

# USER MANUAL

Applicable Models: ProBio(QR)

---

Version: 1.0

Date: May 2021

English

Copyright © 2021 ZKTECO CO., LTD. All rights reserved.

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

## Trademark

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

## Disclaimer

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

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

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

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

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

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

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

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

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

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

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

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

## ZKTeco Headquarters

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

**Phone** +86 769 - 82109991

**Fax** +86 755 - 89602394

For business related queries, please write to us at: [sales@zkteco.com](mailto:sales@zkteco.com).

To know more about our global branches, visit [www.zkteco.com](http://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 **ProBio(QR)**.

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

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






## Document Conventions

Conventions used in this manual are listed below:

### GUI Conventions

For Software	
Convention	Description
<b>Bold font</b>	Used to identify software interface names e.g., <b>OK</b> , <b>Confirm</b> , <b>Cancel</b> .
>	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

<b>SAFETY MEASURES .....</b>	<b>7</b>
<b>1 INSTRUCTION FOR USE .....</b>	<b>10</b>
1.1 STANDING POSITION, FACIAL EXPRESSION AND STANDING POSTURE .....	10
1.2 FACE REGISTRATION .....	11
1.3 STANDBY INTERFACE .....	11
1.4 VERIFICATION MODE .....	12
1.4.1 FACIAL VERIFICATION .....	12
1.4.2 PASSWORD VERIFICATION .....	13
1.4.3 CARD VERIFICATION .....	15
1.4.4 QR CODE VERIFICATION .....	16
1.4.5 COMBINED VERIFICATION .....	17
<b>2 MAIN MENU .....</b>	<b>19</b>
<b>3 USER MANAGEMENT .....</b>	<b>20</b>
3.1 USER REGISTRATION .....	20
3.2 SEARCH USER .....	23
3.3 EDIT USER .....	23
3.4 DELETING USER .....	24
<b>4 USER ROLE .....</b>	<b>25</b>
<b>5 COMMUNICATION SETTINGS .....</b>	<b>27</b>
5.1 NETWORK SETTINGS .....	27
5.2 SERIAL COMM .....	28
5.3 PC CONNECTION .....	29
5.4 CLOUD SERVER SETTING .....	29
5.5 WIEGAND SETUP .....	30
5.5.1 WIEGAND INPUT .....	30
5.5.2 WIEGAND OUTPUT .....	32
5.5.3 CARD FORMAT DETECT AUTOMATICALLY .....	33
<b>6 SYSTEM SETTINGS .....</b>	<b>35</b>
6.1 DATE AND TIME .....	35
6.2 ACCESS LOGS SETTING .....	36
6.3 FACE PARAMETERS .....	37
6.4 FACTORY RESET .....	38
6.5 USB UPGRADE .....	38
<b>7 PERSONALIZE SETTINGS .....</b>	<b>40</b>
7.1 INTERFACE SETTINGS .....	40
7.2 VOICE SETTINGS .....	41
7.3 BELL SCHEDULES .....	41
<b>8 DATA MANAGEMENT .....</b>	<b>44</b>
8.1 DELETE DATA .....	44

8.2	BACKUP DATA .....	45
8.3	RESTORE DATA.....	46
<b>9</b>	<b>ACCESS CONTROL .....</b>	<b>47</b>
9.1	ACCESS CONTROL OPTIONS.....	47
9.2	TIME RULE SETTING .....	49
9.3	HOLIDAYS .....	50
9.4	COMBINED VERIFICATION .....	51
9.5	ANTI-PASSBACK SETUP .....	52
9.6	DURESS OPTIONS SETTINGS.....	53
<b>10</b>	<b>USB MANAGER.....</b>	<b>54</b>
10.1	USB DOWNLOAD.....	54
10.2	USB UPLOAD.....	55
<b>11</b>	<b>ATTENDANCE SEARCH .....</b>	<b>56</b>
<b>12</b>	<b>AUTOTEST .....</b>	<b>57</b>
<b>13</b>	<b>SYSTEM INFORMATION .....</b>	<b>58</b>
<b>14</b>	<b>QR CODE AS THE MOBILE CREDENTIAL.....</b>	<b>59</b>
14.1	CONNECT TO ZKBIOSECURITY SOFTWARE .....	59
14.1.1	SET THE COMMUNICATION ADDRESS .....	59
14.1.2	ADD DEVICE ON THE SOFTWARE.....	60
14.1.3	ADD PERSONNEL ON THE SOFTWARE .....	60
14.2	MOBILE CREDENTIAL.....	61
14.2.1	MOBILE APP CONFIGURATION .....	61
14.2.2	LOGIN THE MOBILE APP .....	62
14.2.3	SCAN THE QR CODE .....	64
<b>APPENDIX 1 .....</b>	<b>65</b>	
	REQUIREMENTS OF LIVE COLLECTION AND REGISTRATION OF VISIBLE LIGHT FACE IMAGES .....	65
	REQUIREMENTS FOR VISIBLE LIGHT DIGITAL FACE IMAGE DATA.....	66
<b>APPENDIX 2 .....</b>	<b>67</b>	
	PRIVACY POLICY .....	67
	ECO-FRIENDLY OPERATION.....	69

## **Safety Measures**

The below instructions intend to ensure that the user can use the product correctly to avoid danger or property loss. The following precautions are to keep users safe and prevent any damage. Please read carefully before installation.

 Noncompliance with instructions could lead to product damage or physical injury (may even cause death).

1. **Read, follow, and retain instructions** - All safety and operational instructions must be properly read and followed before bringing the device into service.
2. **Do not ignore warnings** - Adhere to all warnings on the unit and in the operating instructions.
3. **Accessories** - Use only manufacturer-recommended or product-sold accessories. Please do not use any other components other than manufacturer suggested materials.
4. **Precautions for the installation** – Do not place this device on an unstable stand or frame. It may fall and cause serious injury to persons and damage to the device.
5. **Service** - Do not try to service this unit yourself. Opening or removing covers may expose you to hazardous voltages or other hazards.
6. **Damage requiring service** - Disconnect the system from the Mains AC or DC power source and refer service personnel under the following conditions:
  - When cord or connection control is affected.
  - When the liquid spilled, or an item dropped into the system.
  - If exposed to water or due to inclement weather (rain, snow, and more).
  - If the system is not operating normally, under operating instructions.

Just change controls defined in operating instructions. Improper adjustment of the controls may result in damage and involve a qualified technician to return the device to normal operation.

And do not connect multiple devices to one power adapter as adapter overload can cause over-heat or fire hazard.

7. **Replacement parts** - When replacement parts are needed, service technicians must only use replacement parts provided by the supplier. Unauthorized substitutes can result in a burn, shock, or other hazards.
8. **Safety check** - On completion of service or repair work on the unit, ask the service technician to perform safety checks to ensure proper operation of the device.
9. **Power sources** - Operate the system only from the label's power source form. If the sort of power supply to use is unclear, call your dealer.
10. **Lightning** - Can install external lightning conductors to protect against electrical storms. It stops power-ups from destroying the system.

Recommended installing the devices in areas with limited access.



## Electrical Safety

- Before connecting an external cable to the device, complete grounding properly, and set up surge protection; otherwise, static electricity will damage the mainboard.
- Make sure that the power has been disconnected before you wire, install, or dismantle the device.
- Ensure that the signal connected to the device is a weak-current (switch) signal; otherwise, components of the device will get damaged.
- Ensure that the standard voltage applicable in your country or region is applied. If you are not sure about the endorsed standard voltage, please consult your local electric power company. Power mismatch may cause a short circuit or device damage.
- In the case of power supply damage, return the device to the professional technical personnel or your dealer for handling.
- To avoid interference, keep the device far from high electromagnetic radiation devices, such as generators (including electric generators), radios, televisions, (especially CRT) monitors, or speakers.

## Operation Safety

- If smoke, odour, or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service centre.
- Transportation and other unpredictable causes may damage the device hardware. Check whether the device has any intense damage before installation.
- If the device has major defects that you cannot solve, contact your dealer as soon as possible.
- Dust, moisture, and abrupt temperature changes can affect the device's service life. You are advised not to keep the device under such conditions.
- Do not keep the device in a place that vibrates. Handle the device with care. Do not place heavy objects on top of the device.
- Do not apply rosin, alcohol, benzene, pesticides, and other volatile substances that may damage the device enclosure. Clean the device accessories with a piece of soft cloth or a small amount of cleaning agent.
- If you have any technical questions regarding usage, contact certified or experienced technical personnel.

**NOTE:**

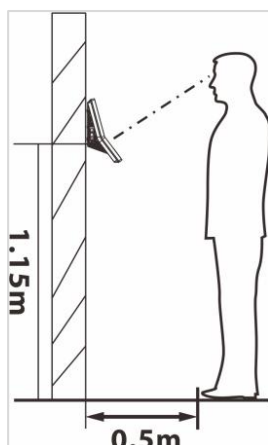
- Make sure whether the positive polarity and negative polarity of the DC 12V power supply is connected correctly. A reverse connection may damage the device. It is not advisable to connect the AC 24V power supply to the DC 12V input port.
- Make sure to connect the wires following the positive polarity and negative polarity shown on the device's nameplate.
- The warranty service does not cover accidental damage, damage caused by mis-operation, and damage due to independent installation or repair of the product by the user.

# 1 Instruction for Use

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

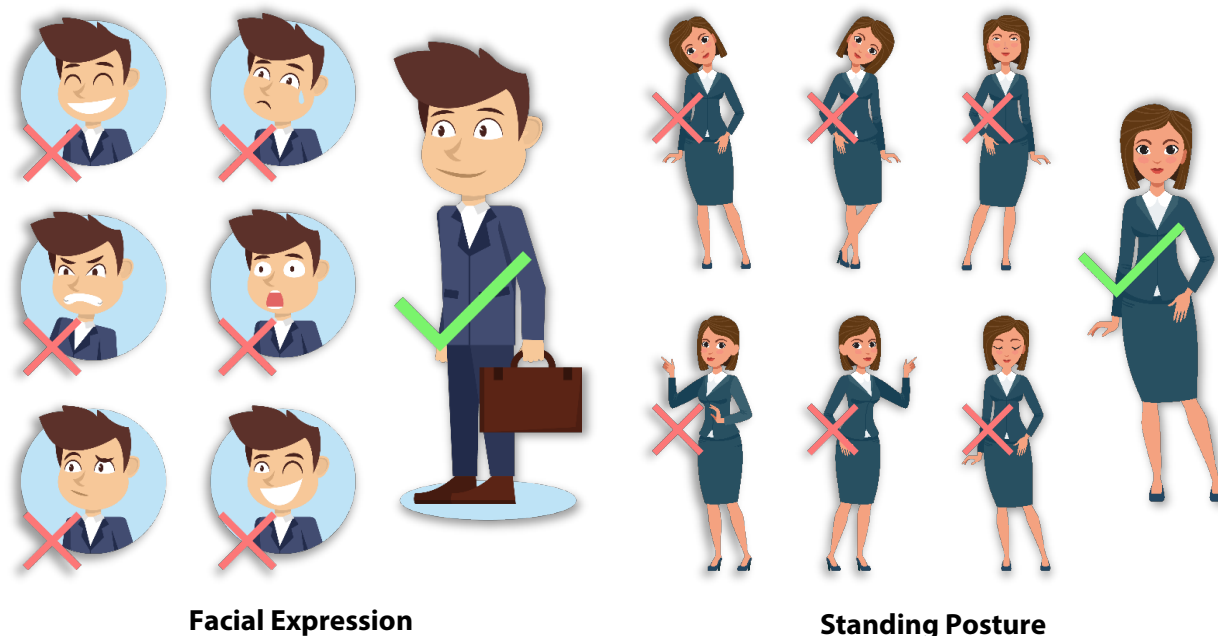
## 1.1 Standing Position, Facial Expression and Standing Posture

- **The recommended distance**



For user heights between 1.5m to 1.8m, it is recommended to install the device at 1.15m above ground (may be modified according to user average height).

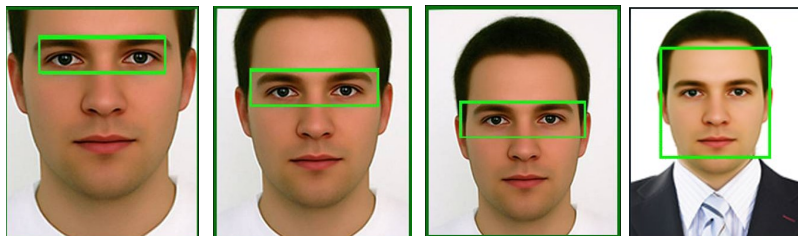
- **Recommended Facial Expression and Standing Posture**



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

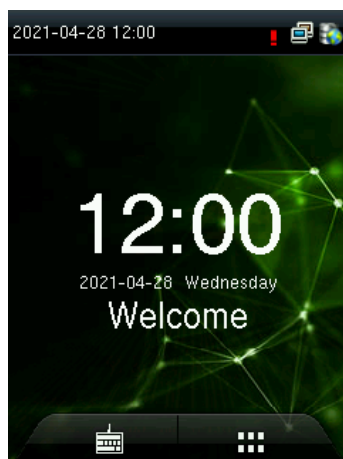
## 1.2 Face Registration



- During registration, it is required to adjust your upper body to fit your eyes into the green frame on the screen.
- During verification, it is required to show your face in the centre of the screen and fit your face into the green frame in the screen.



## 1.3 Standby Interface

After connecting the AC adapter, the following standby interface is displayed:



- Tap  to enter the User ID input interface.
- When there is no Super Administrator set in the device, tap  to go to the menu.
- After adding a Super Administrator on the device, it requires the Super Administrator's verification before opening the menu functions.

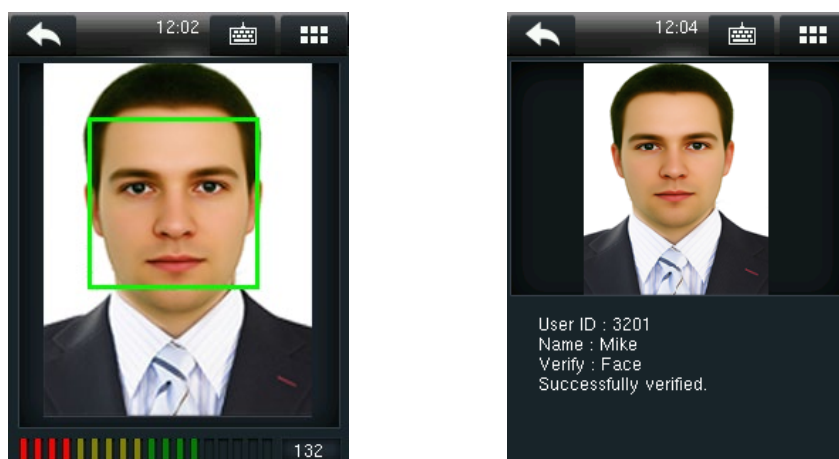
**NOTE:** For the security of the device, it is recommended to register a super administrator the first time you use the device.

## 1.4 Verification Mode

### 1.4.1 Facial Verification

- **1:N Facial Verification**

It compares the acquired facial images with all face data registered in the device. The following is the pop-up prompt box of comparison results.



- **1:1 Facial Verification**

Compare the face captured by the camera with the facial template related to the entered user ID.

Press  on the main interface and enter the 1:1 facial verification mode.

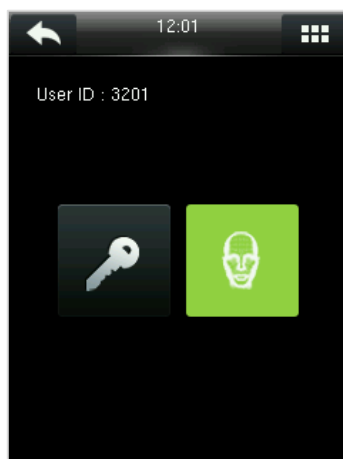
Enter the user ID and click [OK].



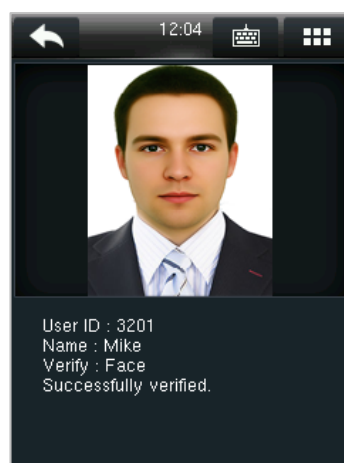
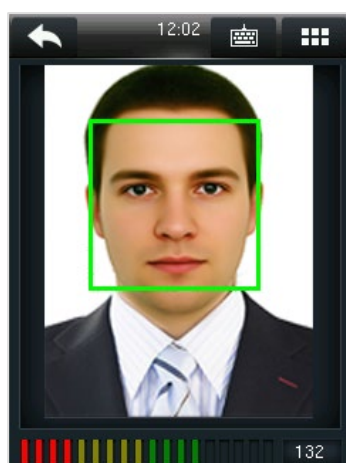
If an employee registers password in addition to the face, the following screen will appear. Select the



to enter face verification mode.




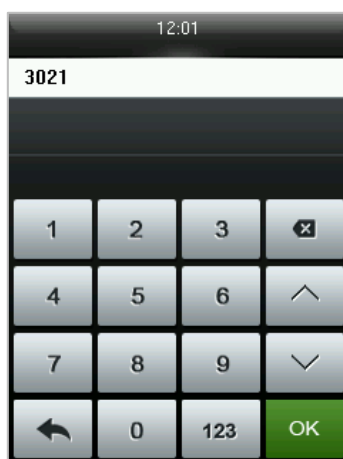
After successful verification, the prompt box displays "**Successfully Verified**", as shown below:




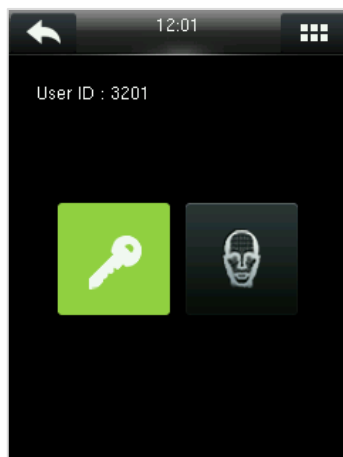
### 1.4.2 Password Verification

The device compares the entered password with the registered password of the given User ID.

