User Manual

G4 Pro Series

Date: March 2022

Doc Version: 1.1

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.

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 **G4 Pro Series**.

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 Software	
Convention	**Description**
Bold font	Used to identify software interface names e.g. **OK**, **Confirm**, **Cancel**.
>	Multi-level menus are separated by these brackets. For example, File > Create > Folder.
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.

Table of Contents

1 Overview

G4 Pro Series is a fully upgraded version of the Visible Light Facial Recognition Terminal, using intelligent engineering facial recognition algorithms and the latest computer vision technology. It supports both facial and palm verification with large capacity and speedy recognition, also intergrated QR Sensor support QR code with Mobile APP, as well as improves security performance in all aspects. G4 Pro Series has two models, G4 Pro[TI] is the upgraded version of G4 Pro with thermal imaging intelligent engineering facial recognition algorithm.

G4 Pro Series supports facial recognition with large capacity and speedy recognition and other authentication methods, including identification with palm, card, password and fingerprint★.

G4 Pro[TI] adopts touchless recognition technology and new functions i.e.,

1) Body Temperature Detection
2) Face Mask Detection

It is also equipped with an ultimate anti-spoofing algorithm for facial recognition against almost all types of fake photos and video intrusions. This device is a perfect choice to reduce the spread of germs and help prevent infections directly at each access point of any premises and public areas such as hospitals, factories, schools, commercial buildings, stations during the recent pandemic condition with its fast and accurate body temperature measurement and face mask detection functions during facial verification.

Features

- Compatible with 4G network, satisfy various market including Europe, the Middle East, Africa, South Korea, Thailand and India
- Scanning of T&A/A&C dynamic QR codes on the ZKBioSecurity Mobile App
- Open Supervised Device Protocol (OSDP v2.1.7)
- Dual-frequency (125kHz and 13.56MHz) card module (standard)
- HID iClass card (optional)
- Android LCDK demo for the 3rd-party application integration
- PoE 802.3af/at power supply
- Mask detection
- Anti-spoofing algorithm against print attack (laser, color, and B/W photos) and video attack

* Facial recognition for masked individuals will increase FAR. Palm verification for masked individuals is recommended.

Special Functions

- Mask detection
- Body temperature detection
- Temperature Measurement Distance: **30cm to 120cm (0.98ft to 3.94ft)**
- Temperature Measurement Accuracy: **±0.3°C (±0.54°F)**
- (Tested at a distance of 80cm (2.63ft) under 25°C (77° F) temperature)
- Temperature Measurement Range: **20°C to 50°C (68°F to 122°F)**

2 Instructions for Use

Before getting into the Device features and its functions, it is recommended to be familiar to the below fundamentals.

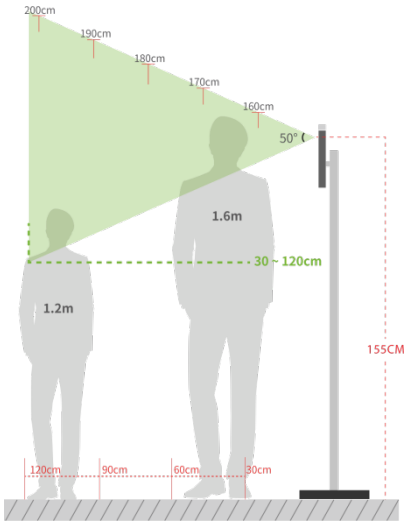
2.1 How to Scan the QR Code?

Open the Mobile Credential of ZKBioSecurity App and parallel the phone screen to the device QR code scanner

NOTE: Place your phone within 15 to 50cm of the device (distance depends on the size of the phone screen), do not block the device QR code scanner and QR code in the phone screen.

2.2 Standing Position, Facial Expression

- **The recommended distance**



The distance between the device and a user whose height is in a range of 1.55m to 1.85m is recommended to be 0.3 to 2.5m. Users may slightly move forward or backward to improve the quality of facial images captured.

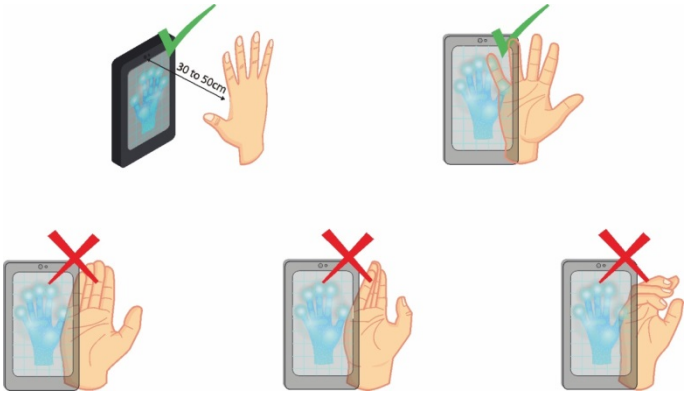
- **Recommended Standing Posture and Facial Expression**

NOTE: Please keep your facial expression and standing posture natural while enrolment or verification.

2.3 Palm Registration

Place your palm in the palm multi-mode collection area, such that the palm is placed parallel to the device.

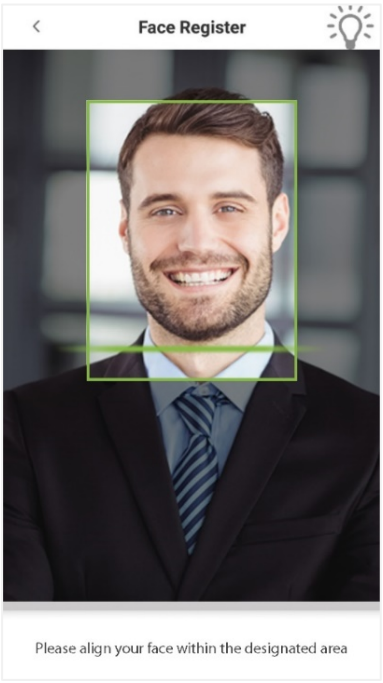
Make sure to keep space between your fingers.



NOTE: Place your palm within 30 to 50cm of the device.

2.4 Face Registration

Try to keep the face in the centre of the screen during registration. Please face towards the camera and stay still during face registration. The screen should look like this:



Correct face registration and authentication method

- **Recommendation for registering a face**
  - When registering a face, maintain a distance of 40cm to 80cm between the device and the face.
  - Be careful not to change your facial expression. (smiling face, drawn face, wink, etc.)

- If you do not follow the instructions on the screen, the face registration may take longer or may fail.
- Be careful not to cover the eyes or eyebrows.
- Do not wear hats, masks, sunglasses, or eyeglasses.
- Be careful not to display two faces on the screen. Register one person at a time.
- It is recommended for a user wearing glasses to register both faces with and without glasses.

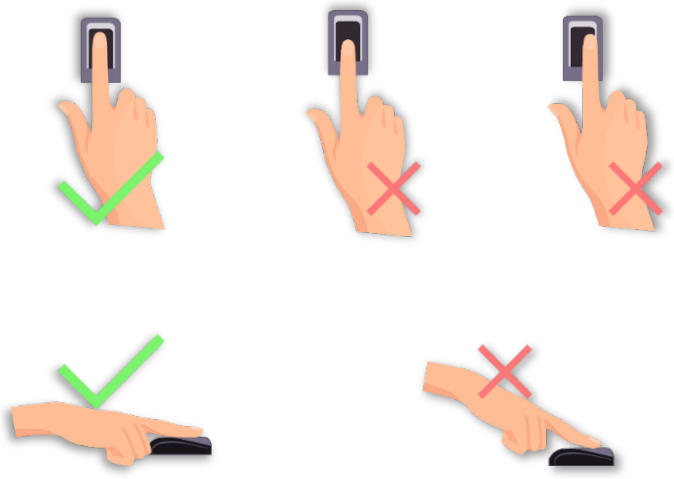
➢ **Recommendation for authenticating a face**

- Ensure that the face appears inside the guideline displayed on the screen of the device.
- If the glasses have been changed, authentication may fail. If the face without glasses has been registered, authenticate the face without glasses further. If the face with glasses has been registered, authenticate the face with the previously worn glasses.
- If a part of the face is covered with a hat, a mask, an eye patch, or sunglasses, authentication may fail. Do not cover the face, allow the device to recognize both the eyebrows and the face.

2.5 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.

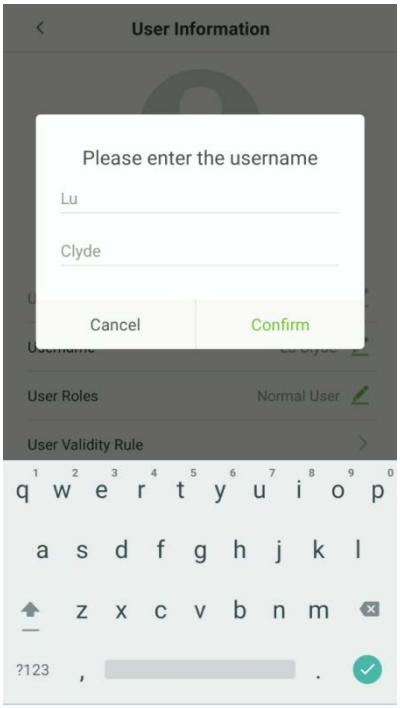
2.6 Standby Interface

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

NOTE:

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.

2.7 Virtual Keyboard



NOTE:

1. Press **[?123]** to switch to the numeric and symbolic keyboard.
2. Click the input box, virtual keyboard appears.

2.8 Verification Mode

2.8.1 QR Code Verification

In this verification mode, the device compares the QR code image collected by the QR code collector with all the QR code data in the device.

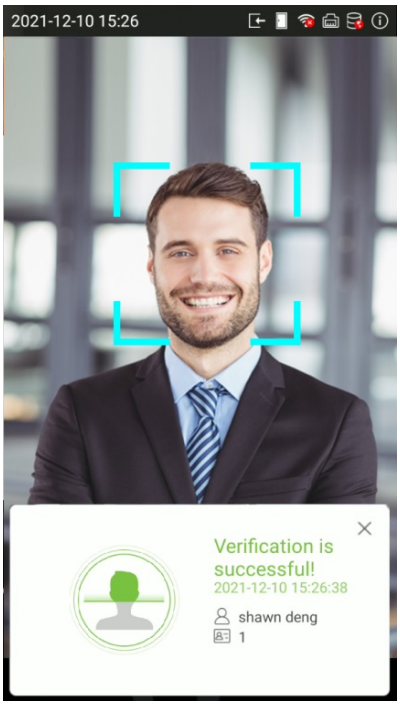
Tap **[Mobile Credential]** on the ZKBioSecurity App, and a QR code will appear, which includes employee ID and card number (static QR code only includes card number) information. The QR code can replace a physical card on a specific device to achieve contactless authentication. Please refer to 11.3 Mobile Credential.

2.8.2 Facial Verification

- **1:N (One to Many) Facial Verification Mode**

  1. **Conventional verification**

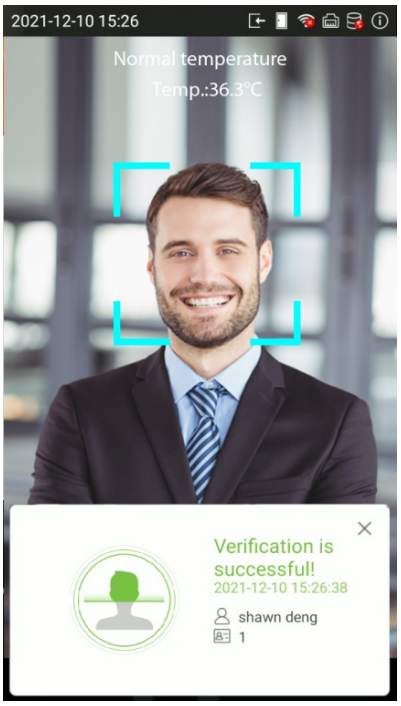
In this verification mode, the device compares the collected facial images with all face data registered in the device. The following is the pop-up prompt of a successful comparison result.

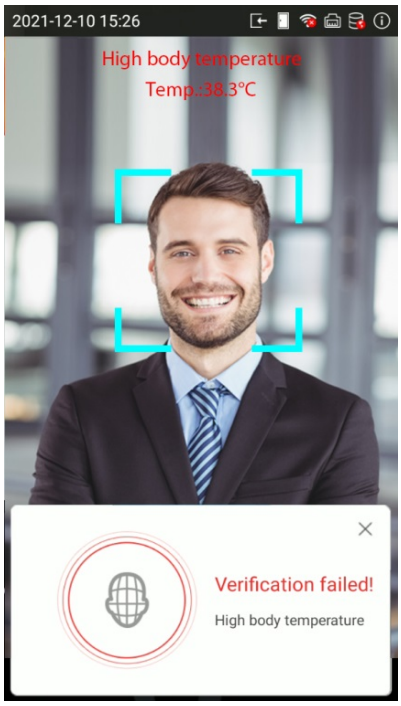


2. Enable temperature screening with infrared ★

When the user enables the **Enable temperature screening with infrared** function, during user verification, in addition to the conventional verification method, the user's face must be aligned with the temperature measurement area to measure the body temperature before the verification can be conducted. The following are the popups of the comparison result prompt interface. (Note: This function is only applicable to products with temperature measurement module.)

NOTE: The temperature measurement data is only for reference, and not for any medical purposes.

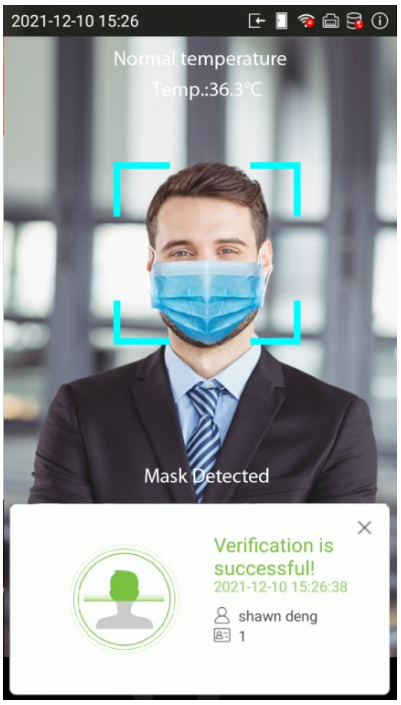


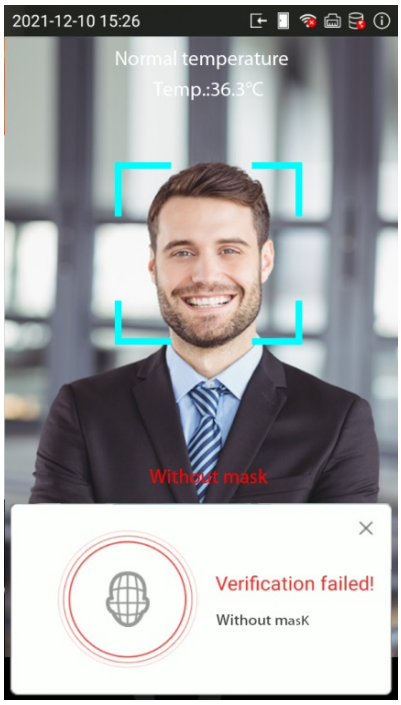


3. Enable mask detection ★

When the user enables the **Enable mask detection** function, the device will identify whether the user is wearing a mask or not while verification. The following are the popups of the comparison result prompt interface. (Note: This function is only applicable to products with temperature measurement module.)

NOTE: The temperature measurement data is only for reference, and not for any medical purposes.

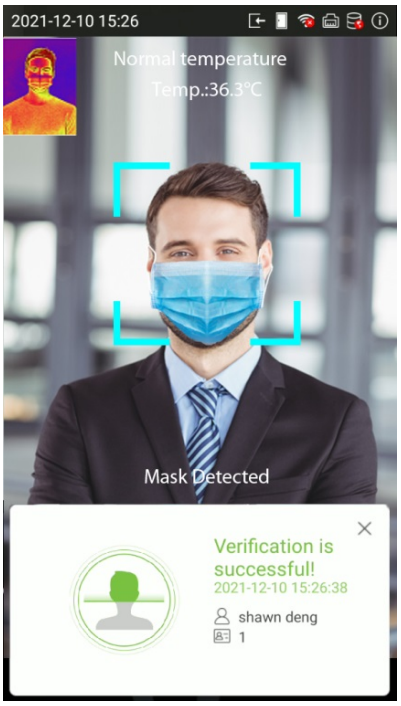


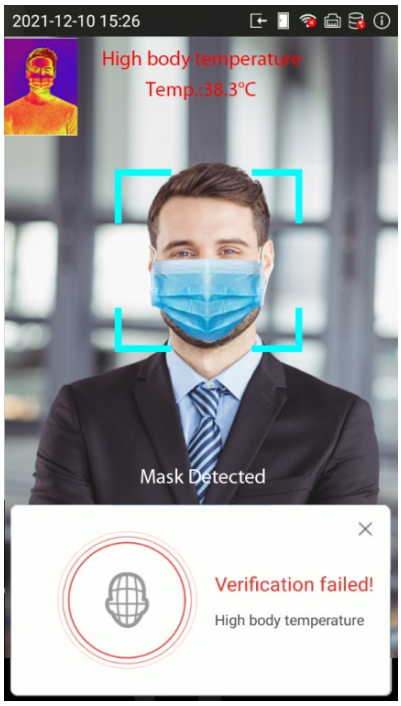


4. Display Thermodynamics Figure ★

When the user enables the **Display Thermodynamics Figure** function, the thermal image of the person is displayed in the upper left corner of the device, while verification. As shown in the images below:

NOTE: The temperature measurement data is only for reference, and not for any medical purposes.

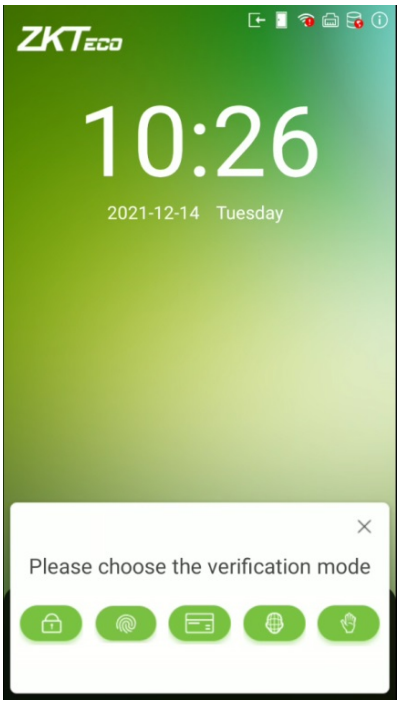




- **1:1 (One to One) Facial Verification Mode**

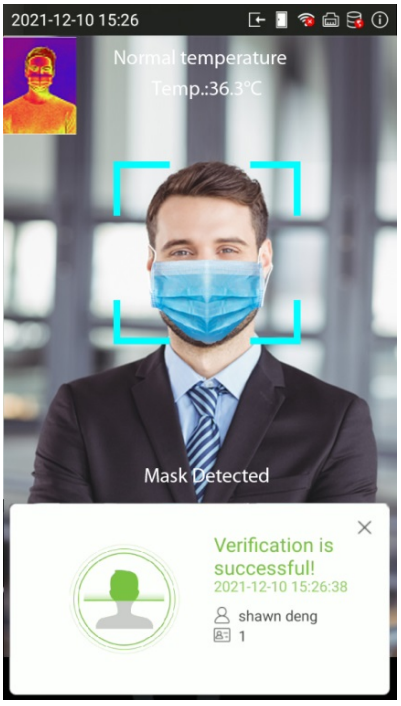
In this verification mode, the device compares the face captured by the camera with the facial template related to the entered user ID. Press on the main interface and enter the 1:1 facial verification mode and enter the user ID and press **[OK]**.

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

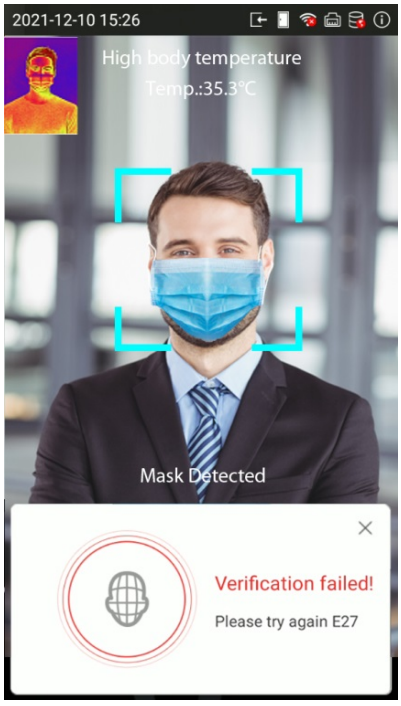


Select the icon to enter the face verification mode. After the prompt "Please verify your face ", adjust your face in the center of the device screen for face verification.

Below are the sample for successful and unsuccessful verification:



Successful Verification



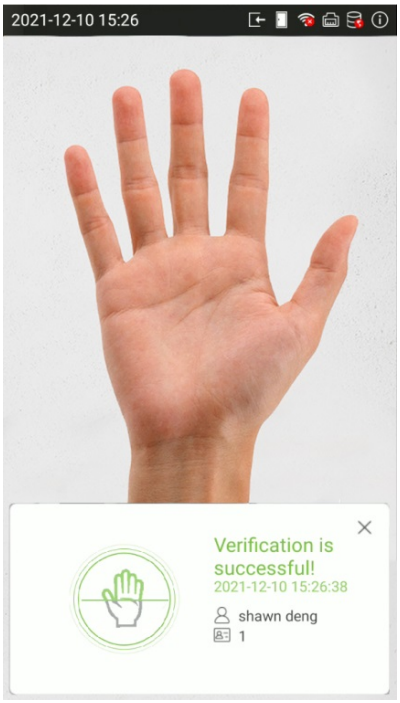
Failed Verification

2.8.3 Palm Verification

- **1:N (One to Many) Palm Verification Mode**

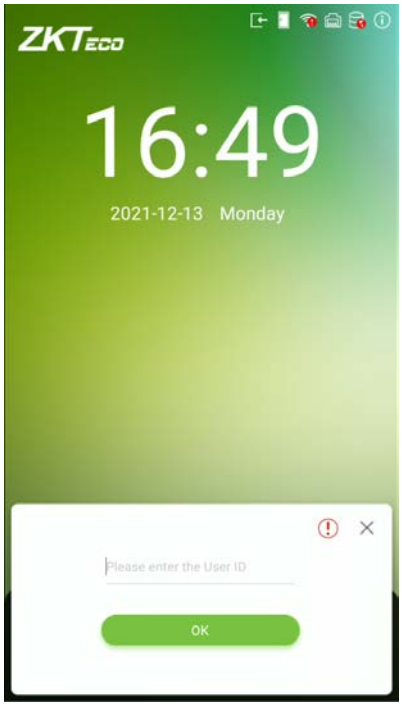
This verification mode compares the palm image collected by the palm module with all the palm data template in the device.

The device will automatically distinguish between the palm and face verification mode. Place the palm in the area that can be collected by the palm module, so that the device will automatically switch to palm verification mode.

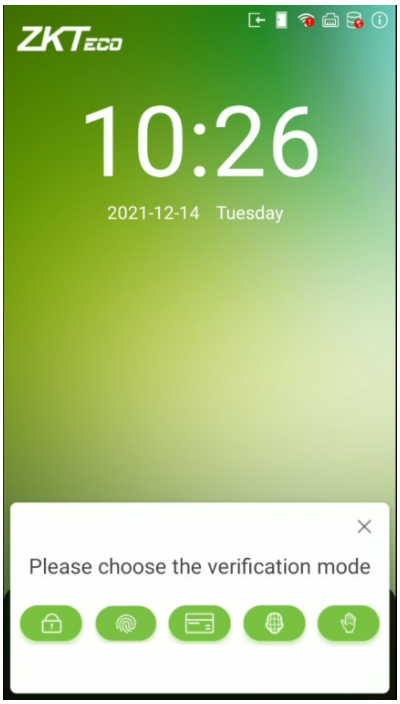


- **1:1 (One to One) Palm Verification Mode**

In this verification mode, the device compares the palm captured by the camera with the palm template related to the entered user ID. Press on the main interface and enter the 1:1 palm verification mode and enter the user ID and press **[OK]**.

