	108
10.2 Date and Time.....	109
10.2.1 Date and Time Settings	110
10.2.2 Date and Time Format Settings.....	112
10.3 ATT Parameters.....	114
10.3.1 Status Mode.....	115
10.3.2 Plugin Function Rules	127
10.3.3 Camera Mode.....	128
10.3.4 Verification Settings.....	129
10.3.5 Validity Period of User Information.....	131
10.4 Cloud Service Settings	133
10.5 Wiegand Settings	134
10.5.1 Wiegand In	135
10.5.2 Wiegand Out.....	136
10.6 Display Settings	138
10.7 Sound Settings	139
10.8 Biometric Parameters	140
10.9 Auto-testing.....	141
10.10 Advanced Settings	143
10.11 About the Device.....	144
Appendix.....	145
Statement on the Right to Privacy	146
Eco-friendly Use.....	147

1. Instruction for Use

1.1 Using Your Fingerprints

Recommended fingers: index, middle, or ring fingers; avoid using the thumb or pinky, as they are difficult to accurately press onto the fingerprint reader.

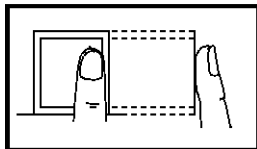
- Diagram of how to correctly press your fingers onto the fingerprint reader.



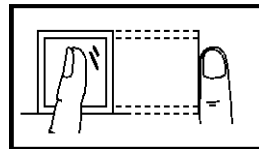
Press your finger onto the fingerprint reader.

Ensure that the center of your finger is aligned with the center of the fingerprint reader.

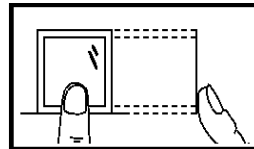
- Incorrect ways of pressing your fingers onto the fingerprint reader.



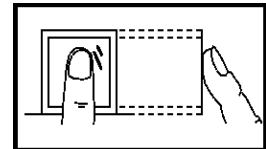
Off-center



Not the fingerprint's
center



Off-center

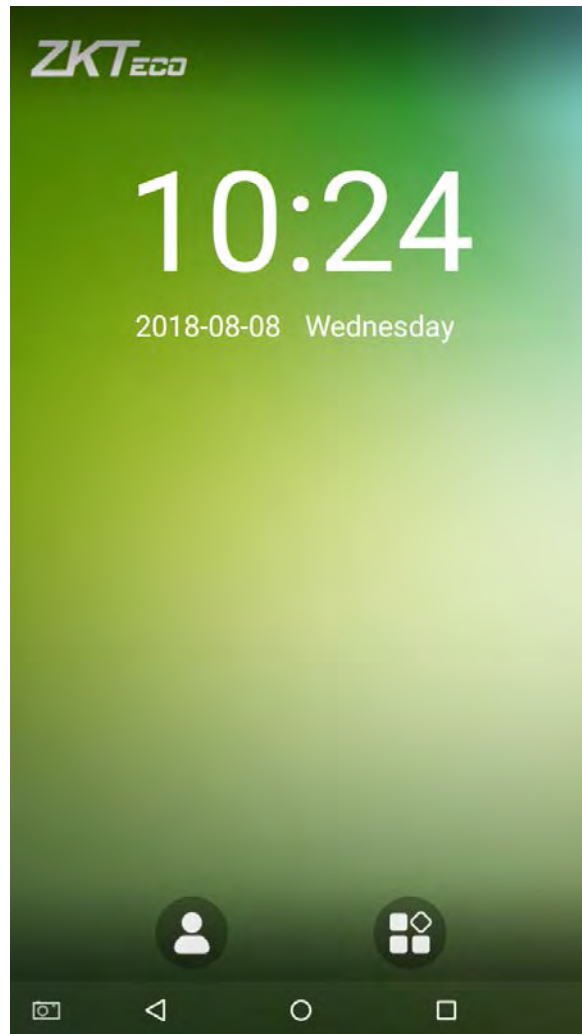


Not the fingerprint's
center



Note: Please use the correct method when pressing your fingers onto the fingerprint reader for registration and identification. Our company will assume no liability for recognition issues that may result from incorrect usage of the product. We reserve the right of final interpretation and modification concerning this point.

1.2 Startup Screen

After plugging in the device, press the On/Off switch located on the side. The following screen will load:

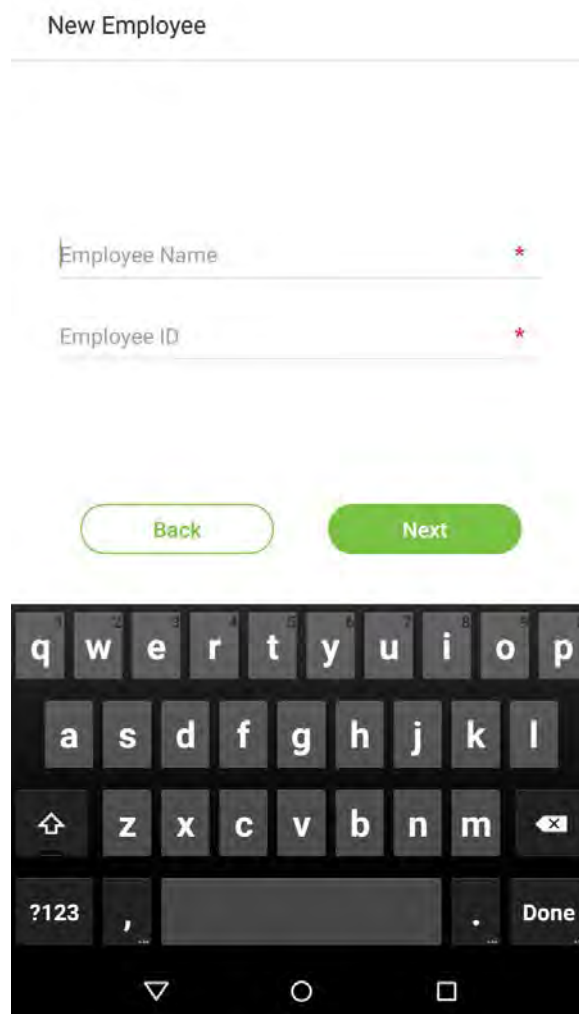


Notes:

- ✧ The wallpaper can be customized. For more details, please refer to “**1.4 Change Theme and Wallpaper**”.
- ✧ Tap on  to enter the personnel ID Input screen in 1:1 verification mode. For further information about the 1:1 verification process, see section “**1.5 Verification Method**”.
- ✧ Tap on  to enter the main menu. 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.

1.3 Virtual Keyboard

- English keyboard



Note: This device supports input methods of Chinese, English, numbers, and symbols. Press [CN] to switch to the Chinese keyboard; press [EN] to switch to the English keyboard; press [?123] to switch to the numbers and symbols keyboard; and press [Back] to return to the alphabet keyboard. If you tap on an input box, the virtual keyboard will pop up on the screen. To hide the keyboard, tap on the downwards arrow ▾.

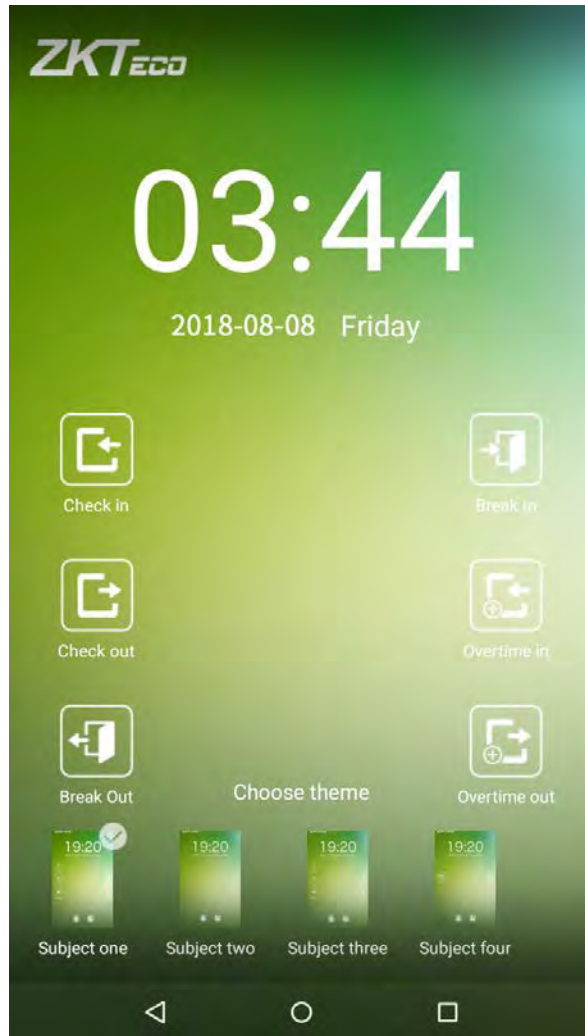
1.4 Change the Theme and Wallpaper

Tap on any blank area with your finger on the initial interface to change the theme and wallpaper, as shown below:

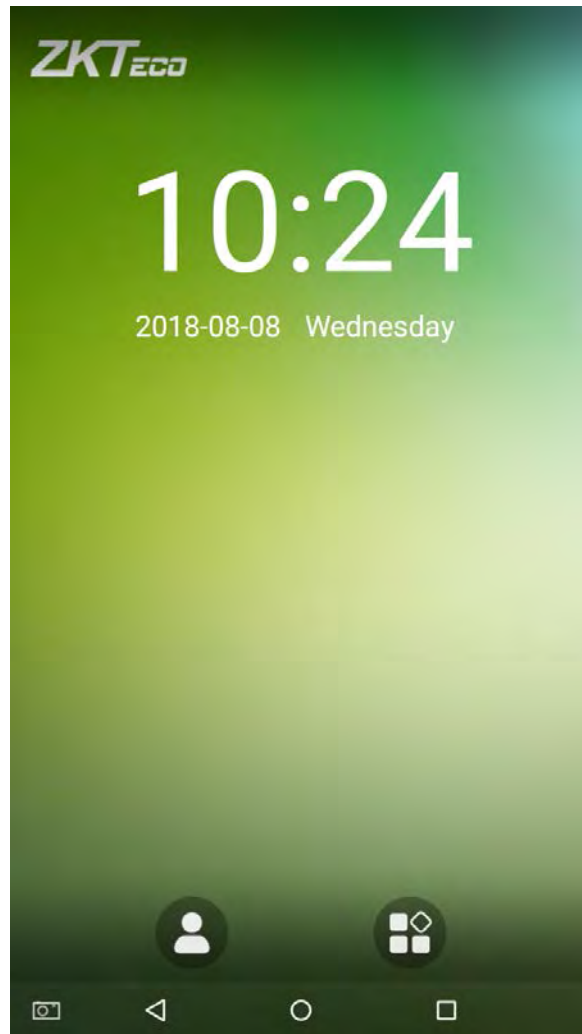


- **Change the theme**

1. Tap on [Choose theme] and select a theme at the bottom of the interface.



2. After the theme was set successfully, it will be displayed on the standby interface.

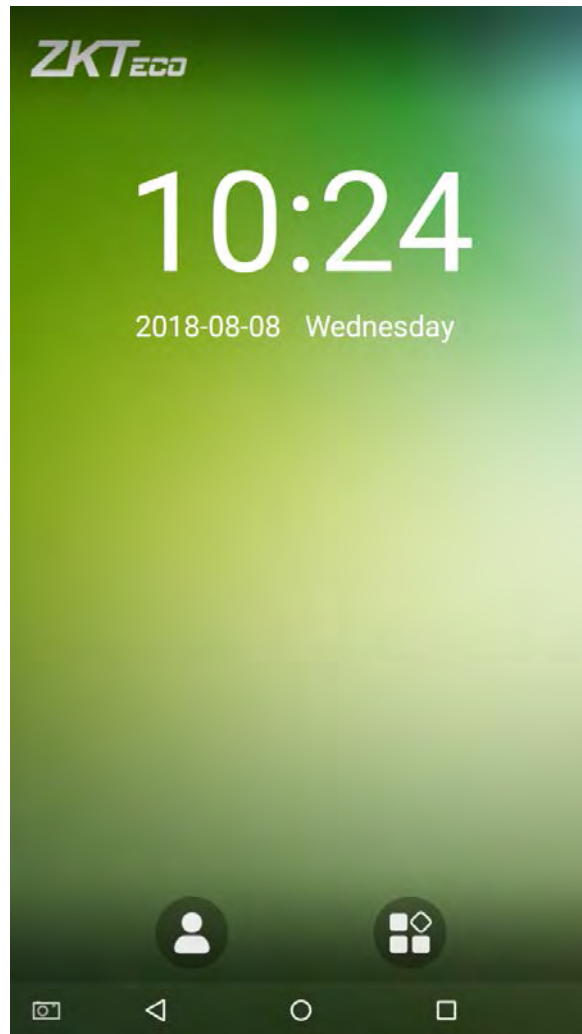


- **Change the wallpaper**

1. Press on any blank area on the screen for a while, then tap on the [Change wallpaper] icon, slide from right to left and back in the wallpaper choosing area to choose the desired wallpaper.



2. The wallpaper is set successfully and displayed on the standby interface.



1.5 Verification Methods

1.5.1 Fingerprint Verification

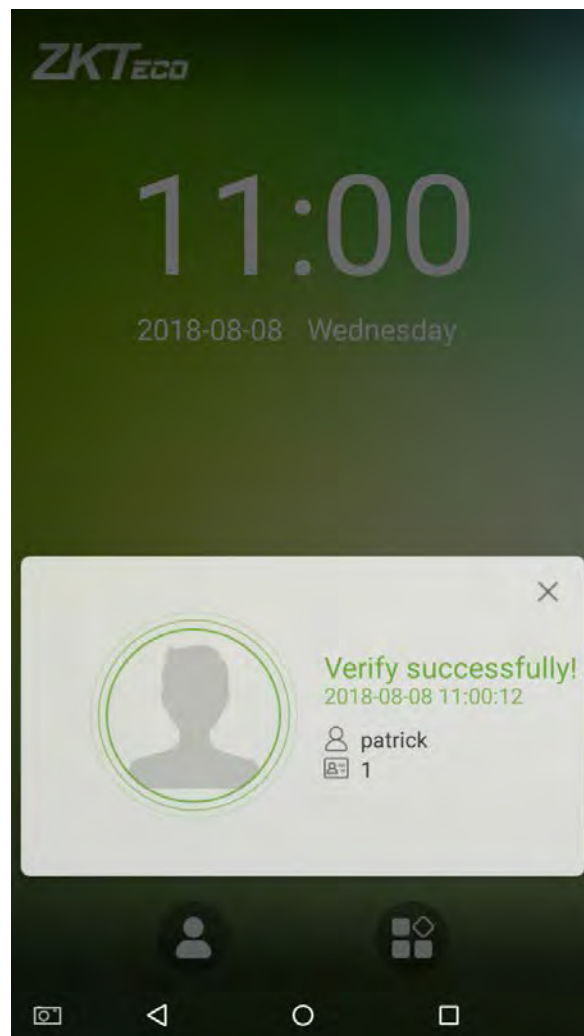
- **1:N fingerprint verification**

Compare the fingerprint that is being pressed onto the fingerprint reader with all of the fingerprint data that is stored in the device.

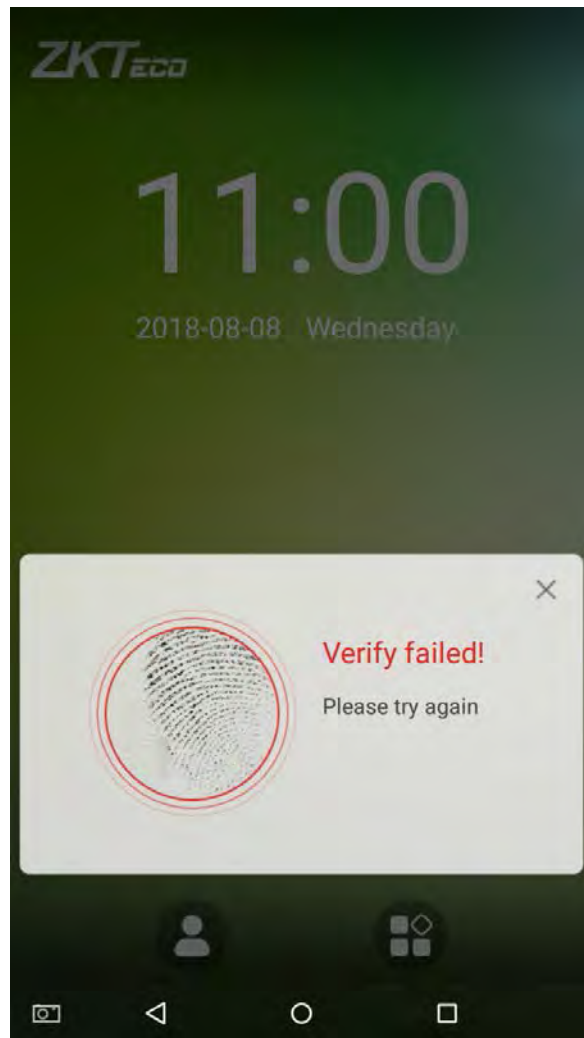
To enter fingerprint verification mode, simply press your finger on the fingerprint reader.

Make sure that you correctly press your fingerprint onto the fingerprint reader. Please refer to section **“1.1 Using your finger”** for further details.

Successful verification:




Verification is failed:

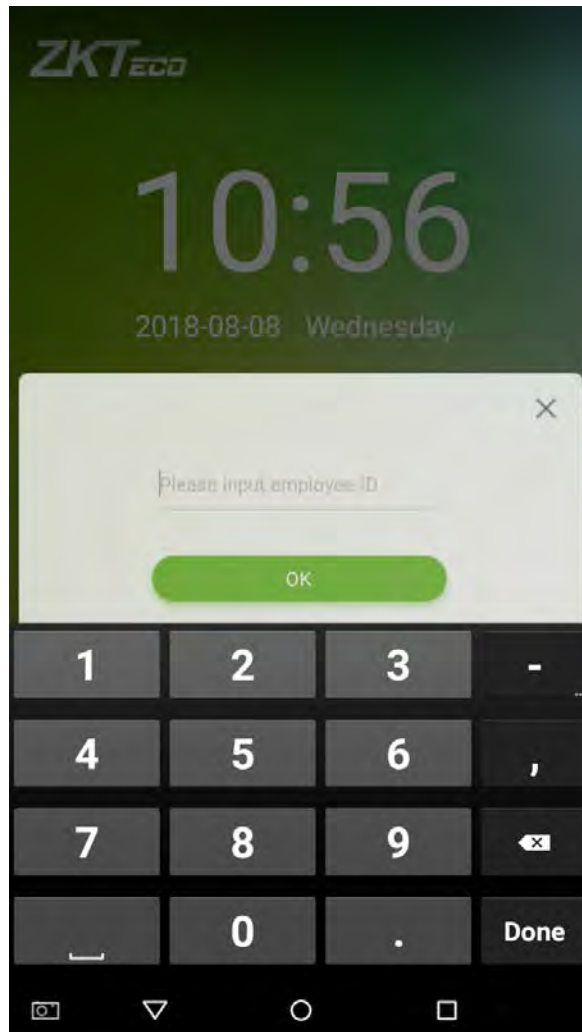


- **1:1 fingerprint verification**

Compares the fingerprint that is being pressed onto the fingerprint reader with the fingerprints that are linked to Employee ID input via the virtual keyboard. This method can be used when the system has trouble recognizing an employee's fingerprints.

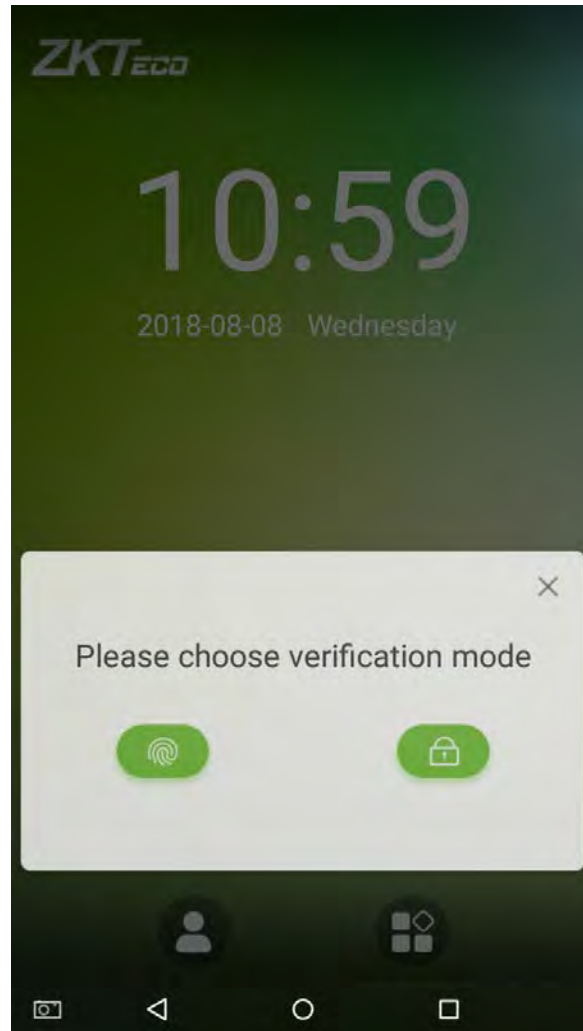
Press the  button on the main screen to enter 1:1 fingerprint verification mode:

1. Enter the Employee ID and press [OK].

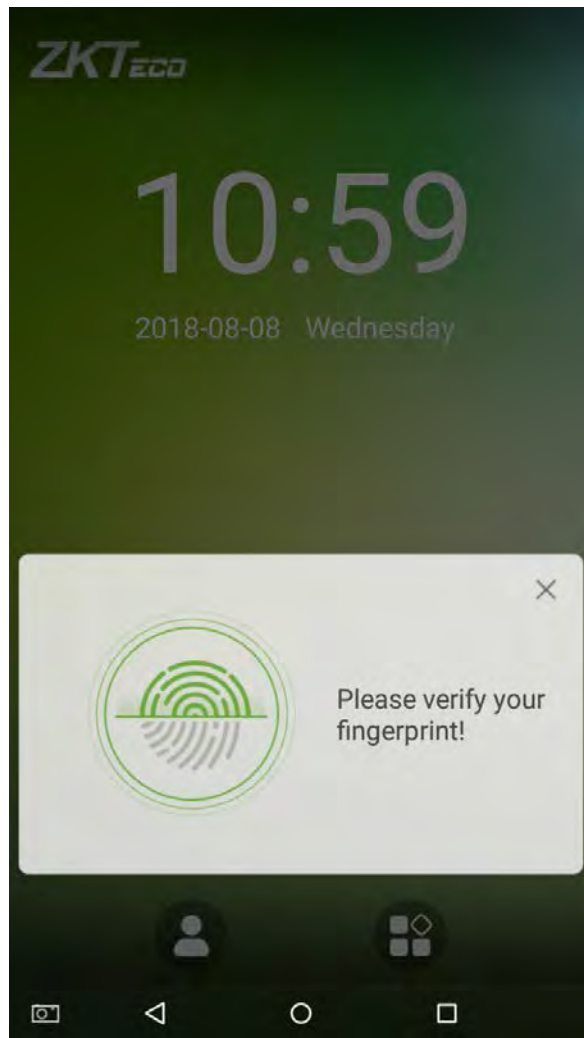


If an employee has registered a password and badge in addition to his/her fingerprints and the verification method is set to fingerprint/ password/ badge verification, the following screen will appear. Select the fingerprint icon

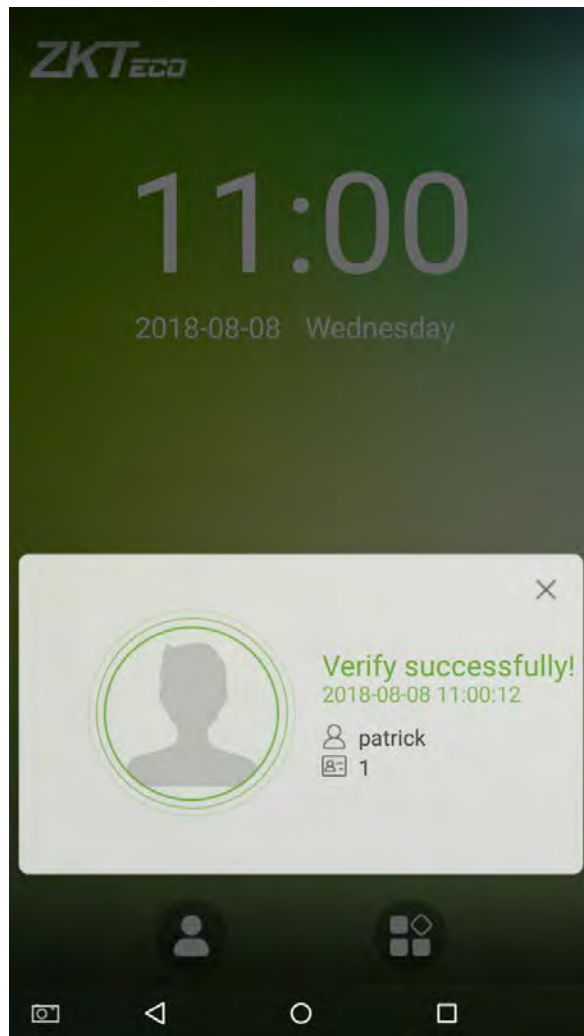
 to enter fingerprint verification mode:



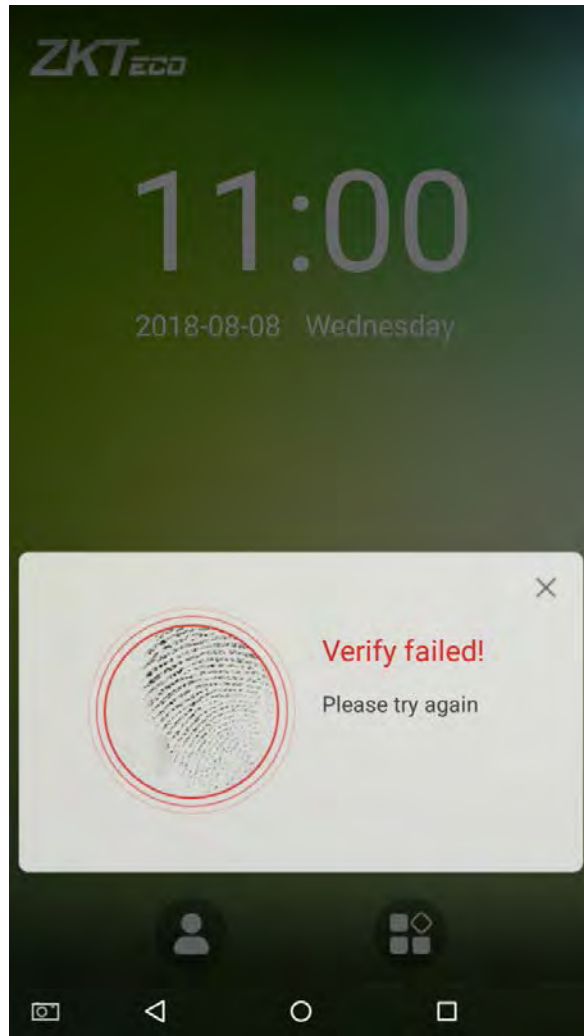
2. Press the finger on the fingerprint reader to proceed with verification.