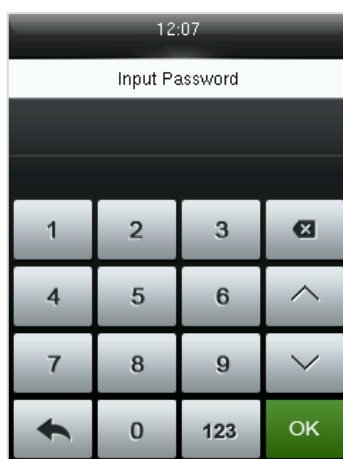
Press  on the main screen to enter the 1:1 password verification mode. Then, input the user ID and press [OK].



If an employee registers a face in addition to password, the following screen will appear. Select the  to enter password verification mode.

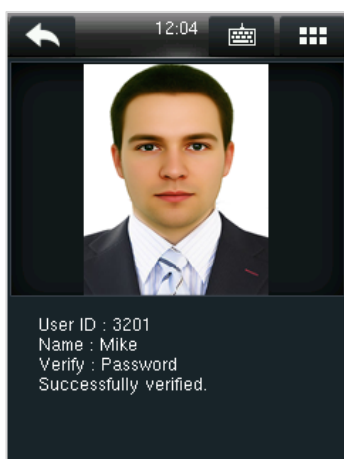


Input the password and press [OK].

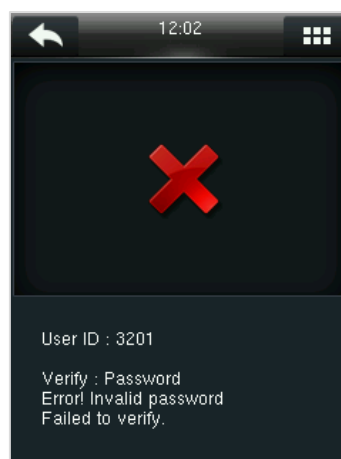


Following are the display screen after entering a correct password and a wrong password respectively.

**Verification is successful:**



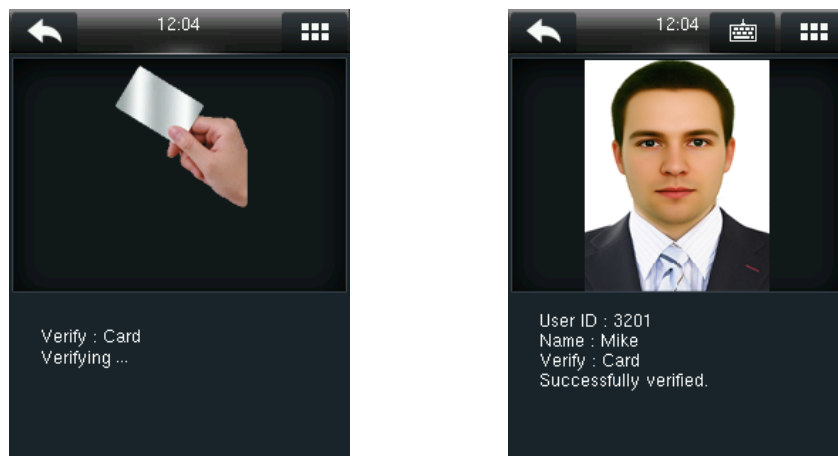
**Verification is failed:**



### 1.4.3 Card Verification


- **1:N Card Verification**

The device compares the card number in the card induction area with all the card number data registered in the device. The following is the comparison result prompt box.

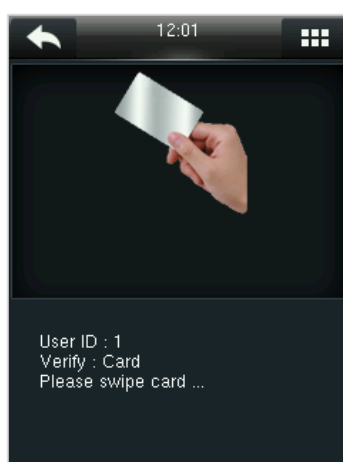


- **1:1 Card Verification**

The device compares the acquired card number with the card data related to the entered User ID.

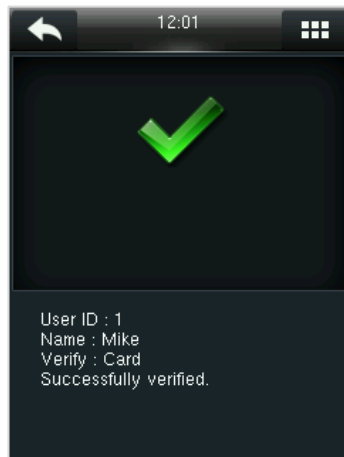
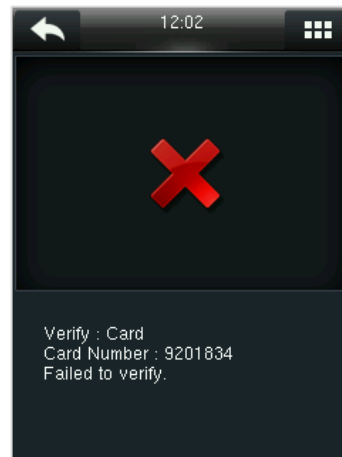
Press  on the main interface and enter the 1:1 card verification mode.

Enter the User ID and click [OK].



Following are the display screens after entering a correct card and a wrong card respectively.

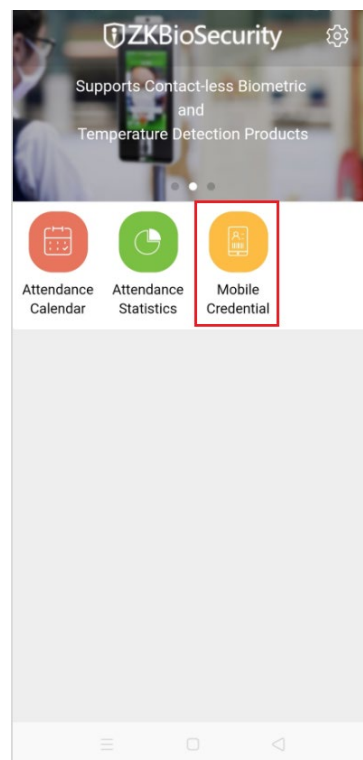
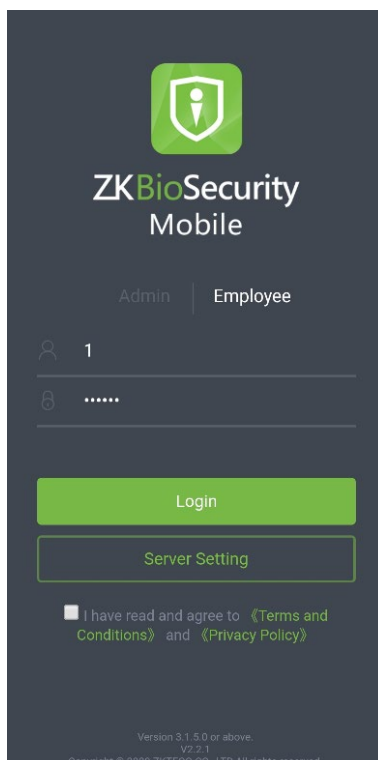


**Verification is successful:****Verification is failed:**

### 1.4.4 QR Code Verification

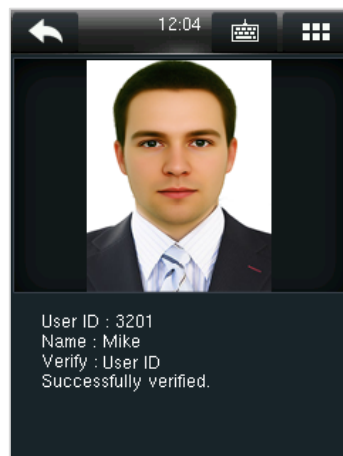
This function is suitable for devices that are equipped with QR code scanners. The camera can recognize the QR code image on the **ZKBioSecurity Mobile APP** captured by the lens or the QR code scanner. Find the **Attendance QR** code on the ZKBioSecurity Mobile App and align it with the QR code scanner at the bottom of the ProBio(QR). You can check in/out when verification is successful. To set up the attendance QR code, please refer to **Chapter 7.5** of the '**ZKBioSecurity Mobile APP User Manual**'.

- Login to the **ZKBioSecurity Mobile APP** and click **[Mobile Credential]** to find the attendance QR code, as shown below:



- Align the attendance QR code with the QR code scanner at the bottom of the device.

- After successful verification, the prompt box displays "**Successfully Verified**", as shown below:

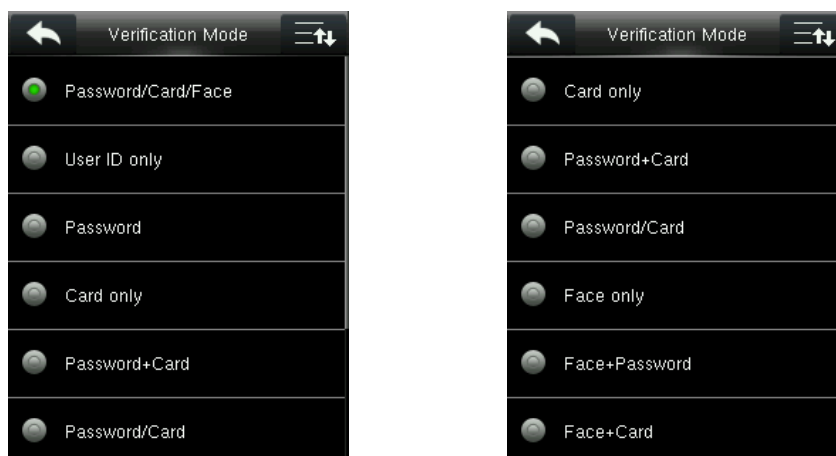


**NOTE:**

- The user must have a card number registered in advance on the device or on the ZKBioSecurity software. The QR code is a dynamic QR code that integrates the User ID and Card number information.
- The QR code and the scanner are kept parallel and at a certain distance (15 to 30cm is recommended, depending on the size of the phone screen and the density of the QR code) when scanning.

### 1.4.5 Combined Verification

To increase security, this device offers the option of using multiple forms of verification methods.



#### Procedure to set for Combined Verification Mode


- Combined verification requires personnel to register all the different verification methods. Otherwise, employees may not be able to successfully verify through the combined verification process.

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

**NOTE:**

- "/" means "**or**", and "+" means "**and**".
- You must register the required verification information before using the combination verification mode, otherwise the verification may fail. For example, if a user uses Face Registration but the verification mode is Face + Password, this user will never pass verification.

## 2 Main Menu

Press  on the initial interface to enter the main menu, as shown below:



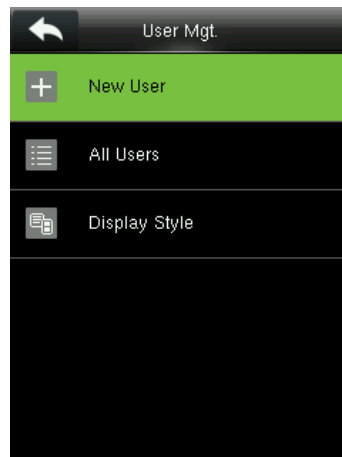
### Function Description

Menu	Descriptions
<b>User Mgt.</b>	To Add, Edit, View, and Delete information of a User.
<b>User Role</b>	To set the permission scope of the custom role and enroller for the users, that is, the rights to operate the system.
<b>COMM.</b>	To set the relevant parameters of Network, Serial Comm, PC Connection, Cloud Server and Wiegand.
<b>System</b>	To set parameters related to the system, including Date & Time, Access Logs Setting, Face parameters, resetting to factory settings and USB Upgrade.
<b>Personalize</b>	To customize settings of User Interface, Voice and Bell Schedules.
<b>Data Mgt.</b>	To delete data including access records, admin role, screen savers and so on, to backup and restore data. Delete access records, delete all data, delete admin role, delete screen savers and so on, to backup, restore data.
<b>Access Control</b>	To set the parameters of the lock and the relevant access control device including options like Time schedule, Holiday Settings, Combine verification, Anti-passback Setup, and Duress Option Settings.
<b>USB Manager</b>	To transfer data such as user data and access records from the USB disk to the supporting software or other devices.
<b>Attendance Search</b>	To query the specified Attendance record, check Attendance Photos and Blocklist attendance photos.
<b>Autotest</b>	To automatically test whether each module functions properly, including the LCD Screen, Audio, Microphone, Camera, and Real-Time Clock.
<b>System Info</b>	To view Data Capacity and Device and Firmware information of the current device.

## 3 User Management

### 3.1 User Registration

Click **User Mgt.** on the **Main Menu**.



#### 1. Register a User ID and Name

Tap **New User** and enter the **User ID** and **Name**.

A screenshot of the "New User" registration form. The form has a title bar with a back arrow and a refresh icon. It contains several input fields: "User ID" with the value "1", "Name" with the value "Mike Lee", "User Role" with the value "Normal User", "Face" with the value "0", "Card Number", and "Password".

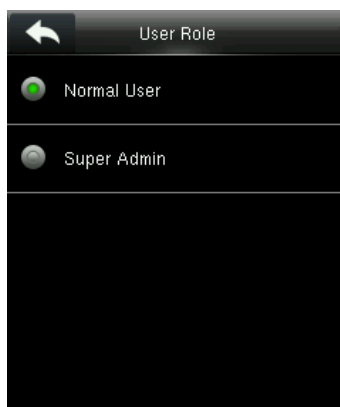
#### **NOTE:**

- A name can take up to 17 characters.
- The user ID may contain 1 to 9 digits by default.
- You can modify your ID during the initial registration but not after registration.
- If a message "**Duplicated!**" pops up, you must choose another ID as the entered User ID already exists.

## 2. Setting the User Role

There are two types of user accounts: the normal user and the Super Admin. If there is already a registered administrator, the normal users have no rights to manage the system and may only access authentication verifications. The administrator owns all management privileges. If a custom role is set, you can also select user defined role permissions for the user.

Click **User Role** to select Normal User or Super Admin.

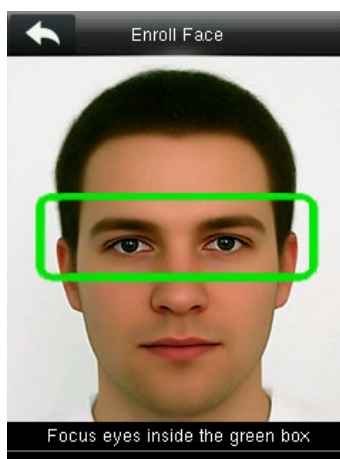


### **NOTE:**

If the selected user role is the Super Admin, the user must pass the identity authentication to access the main menu. The authentication is based on the authentication method(s) that the Super Administrator has registered. Please refer to [1.4 Verification Mode](#).

## 3. Register face

Click **Face** to enter the face registration page. Please face the camera and stay still during face registration. The registration interface is as follows:



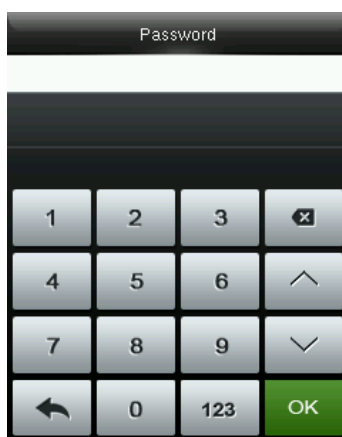
## 4. Register card number

Click **Card Number** to enter the card registration page. Please place the card in the card induction area. The registration interface is as follows:



## 5. Register Password

Tap **Password** to enter the password registration page. Enter a password and re-enter it. Select **OK**. If the two entered passwords are different, then the prompt "**Password not match!**" will appear.

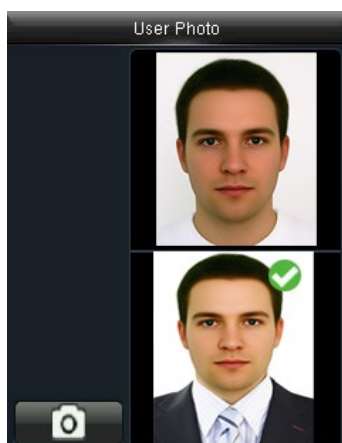


**NOTE:** The password may contain one to eight digits by default.

### • Register User Photo

When a user registered with a photo passes the authentication, the registered photo will be displayed.

Click **User Photo**, click the camera icon to take a photo. The system will return to the New User interface after taking a photo.



**NOTE:**

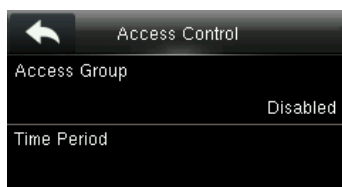
While registering a face, the system will automatically capture a picture as the user photo. If you do not want to register a user photo, the system will automatically set the picture captured as the default photo.

- **Access Control Role**

User access control sets the door unlocking rights of each person, including the group and the time period that the user belongs to.

Click **Access Control Role > Access Group**, assign the registered users to different groups for better management. New users belong to Group 1 by default and can be reassigned to other groups. The device supports up to 99 access control groups.

