User Manual

F18

Date: February 2023

Doc Version: 1.1

English

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

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

Trademark

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

Disclaimer

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

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

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

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

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

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

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

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

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

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

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

ZKTeco Headquarters

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

Phone +86 769 - 82109991

Fax +86 755 - 89602394

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

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

About the Company

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

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

About the Manual

This manual introduces the operations of **F18**.

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

Data Security Statement

ZKTeco, as a smart product supplier, may also need to know and collect some of your personal information in order to better assist you in using ZKTeco's goods and services, and will treat your privacy carefully by developing a Privacy Policy.

Please read and understand completely all the privacy protection policy regulations and key points that appear on the device before using ZKTeco products.

As a product user, you must comply with applicable laws and regulations related to personal data protection when collecting, storing, and using personal data, including but not limited to taking protective measures for personal data, such as performing reasonable rights management for devices, strengthening the physical security of device application scenarios, and so on.

Safety Measures

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

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

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

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

   And do not connect multiple devices to one power adapter as adapter overload can cause over-

heat or fire hazard.

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

    Recommended installing the devices in areas with limited access.

Electrical Safety

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

Operation Safety

- If smoke, odour, or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service centre.
- Transportation and other unpredictable causes may damage the device hardware. Check whether the device has any intense damage before installation.
- If the device has major defects that you cannot solve, contact your dealer as soon as possible.
- Dust, moisture, and abrupt temperature changes can affect the device's service life. You are advised not to keep the device under such conditions.
- Do not keep the device in a place that vibrates. Handle the device with care. Do not place heavy objects on top of the device.

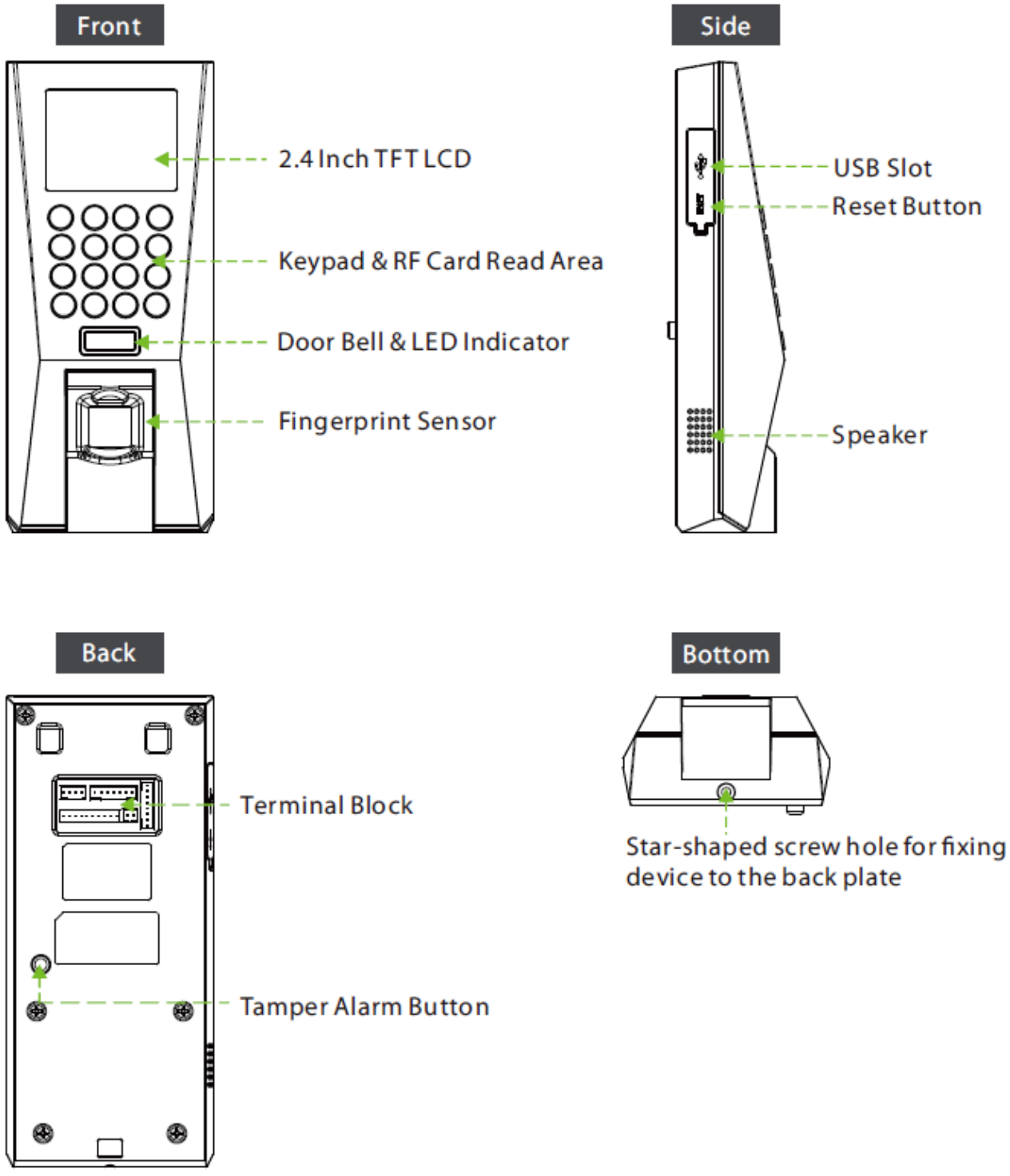
- Do not apply rosin, alcohol, benzene, pesticides, and other volatile substances that may damage the device enclosure. Clean the device accessories with a piece of soft cloth or a small amount of cleaning agent.
- If you have any technical questions regarding usage, contact certified or experienced technical personnel.

Note:

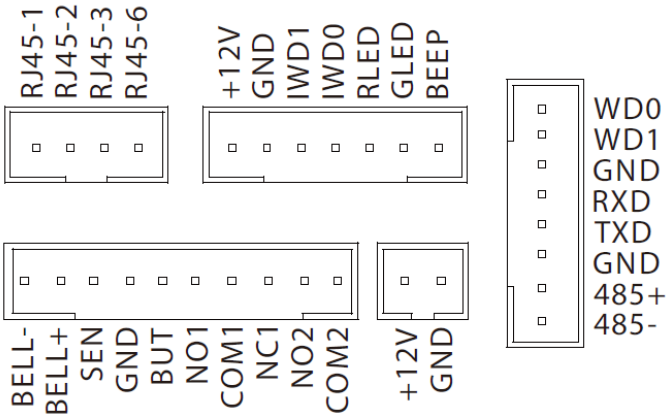
- Make sure whether the positive polarity and negative polarity of the DC 12V power supply is connected correctly. A reverse connection may damage the device. It is not advisable to connect the AC 24V power supply to the DC 12V input port.
- Make sure to connect the wires following the positive polarity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

1 Overview

1.1 Appearance



1.2 Terminal Block

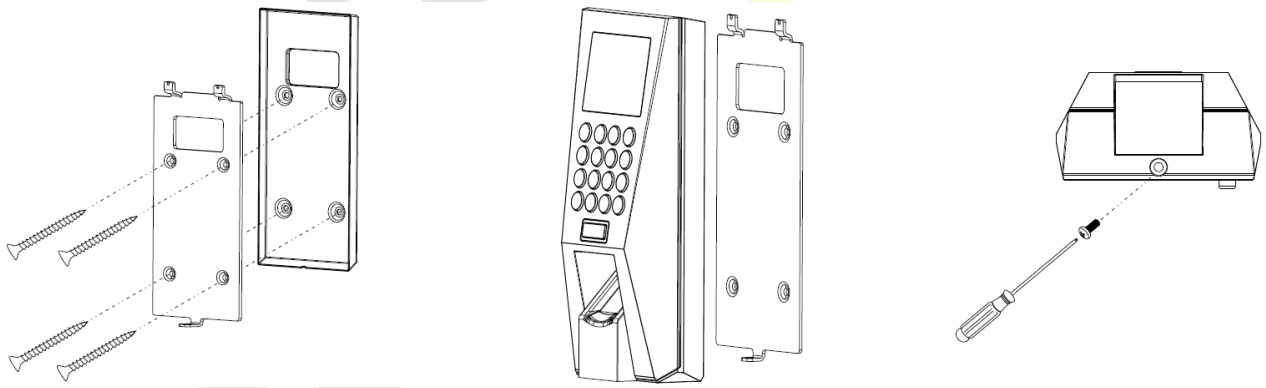


2 Installation and Wiring

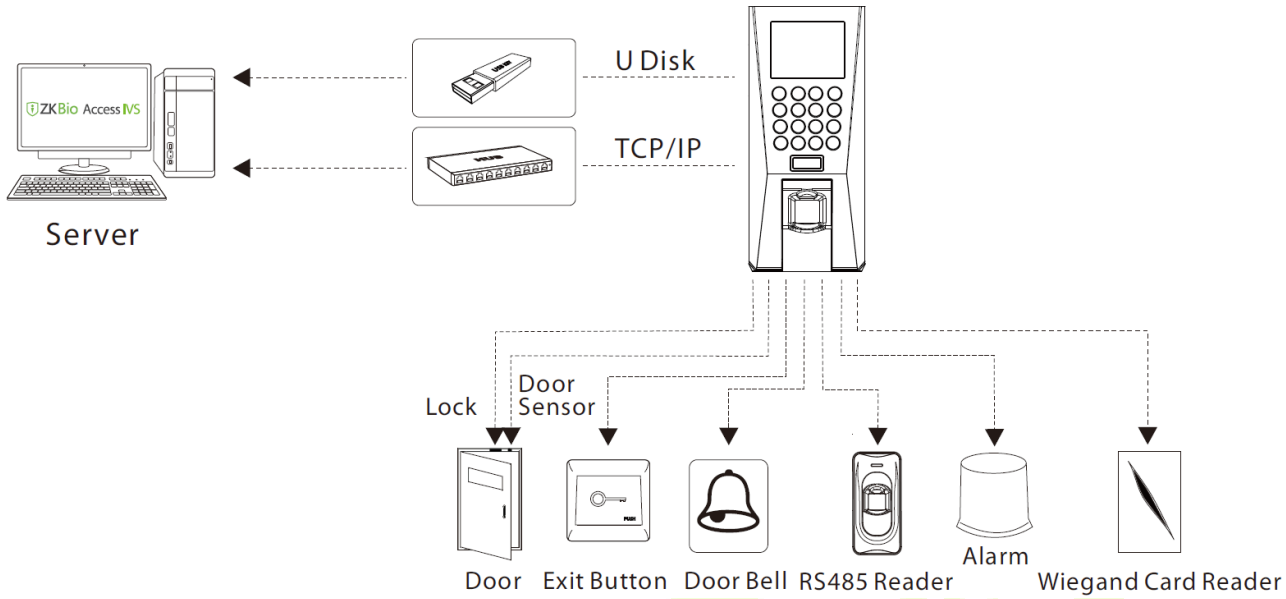
2.1 Installation of Wall-mount

Before the installation, please connect the cables to the connectors.

1. Fix back plate to the wall.
2. Mount the device on the back plate.
3. Secure the device and back plate.



2.2 Wiring Diagram



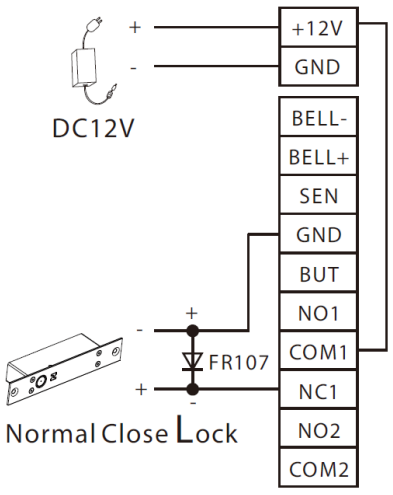
2.2.1 Lock Connection

The system supports Normally Opened Lock and Normally Closed Lock.

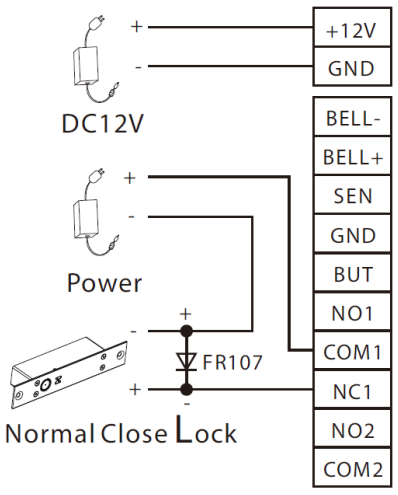
The NO LOCK (normally opened at power on) is connected with 'NO1' and 'COM' terminals, and the NC LOCK (normally closed at power on) is connected with 'NC1' and 'COM' terminals.

Take NC Lock as an example below:

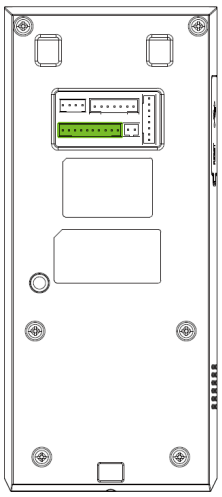
1) Device not sharing power with the lock

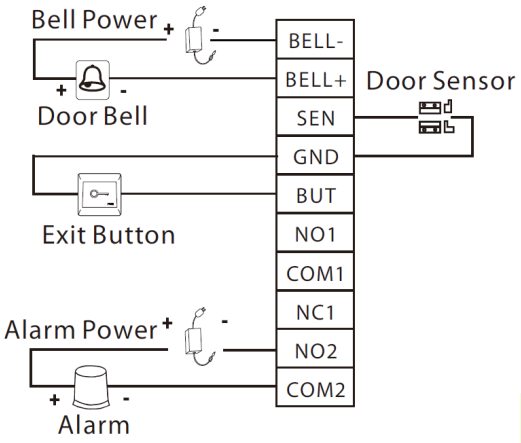


2) Device sharing power with the lock

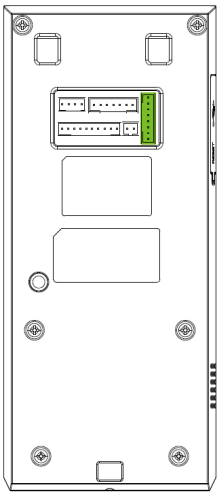


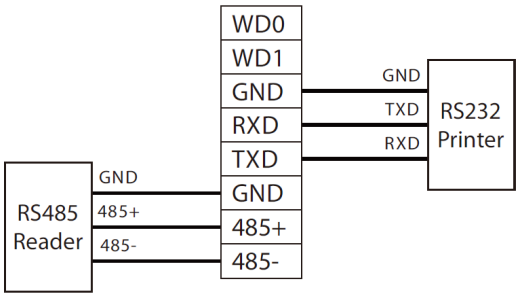
2.2.2 Door Bell & Door Sensor & Exit Button & Alarm Connection





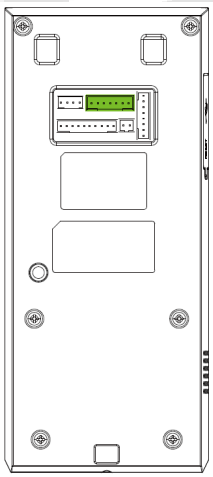
2.2.3 RS485 and RS232 Connection

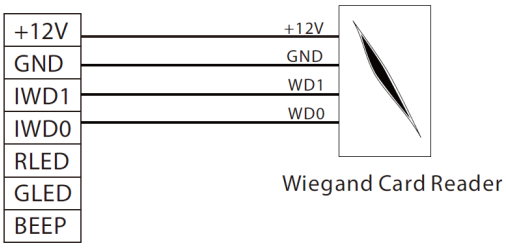




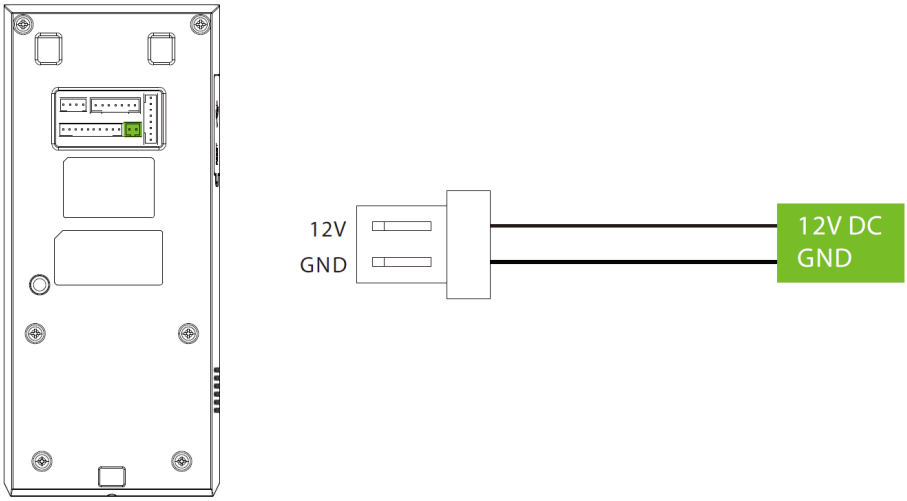
Note: RS232 for TA push firmware connect to the Printer.