3. Successfully verified.




4. Verification is failed.

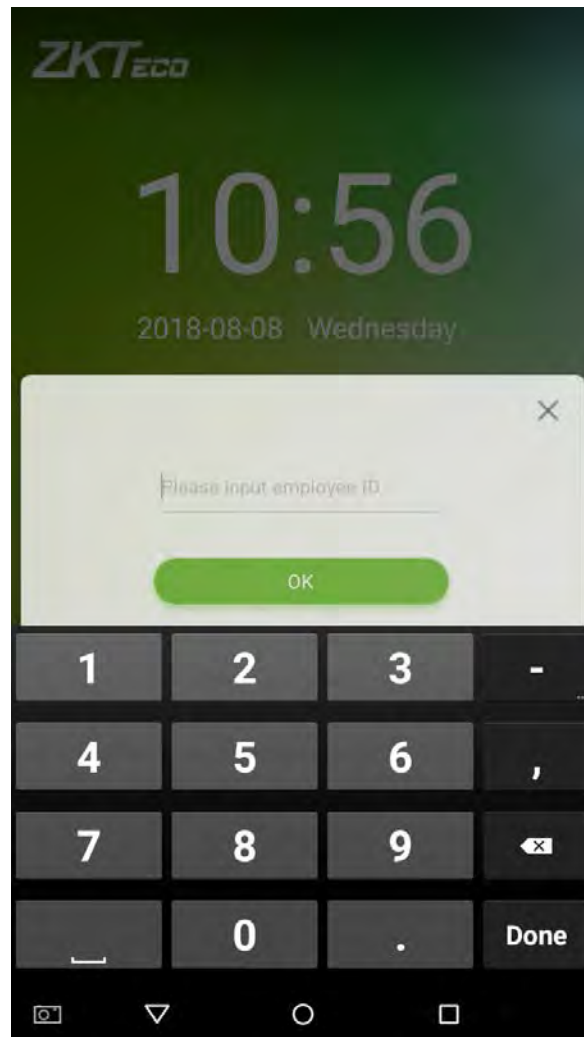



1.5.2 Password Verification

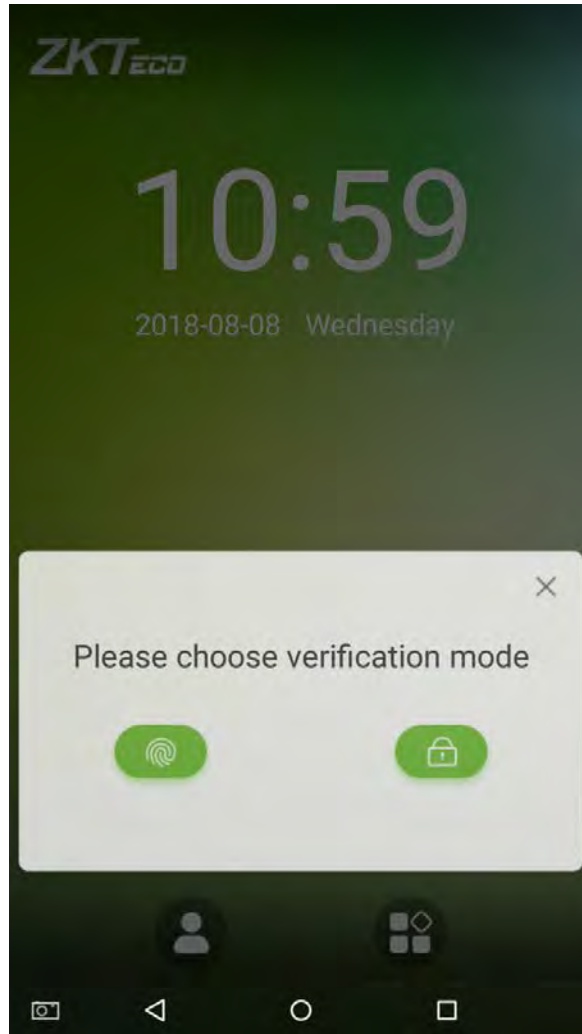
When an employee inputs his/her personnel ID and password into the device, the data will be compared to the personnel IDs and passwords saved in the system.

Tap on the  button on the main screen to enter the 1:1 password verification mode.

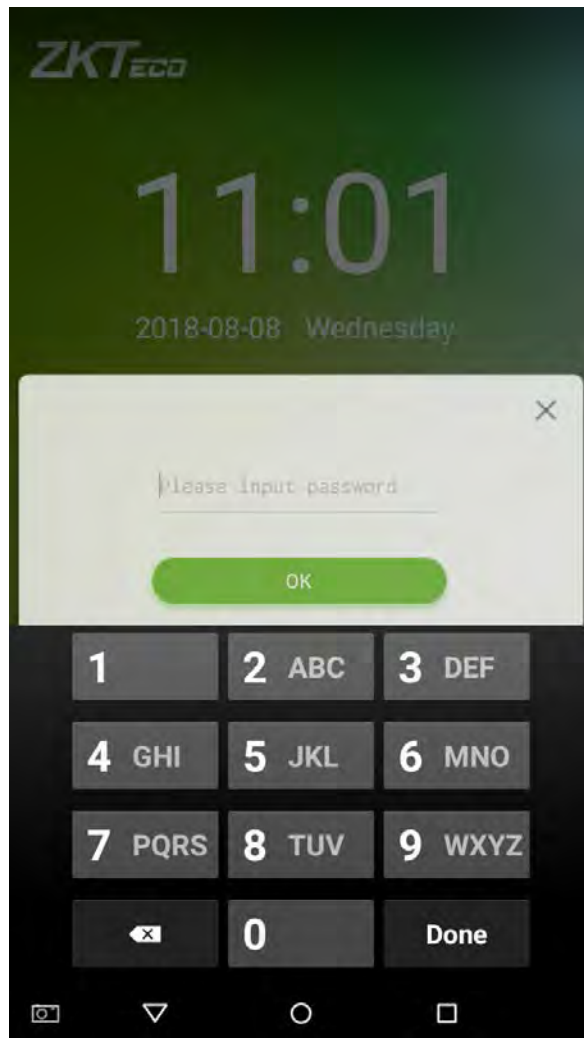
1. Enter the employee ID and press [OK].



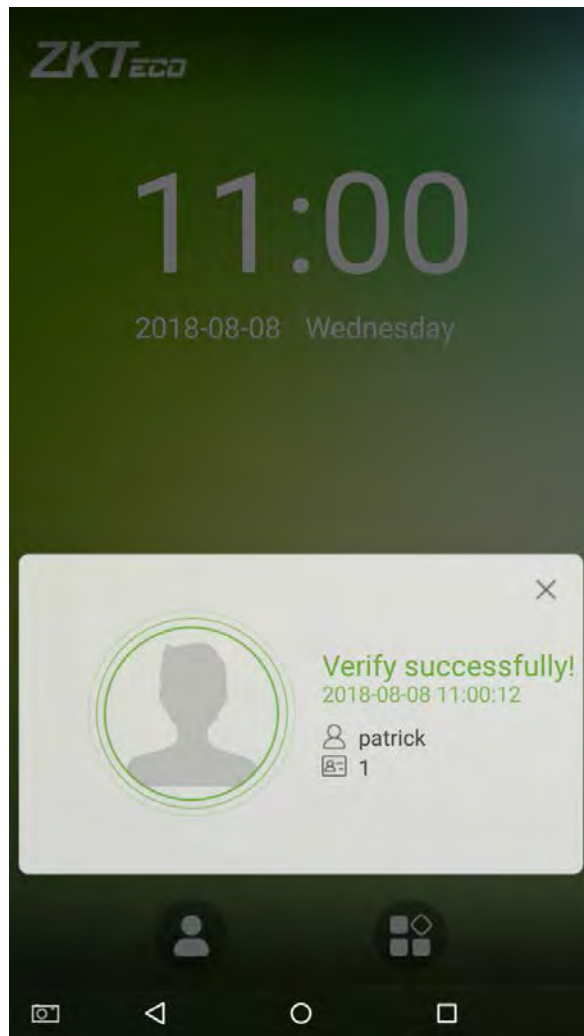
If an employee has registered a fingerprint and card in addition to a password and the verification method is set to fingerprint/password/card verification, the following screen will appear. Select the password icon  to enter password verification mode.



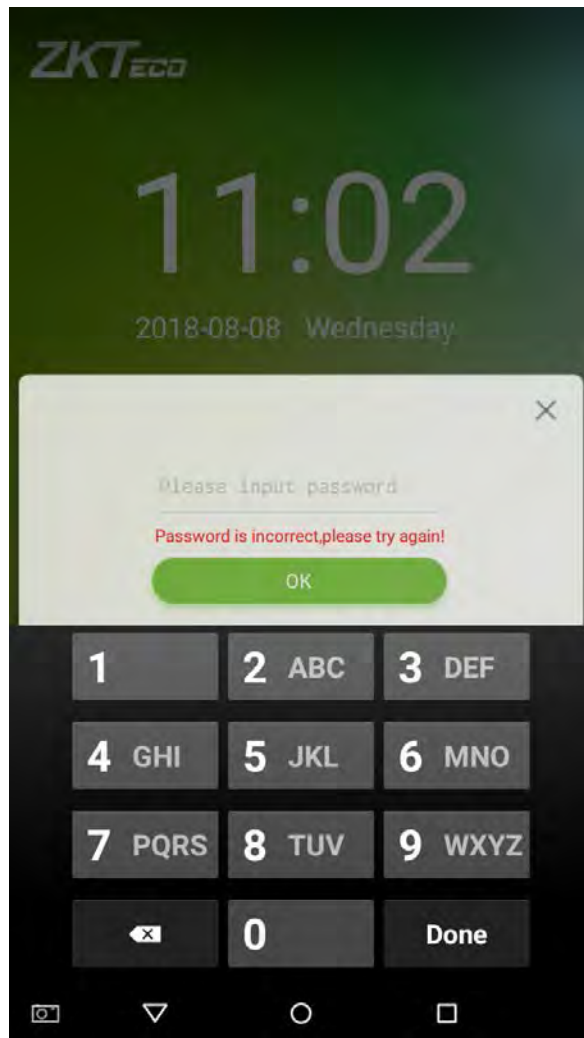
2. Enter a password and press [OK].




3. Successfully verified.



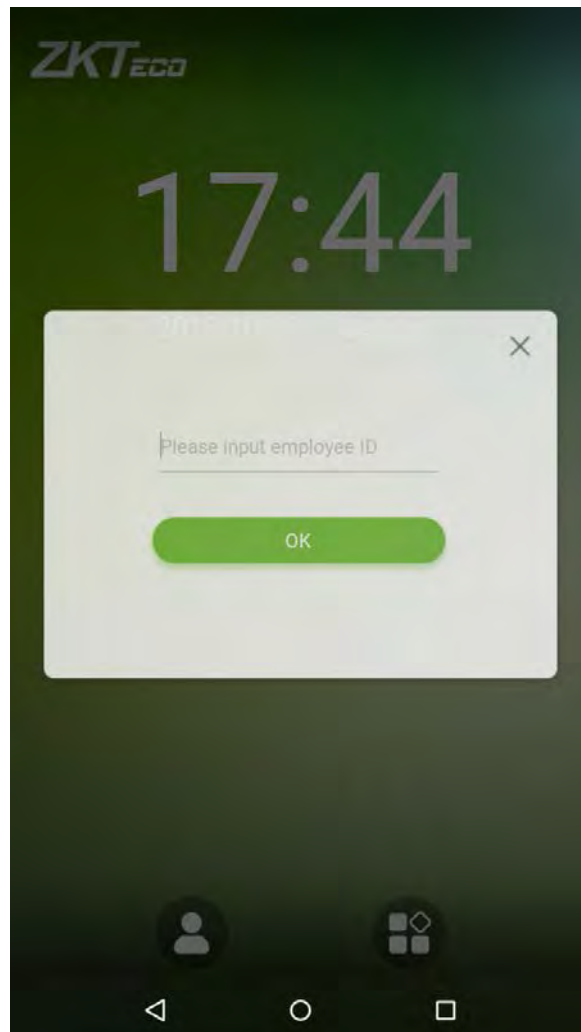
4. Verification is failed.



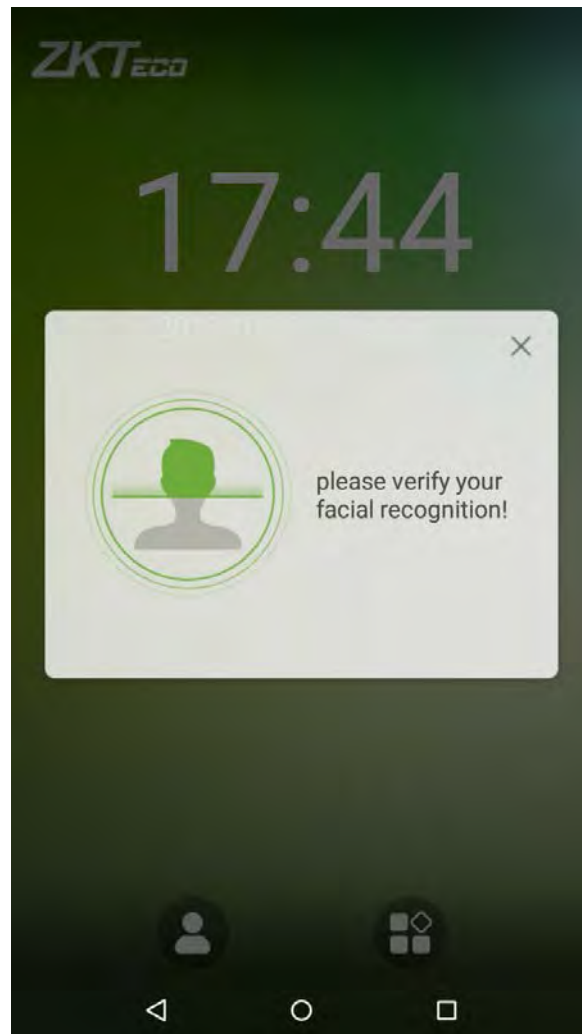
1.5.3 Facial Verification

Compare the face captured by the camera with the facial template related to the personnel ID input. Press  on the main interface and enter the 1:1 facial verification mode.

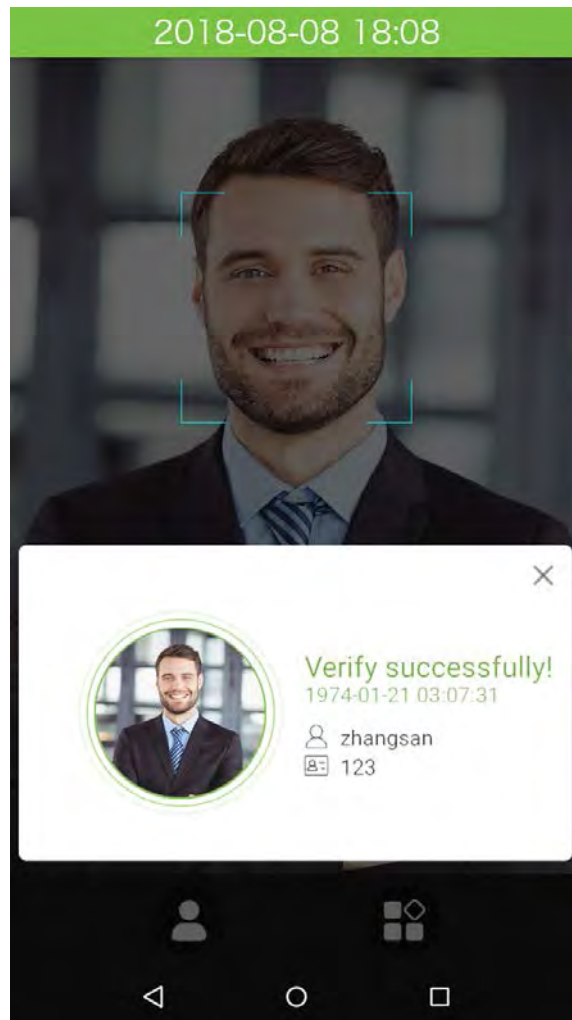
1. Input the personnel ID, click on [OK].



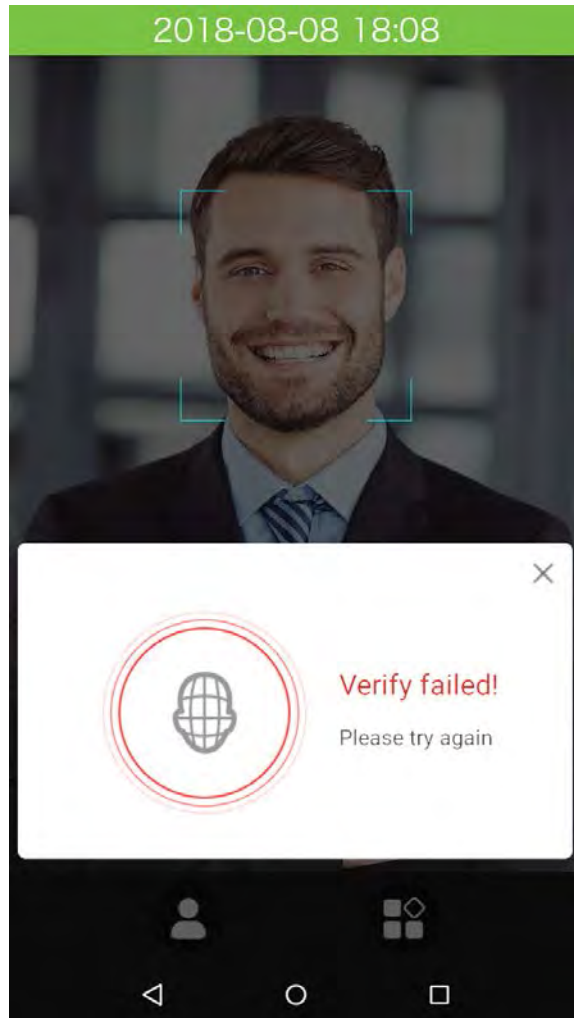
2. Look at the camera, make sure your face stay in the center of the camera.



3. Successfully verified.

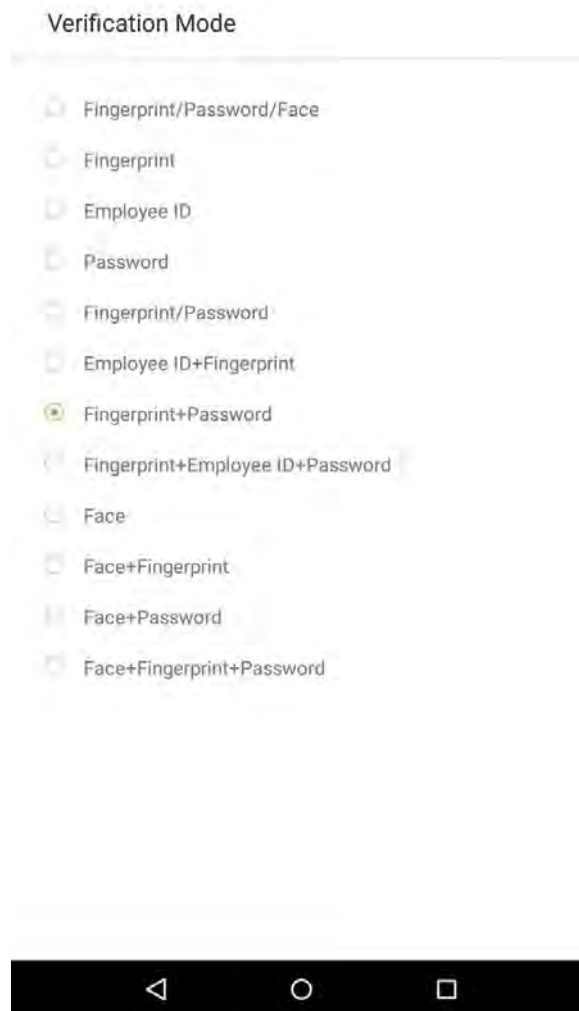


4. Verification is failed.



1.5.4 Combined Verification


To increase security, this device offers the option of using multiple forms of verification methods. A total of 12 different verification combinations can be used, as shown below:

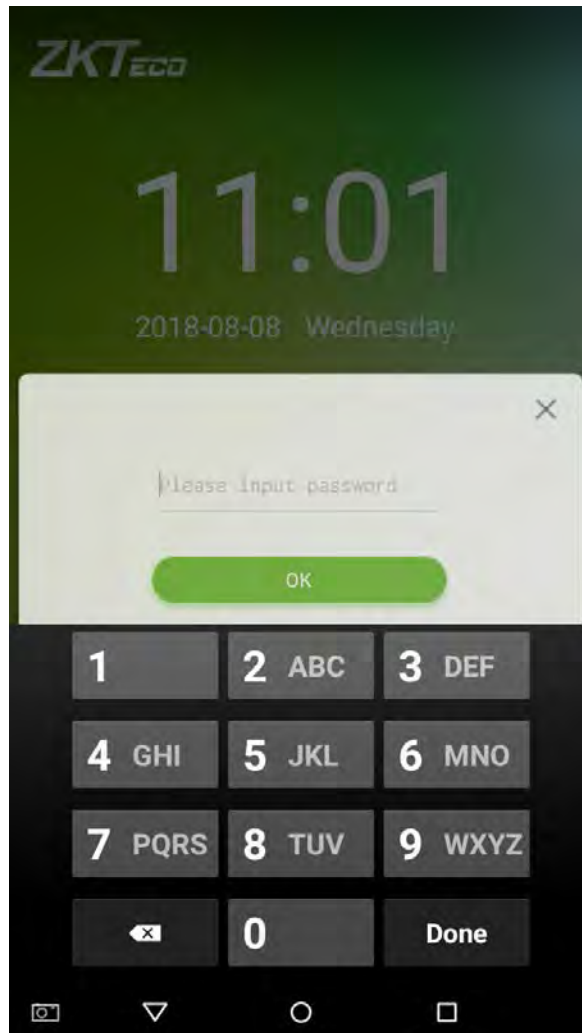


Notes:

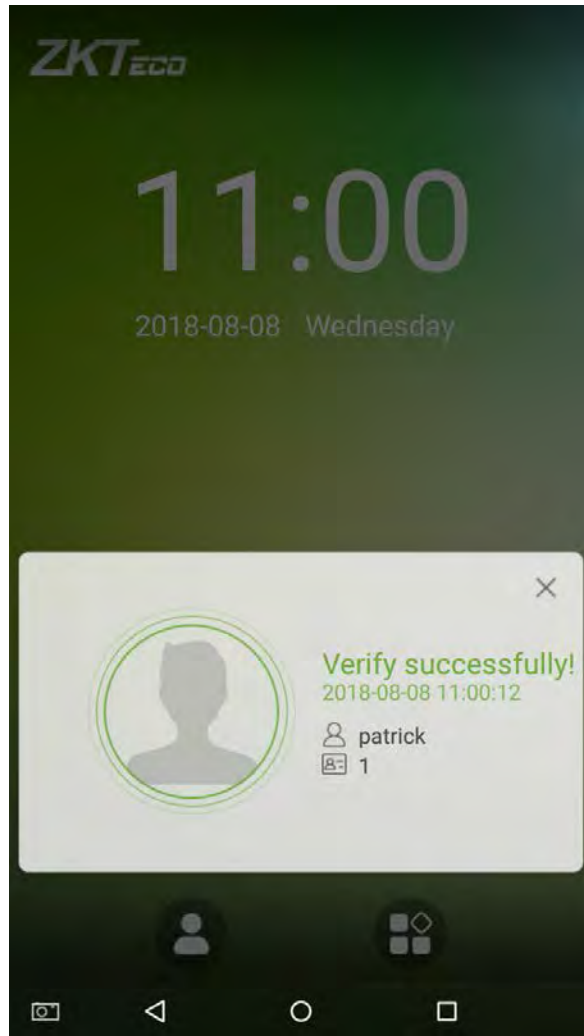
1. "/" means "or" and "+" means "and".
2. Combined verification requires employees to register the information needed to complete verification. Otherwise, employees may not be able to complete the verification process. For instance, when employee A registers with his/her fingerprint data, and the system's verification method is set as "Fingerprint + Password", the employee will not be able to complete the verification process.

The example below shows “Fingerprint + Password” verification. To log in to the system, please follow these steps:

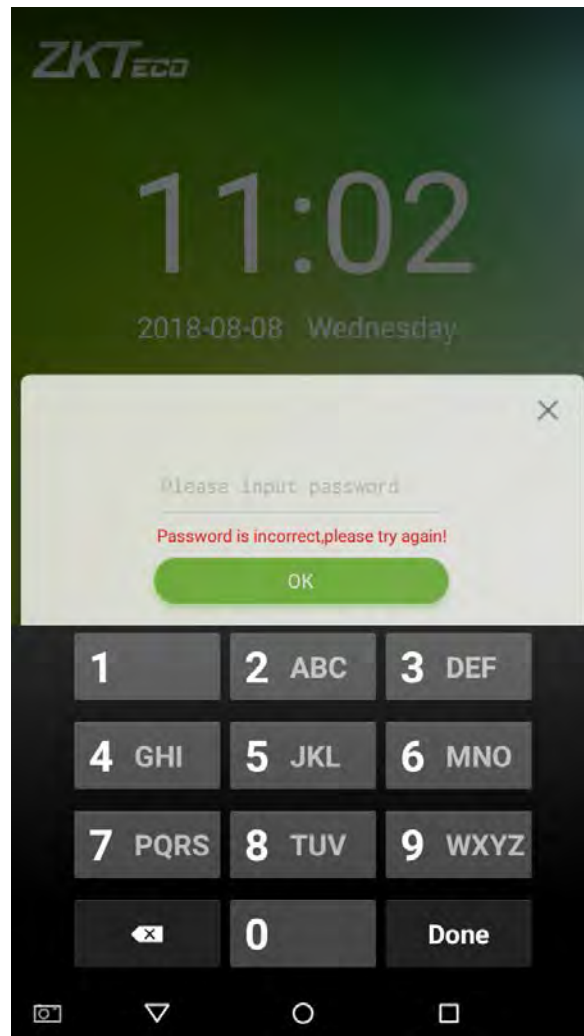
1. Press  to access the multiple verification interface, then the following window will appear. Enter the password and tap on [OK].



