User Manual

G5

Outdoor & Multi-Biometric Access Control Terminal

Date: April 2023

Doc Version: 1.0

English

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

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

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 have 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 **G5 Outdoor & Multi-Biometric Access Control Terminal**.

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

Document Conventions

Conventions used in this manual are listed below:

GUI Conventions

For Software	
Convention	**Description**
Bold font	Used to identify software interface names **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 implies about the notice or pays attention to, in the manual
	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

G5 is an outdoor & multi-biometric access control terminal that features ZKTeco's innovative Enhanced Visible Light Facial Recognition and QR Code Scanning technology. The device with the latest technologies can automatically perform recognition at a distance from 0.5m to 3m when a face is detected to deliver higher recognition quality in speed and accuracy than the near-infrared facial recognition technology. With the applied Deep Learning algorithm, pose angle tolerance, and anti-spoof function have been greatly enhanced against various environmental conditions and different types of spoofing attacks.

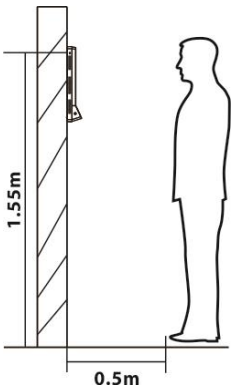
The G5 comes standard with a B133 card module that supports identification ID and IC cards. The G5 also perfectly supports Elatec card modules and can support 125 kHz/134.2 kHz/13.56 MHz RFID cards without replacing the card module.

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

2 Instructions for Use

2.1 Standing Position, Facial Expression and Standing Posture

Recommended Distance



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

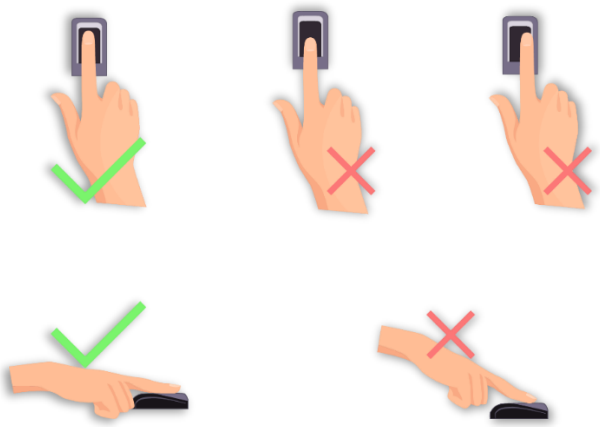
Recommended Facial Expressions

Recommended Standing Postures

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

2.2 Finger Placement

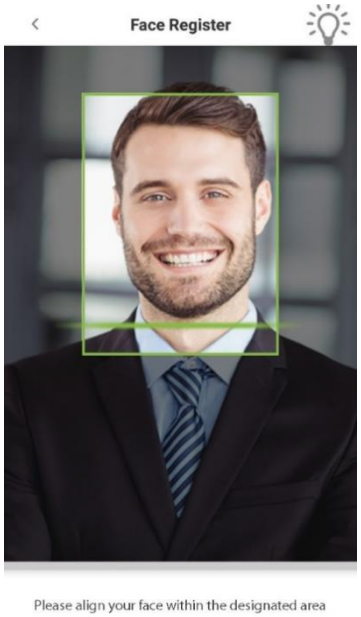
- **Recommended fingers:** Index, middle, or ring fingers.
- Avoid using the thumb or pinky, as they are difficult to accurately tap onto the fingerprint reader.



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

2.3 Face Enrollment

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



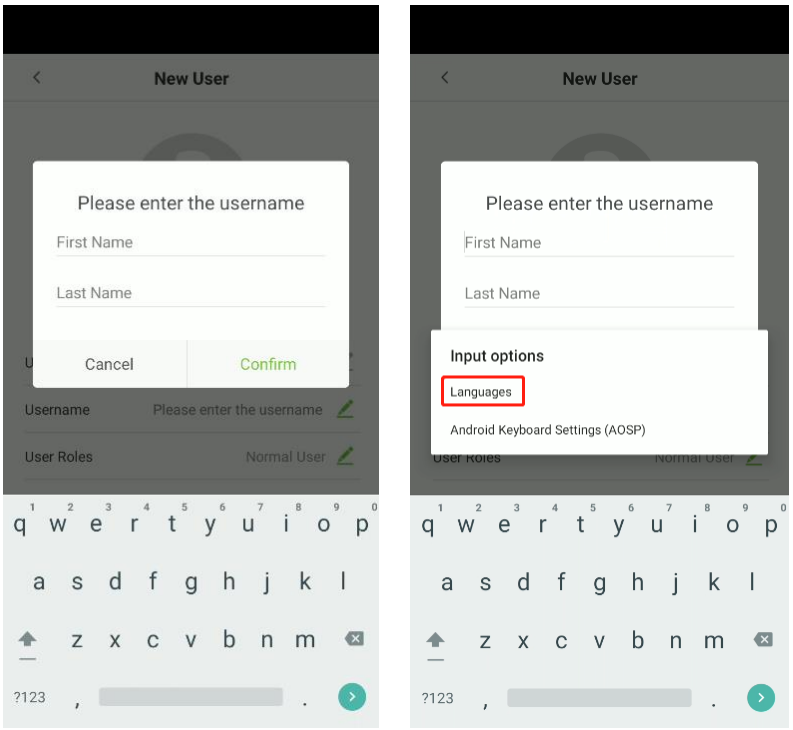
2.4 Standby Interface

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

Notes:

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

2.5 Virtual Keyboard



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

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

2.6 Verification Mode

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

1: N Identification Process

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

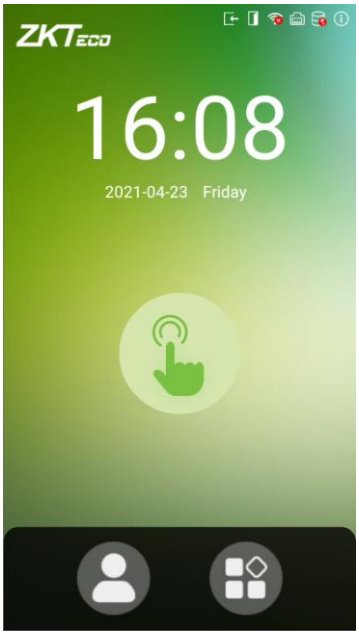
1:1 Verification Process

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

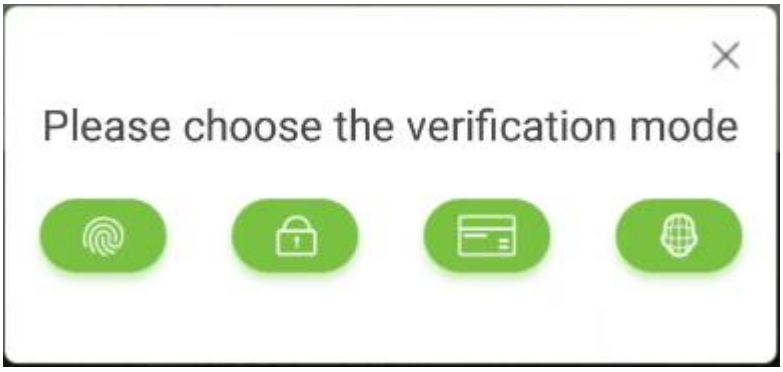
2.6.1 Password Verification

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

- On the **Main** screen, tap on the button to enter the 1:1 password verification mode.
- On the **Input** screen, enter the User ID and tap **[OK]**.



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



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

- Below are the sample for successful and unsuccessful verification

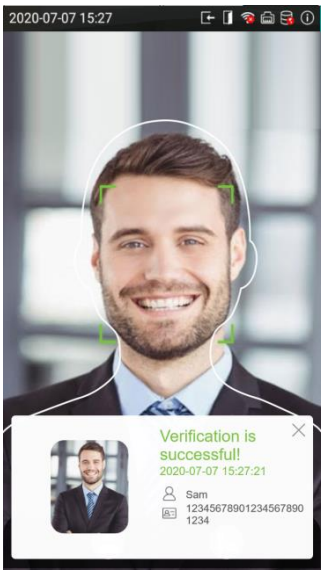
Successful Verification

Failed Verification

2.6.2 Facial Verification

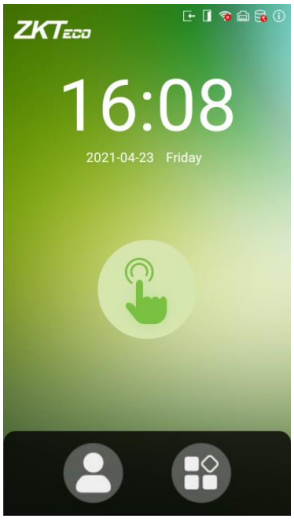
1: N Face Identification

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

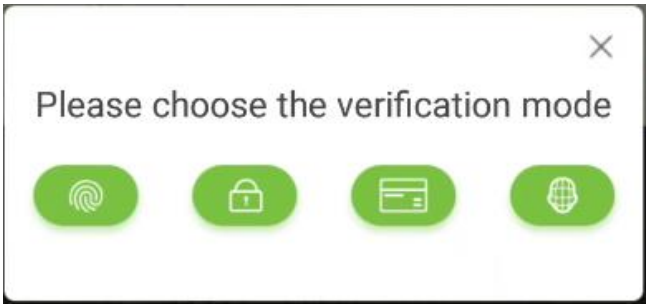


1:1 Face Verification

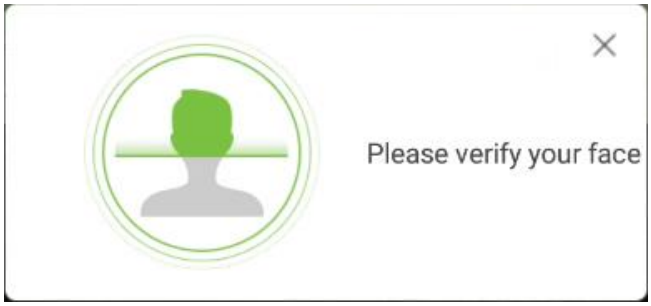
- This method verifies the face of the user captured by the camera with the facial template related to that User ID provided by the user.
- Tap on the **Main** interface to enter the 1:1 facial verification mode Input the User ID, tap [**OK**].



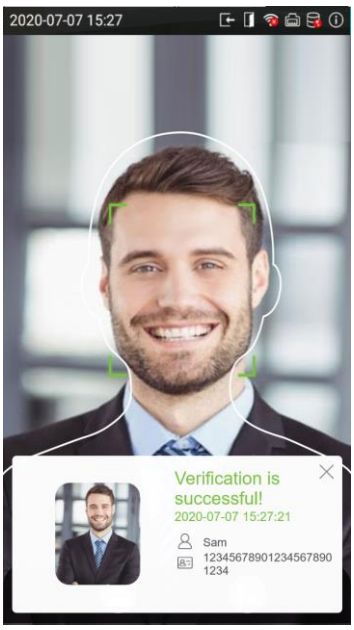
- If a user has registered a fingerprint, a password and card in addition to his/her face and the verification method is set to fingerprint/ password/ card/ face verification, the following screen will appear.
- Tap on the face button to enter the facial verification mode.



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



- Below are the sample for successful and unsuccessful verification.



Successful Verification

Failed Verification

2.6.3 Palm Verification

1: N Fingerprint Identification

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

2.6.4 Fingerprint Verification (Optional)

1: N Fingerprint Identification

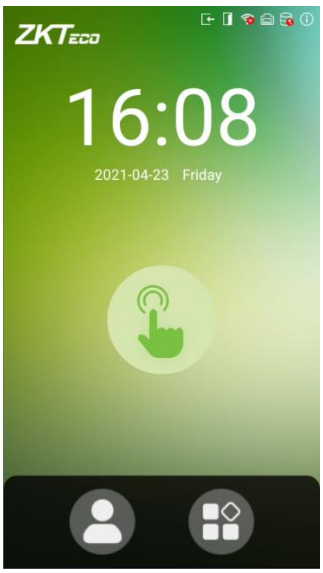
- This method compares the fingerprint of the user that is being pressed onto the fingerprint reader with all the fingerprint data that is pre- stored in the device.
- To enter fingerprint identification mode, simply tap your finger on the fingerprint reader.
- Below are the sample for successful and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

Successful Verification

Failed Verification

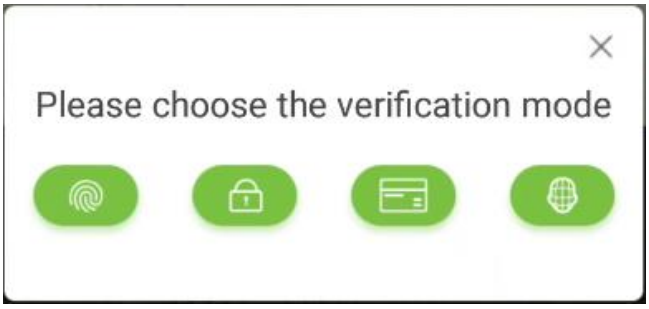
1:1 Fingerprint Verification

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



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

- Select the fingerprint button  to enter fingerprint verification mode.



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

- Below are the sample for successful and unsuccessful verification.

Successful Verification

Failed Verification

2.6.5 Card Verification

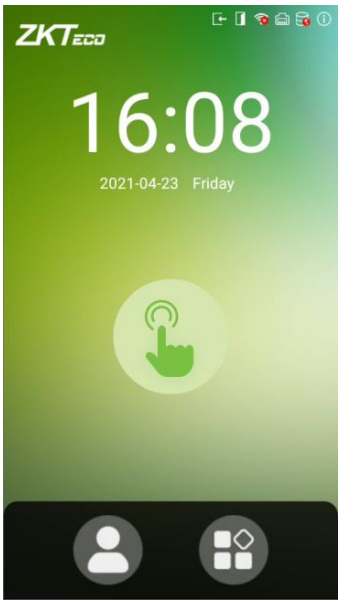
1: N Card Identification

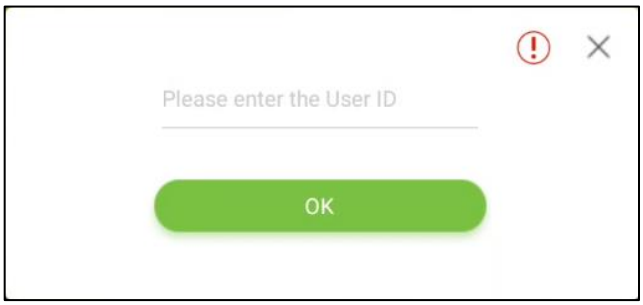
- To enter 1: N card identification mode, please place the registered card on the card reader.
- Below are the sample for successful and unsuccessful identification.

Successful Verification **Failed Verification**

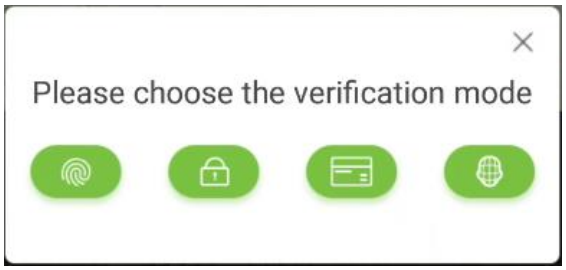
1:1 Card Verification

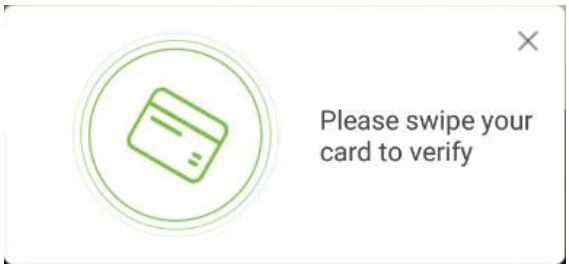
- To enter 1:1 card verification mode, tap the button on the main screen to enter 1:1 card verification mode.
- After that, enter the User ID and tap **[OK].**





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





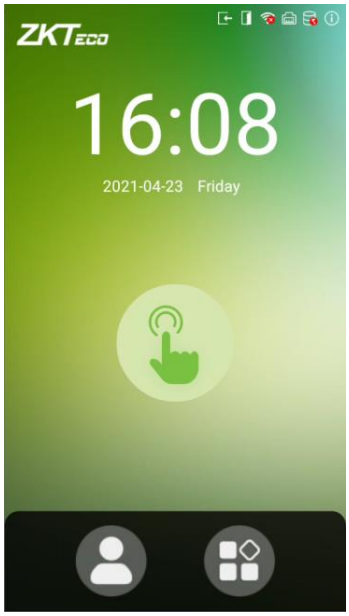
- Below are the sample for successful and unsuccessful identification.

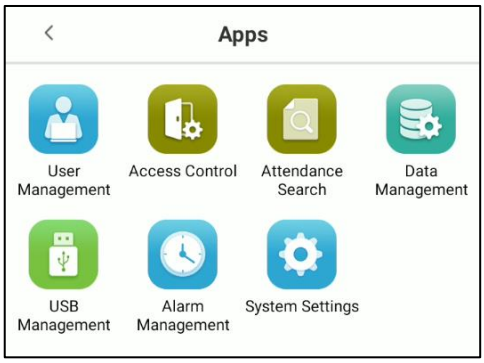
Successful Verification

Failed Verification

3 Main Menu

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





Menu Operations

Menu	Function
User Mgt.	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 and anti-passback setup.
Attendance Search	Query the specified attendance record, check attendance photos and blacklist 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	Set the network, date and time, access record, cloud service, Wiegand, display and sound, biometric parameters, auto testing, and advance settings of the device.