2.2.4 Wiegand Reader Connection





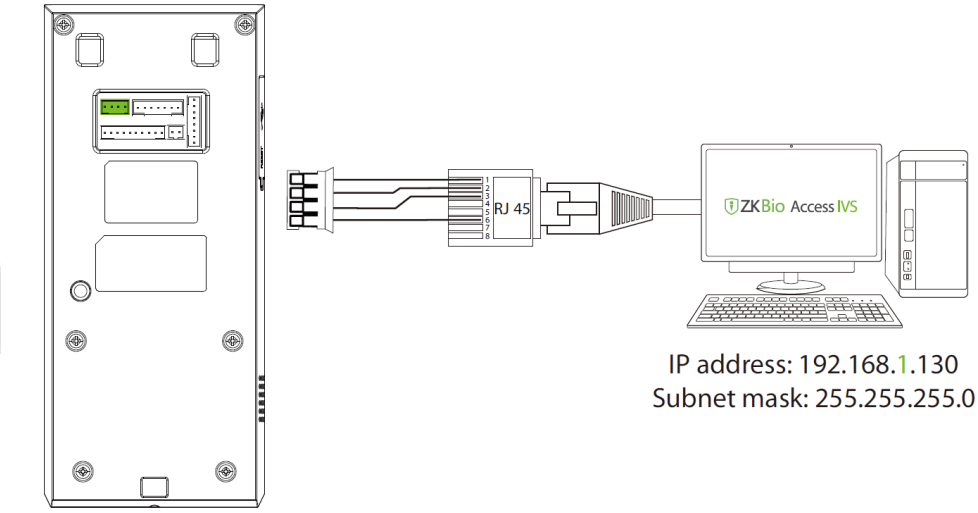
2.2.5 Power Connection



Recommended power supply:

1. 12V ± 10%, at least 500mA.
2. To share the power with other devices, use a power supply with higher current ratings.

2.2.6 Ethernet Connection



Set ethernet parameters refer to 7.1 Ethernet Settings.

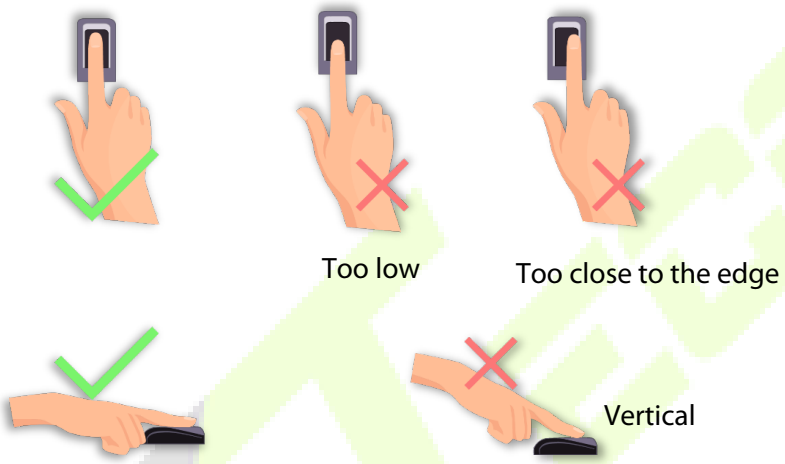
Note: The IP address should be able to communicate with the ZKBioAccess IVS server, preferably in the same network segment with the server address.

3 Instruction for Use

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

3.1 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.

3.2 Standby Interface

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

- Tap number button to enter the User ID input interface.
- When there is no Super Administrator set in the device, tap **M/OK** 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.

3.3 Verification Mode

3.3.1 Fingerprint Verification

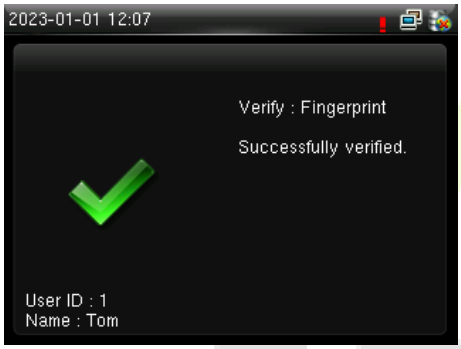
- **1: N Fingerprint Verification Mode**

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

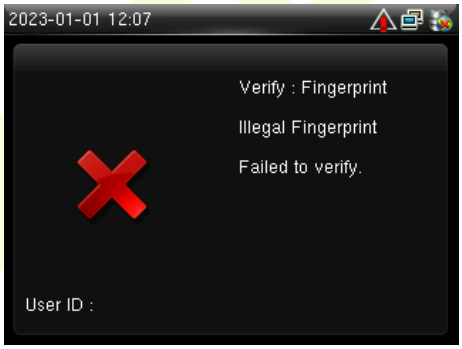
The device enters the fingerprint authentication mode when a user presses his/her finger onto the fingerprint scanner.

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:

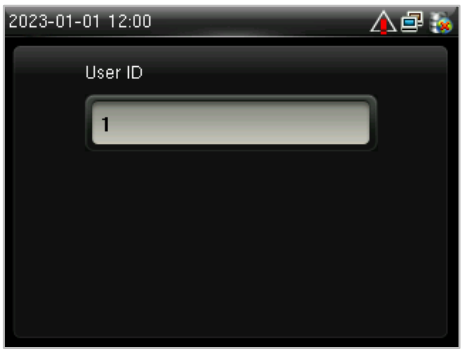


- **1: 1 Fingerprint Verification Mode**

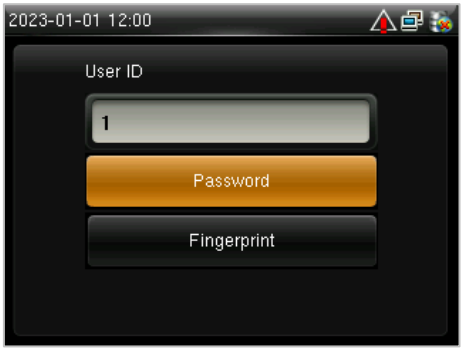
Compares the fingerprint that is being pressed onto the fingerprint reader with the fingerprints that are linked to User ID input via the virtual keyboard.

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

Enter the user ID by using keypad on the initial interface. Then press **M/OK** to enter 1:1 fingerprint verification mode.

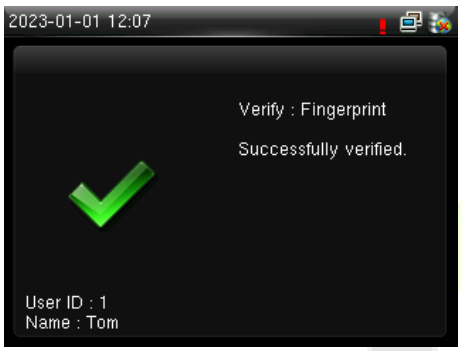


If the user has registered face and password in addition to his/her fingerprints and the verification method is set to Password/Fingerprint/Face verification, the following screen will appear. Select **Fingerprint** to enter fingerprint verification mode.

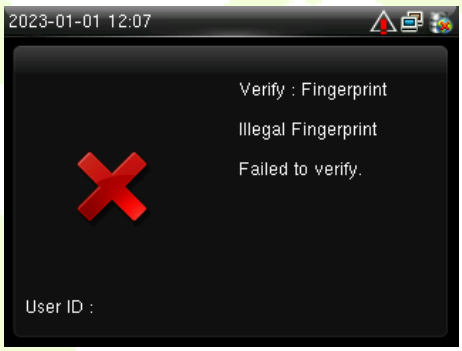


Press the fingerprint to verify.

Verification is successful:



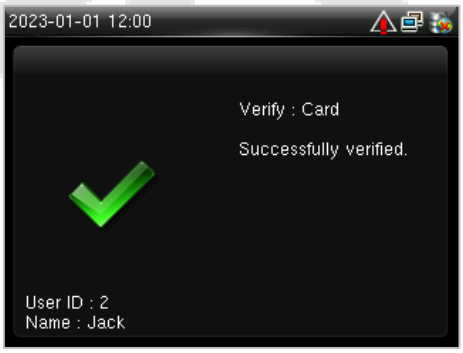
Verification is failed:



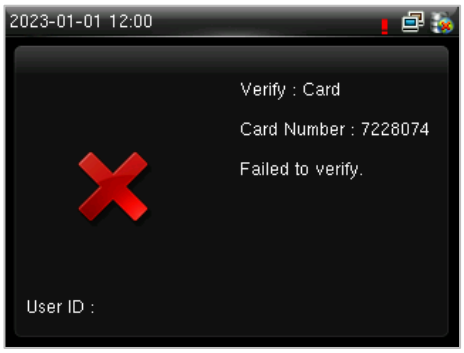
3.3.2 Card Verification

It compares the acquired card information with all card data registered in the device. Following are the display screen after putting a correct card and a wrong card respectively.

Verification is successful:



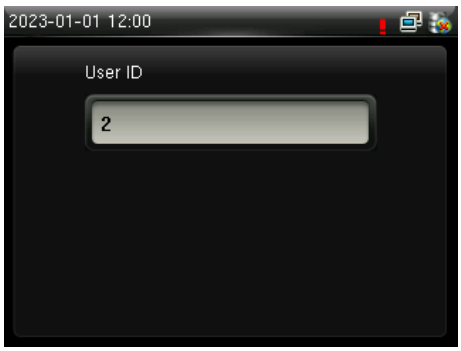
Verification is failed:



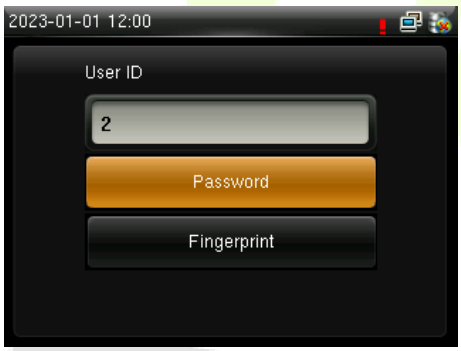
3.3.3 Password Verification

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

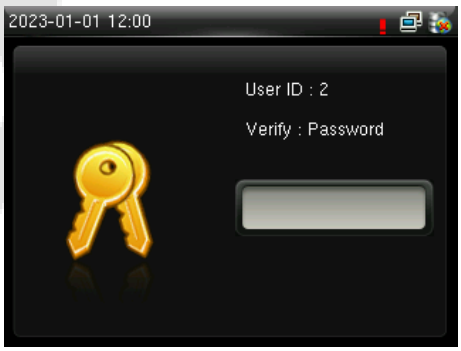
Enter the user ID by using keypad on the initial interface. Then press **M/OK** to enter the 1:1 password verification mode.



If an employee registers fingerprint in addition to password, the following screen will appear. Select **Password** and press **M/OK** to enter password verification mode.

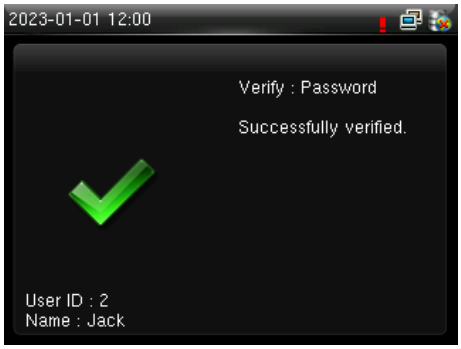


Input the password and press **M/OK**.

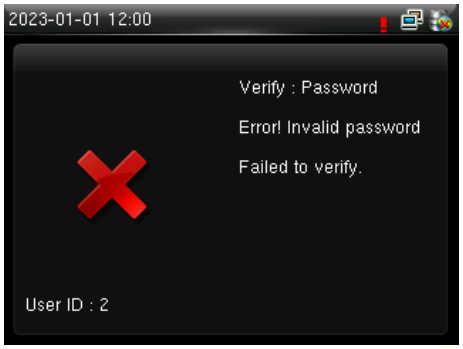


Following are the display screen after entering a correct password and a wrong password respectively.

Verification is successful:



Verification is failed:



4 Main Menu

Press **M/OK** on the initial interface to enter the main menu, as shown below:

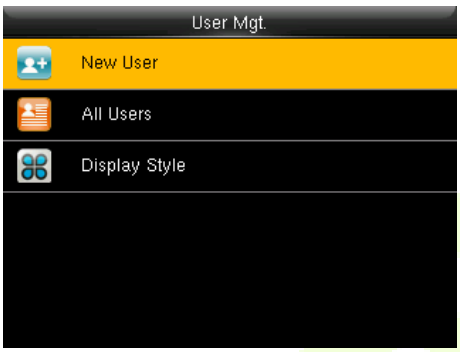
Function Description

Menu	Descriptions
User Mgt.	It can add new users. Contains basic information of registered users, including user ID, name, user role, fingerprint, badge number, password and access control role.
User Role	It is used to set user roles for gaining access to the menu and editing options.
COMM.	It is used to set the related parameters of the communication between the device and PC, including ethernet parameters such as IP address etc., Serial Comm, PC connection, Wireless Network, ADMS and Wiegand settings.
System	It will set related parameters of the system, upgrade firmware, set date & time, set attendance and fingerprint parameters and reset to factory settings.
Personalize	It will set interface display, voice, bell, punch state key mode and shortcut key.
Data Mgt.	It includes deleting attendance data, deleting all data, deleting admin role and deleting screen savers etc. and backup, restore data.
Access Control	It will set the parameters of the control lock and access control devices, including parameters of access control, time schedule, holidays, access groups, combined verification, Anti-Passback and duress options.
USB Manager	It will transfer user data and attendance logs from the USB disk to the supporting software or other devices.
Attendance Search	It will search for the records stored in the device after successful verification.
Autotest	It will automatically test different module's functions, including the LCD, voice, keyboard, fingerprint sensor and clock RTC test.
System Info	It is for checking device capacity, device and firmware information.

5 User Management

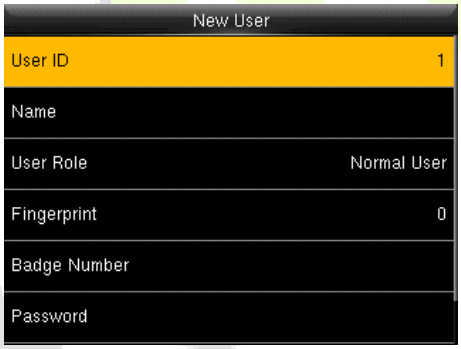
5.1 User Registration

Press **M/OK** on the initial interface. Select **User Mgt.** and press **M/OK**.



5.1.1 Register a User ID and Name

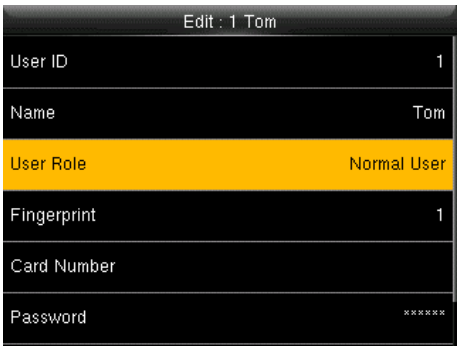
Select **New User** and press **M/OK**. Select **User ID** and **Name**, enter the user ID and name by using keyboard, then press **M/OK**.