2. Successfully verified.




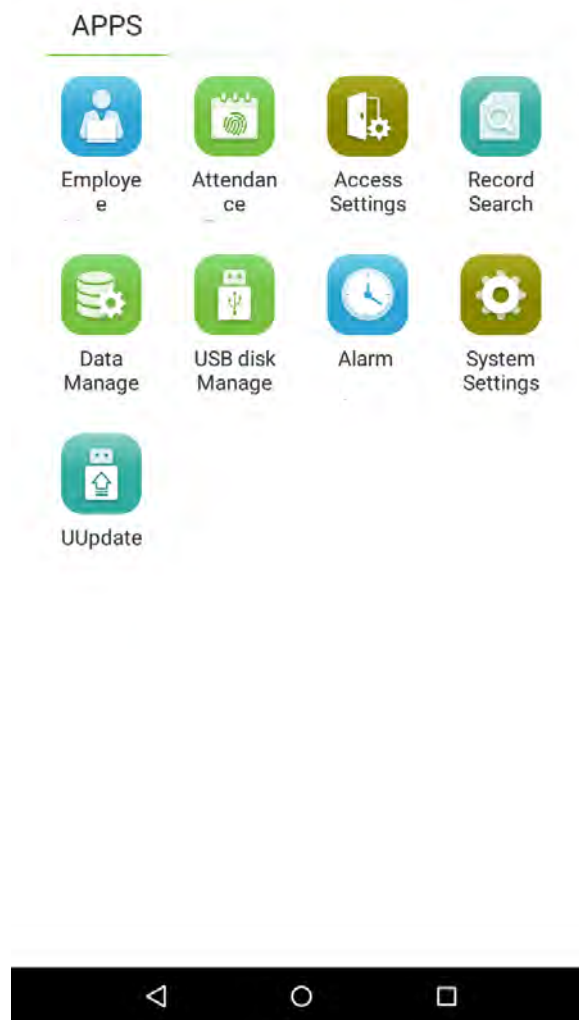
3. Verification is failed.




Note: A combined verification method can only be used when an employee has registered a comparison method and that method has been selected in the system. For further details, please see section “3.1 Add an Employee” below.

2. Main Menu

On the startup screen, press  to enter the main menu, as shown in the diagram below:




Menu Options	Function Description
Employee Management	Add, view and edit employee information.
Attendance Events	Records various clock-in or clock-out data based on different attendance status.
Access Settings	Achieve simple access control settings.
Record Search	Look up attendance log, view attendance photo and blacklist photo.
Data Management	Delete data from the device.
USB Disk Management	Use a USB drive to upload and download.
Alarm Management	Once an alarm has been set, the device will automatically play preselected ringtone when the designed time is reached. It will stop ringing after the alarm time elapsed.
System Settings	Set the network, date, time, attendance parameters, cloud server, Wiegand, display, sound settings, biometric parameters, automatic test, advanced settings of the device.

Note: If the device does not have a super administrator, any user can enter the menu by pressing the  key; after a super administrator has been set on the device, ID verification will be required to enter the menu. Once password verification is successful, users can enter the menu. To ensure the security of the device, we recommend registering an administrator the first time you use this device. For detailed operating instructions, please see section “3.1 Add an Employee”.

3. Employee Management

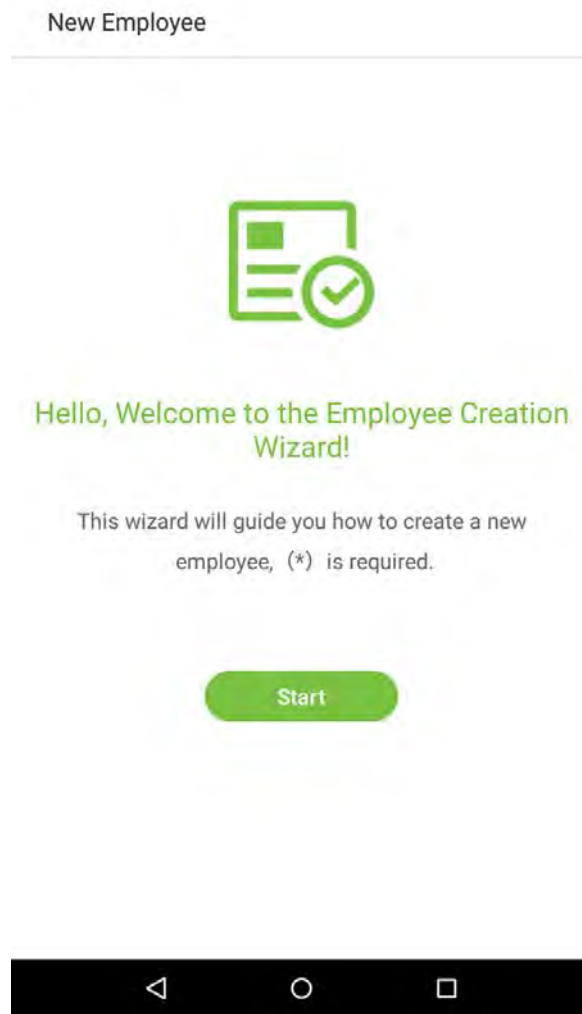
3.1 Add an Employee

Tap on [Employee Management] in the main menu:

1. Tap on  on the "Employee Management" interface to enter the employee creation wizard.



2. Tap on [Start] on the employee creation wizard.



3.1.1 Register Basic Employee Information

Enter the employee name in the [Employee Name] field, and the personnel ID in the [Employee ID] field:

New Employee

Employee Name *

Employee ID *

Back Next


?123 , . Done

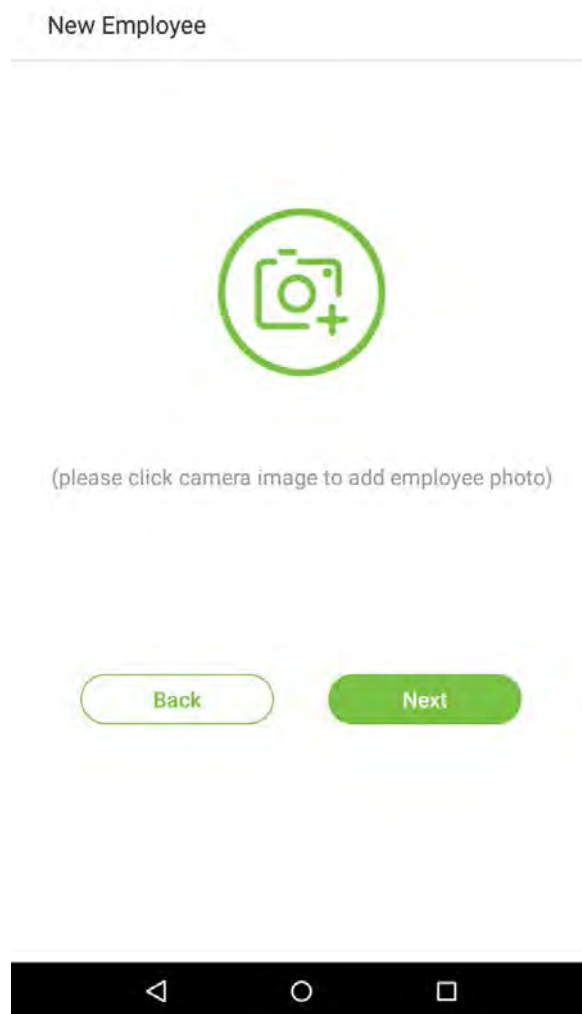
Notes:


1. The name refers to the employee's name. Its maximum length is 24 characters.
2. The system supports employee IDs from 1 to 9 digits by default. A maximum of 23 digits can be input. To increase the number of digits that can be input, please contact our pre-sale tech department.
3. Employee IDs can be changed the first time that they are used to log in to the system. After they have been used to log in, employee numbers can no longer be edited.
4. The message "This Employee ID is already in use!" indicates that the ID number you have input is already being used. Please input another ID number.

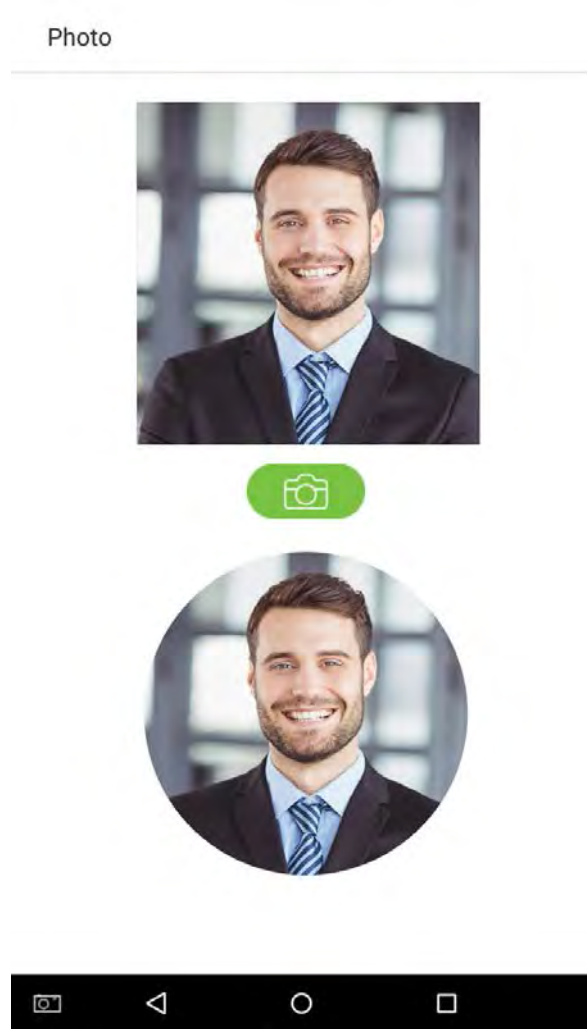
3.1.2 Register Employee Photo



After inputting the employee's basic information, tap on the right arrow to register an employee photo.

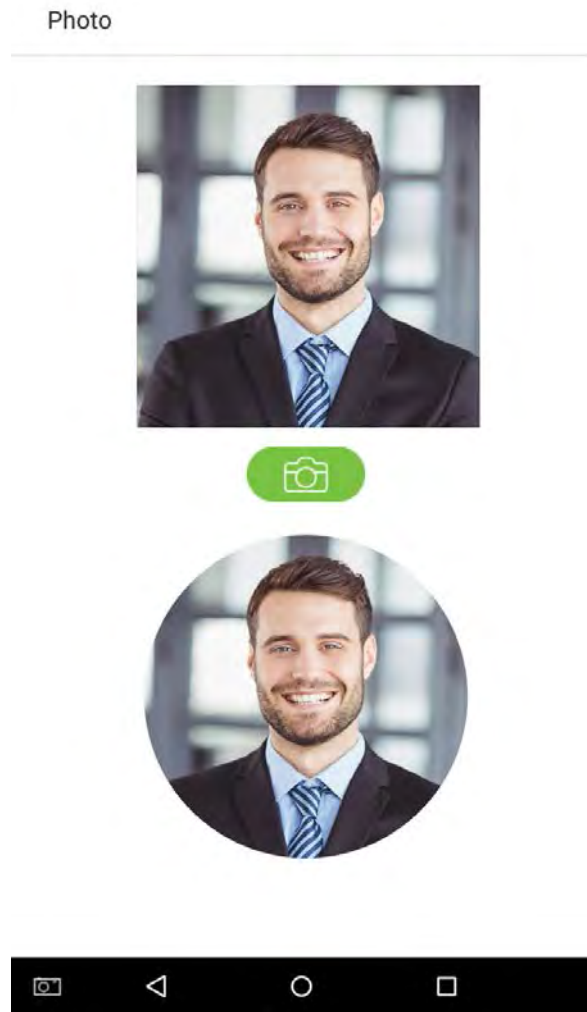
1. Tap on the  icon to enter the camera interface.



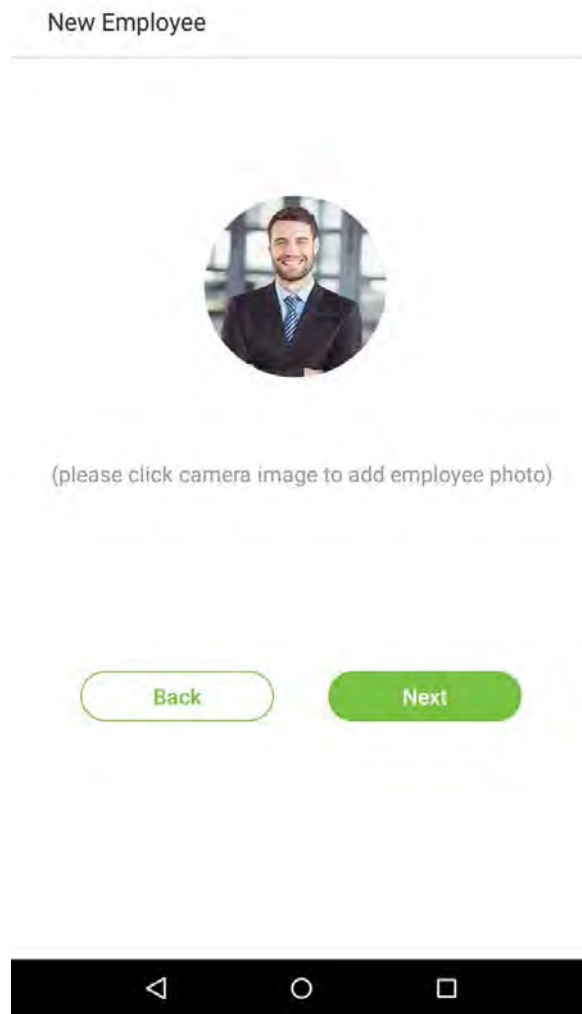
2. Employee should face the lens and then adjust the position. Tap on the  icon to take a photo.



3. Tap on the  icon on the bottom side, select a photo, then tap on the  icon to continue taking another photo.



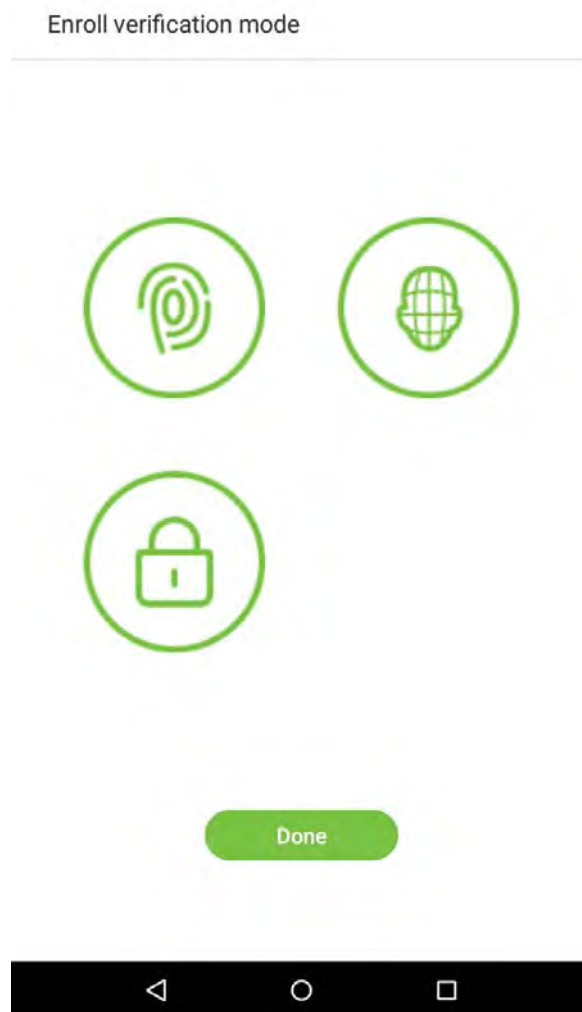
4. Tap on the rightwards arrow to complete adding the photo.




3.1.3 Registration Comparison Methods

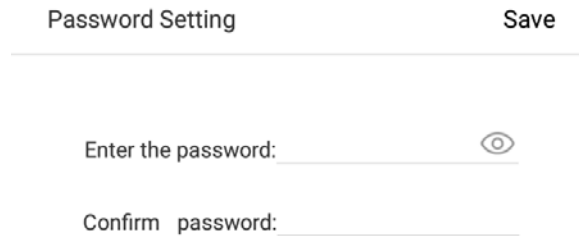
The registration comparison method is the method used to verify a login. This includes registering a password, fingerprint, or badge number. Select a registration that best suits your needs.

Click on the rightwards arrow on the interface shown after the message [Employee photo added successfully], then enter the verification method entry page:




- **Register passwords**

1. On the registration method entry interface, click on the  icon to enter the register password page. Enter a password in the [Enter the password] field, then re-enter the password in the [Confirm password] field. Tap on [Save] (Note: the employee password must be an 8-digit number).

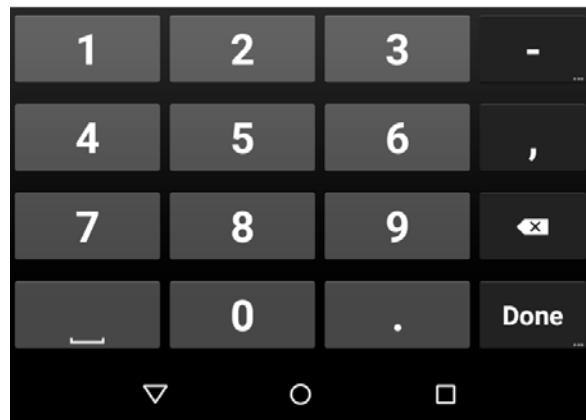


Tap on  to encrypt the password; tap on  to make the password visible, as shown below:

Password Setting Save

Enter the password: 

Confirm password:



2. If the password you input in both fields does not match, you have to re-enter the passwords.

Password Setting Save

Enter the password: 1 👁

Confirm password: 123

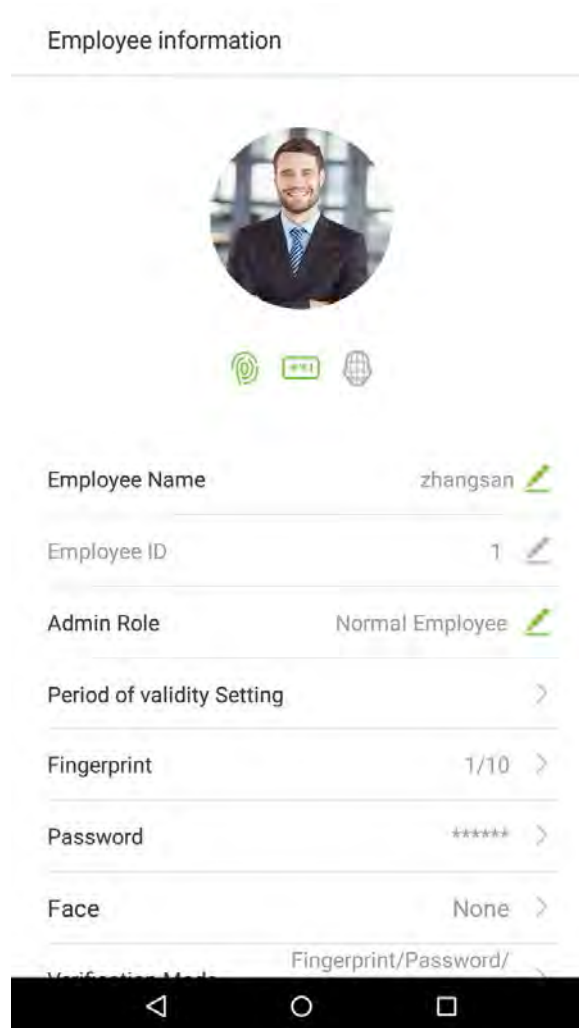
(Password did not match, please try again)

◀ ○ ◻

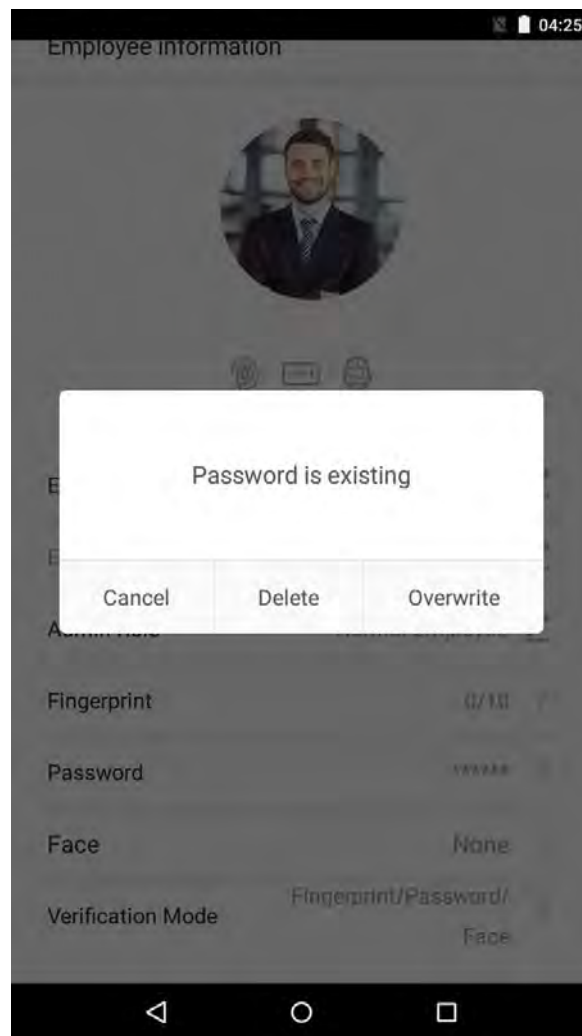
3. The password which has been registered can be deleted or covered.

- **Delete registered passwords**

On the employee management interface, tap an employee in the employee list to enter the employee information page, then tap on [Password].

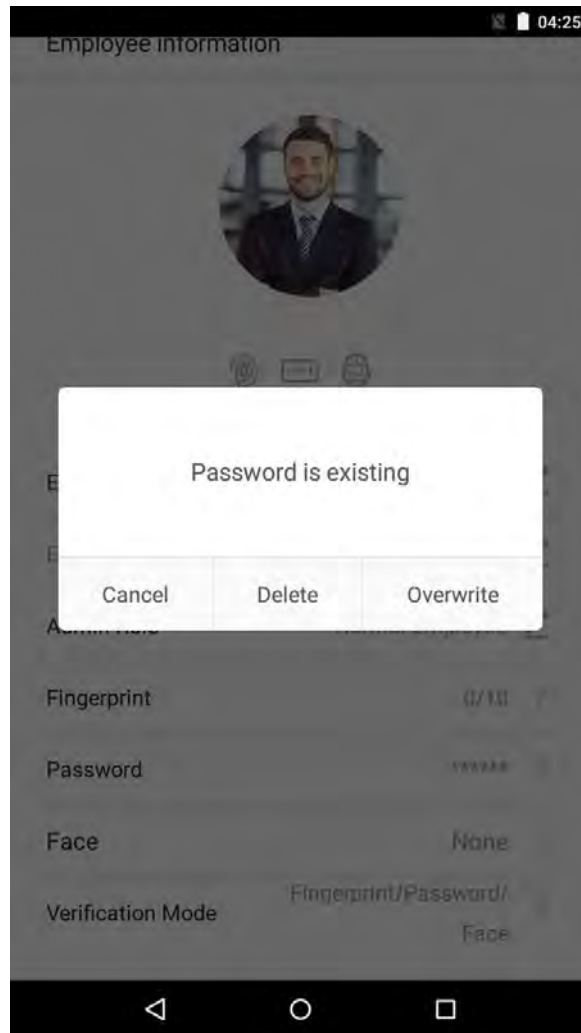


Press [Delete] in the dialog window that pops up.




- **Overwrite registered fingerprints**

Press [Overwrite] in the dialog window that pops up.

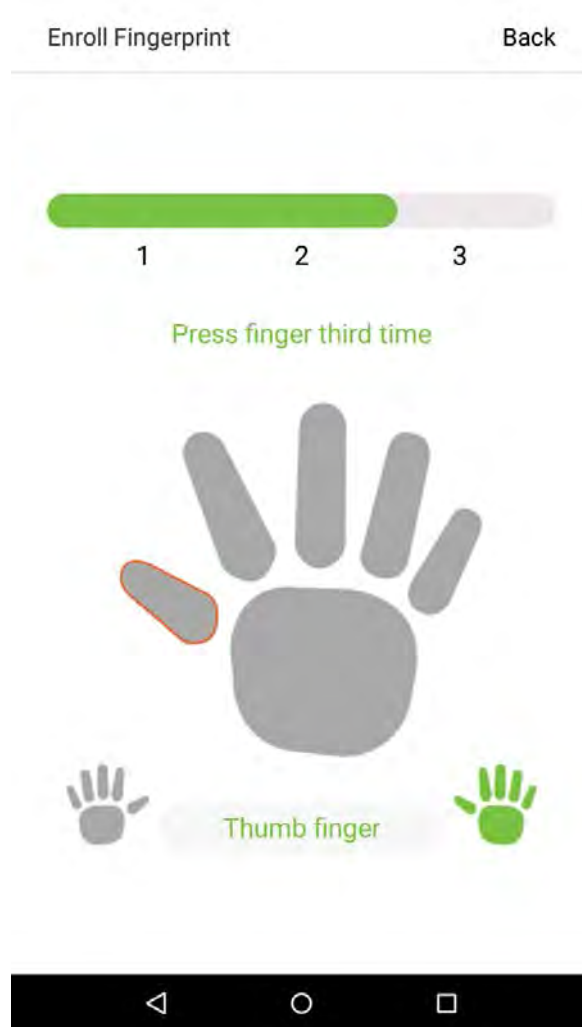


- **Register fingerprints**

1. On the registration method entry interface, tap on the  icon to enter the fingerprint registration page. Select the icon on the left or right side of the screen and then tap on the finger you would like to register a fingerprint for.



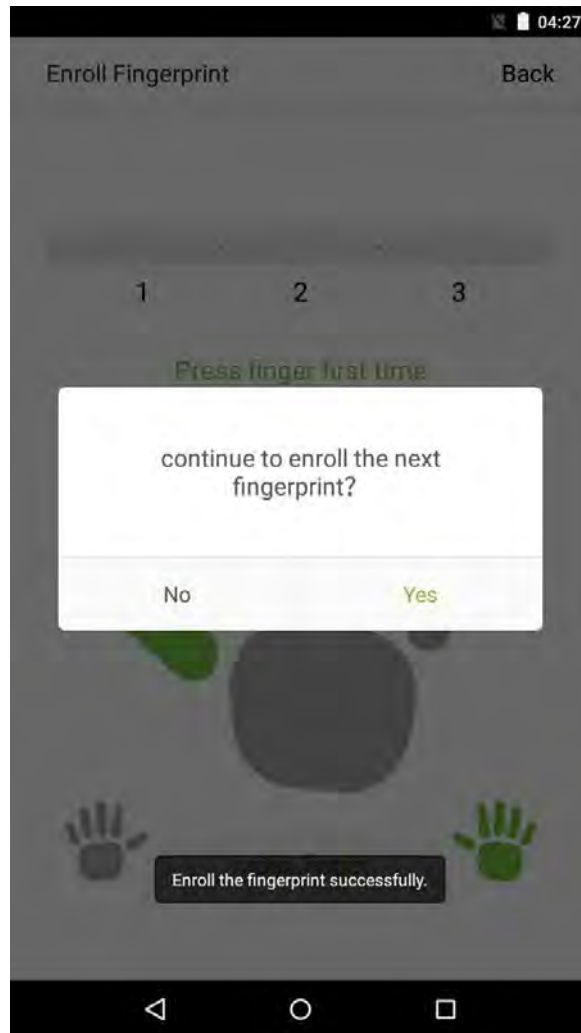
2. Press the same finger on the fingerprint reader three times. Green indicates that the fingerprint was input successfully.