Note:

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

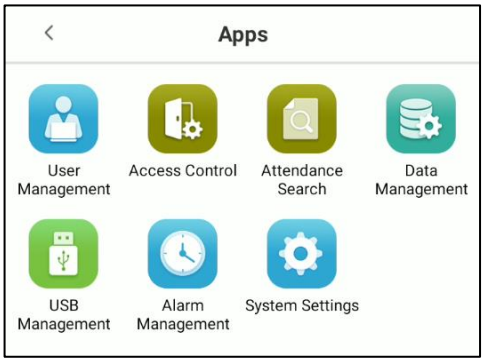
4 User Management

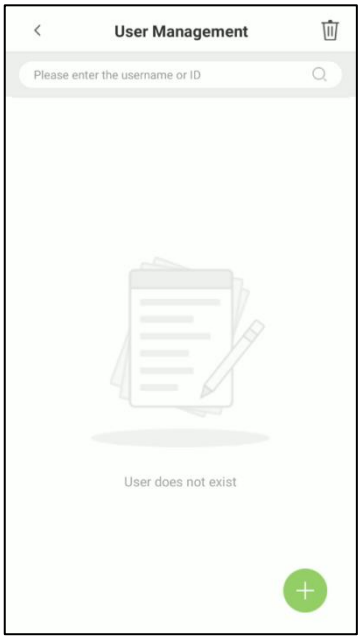
4.1 Add User

There are two methods to add users: Add user via Software or Add via Device.

4.1.1 Add Users via Device

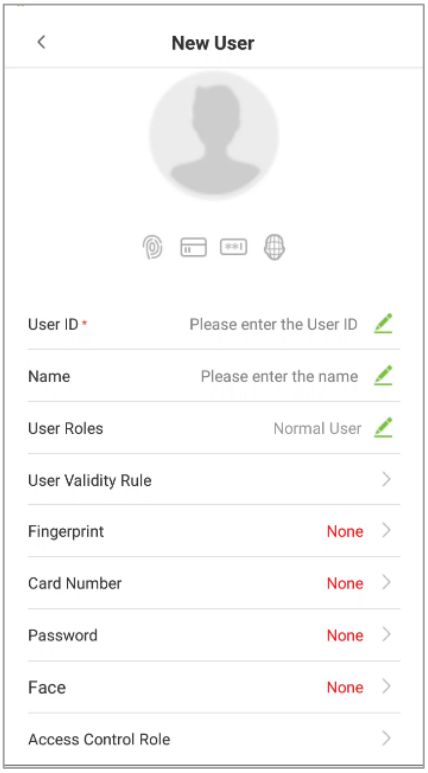
- Tap on button on the **[User Management]** interface to enter the User creation interface.





Register Basic User Information

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

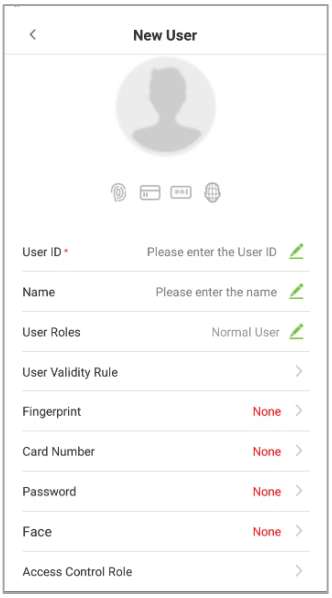


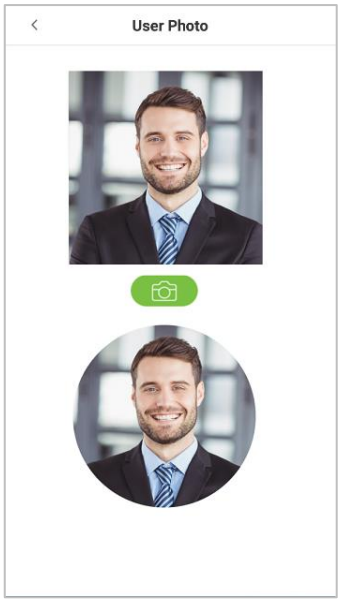
Note:

- Name: The maximum length of characters is 24.
- User ID: The user's ID can contain 1-14 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 **"This User ID already exists!"** indicates that the ID number entered is already being used. In that case, it is recommended to enter another ID number.

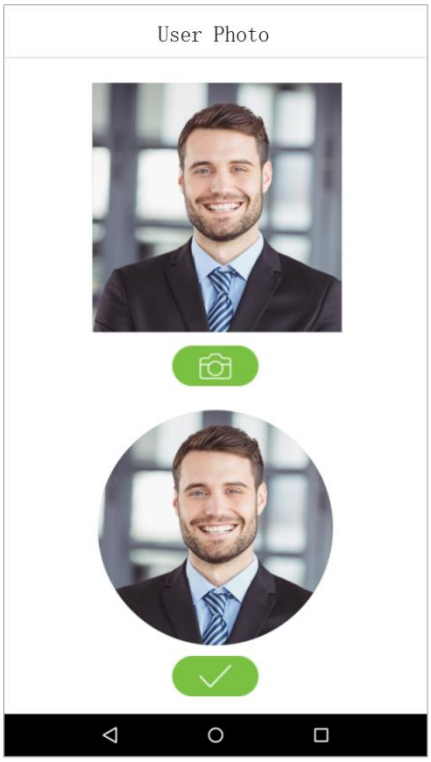
Register User Photo

- 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.





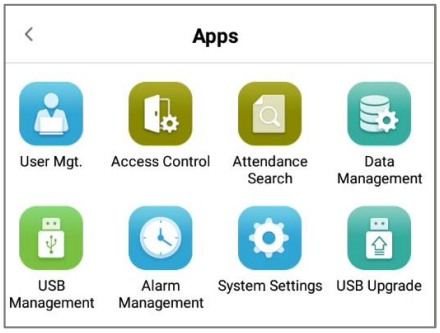
- Tap on  the button on the bottom to successfully add the captured photo.

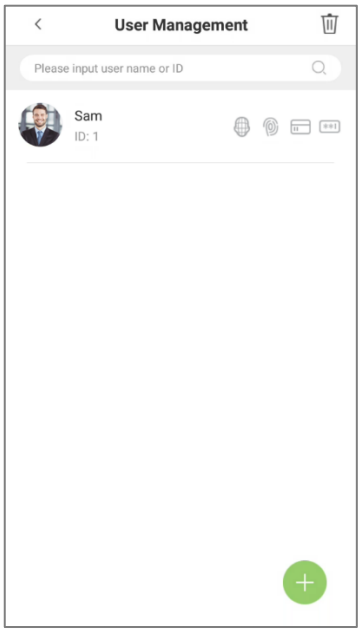


User Role

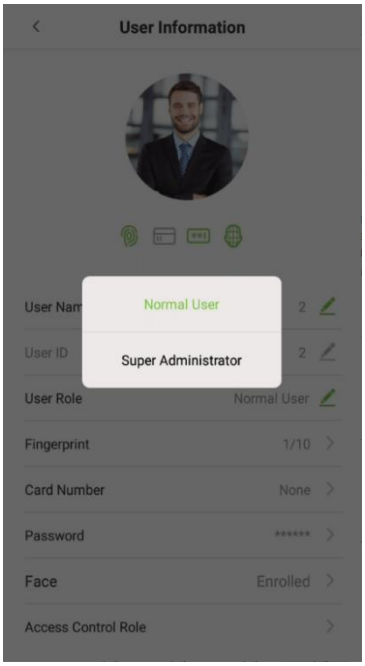
This device has two types of user privileges that is Normal User and Super Administrator. If a Super Administrator exists on the device, Normal Users can only login and view their accounts using different verification modes that have already set for the user. But a Super Administrator will have more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





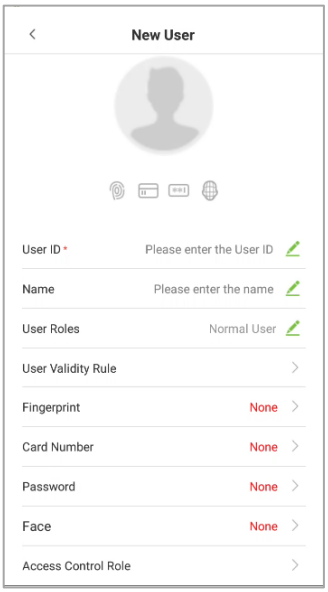
- On the **"User Information"** interface, tap **[User Role],** and then tap **[Normal User]** or **[Super Administrator]** to set the required privilege.



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".

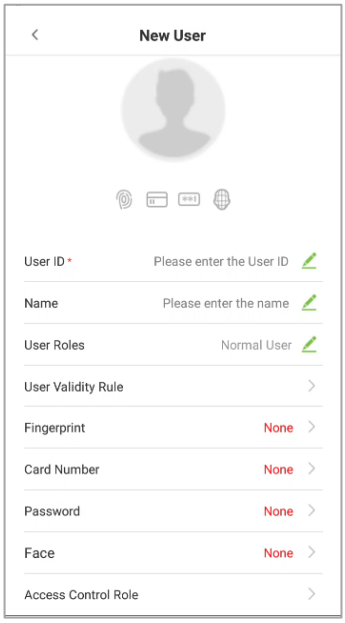
Register Verification Modes

- The different verification modes are used to verify user login.
- The verification mode includes registration of face, a password, fingerprints (optional), or card number of a user.
- On the **New User** interface, tap on the required verification mode (Fingerprint, Card Number, Password) to register for verification.



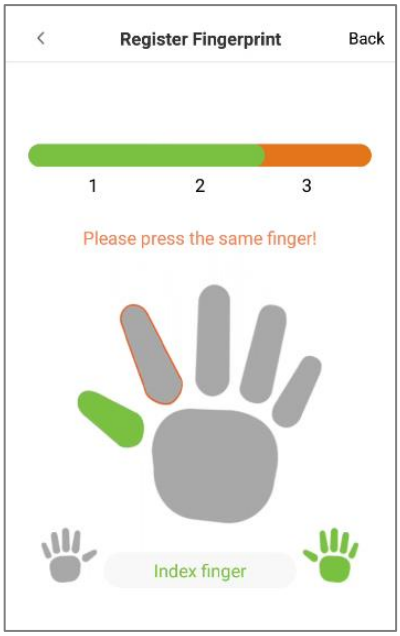
Register Fingerprint (optional)

- 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.

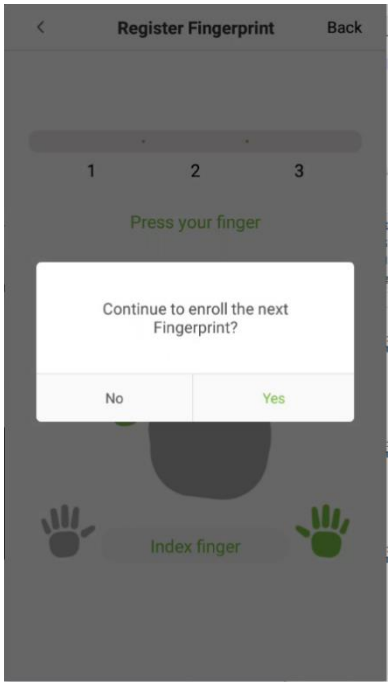


- After the selecting the required finger, press the same finger on the fingerprint reader three times.
- Green indicates that the fingerprint is enrolled successfully.

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.

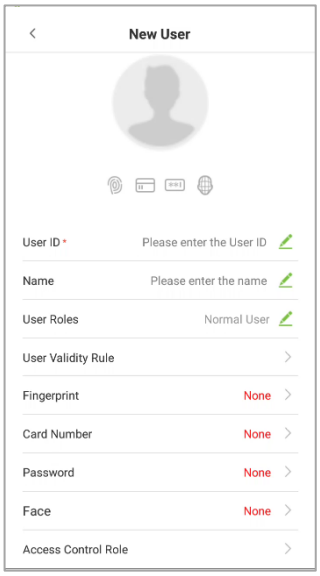


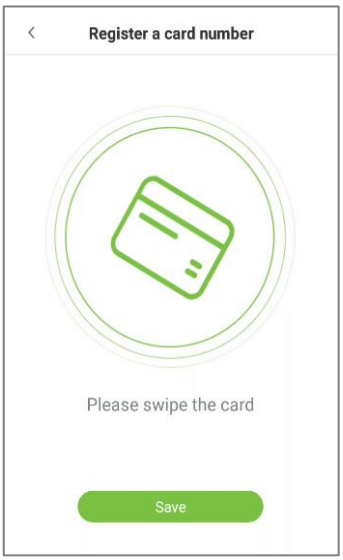
- If the fingerprint is successfully registered, **"Continue to enroll the next Fingerprint?"** dialog box will appear.
- Tap **Yes** to record the next fingerprint, or **No** to return to the fingerprint registration interface.



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.

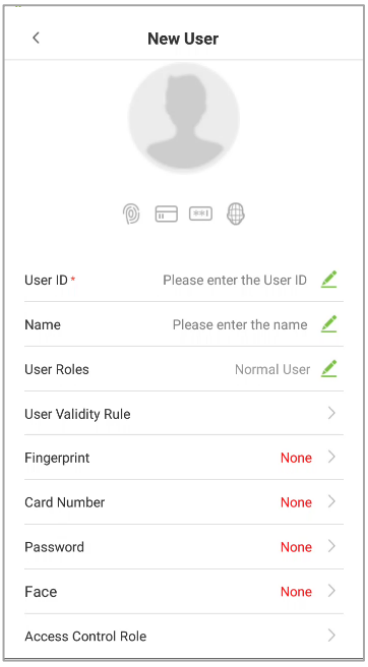


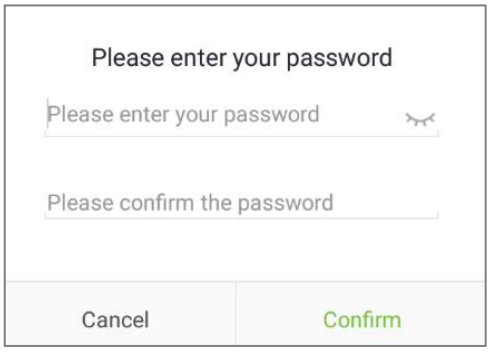


Register Password

- 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.**

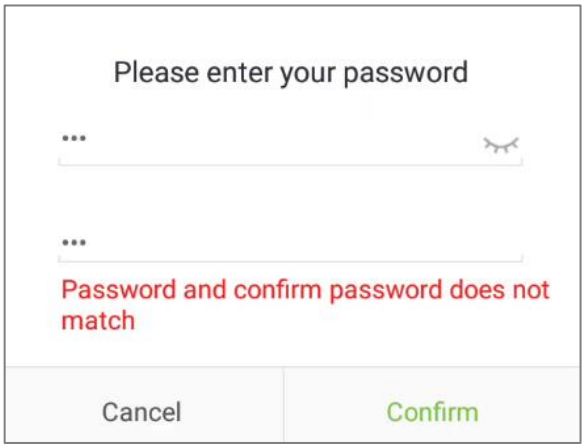
Note: The user password must be 8-digit number.





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

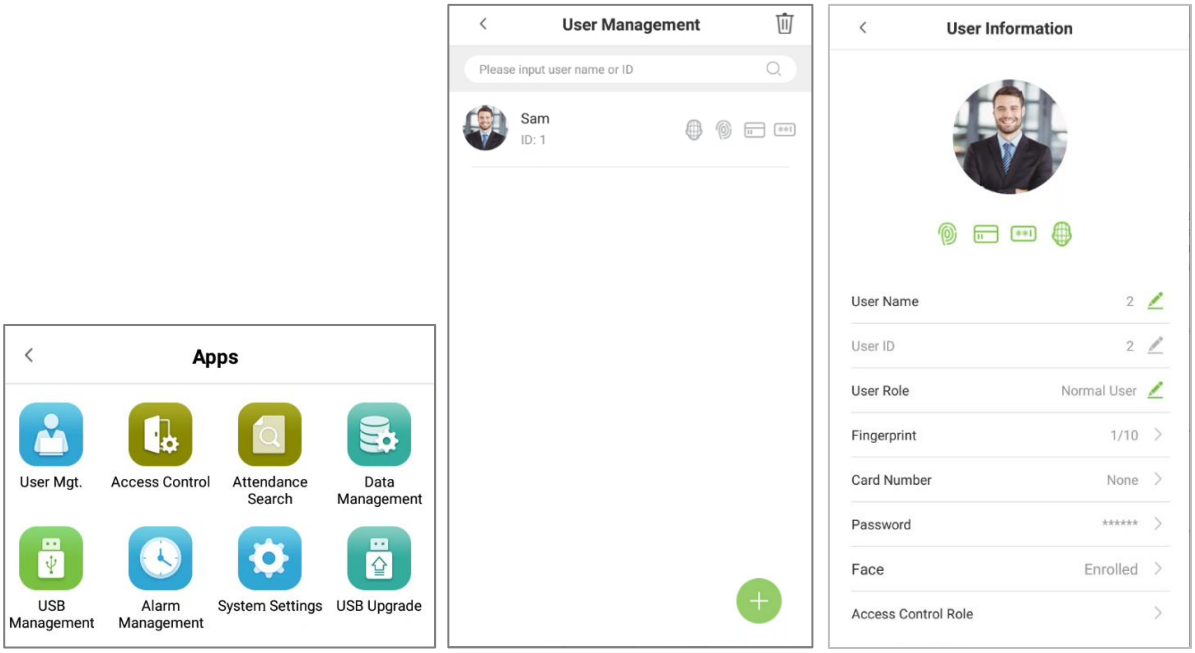
- If the password, entered in both fields does not match, then re-enter the correct password.



