User Manual

2.4-inch Visible Light Terminal

Date: December 2023

Doc Version: 1.0

English

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

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

Trademark

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

Disclaimer

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

The contents of this manual must be read 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 any information contained in this manual or any of the amendments made thereto. ZKTeco does not extend the warranty of any kind, including, without limitation, any warranty of design, merchantability, or fitness for a particular purpose. ZKTeco does not assume responsibility for any errors or omissions in the information or documents which are referenced by or linked to this manual. The entire risk as to the results and performance obtained from using the information is assumed by the user.

ZKTeco in no event shall be liable to the user or any third party for any incidental, consequential, indirect, special, or exemplary damages, including, without limitation, loss of business, loss of profits, business interruption, loss of business information or any pecuniary loss, arising out of, in connection with, or relating to the use of the information contained in or referenced by this manual, even if ZKTeco has been advised of the possibility of such damages.

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

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

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

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

ZKTeco Headquarters

Address ZKTeco Industrial Park, No. 32, Industrial Road,

Tangxia Town, Dongguan, China.

Phone +86 769 - 82109991

Fax +86 755 - 89602394

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

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

About the Company

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

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

About the Manual

This manual introduces the operations of **2.4-inch Visible Light Terminal**.

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

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

Document Conventions

Conventions used in this manual are listed below:

GUI Conventions

For Software	
Convention	**Description**
Bold font	Used to identify software interface names e.g., **OK**, **Confirm**, **Cancel**.
>	Multi-level menus are separated by these brackets. For example, File > Create > Folder.
For Device	
Convention	**Description**
< >	Button or key names for devices. For example, press <OK>.
[ ]	Window names, menu items, data table, and field names are inside square brackets. For example, pop up the [New User] window.
/	Multi-level menus are separated by forwarding slashes. For example, [File/Create/Folder].

Symbols

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

Table of Contents

1 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.

2 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.

3 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:

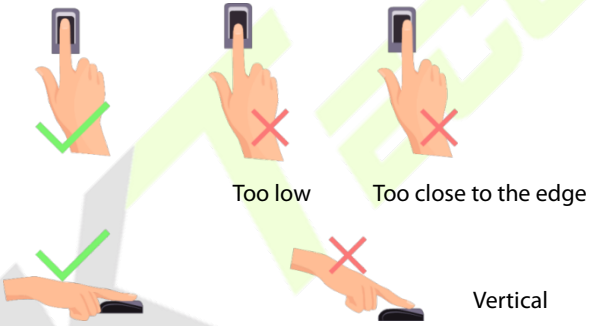
- Make sure whether the positive polarity and negative polarity of the DC 12V power supply is connected correctly. A reverse connection may damage the device. It is not advisable to connect the AC 24V power supply to the DC 12V input port.
- Make sure to connect the wires following the positive polarity 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.

4 Instruction for Use

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

4.1 Finger Positioning★

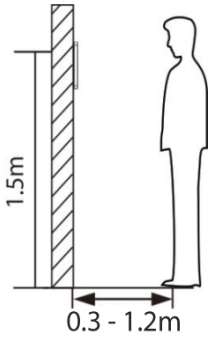
Recommended fingers: Index, middle, or ring fingers; avoid using the thumb or pinky, as they are difficult to accurately press onto the fingerprint reader.



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

4.2 Standing Position, Facial Expression and Standing Posture

- **The recommended distance**



The distance between the device and a user whose height is in a range of 1.55m to 1.85m is recommended to be 0.3 to 1.2m. Users may slightly move forward or backward to improve the character of facial images captured.

- **Recommended standing posture and facial expression**

Facial Expression **Standing Posture**

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

4.3 Registration of Face Template

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

Correct face template registration and authentication method

- **Recommendation for registering a face**
  - When registering a face, maintain a distance of 50cm to 80cm between the device and the face.
  - Be careful to keep your facial expression natural and not to change. (smiling face, drawn face, wink, etc.)
  - If you do not follow the instructions on the screen, the face registration may take longer or may fail.
  - Be careful not to cover the eyes or eyebrows.

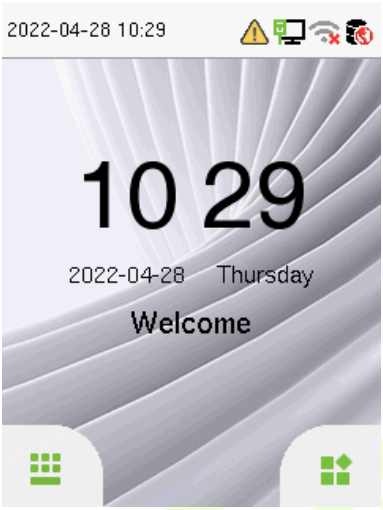
- Do not wear hats, masks, sunglasses or eyeglasses.
- Be careful not to display two faces on the screen. Register one person at a time.
- It is recommended for a user wearing glasses to register both faces with and without glasses.

➢ **Recommendation for authenticating a face**

- Ensure that the face appears inside the guideline displayed on the screen of the device.
- Sometimes, authentication may fail due to the change in the wearing glasses then the one used while registration. In such a case, you may require authenticating your face with the previously worn glasses. If your face was registered without glasses, you should authenticate your face without glasses further.
- If a part of the face is covered with a hat, a mask, an eye patch, or sunglasses, authentication may fail. Do not cover the face, allow the device to recognize both the eyebrows and the face.

4.4 Standby Interface

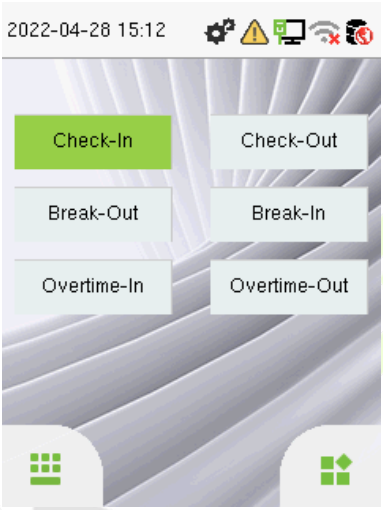
After connecting the power supply, the following standby interface is displayed:



- 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.

- The punch state options can also be displayed and used directly on the standby interface. Tap anywhere on the screen apart from the icons, and six shortcut keys appears on the screen, as shown in the figure below:



- Press the corresponding punch state key to select your current punch state, which is displayed in green. Please refer to "Shortcut Key Mappings" for the specific operation method.

Note: The punch state options are off by default and need to select other mode options in the "Punch State Option" to get the punch state options on the standby screen.

4.5 Virtual Keyboard

Note: The device supports the input in English language, numbers, and symbols.

- Tap **[EN]** to switch to the numeric keyboard.
- Press **[123]** to switch to the symbolic keyboard.
- Tap **[@#&]** to return to the English keyboard.
- Tap [ ] to exit the virtual keyboard.

4.6 Verification Mode

4.6.1 Fingerprint Verification★

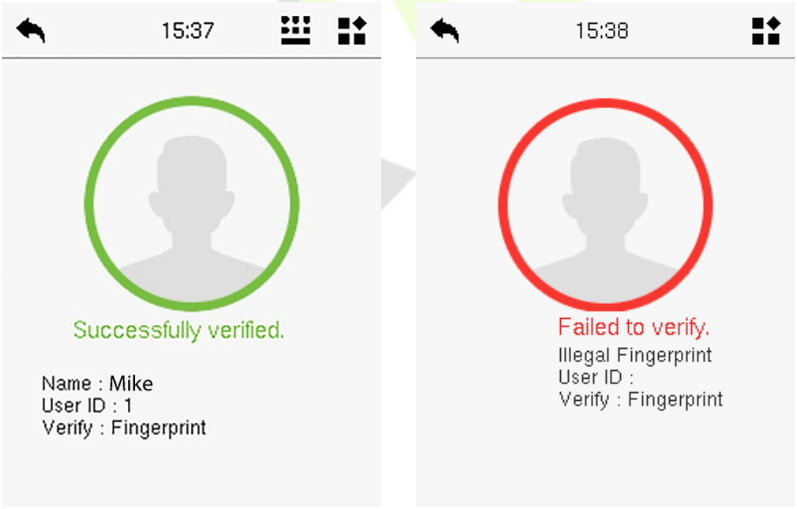
➢ **1:N Fingerprint Verification Mode**

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

The device enters the fingerprint authentication mode when a user presses his/her finger onto the fingerprint scanner.

Please follow the correct way to place your finger onto the sensor. For details, please refer to section Finger Positioning.

Verification is successful: Verification is failed:



➢ **1:1 Fingerprint Verification Mode**

Compares the fingerprint that is being pressed onto the fingerprint reader with the fingerprints that are linked to User ID input via the virtual keyboard.

Users may verify their identities with 1:1 verification mode when they cannot gain access with 1: N authentication method.

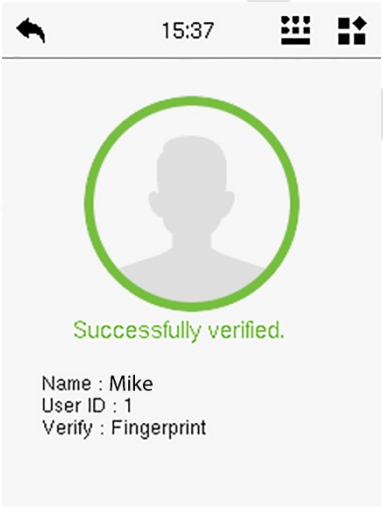
Press on the main interface and enter the 1:1 fingerprint verification mode.

Input the user ID and press [**OK**].

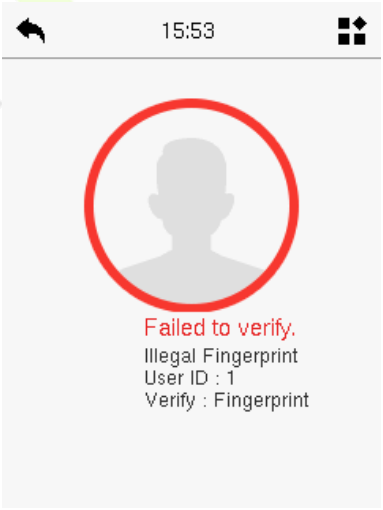
If an employee registers a face template, password and card in addition to the fingerprint, the following screen will appear. Select the icon to enter fingerprint verification mode.

Press the fingerprint to verify.

Verification is successful:



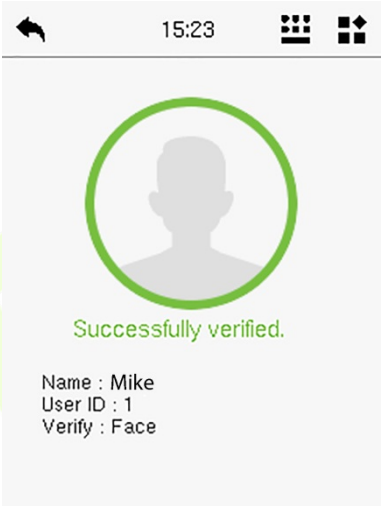
Verification is failed:



4.6.2 Facial Verification

➢ **1:N Facial Verification Mode**

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



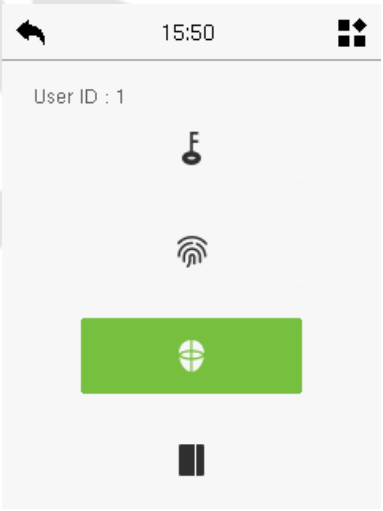
➢ **1:1 Facial Verification Mode**

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

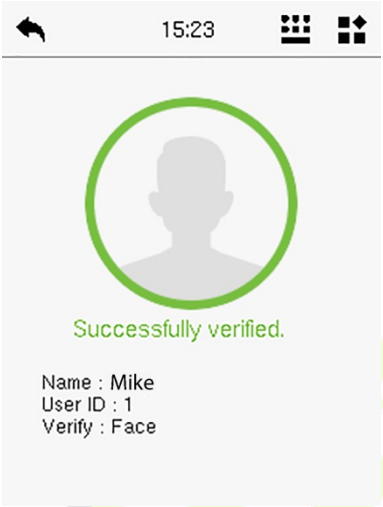
Press on the main interface and enter the 1:1 facial verification mode.

Enter the user ID and click [**OK**].

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



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

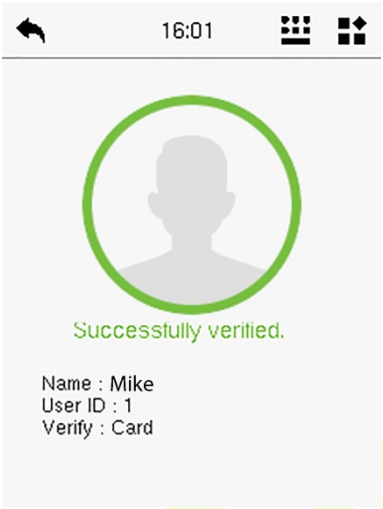


If the verification is failed, it prompts "**Please adjust your position!**".

4.6.3 Card Verification★

- **1: N Card Verification Mode**

The 1: N Card Verification mode compares the card number in the card induction area with all the card number data registered in the device; The following is the card verification screen.



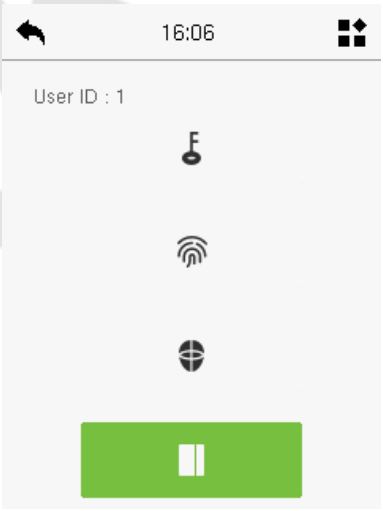
- **1:1 Card Verification Mode**

The 1:1 Card Verification mode compares the card number in the card induction area with the number associated with the employee's User ID registered in the device.

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

Enter the user ID and click [**OK**].

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



4.6.4 QR Code Verification★

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

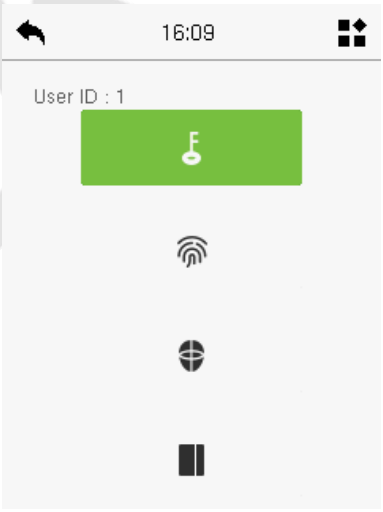
Tap **Mobile Credential** on the ZKBioAccess Mobile Page, and a QR code will appear, which includes employee ID and card number (static QR code only includes card number) information. The QR code can replace a physical card on a specific device to achieve contactless authentication. Please refer to 19.4 Mobile Credential.

4.6.5 Password Verification

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

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

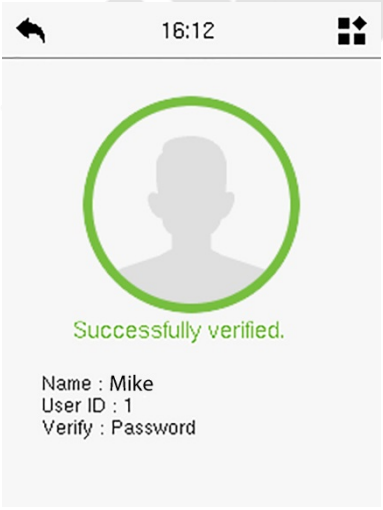
If an employee registers a fingerprint, face template and card in addition to the password, the following screen will appear. Select the icon to enter password verification mode.