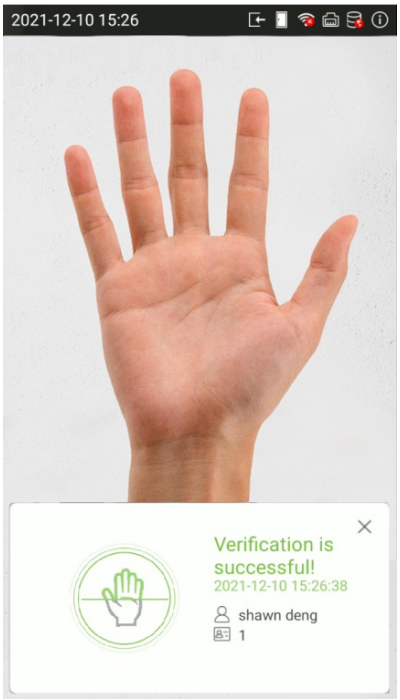


If the user has registered face, card, password and fingerprint★ in addition to palm, and the verification method is set to face/ palm/ card/ password/ fingerprint★ verification, the following screen will appear.

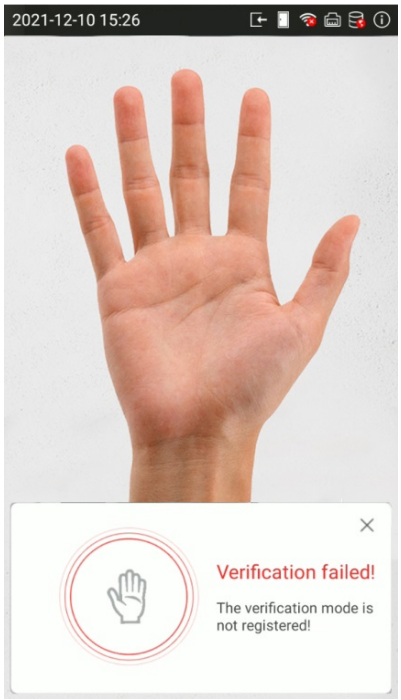


Select the icon to enter the palm verification mode. After the prompt "Please swipe your palm to verify! ", adjust your palm in the center of the device screen for palm verification.

Below are the sample for successful and unsuccessful verification:



Successful Verification



Failed Verification

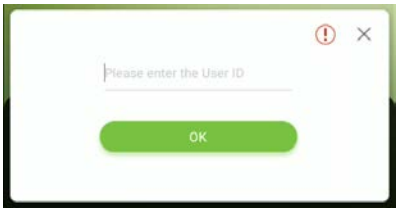
2.8.4 Card Verification

- **1: N (One to Many) Card Identification**

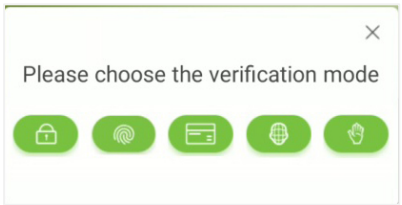
To enter 1: N card identification mode, please place the registered card on the card reader.

- **1:1 (One to One) Card Verification**

Press on the main interface and enter the 1:1 card verification mode and enter the user ID and press **[OK]**.



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



Select the icon to enter the card verification mode. After the prompt "Please swipe your card to verify ".

Below are the sample for successful and unsuccessful verification:

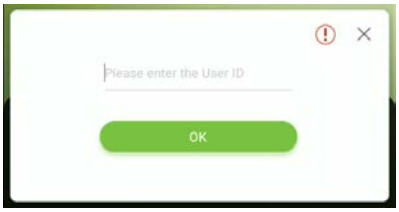
Successful Verification

Failed Verification

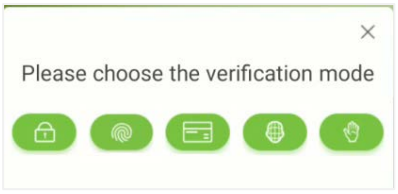
2.8.5 Password Verification

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.

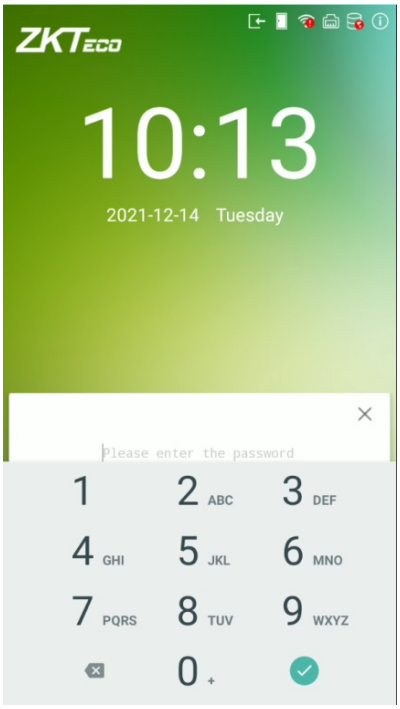
Press on the main interface and enter the 1:1 password verification mode and enter the user ID and press **[OK]**.



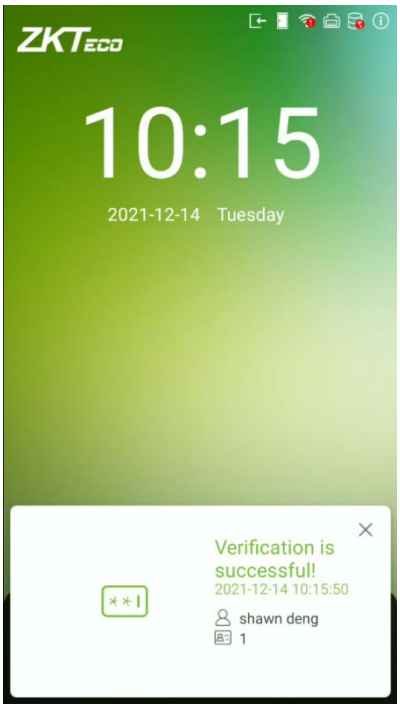
If the user has registered face, palm, card and fingerprint★ in addition to password and the verification method is set to face/ palm/ card/ password/ fingerprint★ verification, the following screen will appear.



Select the icon to enter the password verification mode. After the prompt "Please enter the password".



Below are the sample for successful and unsuccessful verification:



Successful Verification

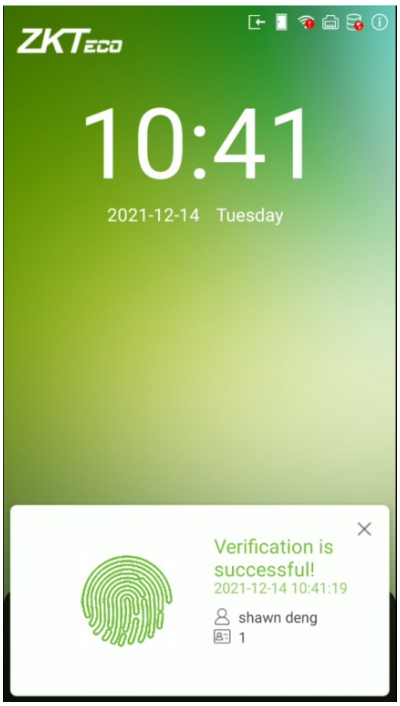
Failed Verification

2.8.6 Fingerprint Verification★

- **1: N (One to Many) 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.

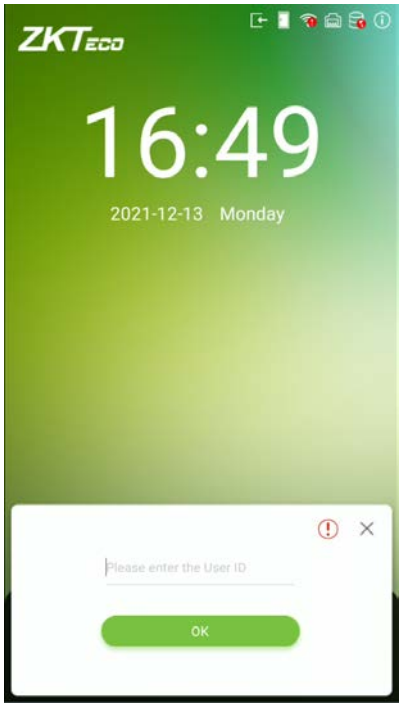
To enter fingerprint identification mode, simply tap your finger on the fingerprint reader.



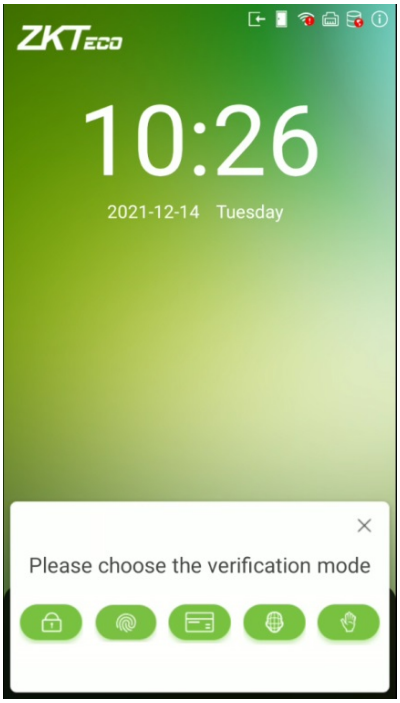
- **1:1 (One to One) Fingerprint Verification**

In this verification mode, the device compares the fingerprint that is being pressed onto the fingerprint reader with the fingerprint templates associated with the respective User ID. This method can be used when the system has trouble in recognizing the user's fingerprints.

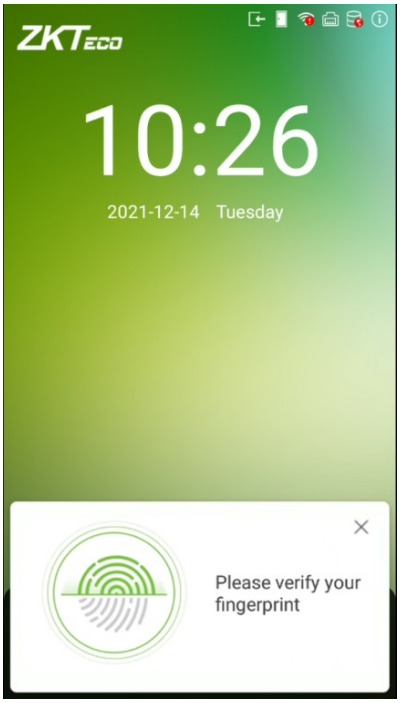
Press  on the main interface and enter the 1:1 fingerprint verification mode and enter the user ID and press **[OK]**.



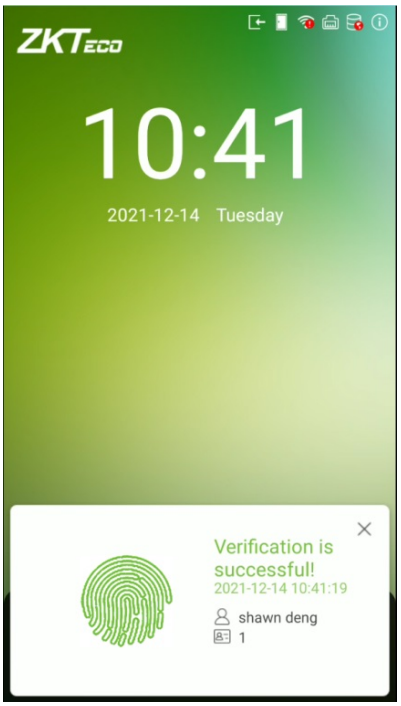
If the user has registered face, palm, password and card in addition to fingerprint and the verification method is set to face/ palm/ card/ password/ fingerprint★ verification, the following screen will appear.



Select the icon to enter the fingerprint verification mode. After the prompt "Please verify your fingerprint ".



Below are the sample for successful and unsuccessful verification:



Successful Verification

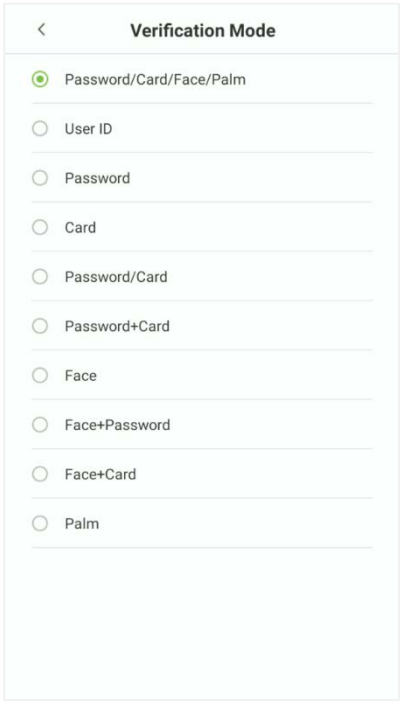
Failed Verification

2.8.7 Combined Verification

To increase security, this device offers the option of using multiple forms of verification methods. A total of 10 different verification combinations can be used, as shown below:

Combined Verification Symbol Definition

Symbol	Definition	Explanation
/	or	This method compares the entered verification of a person with the related verification template previously stored to that Personnel ID in the Device.
+	and	This method compares the entered verification of a person with all the verification template previously stored to that Personnel ID in the Device.

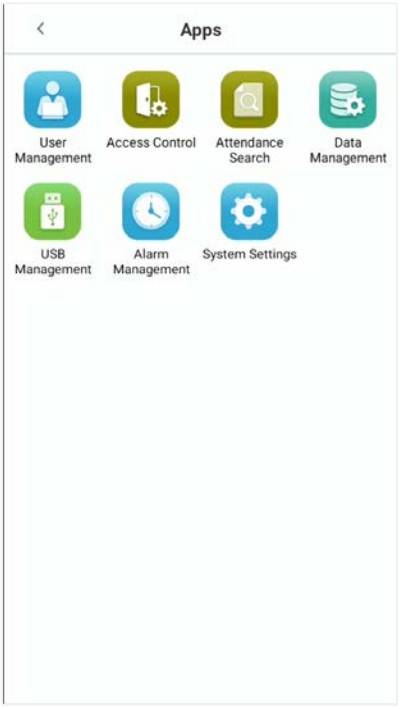


Procedure to set for Combined Verification Mode

- Combined verification requires personnel to register all the different verification method. Otherwise, employees will not be able to successfully verify the combined verification process.
- For instance, when an employee has registered only the face data, but the Device verification mode is set as "Face + Password", the employee will not be able to complete the verification process successfully.
- This is because the Device compares the face template of the person with registered verification template (both the Face and the Password) previously stored to that Personnel ID in the Device.
- But as the employee has registered only the Face but not the Password, the verification will not get completed and the Device displays "Verification Failed".

3 Main Menu

On the **Standby interface**, tap on  to enter the **Main Menu**.



Function Description

Menu	Function
User Management	To Add, Edit, View, and Delete the basic information about a User.
Access Control	To set the parameters of the lock and the relevant access control device Access control options, time rules, holiday settings, verification combination, access group settings, anti-passback and duress alarm.
Attendance Search	Query the specified attendance data, check attendance photos and blocklist photos
Data Management	To delete all the relevant data from the device.
USB Management	To upload or download specific data from a USB drive.
Alarm Management	Once an alarm has been set, the device will automatically play preselected alarm tone when the specific time is reached. It will stop alarm after the alarm time elapsed.
System Settings	To set the parameters related to the system, including network, date and time, attendance data setting, cloud service, wiegand, display and sound, serial port, biometric parameters, detection management, auto testing, advanced and security, reset to factory.

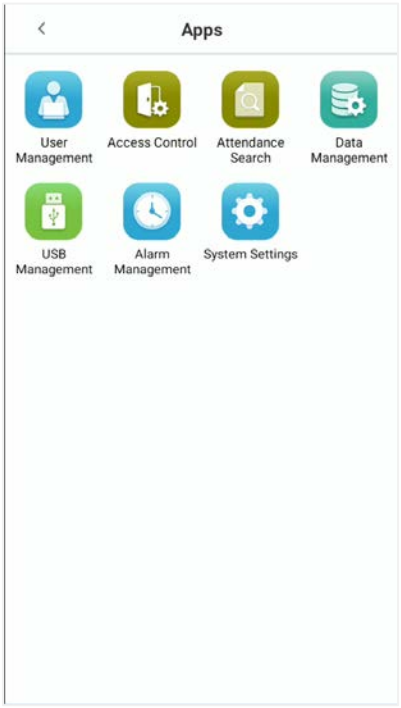
NOTE:

1. If the device does not have a super administrator, any user can enter the menu by tapping the key.
2. 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.
3. 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 Add User.

4 User Management

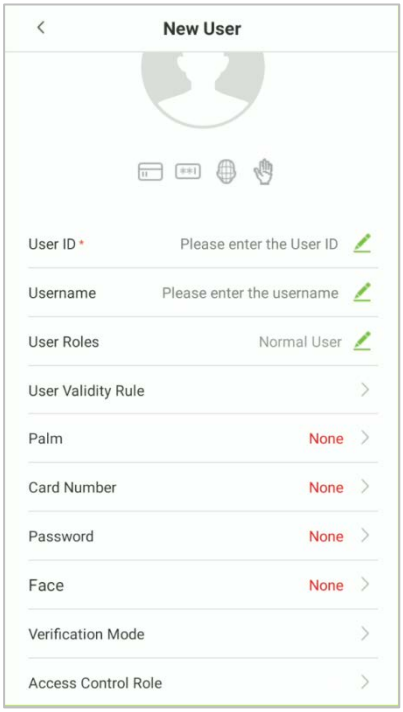
4.1 Add User

Tap on button on the **[User Management]** interface to enter the user creation interface.



Register Basic User Information

On the **New User** interface, tap **User ID** and enter the unique identification number, and then tap **Username** and enter the username.



NOTE:

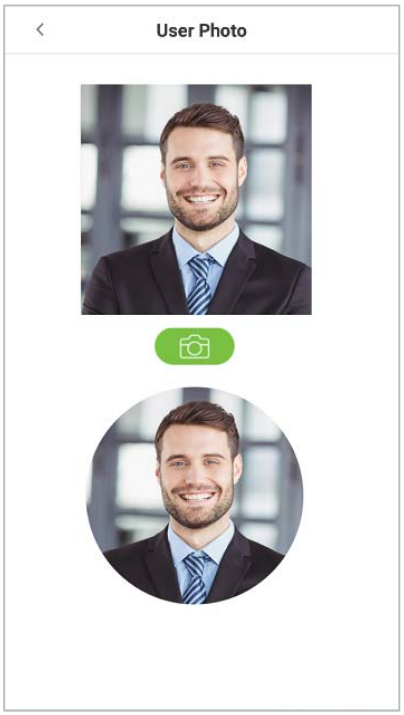
- Name: The maximum length of characters is 24.
- User ID: The user's ID can contain 1-9 digits by default.
- If you need an external reader to swipe the card, please set the card number as the id number.
- User ID can be modified before first login, but cannot be modified once logged in.
- The message "**User ID already exists, please try again**" indicates that the ID number entered is already being used. In that case, it is recommended to enter another ID number.

Register User Photo

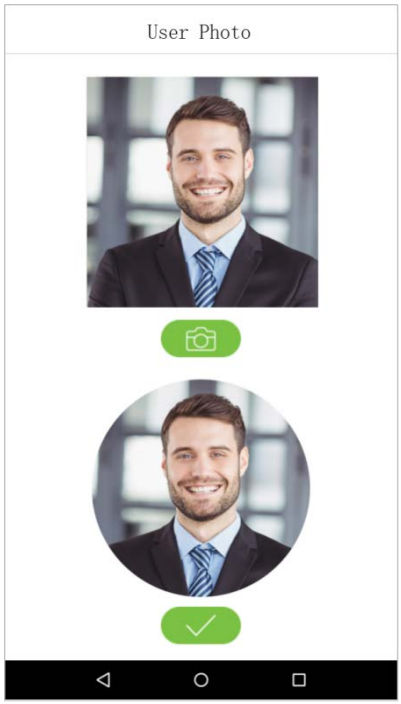
On the **New User** interface, tap on the button to enter the camera interface.

It is recommended to face the lens and then adjust the position.

On the **User Photo** interface, tap on the camera button to capture a photo.



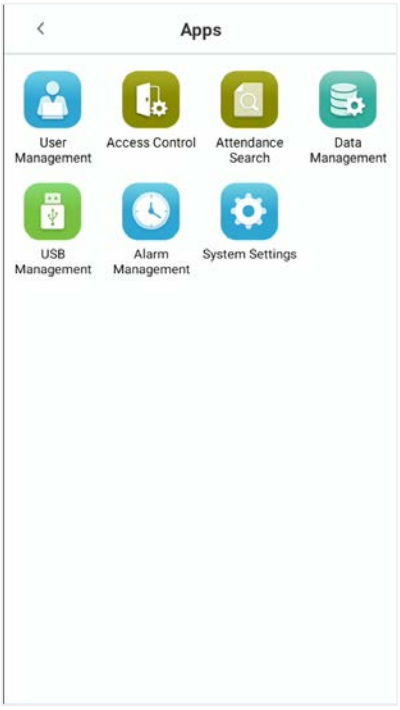
Tap on the button on the bottom to successfully add the captured photo.



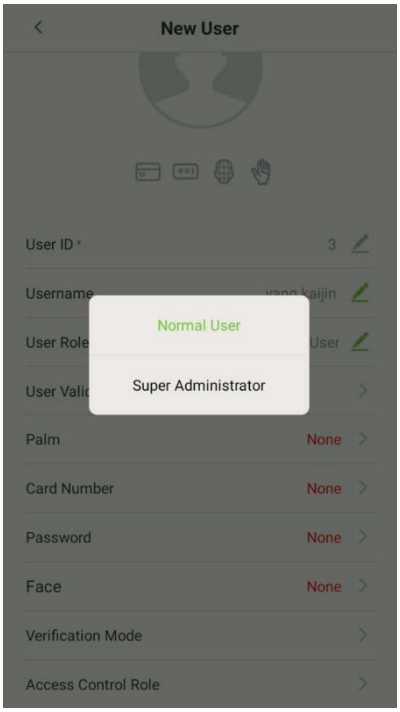
User Role

This device has two types of user privileges that is Normal User and Super Administrator. If a Super Administrator exists on the device, Normal Users can only login and view their accounts using different verification modes that have already set for the user. But a Super Administrator will have more privileges like access to the main menu and will also have the same access as the Normal user.

On the **User Management** interface, tap on the required username from the user list to set the user privilege.



On the **User Information** interface, tap **[User Roles]**, and then tap **[Normal User]** or **[Super Administrator]** to set the required privilege.



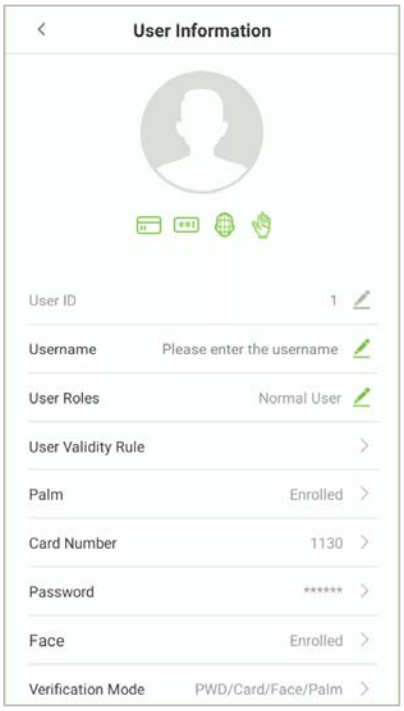
NOTE: When a user is given super administrator privileges, entering the main menu will require ID verification. The verification process depends on the verification method that was used during user registration. See the description in section "Verification Mode".