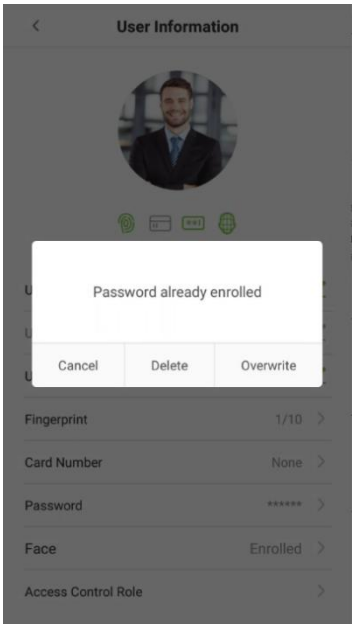
- The password which has been registered can be deleted or modified.

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.

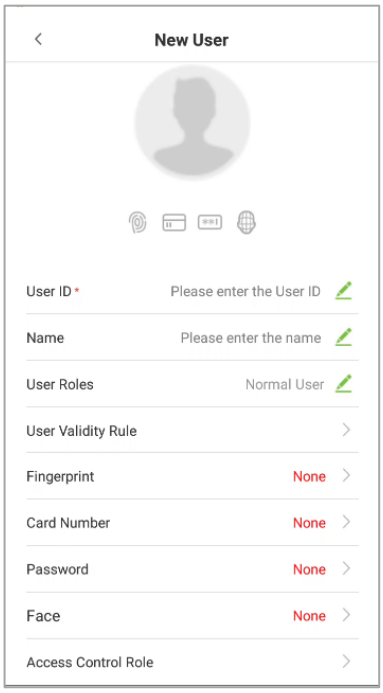


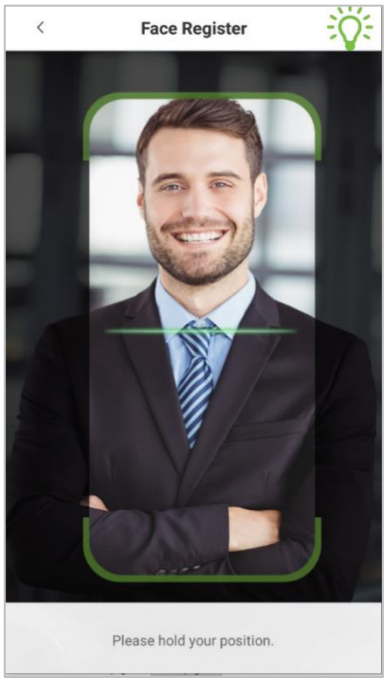
- On the pop window, tap **Delete/ Overwrite** to delete or modify the password.



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.



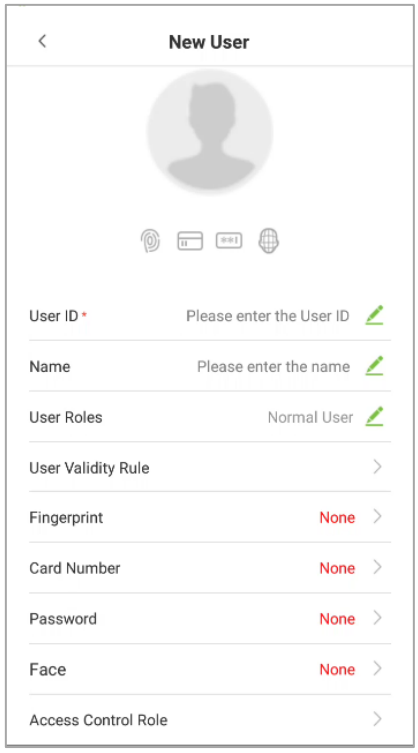


Period of Validity Settings

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.



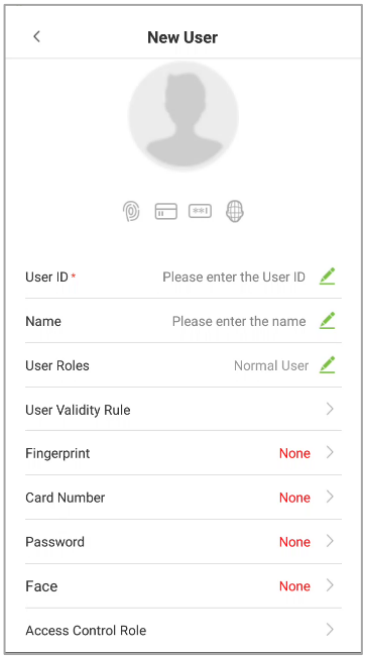
Note:

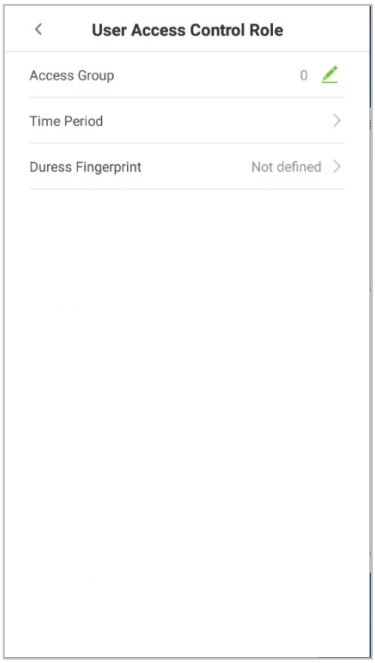
If the function **User Validity Rule** is not displayed on the **New User** interface, then on the **Main** menu, tap **System Settings** > **Access Control Record Settings**, and enable **User Validity Settings**, and then the function **"User Validity Rule"** will appear in the **New User** interface.

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

Access level

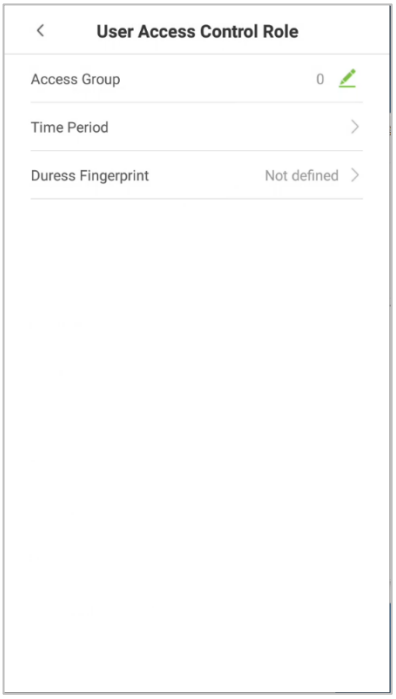
- The Access Control Role sets the door access privilege for each user.
- This includes the access group, fingerprint privilege and also facilitates to set the group access time-period.
- On the **New User** interface, tap **User Access Control Role** to set the access level.

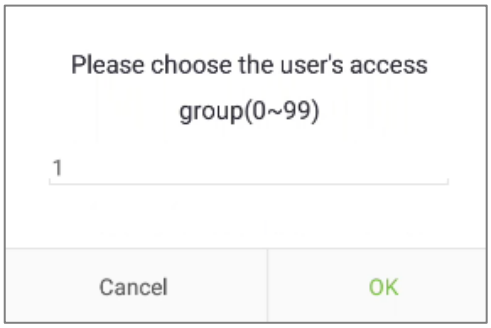




Set the Access group

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



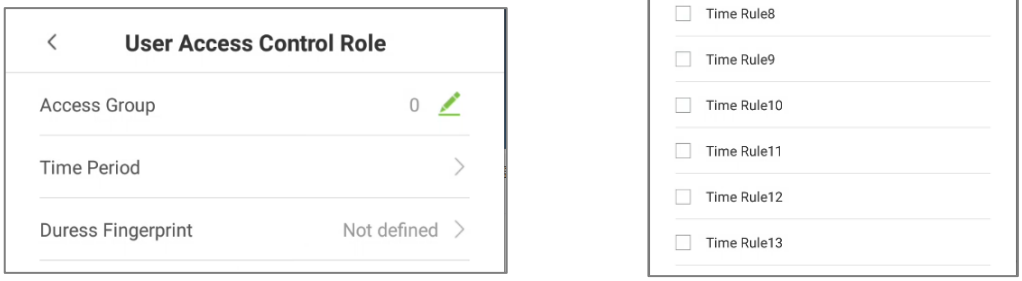


- New users will be added to Group 1 by default, which can be reassigned to other required groups.
- The device supports up to 99 access control groups.

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.

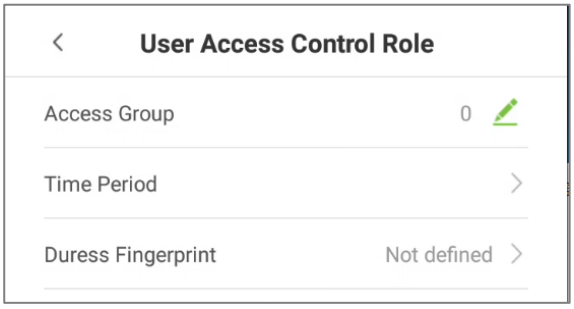


Note: A total of 50 time-rules can be set.

Duress fingerprint

The user may specify one or more fingerprints to register as duress fingerprint(s). Hence, once the user presses the corresponding finger on the sensor, and if the verification is successful, then the system will immediately generate the alarm.

- On the **User Access Control Role**, tap **Duress Fingerprint** to set the duress access.



4.1.2 Add Users on the Software

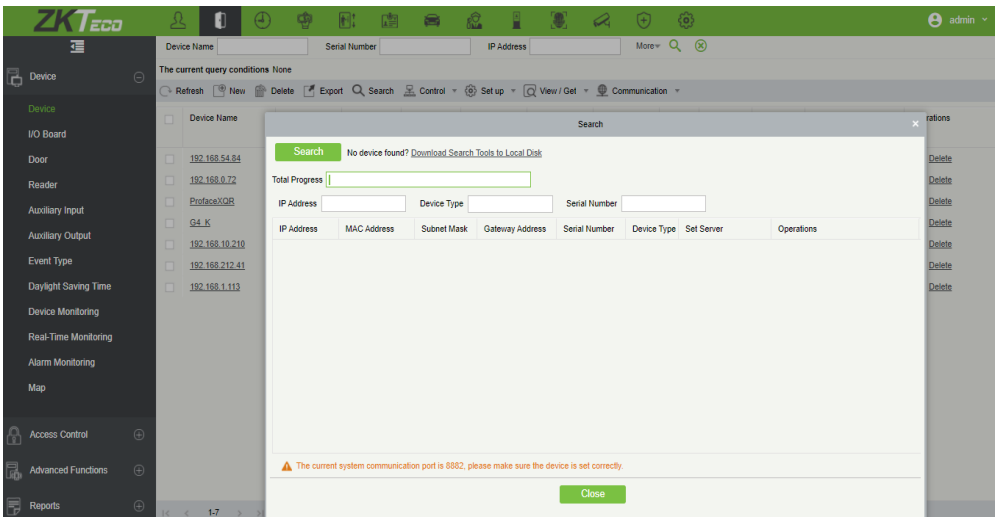
Connect software

Recommended to use **ZKBioSecurity V5000/V6000/V6600**, otherwise the function and interface may be different.

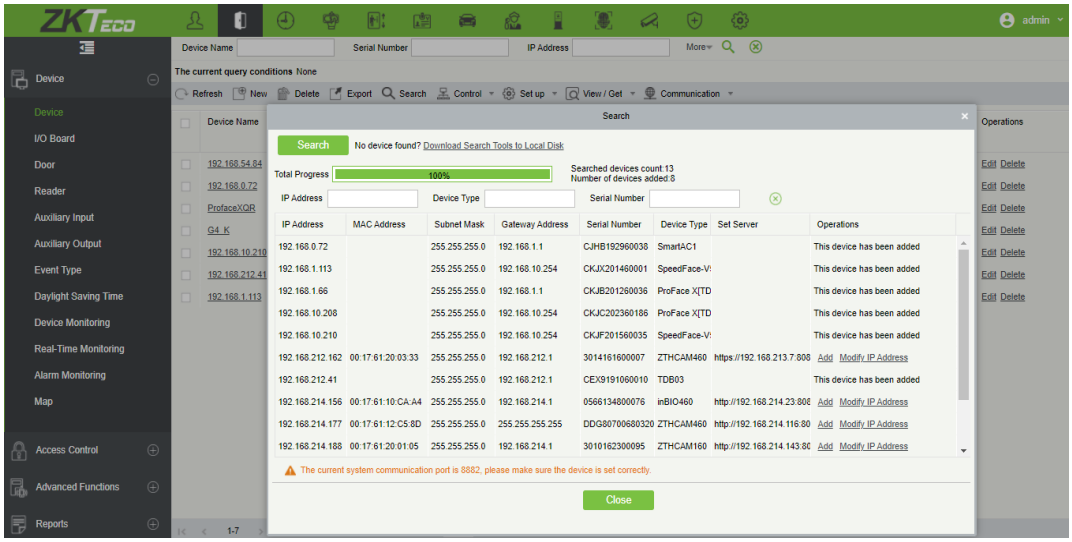
- Before adding employees, please ensure that the device is connected to the PC through the network cable and set the device IP.
- The device IP and computer IP should be in the same network segment.
- Please refer to Ethernet Settings for details.
- Tap **[System Settings]** > **[Cloud Service Settings]** to set the cloud server parameters according to the software address displayed in the browser (Note: the default server port is 8088).
- Please refer to Cloud Service Settings for details.

Add Devices

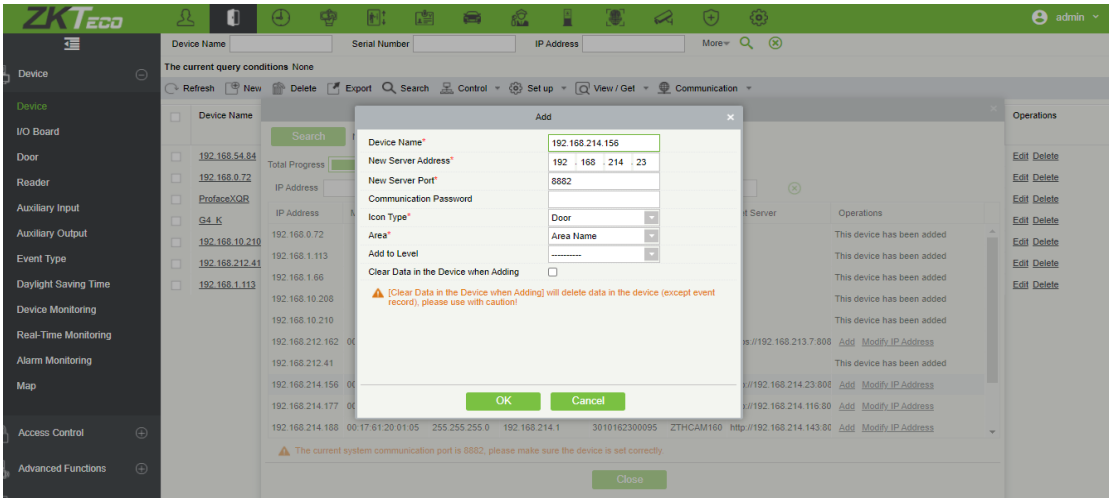
- On the software, click **Access** > **Device** >**Search** to search for the active registered devices.



- Click **"Search"** to search for the registered devices.
- After the search is completed, the total number of registered devices.