If you press different fingers onto the fingerprint scanner during the 2nd and 3rd contacts, you will be prompted to "Please use the same finger".



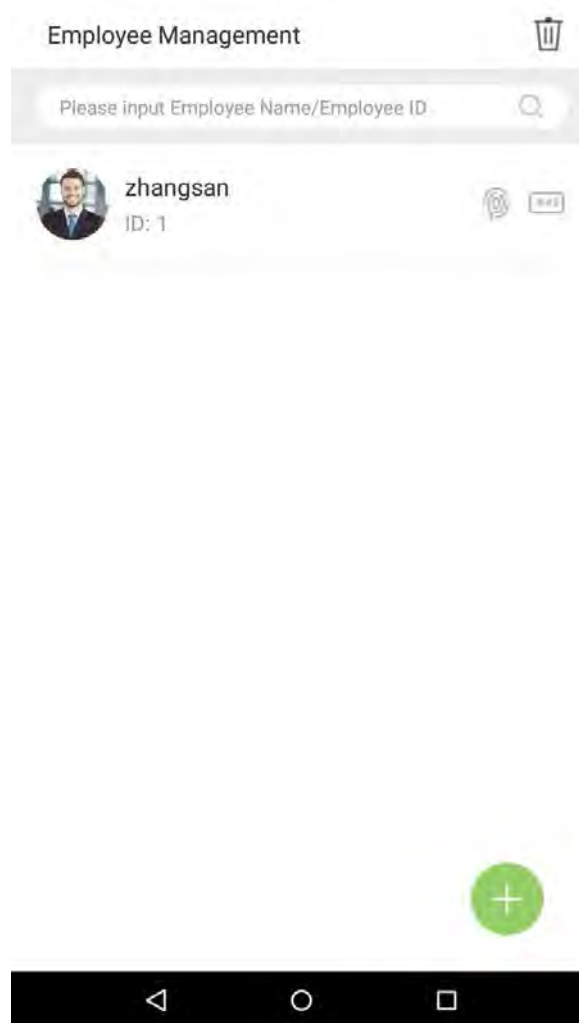
3. If fingerprint is successfully registered, a "Continue to enroll the next fingerprint?" dialog box will appear. Tap on [Yes] to record the next fingerprint, or [No] to return to the fingerprint registration interface.



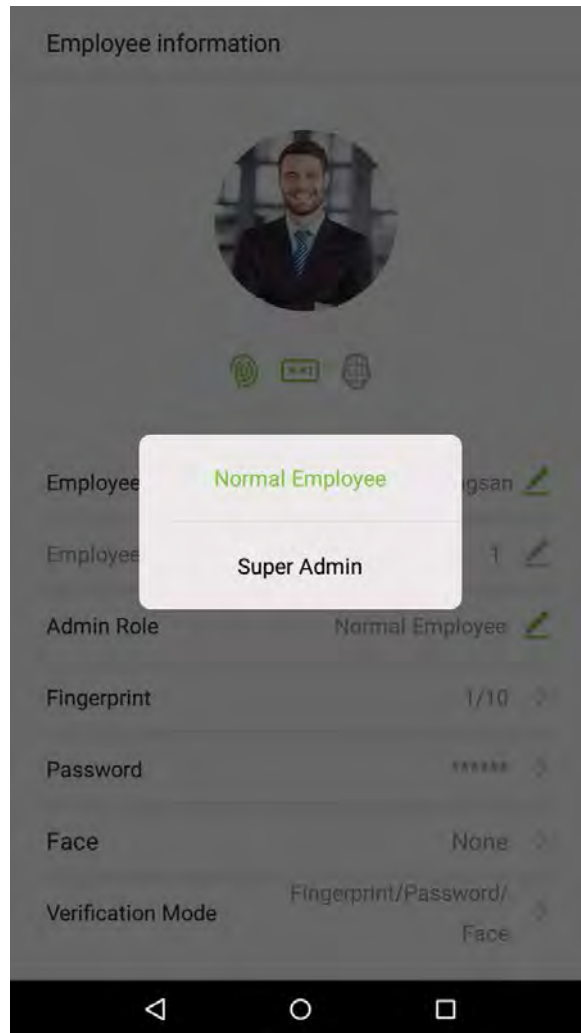
3.1.4 Permission Settings

Personnel who use this device have two types of permissions: general employee and super administrator. After a super administrator is registered on the device, general employees can only verify and compare their accounts using methods that have already been registered. Super administrator has the same privileges as general employees, but can also enter the main menu.

1. On the “Employee Management” interface, tap on an employee in the employee list to visit the employee’s information.



2. Once you have entered the "Employee information" interface, tap on the [Rights] column and select [General Employee] or [Super Administrator] in the window that appears.



Note: When a user is given super administrator privileges, entering the main menu will require ID verification. The verification process depends on the verification method that was used during user registration. See the description in section "1.5 Verification Methods".

3.1.5 Period of Validity Settings

Set a validity period for an employee's verification process. The employee will only be able to verify an account during this period, and will be regarded as an invalid employee after this period.

The validity period can be set as "Disable", "Time Period", "Times", "Time Period + Times".

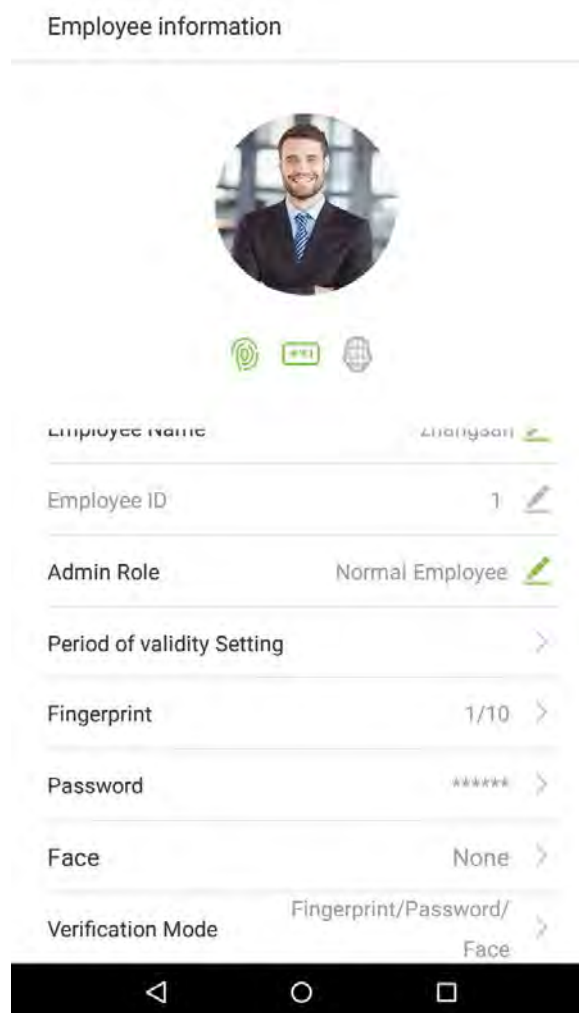
Disable: validity periods are not used.

Time Period: valid between the starting and ending date. This offers precision up to specific days. A day is the period from 00:00 until 23:59, after which the employee will be regarded as invalid.

Times: this amount of entries that an employee can make before their employee status loses validity. This number can be set within a range of 0-10000.

Time Period + Times: if the time limit or number of entries has been exceeded, the employee will become invalid.

1. On this "Employee information" interface, tap on [Period of validity Settings].



2. Check the box of the validity period mode you would like to set.

Employee information

Forbidden

Time Period

Times

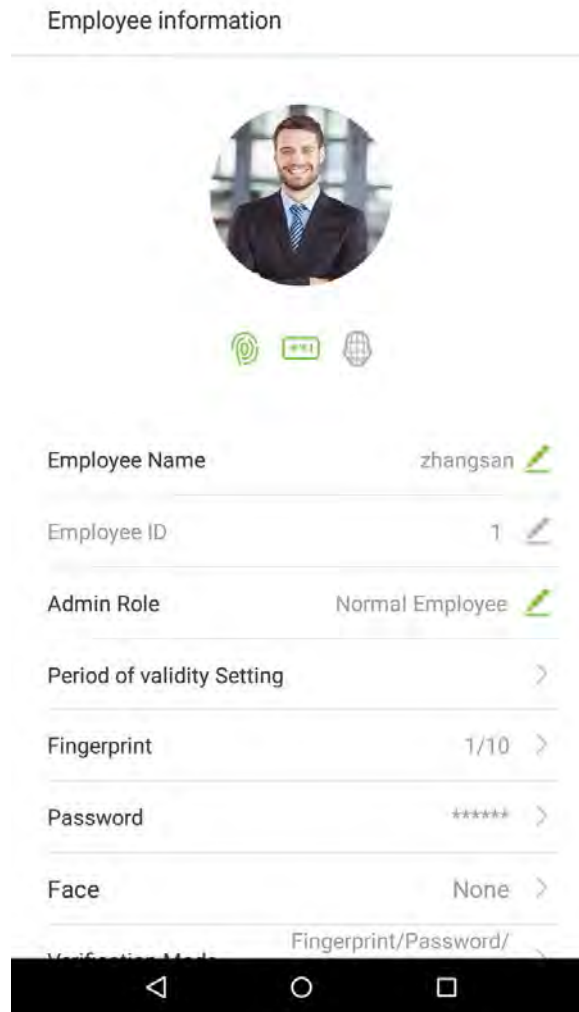
Time Period +Times



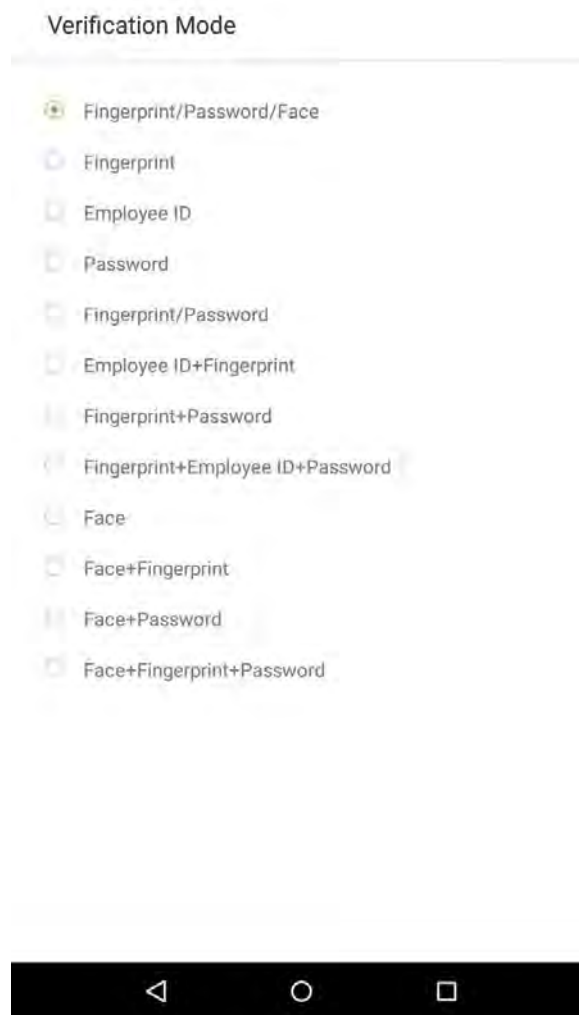
3.1.6 Verification Method Setup

To improve security, this device features combination verification methods, which can create a total of 15 verification methods. Enter an applicable verification method in this line.

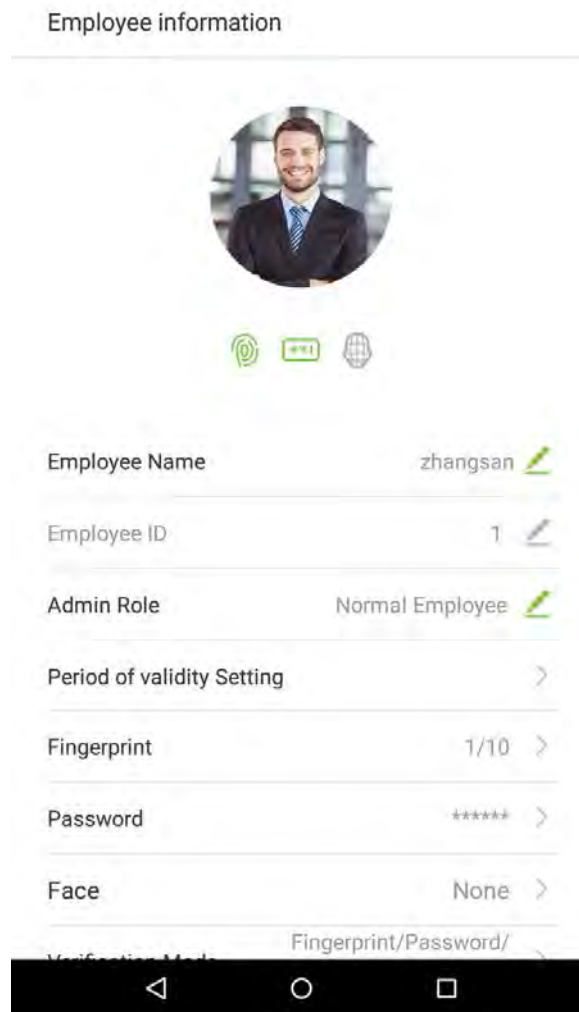
1. Tap on the [Verification Method] field on the “Employee information” interface.



2. Select [Verification Method], and then tap on [OK].



- Return to the “Employee information” interface and it will display the verification method you have chosen.

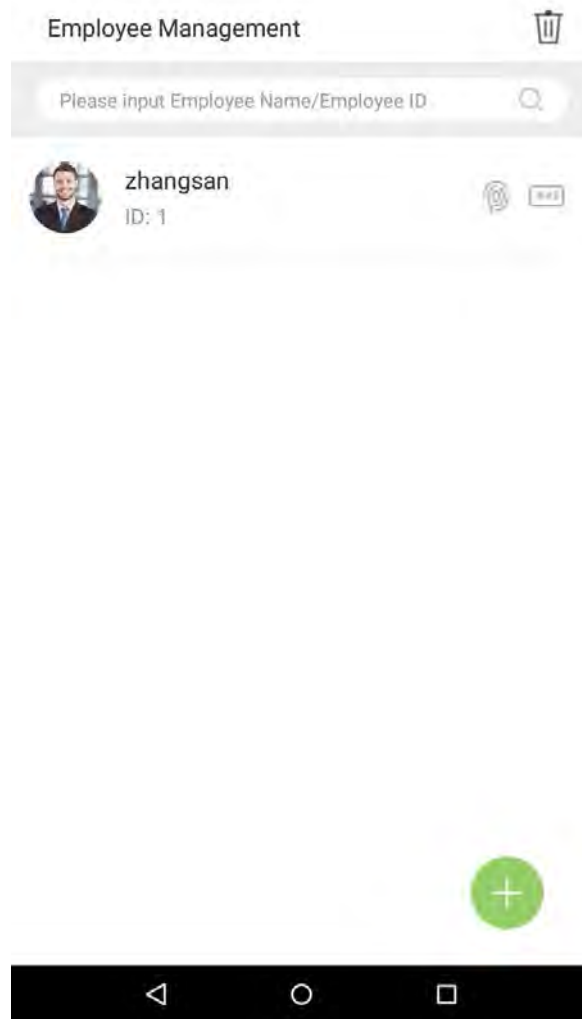


Notes:

- “/” means “or” and “+” means “and”.
- Support 12 different verification method combinations: personnel ID/ fingerprint/ password; fingerprint/ password/ face; fingerprint; employee ID; password; fingerprint/ password; employee ID/fingerprint; fingerprint/ password; fingerprint/ employee ID/ password; face; face fingerprint; face/ password; face/ fingerprint/ password.
- Combined verification requires employees to register the information needed to complete verification. Otherwise, employees may be unable to complete the verification process. For instance, when employee A registers with his/her fingerprints and the system's verification method is set as “Fingerprint + Card”, the employee will not be able to complete the verification process.

3.2 Searching for an Employee

1. Tap on the search bar located on the "Employee Management" interface and enter a search query (Note: search for users based on their personnel IDs, surnames, or given names).

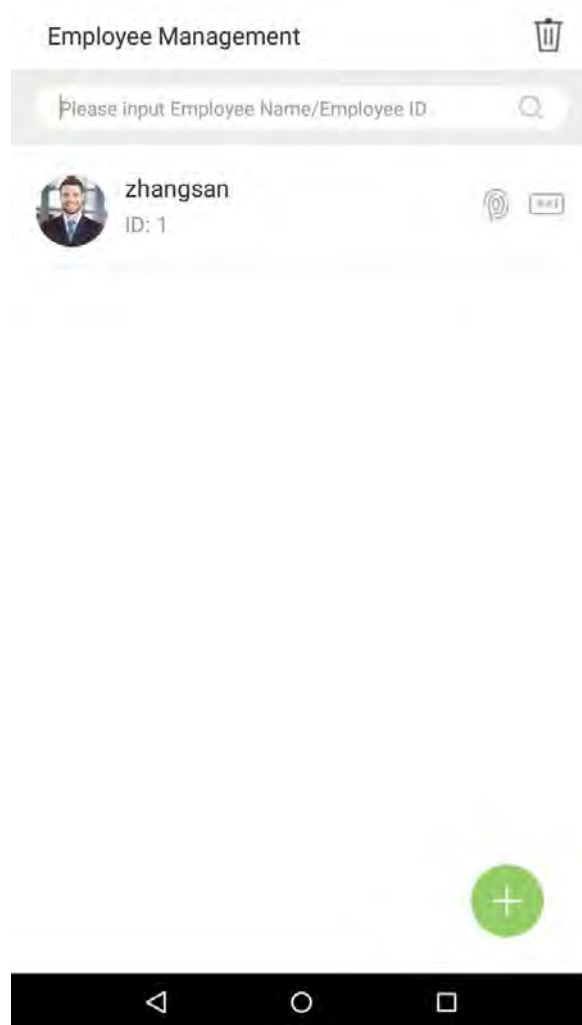


2. Automatically finds employees with information that is relevant to the search query.

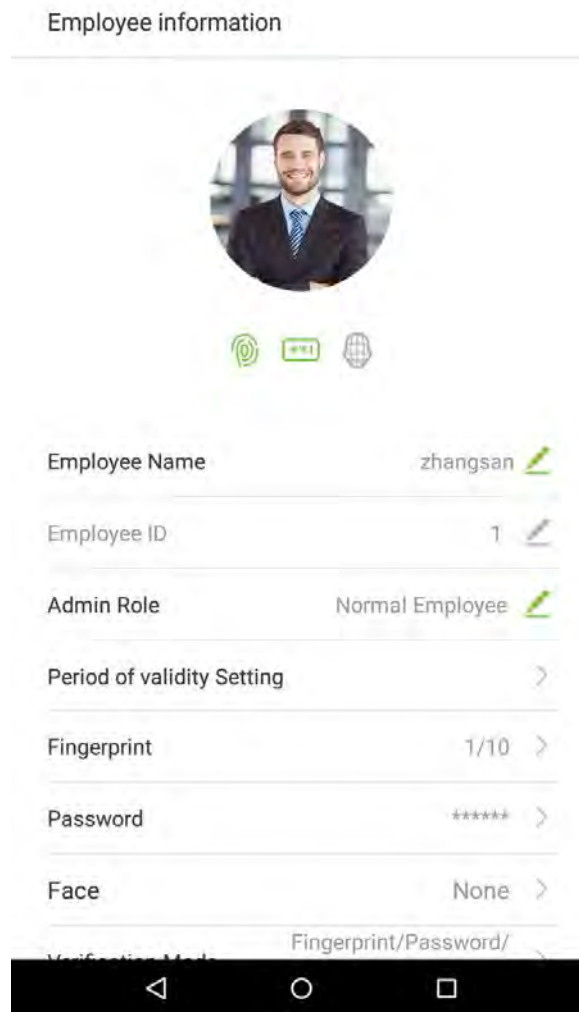


3.3 Edit an Employee

1. Select an employee on the employee list.




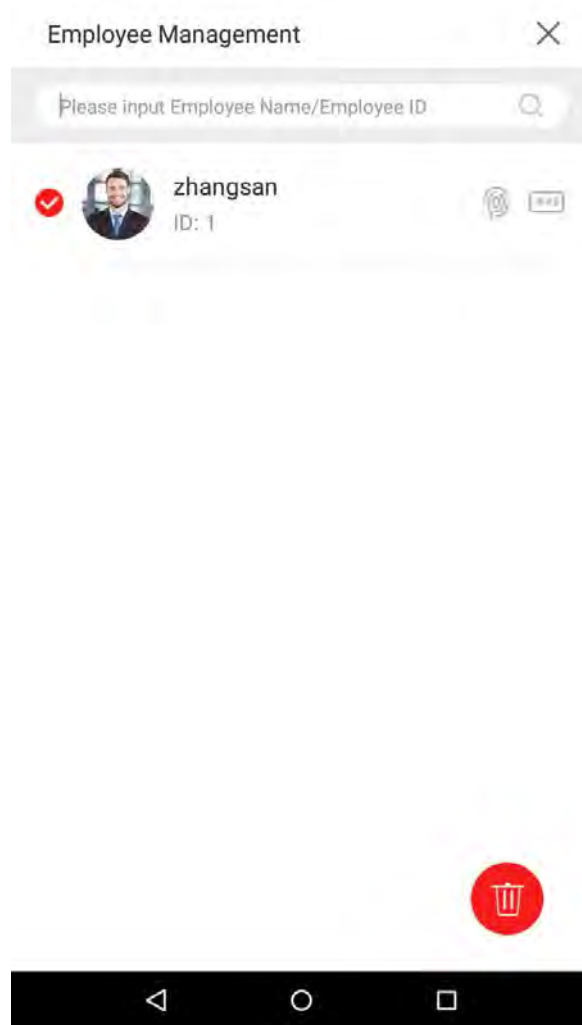
2. Enter the interface where users may edit the employee information.




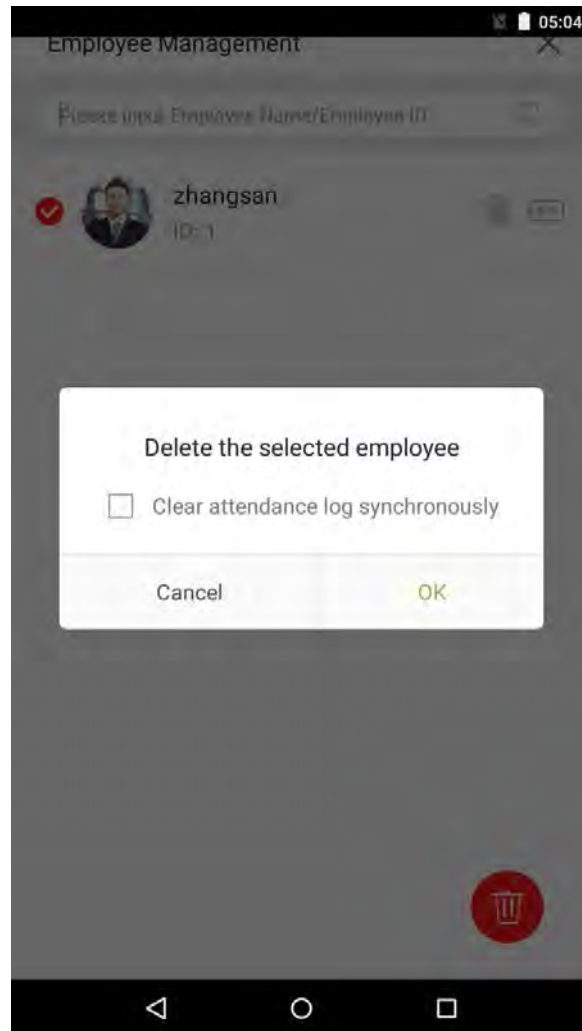
Note: Unless an employee ID cannot be modified, other operations are similar to adding a new employee and will not be discussed here. For further information, please see section “3.1 Add an Employee”.

3.4 Delete Employee

1. On the "Employee Management" interface, tap on the  button in the upper right corner.



2. Select the employee who you would like to delete, tap on the  button in the lower right corner and a window will pop up. Decide whether or not to check the box next to [Clear attendance log synchronously], tap on [OK] (this option can be checked or left un-checked based on your requirements).



3. The employee now has been deleted and will no longer appear.



Note: If [Delete Employee] is selected, all of this employee's related information will be cleared.

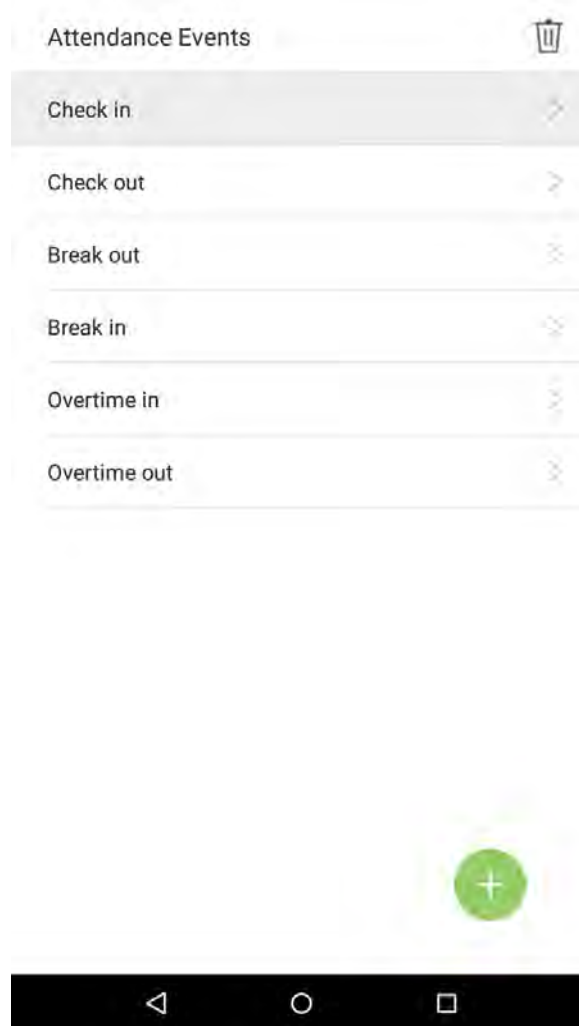
4. Attendance Events

Attendance events are used to record clock-in/out status. There are 6 default attendance statuses, including clock in, clock out, break out, break in, overtime in, overtime out. The 6 default statuses cannot be deleted or modified.

4.1 Add Attendance Events

Tap on [Attendance Events] in the main menu:

1. On the "Attendance Events" interface, tap on  to enter the "Attendance Event" interface.



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

Add Attendance Event



Hello, welcome to attendance event
creation wizard

This wizard will guide you how to create attendance
event,(*) is required

Start



3. Enter the [Name] and [Status Value] of the new attendance event. Tap on the right arrow (note: maximum length of the name is 24 characters; status values must be unique and cannot be duplicated. The value ranges from 6 to250.)