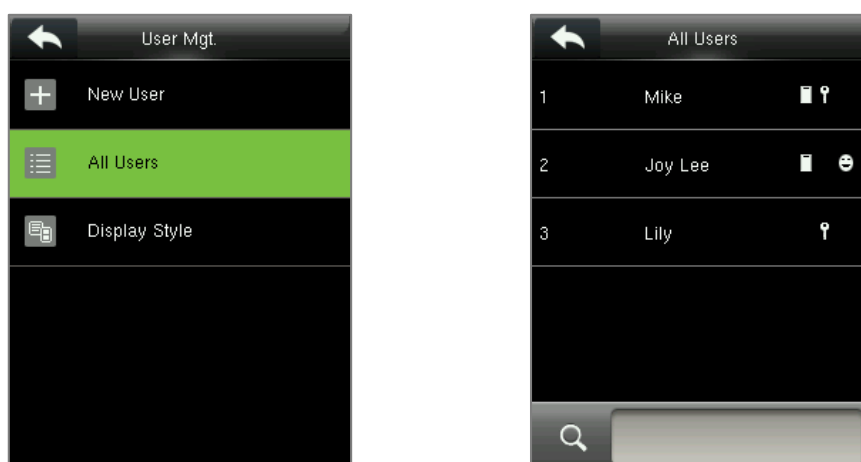
Click **Time Period**, select the time period to use.



## 3.2 Search User

On the **Main Menu**, click **User Mgt.**, and then select **All Users** to search a User.

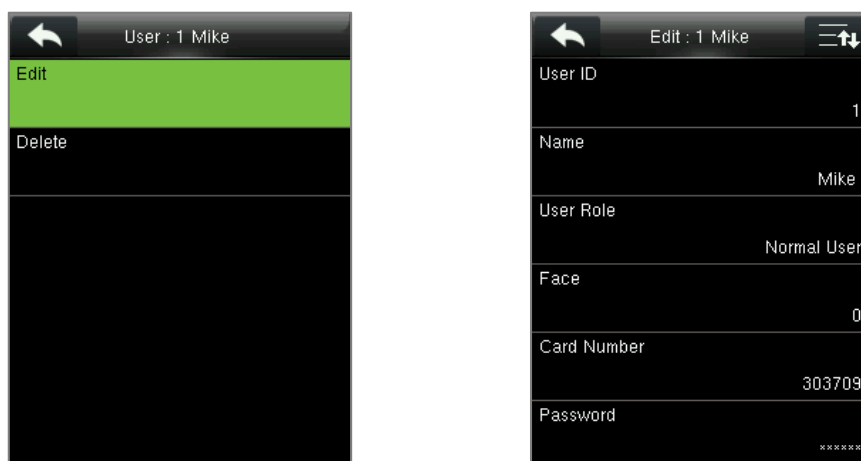
On the **All Users** interface, click on the search bar on the user's list to enter the required retrieval keyword (where the keyword may be the user ID, surname, or full name) and the system will search for the related user information.



## 3.3 Edit User

On the **All Users** interface, click on the required user from the list and select **Edit** to edit the user information.

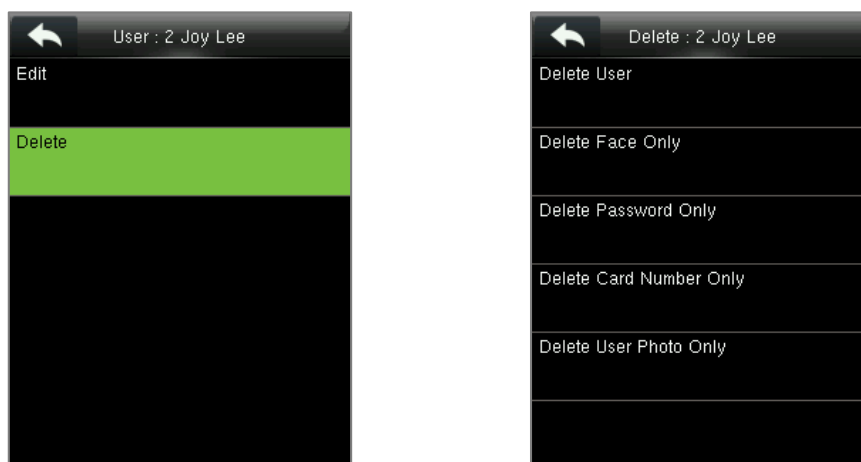




**NOTE:** The process of editing the user information is the same as adding a new user, except that the User ID cannot be modified when editing a user. The process in detail refers to "[3.1 User Registration](#)".

### 3.4 Deleting User

On the **All Users** interface, click on the required user from the list and select **Delete** to delete the user or specific user information from the device. On the **Delete** interface, click on the required operation and then select **OK** to confirm the deletion.



#### Delete Operations

**Delete User:** Deletes all the user information (deletes the selected User as a whole) from the Device.

**Delete Face Only:** Deletes the Face information of the selected user.

**Delete Password Only:** Deletes the password information of the selected user.

**Delete Card Number Only:** Deletes the card number information of the selected user.

**Delete User Photo Only:** Deletes the user photo information of the selected user.

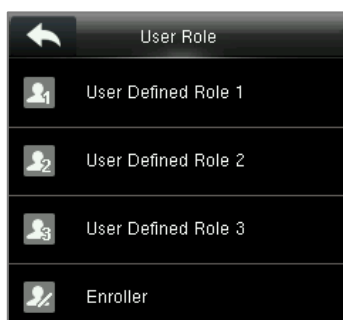
**NOTE:** If you select **Delete User**, all information of the user will be deleted.

## 4 User Role

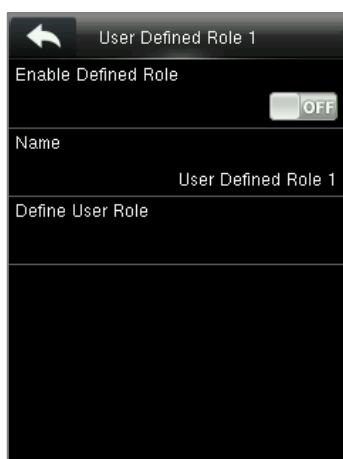
If you need to assign some specific permissions to certain users, you may edit the “**User Defined Role**” under the **User Role** menu.

You may set the permission scope of the custom role (up to 3 roles) and enroller, that is, the permission scope of the operation menu.

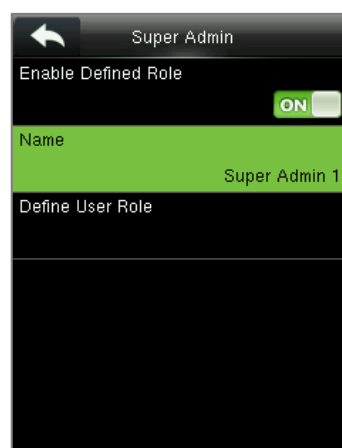
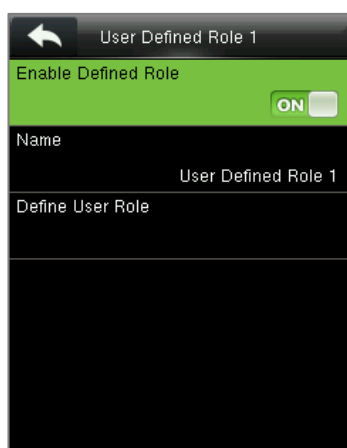
Click **User Role** on the main menu interface.



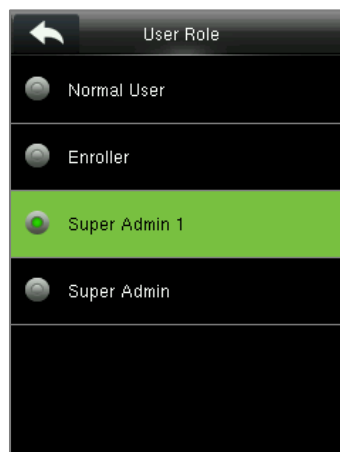
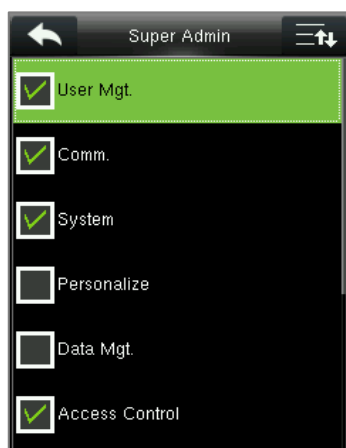
- On the **User Defined Role** interface, toggle **Enable Defined Role** to enable or disable the user-defined role.



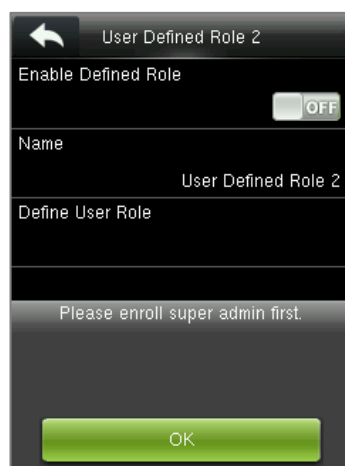
- Click on **Name** and enter the custom name of the role.



- Then, click on **Define User Role** and select the required privileges to assign to the new role, and then click on the **Return** button.
- During privilege assignment, the **Main Menu** function names will be displayed on the left and its sub-menus will be listed on its right.
- First, click on the required **Main Menu** functions, and then select its required sub-menus from the list which the user can access.

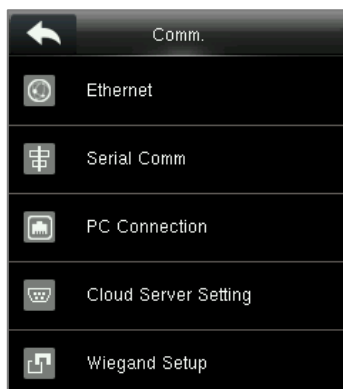


**Note:** If the User Role is enabled for the device, click on **User Mgt. > New User > User Role** to assign the created roles to the required users. But if there is no super administrator registered in the device, then the device will prompt "**Please enrol super admin first!**" when enabling the User Role function.



## 5 Communication Settings

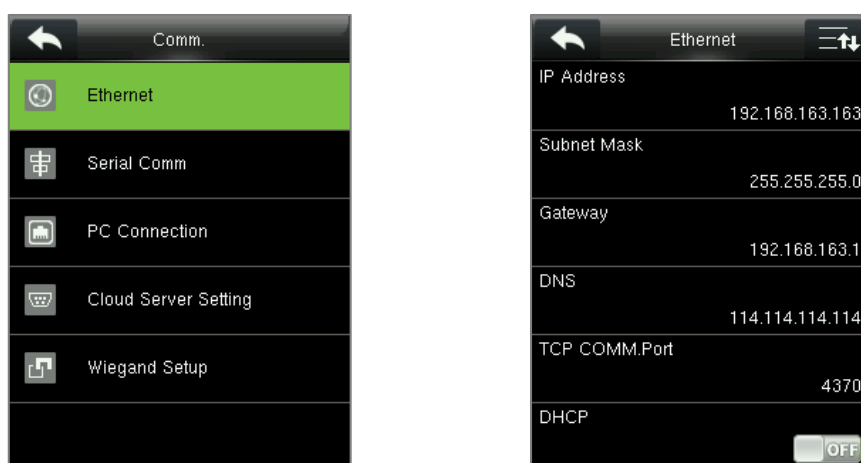
Click **COMM.** on the **Main Menu** to set the Ethernet, Serial Comm, PC connection, Cloud Server setting and Wiegand.



### 5.1 Network Settings

When the device needs to communicate with a PC over the Ethernet, you need to configure network settings and ensure that the device and the PC connect to the same network segment.

Tap **Ethernet** on the **Comm.** Settings interface to configure the settings.



#### Function Description

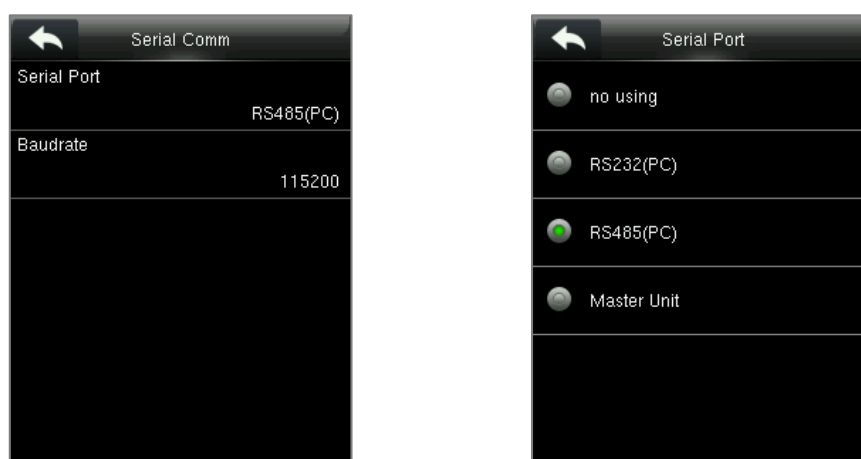
Function Name	Descriptions
<b>IP Address</b>	The default IP address is 192.168.1.201. It can be modified according to the network availability.
<b>Subnet Mask</b>	The default Subnet Mask is 255.255.255.0. It can be modified according to the network availability.
<b>Gateway</b>	The default Gateway address is 0.0.0.0. It can be modified according to the network availability.

<b>DNS</b>	The default DNS address is 0.0.0.0. It can be modified according to the network availability.
<b>TCP COMM. Port</b>	The default TCP COMM Port value is 4370. It can be modified according to the network availability.
<b>DHCP</b>	Dynamic Host Configuration Protocol dynamically allocates IP addresses for clients via server.
<b>Display in Status Bar</b>	Toggle to set whether to display the network icon on the status bar.

## 5.2 Serial Comm.

To establish communication with the device through a serial port (RS232/RS485), you need to conduct serial port settings.

Click **Serial Comm** on the **Comm.** Settings interface to configure the settings.



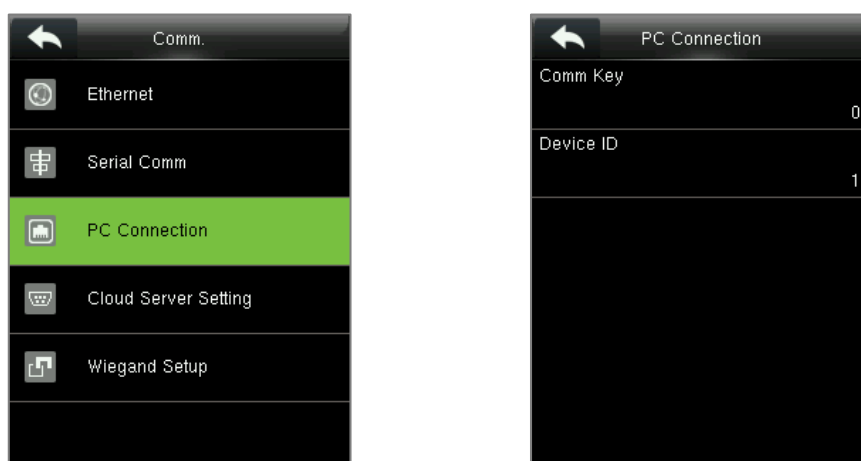
### Function Description

Function Name	Descriptions
<b>Serial Port</b>	<p><b>no using:</b> Do not communicate with the device through the serial port.</p> <p><b>RS232(PC):</b> Communicates with the device through RS232 serial port.</p> <p><b>RS485(PC):</b> Communicates with the device through RS485 serial port.</p> <p><b>Master Unit:</b> When RS485 is used as the function of "<b>Master unit</b>", the device will act as a master unit, and it can be connected to RS485 fingerprint &amp; card reader.</p>
<b>Baudrate</b>	<p>The rate at which the data is communicated with PC, there are 4 options of baud-rate: 115200 (default), 57600, 38400, 19200 and 9600.</p> <p>The higher is the baud rate, the faster is the communication speed, but also the less reliable. Hence, a higher baud rate can be used when the communication distance is short; when the communication distance is long, choosing a lower baud rate would be more reliable.</p>

## 5.3 PC Connection

**Comm** Key facilitates to improve the security of data by setting the communication between the device and the PC. Once the Comm Key is set, a password is required to connect the device to the PC software.

Click **PC Connection** on the **Comm.** Settings interface to configure the communication settings.

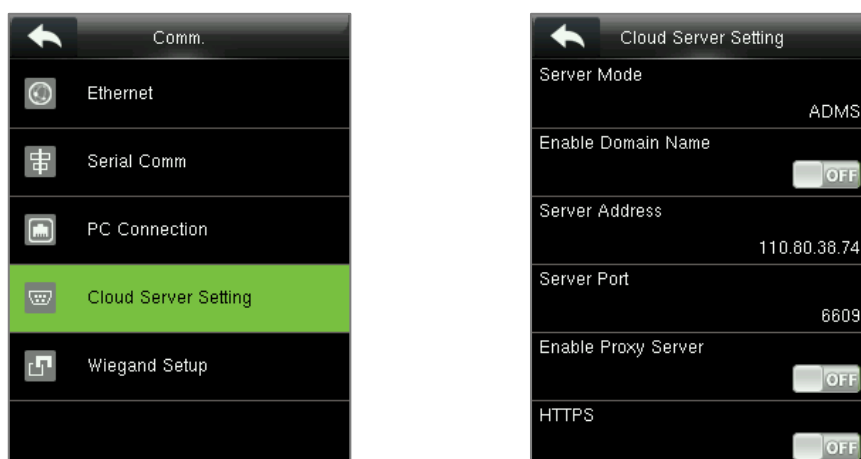


### Function Description

Function Name	Descriptions
<b>Comm Key</b>	The default password is 0 and can be changed. The Comm Key can contain 1-6 digits and ranges between 0~999999.
<b>Device ID</b>	It is the identification number of the device, which ranges between 1 and 254. If the communication method is RS232/RS485, you need to input this device ID in the software communication interface.