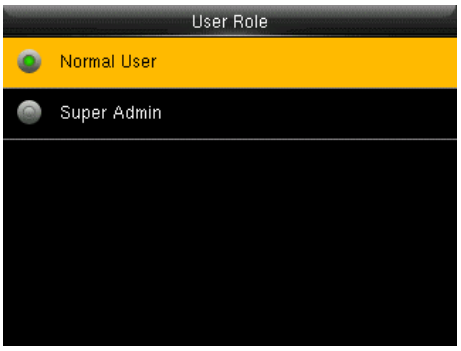


5.1.2 Setting the User Role

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

Press ▲/▼ to select **User Role** and press **M/OK**.

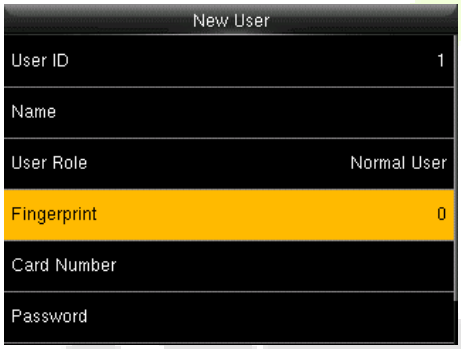


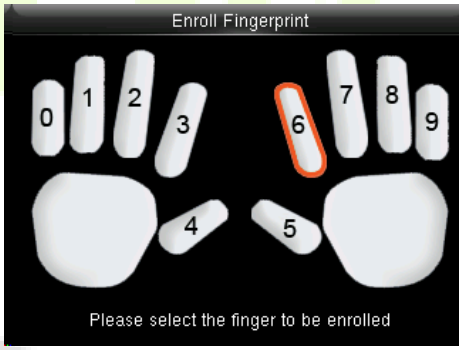


Note: If the selected user role is the Super Admin, the user must pass the identity authentication to access the main menu. The authentication is based on the authentication method(s) that the super administrator has registered. Please refer to "Verification Mode".

5.1.3 Register Fingerprint

Press ▲/▼ select **Fingerprint** and press **M/OK**. Select a finger and press **M/OK**.

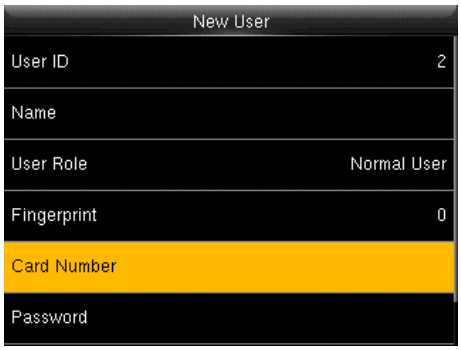




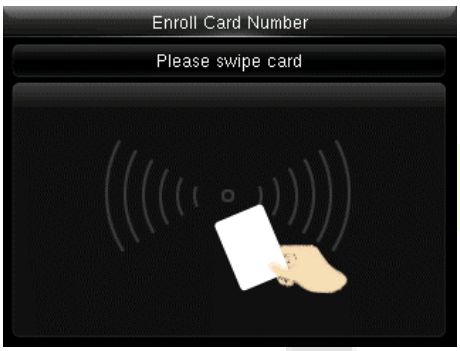
Press the same finger on the fingerprint reader three times. Green indicates that the fingerprint was enrolled successfully.

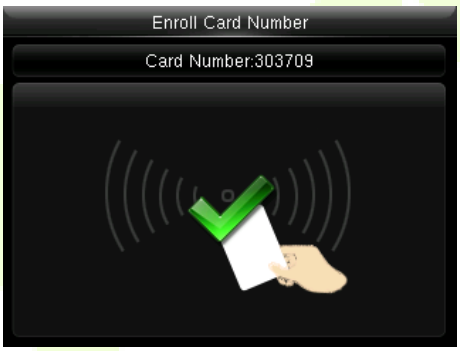
5.1.4 Register Card Number

Press ▲/▼ select **Card Number** and press **M/OK** in the **New User** interface.



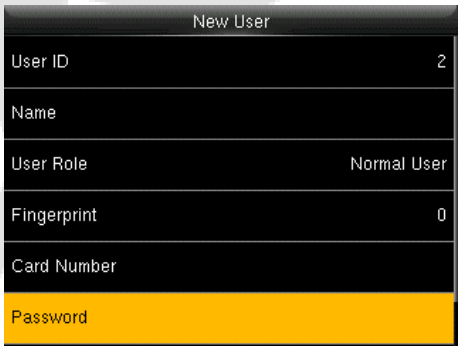
Put a correct card to swipe.



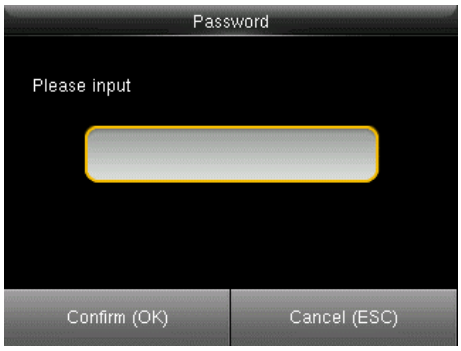


5.1.5 Register Password

Press ▲/▼ select **Password** and press **M/OK** in the **New User** interface.



Enter a password using keypad and re-enter the password, press **M/OK**. If the two entered passwords are different, the prompt "**Password not match**!" will appear.

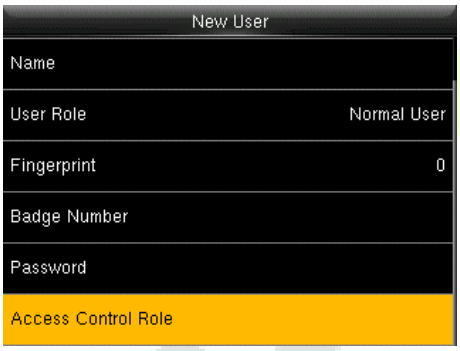


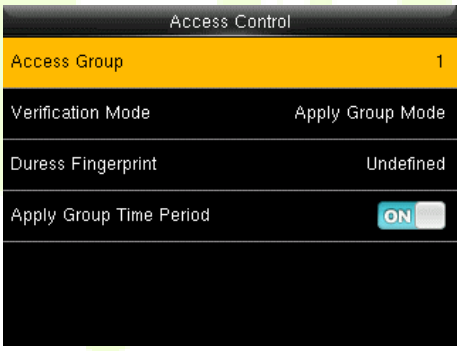
Note: The password may contain one to eight digits by default.

5.1.6 Access Control Role

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

Press ▲/▼ to select **Access Control Role**, press **M/OK**.



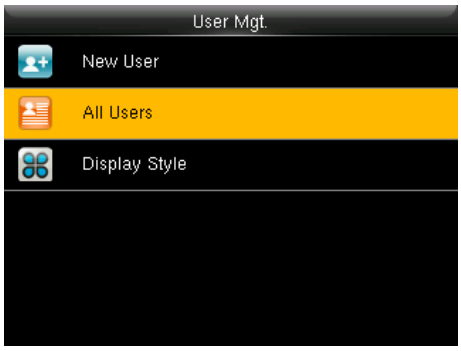


Function Description

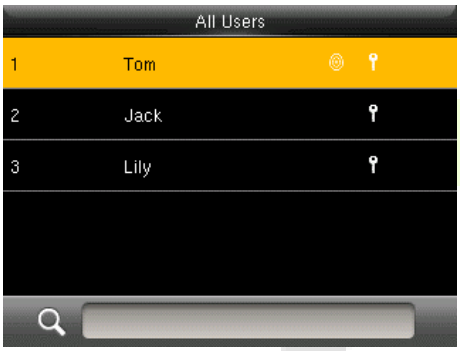
Function	Descriptions
Access Group	To allocate different access control groups to users for management. New users will belong to Group 1 as per default settings, but they can be reallocated to other groups.
Verfication Mode	User can choose either group or individual verification. If individual verification is selected, the verification method used by other group members will not be affected.
Duress Fingerprint	User can choose one or more registered fingerprint(s) as Duress Fingerprint. When verifying through duress fingerprint, duress alarm will be triggered.
Apply Group Time Period	When this function is ON, the user will be in the default time zone of his/her group. When this function is OFF, the user needs to be added in a personal time zone (because the user will be moved out of the default time zone of his/her group). This will not affect the access time zone of other group members. **Note:** Every user (who doesn't use default group time) can be set in maximum 3 time periods.

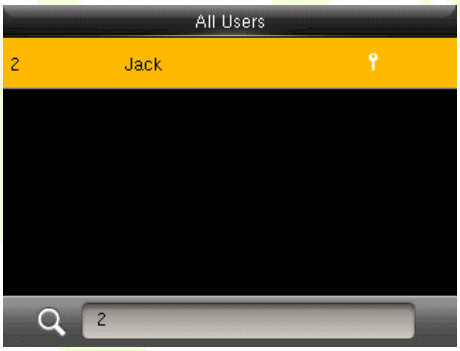
5.2 Search User

On the **Main Menu**, select **User Mgt.** and press **OK.,** and select **All User** and press **M/OK** to search a User.



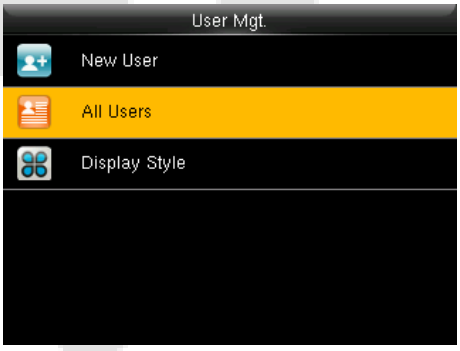
On the **All Users** interface, Enter the user ID, such as 2, and press **M/OK**, and the system will search for the related user information.

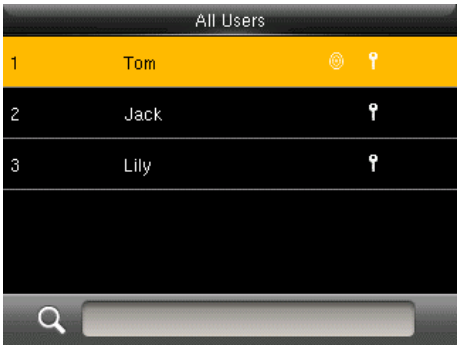




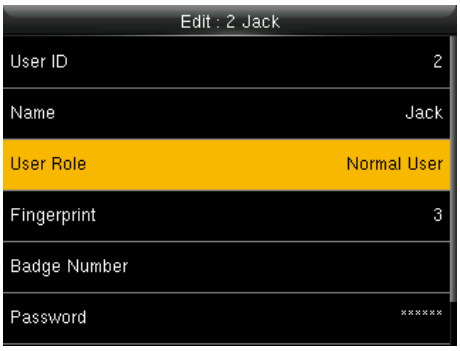
5.3 Edit User

In **User Mgt.** interface, Select **All User** and press **M/OK**.





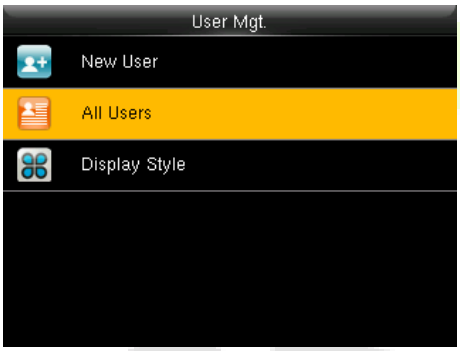
Press ▲/▼ to select a user and press **M/OK**. Press ▲/▼ to select **Edit** and press **M/OK**.

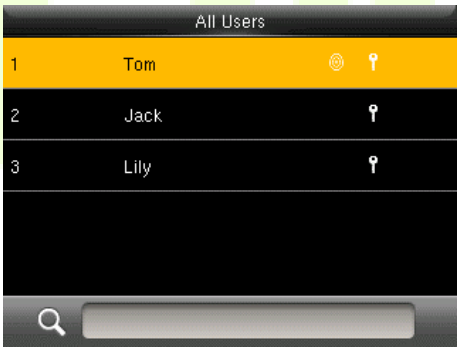


Note: The process of editing the user information is the same as adding a new user, except that the User ID cannot be modified when editing a user. The process in detail refers to "User Registration".

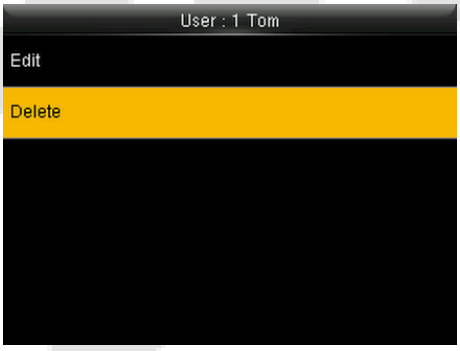
5.4 Deleting User

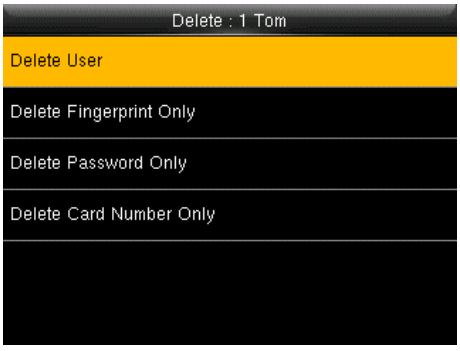
In **User Mgt.** interface, Select **All User** and press **M/OK**.





Press ▲/▼ to select a user and press **M/OK**. Press ▲/▼ to select **Delete** and press **M/OK**.





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.

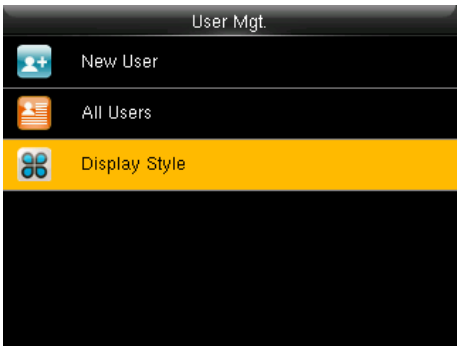
Delete Password Only: Deletes the password information of the selected user.

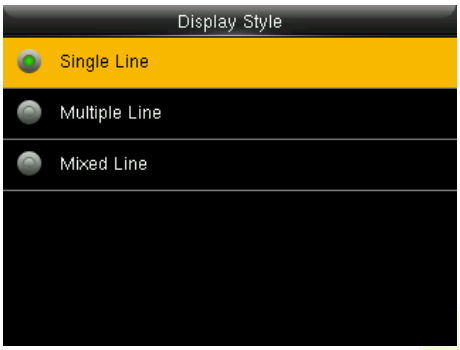
Delete Card Number Only: Deletes the card number of the selected user.

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

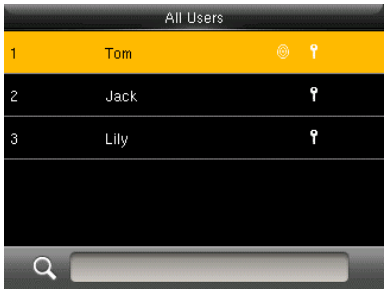
5.5 Display Style

In **User Mgt.** interface, Select **Display Style** and press **M/OK** to choose the style of **All Users** interface's list.

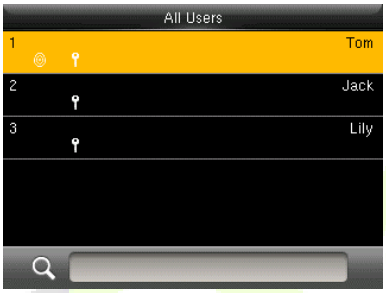




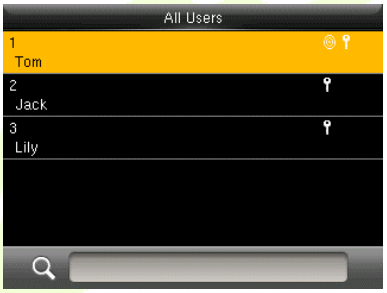
Different display styles are shown as below:



Single Line Style



Multiple Line Style



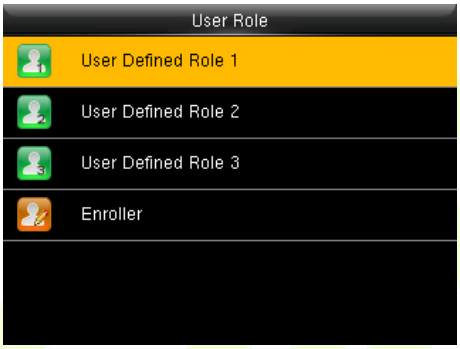
Mixed Line Style

6 User Role

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

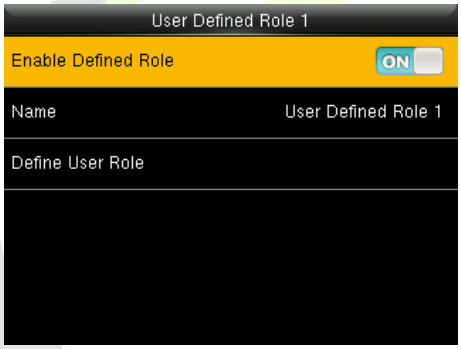
You may set the permission scope of the custom role (up to 3 roles) and enroller, that is, the permission scope of the operation menu.