Add Attendance Event

Please input name *

Please input the status value(6 ~ 250) *

Back Next


If the input status value is a duplicate or exceeds the permitted range, the following message will appear:

Add Attendance Event

Please input name *

Please input the status value(6 ~ 250) *

Back Next



4. Successfully created.

Add Attendance Event



Hello, ATT event was created
succesfully!

After done, please choose to continue to add or click
complete the wizard

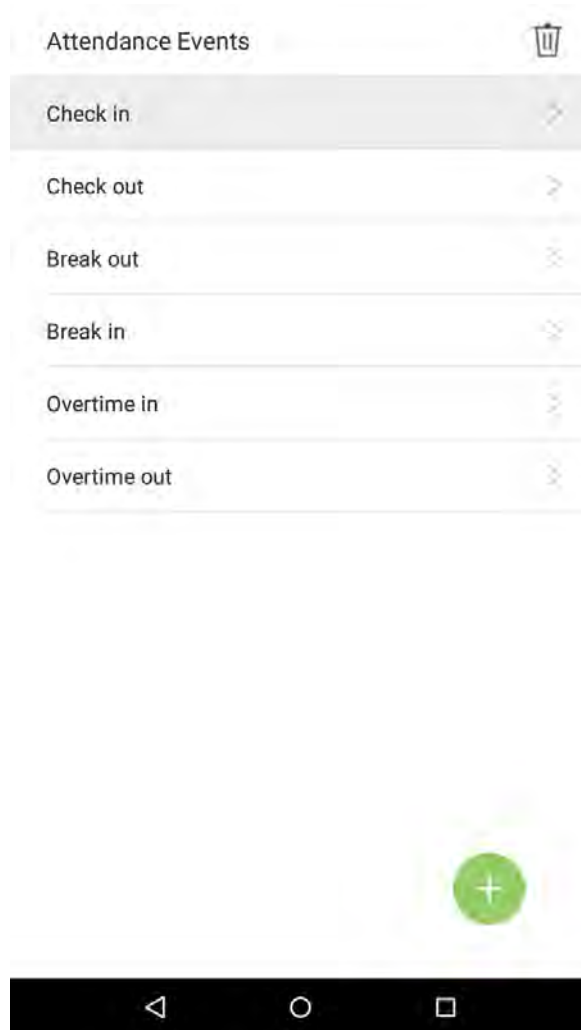
Continue To Add

Done

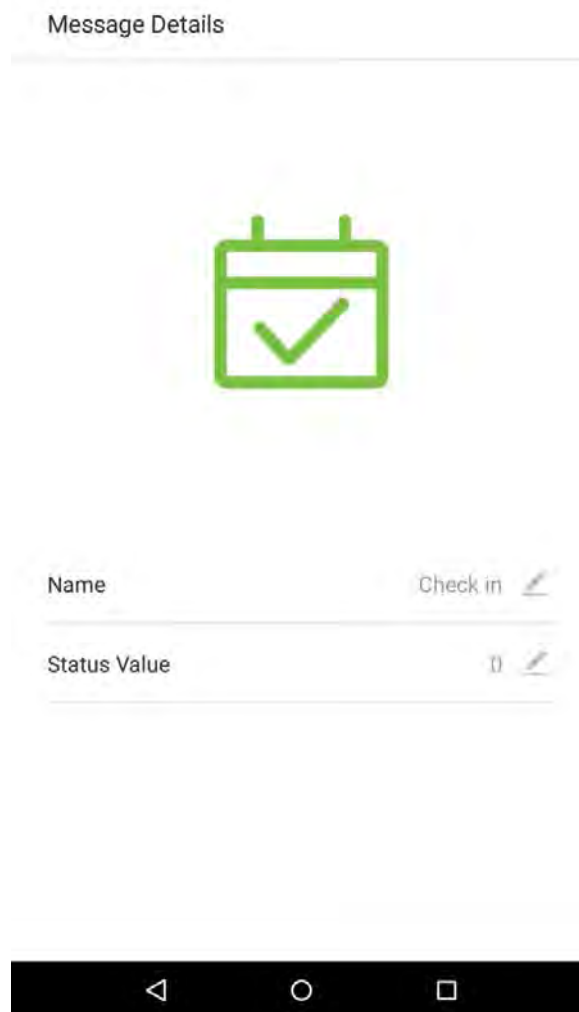


4.2 Edit Attendance Events

1. Select an employee attendance event.




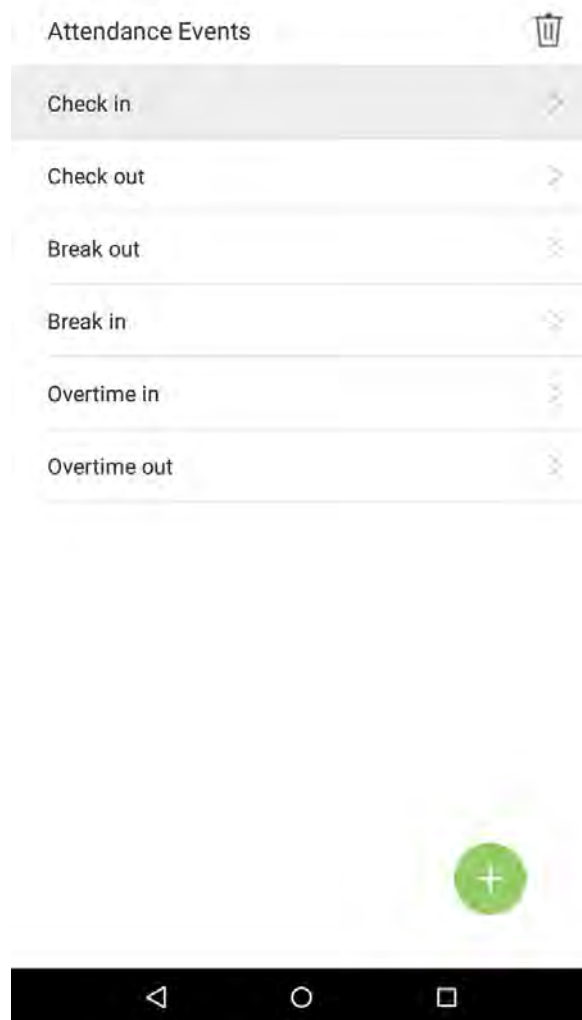
2. Tap on [Name] or [Status Value] to edit (note: the first 6 attendance events cannot be edited; status values must be unique and cannot be duplicated)



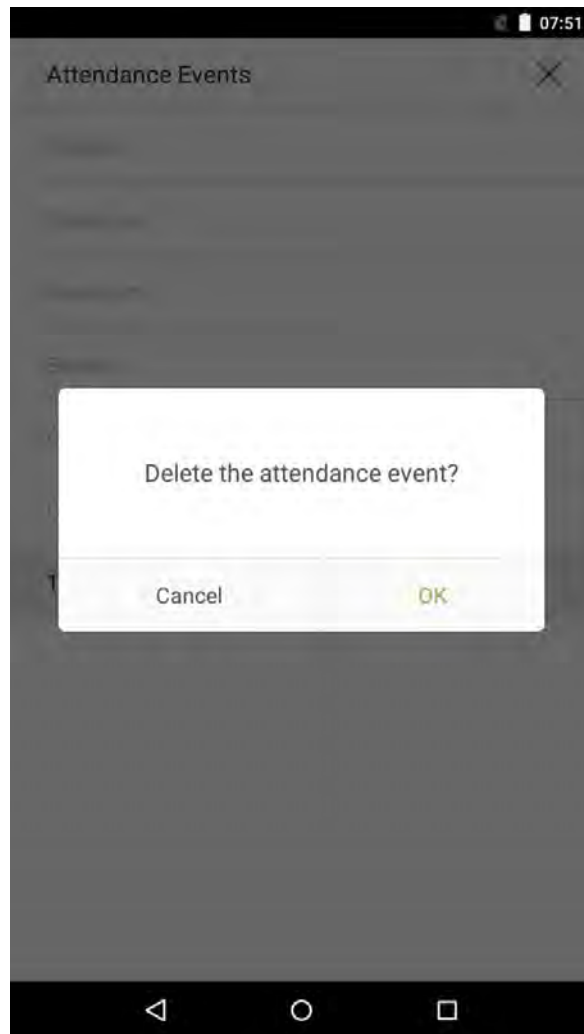
This operation is similar to adding a new event and will not be described here. For further information, see section "4.1 Add Attendance Events".

4.3 Delete Attendance Events

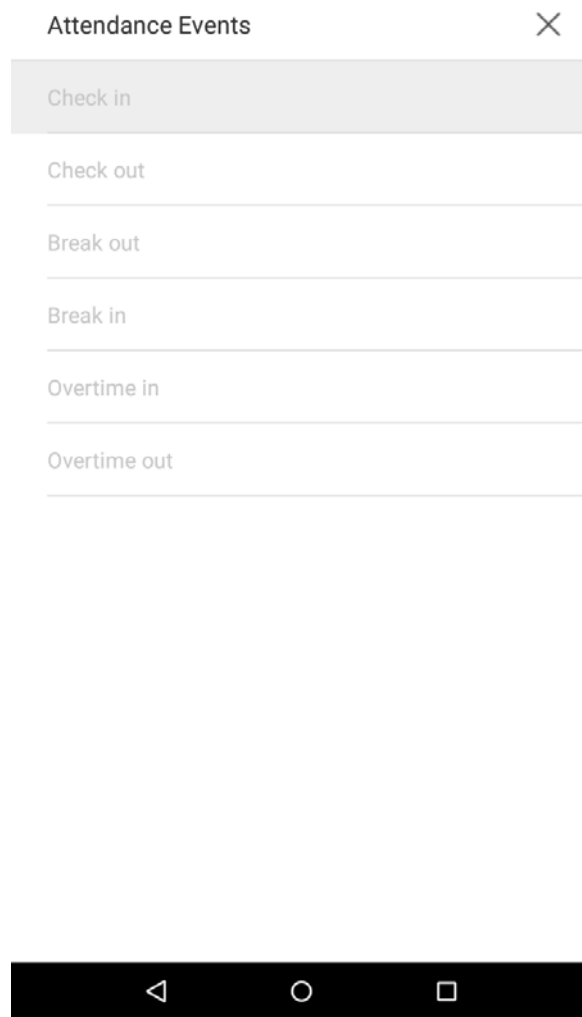
1. Select an attendance event and tap on the  icon in the upper right corner (Note: the first 6 events cannot be deleted, so the delete button will not appear).



2. A window will appear. Tap on [OK].

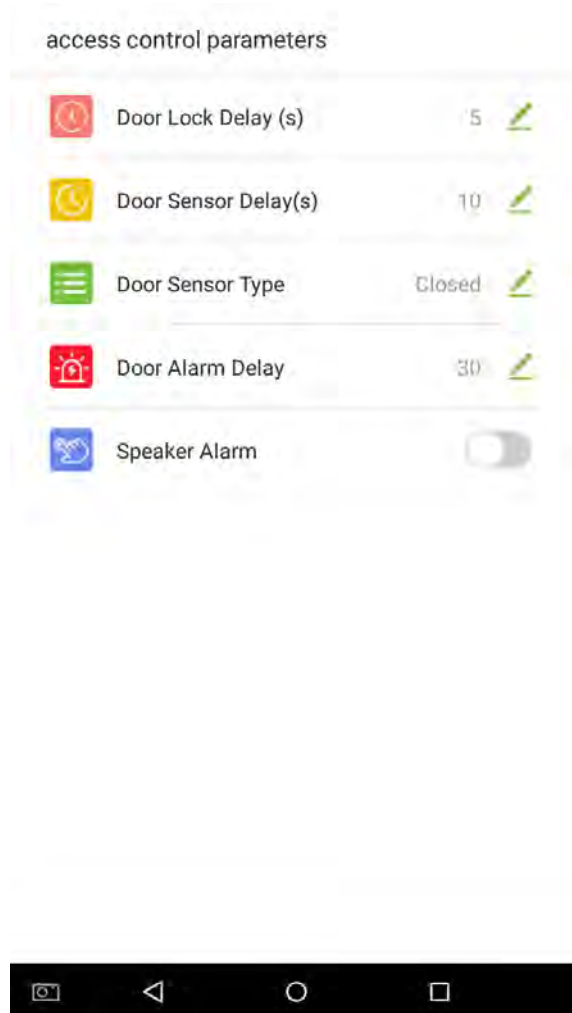


3. The event is now deleted and will not appear on the list.



5. Access Control Settings

The access management allows users to set access parameters.
On the main menu, tap on [Access Settings].



Menu Options	Function Description
Door Lock Delay	When the door opens, the lock begins to count down. When the time is over, the lock will close.
Door Sensor Delay	When the door opens, the door delay timer starts counting down. When the countdown is completed, the system will send an alarm signal from the local, then the door sensor delay timer will continue to be effective.
Type of Door Sensor	There are different types of door sensors. Subject to different locations, the status value of the door sensor is different; the value of the magnetic door in the "always open" mode is the opposite of that in the "always close" mode .
Door Alarm Delay	When the door delay ends and the status of the door is not "closed", the door alarm delay timer will start counting down. When the countdown is completed and the status is still not "closed", an external alarm signal will be transmitted and output to relay.
Alarm Switch From Local	To transmit a sound alarm signal from the local, then send an unpack alarm signal. When the door is closed, the system will cancel the alarm from the local. After the signal is successfully confirmed, the alarm will be cancelled from the local.

Note: Registered employees need to fulfil certain conditions before unlocking the system, which means that the current unlock time should be within the effective time period, or the door cannot be opened.

6. Record Search

Employee attendance records will be saved in the device, making it easier to find employees' attendance records. Users can search for ATT Logs, ATT Photos, and Blacklist Photos. Searches support retrieval queries, date queries, or a combination of the two.

6.1 Search for Attendance Records

1. Tap on [Record Search] in the main menu, then the following interface of work record history will pop up.




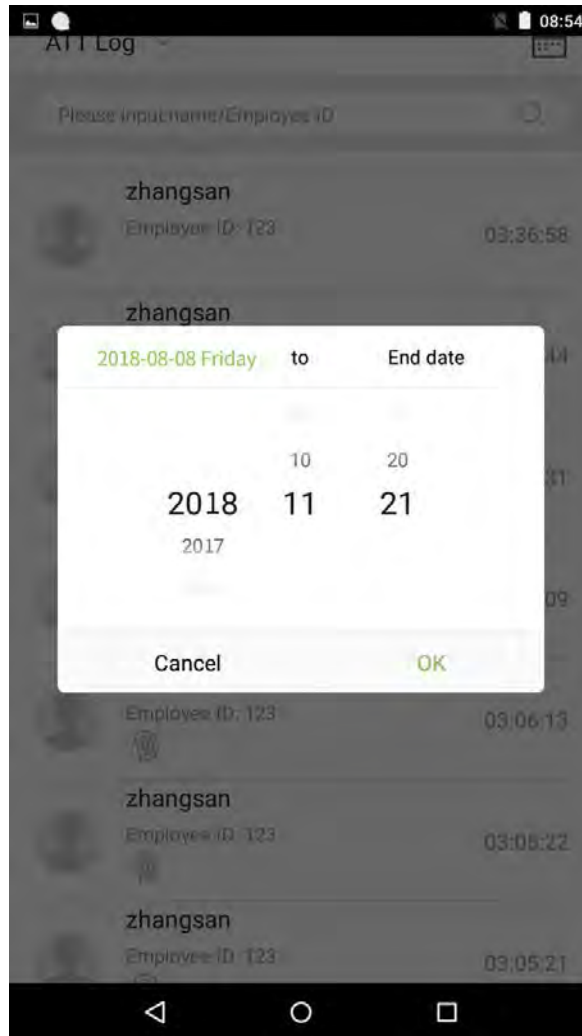
2. Enter information such as the employee ID, first or last name of an employee in the search bar.



3. Automatically finds the employees with information that is relevant to the search query.



4. Tap on the  button to access the following window where you can select the [Starting Date] and [Ending Date]. Tap on [OK].



5. Show search results.



6.2 Search for Attendance Photos

The query operation supports search bar queries, date queries, and combined search bar + date queries.

1. Tap on the drop-down button in attendance logs and select [ATT Photos].




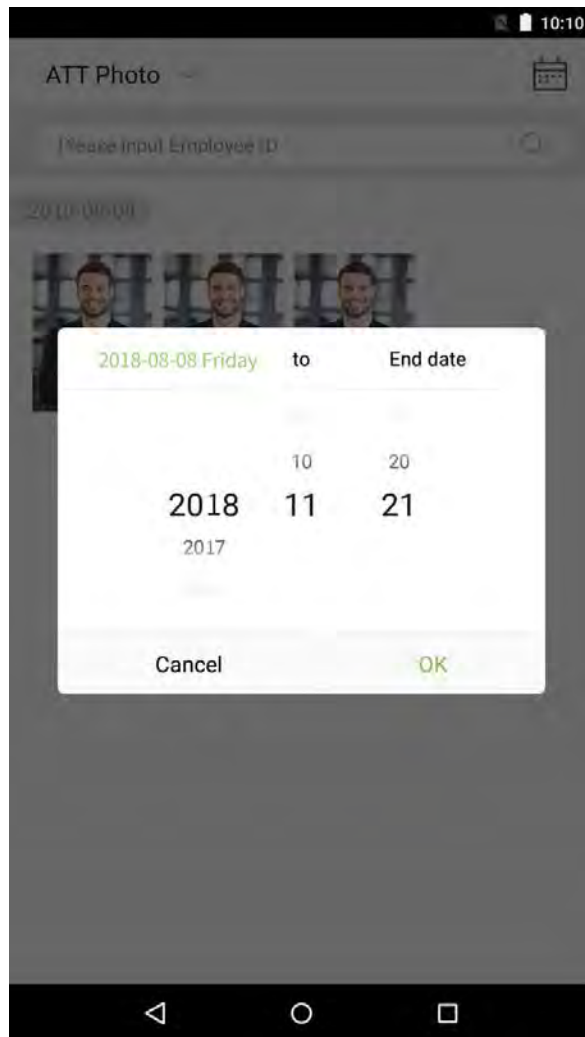
2. Enter the ATT photos interface.



3. Enter search information interface, namely, the personnel ID, in the search bar, the system the system will then automatically search for the employee with the corresponding personnel ID.



4. Tap on  and a window will pop up. Select the [Starting Date] and [Ending Date].

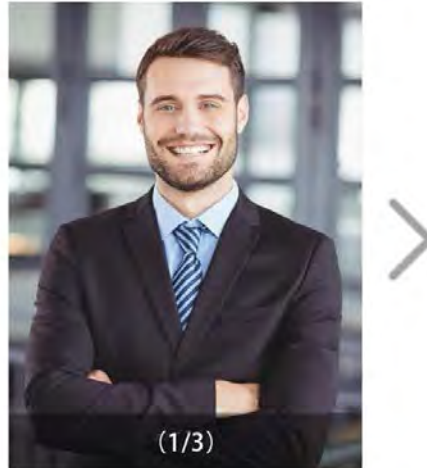


5. Show search results.



6. Tap on an attendance photo to view that photo's details.

ATT Photo



2018-08-08 10:07:27 Employee ID: 890



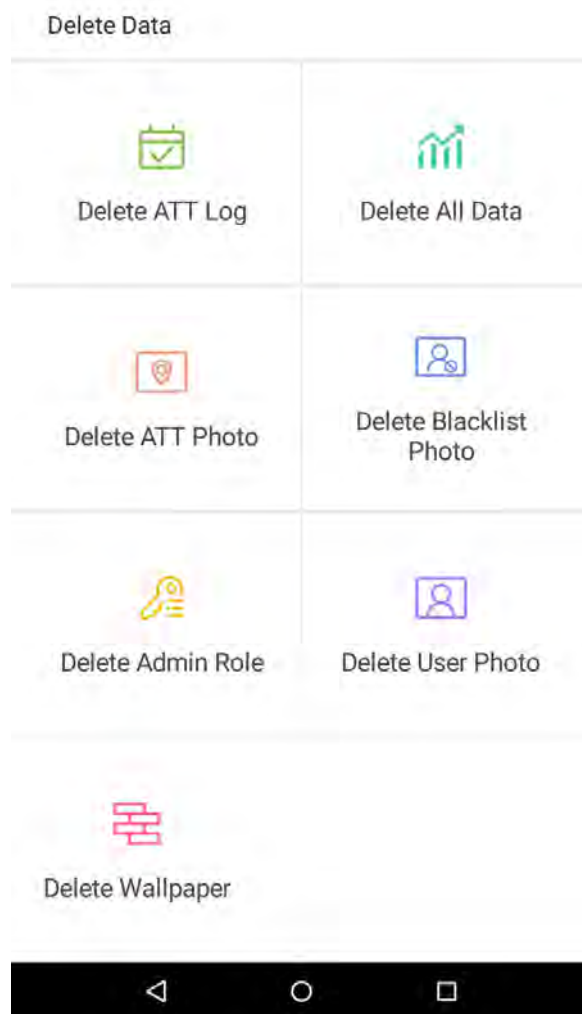
6.3 Search for Blacklist Photos

To conduct a blacklist photo query, follow the same steps required to complete an attendance photo query. For exact operation details, see section **"6.2 Search for Attendance Photos"**.

7. Data Management

Manage the device's data, including Delete an ATT Log, Delete an ATT Photo, Delete a Blacklist Photo, Delete All Data, Delete Admin Role, Delete a User Photo, and Delete Wallpaper.

In the main menu, tap on [Data Management].

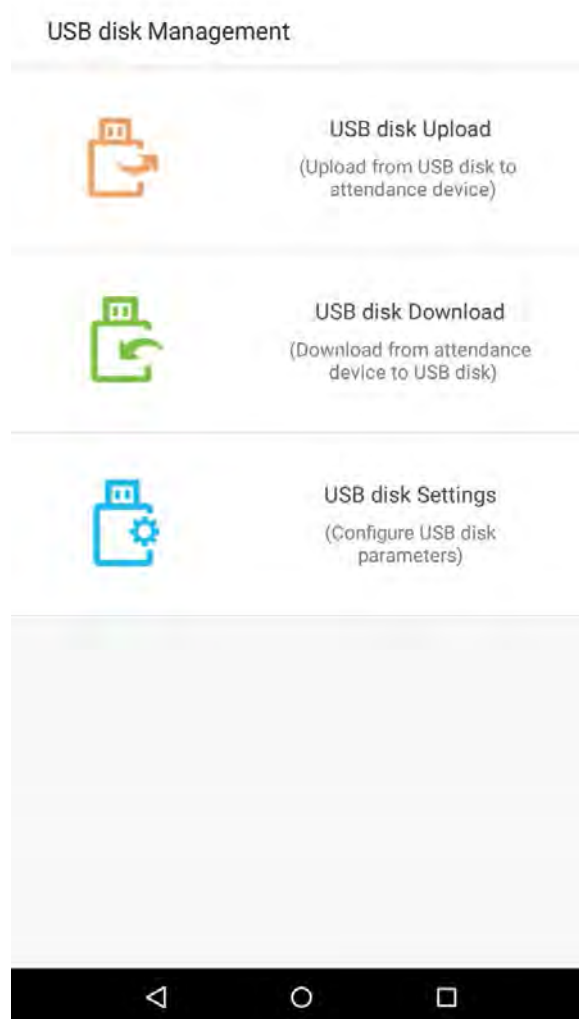


Menu Options	Function Description
Delete an ATT Log	1. Delete all; 2. delete invalid user accounts (deleting the account will not delete the attendance log); 3. delete the attendance logs within a specified time range.
Delete an ATT Photo	1. Delete all; 2. delete invalid user accounts; 3. delete the attendance photos within a specified time range.
Delete Blacklist Photos	1. Delete all (including attendance records and the photos of the employee in blacklist); 2. delete the blacklist photos, together with the attendance records, within a specified time range.
Delete All Data	Delete business data stored in the terminal device, including attendance logs, attendance pictures, blacklist pictures, fingerprint/ facial biometric data, privileges of the super admin, employee photos, wallpaper, employee data, work codes and access control data.
Delete Admin Role	Turn the super administrator into a general employee.
Delete a User Photo	Delete all employee photos.
Delete Wallpaper	Delete all wallpapers stored in the device.

8. USB Disk Management

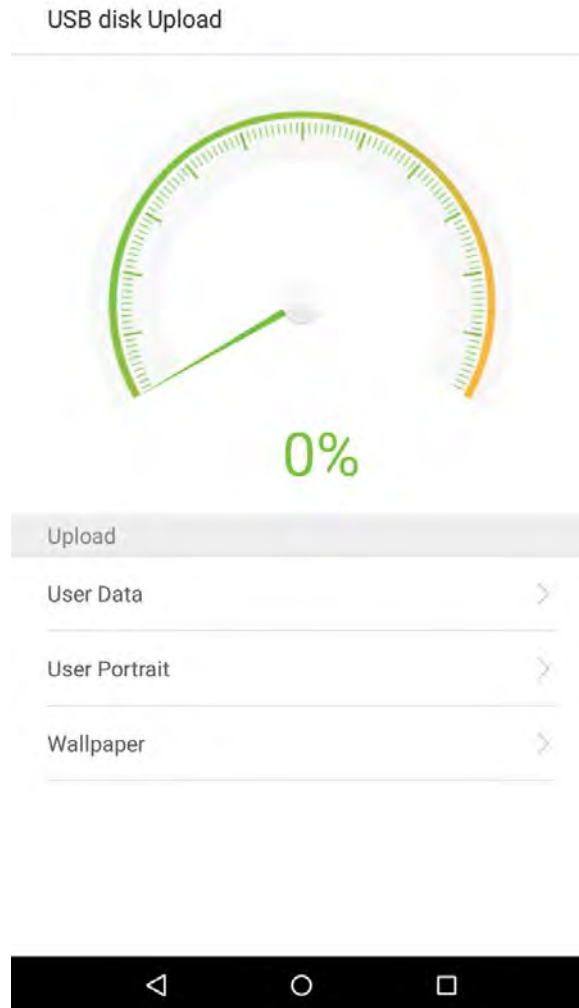
Use a USB drive to import the system's employee information, fingerprint template, or attendance data into the accompanying attendance software for processing, or import employee information and fingerprints onto another fingerprint device for use. Before uploading or downloading using a USB drive, plug the USB drive into the device's USB port, then conduct each operation.