## 5.4 Cloud Server Setting

Click **Cloud Server Setting** on the **Comm.** Settings interface to connect with the ADMS server.



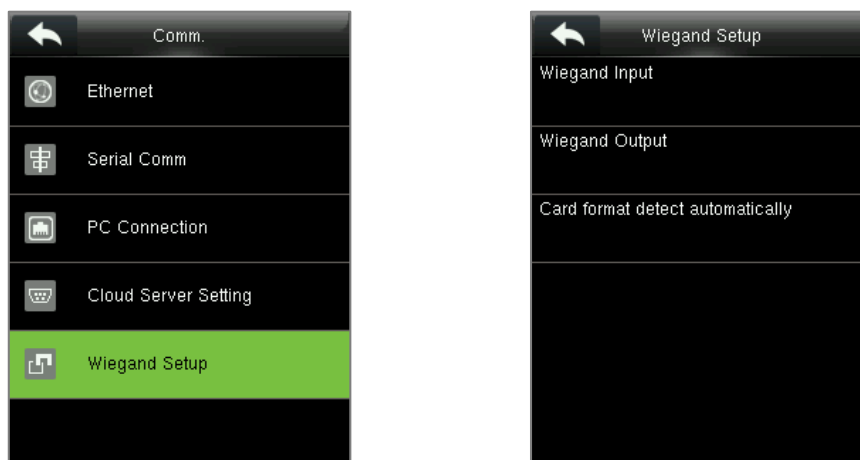
## Function Description

Function Name		Description
<b>Enable Domain Name</b>	<b>Server Address</b>	Once this mode is turned <b>ON</b> , the domain name mode "http://..." will be used, such as http://www.XYZ.com, while "XYZ" denotes the domain name.
<b>Disable Domain Name</b>	<b>Server Address</b>	The IP address of the ADMS server.
	<b>Server Port</b>	Port used by the ADMS server.
<b>Enable Proxy Server</b>		The IP address and the port number of the proxy server is set manually when the proxy is enabled.
<b>HTTPS</b>		Based on HTTP, transmission encryption and identity authentication ensure the security of the transmission process.

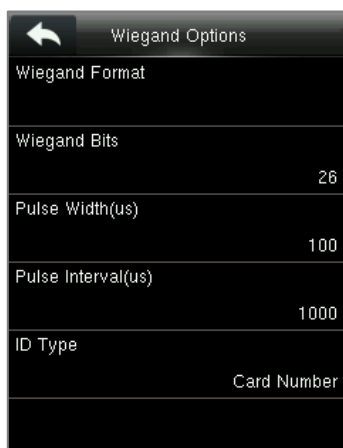
## 5.5 Wiegand Setup

It is used to set the Wiegand input and output parameters.

Tap **Wiegand Setup** on the **Comm.** Settings interface to set the Wiegand input and output parameters.



### 5.5.1 Wiegand input



**Function Description**

Function Name	Descriptions
<b>Wiegand Format</b>	Its value can be 26 bits, 34 bits, 36 bits, 37 bits, and 50 bits.
<b>Wiegand Bits</b>	The number of bits of the Wiegand data.
<b>Pulse Width(us)</b>	The value of the pulse width sent by Wiegand card reader and 100 microseconds by default, which can be adjusted within the range of 20 to 400 microseconds.
<b>Pulse Interval(us)</b>	The default value is 1000 microseconds and can be adjusted within the range of 200 to 20000 microseconds.
<b>ID Type</b>	Select between the User ID and card number.

**Various Common Wiegand Format Description:**

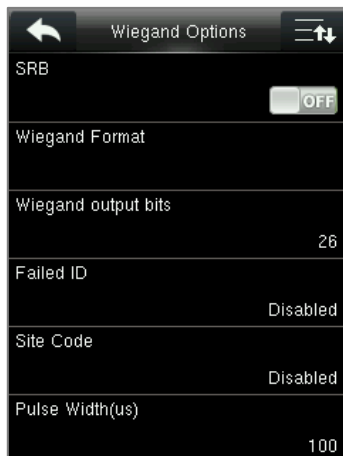
Wiegand Format	Description
<b>Wiegand26</b>	<p>EEEEEEEEEEEEEEEEEEEEEEEEEEEECO</p> <p>It consists of 26 bits of binary code. The 1<sup>st</sup> bit is the even parity bit of the 2<sup>nd</sup> to 13<sup>th</sup> bits, while the 26<sup>th</sup> bit is the odd parity bit of the 14<sup>th</sup> to 25<sup>th</sup> bits. The 2<sup>nd</sup> to 25<sup>th</sup> bits is the card numbers.</p>
<b>Wiegand26a</b>	<p>ESSSSSSSSSSSSSSSSSSSSSSSSSSCO</p> <p>It consists of 26 bits of binary code. The 1<sup>st</sup> bit is the even parity bit of the 2<sup>nd</sup> to 13<sup>th</sup> bits, while the 26<sup>th</sup> bit is the odd parity bit of the 14<sup>th</sup> to 25<sup>th</sup> bits. The 2<sup>nd</sup> to 9<sup>th</sup> bits is the site codes, while the 10<sup>th</sup> to 25<sup>th</sup> bits are the card numbers.</p>
<b>Wiegand34</b>	<p>EEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEECO</p> <p>It consists of 34 bits of binary code. The 1<sup>st</sup> bit is the even parity bit of the 2<sup>nd</sup> to 17<sup>th</sup> bits, while the 34<sup>th</sup> bit is the odd parity bit of the 18<sup>th</sup> to 33<sup>rd</sup> bits. The 2<sup>nd</sup> to 25<sup>th</sup> bits is the card numbers.</p>
<b>Wiegand34a</b>	<p>ESSSSSSSSSSSSSSSSSSSSSSSSSSSSCO</p> <p>It consists of 34 bits of binary code. The 1<sup>st</sup> bit is the even parity bit of the 2<sup>nd</sup> to 17<sup>th</sup> bits, while the 34<sup>th</sup> bit is the odd parity bit of the 18<sup>th</sup> to 33<sup>rd</sup> bits. The 2<sup>nd</sup> to 9<sup>th</sup> bits is the site codes, while the 10<sup>th</sup> to 25<sup>th</sup> bits are the card numbers.</p>
<b>Wiegand36</b>	<p>OFFFFFFFFFCCCCCCCCCCCCCCCCMME</p> <p>It consists of 36 bits of binary code. The 1<sup>st</sup> bit is the odd parity bit of the 2<sup>nd</sup> to 18<sup>th</sup> bits, while the 36<sup>th</sup> bit is the even parity bit of the 19<sup>th</sup> to 35<sup>th</sup> bits. The 2<sup>nd</sup> to 17<sup>th</sup> bits is the device codes. The 18<sup>th</sup> to 33<sup>rd</sup> bits is the card numbers, and the 34<sup>th</sup> to 35<sup>th</sup> bits are the manufacturer codes.</p>
<b>Wiegand36a</b>	<p>EEEEEEEEEEEEEEEEEEEEEEEEEEEECO</p> <p>It consists of 36 bits of binary code. The 1<sup>st</sup> bit is the even parity bit of the 2<sup>nd</sup> to 18<sup>th</sup> bits, while the 36<sup>th</sup> bit is the odd parity bit of the 19<sup>th</sup> to 35<sup>th</sup> bits. The 2<sup>nd</sup> to 19<sup>th</sup> bits is the device codes, and the 20<sup>th</sup> to 35<sup>th</sup> bits are the card numbers.</p>



<b>Wiegand37</b>	OMMMMMSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCE It consists of 37 bits of binary code. The 1 <sup>st</sup> bit is the odd parity bit of the 2 <sup>nd</sup> to 18 <sup>th</sup> bits, while the 37 <sup>th</sup> bit is the even parity bit of the 19 <sup>th</sup> to 36 <sup>th</sup> bits. The 2 <sup>nd</sup> to 4 <sup>th</sup> bits is the manufacturer codes. The 5 <sup>th</sup> to 16 <sup>th</sup> bits is the site codes, and the 21 <sup>st</sup> to 36 <sup>th</sup> bits are the card numbers.
<b>Wiegand37a</b>	EMMMFFFFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCCCCCO It consists of 37 bits of binary code. The 1 <sup>st</sup> bit is the even parity bit of the 2 <sup>nd</sup> to 18 <sup>th</sup> bits, while the 37 <sup>th</sup> bit is the odd parity bit of the 19 <sup>th</sup> to 36 <sup>th</sup> bits. The 2 <sup>nd</sup> to 4 <sup>th</sup> bits is the manufacturer codes. The 5 <sup>th</sup> to 14 <sup>th</sup> bits is the device codes, and 15 <sup>th</sup> to 20 <sup>th</sup> bits are the site codes, and the 21 <sup>st</sup> to 36 <sup>th</sup> bits are the card numbers.
<b>Wiegand50</b>	ESSSSSSSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO It consists of 50 bits of binary code. The 1 <sup>st</sup> bit is the even parity bit of the 2 <sup>nd</sup> to 25 <sup>th</sup> bits, while the 50 <sup>th</sup> bit is the odd parity bit of the 26 <sup>th</sup> to 49 <sup>th</sup> bits. The 2 <sup>nd</sup> to 17 <sup>th</sup> bits is the site codes, and the 18 <sup>th</sup> to 49 <sup>th</sup> 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.

### 5.5.2 Wiegand output



### Function Description

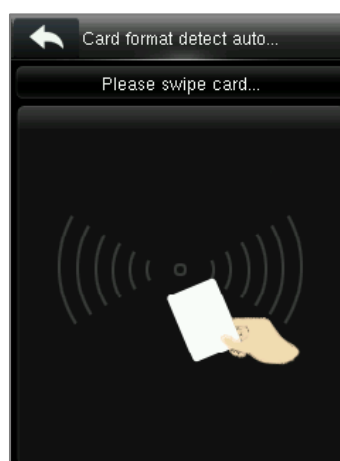
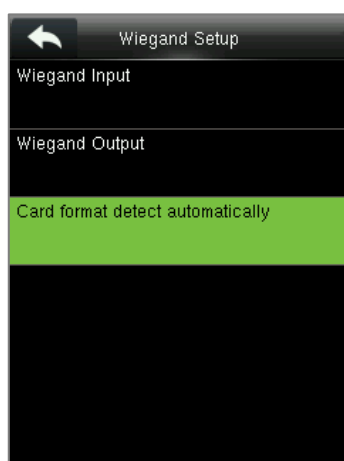
Function Name	Descriptions
<b>SRB</b>	When SRB is enabled, the lock is controlled by the SRB to prevent the lock from opening due to device removal.
<b>Wiegand Format</b>	Its value can be 26 bits, 34 bits, 36 bits, 37 bits, and 50 bits.
<b>Wiegand output bits</b>	After selecting the required Wiegand format, select the corresponding output bit digits of the Wiegand format.
<b>Failed ID</b>	If the verification fails, the system will send the failed ID to the device and replace the card number or personnel ID with the new one.

<b>Site Code</b>	It is similar to the device ID. The difference is that a site code can be set manually and is repeatable on a different device. The valid value ranges from 0 to 256 by default.
<b>Pulse Width(us)</b>	The time width represents the changes in the quantity of electric charge with regular high-frequency capacitance within a specified time.
<b>Pulse Interval(us)</b>	The time interval between pulses.
<b>ID Type</b>	Select the ID types as either User ID or card number.

### 5.5.3 Card Format Detect Automatically

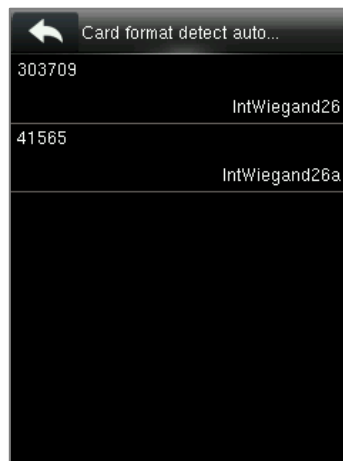
The function aims at assisting user with quickly detecting the card type and its corresponding format. Various card formats are present in the device. After card swiping, the system will read the card number and will compare the detected card format with different card formats. The user only needs to choose the item equivalent to the actual card number and set the format as the Wiegand format for the device. This function is also applicable to card reading function and auxiliary Wiegand reader.

Click **Card format detect automatically** on the Wiegand Setup interface. Then place the card in the card induction area, as shown below:

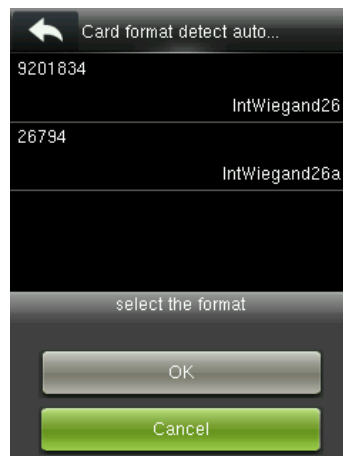


#### Operating Procedure:

- 1) After entering the **Card Format Detect Automatically** interface of an ID device, swipe the ID card above the card reader (on the local device or auxiliary card reader), the interface will show the automatically detected Wiegand formats and the analyzed card numbers.



- 2) Choose the item corresponding to the actual card number as the device's [**Wiegand format**], which is the Wiegand format for reading that type of card.

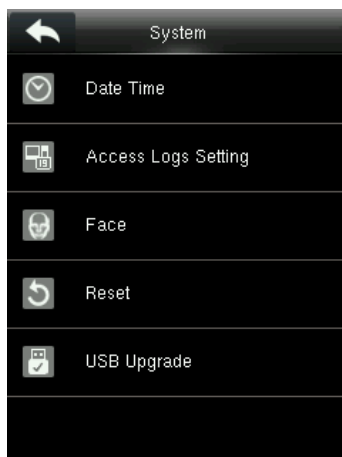


**NOTE:** In the [**Card format detect automatically**] interface of an IC device, the device cannot detect the card number or Wiegand format only by swiping an IC card. For detecting the Wiegand format of an IC card, it is needed to connect an IC card reader with the device and swipe an IC card above the auxiliary card reader, so that the device will show the card number and the Wiegand format.

## 6 System Settings

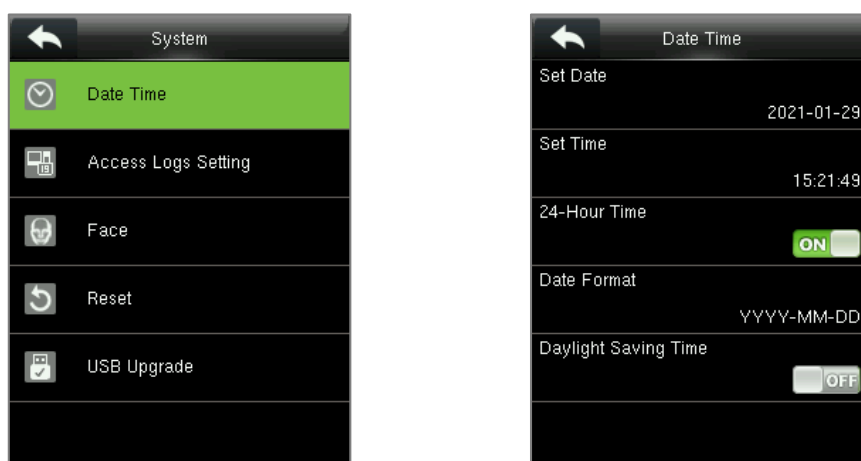
It helps to set related system parameters to optimize the accessibility of the device.

Tap **System** on the **Main Menu** interface to get into its menu options.

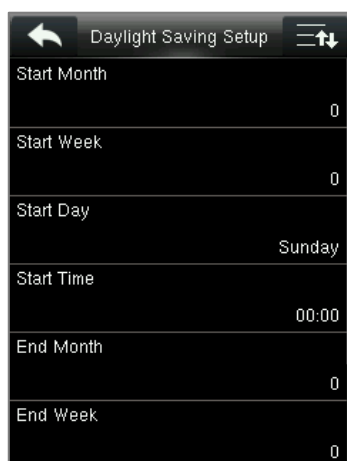


### 6.1 Date and Time

Tap **Date Time** on the **System** interface to set the date and time.



1. Tap **Set Date** to manually set time and tap **Confirm** to save.
2. Tap **Set Time** to select a time zone then tap the return button to save and exit.
3. Tap **24-Hour Time** to enable or disable this format. If enabled, then select the **Date Format** to set the date format i.e., the way date should be displayed on the device.
4. Tap **Daylight Saving Time** to enable or disable the function. If enabled, tap **Daylight Saving Mode** to select a daylight-saving mode and then tap **Daylight Saving Setup** to set the switch time.

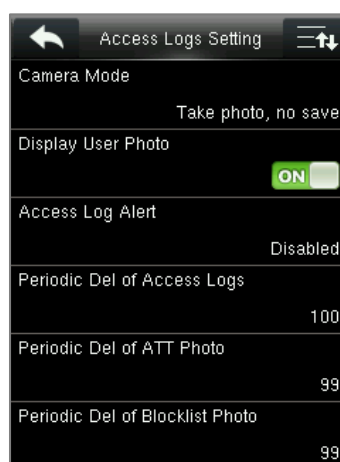
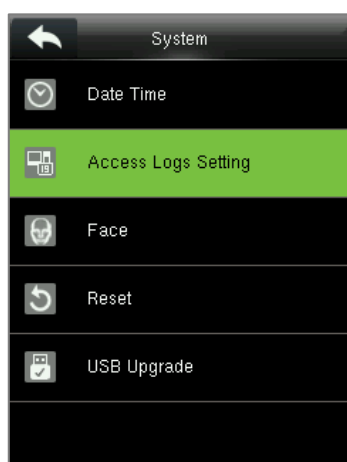
**Week Mode****Date Mode**

When restoring the factory settings, the time (24-hour) and date format (**YYYY-MM-DD**) can be restored, but the device date and time cannot be restored.