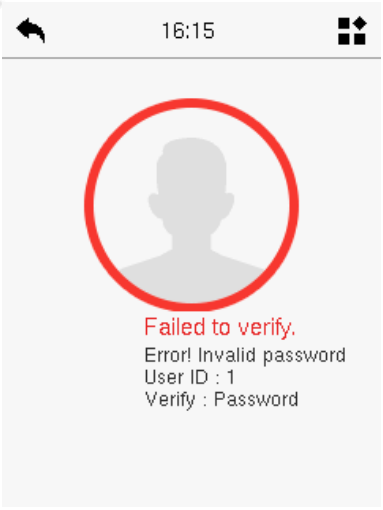
Input the password and press [**OK**].

Below are the display screens after entering a correct password and a wrong password, respectively.

Verification is successful:



Verification is failed:

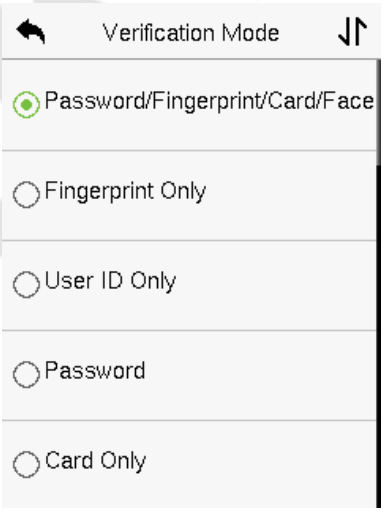


4.6.6 Combined Verification

This device allows you to use a variety of verification methods to increase security. There are a total of 21 distinct verification combinations that can be implemented, as listed below:

Combined Verification Symbol Definition

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



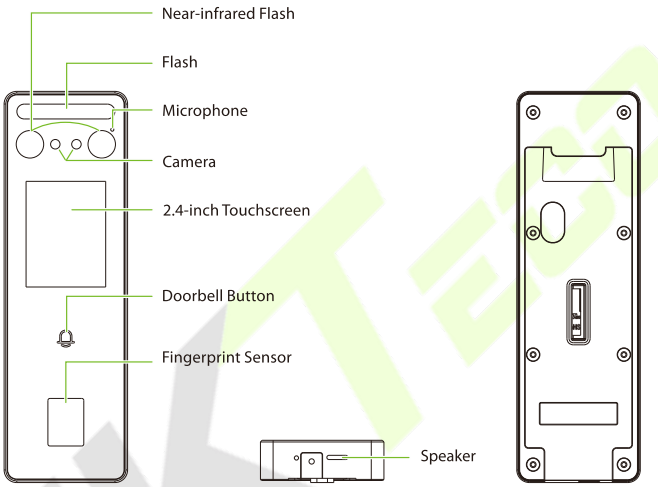
Procedure to set for Combined Verification Mode

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

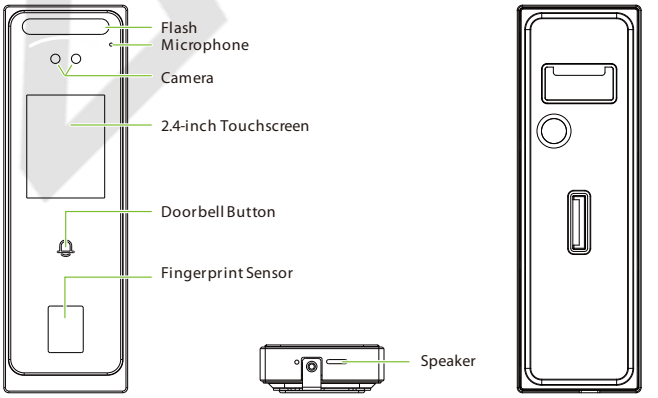
5 Overview

5.1 Appearance

SpeedFace V3L:



SpeedFace V3LM1:



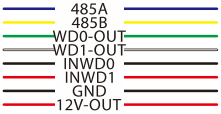
5.2 Connection Cables and Wiring Description

5.2.1 Connection Cables

Pin	Description
6	Power In

Pin	Description
4	Network

Pin	Description
4	USB



Pin	Description	
8	485A	RS485
	485B	

	WD0-OUT	Wiegand Out, Wiegand In
	WD1-OUT	
	INWD0	
	INWD1	
	GND	
	12V-OUT	

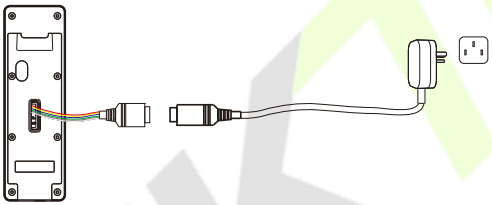
Pin	Description	
12	NC	Lock
	COM	
	NO	
	SEN	Door sensor, Exit Button and Auxiliary In
	GND	
	BUT	
	AUX	
	GND	

	BELL+	Bell
	BELL-	
	ALARM+	Alarm
	ALARM-	

5.2.2 Wiring Description

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

➢ **Power Connection**

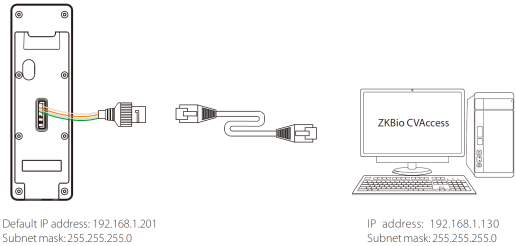


Recommended AC Adapter

1. 12V ± 10%, at least 1500mA.
2. To share the power with other devices, use an AC Adapter with higher current ratings.

➢ **Ethernet Connection**

Connect the device and computer software over an Ethernet cable. As shown in the example below:



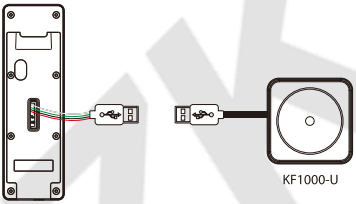
Click on [COMM.] > [Ethernet] > [IP Address], input the IP address and click on [OK].

Note: In LAN, the IP addresses of the server (PC) and the device must be in the same network segment when connecting to the ZKBio CVAccess software.

- **USB Connection**

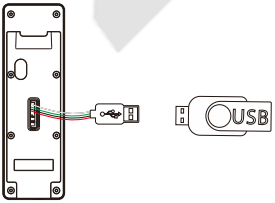
The device supports the connection of KF1000-U reader★ and USB disk.

KF1000-U Reader★:



For more details, please refer to the *KF1000-U User Manual*.

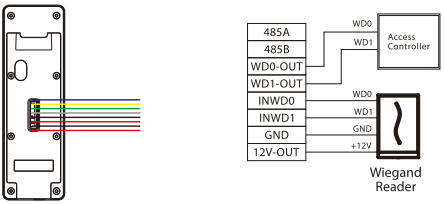
USB Disk:



For more details, please refer to the 15 USB Manager.

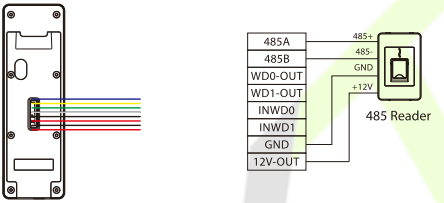
➢ RS485 and Wiegand Connection

RS485:



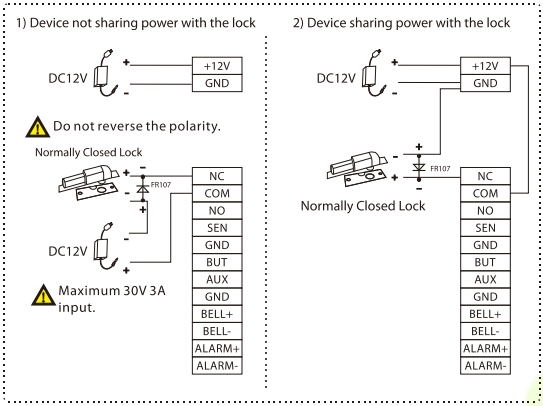
Note: 485A and 485B can be connected to the Barrier gate or the 485 Reader, separately, but cannot be connected to the gate and reader at the same time.

Wiegand:

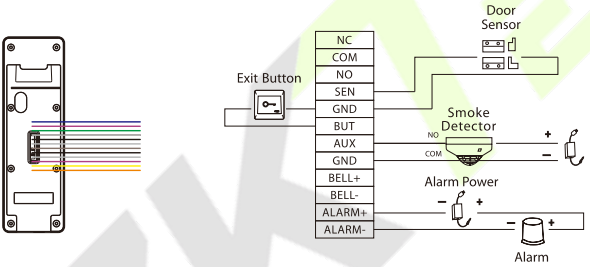


➢ Lock Relay Connection

The system supports Normally Opened Lock and Normally Closed Lock. The NO LOCK (normally unlocked when power-on) is connected with 'NO' and 'COM' terminals, and the NC LOCK (normally locked when power-on) is connected with 'NC' and 'COM' terminals. Take NC Lock as an example below:



➢ Door Sensor, Exit Button, Alarm & Auxiliary Connection



6 Installation

6.1 Installation Environment

Please refer to the following recommendations for installation.


INSTALL INDOORS ONLY

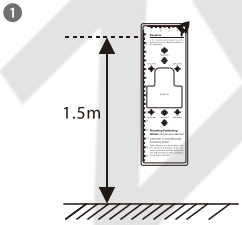

AVOID GLASS REFRACTION

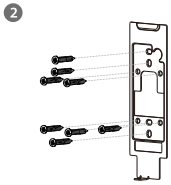

AVOID DIRECT SUNLIGHT AND EXPOSURE

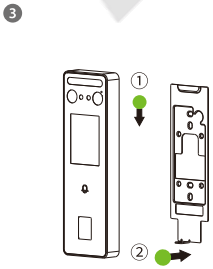

KEEP EFFECTIVE DISTANCE 0.3-1.2m

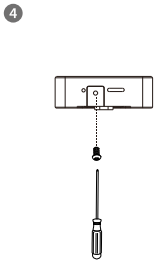
6.2 Device Installation

1. Attach the mounting template sticker to the wall, and drill holes according to the mounting paper.
2. Fix the backplate on the wall using wall mounting screws.
3. Attach the device to the backplate.
4. Fasten the device to the backplate with a security screw.



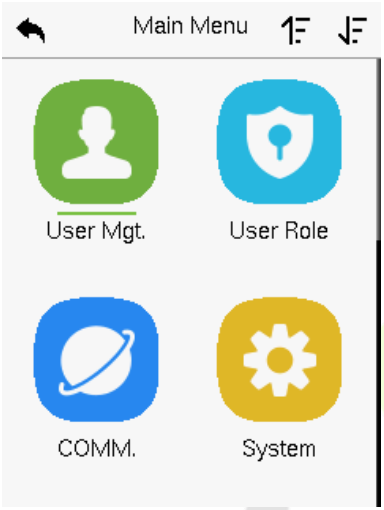


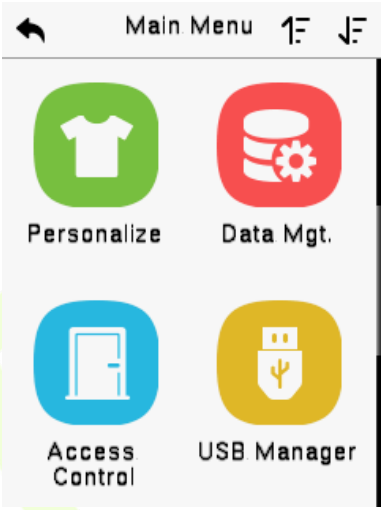


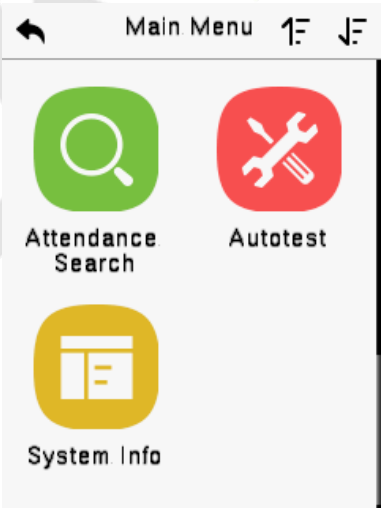


7 Main Menu

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







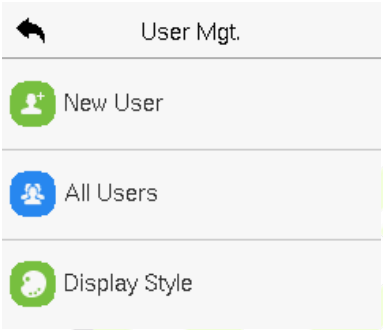
Function Description

Menu	Description
User Mgt.	To Add, Edit, View, and Delete information of a User.
User Role	To set the permission scope of the custom role and enroller for the users, that is, the rights to operate the system.
COMM.	To set the relevant parameters of Network, Serial Comm., PC Connection, Wi-Fi, Cloud Server, Wiegand and Network Diagnosis.
System	To set parameters related to the system, including Date & Time, Access Logs Setting, Face & Fingerprint parameters, Video Intercom parameters, Security Setting and resetting to factory settings.
Personalize	To customize settings of User Interface, Voice, Bell Schedules, Punch State Options and Shortcut Key Mappings settings.
Data Mgt.	To delete all relevant data in the device.
Access Control	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.
USB Manager	To upload or download specific data from a USB drive.
Attendance Search	To query the specified Event logs.
Autotest	To automatically test whether each module functions properly, including the LCD Screen, Audio, Microphone, Fingerprint sensor, Camera, and Real-Time Clock.
System Info	To view Privacy Policy, Data Capacity and Device and Firmware information of the current device.

8 User Management

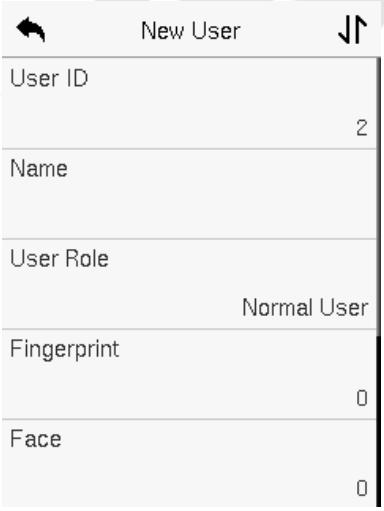
8.1 User Registration

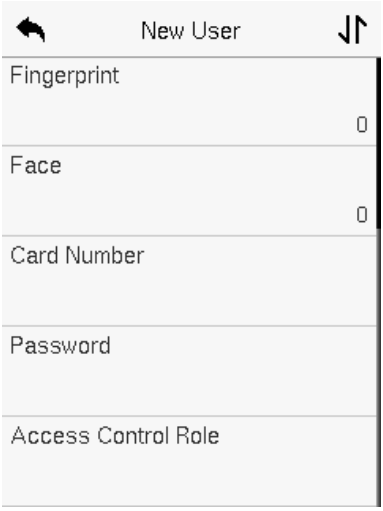
Tap **User Mgt.** on the main menu.



8.1.1 Register a User ID and Name

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





Note:

1) A name can take up to 36 characters.

2) The user ID may contain 1-14 digits by default, support number and alphabetic.