Register Verification Modes

The different verification modes are used to verify user login.

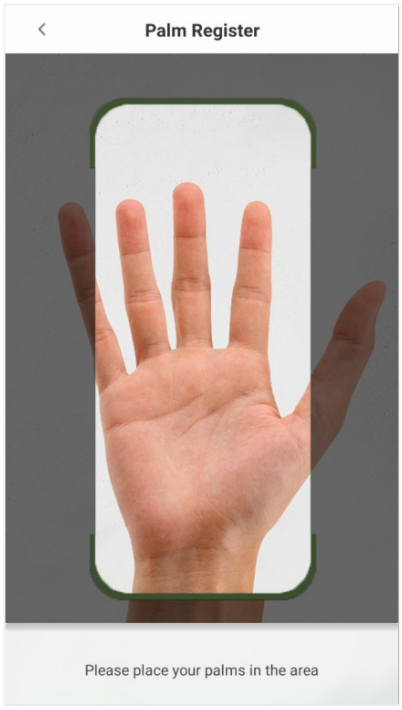
The verification mode includes registration of palm, face, password, fingerprints★, or card number of a user.

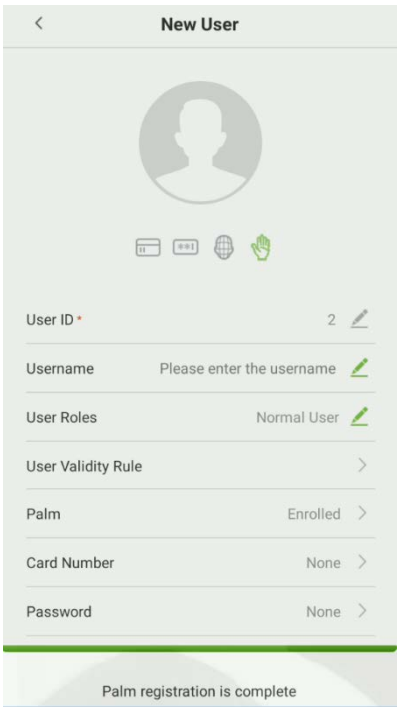
On the **New User** interface, tap on the required verification mode (Palm, Card Number, Password, Face, Fingerprint★) to register for verification.



Register Palm

On the **New User** interface, tap **[Palm]** to enter the palm registration interface.



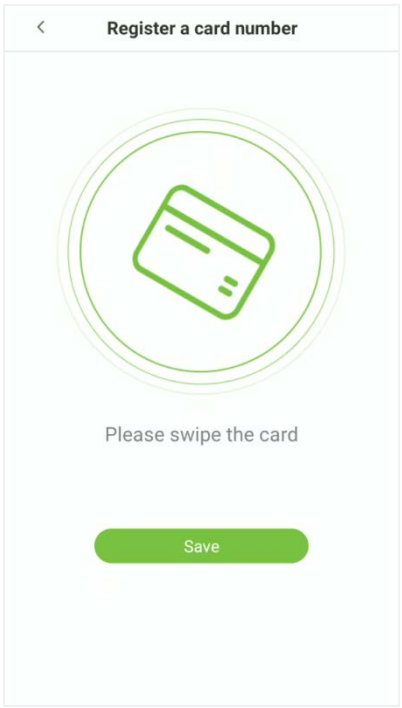


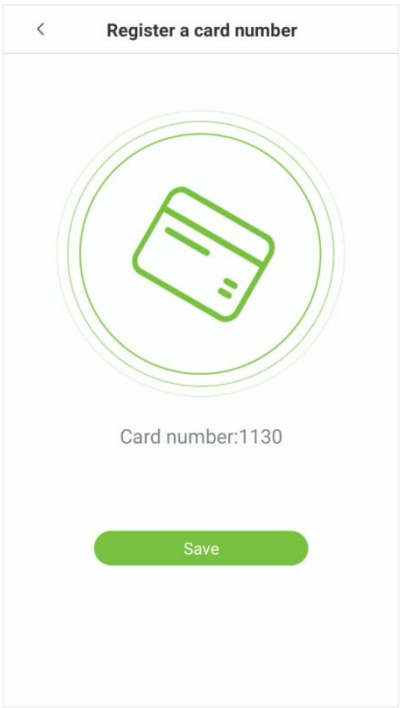
Register Card Number

On the **New User** interface, tap **Card Number** to enter the card number registration page.

On the **Register a card number** interface, swipe the card to register.

And once a successful prompt is displayed, tap **Save** to update the card details.





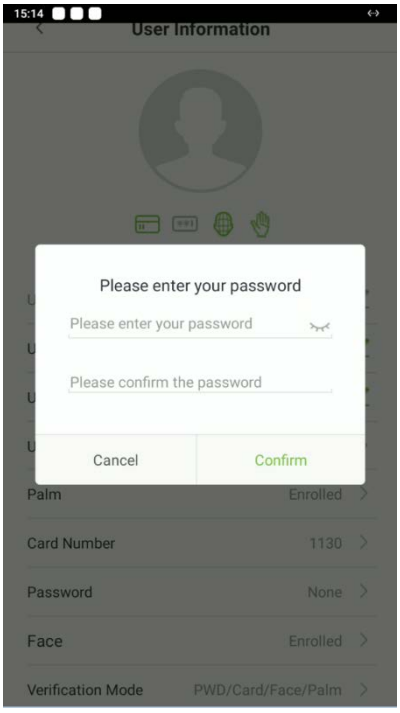
Register Password

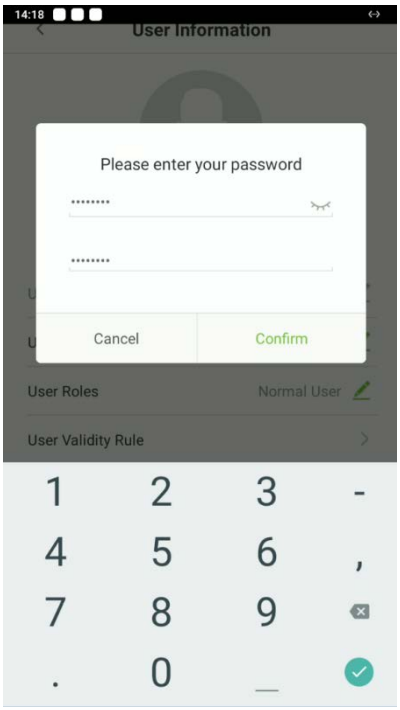
On the **New User** interface, tap **Password** to register password.

On the Enter the password field enter the password, then on the Confirm password field re-enter the same password.

Tap **Confirm**.

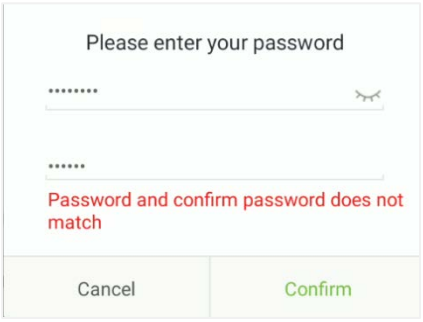
NOTE: The user password must be 8-digit number.





Function	Description
	Tap on this button to encrypt the password.
	Tap on this button to make the password visible.

If the password, entered in both fields does not match, then re-enter the correct password.

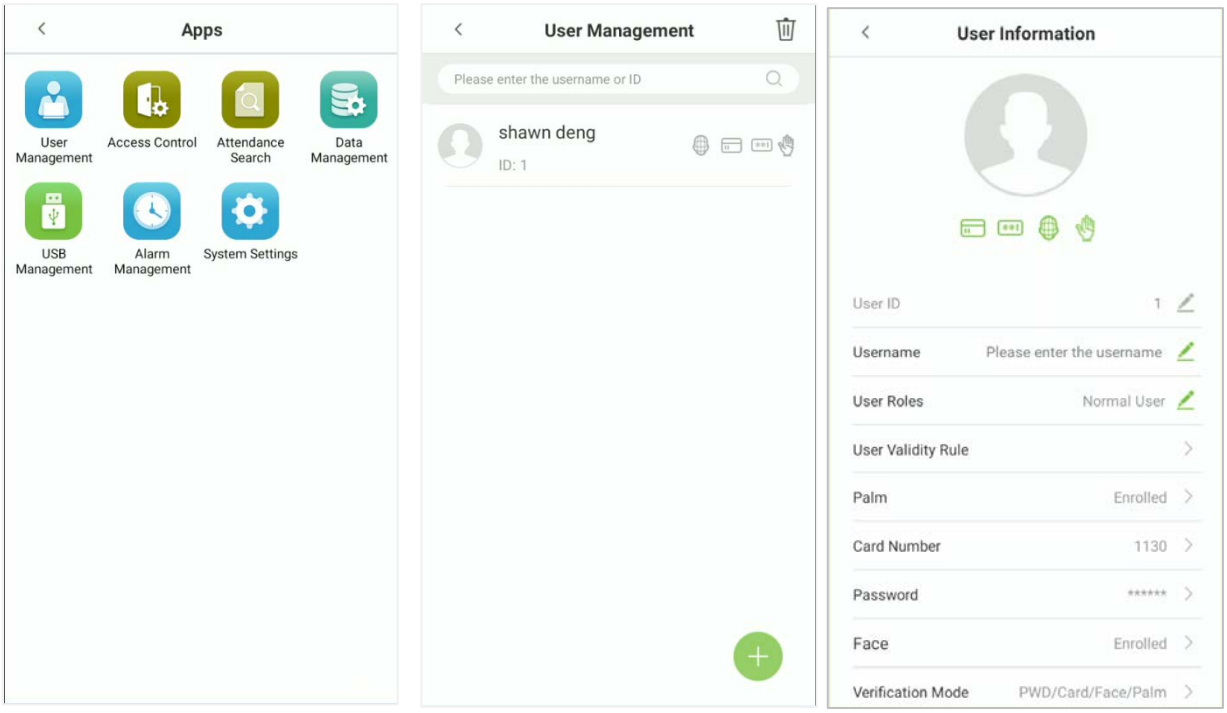


The password which has been registered can be deleted or modified.

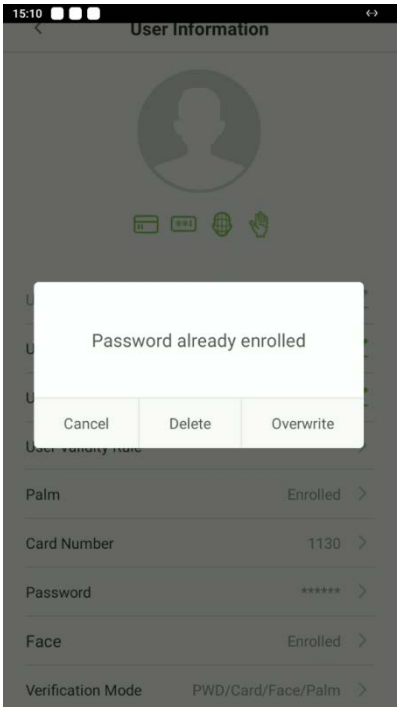
Delete/Overwrite Registered Password

On the **User management** interface, tap on the required username from the user list to delete or modify the password.

On the **User information** interface, tap **[Password]** to delete or modify.



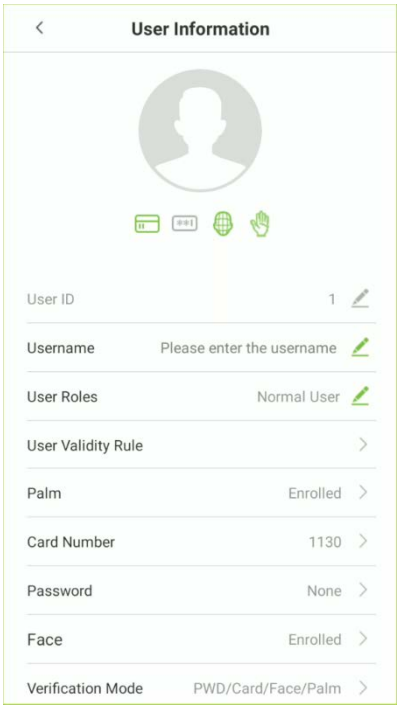
On the pop window, tap **Delete/ Overwrite** to delete or modify the password.



Register Face

On the **New User** interface, tap **Face** to enter the face registration page.

On the **Face Register** interface, move and adjust your face on the registration area.



Register Fingerprint★

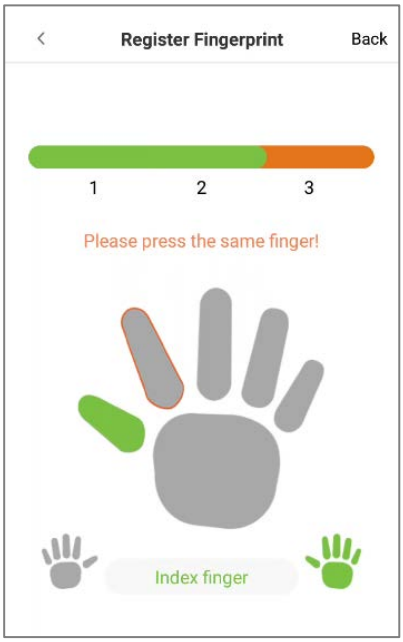
On the **New User** interface, tap **[Fingerprint]** to enter the fingerprint registration interface.

Tap on the required button (left or right) situated on the left and right side of the screen and then tap on the required finger to register.

After the selecting the required finger, press the same finger on the fingerprint reader three times.

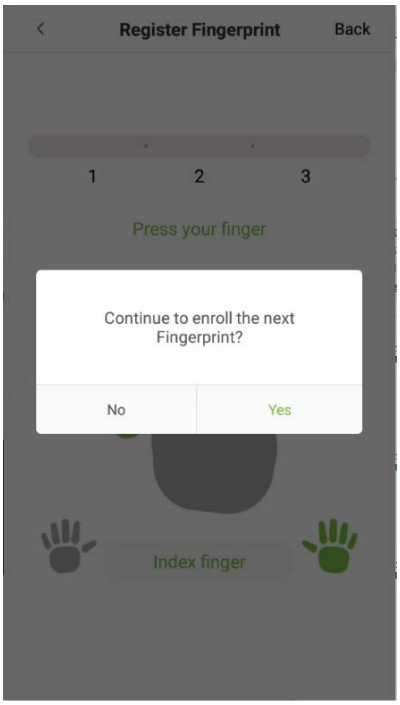
Green indicates that the fingerprint is enrolled successfully.

NOTE: If you tap different fingers onto the fingerprint scanner during the 2nd and 3rd time, the user will be prompted to "**Please use the same finger**" as shown in the below image.



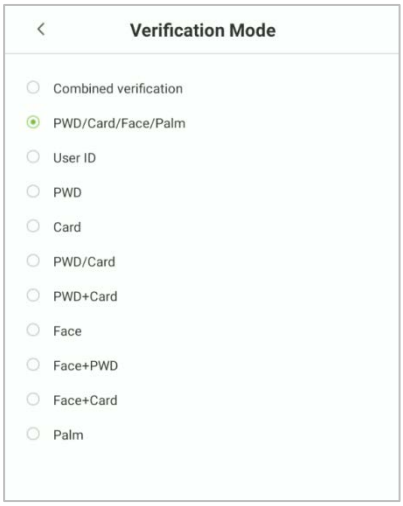
If the fingerprint is successfully registered, "**Continue to enroll the next Fingerprint?**" dialog box will appear.

Tap **Yes** to record the next fingerprint, or **No** to return to the fingerprint registration interface.



Verification Mode

Tap on the **[Verification Mode]** field on the User information interface. Select verification mode, and then tap on **[OK]**.

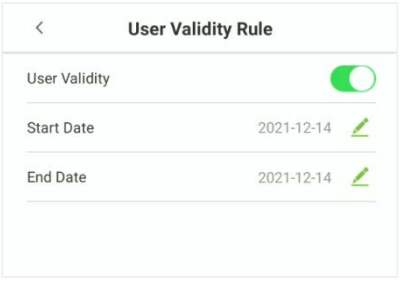


Period of Validity Settings

This function sets the validity period for an employee's verification process for attendance. So once this validity period has set, the Employee will be able to verify attendance only during this set time. And if the Employee authenticates attendance before or after the defined time, the attendance will be invalid.

The attendance verification is valid between the defined starting and ending time-period of the set number of days; this offers precision up to specific days. The validity period of a day is from 00:00 to 23:59; once this validity period expires, the employee's verification for attendance will be invalid.

On the **User Information** interface, tap **[User Validity Rule]** to set the validity period.



NOTE: If the function **User Validity Rule** is not displayed on the **New User** interface, then on the **Main** menu, tap **System Settings** > **Access control record settings**, and enable **User validity settings**, and then the function "**User Validity Rule**" will appear in the **New User** interface.

On the **User Validity Rule**, set the user validity rule by configuring the required date and time.

Access level

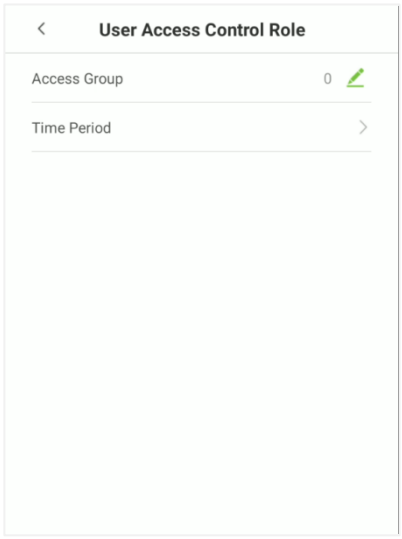
The **Access Control Role** sets the door access privilege for each user.

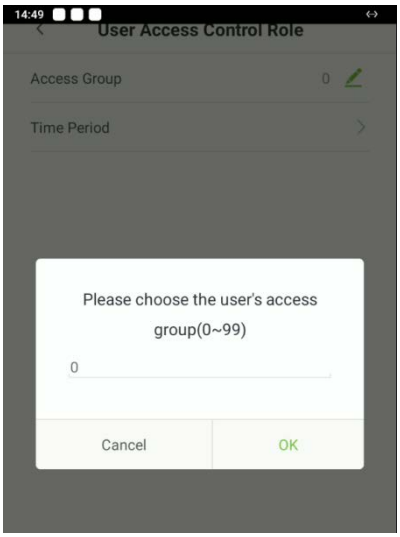
This includes the access group, and the time-period.

On the **New User** interface, tap **Access Control Role** to set the access level.

Set the Access Group

On the **User Access Control Role**, tap on **Access Group** to assign the registered users to different groups for better management.





New users will be added to Group 1 by default, which can be reassigned to other required groups.

The device supports up to 99 access control groups.

Set the Time Period

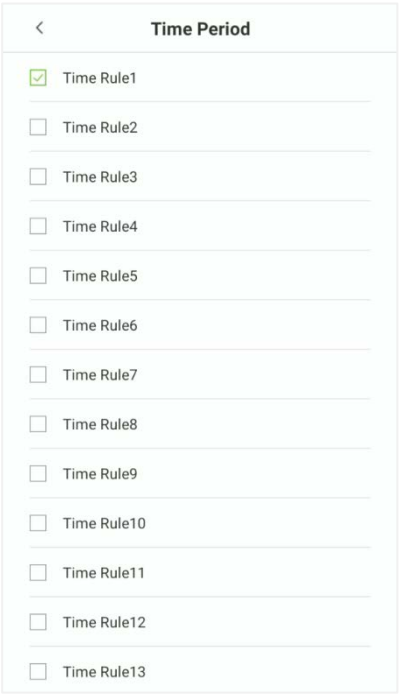
Tap **Time Period** to set the time of access for the user.

By default, users follow the defined settings of their groups.

If the time-period is not applied, the access time of the specific user should be set.

Such configuration will not affect the time settings of other group members.

NOTE: A total of 50 time-rules can be set.

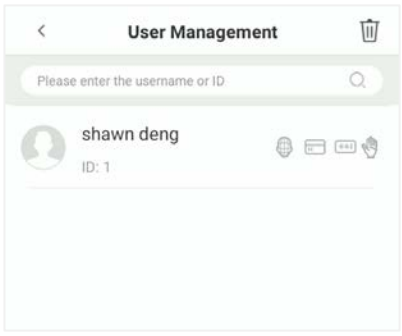


4.2 Search User

Search User function facilitates to search for the required user from the list.

Tap on the search bar located on the **[User Management]** interface and search for the required username.

NOTE: The required users can be searched based on their IDs, username, surname, or full name.

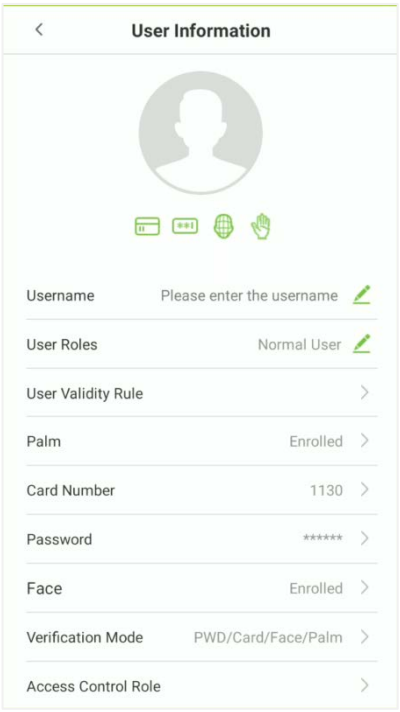


Tap on the **Search** bar to search for the users with the relevant user ID/name and the system will automatically find the users with information that is relevant to the search query.

4.3 Edit User

On the **User Management** interface, tap on the required user from the list to edit.

On the **User Information** interface, tap on the corresponding **Edit** button to edit the required user information.

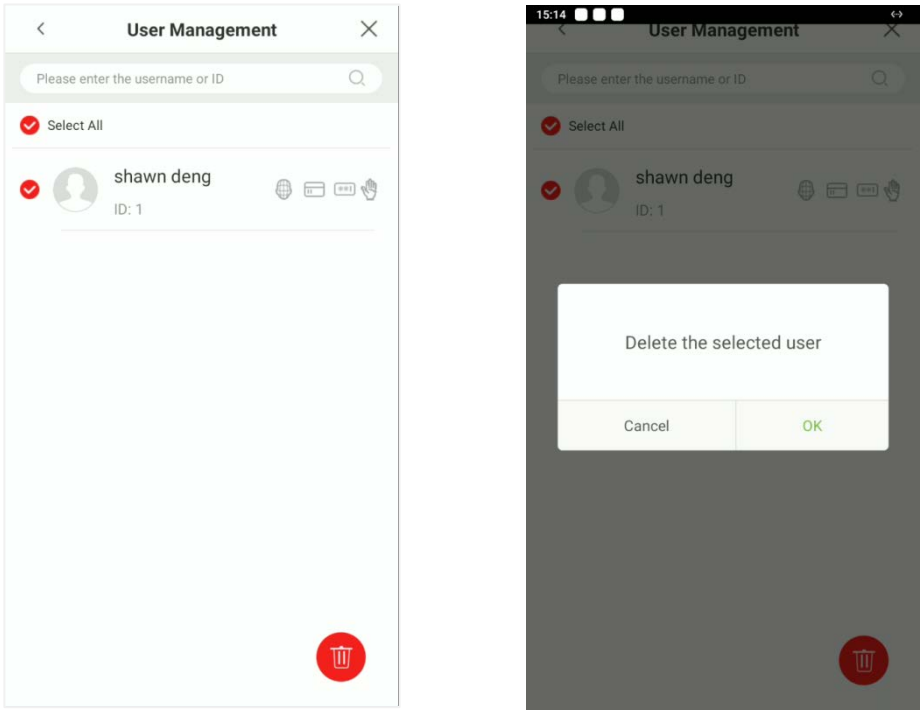


NOTE: Please notice that the user ID cannot be modified, and other operations are similar to adding a new user. For further information, please see section "Add User".

4.4 Delete User

On the "**User Management**" interface, select the required user to delete and tap on the **Delete** button to delete.