**NOTE:** For example, if a user sets the time of the device (18:35 on March 15, 2019) to 18:30 on January 1, 2020. After restoring the factory settings, the time of the device will remain at 18:30 on January 1, 2020.

## 6.2 Access Logs Setting

Click **Access Logs Setting** on the System interface.



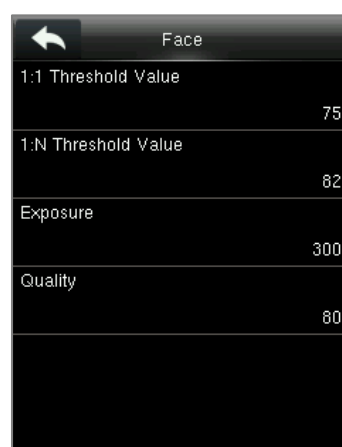
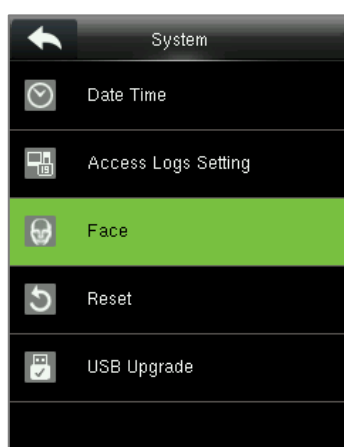
### Function Description

Function Name	Description
<b>Camera Mode</b>	<p>Choose whether to capture and save the current snapshot image during verification. There are 5 modes:</p> <p><b>No Photo:</b> No photo is taken during user verification.</p> <p><b>Take photo, no save:</b> Photo is taken but not saved during verification.</p> <p><b>Take photo and save:</b> All the photos taken during verification is saved.</p>

	<p><b>Save on successful verification:</b> Photo is taken and saved for each successful verification.</p> <p><b>Save on failed verification:</b> Photo is taken and saved only for each failed verification.</p>
<b>Display User Photo</b>	Choose whether to display the user photo when the user passes the verification.
<b>Access Log Alert</b>	When the record space of the attendance access reaches the maximum threshold value, the device automatically displays the memory space warning. Users may disable the function or set a valid value between 1 and 9999.
<b>Periodic Del of Access Logs</b>	When access logs reach its maximum capacity, the device automatically deletes a set of old access logs. Users may disable the function or set a valid value between 1 and 999.
<b>Periodic Del of ATT Photo</b>	When attendance photos reach its maximum capacity, the device automatically deletes a set of old attendance photos. Users may disable the function or set a valid value between 1 and 99.
<b>Periodic Del of Blocklist Photo</b>	When block listed photos reach its maximum capacity, the device automatically deletes a set of old block listed photos. Users may disable the function or set a valid value between 1 and 99.
<b>Authentication Timeout(s)</b>	The amount of time taken to display a successful verification message. Valid value: 1 to 9 seconds.
<b>Face comparison Interval (s)</b>	The amount of time required to compare facial templates. Valid value: 0 to 9 seconds.

## 6.3 Face Parameters

Click **Face** on the **System** interface to go to the face parameter settings.



### Function Description

Function Name	Description
---------------	-------------

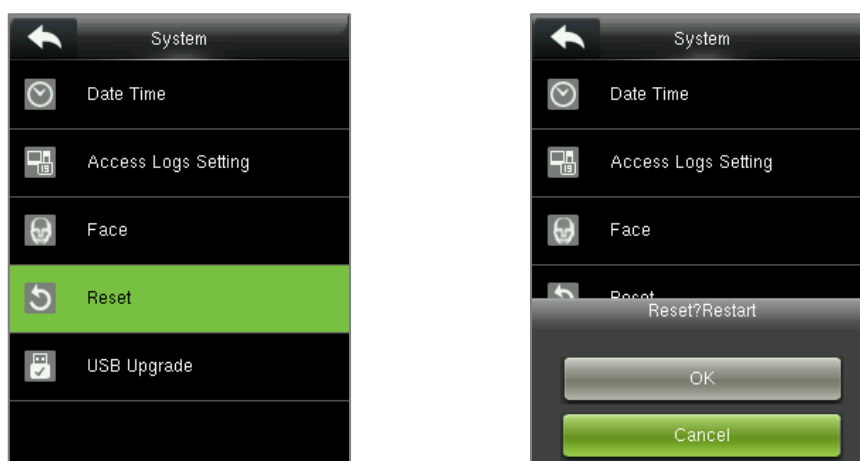
<b>1:1 Threshold Value</b>	Under 1:1 verification mode, the verification will only be successful when the similarity between the acquired facial image and the user's facial templates enrolled in the device is greater than the set value. The valid value ranges from 55 to 120. The higher the thresholds, the lower the misjudgement rate and the higher the rejection rate, and vice versa. It is recommended to set the default value of 75.
<b>1:N Threshold Value</b>	Under 1:N verification mode, the verification will only be successful when the similarity between the acquired facial image and all registered facial templates is greater than the set value. The valid value ranges from 65 to 120. The higher the thresholds, the lower the misjudgement rate and the higher the rejection rate, and vice versa. It is recommended to set the default value of 82.
<b>Exposure</b>	This parameter is used to set the exposure value of the camera.
<b>Quality</b>	It is the image quality for facial registration and comparison. The higher the value, the clearer image is required.

**NOTE:** Improper adjustment of the exposure and quality parameters may severely affect the performance of the device. Please adjust the exposure parameter only under the guidance of the after-sales service personnel of our company.

## 6.4 Factory Reset

The Factory Reset function restores the device settings such as communication settings and system settings, to the default factory settings (this function does not clear registered user data).

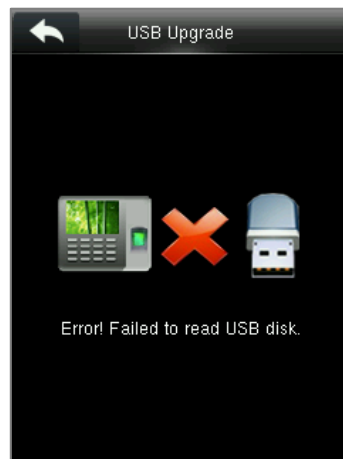
Click **Reset** on the **System** interface and then select **OK** to restore the default factory settings.



## 6.5 USB Upgrade

With this option, the device firmware can be upgraded by using the upgrade file in a USB disk. Before conducting this operation, ensure that the USB disk is properly inserted into the device and contains the correct upgrade file.

If no USB disk is inserted in, the system gives the following prompt after you click **USB Upgrade** on the **System** interface.

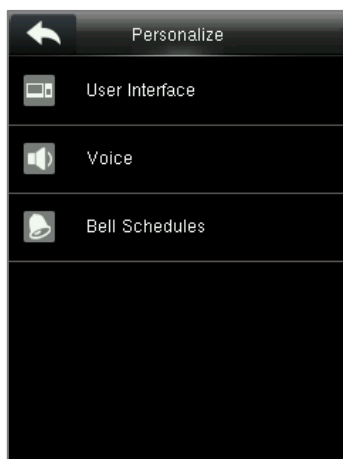


**NOTE:** If upgrade file is needed, please contact our technical support. Firmware upgrade is not recommended under normal circumstances.



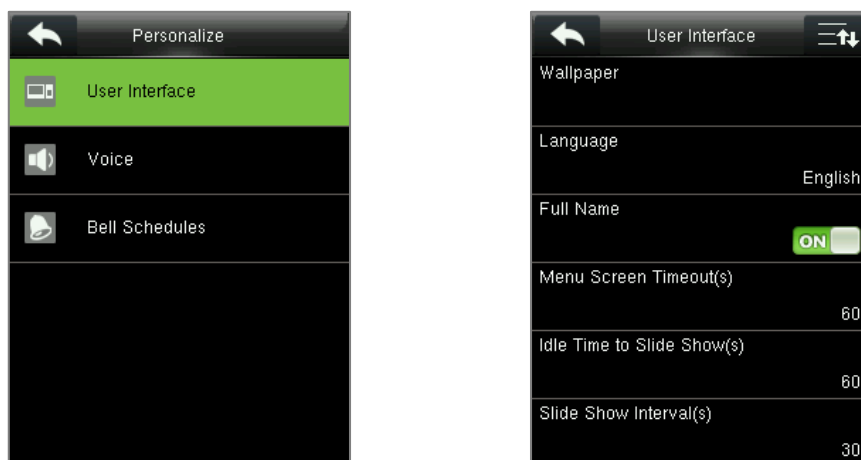
## 7 Personalize Settings

Click **Personalize** on the **Main Menu** interface to customize interface settings, voice, bell, punch state options, and shortcut key mappings.



### 7.1 Interface Settings

Select **User Interface** on the **Personalize** interface to customize the display style of the main interface.



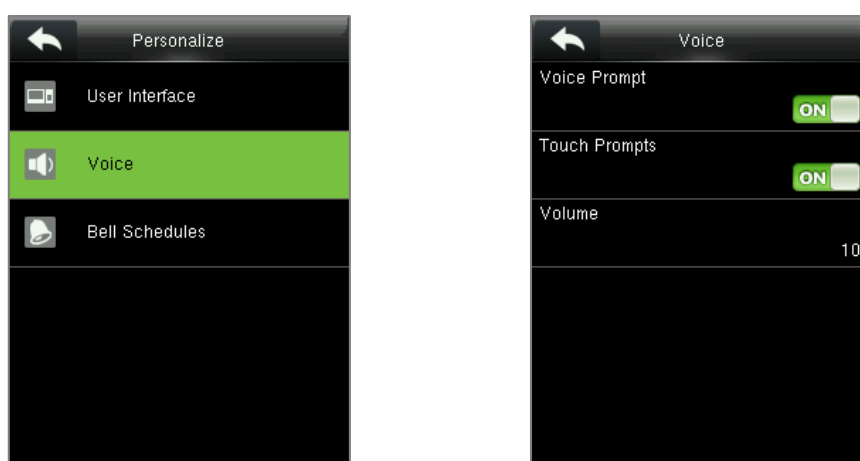
#### Function Description

Function Name	Description
<b>Wallpaper</b>	It helps to select the main screen wallpaper according to the user preference.
<b>Language</b>	It helps to select the language of the device.
<b>Full Name</b>	Once enabled, the user will need to fill in his/her last name and first name when registering.
<b>Menu Screen Timeout (s)</b>	When there is no operation, and the time exceeds the set value, the device automatically goes back to the initial interface.

	The function can either be disabled or set the required value between 60 and 99999 seconds.
<b>Idle Time To Slide Show (s)</b>	When there is no operation, and the time exceeds the set value, a slide show is displayed. The function can be disabled, or you may set the value between 3 and 999 seconds.
<b>Slide Show Interval (s)</b>	It is the time interval in switching between different slide show pictures. The function can be disabled, or you may set the interval between 3 and 999 seconds.
<b>Idle Time To Sleep (m)</b>	If the sleep mode is activated, and when there is no operation in the device, then the device will enter standby mode. Press any key or finger to resume normal working mode. This function can be disabled or set a value within 1-999 minutes.
<b>Main Screen Style</b>	The style of the main screen can be selected according to the user preference.

## 7.2 Voice Settings

Select **Voice** on the **Personalize** interface to configure the voice settings.

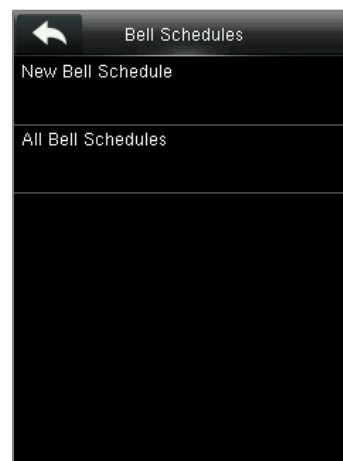
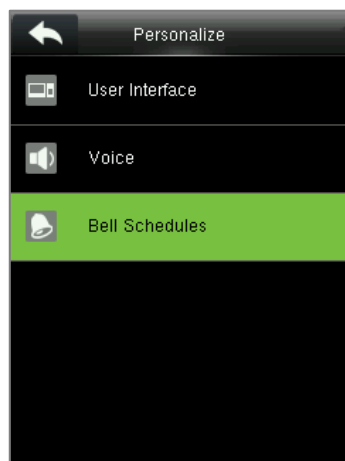


### Function Description

Function Name	Description
<b>Voice Prompt</b>	Select whether to enable voice prompts during operating.
<b>Touch Prompt</b>	Select whether to enable keypad sounds.
<b>Volume</b>	Adjust the volume of the device; valid value: 0-100.

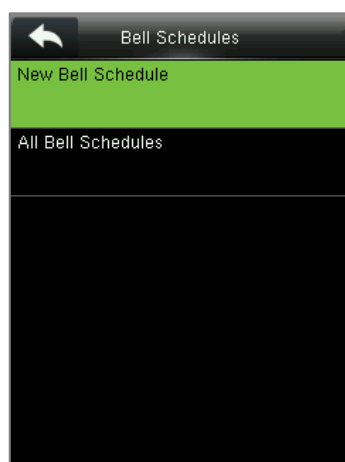
## 7.3 Bell Schedules

Select **Bell Schedules** on the **Personalize** interface to configure the Bell settings.



### New Bell Schedule

Click **New Bell Schedule** on the **Bell Schedule** interface to add a new bell schedule.

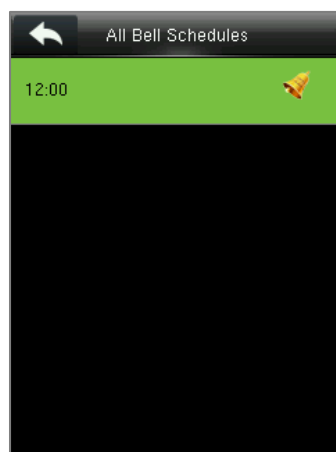
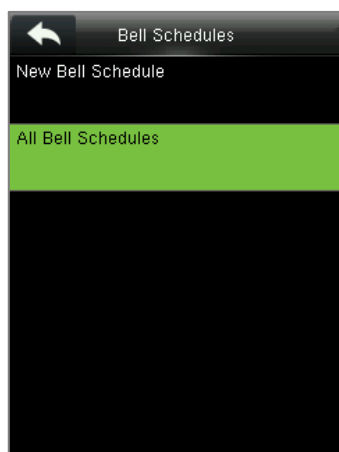


### Function Description

Function Name	Description
<b>Bell Status</b>	Toggle to enable or disable the bell status.
<b>Bell Time</b>	Once the required time is set, the device automatically triggers to ring the bell during that time.
<b>Repeat</b>	Set the required number of counts to repeat the scheduled bell.
<b>Ring Tone</b>	Select a ringtone.
<b>Internal bell delay(s)</b>	Set the replay time of the internal bell. Valid values range from 1 to 999 seconds.

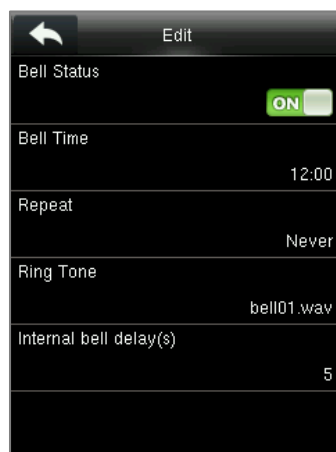
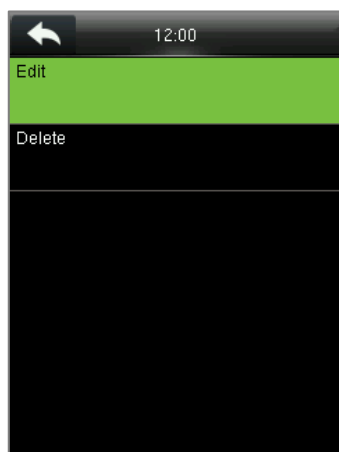
### All Bell Schedules

Once the bell is scheduled, on the **Bell Schedules** interface, click **All Bell Schedules** to view the newly scheduled bell.



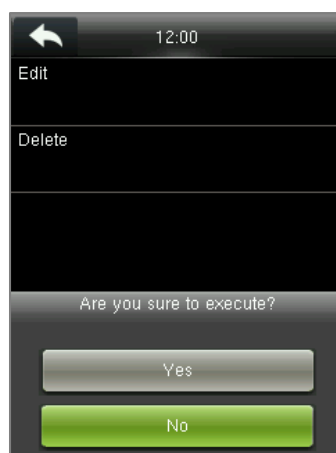
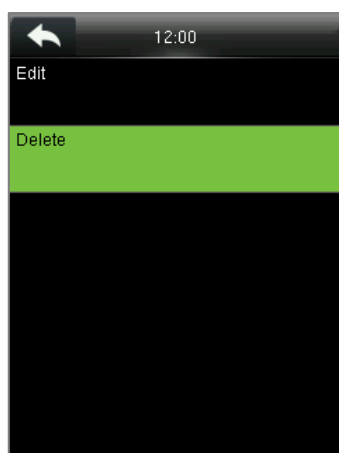
### Edit the scheduled bell

On the **All Bell Schedules** interface, click on the required bell schedule, and select **Edit** to edit the selected bell schedule. The editing method is the same as the operations of adding a new bell schedule.



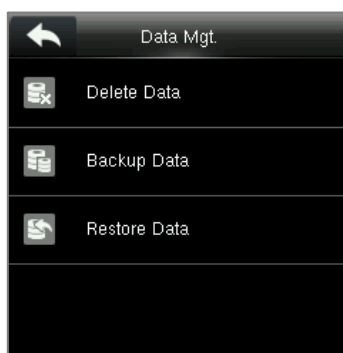
### Delete a bell

On the **All Bell Schedules** interface, click the required bell schedule, and select **Delete**, and then click **Yes** to delete the selected bell.