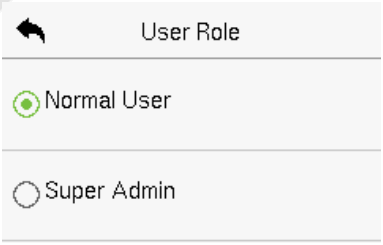
3) During the initial registration, you can modify your ID but not after the registration.

4) If the message "**Duplicated!**" appears, you must choose a different User ID because the one you entered already exists.

8.1.2 User Role

On the New User interface, tap on **User Role** to set the user's duty as either **Normal User or Super Admin**.

- **Super Admin:** The Super Administrator owns all management privileges in the Device.
- **Normal User:** If the Super Admin is registered already in the device, then the Normal Users will not have the privilege to manage the system and can only access authentic verifications.
- **User Defined Roles:** The Normal User can also be assigned custom roles with User Defined Role. The user can be permitted to access several menu options as required.



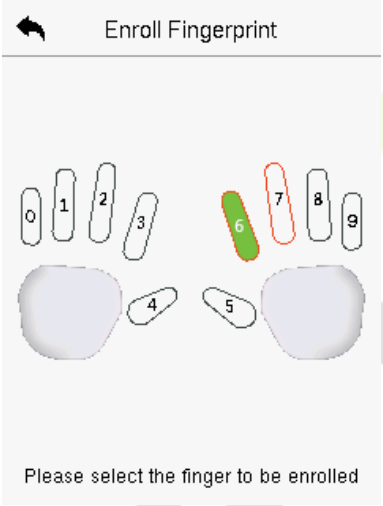
Note: If the selected user role is the Super Admin, then the user must pass the identity authentication to access the main menu. The authentication is based

on the authentication method(s) that the super administrator has registered.

8.1.3 Register Fingerprint★

Tap **Fingerprint** in the **New User** interface to enter the fingerprint registration page.

- Select the finger to be enrolled.
- Press the same finger on the fingerprint reader three times.
- Green indicates that the fingerprint was enrolled successfully.



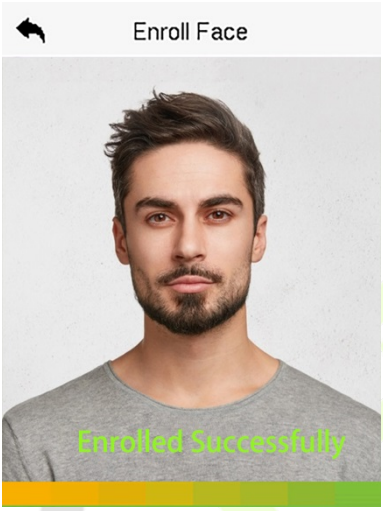
8.1.4 Face

Tap **Face** in the **New User** interface to enter the face registration page.

- Please face towards the camera and place yourself in such a way that your face image fits inside the white guiding box and stays still during face registration.
- A progress bar shows up while registering the face and then "**Enrolled**

Successfully" message is displayed as the progress bar completes.

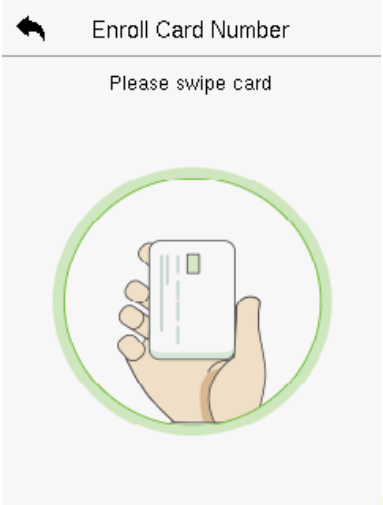
- If the face is registered already then, the "**Duplicated Face**" message shows up. The registration interface is as follows:

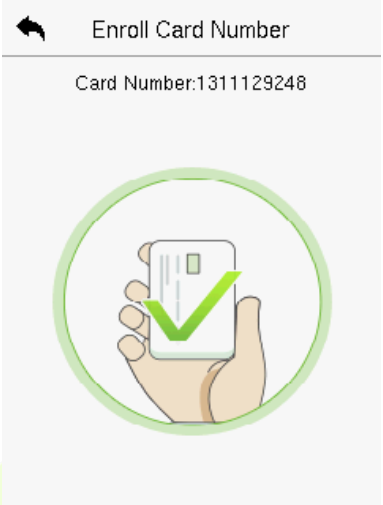


8.1.5 Card★

Tap **Card** in the **New User** interface to enter the card registration page.

- Swipe the card underneath the card reading area on the Card interface. The registration of the card will be successful.
- If the card has already been registered, the message "**Error! Card already enrolled**" appears. The registration interface looks like this:

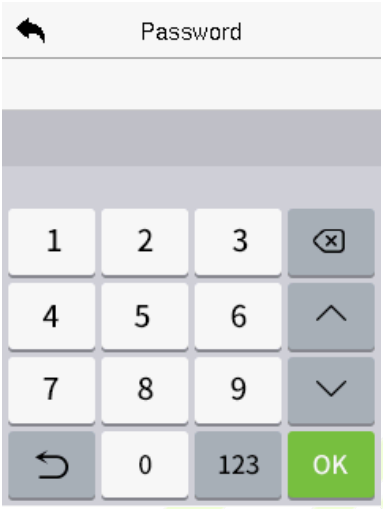




8.1.6 Password

Tap **Password** in the **New User** interface to enter the password registration page.

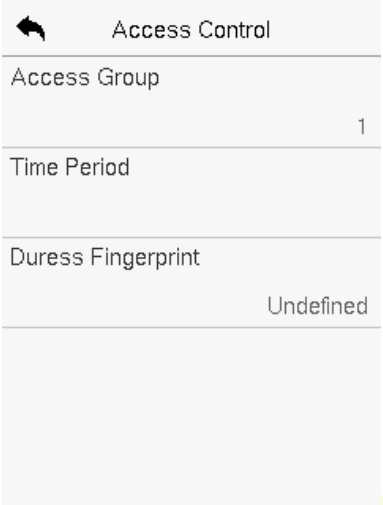
- On the Password interface, enter the required password and re-enter to confirm it and tap **OK**.
- If the re-entered password is different from the initially entered password, then the device prompts the message as "**Password does not match!**", where the user needs to re-confirm the password again.
- The password may contain 6 to 8 digits by default.

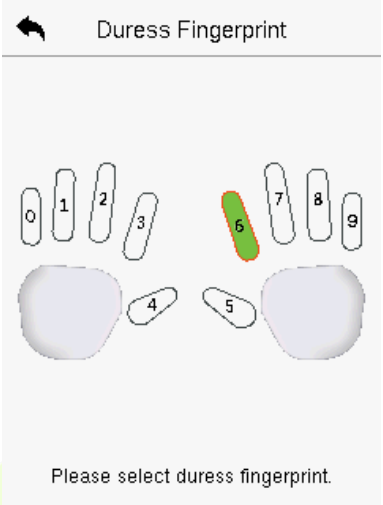


8.1.7 Access Control Role

The **Access Control Role** sets the door access privilege for each user. It includes the access group, verification mode and it facilitates setting the group access time period.

- Tap **Access Control Role** > **Access Group** to 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.
- Tap **Time Period**, to select the time to use.
- The user may specify one or more fingerprints that have been registered as a duress fingerprint(s). When press the finger corresponding to the duress fingerprint on the sensor and pass the verification, the system will immediately generate a duress alarm.

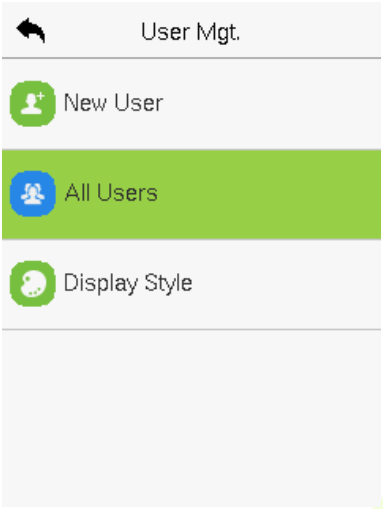




8.2 Search User

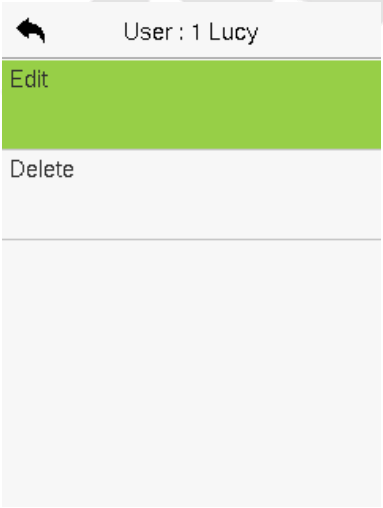
On the **Main Menu**, tap **User Mgt.**, and then tap **All Users** to search a User.

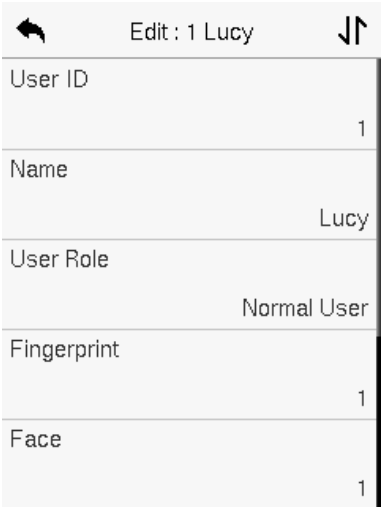
- On the **All-Users** interface, tap on the search bar on the user's list to enter the required retrieval keyword (where the keyword may be the user ID, surname, or full name) and the system will search for the related user information.



8.3 Edit User

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





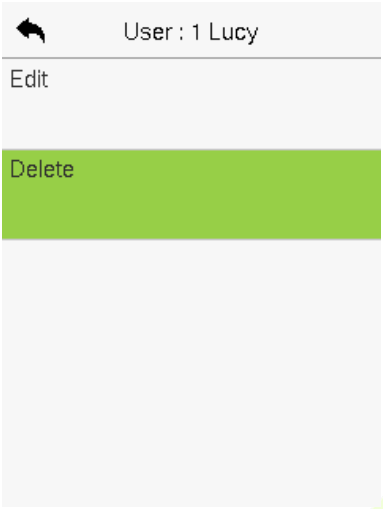
Note: The process of editing the user information is the same as adding a new user, except that the User ID cannot be modified while editing a user. The process in detail refers to "6.1 User Registration".

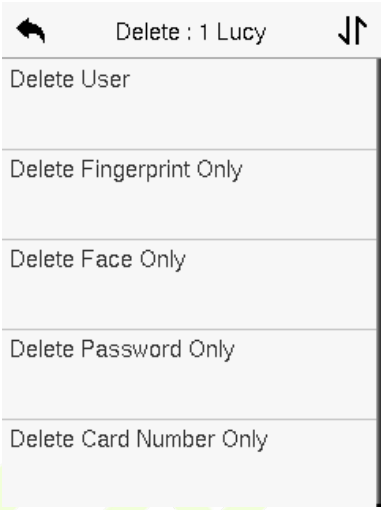
8.4 Delete User

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

Delete Operations

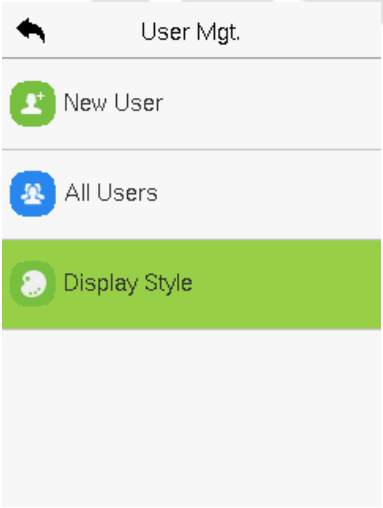
- **Delete User:** Deletes all the user information (deletes the selected User as a whole) from the Device.
- **Delete Fingerprint Only:** Deletes the fingerprint information of the selected user.
- **Delete Face Only:** Deletes the face information of the selected user.
- **Delete Password Only:** Deletes the password information of the selected user.
- **Delete Card Number Only:** Deletes the card information of the selected user.

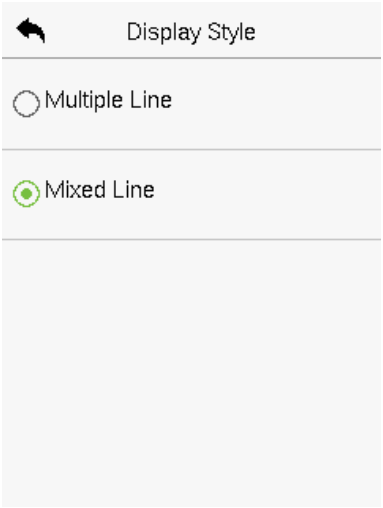




8.5 Display Style

On the **Main Menu**, tap **User Mgt.**, and then tap **Display Style** to enter Display Style setting interface.





All the Display Styles are shown as below:

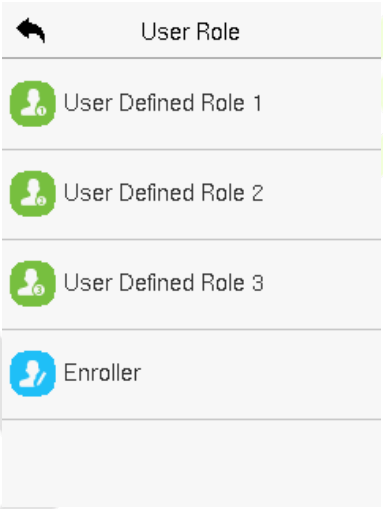
Multiple Line:

Mixed Line:

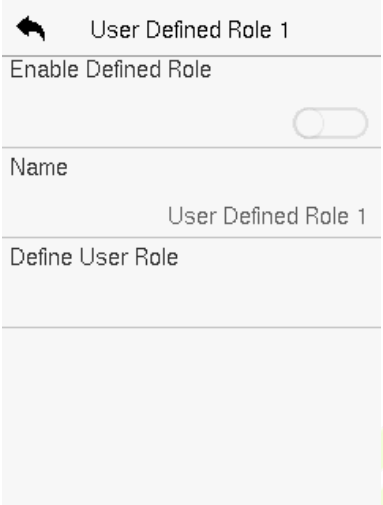
9 User Role

User Role facilitates to assign some specific permissions to certain users, based on the requirement.

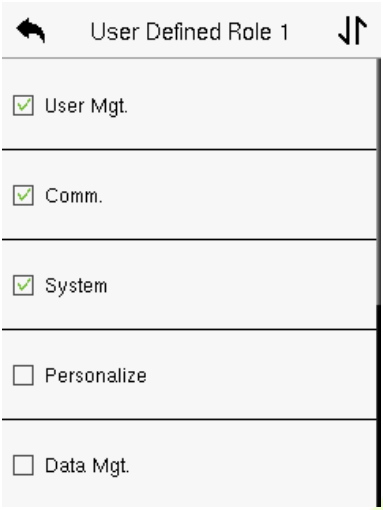
- On the **Main** menu, tap **User Role**, and then tap on the **User Defined Role** to set the user defined permissions.
- The permission scope of the custom role can be set up into 3 roles, that is, the custom operating scope of the menu functions of the user.

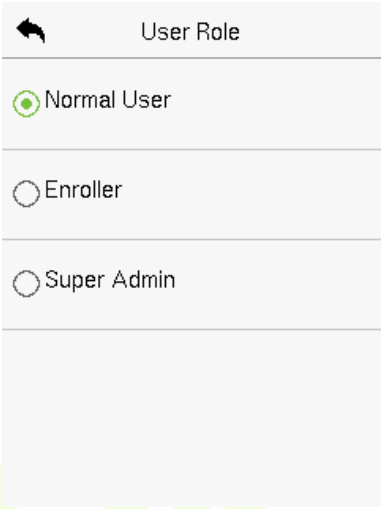


- On the **User Defined Role** interface, toggle **Enable Defined Role** to enable or disable the user defined role.
- Tap on **Name** and enter the custom name of the role.