On the pop-up window, tap **OK** to confirm the deletion.



NOTE: If you are deleting the selected user, all user's related information will be cleared.

5 Access Control Settings

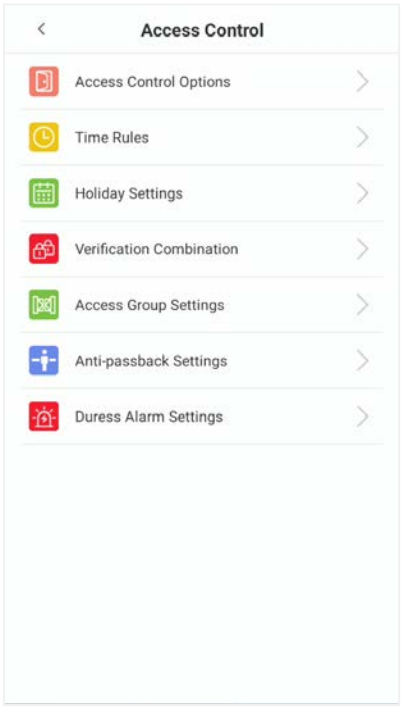
The access management allows users to set Access control parameters, Time rules, Holidays, Verification combinations, Access Groups, Anti-passback settings, Duress Settings, etc.

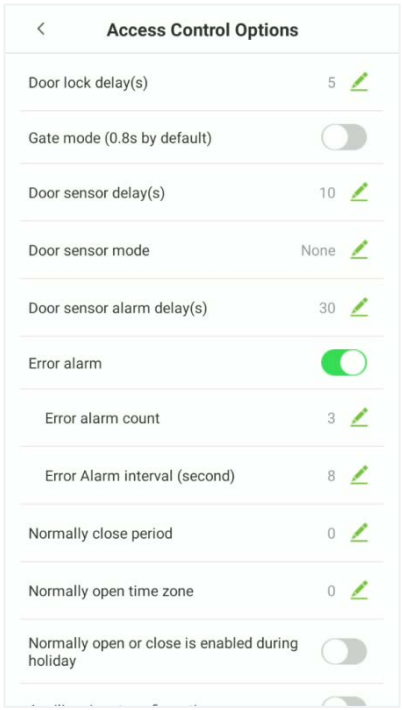
5.1 Access Control Options

Access Control Options are used for setting the access parameters.

On the **Main** menu, tap **[Access Control]**.

The **Access Control Options** includes the following functions.





Function Description

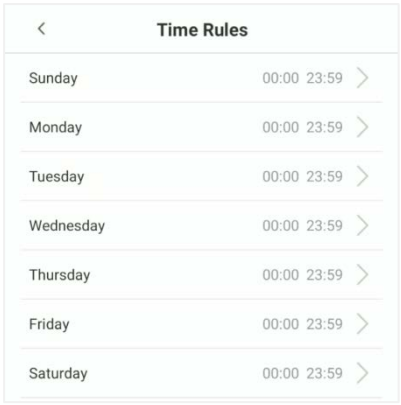
Function Name	Function Description
Door lock delay	The length of time that the device controls the electric lock to be in unlock state. Valid value: 1 to 254 seconds.
Gate mode (0.8s by default)	Toggle between **ON** or **OFF** switch to get into gate mode or not. When set to ON, on this interface will remove Door lock delay, Door sensor delay and Door sensor type options.
Door sensor delay (s)	If the door is not locked and is being left open for a certain duration (Door Sensor Delay), an alarm will be triggered. The valid value of Door Sensor Delay ranges from 1 to 255 seconds.
Door sensor mode	There are three Sensor types: None, Normal open (NO) and Normal closed (NC). **None:** It means door sensor is not in use. **Normal open (NO):** It means the door is always left opened when electric power is on. **Normal closed (NC):** It means the door is always left closed when electric power is on.
Door sensor alarm	When the state of the door sensor is inconsistent with that of the door sensor type, an alarm will be triggered after a specific time period, i.e. the

delay (s)	Door Alarm Delay. The valid value ranges from 1 to 999 seconds. 0 indicates an immediate alarm.
Error alarm	If enabled, when the number of failed verifications reaches 3 times, an alarm will be triggered.
Normally close period	Time period is scheduled for the "Normal Close" mode so that no one can gain access during this period.
Normally open Time zone	Scheduled time period for "Normal Open" mode, so that the door is always left open during this period.
Normally open or close is enabled during holiday	To set if Normal Close Period or Normal Open Period settings are valid during the holiday time period. Choose ON to enable the functions during a holiday.
Auxiliary Input Configuration	Sets the door unlock time period and auxiliary output type of the auxiliary terminal device. Auxiliary output types include None, Trigger door open, Trigger Alarm, Trigger door open and Alarm.
Alarm	The default is Off.
Local Alarm	Transmits a sound alarm or disassembly alarm from the local. When the door is closed or the verification is successful, the system will cancel the alarm from the local.
External Alarm	The default is Off.
Reset access settings	The restored access control parameters include door lock delay, door sensor delay, door sensor mode, normally close period, normally open time zone, auxiliary input configuration and alarm. However, the access control data in Data Mgt. is excluded.

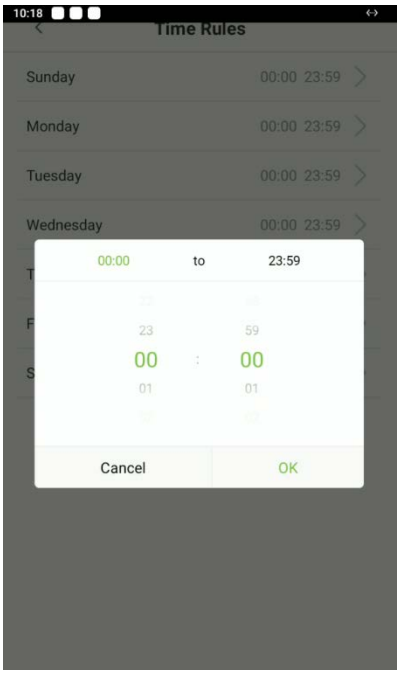
5.2 Time Rules Settings

Time Rule is the minimum time unit of access control settings and a maximum of 50 **Time Rules** can be set for the system. Each **Time Rule** consists of 7 time periods (a week) and 3 holiday time schedules, and each time section is valid for 24 hours.

The user may set a maximum of 3 time periods for every time rule. The relationship among these time periods is "or". When the verification time falls in any one of these time periods, the verification is valid. The time period format is HH:MM-HH:MM in the 24-hour system with precision to minute.



Tap the date on which time rule settings is required. Set the starting and ending time, and then press **[OK]**.



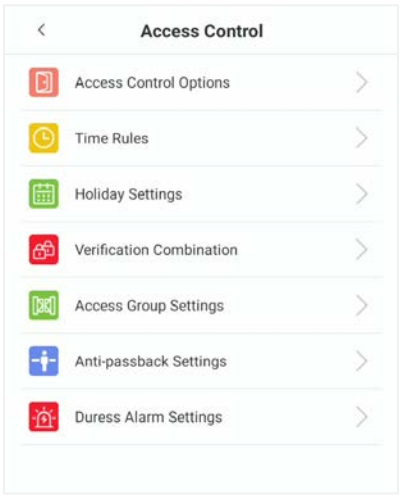
NOTE:

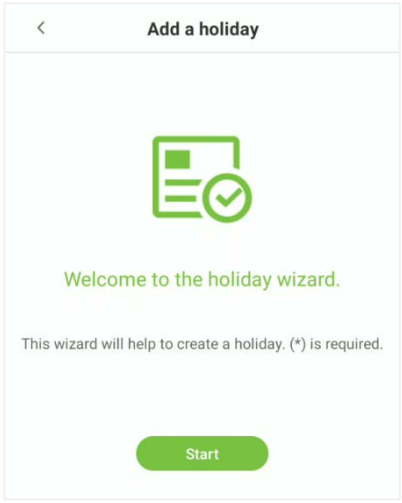
- When the End Time is earlier than the Start Time, (such as 23:57~23:56), it indicates that access is prohibited all day.
- When the End Time is later than the Start Time, (such as 00:00~23:59), it indicates that the interval is valid.
- The effective Time Period to keep the Door unlock or open all day is (00:00~23:59) and also when the End Time is later than the Start Time, (such as 08:00~23:59).
- The default Time Zone 1 indicates that door is open all day long and it cannot be edited.

5.3 Holiday Settings

Whenever there is a holiday, the user may need a special access time; but changing everyone's access time one by one is extremely cumbersome, so you can set a holiday access time which is applicable to all the users, and the user will be able to open the door during the holidays. The time period set here is taken as the standard.

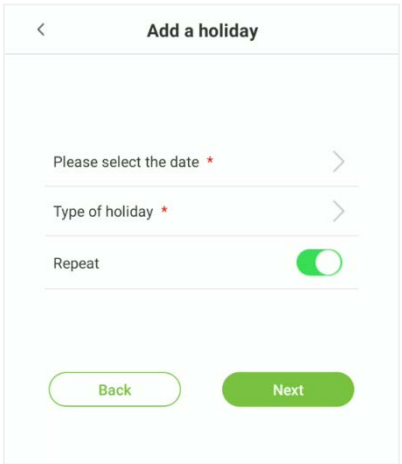
Tap **[Holiday Settings]** and then tap on the button to create a new holiday.

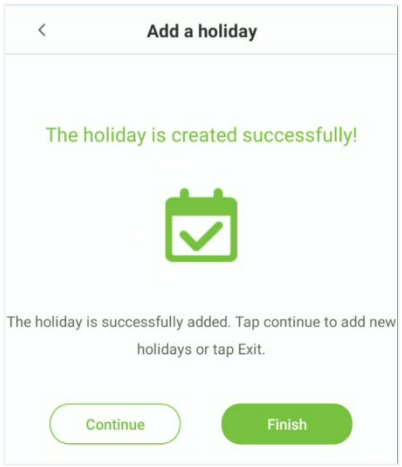


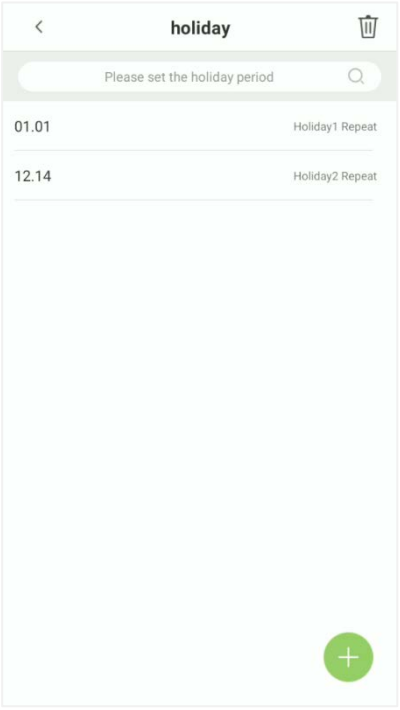


On the **[Holiday Settings]** interface, select a date and type of the holiday. Enable **[Repeat]** to repeat the holiday yearly and then tap **[Next]**.

On this interface, tap either **Finish** to successfully add the newly created holiday, or tap **Continue** to create another holiday.







Edit Holiday

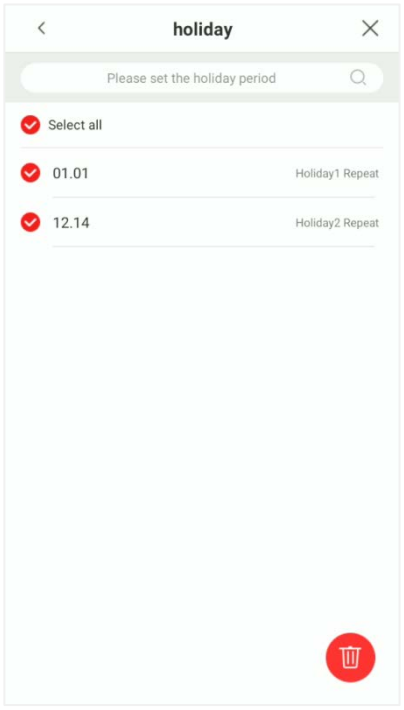
On the "**holiday**" interface, tap on the required holiday to modify.

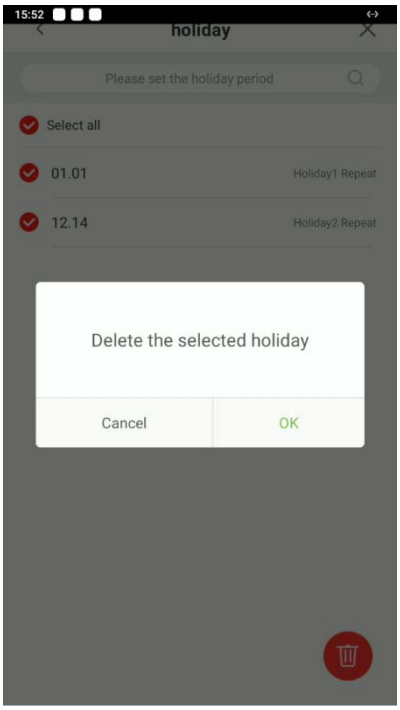
Delete a holiday

On the **holiday** interface, tap on the button to delete the holiday.

Select the holiday which you would like to delete, tap on the button in the lower right corner.

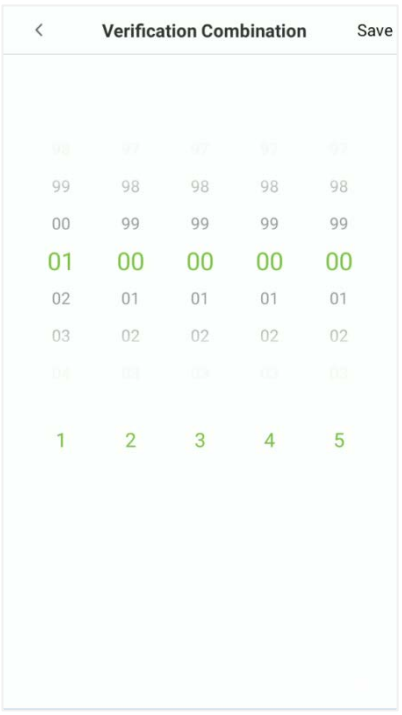
On the pop-up window, tap **OK** to confirm deletion.





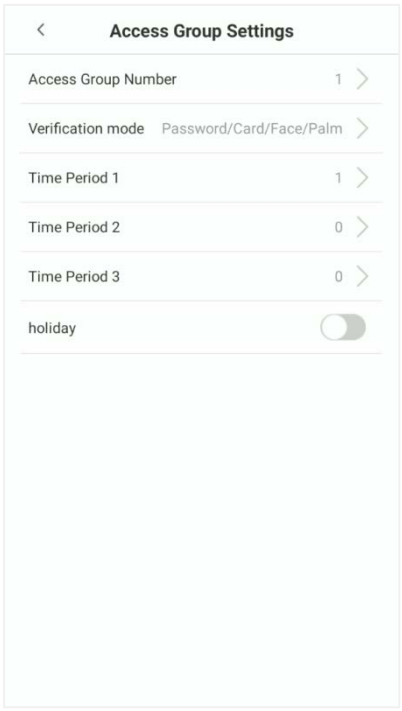
5.4 Verification Combination

Verification Combination function refers to a function that requires any member in different access control groups or multiple members in the same access control group to verify in turn (without sequence) within a certain period of time (the interval is 8 seconds), and then the door can be opened. It is mainly used in some special occasions with relatively high requirements. There can be a maximum of 5 personnel in each group, and a maximum of 10 groups can be set. The interface is as follows:



5.5 Access Group Settings

The Access Control group setting is used to create an Access Group and configure Time Period as per the requirements. For the newly created access control group, the Verification mode, Time period and Holiday can be set accordingly. The interface is given below:



5.6 Anti-passback Setup

Anti-passback is a directional-control method used to control the misuse of an access control system. This feature involves a specific sequence where the access control devices must be mounted both inside and outside the door for access.

So, if any personnel enter an access-controlled area following another person without authenticating on the biometric device, then the next time during his out-time, the door does not open when that person attempts to leave the area. This function uses to detect whether the user's access is legal by determining the user's last access record and the local control direction, which can effectively prevent tailgating.

The Anti-passback setup can be divided into three types:

No Anti-passback: Anti-passback function is disabled, which means successful verification through either the master device or slave device can unlock the door. The attendance state is not saved in this option.

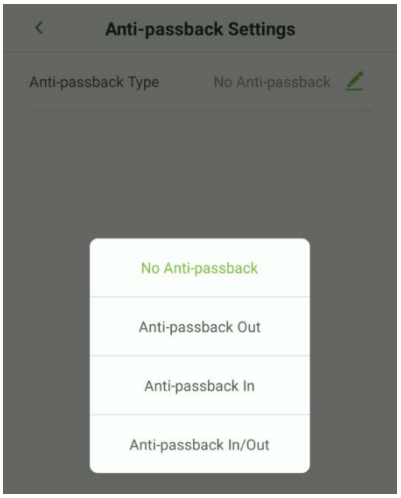
Anti-passback Out: After a user checks out, only if the last record is a check-in record, the user can check-out again; otherwise, the alarm will be triggered. However, the user can check-in freely.

Anti-passback In: After a user checks in, only if the last record is a check-out record, the user can check-in again; otherwise, the alarm will be triggered. However, the user can check-out freely.

Anti-passback In/Out: After a user checks in/out, only if the last record is a check-out record, the user can check-in again; or if it is a check-in record, the user can check-out again; otherwise, the alarm will be triggered.

NOTE: When the user has no record during the first verification, the anti-passback approval is passed directly. This access direction depends on the selection of the control direction of the device, corresponding to the state of the device.

The interface is shown below:



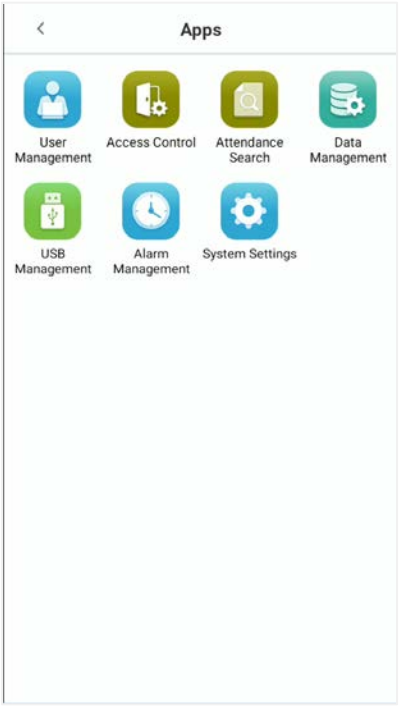
5.7 Duress Alarm Settings

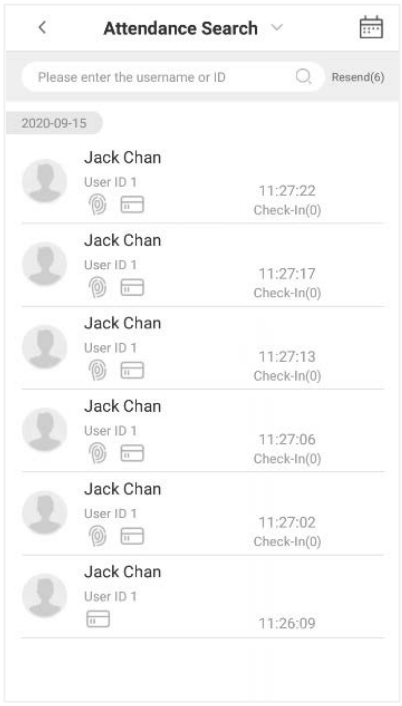
Duress alarm refers to the alarm when the specified user verifies the duress fingerprint and duress password in an emergency After using the duress fingerprint and duress password, the alarm will be delayed according to the alarm delay parameters to achieve the purpose of duress alarm. The specific parameter setting interface is as follows:

6 Attendance Search

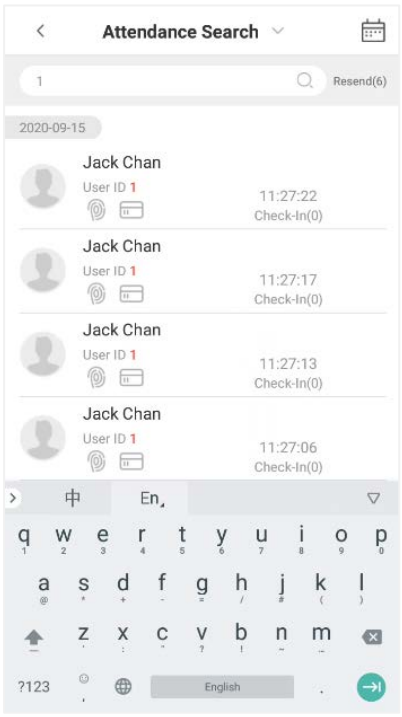
The user's attendance records will be saved in the device, making it easier to find users' attendance records. The users can search for Attendance Logs and Visitor photos.

On the **Main** menu, tap **Attendance Search**, to search for required user's attendance record.

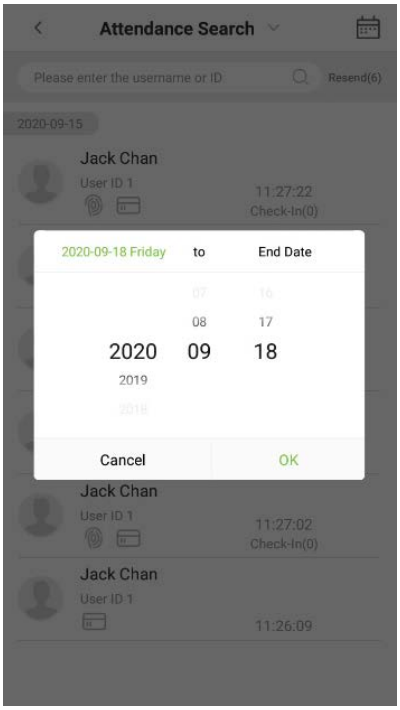




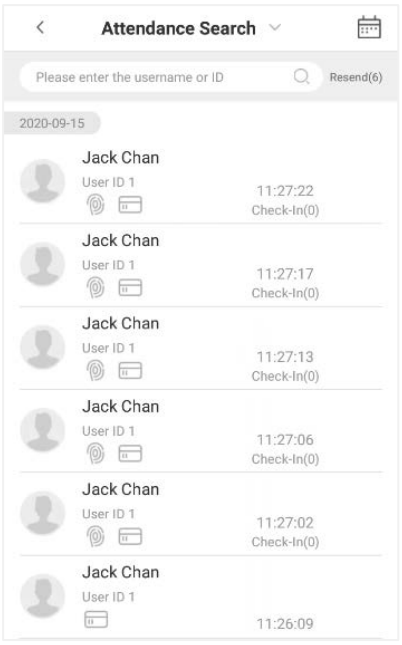
1. Enter the query conditions such as the User ID, First or Last name of an employee in the search bar. Automatically the system displays the users with information that is relevant to the search query.



2. Tap on the icon to access the following window where you can select the **[Starting Date]** and **[Ending Date]** to search the records.
3. After setting the Start and End date, tap on **[OK]**.