Press **M/OK** on the initial interface. Select **User Role** and press **M/OK**.

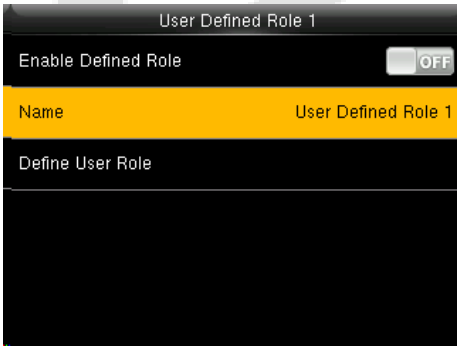


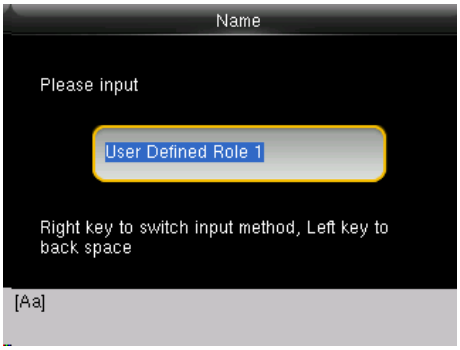
Press ▲/▼ to select a **User Defined Role** on the **User Role** interface and press **M/OK**.

Press ▲/▼ to select **Enable Defined Role** and press **M/OK** to enable or disable the user-defined role.



Press ▲/▼ to select **Name** and press **M/OK** to enter the custom name of the role.

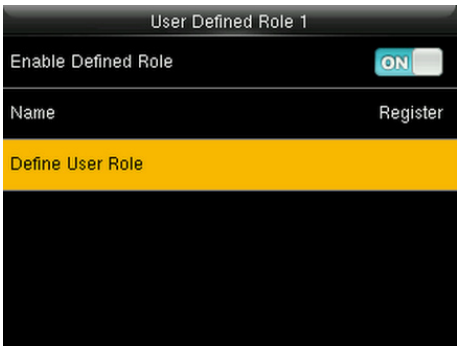


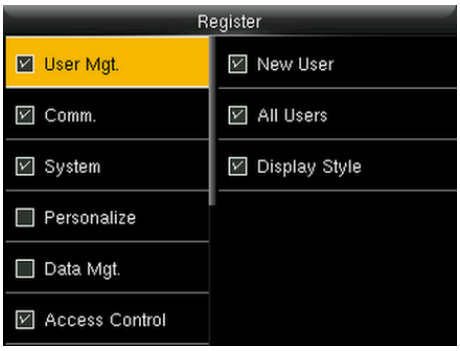


Then, press ▲/▼ to select a **Define User Role** and press **M/OK**.

Press ▲/▼ to select rights and press **M/OK** to turn on or turn off.

During privilege assignment, the **Main Menu** function names will be displayed on the left and its sub-menus will be listed on its right.

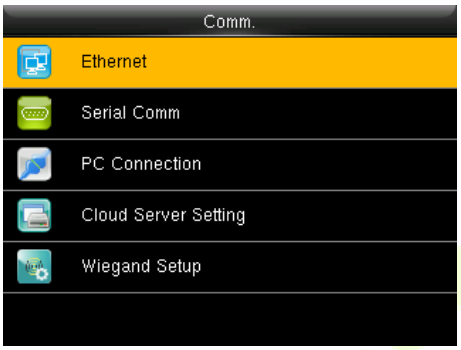




Note: If the User Role is enabled for the device, go on **User Mgt. > New User > User Role** to assign the created roles to the required users. But if there is no super administrator registered in the device, then the device will prompt "**Please enroll super admin first!**" when enabling the User Role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

7 Communication Settings

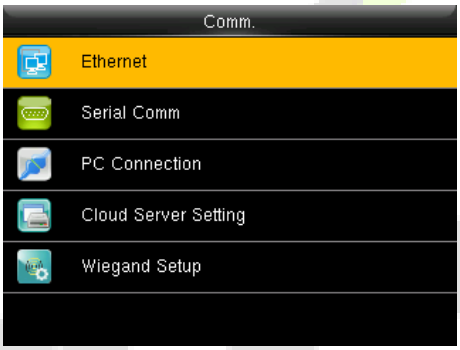
Press **M/OK** on the initial interface. Select **COMM.** and press **M/OK** to set the ethernet, serial communication, PC connection, cloud server, and Wiegand.

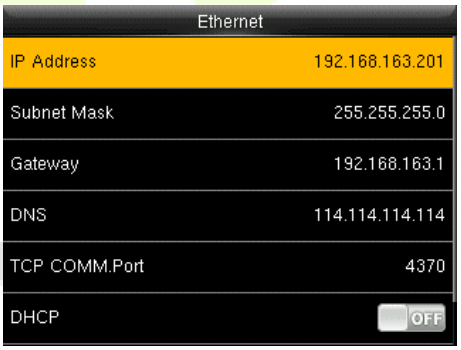


7.1 Ethernet Settings

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.

Select **Ethernet** on the **Comm.** interface and press **M/OK** to configure the settings.





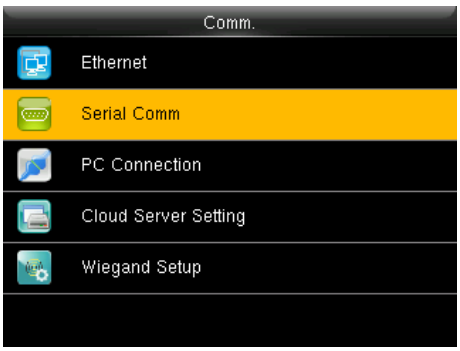
Function Description

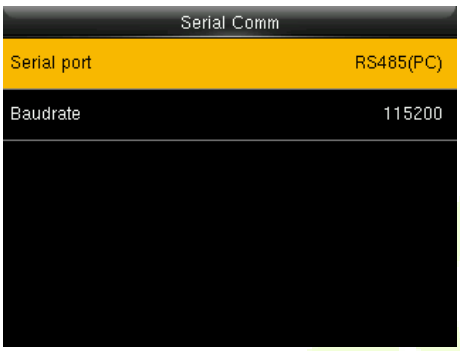
Function Name	Descriptions
IP Address	The default IP address is 192.168.1.201. It can be modified according to the network availability.
Subnet Mask	The default Subnet Mask is 255.255.255.0. It can be modified according to the network availability.
Gateway	The default Gateway address is 0.0.0.0. It can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

7.2 Serial Comm. Settings

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

Select **Serial Comm.** on the **Comm.** interface and press **M/OK**.





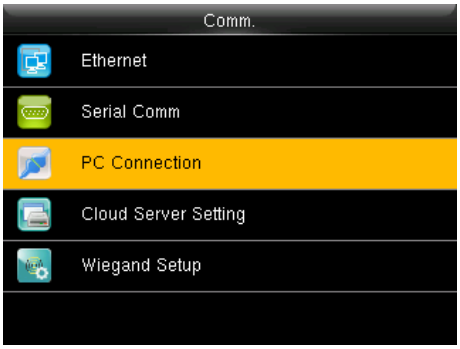
Function Description

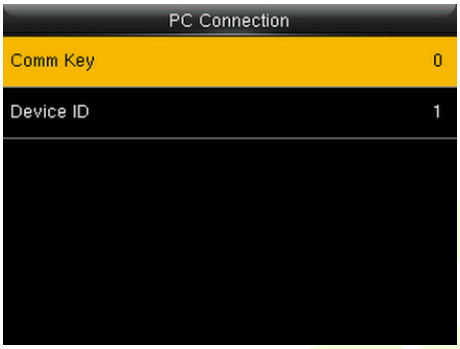
Function Name	Descriptions
Serial Port	**Disable:** Do not communicate with the device through the serial port. **RS485(PC):** Communicates with the device through RS485 serial port. **Master Unit:** When RS485 is used as the function of "**Master unit**", the device will act as a master unit, and it can be connected to RS485 fingerprint & card reader.
Baud Rate	The rate at which the data is communicated with PC, there are 5 options of baud rate: 115200 (default), 57600, 38400, 19200 and 9600. The higher is the baud rate, the faster is the communication speed, but also the less reliable. Hence, a higher baud rate can be used when the communication distance is short; when the communication distance is long, choosing a lower baud rate would be more reliable.

7.3 PC Connection

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

Select **PC Connection** on the **Comm.** interface and press **M/OK** to configure the communication settings.



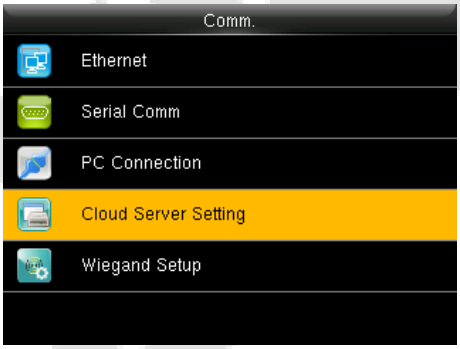


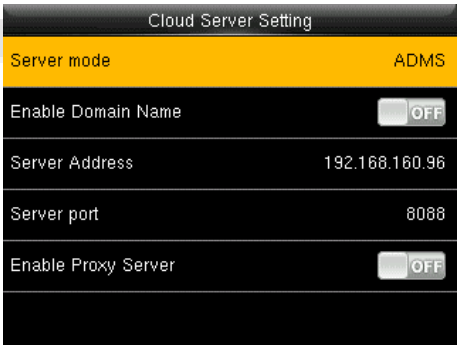
Function Description

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

7.4 Cloud Server Setting

Select **Cloud Server Setting** on the **Comm.** interface and press **M/OK** to connect with the ADMS server.





Function Description

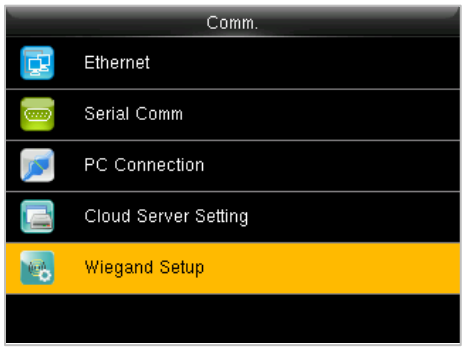
Function Name		Description
Enable Domain Name	**Server Address**	Once this mode is turned **ON**, the domain name mode "http://..." will be used, such as http://www.XYZ.com, while "XYZ" denotes the domain name.
Disable Domain Name	**Server Address**	The IP address of the ADMS server.
	Server Port	Port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

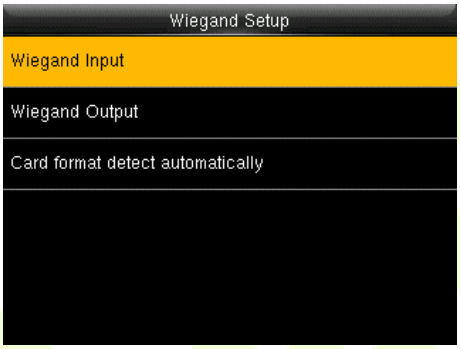
Note: When the Web server is connected successfully, the main interface will display the logo.

7.5 Wiegand Setup

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

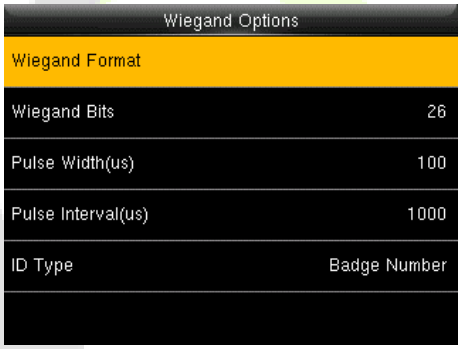
Select **Wiegand Setup** on the **Comm.** interface and press **M/OK** to set the Wiegand input and output parameters.





7.5.1 Wiegand Input

Select **Wiegand Input** on the **Wiegand Setup** interface and press **M/OK**



Function Description

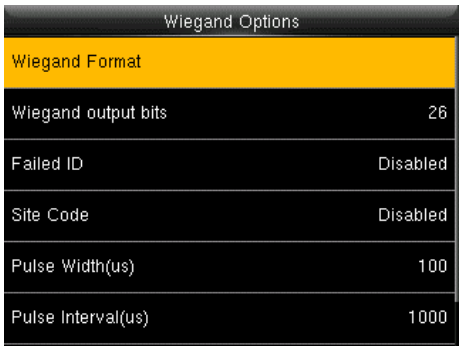
Function Name	Descriptions
Wiegand Format	Its value can be 26 bits, 34 bits, 36 bits, 37 bits, and 50 bits.
Wiegand Bits	The number of bits of the Wiegand data.
Pulse Width (us)	The value of the pulse width sent by Wiegand is 100 microseconds by default, which can be adjusted within the range of 20 to 100 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.

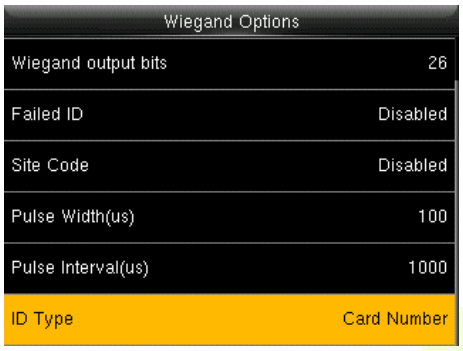
Various Common Wiegand Format Description

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 is the card numbers.
Wiegand26a	ESSSSSSSSCCCCCCCCCCCCCCCCO 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	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO 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 is the card numbers.
Wiegand34a	ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCO 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	OFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME 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	EFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCO 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	OMMMMSSSSSSSSSSSCCCCCCCCCCCCCCCCCCE 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	ESSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO 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.	

7.5.2 Wiegand Output

Select **Wiegand Output** on the **Wiegand Setup** interface and press **M/OK**



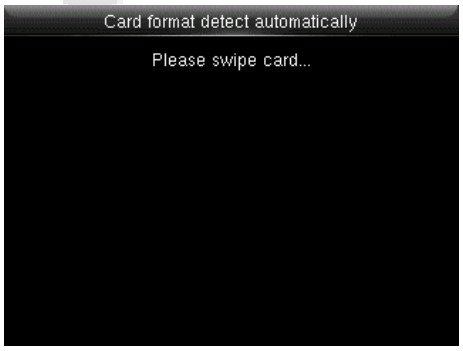


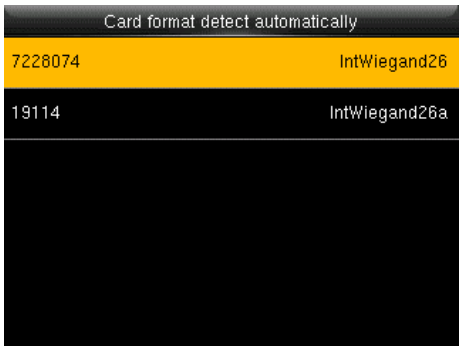
Function Description

Function Name	Descriptions
SRB	When SRB is enabled, the lock is controlled by the SRB to prevent the lock from opening due to device removal.
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 of 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.

7.5.3 Card Format Detect Automatically

Select **Card format detect automatically** on the **Wiegand Setup** interface and press **M/OK**. Swipe a card to get the card format.