- Then, by tapping on Define User Role, select the required privileges for the new role, and then press 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 the right.
- First tap on the required **Main Menu** function name, and then select its required sub-menus from the list.



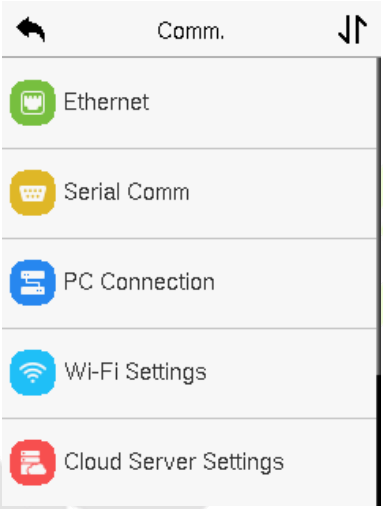


Note: If the User Role is enabled for the Device, tap on **User Mgt. > New User > User Role** to assign the created roles to the required users. But if there is no super administrator registered in the Device, then the device will prompt "**Please enroll super admin first!**" when enabling the User Role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

10 Communication Settings

Communication Settings are used to set the parameters of the Network, Serial Comm, PC Connection, Wi-Fi, Cloud Server, Wiegand, and Network Diagnosis.

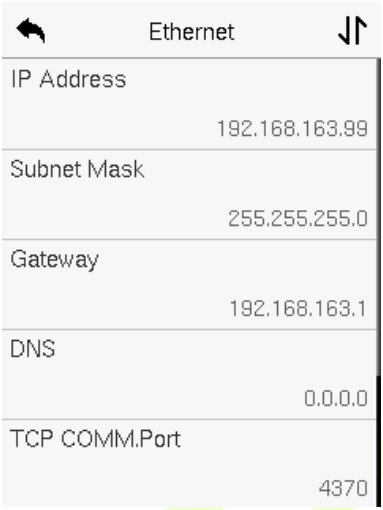
Tap **COMM.** on the main menu.



10.1 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

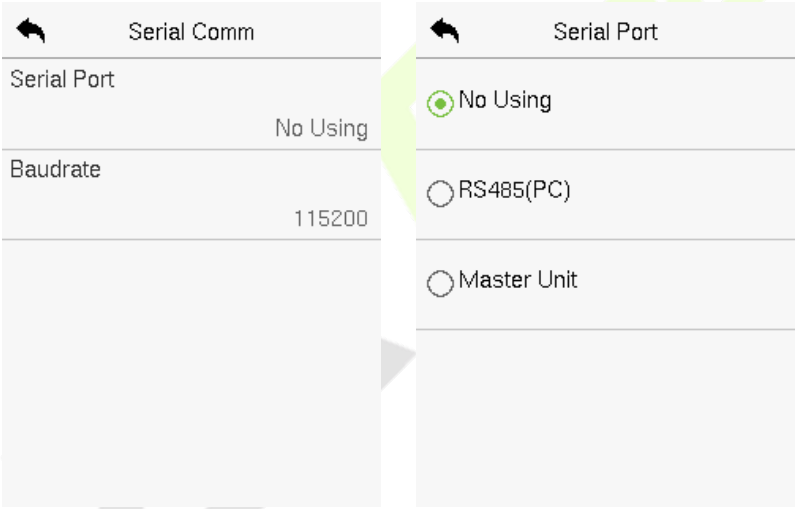
Function Name	Description
IP Address	The default IP address is 192.168.1.201. It can be modified according to the network availability.
Subnet Mask	The default Subnet Mask is 255.255.255.0. It can be modified according to the network availability.
Gateway	The Default Gateway address is 0.0.0.0. It can be modified according to the network availability.
DNS	The default DNS address is 0.0.0.0. It can be modified according to the network availability.
TCP COMM. Port	The default TCP COMM Port value is 4370. It can be modified according to the network availability.
DHCP	Dynamic Host Configuration Protocol dynamically allocates IP addresses for clients via server.

Display in Status Bar	Toggle to set whether to display the network icon on the status bar.

10.2 Serial Comm

Serial Comm function establishes communication with the device through a serial port (RS485/Master Unit).

Tap **Serial Comm.** on the **Comm.** Settings interface.



Function Description

Function Name	Description
Serial Port	**No Using:** No communication with the device through the serial port. **RS485(PC):** Communicate with the device through the RS485 serial port. **Master Unit:** When RS485 is used as the function of "**Master unit**", it can be connected to a card reader.

Baud Rate	There are 4 baud rate options at which the data communicates with PC. They are: 115200 (default), 57600, 38400, and 19200. The higher the baud rate, the faster is the communication speed, but also 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 is more reliable.

10.3 PC Connection

Comm Key facilitates to improve the security of the data by setting up 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.

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

Function Description

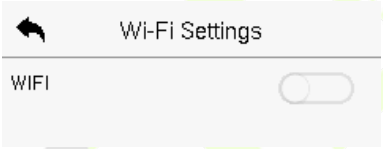
Function Name	Description
Comm Key	The default password is 0 and can be changed. The Comm Key can contain 1-6 digits.
Baud Rate	It is the identification number of the device, which ranges between 1 and 254. If the communication method is RS485, you need to input this device ID in the software communication interface.

10.4 Wi-Fi Settings

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

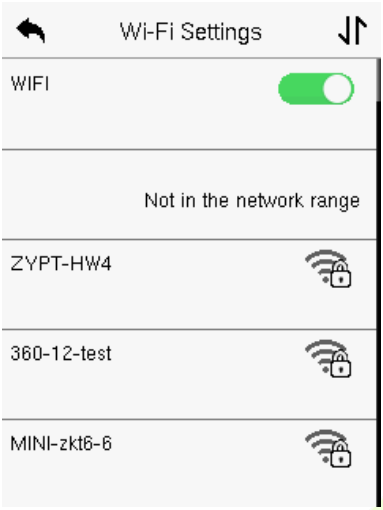
The Wi-Fi module enables data transmission via Wi-Fi (Wireless Fidelity) and establishes a wireless network environment. Wi-Fi is enabled by default in the device. If you don't need to use the Wi-Fi network, you can toggle the Wi-Fi to disable the button.

Tap **Wi-Fi Settings** on the **Comm.** Settings interface to configure the Wi-Fi settings.

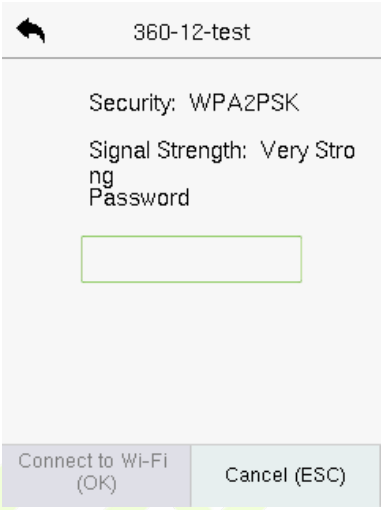


➢ **Searching the Wi-Fi Network**

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



WIFI Enabled: Tap on the required network from the searched network list.

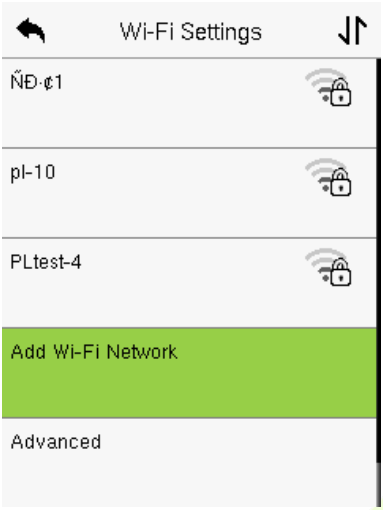


Tap on the password field to enter the password and tap on **Connect to Wi-Fi (OK).**

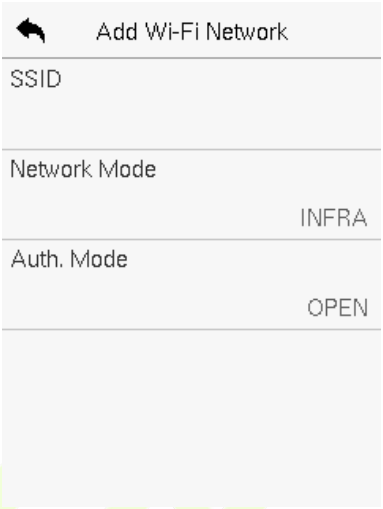
- When the WIFI is connected successfully, the initial interface will display the Wi-Fi logo.

➢ **Adding Wi-Fi Network Manually**

The Wi-Fi can also be added manually if the required Wi-Fi does not show on the list.



Tap on **Add Wi-Fi Network** to add the Wi-Fi manually.

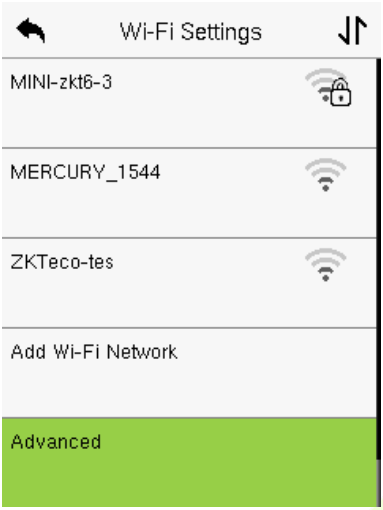


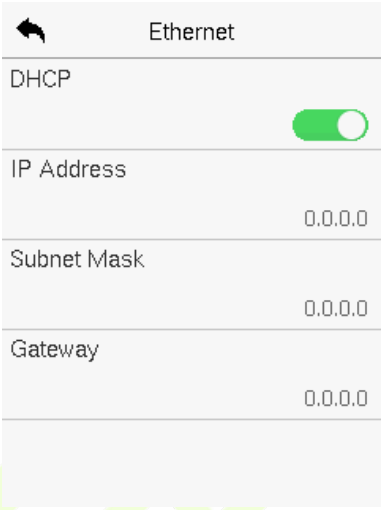
On this interface, enter the Wi-Fi network parameters. (The added network must exist.)

Note: After successfully adding the WIFI manually, follow the same process to search for the added Wi-Fi name.

- **Advanced Setting**

On the **Wi-Fi Settings** interface, tap on **Advanced** to set the relevant parameters as required.



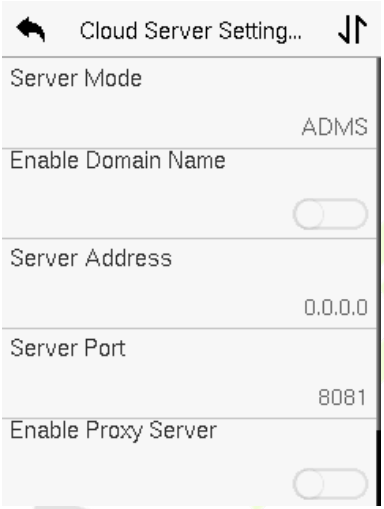


Function Description

Function Name	Description
DHCP	Dynamic Host Configuration Protocol (DHCP) dynamically allocates IP addresses to network clients. If the DHCP is enabled, then the IP cannot be set manually.
IP Address	The IP address for the Wi-Fi network, the default is 0.0.0.0. It can be modified according to the network availability.
Subnet Mask	The default Subnet Mask of the Wi-Fi network is 255.255.255.0. It can be modified according to the network availability.
Gateway	The Default Gateway address is 0.0.0.0. It can be modified according to the network availability.

10.5 Cloud Server Setting

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



Function Description

Function Name		Description
Enable Domain Name	**Server Address**	Once this mode is turned ON, the domain name mode "http://... " will be used, such as http://www.XYZ.com, while "XYZ" denotes the domain name.
Disable Domain Name	**Server Address**	The IP address of the ADMS server.
	Server Port	Port used by the ADMS server.
Enable Proxy Server		The IP address and the port number of the proxy server is set manually when the proxy is enabled.

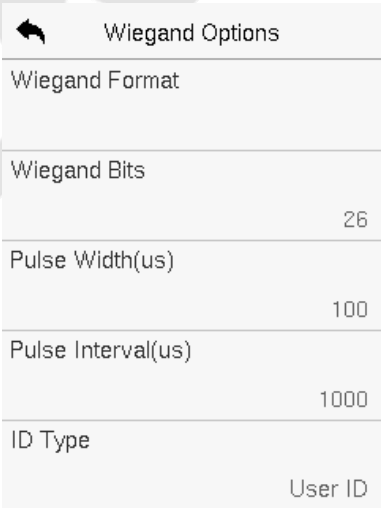
HTTPS	Based on HTTP, transmission encryption and identity authentication ensures the security of the transmission process.

10.6 Wiegand Setup

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

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

10.6.1 Wiegand Input



Function Description

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

Various Common Wiegand Format Description:

Wiegand Format	Description
Wiegand26	ECCCCCCCCCCCCCCCCCCCCCCCCO It consists of 26 bits of binary code. The 1st bit is the even parity bit of the 2nd to 13th bits, while the 26th bit is the odd parity bit of the 14th to 25th bits. The 2nd to 25th bits are the card numbers.

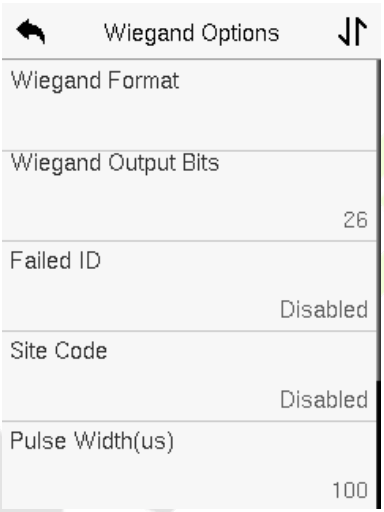
Wiegand26a	ESSSSSSSSCCCCCCCCCCCCCCCO It consists of 26 bits of binary code. The 1st bit is the even parity bit of the 2nd to 13th bits, while the 26th bit is the odd parity bit of the 14th to 25th bits. The 2nd to 9th bits is the site codes, while the 10th to 25th bits are the card numbers.
Wiegand34	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO It consists of 34 bits of binary code. The 1st bit is the even parity bit of the 2nd to 17th bits, while the 34th bit is the odd parity bit of the 18th to 33rd bits. The 2nd to 25th bits are the card numbers.
Wiegand34a	ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCO It consists of 34 bits of binary code. The 1st bit is the even parity bit of the 2nd to 17th bits, while the 34th bit is the odd parity bit of the 18th to 33rd bits. The 2nd to 9th bits is the site codes, while the 10th to 25th bits are the card numbers.
Wiegand36	OFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME It consists of 36 bits of binary code. The 1st bit is the odd parity bit of the 2nd to 18th bits, while the 36th bit is the even parity bit of the 19th to 35th bits. The 2nd to 17th bits is the device codes. The 18th to 33rd bits is the card numbers, and the 34th to 35th bits are the manufacturer codes.