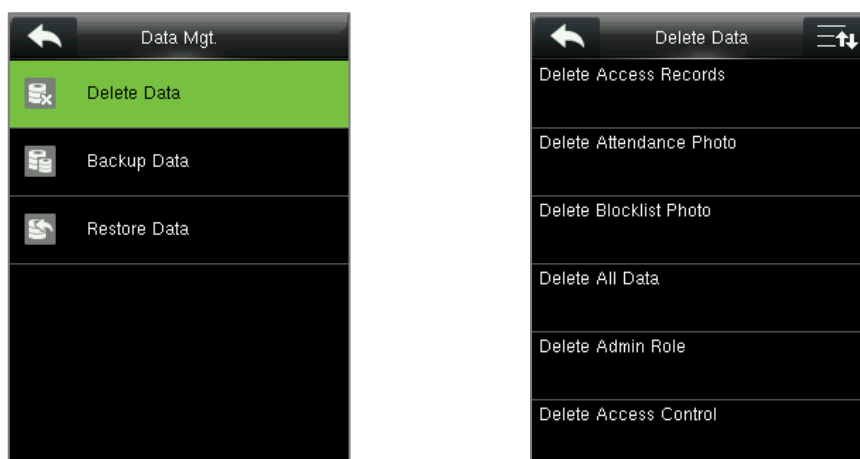
## 8 Data Management

On the **Main Menu**, click **Data Mgt.** to delete the relevant data in the device.



### 8.1 Delete Data

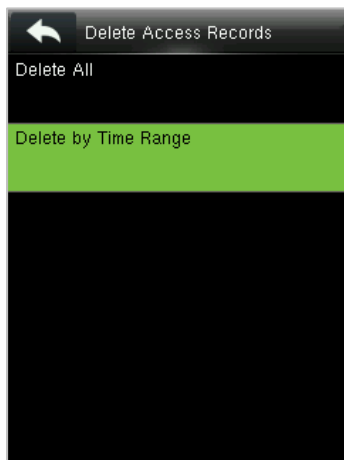
Select **Delete Data** on the **Data Mgt.** interface to delete the required data.



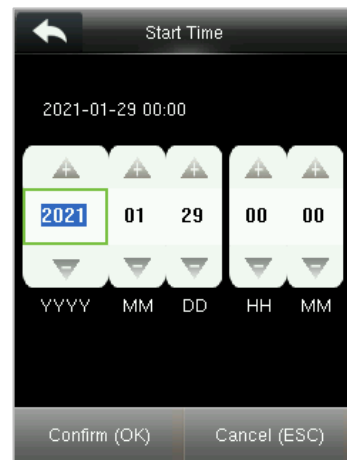
#### Function Description

Function Name	Description
<b>Delete Access Records</b>	To delete attendance data/access records conditionally.
<b>Delete Attendance Photo</b>	To delete attendance photos of designated personnel.
<b>Delete Blocklist Photo</b>	To delete the photos taken during failed verifications.
<b>Delete All Data</b>	To delete information and attendance logs/access records of all registered users.
<b>Delete Admin Role</b>	To remove administrator privileges.
<b>Delete Access Control</b>	To delete all access data.
<b>Delete User Photo</b>	To delete all user photos in the device.
<b>Delete Wallpaper</b>	To delete all wallpapers in the device.
<b>Delete Screen Savers</b>	To delete the screen savers in the device.

The user may select **Delete All** or **Delete by Time Range** when deleting the access records, attendance photos or block listed photos. Selecting **Delete by Time Range**, you need to set a specific time range to delete all data within a specific period.



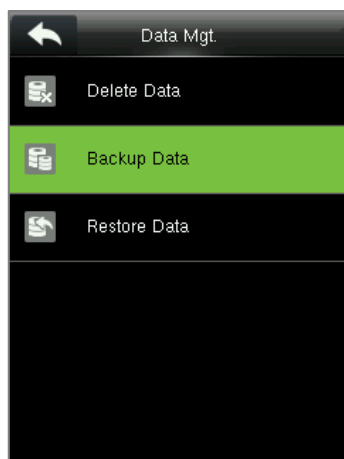
Select Delete by Time Range



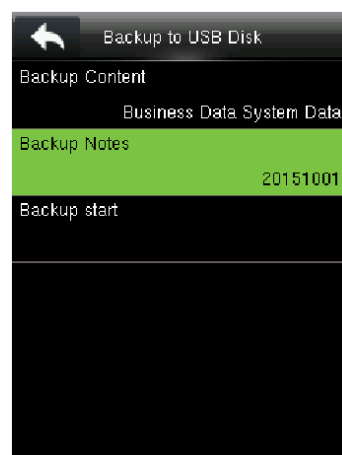
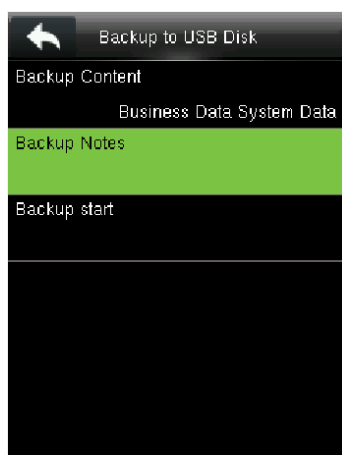
Set the time range and click **OK**

## 8.2 Backup Data

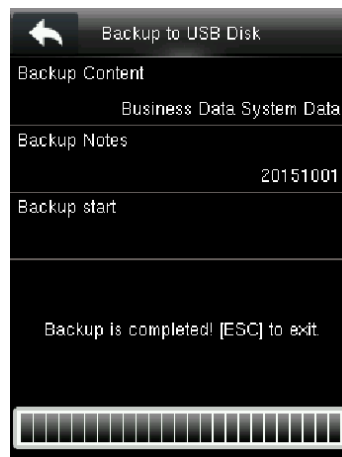
Tap **Backup Data** on the **Data Mgt.** interface to back up the data to the device or U disk.



Press **Backup to USB Disk** on the **Backup Data** interface. Click **Backup Notes** to input backup notes.



The following is the backup complete result interface.



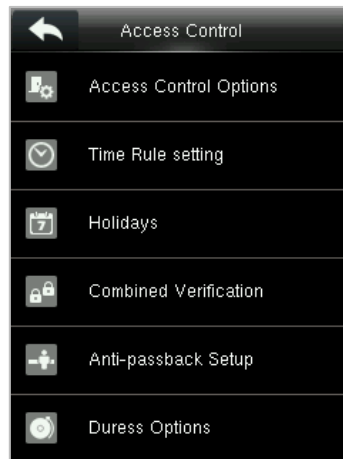
## 8.3 Restore Data

Tap **Restore Data** on the **Data Mgt.** interface to restore the data in the device or U disk to the device.



## 9 Access Control

On the **Main Menu**, tap **Access Control** to set the schedule of the door opening, locks control and to configure other parameters settings related to access control.

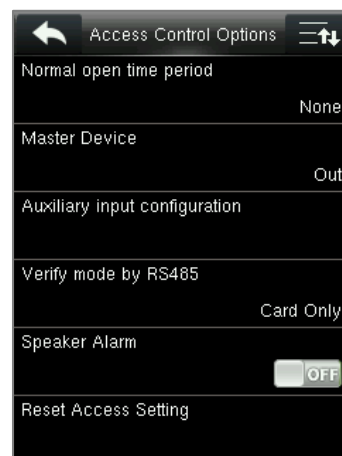
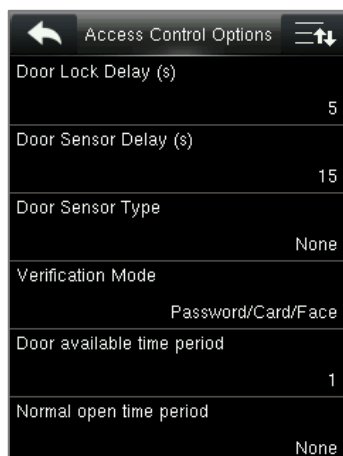


**To gain access, the registered user must meet the following conditions:**

1. The relevant door's current unlock time should be within any valid time zone of the user's time period.
2. The corresponding user's group must be already set in the door unlock combination (and if there are other groups, being set in the same access combo, then the verification of those group's members is also required to unlock the door).
3. In default settings, new users are allocated into the first group with the default group time zone, where the access combo is "1" and is set in unlock state by default.

### 9.1 Access Control Options

Tap **Access Control Options** on the **Access Control** interface to set the parameters of the control lock of the terminal and related equipment.





## Function Description

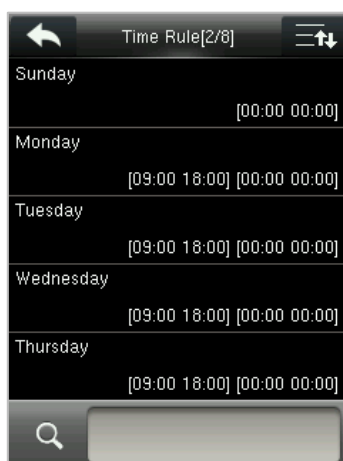
Function Name	Description
<b>Door Lock Delay (s)</b>	The length of time that the device controls the electric lock to be in unlock state. Valid value: 1 to 10 seconds; 0 seconds represents disabling the function.
<b>Door Sensor Delay (s)</b>	If the door is not locked and is left open for a certain duration (Door Sensor Delay), an alarm will be triggered. The valid value of Door Sensor Delay ranges from 1 to 255 seconds.
<b>Door Sensor Type</b>	There are three Sensor types: <b>None</b> , <b>Normal Open</b> , and <b>Normal Closed</b> . <b>None:</b> It means the door sensor is not in use. <b>Normally Open:</b> It means the door is always left open when electric power is on. <b>Normally Closed:</b> It means the door is always left closed when electric power is on.
<b>Verification Mode</b>	The supported verification mode includes Password/Card/Face, User ID only, Password, Card only, Password + Card, Password/Card, Face only, Face + Password, and Face+Card.
<b>Door available time period</b>	It sets the timing for the door so that the door is accessible only during that period.
<b>Normal open time Period</b>	It is the scheduled time-period for “ <b>Normal Open</b> ” mode so that the door is always open during this period.
<b>Master Device</b>	While configuring the master and slave devices, you may set the state of the master as <b>Out</b> or <b>In</b> . <b>Out:</b> A record of verification on the master device is a check-out record. <b>In:</b> A record of verification on the master device is a check-in record.
<b>Auxiliary input configuration</b>	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.
<b>Verify mode by RS485</b>	It is the verification mode used by the device when it is the master unit. This option will be displayed only if RS485 reader function is enabled.
<b>Speaker Alarm</b>	It transmits a sound alarm or disassembly alarm from the local. When the door is closed or the verification is successful, the system cancels the alarm from the local.
<b>Reset Access Setting</b>	The access control reset parameters include door lock delay, door sensor delay, door sensor type, verification mode, door available time period, normal open time period, master device, and alarm. However, erased access control data in Data Mgt. is excluded.

## 9.2 Time Rule Setting

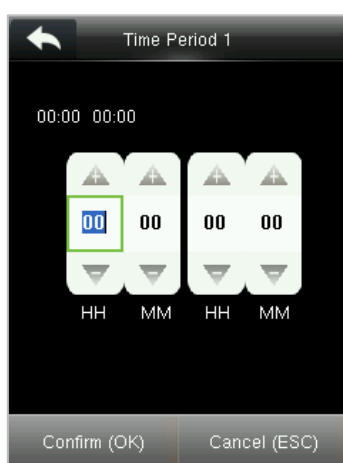
Select **Time Rule Setting** on the Access Control interface to configure the time settings.

- The entire system can define up to 50 Time Periods.
- Each time-period represents **10** 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.
- One can set a maximum of 3 time periods for every time zone. The relationship among these time-periods is "**OR**". Thus, when the verification time falls in any one of these time-periods, the verification is valid.
- The Time Zone format of each time-period is **HH MM-HH MM**, which is accurate to minutes according to the 24-hour clock.

Tap the grey box to search the required Time Zone and specify the required Time Zone number (maximum up to 50 zones).



On the selected Time Zone number interface, click on the required day (that is Monday, Tuesday, etc.) to set the time.



Specify the start and the end time, and then click **OK**.

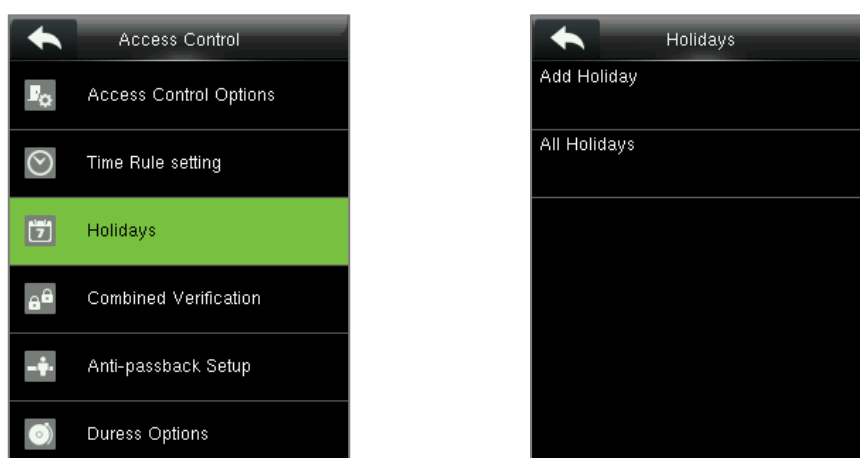
**NOTE:**

1. The door is inaccessible for the whole day when the End Time occurs before the Start Time (such as **23:57 to 23:56**).
2. It is the time interval for valid access when the End Time occurs after the Start Time (such as **08:00 to 23:59**).
3. The door is accessible for the whole day when the End Time occurs after the Start Time (such that Start Time is **00:00** and End Time is **23:59**).
4. The default Time Zone 1 indicates that the door is open all day long.

## 9.3 Holidays

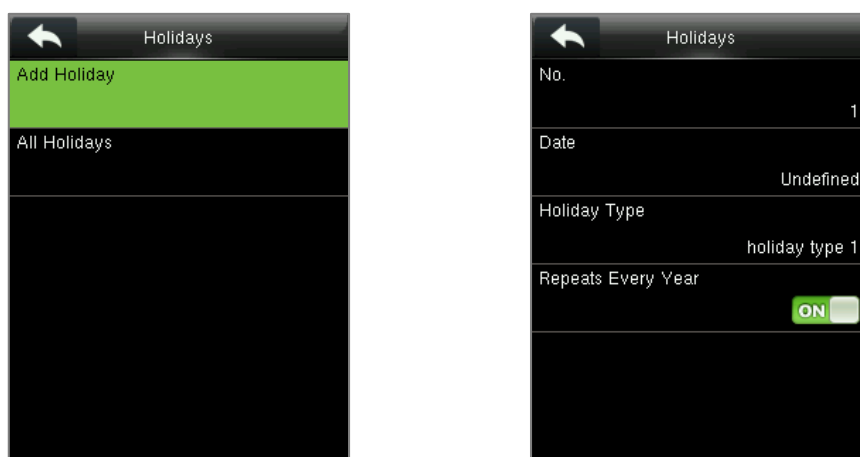
Whenever there is a holiday, you may need a distinct access time; but changing everyone's access time one by one is extremely cumbersome, so a holiday access time can be set that applies to all employees and the user will be able to open the door during the holidays.

Click **Holidays** on the **Access Control** interface to set the Holiday access.



### ● Add a New Holiday

Tap **Add Holiday** on the **Holidays** interface and set the holiday parameters.



- **Edit a Holiday**

On the **Holidays** interface, select a holiday item to be modified. Tap **Edit** to modify holiday parameters.

- **Delete a Holiday**

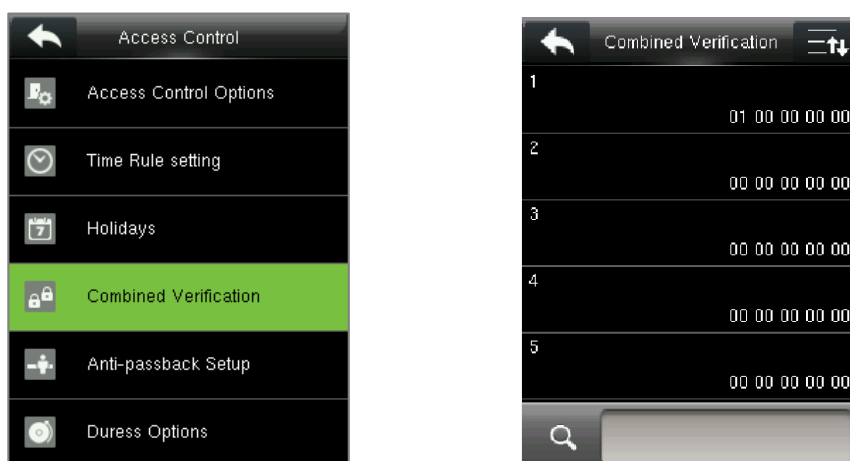
On the **Holidays** interface, select a holiday item to be deleted and tap **Delete**. Press **OK** to confirm the deletion. After deletion, this holiday does not display on the **All Holidays** interface.

## 9.4 Combined Verification

Access groups are arranged into different door-unlocking combinations to achieve multiple verifications and strengthen security.

In a door-unlocking combination, the range of the combined number N is  $0 \leq N \leq 5$  and the number of members N may all belong to one access group or may belong to five different access groups.

Tap **Combined Verification** on the **Access Control** interface to configure the combined verification setting.