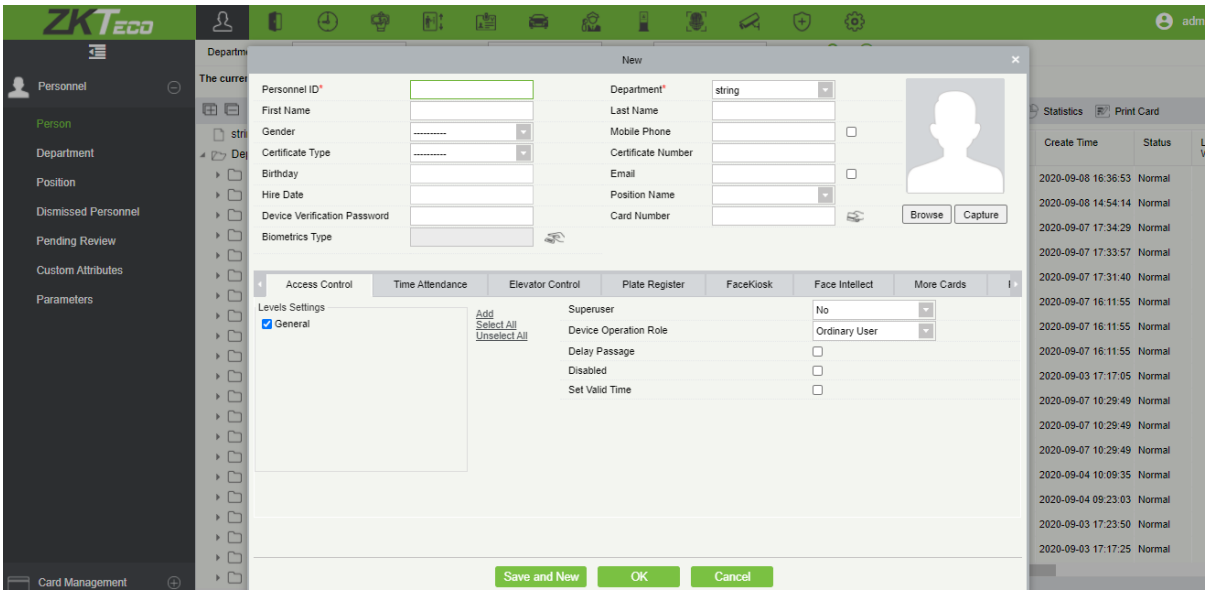
- Click **"Add"**, fill in the device's details, and then click **"OK"** to complete adding devices.



- The default IP address of the device may conflict with others in the network, so the IP address of the new device needs to be modified before use.

Add Person

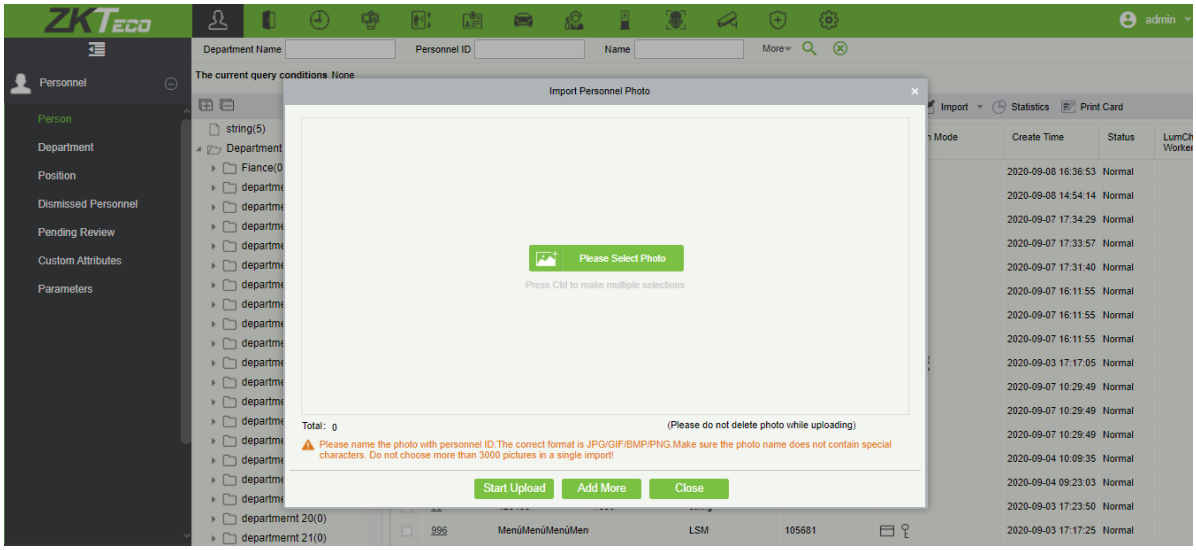
- On the **Personnel** module, click **Person**> **New/Add** to configure the Personnel details.



- After filling in the personnel information, click **OK** to save and exit, and the personnel will be displayed in the personnel list.

Batch import personnel photos

- On the **Personnel** module, click **Person** > **Import**>-**Import Personnel Photo**, select the photo to import.

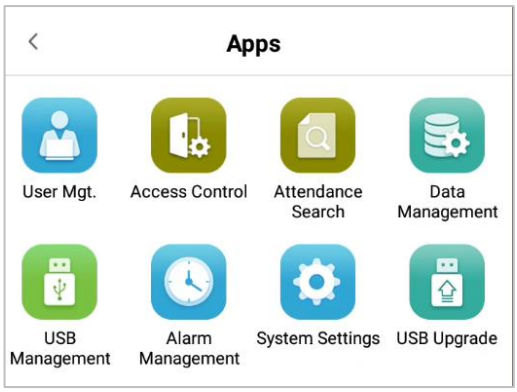


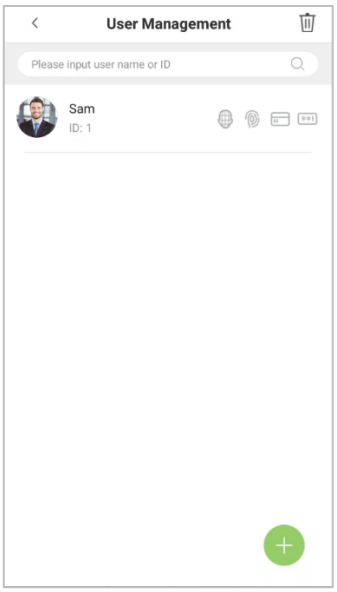
4.2 Search User

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

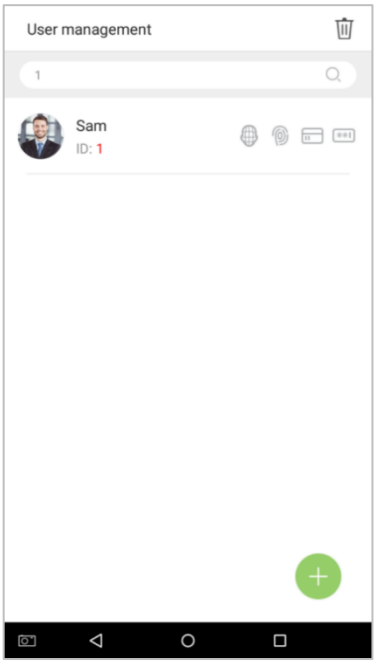
- Tap on the search bar located on the [**User Management**] interface and search for the required username.

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



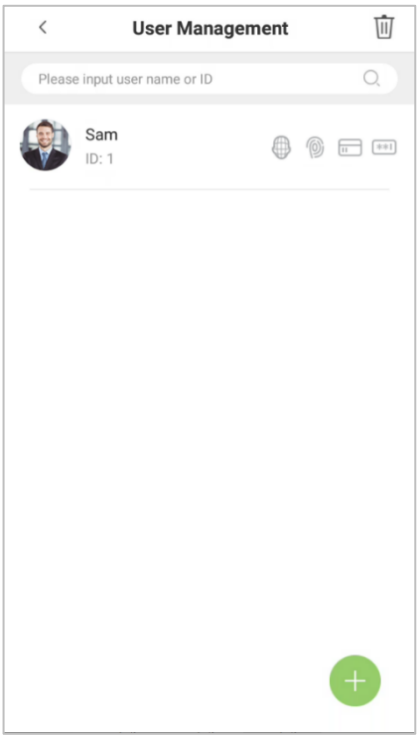


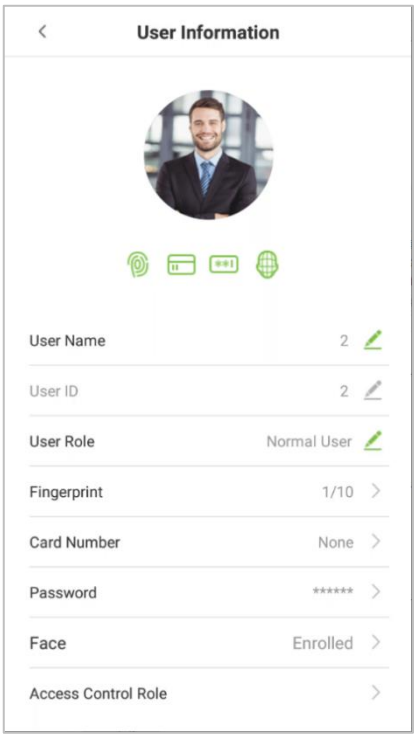
- Tap on the **Search** bar to search for the users with the relevant user ID/name and the system will automatically find the users with information that is relevant to the search query.



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.

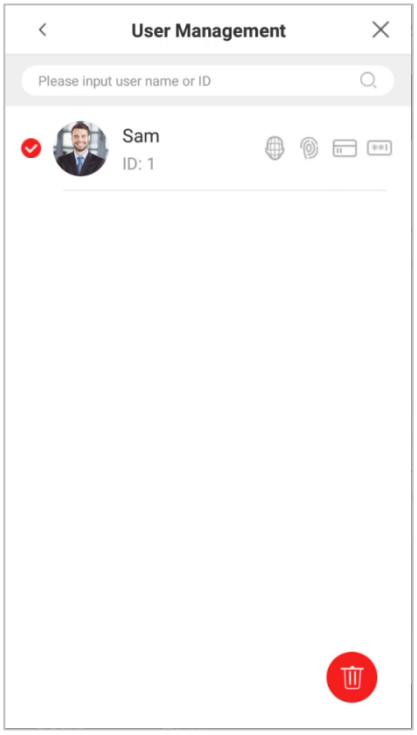


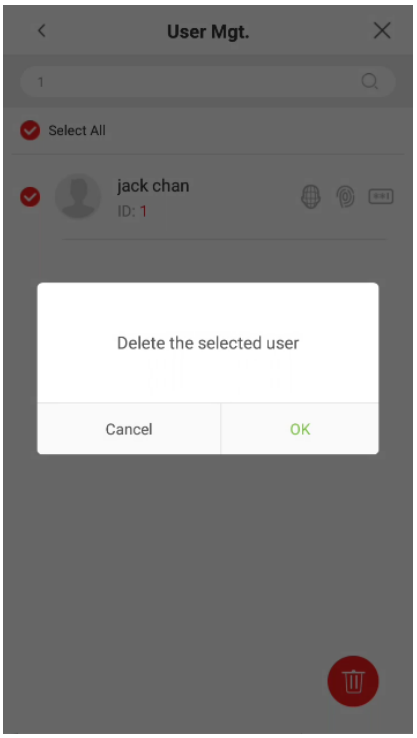


Note: Please notice that the user ID cannot be modified, and other operations are similar to adding a new user. For further information, please see section "Add User".

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.

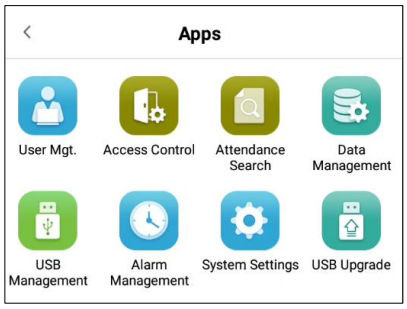
5 Access Settings

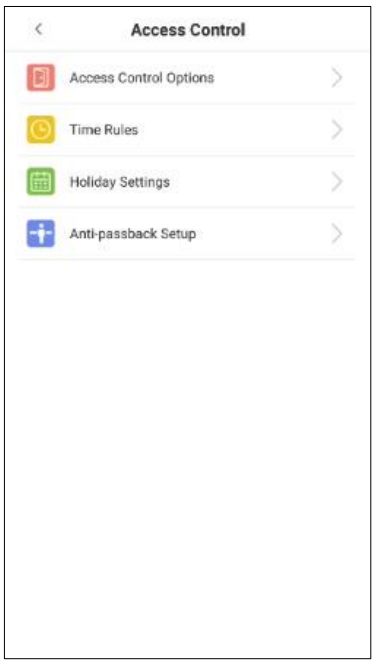
The **Access Settings** facilitates to set the access parameters.

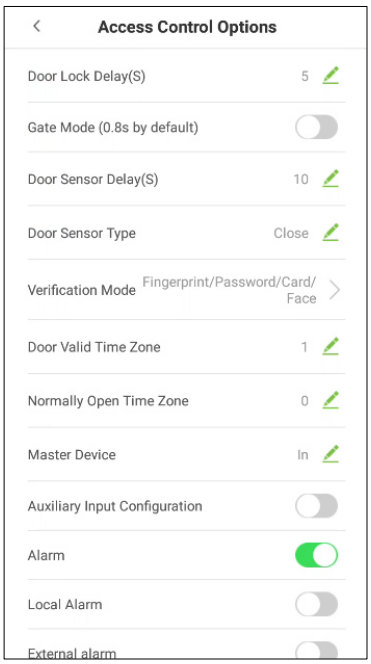
5.1 Access Control Options

Access Control Options are used for setting the access parameters.

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







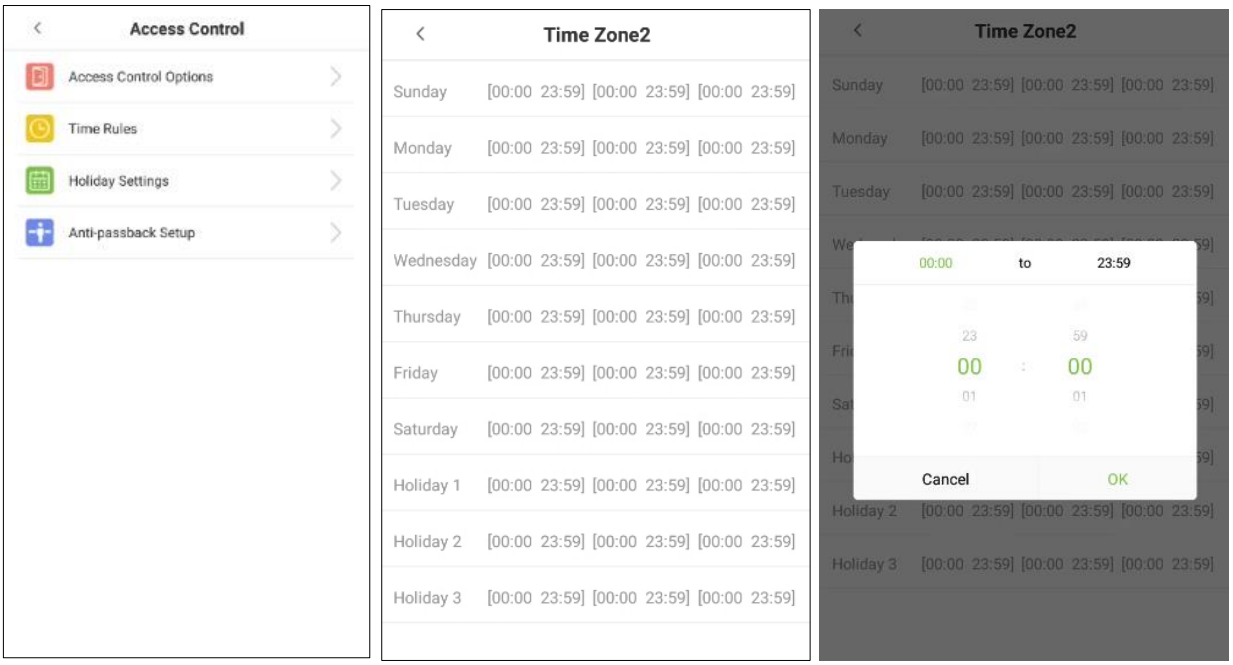
- The **Access control** options includes the following functions.

Menu Options	Function Description
Door lock delay	The length of time that the device controls the electric lock to be in unlock state. Valid value: 1~10 seconds; 0 second represents disabling the function.
Gate Mode	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	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 type	There are three Sensor types: Close, Normal Open and Normal Closed. Close: It means door sensor is not in use. Normal Open: It means the door is always left opened when electric power is on. Normal Closed: It means the door is always left closed when electric power is on.

Verification Mode	The supported verification mode includes fingerprint/password/face/card, User ID only, password, face only, and face + password. The default is fingerprint/password/face/card.
Door Valid Time Zone	To set time period for door, so that the door is available only during that period.
Normally Open Time Zone	Scheduled time period for "Normal Open" mode, so that the door is always left open during this period.
Master device	When setting up the master and slave, the status of the master can be set to exit on enter. Exit: The record verified on the host is the exit record. Enter: The record verified on the host is the entry record.
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 access control reset parameters include door lock delay, door sensor delay, door sensor type, verification mode, door valid time zone, normally open time zone, master device, and alarm. However, erased access control data in Data Mgt. is excluded.