Wiegand36a	EFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCO It consists of 36 bits of binary code. The 1st bit is the even parity bit of the 2nd to 18th bits, while the 36th bit is the odd parity bit of the 19th to 35th bits. The 2nd to 19th bits is the device codes, and the 20th to 35th bits are the card numbers.
Wiegand37	OMMMMSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCE It consists of 37 bits of binary code. The 1st bit is the odd parity bit of the 2nd to 18th bits, while the 37th bit is the even parity bit of the 19th to 36th bits. The 2nd to 4th bits is the manufacturer codes. The 5th to 16th bits is the site codes, and the 21st to 36th bits are the card numbers.
Wiegand37a	EMMMFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCCO It consists of 37 bits of binary code. The 1st bit is the even parity bit of the 2nd to 18th bits, while the 37th bit is the odd parity bit of the 19th to 36th bits. The 2nd to 4th bits is the manufacturer codes. The 5th to 14th bits is the device codes, and15th to 20th bits are the site codes, and the 21st to 36th bits are the card numbers.
Wiegand50	ESSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO It consists of 50 bits of binary code. The 1st bit is the even parity bit of the 2nd to 25th bits, while the 50th bit is the odd parity bit of the 26th to 49th bits. The 2nd to 17th bits is the site codes, and the 18th to 49th bits are the card numbers.

"C" denotes the card number; **"E"** denotes the even parity bit; **"O"** denotes the odd parity bit.

"F" denotes the facility code; **"M"** denotes the manufacturer code; **"P"** denotes the parity bit; and **"S"** denotes the site code.

10.6.2 Wiegand Output



Function Description

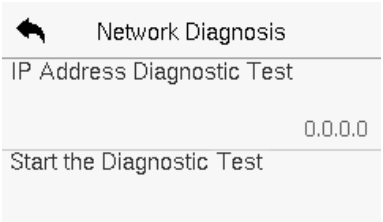
Function Name	Description
Wiegand Format	Its value can be 26 bits, 34 bits, 36 bits, 37 bits, and 50 bits.
Wiegand Output Bits	After selecting the required Wiegand format, select the corresponding output bit digits from the Wiegand format.

Failed ID	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.
Site Code	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.
Pulse Width(us)	The time width represents the changes in the quantity of electric charge with regular high-frequency capacitance within a specified time.
Pulse Interval(us)	The time interval between pulses.
ID Type	Select the ID types as either User ID or card number.

10.7 Network Diagnosis

It helps to set the network diagnosis parameters.

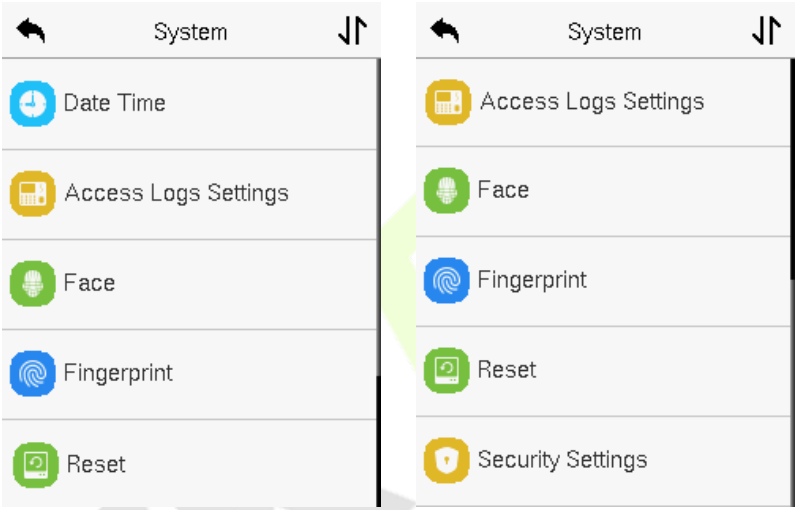
Tap **Network Diagnosis** on the **Comm.** Settings interface. Enter the IP address that needs to be diagnosed and tap **Start the Diagnostic Test** to check whether the network can connect to the device.



11 System Settings

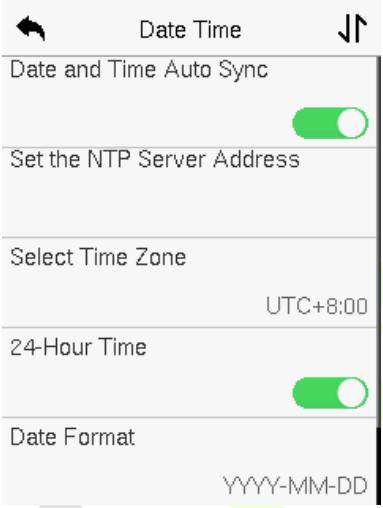
It helps to set related system parameters to optimize the accessibility of the device.

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

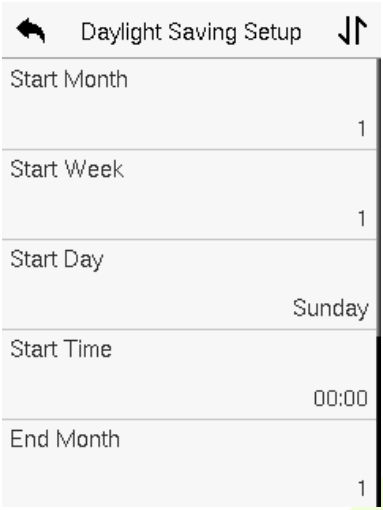


11.1 Date and Time

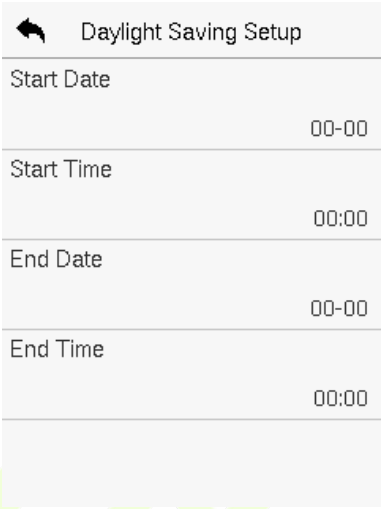
Tap **Date Time** on the **System** interface to set the date and time.



- Tap **Date and Time Auto Sync** to enable automatic time synchronization based on the service address you enter.
- Tap **Manual Date and Time** to manually set the date and time and then tap to **Confirm** and save.
- Tap **Select Time Zone** to manually select the time zone where the device is located.
- Enable or disable this format by tapping 24-Hour Time. If enabled, then select the **Date Format** to set the date.
- 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



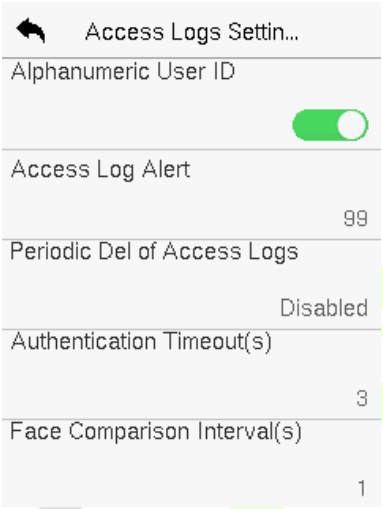
Date Mode

- 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, 2020) to 18:30 on January 1, 2021. After restoring the factory settings, the time of the device will remain at 18:30 on January 1, 2021.

11.2 Access Logs Setting

Tap **Access Logs Settings** on the **System** interface.



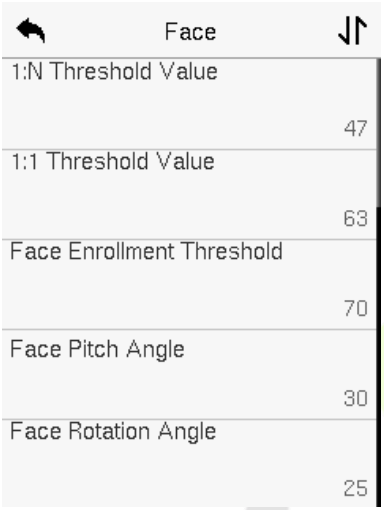
Function Description

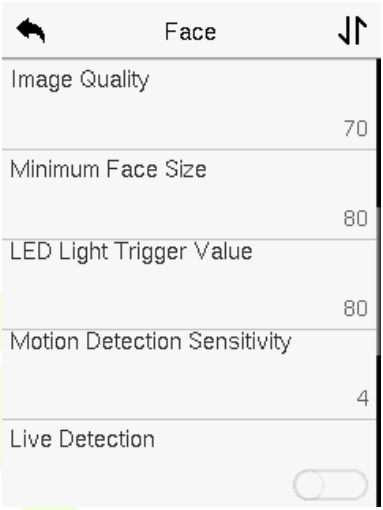
Function Name	Description
Alphanumeric User ID	Enable/Disable the alphanumeric as User ID.
Access Log Alert	When the record space of the attendance access reaches the maximum threshold value, the device automatically displays the memory space warning. Users may disable the function or set a valid value between 1 and 9999.

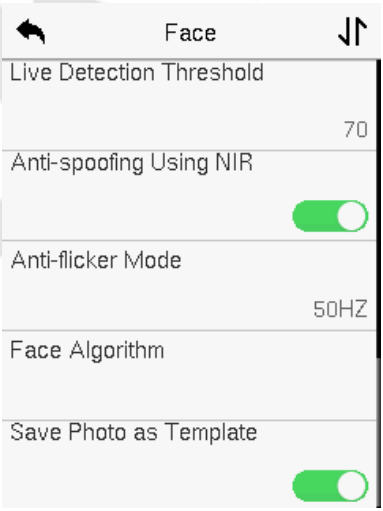
Periodic Del of Access Logs	When access logs reach its maximum capacity, the device automatically deletes a set of old access logs. Users may disable the function or set a valid value between 1 and 999.
Authentication Timeout(s)	The amount of time taken to display a successful verification message. Valid value: 1 to 9 seconds.
Face comparison Interval(s)	After the interval identifying is clicked (selected), for example, if the comparison interval is set to 5 seconds, then the face recognition will verify the face every 5 seconds. Valid value: 0 to 9 seconds. 0 means continuous identifying, 1 to 9 means identifying at intervals.

11.3 Face Parameters

Tap **Face** on the **System** interface to go to the Face parameter settings.







Function Description

Function Name	Description
1:N Threshold Value	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 0 to 100. 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 47.
1:1 Threshold Value	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 0to 100. 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 63.
Face Enrollment Threshold	During face enrollment, 1:N comparison is used to determine whether the user has already registered before. When the similarity between the acquired facial image and all registered facial templates is greater than the set threshold, it indicates that the face has already been registered.
Face Pitch Angle	It is the pitch angle tolerance of a face for facial

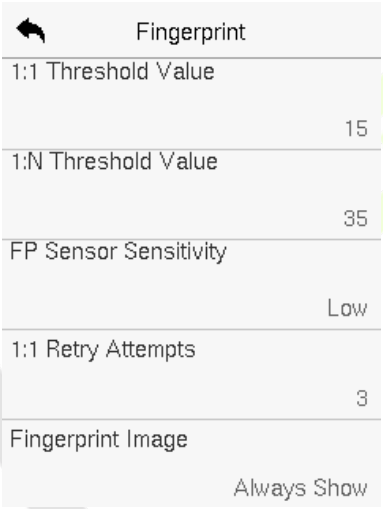
	template registration and comparison. If a face's pitch angle exceeds the set value, it will be filtered by the algorithm, i.e., ignored by the terminal thus no registration and comparison interface will be triggered.
Face Rotation Angle	It is the rotation angle tolerance of a face for facial template registration and comparison. If a face's rotation angle exceeds the set value, it will be filtered by the algorithm, i.e., ignored by the terminal thus no registration and comparison interface will be triggered.
Image Quality	It is the image quality for facial registration and comparison. The higher the value, the clearer image is required.
Minimum Face Size	It sets the minimum face size required for facial registration and comparison. If the minimum size of the captured image is smaller than the set value, then it will be filtered off and not recognized as a face. This value can also be interpreted as the face comparison distance. The farther the individual is, the smaller the face, and the smaller number of pixels of the face obtained by the algorithm. Therefore, adjusting this parameter can adjust the farthest comparison distance of faces. When the value is 0, the face comparison distance is not limited.

LED Light Trigger Threshold	This value controls the turning on and off of the LED light. The larger the value, the LED light will turn on or off more frequently.
Motion Detection Sensitivity	It sets the value for the amount of change in a camera's field of view known as potential motion detection that wakes up the terminal from standby to the comparison interface. The larger the value, the more sensitive the system would be, i.e., if a larger value is set, the comparison interface activates with much ease, and the motion detection is frequently triggered.
Live Detection	It detects the spoof attempt using visible light images to determine if the provided biometric source sample is of a real person (a live human being) or a false representation.
Live Detection Threshold	It facilitates judging whether the captured visible image is a real person (a live human being). The larger the value, the better the anti-spoofing performance using visible light.
Anti-spoofing Using NIR	Using near-infrared spectra imaging to identify and prevent fake photos and videos attack.
Anti-flicker Mode	It is used when WDR is turned off. It helps to reduce flicker when the device's screen flashes at the same frequency as the light.
Face algorithm	It has facial algorithm related information and pause the facial template update.

Save Photo as Template	After disable this function, face re-registration is required after an algorithm upgrade.

11.4 Fingerprint★

Tap **Fingerprint** on the **System** interface to go to the Fingerprint parameter settings.



Function Description

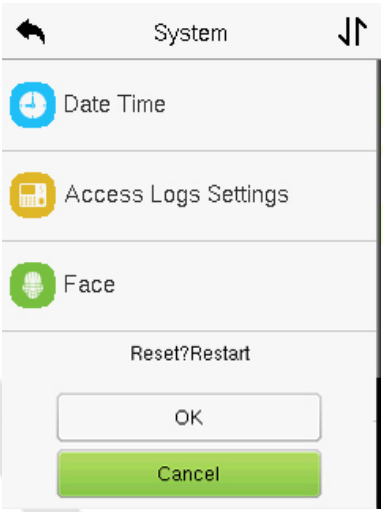
Function Name	Description
1:1 Threshold Value	Under 1:1 verification method, the verification will only be successful when the similarity between the acquired fingerprint data and the fingerprint template associated with the entered user ID enrolled in the device is greater than the set value.

1:N Threshold Value	Under 1:N verification method, the verification will only be successful when the similarity between the acquired fingerprint data and the fingerprint templates enrolled in the device is greater than the set value.
FP Sensor Sensitivity	To set the sensibility of fingerprint acquisition. It is recommended to use the default level "**Medium**". When the environment is dry, resulting in slow fingerprint detection, you can set the level to "**High**" to raise the sensibility; when the environment is humid, making it hard to identify the fingerprint, you can set the level to "**Low**".
1:1 Retry Times	In 1:1 Verification, users might forget the registered fingerprint, or press the finger improperly. To reduce the process of re-entering user ID, retry is allowed.
Fingerprint Image	To set whether to display the fingerprint image on the screen during fingerprint enrollment or verification. Four choices are available: **Show for Enroll:** to display the fingerprint image on the screen only during enrollment. **Show for Match:** to display the fingerprint image on the screen only during verification. **Always Show:** to display the fingerprint image on screen during enrollment and verification. **None:** not to display the fingerprint image.

11.5 Factory Reset

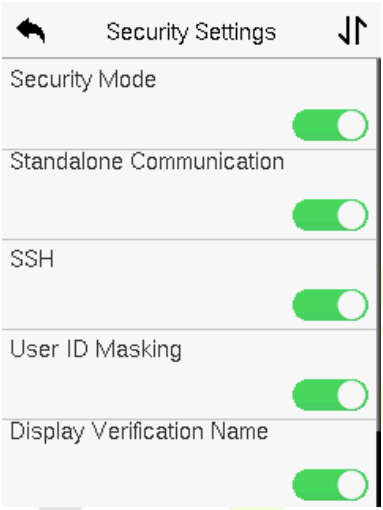
The Factory Reset function restores the device settings such as communication settings and system settings, to the default factory settings (this function does not clear registered user data).

Tap **Reset** on the **System** interface and then tap **OK** to restore the default factory settings.



11.6 Security Settings

Tap **Security Settings** on the **System** interface to go to the Security settings.