On the combined verification interface, click the Door-unlock combination to be set, and select the **up** and **down** arrows to input the combination number, and then press **OK**.

**For Example:**

- If the **Door-unlock combination 1** is set as **(01 03 05 06 08)**. It indicates that the unlock combination 1 consists of 5 people and all the 5 individuals are from 5 groups, namely, AC Group 1, AC Group 3, AC Group 5, AC Group 6, and AC Group 8, respectively.
- If the **Door-unlock combination 2** is set as **(02 02 04 04 07)**. It indicates that the unlock combination 2 consists of 5 people; the first two are from AC Group 2, the next two are from AC Group 4, and the last person is from AC Group 7.
- If the **Door-unlock combination 3** is set as **(09 09 09 09 09)**. It indicates that there are 5 people in this combination; all of which are from AC Group 9.
- If the **Door-unlock combination 4** is set as **(03 05 08 00 00)**. It indicates that the unlock combination 4 consists of only three people. The first person is from AC Group 3, the second person is from AC Group 5, and the third person is from AC Group 8.

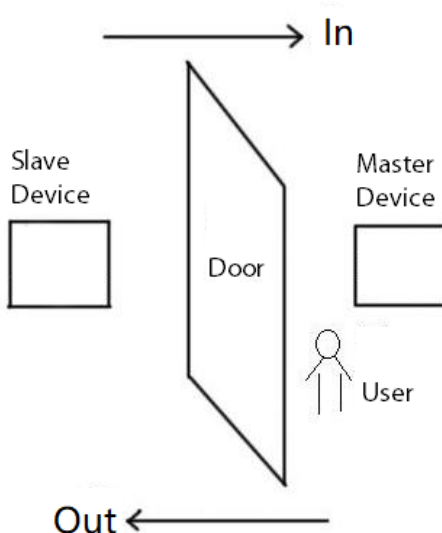
**NOTE:** To delete the door-unlock combination, set all Door-unlock combinations to 0.

## 9.5 Anti-passback Setup

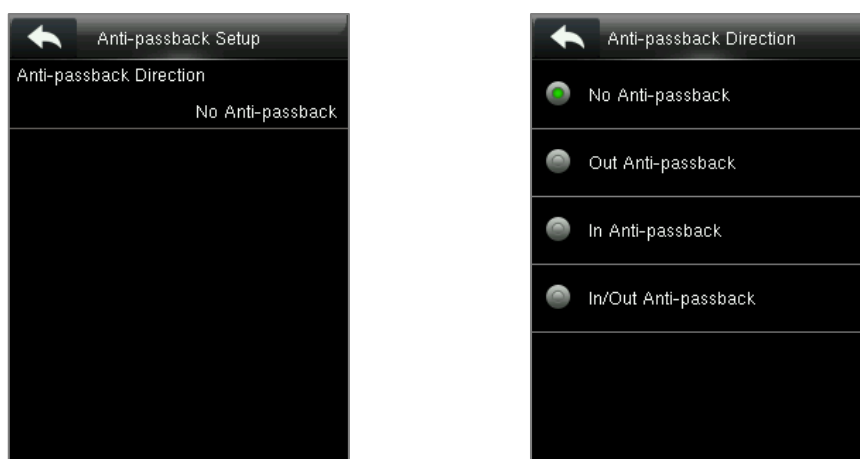
A user may be followed by some person(s) to enter the door without verification, resulting in a security breach. So, to avoid such situations, the Anti-Passback option was developed. Once it is enabled, the check-in and check-out record must occur alternatively to open the door to represent a consistent pattern.

This function requires two devices to work together:

One device is installed on the indoor side of the door (master device), and the other one is installed on the outdoor side of the door (the slave device). The two devices communicate via the Wiegand signal. The Wiegand format and Output type (User ID / Card Number) adopted by the master device and slave device must be consistent.



Tap **Anti-Passback Setup** on the **Access Control** interface.



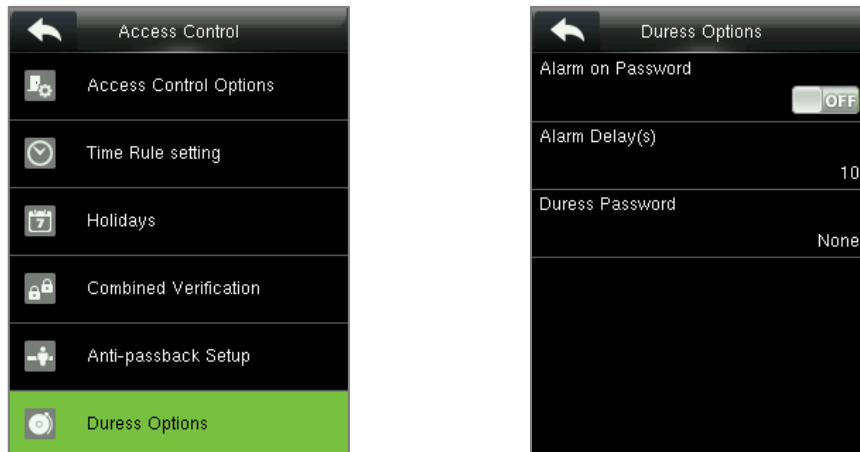
## Function Description

Function Name	Description
<b>Anti-passback direction</b>	<p><b>No Anti-Passback:</b> The Anti-Passback function is disabled, which means successful verification through either the master device or slave device can unlock the door. The attendance state is not saved in this option.</p> <p><b>Out Anti-Passback:</b> The user can check-out only if the last record is a check-in record otherwise an alarm is raised. However, the user can check-in freely.</p> <p><b>In Anti-Passback:</b> The user can check-in again only if the last record is a check-out record otherwise an alarm is raised. However, the user can check-out freely.</p> <p><b>In/Out Anti-Passback:</b> In this case, a user can check-in only if the last record is a check-out or the user can check-out only if the last record is a check-in otherwise the alarm is triggered.</p>

## 9.6 Duress Options Settings

Once a user activates the duress verification function with a specific authentication method(s), and when he/she is under coercion and authenticates using duress verification, the device unlocks the door as usual. At the same time, a signal is sent to trigger the alarm as well.

On the **Access Control** interface, select **Duress Options** to configure the duress settings.



## Function Description

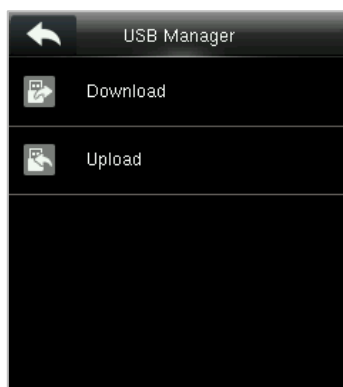
Function Name	Description
<b>Alarm on Password</b>	When a user uses the password verification method, an alarm signal will be generated, otherwise there will be no alarm signal.
<b>Alarm Delay (s)</b>	Alarm signal will not be transmitted until the alarm delay time is elapsed. The value ranges from 1 to 999 seconds.
<b>Duress Password</b>	Set the 6-digit duress password. When the user enters this duress password for verification, an alarm signal will be generated.

## 10 USB Manager

Upload or download data between device and the corresponding software by USB disk.

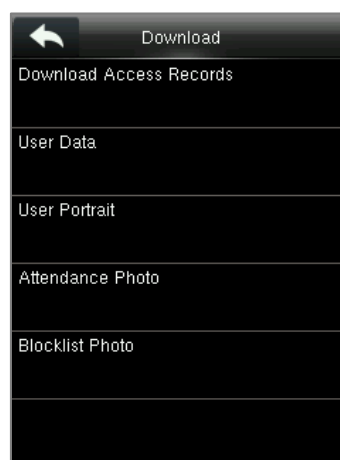
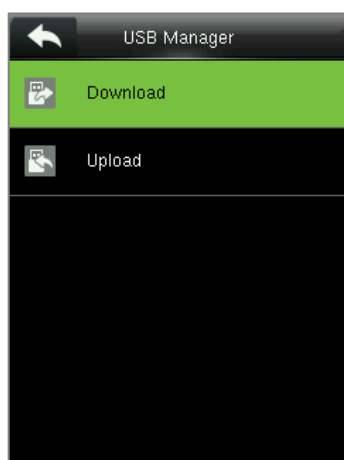
Before uploading/downloading data from/to the USB disk, insert the USB disk into the USB slot first.

Click **USB Manager** on the **Main Menu** interface.



### 10.1 USB Download

Select **Download** on the **USB Manager** interface.

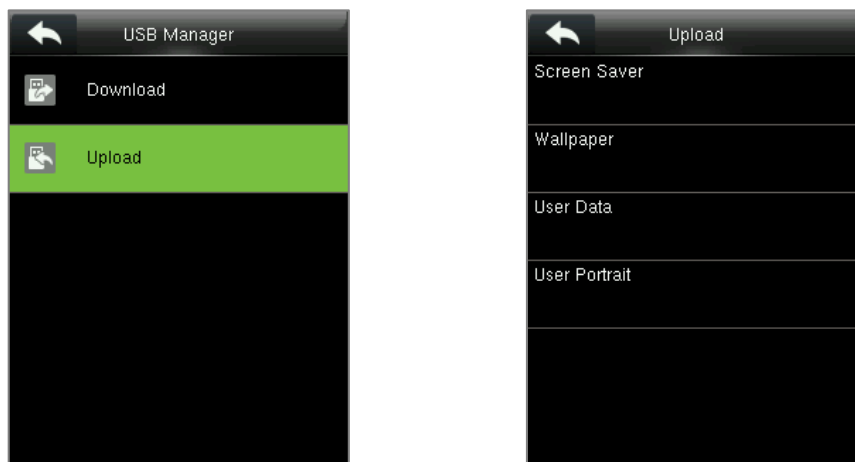


#### Function Description

Function Name	Description
<b>Download Access Records</b>	Download access records in specified time period into USB disk.
<b>User Data</b>	Import all the user information, fingerprints and facial images from the device to a USB disk.
<b>User Portrait</b>	Import the employees' photos from the terminal to a USB disk.
<b>Attendance Photo</b>	Download attendance photos saved in device to U disk. The format of photo is JPG.
<b>Blocklist Photo</b>	Download block list photos saved in device to U disk. The format is JPG.

## 10.2 USB Upload

Select **Upload** on the **USB Manager** interface.



### Function Description

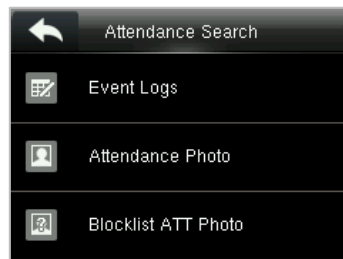
Function Name	Description
Screen Saver	To upload all screen savers from USB disk into the device. You can choose <b>Upload selected picture</b> or <b>Upload all pictures</b> . The images will be displayed on the device's main interface after upload.
Wallpaper	To upload all wallpapers from USB disk into the device. You can choose <b>Upload selected picture</b> or <b>Upload all pictures</b> . The images will be displayed on the screen after upload.
User Data	Upload the message stored in a USB disk to the terminal.
User Portrait	Upload the JPG documents that are named after the user IDs and stored in a USB disk to the terminal, so that user photos can be displayed after the employees pass the verification.



## 11 Attendance Search

Once the identity of a user is verified, the access record is saved in the device. This function enables users to check their access records.

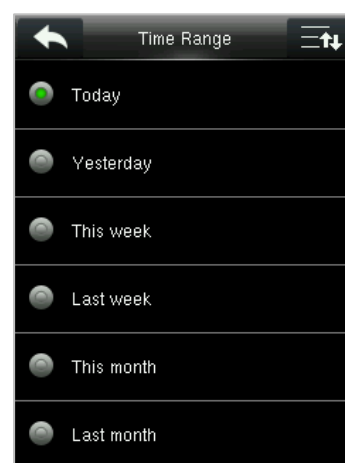
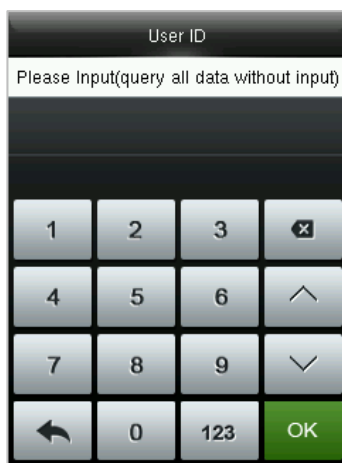
Select **Attendance Search** on the **Main Menu** interface to search for the required Access/Attendance log.



The process of searching for attendance and blocklist photos is similar to that of searching for access records. The following is an example of searching for access records.

On the **Attendance Search** interface, tap **Event Logs** to search for the required record.

1. Enter the user ID to be searched and tap **OK**. If you want to search for records of all users, tap **OK** without entering any user ID.
2. Select the time range in which the records need to be searched.



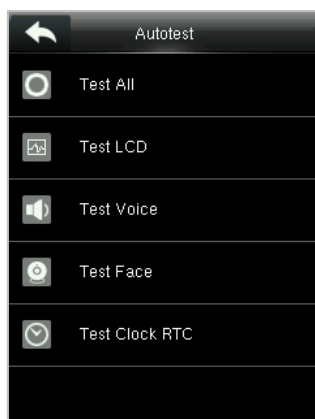
3. Once the record search completes. Tap the record highlighted in green to view its details.
4. The below figure shows the details of the selected record.

Personal Record Search		
Date	User ID	Event Logs
01-29	63	
	1	17:03 16:58 16:55 15:13 15:12 15:12 15:12 12:22 12:21 12:02 12:02 12:02 12:01 12:01
	2	14:07
	0	13:09 13:05 13:05 12:34 12:34 12:34 12:34 12:34 12:34 12:34 12:34 10:54 10:53 10:53 10:45 10:45 10:45 10:45

Personal Record Search		
User ID	Name	Event Logs
1	Mike	01-29 17:03
1	Mike	01-29 16:58
1	Mike	01-29 16:55
1	Mike	01-29 15:13
1	Mike	01-29 15:12
1	Mike	01-29 15:12
1	Mike	01-29 15:12
2	Joy Lee	01-29 14:07
0		01-29 13:09
0		01-29 13:05
0		01-29 13:05
Verification Mode : Card Status : Out		

## 12 Autotest

Select **Main Menu**, tap **Autotest**. It enables the system to automatically test whether the functions of various modules are working normally, including the LCD, Voice, Camera, and Real-Time Clock (RTC).

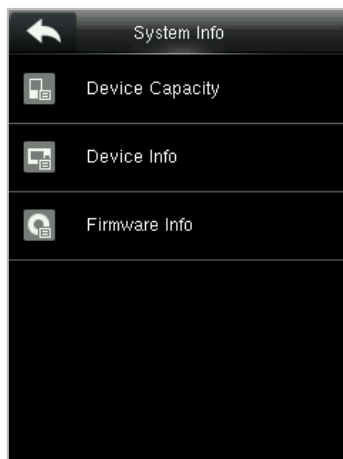


### Function Description

Function Name	Description
<b>Test All</b>	To automatically test whether the LCD, audio, camera and RTC are normal.
<b>Test LCD</b>	To automatically test the display effect of LCD screen by displaying full-color, pure white, and pure black to check whether the screen displays colors normally.
<b>Test Voice</b>	To automatically test whether the audio files stored in the device are complete and the voice quality is good.
<b>Test Face</b>	To test if the camera functions properly by checking the pictures taken to see if they are clear enough.
<b>Test Clock RTC</b>	To test the RTC. The device tests whether the clock works normally and accurately with a stopwatch. Touch the screen to start counting and press it again to stop counting.

## 13 System Information

On the **Main Menu**, click **System Info** to view the storage status, the version information of the device, and firmware information.



### Function Description

Function Name	Description
<b>Device Capacity</b>	Displays the current device's user storage, administrators, password, and face storage, access records, attendance and blocklist photos, and user photos.
<b>Device Info</b>	Displays the device's name, serial number, MAC address, face algorithm, platform information, and manufacturer and manufacture date.
<b>Firmware Info</b>	Displays the firmware version and other version information of the device.

## 14 QR Code as the Mobile Credential

### 14.1 Connect to ZKBioSecurity Software

#### 14.1.1 Set the Communication Address

- **Device side**

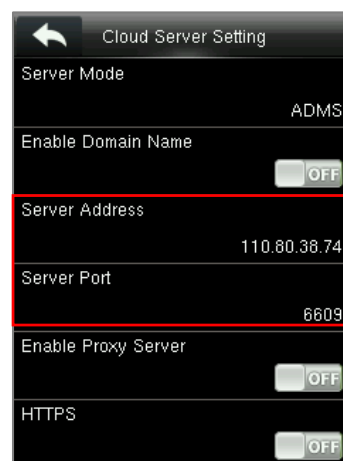
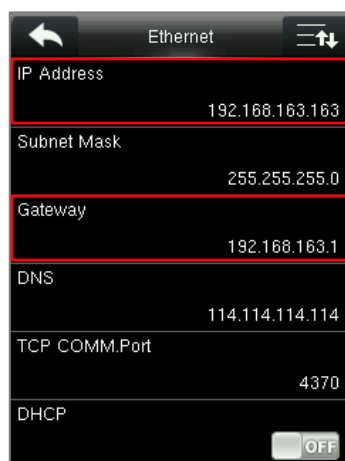
1. Select **COMM.** > **Ethernet** in the main menu to set the IP address and gateway of the device.