5.2 Time Rules Settings

- On the **Access Control** interface, tap **Time Rules** to set the Time Rule.
- The entire system can define up to **50** Time Rules (that is Time Rule1, Time Rule2, …. Time Rule 50).
- Each Time Rule represents **7** Time Zones, i.e. **1** week and 3 holidays, and each Time Zone is a standard 24-hour period per day and the user can only verify within the valid time period.
- For each Time Zone you can set a maximum of **3** Time Periods. The relationship among these Time Periods is "or".
- When the Verification Time falls in any one of these Time Periods, the verification will be successful and valid.
- Time Zone format for each Time Period: HH MM-HH MM, accurate to minutes by 24-hour clock.
- Tap on the grey box to search for the required **Time Rule.** Enter the required Time Rule set (that is, search as "Time Rule 1" …" Time Rule 50").
- On the **Time Zone** interface, tap on the day (that is Sunday, Monday …) in which the Time Period needs to be set.
- On the **Time Period 1** interface, set the Start and End time, and then tap **OK.**



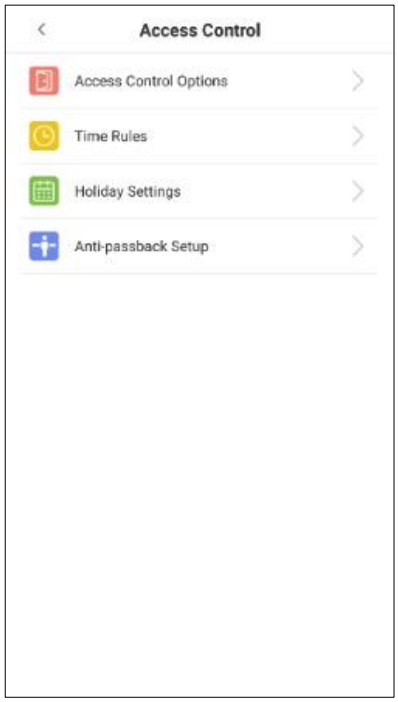
Note:

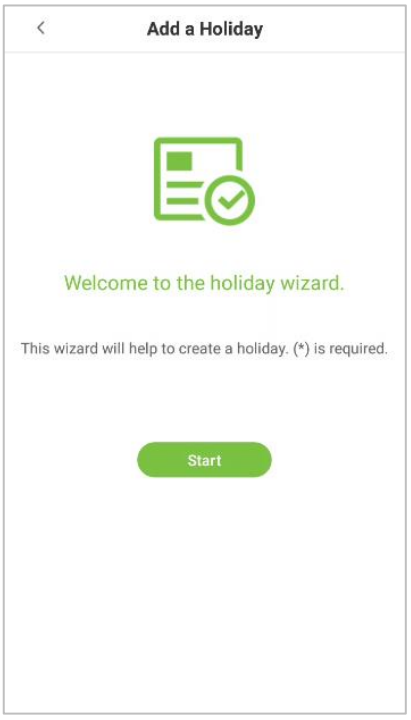
- When the End Time is earlier than the Start Time, (such as 23:57~23:56), it indicates that access is prohibited all day.
- When the End Time is later than the Start Time, (such as 00:00~23:59), it indicates that the interval is valid.
- The effective Time Period to keep the Door unlock or open all 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

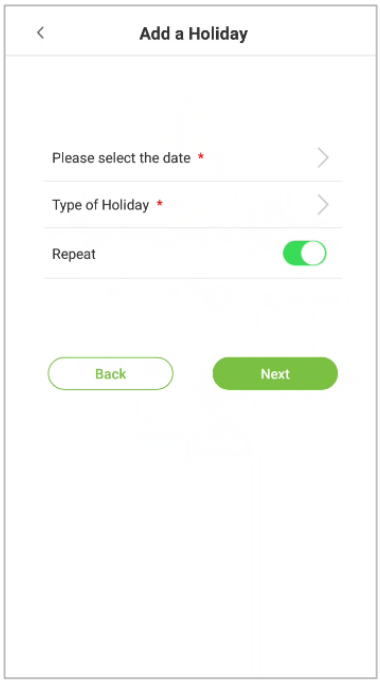
Whenever there is a holiday, you may need a special access time; but changing everyone's access time one by one is extremely cumbersome, so you can set a holiday access time which is applicable to all users, and the user will be able to open the door during the holidays. The time set here is taken as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

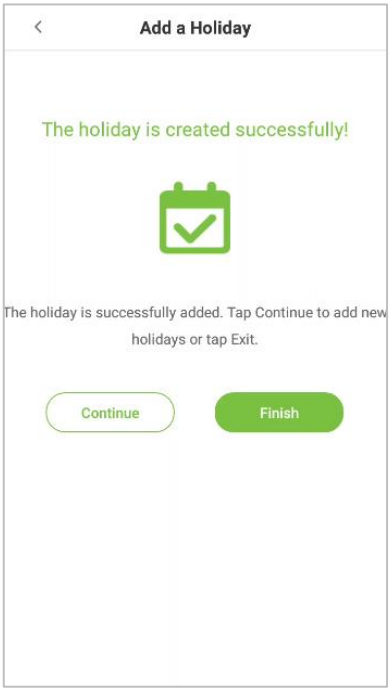
- Tap **[Holiday setting]** and then tap on + the button to create a new holiday.

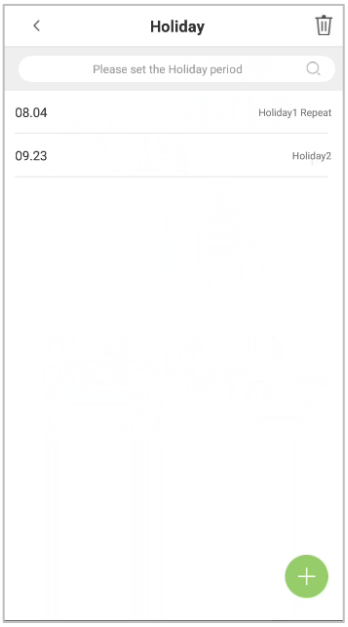




- On the **[Holiday setting]** interface, select a date and type of the holiday. Enable [Repeat] to repeat the holiday yearly and then tap [**Next**].
- On this interface, tap either **Finish** to successfully add the newly created holiday, or tap **Continue** to create another holiday.





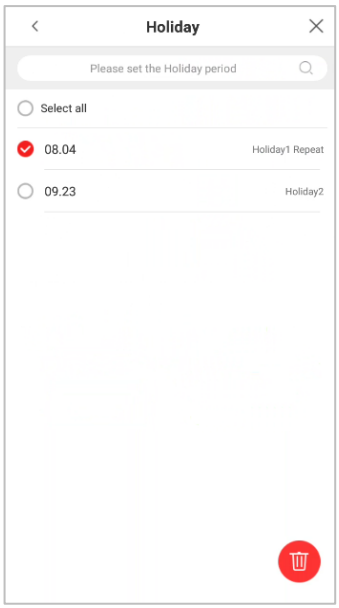


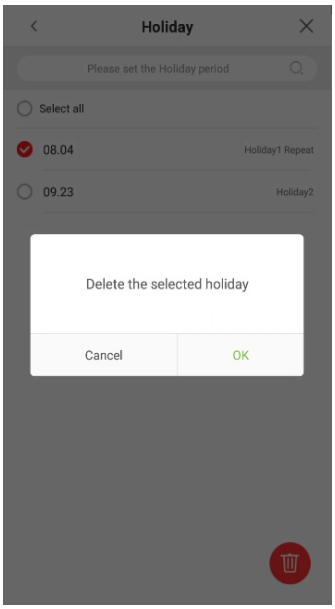
Edit Holiday

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

Delete a Holiday

- On the "**Holiday period**" 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 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.

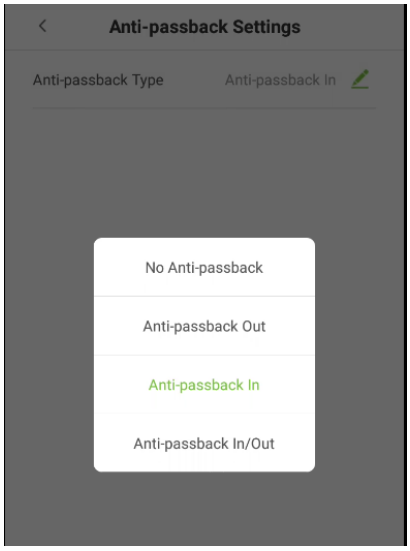
So, if any personnel enter an access-controlled area following another person without authenticating on the biometric device, then the next time during his out-time, the door does not open when that person attempts to leave the area. This function uses to detect whether the user's access is legal by 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:

- **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.

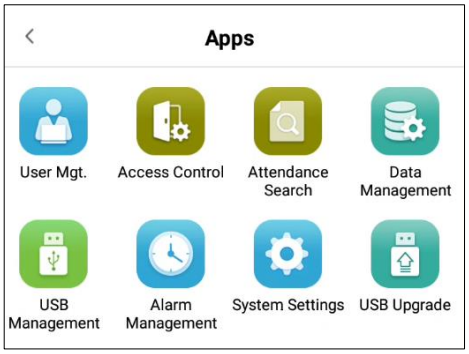
Note: When the user has no record during the first verification, the anti-passback approval is passed directly. This access direction depends on the selection of the control direction of the device, corresponding to the state of the device.

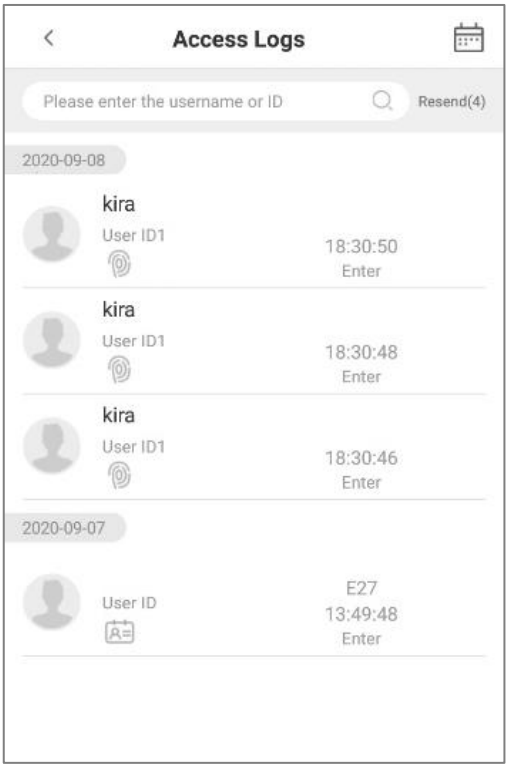
- The interface is shown below:



6 Attendance Search

- User access records will be saved in the device, making it easier to find the required attendance records of the users.
- Users can search for access logs, access photos, and block listed photos.
- Searches support searching by either username or ID or a combination of the two.
- On the **Main** menu, tap **Attendance Search**, to search for required user's access log.

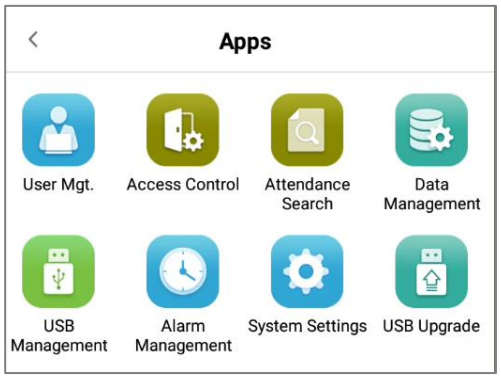


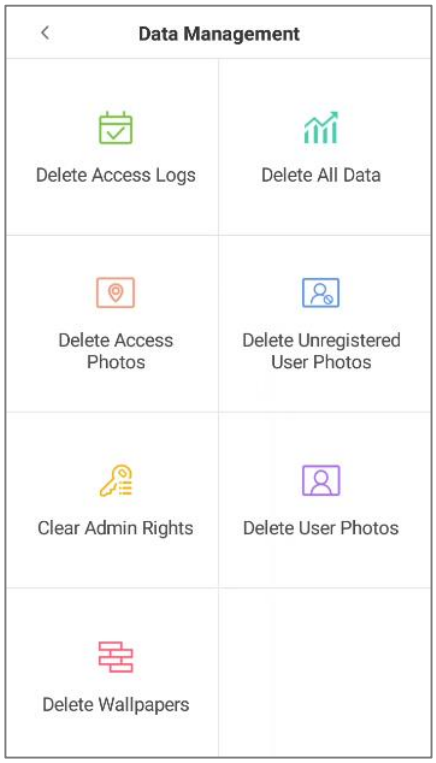


7 Data Management

The Data Management Settings allows the users to manage the device data, including Delete Access Logs, Delete All Data, Delete Access Photos, Delete Unregistered User Photos, Clear Admin Rights, Delete User Photos, And Delete Wallpapers.

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





Function Description

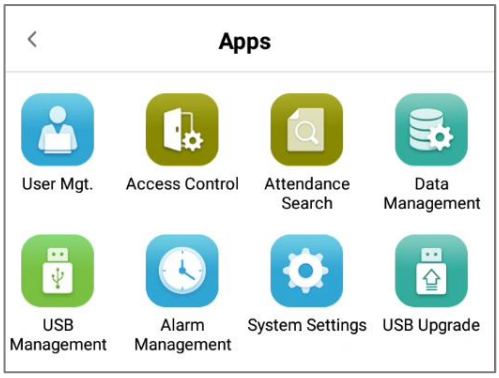
Function Name	Function Description
Delete Access Logs	1. Deletes all the logs. 2. Deletes the access logs within a specified time range.
Delete All Data	Deletes the business data stored in the device, including access logs, password/ facial biometric data, privileges of the super admin, user photos, user data, and access control data.
Delete Access Photos	1. Deletes all the logs 2. Deletes invalid user accounts 3. Deletes the access photos within a specified time range.
Delete Unregistered User Photos	1. Deletes all (including access records and the photos of the user in blocklist) 2. Deletes the unregistered user photo within specified time range.

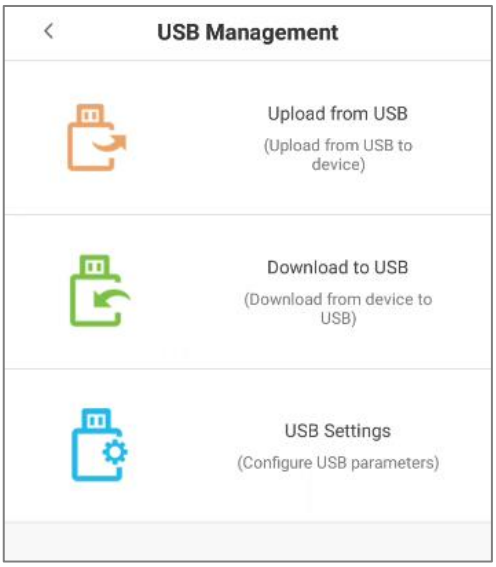
Delete Admin Rights	Changes the super administrator into a normal user.
Delete User Photos	Deletes all the user photos.
Delete Wallpapers	Deletes all the wallpapers stored in the device.

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.





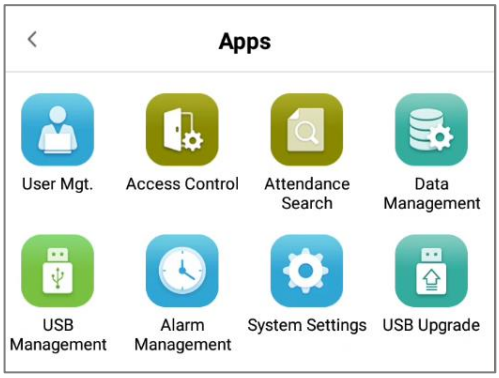
Function Description

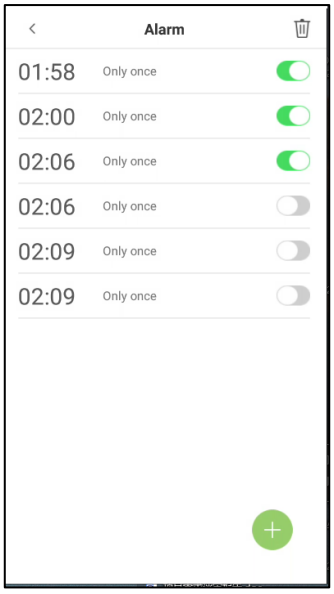
Menu Options	Function Description
Upload from USB	Upload USB disk content to the device.
Download to USB	Download the data from the device to the USB disk.
USB Settings	Configure the parameters of USB disk.

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.

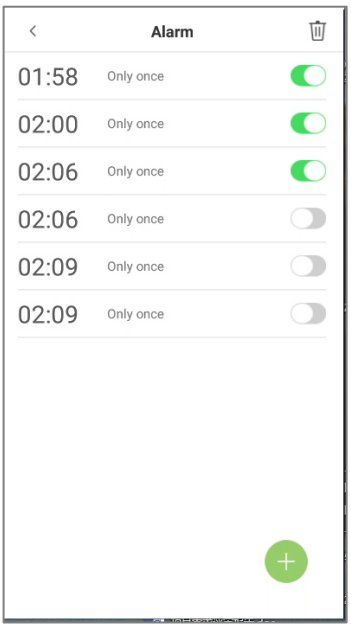
- On the **Main** menu, tap **Alarm Management** to configure the alarm settings.