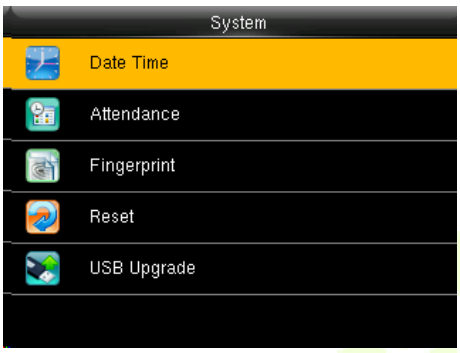




8 System Settings

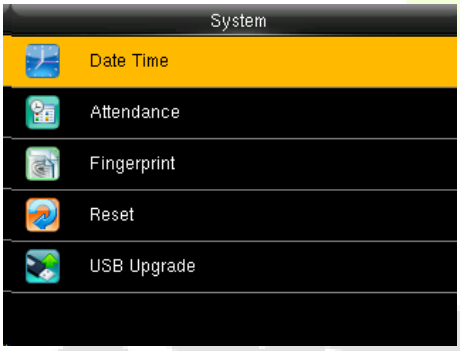
It helps to set related system parameters to optimize the accessibility of the device.

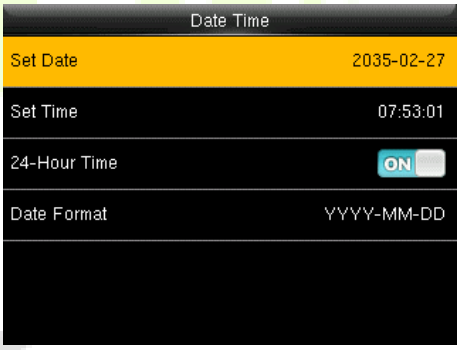
Press **M/OK** on the initial interface. Select **System** and press **M/OK** to get into its menu options.



8.1 Date and Time

Select **Date Time** on the **System** interface and press **M/OK** to set the date and time.



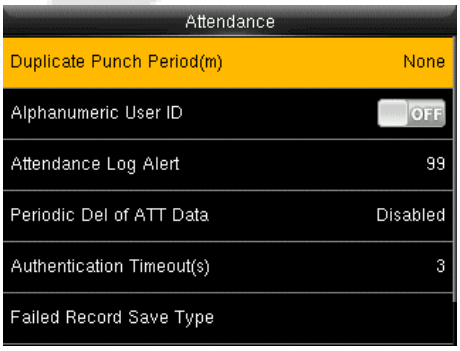


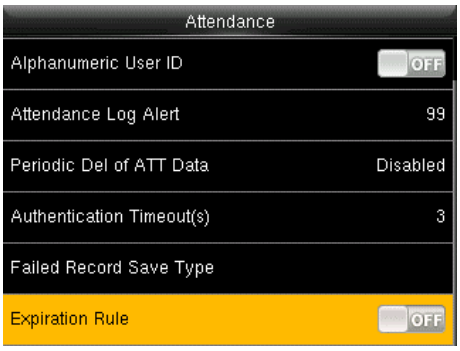
Select **Set Date** or **Set Time** and press **M/OK** to input date and time.

Select **24-Hour Time** and press **M/OK** to enable or disable this format. If enabled, then select the **Date Format** to set the date format i.e., the way date should be displayed on the device.

8.2 Attendance

Select **Attendance** on the **System** interface and press **M/OK**.



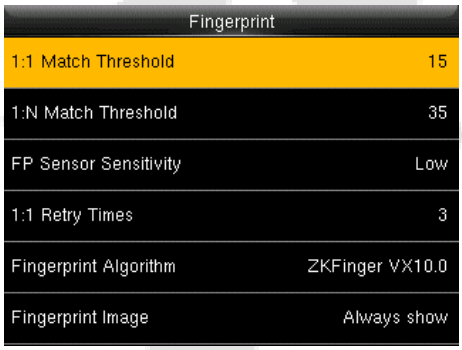


Function Description

Function Name	Description
Duplicate Punch Period (m)	Within a set time period (unit: minutes), the duplicate attendance logs will not be saved (value ranges from 1 to 999999 minutes). When the value is set to None, all the duplicate attendance logs will be saved.
Alphanumeric User ID	Whether to support letters in employee ID.
Attendance Log Alert	When the remaining storage becomes lesser than the set value, the device will automatically alert users about the remaining storage information. It can be disabled or set to a value ranged from 1 to 9999.
Periodic Det of ATT Date	When attendance photos reach its maximum capacity, the device automatically deletes a set of old attendance photos. Users may disable the function or set a valid value between 1 and 99.
Authentication Timeout(s)	The amount of time taken to display a successful verification message. Valid value: 1 to 9 seconds.
Failed Record Save Type	There are four failed record types to choose from, such as 1:N verification failed records, 1:1 verification failed records, invalid time period records and invalid group records.
Expiration Rule	Whether to enable the expiration rule. If yes, conduct the expiration settings, including: retaining user information, and not saving attendance record; retaining user information, and saving attendance record; and deleting user information.

8.3 Fingerprint Parameters

Select **Fingerprint** on the **System** interface and press **M/OK**.



FRR	FAR	Recommended matching thresholds	
		1:N	1:1
High	Low	45	25
Medium	Medium	35	15
Low	High	25	10

Function Description

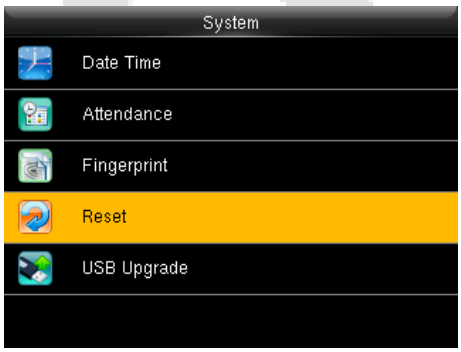
Function Name	Descriptions
1:1 Match Threshold	Under 1:1 verification method, the verification will only be successful when the similarity between the acquired fingerprint data and the fingerprint template associated with the entered user ID enrolled in the device is greater than the set value.

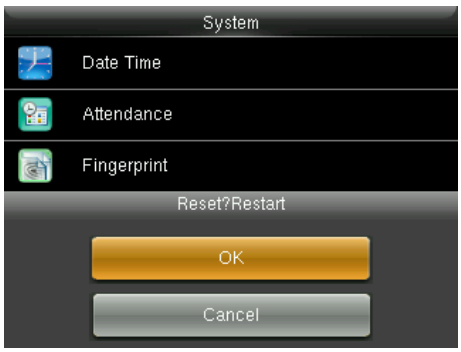
1:N Match Threshold	Under 1:N verification method, the verification will only be successful when the similarity between the acquired fingerprint data and the fingerprint templates enrolled in the device is greater than the set value.
FP Sensor Sensitivity	To set the sensibility of fingerprint acquisition. 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 Algorithm	To switch the fingerprint algorithm versions.
Fingerprint Image	This function is disabled by default. After disabling it, the fingerprint image will not be displayed when registering and verifying fingerprints. The menu interface allows to enable or disable this function, and there are security prompts when switching. 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.

8.4 Factory Reset

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

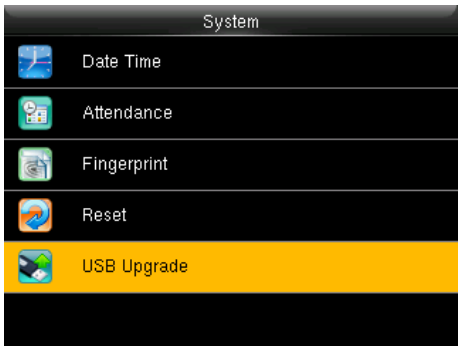
Select **Reset** on the **System** interface and press **M/OK** to restore the default factory settings.





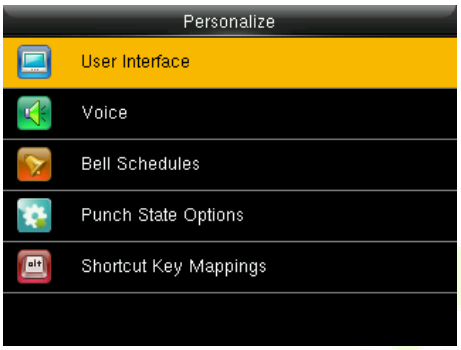
8.5 USB Upgrade

Insert the U disk with the upgrade file into the device's USB port, select **USB Upgrade** on the **System** interface and press **M/OK** to complete firmware upgrade operation.



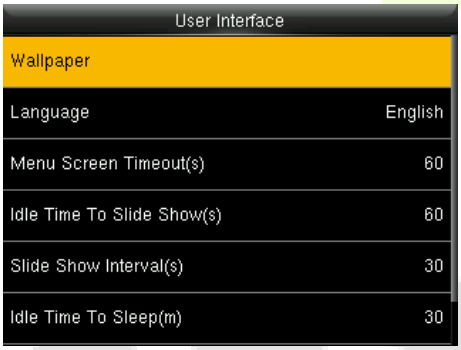
9 Personalize Settings

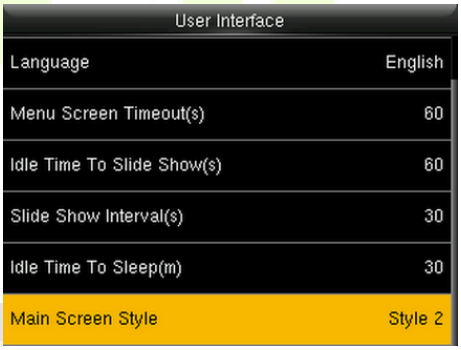
Press **M/OK** on the initial interface. Select **Personalize** and press **M/OK** to customize interface settings, voice, bell, punch state options, and shortcut key mappings.



9.1 Interface Settings

Select **User Interface** on the **Personalize** interface and press **M/OK** to customize the display style of the main interface.



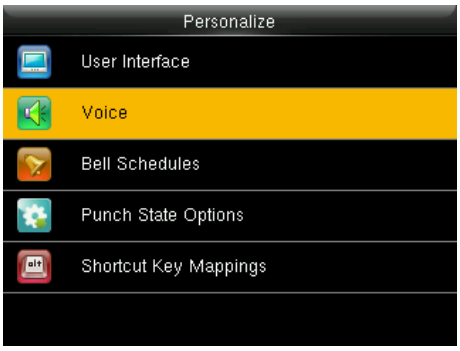


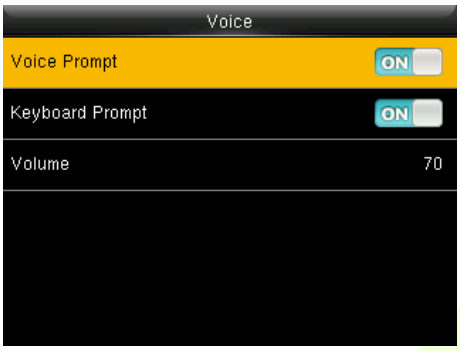
Function Description

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.

9.2 Voice Settings

Select **Voice** on the **Personalize** interface and press **M/OK** to configure the voice settings.



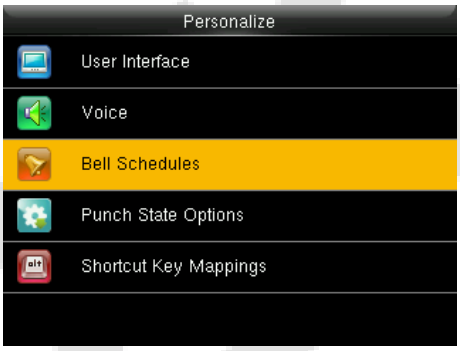


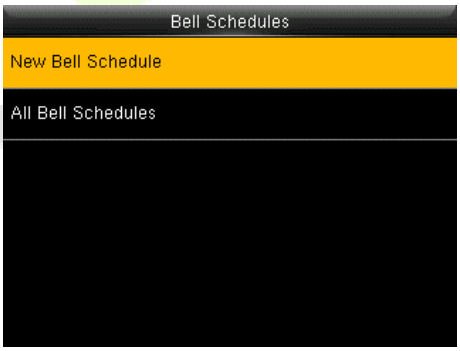
Function Description

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

9.3 Bell Schedules

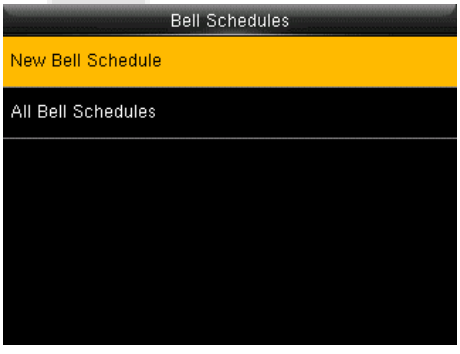
Select **Bell Schedules** on the **Personalize** interface and press **M/OK** to configure the Bell settings.

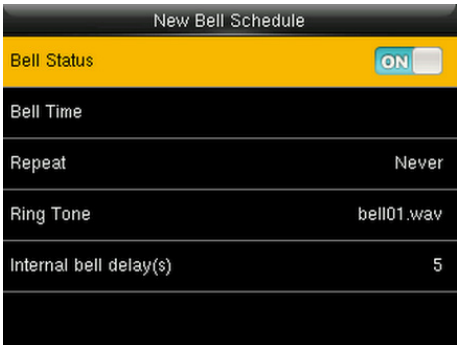




- **New Bell Schedule**

Select **New Bell Schedule** on the **Bell Schedule** interface and press **M/OK** 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, select **All Bell Schedules** and press **M/OK** to view the newly scheduled bell.

- **Edit the Scheduled Bell**

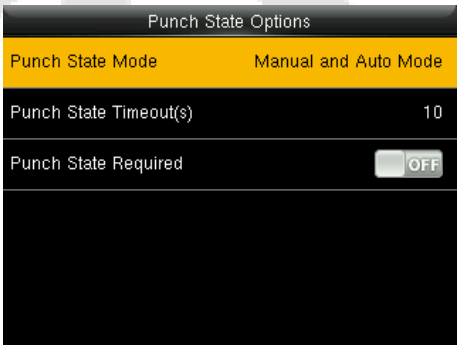
On the **All Bell Schedules** interface, select a required bell schedule and press **M/OK**. Then, select **Edit** and press **M/OK** to edit the selected bell schedule. The editing method is the same as the operations of adding a new bell schedule.

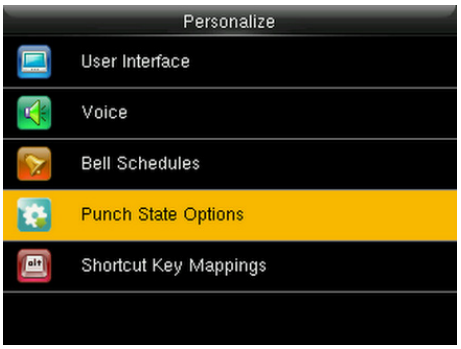
- **Delete a Bell**

On the **All Bell Schedules** interface, select a required bell schedule and press **M/OK**. Then, select **Delete** and press **M/OK** to delete the selected bell.

9.4 Punch States Options

Select **Punch State Options** on the **Personalize** interface and press **M/OK** to configure the punch state settings.





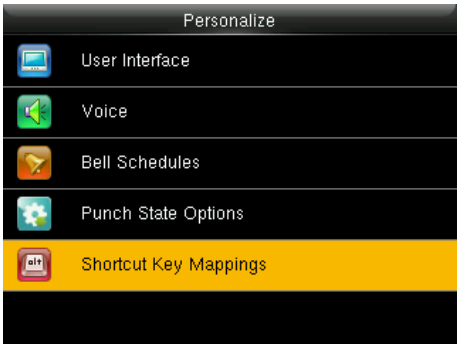
Function Description

Function Name	Description
Punch State Mode	Select a punch state mode, which can be: **Off:** It disables the punch state function. And the punch state key set under the **Shortcut Key Mappings** menu becomes 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 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 an alternative that is the manual attendance status. After the timeout, the manual switching punch state key will become an 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 manually switched again. **Fixed Mode:** Only the manually fixed punch state key is shown. Users cannot change the status by pressing any other keys.
Punch State Timeout (s)	It is the amount of time for which the punch state is displayed. The value ranges from 5~999 seconds.
Punch State Required	To choose whether an attendance state needs to be selected during verification.