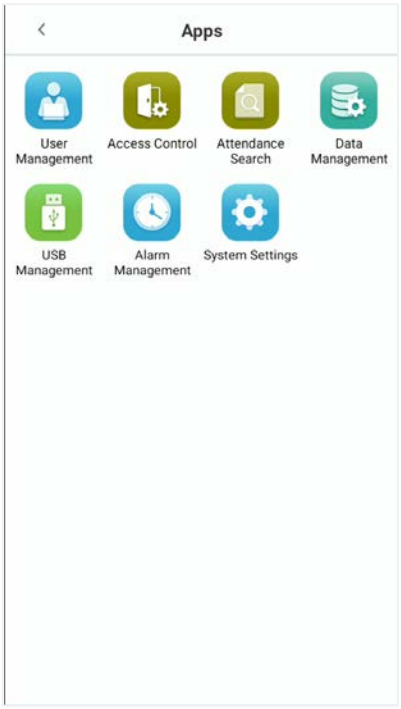
4. The search results will be displayed as shown below:

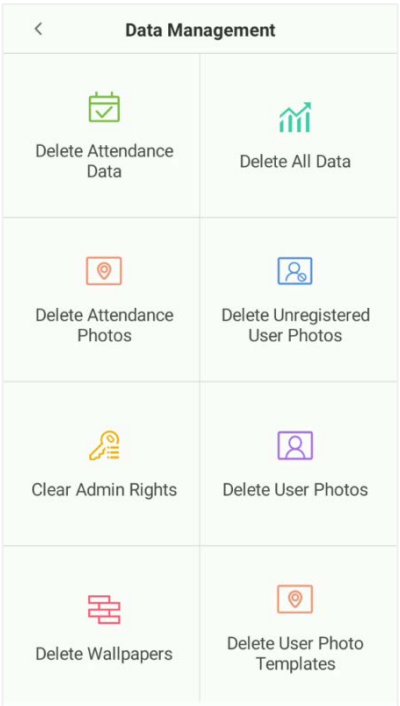


7 Data Management

The Data Management Settings allows the users to manage the device data, including Delete Attendance data, Delete All Data, Delete Attendance Photos, Delete Unregistered User Photos, Clear Admin Rights, Delete User Photos, Delete Wallpapers and Delete User Photo Templates.

On the **Main** menu, tap on **Data Management** to manage the data.





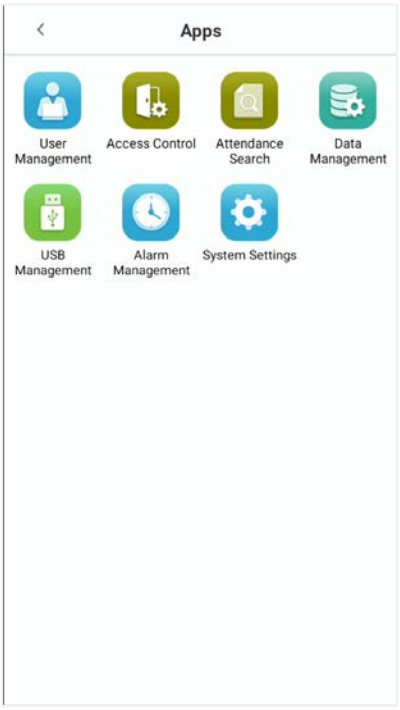
Function Description

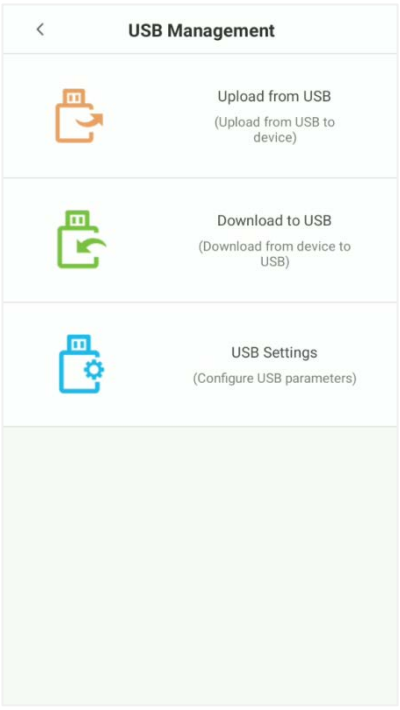
Function Name	Function Description
Delete Attendance Data	1. Deletes all the attendance data. 2. Deletes the attendance data within a specified time range.
Delete All Data	Deletes the business data stored in the device, including attendance data, password/facial/palm/fingerprint★/card biometric data, privileges of the super admin, user photos, user data, and access control data.
Delete Attendance Photos	Deletes all the logs. Deletes invalid user accounts Deletes the attendance photos within a specified time range.
Delete Unregistered User Photos	1. Deletes all (including attendance records and the photos of the user in blocklist) 2. Deletes the unregistered user photo within specified time range.
Clear Admin Rights	Changes the super administrator into a normal user.
Delete User Photos	Deletes all the user photos.
Delete Wallpapers	Deletes all the wallpapers stored in the device.
Delete User Photo Templates	Deletes the face templates in the device.

8 USB Management

The specific functions of the USB management interface are USB disk upload, USB disk download and USB disk settings.

On the **Main** menu, tap **USB Management** to manage the USB settings





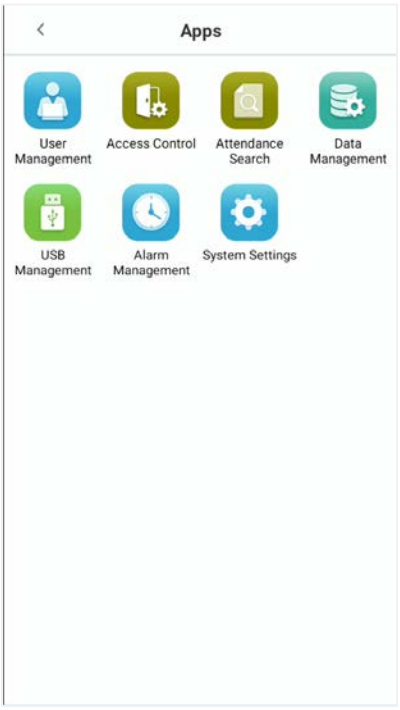
Function Description

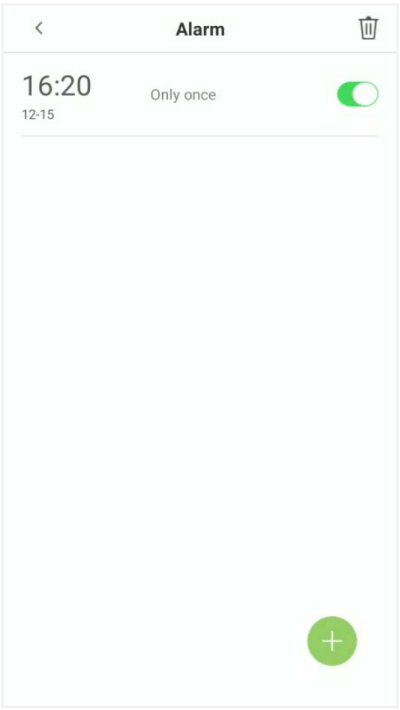
Function Name	Function Description
Upload from USB	Upload USB disk content to the device.
Download to USB	Download the data from the device to the USB disk.
USB Settings	Configure the parameters of USB disk.

9 Alarm Management

Once an alarm has been set, the device will automatically play the preselected alarm tone when the set alarm time is reached. It will stop ringing once the set time is elapsed.

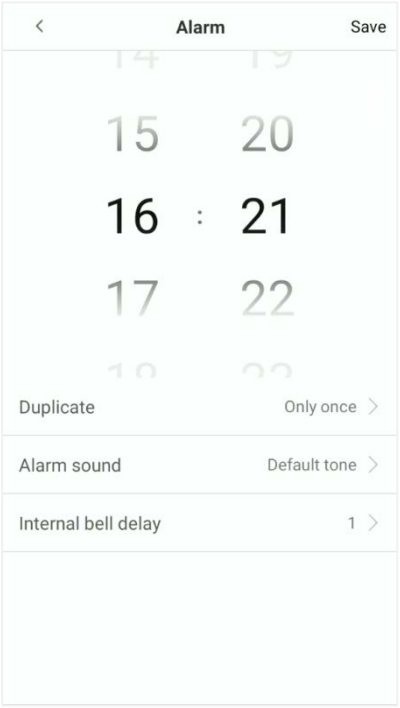
On the **Main** menu, tap **Alarm Management** to configure the alarm settings.





9.1 Add Alarm

On the **Alarm** interface, tap on the button to set the alarm, and then tap **Save** to save and update.



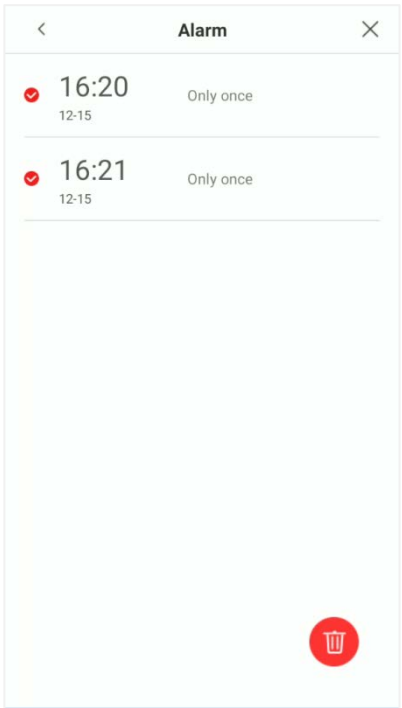
Function Description

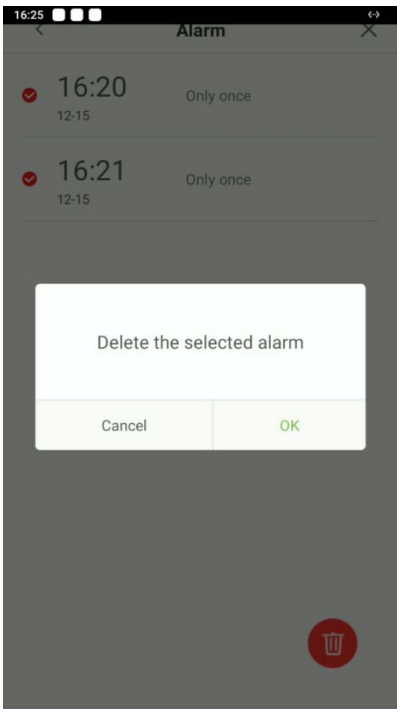
Function Name	Function Description
Duplicate	Set the required number of counts to repeat the scheduled bell.
Alarm sound	Select a ring tone.
Internal bell delay	Set the replay time of the internal bell. Valid values range from 1 to 999 seconds.

9.2 Delete Alarm

On the **Alarm** interface, tap on the delete button, then select the required alarm clock to delete.

And then tap on button that is displaying in the lower-right corner of the screen.

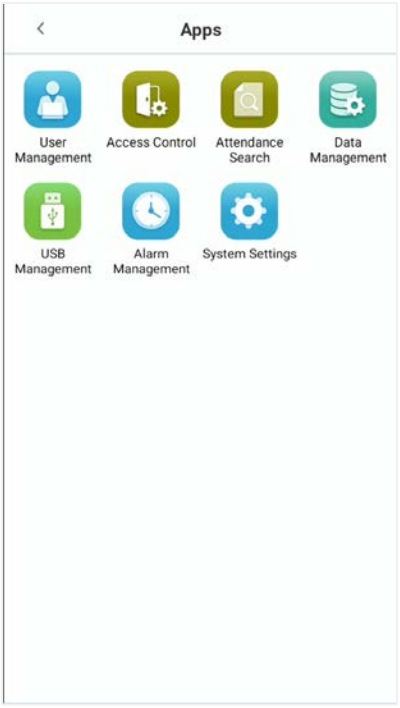


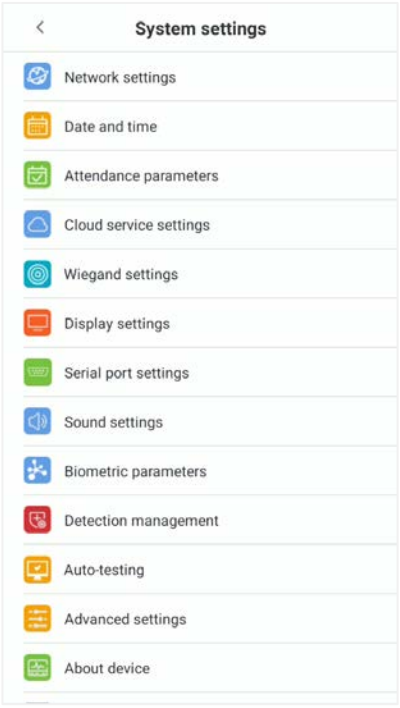


10 System Settings

System Settings are used for setting system parameters to maximize the device's ability as per the user requirements. In this interface, user can edit Network settings, Date and time, Attendance parameters, Cloud service settings, Wiegand settings, Display and Sound, Serial port, Biometric parameters, Detection management etc.

On the **Main** menu, tap **[System settings]** to configure the device settings.



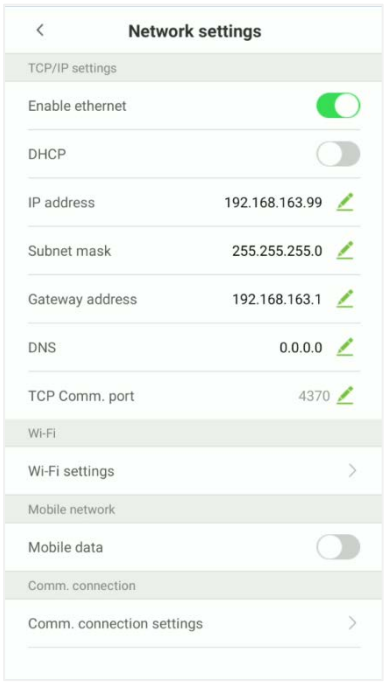


10.1 Network Settings

On the **System settings** interface, tap **[Network settings]** to configure the settings

10.1.1 Ethernet Settings

When the device communicates with a PC via Ethernet, the network must be set up to make the device and the computer in the same network segment. When the device is not connected to the network, tap **[TCP/IP settings]** on the **Network settings** interface. The following screen will display:



Function Description

Function Name	Function Description
Enable ethernet	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. If DHCP is on, you cannot manually set the IP of the device.
IP Address	The default IP is 0.0.0.0 (can be changed).
Subnet mask	The default IP is 0.0.0.0 (can be changed).
Gateway address	The default IP is 0.0.0.0 (can be changed).
DNS	The default IP is 0.0.0.0 (can be changed).
TCP COMM. port	The default TCP port is 4370 (can be changed).

NOTE: When the device is not connected to the network, the parameters such as IP address and subnet mask are 0.0.0.0; when the device is connected to the network, the parameters such as IP address and subnet mask are automatically displayed as set values.

10.1.2 Wi-Fi Settings

The device provides a Wi-Fi module, which can be built-in within the device mould or can be externally connected.

The Wi-Fi module enables data transmission via Wi-Fi (Wireless Fidelity) and establishes a wireless network environment. Wi-Fi is enabled by default in the device. If you don't need to use the Wi-Fi network, you can toggle the Wi-Fi to disable button.

Tap **[Wi-Fi settings]** on the **Network settings** interface. The following screen will display:

- Wi-Fi is disenabled in the Device by default. Toggle on button to enable or disable Wi-Fi.
- Once the Wi-Fi is turned on, the device will search for the available Wi-Fi within the network range.
- Tap on the appropriate Wi-Fi name from the available list, and input the correct password in the password interface, and then tap Connect to Wi-Fi I (**Save**).

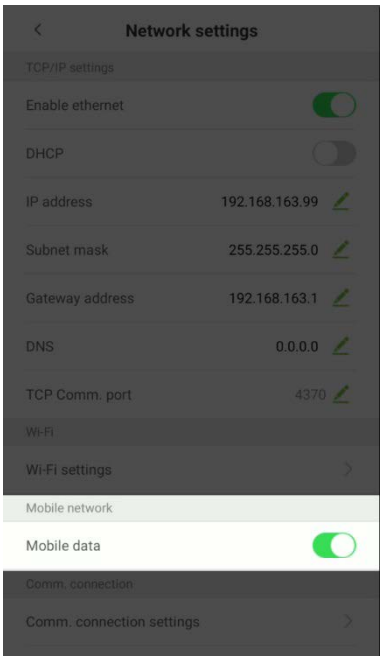
When the Wi-Fi is connected successfully, prompt "Successfully save!" display on the Wi-Fi list, and the initial interface will display the Wi-Fi logo.

10.1.3 Mobile Network Settings

When the device is applied to a dial-up network, make sure that the device is within the signal coverage of the mobile operator (GPRS/4G).

Please insert the IOT card into the 4G module before enabling. Then tap on **[Mobile data]** to enable or disable mobile network in the **Network settings** interface.

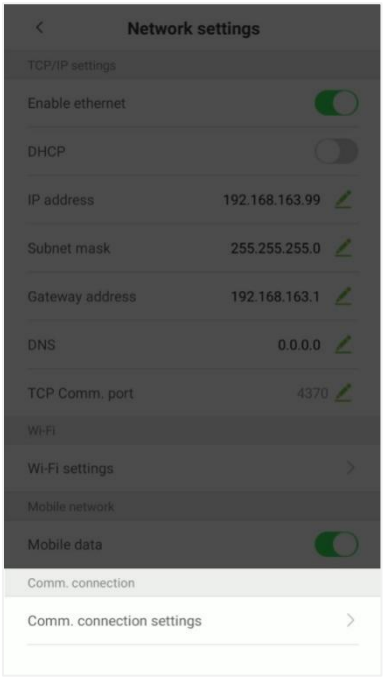
Once turned on, the device is automatically connected.



10.1.4 Comm. Connection Settings

To develop the security and confidentiality of the access data, you need to set a connection password. For a successful connection between the PC software and the device, the connection password must be accurate.

On the **Network settings** interface, tap on **Comm. connection settings**.



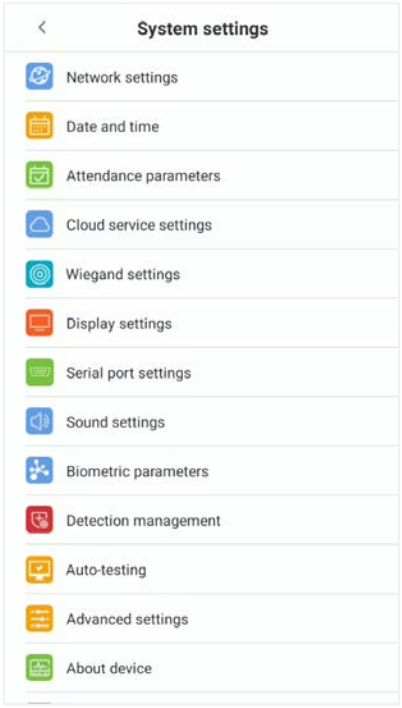
Function Description

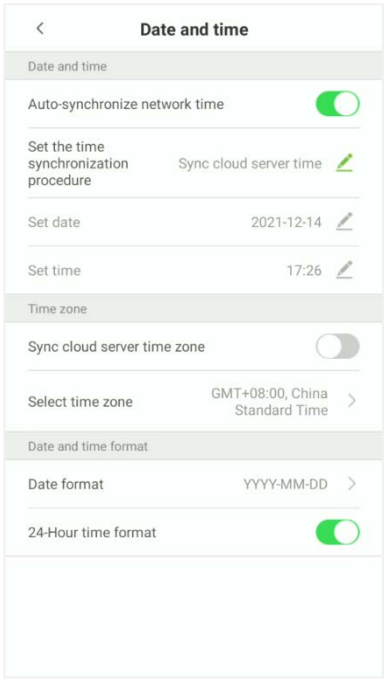
Function Name	Function Description
PC Communication password	It is used to gain the connection permission when using offline SDK or PULL SDK connection. If the password is not correct, the communication connection cannot be built. The value ranges from 0 to 999999. When the value is 0, there is no code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

10.2 Date and Time

10.2.1 Date and Time Settings

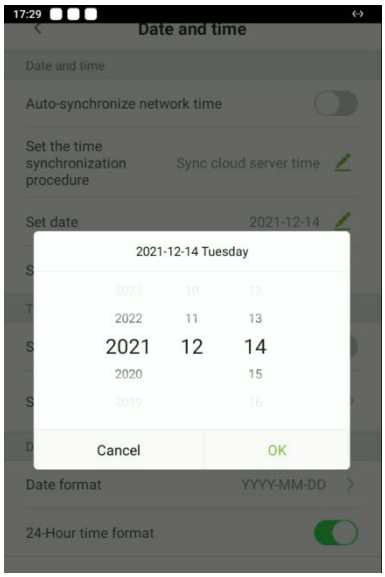
On the **System settings** interface, tap **Date and time** to enter the date and time settings interface.





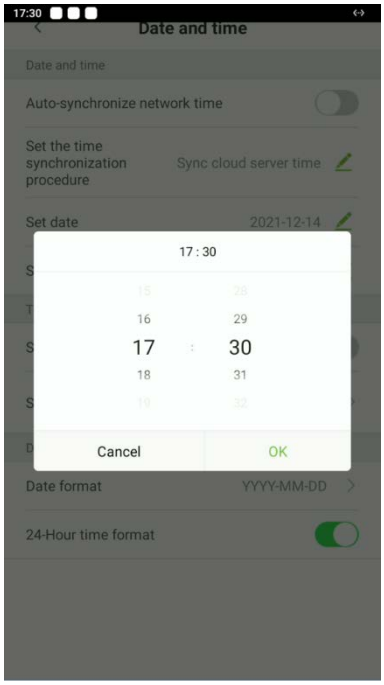
Tap **Set date** and swipe up and down to set the year, month, and day.

After setting required Date, tap **OK**.



Tap **Set time** and swipe up and down to set the hour and minute.

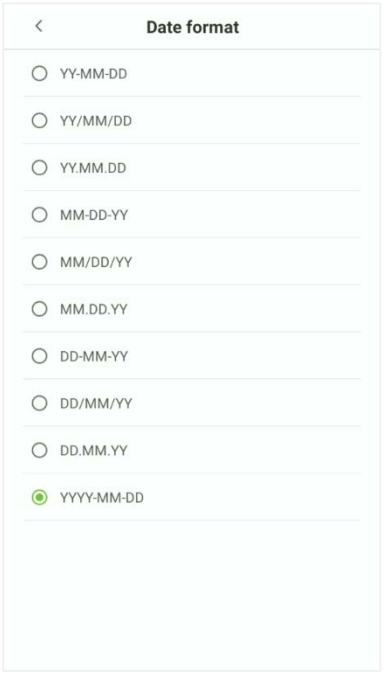
After setting time, tap **OK**.



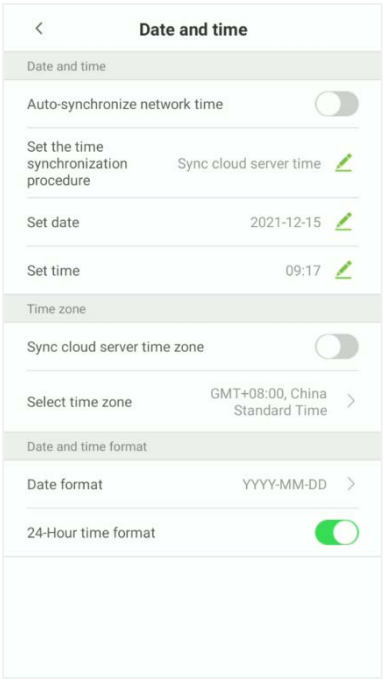
10.2.2 Date and Time Format Settings

On **Date and time** interface, tap **Date format**.

On **Date format** interface, select a required date format.



On Date and time interface, tap **24-Hour time format** option to enable this function.



Function Descriptions

Function Name	Function Description
Auto-synchronize network time	It is enabled by default. Users can modify the time synchronization source. After disable, users can modify the time synchronization procedure, and set the date and time.
Sync cloud server time	It is used for synchronizing the time between the software and server to which the device is connected.
Sync network time	It is used for synchronizing the actual time of the internet.
Sync cloud server time zone	This option is enabled by default and used for synchronizing the time zone issued by the software.
Select time zone	The default time zone is GMT + 8: 00, China Standard Time. Users can select time zone as per their requirements.

10.3 Attendance Parameters

On the **System settings** interface, tap on **Attendance parameters** to enter the attendance record settings interface.