On the USB disk management interface, tap on the [USB disk upload] field:



8.1 Upload to USB Drive

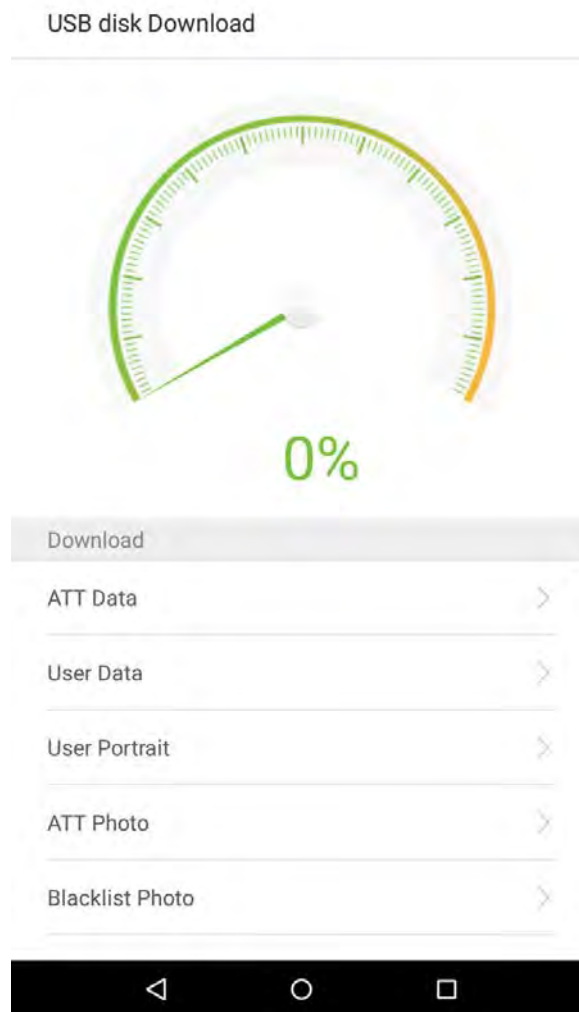
On the USB disk management interface, tap on the [USB disk upload] field:



Menu Options	Function Description
Upload Employee Data	Upload employee information, fingerprint templates, facial templates from a USB drive to the device.
Upload Employee Photos	Upload a JPG photo that is named with a personnel ID from a USB drive to the device. Each photo may not exceed 250k, otherwise the system will remind the user that the uploading is failed.
Upload Work Code	Upload work codes from a USB drive to the device.
Upload Wallpapers	Upload all JPG pictures from a USB drive to the device.

8.2 Download to a USB Drive

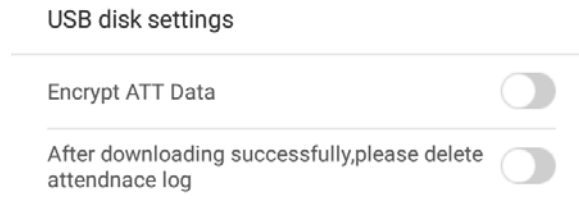
On the USB disk management interface, tap on the [USB Disk Upload] field.



Menu Options	Function Description
Download ATT Data	Save the attendance data within the specified time range (all, this week, last week, this month, user-defined) onto the USB drive. If there is no data, there will be no prompt.
Download Employee Data	Download all the user information, fingerprint and facial biometric data and stored them in the USB drive.
Download Employee Photos	Copy JPG pictures to the USB.
Download ATT Photos	Copy attendance pictures stored in the device to the USB drive. The format of the picture is JPG.
Download Blacklist Photos	Download the blacklist photos within the specified time range (all, the current week, last week, the current month, last month, user-defined).

8.3 USB Disk Settings

On the USB drive management interface, tap on the [Settings] field:




Menu Options	Function Description
Encrypt ATT Data	Encrypt employee attendance logs while downloading or uploading.
Delete Attendance Logs after Successfully Downloading	After attendance logs have been successfully copied to the USB drive, the logs stored on the device will be deleted.

9. Alarm Management

Employees can set an alarm time according to their needs. Once an alarm has been set, the device will automatically begin playing a preselected ringtone when the designated time is reached. It will stop ringing after the alarm time has elapsed.

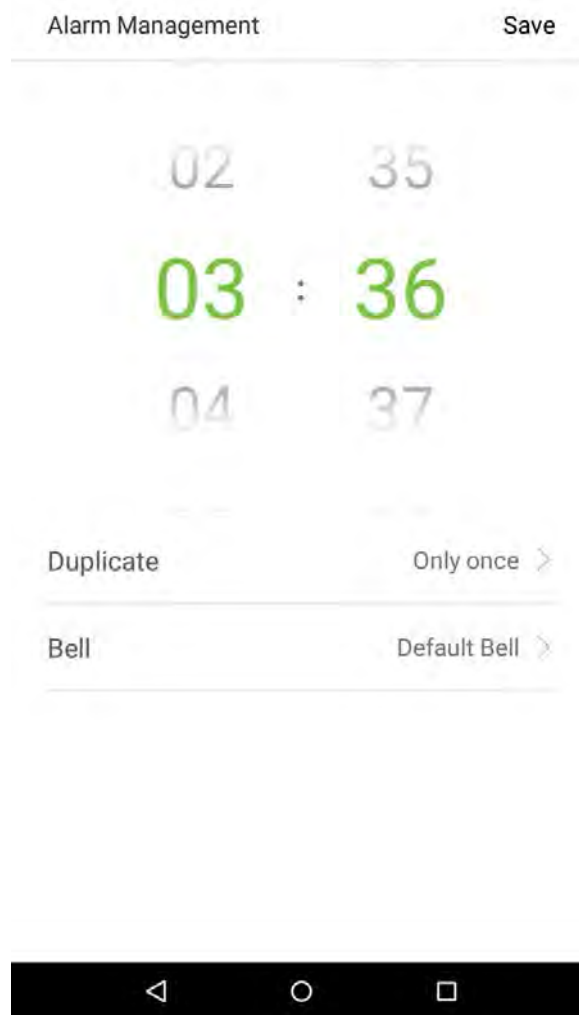
9.1 Add Alarms

In the main menu, tap on [Alarm Management]:

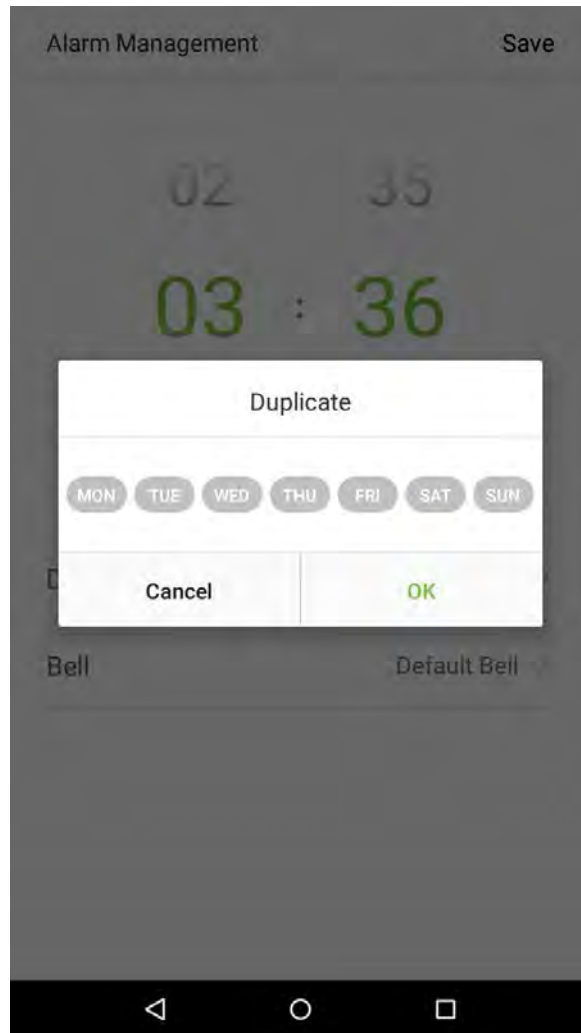
1. On the alarm management interface, tap on  to enter the "Add Alarms" page.



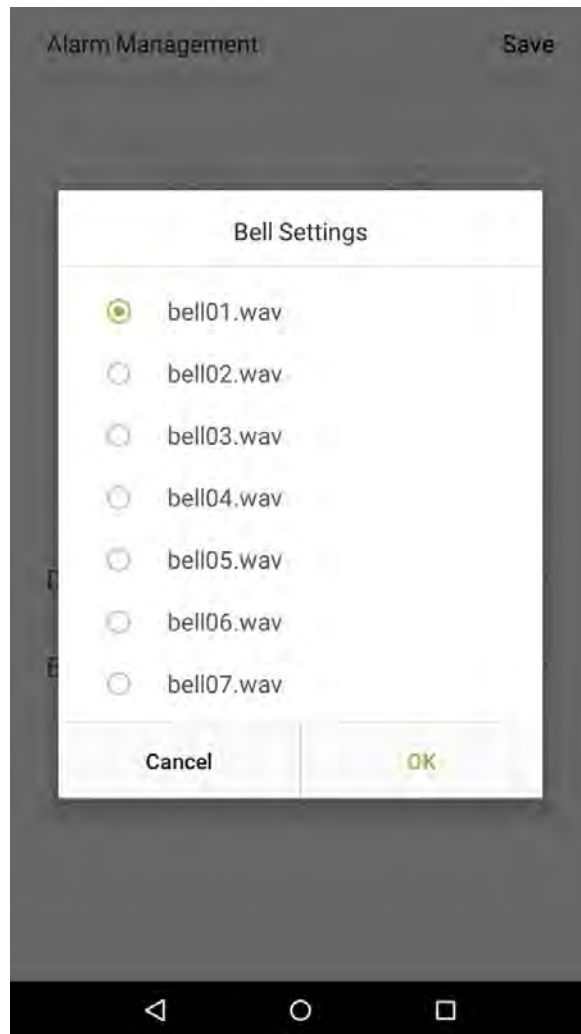
2. Set Time-- select [AM] or [PM], select [Hour] and [Minute].



3. Duplicate-- the default is set to "Only once". To copy the settings, tap on the [Duplicate] button and a window will pop up. Select the date and tap on [OK].



4. Tap on the [Bell] button and a window will pop up. Select a ringtone and tap on [OK].



5. Tap on the [Save] key and the alarm will be successfully added. The alarm will be enabled by default.



6. Enable [Alarm Switch] to change the alarm's status. Green indicates that the alarm is on, while gray indicates that the alarm is off.

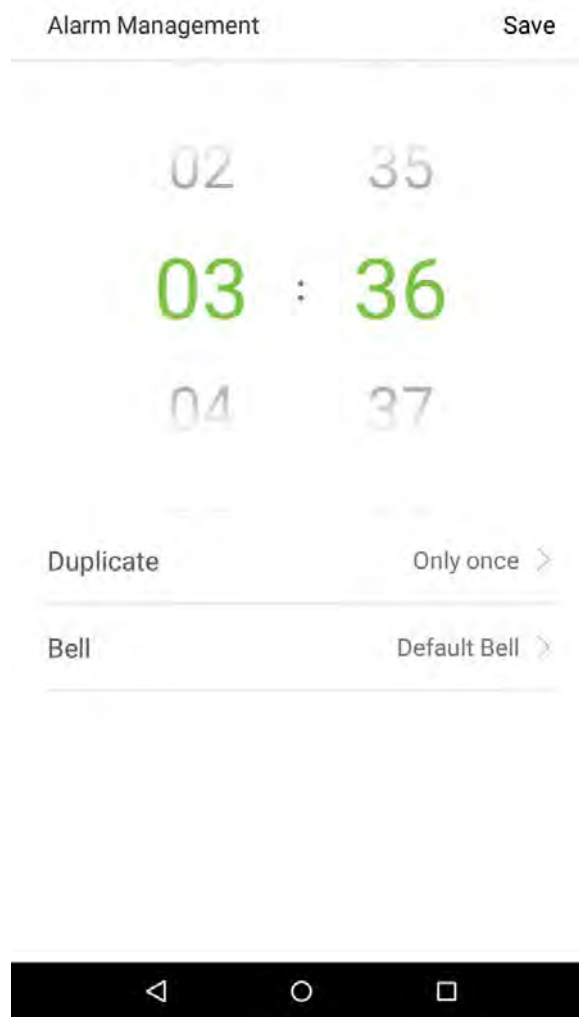


9.2 Edit Alarms

1. Select an alarm from the alarm list.




2. Enter the alarm editing interface.




This operation is similar to adding a new event and will not be described here. See section **“9.1 Add Alarms”** for more details.

9.3 Delete Alarms

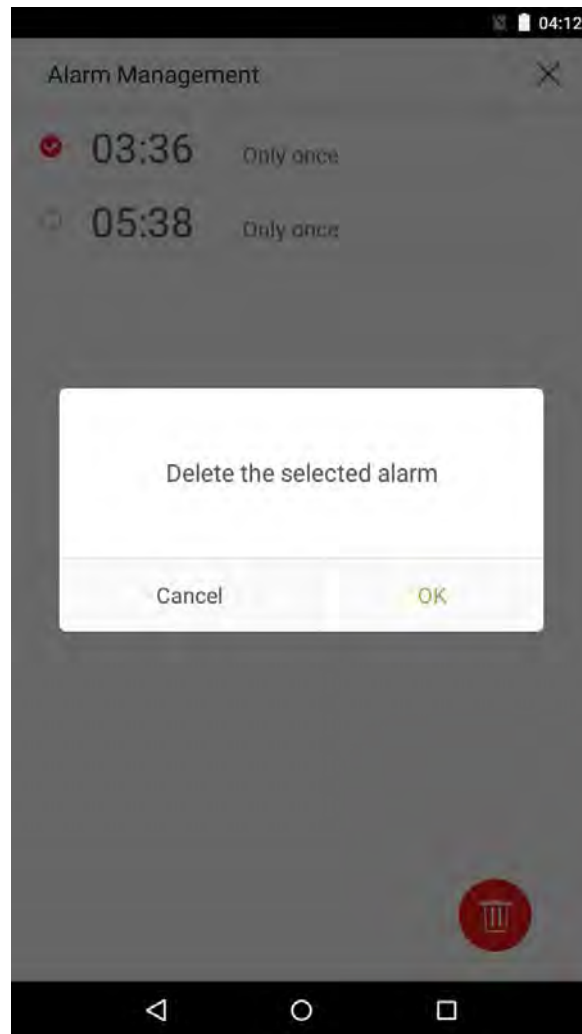
1. On the Alarm Management interface, tap on the  button on the upper right corner.



2. Select the alarm that you would like to delete, and then tap on the  button on the lower right-hand corner.



3. A window will appear. Tap on [OK].



- The event is now deleted and will not appear on the list.

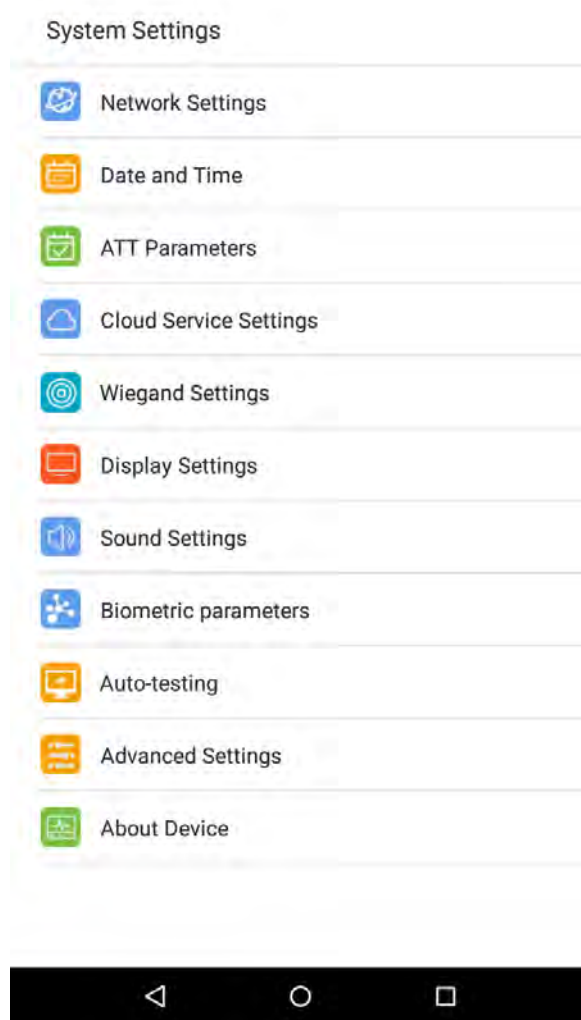
Alarm Management



10. System Settings

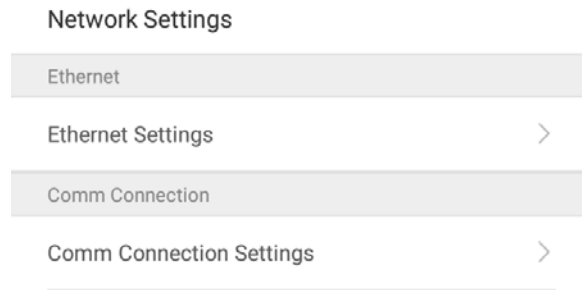
Set system parameters to maximize the device's ability to meet the needs of employees.

In the main menu, tap on [System Settings]:



10.1 Network Settings

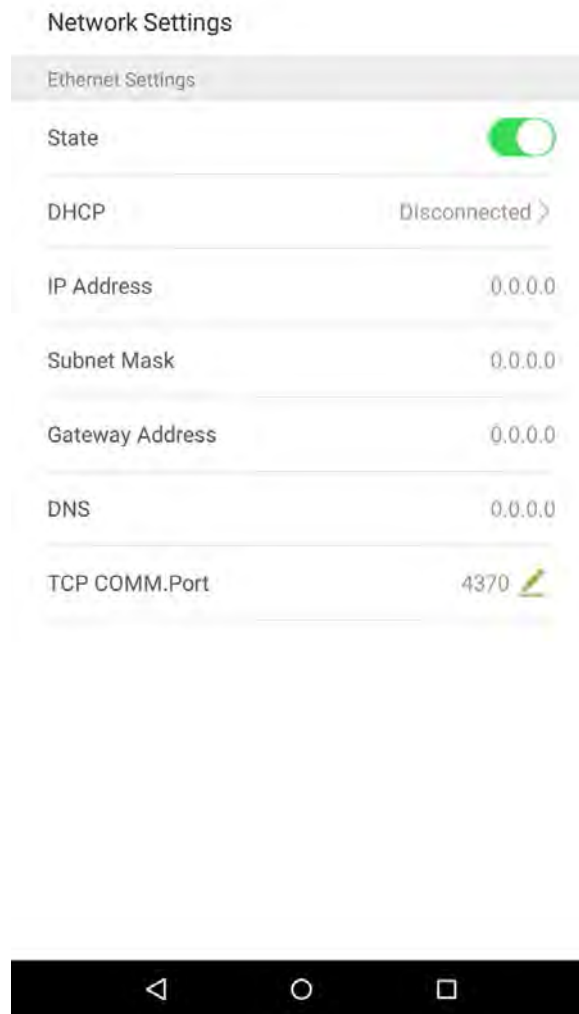
On the system settings list, tap on [Network Settings] to enter the Network Settings interface:



10.1.1 Ethernet Settings

When the device communicates with a PC via Ethernet, the network must be set up.

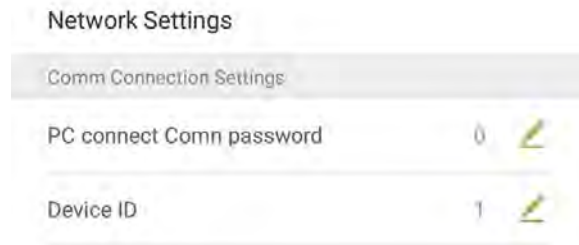
When the device is not connected to the network, tap on [TCP/IP Settings] on the "Network Settings" interface. The following page will display:



Menu Options	Function Description
Enable Ethernet Switch	Enable to modify the Ethernet network address parameters. If this is not enabled, users cannot modify the Ethernet network address parameters.
DHCP	Enable DHCP to assign an IP address to the internal network or network service provider.
IP Address	The default IP is 0.0.0.0; Changeable.
Subnet Mask	The default subnet mask is 0.0.0.0 (can be changed).
Gateway Address	The default gateway address is 0.0.0.0 (can be changed).
DNS	The default address is 0.0.0.0 (can be changed).
TCP Port	The default TCP port is 4370 (can be changed).

10.1.2 Comm Connection Settings

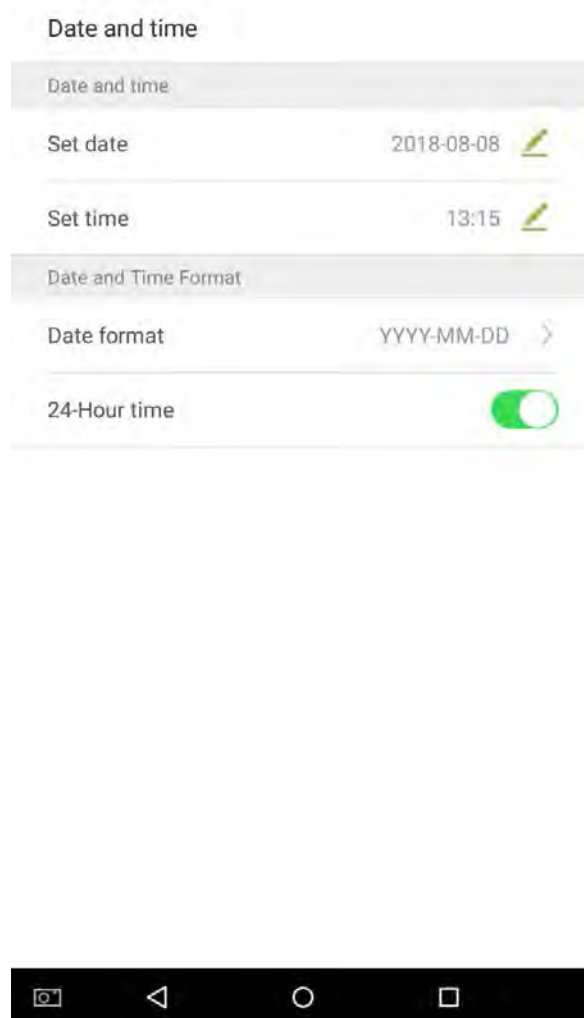
To develop the security and confidentiality of the attendance data, you need to set a connection password. Before successful connection between the PC software and the device, the connection password must be input correctly. On the “Network Settings” interface, tap on [Comm Connection Settings]:



Menu Options	Function Description
PC Connection Password	It is used to gain the connection permission when using offline SDK or PULL SDK connection. If the password is not correct, the communication connection cannot be built. The value ranges from 0 to 999999. When the value is 0, there's no code status.
Device ID	The ID ranges from 1 to 255. If the system is using the RS232/RS485 communication method, please input the device ID during software communication.

10.2 Date and Time

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



10.2.1 Date and Time Settings

1. Tap on [Set Date] and swipe up and down to set the year, month, and day. Tap on [OK].

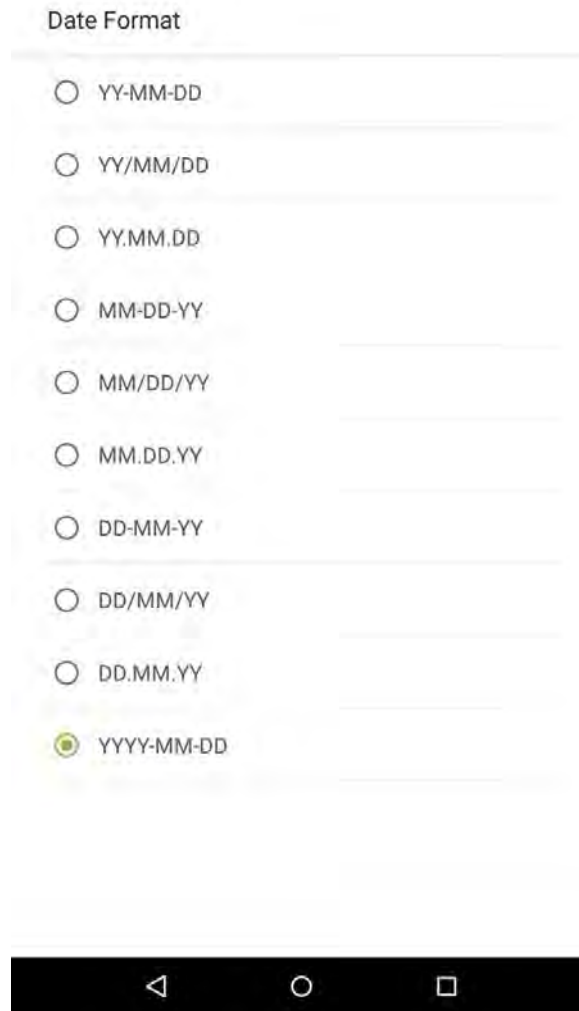


2. Tap on [Set Time] and swipe up and down to set the hour and minute. Tap on [OK].

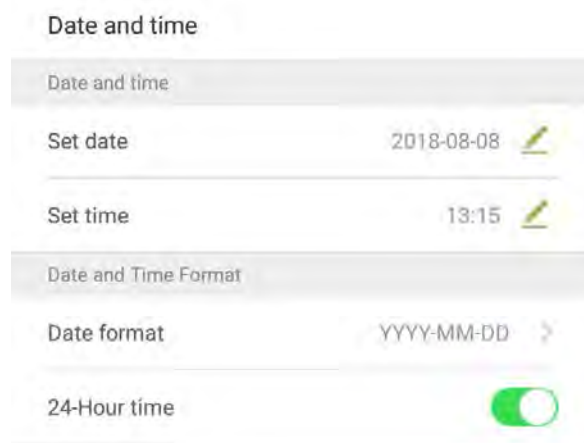


10.2.2 Date and Time Format Settings

1. Tap on [Date Format] and select a date format.

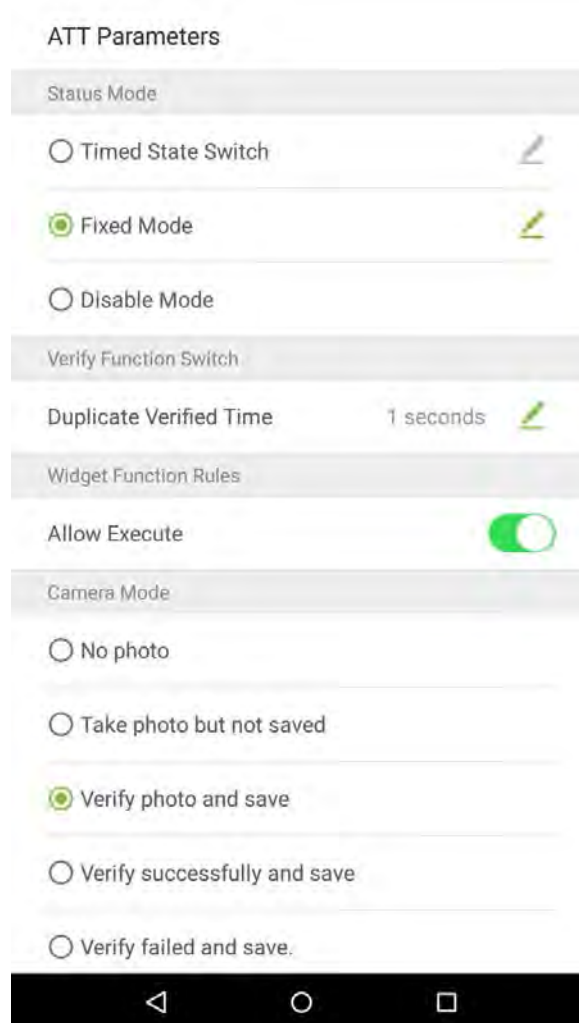


2. Tap on [Use 24-Hour Time Format] to enable this function. It will appear green if enabled or gray if disabled.



10.3 ATT Parameters

In system settings, tap on [ATT Parameters] to enter the ATT parameters settings interface:



10.3.1 Status Mode

1. Status mode settings

There are three modes for attendance statuses:

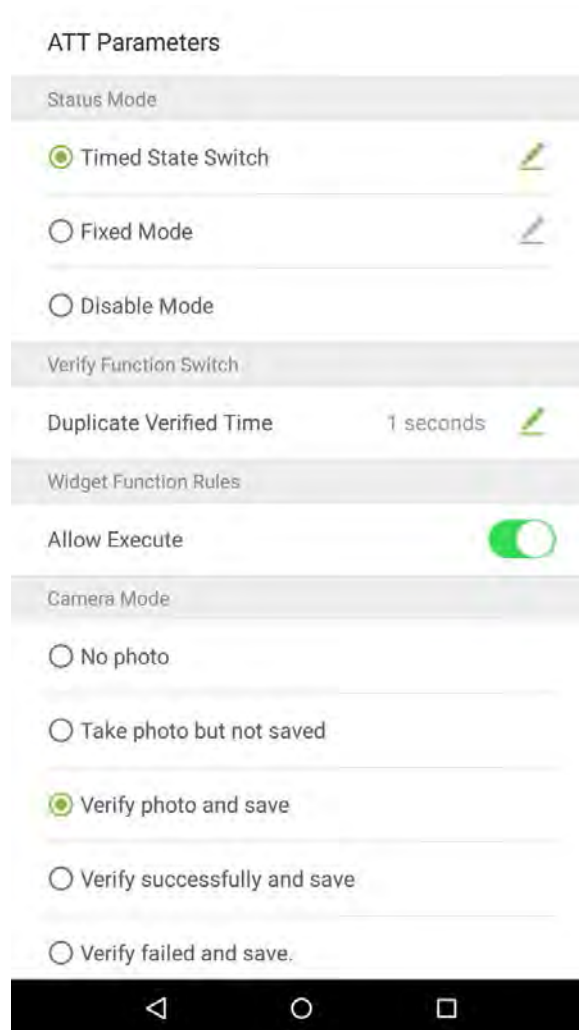
Timed Status Mode: display different attendance statuses at different times.