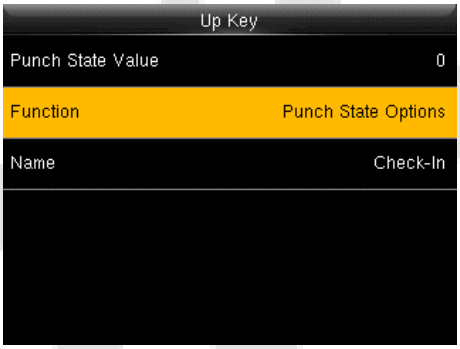
9.5 Shortcut Keys Mappings

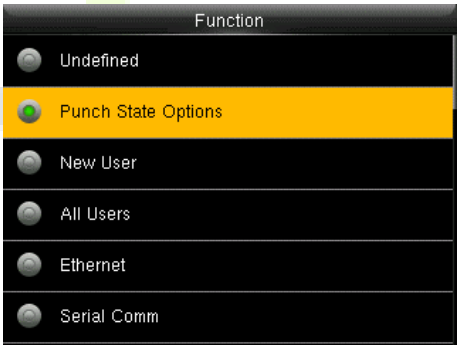
Users may define shortcut keys for attendance status and functional keys on the main interface. So, on the main interface, when the shortcut keys are pressed, the corresponding attendance status or the function interface displays directly.

Select **Shortcut Key Mappings** on the **Personalize** interface and press **M/OK** to set the required shortcut keys.



- On the **Shortcut Key Mappings** interface, select a required shortcut key and press **M/OK** to configure the shortcut key settings.
- On the **Shortcut Key** ("Up Key") interface, select **function** and press **M/OK** 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 done as shown in the image below.

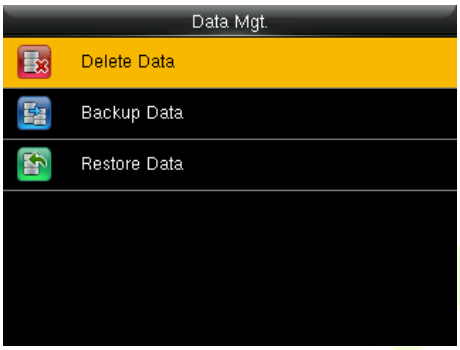




- If the Shortcut key is set as a punch state key (such as check-in, check-out, etc.), then it is required to set the punch state value (valid value 0~250), name, and switch time.

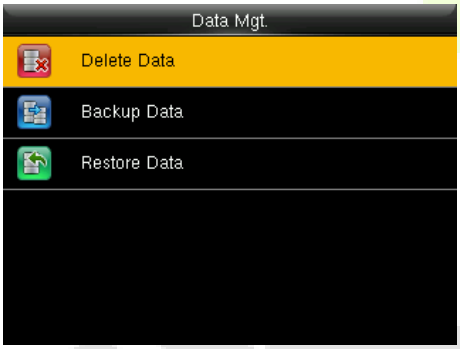
10 Data Management

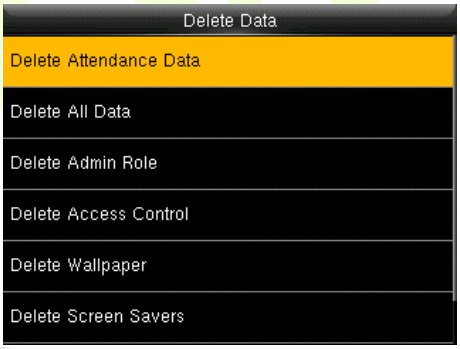
Press **M/OK** on the initial interface. Select **Data Mgt.** and press **M/OK** to delete the relevant data in the device.



10.1 Delete Data

Select **Delete Data** on the **Data Mgt.** interface and press **M/OK** to delete the required data.

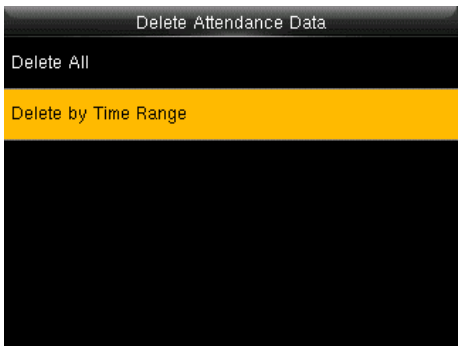




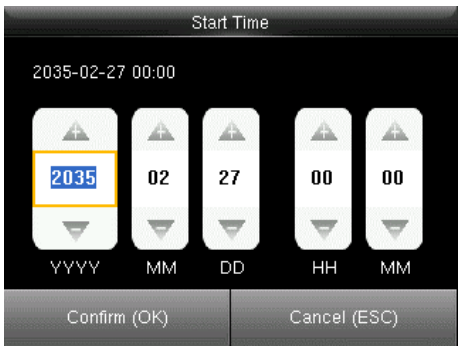
Function Description

Function Name	Description
Delete Attendance Data	To delete all attendance data in the device.
Delete All Data	To delete information and attendance logs/access records of all registered users.
Delete Admin Role	To remove all administrator privileges.
Delete Access Control	To delete all access data.
Delete Wallpaper	To delete all wallpapers in the device.
Delete Screen Savers	To delete the screen savers in the device.

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



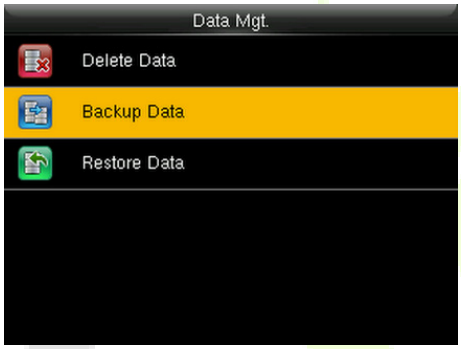
Select Delete by Time Range



Set the time range and click **OK**

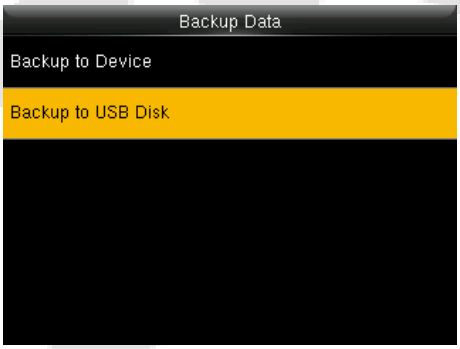
10.2 Data Backup

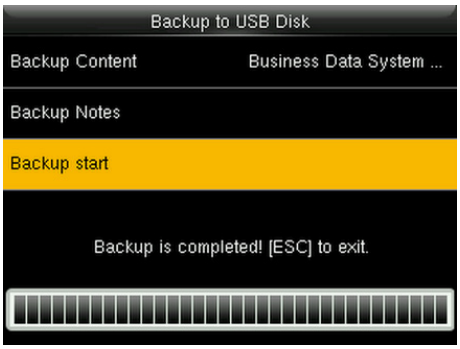
Select **Backup Data** on the **Data Mgt.** interface and press **M/OK** to back up the business data, or configuration data to the device or USB disk.



Select **Backup to Device** (or **Backup to USB Disk**) on the **Backup Data** interface and press **M/OK.**

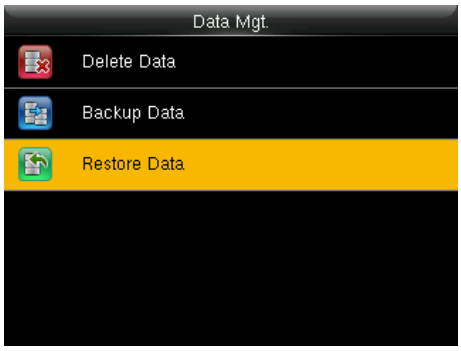
Select **Backup Content** and press **M/OK** to choose content to be backed up, and then select **Backup Start** to start backup. Restarting the device is not needed after backup is completed.





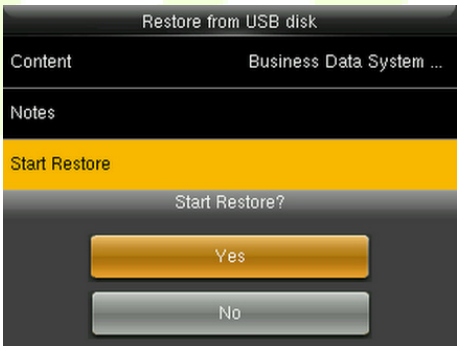
10.3 Data Restoration

Select **Restore Data** on the **Data Mgt.** interface and press **M/OK** to restore the data in the device or USB disk to the device.



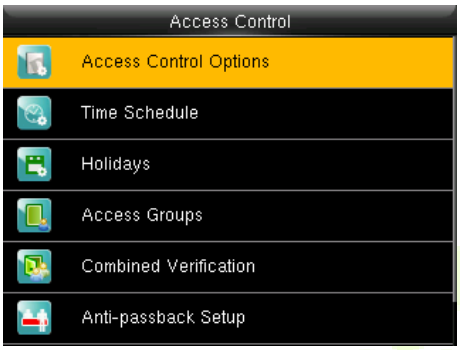
Select **Restore from Device** (or **Restore from USB disk**) on the **Restore Data** interface and press **M/OK.**

Select **Content** and press **M/OK** to choose content to be restored, and then select **Start Restore** to start restore.



11 Access Control

Press **M/OK** on the initial interface. Select **Access Control** and press **M/OK** to set the schedule of the door opening, locks control and to configure other parameters settings related to access control.

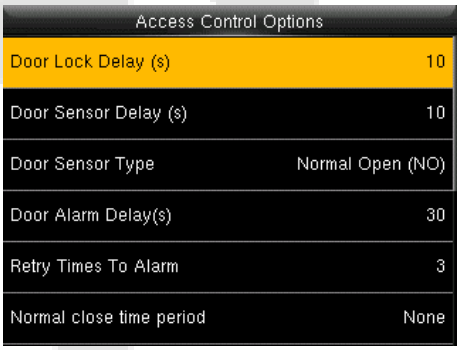


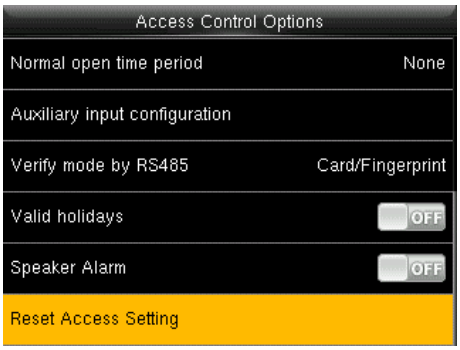
To gain access, the registered user must meet the following conditions:

- The relevant door's current unlock time should be within any valid time zone of the user's time period.
- 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).
- 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.

11.1 Access Control Options

Select **Access Control Options** on the **Access Control** interface and press **M/OK** to set the parameters of the control lock of the terminal and related equipment.





Function Description

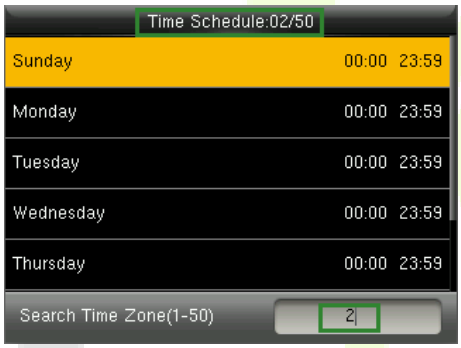
Function Name	Description
Door Lock Delay (s)	The length of time that the device controls the electric lock to be in unlock state. Valid value: 1~10 seconds; 0 seconds represents disabling the function.
Door Sensor Delay (s)	If the door is not locked and is left open for a certain duration (Door Sensor 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.
Door Alarm Delay(s)	When the state of the door sensor is inconsistent with that of the door sensor type, alarm will be triggered after a time period; this time period is the Door Alarm Delay (the value ranges from 1 to 999 seconds).
Retry Times to Alarm	When the number of failed verification reaches the set value (value ranges from 1 to 9 times), the alarm will be triggered. If the set value is none, the alarm will not be triggered after failed verification.
Normal Close Time Period	It is used to set a time period for Normally Closed mode, so that no one can gain access during this period.
Normal Open Time Period	It is used to set a time period for Normally Open, so that the door is always unlocked during this period.
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.
Verify Mode by RS485	The verification mode is used when the device is used either as a host or slave. The supported verification mode includes Card only, and Card + Password.
Valid holidays	It will set if **NC Time Period** or **NO Time Period** settings are valid in set holiday time period. Choose **[ON]** to enable the set **NC** or **NO** time period in holiday.
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.

11.2 Time Schedule

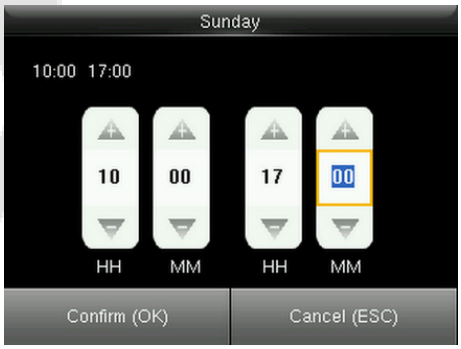
Select **Time Schedule** on the **Access Control** interface and press **M/OK** to configure the time settings.

- The entire system can define up to 50 Time Periods.
- Each time-period represents **10** Time Zones, i.e., **1** week and **3** holidays, and each time zone is a standard 24 hour period per day and the user can only verify within the valid time-period.
- One can set a maximum of 3 time periods for every time zone. The relationship among these time-periods is "**OR**". Thus, when the verification time falls in any one of these time-periods, the verification is valid.
- The Time Zone format of each time-period is **HH MM-HH MM**, which is accurate to minutes according to the 24-hour clock.

Press number button and then press **M/OK** 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, select the required day (that is Monday, Tuesday, etc.) and press **M/OK** to set the time.



Specify the start and the end time, and then press **M/OK**.

Note:

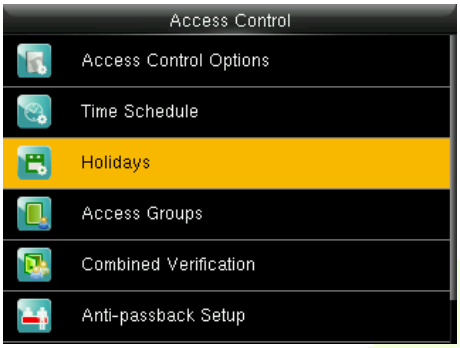
- The door is inaccessible for the whole day when the End Time occurs before the Start Time (such as **23:57~23:56**).
- It is the time interval for valid access when the End Time occurs after the Start Time (such as **08:00~23:59**).

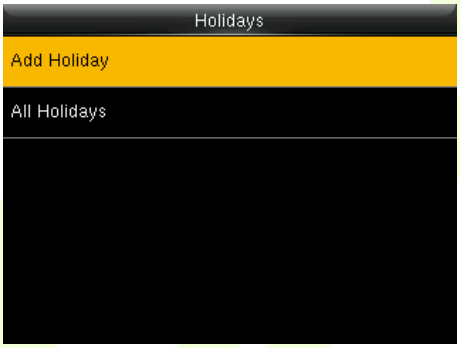
- The door is accessible for the whole day when the End Time occurs after the Start Time (such that Start Time is **00:00** and End Time is **23:59**).
- The default Time Zone 1 indicates that the door is open all day long.

11.3 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.

Select **Holidays** on the **Access Control** interface and press **M/OK** to set the Holiday access.





- **Add a New Holiday**

Select **Add Holiday** on the **Holidays** interface and press **M/OK** to set the holiday parameters.

- **Edit a Holiday**

On the **All Holidays** interface, select a holiday item and press **M/OK**. Then select **Edit** to modify holiday parameters.

- **Delete a Holiday**

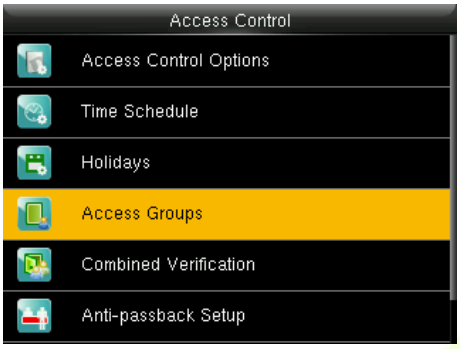
On the **All Holidays** interface, select a holiday item and press **M/OK**. Then select **Delete** to confirm the deletion. After deletion, this holiday does not display on the **All Holidays** interface.