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

2. In the main menu, click **COMM.** > **Cloud Server Setting** to set the server address and server port.

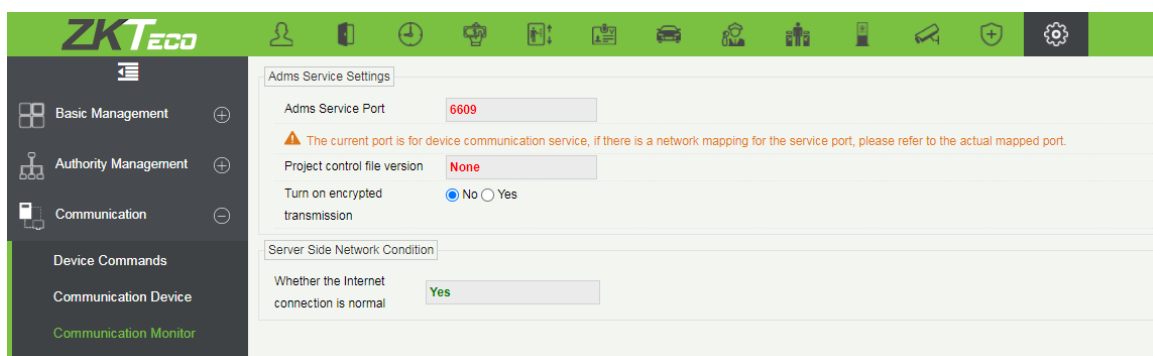
**Server address:** Set the IP address as of ZKBioSecurity server.

**Server Port:** Set as the service port of ZKBioSecurity (the default is 6609).



- **Software side**

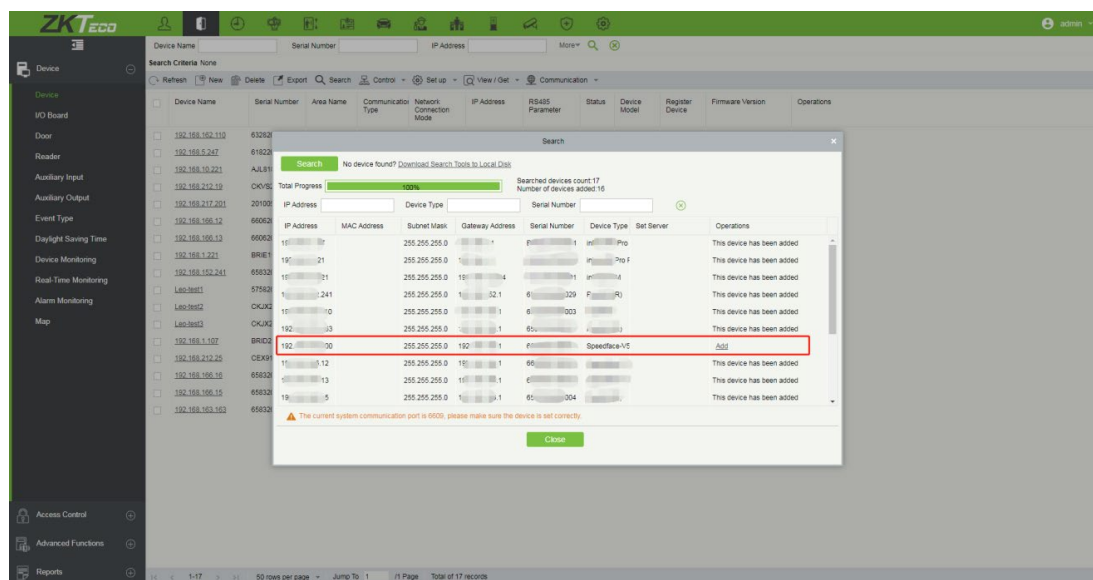
Login to ZKBioSecurity software, click **System** > **Communication** > **Communication Monitor** to set the ADMS Service Port, as shown in the figure below:



## 14.1.2 Add Device on the Software

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

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



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

## 14.1.3 Add Personnel on the Software

1. Click **Personnel > Person > New**:

2. Fill in all the required fields and click **[OK]** to register a new user.
3. Click **Access > Device > Control > Synchronize All Data to Devices** to synchronize all the data to the device including the new users.

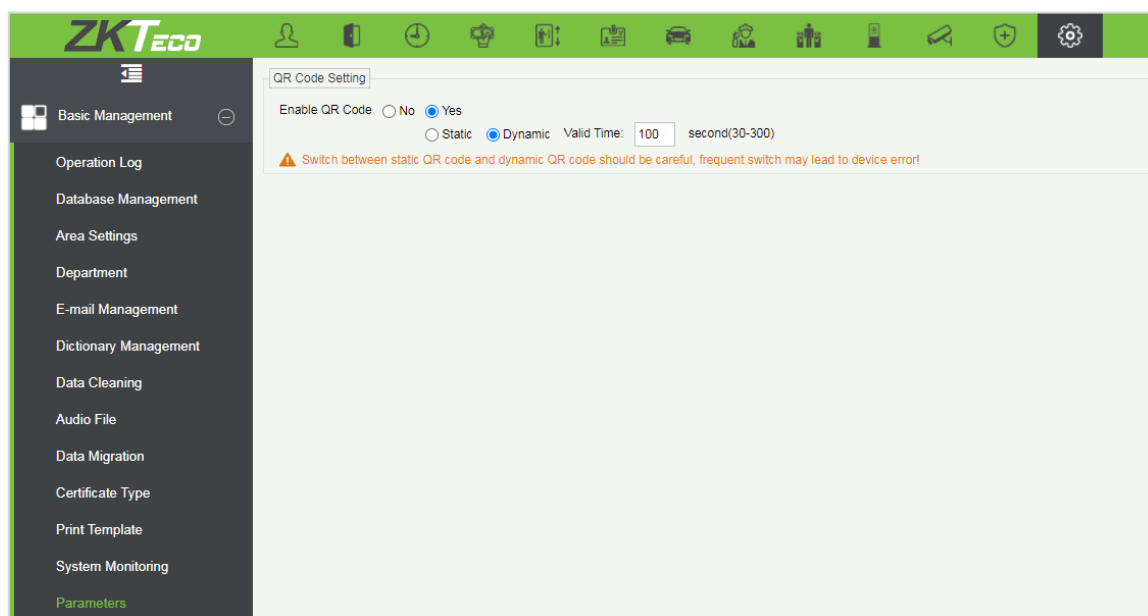
## 14.2 Mobile Credential

The device can recognize the QR code image on the ZKBioSecurity Mobile APP captured by the QR code scanner. Making the QR code as a Mobile Credential, you can check in/out conveniently and achieve contactless access. The steps are given below:

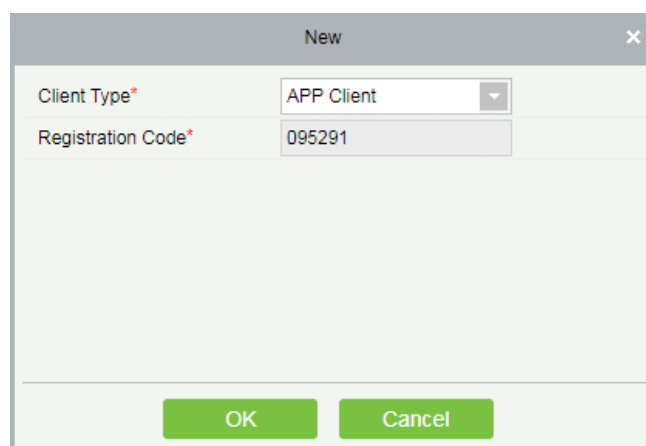
### 14.2.1 Mobile APP Configuration

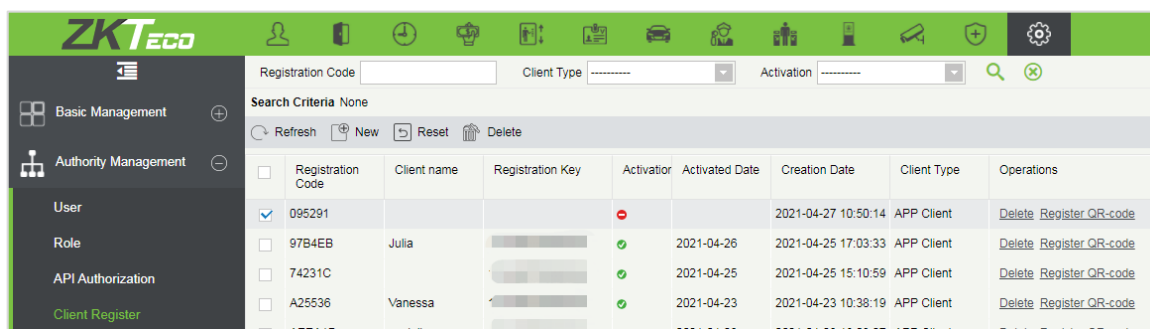
After downloading and installing the App, the user needs to set the Server before login.

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



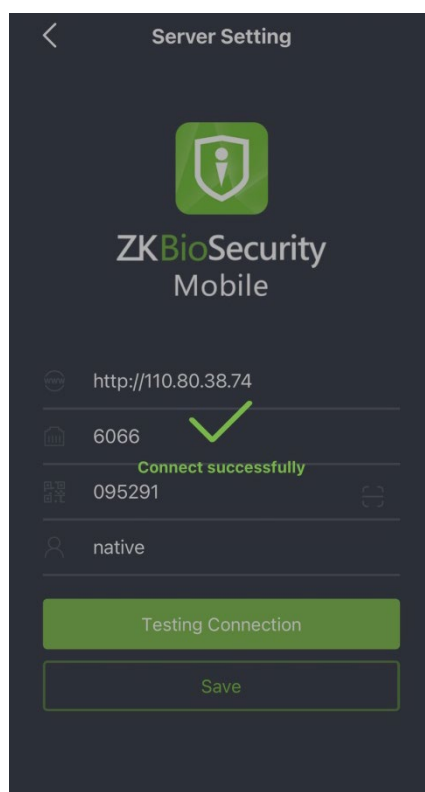
2. On the Server, choose **[System] > [Authority Management] > [Client Register]** to add a registered App client.





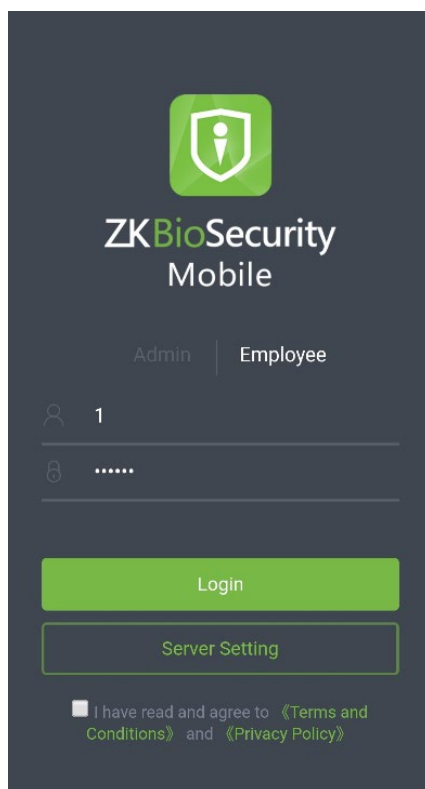
Registration Code	Client name	Registration Key	Activation	Activated Date	Creation Date	Client Type	Operations
095291					2021-04-27 10:50:14	APP Client	Delete Register QR-code
97B4EB	Julia			2021-04-26	2021-04-25 17:03:33	APP Client	Delete Register QR-code
74231C				2021-04-25	2021-04-25 15:10:59	APP Client	Delete Register QR-code
A25536	Vanessa			2021-04-23	2021-04-23 10:38:19	APP Client	Delete Register QR-code
A5EA1D	evak line			2021-04-23	2021-04-23 10:38:19	APP Client	Delete Register QR-code

3. Open the App on the Smartphone. On the login screen, choose [**Server Setting**] and type the IP Address or the Domain Name of the Server, and its Port Number.
4. Select the **QR Code** icon to scan the QR code of the new App client. After the client is identified successfully, set the Client Name and select [**Connection Test**].
5. After the network is connected successfully, select [**Save**].

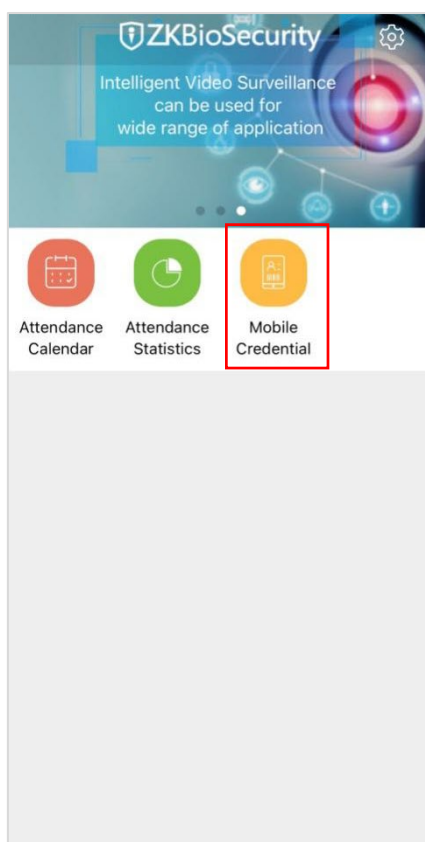


### 14.2.2 Login the Mobile APP

1. The Mobile Credential function is only valid when logging in as an employee, click on Employee to switch to Employee Login screen. Employees can login with the Personnel ID in [**Personnel**] > [**Personnel**] > [**Person**] and self-service password. The default self-service password is **123456**.



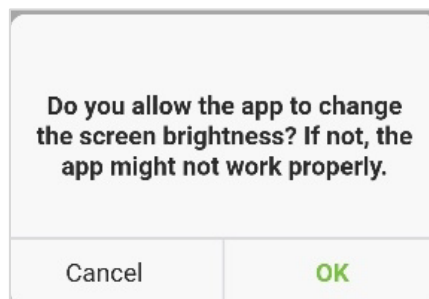
2. After successful login, select [**Mobile Credential**] on the App, and a QR code will appear, which includes employee ID and card number (static QR code only includes card number) information.





**NOTES:**

1. The QR code can replace a physical card on a specific device to achieve contactless authentication to open the door.
2. When using this function for the first time, the App will prompt to authorize the modification of screen brightness settings, as shown in the figure:



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

**14.2.3 Scan the QR Code**

Find the access control QR code on the ZKBioSecurity Mobile App. Align it with the QR code scanner of the device. The device prompts that the verification is successful.

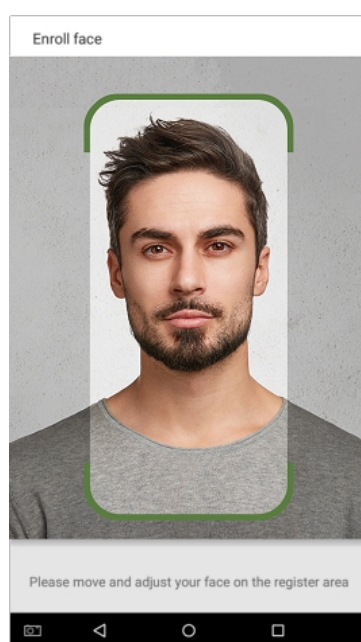


**NOTE:** For other specific operations, please refer to **ZKBioSecurity Mobile App User Manual**.

## **Appendix 1**

### **Requirements of Live Collection and Registration of Visible Light Face Images**

1. It is recommended to perform registration in an indoor environment with an appropriate light source without underexposure or overexposure on the face.
2. Do not place the device towards outdoor light sources like door or window or other harsh light sources.
3. Dark-color apparels other than the background color are recommended for registration.
4. Expose your face and forehead properly and do not cover your face and eyebrows with your hair.
5. It is recommended to show a normal facial expression. (A smile is acceptable, but do not close your eyes, or incline your head to any orientation).
6. Two images are required for persons with eyeglasses, one image with eyeglasses and one other without them.
7. Do not wear accessories like scarf or mask that may cover your mouth or chin.
8. Please face right towards the capturing device and locate your face in the image capturing area as shown in the image below.
9. Do not include more than one face in the capturing area.
10. A distance of 50cm to 80cm is recommended for capturing the image. (the distance is adjustable, subject to body height).



## Requirements for Visible Light Digital Face Image Data

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

- **Eye Distance**

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

- **Facial Expression**

A neutral face or smile with eyes naturally open are recommended.

- **Gesture and Angel**

The horizontal rotating angle should not exceed  $\pm 10^\circ$ , elevation should not exceed  $\pm 10^\circ$ , and depression angle should not exceed  $\pm 10^\circ$ .

- **Accessories**

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

- **Face**

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

- **Image Format**

Should be in BMP, JPG or JPEG.

- **Data Requirement**

Should comply with the following requirements:

1. White background with dark-coloured apparel.
2. 24bit true color mode.
3. JPG format compressed image with not more than 20kb size.
4. Resolution should be between 358 x 441 to 1080 x 1920.
5. The vertical scale of head and body should be in a ratio of 2:1.
6. The photo should include the captured person's shoulders at the same horizontal level.
7. The captured person's eyes should be open and with clearly seen iris.
8. A neutral face or smile is preferred, showing teeth is not preferred.
9. The captured person should be easily visible, natural in color, no harsh shadow or light spot or reflection in the face or background. The contrast and lightness level should be appropriate.

## **Appendix 2**

### **Privacy Policy**

#### **Notice:**

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

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

#### **I. Collected Information**

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

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

#### **II. Product Security and Management**

- 1.** When you use our products for the first time, you shall set the Administrator privilege before performing specific operations. Otherwise, you will be frequently reminded to set the Administrator privilege when you enter the main menu interface. **If you still do not set the Administrator privilege after receiving the system prompt, you should be aware of the possible security risk (for example, the data may be manually modified).**

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

### III. Others

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

## Eco-friendly Operation



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

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

### Hazardous or Toxic substances and their quantities

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

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

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

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

# Green Label

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

Tel: +86 769-82109991

Fax: +86 755-89602394

[www.zkteco.com](http://www.zkteco.com)