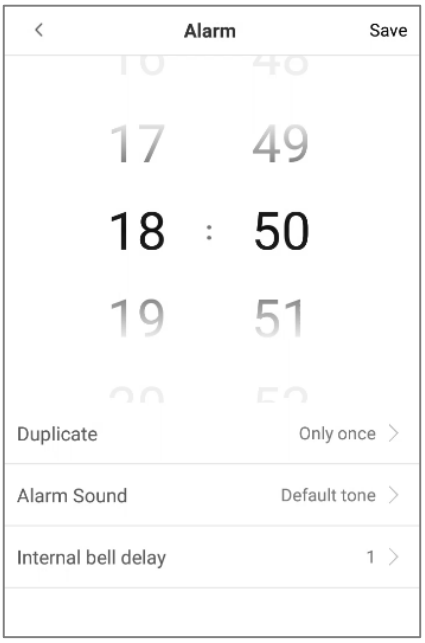




9.1 Add Alarm

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



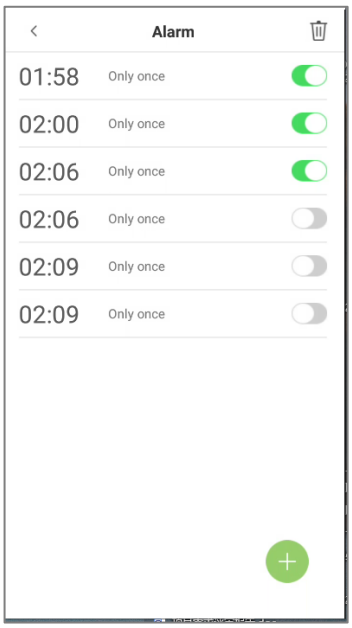


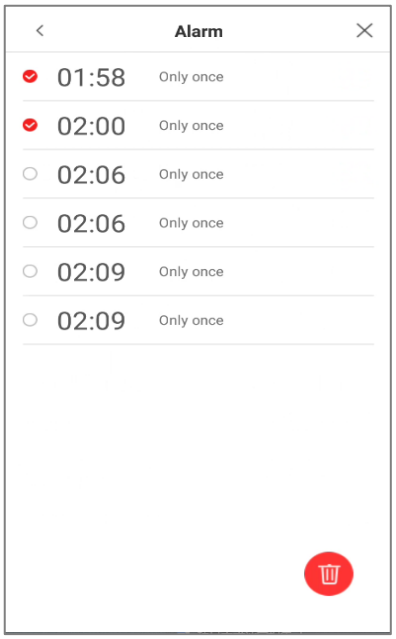
Menu Options	Function Description
Duplicate	Set the required number of counts to repeat the scheduled bell.
Alarm Sound	Select a ring tone.

Internal bell delay(s)	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 click the button that is displaying in the lower-right corner of the screen.

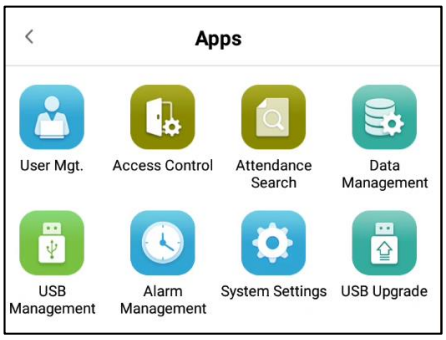


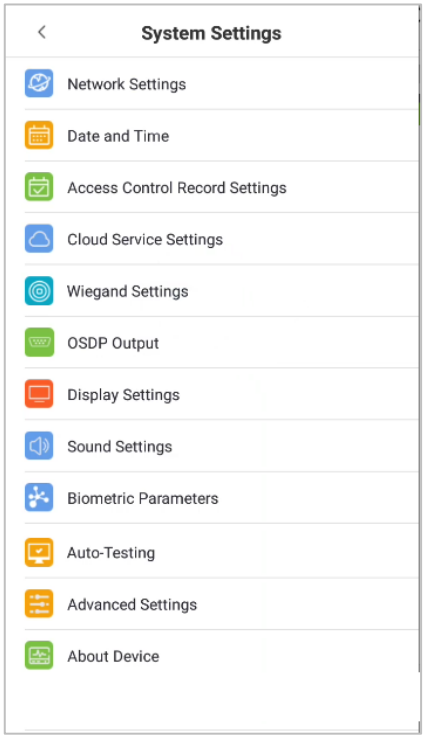


10 System Settings

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, access control record settings, Cloud service settings, Wiegand settings etc.

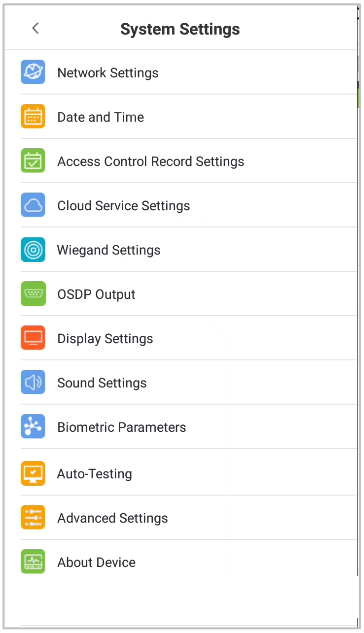
- On the **Main** menu, tap **[System Settings]** to configure the device settings.

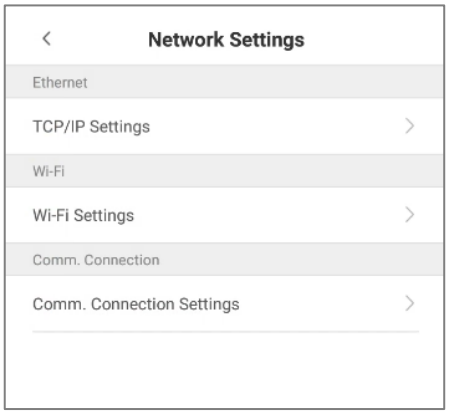




10.1 Network Settings

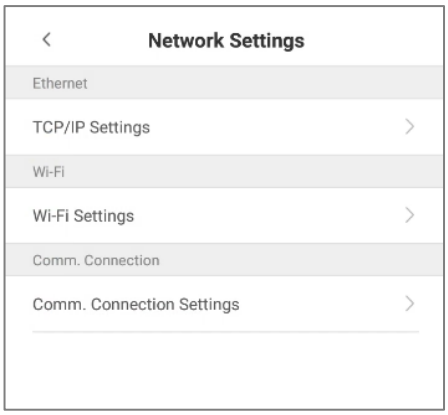
- On the **System Settings** interface, tap **[Network Settings]** to configure the settings

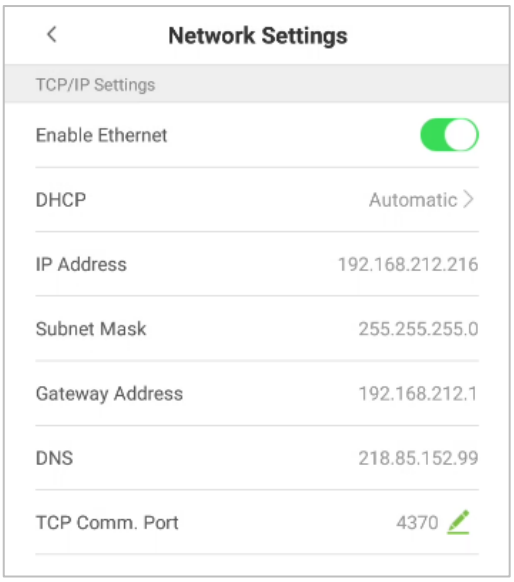




10.1.1 Ethernet Settings

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:





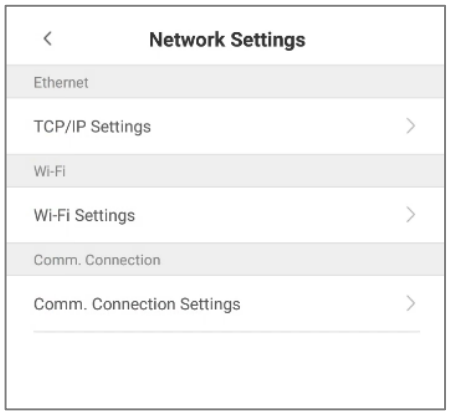
Function Descriptions

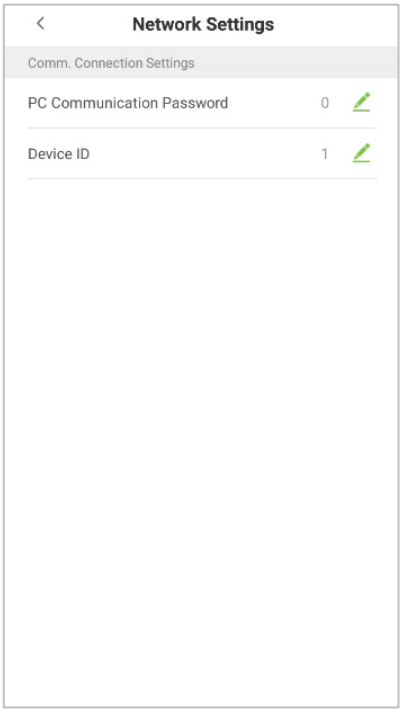
Menu Options	Function Description
Enable Ethernet Switch	Enable to modify the Ethernet network address parameters. If this is not enabled, users cannot modify the Ethernet network address parameters.
DHCP	Enable DHCP to assign an IP address to the internal network or network service provider. If DHCP 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 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.**





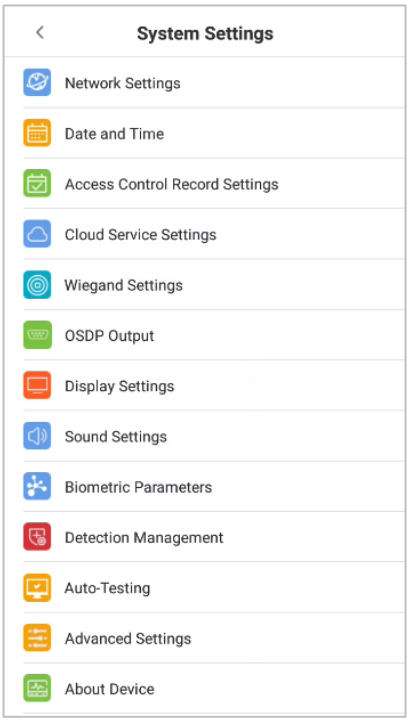
Function Description

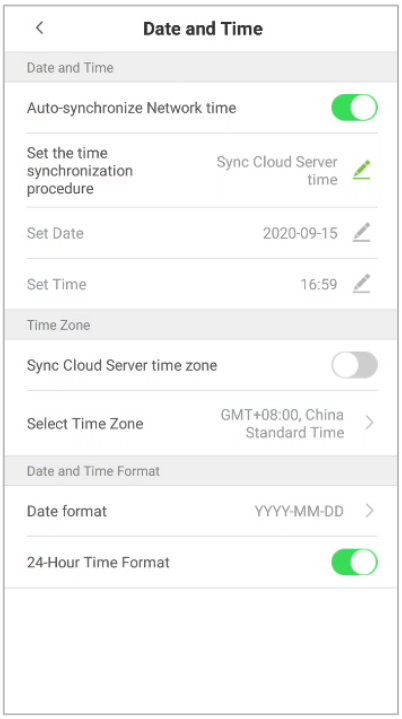
Menu Options	Function Description
PC Communication password	It is used to gain the connection permission when using offline SDK or PULL SDK connection. If the password is not correct, the communication connection cannot be built. The value ranges from 0 to 999999. When the value is 0, there is no code 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

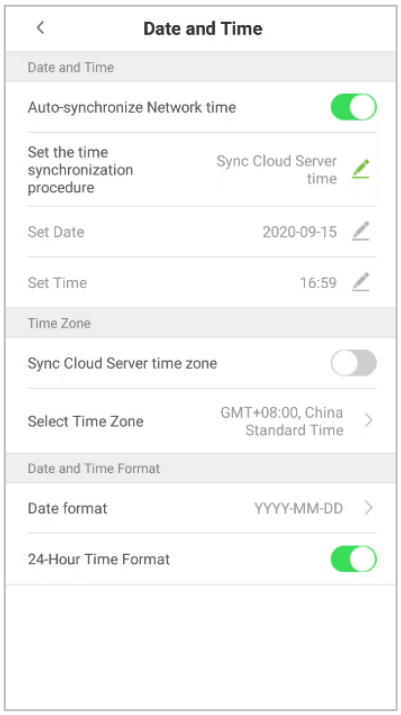
10.2.1 Date and Time Settings

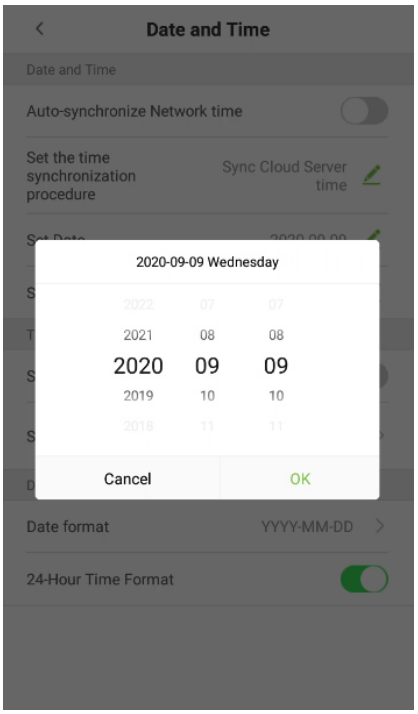
- On the **System Settings** interface, tap **Date and Time** to enter the **Date and Time** Settings interface.



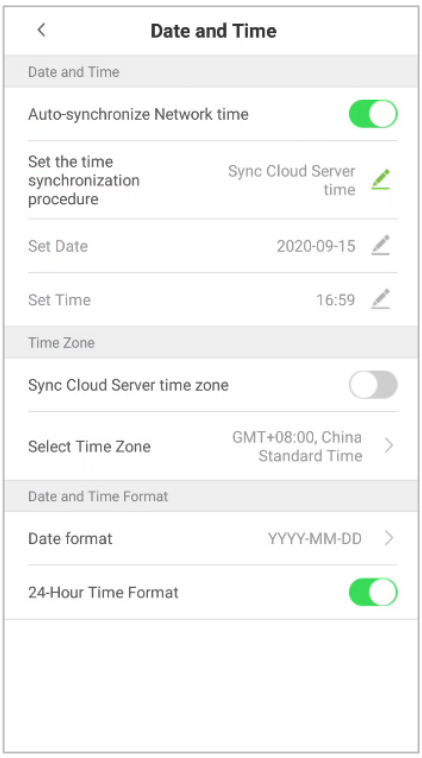


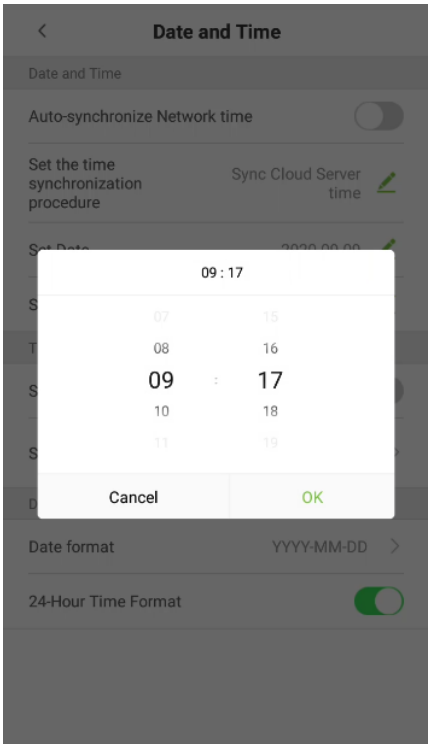
- Tap **Set Date** and swipe up and down to set the year, month, and day.
- After setting required Date, tap **OK.**





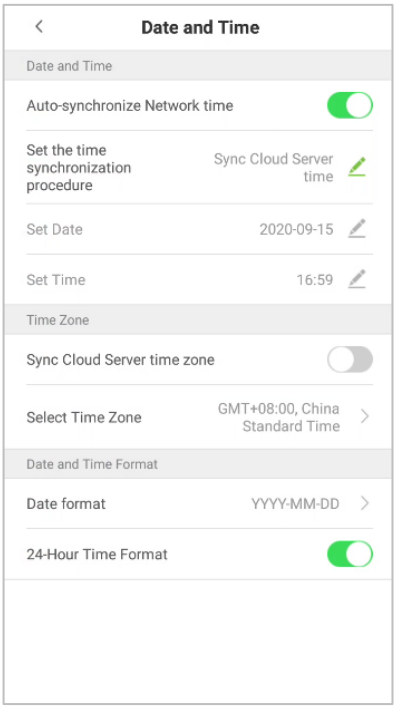
- Tap **Set Time** and swipe up and down to set the hour and minute.
- After setting time, tap **OK.**

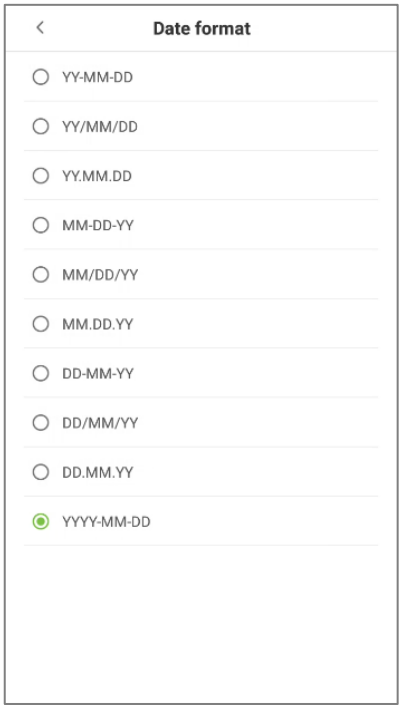




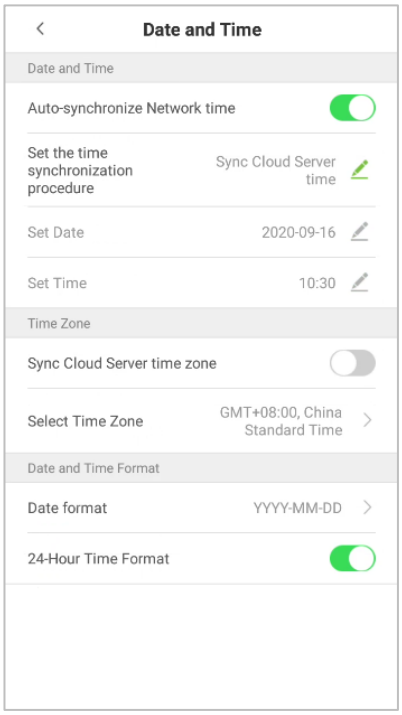
10.2.2 Date and Time Format Settings

- 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

Menu Options	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.