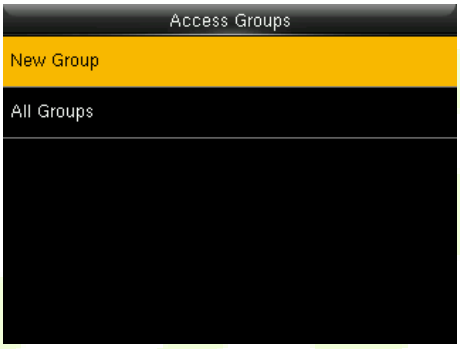
11.4 Access Group Settings

Grouping is to manage users in groups. Group users' default time zone is set to be the group time zone, while users can set their personal time zone. Each group can have 3 time periods at most, the user should verify in any one of the time period to get the access.

By default, newly enrolled users will be added to Access Group 1, but can be moved/added to other access group.

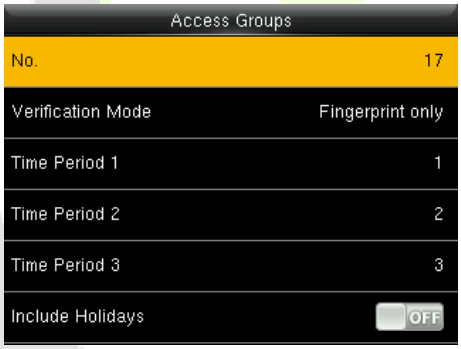
Select **Access Group** on the **Access Control** interface and press **M/OK** to set the group.





- **Add a New Group**

Select **New Group** on the **Access Groups** interface and press **M/OK** to set the group parameters.



- **To Enable Holiday Function**

Select **Include Holidays** on the **Access Groups** interface and press **M/OK** to turn the access group ON.

Note:

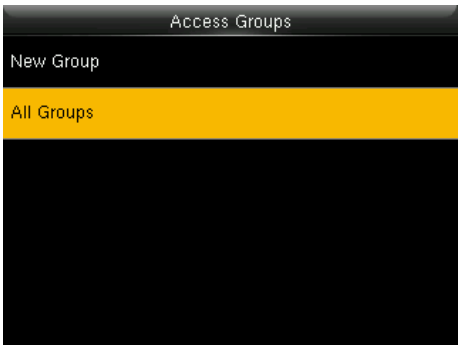
1. When the Holiday function is enabled, the members can gain access only when the time schedules of access group have included the holiday.
2. If the Holiday function is disabled, the access time of users in an access group will not be affected.

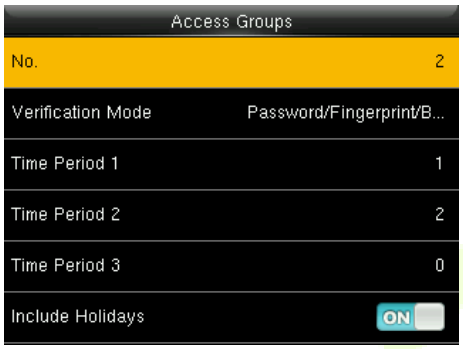
For Example: If Access Group 2 requires to use Holiday Time Schedule 2 on International Worker's Day, to let users gain access during 10:00 ~ 17:00 (Time Schedule 2) from May 1 to 3.

- **Operating Method**

1. Set Time Period 2 as 10:00 ~ 17:00 from Sunday to Saturday. For the setting method, please refer to the example of setting Time Zone 2 in 9.2 Time Schedule.
2. Use Time Period 2 for holiday. For method of setting holiday, please refer to 9.3 Holidays.

3. For setting access group, please refer to 9.4 Access Group Settings for instruction.
4. Enable Holiday function: Select **All Groups** on the **Access Groups** interface and press **M/OK**. Then, select **Edit** on the **Access Groups** interface and press **M/OK**, and select **Include Holidays** and press **M/OK** to turn the access group ON.





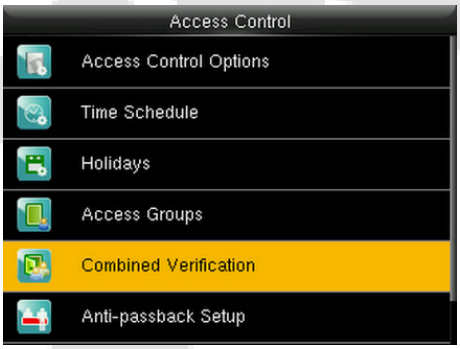
Note: If a holiday is to be valid for all users, allocate all users to the same group or enable the **Include Holidays** for all access groups.

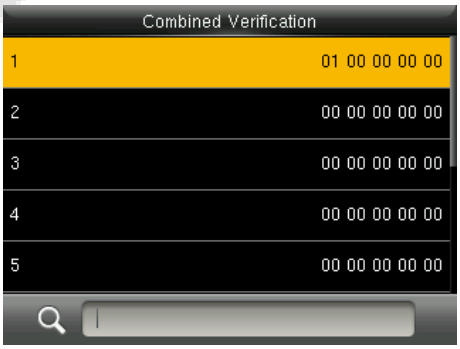
11.5 Combined Verification

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.

Select **Combined Verification** on the **Access Groups** interface and press **M/OK** to configure the combined verification setting.





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

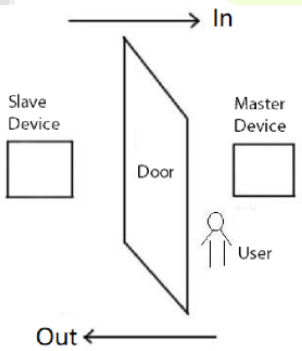
Note: To delete the door-unlock combination, set all Door-unlock combinations to 0.

11.6 Anti-passback Setup

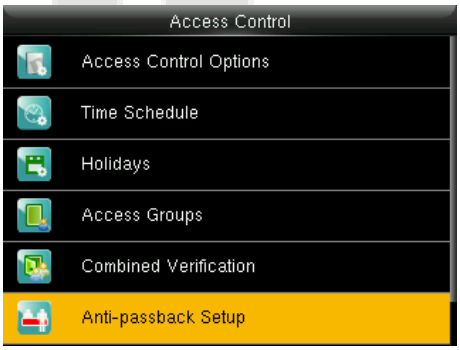
A user may be followed by some person(s) to enter the door without verification, resulting in a security breach. So, to avoid such situations, the Anti-Passback option was developed. Once it is enabled, the check-in and check-out record must occur alternatively to open the door to represent a consistent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

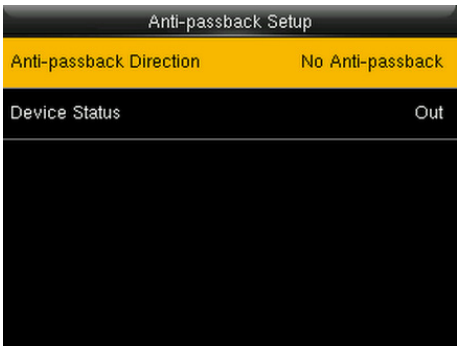
This function requires two devices to work together:

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.



Select **Anti-Passback Setup** on the **Access Control** interface and press **M/OK**.





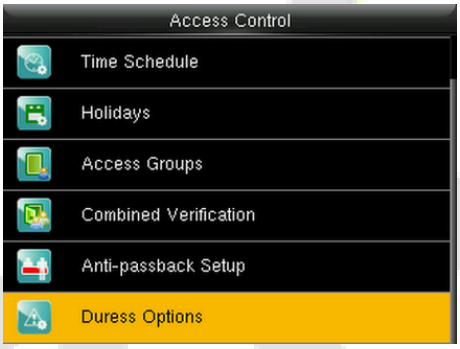
Function Description

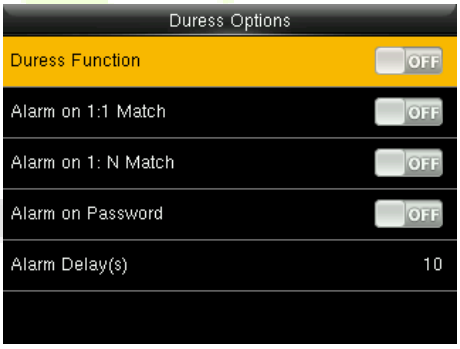
Function Name	Description
Anti-passback Direction	**No Anti-Passback:** The Anti-Passback function is disabled, which means successful verification through either the master device or slave device can unlock the door. The attendance state is not saved in this option. **Out Anti-Passback:** The user can 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. **Null and Save:** Anti-passback function is disabled, but attendance state is saved.

11.7 Duress Options Settings

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

On the **Access Control** interface, select **Duress Options** and press **M/OK** to configure the duress settings.





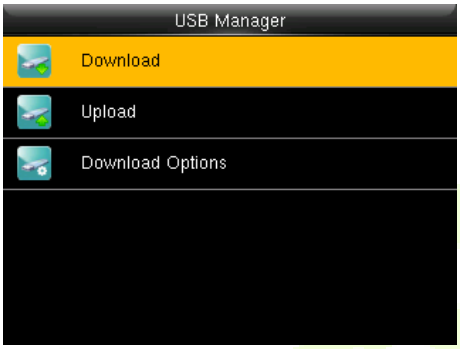
Function Description

Function Name	Description
Duress Function	In ON state, press "Duress Key" and then press any registered fingerprint (within 10 seconds), duress alarm will be triggered after successful verification. In OFF state, pressing "Duress Key" will not trigger the alarm.
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 on Password	When a user uses the password 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.

12 USB Manager

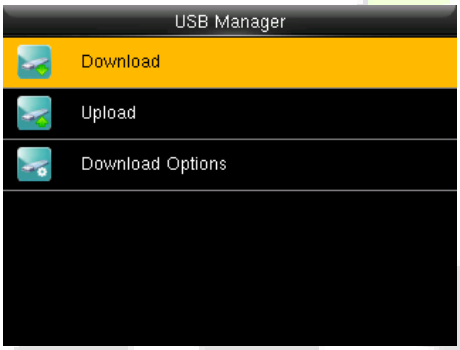
Press **M/OK** on the initial interface. Select **USB Manager** and press **M/OK** to Upload or download data between device and the corresponding software through a USB disk.

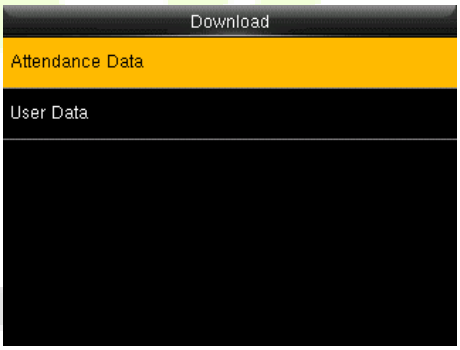
Note: Before uploading/downloading data from/to the USB disk, insert the USB disk into the USB slot first.



12.1 USB Download

On the **USB Manager** interface, select **Download** and press **M/OK**.



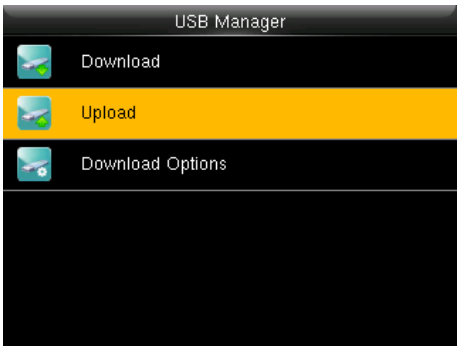


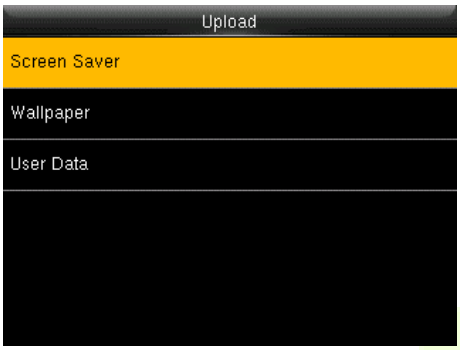
Function Description

Function Name	Description
Attendance Data	To download attendance data for a specific time period to USB disk.
User Data	To download all user information and fingerprints from the device to USB disk.

12.2 USB Upload

On the **USB Manager** interface, select **Upload** and press **M/OK**.



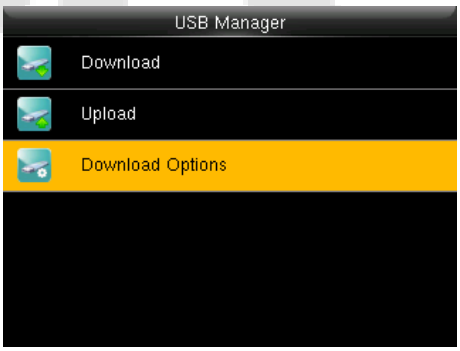


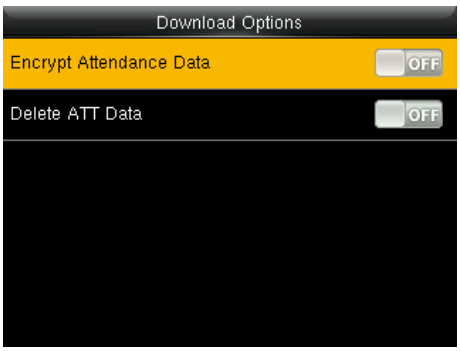
Function Description

Function Name	Description
Screen Saver	To upload all screen savers from USB disk to the device. You can select **Upload selected picture** or **Upload all pictures**. The images will be displayed in the device's main interface after the upload.
Wallpaper	To upload all wallpapers from USB disk to the device. You can select **Upload selected picture** or **Upload all pictures**. The images will be displayed in the device's main interface after the upload.
User Data	To upload all the user's information and fingerprints from USB disk to the device.

12.3 Download Options Settings

It is used to encrypt attendance data in the USB disk or delete attendance data. On the **USB Manager** interface, select **Download Options** and press **M/OK**.





Press **M/OK** to enable or disable the **Encrypt Attendance Data** and **Delete ATT Data** options.

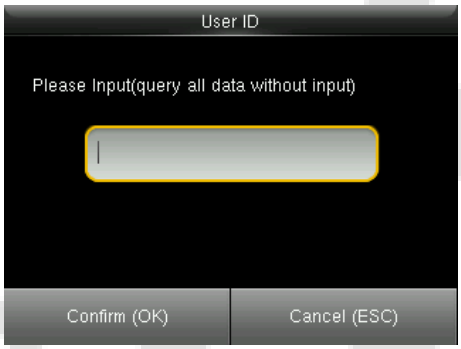
13 Attendance Search

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.

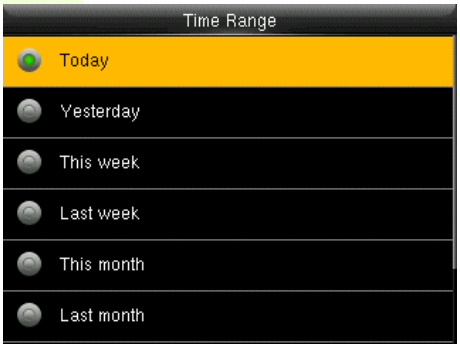
Select **Attendance Search** on the **Main Menu** interface and press **M/OK** to search for the required event Logs.

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

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

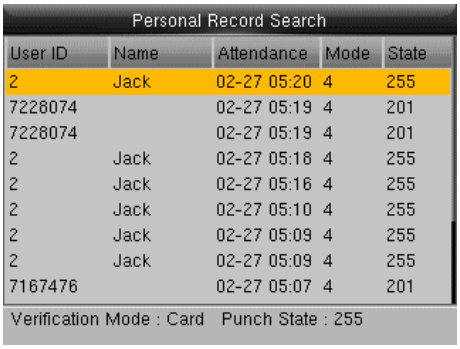


2. Select the time range in which the records need to be searched and press **M/OK**.



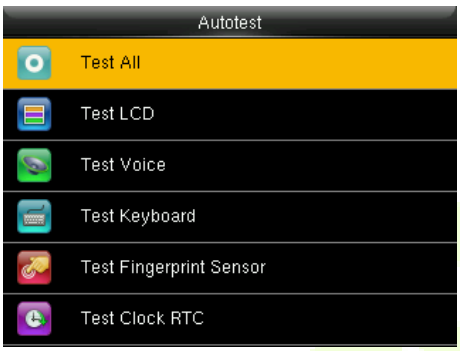
3. Once the record search completes. select the record highlighted in yellow and press **M/OK** to view its details.