Fixed Mode: there is only one fixed attendance mode.

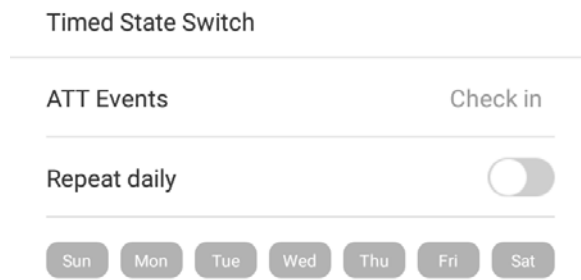
Disable Mode: this function is not used.

- Set in [Timed State Switch] mode

1. After selecting "Timed State Switch", tap on the  button to enter the related settings interface.

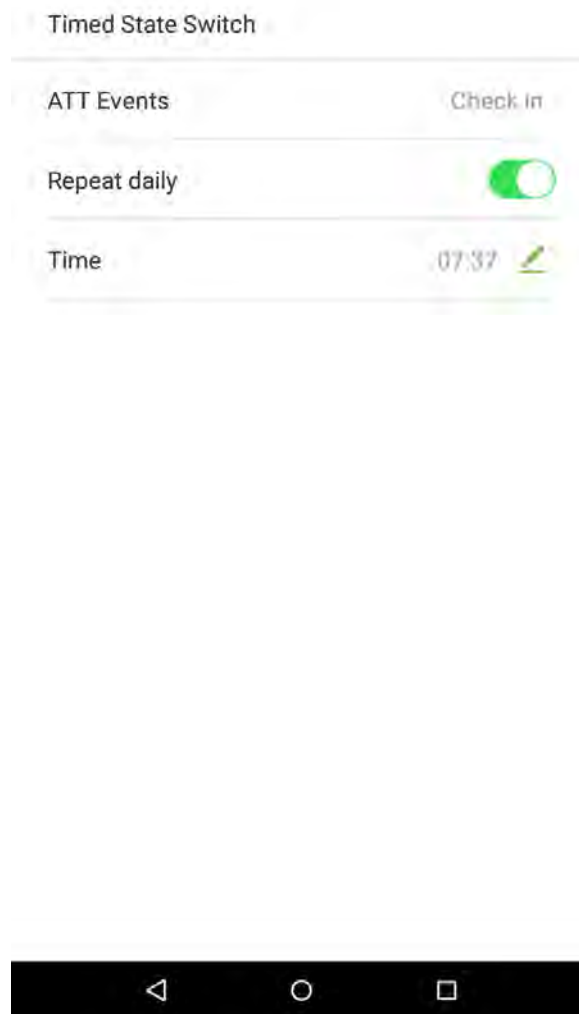


2. On the timed state switch interface, tap on [Check in], then tap on [Repeat Daily]. This will appear green if enabled or gray if disabled.

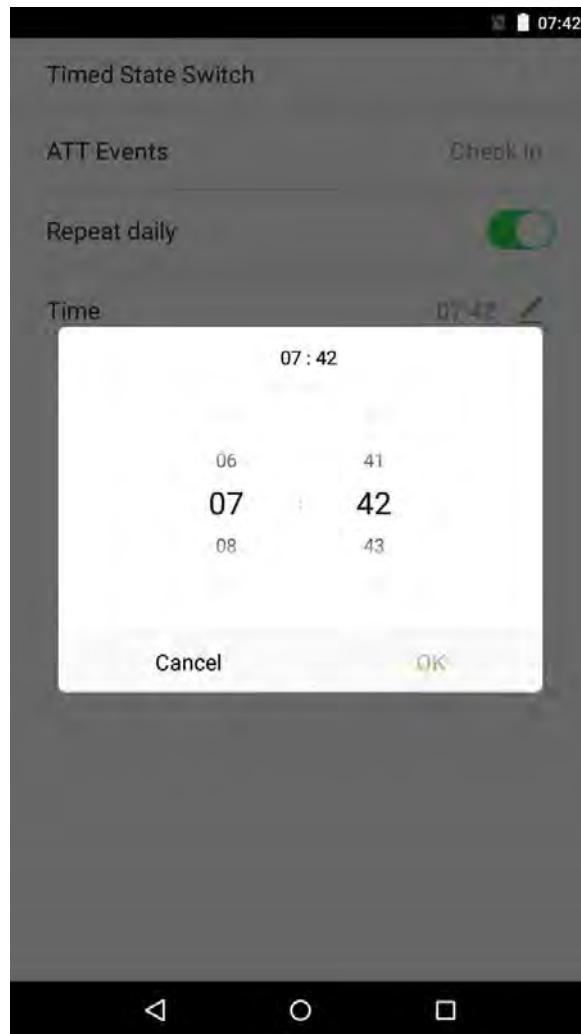


3. Set the time

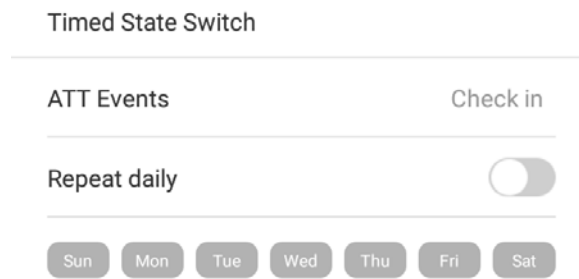
When the [Repeat daily] switch is turned on, the following will display:



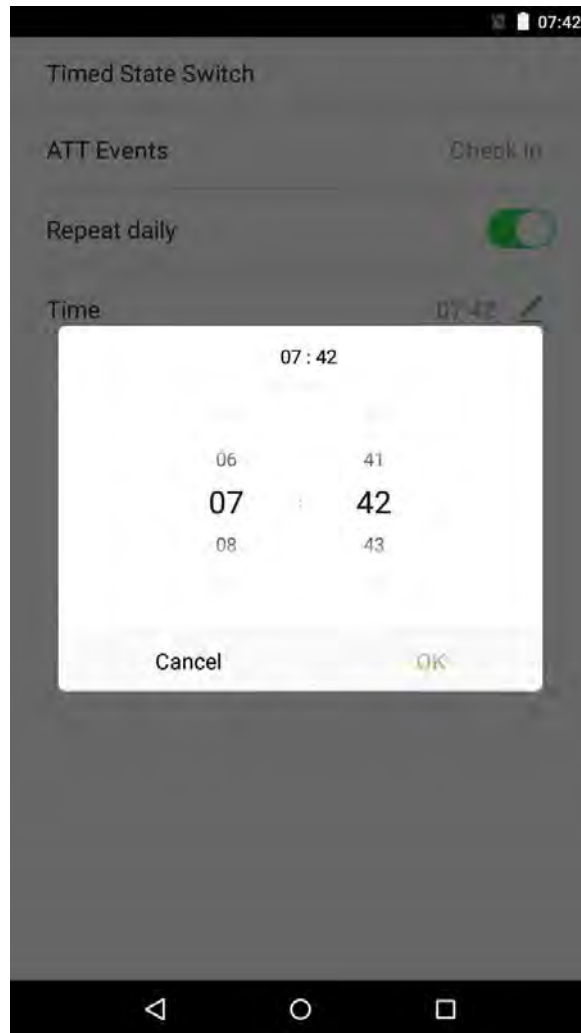
4. Tap on the [Time] button and swipe up and down to set the corresponding time. Tap on [OK].



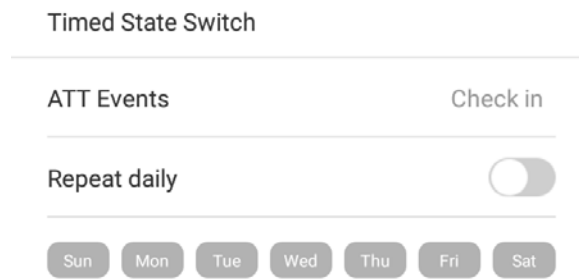
5. When the [Repeat Daily] switch is disabled, the following will display:



6. Tap on the button for the date you would like to set, then swipe up and down to set the corresponding time. Tap on [OK].




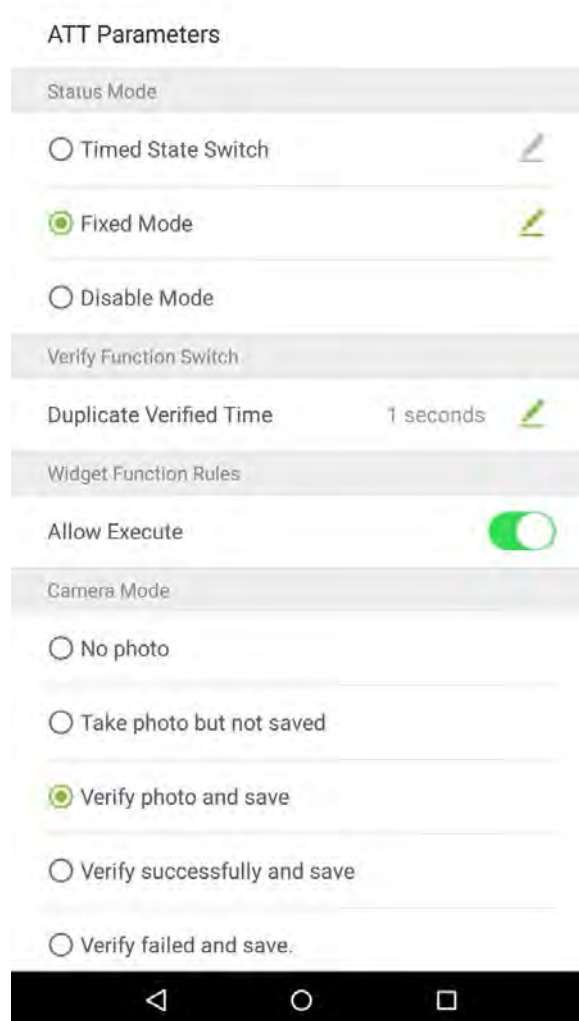
7. Settings Applied



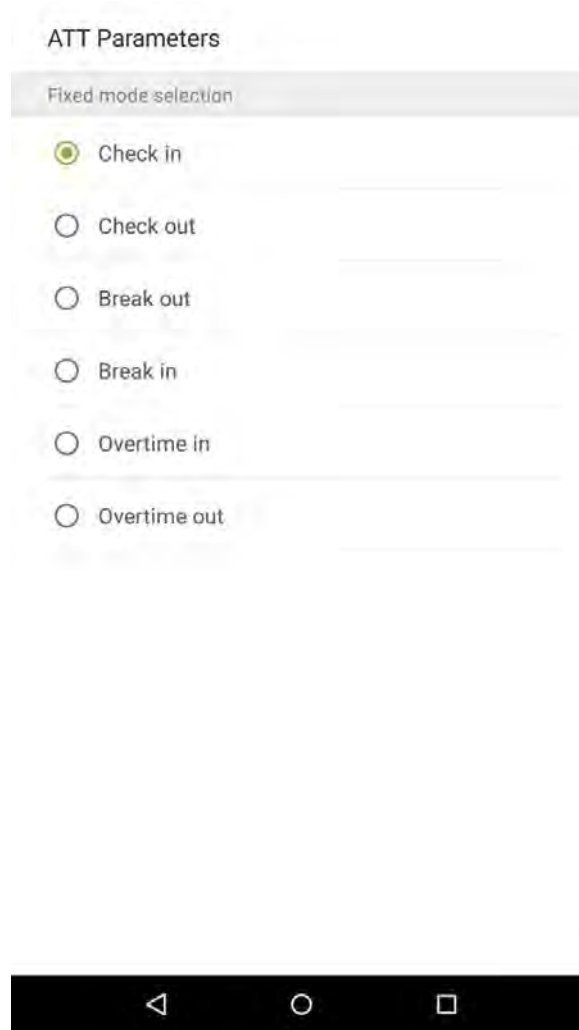
Note: The settings process for "Clock out", "Break out", "Break in", "Overtime in", and "Overtime out" is the same as "Clock in".

- Set to [Fixed Mode] status.

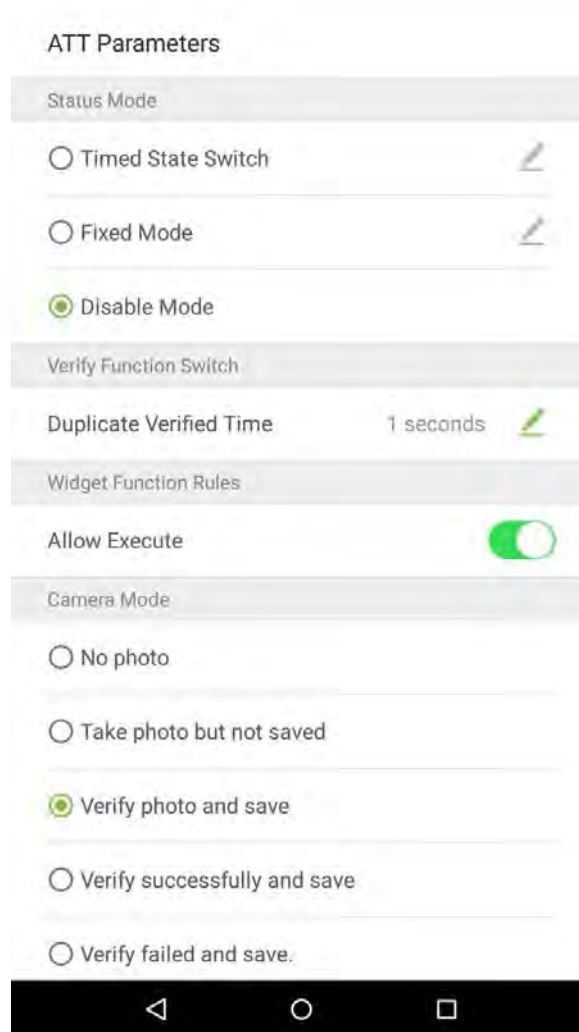
1. Once the status mode is set to "Fixed Mode", tap on the  button to enter the Fixed Mode options menu.



2. In the Fixed Mode selection menu, select the attendance status that you would like to set.

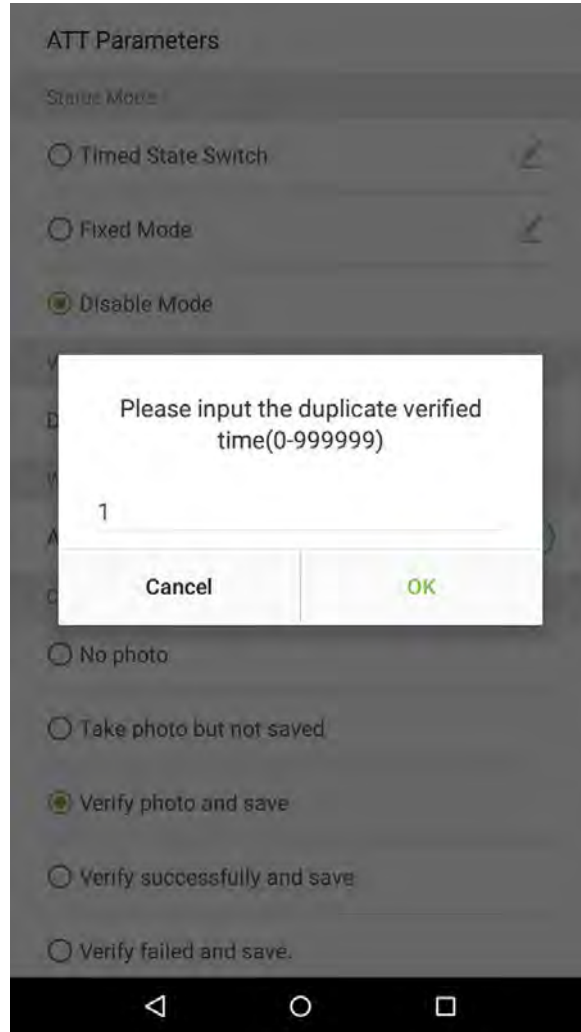


- Set this mode to disabled.
1. Select the Status Mode as "Disable Mode".



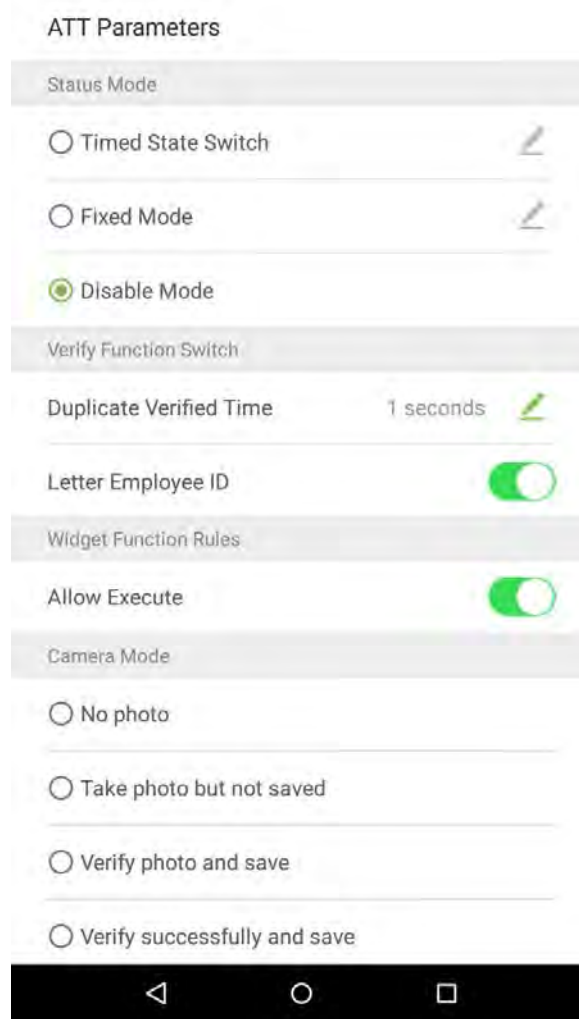
- Duplicate verified time settings.

1. Tap on [Duplicate verified time] and a dialog box will appear asking you to input time (unit: seconds). Tap on [OK].



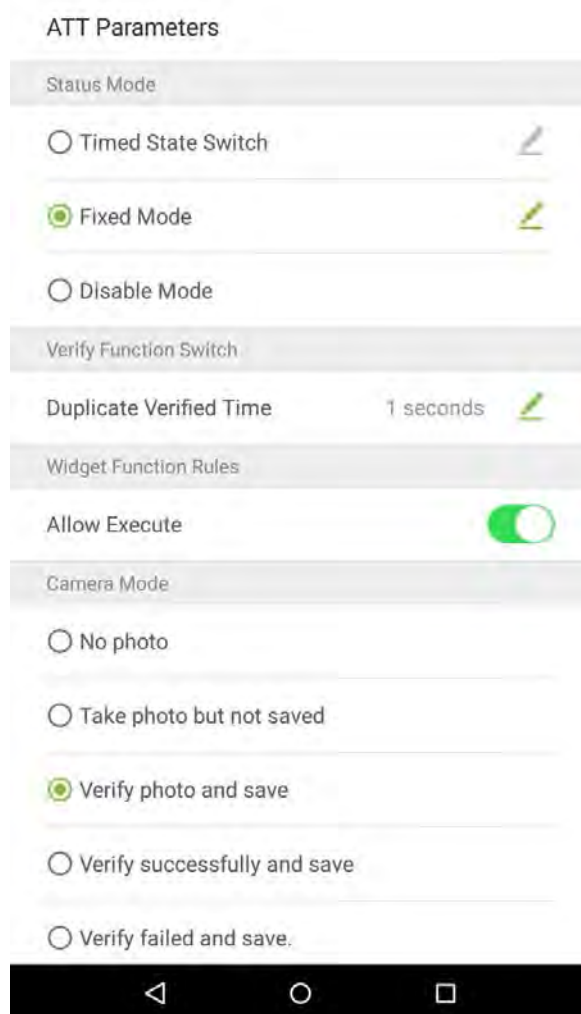
- Support letter personnel IDs settings.

1. Tap on the [Letter Employee ID] switch. It will turn green when enabled and gray when disabled.



10.3.2 Plugin Function Rules

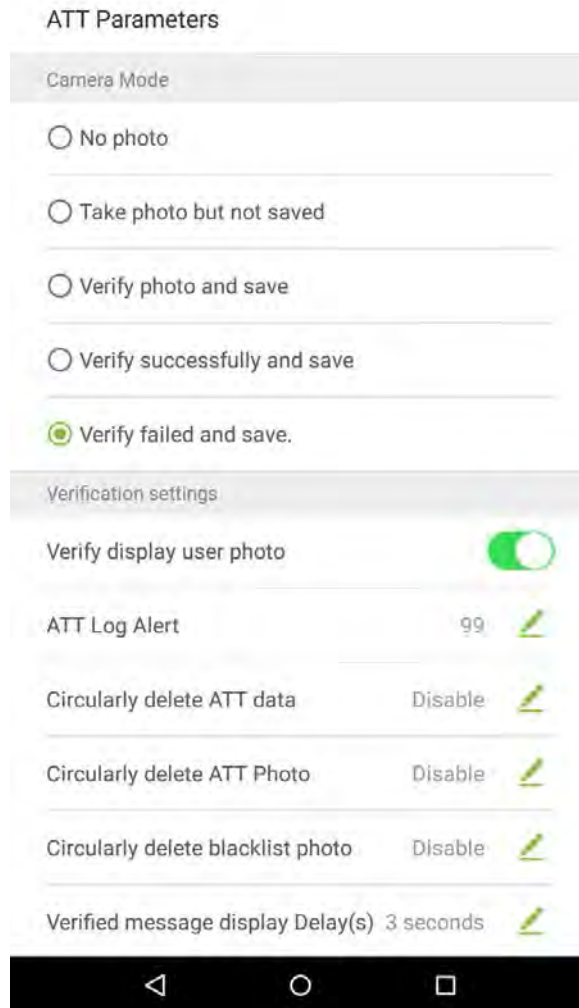
Tap on the [Allow Execute] switch. It will turn green when enabled and gray when disabled:



10.3.3 Camera Mode

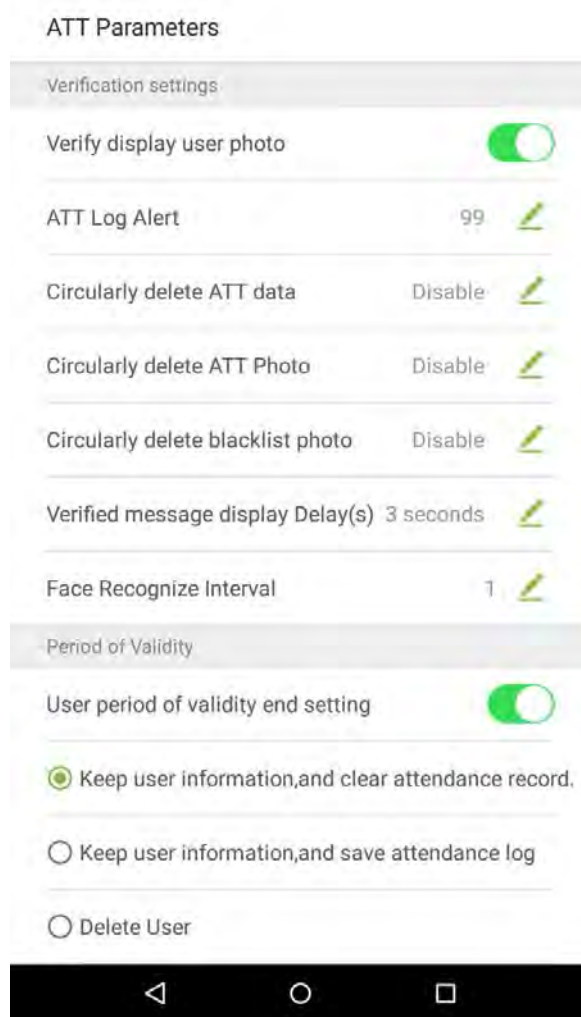
Select the circumstances in which the camera will take photos and whether or not the photos are saved to assist with attendance records.