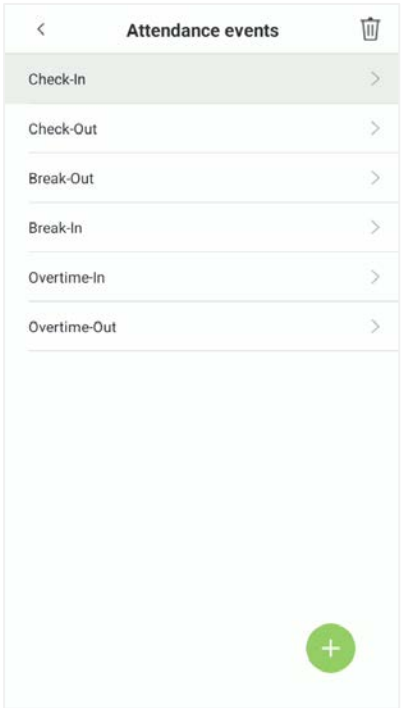
10.3.1 Attendance Events

Attendance Events are used to record the 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.

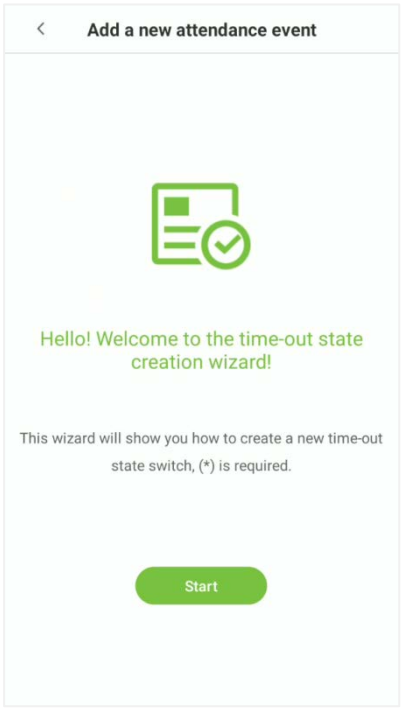
Add Attendance Events

Tap on **[Attendance events]**.

1. On the **Attendance Events** interface, tap on to open the attendance event interface.

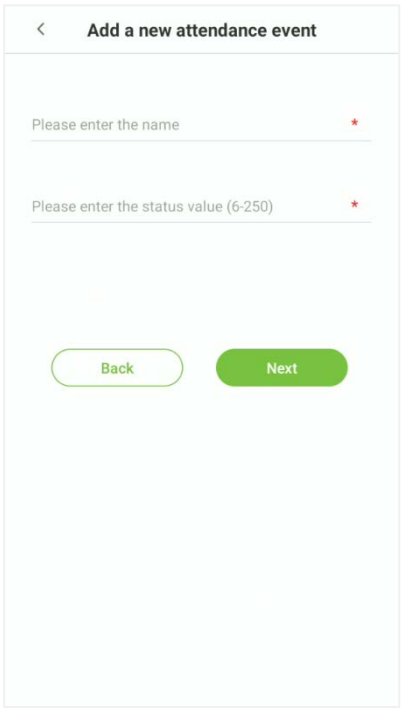


2. In the attendance event creation wizard, tap on **[Start]**.

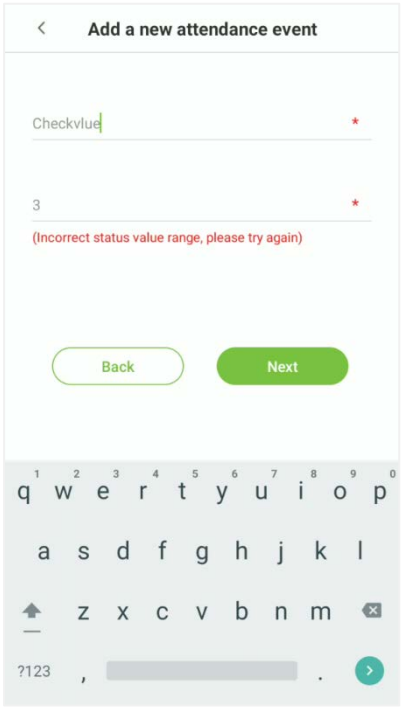


3. Enter the **[Name]** and **[Status Value]** of the new attendance event.

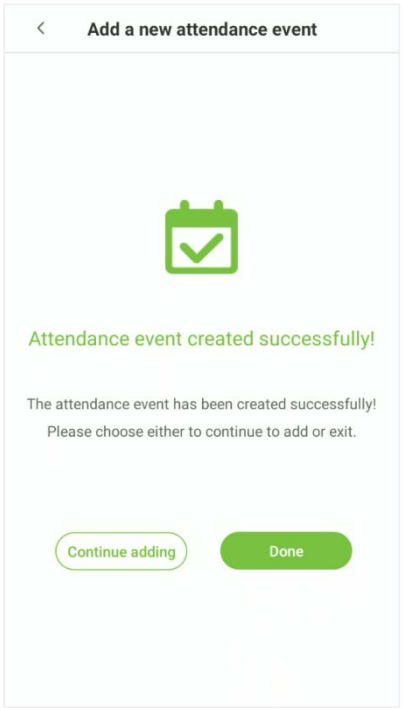
NOTE: The maximum length of the name is 24 characters. The status values must be unique and cannot be duplicated. The value ranges from 6 to 250.



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

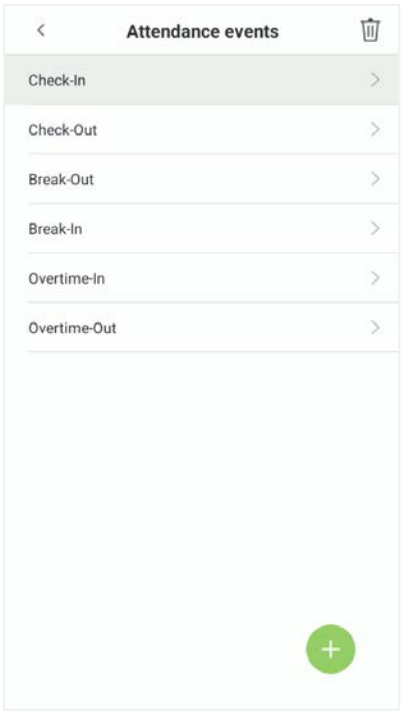


5. If the attendance event is created successfully, the success message appears as shown below:



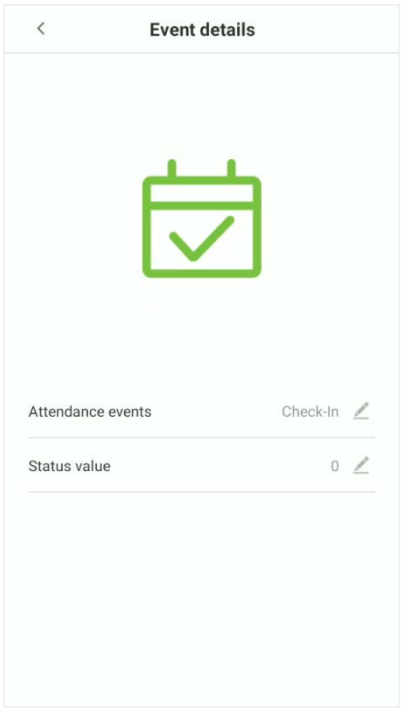
Edit Attendance Events

1. Select an attendance event.



2. Tap on **[Name]** or **[Status value]** to edit.

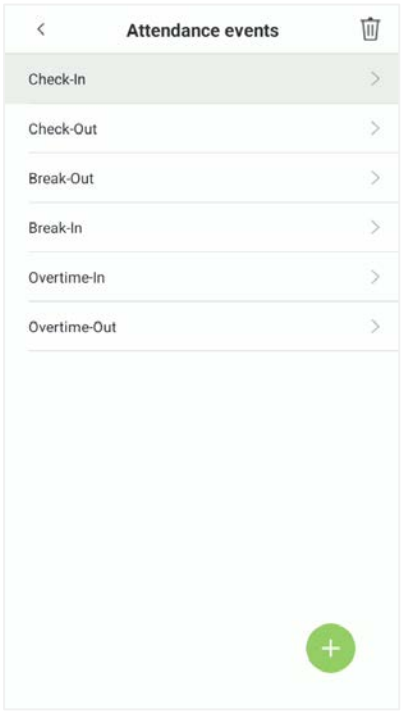
NOTE: The first 6 attendance events cannot be edited. The status values must be unique and cannot be duplicated.



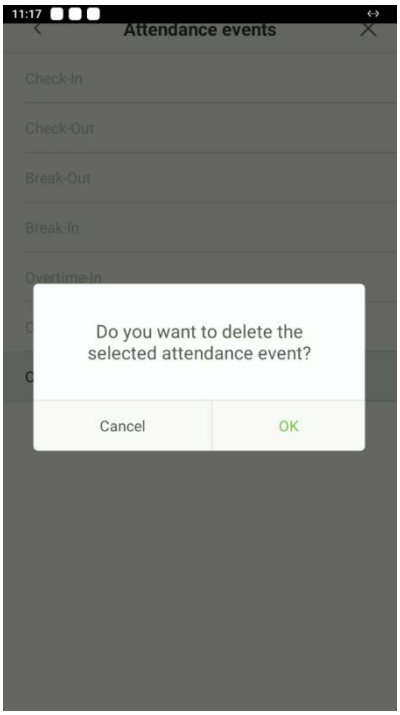
Delete Attendance Events

1. Select an attendance event and tap on the icon on the upper right corner.

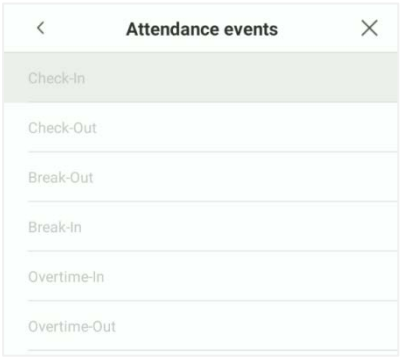
NOTE: The first 6 events cannot be deleted, so the delete button will not appear).



2. Tap on **[OK]** on the appearing window to delete the attendance event.



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



10.3.2 Status Mode

There are three modes for attendance statuses.

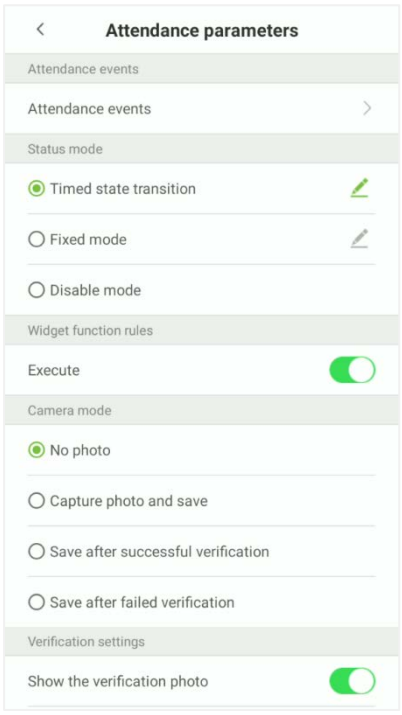
Timed state transition: Displays different attendance statuses at different times.

Fixed mode: There is only one fixed attendance mode.

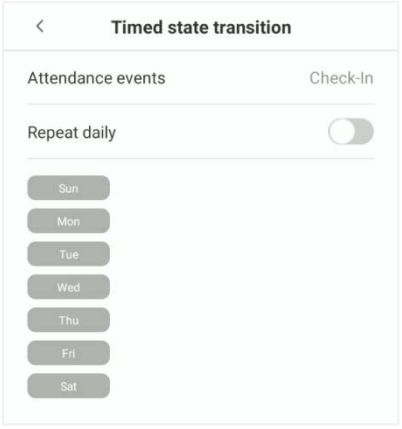
Disable mode: The Status mode will not be used.

Timed State Transition

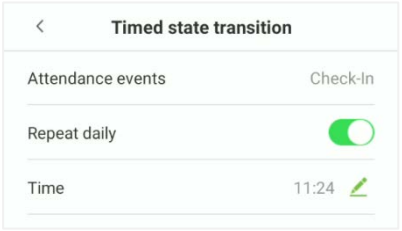
1. After selecting the **[Timed State Transition]** button, tap on the button to set the related parameters.



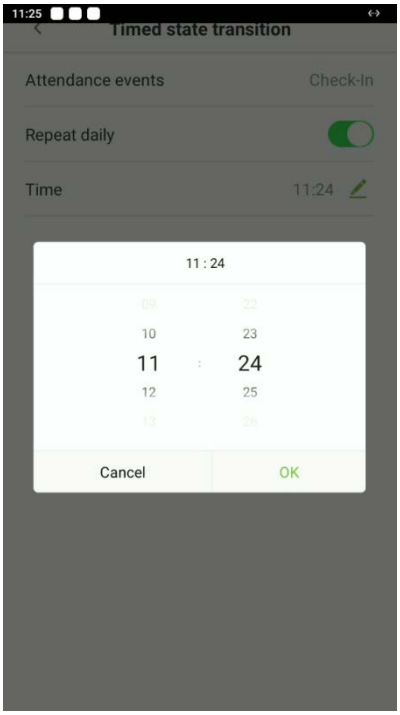
2. On the Timed state transition interface, tap on **[Check in]**, then tap on **[Repeat daily]**.



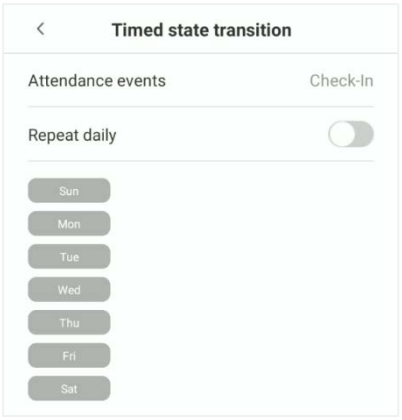
3. When the **[Repeat daily]** option is enabled, the following screen will be displayed.



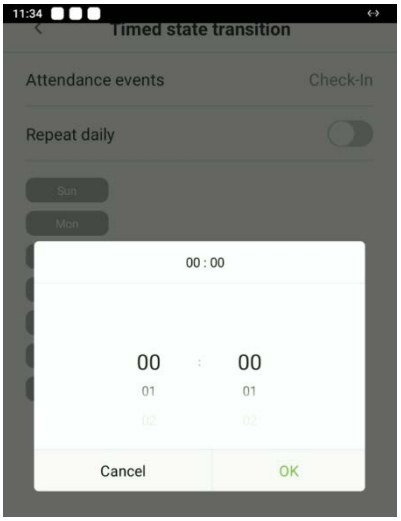
4. Tap on the **[Time]** button and swipe up and down to set the time. Tap on **[OK]**.



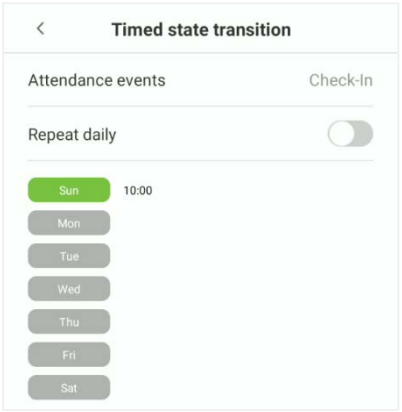
5. When the **[Repeat daily]** option is disabled, the following screen will be displayed.



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]**.



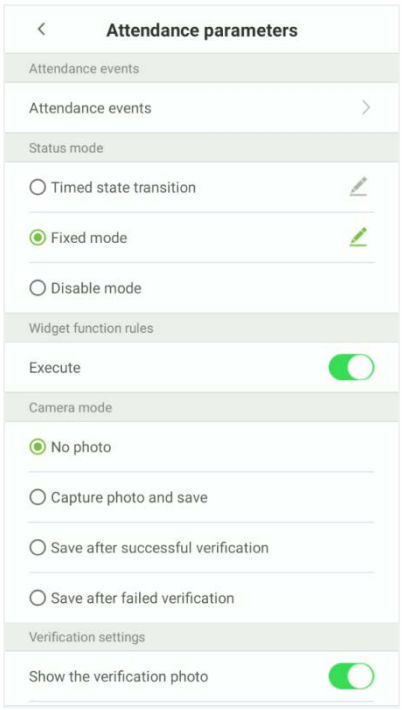
7. After applying the settings, the interface appears as shown below:



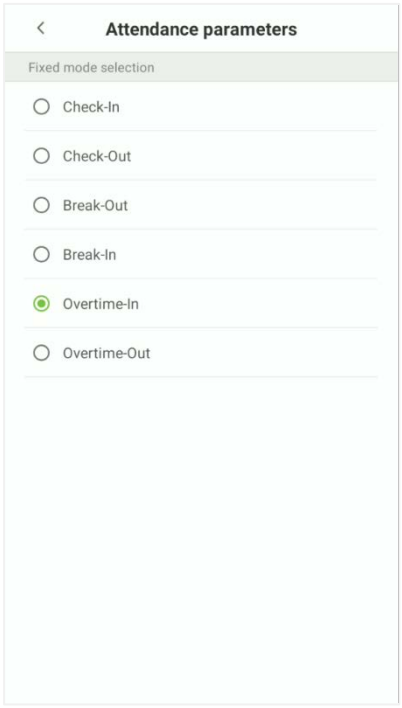
NOTE: The settings process for "Clock out", "Break out", "Break in", "Overtime in", and "Overtime out" is the same as "Clock in".

Fixed Mode

1. The status mode is set to **Fixed mode**, tap on the button to open the Fixed Mode options menu.

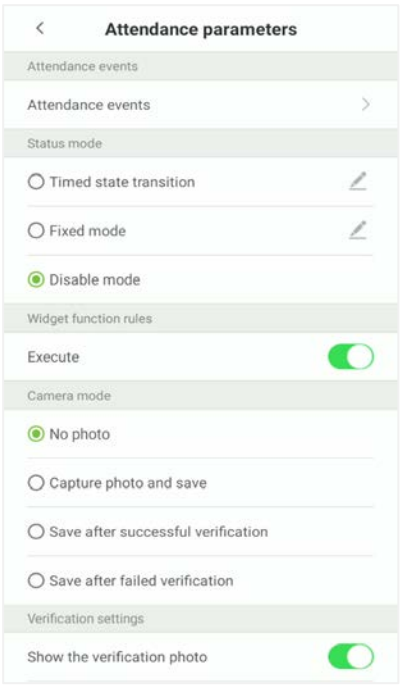


2. In the Fixed mode selection menu, select the attendance status that the user would like to set.



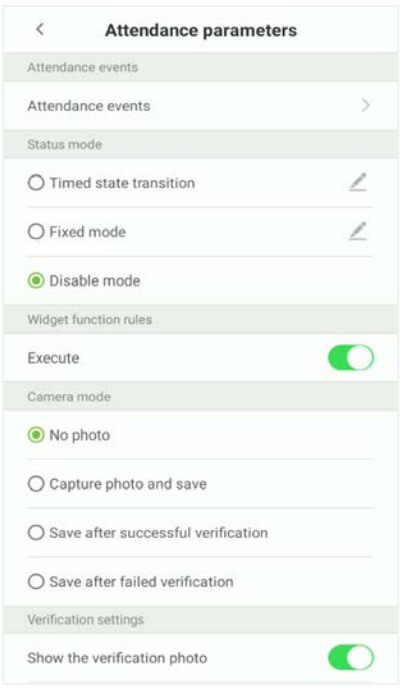
Disable Mode

Select the Status mode as "**Disable Mode**".



10.3.3 Widget Function Rules

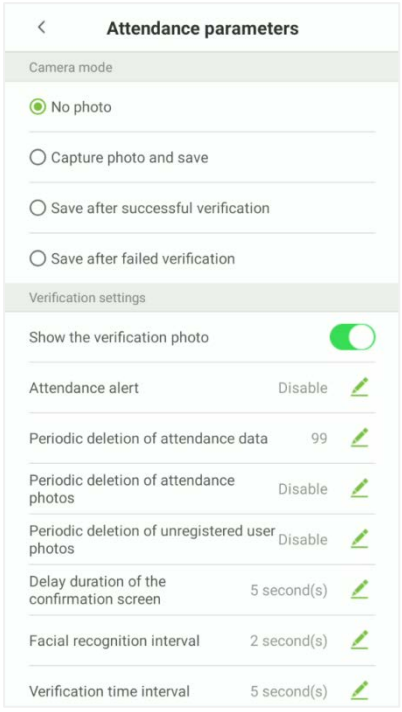
Tap on the **[Execute]** toggle button to enable. The main interface will display the attendance status widget.



10.3.4 Camera Mode

Here, the user can set the procedure of capturing and saving the user photos after verification as per the requirements.

Tap on the **[Camera mode]** to set the required parameters.



No photo: User's photo will not be saved during verification.

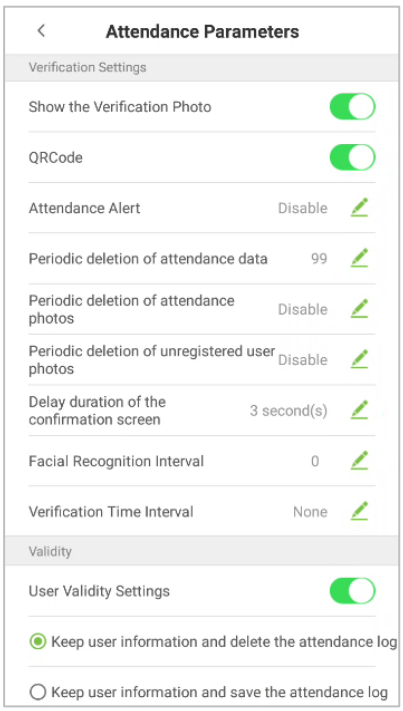
Capture photo and save: User's photo will be taken and saved during verification.

Save after successful verification: When the user verification is successful, the photo is taken and saved.

Save after failed verification: When the user verification is failed, the photo is captured and saved.

10.3.5 Verification Settings

Here, the user can configure the parameters for user verification.



Function Descriptions

Function Name	Function Description
Show the verification photo	If it is enabled, the user photo will be displayed; if not, the user photo will not be displayed.
QRCode	If it is enabled, the camera can recognize the QR code image captured by the lens.
Attendance alert	When the remaining record memory space reaches a set value, the device will automatically display a warning. When the value is set as 0, the function will be disabled.
Periodic deletion of attendance data	When the attendance record memory has reached the full capacity, the device will automatically delete a set value of old attendance records. When the value is set as 0, the function will be disabled.
Periodic deletion of attendance photos	When the space storing blocklisted photos have reached full capacity, the device will automatically delete a set value of old blocklisted photos. When the value is set as 0, the function is disabled.
Periodic deletion of unregistered user photos	When the capacity of blocklisted photos have reached the full capacity, the device will automatically delete a set value of old blocklisted photos. When the value is set as 0, the function will be disabled.
Delay duration of the confirmation	This is the length of time that a user's information will display on the

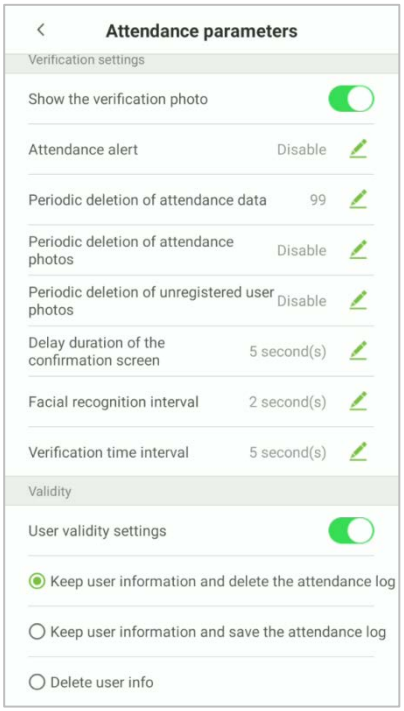
screen	system's screen after successful verification.
Facial verification interval	This is the facial template matching time interval that users can set as 0 to 9 seconds.
Verification time interval	Set the verification time interval as needed. The valid range is 0 to 999999 seconds.

10.3.6 Validity Period of User Information

This is used to determine if user validity periods are enabled or disabled when registering users.