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



14 Autotest

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

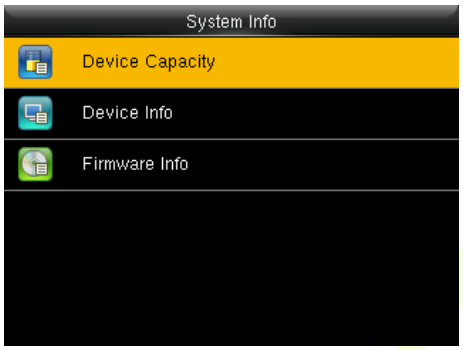


Function Description

Function Name	Description
Test All	To automatically test whether the LCD, audio, camera and 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.
Test Keyboard	To automatically test whether all keys are functioning properly or not.
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 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.

15 System Information

Select **System Information** on the **Main Menu** interface and press **M/OK** to view the storage status, the version information of the device, and firmware information.



Function Description

Function Name	Description
Device Capacity	Displays the current device's user storage, password, fingerprint, card storage, and ATT record.
Device Info	Displays the device's name, serial number, MAC address, fingerprint algorithm, platform information, MCU version and manufacturer.
Firmware Info	Displays the firmware version and other version information of the device.

16 Connect to ZKBioAccess IVS Software

16.1 Set the Communication Address

- **Device Side**

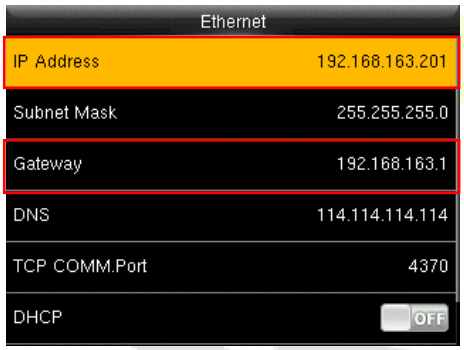
1. Press **M/OK** on the initial interface. Select **COMM.** and press **M/OK**. Then, select **Ethernet** on the **Comm.** Interface, press **M/OK** to set the IP address and gateway of the device.

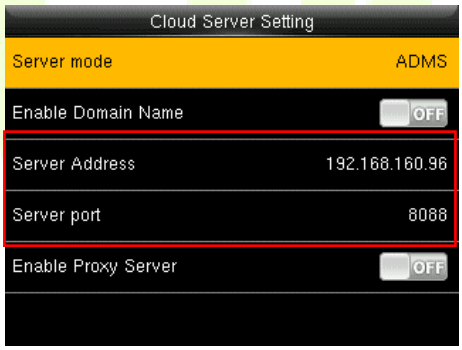
   (**Note:** The IP address should be able to communicate with the ZKBioAccess IVS server, preferably in the same network segment with the server address.)

2. Select **Cloud Server Setting** on the **Comm.** Interface and press **M/OK** to set the server address and server port.

   Server address: Set the IP address as of ZKBioAccess IVS server.

   Server port: Set the server port as of ZKBioAccess IVS (The default is 8088).





- **Software Side**

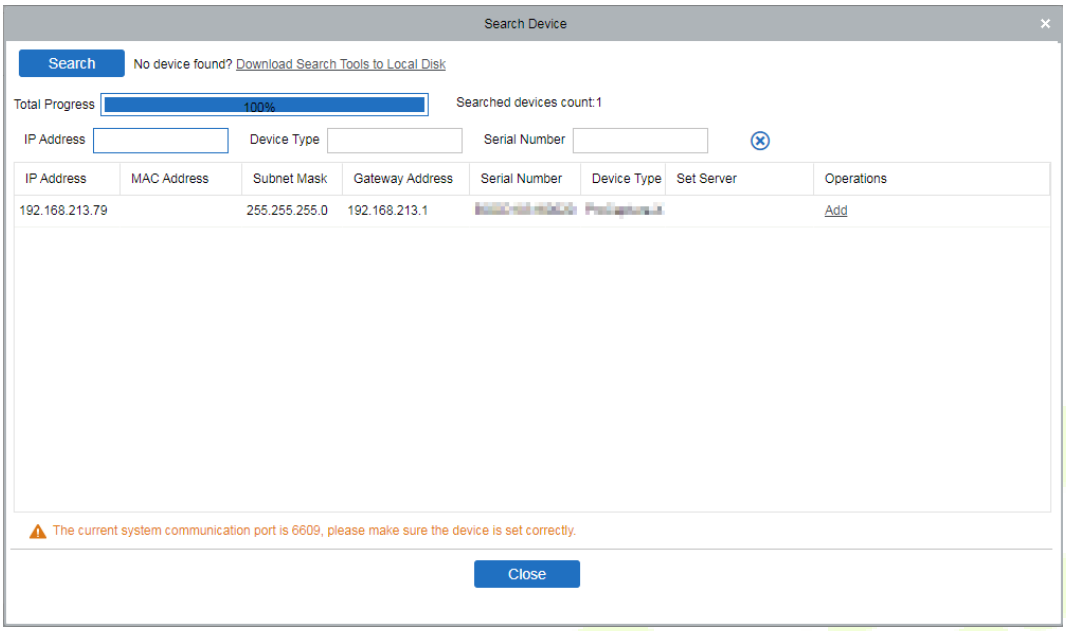
Login to ZKBioAccess IVS software, click **System** > **Communication** > **Communication Monitor** to set the ADMS service port, as shown in the figure below:

16.2 Add Device on the Software

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

1. Click **Access Control** > **Device** > **Search Device** to open the Search interface in the software.
2. Click **Search**, and it will prompt "**Searching**……".

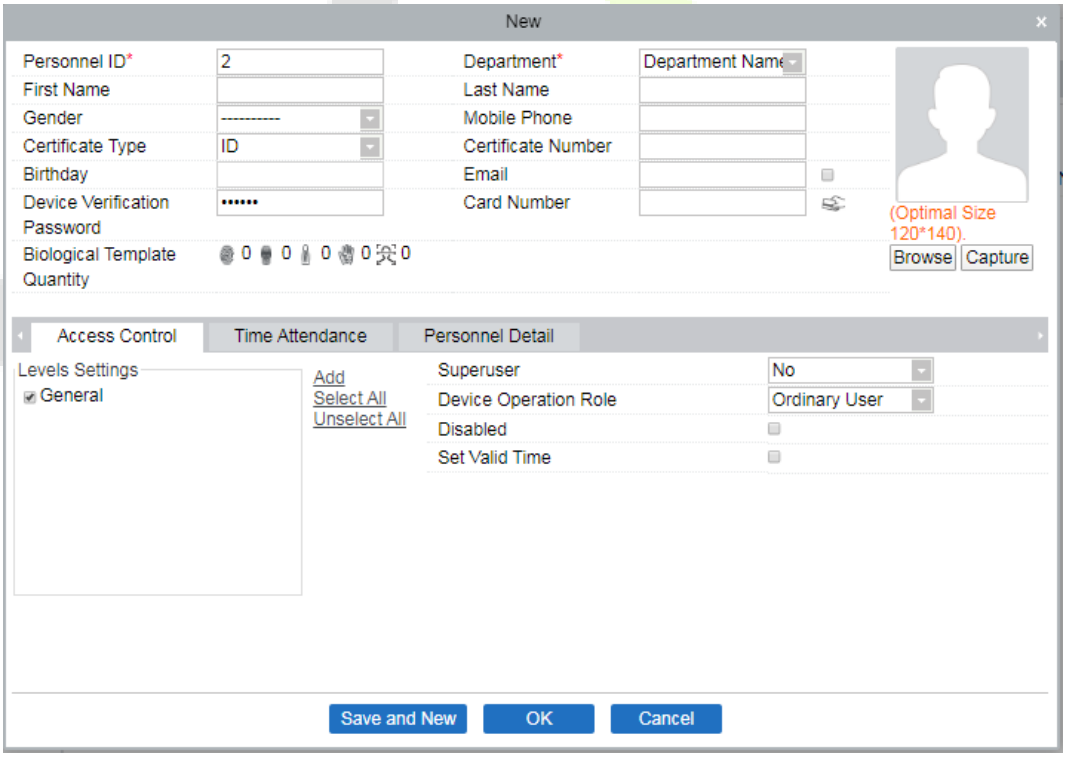
3. After searching, the list and total number of access controllers will be displayed.



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.

16.3 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 > Device Control > Synchronize All Data to Devices** to synchronize all the data to the device including the new users.

17 Connect to ZKBioTime 8.0 Software★

17.1 Set the Communication Address

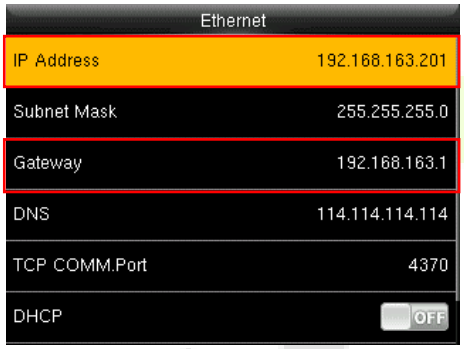
1. Press **M/OK** on the initial interface. Select **COMM.** and press **M/OK**. Then, select **Ethernet** on the **Comm.** Interface, press **M/OK** to set the IP address and gateway of the device.

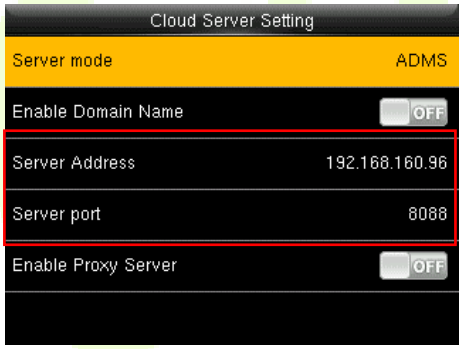
   (**Note:** The IP address should be able to communicate with the BioTime 8.0 server, preferably in the same network segment with the server address)

2. Select **Cloud Server Setting** on the **Comm.** Interface and press **M/OK** to set the server address and server port.

   Server address: Set the IP address as of BioTime 8.0 server.

   Server port: Set the server port as of BioTime 8.0 (The default is 8081).

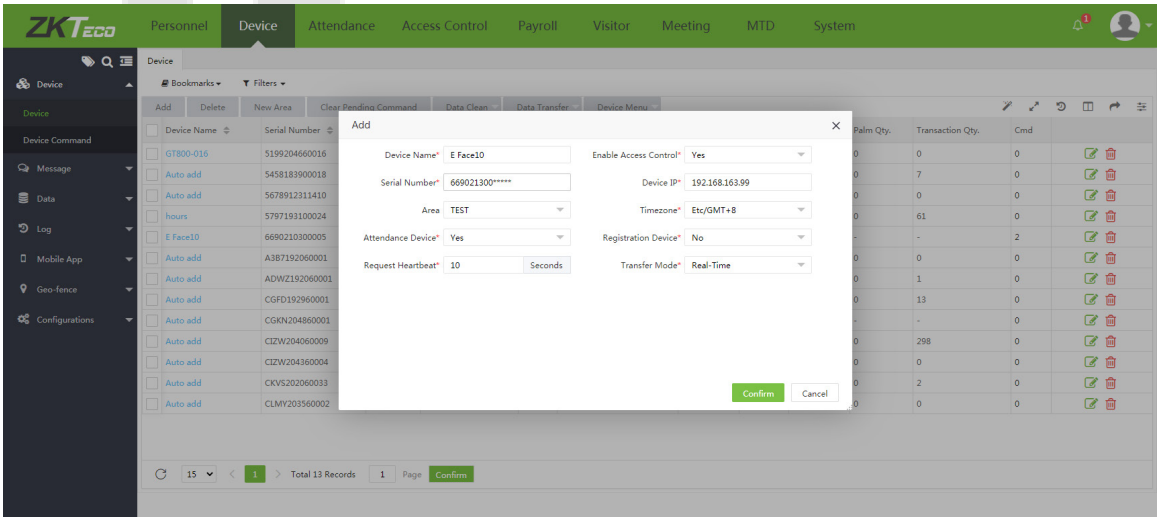




17.2 Add Device on the Software

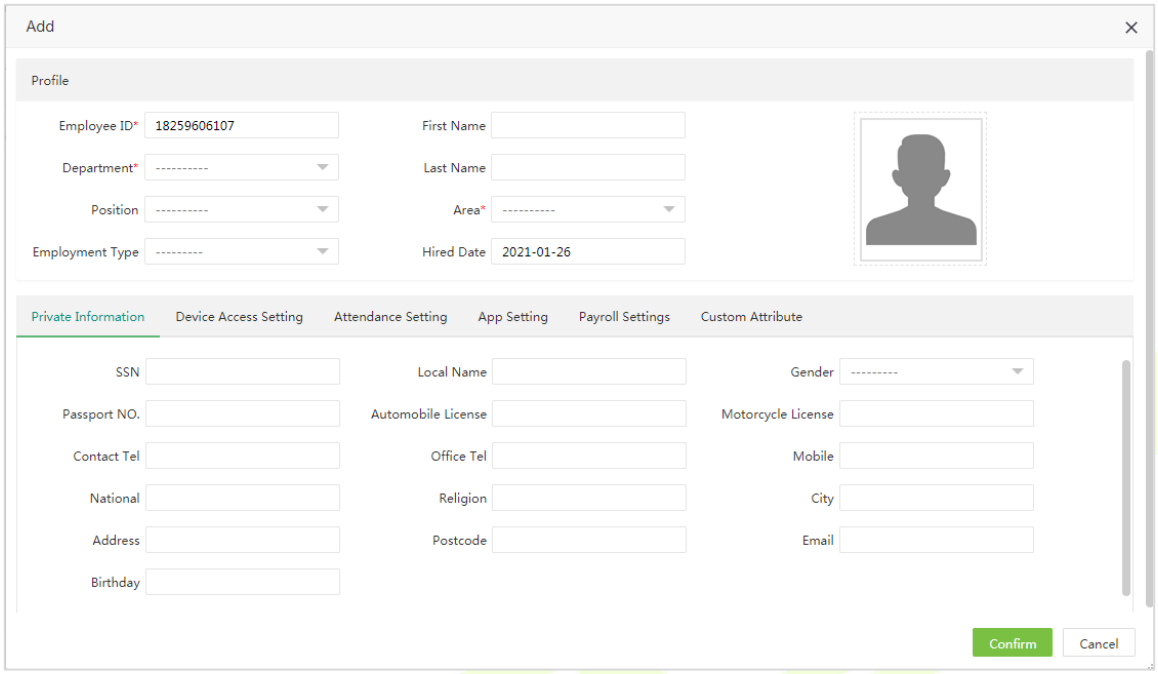
Add the device by searching. The process is as follows:

1. Click **Device** > **Device** > **Add**, to add the device on the software.
2. A new window pops-up on clicking **Add**. Enter the required information about the device and click **Confirm**, then the added devices are displayed automatically.



17.3 Add Personnel on the Software

1. Click **Personnel** > **Employee** > **Add**:



2. Fill in all the required fields and click **Confirm** to register a new user.

3. Click **Device** > **Device** > **Data Transfer** > **Sync Data to Device** to synchronize all the data to the device including the new users.

18 Troubleshooting

- **Fingerprint sensor can't read and verify the fingerprint effectively.**

  1. Check if the fingertip is wet, or the fingerprint sensor is wet or dusty.
  2. Clean the fingertip and the fingerprint sensor and try again.
  3. If the fingertip is too dry, blow air onto it and try again.

- **"Invalid time zone" is displayed after verification.**

  Contact Administrator to check if the user has the privilege to gain access within that time schedule.

- **Failed to gain access after successful verification.**

  1. Check whether the user privilege is set correctly.
  2. Check whether the lock wiring is correct.

- **The Tamper Alarm rings.**

  Check if the device and the back plate are fixed together properly; if not, the tamper switch on the back of the device will be triggered and raises an alarm. Warning sign ⚠ will be shown on the top right corner on the interface. To get the alarm sound, the speaker should be ON in setting **Access Control** > **Access Control Options** > **Speaker Alarm**.

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