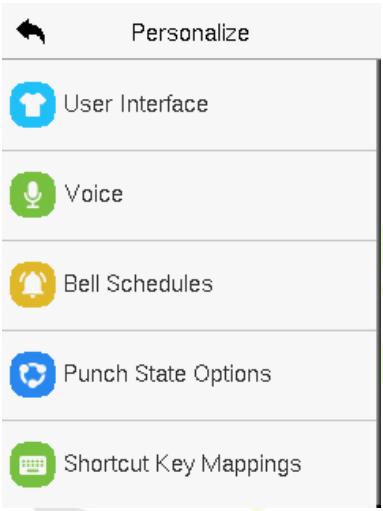
Function Description

Function Name	Description
Security Mode	Select whether to enable the security mode to protect the device and the user's personal information. You can set the device to work offline and hide the user's personal information to prevent leakage during user verification.
Standalone Communication	To avoid being unable to use when the device is offline, you can download the C/S software (such as ZKAccess 3.5) on your computer in advance for offline use.

SSH	SSH is used to enter the background of the device for maintenance.
User ID Masking	When enabled, and then the user is successfully compared and verified, the User ID in the displayed verification result will be replaced with an * to achieve secure protection of sensitive private data.
Display Verification Name	Set whether to display the username in the verification result interface.
Display Verification Mode	Set whether to display the verification mode in the verification result interface.

12 Personalize Settings

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



12.1 Interface Settings

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

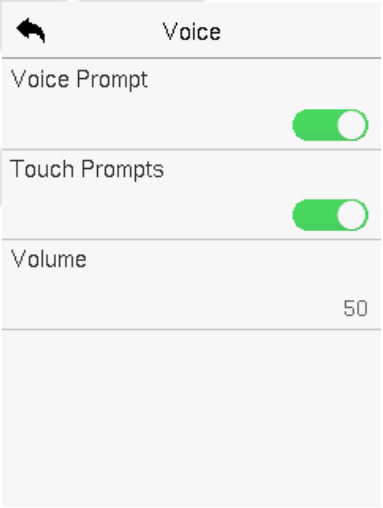
Function Description

Function Name	Description
Wallpaper	It helps to select the main screen wallpaper according to the user preference.
Language	It helps to select the language of the device.
Menu Screen Timeout (s)	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.
Idle Time to Slide Show (s)	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.

Slide Show Interval (s)	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.
Idle Time to Sleep (m)	If the sleep mode is activated, and when there is no operation in the device, then the device will enter standby mode. This function can be disabled or set a value within 1-999 minutes.
Main Screen Style	The style of the main screen can be selected according to the user preference.

12.2 Voice Settings

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

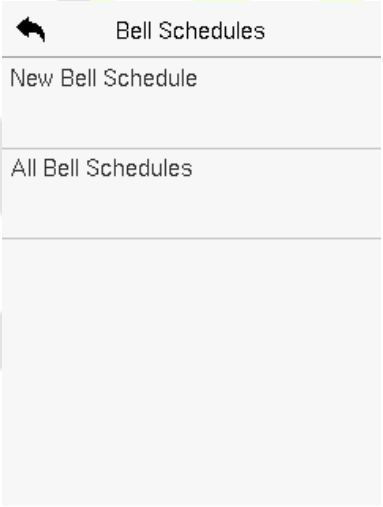


Function Description

Function Name	Description
Voice Prompt	Toggle to enable or disable the voice prompts during function operations.
Touch Prompt	Toggle to enable or disable the keypad sounds.
Volume	Adjust the volume of the device which can be set between 0-100.

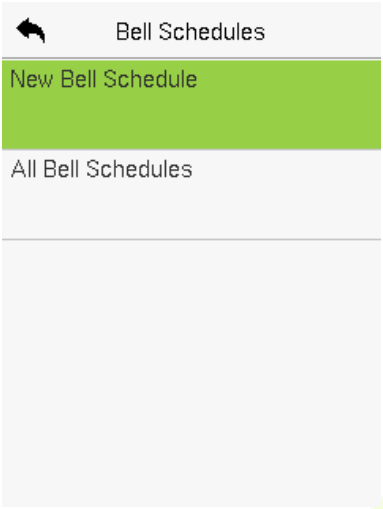
12.3 Bell Schedules

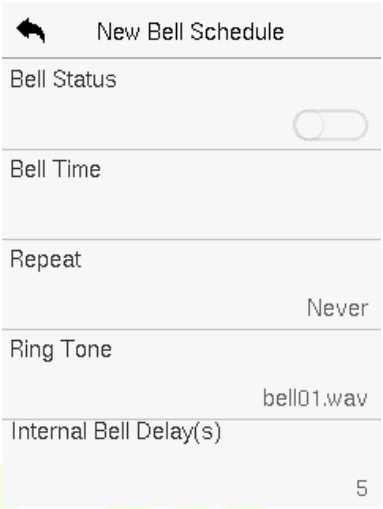
Tap **Bell Schedules** on the **Personalize** interface to configure the Bell settings.



➢ **New Bell Schedule**

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





Function Description

Function Name	Description
Bell Status	Toggle to enable or disable the bell status.
Bell Time	Once the required time is set, the device automatically triggers to ring the bell during that time.
Repeat	Set the required number of counts to repeat the scheduled bell.
Ring Tone	Select a ringtone.
Internal Bell Delay(s)	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, tap **All Bell Schedules** to view the newly scheduled bell.

- **Edit the Scheduled Bell**

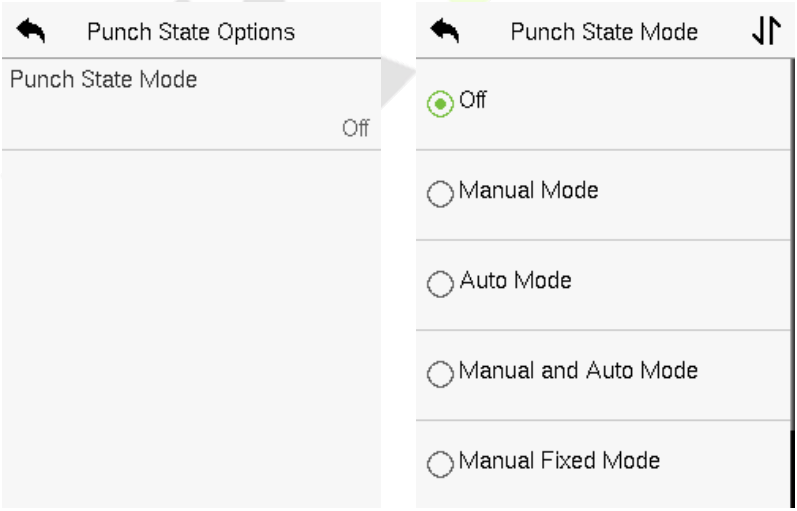
  On the **All Bell Schedules** interface, tap on the required bell schedule, and tap **Edit** to edit the selected bell schedule. The editing method is the same as the operations of adding a new bell schedule.

- **Delete a Bell**

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

12.4 Punch States Options

Tap **Punch States Options** on the **Personalize** interface to configure the punch state settings.



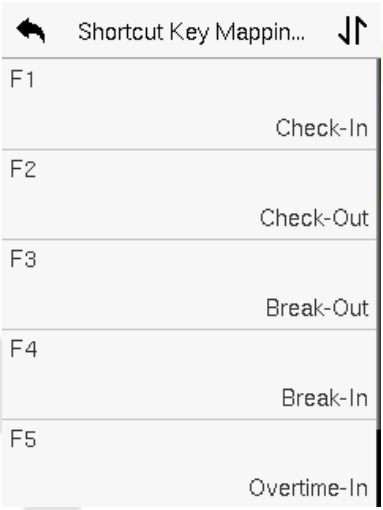
Function Description

Function Name	Description
Punch State Mode	**Off:** Disable the punch state function. Therefore, the punch state key set under Shortcut Key Mappings menu will become invalid. **Manual Mode:** Switch the punch state key manually, and the punch state key will disappear after Punch State Timeout. **Auto Mode:** The punch state key will automatically switch to a specific punch status according to the predefined time schedule which can be set in the Shortcut Key Mappings. **Manual and Auto Mode:** The main interface will display the auto-switch punch state key. However, the users will still be able to select alternative that is the manual attendance status. After timeout, the manual switching punch state key will become auto-switch punch state key. **Manual Fixed Mode:** After the punch state key is set manually to a particular punch status, the function will remain unchanged until it is being manually switched again. **Fixed Mode:** Only the manually fixed punch state key will be shown. Users cannot change the status by pressing any other keys.

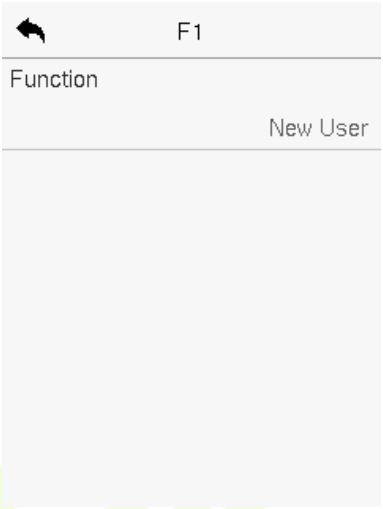
12.5 Shortcut Key Mappings

Users may define shortcut keys for attendance status and for functional keys which will be defined on the main interface. So, on the main interface, when the shortcut keys are pressed, the corresponding attendance status or the function interface will be displayed directly.

Tap **Shortcut Key Mappings** on the **Personalize** interface to set the required shortcut keys.



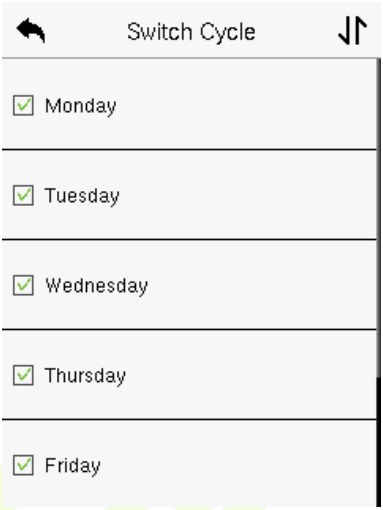
- On the **Shortcut Key Mappings** interface, tap on the required shortcut key to configure the shortcut key settings.
- On the **Shortcut Key (that is "F1") interface, tap function** to set the functional process of the shortcut key either as punch state key or function key.
- If the Shortcut key is defined as a function key (such as New user, All users, etc.), the configuration is completed as shown in the image below.

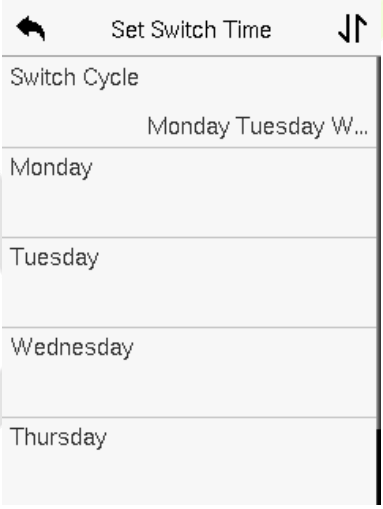


- If the Shortcut key is set as a punch state key (such as check in, check out, etc.), then it is required to set the punch state value (valid value 0~250), name.

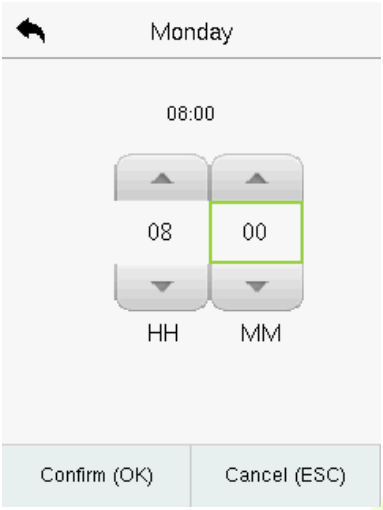
➢ **Set the Switch Time**

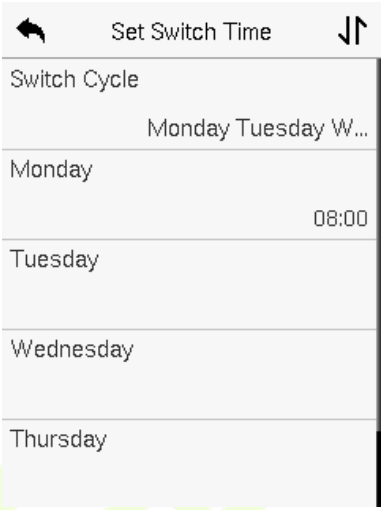
- The switch time is set in accordance with the punch state options.
- When the **Punch State Mode** is set to **Auto Mode**, the switch time should be set.
- On the **Shortcut Key** interface, tap **Set Switch Time** to set the switch time.
- On the **Switch Cycle** interface, select the switch cycle (Monday, Tuesday, etc.) as shown in the image below.





- Once the Switch cycle is selected, set the switch time for each day, and tap **OK** to confirm, as shown in the image below.

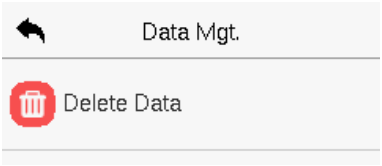




Note: When the function is set to Undefined, the device will not enable the punch state key.

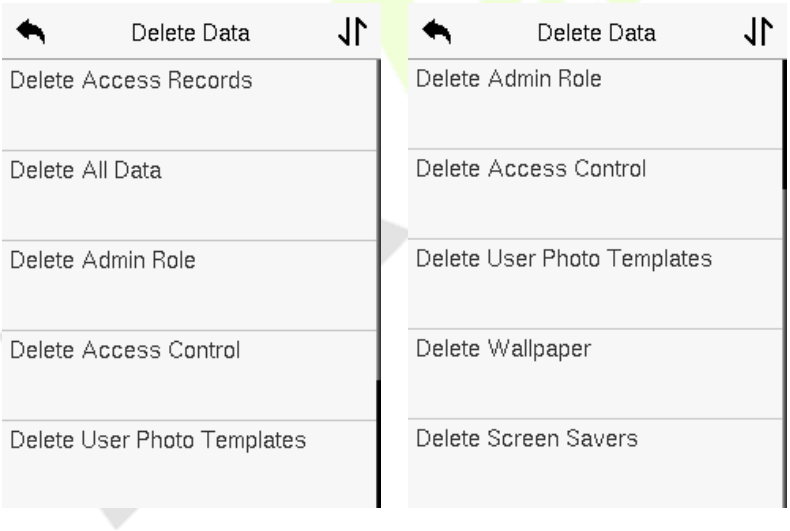
13 Data Management

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



13.1 Delete Data

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

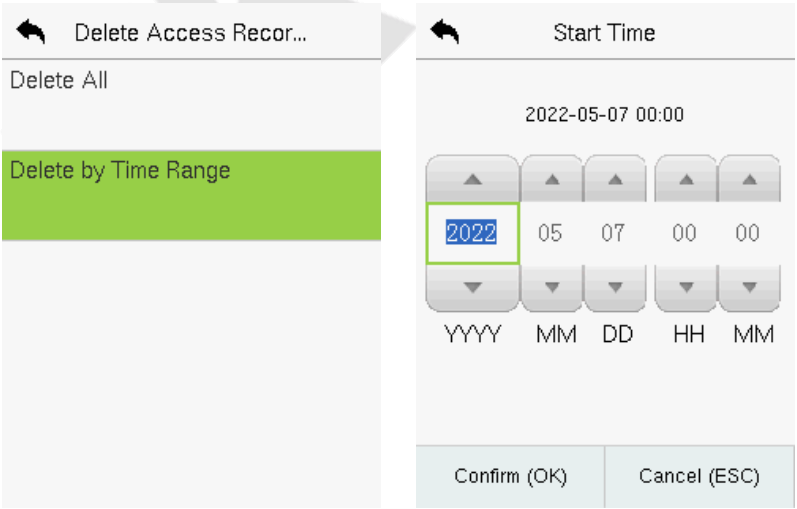


Function Description

Function Name	Description
Delete Access Records	To delete the access records conditionally.