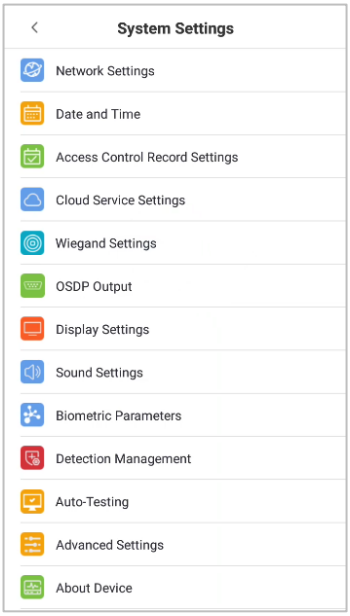
10.3 Access Control Record Settings

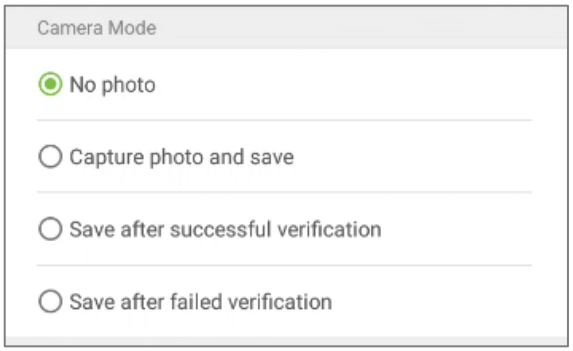
- On the **System Settings** interface, tap on **Access Control Record Settings** to enter the access record settings interface.

10.3.1 Camera Mode

This function facilitates to set the conditions like whether it is required to save the photos and the attendance records after once the device captures the photo of the personnel.

- Tap on the required **Camera Mode** that you would like to configure:





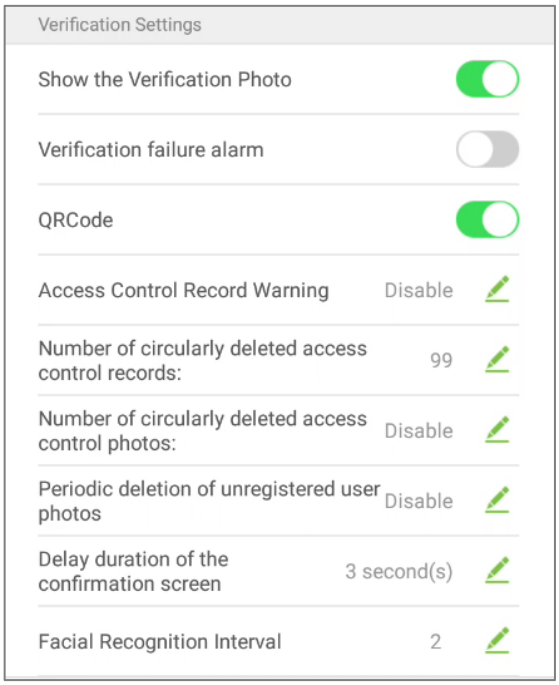
- On the **Camera Mode** interface, the users can set whether to take photos and save photos during user access verification. The settings are applicable to all users.

Function Descriptions

Function	Description
No photo	If this mode is selected, the device does take photos during authentication.
Capture photo and save:	If this mode is selected, the device takes users' photos and save photos during authentication.
Save after successful verification:	If this mode is selected, then when the user passes the verification, the photo is taken, and then photo is saved.
Save after failed verification:	If this mode is selected, the device takes a photo when the user fails verification and save it.

10.3.2 Verification Settings

Verification Settings facilitates configuring the settings for access verification parameters.



Function Descriptions

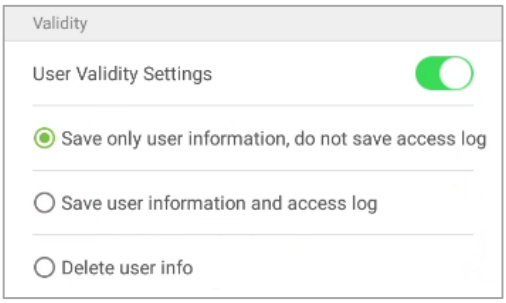
Menu Options	Function Description
Show the Verification Photo	If it is enabled, the user photo will be displayed; if not, the user photo will not be displayed.
Verification Failure Alarm	The alarm will ring when the verification fails. Verification failure alarm times can be set as 3-100s and verification failure interval can be set as 8-60s.
Access Control Record Warning	When the remaining access control record space reaches a set value, the device will automatically display a remaining record memory warning. When the value is set as 0, the function is disabled.
Number of Circularly Delete Access Control Records	When the access record memory has reached full capacity, the device will automatically delete a set value of old access records. When the value is set as 0, the function is disabled.
Number of Circularly Delete Access Control Photos	When the space storing the access control photos have reached full capacity, the device will automatically delete a set value of old access control photos. When the value is set as 0, the function is disabled.
Periodic Deletion of Unregistered User Photos	When the space storing block listed photos have reached full capacity, the device will automatically delete a set value of old block listed photos. When the value is set as 0, the function is disabled.
Delay Duration of the Confirmation Screen	This is the length of time that a user's information will display on the 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.

10.3.3 Validity Period of User Information

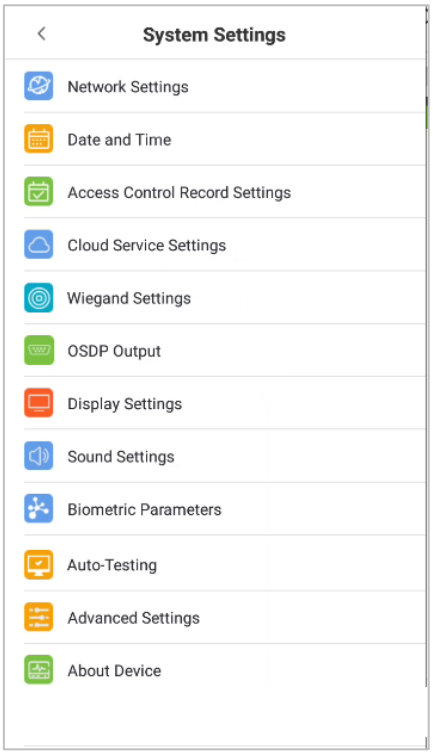
This is used to determine if user validity periods are enabled or disabled when registering users.

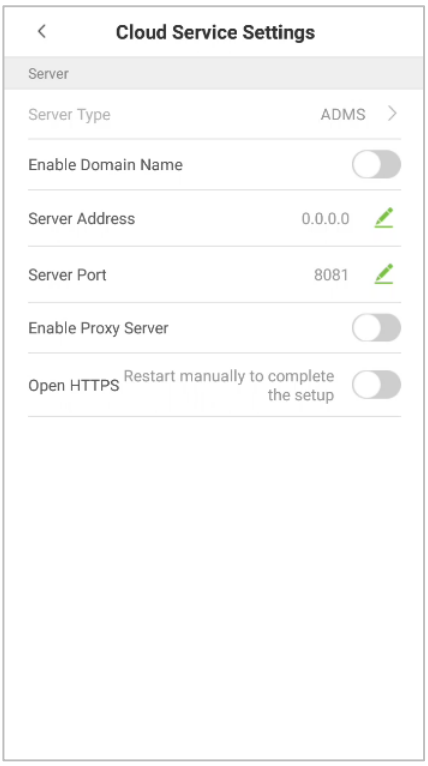
- Tap **User Validity Settings** to enable.
- When User Validity Settings is enabled, the following interface will display. Select the setting you would like to configure.



10.4 Cloud Service Settings

On **System Settings** interface, tap **[Cloud Service Settings]** to enter the **Cloud Service Settings** interface.



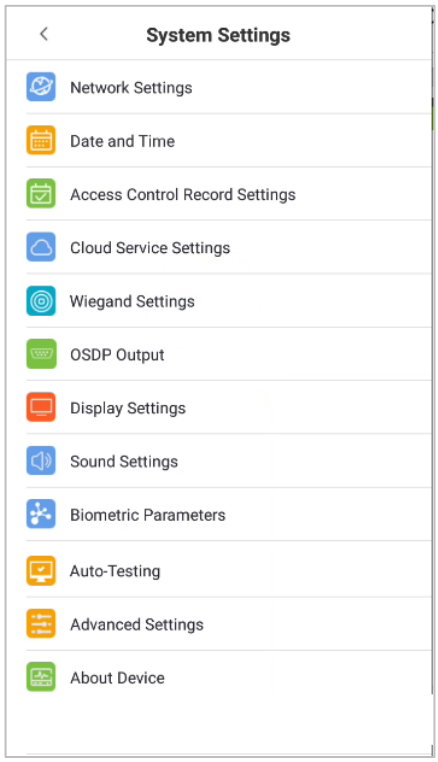


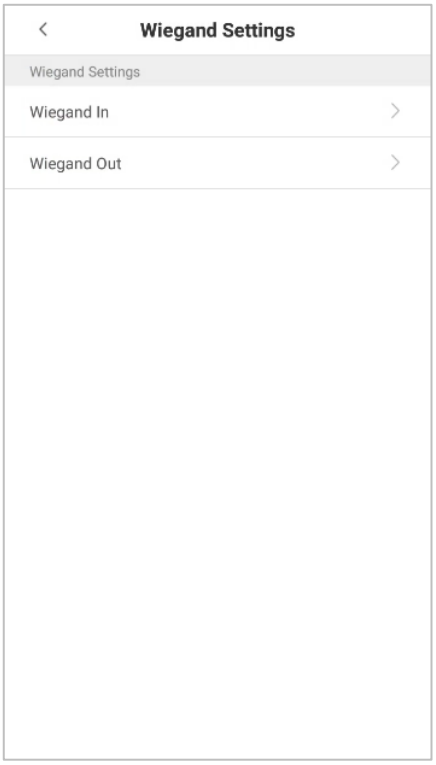
Function Descriptions

Item		Descriptions
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

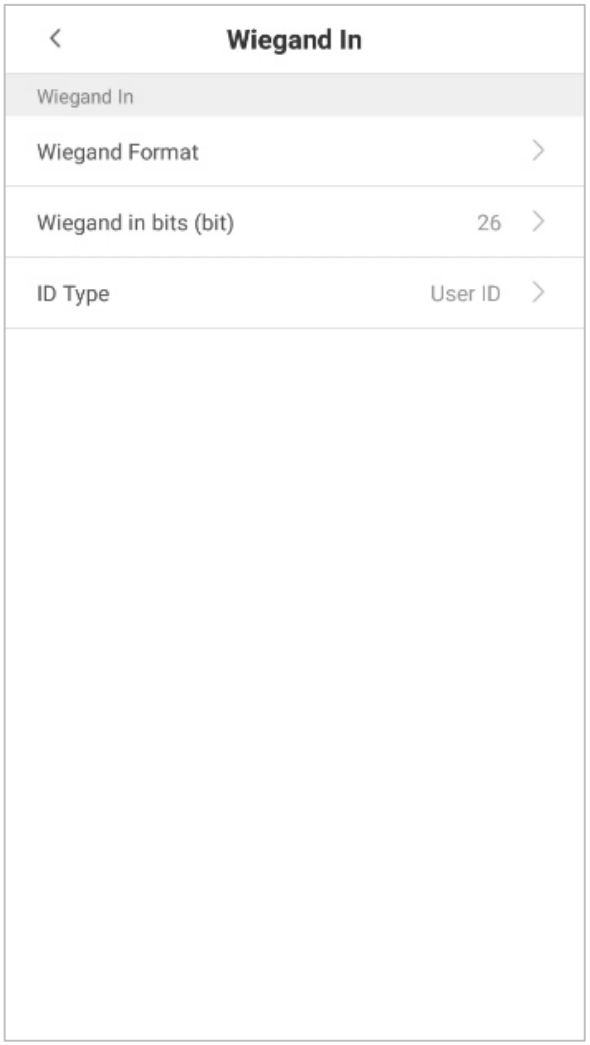
On **System Settings** interface, tap **Wiegand Settings** to access the interface as shown below.





10.5.1 Wiegand In

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



Function Descriptions

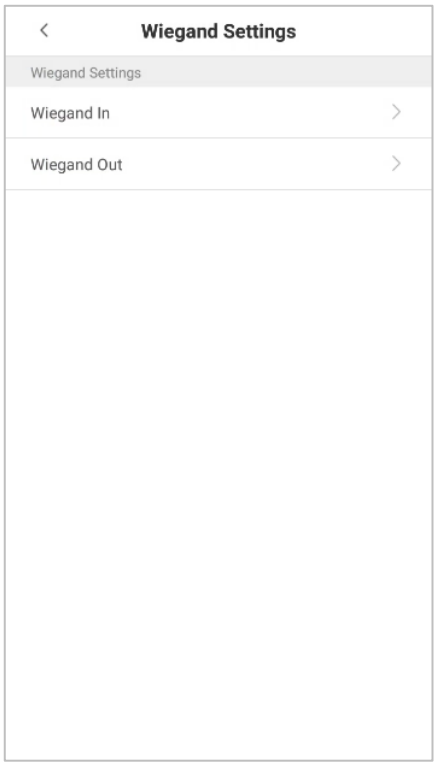
Menu Options	Function Description
Wiegand Format	The Wiegand value could be 26bits, 34bits, 36bits, 37bits, or 50bits.
Wiegand in bits	It displays the number of bits of Wiegand data. After choosing **Wiegand input bits**, the device will use the set number of bits to find the suitable Wiegand format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

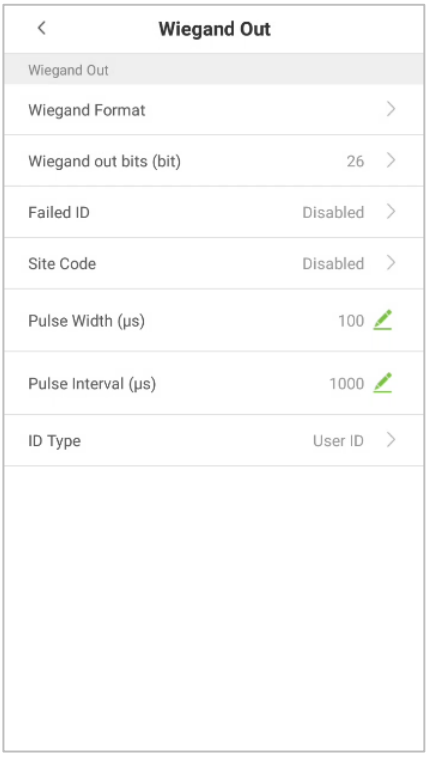
Various common Wiegand format definitions:

Wiegand Format	Description
Wiegand26	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.



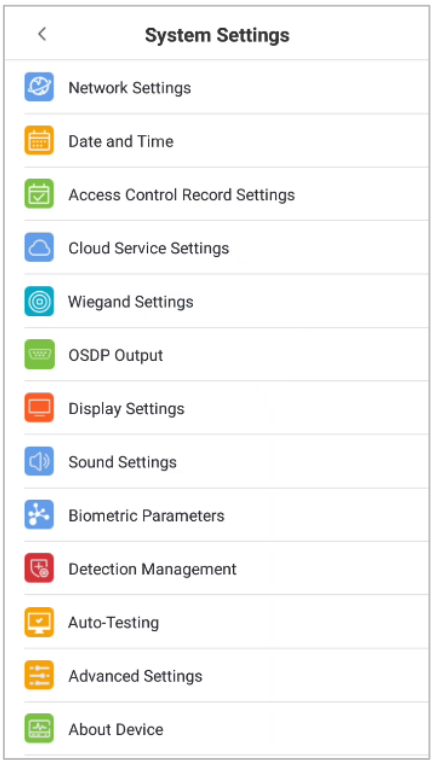


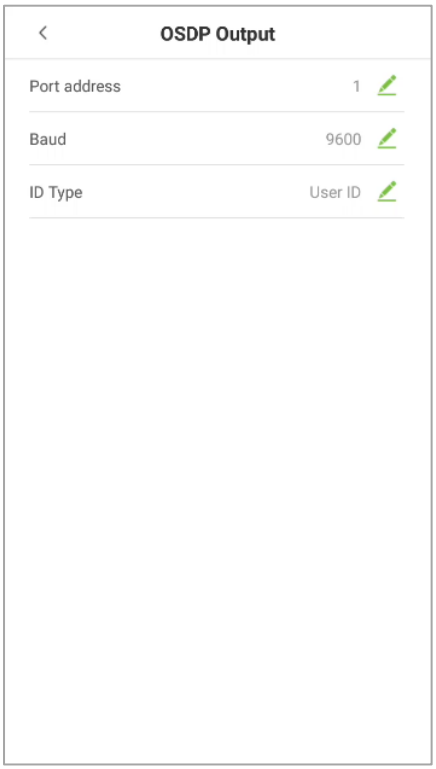
Function Description

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

10.6 OSDP Output

- On the **System Settings** interface, tap **OSDP Output** to enter the OSDP output settings interface.