Tap on the [Camera Mode] that you would like to configure:



10.3.4 Verification Settings

Configure settings for attendance verification parameters:

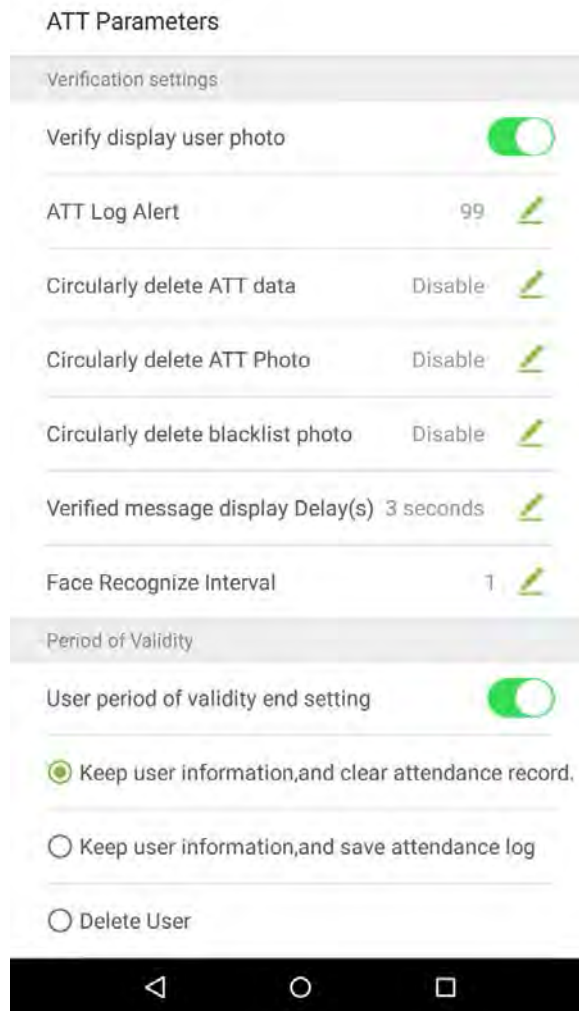


Menu Options	Function Description
Show Employee Photo After Verification	If it is enabled, the employee photo will be displayed; if not, the employee photo will not be displayed.
ATT Log Alert	When the remaining record space reaches a set value, the device will automatically display a remaining record memory warning. When the value is set as 0, the function is disabled.
Cyclically Delete ATT Data	When the attendance record memory has reached full capacity, the device will automatically delete a set value of old attendance records. When the value is set as 0, the function is disabled.
Cyclically Delete ATT Photos	When the space storing the attendance photos have reached full capacity, the device will automatically delete a set value of old attendance photos. When the value is set as 0, the function is disabled.
Cyclically Delete Blacklist Photos	When the space storing blacklisted photos have reached full capacity, the device will automatically delete a set value of old blacklisted photos. When the value is set as 0, the function is disabled.
Verify Message Display Delay	This is the length of time that an employee's information will display on the system's screen after successful verification. Unit: seconds.

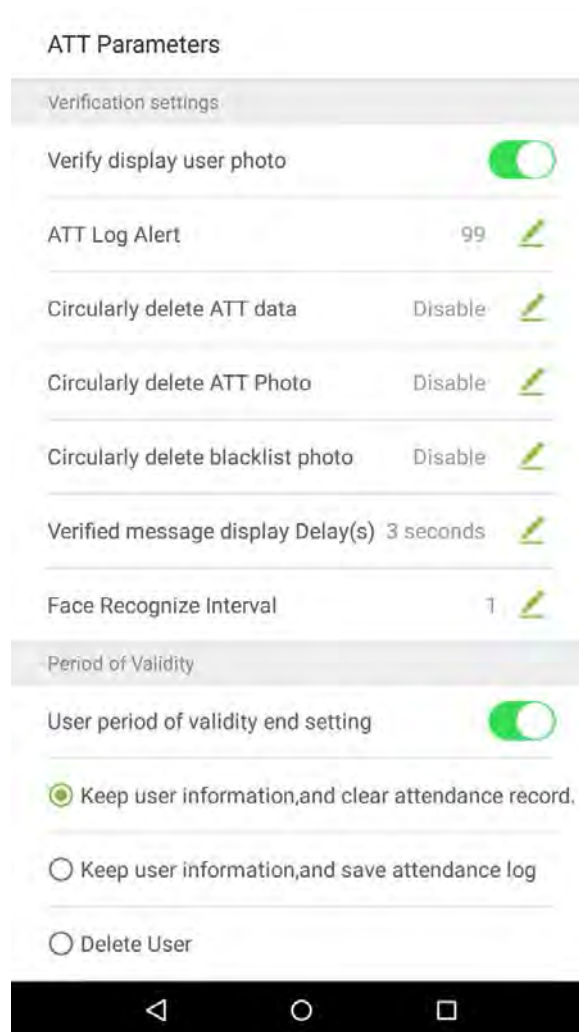
10.3.5 Validity Period of User Information

This is used to determine if employee validity periods are enabled or disabled when registering employees.

1. Tap on the [User period of validity end setting] switch. It will turn green when enabled and gray when disabled.

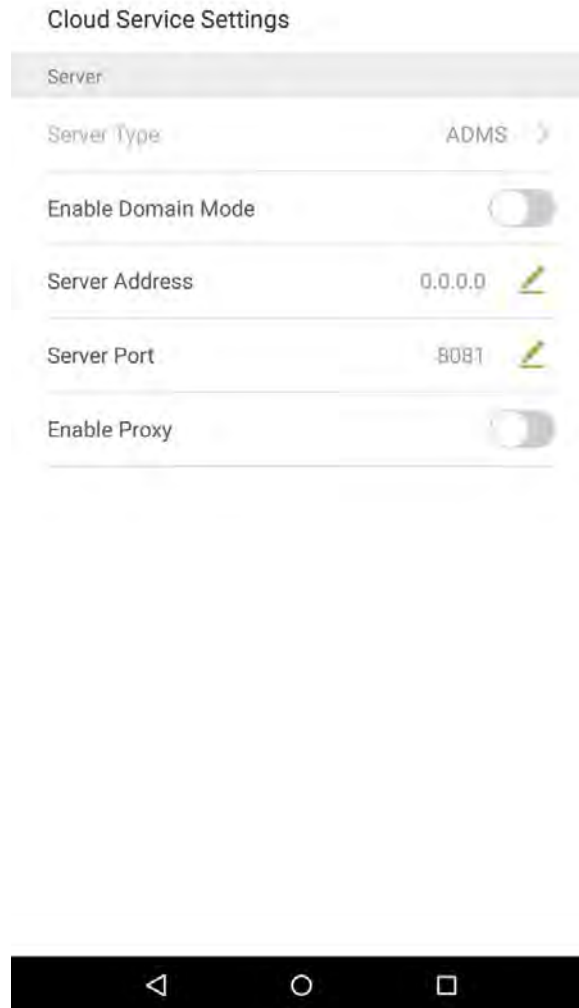


2. When User period of validity end setting is enabled, the following will display. Select the setting you would like to configure.



10.4 Cloud Service Settings

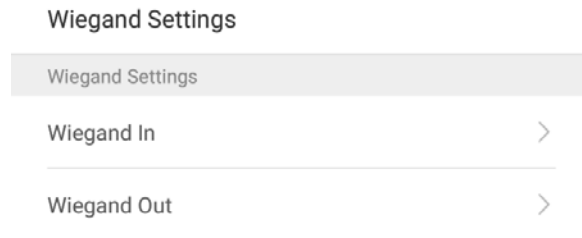
In the system settings list, tap on [Cloud Service Settings] to enter the Cloud service settings interface:



Menu Options	Function Description
Enable Domain Mode	When domain mode is enabled, use a domain name mode of http://... For example, if the server is installed on http://www.XXX.com, XXX indicates the domain name. If this is disabled, users must input an IP address.
Server Address	The IP address of ADMS server.
Server Port	The port that ADMS server uses.
Enable Proxy	When you enable a proxy, you need to set an IP address and port number for the proxy server.

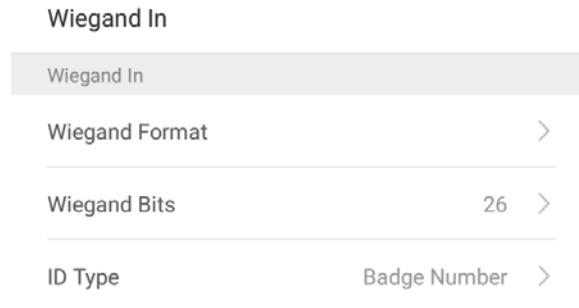
10.5 Wiegand Settings

Tap on [Wiegand Settings] in the system setting list to access the interface as shown below.



10.5.1 Wiegand In

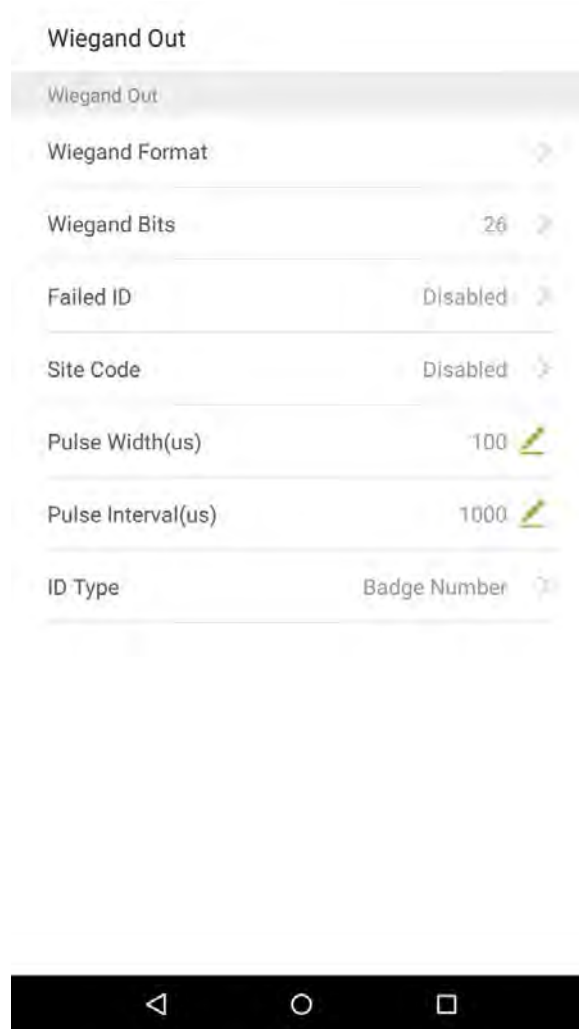
Tap on [Wiegand In] to enter the interface of settings of “Wiegand In”.



Menu Options	Function Description
Wiegand Format	The Wiegand value could be 26bits, 34bits, 36bits, 37bits, or 50bits.

10.5.2 Wiegand Out

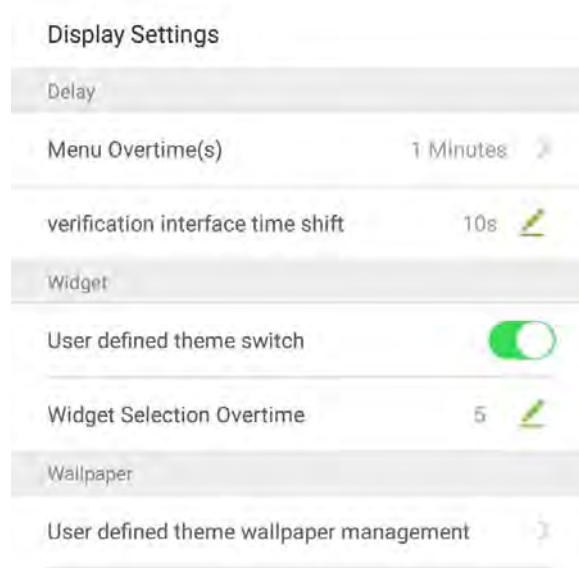
Tap on [Wiegand Out] to enter the below interface:



Menu Options	Function Description
Wiegand Format	The Wiegand value could be 26bits, 34bits, 36bits, 37bits, 50bits.
Wiegand output Digits	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.
Location Code	0-256.
Pulse Width	The time width represents the changes of the quantity of electric charge with high-frequency capacitance regularly within a specified time.
Pulse Interval	The time interval between pulses.
Verification Method	Users may be verified with the specific work codes and card numbers. If the device supports alphabetical work codes, work code output will not be supported and only card number output can be available.

10.6 Display Settings

In the system settings list, tap on [Display Settings] to enter the display settings page:



Menu Options	Function Description
Menu Timeout	Menu timeout occurs when no operations are performed for a certain amount of time after a user has entered the menu, and the menu enters a standby screen. Parameter options include: 30 seconds, 1 minute, 2 minutes, 5 minutes, 10 minutes, or disabled. When this feature is disabled, the menu (including sub-menus) will not automatically close. Users must press "Exit" to exit the menu.
Custom Theme Switch	When this switch is enabled, users can drag plugin; when disabled, widgets cannot be dragged. (When this is enabled, anyone can modify the theme. We recommend that the administrator disable this function after making the desired changes).
Plugin Selection Timeout	If a timeout message occurs while selecting plugin status time, the default status will be restored. When the value is set as 0, this function is disabled. Unit: seconds.
Custom Theme Wallpaper Management	This displays all uploaded custom wallpapers. Users can set and delete wallpapers.

10.7 Sound Settings

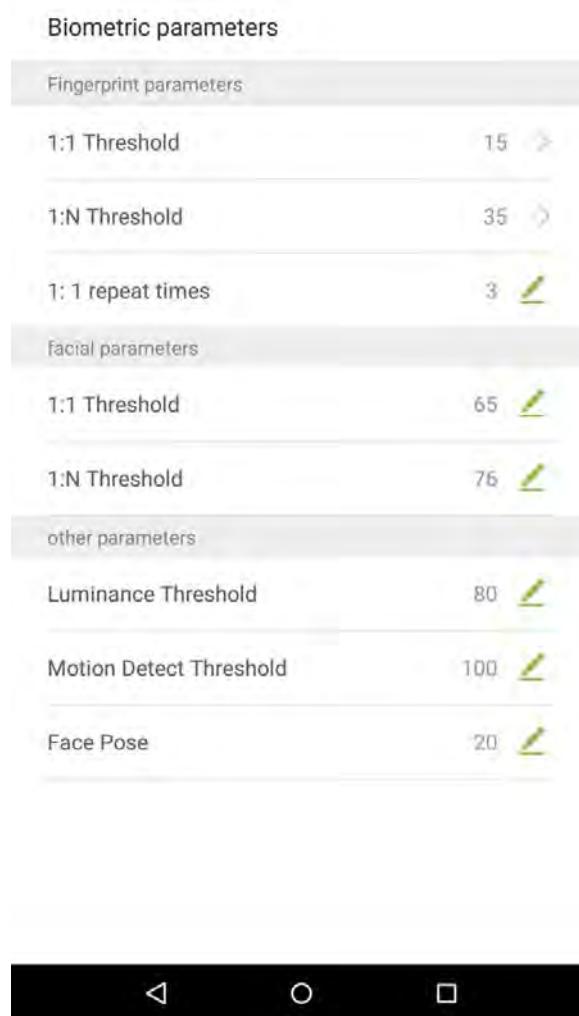
On the system settings list, tap on [Sound Settings] to enter the interface of sound settings.



Menu Options	Function Description
Audio Prompts	When audio prompts are enabled, users will receive audio prompts. Audio prompts will not be received when this setting is disabled. When disabled and then re-enabled, the volume level will be set to 1.
Touch Prompt	This switch enables/disables touchscreen prompt. When enabled, users will receive touchscreen prompts. When disabled, no touchscreen prompts will be received.
Voice Settings	Adjust volume settings. This can only be used if audio prompts are enabled. It can be set from 0-15.

10.8 Biometric Parameters

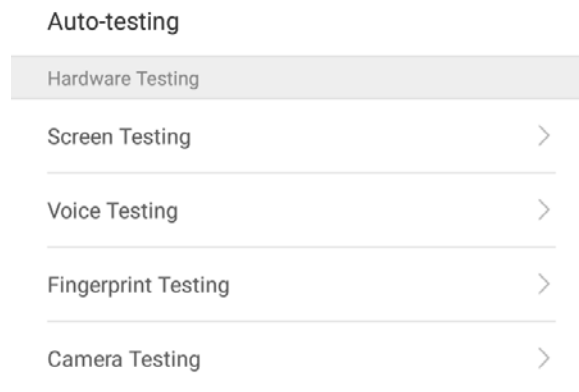
On the system settings list, tap on [Biometric Parameters] to enter the “Biometric parameters” interface:



Menu	Function Description
1:1 Thresholds	When conducting 1:1 fingerprint verification, fingerprint data is collected and instantly compared with fingerprint data using a 1:1 algorithm. This is converted into a value that is then compared to a set value. If the value of the scanned fingerprint exceeds that of the set value, the verification passes. If it does not, the verification fails.
1:N Thresholds	When conducting 1:N verification, fingerprint data is collected and instantly compared with all fingerprint templates on the system using a 1:N algorithm. This is converted into a value that is compared to a set value. If the value of the scanned fingerprint exceeds that of the set value, the verification has passes. If it does not, the verification fails.
1:1 Retry Times	The upper limit of the number of failed verification under 1:1 verification. When the number of failed verification reaches the set value, the system will return to the standby interface.

10.9 Auto-testing

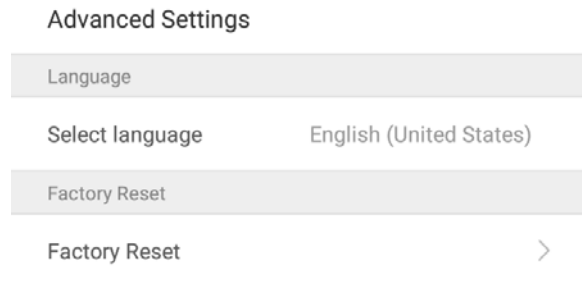
On the system settings list, tap on [Auto-testing] to enter the auto testing interface:



Menu Options	Function Description
Screen Testing	Test the screen's display. The screen will display red, green, blue, white, and black tests. Check if the screen color is uniformly correct across each area of the screen. Tap on anywhere on the screen during testing to continue testing. Tap on the back key to exit testing.
Voice Testing	The device automatically tests audio prompts by playing back audio files that are stored in the device to test if the device's audio files are complete and if the audio effects are in good working order. Tap on the back key to exit testing.
Fingerprint Testing	The device automatically tests if the fingerprint scanner is functioning properly by testing a fingerprint that is pressed onto the scanner, and seeing if the fingerprint image is clear and usable. When pressing a fingerprint onto the scanner, the screen will display an image of the scanned fingerprint.
Camera Testing	Test if the camera is functioning properly. Check to see if the image quality is clear and usable.

10.10 Advanced Settings

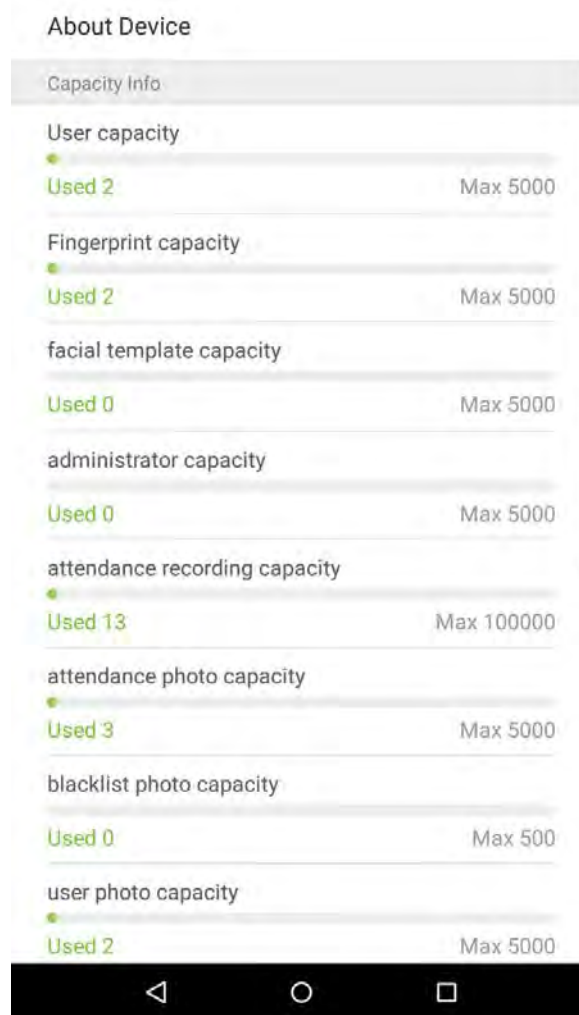
On the system settings list, tap on [Advanced Settings] to enter the “Advanced Settings” interface:



Menu Options	Function Description
Select Language	Select Simplified Chinese.
Restore Factory	Restores the settings of the device, including communication settings, system settings, to the factory settings.
Upgrade USB	Adjust volume. Volume can only be adjusted if audio prompts are enabled. The effective range is 0-15.

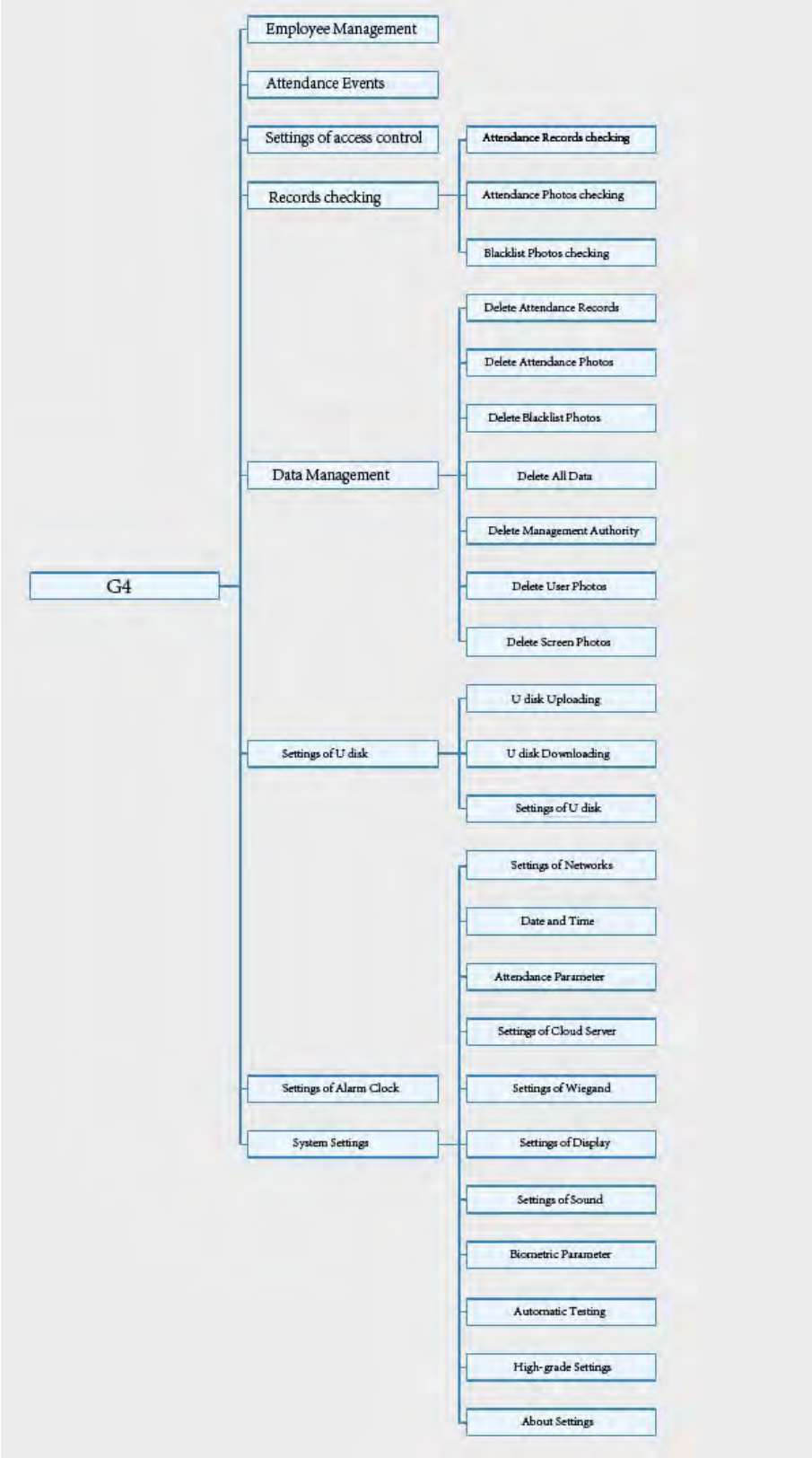
10.11 About the Device

On the system settings list, tap on [About the Device] to enter the “About the Device” interface:



Menu Options	Function Description
Capacity Information	Displays the current device's employee storage, fingerprint storage, administrators, attendance records, attendance photos, blacklist photos, and employee photos.
Device Information	Displays the device's name, serial number, MAC address, fingerprint algorithm version information, platform information, and manufacturer.
Version	Displays all the versions of all the system's apps, such as the system settings, quick parts, data manager, and other installed apps.

Appendix



Statement on the Right to Privacy

Dear Customers:

Thank you for choosing this hybrid biometric recognition product, which was designed and manufactured by ZKTeco. As a world-renowned provider of core biometric recognition technologies, we are constantly developing and researching new products, and strive to follow the privacy laws of each country in which our products are sold.

We Declare That:

1. All of our civilian fingerprint recognition devices capture characteristics, not fingerprint images, and do not involve privacy protection.
2. None of the fingerprint characteristics that we capture can be used to reconstruct an image of the original fingerprint, and do not involve privacy protection.
3. As the provider of this device, we will assume no direct or indirect responsibility for any consequences that may result from your use of this device.
4. If you would like to dispute human rights or privacy issues concerning your use of our product, please directly contact your employer.

Our other police fingerprinting devices or development tools can capture original images of citizens' fingerprints. As to whether or not this constitutes infringement of your rights, please contact your government or the final supplier of the device. As the manufacturers of the device, we will assume no legal liability.

Notes:

Chinese law includes the following provisions on the personal freedoms of its citizens:

1. There shall be no illegal arrest, detention, search, or infringement of persons;
2. Personal dignity as related to personal freedom shall not be infringed upon;
3. A citizen's house may not be infringed upon;
4. A citizen's right to communication and the confidentiality of that communication is protected by law.

As a final point we would like to further emphasize that biometric recognition is an advanced technology that will undoubtedly be used in e-commerce, banking, insurance, legal, and other sectors in the future. Every year the world is subjected to major losses due to insecure nature of passwords. Biometric products serve to protect your identity in high-security environments.

Eco-friendly Use



- This product's "eco-friendly use period" refers to the period during which this product will not leak toxic or hazardous substances, when used in accordance with the conditions in this manual.
- The eco-friendly use period indicated 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 use 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	○	○	○	×	○	○

○: indicates that the total amount of toxic content in all of the homogeneous materials is below the limit requirements specified in SJ/T 11363—2006.

×: indicates that the total amount of toxic content in all of the homogeneous materials exceeds the limit requirements specified in SJ/T 11363—2006.

Note: 80% of this project's components are made using non-toxic, eco-friendly materials. Those which contain toxins or harmful materials or elements are included due to current economic or technical limitations which prevent their replacement with non-toxic materials or elements.

ZK Building, Wuhe Road, Gangtou, Bantian, Buji Town,
Longgang District, Shenzhen China 518129

Tel: +86 755-89602345

Fax: +86 755-89602394

www.zkteco.com