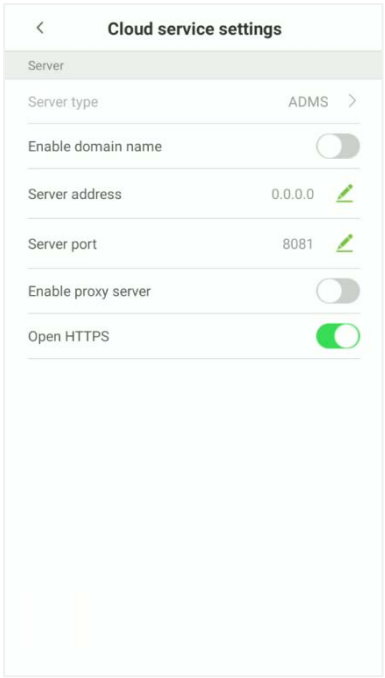
Tap **User validity settings** to enable.

When User validity settings is enabled, the following interface will display. Select the setting you would like to configure.



10.4 Cloud Service Settings

On **System settings** interface, tap **[Cloud service settings]** to enter the cloud service settings interface.

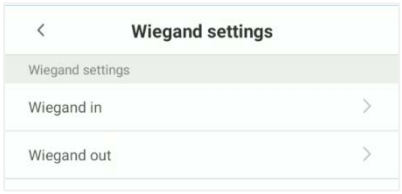


Function Descriptions

Item		Function Description
Enable domain name	Server address	When this function is enabled, the domain name mode "http://..." will be used, such as http://www.XYZ.com, while "XYZ" denotes the domain name when this mode is turned ON.
Disable Domain Name	Server address	IP address of the ADMS server.
	Server port	Port used by the ADMS server.
Enable proxy server		When you choose to enable the proxy, you need to set the IP address and port number of the proxy server.
Open HTTPS		If it is enabled, it needs to restart to take effect, and the data is uploaded to the push terminal. The address is changed from HTTP to HTTPS.

10.5 Wiegand Settings

On **System settings** interface, tap **Wiegand settings** to access the interface as shown below.



10.5.1 Wiegand In

On **Wiegand settings** interface, tap **Wiegand in** to open the settings.

Function Descriptions

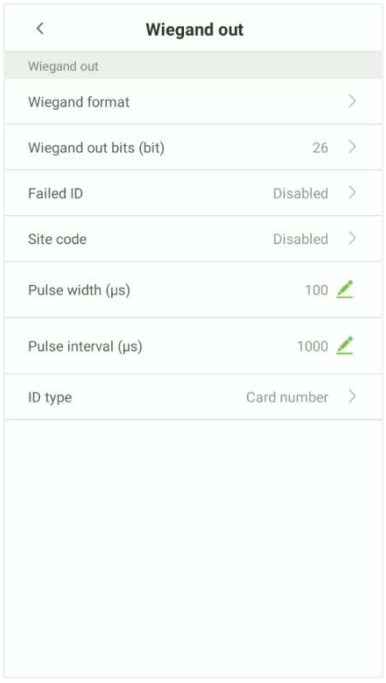
Function Name	Function Description
Wiegand format	The Wiegand value could be 26bits, 34bits, 36bits, 37bits, or 50bits.
Wiegand in bits (bit)	It displays the number of bits of Wiegand data. After choosing **Wiegand input bits**, the device will use the set number of bits to find the suitable Wiegand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

Various common Wiegand format definitions:

Wiegand Format	Description
Wiegand26	ECCCCCCCCCCCCCCCCCCCCCCCCO 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.
Wiegand26a	ESSSSSSSSCCCCCCCCCCCCCCCCO 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.
Wiegand34	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO 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.
Wiegand34a	ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCO 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.
Wiegand36	OFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME 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.
Wiegand36a	EFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCO 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.
Wiegand37	OMMMMSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCE 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.
Wiegand37a	EMMMFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCCO 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, and15th to 20th bits are the site codes, and the 21st to 36th bits are the card numbers.
Wiegand50	ESSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO 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.
"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.	

10.5.2 Wiegand Out

On **Wiegand settings** interface, tap [**Wiegand Out**] to open the wiegand out interface.

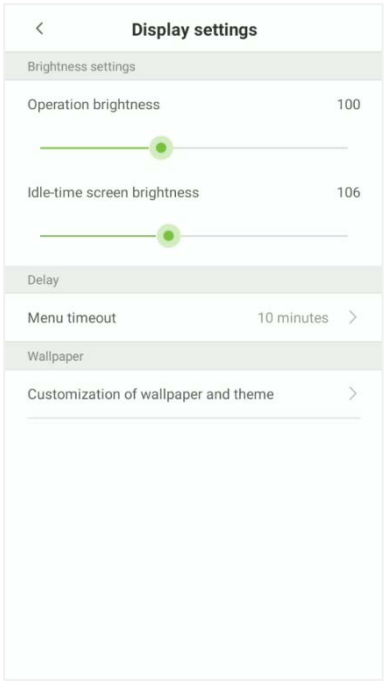


Function Description

Function Name	Function Description
Wiegand format	The Wiegand format value could be 26bits, 34bits, 36bits, 37bits, 50bits.
Wiegand out bits (bit)	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.

10.6 Display Settings

On the **System settings** interface, tap **Display settings** to enter the display settings interface.



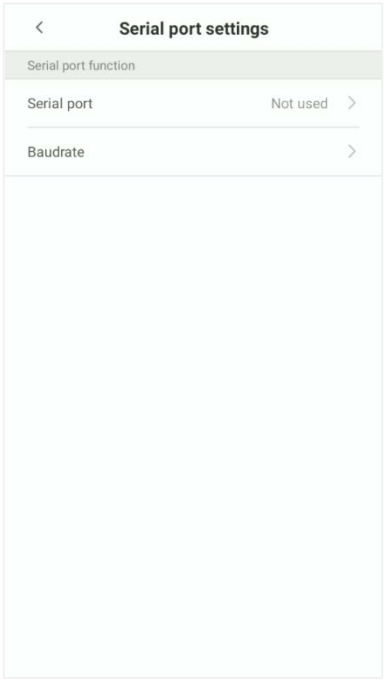
Function Descriptions

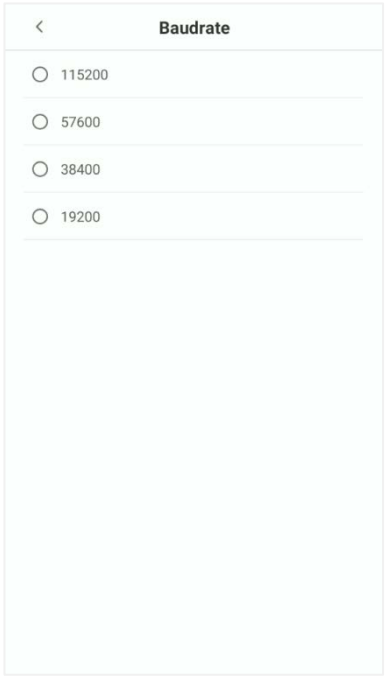
Function Name		Function Description
Brightness setting	Operation brightness	Set the device working brightness, such as when setting parameter or face recognition.
	Idle-time screen brightness	Screen brightness when the device is on the standby mode.
Delay	Menu timeout	Menu timeout occurs when no operations are performed for a certain amount of time after a user has entered the menu, and the menu enters into standby screen. Parameter options include: 1 minute, 2 minutes, 5 minutes, 10 minutes, the menu (including sub-menus) will not automatically close. Users must tap "Exit" to exit the menu.
Wallpaper	Customization of wallpaper and theme	Choose your favourite wallpaper from the theme wallpaper interface

10.7 Serial Port Settings

Serial Comm function facilitates to establish communication with the device through a serial port.

On the **System settings** interface, tap **Serial port settings** to enter the **Serial port settings** interface.



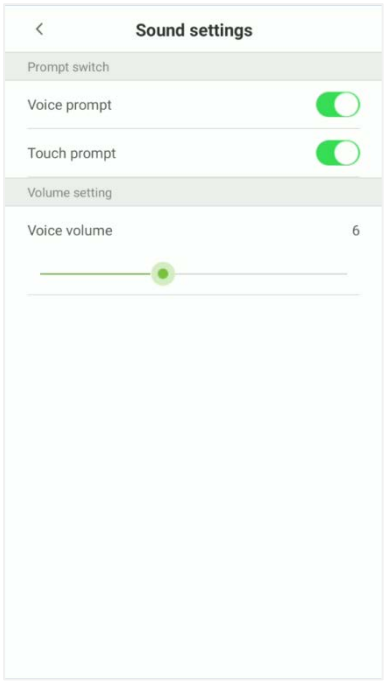


Function Descriptions

Function Name	Function Description
Serial port	No 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, 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.

10.8 Sound Settings

On the **System settings** interface, tap **Sound settings** to enter **Sound settings** interface.

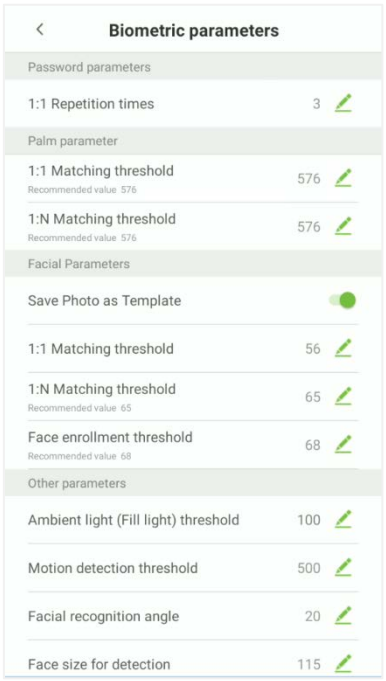


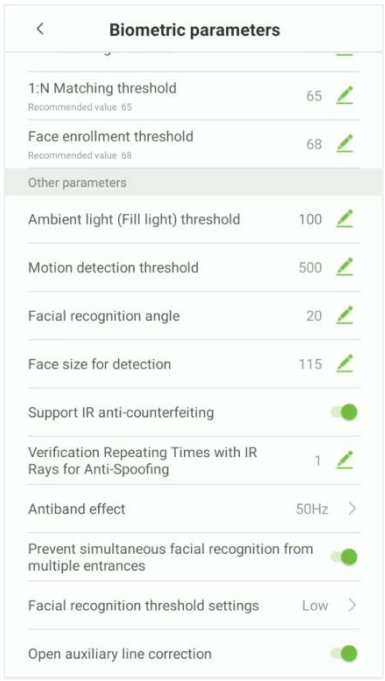
Function Descriptions

Function Name	Function Description
Voice prompt	When voice prompts are enabled, users will receive voice prompts. Voice prompts will not be received when this setting is disabled. When voice prompts are disabled and then re-enabled, the volume level will be automatically set to 1.
Touch prompt	This switch enables/disables touchscreen prompt. When touch prompt is enabled, users will receive touchscreen prompts. When touch prompt is disabled, no touchscreen prompts will be received.
Voice volume	It is used for adjusting volume. This can only be used if audio prompts are enabled. It can be set from 0-15.

10.9 Biometric Parameters

On the **System settings** interface, tap **Biometric parameters** to enter the **Biometric parameters** interface.





Function Descriptions

Function Name		Function Description
Password parameters	1:1 Repetition times	The upper limit of the number of failed verifications under 1:1 verification. When the number of failed verifications reaches the set value, the system will return to the standby interface.
Palm parameters	1:1 Matching threshold	Only when the similarity between the verifying palm and the user's registered palm is greater than this value can the verification succeed.
	1: N Matching threshold	Under 1:N Verification Method, only when the similarity between the verifying palm and all registered palm is greater than this value can the verification succeed.
Facial Parameters	Save Photo as Template	Select whether to enable or disable
	1:1 Matching threshold	When conducting 1:1 face verification, face data is collected and instantly compared with face data using a

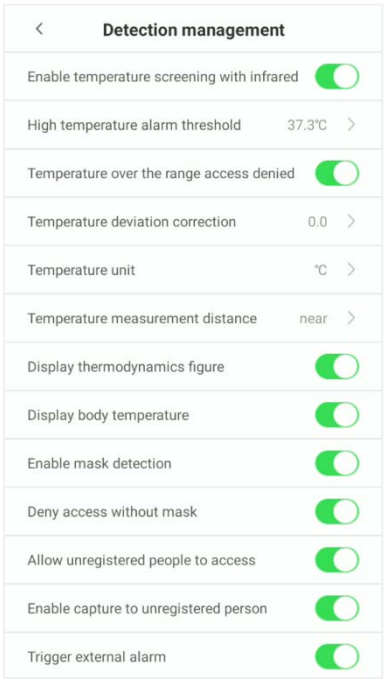
		1:1 algorithm. This is converted into a value that is then compared to a set value. If the value of the scanned face exceeds that of the set value, the verification passes. If it does not, the verification fails. The higher the threshold, the more accurate the matching; the lower the threshold, the higher the matching success rate.
	1: N Matching threshold	When conducting 1: N verification, face data is collected and instantly compared with all face 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 face exceeds that of the set value, the verification has passes. If it does not, the verification fails. The higher the threshold, the more accurate the matching; the lower the threshold, the higher the matching success rate.
	Face enrollment threshold	In face recognition, the higher the threshold is set, the higher the accuracy of face recognition will be, which may lead to unrecognizable. On the contrary, if the threshold is too low, the accuracy of face recognition will be lower, which may lead to misjudgement and other phenomena. The default value is 68.
Other parameters	Ambient light (Fill light) threshold	It is used for detecting ambient light brightness. When the brightness of the surrounding environment is less than the threshold, the complementary light is turned on; when the brightness is greater than the threshold, the complementary light is not turned on. The default value is 100.
	Motion detection threshold	It is used for detecting whether there is a moving person in front of the device to determine whether the face recognition function is enabled. The default value is 500.
	Face recognition angle	To limit the face angle at face recognition, the recommended threshold is 20.
	Face size for detection	The size of the face when face recognition. The range is 65-320 cm. The smaller the value, the farther the detectable distance is otherwise, the closer it is.

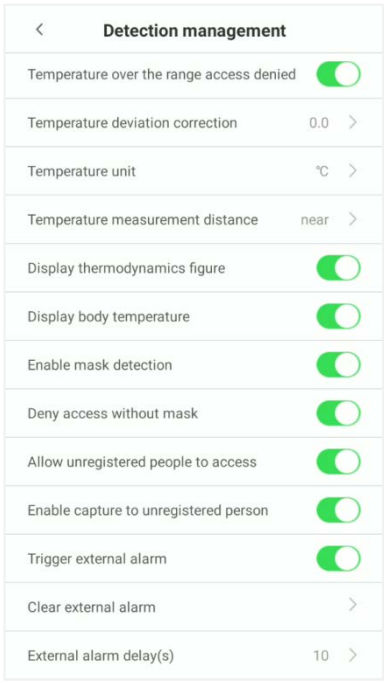
	Support IR anti-counterfeiting	It supports face anti-counterfeiting. After enable, it can anti-counterfeiting recognition on face photos to ensure the authenticity of face
	Verification Repeating Time with IR Rays for Anti-Spoofing	The upper limit of the number of failed verifications under face verification when IR Anti-counterfeiting is enable. Valid values 1 to 6. When the number of failed verifications reaches the set value, the system will return to the standby interface.
	Antiband effect	When using an external power supply with AC power, the pictures taken by the device will produce noise due to the AC power changing back and forth. According to the specific use of AC power can be adjusted to 50Hz or 60Hz.
	Prevent simultaneous facial recognition from multiple entrances	When multiple devices are installed on the side-by-side entrance, please enable this function to prevent multiple devices from simultaneously recognizing the face. Set the threshold to three types: high, medium, and low. The higher the threshold, the narrower the distance between the guidelines and the smaller the face recognition range on the screen. When setting the threshold, it is recommended to open auxiliary line correction function.
	Facial recognition threshold settings	When the Prevent simultaneous facial recognition from multiple entrances is enabled, you can set the threshold value of the face, low, medium and high.
	Open auxiliary line correction	When this feature is enabled, the user is prompted to place their face in the center of the device screen to quickly pass authentication.

10.10 Detection Management

On the **System settings** interface, tap **Detection management** to enter into detection management interface.

This interface is added for enabling temperature screen with infrared and mask detection.





Function Descriptions

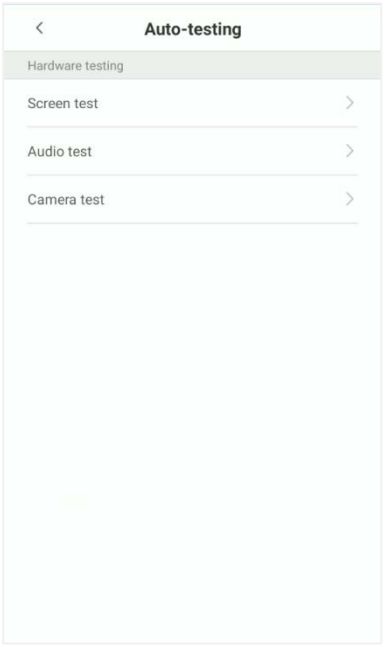
Function Name		Function Description
Temperature Screening with Infrared	Enable temperature screen with infrared	The temperature screen with infrared module is set as **Off** or **On**.
	High temperature alarm threshold	To set the value of the alarm threshold for high body temperature. When the temperature measured during verification is higher than the set value, the device will give a prompt and audio alarm. The default alarm threshold is 37.30°C.
	Temperature over the range access denied	When enabled, if the user's body temperature measured is above (or below) the alarm threshold, the user will not be granted access even if his/her identity is verified. When disabled, access is granted to the user if his/her identity is verified, regardless of his/her body temperature.
	Temperature deviation correction	As the temperature measurement module reads a small range of variation of an observed value under unusual environments (humidity, extreme room temperature and such), the users may set the deviation value here to reflect the true

		temperature of the person.
	Temperature unit	The unit of body temperature can be toggled between Celsius (℃) and Fahrenheit (℉).
	Temperature measurement distance	There are three modes while measuring temperature during the verification process, they are: **Near, Close** and **Far**.
	Display thermodynamics figure	To enable or disable the display of the thermal image of a person. When enabled, the thermal image of the person is be displayed in the upper left corner of the device during the detection process.
	Display body temperature	To enable or disable the display of body temperature. When enabled, the device will display the user's body temperature value during the verification process.
Mask Detection	Enable Mask Detection	To enable or disable the mask detection function. When enabled, the device will identify whether the user is wearing a mask or not during verification.
	Deny access without mask	To enable or disable the access of a person without mask. When enabled, the device will deny access of a person, if not wearing a mask.
	Allow unregistered people to access	To enable or disable the access of unregistered person. When enabled, the device allows the person to enter without registration, as long as the person who passes the detection.
	Trigger external alarm	When enabled, if the user's temperature is higher than the set threshold value or the mask detection is enabled, but the mask is not worn by the person, it will trigger an alarm.

	Clear external alarm	It clears the triggered alarm records of the device.
	External Alarm Delay(s)	The delay (s) time for triggering an external alarm. It can be set in seconds. Users may disable the function or set a value between 1 to 255.

10.11 Auto-testing

On the **System settings** interface, tap on **Auto-testing** to enter the auto testing interface.



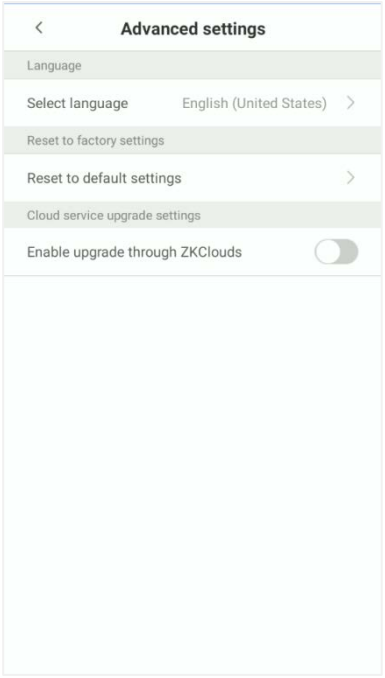
Function Descriptions

Function Name	Function Description
Screen test	It is used for testing 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.
Audio test	The device automatically tests audio prompts by playing back audio files that are stored in the device. Voice testing mainly 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.

Camera test	It is used for testing if the camera is functioning properly. Check captured image to see if the image quality is clear and usable.

10.12 Advanced Settings

On the **System settings** list, tap on **Advanced settings** to enter the **Advanced settings** interface.

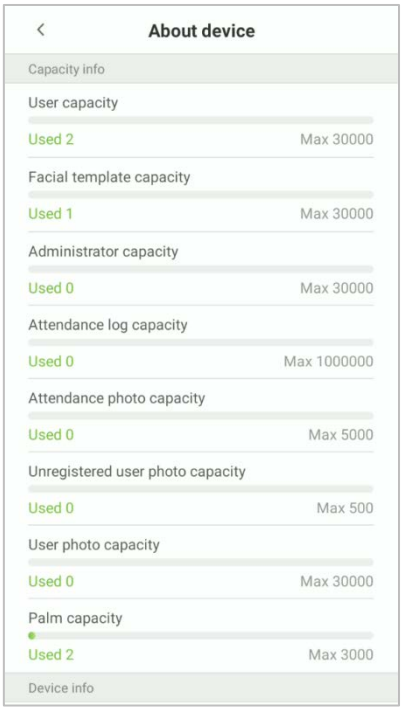


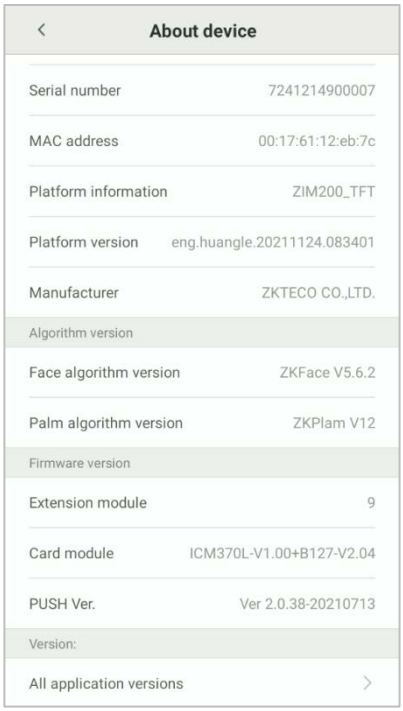
Function Descriptions

Function Name	Function Description
Select language	Select the language of the device.
Reset to factory settings	It is used for restoring the settings of the device, including communication settings, system settings, to the factory settings.
Cloud service upgrade settings	Whether to enable ZKClouds upgrade.

10.13 About Device

On the **System settings** interface, tap **About device** to open the **About device** interface.



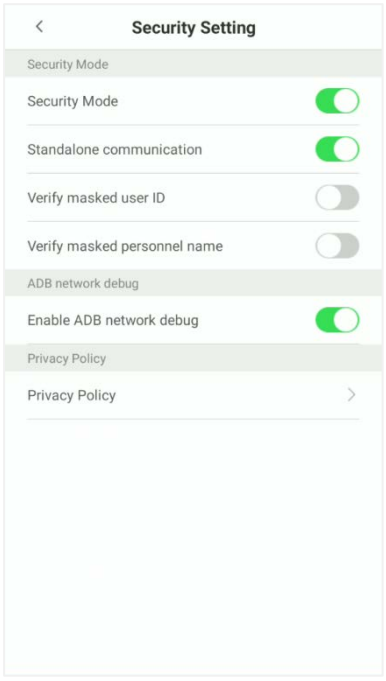


Function Description

Function Name	Function Description
Capacity info	It displays the current device's capacity of user, palm and facial template, administrators, attendance records, attendance photos, unregistered user photos, and user photos.
Device Information	It displays the device's name, device type, serial number, MAC address, algorithm version, platform information, and manufacturer.
Algorithm version	It displays the device's face and palm algorithm version.
Firmware version	It displays the device's extension and card module, push version.
Version	It displays all the versions of all the system's apps, such as the system settings, data management, and other installed apps.