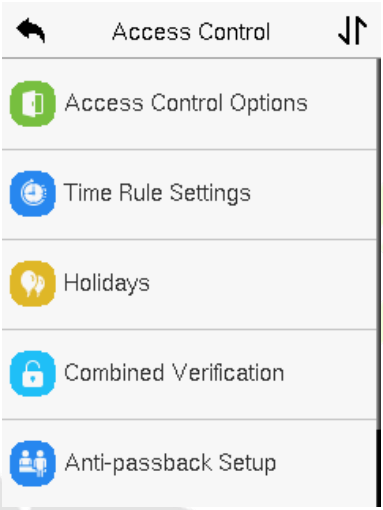
Delete All Data	To delete the information and access records of all registered users.
Delete Admin Role	To remove all the administrator privileges.
Delete Access Control	To delete all the access data.
Delete User Photo Templates	To delete all the user photo templates on the device.
Delete Wallpaper	To delete all the wallpapers in the device.
Delete Screen Savers	To delete all 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.



14 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.

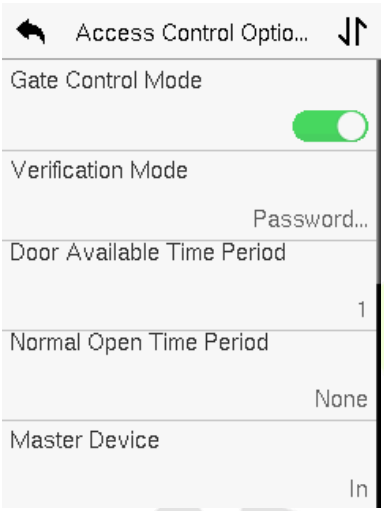


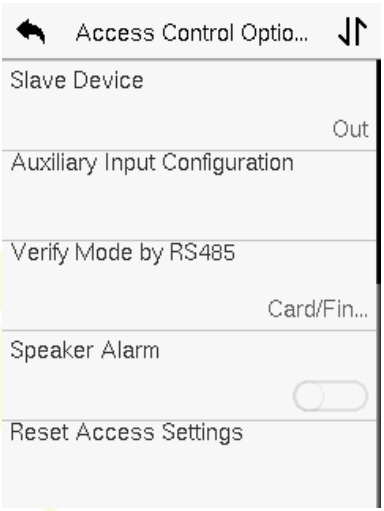
To gain access, the registered user must meet the following conditions:

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.

14.1 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
Gate Control Mode	It toggles between **ON** or **OFF** switch to get into gate control mode or not. When set to **ON**, the interface removes the Door Lock Delay, Door Sensor Delay, and Door Sensor Type options.
Door Lock Delay (s)	The length of time that the device controls the electric lock to be in unlock state. Valid value: 1~99 seconds.

Door Sensor Delay (s)	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.
Door Sensor Type	There are three Sensor types: **None**, **Normal Open**, and **Normal Closed**. **None:** It means the door sensor is not in use. **Normally Open:** It means the door is always left open when electric power is on. **Normally Closed:** It means the door is always left closed when electric power is on.
Verification Mode	The supported verification mode includes Password/Fingerprint/Card/Face, Fingerprint Only, User ID Only, Password, Card Only, Fingerprint/Password, Fingerprint/Card, User ID + Fingerprint, Fingerprint + Password, Fingerprint + Card, Fingerprint + Password + Card, Password + Card, Password/Card, User ID + Fingerprint + Password, Fingerprint + (Card/User ID), Face Only, Face + Fingerprint, Face + Password, Face + Card, Face + Fingerprint + Card, Face + Fingerprint + Password.
Door Available Time Period	It sets the timing for the door so that the door is accessible only during that period.

Normal Open Time Period	It is the scheduled time-period for "Normal Open" mode so that the door is always open during this period.
Master Device	While configuring the master and slave devices, you may set the state of the master as **Out** or **In**. **Out:** A record of verification on the master device is a check-out record. **In:** A record of verification on the master device is a check-in record.
Slave Device	While configuring the master and slave devices, you may set the state of the slave as **Out** or **In**. **Out:** A record of verification on the slave device is a check-out record. **In:** A record of verification on the slave device is a check-in record.
Auxiliary Input Configuration	Sets the door unlock time period and auxiliary output type of the auxiliary terminal device. Auxiliary output types include None, Trigger door open, Trigger Alarm, Trigger door open and Alarm.
Speaker Alarm	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.

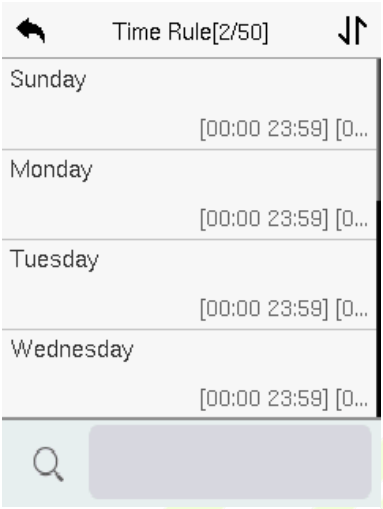
Reset Access Setting	The access control reset parameters include door lock delay, door sensor delay, door sensor type, verification mode, door available time period, normal open time period, master device, and alarm. However, erased access control data in Data Mgt. is excluded.

14.2 Time Schedule

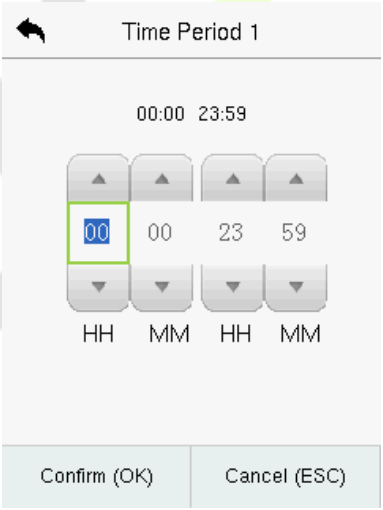
Tap **Time Rule Setting** on the Access Control interface to configure the time settings.

- 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 H**H 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, tap on the required day (that is Monday, Tuesday, etc.) to set the time.



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

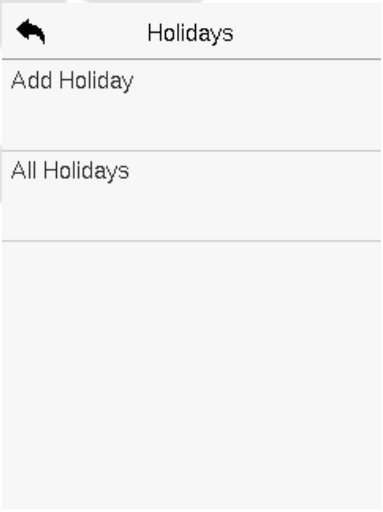
Note:

1. The door is inaccessible for the whole day when the End Time occurs before the Start Time (such as **23:57~23:56**).
2. It is the time interval for valid access when the End Time occurs after the Start Time (such as **08:00~23:59**).
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.

14.3 Holidays

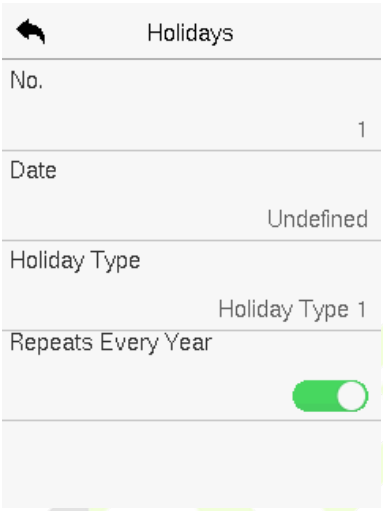
Whenever there is a holiday, you may need a distinct access time; but changing everyone's access time one by one is extremely cumbersome, so a holiday access time can be set that applies to all employees and the user will be able to open the door during the holidays.

Tap **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.

14.4 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 ≤ N ≤ 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, tap the Door-unlock combination to be set, and tap 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.

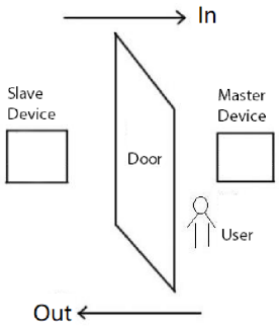
Note: To delete the door-unlock combination, set all Door-unlock combinations to 0.

14.5 Anti-passback Setup

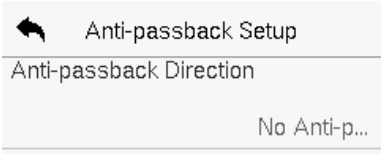
A user may be followed by some person(s) to enter the door without verification, resulting in a security breach. So, to avoid such situations, the Anti-Passback option was developed. Once it is enabled, the check-in and check-out record must occur alternatively to open the door to represent a consistent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

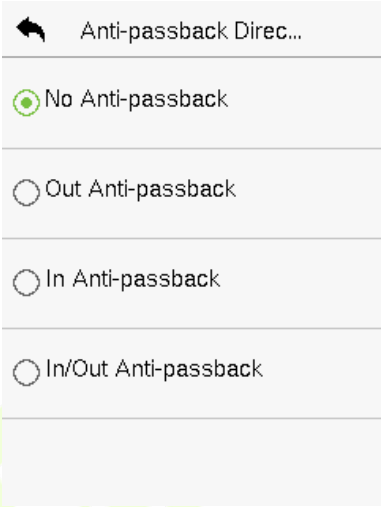
This function requires two devices to work together:

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

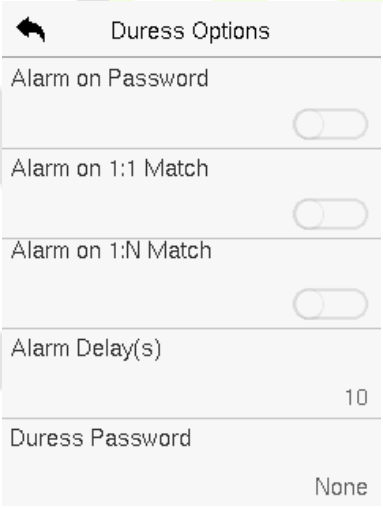
Function Name	Description
Anti-passback Direction	**No Anti-passback:** The Anti-Passback function is disabled, which means successful verification through either the master device or slave device can unlock the door. The attendance state is not saved in this option. **Out Anti-passback:** The user can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

	In/Out Anti-passback: 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.

14.6 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, tap **Duress Options** to configure the duress settings.



Function Description

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

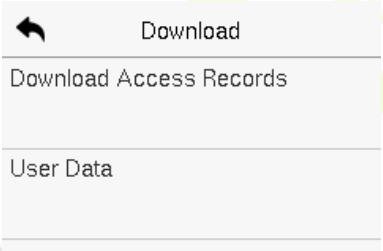
15 USB Manager

You can import user information, access data and other data from a USB drive to computer or other devices.

Before uploading or downloading data from or to the USB drive, insert the USB drive into the USB slot first.

Click **USB Manager** on the main menu interface.

15.1 Download

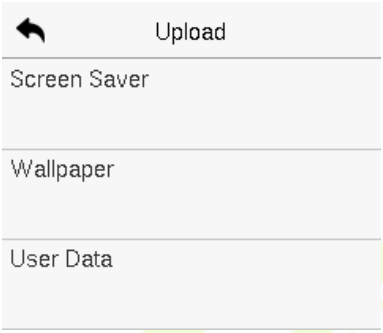


Function Description

Function Name	Description
Download Access Records	To download access data within a specified time period or all data to a USB drive.
User Data	To download all user information from the device to a USB drive.

15.2 Upload

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



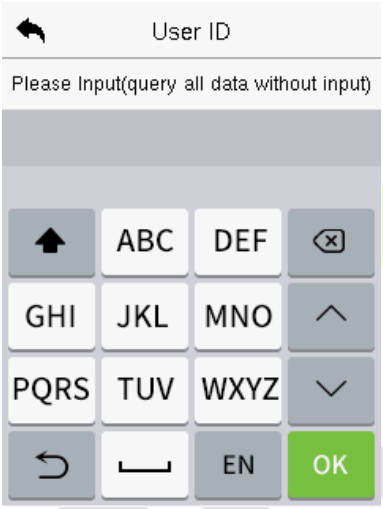
Function Description

Function Name	Description
Screen Saver	To upload a screen saver from a USB drive to the device. Before uploading, you may select **Upload selected picture** or **Upload all pictures**.
Wallpaper	To upload a wallpaper from a USB drive to the device. Before uploading, you may select **Upload selected picture** or **Upload all pictures**. The images will be displayed on the screen after manual settings.
User Data	To upload all user information from a USB drive to the device.

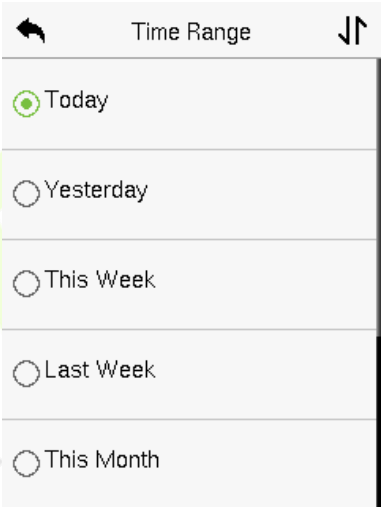
16 Attendance Search

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

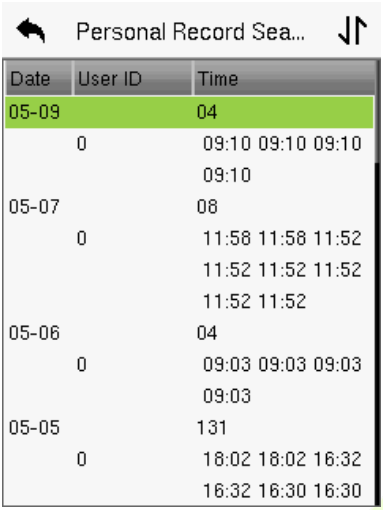
Select **Attendance Search** on the **Main Menu** interface to search for the required event Logs.



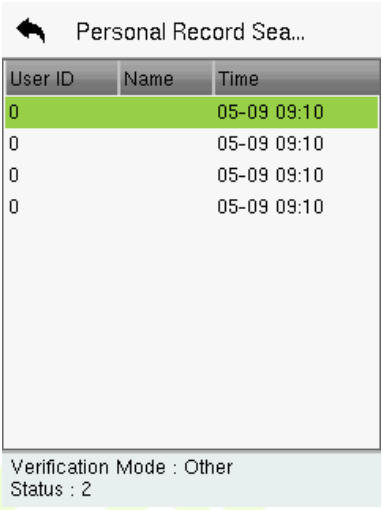
1. Enter the user ID to be searched and tap **OK**. If you want to search for records of all users, tap **OK** without entering any user ID.