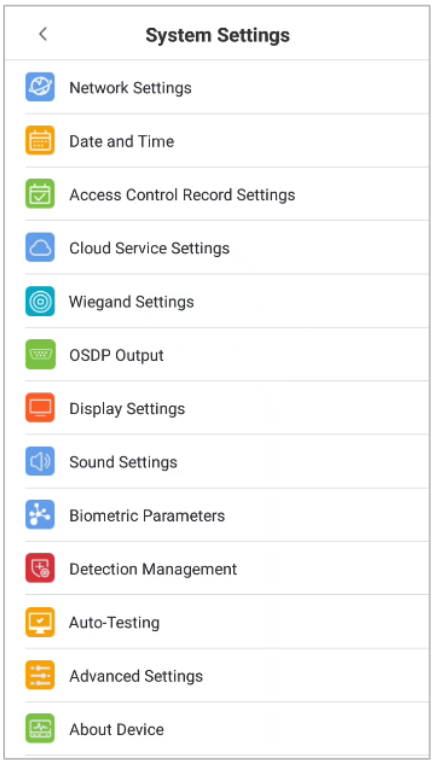


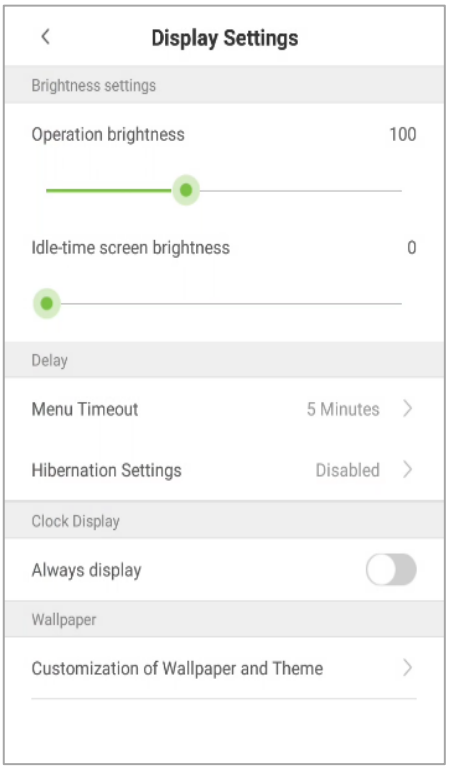


- The device can connect the external devices such as a printer via RS232, OSDP output is used for setting the Serial port address, Baud rate and ID type.

10.7 Display Settings

- On the **System Settings** interface, tap **Display Settings** to enter the Display Settings interface.





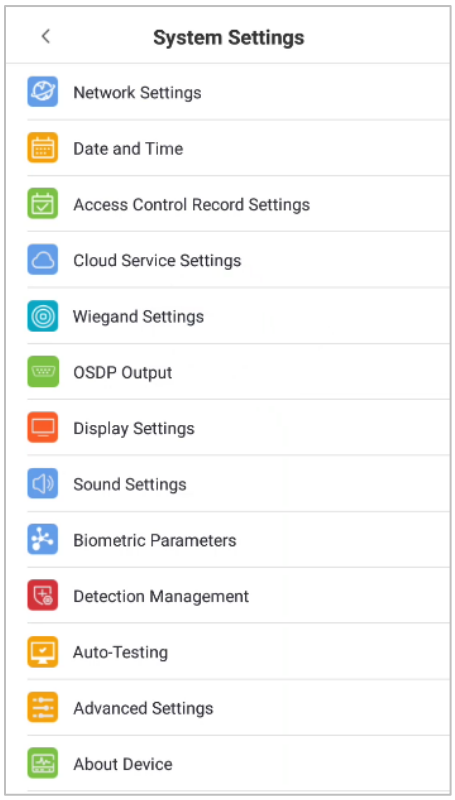
Function Descriptions

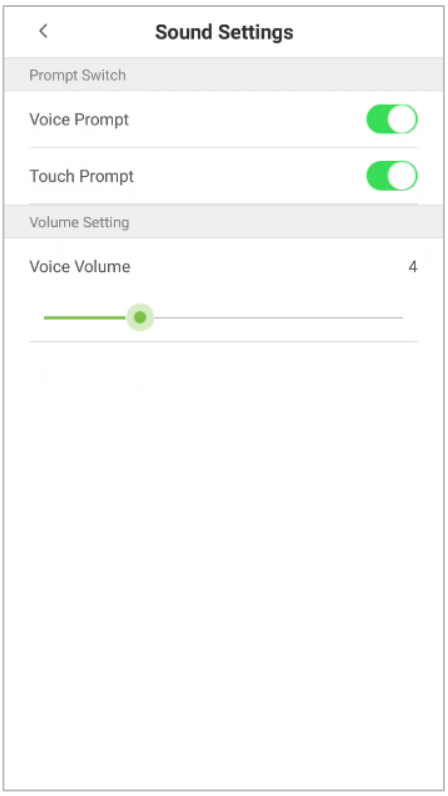
Menu Options		Function Description
Brightness Setting	Operation Brightness	Set the device working brightness, such as when setting parameter or face recognition.
	Idle-Time Screen Brightness	Screen brightness when the device is on the standby mode.
Delay	Menu Time Out	Menu time out occurs when no operations 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: 30 seconds, 1 minute, 2 minutes, 5 minutes, 10 minutes, or disabled. When this feature is disabled, the menu (including sub-menus) will not automatically close. Users must tap "Exit" to exit the menu.

	Hibernation Settings	After verification, the time from pop-up verification result to jump to standby interface. Optional parameter value ranges from 5 to 30 seconds.
Clock Display	Always Display	The clock is always displayed as on or off.
Wallpaper	Customization Of Wallpaper and Theme	Choose your favourite wallpaper from the theme wallpaper interface.

10.8 Sound Settings

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



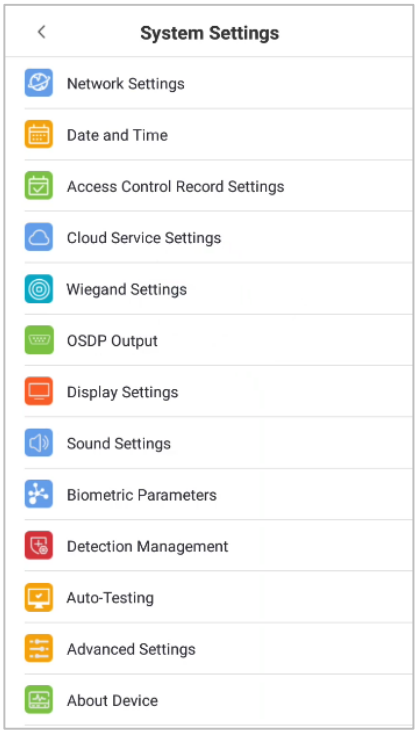


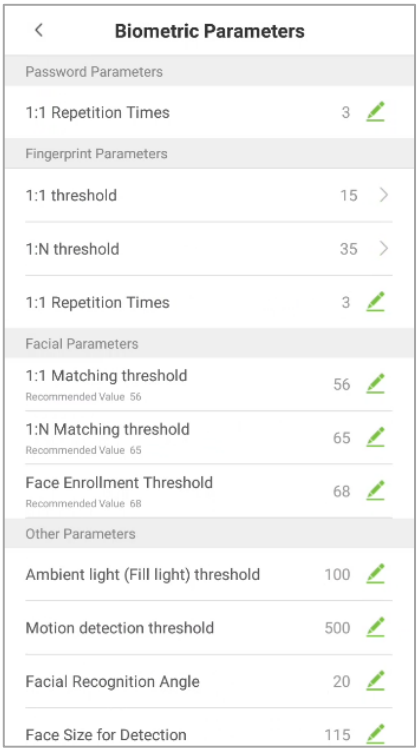
Function Descriptions

Menu Options	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

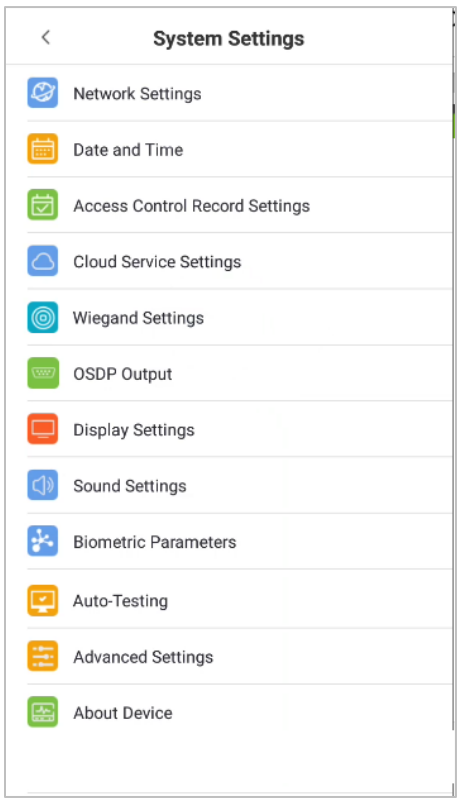
Menu		Function Description
Password Parameters	1:1 Repetition Times	The upper limit of the number of failed verifications under 1:1 verification. When the number of failed verifications reaches the set value, the system will return to the standby interface.

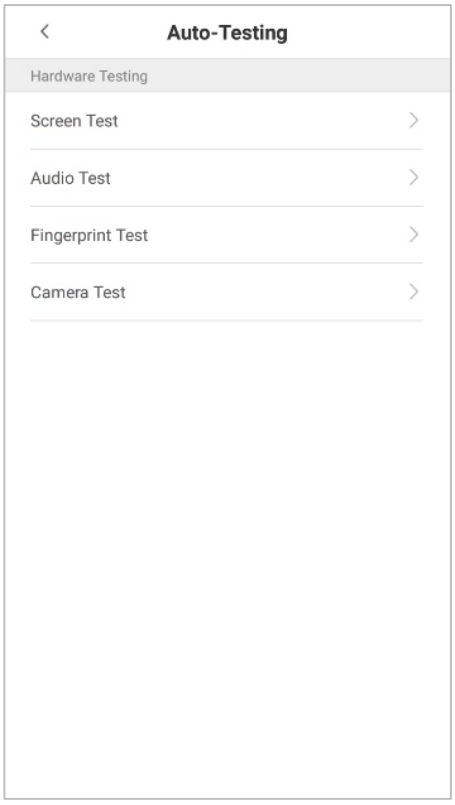
Fingerprint Parameters	1:1 Threshold Value	When conducting 1:1 fingerprint verification, fingerprint data is collected and instantly compared with fingerprint data using a 1:1 algorithm. This is converted into a value that is then compared to a set value. If the value of the scanned fingerprint exceeds that of the set value, the verification passes. If it does not, the verification fails. The higher the threshold, the more accurate the matching; the lower the threshold, the higher the matching success rate.
	1: N Threshold Value	When conducting 1: N verification, fingerprint data is collected and instantly compared with all fingerprint templates on the system using a 1: N algorithm. This is converted into a value that is compared to a set value. If the value of the scanned fingerprint exceeds that of the set value, the verification has passes. If it does not, the verification fails. The higher the threshold, the more accurate the matching; the lower the threshold, the higher the matching success rate.
	1:1 Repeat 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.
Facial Parameters	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.
	Enrollment Threshold Value	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 76.
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 80.
	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 100.
	Facial 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
	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.

10.10 Auto-testing

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



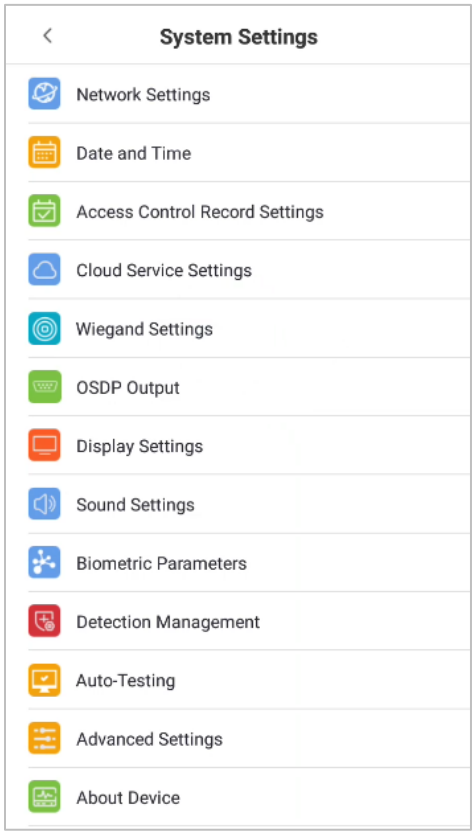


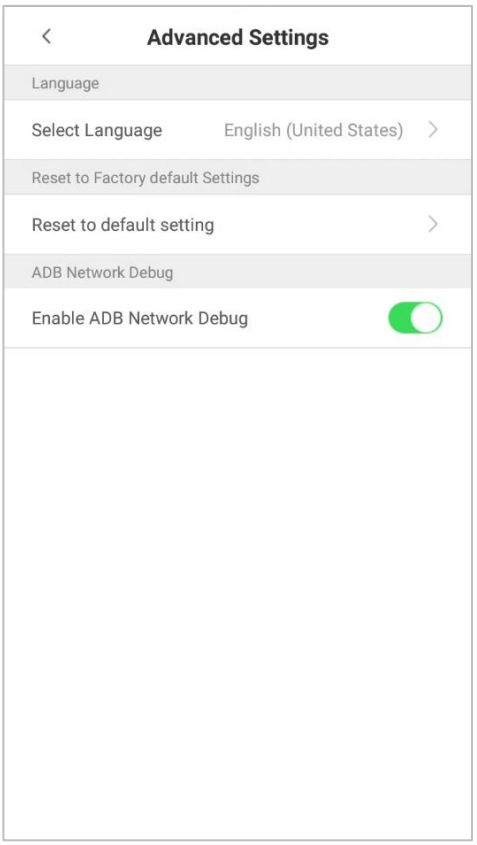
Function Descriptions

Menu Options	Function Description
Screen Testing	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.
Voice Testing	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.
Fingerprint Testing	It is used for testing if the fingerprint scanner is functioning properly. Check whether fingerprint image is clear and usable.
Camera Testing	It is used for testing if the camera is functioning properly. Check captured image to see if the image quality is clear and usable.

10.11 Advanced Settings

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



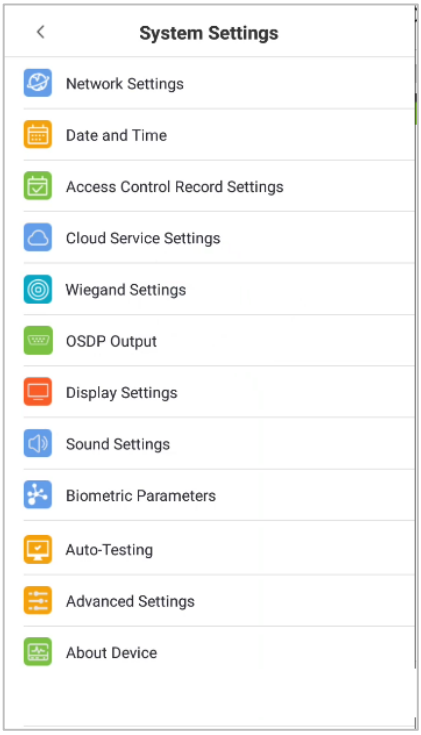


Function Descriptions

Menu Options	Function Description
Select Language	The user can select English or Simplified Chinese.
Restore Factory	It is used for restoring the settings of the device, including communication settings, system settings, to the factory settings.
ADB Network Debug	The ADB tool is Android debug bridge tool. It is a command line window, which is used to interact with the simulator or real device through the computer.

10.12 About the Device

- On the **System Settings** interface, tap **About the Device** to open the About the Device interface.



Function Description

Menu Options	Function Description
Capacity Information	It displays the current device's capacity of user, fingerprint (optional) and facial template, administrators, access control records, access control photos, unregistered user photos, and user photos.
Device Information	It displays the device's name, serial number, MAC address, algorithm version, platform information, and manufacturer.
Version	It displays all the versions of all the system's apps, such as the system settings, data management, and other installed apps.

11 USB Upgrade

The device's firmware program can be upgraded with the upgrade file in a USB drive. Before conducting this operation, please ensure that the USB drive contains the latest upgrade file and is properly inserted into the device.

Note: If you need an upgrade file, please contact out technical staff. Firmware upgrade is not recommended under normal circumstances.

Statement on the Right to Privacy

Dear Customers,

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

We Declare That:

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

Our other law-enforcement fingerprint devices or development tools can capture the original images of citizen's fingerprints. As to whether or not this constitutes an infringement of your rights, please contact your government or the final supplier of the device. As the manufacturer of the device, we will assume no legal liability.

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

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