10.14 Security Setting

On the **System settings** interface, tap **Security Setting** to open the security setting interface.

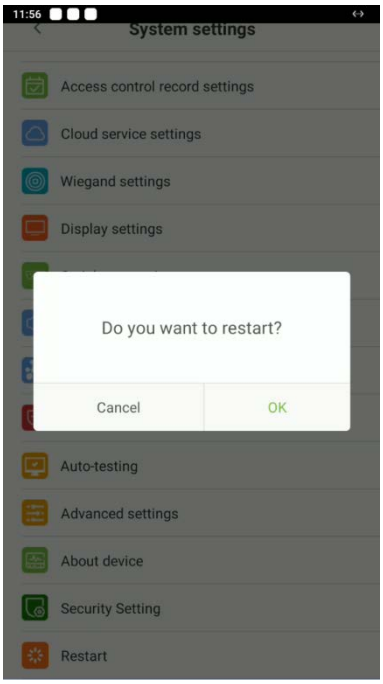


Function Description

Function Name	Function Description
Security Mode	Select whether to enable security mode to protect the device and the user's personal information. You can set the device to work offline, and hide the user's personal information to prevent leakage during user verification.
ADB network	It displays the device's name, device type, serial number, MAC address, algorithm version, platform information, and manufacturer.
Privacy Policy	Display the device's privacy policy.

10.15 Restart

On the **System settings** interface, tap **Restart**, the device will pop-up, please choose whether to restart according to your needs.



11 Connect to ZKBioSecurity Software

11.1 Set the Communication Address

- **Device side**

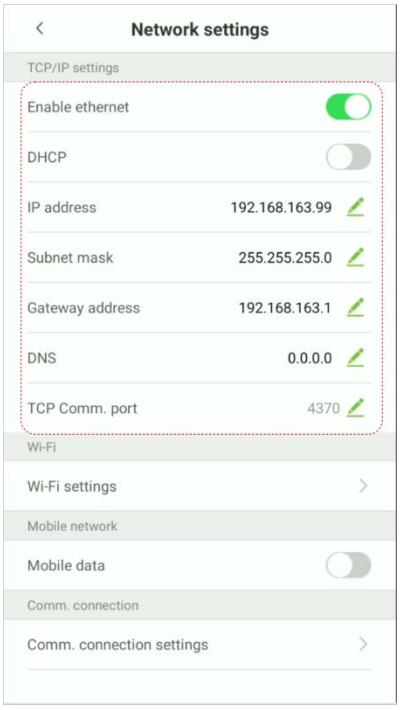
1. Tap **System settings** > **Network settings** > **TCP/IP settings** in the main menu to set the IP address and gateway of the device.

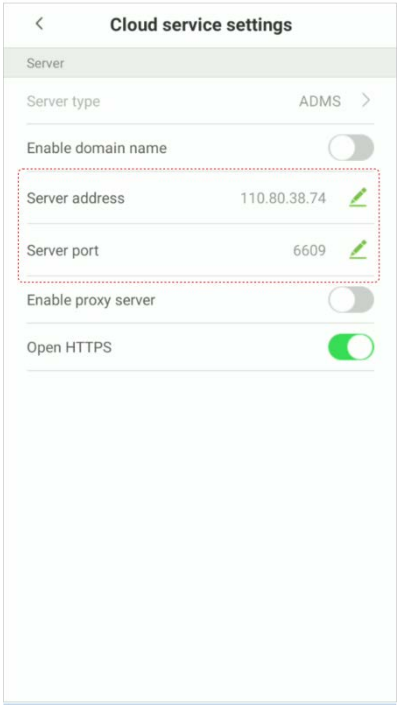
   (***NOTE***: The IP address should be able to communicate with the ZKBioSecurity server, preferably in the same network segment with the server address)

2. In the main menu, click **System settings** > **Cloud server settings** to set the server address and server port.

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

   Server port: Set the server port as of ZKBioSecurity (The default is 6609).





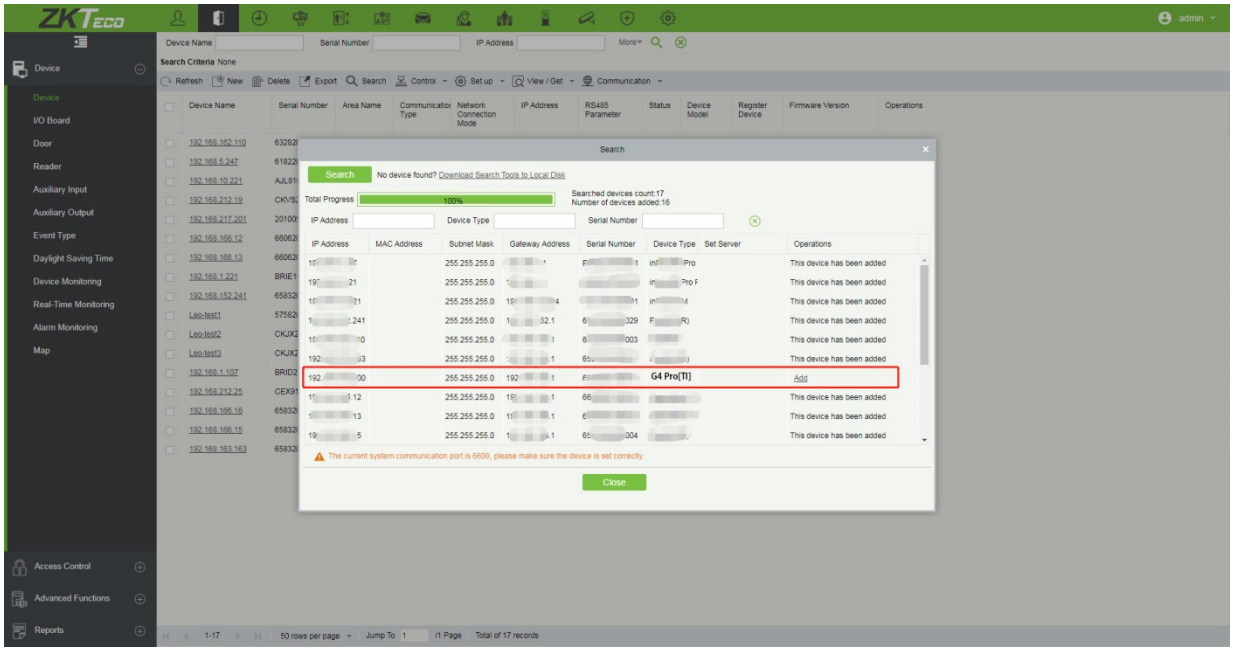
- **Software side**

Login to ZKBioSecurity software, click **System** > **Communication** > **Communication Monitor** to set the ADMS Service Port, as shown in the figure below:

11.2 Add Device on the Software

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

1. Click **Access** > **Device** > **Search**, to open the Search interface in the software.
2. Click **Search**, and it will prompt **[Searching……]**.
3. After searching, the list and total number of access controllers will be displayed.

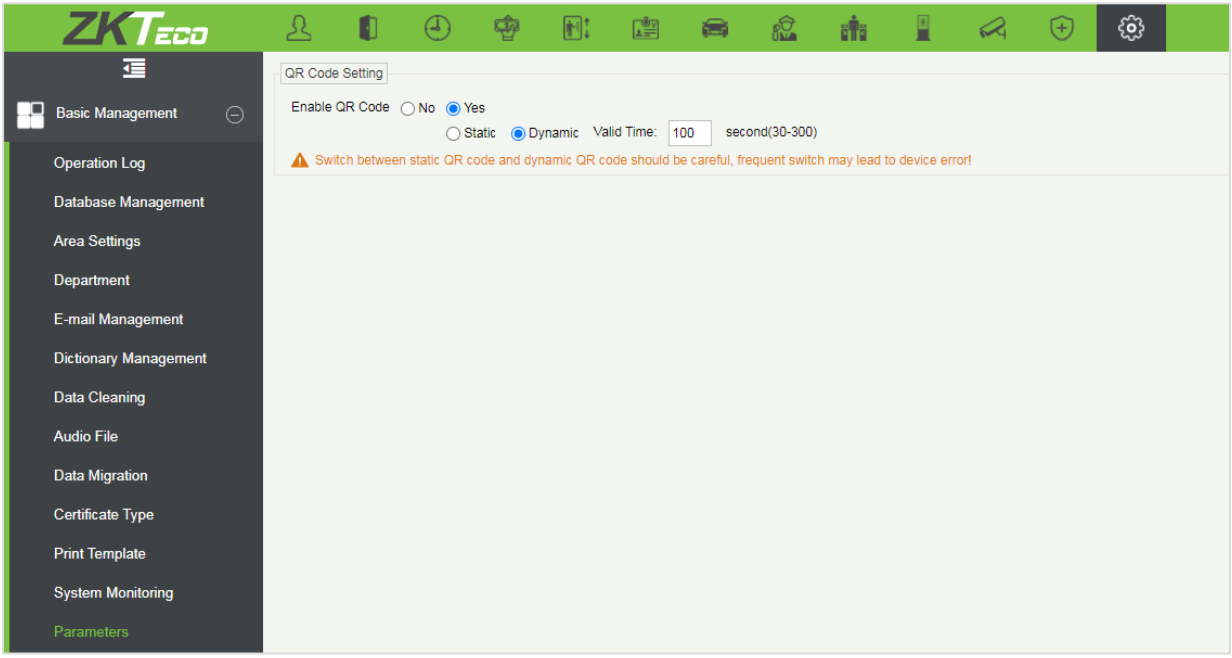


4. Click **[Add]** in operation column, a new window will pop-up. Select Icon type, Area, and Add to Level from each dropdown and click **[OK]** to add the device.

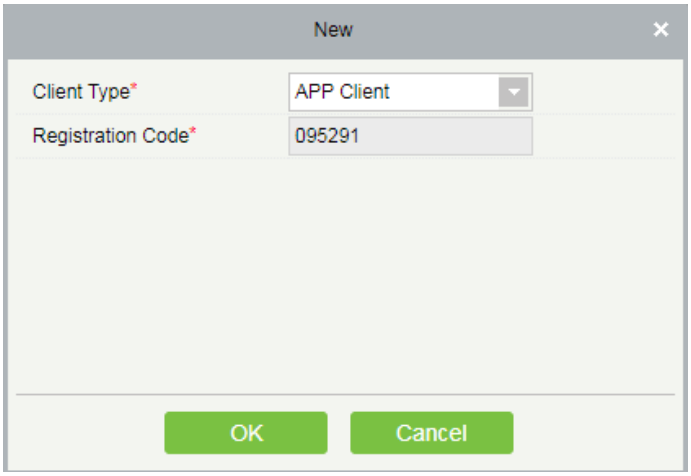
11.3 Mobile Credential

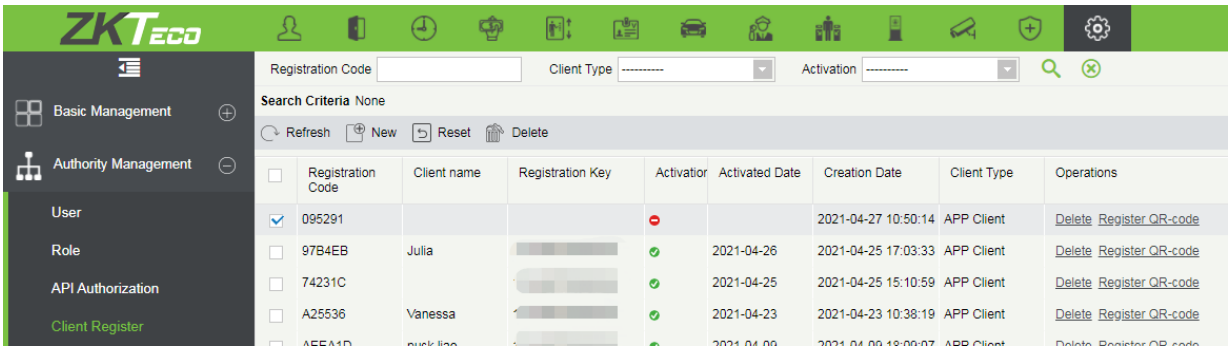
After downloading and installing the App, the user needs to set the Server before login. The steps are given below:

1. In **[System]** > **[Basic Management]** > **[Parameters]**, set **Enable QR Code** to "Yes", and select the QR code status according to the actual situation. The default is **Dynamic**, the valid time of the QR code can be set.



2. On the Server, choose **[System]** > **[Authority Management]** > **[Client Register]** to add a registered App client.

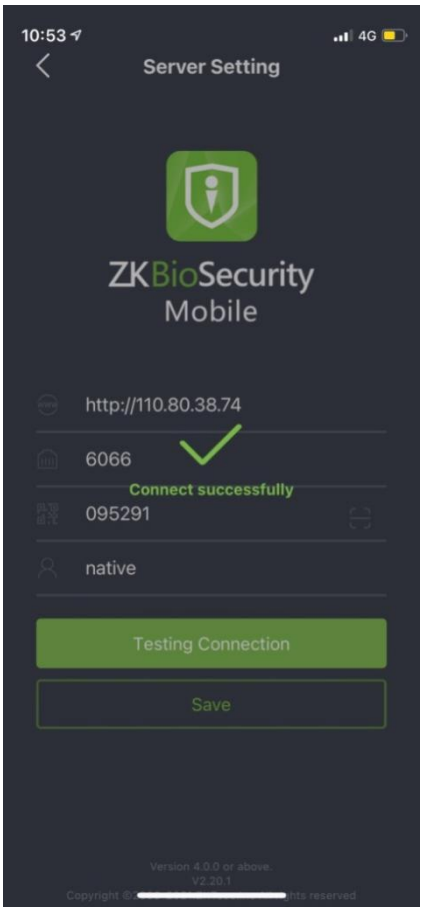




3. Open the App on the Smartphone. On the login screen, tap **[Server Setting]** and type the IP Address or the Domain Name of the Server, and its Port Number.

4. Tap the **QR Code** icon to scan the QR code of the new App client. After the client is identified successfully, set the Client Name and tap **[Connection Test]**.

5. After the network is connected successfully, tap **[Save]**.

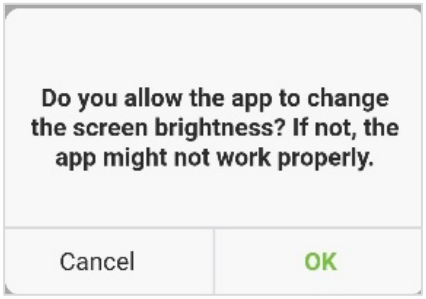


The Mobile Credential function is only valid when logging in as an employee, tap on Employee to switch to Employee Login screen. Enter the Employee ID and Password (Default: 123456) to login.

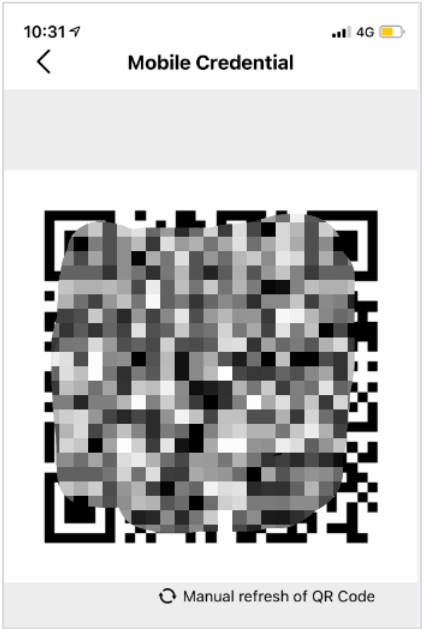
6. Tap **[Mobile Credential]** on the App, and a QR code will appear, which includes employee ID and card number (static QR code only includes card number) information.

The QR code can replace a physical card on a specific device to achieve contactless authentication to open the door.

When using this function for the first time, the App will prompt to authorize the modification of screen brightness settings, as shown in the figure:



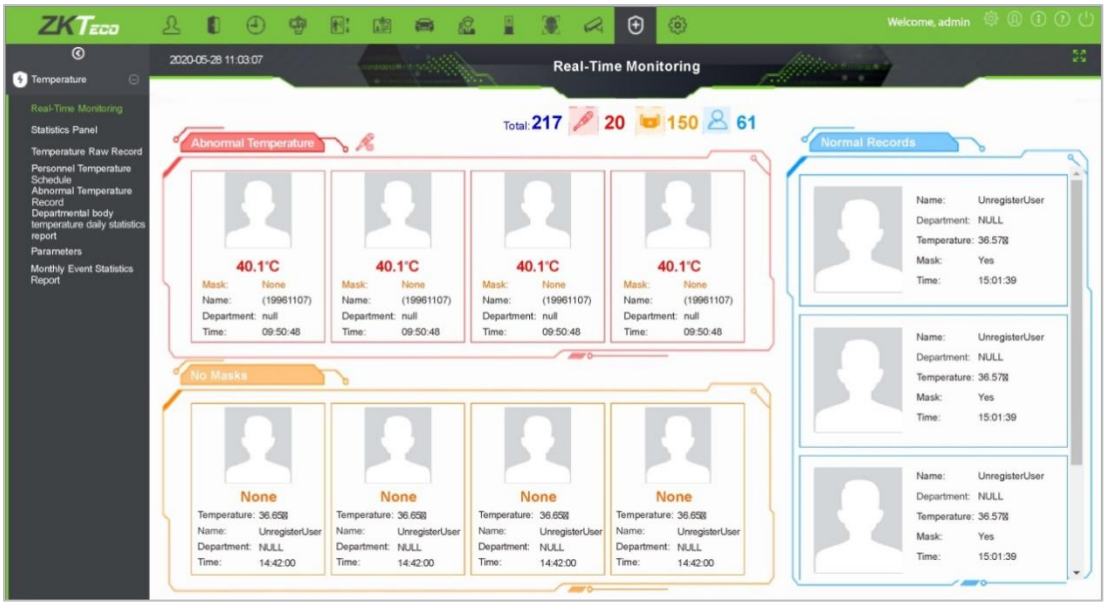
The QR code is automatically refreshed for every 30s, and it also supports manual refresh.



NOTE: For other specific operations, please refer to ZKBioSecurity Mobile App User Manual.

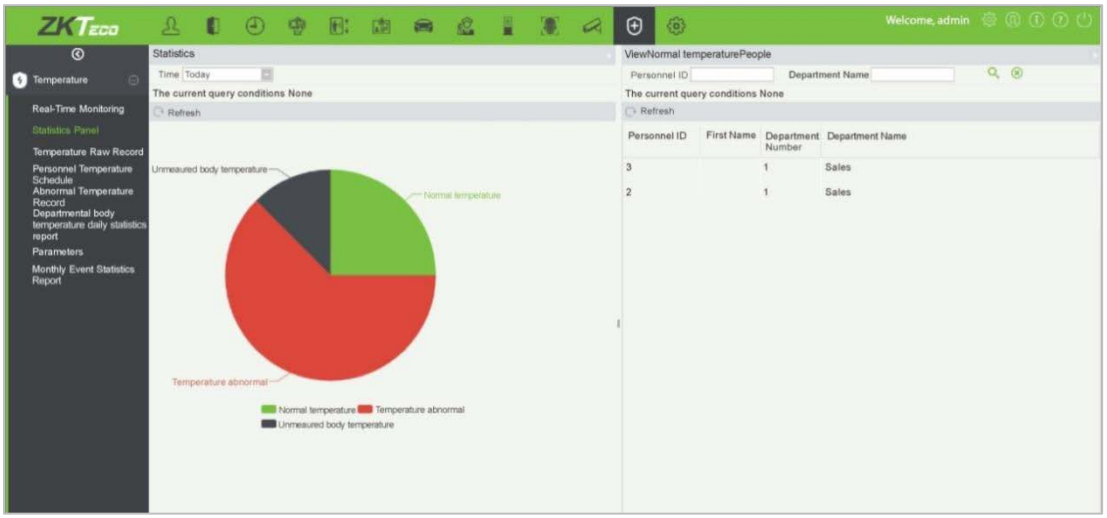
11.4 Real-time Monitoring on the ZKBioSecurity Software

1. Click **Prevention** > **Epidemic** > **Temperature Detection** > **Real-time monitoring** to view all the personnel's events present under the Abnormal Temperature, No Masks, and Normal Records.



The user data of abnormal body temperature is displayed on the Abnormal Temperature information bar automatically according to the Temperature Threshold Setting is set.

2. Click **Epidemic** > **Temperature Management** > **Statistics Panel** to view the analysis of statistical data in the form of a pie-chart and view the personnel with normal temperature, abnormal temperature, and unmeasured body temperature. Also, detailed information of the personnel can be seen on the right by clicking on the particular category on the pie-chart.



NOTE: For other specific operations, please refer to ZKBioSecurity User Manual.

Appendix 1

Requirements of Live Collection and Registration of Visible Light Face Images

1) It is recommended to perform registration in an indoor environment with an appropriate light source without underexposure or overexposure.

2) Do not shoot towards outdoor light sources like door or window or other strong light sources.

3) Dark-color apparels which are different from the background color are recommended for registration.

4) Please show your face and forehead, and do not cover your face and eyebrows with your hair.

5) It is recommended to show a plain facial expression. Smile is acceptable, but do not close your eyes, or incline your head to any orientation. Two images are required for persons with eyeglasses, one image with eyeglasses and one other without.

6) Do not wear accessories like scarf or mask that may cover your mouth or chin.

7) Please face right towards the capturing device, and locate your face in the image capturing area as shown in Image 1.

8) Do not include more than one face in the capturing area.

9) 50cm - 80cm is recommended for capturing distance adjustable subject to body height.

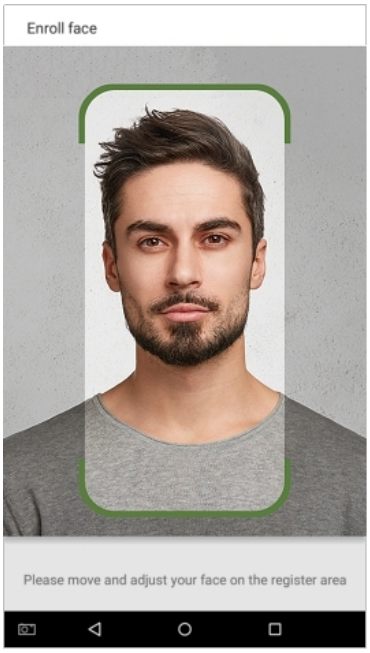


Image1 Face Capture Area

Requirements for Visible Light Digital Face Image Data

The digital photo should be straight-edged, colored, half-portrayed with only one person, and the person should be uncharted and in casuals. Persons who wear eyeglasses should remain to put on eyeglasses for getting photo captured.

- **Eye Distance**

200 pixels or above are recommended with no less than 115 pixels of distance.

- **Facial Expression**

Neutral face or smile with eyes naturally open are recommended.

- **Gesture and Angel**

Horizontal rotating angle should not exceed ±10°, elevation should not exceed ±10°, and depression angle should not exceed ±10°.

- **Accessories**

Masks or colored eyeglasses are not allowed. The frame of the eyeglasses should not cover eyes and should not reflect light. For persons with thick eyeglasses frame, it is recommended to capture two images, one with eyeglasses and the other one without the eyeglasses.

- **Face**

Complete face with clear contour, real scale, evenly distributed light, and no shadow.

- **Image Format**

Should be in BMP, JPG or JPEG.

- **Data Requirement**

Should comply with the following requirements:

1) White background with dark-colored apparel.

2) 24bit true color mode.

3) JPG format compressed image with not more than 20kb size.

4) Resolution should be between 358 x 441 to 1080 x 1920.

5) The vertical scale of head and body should be in a ratio of 2:1.

6) The photo should include the captured person's shoulders at the same horizontal level.

7) The captured person's eyes should be open and with clearly seen iris.

8) Neutral face or smile is preferred, showing teeth is not preferred.

9) The captured person should be clearly visible, natural in color, no harsh shadow or light spot or reflection in face or background. The contrast and lightness level should be appropriate.

Appendix 1

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 period 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	○	○	○	×	○	○

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