2. Select the time range in which the records need to be searched.



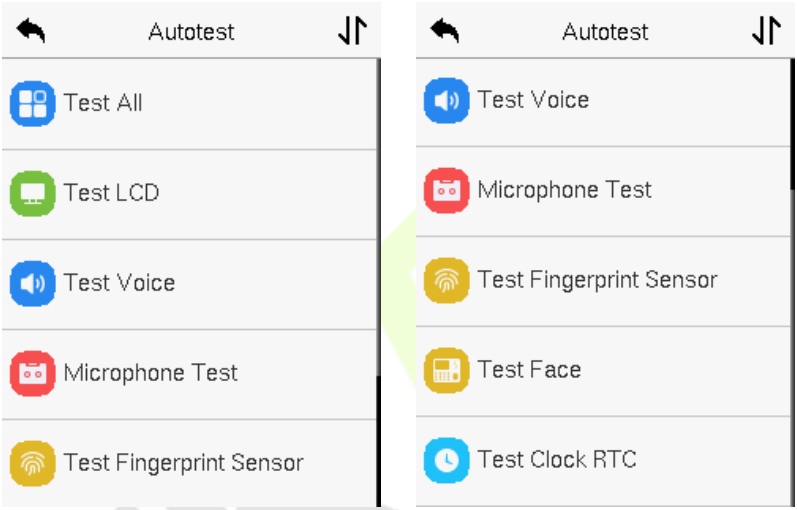
3. Once the record search completes. Tap the record highlighted in green to view its details.



4. The figure shows the details of the selected record.

17 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, Microphone, Fingerprint, Camera and Real-Time Clock (RTC).



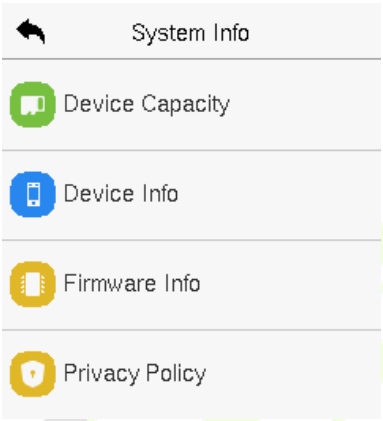
Function Description

Function Name	Description
Test All	To automatically test whether the LCD, Voice, Microphone, Fingerprint, Camera and Real-Time Clock (RTC) are normal.
Test LCD	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.

Test Voice	To automatically test whether the audio files stored in the device are complete and the voice quality is good.
Microphone test	To test if the microphone is working properly by speaking into the microphone.
Test Fingerprint Sensor	To test the fingerprint sensor by pressing a finger on the scanner to check if the acquired fingerprint image is clear. When you are pressing a finger on the scanner, the fingerprint image will display on the screen.
Test Face	To test if the camera functions properly by checking the pictures taken to see if they are clear enough.
Test Clock RTC	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.

18 System Information

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



Function Description

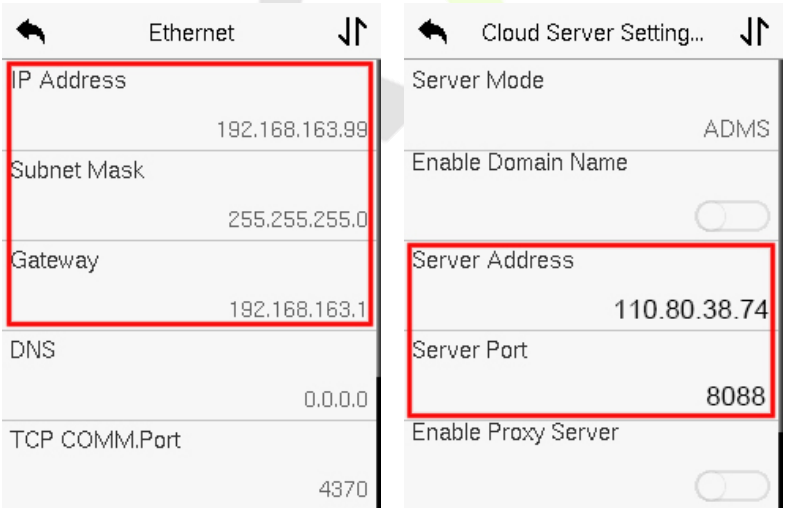
Function Name	Description
Device Capacity	Displays the current device's user storage, fingerprint, card, password and face storage, administrators and records.
Device Info	Displays the device's name, serial number, MAC address, fingerprint algorithm, face algorithm, platform information, MCU Version, Manufacturer, and manufacture date.
Firmware Info	Displays the firmware version and other version information of the device.
Privacy Policy	Display the device's privacy policy.

19 Connect to ZKBio CVAccess Software

19.1 Set the Communication Address

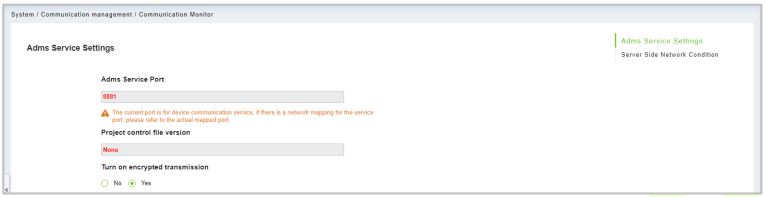
➢ **Device side**

1. Tap **COMM.** > **Ethernet** in the main menu to set the IP address and gateway of the device.
   (***Note:*** Please ensure that the IP address is in the same network segment as the server address and can communicate with the ZKBio CVAccess server.)
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 ZKBio CVAccess server.
   Server port: Set the server port as of ZKBio CVAccess.



➢ **Software side**

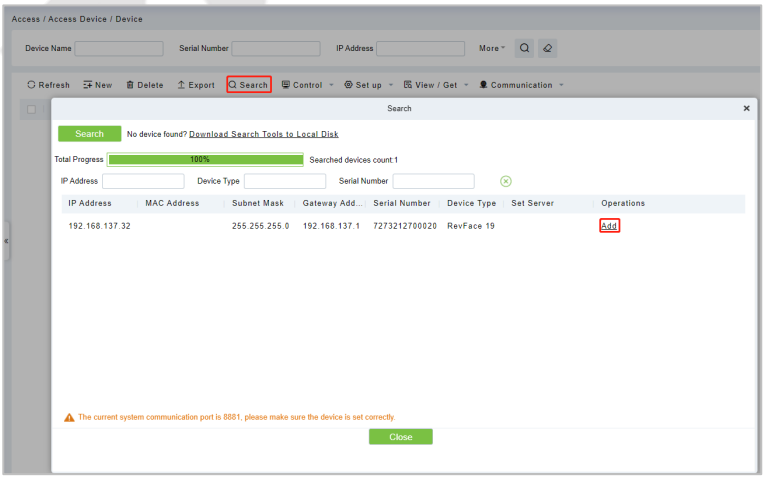
Login to ZKBio CVAccess software, click **System** > **Communication** > **Communication Monitor** to set the ADMS service port, as shown in the figure below:



19.2 Add Device on the Software

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

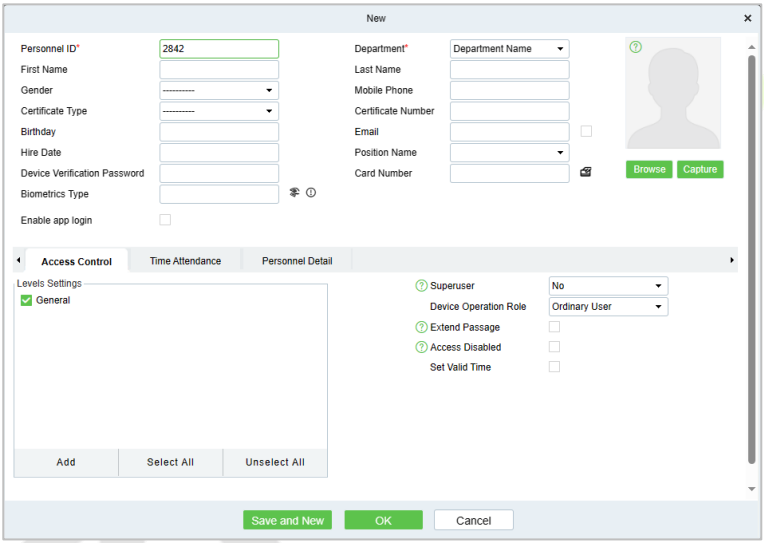
1. Click **Access** > **Device** > **Search Device**, to open the Search interface in the software.
2. Click Search, and it will prompt [**Searching……**].
3. After searching, the list and total number of access controllers will be displayed.



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

19.3 Add Personnel on the Software

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

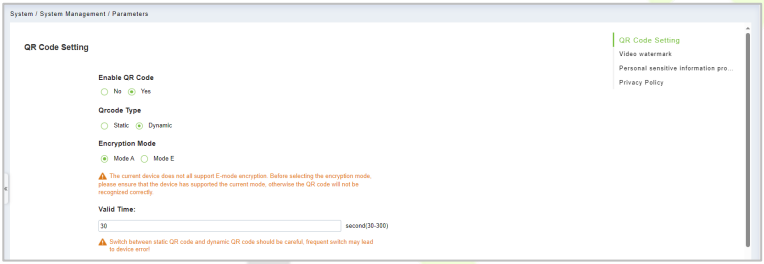


2. Fill in all the required fields and click [**OK] to register a new user.**
3. Click **Access > Device > Control > Synchronize All Data to Devices** to synchronize all the data to the device including the new users.

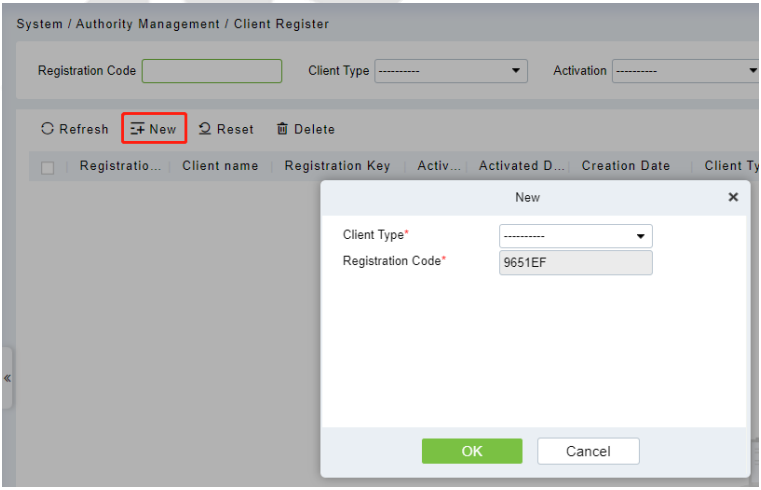
19.4 Mobile Credential★

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

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



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

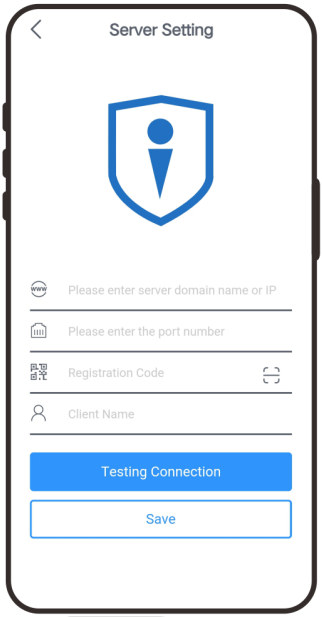


3. Open the App on the Smartphone. On the login screen, tap **Server Setting** and type the IP Address or the domain name of the Server, and its port number.

   Note: Smartphone and the Server must be in the same network segment.

4. Tap the **QR Code** icon to scan the QR code of the new App client. After the client is identified successfully, set the client's name and tap **Connection Test**.

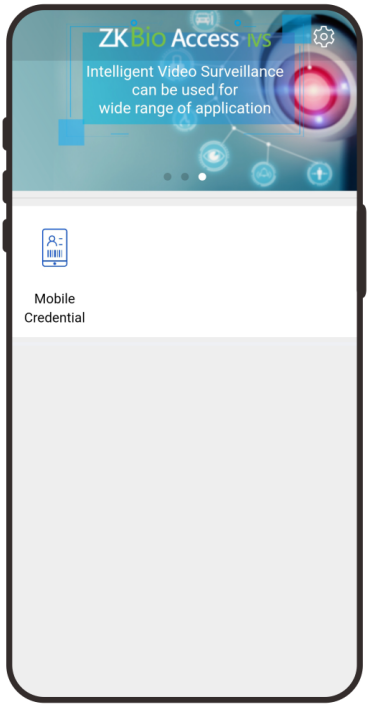
5. After the network is connected successfully, tap **Save**.



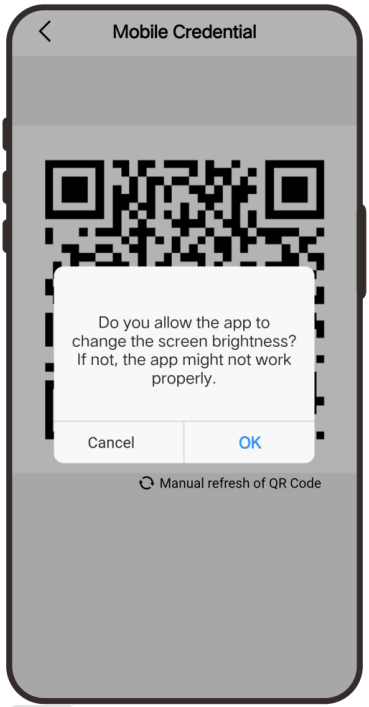
The Mobile Credential function is only valid when logging in as an employee, tap on Employee to switch to employee login screen. Enter the employee ID and password (Default: 123456) to login.

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

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



8. 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:



9. The QR code refreshes automatically for every 30s and supports manual refresh.

Note: For other specific operations, please refer to ZKBio CVAccess User Manual.

Appendix 1

Requirements of Live Collection and Registration of Visible Light Face Templates

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

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

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

I. Collected Information

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

1. **User Registration Information: At your first registration, the feature template (Fingerprint template/Face template/Palm template**) will be saved on the device according to the device type you have selected to verify the unique similarity between you and the User ID you have registered. You can optionally enter your Name and Code. The above

information is necessary for you to use our products. If you do not provide such information, you cannot use some features of the product regularly.

2. **Product information:** According to the product model and your granted permission when you install and use our services, the related information of the product on which our services are used will be collected when the product is connected to the software, including the Product Model, Firmware Version Number, Product Serial Number, and Product Capacity Information. **When you connect your product to the software, please carefully read the privacy policy for the specific software.**

II. Product Security and Management

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

2. All the functions of displaying the biometric information are disabled in our products by default. You can choose Menu > System Settings to set whether to display the biometric information. If you enable these functions, we assume that you are aware of the personal privacy security risks specified in the privacy policy.

3. Only your user ID is displayed by default. You can set whether to display other user verification information (such as Name, Department, Photo, etc.) under the Administrator privilege. **If you choose to display such**

information, we assume that you are aware of the potential security risks (for example, your photo will be displayed on the device interface).

4. The camera function is disabled in our products by default. If you want to enable this function to take pictures of yourself for attendance recording or take pictures of strangers for access control, the product will enable the prompt tone of the camera. **Once you enable this function, we assume that you are aware of the potential security risks.**

5. All the data collected by our products is encrypted using the AES 256 algorithm. All the data uploaded by the Administrator to our products are automatically encrypted using the AES 256 algorithm and stored securely. If the Administrator downloads data from our products, we assume that you need to process the data and you have known the potential security risk. In such a case, you shall take the responsibility for storing the data. You shall know that some data cannot be downloaded for sake of data security.

6. All the personal information in our products can be queried, modified, or deleted. If you no longer use our products, please clear your personal data.

III. How we handle personal information of minors

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

We will only use or disclose personal information of minors collected with

their parents' or guardians' consent if and to the extent that such use or disclosure is permitted by law or we have obtained their parents' or guardians' explicit consent, and such use or disclosure is for the purpose of protecting minors.

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

IV. Others

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

Eco-friendly Operation

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

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

Hazardous or Toxic substances and their quantities

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

Adapter	×	○	○	○	○	○
Screws	○	○	○	×	○	○

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

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

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

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